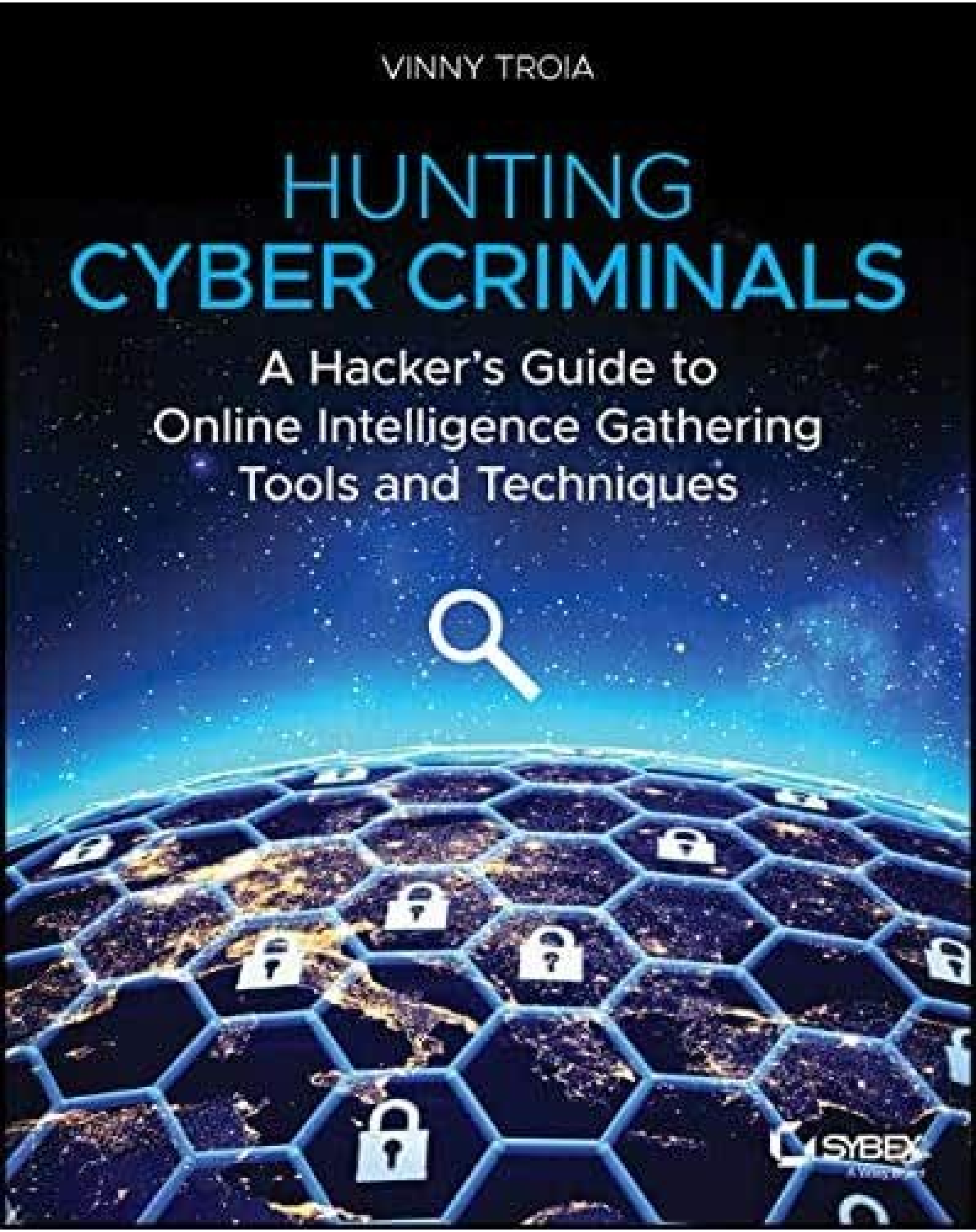
VINNY TROIA

HUNTING CYBER CRIMINALS

A Hacker's Guide to Online Intelligence Gathering Tools and Techniques



Охота на киберпреступников

Первод сделан специально для

лучшего кунала в Telegram

Max Open Source

Academy: Information technologies

(https://t.me/coursmax)

Альтруист и подпищик канала.

Также спасибо администрации проекта, за ваш вклад в IT.

Охота на киберпреступников

Руководство хакера по

Сбор информации в Интернете

Инструменты и методы

Винни Троя, доктор философии

Авторские права © 2020 by John Wiley & Sons, Inc., Индианаполис, Индиана
Издается одновременно в Канаде
ISBN: 978-1-119-54092-2
ISBN: 978-1-119-54089-2 (ebk)
ISBN: 978-1-119-54099-1 (ebk)
Произведено в Соединенных Штатах Америки.
Никакая часть этой публикации не может быть воспроизведена, сохранена в поисковой системе или передана в любой форме и любыми средствами.
электронные, механические, ксерокопирование, запись, сканирование или иное, за исключением случаев, разрешенных Разделами 107 или 108
Закона США об авторском праве 1976 г., без предварительного письменного разрешения Издателя или разрешения путем оплаты соответствующей пошлины за копию в Центр защиты авторских прав, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, факс (978) 646-8600. Запросы к Издателю о разрешении следует направлять Пер-Департамент миссий, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, факс (201) 748-6008, или на сайте http://www.wiley.com/go/permissions.
Предел ответственности / отказ от гарантии: издатель и автор не делают никаких заявлений или гарантий с в отношении точности или полноты содержания этой работы и, в частности, отказываемся от всех гарантий, включая без ограничения гарантии пригодности для определенной цели. Никакая гарантия не может быть создана или продлена продажей или
Промоматериалы. Приведенные здесь советы и стратегии могут не подходить для каждой ситуации. Эта работа продается с пониманием того, что издатель не занимается предоставлением юридических, бухгалтерских или иных профессиональных услуг
Сервисы. Если требуется профессиональная помощь, следует обратиться за помощью к компетентному специалисту. Nei-
ни издатель, ни автор не несут ответственности за убытки, возникшие в связи с этим. Тот факт, что организация или веб-сайт
упоминается в данной работе как ссылка и / или потенциальный источник дополнительной информации не означает, что автор
или издатель одобряет информацию, которую организация или веб-сайт может предоставить, или рекомендации, которые она может дать.
Кроме того, читатели должны знать, что интернет-сайты, перечисленные в этой работе, могли измениться или исчезнуть между
когда это произведение было написано и когда оно прочитано.
Для получения общей информации о других наших продуктах и услугах, пожалуйста, свяжитесь с нашим отделом обслуживания клиентов в
США по телефону (877) 762-2974, за пределами США по телефону (317) 572-3993 или по факсу (317) 572-4002.

Wiley издает материалы в различных печатных и электронных форматах, а также по запросу. Некоторые материалы включены в
стандартные печатные версии этой книги могут не входить в электронные книги или печататься по запросу. Если эта книга относится к СМИ
например, компакт-диск или DVD, который не включен в приобретенную вами версию, вы можете загрузить этот материал по адресу http: //
booksupport.wiley.com. Для получения дополнительной информации о продуктах Wiley посетите сайт www.wiley.com.
Контрольный номер Библиотеки Конгресса : 2019940773
Товарные знаки: Wiley и логотип Wiley являются товарными знаками или зарегистрированными товарными знаками John Wiley & Sons, Inc. и / или ее
аффилированными лицами в США и других странах, и их нельзя использовать без письменного разрешения. Вся остальная торговля-
товарные знаки являются собственностью их владельцев. John Wiley & Sons, Inc. не связана с каким-либо продуктом или поставщиком.
упоминается в этой книге.

Моей прекрасной дочери Арии и моей невероятной жене Джесс. Я никогда не понимал, что за радость стать отцом, и я благодарен каждый день, что у вас есть оба

подарил мне самый удивительный подарок в моей жизни.

об авторе

Винни Троя , доктор философии, CEH, CHFI, в настоящее время возглавляет службу Night Lion Security,
консалтинговая компания по кибербезопасности из Сент-Луиса, специализирующаяся на предоставлении первоклассных
этический взлом и услуги по управлению рисками.

Троя была признана идейным лидером в области кибербезопасности и стала эксперт по СМИ для обсуждения вопросов безопасности крупных корпоративных нарушение данных, кибер-закон и законодательство, взлом авиакомпаний и автомобилей, а также
кибер-скандалы.

Его опыт в области ИТ-безопасности проистекает из целой жизни программирования, сложной проблемы.
решения и самообучения на компьютере. Троя теперь путешествует по миру, выступая на
конференции и мероприятия, связанные с безопасностью, и большую часть своего свободного времени проводит на охоте
за утечку данных и проникновение в частные криминальные круги в даркве бе.

С каждым новым взломом остаются ценные подсказки относительно эволюции методы злоумышленника. Во время своих выступлений Троя использует эту информацию, чтобы
учить и информировать других о том, как усилить их защиту и поставить необходимые
наличие стратегий реагирования на случай возникновения инцидентов.

До запуска Night Lion Security Троя почти десять лет работала над
проекты, связанные с безопасностью и рисками, для Министерства обороны США.
Троя имеет докторскую степень в Университете Капеллы и является
сертифицированным этическим хакером.
и сертифицированный судебный следователь по взлому.
Для получения дополнительной информации, включая образцы выступлений Трои,
посетите сайт www.
.vinnytroia.com .
Вы также можете связаться с Винни в LinkedIn по адресу https://linkedin.com/in/.
vinnytroia или через Twitter по адресу http://www.twitter.com/vinnytroia .

О техническом редакторе

Риа Дансел проводит оценку информационной безопасности на всей
территории США.
Государства, уделяя особое внимание платформам OSINT и риск-
ориентированного управления с ключевыми
взаимодействия с Министерством обороны и частным сектором.
Технический и аналитический опыт Риа берет свое начало в химии.
степень, применяемая в фармацевтической промышленности более 15 лет. Риа
теперь поддерживает организации в их усилиях по внедрению средств
контроля безопасности и
достичь целей информационной безопасности с помощью нескольких
программ безопасности. Риа
также продолжает предоставлять технический вклад в проекты, основанные на
оценке рисков и безопасности.

Благодарности

Я хотел бы поблагодарить следующих людей:

Моя жена , за то, что мирилась с моими бесчисленными бессонными ночами и безостановочно
одержимость, пока я работал над разгадыванием этой головоломки.

Бев Робб , без тебя, я не думаю, что смог бы разгадать загадку.
тери TDO. Иногда самые случайные связи и обрывки информации
может привести к самым значительным открытиям, и именно это и произошло.

Большое вам спасибо за то, что вы терпели мои миллионы вопросов и поздно вечером
текстовые сообщения. Я бесконечно благодарен вам и надеюсь, что однажды смогу вернуть
услуга.

Кристоферу Менье , за то, что он никогда не отпускал легко узнаваемый чип на ваше плечо, которое безжалостно бормотало подобные заявления, давая мне все мотивация, на которую мне нужно было продолжать настаивать:
whitepacket@xmpp.is: Извини, чувак, но ты говоришь так, будто ты тоже LE или чертов дебил, наверное, последнее .

Деннис Карвуниарис , Спасибо за всю информацию и помощь, которую вы мне дали
путь. Мне жаль, что все так сложилось. Мне всегда нравятся наши чаты и надеюсь, что к тому времени, как вы это прочтете, вы примете мой совет.

Крис «Человек-хакер» Хэднаги за то, что поверил в меня достаточно, чтобы подключиться

я с хорошими людьми из Wiley, в конечном итоге заключив со мной сделку с этой книгой.

Алекс Хейд и Джесси Берк, за постоянную помощь и поддержку.
соединяя некоторые из этих частей вместе.

И всем приглашенным экспертам этой книги я не могу поблагодарить вас за добровольно-
уделите время тому, чтобы поделиться своими историями и мнениями для этой книги. я буду
буду давать вам все должные заслуги в первой главе, но я должен был дать вам всем должное
дополнительный крик и здесь.

---

xiii

краткое содержание

Пролог
XXV
Глава 1 Начало работы
1
Глава 2 Расследования и исполнители угроз
19
Часть I
Исследование сети
43 год
Глава 3 Ручное исследование сети
45
Глава 4 Поиск сетевой активности (расширенные методы NMAP)
67
Глава 5 Автоматизированные инструменты для обнаружения сети
83
Часть II
Веб-исследование
119
Глава 6 Сбор информации на веб-сайте
121
Глава 7 Поиск в каталоге
143
Глава 8.
159
Глава 9 WHOIS
175
Глава 10 Прозрачность сертификатов и Интернет-архивы
201
Глава 11 Iris от DomainTools
221
Часть III.
Копаем золото
243
Глава 12 Метаданные документа
245
Глава 13 Интересные места для поиска
267
Глава 14 Общедоступное хранилище данных

293
Охота на людей
323
Глава 15 Исследование людей, изображений и мест
325
Глава 16 Поиск в социальных сетях
349
Глава 17 Подсказки для отслеживания профиля и сброса пароля
377
Глава 18 Пароли, дампы и Data Viper
407
Глава 19 Взаимодействие с исполнителями угроз
433
Глава 20.
Взлом на 10 миллионов долларов
453
Эпилог
483
Показатель
487

СОДЕРЖАНИЕ

Пролог
XXV
Глава 1 Начало работы
1
Почему эта книга отличается
2
Что вы найдете и чего не найдете в этой книге
2
Знакомство с коллегами-экспертами
3
Примечание о криптовалютах
4
Что тебе нужно знать
4
Платные инструменты и исторические данные
5
А что насчет Мальтего?
5
Предпосылки
5
Знайте, как использовать и настраивать Linux
5
Получите ключи API по порядку
6
Важные ресурсы
6
OSINT Framework
6
OSINT.link
6
IntelТехники
7
Термбин
8

С пониманием
9
Списки слов и генераторы
9
SecLists
9
Cewl
10
Хруст
10
Прокси
10
Прокси-серверы Storm (с автоповоротом)
10
Криптовалюты 101
11
Как работают криптовалюты?
12
Исследователи блокчейнов
13

---

xvi Содержание
Следуя за деньгами
15
Выявление бирж и трейдеров
17
Резюме
18
Глава 2 Расследования и исполнители угроз
19
Путь следователя
19
Со щитом или на щите
20
Нарушение, которого никогда не было
21 год
Что бы вы сделали?
22
Моральные серые области
24
Различные следственные пути
25
Расследование киберпреступников
26 год
Начало охоты (для TDO)
27
Темный повелитель
27
Список жертв
28 год
Краткий обзор
29
Стиль общения
30
Структура и члены группы
30
Сайпер
31 год
Арни
32

Cr00k (пинг)
35 год
АНБ (душевное спокойствие)
36
Темный повелитель
38
Резюме
41 год
Часть I
Исследование сети
43 год
Глава 3 Ручное исследование сети
45
Цели главы: Pepsi.com и Cyper.org
46
Обнаружение активов
46
Поиск по ARIN
47
Поисковые машины Dorks
48
DNSDumpster
49
Хакерская цель
52
Shodan
53
Censys (поиск субдоменов)
56
Поиск субдоменов Censys
56
Яростный
57 год
Sublist3r
58
Enumall
59
Полученные результаты
60
Фишинговые домены и опечатки
61
Резюме
64
Глава 4 Поиск сетевой активности (расширенные методы NMAP)
67
Начиная
67
Подготовка списка активных хостов
68
Полное сканирование портов с использованием различных типов сканирования
68
Сканирование окна TCP
70
Работа с межсетевыми экранами и IDS
70
Использование Reason Response
71
Идентификация живых серверов
71
Уклонение от брандмауэра
73

Распределенное сканирование с использованием прокси и TOR
73
Фрагментированные пакеты / MTU
74
Уловка с обнаружением сервисов
74
Низко и медленно
76
Плохие контрольные суммы, приманка и случайные данные
76
Огнехождение
79
Сравнение результатов
79
Стилизация отчетов NMAP
81 год
Резюме
82

Глава 5 Автоматизированные инструменты для обнаружения сети
83
Паук
84
SpiderFoot HX (Премиум)
91
Intrigue.io
95
Вкладка Entities
96
Анализируем uberpeople.net
99
Анализ результатов
104
Экспорт ваших результатов
105
Recon-NG
107
Поиск модулей
111
Использование модулей
111
Ищем порты с Shodan
115
Резюме
116
Часть II Веб-исследование
119
Глава 6 Сбор информации на веб-сайте
121
Построен с
121
Поиск общих сайтов с помощью Google Analytics Tracker
123
История IP и связанные сайты
124
Сборщик информации Webapp (WIG)
124

CMSMap
129
Сканирование одного сайта
130
Сканирование нескольких сайтов в пакетном режиме
130
Обнаружение уязвимостей
131
WPScan
132
Работа с WAF / WordPress не обнаружена
136
Резюме
141
Глава 7 Поиск в каталоге
143
Dirhunt
143
Wfuzz
146
Фотон
149

Сканирование веб-сайта
151
Intrigue.io
152
Резюме
157
Глава 8.
159
Essential Search Dorks
160
Знак минус
160
Использование цитат
160
Сайт: Оператор
161
Название: Оператор
161
Allintitle: Оператор
162
Тип файла: Оператор
162
Inurl: Оператор
163
Кеш: Оператор
165
Allinurl: Оператор
165
Имя файла: Оператор
165
Интекст: Оператор
165
Сила придурка
166
Не забывайте о Bing и Yahoo!
169
Автоматизированные инструменты доркинга
169

Inurlbr
169
Использование Inurlbr
171
Резюме
173
Глава 9 WHOIS
175
КТО
175
Использование данных WHOIS
176
Исторический WHOIS
177
Поиск похожих доменов
177
Namedroppers.com
177
Поиск по нескольким ключевым словам
179
Расширенный поиск
181

Ищем злоумышленников
182
Whoisology
183
Расширенный поиск домена
187
Стоит денег? Абсолютно
188
ДоменИнструменты
188
Поиск домена
188
Массовый WHOIS
189
Обратный поиск IP
189
Записи WHOIS о стероидах
190
История WHOIS
192
Сила скриншотов
193
Копаться в истории WHOIS
193
Ищете изменения в собственности
194
Обратный WHOIS
196
Перекрестная проверка *всей* информации
197
Резюме
199
Глава 10 Прозрачность сертификатов и Интернет-архивы
201
Сертификат прозрачности
201
Какое отношение это имеет к цифровым расследованиям? 202
Скаутинг с CTFR

202
Crt.sh
204
CT в действии: Обходной Cloudflare
204
Тестирование большего количества целей
208
CloudFlair (сценарий) и Censys
209
Как это работает?
210
Архивы Wayback Machine и поисковых систем
211
Кеши поисковых систем
212
CachedView.com
214
Скребок для машин Wayback
214
Enum Wayback
215

Очистка пути назад с помощью Photon
216
URL-адреса поиска по сайту Archive.org
217
Дайджест сайта Wayback: список URL-адресов всех сайтов, сохраненных в кеше
Путь назад
219
Резюме
220
Глава 11 Iris от DomainTools
221
Основы ириса
221
Управляемые повороты
223
Конфигурирование ваших настроек
223
Настройка исторического поиска
224
Пивоттт !!!
225
Вращение по хешам сертификатов SSL
227
Ведение заметок
228
История WHOIS
230
История скриншотов
232
История хостинга
232
Собираем все вместе
234
Основная находка
240
Резюме
241

Часть III.
Копаем золото
243
Глава 12 Метаданные документа
245
Exiftool
246
Метагофил
248
Модули метаданных Recon-NG
250
Метакраулер
250
Модуль "Интересные_файлы"
252
Модули геолокации канцелярских кнопок
254
Intrigue.io
257
FOCA
261

Запуск проекта
262
Извлечение метаданных
263
Резюме
266
Глава 13 Интересные места для поиска
267
TheHarvester
268
Запуск сканирования
269
Вставить сайты
273
СОДЕРЖАНИЕ
Psbdmp.ws
273
Форумы
274
Изучение истории форума (и TDO)
275
После панировочных сухарей
276
Отслеживание личности Сайпера
278
Репозитории кода
280
SearchCode.com
281
Поиск кода
282
Ложноотрицательные
283
Гитроб
284
Журналы фиксации Git
287

Вики-сайты
288
Википедия
289
Резюме
292
Глава 14 Общедоступное хранилище данных
293
Утечка Exactis и Шодан
294
Атрибуция данных
295
Параметры командной строки Shodan
296
Запрос исторических данных
296
CloudStorageFinder
298
Amazon S3
299
Цифровые океанические пространства
300

Базы данных NoSQL
301
MongoDB
302
Робот 3T
302
Инструменты командной строки Mongo
305
Elasticsearch
308
Запрос Elasticsearch
308
Сброс данных Elasticsearch
311
Нет
311
MongoDB
313
Elasticsearch
314
Сканировать
314
Поиск
315
Свалка
317
MatchDump
317
Кассандра
318
Amazon S3
320
Использование ваших собственных учетных данных S3
320
Резюме
321
Часть IV.
Охота на людей

323
Глава 15 Исследование людей, изображений и мест
325
PIPL
326
Поиск людей
327
Публичные записи и проверка биографических данных
330
Ancestry.com
331
У опасных актеров тоже есть отцы
332
Судебные обыски
332
Поиск изображений
333
Google картинки
334
В поисках золота
335
По следу
335

TinEye
336
Орлиный глаз
340
Поиск изображений
340
Cree.py и геолокация
343
Начиная
343
Отслеживание IP-адресов
346
Резюме
347
Глава 16 Поиск в социальных сетях
349
OSINT.rest
350
Другой подопытный
355
Твиттер
357
SocialLinks: для пользователей Maltego
358
Skiptracer
361
Выполнение поиска
361
Поиск адреса электронной почты
361
Поиск номера телефона
364
Поиск имен пользователей
366
Еще один поиск по имени пользователя
368
Userrecon

370
Reddit Investigator
372
Критический «мир» расследования TDO
374
Резюме
375
Глава 17 Подсказки для отслеживания профиля и сброса пароля
377
С чего начать (с TDO)?
377
Построение матрицы профиля
378
Поиск по форуму
379
Списки запретов
381
Социальная инженерия
381
SE'ing Threat Actors: История «Аргона»
383
Каждый получает SE'd - урок усвоен
387
Конец TDO и форума KickAss
388
Использование подсказок для сброса пароля
390
Запуск вашего контрольного листа
391
Gmail
391
Facebook
393
PayPal
394
Твиттер
397
Microsoft
399
Instagram
400
Использование ответов веб-сайта jQuery
400
Аська
403
Резюме
405
Глава 18 Пароли, дампы и Data Viper
407
Использование паролей
408
Заполнение матрицы профиля F3ttywap
409
Важный неверный поворот
412
Получение ваших данных
413
Качество и сбор данных 1–5
413
Всегда проверяйте данные вручную
415

Где найти качественные данные
420
Data Viper
420
Форумы: Недостающее звено
421
Определение настоящего «Cr00k»
422
Отслеживание перемещений на форуме Cr00k
423
Анализ временной шкалы
423
Момент Эврики
427
Тщеславие над OPSEC, каждый раз
429
Почему эта связь важна
429
Начнем с малого: Data Viper 1.0
430
Резюме
431

Глава 19 Взаимодействие с исполнителями угроз
433
Вытаскивая их из тени
433
Кто такой WhitePacket?
434
Связь Бев Робба
435
Страдинатрас
436
Обфускация и TDO
437
Кто такой Билл?
439
Так кто же на самом деле Билл?
440
МолодойБандит
440
Как я узнал, что это Крис?
441
Подключение к ботнету Mirai?
442
Почему это открытие было таким потрясающим?
444
Вопрос ко всему!
445
Создание потока информации
446
Использование хакерской драмы
447
Было ли это реальным?
448
В поисках других улик
449
Возвращение в TDO
450
Решение последнего вопроса

451
Вывод биткойнов
451
Резюме
452
Глава 20.
Взлом на 10 миллионов долларов
453
Гностик
454
Сайты, взломанные GnosticPlayers
456
Техники взлома гностиков
457
Сообщения GnosticPlayers
459
GnosticPlayers2 Emerges
461
Таинственный третий член
462
NSFW / Photon
463

Перчатки оторваться
464
Установление контакта
465
Габриэль / Бильдштейн aka Kuroi'sh
465
Связь с его друзьями
467
Прополка через дезинформацию
468
Проверка с помощью Wayback
468
Собираем все вместе
469
Data Viper
469
Доверяй, но проверяй
472
Ирис доменных инструментов
474
Проверка с помощью второго источника данных
475
Конец строки
476
Что на самом деле произошло?
476
Вне досягаемости
476
Волшебное появление Курои
477
Что я узнал, наблюдая за потерянным
477
Кто взломал GateHub?
478
Разгадывая ложь
479
Был ли замешан Габриэль? Моя теория
479

Габриэль - это Нклей: альтернативная теория
479
Все дороги ведут обратно в NSFW
480
Резюме
481
Эпилог
483
Показатель
487

---

xxv

Пролог

Одно из недавних расследований, над которыми я работал, касалось взлома нескольких
миллиардная организация. Их украденные данные были выставлены на продажу в частном порядке.
cles, и, узнав об этом, сразу связался с организацией. В
у организации было много вопросов, и, учитывая мою предыдущую следственную работу, я
возможность связаться с злоумышленником от его имени и получить информацию о как произошло нарушение.
Следующий текст представляет собой часть представленной рецензии NSFW, *угрозу актер*
мы будем более подробно освещать эту книгу , где он описывает,
подробно, как ему удалось взломать сеть этой организации. Процесс он
used был изощренным и ни в коем случае не заурядным проездным.
Это было очень хорошо спланировано и выполнено.
Вся идентифицирующая информация была изменена .

Во-первых, я понял, что GitHub добавляет проверку нового устройства в течение недели, там-
поэтому я попытался идентифицировать как можно больше разработчиков и войти в их GitHub
аккаунт для доступа к закрытым репо организации.
Затем я определил разработчиков программного обеспечения, работающих на

компанию через LinkedIn.
Частично доксируя каждую для получения учетных записей Gmail, я нашел Боба.
Выполнение поиска в базе данных в надежде на повторное использование пароля (или правила, которые будут применяться к
их предыдущий пароль), чтобы войти с действующими учетными данными.
Я попал в GitHub благодаря Бобу, который повторно использовал пароль «BobsTiger66» (который, как сообщил GitHub, небезопасен с красным знаменем, но он выбрал
чтобы игнорировать его), и был повторно использован в нескольких частных базах данных и одной общедоступной базе данных
(ArmorGames).

После входа в систему мне пришлось действовать быстро, чтобы избежать блокировки нового алгоритма машинного обучения GitHub.
учетных записей, не использующих новые IP-адреса, поэтому я немедленно использовал ssh-keygen, чтобы добавить новый общедоступный
SSH-ключ к профилю пользователя, я понял, что вы добавили Okta SSO, предотвращая
clone частных репозиториев, чтобы обойти это, я рассмотрел потенциальные интеграции.
CircleCI - популярный инструмент CI / CD, который по своей сути связан с организациями через:
Связь ключей SSH или PAT, поэтому я понял, что процессы сборки могут быть использованы
чтобы получить частные репо, однако в этом не было необходимости. Вы, ребята, добавили
странная реализация Okta STS с AWS, производящая ограниченные по времени токены, я
понял, что они порождались каждый раз, когда запускался новый процесс сборки, поэтому
Я получил доступ к режиму отладки Circle и мне удалось извлечь эти ограниченные по времени токены, и
использовал их для загрузки ваших внутренних данных.
К сожалению, этим токенам не было предоставлено никаких дополнительных привилегий, поэтому вы
повезло, иначе я бы получил доступ к RDS через CLI и клонировал снимок.
Когда я прочитал это, я был немедленно впечатлен уровнем усилий, которые он приложил.
в хак. И, несмотря на результат, клиент тоже.
В конце концов, у этой бреши был счастливый конец, потому что я смог предоставить
полная информация для клиента, которая позволила им определить, как произошло нарушение,
а также принять надлежащие меры, чтобы этого больше не повторилось.
В этом вся суть, не так ли?
Не предоставлять клиентам бесполезное описание общих ДТС (тактика,
методы и процедуры) в отношении предполагаемых субъектов угрозы - вот что
так много компаний, занимающихся разведкой угроз, но чтобы предоставить полезные сведения
текст о том, как злоумышленник взламывает их системы.
Многие компании просто полагаются на существующие отчеты об угрозах.
группы и никогда не вникают в суть того, как произошло нападение. Некоторые-
раз требуется выследить злоумышленников и поговорить с ними

напрямую. Обычно они довольно открыты и готовы хвастаться своими успехами.
это потому, что на каком-то уровне все хакеры хотят прославиться; и как мы увидим в
В будущих главах *тщеславие всегда превосходит OPSEC* (оперативная безопасность).
В этом конкретном случае я уже говорил с NSFW о нескольких других
хаки, с которыми он связан, поэтому не было проблем спросить, как он смог вытащить
это выкл.
И если вы внимательно посмотрите, то заметите несколько опечаток:
слова и важные «подсказки», связанные с его описанием. Распространенные орфографические ошибки
или даже региональные различия в написании (например, организация или организация) могут
будут очень важными следственными уликами, которые мы обсудим в следующих главах.
Но прежде чем мы углубимся во все это, я считаю важным пролить свет на
кто я, чтобы вы могли узнать меня немного лучше, понять, что делает
и, может быть, привыкну к сухому юмору и сарказму, которые
вы найдете разбросанные по всей этой книге.

Моя история

Когда я начал писать эту книгу, я задал себе простой вопрос: квалифицирован ли я?
написать эту книгу? По сей день мой ответ по-прежнему «вероятно, нет». Я не верю
один человек может знать все, что нужно знать по теме, поэтому
в этой книге вы найдете советы и рассказы других экспертов отрасли.
Я восхищаюсь и уважаю каждого из людей, которых я попросил внести свой вклад в это
книга. Я знаю их работу не понаслышке, поэтому чувствую, что каждый из них
собственная уникальная перспектива, которая дополняет и усиливает темы, которые я буду
выдвигая.
Но прежде чем мы перейдем к этому, вот небольшое представление о том, кто я и что делает
мне поставить галочку.

История

Мне было около 10 лет, когда мой отец принес домой IBM PS / 2. у меня нет
идея, что это было или что он может сделать, но я был загипнотизирован. Это было раньше
Винда 3.1 дн. Я помню, как включил его и посмотрел на приглашение DOS
и просто пробиваюсь сквозь него. Все это было похоже на гигантскую головоломку,
наверное, поэтому меня это затянуло.
Я большой любитель головоломок. Чем сложнее, тем лучше. Одна из моих сильных сторон
(а также, по общему признанию, слабость) в том, что я могу быть безжалостным, когда пытаюсь
найти решение сложной проблемы. Некоторые называют это поведение
"Навязчивый". Я понимаю и признаю такое поведение.
Бывают ночи, когда я все еще ломаю голову в 4 часа утра, потому что просто не могу
останавливаться. Это часть того, кем я являюсь, и большая часть того, почему я чувствую, что я очень хорош
в том, что я делаю - будь то попытка взлома системы или сборка
История уголовного расследования.

Корни и Рейвы

Если вам интересно, я начал свою карьеру веб-разработчика, писавшего
HTML и JavaScript в конце 90-х. Я вырос в Нью-Джерси и всегда был
в электронную музыку. Естественно, я тоже был очарован рейв-культурой.
Ночные клубы, такие как Limelight и Tunnel, были большим событием, и я хотел
часть этого.
К сожалению, в этих клубах был возрастной ценз 21+, что было проблемой.
потому что мне было 16. Я выучил HTML и предложил создать бесплатный веб-сайт.

для одного из диджеев-резидентов клуба. С тех пор я мог просто зайти с ним
потому что я был его «веб-парнем». Задача решена.

Тестирование на проникновение не сильно отличается, поэтому я его и проводил.
(в той или иной форме) всю жизнь. Все дело в понимании того, что
правила есть, а затем найти способ их обойти.
Я всегда умел находить способы обойти правила, и я
думать - это черта, которую разделяют большинство тестеров на проникновение.
Не поймите меня неправильно, правила важны. Некоторым людям нравится жить своей жизнью
в четко определенной песочнице, в то время как другим нравится пытаться найти
способы вырваться из этого. Я последний.

Разработка бизнес-модели (с помощью лазеров !!)

Однажды вечером около 2011 года я просматривал Интернет так же, как и большинство людей.
do: с активным пакетом Burp и запущенной пассивной разведкой на всех сайтах, которые я посещал.
Я рассказывал жене об отличном сайте, где продаются мощные лазеры в
разных цветов, надеясь, что она позволит мне купить один. Это было сложно, но очень
к моему удивлению, пакет Burp обнаружил на сайте уязвимость пассивного SQL-инъекции.
Мне нужно было это проверить, и, прежде чем я это понял, я смог увидеть пользователя сайта
учетные записи с хешированными паролями. Авторизация на сайте с одним из админов
учетные записи означали необходимость взлома хеш-пароля администратора, чего не было
сложно использовать любое количество онлайн-взломщиков хеша, учитывая, что пароль был
какая-то вариация Admin123.
Я зашел на сайт и вуаля! У меня был полный доступ ко всему. Системные записи,
учетные записи пользователей, информация о заказе и все такое.

Да, теперь я понимаю, что это действие было не совсем «законным», но не осуждаю. Мы все надо где-то начинать. К тому же у этой истории счастливый конец.

Именно в этот момент я почувствовал искру предпринимательства. Что, если бы я мог
возьмите эту информацию и передайте ее владельцам сайта, чтобы они могли исправить инъекцию.
ошибка, препятствующая доступу других пользователей к сайту таким же образом? Конечно они
отплатили бы за этот случайный акт доброты некоторыми из своих крутых и могущественных
лазеры?
Теперь я счастливый обладатель синего лазера мощностью 2000 мВт и зеленого лазера мощностью 1000 мВт.
лазер! Красиво, правда? Лазеры действительно сжигают вещи. Они довольно крутые.
Что еще более важно, сайт закрыл уязвимость SQL-инъекций, и у меня был
модель для бизнеса по предоставлению услуг, которые действительно могут помочь людям.
В процессе я также извлек чрезвычайно ценный урок: если вы взломаете
сначала веб-сайт, *затем* попробуйте предложить решение клиенту и попросите «чаевые»

в виде продукта с их веб-сайта, это может быть истолковано как вымогательство.
Ой. Это явно не было моим намерением, которое, как мне кажется, появилось в моем электронном письме с
генеральный директор, но, оглядываясь назад, я уверен, что у меня могли быть проблемы. Так что пока
это конкретное упражнение хорошо сработало для всех, я определенно должен был
работать над доработкой бизнес-модели.

Образование

Однажды, когда я работал в Министерстве обороны, я получил известие от
старшего руководителя, что он собирался привлечь в свою команду кого-то, кто
недавно прошел сертификацию «этического взлома».
Сертификация? Бьюсь об заклад, я смогу это сделать, поскольку у меня уже были навыки
взламывать вещи и делал это всю свою жизнь. Это звучало как отличная карьера
path занимался тем, что мне действительно нравилось, поэтому я начал изучать это.
К этому моменту я уже получил степень бакалавра. Я начал работать
работа в техподдержке, когда я учился в старшей школе, тогда я проучился только семестр в колледже
перед тем, как бросить учебу. Лишь намного позже я решил вернуться и
закончить онлайн-бакалавриат.
После некоторого исследования я нашел магистерскую программу в Западном губернаторском университете.
Versity (WGU), специализирующаяся на информационной безопасности и включающая Сертифицированный
Этичный хакер (CEH) и сертифицированный судебный следователь по взлому (CHFI)
сертификаты в рамках курсовой работы. Поэтому я решил получить степень магистра.
Через несколько лет я закончил магистратуру и получил все сертификаты,
Я хотел. Оглядываясь назад, думаю, я чувствовал себя очень похожим на Форреста Гампа, когда он был
бегать по стране: я уже добрался так далеко, так что я мог бы
продолжай, верно? Поэтому я решил пропустить обычную сертификацию CISSP и
пошел на мою докторскую степень.
Я потратил еще около четырех лет на онлайн-уроки и написал диссертацию.
о «предполагаемой эффективности системы кибербезопасности среди руководителей информационной безопасности».
различных отраслей ». Я получил докторскую степень в 2018 году.

Запуск Night Lion Security

Работал с рядом крупных организаций, в том числе был директором
служб безопасности для RSM (входит в пятерку бухгалтерских фирм), я почувствовал, что у меня есть уникальный
взгляд на то, как другие организации проводили тестирование на проникновение и риск
оценки, и я знал, что могу предоставить что-то лучшее.
В 2014 году я решил начать Night Lion Security, мой собственный консалтинг по безопасности.
фирма. Моим видением было (и остается) собрать элитный отряд хакеров и пенальтистов.
тестировщиков, чтобы предоставить подробный и полезный отчет.
Быть начинающей консалтинговой фирмой по вопросам безопасности само по себе достаточно сложно. Существование
стартап в области безопасности и пытается конкурировать с такими гигантами, как Optiv, KPMG,
SecureWorks и AT&T были чрезвычайно трудными.

Я чувствую, что смог выделиться на таком перенасыщенном рынке, будучи
очень активен в новостях и СМИ. Я чувствую, что быть на телевидении - одно из основных
причины, по которым компании были готовы рискнуть с небольшим стартапом
о котором никто никогда не слышал. Я не думаю, что смог бы это сделать
так далеко без этого.

Меня критиковали за такой подход, потому что меня считают человеком, который
«саморекламируется», выходя на телевидение. Но, в конце концов, я чувствую, что оно того стоило, потому что
это позволило мне отдать так, что я не смог бы
в противном случае. Следующее - прекрасный пример.
Недавно мы завершили тест на проникновение для крупного публичного банка.
В конце теста вице-президент по безопасности изо всех сил сказал мне, что наша
test был «первым *настоящим* тестом на проникновение, который они когда-либо проходили». Вся большая «доска»
одобренные »компании, с которыми они работали в прошлом, не сделали ничего, кроме
прославили сканирование уязвимостей, и мы смогли дать им что-то очень
более ценным. Я очень горжусь этим и очень благодарен за то, что он сказал мне
потому что это *именно* то видение, которое я намеревался реализовать, когда создавал Night Lion.

Цифровые расследования и утечки данных

Переход к цифровым расследованиям был настолько плавным, что это не было переходом
вообще. Я бы даже не сказал, что «перешел» к цифровым расследованиям, потому что это было
всегда просто то, что я делал. Случаи реагирования на рабочие инциденты, проникновение
тестирование, решение сложных задач - это все одно и то же. Все дело в том, чтобы взломать
головоломка.
Как я быстро выяснил, работая над своими делами (т. Е. Ища незащищенные
утечки данных и утечки данных) могут быстро стать проблемой при работе с
с последствиями, чем фактическое обнаружение и раскрытие данных.
Я обнаружил ряд громких утечек данных, включая Exactis, Apollo.io,
и Verifications.io (о которых я подробнее расскажу в главе 14), и в каждом случае
Последствия воздействия каждый раз были разными.
Verification.io был особенно интересен, потому что это привело к ситуации
обнаружения того, что раскрытые данные на самом деле были украдены у кого-то
еще. Компания оказалась полностью фейковой, и однажды я начал тыкать
вокруг, они все выключили и побежали.
Также было *много* раз, когда я ходил по кругу, отправляя копии
данных десяткам компаний, пытающихся найти владельца.
На что следует обратить внимание: если вы обратитесь в компанию, чтобы узнать о возможных
нарушение (или утечка) данных, эта компания *не обязана сообщать вам,*
данные фактически принадлежат им .
Несмотря на то, что люди в этой отрасли могут пытаться делать правильные
вещь, есть значительные последствия, которые сопровождают компанию, имеющую

публично признаться в утечке (или утечке) данных - например, кто-то почти всегда
меня уволят, или того хуже. . . .
В главе 14 я подробно описываю свою собственную версию нарушения Exactis и другие открытия.
эри. Скажем так, когда генеральный директор отправляет вам текстовое сообщение, никогда не бывает весело (или легко).
в субботу вечером, спрашивая, почему ты разрушил его жизнь. Вот Трой Хант, владелец
из HaveIBeenPwned, с похожей историей:

Пролог XXXI

На ум приходит случай, когда гонконгский производитель игрушек V-Tech
нарушен. Это было примерно в 2015 году. Это был огромный объем данных, касающихся
детям, в том числе детские фотографии. В V-Tech повсюду была внедрена SQL-инъекция, это было
просто крушение поезда.
Проблема в том, что это гонконгский производитель игрушек.
чтобы попасть в эту часть мира, может быть очень, очень трудно получить право собственности на эти
инциденты, потому что компания просто закроет перед вами двери и проигнорирует это,
что и произошло в моем случае.
Я думаю, что нарушения с таким уровнем чувствительности особенно интересны.
Аналогичным образом у Службы крови Красного Креста в Австралии.
инцидент пару лет назад, поскольку это был большой объем очень конфиденциальных данных,
в том числе и мой. Моя заявка на сдачу крови была там.
Это было около полумиллиона австралийцев, включая вашу группу крови и в том числе
критерии приемлемости или вопросы по критериям приемлемости, например, были ли вы в группе риска
сексуальная активность. Это вполне уместный вопрос - спросить кого-нибудь о сдаче крови,
но не совсем верная вещь для резервного копирования с рабочего сервера на общедоступный
тестовый сервер с включенным просмотром каталогов.
Разница с Красным Крестом в том, что они просто очень хорошо поработали.
урегулирование инцидента после того, как он действительно был запущен. Они регулярно выделяются сейчас как
золотой стандарт для обработки инцидентов после взлома, и это хорошо.

У всего есть свои взлеты и падения, но, в конце концов, мне нравится то, что я делаю.
Эта книга - кульминация последних двадцати лет моей жизни. Я заполнил
это с реальными историями, сценариями и техниками, которые, надеюсь, однажды
помочь вам в ваших собственных исследованиях.
С этим, давайте рок-н-ролл.

Охота на киберпреступников

1

1

В этой главе рассказывается о важных моментах, которые вам следует знать перед тем, как получить
начал, а также такие темы, как то, что вы найдете и чего не найдете в этой книге, верхняя
выводы из этой книги, которые будут регулярно обсуждаться в следующей главе.
ters и некоторые предварительные условия, которые помогут упростить вам путь киберразведкам.
Некоторые из вас могут искать причину, чтобы заняться этой областью. Некоторые из вас
возможно, уже работает в поле и ищет новые методы, которые можно использовать во время
собственные исследования.
В любом случае, я считаю необходимым предупредить вас, что начало расследования может
быть как марафон. Это может быть медленным и утомительным, и на то, чтобы получить
куда ты идешь.
Вы должны быть очень мотивированы, потому что пытаетесь соединить точки в
целый Интернет неорганизованных подсказок и информации может быть крайне неприятным.
мужество.
Но если вы надавите и постараетесь преодолеть эту первоначальную боль, она в конечном итоге
случаться.
Есть ощущение, что в конце концов ты найдешь в ходе расследования. Это
такое же чувство, которое испытывают программисты или хакеры - оно запускается в тот момент, когда вы нажимаете
на этом первом основном потоке или разблокировать тот первый тумблер, который уступает место
второй и третий. . . и в конце концов весь мир загорается.
Нет ничего лучше и увлекательнее, чем войти в «зону». Это как
состояние с точной лазерной фокусировкой - ваше собственное «время пули» - где вы не можете быть
замедлился или остановился, пока вы не решите загадку, не взломаете систему или не решите

Начиная

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

отполировал то, над чем вы работаете. Это прилив лучше, чем любой стимулятор
или наркотик - одним словом, это *потрясающе* .
В этой книге я буду предоставлять вам информацию о моих личных
арсенал инструментов, которые, я надеюсь, помогут вам именно туда. я также буду
предоставить вам мой собственный опыт и мыслительные процессы с использованием многих из
эти инструменты, потому что я нашел , что это может быть намного более полезным , чтобы узнать , *как*
человек использует определенный инструмент, а не просто воссоздает руководство пользователя.

Почему эта книга отличается

Я прочитал несколько книг по электронным расследованиям, и все они кажутся просто
перечислите все возможные инструменты, дайте краткое описание того, что делает этот инструмент, и
перейти к следующему. Почти как выпас программного скота.
Многие из OSINT и расследовательских книг, которые я читал или на которые ссылался перед тем, как начать
эта книга заставила меня чувствовать себя перегруженным информацией, как будто я пытался недооценить
выдерживать техническую энциклопедию, фактически не давая вам никаких указаний или
полезный совет, связанный с тем, что вы читаете.
Я чувствую, что эта книга отличается от других, потому что я глубоко погружаюсь в инструменты и пытаюсь продвигать
видео рассказы о реальных расследованиях и о том, как эти инструменты использовались в
способ, который на самом деле оказался полезным (или нет).
Другое отличие состоит в том, что примеры показывают не только положительные результаты.
с каждым примером. Ненавижу, когда это делают другие книги, потому что результаты
как правило, нереально. Реальное тестирование часто не дает полезной информации, а именно:
кое-что я покажу при сравнении разных инструментов.

Что вы найдете и чего не найдете в этой книге

В этой книге будет рассказано о многих инструментах и их техническом использовании. Это также будет
охватить мой мыслительный процесс и истории о том, как я использовал определенные инструменты для
дальнейшее расследование.
Эта книга будет содержать ряд моих личных переживаний во время настоящих
расследования или сценарии взлома. Хотя имена могут быть изменены для защиты
компании или люди, участвующие (но в основном, чтобы защитить меня), истории и сценарии
представлены полностью документальная литература. У меня очень нестандартный подход к жизни,
так что я буду предлагать жизненные уроки и полезные советы, которые когда-нибудь могут вам помочь.
Мне также не нравится, что в большинстве технических книг представлена только точка зрения
одинокий человек (автор).
Я буду первым, кто признает, что не знаю всего об OSINT или цифровых технологиях.
расследования. Во время исследования может возникнуть множество различных аспектов технологии.

проблема, которая может потребовать уникальной точки зрения или понимания, которое приходит
из-за многолетнего практического опыта, поэтому я всегда старался окружить
я с людьми, которых я уважаю и которых я считаю экспертами, у которых я могу учиться.

3

Я подумал, что вам, читатель, было бы действительно интересно, если бы я также включил
мнения и опыт некоторых из этих людей наряду со мной. С
Я пишу книгу по теме, почему бы также не включить мнения людей
кто также действительно хорош в указанном предмете?
Поэтому я попросил несколько человек, которых я считаю экспертами в своей области, согласиться
отдать должное истории, мнению или даже технике в отношении некоторой части информации -
сбор или следственный процесс.
Я считаю, что каждая из их историй уникальна и заставляет задуматься, и я знаю
ты тоже будешь!

Знакомство с коллегами-экспертами

Я хотел бы выразить особую благодарность и привет следующим
людям за их вклад в качестве экспертов в эту книгу (в алфавитном порядке):

■ Алекс Хайд

Вице-президент по исследованиям SecurityScoreCard и основатель HackMiami

■ Боб Дьяченко

Исследователь безопасности, основатель SecurityDiscovery.com

■ Кот Мердок

Моделирование угроз и атак, Guidepoint Security

■ Крис Хэднаги

Главный хакер, социальный инженер, OOO, владелец SEVillage

■ Крис Робертс

Главный специалист по безопасности, Attivo Networks

■ Лесли Кархарт

Главный охотник за угрозами, Dragos, Inc.

■ Джон Стрэнд

Основатель Black Hills Information Security, старший инструктор SANS

■ Джонатан Кран

Основатель, Intrigue.io, руководитель отдела исследований, Kenna Security

■ Ник Фюрнё

Компьютерный криминалист, эксперт по криптографическим расследованиям

■ Роб Фуллер

Красная команда в тяжелом весе

■ Трой Хант

Исследователь безопасности, вице-президент Microsoft, основатель, Have I Been Pwned

■ Уильям Мартин

Исследователь, разработчик SMBetray

Примечание о криптовалютах

Еще один супер-благодарность Нику Фюрнё за написание учебника по криптографии.
дальнейшие исследования в этой главе. Для тех, кто хочет по-настоящему погрузиться в
как исследовать криптовалюты, ознакомьтесь с его книгой " *Расследование"*
Криптовалюты: понимание, извлечение и анализ доказательств блокчейна
(опубликовано Wiley).

Что тебе нужно знать

Следующие темы будут регулярно обсуждаться в этой книге и
следует считать ключевыми выводами. Еда на вынос заказывается естественным
поток информации, а не по степени важности:

1. Имея дело с молодым и честолюбивым хакером (он же skid aka script kid-
die), *тщеславие всегда будет выше OPSEC* . В этой книге будет много примеров.
доказывая это утверждение.
2. Доступ к исторической информации часто может сделать или сорвать все расследование.
тигация. Если молодой или амбициозный киберпреступник готов пожертвовать OPSEC
из-за собственного тщеславия, то возможность оглянуться назад, скорее всего,
приведет вас к ответу, который вы ищете. Более историческая информация-
Если у вас есть доступ, тем выше шансы найти кого-нибудь или что-то еще
это вы ищете.
3. Вы всегда получаете то, за что платите. Если вы хотите получить доступ к лучшему и самому
полные источники исторической информации, это будет недешево. Если хочешь
дешево (или бесплатно), не ожидайте, что у вас будет доступ ко всему.
4. Никогда не полагайтесь на один инструмент для получения всех ответов. Вы всегда должны пробовать все
инструменты и методы в вашем распоряжении, даже если в прошлом они не
предоставил какие-либо полезные результаты. Иногда везет. Эта книга полна
примеров, когда я был полностью поражен результатами,
почему вы должны. . .
5. *Сохраните все* и храните подробную документацию, чтобы вы могли ее найти.
потом.

Это худшая часть любого расследования, особенно когда вы
на ходу нахожу новые подробности. . . так что я не могу этого достаточно подчеркнуть. Есть несколько ключевых моментов
из моего собственного исследования, которое я не могу поверить, что не сохранил. Я был уверен, что сделал скриншоты,
но я, должно быть, был настолько поглощен исследованиями (и в зоне), что забыл
сохраните предметы. Теперь этих вещей больше нет, и я каждый день ругаю себя по этому поводу.
Так что еще раз *сохраните все* .

5

Платные инструменты и исторические данные

На протяжении всей этой книги я буду изо всех сил стараться использовать бесплатные инструменты с открытым исходным кодом в качестве
как можно больше, но вернемся к выводу № 3: вы *всегда* получаете то, за что платите.
Разведывательные исследования и сбор информации ничем не отличаются. Вы всегда можете
пойти по дешевому пути и полагаться на действительно «бесплатные» инструменты, но в конечном итоге это может стоить
качество информации, которую вы можете получить, и количество
времени, которое вы тратите на поиск информации.
Я искренне верю, что самая важная часть расследования часто наступает
вплоть до уровня исторических данных, к которым вы можете получить доступ. Редко встретишь открытые исходные инструменты с большим количеством накопившихся исторических данных.
В частности, некоторые инструменты содержат огромное количество информации, за которую я с радостью плачу.
Я расскажу об этих инструментах более подробно позже, а пока просто знайте, что
не все методы, которые я обсуждаю, будут использовать полностью бесплатные инструменты. Это компромисс.
Вам нужно будет решить, хотите ли вы тратить деньги, но
просто имейте в виду, что не все может быть бесплатным.

А что насчет Мальтего?

Maltego - мощный инструмент для цифровых расследований, возможно, даже *для* отрасли
стандартный следственный инструмент. Он широко освещался практически в каждом
другие книги о цифровых исследованиях и, конечно же, в книгах, посвященных только
с его многочисленными применениями и приложениями, поэтому я решил оставить
Мальтего из этой книги.
Не поймите меня неправильно, я неукоснительно использую Maltego, но программа настолько обширна, что
чтобы осветить это должным образом, мне пришлось бы посвятить большую часть этой книги этому
одна тема. Доступно так много других полезных и заслуживающих внимания инструментов, которые просто
не получают того внимания, которого они заслуживают. Теперь они это сделают.

Предпосылки

Для эффективного использования инструментов и методов требуются только два предварительных условия.
описано в этой книге.

Знайте, как использовать и настраивать Linux

Большинство предоставленных инструментов и примеров будут в Linux. Имея в
по крайней мере, будет важно базовое понимание того, как запускать команды.

Вам нужно будет настроить и установить инструменты и их соответствующие зависимости.
плотности. У вас есть много разных сред Linux на выбор, каждая
со своим набором преимуществ. Я бы предпочел уделить время техникам
и рассказы, которые помогут в вашем расследовании, вместо того, чтобы пытаться предоставить исчерпывающую
информацию.
активная техподдержка.

Если вы не знаете, как создать свой собственный дистрибутив Linux, я настоятельно рекомендую
исправить скачав Kali Linux. Большинство всего, что вам понадобится, будет
уже настроен для вас. Вы можете скачать Kali с www.kali.org .

Получите ключи API по порядку

Многие инструменты в этой книге будут иметь API-соединения с несколькими сайтами / серверами.
пороки. Одна из самых неприятных вещей, с которой приходится иметь дело при первоначальной настройке
необходимо настроить ключи API в каждом инструменте.
Ведите общий список. Я не могу больше сказать по этой теме, но я
хочу назвать это из-за того, сколько времени это сэкономит вам в долгосрочной перспективе.
Если у вас нет длинного списка ключей API, ничего страшного. Начните с одного. Я использую
формат Sitename: APIKEY, и я сохраняю все в моем хранилище 1password. Это
просто и легко добраться, когда мне это нужно.
Я бы, вероятно, не публиковал ваши ключи на любом общедоступном сайте, таком как AWS.
ведро, доска Trello или файл OneNote. Я никогда не знал, что доски Trello публично
доступен для поиска, пока однажды не появилась история о паролях и других деталях учетной записи
выставлены на сервисе. Я считаю, что я бы, вероятно, держался подальше от пост-
использование ключей или паролей в том, что у вас нет прямого контроля.

Важные ресурсы

Следующие ресурсы являются чрезвычайно полезными руководствами, которые помогут вам продвинуться вперед.
знание OSINT и расследований.

OSINT Framework

Платформа OSINT представляет собой набор инструментов Open Source Intelligence, разработанных
чтобы упростить процесс сбора разведданных и данных.
Фреймворк OSINT предоставляет исчерпывающий список инструментов (гораздо больше, чем
то, что описано в этой книге) в удобном веб-интерфейсе.
Онлайн-интерфейс (показанный на рисунке 1.1) предоставляет категории и классификации.
для различных источников разведки, что делает его важным контрольным списком (или дорожной картой)
чтобы убедиться, что вы исследуете все возможные источники.
Фреймворк OSINT - отличный ресурс для исследователей и исследователей.
ции, и вы можете найти ее на https://osintframework.com .

OSINT.link

OSINT.link (www.osint.link) предоставляет исчерпывающий ресурс ссылок, поиск
движки и веб-каталоги, предназначенные для сбора информации. Рисунок 1.2.
показывает различные категории "поисковых систем", что является лишь одной из многих
доступные родительские категории доступных ссылок и ресурсов.

IntelТехники

Соавтор и эксперт по OSINT Майкл Баззелл ведет сайт www.inteltechniques .com , который до недавнего времени предоставлял очень полезные социальные сети и поисковые системы. С апреля 2019 года этот сайт больше не является бесплатным и доступен только для платные участники сайта по видео-обучению. Посмотри, что я имею в виду, ты понимаешь, что вы платите за?

Я пользовался этим сайтом много раз, поэтому стоит предложить если вы готовы платить за обучение.

Рисунок 1.1.

Термбин

Я *люблю* Термбина (www.termbin.com).

Были ли вы когда-нибудь в ситуации, когда вы работаете в Linux и вам нужно отправить себе текстовые данные, но не может напрямую передать данные из машина?

Rsync может не подходить, если вы подключены через один или несколько уровней. серверов перехода. Настройка веб-сервера означала бы пробить дыру в брандмауэр, что, вероятно, плохо, так что делать, если вам нужно отправить себе текст с одного из этих серверов?

В этом случае Термбин для вас!

Отправьте содержимое файла на termbin.com с помощью netcat и получите частный ссылка, по которой вы можете скачать свой текст.

Например, давайте отправим Termbin файл с именем неожиданность.txt, используя следующую команду: команда мычания:

```
корень @ osint> кот сюрприз.txt | NC termbin.com 9999
```

Вы получите собственный URL-адрес, который выглядит следующим образом: https://termbin.com/cpc4 .

Рисунок 1.2.

С пониманием

Hunchly - это последнее дополнение к этой книге. Если бы я знал об инструменте
раньше я бы рассмотрел это более подробно в другой главе, потому что это
совершенно фантастический.

Hunchly - это инструмент для онлайн-расследований, который автоматически собирает документы
комментирует и аннотирует каждую посещаемую вами веб-страницу.

Есть так много случаев, когда я хотел бы сохранить конкретный
снимок экрана, или даже когда я знаю, что сохранил его, но я просто не могу его найти. С пониманием
устраняет это, захватив все в вашем браузере и пометив его в
конкретное расследование.

Если вы профессионал в области расследований или даже просто любитель OSINT,
вам обязательно нужно скачать этот инструмент.

Hunchly доступен для Windows, Mac и Linux и напрямую интегрируется
с Chrome для беспроблемной работы. Когда вы будете готовы начать исследование
конкретное расследование, вы можете быстро включить плагин, выбрать который
Дело, над которым вы работаете, и Hunchly сделает все остальное за вас.

Хотел бы я описать этот инструмент более подробно, потому что я мог
правильно сохранить и задокументировать результаты расследования - это невероятно важно.
даже с точки зрения возможности вернуться назад и выяснить, как вы
пришел к определенному выводу.

Hunchly доступен на www.hunch.ly .

Списки слов и генераторы

Использование списков слов будет регулярно появляться в этой книге. Множество универсальных
списки слов доступны, и они, как правило, будут выполнены на большинстве сидячих мест.
uations. Когда вы совершаете перебор или ищете спрятанное сокровище, вы будете
обычно хотят использовать свои собственные варианты списка.

SecLists

Ваша первая остановка должна быть на странице SecLists на GitHub.

SecLists - это страница GitHub, поддерживаемая Даниэлем Мисслером и являющаяся домом для
отличная коллекция множества различных типов словарей, включая имена пользователей,
пароли, комбинации имен, шаблоны данных, фаззинг полезной нагрузки и многое другое.

Загрузите списки слов на странице SecLists GitHub по адресу https://github.com/
danielmiessler / SecLists .

SecLists - отличная отправная точка для создания списков слов. Вы можете использовать следующее:
инструменты для создания собственных списков слов, все из которых доступны в
Kali Linux.

Cewl

Cewl - это настраиваемый генератор списков слов с открытым исходным кодом, предназначенный для создания списков слов.
специфичны для ваших целей. Cewl создает свои списки, отслеживая целевые URL-адреса и
возвращение списков ключевых слов, которые можно использовать при взломе паролей
такие приложения, как JTR.
Если вы хотите составить список ключевых слов, специфичных для вашей цели, Cewl - это
снайперская винтовка, которую вы ищете.
Подумайте, сколько конкретных ключевых слов вы можете получить, удалив
страницы в социальных сетях. Как только у вас появятся эти ключевые слова, вы можете сгенерировать постоянные
с использованием стандартных комбинаций приложения или вашего собственного синтаксиса.
Вы можете скачать Cewl по адресу https://github.com/digininja/CeWL .

Хруст

Crunch - это бесплатный инструмент, который создает сложные и исчерпывающие списки слов, используя
нестандартные шаблоны и перестановки.
Crunch был бы вашим дробным подходом к разработке списка слов, а
отличный инструмент для поиска общедоступных репозиториев с непонятными названиями и
Ковши S3.
Вы можете скачать Crunch по адресу https://sourceforge.net/projects/crunch-
список слов .

Прокси

При запуске OSINT-поиска (например, сканирования NMAP или перебора каталогов)
ing), может иметь смысл использовать прокси, чтобы избежать обнаружения.
Один из вариантов - купить 50 или 100 частных прокси, которые вы можете автоматически
вращать с помощью такого инструмента, как ProxyChains. Доступны сотни прокси-сайтов
где вы можете приобрести частные качественные прокси.
Два моих любимых:

- Известковые прокси (www.limeproxies.com)
- Прокси- кальмары (www.squidproxies.com)

Прокси-серверы Storm (с автоповоротом)

Мой любимый прокси-сайт для OSINT-поиска, расследований и веб-скрапинга
это Storm Proxies (www.stormproxies.com).
Storm Proxies автоматически меняет прокси за вас без необходимости настраивать
ProxyChains или другой ротационный прокси-сервер на вашем сервере. Со штормом
Прокси-серверы, вы отправляете все запросы на определенный IP-адрес, который затем направляет ваш
трафик через один из тысяч собственных частных прокси-серверов.

Вы можете выбрать 3- или 15-минутный прокси, который меняет ваш IP каждый раз.
3 или 15 минут соответственно, или даже отправлять каждый запрос через другой
прокси-сервер (отличный способ избежать обнаружения брандмауэром).
Storm Proxies - платная услуга, но довольно недорогая с учетом суммы.
стоило бы приобрести и управлять сотнями частных прокси самостоятельно.
А теперь слово от Ника Фюрнё: введение в исследование криптовалюты.
валюты.

Криптовалюты 101

Автор: Ник Фюрнё

В конце 2008 года загадочный Сатоши Накамото написал технический документ.
о самосоздающейся, самоуправляемой валюте на основе нового типа базы данных
называется блокчейн. В начале 2009 года проверенная концепция блокчейн-системы под названием
Был создан биткойн, который обещал революционизировать валюты своей моделью
децентрализации - по сути, никакого банковского или государственного контроля. Биткойн имеет
стал чем-то вроде загадки, не совсем подходящей под критерии
валюта, при этом каким-то образом создавая приемлемую стоимость и торгуемость. Самый
комментаторы теперь предпочитают термин *криптоактив,* а не *криптовалюта* .
Концепция блокчейна - это, по сути, умный способ хранения контрактов, таких как
как транзакции с монетами в базе данных, которая защищает свои данные с помощью криптографических
методы и очень затрудняет злоумышленнику изменение записей в данных -
база без значительной вычислительной мощности. Термин *блокчейн* присоединился к другим
технологические термины, такие как *AI* и *Cloud,* которые будут использоваться для продажи систем, которые редко
требовать, чтобы указанные технологии работали хорошо или даже улучшили текущие
методы, но они хорошо подходят для маркетинговых материалов и, следовательно, люди покупают
в них. В 2017 году компания Bioptix сменила название на Riot Blockchain.
и его акции выросли на 394%, и эта тенденция резко изменилась после того, как CNBC
транслировать предположение, что изменение имени было сделано исключительно для повышения
стоимость компании!
С 2009 года было построено много новых криптовалют; на момент написания,
www.coinmarketcap.com содержит 2164 торгуемых криптовалюты разных типов.
Большинство используют вариант блокчейна; однако мы начали видеть разные технологии
такие технологии, как «Клубок», используемые IOTA. Некоторые криптовалюты предоставляют
частичная анонимность пользователей, а некоторые действительно очень анонимны. Выгоды
все очень похожи и включают:

- Отсутствие центрального контролирующего органа
- Отсутствие клиринга средств, что приводит к более быстрым транзакциям.
- Неизменяемая история транзакций

■ Частичная или полная анонимность

Поскольку большинство популярных криптовалют имеют журналы транзакций с открытым исходным кодом, они соответствуют определению открытого исходного кода, и общедоступные реестры могут быть очень полезно для следователя. Однако псевдоанонимные данные, используемые криптовалюты, такие как Биткойн и Эфириум, могут очень затруднить следователь, чтобы разобраться в данных.

Как работают криптовалюты?

Криптовалюты - довольно сложные системы, и написаны целые книги.
об их внутренней работе, которую мы не будем здесь повторять. Тем не мение,
Некоторые подробности будут полезны исследователю OSI.
Адрес криптовалюты - это комбинация букв и цифр, которая
часто представлен в Base58. Обычно они состоят из 34, 42 или даже 96 символов,
хотя есть и другие длины.
Биткойн-адрес выглядит так: 1BoatSLRHtKNngkdXEeobR76b53LETtpyT
Адрес Ethereum выглядит так: 0x89205A3A3b2A69De6Dbf7f01E-
D13B2108B2c43e7
Адрес Monero выглядит так: 44AFFq5kSiGBoZ4NMDwYtN18obc8Aem-
S33DBLWs3H7otXft3XjrpDtQGv7SqSsaBYBb98uNbr2VBBEt7f2wfn3RVGQBEP3A
Адрес - это, по сути, открытый ключ, который пользователь валюты может передать
всем, кто желает отправить им монеты. Однако для перемещения любых монет, хранящихся в
адрес необходим прилагаемый закрытый ключ. (Вы можете найти отличный
обзор систем публичных / приватных ключей здесь: https://medium.com/@vrypan/
объяснение криптографии с открытым ключом для не вундеркиндов-f0994b3c2d5).
Исследуя онлайн, следователь увидит много криптовалюты.
адреса, но это всегда будет адрес открытого ключа. Хотя некоторые
закрытые ключи попадают в сеть из-за утечек или ошибок пользователей, это очень редко
и любые монеты, контролируемые ключом, обычно уже давно исчезнут.
Адреса криптовалюты являются псевдоанонимными в том смысле, что они не являются напрямую
связаны с учетной записью или личностью, но существуют методы, позволяющие определить владельца:
отправьте, даже если это сложно и требует много времени.
Когда пользователь желает отправить значение криптовалюты другому пользователю, он
создать транзакцию, которая будет передана каждому регистру (пользователь полного узла)
этой валюты. Затем так называемые майнеры добавляют транзакции в блок (подумайте о
мысленный образ коробки, полной транзакций) и использовать сверхмощные компьютеры
для решения сложной математической задачи, которая блокирует блок, чтобы данные не могли
легко изменить. Если кто-то пытался изменить элементы транзакции, они
необходимо будет сообщить об этом изменении в каждую бухгалтерскую книгу на планете и
пересчитать математическую задачу. Чем больше блоков для расчета
над блоком, содержащим измененную транзакцию, тем сложнее, или действительно

невозможно, это так.

Исследователи блокчейнов

За исключением некоторых закрытых или очень безопасных криптовалют, реестр
открытый исходный код и, следовательно, полезный ресурс для исследователя. Если следователь
находит адрес подозреваемого, например, в подписи сообщения на форуме.
Например, легко определить значение, которое прошло через
адрес или, возможно, все еще хранится по этому адресу. Для этого нам нужно
используйте проводник блоков. Вы можете найти множество примеров для всех основных валют.
Вот несколько примеров биткойнов:

- www.blockchain.com
- www.blockcypher.com
- www.btc.com

**При использовании blockchain.com найдите адрес и затем прокрутите до бот-
том страницы и щелкните ссылку Дополнительно - Включить. Это предоставит значения для каждого
ввод и вывод.**

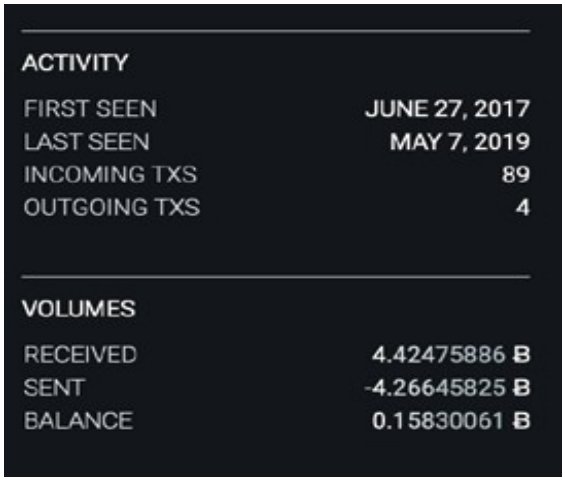
Другие, такие как www.blockchair.com и www.bitinfocharts.com , предоставляют
исследователи для многих валют, таких как Bitcoin, Bitcoin Cash, Dogecoin, Ethe-
reum, Litecoin и другие. По сути, все они отображают одну и ту же информацию
но в разных графических интерфейсах, поэтому важно понимать
первичные элементы.
Давайте посмотрим на blockchain.com/explorer . Здесь мы можем искать биткойн,
Bitcoin Cash или адрес Ethereum. Это вернет список всех транзакций.
где адрес был «вводом», где деньги были выплачены на другой адрес,
или «выход», когда он получил деньги с другого адреса.
Если мы посмотрим на биткойн-адрес, мы увидим блок метаданных вверху.
панель, за которой следует серия транзакций (рис. 1.3).

Рисунок 1.3.



Метаданные об адресе могут быть очень интересными, поскольку они могут помочь нам создать
вверх картинку использования этого адреса. Например, сколько транзакций
был задействован этот адрес? Сколько биткойнов было получено этим
адрес через какое-то время и сколько там осталось сейчас? Значения также имеют график
вариант. Это покажет движение монет во времени. Когда был первый
оплата произведена и какие закономерности мы видим? Получены ли монеты немедленно
переехали или сохранили в адресе? Когда был произведен первый платеж?
Почему эти вопросы важны? Возьмем пример мошенничества, когда
компьютер жертвы заражен вирусом, который шифрует все данные, и
за код разблокировки требуется выкуп в биткойнах. Заданные вопросы могли
сообщите нам, когда, вероятно, началось мошенничество, сколько жертв заплатили мошенникам
адрес, сколько денег было заработано, перемещены ли монеты или
сохранил и так далее. В случае с программой-вымогателем Petya / NoPetya монеты
были сохранены в адресе в течение нескольких дней после выплаты потерпевшим перед переездом
монеты прочь. Это можно четко увидеть, выполнив поиск адреса, используемого
мошенники: 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX. Взглянув
на графике баланса и выделив очевидный пик в июне 2017 г.
легко определить, когда жертвы начали платить, сколько было
получил, и когда монеты были перемещены.
Из графика видно, что выплаты начались 27 июня 2017 г., а первичный
выплаты были завершены до 28 июня 2017 года. Монеты оставались в адресе до июля.
4 августа 2017 г., когда они были заключены. Это помогает нам понять жизненный цикл
аферы; выплаты жертвам действительно происходили в течение 24 часов и
хранятся в адресе всего несколько дней, прежде чем они были перемещены. Нет
были произведены другие существенные выплаты. Это хороший пример того, как метаданные
всего один адрес может помочь нам составить представление об адресе, использованном в преступлении.
Количество выплат может помочь нам определить вероятное количество жертв,
и сайт под названием https://oxt.me помогает нам в этом. Просмотрите к
сайт и посмотрите адрес 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
снова (рисунок 1.4).

Рисунок 1.4.

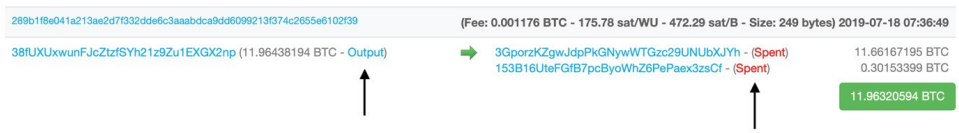


Я считаю эти данные очень полезными, поскольку они быстро перестают работать, когда адрес начал использоваться, когда его видели в последний раз, и отдельные значения для монет получил и отправил. Также разбивка входящих и исходящих транзакций помогает нам понять, в этом примере, количество вероятных жертв, 89 входящих платежи, и сколько адресов было использовано для перемещения монет подальше от мошеннического адреса. Если бы мы анализировали платежи в незаконный темный-Интернет-магазин, например, то входящие платежи, скорее всего, будут покупателями.

Жертвами мошенничества обычно являются новички в области криптовалюты, и поэтому они склонны к гоняйте монеты прямо с биржи и отправляйте их мошеннику. Если обмен можно идентифицировать, легко сделать запрос на обмен на KYC (Know Your Заказчик) информация и контактные данные потерпевших.

Следуя за деньгами

Когда следователи описывают расследования криптовалюты, они часто имеют в виду после некоторых видов незаконных платежей от исходного адреса до места назначения. Из-за псевдоанонимного характера криптовалют, таких как Биткойн с его 34-символьная адресация Base58 сложно достичь. Что я описываю как «Адресная слепота» может быстро устанавливаться при переходе от транзакции к транзакции. Переход от транзакции к транзакции немного отличается во всех различных исследователи блокчейнов. Используя Blockchain.info, вы используете выделенный «Израсходованный» ссылка на выходной стороне транзакции для перехода к следующей / более поздней транзакции, и довольно сбивает с толку ссылку «Вывод» на стороне ввода транзакции. Чтобы вернуться к предыдущей транзакции



(рисунок 1.5).

Предположим на мгновение, что вы получили сообщение о том, что биткойн
адрес на рисунке 1.5 (38fUXUxwunFJcZtzfSYh21z9Zu1EXGX2np) является мошенничеством
адрес. Имеет 11.964. . . Биткойн в нем. куда деваются деньги? Мы можем увидеть
что 11.66 идет по адресу 3Gpor. . . и небольшая сумма до 153b. . . .

Я использую только первые пять символов при аннотации адресов биткойнов. В паттерны запоминаются гораздо эффективнее, чем 34 символа, и помогают с адресная слепота. Не волнуйтесь, что вы увидите другой адрес с теми же пятью символы; это работает как (забывая, что первый символ равен 1 или 3) 34 * 34 * 34 * 34, что составляет более 1,3 миллиона перестановок!

Рисунок 1.5.

Затем нам нужно выяснить, является ли один из адресов платежным. в
подавляющее большинство транзакций с адресами типа "один ко многим" или "многие ко многим",
один из выходов будет измененным адресом. Причина в том, что каждый биткойн
состоит из 100 миллионов сатоши, поэтому вероятность того, что выплаты нескольким
Адреса будут складываться в точности до крошечных входных сумм. В этом примере
оплата из кошелька «3». Биткойн-адреса, начинающиеся с цифры 3
используются для мультиподписи или более сложных транзакций, чем просто прямая
адресная оплата. Выходы предназначены для 3-го адреса и для 1-го адреса.
Значительно более вероятно, что адрес изменения также является адресом 3. Следовательно
мы можем сделать вывод, что адрес 3 - это сдача, а адрес 1 - платеж.
Существуют и другие методы определения того, какой выходной адрес является изменением.
адрес. Например, на рис. 1.6 за любой из трех входов можно было бы заплатить
3HfFw. . . оплата, но все 3 нужны для суммы, отправленной на 3B5kC. Этот
помогает нам сделать вывод, что адресом изменения является адрес 3HfFw, и, следовательно, мы
нужно следовать за другим.
Как только мы определили адрес или адреса, по которым возможны платежи,
мы можем проследить за ними до следующей транзакции, нажав кнопку «Израсходовано». В этом
Например, оба выхода неизрасходованы, так что мы в тупике.
Щелчок по следующей или предыдущей транзакции просто предоставит другой список
входы и выходы, и следователь может сразу потеряться. Я рекомендую
останавливаться после каждого щелчка и изучать адреса, и строить картину
еще раз, прежде чем двигаться дальше. После того, как вы переместили две-три транзакции из
ваша отправная точка, опыт показывает, что вы часто выходите за рамки
изучение. Если только ваш подозреваемый не использует миксеры и тумблеры для перемещения и разделения
монеты, за которыми крайне сложно следить без помощи рекламы
инструмент, то выплаты процентов, как правило, происходят в пределах нескольких транзакций вашего
Начальная точка.
Я работал над многочисленными сделками, где это правда. Есть даже
контртеррористическое расследование, в котором люди, жертвующие «делу», просто
покупка на биржах и пожертвование прямо группе, а затем деньги
были обналичены всего за один или два прыжка на другую биржу. Вы могли нарисовать
весь график транзакции на небольшом листе бумаги.
Конечно, бывают случаи, когда преступники очень изощренны и
пойдут на чрезвычайные меры, чтобы запутать их конечный пункт назначения через



Рı

разделение и рекомбинация монет, перемещение через биржи или обмен на
другие валюты. Вот где коммерческие инструменты действительно вступают в свои права.

Выявление бирж и трейдеров

Переход от транзакции к транзакции прост, но принципиально
бессмысленно, если мы не сможем определить надежный и реальный ресурс, который
может иметь информацию о KYC или данные журнала, такие как IP-адреса. Выявление этих
ресурсы - ключ к успеху в большинстве расследований. Следует отметить, что это невозможно
отслеживать через обмен. Внесение монеты на биржу с последующим внесением
вывод не вернет вам ту же монету, как если бы вы заплатили 10 долларов в
банк, а затем сняв его в банкомате, вернет ту же купюру. Один раз
внесен депозит, ваш единственный шанс на отслеживание - биржа работает
с вами, чтобы предоставить необходимые данные KYC.
Некоторые веб-сайты пытаются идентифицировать адреса, принадлежащие биржам и
торговцы; самые надежные - www.walletexplorer.com и www.bitcoinwhoswho.
com . Последний сайт также имеет функцию отчетов о мошенничестве и также выполняет поиск в Интернете.
ищите упоминания об адресах, которые вы искали.
Walletexplorer.com пытается использовать методы кластеризации для определения одного
адрес, а затем сделать вывод о владении другими адресами, принадлежащими той же организации.
Это тот же метод, который используется в коммерческих предложениях программного обеспечения, но без
бюджет! Процесс прост: внесите депозит на биржу, и они
предоставит платежный адрес; выведите монету, и вы увидите ввод
адрес. Теперь у вас есть два адреса, которые, как вы знаете, принадлежат бирже.
Затем используйте методы и алгоритмы кластеризации, чтобы найти другие адреса.
принадлежит одному и тому же лицу. Полное обсуждение кластеризации выходит за рамки этого введения.
д.), но в качестве примера ищите транзакции, в которых известный адрес и
входной адрес используется совместно с другими входными адресами. Вполне вероятно, что те
адреса принадлежат одному и тому же лицу.
Именно здесь коммерческие инструменты выгодны, и если вы серьезно относитесь к инвестированию,
Если вы столкнетесь с преступлениями, связанными с криптовалютой, ваша жизнь будет действительно очень тяжелой
без покупки одного из основных инструментов. Все инструменты пытаются идентифицировать
кластеры адресов, принадлежащие биржам, трейдерам, даркверб-сайтам и т. д.
в помощь следователю. Большинство из них имеют возможности визуализации, чтобы сделать работу
отслеживания вашей подозрительной транзакции на биржу или другое известное лицо
намного легче.
На момент написания основными коммерческими инструментами были:

- Chainalysis (chainalysis.com)
- Ciphertrace (ciphertrace.com)
- Elliptic (www.elliptic.co)

Maltego (не описанный в этой книге) также предлагает бесплатные преобразования, доступные для установки. из хаба. Они предоставляются blockchain.com и обеспечивают преобразования для определения адресов ввода и вывода транзакций. Это может быть очень полезно как недорогой инструмент визуализации. Ciphertrace также продает преобразования для предоставления доступа в свою базу данных идентификации биткойнов от Maltego.

Резюме

В этой главе представлен обзор типов контента и инструментов, которые вы можете ожидайте найти в этой книге. Эта глава также предоставила несколько технические ресурсы, которые следует считать основными в вашем путешествии по эта книга и будущие исследования.

В следующей главе будет представлена справочная информация и рассказы, касающиеся группам злоумышленников, таким как The Dark Overlord и Gnostic Players, и будут заложить основу для расследования киберпреступников.

19

2

В этой главе основное внимание будет уделено тому, что значит быть кибер-расследователем. Мы будем углубиться в различные типы исследователей и ролей исследователей, некоторые моральные проблемы, с которыми вы можете столкнуться, и разные пути, которые вам, возможно, придется избрать чтобы завершить ваше исследование. В этой главе также будет представлен обзор и знакомство с различными участниками и группами угроз, которые будут обсуждаться всюду по этой книге.

Прежде чем мы начнем, я хотел бы извиниться за буквально море имен пользователей. и псевдонимы, которые я буду кидать вам в этой книге. Некоторая угроза актеры используют разные псевдонимы на каждом форуме или веб-сайте, в то время как более опытные навязанные субъекты намеренно будут использовать псевдонимы, принадлежащие другим известным хакерам. в сообществе. Также известен как «Взлом псевдонима». Это может быть невероятно расстраивает и сбивает с толку, что усугубляется тем фактом, что злоумышленники могут даже поменяться псевдонимами внутри своей группы, чтобы сбить с толку следователей или закон исполнение.

Путь следователя

Цитируя Дракса из « *Стражей Галактики 2»* , «в *этом мире есть два типа людей. Мир. Те, кто танцуют, и те, кто нет* ».

Я чувствую, что это довольно точное суммирование для фундаментального вопроса. в том, как вы проводите расследование: хотите ли вы участвовать в

Расследования и исполнители угроз

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

людей и организации, которых вы расследуете, или вы хотите скрыться
режим и спокойно наблюдать?

В зависимости от вашей работы есть большая вероятность, что этот ответ будет предоставлен
вам на основании корпоративных и правовых норм. У некоторых компаний есть строгие
политика невзаимодействия. В этом случае вам не нужно решать. Во многих случаях
однако здесь будет некоторая свобода действий, так что вам решать, как
вы планируете собирать вашу информацию.

Очевидно, что у каждого стиля есть свои достоинства и недостатки. Я пер-
По слухам, никогда не был человеком, который спокойно сидел бы и наблюдал. Так мой мозг
подключен - мне нужно постоянно находиться в движении. Так что для меня я должен принять участие.

Со щитом или на щите

Обычно я манипулирую четырьмя или пятью активными псевдонимами одновременно. У каждого псевдонима есть
история на обложке и немного предыстории персонажей. Я стараюсь по-настоящему погрузиться в
что бы я ни делал, поэтому, если я смотрю на русского кардера, я могу попробовать
с ломаным английским акцентом и используйте имя, которое несколько знакомо в этих кругах.
Также я всегда буду стараться сыграть под другим именем актера. Люди меняют псевдонимы и
контактную информацию так часто, что очень легко создать новую учетную запись с
похожее имя и попытайтесь связаться с людьми в их сети. Угон псевдонима
имеет много преимуществ, и если вы хорошо разбираетесь в социальной инженерии, вы можете
используйте более старый псевдоним, чтобы быстро поднять свой рейтинг. Если вы убедительны,
есть большая вероятность, что вам повезет и вы поговорите с кем-то, кто думает о вас
кто-то, кого они знали.

Но опять же, все зависит от ваших целей.

**Я думаю, что важно помнить об открытых источниках информации, OSINT, это
что на самом деле это просто информация из *открытых источников,* пока вы не сможете сделать ее *действенной* .
Например, если вы собираете информацию о корпорации или готовитесь к
широкомасштабная фишинговая кампания, вы будете искать совсем другую информацию, чем
вы были бы за то, чтобы нацелить подводную рыбу на одного конкретного человека. Вы будете искать
больше информации о целевой сети и событиях, которые могут происходить с
компания в целом, а не события, которые могут происходить с отдельным лицом.
Поэтому, когда вы начинаете свое расследование, действительно важно сделать шаг назад.
и спросите себя, почему вы исследуете эту цель. Если вы хотите выполнить
Spearfish, то это как бы открывает совершенно другой путь для расследования, потому что
вам нужно гораздо больше заботиться о том, кто этот актер, и о конкретных особенностях этого человека.
Что ими движет? С кем они взаимодействуют?
Тогда следующий вопрос, который вы хотите задать себе - в рамках
участие - как вы можете связаться с этим человеком? А потом, какой у тебя интеллект
на самом деле хотите? Потому что даже если определенная информация, например, жилищные записи, может быть
полезно в определенных контекстах, вы не будете использовать эту информацию, чтобы пытаться ловить рыбу**

ваша цель.

---

21 год

Если это разрешено в соответствии с руководящими принципами вашего расследования, прямой контакт с вашей целью, очевидно, может предоставить вам информацию, которой вы, возможно, никогда не будете смог найти в сети. Прямое общение с вашими целями может быть чрезвычайно полезным.
Сиальный - и чрезвычайно опасный. Если вы не будете осторожны, прямой контакт с реальной угрозой актер или преступник могут иметь очень серьезные последствия для следствия.

При взаимодействии с злоумышленниками мне очень нравится придумывать прикрытие.
рассказы и попытки напрямую участвовать в группах, которые я исследую.
Одним из «бонусов» вашего пути в одну из этих групп является то, что они *всегда*
занятый. Чем больше вы узнаете их лично и тем больше они вам доверяют,
тем больше вероятность, что они поделятся с вами новой информацией.
Они всегда работают над новым хаком, и, как только вы окажетесь в их внутреннем мире,
круг, они, как правило, более чем готовы хвастаться своими последними хитростями или
подвиги.
Я чувствую, что такой практический сбор информации об угрозах отсутствует в
большинство организаций. Большинство групп разведки угроз, с которыми я столкнулся, ищут
пассивная информация, но очень немногие из тех, кого я видел, активно ищут ее.
Возможно, вы думаете про себя: «Да, все это звучит великолепно и захватывающе,
но насколько это полезно? Стоит ли прилагать усилия? »
Я рад, что вы спросили.

Нарушение, которого никогда не было

Однажды вечером я написал письмо генеральному директору и генеральному директору по информационной безопасности крупной авиакомпании.
Заголовок гласил: «- СРОЧНО - нарушение данных в вашей сети». Я получил телефон
перезвонил позже тем же вечером и сообщил администратору службы безопасности, что я
получил сообщение от одного из моих контактов в дарквебе, что данные из их сети
вот-вот поступит в продажу.
В частности, данные «собирались» поступить в продажу, потому что хакер все еще
в их сети, извлекая данные.
Они сказали, что изучат это, и примерно через два дня вернулись в
меня. *Они не смогли найти доказательств того, что кто-то был в их сети или взломал их системы* .
Хакер также продавал доступ к сети (обычная практика), поэтому я
обратился к хакеру и попросил подтверждение доступа, прежде чем я завершил
покупка. Он был достаточно любезен, чтобы предоставить мне скриншоты живого общения.
мандаты, которые он запускал в сети компании, которая также включала
список учетных записей администратора компании.
Ниже приводится часть вывода, которую я предоставил в качестве доказательства доступа к
сеть:

```
маяк> оболочка сетевая группа "администраторы домена" / домен
```

[*] Заданный маяк для запуска: сетевая группа "администраторы домена" / домен
[+] хост позвонил домой, отправлено: 64 байта

[+] получил вывод:
Запрос будет обработан на контроллере домена для домена ***. Com.
Имя группы Администраторы домена
Комментарий
Назначенные администраторы домена
Члены
---------- ----------
A ****
a ****
a ****
A ****
A ****
A ****
A ****
a ****
a ****
A ****
a ****
A ****
M ****
SP ****
svc _ ****
svc _ ****
Команда успешно выполнена.

Что бы вы сделали?

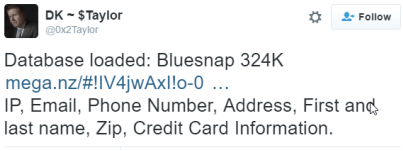
Этот сценарий поставил меня перед большой дилеммой. С одной стороны, я мог это выдержать
новую информацию и представить ее компании, чтобы они могли найти и заблокировать
хакерам до того, как кража их данных была завершена.
С другой стороны, это будет означать, что хакеры, скорее всего,
понимают, что я утечка, и выталкивают меня из своего круга. Месяцы упорной работы
проникновение в их ряды будет отброшено, а мои псевдонимы будут взорваны.
Что бы вы сделали?
Я решил снова связаться с компанией и сообщить, что у меня есть еще
Информация. Я также дал им понять, что предоставление им этой информации легко
взорвать мое прикрытие, так что я был бы очень признателен, если бы они предоставили мне что-нибудь
разведданные, которые они собрали в ходе расследования. Я уже знал как они
смогли получить доступ, поэтому я специально следил за IP-адресами, использованными в атаке.
Они согласились ответить взаимностью.
Эта компания не была одним из моих клиентов, и у меня не было предыдущих отношений.
отправляйте вместе с кем-либо из их команды безопасности. Я знал, что попадая в эту ситуацию,
они не были обязаны предоставлять мне что-либо после того, как я предоставил
им мой конец информации.

Я все равно решил двигаться вперед, борясь со своей естественной склонностью предполагать
они не будут сдерживать свою часть сделки. Я отправил информацию обратно в
admin в авиакомпании и (что неудивительно) не получил ответа.
Спустя еще два дня без ответа на электронные письма мне позвонили из
админ. Он сказал, что ценит мою помощь - они смогли найти пользователя, потому что
данных, которые я предоставил, и успешно выгнал хакера из их сети.
К сожалению, вмешался юрист, и он даже не должен был разговаривать с
меня. Из-за всех публикаций в прессе и раскрытия информации о нарушениях, связанных с
Меня зовут, компания боялась, что я обращусь к СМИ с информацией.

По крайней мере, он был достаточно любезен, чтобы перезвонить мне и сказать, что информация
был реальным, но он не мог дать мне никакой другой информации.
Организация в конечном итоге так и не раскрыла и решила полностью игнорировать
ситуация. Вы должны помнить об этом, когда решаете, что делать с
информацию, которую вы обнаружили.

Да, мой контакт перестал со мной разговаривать. Ему было нетрудно понять
выяснилось, что я был причиной того, что он был выгружен из сети. Я разговаривал с номером
других компаний по разведке угроз, чья позиция очень ясна: никогда
вовлечены, вероятно, именно по этой причине.
Иногда бывает сложно заставить клиента признать, что данные принадлежат им.
Вот Трой Хант, владелец «Have I Been Pwned» (www.haveibeenpwned.com), с
похожая история.

Некоторое время назад в Твиттере был парень, которого звали 0x2Taylor. Он просто постоянно был
сбрасывая довольно полно всякой всячины. Просто бац! Полные взломанные данные прямо на его временной шкале. А
пару лет назад он выбросил тот, у которого были сотни тысяч платежных записей
от компании Blue Snap



(рис. 2.1).

Полные, законные платежные записи, включая полные номера карт, CVV, дом человека
адрес, телефон, все работы. Все в открытом виде. Когда я прошел и
начал просматривать данные, я увидел много ссылок на компанию под названием Regpack. Это
было немного странно, потому что данные были представлены как одно целое (Blue Snap),
но глядя на данные подразумевает другого владельца.
Я обнаружил, что Regpack запускает службу регистрации, которую вы можете встроить в
ваш веб-хостинг. С небольшим количеством JavaScript, будь то группа скаутов или школа
благотворительность, теперь вы можете принимать платежи на своем сайте.
Цитата из Regpack гласила: «Мы запустили полный протокол безопасности.
в этих случаях и окончательно определить, что наши серверы не были задействованы ». потом
буквально на следующий день они оборачиваются и выдают следующее утверждение, что данные
действительно исходил от них.

Их заявление гласило: «Мы определили, что эти расшифрованные файлы, которые должны быть доступны общедоступному серверу, и это было источником этой потери ». Затем они продолжают и говорят: «Системы Regpack не были взломаны».
Рисунок 2.1.

Но есть 324 000 платежных записей, представленных в виде простого текста. . . . Так что случилось? Если это не была утечка данных, то что же это было? Они сказали, что это был «инцидент с данными». Не «Нарушение», но инцидент с данными. Да ладно тебе. . . пожалуйста.
Мне как бы интересно, пытались ли они избежать слова о *нарушении,* потому что у них какое-то конкретное нормативное обязательство, которое применялось бы, если бы у них действительно была нарушение . . . но вы только что слили сотни тысяч полных номеров счетов и Коды CVV. У вас есть нормативное требование к PCI DSS, которое вас ударит уже.
Всегда весело иметь дело с людьми, которые будут отрицать, что данные исходят от них. несмотря на неопровержимые доказательства.

Моральные серые области

В ходе расследования вы неизбежно придете к числу морально серых зон. Ищет ли он утечки общедоступных данных, расследует субъекты угроз или даже проникновение в определенные группы угроз, всегда есть линия что вам, возможно, придется перейти, чтобы достичь своих целей.

Субъекты угроз и преступники никогда не будут уважать моральные или юридические границы, поэтому это может быть немедленным красным флагом, если они увидят, что вы пытаетесь отстаивать некоторые моральный стандарт. Следует иметь в виду, что преступление - это их средства к существованию. Кибер преступники здесь, чтобы зарабатывать деньги, так что кто-то законно присутствует на сцене для те же причины неизбежно приведут разговор к чему-то противозаконному.

Зачем ты там, если не для заработка? Обычно это первая и самая очевидный красный флаг, и почему так много следователей обнаруживаются немедленно. Этих сценариев возникает довольно часто, особенно во время социальной инженерии, что по определению означает, что вы лжете. Обсуждаю несколько собственных сценариев в главе 15, когда мы больше углубимся в социальную инженерию. А пока вот очень интересная точка зрения Джона Стрэнда.

Когда ВИДИТ цель, нет ничего сильнее ненависти. Где, если вы начнете троллить кого-то, например, если он очень религиозный человек, а вы подходите к нему и говорите: «Ну, я атеист, и все, во что ты веришь, неправильно, Иисус был сфабрикован. идея Римской империи по контролю над евреями », и это действительно рассердило людей. Вы их рассердите, можете дать им ссылки и подумать: «Вот ссылка на этом сайте опровергает все, во что вы верите ». Этот человек собирается щелкнуть эта ссылка.
Обратной стороной этого является то, что большинство наших клиентов никогда не позволят нам зайти так далеко. потому что это довольно неприятная территория.
Это определенно пересекает черту, и я думаю, что если вы можете рассказать об этом в книге, мы сделаем это. это профессионально. Мы делаем очень злые дела с контрактом, и когда вы начинаете говорить о социальной инженерии, когда вы начинаете говорить о разведке, особенно об отдельных uals, вы действительно приближаетесь к линии, где она размывается из-за помолвки и это начинает размываться во что-то более личное.

25

Знание того, где эта линия существует, - вот что многие люди в этом
промышленность не имеет, пока они не пересекут ее. Они не понимают, что сделали не так,
и я думаю, что это важная концепция. Итак, вы знаете, это номер один.
Во-вторых, я действительно большой поклонник разведки против злых людей. Как ты можешь сделать
разведка против противника? Кибер-атрибуция. Есть некоторые инструменты, которые я люблю использовать, если
мы пытаемся получить некоторый уровень кибер-атрибуции. Медовый барсук, написанный мета-инструмент
Автор [Тим Томес 00:11:03], когда он работал в HIS, это замечательный инструмент, в котором
если вы можете побудить противника запустить апплет, запустить документ Word или Excel
таблицу с макросом, мы можем определить местоположение этого человека в пределах 20 метров.
Если вы перейдете в Canary Tokens, у них есть удивительные токены, которые вы можете создать в Word.
документы, PDF-файлы, ключи AWS. Настройте что-нибудь, если злоумышленник клонирует ваш
веб-сайт, он вернется, и это тоже форма разведки. Это целая форма разведки
против злоумышленников и кибер-атрибуции с помощью веб-ошибок Word, из-за которых многие люди
в индустрии об этом не думают. Многие инструменты и методы, которые у нас есть,
красные команды, они могут быть очень эффективны в сфере синих команд, чтобы получить высокую степень
уверенность в кибер-атрибуции против злоумышленника, если вы знаете, как их использовать
должным образом.

Различные следственные пути

Вы можете выбрать множество различных карьерных путей, связанных с кибер-исследованиями.
gations. В роли реагирования на инциденты вы, скорее всего, сосредоточитесь на расследовании.
Отражение преступления больше, чем преступников. Если вы работаете в службе безопасности
center (SOC), возможно, вы хотите проверить и понять различные типы
потенциальных угроз, исходящих от вас с множества различных форумов каналов данных.
Даже в этом случае ваша отрасль может диктовать тип следственной работы, которую вы выполняете.
или ваша роль может включать как проактивную, так и реактивную следственную работу.

Я бы сказал, что львиная доля моего времени делится между охотой, которая носит активный характер,
и реагирование на инциденты, реактивное.
Мы очень активно участвуем в выявлении продвинутых противников. Не обязательно
приписывая их национальным государствам, но относя их к организованным группам, к недо-
положение, какие группы занимаются какими видами деятельности, на кого они нацелены и как
они нацелены на них.
Мы хорошо осведомлены о конкретных группах актеров, о том, на кого они нападают и
как они это делают. Мы всегда пытаемся собрать больше информации о том, кто там
в промышленном пространстве сеют хаос. Это основная часть нашего бизнеса и нашей
общественная работа также заключается в выявлении противоборствующих групп и понимании того, как они
работать.

26 год

Как и при любом реагировании на инцидент, не вызывает большого удовольствия видеть людей, пойманных за нападения, которые они вызвали. Это не наше место как охранной фирмы. Это требует международное правоохранительное сотрудничество.

Но мы всегда стараемся улучшить наше обнаружение и предотвращение на основе того, что мы знаем, как действуют противники, как они должны действовать, как они функционировал. Это основная часть эффективного реагирования на инциденты и обеспечения безопасности. операции.

Например, в случае с промышленными игроками есть вещи, которые продвинутые противники больше занимаются математикой, например, разведкой, эти вещи довольно легко отследить потому что они поступают одновременно с множеством организаций. Уникальный и новые атаки на системы, например, кинетическое воздействие на системы, есть вещи, которые используются повторно, но обычно они настолько передовые и новаторские, что много новинок.

Я в основном разделяю атаки на промышленные системы, которые происходят правильно теперь на три категории. Первый - это продвинутые противники. Человек который либо проводят разведку и строят плацдармы внутри промышленных сетей, либо активно в некоторых редких случаях запускает атаки.

Затем есть категория инсайдеров, и они существуют уже давно. время. Обычно это недовольные сотрудники-инсайдеры, у которых слишком много системного доступ или сохранить доступ после того, как они закрыты, и они решают все испортить через логические сценарии типа бомбы или просто используя свои знания о слабости системы. потребности и уязвимости, чтобы потом что-то подделать. Подобные инциденты случаются все время, но обычно об этом не попадают в новости, если только нет большого гражданского влияние; но инсайдеры всегда проблема.

И наконец, товарные атаки. Вы получаете вымогательское ПО на промышленном сеть, на которой работают компьютеры с Windows, и это окажет некоторое влияние, особенно если это системы с низким уровнем ресурсов, системы, которые используются в качестве интерфейсов для системных Темы, человеко-машинные интерфейсы, мониторинг поведения и безопасности системы и т. д. Те определенно могут иметь непредвиденные последствия.

Для более продвинутых противников мы всегда видим диапазон разведки и основные точки опоры в промышленных системах, а затем мы видим эти новые атаки которые реже возникают против отдельных систем, особенно в местах, которые используются в качестве Испытательные стенды продвинутых противников.

Расследование киберпреступников

В зависимости от вашей роли расследование киберпреступности может включать в себя изучение технические аспекты преступления (например, понимание того, как произошел взлом), или может включать исследования и атрибуцию самих преступников.

Ключевой элемент любого кибер-расследования обычно включает в себя некоторый уровень понимание субъектов угрозы и того, как они действуют. Особенно во время нарушение, понимание преступной группы и их MO (*modus operandi*)

может предоставить важную информацию, например, как они получили первоначальный доступ, их опорные точки сети, файлы, которые они обычно просматривают, и многое другое.

Примеры и сценарии в этой книге взяты из моего реального опыта. расследование и взаимодействие с Темным Повелителем (TDO) и Гностическими игроками группы. Многие из примеров в главах этой книги могут упоминать группа как коллектив, ее отдельные члены или одно из их множества псевдонимов.

Начало охоты (для TDO)

Однажды, примерно в 2017 году, друг сказал мне, что у одного из их филиалов вымогали «Темный Повелитель», и спросил, знаю ли я что-нибудь о них. В этот момент в время, я помню, как группа была во всех новостях за попытку вымогательства у Netflix, и угрожая выпустить предварительные копии *Orange Is the New Black* , и взломать продавать / продавать данные, украденные у десятков поставщиков медицинских услуг.

В тот день почти два года назад я бросился в темную паутину киберпреступное подполье. Это не было оплачиваемым мероприятием; это было больше похоже на это новое увлекательное хобби, которым ты не можешь насытиться.

Отслеживание группы за последние несколько лет было одним из самых захватывающих и полезный опыт моей жизни. Я встретил столько интересных людей, и узнали так много о технологиях и человеческом поведении на своем пути.

В некотором смысле, я полагаю, мне следует их поблагодарить. Если бы не группа детское, противозаконное и развратное поведение, я бы не стал этот путь, и не писал бы эту книгу.

Темный повелитель

В 2016 году хакерская группа, известная как The Dark Overlord (TDO), начала терроризировать и вымогатели. Группа быстро стала известна во всем СМИ от большого количества взломов медицинских провайдеров. Некоторые из их первые опубликованные хакеры включали Среднезападную ортопедическую клинику боли и позвоночника в Фармингтон, Миссури; Midwest Imaging Center, LLC; и Van Ness Orthopaedic и спортивная медицина.

Как упоминалось ранее, в 2017 году группа получила дополнительные заголовки по взлом Netflix и угроза выпустить предварительные копии *Orange Is the New Блэк,* если их требования выкупа не будут выполнены.

Позже в том же году группа перешла от традиционного «взлома» к большему терроризму. основанные атаки. Группа угрожала расправой родителям студентов в Водопад Колумбия, штат Монтана, школьные округа, в результате чего было закрыто более 30 школ и вынуждает более 15 000 учеников оставаться дома на всю неделю.

Группа регулярно публиковала свои требования и последние взломы в Twitter, со вспомогательной информацией о Pastebin. Изображение на рис. 2.2 - это группа официальный аватар, картина сирийской художницы Аулы Аль Аюби. В следующих разделах представлена сводная информация о группе история, его мотивы и информация о каждом из его членов.

Список жертв

Следующие ниже организации публично заявили о нападениях или вымогательстве. пользователя The Dark Overlord. Это не исчерпывающий список всех жертв TDO. А ряд организаций не объявили о своем участии в группе.

Нахождение в этом списке не означает успешного взлома или выкупа **. Это просто означает, что существует публичная запись о том, что организация была взломана или терроризирована группа каким-то образом. DataBreaches.net поддерживает отличный публичный рекорд из многих хаков группы.**



Рисунок 2.2.

■ AM Pinard et Fils, Inc.

■ Студия ABC / Стив Харви

■ Внутренняя медицина взрослых H. Скоттсдейл

■ Эстетическая стоматология
■ Всеамериканские развлечения
■ Американские технические службы
■ Ортопедическая клиника Афин
■ Auburn Eyecare
■ Мануальная терапия Остина
■ Налоговая служба ЦБ
■ Детская стоматология Coliseum
■ Columbia Falls, MT
■ Студия Диснея

■ Dougherty Laser Vision
■ Заголовок DRI
■ Центр поддержки семьи
■ Файнштейн и Роу
■ Школьный округ Флэтхед-Фолс
■ GS Polymers
■ клей Gorilla Glue
■ HE Parts Morgan
■ Специалисты по реабилитации рук
■ Hiscox (мистификация)
■ Голландская хирургия глаза и лазер
Центр
■ Джинсы Indigofera
■ Международный текстиль и одежда
■ Общественная школа Джонстона
Округ
■ La Parfumerie Europe
■ Центр косметики La Quinta
Стоматология
■ Строка 204
■ Онкологическая служба Little Red Door
Центрально-Восточной Индианы
■ Lloyd's of London
■ Пластическая хирургия Лондонского моста
■ Марко Зеннер
■ Menlo Park Dental
■ Mercy Healthcare
■ Центр визуализации Среднего Запада
■ Ортопедическая клиника Среднего Запада
■ Центр боли в минеральной зоне
■ Netflix / Larson Studios
■ OG Gastrocare
■ PcWorks, LLC
■ Ортопедическая клиника Пичтри

- Photo-Verdaine
- Технология PilotFish (PFT)
- Pre-Con Products
- Протезирование и ортопедическая помощь
- Purity Bakery Bahamas
- Quest Records, LLC
- Королевский банк Канады
- Саксонские партнеры
- Школьный округ 6
- Выберите "Боль и позвоночник".
- SMART физиотерапия
- Система здравоохранения Св. Франциска

- Хирургический центр Тампа-Бэй
- UniQoptics, LLC
- Ортопедия и спорт Van Ness

Медицина

- WestPark Capital

Краткий обзор

Считается, что изначально группа приобрела протокол удаленного рабочего стола (RDP).
доступ в свою первую медицинскую клинику, купив доступ в Xdedic, дарквебе
торговая площадка, которая продавала недорогой доступ к взломанным компьютерам по всему миру.
Считается, что оттуда группа смогла получить доступ к дальнейшим
клиники и медицинские учреждения с помощью медицинского программного обеспечения HL7. В интервью
С databreaches.net представитель TDO сделал следующее заявление:

«. . . Я использовал код [HL7], чтобы найти эксплойты во всех их клиентах. . . . Кроме того, поскольку я был в их системе я подписал бэкдор в их клиент, потому что у меня был доступ к их подписание сертификата. Он был выпущен в обновлении несколько недель назад ».

Преследуемые компании различались по размеру и отрасли, и их часто спрашивали
платить чрезмерные суммы денег в обмен на их конфиденциальность
документы, опубликованные в Интернете.
Помимо взлома медицинских учреждений, группа также регулярно атаковала
клиники пластической хирургии, угрожающие выпустить до и после операции по увеличению груди
фотографии известных голливудских пациентов.
TDO сдержит свое слово и предоставит информацию, если их требования
не встречались. Совсем недавно группа слила обнаженные фото Фрэнки Эссекса, когда
London Bridge Plastic Surgery отказалась оплатить требования группы о выкупе.

Стиль общения

Официальные сообщения от группы стандартизированы против «Королевы
Английский." Члены группы строго придерживались этого диалекта на протяжении всей жизни.
все их коммуникации. Прямое общение с TDO всегда содержит
высокий уровень помпезности, особенно при обсуждении бизнеса или их «взлома».
навыки ».
Персонажи сохраняют образ работы в большой организации,
и регулярно называют себя «мы».
TDO очень тщательно описывали свою деловую смекалку и часто
опишите успех созданного ими «бренда».
Когда группа только начала свою деятельность в 2016 году, общение через свой аккаунт в Твиттере
Судя по всему, исходил от кого-то с ломаным английским языком.
По мере того, как группа повзрослела, они сформировали более формальный образ со стандартными
Они использовали формальный английский, возможно, чтобы создать видимость, что они были из Великобритании.
После смены руководства в 2017 году общий тон группы

становился все более враждебным. Связь с организациями потерпевших стала
значительно более агрессивным, как и тон группы в Твиттере.
Этот переход также отмечает тенденции группы к менее традиционным хакерским атакам.
и других террористических атак, о чем свидетельствует их поведение при отправке
угрозы убийством ученикам школьных округов Колумбия-Фолс.

Структура и члены группы

Я считаю, что группа The Dark Overlord состояла из четырех основных членов и небольшого
сеть «подрядчиков», которые выполняли черную работу. Доказательства также предполагают
Группу Dark Overlord свободно и неофициально возглавляет администратор Сайпер.
форума KickAss.

---

31 год

Группа была сформирована примерно в 2015 году, где каждый из участников встретился в аду,
старый форум взлома даркнета. Арни был первым общественным лидером группы,
в то время как Cr00k оказался лицом, ответственным за продажу украденных данных и
общий маркетинг.
Каждый из членов группы сыграл свою роль во взломе различных жертв. В
В 2017 году TDO публично объявила в Твиттере, что находится под новым руководством.
Считается, что после этого перехода руководство группы изменилось.
передано в АНБ (@ rows.io).
Ниже приводится отрывок из частной беседы с оригинальным TDO.
(2016) через аккаунт группы в Twitter (@ tdohack3r):

ты знаешь, что я не одинок?
у меня есть команда
у нас есть эксперт по английскому языку за выкуп
я делаю хаки
другие крадут данные
я хорошо умею эксплуатировать и атаковать
партнер хорош в английском и бизнесе
другой хорош для кражи данных, а также для резервного копирования и создания серверов.
вымогатель

Сайпер

Неофициальный лидер группы носит имя Cyper (no H) или CyPeRtRoN. Он
является самым старым членом группы (по возрасту) с очень сильным пониманием
C ++ и другие языки программирования. Его легко узнать по сломанному
Английский. Насколько мне известно, он живет в Австрии, ему за 40.
Хотя он, возможно, не был «лидером» в традиционном смысле, он определенно был
наставник для других членов группы и присутствует с членами группы
через всю эту историю.
С 2002 по 2013 год CyPeRtRoN проводил большую часть своего свободного времени
публично портить веб-сайты. Список из 208 повреждений его веб-сайта может быть
видно с использованием архива искажений zone-h по адресу http://www.zone-h.org/archive/
notifier = CyPeRtRoN .
По его собственному мнению, самой известной порчей Сайпера была альтернатива 2003 года.
Использование сайта OWA BMC США (рис. 2.3): http://zonehmirrors.org/
defaced / 2003/03/04 / owa.navseadn.navy.mil / Cy.jpg .



Рисунок 2.3.

Сайпер также является известным администратором очень эксклюзивного форума BlackBox (под имя Ghost) и более поздний форум KickAss (под названием NSA).

Другие псевдонимы Сайпера включают:

- Cypertron
- АНБ
- Призрак
- 100 тыс.
- l00k2

Важно отметить, что члены группы часто меняли псевдонимы на создать путаницу. В данном случае NSA, лидер форума KickAss, взяло на себя псевдоним из NSA (@ rows.io), который был напрямую связан с несколькими взломами, связанными с TDO, включая DMV Луизианы (в чем он открыто признается в чате. При упоминании Агентство национальной безопасности TDO, я буду называть его NSA (@ rows.io), чтобы обозначить его адрес jabber. я по возможности будет называть администратора форума KickAss Cyper.

Арни

Данные свидетельствуют о том, что Арни - это Натан Вятт (он же CraftyCockney), 30-летний мужчина. старый житель Соединенного Королевства.

Имеющиеся данные также предполагают, что Вятт был вовлечен в TDO в начале формирование группы в 2016 году, он был оригинальной персоной The Dark Overlord (тот, кто говорил на ломаном английском), а также был оригиналом группы ведущая фигура под псевдонимом Арни.

Арни впервые привлек внимание средств массовой информации, объявив об оригинальном TDO Healthcare. взлом и продажа соответствующих медицинских данных на форуме Hell Reloaded (рис. 2.4).



Рисунок 2.4.

Арни был указан как основной продавец аналогичных данных на других форумах, и
будет открыто рекламировать, что он был человеком, взломавшим систему здравоохранения
клиники на различных форумах.

24 сентября 2016 года Вятт был арестован по подозрению в злоупотреблении компьютером.
Правонарушения, связанные с попыткой посредничества при продаже картин Пиппы Миддлтон
которые были взломаны с ее iPhone.

В декабре 2016 года после обыска устройств Уайатта лондонский метрополитен
Политан Полицейская служба нашла доказательства тысяч украденных документов из
британская юридическая фирма, ранее привлеченная TDO.

После ареста Вятт согласился дать интервью репортеру Dissent Doe.
для DataBreaches.net .

Во время интервью

Вятт описывает свои отношения с Темным Повелителем, которые включали обучение
методы мошенничества Darkoverlord, и TDO просит его вымогать
телефонный звонок жертве из США.

Дополнительные детали к эксклюзивному интервью опубликовал Vocativ.com.
(следующие цитаты можно найти на https://www.vocativ.com/362147/
Пиппа-миддлтон-хак-фото-арест-великобритания):

Крафти говорит, что он не хакер и действует исключительно как агент для отдельных лиц.
желая продать материал. «Я не хакер, - сказал он. - Я тоже не совершал
взломать. Я из сообщества, но, честно говоря, удивляюсь, что мне удалось получить
простое шифрование работает ».

Вятт также описывает технику группы по использованию средств массовой информации для продвижения
цена их вымогательства за фотографии Пиппы Миддлтон:

Британская пресса сыграла нам на руку. Я не собирался им ничего продавать.
Но они напечатали свою подлинность. Это половина трудностей, сделанных для меня. . .

Обвинение и экстрадиция

Вятт был экстрадирован в США по нескольким обвинениям, связанным с
преступления, связанные с группой The Dark Overlord.

Следующая выдержка из обвинений против Вятта была получена из
официальное обвинительное заключение суда и документ об экстрадиции (который Вятт любезно
достаточно, чтобы прислать мне):

■ Средства жертвы были переведены на счет PayPal с адресом электронной почты tashiadsmith @
tutanota.com

■ Текстовые сообщения с угрозами вымогательства были отправлены с номера 337-214-5137, который
был зарегистрирован с использованием домашнего IP-адреса Wyatt

■ Wyatt зарегистрировал учетную запись WhatsApp с номером 337-214-5137 и загрузил его фото в качестве аватара

■ Тот же номер использовался для входа в учетную запись PayPal, которая получила Платежи жертвы (ташиадсмит) и был настроен как домашний телефон для этого аккаунта

■ Электронное письмо с вымогательством, отправленное жертве, с просьбой разделить денежные средства на четыре части.

ferent банковские счета в Великобритании. Электронные письма включали информацию о банковском счете на имя Вятта и имя его девушки

■ Номер в Великобритании 44 775-481-6126 был зарегистрирован на Натана Файффа. Что номер был использован для регистрации личной учетной записи Wyatt Facebook и @ TDOHACK3R Твиттер-аккаунт, используемый группой

■ Тот же номер телефона использовался для заказа пиццы с доставкой на дом в Домашний адрес Вятта, а также использовался для регистрации службы VPN, которая был использован для входа в вышеупомянутый

Огромное количество улик против Вятта трудно игнорировать. Я не сомневаюсь что Вятт был связан с другими членами TDO в течение их первого года операции. Я также думаю, что его связь с другими участниками сделала его идеальный кандидат, чтобы взять на себя падение для других членов группы.

Как мы обсудим в следующих главах, особые характеристики других членов группы - это их способность найти парня или кого-то, на кого они могут повесить все их преступления.

В обвинительном заключении говорится, что Вятт охотно использовал банковские счета для своих *и* своих имя девушки, которые должны были использоваться для обналичивания денег, заработанных на схемы группового вымогательства. Это тот заряд, который я лично считаю немного сложно поверить. Согласно обвинительному заключению, использовались номера счетов. в электронном письме с вымогательством TDO.

Учитывая MO других членов группы, вполне возможно, что они смогли найти номера его счетов и намеренно включить их в электронное письмо жертве.

При этом Вятт ***охотно*** записал и опубликовал аудиоклип на YouTube о том, как он *произносит* угрожающую голосовую почту / требует оплаты одному жертв группового вымогательства. Во время разговора он даже назвал себя часть «Темных повелителей».

Вы можете послушать аудио здесь: https://youtu.be/DzApepLbA70 .

Другие псевдонимы Арни включают:

■ CraftyCockney

■ craftycockn3y

35 год

- гингервит
- Джейсон Вурхиз
- l00t5
- Mari0

Cr00k (пинг)

Роль Cr00k в TDO заключалась в том, чтобы выступать в качестве их основного продавца / брокера данных. Cr00k имеет на протяжении многих лет имел несколько разных псевдонимов. Первоначально он получил известность в 2015 году, когда он был объявлен как «Пинг», владелец и администратор Hell Forum, подпольный форум хакеров дарквеб.

Помимо всех этих достижений, он также невероятно опытен. хакер, с очень глубоким пониманием различных технологий.

Cr00k любит создавать путаницу и обман, перехватив псевдонимы известные хакеры, и часто используют прессу, чтобы привлечь внимание к его взломам. и товары, которыми он занимается.

Он также мастерски использует средства массовой информации для управления событиями и бросания правоохранительные органы ушли от его следа.

А ему всего 18 лет.

На мой взгляд, у него есть талант к долгосрочному планированию и стратегии, создавая поддельные сценарии, публикация поддельных доксов и манипулирование разговорами для создания истории, предназначенные для того, чтобы отправить следователей в бесконечные кроличьи норы неверных Информация.

Другие псевдонимы Cr00k включают:

- C86x
- Dio_the_plug
- F3ttywap
- Морозный
- Джинн
- Лава
- Nakk3r
- NSFW
- Малум
- Ping
- Фотон

■ Прометей

■ Overfl0w

■ радуйтесь

■ ROR [RG]

■ Райдер

■ русский

АНБ (душевное спокойствие)

NSA, nsa@rows.io (не путать с Сайпером, также известным как NSA),
был активен под этим именем всего несколько месяцев.
АНБ стало известно благодаря рекламе продажи взломанных записей из
Департамент транспортных средств Луизианы на рынке TheRealDeal. Его происхождение
можно проследить до 2015 года, когда он был администратором оригинального форума Hell
как «Revolt», а рынок TheRealDeal - как «Peace of Mind».
Свидетельства говорят о том, что АНБ является истинным лицом Темного Повелителя и,
по словам Натана Вятта, «ребенка», который стал лидером группы.
Я считаю, что его величайшая сила - это его способность обманывать и создавать путаницу.
что он делает под видом нескольких псевдонимов. Я прочитал множество сообщений
фронтальные разговоры, которые он вел с собой под разными псевдонимами
просто чтобы создать путаницу и дезинформацию.
Любые репортеры или следователи, которые беседовали с TDO после 2017 года.
скорее всего говорили с ним.

**Ping and Revolt, также известные как Cr00k и NSA, живут примерно в 5 милях от каждого из них.
другие в Калгари, Канада. Они выросли вместе и регулярно участвовали в хакерских атаках.
вместе восходит к адскому форуму.**

Новый лидер TDO

В 2017 году TDO объявил о смене руководства в Twitter, опубликовав твит под названием
«Новый год, новые мы». Твит содержал ссылку Pastebin на pastebin.com/kekU-
JRU7 , который с тех пор был удален (и, к сожалению, не в каких-либо архивах). Этот
изменение знаменует конец Арни как лидера TDO и начало нового
режим под NSA@rows.io .
До 2017 года атаки TDO были в основном сосредоточены на получении доступа через
Серверы RDP и взломанное медицинское ПО. После смены руководства на
АНБ, атаки стали враждебными и гораздо более агрессивными.

Язык TDO также стал намного более агрессивным и оскорбительным, и их
стиль атак перешел от типичных технологических взломов к откровенному террору.
Позже в том же году группа была внесена в список национальных террористов после того, как они вынудили
закрытие нескольких школьных округов из-за угрозы убийством родителям
из студентов.
На рис. 2.5 представлен снимок экрана текстовых сообщений, отправленных родителям одного ученика.
Другой пример жестокости группы связан с вымогательством «Маленького
Red Door », некоммерческая онкологическая клиника в Индиане. NPR.com сообщил, что TDO
общение с клиникой осуществлялось по электронной почте с темой «Рак.
Отстой, но мы - отстой! »
Когда Little Red Door не выплатила выкуп в размере почти 50 000 долларов, TDO решила
Twitter и опубликовал скорбные письма, разосланные семьям клиентов, которые скончались.

Отношение и враждебность

Помимо его чрезмерно враждебного тона, история АНБ на хакерских форумах показывает
склонность к избиению геев, в то время как его личные страницы в социальных сетях демонстрируют
количество про-гомосексуальных изображений и упоминаний.
Я имел удовольствие много раз разговаривать с ним через его личное лицо.
book, Twitter и Jabber. Ниже приводится небольшой отрывок, показывающий
его общее отношение (обратите внимание на постоянное употребление слова d ** k):

XXX Мне жаль, чувак, но ты говоришь так, будто ты ЛИ или черт возьми
ретард, наверное, последнее.
B.T. почему я умственно отсталый?
XXX вы и ваши друзья NightCat / jasonvoorhees / hafez asad и другие
Ублюдки могут взобраться на стену хуев
VT NightCat? Ясонвурхиз?
XXX отстой * * к

Некоторые из других псевдонимов NSA включают:

■ BTC

■ Колумбина

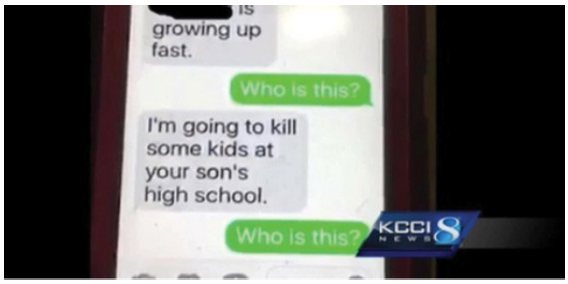


Рисунок 2.5.

- L3tm3
- NSFW
- Оббилорд
- Обфускация
- Душевное спокойствие
- Бунт
- Страдинатрас
- WhitePacket
- Владимир

Темный повелитель

Всякий раз, когда мы общались как фигура TDO, казалось, что есть язык руководящие принципы и строгий формальный тон, чтобы создать видимость большего структура группы с внутренними процессами и процедурами.

Что-то, что я всегда находил смешным, - это усилия, которые TDO приложит, пытаясь представить себя как законный бизнес. В многочисленных беседах с члены группы, они всегда обсуждают контракты, счета или другие формальные деловые документы, необходимые для использования их услуг.

4. TERMINATION AND GUARANTEES
   a. thedarkoverlord reserves the right to rescind this agreement if the "Client" and/or associated parties of the "Client" fail to understand the agreement before the aforementioned deadline.
   b. thedarkoverlord reserves the right to rescind, cancel, or otherwise terminate this agreement if this agreement is not accorded and satisfied by the aforementioned deadline.
   c. Conditionally, thedarkoverlord will make no attempts to defraud this agreement after the understanding of this agreement by the "Client" and/or associated parties of the "Client".
      i. Condition A is that the thedarkoverlord may defraud this agreement if the "Client" and/or associated parties of the "Client" fail to accord and satisfy the terms of this contract.
   d. The "Client" and/or associated parties of the "Client" will make no attempts to defraud this agreement after the understanding of this agreement.
      i. If any attempts by the "Client" and/or associated parties of the "Client" are made to defraud this agreement after the understanding of this agreement, thedarkoverlord reserves the right to rescind, cancel, or otherwise terminate this agreement,
      ii. If any attempts by the "Client" and/or associated parties of the "Client" are made to defraud this agreement after the understanding of this agreement, thedarkoverlord reserves the right to inflict harm and further adversarial action against by the "Client" and/or associated parties of the "Client".

Рисунок 2.6.

39

На рисунке 2.6 показан фрагмент предполагаемого контракта между Темным Повелителем.
и жертва, опубликованная Джозефом Коксом на Материнской плате.
Несмотря на внешность, деловой тон группы быстро ухудшился, если
жертва не заплатила выкуп. Всякий раз, когда смехотворные требования TDO
не встретились, группа быстро волновалась и устраивала публичную истерику
в Твиттере, ничем не отличается от поведения ребенка, не получающего то, что он
хотите



(рисунок 2.7).

Ниже приводится отрывок из трехчасового разговора с TDO.
в чате Jabber в октябре 2018 года. TDO знал, что разговаривает со мной, Винни Троя.
В этой книге будут анализироваться дополнительные разговоры и отрывки.
поскольку они относятся к материалу в разных главах. Эти отрывки дают
Отличный взгляд на агрессивную, самовозвеличивающую и непристойную личность TDO:

00:27 TDO Тупой пр ** к.
12:27 TDO Вы с удовольствием подключили один из немногих
из нас.
00:31 TDO Тебе сегодня повезло.
00:32 TDO Я сижу здесь, перемещаю терабайты данных в новый
сервер, и мне скучно, так что вы были благословлены
общается со мной.
12:52 TDO. Приятно наконец поговорить с тобой, Троя.
00:53 VT Вы тоже.
00:53 TDO Послушайте, ребята воспитаны тщательно, чтобы
понимать лингвистические системы, которые мы используем,
так что вы простите их краткость.
00:54 TDO Опять же, это редкая возможность, не упускайте ее.

——

00:59 TDO Слушай, приятель, забудь Кребса ... Ты понимаешь, что твоя
национальное государство исследовало нас безуспешно?
1:00 утра TDO Об этом стало известно публично. Проверить Биллингс
Вестник в Монтане. Утекла информация о том, что ЦРУ и
АНБ расследовало нас.
1:01 утра VT поздравляю с уклонением от их усилий
1:01 утра TDO. Ваше АНБ и GCHQ не так хороши, как им хотелось бы.
людям верить. Пассивное наблюдение только так
успешный.
1:02 утра VT Я не сомневаюсь, что

1:02 утра TDO
Вы понимаете, что мы закрыли шесть разных
школьные округа в Монтане на 5 рабочих дней?
1:02 утра TDO
Мы исключили из школы 36 000 учеников.
1:03 утра TDO
Теперь мы все слышали о закрытии "бомбовых угроз"
школы на день, но что кому-то нужно
сделать, чтобы закрыть школы на 5 дней?
1:03 утра TDO
Вы когда-нибудь задумывались об этом?
1:03 утра VT
честно, нет
1:03 утра TDO
Тогда ты идиот. Какие есть у других организаций
закрыли целый регион так долго?
1:04 утра TDO
Думаю об этом. Что нам нужно было сделать, чтобы достичь
эта цель?
1:04 утра TDO
5 дней. Не 1, а 5.
1:04 утра TDO
Поразмыслите над этим. У нас на самом деле было ваше ФБР физически
преследуя нас,
1:04 утра TDO
В погоне за призраком.
1:04 утра VT
Я не знал, что школы закрыты на
всю неделю. Вы правы, это красиво
существенный
1:05 утра TDO
Вы должны это прочитать. Это все OSINT.
1:05 утра VT
освежите меня в истории, вы, ребята, звонили
школа, правильно?
1:05 утра TDO
Вызов? Намного больше.
1:05 утра TDO
Мы установили физические устройства, используя непритязательные
третьи стороны.
1:06 утра VT
я понятия не имею, что это значит
1:06 утра TDO
Гребаный придурок.
1:06 утра TDO
Считать.
1:06 утра TDO
Используйте этот гребаный кусок серого вещества между своими
глаза.
1:06 утра VT
что такое скромная третья сторона
1:06 утра TDO
Вот почему ваше АНБ и ЦРУ расследовали нас, и
проводил рейды в Лондоне.
1:07 утра TDO
Имейте в виду, неудачные рейды.

1:07 утра VT
Я не знал, что какое-то место подверглось рейду.
1:07 утра TDO
ПРОЧИТАЙТЕ БИЛЛИНГС ГАЗЕТУ, великий
OSINT на TDO EVER.
1:07 утра TDO
Гребаный придурок, Троя.
1:07 утра VT
Извините, Billings Gazette был не совсем высоким
на моем PR-радаре
1:08 утра TDO
Бля, я сижу здесь сегодня вечером и говорю
с самым большим идиотом на этой гребаной скале.

Работа с TDO была интересной и полезной. Возможность срабатывания
его необдуманные эмоциональные всплески пригодятся позже, когда я буду говорить
на другие псевдонимы. Пока у вас есть на это смелость, вы можете запустить
одни и те же вспышки, просто задавая правильные вопросы, - невероятно эффективный способ
чтобы лучше понять, с кем вы разговариваете.

Резюме

В этой главе представлен обзор некоторых различных путей, доступных как
следователь, и некоторые из сценариев, в которых я лично участвовал
в моем стремлении помочь информировать организации о взломе.
В этой главе также представлена справочная информация о Темном повелителе.
и членов его основной группы, которые будут обсуждаться более подробно позже
главы.

Я

Исследование сети

В этой части

Глава 3: Исследование сети вручную
Глава 4: Поиск сетевой активности (расширенные методы NMAP)
Глава 5: Автоматизированные инструменты для обнаружения сети
Как следует из названия, в этой части книги обсуждаются многие тонкости
сетевое расследование и разведка. Следователи и проникновение в черный ящик
тестировщикам часто нечего делать, кроме одного IP-адреса, так что
где начинается наше следственное путешествие. В следующих трех главах мы рассмотрим
процессы и инструменты, предназначенные для тщательного изучения сетевого пространства и помощи
чтобы собрать как можно больше информации.

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

45

3

Эта глава предназначена для того, чтобы дать вам обзор выполнения общих сетевых задач.
разведка работы организации, а также сканирование и идентификация
сетевые хосты. В этой главе основное внимание уделяется процессу, а не конкретным
инструменты, которые используются, потому что, когда дело доходит до OSINT или, возможно, любого аспекта
информационная безопасность, всегда будут новые, лучшие и блестящие инструменты.
Существуют сотни различных инструментов и сервисов, которые вы можете использовать для сбора
информация об организациях. Новые инструменты выходят почти ежедневно; это невозможно
поддерживать. Я не хочу, чтобы это было в центре внимания. Я уверен, что пропустил некоторые инструменты, и
Я уверен, что к тому времени, как вы это прочтете, некоторые из них уже устареют. Моя цель показать
некоторые инструменты, которые я считаю полезными *сейчас* , но я полностью понимаю, что
в будущем могут быть лучшие.
Тем не менее, инструменты не должны быть в центре внимания. Дело в *том,* как информация
собирается, и, что более важно, как процесс открытия новых
информация *никогда не* должна ограничиваться одним инструментом.
Всегда пробуйте что-то новое, потому что, как я продемонстрирую, один инструмент никогда не
дать вам исчерпывающий ответ.

Ручное исследование сети

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

Цели главы: Pepsi.com и Cyper.org

Чтобы проиллюстрировать различия между различными инструментами и службами, я запущу все тесты проводятся на двух разных серверах, pepsi.com и cyper.org. Я показываю два очень разных сайта, чтобы показать различия в выводе программного обеспечения, когда работа с двумя очень разными целями.

Почему pepsi.com и cyper.org? Pepsi.com, потому что я пью один как Я пишу это. Cyper.org из-за названия. Насколько мне известно, cyper.org не связан с злоумышленником Сайпером (который, как я полагаю, связан с The-Хакерская группа DarkOverlord). В ходе любого расследования новые появятся возможности для подобных исследований, и необходимость исследования необычных доменные имена (например, cyper.org) будут необходимы.

Pepsi, безусловно, очень известный бренд и популярный веб-сайт, поэтому результаты между двумя веб-сайтами будут сильно отличаться.

Прежде чем мы начнем, я хотел бы отметить, что IP-атрибуция, вероятно, одна из самых сложных задач, стоящих перед следователями. Чтобы дать вам пример, у меня есть обнаружил многочисленные утечки данных, в том числе Exactis, Apollo.io и Verifications.io. В В каждом из этих случаев все, с чем мне приходилось работать, это IP-адрес дырявой базы данных. сервер. Серверы баз данных обычно не ссылаются на основной домен, поэтому это зависит от следователь, чтобы найти истинное происхождение данных. Я буду давать советы по пути с ссылки на реальные ситуации, с которыми я имел дело. Надеюсь, мой опыт поможет некоторые из вас по пути.

Обнаружение активов

Начать работу с исследованием сети обычно довольно просто. Если вы выполняете тест черного ящика, тогда вы знаете имя клиента и его домен. Чтобы узнать их IP-адрес, вы можете выполнить поиск в Dig. Копать включен в Linux / Mac по умолчанию. Выполнение следующей команды даст вам IP для apple.com :

```
root @ INTEL: ~: копать apple.com
; << >> Dig 9.10.3-P4-Ubuntu << >> apple.com
;; глобальные параметры: + cmd
;; Получил ответ:
;; - >> HEADER << - код операции: QUERY, статус: NOERROR, id: 7666
;; флаги: qr rd ra; ЗАПРОС: 1, ОТВЕТ: 3, АВТОРИТЕТ: 0, ДОПОЛНИТЕЛЬНО: 1
;; ОПТИЧЕСКАЯ ПСЕВДОЗЕКЦИЯ:
; EDNS: версия: 0, флаги :; UDP: 512
;; РАЗДЕЛ ВОПРОСА:
; apple.com.
В
```

;; РАЗДЕЛ ОТВЕТА:
apple.com.
1100 IN A 17.172.224.47
apple.com.
1100 IN A 17.142.160.59
apple.com.
1100 IN A 17.178.96.59
;; Время запроса: 1 мсек.
;; СЕРВЕР: 8.8.8.8 # 53 (8.8.8.8)
;; КОГДА: Пн, 10 декабря, 09:02:24 UTC 2018
;; РАЗМЕР MSG rcvd: 86

Поиск по ARIN

Один IP-адрес - это хорошо, но мы хотели бы узнать больше о таргетинге.
получить IP-адрес. Американский реестр интернет-номеров (ARIN) управляет
раздача адресов IPv4 и IPv6. Многие крупные организации зарегистрируют
целые сетевые диапазоны, поэтому их IP-пространство будет легко доступно для поиска. ARIN предоставляет
бесплатный поиск для быстрого определения этих диапазонов IP.
Протокол WHOIS (который будет обсуждаться в главе 9) используется для запроса
базы данных, содержащие всевозможную общедоступную информацию в Интернете
ресурсы, включая доменные имена и IP-адреса. Протокол WHOIS
используется для запроса к широкой сети серверов WHOIS любой информации о
доменов, стоящих за миллиардами веб-сайтов по всему миру (вместе известных
как данные WHOIS).
Поиск WhoisRWS просматривает данные специально в рамках регистрации ARIN.
данные. Часто это может быть хорошим первым шагом при проведении оценки методом черного ящика.
и все, что вам нужно, это название компании. На рисунке 3.1 показан пример.
Окно поиска ARIN.
Ввод «Google» в поиске WhoisRWS дает нам несколько разных сетей.
диапазоны, которые мы можем добавить к нашим поискам, как показано на рисунке 3.2.

**Это отличная первая остановка для меня, потому что иногда вам повезет и
обнаруживают, что IP-адрес (или даже весь IP-блок) принадлежит определенному владельцу.
Когда вы ищете атрибуцию сервера или базы данных, такое случается редко, но
Мне несколько раз везло. Особо хочу упомянуть об одной утечке данных. А
Китайская телекоммуникационная компания потеряла более 3 ТБ данных, включая имена клиентов,
адреса электронной почты, номера мобильных телефонов и номера дебетовых карт. К счастью, они владели своим
весь сетевой блок, поэтому атрибуция была довольно простой. Так бывает не всегда, но
сначала стоит попробовать.**



Рисунок 3.1.

Поисковые машины Dorks

Поиск активных поддоменов - довольно простая задача с помощью Google dorks (расширенный
строки поиска).

**. «Дорк» - это строка поиска, в которой используются расширенные операторы для создания новых
полученные результаты. Более подробно поисковые системы будут рассмотрены в главе 8. А пока
в этом разделе рассматриваются некоторые действительно простые придурки, которые можно использовать для поиска информации о
конкретный адрес веб-сайта.**

Для поиска результатов на определенном веб-сайте просто используйте следующую команду:

Сайт: pepsi.com

Теперь мы можем еще больше улучшить результат поиска, удалив поддомены,
мы не хотим (например, www), используя «-inurl» (минус inurl). Inurl будет искать
строка в URL-адресе, и мы хотим сделать наоборот - удалить что-либо в
URL-адрес, соответствующий нашей строке:

Сайт: pepsi.com -inurl: www

You searched for: **google**

Networks	
GOOGLE (NET6-2620-E7-4000-1)	2620:E7:4000:: - 2620:E7:4000:FFFF:FFFF:FFFF:FFFF:FFFF
GOOGLE (NET6-2620-E7-C000-1)	2620:E7:C000:: - 2620:E7:C000:FFFF:FFFF:FFFF:FFFF:FFFF
GOOGLE (NET-108-170-192-0-1)	108.170.192.0 - 108.170.255.255
GOOGLE (NET-108-177-0-0-1)	108.177.0.0 - 108.177.127.255
GOOGLE (NET-142-250-0-0-1)	142.250.0.0 - 142.251.255.255
GOOGLE (NET-172-217-0-0-1)	172.217.0.0 - 172.217.255.255
GOOGLE (NET-172-253-0-0-1)	172.253.0.0 - 172.253.255.255
GOOGLE (NET-173-194-0-0-1)	173.194.0.0 - 173.194.255.255
GOOGLE (NET-192-178-0-0-1)	192.178.0.0 - 192.179.255.255
GOOGLE (NET-199-87-241-32-1)	199.87.241.32 - 199.87.241.63
GOOGLE (NET-199-88-130-0-1)	199.88.130.0 - 199.88.130.255
GOOGLE (NET-199-89-220-0-1)	199.89.220.0 - 199.89.220.255
GOOGLE (NET-207-223-160-0-1)	207.223.160.0 - 207.223.175.255
GOOGLE (NET-209-170-110-128-1)	209.170.110.128 - 209.170.110.191
GOOGLE (NET-209-170-110-192-1)	209.170.110.192 - 209.170.110.255
GOOGLE (NET-209-170-119-128-1)	209.170.119.128 - 209.170.119.191

Рисунок 3.2.

Всего 609 страниц результатов, и только первая страница (рис. 3.3) выглядит так.
есть цели, которые стоит исследовать.

DNSDumpster

Люди заняты. Чем они заняты, тем более забывчивыми они становятся
о наведении порядка. При просмотре записей DNS или даже просто поиске
для получения дополнительной информации о цели я всегда могу найти информацию о
поддомены, которые должны были быть выведены из эксплуатации. Весьма вероятно, что развитие
операторы создадут «тестовые» поддомены для проектов разработки, которые еще не отправлены на
производство. Разработчики не всегда хорошо очищают свой код и часто
использовать ярлыки, особенно при работе над собственными сайтами разработки.
Эти поддомены и ярлыки часто могут предоставить золотую жилу информации.

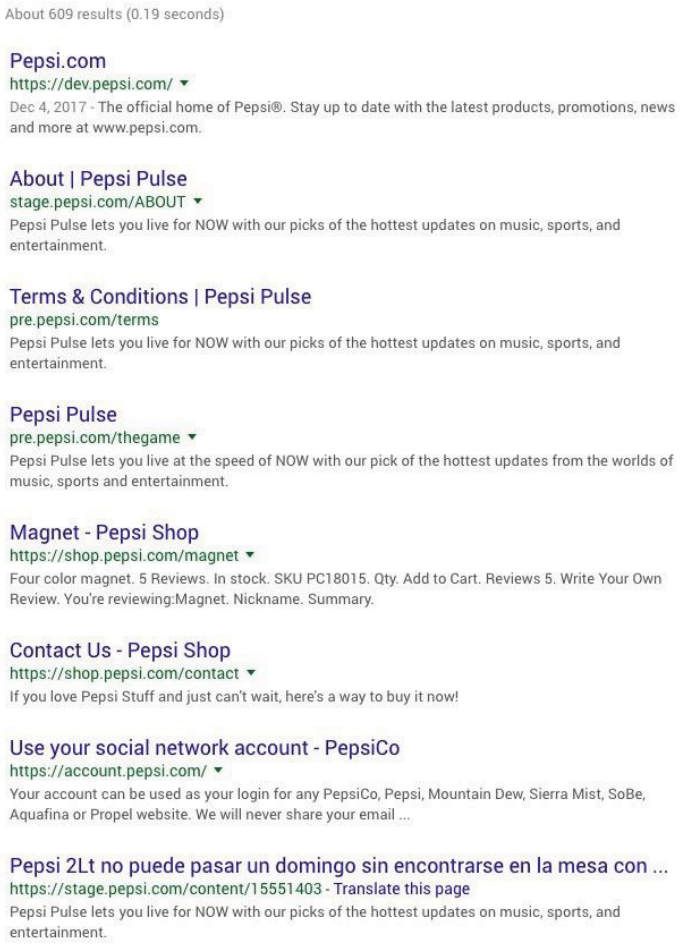


Рисунок 3.3.

Вы можете найти их с помощью DNSDumpster, бесплатного инструмента поиска доменов, который может быстро обнаружить связанные хосты по IP-адресу.

Часто субдомен указывает на старый IP-адрес. Я сидел-
случаи, когда субдомен компании указывал на IP-адрес, который был
даже не принадлежит компании. IP-адрес был на случайный общедоступный FTP-сайт, и
без ведома банка, blah.bank.com указывал на субдомен,
держал пиратское программное обеспечение. Они были очень благодарны за находку.

DNSDumpster очень прост в использовании (см. Рис. 3.4). Просто введите домен или
IP, который вы ищете, и он будет отображать для вас действительно хороший графический вывод.

На рис. 3.5 показан пример выходных данных с использованием pepsi.com в качестве нашей цели. DNS-
Dumpster дает нам 19 записей о хостах. Ниже приводится лишь небольшая часть
результаты, но отсюда мы уже видим четыре различных потенциальных целевых IP-адреса,
все с интересными названиями (баллы, счет, магазин и безопасность).

Существует также вариант бесплатной загрузки XLS, который дает вам отличную информацию.
которые вы можете легко импортировать в другую программу (см. рис. 3.6).

На рис. 3.7 показан красивый вариант построения графика, с помощью которого будет создана сетевая карта
обнаруженные устройства. Это отличный бесплатный инструмент для тестирования на проникновение.
отчеты для небольшого дополнительного «вау» фактора.

Когда мы запускаем такой же поиск для нашего второго домена, cyper.org , мы
получить 1 результирующую запись хоста:

www.cyper.org — 162.210.102.59

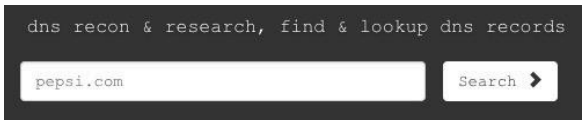


Рисунок 3.4.



Рисунок 3.5.

Hostname	IP Address	Type	Reverse DNS	Netblock Owner	Country	HTTP Server	Title (HTTP)	HTTPS Ser	Title (HTT
pepsi.com	45.60.135.51	A			United States				
signup.pepsi.com	159.127.185.121	A		AS19137 Epsilon Interactive LLC	United States				
account.pepsi.com	159.127.185.117	A		AS19137 Epsilon Interactive LLC	United States				
shop.pepsi.com	161.47.125.72	A	885589-DB1.tmpcompany.com	AS19994 Rackspace Ltd.	United States	Apache	302 Found	Apache	
promo1.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
promo2.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
promo3.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
promo4.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
fbfoodservice.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
halftime.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
therecipe.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
secure.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
promo.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
thesounddrop.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
thesoundrop.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
pass.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
points.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
www.points.pepsi.com	18.214.229.99	A	ec2-18-214-229-99.compute-1.amazonaws.com		United States				
mta.em.pepsi.com	13.111.110.249	A	mta.em.pepsi.com		United States				

Рисунок 3.6.

Хакерская цель

Хакерская цель (https://hackertarget.com/reverse-dns-lookup) делает поиск-
Для поддоменов и обратного поиска DNS очень легко использовать их API. Ты
можно просто запросить домен или IP-адрес с одним URL-адресом, например:
https://api.hackertarget.com/reversedns/?q=url.com

Быстрый поиск pepsi.com на hackertarget.com обнаруживает 31 различную под-
домены:

https://api.hackertarget.com/reversedns/?q=pepsi.com
sadad scl-pepsi.com, 124.29.219.220 58.27.215.220 124.29.219.221
moscntx3.russia.intl.pepsi.com , 195.239.40.163
www.wpbpepsi.com, 209.142.183.140
mail.hbcpepsi.com, 210.56.13.100

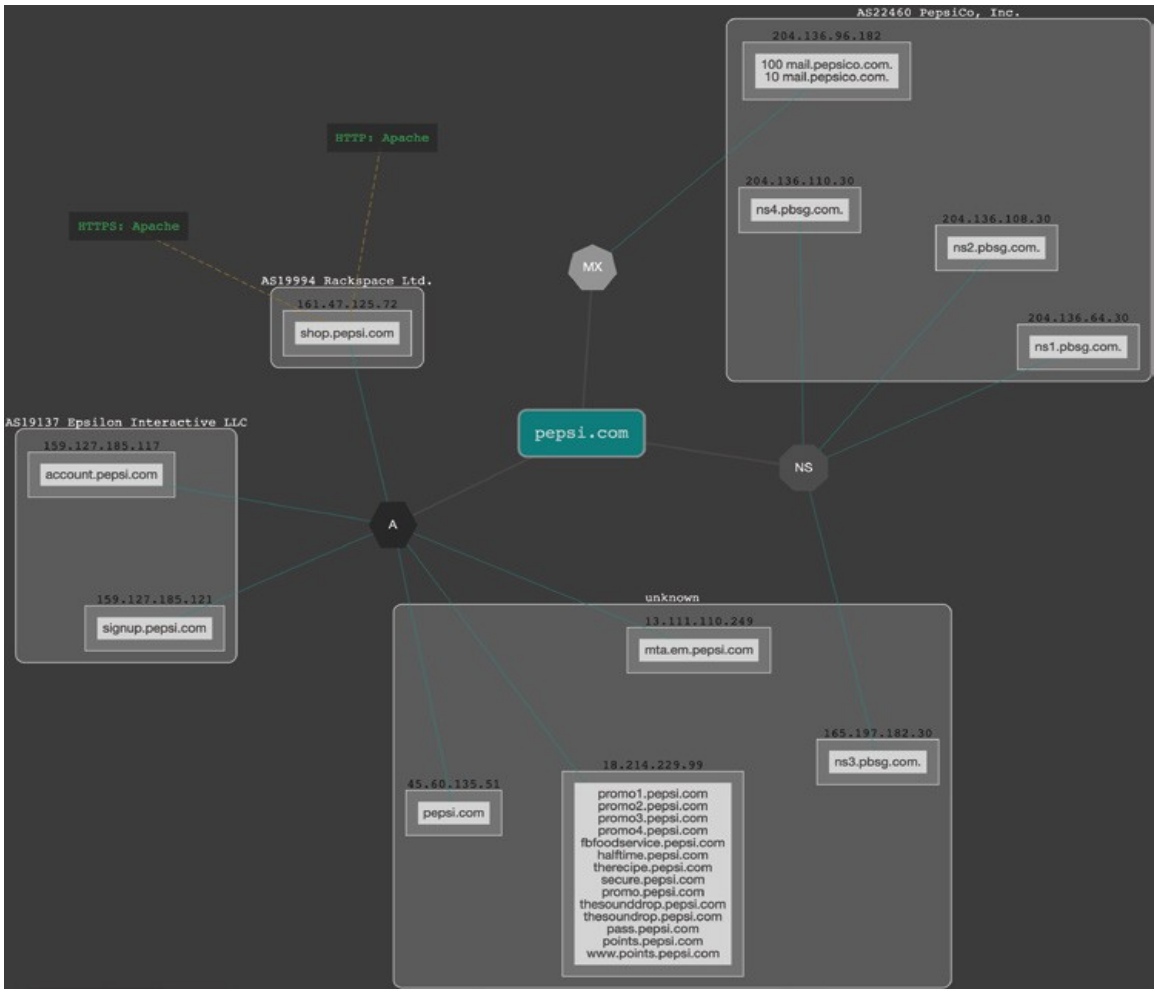


Рисунок 3.7.

mbcpepsi.com, 156.46.83.96
router.mbcpepsi.com, 69.29.19.133
mx.mbcpepsi.com, 69.29.19.134
mail.nbcpepsi.com, 116.58.32.20
sticladepepsi.com, 216.247.113.7
lakesidepepsi.com, 71.13.1.74
iwanttoservepepsi.com, 165.197.98.42 204.136.80.125
host170.mbgpepsi.com, 205.244.118.170
host171.mbgpepsi.com, 205.244.118.171
mbg1.mbgpepsi.com, 205.244.118.161
host162.mbgpepsi.com, 205.244.118.162
mail2.mbgpepsi.com, 173.219.102.86
host163.mbgpepsi.com, 205.244.118.163
host173.mbgpepsi.com, 205.244.118.173
host164.mbgpepsi.com, 205.244.118.164
host165.mbgpepsi.com, 205.244.118.165
host166.mbgpepsi.com, 205.244.118.166
host167.mbgpepsi.com, 205.244.118.167
host168.mbgpepsi.com, 205.244.118.168
host169.mbgpepsi.com, 205.244.118.169
mail.mbgpepsi.com, 206.107.106.67
gjpex01.gjpepsi.com, 173.226.224.197
cin_prd.gjpepsi.com, 38.155.184.10
autodiscover.exchangedelegation.gjpepsi.com, 173.226.240.194
domino.forumpepsi.com, 207.245.55.250 207.245.55.251
mail.bremertonpepsi.com, 70.90.189.233
viv.vivehoypepsi.com, 174.120.246.142

Второй поиск cyper.org обнаруживает пять поддоменов:

https://api.hackertarget.com/reversedns/?q=cyper.org
office.cyper.org, 65.100.252.81
zone.cyper.org, 65.100.252.84
seek.cyper.org, 65.100.252.82
storm.cyper.org, 65.100.252.83
www.cyper.org, 65.100.252.85

Shodan

Shodan - это поисковая машина для интернет-устройств. Shodan делает довольно удивительный
работа с картографическими устройствами в Интернете, поэтому все, что вам нужно сделать, это спросить
правильный вопрос.

Shodan буквально запрашивает каждый IP-адрес и его порты и собирает информацию.
об ответах сервера. Что делает Shodan таким замечательным, так это то, что вы можете использовать
это для детализации и поиска конкретных целей технологии. Например, являются

Вам интересно узнать, какие ветряные турбины имеют доступные IP-адреса?
Спросите Шодана. Хотите знать, какие базы данных Elasticsearch или MongoDB можно использовать
доступ без учетных данных? Хотите знать, какие камеры или домашние роутеры
все еще используете пароль по умолчанию? Ты угадал. У Шодана есть ответы на эти вопросы.

Shodan предлагает лишь ограниченное количество бесплатных запросов, поэтому, если вы хотите возможность искать больше и делать интересные вещи, например использовать свой API для загрузки списков данных в оптом, за доступ нужно платить.

Поиск Shodan очень хорошо спроектирован и предлагает возможность использовать расширенные
поисковые операторы (dorks) для быстрого поиска конкретных целей. Вот основные
фильтры, которые можно использовать с Shodan:

- **город:** поиск устройств в определенном городе.
- **страна:** поиск устройств в определенной стране.
- **geo:** использовать географические координаты
- **имя хоста:** ищите устройства, соответствующие определенному имени хоста.
- **net:** поиск по IP или CIDR
- **ОС:** поиск по операционной системе
- **порт:** ищите определенные порты
- **до / после:** поиск результатов в течение определенного периода времени.
- **Организация:** поиск по названию конкретной организации.

Мы можем искать конкретную организацию так:

```
Организация: Название компании
```

Для поиска Pepsi как организации мы можем использовать следующий поиск:

```
Организация: Pepsi
```

Если параметр поиска организации слишком широк, мы можем попытаться сузить
наши поиски путем поиска любых результатов с конкретными именами хостов (см. рисунок 3.8):

```
Имя хоста: pepsi.com
```

Это дает нам 28 результатов, связанных с pepsi.com, и является хорошим началом.
Если вы не можете найти конкретное имя хоста в Shodan или просто хотите
Чтобы быть внимательным, вы можете попробовать поискать IP-адрес домена.
В случае cyper.org поиск по имени хоста возвращает 0 результатов. Мы можем быстро
найдите IP-адрес, связанный с cyper.org, с помощью Dig:

```
root @ OSINT: dig cyper.org
<< >> DiG 9.10.6 << >> cyper.org
```

глобальные параметры: + cmd
;; Получил ответ:
;; - >> HEADER << - код операции: QUERY, статус: NOERROR, id: 12771
;; флаги: qr rd ra; ЗАПРОС: 1, ОТВЕТ: 1, АВТОРИТЕТ: 0, ДОПОЛНИТЕЛЬНО: 1
;; ОПТИЧЕСКАЯ ПСЕВДОЗЕКЦИЯ:
; EDNS: версия: 0, флаги :; UDP: 4096
;; РАЗДЕЛ ВОПРОСА:
; cyper.org
B
A
;; РАЗДЕЛ ОТВЕТА:
cyper.org. 3155 B
A **162.210.102.59**

Теперь давайте проверим Shodan на предмет совпадений на основе этого IP-адреса (также называемого обратный поиск DNS).

В этом выводе нет субдоменов; вместо этого нам предоставляется значительный объем метаданных с этого IP, включая другие связанные домены. Мы обсудим обратный поиск DNS (RDNS) более подробно в Части II Руководства. эта книга (сбор информации о веб-сайтах) - особенно если смотреть на домен имена. Как следует из названия, обратный поиск DNS принимает IP-адрес и возвращает все домены, связанные с этим IP.



Рисунок 3.8

Censys (поиск субдоменов)

Censys.io (www.censys.io) - сервис, очень похожий на Shodan в том, что они оба обеспечивать видимость устройств, подключенных к Интернету. Как Shodan, Censys это инструмент, который помогает организациям понять, какие серверы и устройства они выставили в интернете. Censys.io можно использовать для поиска активов на конкретной сети и даже обнаруживать неизвестные хосты, которые могли быть созданы съедены сотрудниками и забыты. Открытие открытой инфраструктуры - это очень важная часть внешнего теста на проникновение, потому что он определяет открытые порты или источники утечки информации.

На мой взгляд, главное отличие Shodan от Censys.io в том, что Censys предоставляет исторические данные. Эти данные имеют свою цену, поскольку Censys считает: значительно дороже, чем Shodan. При этом, поскольку мы продолжаем обсуждать потенциальные возможности расследования, станет очевидно, что доступ к исторические данные часто могут быть краеугольным камнем всего расследования.

Поиск субдоменов Censys

Поиск субдоменов Censys (https://github.com/christophetd/censys-subdomain-finder) - это простой в использовании инструмент командной строки, который использует Censys.io API для вернуть список доступных поддоменов. Поскольку мои результаты часто будут варьироваться от Shodan и Censys (или любой другой инструмент исследования поддоменов), это отличный способ быстро запросить Censys, чтобы проверить наличие дополнительных совпадений.

Для технически подкованных читателей сценарий запрашивает Censys.io, чтобы получить список доступные поддомены с использованием журналов прозрачности сертификатов (CT). Сертификат журналы прозрачности удивительны и могут использоваться для нескольких различных типов атрибуции. Мы рассмотрим KT более подробно в главе 10.

Используя два наших примера, во-первых, поиск по сайту pepsi.com обнаруживает 42 уникальных поддомены:

```
корень @ OSINT: python censys_subdomain_finder.py pepsi.com
[*] Поиск Censys для поддоменов pepsi.com
[*] Найдено 42 уникальных поддомена pepsi.com за ~ 1,4 секунды
```

Далее поищем Cyper.org :

```
root @ OSINT: python censys_subdomain_finder.py cyper.org
[*] Поиск Censys для поддоменов cyper.org
[-] Не найдено ни одного субдомена
```

Мы уже можем видеть, что результаты между двумя сервисами очень разные.
энт. В основном это связано с размером двух организаций, но это напоминание.
что разные инструменты дадут разные результаты.

Яростный

Fierce - это инструмент перечисления DNS, который помогает находить несмежное IP-пространство и имена хостов для указанных доменов.
Это действительно предшественник NMAP, так как это уже требует от вас
знать, какое пространство IP вы ищете.
Чтобы инструмент был отличным, не обязательно иметь 100 вариантов. Fierce предназначен для DNS перечисление, и он просто делает то, что обещал. Возможные варианты:

- **-dns-server:** указывает DNS-серверы для использования.
- **-domain:** домен для тестирования
- **-subdomain-file:** использовать поддомены, указанные в этом файле (по одному в каждой строке)
- **-range:** сканировать внутренний диапазон IP-адресов, использовать нотацию cidr
- **-delay:** время ожидания между поисками

Для простоты давайте запустим Fierce для двух наших примеров доменов.
Мы также можем вывести результаты в текстовый файл с помощью команды вывода Linux.

```
свирепый --домен pepsi.com> output.txt
```

Результат жесткого сканирования показывает шесть уникальных записей о субдомене / хосте:

```
159.127.187.12 e.pepsi.com
18.214.229.99 Promo.pepsi.com
18.214.229.99 secure.pepsi.com
161.47.125.72 shop.pepsi.com
159.127.185.121 signup.pepsi.com
209.143.254.67 stage.pepsi.com
Найдены подсети (возможно, вы захотите проверить здесь с помощью nmap или unicornscan):
159.127.185.0-255: найдено 1 имен хостов.
159.127.187.0-255: найдено 1 имен хостов.
161.47.125.0-255: найдено 1 имен хостов.
18.214.229.0-255: найдено 2 имени хоста.
209.143.254.0-255: найдено 1 имен хостов.
Найдено 6 записей.
```

Теперь попробуем с другим нашим доменом:

```
root @ OSINT: fierce --dns cyper.org --threads 5 --file dns.txt
```

Результат этого сканирования:

```
Проверка DNS с подстановочными знаками ...
Неа. Хороший.
Сейчас выполняется 1917 тестов ...
198.23.53.116 imap.cyper.org
198.23.53.116 pop3.cyper.org
198.23.53.116 smtp.cyper.org
162.210.102.59 www.cyper.org
Найдено 4 записи.
```

Неплохое начало. Мы уже на четыре поддомена дальше, чем с предыдущим
сканировать. Давайте продолжим.

Sublist3r

Sublist3r, наверное, мой любимый из всех сотен переборов поддоменов.
инструменты. Запуск сценария только с доменным именем проверит наличие субдоменов в
ряд различных движков, включая Yahoo, Bing, Netcraft, DNSDumpster,
PassiveDNS и многое другое.

Я использую Sublist3r в течение многих лет, и я также знаю многих своих приятелей-хакеров.
клянусь этим. Я также стараюсь не отставать от тенденций охотников за ошибками,
и Sublist3r по-прежнему кажется фаворитом. Это невероятно простой в использовании инструмент,
и широта результатов поиска впечатляет.

Sublist3r включает следующие параметры.

- -d : домен для поиска
- -b : включить модуль грубой силы
- -p : список портов для сканирования
- -v : подробный
- -t : количество параллельных потоков
- -e : указать, какие поисковые системы использовать.
- -o : вывод в файл

Sublist3r не требует большой настройки или настройки. Ты можешь просто
запустите его со стандартной опцией -d, чтобы найти домен и позволить ему творить чудеса:

```
корень @ OSINT: python sublist3r.py -d pepsi.com
[-] Перечисление субдоменов теперь для pepsi.com
[-] Сейчас ищу в Baidu ..
[-] Сейчас ищу в Yahoo ..
```

[-] Сейчас ищу в Google ..
[-] Сейчас ищу в Bing ..
[-] Ищем сейчас в Спросите ..
[-] Сейчас ищу в Netcraft ..
[-] Поиск в DNSdumpster ..
[-] Сейчас ищем в Virustotal ..
[-] Сейчас поиск в ThreatCrowd ..
[-] Выполняется поиск по SSL-сертификатам ..
[-] Поиск в PassiveDNS ..
[-] Всего найдено уникальных субдоменов: 56

Этот первоначальный запрос привел к возврату нескольких сотен поддоменов.
с сайта pepsi.com . Попробуем ту же команду с нашим вторым доменом:

корень @ OSINT: python sublist3r.py -d cyper.org
www.cyper.org
office.cyper.org
seek.cyper.org
storm.cyper.org
zone.cyper.org
[-] Всего найдено уникальных субдоменов: 5

Теперь мы увидели несколько инструментов с графическим интерфейсом и командной строки, которые мы можем использовать.
получить списки поддоменов с помощью более традиционных методов поиска. Давайте
сделайте еще один шаг и попробуйте выполнить брутфорс.

Enumall

Enumall - это скрипт, созданный Джейсоном Хаддиксом для выполнения исчерпывающего поддомена.
открытие с помощью одной команды. Enumall разработан, чтобы делать все, что вы
рассматривается в этой главе с помощью одной команды.
Enumall использует механизм разведки , чтобы:

- Перечислить субдомены
- Выполните парсинг Google, Bing, Yahoo и Netcraft.
- Брутфорс для поиска поддоменов
- Поиск Shodan
- Преобразование всех активных адресов в IP-адреса.
- Вывести все в красивый и удобный CSV-файл.

Скрипт использует комбинацию списков слов для создания разных поддоменов.
комбинации, которые нужно попробовать во время попытки перебора. Перед запуском скрипта,
вы должны знать об этих конкретных параметрах:

- -a : использовать alt-dns для создания перестановки слов на основе начального списка
- -p : список семян, который мы хотим передать в alt-dns.
- -w : настраиваемый список слов для использования с реконструкцией при брутфорсе.

Использование опций alt-dns **может быть излишним в зависимости от уровня тестирование, которое вы хотите провести. Это создаст миллионы возможных перестановок для тестирования. и часто это занимает очень много времени (более 12 часов). Используя стандартный брут-форсировать словарь с** -w **, вероятно, будет достаточно в большинстве случаев. Если нет, вы также можете попробовать разные словари.**

Давайте сначала запустим скрипт на сайте pepsi.com :

```
корень @ OSINT: python enumall.py pepsi.com -a -p ../altdns/words.txt -w \
/SecLists/sortedcombied-knock-dnsrecon-fierce-reconng.txt
РЕЗЮМЕ
-------
[*] Всего найдено 78 (51 новых) хостов.
[*] В '/opt/recon/domain/pepsi.com.csv' добавлено 167 записей.
корень @ OSINT: python enumall.py cyper.org -a -p ../altdns/words.txt -w \
/SecLists/sortedcombied-knock-dnsrecon-fierce-reconng.txt
[*] Всего найдено 5 (5 новых) хостов.
[*] В '/opt/recon/domain/cyper.org.csv' добавлено 6 записей.
```

Полученные результаты

В таблице 1.1 показаны результаты использования различных инструментов.

Таблица 1.1: Результаты поиска субдоменов

DNSDumpster
19
1
Хакерская цель
31 год
5
Shodan
28 год
0

Если вы уберете что-нибудь из этой главы, должно быть так, что не все инструменты
идеален, и каждый инструмент, который вы используете, часто дает вам разные (или разные)
полученные результаты. Вы всегда должны использовать несколько инструментов в своем арсенале. Скрипты вроде
Enumall хорош, потому что он будет использовать несколько инструментов, чтобы дать вам максимальную отдачу.
возможные результаты.

Фишинговые домены и опечатки

Типосквоттинг - это метод регистрации фальшивых *доменных* имен, которые выглядят одинаково.
на исходное / законное доменное имя. Это действительно просто причудливый способ сказать это
URL-адрес с ошибкой. Злоумышленники воспользуются тем, что люди делают
орфографические ошибки при вводе и зарегистрируют поддельные доменные имена с
намерение собирать учетные данные, распространять вредоносное ПО или делать что-то
злонамеренный. Злоумышленники часто используют домены с ошибками в фишинговых письмах в качестве
быстрый способ заставить кого-то щелкнуть ссылку.

Гомоглифы сейчас также очень популярны при фишинговых атаках. *Гомоглифы*
символы (или глифы), которые кажутся очень похожими. Сюда часто входят персонажи
из других алфавитов, которые очень похожи на исходный символ. Например,
глядя на pepsi.com и pepsì.com, можете ли вы сразу заметить разницу? «Я»
отличается.

Поиск фишинговых / опечатанных доменов обычно полезен для одного из
две причины. Либо 1) вы хотите включить список потенциальных фишинговых доменов.
для клиента по отчету внешнего теста на проникновение (что вы всегда должны делать);
или 2) вы были наняты для социальной инженерии клиента и вам нужно найти
умный способ обманом заставить пользователей предоставить вам свои учетные данные.
Лучший инструмент, который я нашел для обнаружения опечаток в доменах, - это DNSTwist.
Использование DNSTwist чрезвычайно просто и по делу. Просто вставьте свой
желаемый целевой домен, и он сгенерирует список потенциальных фишинговых доменов
и автоматически проверяет, зарегистрированы ли они и / или активны ли они.
Вы также можете указать следующие переключатели для улучшения результатов:

- -d : использовать собственный файл словаря
- -f : вывод в формат файла (CSV, JSON)

Censys
42
0
Яростный
6
4
Sublist3r
56
5
Enumall / Recon-ng
78
5

■ -r : показать только зарегистрированные домены

■ -w : выполнить поиск в WHOIS по доменам.

■ -b : получать баннеры с хостов.

■ -a : Показать все записи DNS

Давайте запустим его, чтобы показать только зарегистрированные домены и посмотреть результаты:

```
корень @ OSINT: python dnstwist.py -r pepsi.com
```

Сразу с вершины с минимальными усилиями мы получаем 81 попадание (следующие результаты были усечены):

```
Обработка 936 вариантов домена ..... 81 обращение
Дополнение pepsia.com 185.18.82.122 NS: ns.dynamixhost.com
MX: mx2.dynamixhost.com
Дополнение pepsib.com -
Дополнение pepsic.com 78.41.204.29 NS: ns1.torresdns.com
Дополнение pepsid.com 104.31.76.91 2606: 4700: 30 :: 681f: 4c5b
NS: igor.ns.cloudflare.com
Дополнение pepsie.com 199.59.242.151 NS: ns1.bodis.com
MX: mx76.m2bp.com
Дополнение pepsif.com -
Дополнение pepsig.com 184.168.221.50 NS: ns53.domaincontrol.com
MX: mailstore1.secureserver.net
Дополнение pepsih.com -
Дополнение pepsii.com 66.63.171.125 NS: ns1.ehostinginc.com
MX: mail.pepsii.com
Дополнение pepsij.com -
Дополнение pepsik.com 94.152.37.52 NS: ns1.kei.pl MX: pepsik.com
Дополнение pepsil.com NS: juming.dnsdun.com
Дополнение pepsim.com 184.168.221.56 NS: ns65.domaincontrol.com
MX: mailstore1.secureserver.net
Дополнение pepsis.com 69.172.201.153
NS: ns1.uniregistrymarket.link
Дополнение pepsit.com 162.255.119.194
NS: dns1.registrar-servers.com
Дополнение pepsix.com 104.217.67.249 NS: v1.dns234.net
Дополнение pepsiy.com 162.255.119.196
NS: dns1.registrar-servers.com
Пропуск pepi.com 206.220.201.245 NS: ns.net10.net
MX: pepi.com.mx1.net10.rcimx.net
Пропуск pesi.com 216.56.243.144 NS: ns-1311.awsdns-35.org
MX: d140747a.ess.barracudanetworks.com
Пропуск peps.com 213.1.249.100 NS: ns.planit.com
Пропуск ppsi.com 208.91.197.128 NS: ns33.worldnic.com
MX: mx1.netsolmail.net
Пропуск epsi.com 216.198.200.146 NS: ns23.domaincontrol.com
MX: mail.epsi.com
```

Повторение pepssi.com -
Повторение peppsi.com 172.98.192.36 NS: ns1.rentondc.com
Повторение peepsi.com 23.20.239.12 NS: ns1.namebrightdns.com
Повторение ppepsi.com 50.63.202.54 NS: ns01.domaincontrol.com
MX: mailstore1.secureserver.net
Замена pemsi.com -
Замена p3psi.com 184.168.131.241 NS: ns53.domaincontrol.com
MX: mailstore1.secureserver.net
Замена peosi.com 192.185.188.86 NS: ns825.websitewelcome.com
MX: mail.peosi.com
Замена peps9.com -
Замена peps8.com -
Замена pelsi.com 64.118.87.10 NS: ns1.mywwwserver.com
MX: pelsi.com
Замена pepei.com 72.52.179.174 NS: ns1.parklogic.com
Замена pwpsi.com 23.20.239.12 NS: ns1.namebrightdns.com
Замена prpsi.com -
Замена pspsi.com NS: ns1.bdm.microsoftonline.com
MX: pspsi-com.mail.protection.outlook.com
Замена pepsu.com 46.30.215.63 2a02: 2350: 5: 104: cfc0: 0: 8428
NS: ns01.one.com
MX: mx1.pub.mailpod6-cph3.one.com
Замена pepso.com 50.63.202.54 NS: ns63.domaincontrol.com
MX: mailstore1.secureserver.net
Замена pepsj.com 192.232.223.72 NS: ns6175.hostgator.com
MX: mail.pepsj.com
Замена pepdi.com 107.180.21.19 NS: ns67.domaincontrol.com
MX: mail.pepdi.com
Замена pepai.com 185.53.179.24 NS: ns1.parkingcrew.net
MX: mail.h-email.net
Замена pepyi.com 198.1.175.40 NS: ns1.dnsowl.com
Замена mepsi.com 192.64.147.150 NS: dns1.yoho.com
MX: mx1.mepsi.com
Замена гласных pipsi.com 199.59.242.151 NS: ns1.bodis.com
MX: mx76.m2bp.com
Замена гласных popsi.com 35.186.238.101 NS: ns1.namefind.com
Замена гласных pepse.com 198.60.86.20 NS: ns1.markmonitor.com
MX: mailn.scientech.com

Теперь давайте снова запустим его без ключа -r, чтобы найти потенциальные домены, которые мы можем зарегистрироваться в качестве целей фишинга:

корень @ OSINT: python dnstwist.py pepsi.com

Вот сокращенный список некоторых потенциальных доменов, которые мы можем зарегистрировать, чтобы попытаться фиш-пепси (с их разрешения):

Гомоглиф þepsï.com -
Гомоглиф þepsı.com -
Гомоглиф реþśi.com -

Гомоглиф pępȩi.com -
Гомоглиф pepsĭ.com -
Гомоглиф pĕpsı.com -
Гомоглиф pëpsi.com -
Гомоглиф pĕpsï.com -
Гомоглиф ρερsï.com -
Гомоглиф pepsi.com -
Гомоглиф pepsı.com -
Гомоглиф þēþsi.com -
Гомоглиф þepsi.com -
Гомоглиф p
q
epsï.com -
Гомоглиф p
q
epsí.com -
Гомоглиф pepsı.com -
Гомоглиф þepsi.com -
Гомоглиф pepsĭ.com -
Гомоглиф þepsl.com -
Гомоглиф pépsi.com -
Гомоглиф pepsĭ.com -
Гомоглиф þeps1.com -
Прошивка pelpsi.com -
Прошивка pepwsi.com -
Прошивка p4epsi.com -
Прошивка pepsai.com -
Прошивка psepsi.com -
Прошивка pepswi.com -
Прошивка pepasi.com -
Прошивка pepdsi.com -
Прошивка pe4psi.com -
Прошивка pep0si.com -
Прошивка peopsi.com -
Прошивка pzepsi.com -
Прошивка pe3psi.com -
Прошивка pezpsi.com -
Прошивка pepsyi.com -
Прошивка pepxsi.com -
Прошивка pempsi.com -
Прошивка pewpsi.com -

Резюме

В этой главе было рассмотрено множество вопросов, касающихся сети и субдоменов. открытие и разведка. Мы рассмотрели такие инструменты, как Sublist3r, fierce и Enumall, которые необходимы любому цифровому исследователю или тестеру на проникновение, потому что их способности обнаруживать субдомены в целевом домене.

В этой главе также были затронуты такие сервисы, как Shodan и Censys.io, которые
большие хранилища доступной для обнаружения информации о сервере, а также могут использоваться для
определить серверы или устройства для вашей целевой организации.
Наконец, в этой главе сравнивается эффективность поиска этих разных
инструменты и услуги, глядя на тип результатов, которые они предоставляют при тестировании
веб-сайты разных размеров.

Рискуя показаться излишним, вы никогда не должны полагаться на один инструмент.
для всех ваших результатов.

В следующей главе мы будем опираться на эти результаты, используя недавно обнаруженные нами
поддомены и поиск сетевой активности, и, в конечном итоге, утечка информации
возраст в инфраструктуре организации.

67

4

В этой главе основное внимание уделяется идентификации активных хостов и портов с помощью расширенных Методы сканирования NMAP. Практически для каждого случая NMAP является святым Грааль «какой инструмент использовать в первую очередь» для поиска активных хостов. Потому что NMAP - такой неизбежный инструмент для каждого хакера и исследователя. арсенал Тора, я чувствую, что он уже до смерти покрыт множеством других книги. Вместо того чтобы перефразировать основы выполнения сканирования NMAP, в этой главе сосредоточусь на нескольких передовых сценариях использования и методах, которые я использовал для обнаруживать активность хоста даже через самые сложные брандмауэры.

Начиная

Значительный объем критических данных может быть получен в результате выполнения протокола NMAP. сканы, которые действительно могут задать тон для остальной части вашего участия. Прежде, чем мы Для начала, эта книга предполагает, что вы имеете базовое представление о NMAP - что это такое, как это работает и как им пользоваться. Если вы новичок в NMAP, вы возможно, захотите ознакомиться с бесплатными онлайн-уроками; или если ты похож на меня, просто поиграйте с этим.

Ищу сетевую активность (Расширенные методы NMAP)

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

Подготовка списка активных хостов

Обычно это первое сканирование, которое я выполняю. Он предназначен для сканирования всего локального IP-пространства.

и вернитесь с красиво оформленным списком активных хостов. Я использую это

для внутренних тестов на проникновение, но его можно легко адаптировать, чтобы определить, какие внешние адреса живые.

Я использую следующую команду, чтобы получить список всех активных хостов на внутреннем

сеть:

```
root @ OSINT: nmap -n -sn 10.0.0.0/8 172.16.0.0/12 192.0.0.0/16 -oG - | \
awk '/ Up $ / {print $ 2}'> outputfile.txt
```

Эта команда выполняет следующие действия:

1. -sn выполняет сканирование ping (используйте -sS, если ping отключен)
2. Сканирует все внутренние IP-адреса.
3. -oG - выводит в greppable формат
4. Отправляет вывод в AWK, чтобы отображать только IP-адреса, помеченные как Up.
5. Отправляет вывод в outputfile.txt.

Результатом будет очень чистый список *активных* IP-адресов, которые вы можете использовать для

твоя следующая задача. Список будет выглядеть так:

```
192.168.0.1
192.168.0.2
192.168.0.3
... и так далее.
```

Полное сканирование портов с использованием различных типов сканирования

Мне редко везет с одним типом сканирования над другим. Обычно это удача розыгрыша,

и я всегда считаю хорошей практикой запускать полное сканирование NMAP,

Найдите способы убедиться, что я ничего не пропустил. *Я также сканирую каждый порт. Всегда* .

Для менее сложных сетей обычное сканирование SYN работает.

потому что целевая машина ответит SYN / ACK, если порт открыт

и RST (сброс), если он закрыт.

Но на самом деле стандартное сканирование TCP с использованием SYN или FIN будет типичным

могут быть заблокированы, особенно если вы имеете дело с IDS

/ IPS. Лучше всего начать с рождественского сканирования (-sX), но если вы не получаете

желаемых результатов вы должны поэкспериментировать с –scanflags .

Вот как мы настраиваем наше сканирование:

■ -p- : сканировать все порты, а не только стандартные или стандартные. Это будет

добавить некоторое время отсканированного как NMAP будет сканировать порты 1 - 65535.

■ -sU : сканировать UDP.

Большинство сканирований сосредоточены только на TCP-портах. Несколько сервисов и портов используют UDP общаться и их часто не хватает. Наши предыдущие типы сканирования (-sS , -sX , и т. д.) не найдет UDP-порты. Чтобы найти эти порты и сервисы, нам нужно включают -sU переключатель.

■ --scanflags : Сообщает NMAP, какие типы сканирования использовать. При беге сканирование NMAP, вы должны определить этот параметр. Некоторые типы сканирования включают нулевое сканирование, сканирование FIN и сканирование Xmas. --scanflags позволяет вам установить несколько Типы сканирования.

■ Стоит попробовать следующие настройки: PSH , FINPSH и SYNFIN . PSH постарается получить ответ, манипулируя флагом PSH заголовка TCP. ФИНПШ постарается та же тактика, но также будет пытаться манипулировать флагами FIN . SYNFIN будет попробуйте манипулировать флагами FIN, а также попытайтесь получить ответ, используя метод SYN / ACK .

Запустим полное сканирование портов pepsi.com :

```
root @ OSINT: nmap -v -p- -sX -sU pepsi.com --scanflags PSH
```

Результаты этого сканирования не были идеальными. Все порты возвращаются как открытые / отфильтровано:

```
Запуск Nmap 7.70 (https://nmap.org) в 2018-12-11 01:03 CST
Запуск сканирования Ping в 01:03
Сканирование pepsi.com (18.214.229.99) [4 порта]
Сканирование Ping завершено в 01:03, прошло 0,06 с (всего 1 хост)
Запуск параллельного разрешения DNS для 1 хоста. в 01:03
Завершено параллельное разрешение DNS для 1 хоста. в 01:03, прошло 0,00 с
Запуск сканирования XMAS в 01:03
Сканирование pepsi.com (18.214.229.99) [65535 портов]
Время сканирования XMAS: выполнено около 18,48%; ETC: 01:06 (осталось 0:02:17)
Статистика: прошло 0:00:39; 0 хостов завершено (1 вверх), 1 проходит сканирование XMAS
Время сканирования XMAS: выполнено около 25,85%; ETC: 01:06 (осталось 0:01:52)
Время сканирования XMAS: выполнено около 53,74%; ETC: 01:06 (осталось 0:00:59)
Завершено сканирование XMAS в 01:05, прошло 117,00 с (всего 65535 портов)
Запуск сканирования UDP в 01:05
Сканирование pepsi.com (18.214.229.99) [65535 портов]
Статистика: прошло 0:02:17; 0 хостов завершено (1 загружено), 1 проходит сканирование UDP
Время сканирования UDP: выполнено около 11,73%; ETC: 01:08 (осталось 0:02:30)
Время сканирования UDP: выполнено около 35,76%; ETC: 01:08 (осталось 0:01:30)
Время сканирования UDP: выполнено около 66,45%; ETC: 01:07 (осталось 0:00:40)
Завершено сканирование UDP в 01:07, прошло 108,80 с (всего 65535 портов)
Отчет о сканировании Nmap для pepsi.com (18.214.229.99)
Хост работает (задержка 0,058 с).
Запись rDNS для 18.214.229.99: ec2-18-214-229-99.compute-1.amazonaws.com
Все 131070 просканированных портов на pepsi.com (18.214.229.99) открыты | фильтруется
```

Сканирование окна TCP

-Sw выключатель NMAP будет выполнять «окна сканирования.» Сканирование окна TCP похоже на сканирование ACK, но было разработано, чтобы различать открытые и закрытые порты вместо того, чтобы показывать порты как неотфильтрованные:

```
корень @ OSINT: nmap -v -p- pepsi.com -sW
Запуск Nmap 7.70 (https://nmap.org) в 2018-12-11 01:15 CST
Запуск сканирования Ping в 01:15
Сканирование pepsi.com (18.214.229.99) [4 порта]
Сканирование Ping завершено в 01:15, прошло 0,05 с (всего 1 хост)
Запуск параллельного разрешения DNS для 1 хоста. в 01:15
Завершено параллельное разрешение DNS для 1 хоста. в 01:15, прошло 0,00 с
Запуск сканирования окна в 01:15
Сканирование pepsi.com (18.214.229.99) [65535 портов]
Время сканирования окна: выполнено около 13,16%; ETC: 01:19 (осталось 0:03:25)
Время сканирования окна: выполнено около 26,85%; ETC: 01:19 (осталось 0:02:46)
Время сканирования окна: выполнено около 41,15%; ETC: 01:19 (осталось 0:02:10)
Время сканирования окна: выполнено около 54,07%; ETC: 01:19 (осталось 0:01:43)
Время сканирования окна: выполнено около 64,15%; ETC: 01:19 (осталось 0:01:24)
Время сканирования окна: выполнено около 74,69%; ETC: 01:19 (осталось 0:01:01)
Время сканирования окна: выполнено около 85,98%; ETC: 01:19 (осталось 0:00:34)
Статистика: прошло 0:03:37; 0 хостов завершено (1 вверх), 1 проходит сканирование
Время сканирования окна: выполнено около 89,93%; ETC: 01:19 (осталось 0:00:24)
Завершено сканирование окна в 01:19, прошло 244,88 с (всего 65535 портов)
Отчет о сканировании Nmap для pepsi.com (18.214.229.99)
Хост работает (задержка 0,061 с).
Запись rDNS для 18.214.229.99: ec2-18-214-229-99.compute-1.amazonaws.com
Не показано: 65533 отфильтрованных порта
ПОРТОВАЯ ГОСУДАРСТВЕННАЯ СЛУЖБА
80 / tcp закрыт http
443 / tcp закрыт https
```

Посмотри на это! По крайней мере, мы видим, что порты 80 и 443 открыты (что мы уже знал, но приятно иметь подтверждение).

Работа с межсетевыми экранами и IDS

Любой современный брандмауэр или система обнаружения вторжений будет иметь огромный список предварительно настроенных правил блокировки, предназначенных для блокировки или минимизации вашей способности сканировать
их инфраструктура. Если трафик не блокируется напрямую брандмауэром, есть вероятность, что он контролируется IDS. В этом разделе представлены полезные руководства, которые помогут обойти обнаружение этими системами.

Использование Reason Response

Когда NMAP запускает сканирование портов, он возвращает значение каждого порта как находящегося в состоянии открытого, закрытого или отфильтрованного, а также предоставляет имя службы обычно работает на этом порту. Переключатель --reason также вернет причину почему NMAP определил, что порт находится в определенном состоянии. Другими словами, если порт отображается как подключенный, NMAP также вернет код причины, по которому он используется для определения того, почему порт находится в сети.

Идентификация живых серверов

Были ли вы когда-нибудь в ситуации, когда вы сканируете диапазон сети и *каждый* порт на *каждом* IP-адресе активен? Это неприятная ситуация, чтобы столкнуться с ней, особенно официально, когда вы этого не ожидаете. Некоторые современные IDS / IPS могут обнаружить, что вы выполняют сканирование NMAP и переключают его ответы, чтобы каждый порт отображался как открытым. Не зная этого, вы устанавливаете свою команду NMAP для запуска и вывода на XML-файл, затем выясните, что это займет несколько часов. Когда ты придешь назад, вы обнаружите, что размер XML увеличился до нескольких ГБ, потому что NMAP регистрация каждого порта как открытого. Такое случается.

Есть два способа обойти это. Первый - использовать ответ причины коды. Второй - с атаками по времени (о которых пойдет речь в следующем раздел). Коды ответа причины могут использоваться для обнаружения действующих серверов из-за способ, которым активный (или несуществующий) сервер отвечает на ваши проблемные запросы. При использовании переключателя --reason вы получите один из трех ответов:

- Закрыто: сбросить
- Открыть: синхронизировать
- Отфильтровано: порт недоступен

Если порт действительно недоступен, ответа не будет и результат вернется как отфильтрованный. Однако, если вы получите ответ сброса , вы знаете, что на другом конце есть что-то живое.

Основываясь на нашем предыдущем примере, вот FIN-сканирование списка / 24 (реальные IP-адреса опущено). Это реальный сценарий, когда клиент владел всем ассортиментом и Каждый IP-адрес предназначен для отображения полностью активных портов, чтобы отпугнуть злоумышленника:

```
корень @ OSINT: nmap -T4 -sF --send-ip --reason 1.2.3.4/24 -oX new-out.xml
```

Следующий XML-код представляет собой образец результатов. Каждый IP-адрес показывает статус «работает», но обратите внимание на значение поля причины . В тех случаях, когда не было активности, причина - «нет ответов» . В случаях, когда брандмауэр законно блокирует наши сканы, ответ покажет «сбрасывает» :

```
<host starttime = "1544321477" endtime = "1544321651"> <status state = "up"
причина = "эхо-ответ" причина_ttl = "246" />
```

<адрес addr = "1.2.3.4" addrtype = "ipv4" />
<имена хостов>
</hostnames>
<ports> <extraports state = "closed" count = "1000">
<extrareasons reason = "resetts" count = "1000" />
</extraports>
</ports>
<times srtt = "39452" rttvar = "16489" to = "105408" />
</host>
<host starttime = "1544321477" endtime = "1544321604"> <status state = "up"
причина = "эхо-ответ" причина_ttl = "53" />
<адрес addr = "1.2.3.5" addrtype = "ipv4" />
<имена хостов>
<hostname name = "cassutility.com" type = "PTR" />
</hostnames>
<ports> <extraports state = "open | filter" count = "1000">
<extrareasons reason = "no-answers" count = "1000" />
</extraports>
/ порты>
<times srtt = "23131" rttvar = "23131" to = "115655" />
</host>
<host starttime = "1544321477" endtime = "1544321639"> <status state = "up"
причина = "эхо-ответ" причина_ttl = "53" />
<адрес addr = "1.2.3.6" addrtype = "ipv4" />
<имена хостов>
</hostnames>
<ports> <extraports state = "open | filter" count = "1000">
<extrareasons reason = "no-answers" count = "1000" />
</extraports>
</ports>
<times srtt = "23763" rttvar = "23763" to = "118815" />
</host>
<times srtt = "22516" rttvar = "22516" to = "112580" />
</host>
<host starttime = "1544321477" endtime = "1544321633"> <status state = "up"
причина = "эхо-ответ" причина_ttl = "53" />
<адрес addr = "1.2.3.7" addrtype = "ipv4" />
<имена хостов>
</hostnames>
<ports> <extraports state = "open | filter" count = "1000">
<extrareasons reason = "no-answers" count = "1000" />
</extraports>
</ports>
<times srtt = "22949" rttvar = "22949" to = "114745" />
</host>

Используя эту информацию, вы можете фильтровать IP-адреса с ответом «сбрасывает» в чтобы определить актуальный список действующих адресов.

Уклонение от брандмауэра

Обход межсетевого экрана с использованием протокола NMAP становится все более трудным, поскольку IDS / IPS становится более изощренным. Есть еще несколько ошибок и много случаев
где многие из этих устройств неправильно настроены.
Некоторые новые конфигурации IDS покажут, что все порты закрыты. Это
очевидно, когда вы тестируете IP-адрес с веб-сайта, так как порт веб-сайта
должен хотя бы отображаться как открытый.

Распределенное сканирование с использованием прокси и TOR

Один из способов полностью анонимизировать ваши отсканированные изображения - распределить их по случайные прокси. В следующих разделах описывается несколько способов сделать это.

Служба ротации прокси

Есть много сервисов, которые продают вам вращающиеся прокси (просто
Google «вращающиеся прокси»). Это работает так: вы получаете один IP-адрес для подключения.
nect through, и этот IP-адрес подключается к Интернету, используя любое количество
случайно вращающиеся прокси. Теперь вы можете легко распространять свои сканы NMAP
через тысячи разных IP-адресов, которые могут сильно отличаться
Это повлияет на результаты сканирования.
Чтобы использовать прокси с NMAP, укажите адрес с помощью переключателя --proxy :

```
root @ OSINT: nmap -sX –proxy http://1.1.1.1:1080 -iL targetlist.txt
```

Прокси-цепочки

Вместо использования одного прокси, proxychains позволяет использовать строку
вместе несколько прокси, что затрудняет определение исходного IP-адреса. Один раз
proxychains установлен в вашей системе Linux, вы можете редактировать proxychains.
conf, чтобы добавить список прокси, которые вы хотите объединить в цепочку. Результат
похоже на то, как TOR распределяет ваш трафик, но TOR довольно медленный. Этот
подход намного быстрее.
Запуск прокси-цепочек довольно прост. Команда такая:

```
proxychains <команда, которую вы хотите запустить>
```

Выполнение команды NMAP через прокси-цепочки будет выглядеть так:

```
корень @ OSINT: прокси-цепи nmap -T4 -sX 1.2.3.4
```

Другой способ добиться аналогичного эффекта - использовать прокси TOR. Вы уже можете использовать прокси в NMAP с помощью переключателя –proxy **и отправить сканирование через локальный TOR прокси. Или вы можете использовать** proxychains **для объединения нескольких прокси вместо**

используя сеть TOR. Есть также отличные сервисы, такие как Storm Proxies, которые подойдут это для вас за ежемесячную плату. Этот подход лучше всего, если вы не хотите поддерживать ваша собственная прокси-сеть. Storm Proxies автоматически меняет за вас 70 000 прокси. так что вам не нужно беспокоиться об обнаружении вашего IP-адреса или хлопотах с настройкой и запускаете собственный прокси TOR.

Фрагментированные пакеты / MTU

Хотя существует очень низкая вероятность того, что использование только фрагментированных пакетов переключатель будет работать (-f), стоит попробовать, если есть неправильно настроенная IDS.

-F переключатель указывает Nmap посылать 8-байтовых пакетов, фрагментацию зонд в пакеты гораздо меньшего размера:

```
корень @ OSINT: nmap -f -sX -Pn -v pepsi.com
```

Параметр --mtu (максимальная единица передачи) аналогичен -f тем, что отправляет ограниченный объем данных во время передачи. Это потенциально может сбить с толку некоторые старые брандмауэры, и потребуется немного поэкспериментировать, чтобы они заработали правильно:

```
root @ OSINT: nmap -sX -v --mtu 32 pepsi.com
```

Уловка с обнаружением сервисов

Если порт отображается как закрытый или отфильтрованный, вы можете обмануть хост предоставление ответа путем запроса версии службы. Уловка за обоими эти методы должны заставить NMAP предполагать, что все порты открыты с -Pn переключатель. Не нужно решать, открыт порт или закрыт, NMAP будет независимо от того, запускать все тесты на обнаружение операционной системы и служб. Ты можешь повезет и получите ответ.

-A переключатель позволит «продвинутой и агрессивную» функцию обнаружения ОС. Использование переключателя -A аналогично указанию нескольких различных опций NMAP. например -O (определение ОС) и -sC (запускает скрипты по умолчанию для хоста).

-SV переключатель позволит определение версии на порт. Это невероятно шумно из-за того, что при сканировании необходимо проверить наличие нескольких версий. Если вы не заботитесь о создании шум, возможно, стоит попробовать. Переключатель -sV часто требуется для различения между открытыми и отфильтрованными портами UDP. Также важно отметить, что определение версии работает очень медленно, так как включает отправку большого количества тестов, специфичных для приложения. в каждый открытый порт. Из-за этого эта команда также может вылетать плохо написанные приложения, поэтому используйте их с осторожностью.

Следующие результаты демонстрируют, как это работает. Сначала запустим стандартный Рождественское сканирование на сайте pepsi.com :

```
корень @ OSINT: nmap -sX pepsi.com
Запуск Nmap 7.70 (https://nmap.org) в 2019-03-08 23:45 CST
Примечание. Хост не работает. Если это действительно так,
но блокируя наши зонды ping, попробуйте -Pn
Выполнено Nmap: 1 IP-адрес (0 подключенных хостов) просканирован за 3,07 секунды
```

Теперь давайте запустим сканирование того же хоста, но проинструктируем NMAP принять все порты открыты и для определения версии сервиса:

```
корень @ OSINT: nmap -Pn -sV pepsi.com
Запуск Nmap 7.70 (https://nmap.org) в 2019-03-08 23:29 CST
Отчет о сканировании Nmap для pepsi.com (45.60.135.51)
Хост работает (задержка 0,049 с).
Другие адреса для pepsi.com (не проверяются): 45.60.75.51
Не показано: 778 фильтрованных портов
ВЕРСИЯ ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПОРТА
25 / tcp открыть http Incapsula CDN httpd
53 / tcp открытый домен?
80 / tcp открыть http Incapsula CDN httpd
81 / tcp открыть http Incapsula CDN httpd
82 / tcp открыть http Incapsula CDN httpd
83 / tcp открыть http Incapsula CDN httpd
84 / tcp открыть http Incapsula CDN httpd
85 / tcp открыть http Incapsula CDN httpd
88 / tcp открыть http Incapsula CDN httpd
89 / tcp открыть http Incapsula CDN httpd
90 / tcp открыть http Incapsula CDN httpd
99 / tcp открыть http Incapsula CDN httpd
389 / tcp открыть ssl / http Incapsula CDN httpd
443 / tcp открыть ssl / http Incapsula CDN httpd
444 / tcp открыть ssl / http Incapsula CDN httpd
555 / tcp открыть http Incapsula CDN httpd
587 / tcp открыть http Incapsula CDN httpd
631 / tcp открыть http Incapsula CDN httpd
636 / tcp открыть ssl / http Incapsula CDN httpd
777 / tcp открыть http Incapsula CDN httpd
800 / tcp открыть http Incapsula CDN httpd
801 / tcp открыть http Incapsula CDN httpd
843 / tcp открыть http Incapsula CDN httpd
888 / tcp открыть http Incapsula CDN httpd
[результаты усечены]
1 сервис не распознан, несмотря на возвращение данных.
SF-Port53-TCP: V = 7,70% I = 7% D = 3/8% Время = 5C834F5B [усечено]
```

Теперь, когда мы знаем, что хост находится за CDN, мы, вероятно, можем предположить, что большинство этих портов фактически не открыты. Тем не менее, эти результаты значительны. сильно отличается от первого сканирования.

Низко и медленно

Параметр -T в протоколе NMAP изменяет время между запросами. Варианты сроков
могут быть использованы для обмана передовых систем обнаружения. Если разложить сканы,
может показаться менее вероятным, что вы действительно выполняете сканирование портов. Понижение
скорость между запросами - хороший способ избежать обнаружения брандмауэра, но
Стоимость этого значительно увеличивает время сканирования. Следующие сроки
доступны настройки:

- T0 : параноик (ждет 5 минут между отправкой каждого зонда, обычно не
обнаруживается IDS / IPS)
- T1 : Подлый (ждет 15 секунд)
- T2 : вежливый
- T3 : Нормальный
- T4 : агрессивный
- T5 : Безумие (легко обнаруживается)

В типичной ситуации сканирования я часто использую -T4 . -T3 - поведение NMAP по умолчанию,
поэтому -T4 немного повысит скорость. Использование переключателя времени не приведет к
отображаются в выводе инструмента по-разному, но могут давать разные результаты. Следующие
В примере нижнего сканирования время между сканированиями устанавливается на «агрессивное», что устанавливает
максимальная задержка 10 мс между каждым датчиком:

```
корень @ OSINT: nmap -sX -T4 yourtarget.com
```

Плохие контрольные суммы, приманка и случайные данные

В этом разделе будут рассмотрены три различных метода NMAP, которые включают отправку
недопустимые или поддельные данные для цели, чтобы вызвать ответ.

Плохие контрольные суммы

Протокол TCP / IP использует «контрольные суммы» для обеспечения целостности данных.
Создавая пакеты с неверной информацией о контрольной сумме, мы могли бы
чтобы заставить целевой хост отправить ответ. Обычно это работает только в
случай неправильно настроенных серверов, но если вы застряли, стоит попробовать, особенно
если вы пытаетесь обойти брандмауэр.

Мы можем отправлять неверные контрольные суммы нашим целям, используя переключатель -badsum . Потому что
CDN, мы видели в предыдущем сканировании, что результаты использования --badsum могут быть
вводящие в заблуждение. При использовании --badsum против pepsi.com мы видим следующие результаты:

```
корень @ OSINT: nmap -sX -T4 --badsum 45.60.135.51
Запуск Nmap 7.70 (https://nmap.org)
Отчет сканирования Nmap для 45.60.135.51
```

Хост работает (задержка 0,050 с).
Не показано: 778 фильтрованных портов
ПОРТОВАЯ ГОСУДАРСТВЕННАЯ СЛУЖБА
25 / tcp открыть smtp
53 / tcp открытый домен
80 / tcp открыть http
81 / tcp открыть hosts2-ns
82 / TCP открытый xfer
83 / tcp открыть mit-ml-dev
84 / tcp открыть ctf
85 / tcp открыть mit-ml-dev
88 / tcp открыть kerberos-sec
89 / тцп открытый су-мит-тг
90 / tcp открытый dnsix
Открытая метаграмма 99 / tcp
389 / TCP открыть LDAP
443 / TCP открыть https
444 / tcp открыть snpp
555 / tcp открытый dsf
587 / tcp открытое представление

Результаты всех портов оказались открытыми, хотя мы уже знаем
за ними стоит сеть CDN, которая влияет на наши результаты.

Сканирование с ловушкой

При выполнении сканирования-ловушки NMAP будет имитировать дополнительные появляющиеся пакеты.
приходить с разных поддельных адресов-ловушек. Это может
заставить хост думать, что он подвергается бомбардировке из нескольких систем одновременно.
и заставит IDS / брандмауэр игнорировать сканирование нашей основной системы.
Чтобы включить ложные пакеты, используйте команду -D , за которой следует RND: [число] .
Это скажет NMAP сгенерировать *X* случайных ловушек.
Эта команда больше предназначена для сокрытия вашего IP-адреса, чем для обхода IDS.
При выполнении сканирования-ловушки IDS может сообщить о 10 различных сканированиях портов.
с уникальных IP-адресов, не зная, какой IP-адрес фактически выполняет
сканировать. Это может быть хорошим способом замаскировать ваш реальный IP-адрес, создав много
шума. Очевидно, эта атака очень шумная, но если цель - замаскировать IP-адрес
машина, выполняющая сканирование, обратите внимание, что ваш реальный IP-адрес все равно будет
в журналах. Лучший способ замаскировать ваш IP-адрес - использовать прокси, как раньше.
обсуждали.
Следующая команда сгенерирует 10 ложных пакетов при использовании SYN
Сканирование против цели:

root @ INTEL: nmap -D RND: 10 **-sS** pepsi.com

Результаты такие же, как вы только что видели, поскольку мы не меняем тип
сканирования, только добавление ложных целей.

Изменить длину данных

Сканеры портов обычно отправляют запросы одинакового размера, поэтому некоторые брандмауэры / IDS предназначен для обнаружения сканирования портов по размеру пакета. Мы можем попробовать избежать такого типа обнаружения, используя параметр -data-length и указав дополнительные данные для отправки с пакетами. Если вы собираетесь поэкспериментировать с это, попробуйте просканировать один порт, который, как вы знаете, открыт (например, 80 или 443), и сыграйте вокруг размера пакета, пока вы не получите ответ, который вам нравится:

```
корень @ OSINT: nmap -sS -data-length 300 scanme.nmap.org
Запуск Nmap 7.01 (https://nmap.org) в 2018-12-12 08:52 UTC
Отчет о сканировании Nmap для scanme.nmap.org (45.33.32.156)
Хост работает (задержка 0,085 с).
Другие адреса для scanme.nmap.org (не проверяются):
2600: 3c01 :: f03c: 91ff: fe18: bb2f
Не показано: 996 закрытых портов
ПОРТОВАЯ ГОСУДАРСТВЕННАЯ СЛУЖБА
22 / TCP открыть SSH
80 / tcp открыть http
9929 / tcp открыть nping-echo
31337 / TCP Open Elite
Выполнено Nmap: 1 IP-адрес (1 хост активен) просканирован за 2,41 секунды
```

Подмена IP / MAC-адреса

Другой способ обойти обнаружение брандмауэра - подменить MAC. адрес вашего хоста. Этот метод может быть очень эффективным, если на сервере есть Правило фильтрации MAC, которое разрешает трафик только с определенных MAC-адресов. В Обратной стороной является то, что вам нужно знать MAC-адрес машины, которая разрешено запрашивать ваши серверы. Этот метод с большей вероятностью будет использоваться на сканирование внутренней сети. Если вы знаете, что цель использует конкретного поставщика, вы можете попробовать соберите образцы MAC-адресов из их продуктов и используйте их в своем сканировании.

Точно так же вы можете подделать исходный порт или IP-адрес, чтобы цель думала вы поступаете с хоста в целевой подсети. Есть экземпляры где брандмауэры разрешают запросы с определенных портов или IP-адресов, поэтому это может быть стоит попробовать.

Подмена вашего IP-адреса означает, что вы *никогда не* увидите ответный пакет, если только у вас есть доступ к этому IP-адресу. Подмена IP-адреса сканирования требует от вас чтобы привязать ваш запрос к сетевому интерфейсу с помощью переключателя -e **. Обычно это требуют, чтобы вы установили на вашем компьютере фальшивую внутреннюю сетевую карту (например, vnic1) и**

отправьте запрос оттуда. Подмена MAC-адреса - это тактика, которая обычно не используется сканирование внешнего обнаружения. Это наиболее эффективно при сканировании внутренней сети, когда вы могут идентифицировать доверенные машины в сети.

Следующая команда подделает IP-адрес:

```
nmap -sF -e vnic1 -S 192.168.0.182 pepsi.com
```

Чтобы подменить MAC-адрес в сети, используйте переключатель --spoof-mac :

```
nmap -sF -e vnic1 –spoof-mac <MAC-адрес> pepsi.com
```

Огнехождение

Firewalking собирает информацию о хосте с помощью IP TTL (время жизни) алгоритм истечения срока, чтобы определить, активен хост или нет. Вкратце, маршрут к хосту определяется с помощью traceroute. Затем пакет отправляется на хост с TTL равным расстоянию до цели. Если время ожидания пакета истекло, он отправляется повторно. с предыдущим значением минус один. Если ICMP тип 11 код 0 (превышен TTL) получен, это означает, что пакет был переадресован и порт не заблокирован. Если ответ не получен, порт на шлюзе заблокирован. Поскольку traceroute зависит от уровня IP (поле TTL), может использоваться любой транспортный протокол таким же образом (TCP, UDP и ICMP).

Механизм сценариев NMAP (NSE) имеет сценарий firewalk, который автоматически выполните все эти шаги. Скрипт попытается обнаружить правила брандмауэра, используя ранее описанный метод истечения срока действия IP TTL.

Мы можем запустить скрипт firewalk, используя следующую команду:

```
nmap --script = firewalk --script-args = firewalk.max.probed.ports = 5 \
--traceroute host
```

Сравнение результатов

В предыдущих примерах мы запускали несколько различных типов сканирования и предварительно в конечном итоге вывести их все в какой-то формат, к которому мы можем вернуться и посмотреть at (я обычно использую XML).

Ndiff - это инструмент, похожий на команду Linux diff . Он покажет вам различия между файлами. Ndiff специально разработан, чтобы показать вам различия между Результаты NMAP.

Обычно я запускаю три или четыре различных варианта сканирования, чтобы убедиться, что у меня есть все моих баз накрыл. Ndiff разработан в этих случаях, чтобы показать вам, что изменилось между разными сканированиями.

Другой вариант использования - системный администратор, который запускает сканирование NMAP в своей сети. работают каждую неделю и хочет узнать, не появилось ли что-нибудь новое. Ndiff бы быть самым быстрым способом сделать это.

Запускать Ndiff очень просто. Просто запустите ndiff, а затем два файла
вы хотите сравнить:

```
корень @ OSINT: ndiff nmap-scan1.xml nmap-scan2.xml
```

Наш вывод покажет нам любые различия между двумя типами сканирования:

```
-Nmap 7.01 сканирование инициировано как: nmap -p- -sX -iL ips.txt -oX nmap-scan1
+ Сканирование Nmap 7.01 инициировано как: nmap -sP -T4 --send-ip --reason \
-iL ips.txt -oX nmap-scan2
1.2.3.4:
-Не показано: 65534 закрытых порта
СОСТОЯНИЕ ПОРТА
СЕРВИСНАЯ ВЕРСИЯ
-11211 / tcp open | отфильтровано
1.2.3.5:
-Не показано: 65535 открытых | отфильтрованных портов
1.2.3.6:
-Не показано: 65534 открытых | отфильтрованных портов
ВЕРСИЯ ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПОРТА
-443 / tcp закрыт https
1.2.3.7
-Не показано: 65534 открытых | отфильтрованных портов
ВЕРСИЯ ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПОРТА
-443 / tcp закрыт https
1.2.3.8:
-Не показано: 65535 открытых | отфильтрованных портов
-1.2.3.9:
+ имя хоста (1.2.3.9):
-Не показано: 65535 открытых | отфильтрованных портов
12.109.109.165:
-Не показано: 65535 открытых | отфильтрованных портов
1.2.3.10:
-Не показано: 65534 закрытых порта
СОСТОЯНИЕ ПОРТА
СЕРВИСНАЯ ВЕРСИЯ
-11211 / tcp open | отфильтровано
-1.2.3.11:
-Хозяин встал.
-Не показано: 65535 открытых | отфильтрованных портов
1.2.3.12:
-Не показано: 65534 закрытых порта
СОСТОЯНИЕ ПОРТА
СЕРВИСНАЯ ВЕРСИЯ
-11211 / tcp open | отфильтровано
```

Основываясь на этих результатах, похоже, что наше рождественское сканирование выявило, что порт 11211 открыт на нескольких хостах (который обычно связан с Memcached).

Стилизация отчетов NMAP

У меня всегда были проблемы с визуализацией результатов NMAP. Там есть несколько программ, которые говорят, что они это делают, но я ничего не нашел стоит. Фактически вы можете стилизовать вывод файла NMAP XML с помощью XSL таблицы стилей с параметром –stylesheet . Андреас Хонциа из Германии cre- использовал действительно хороший XSL-лист для оформления вывода NMAP в хорошо читаемый отчет:

```
nmap -sS pepsi.com -oA имя файла --stylesheet \
https://raw.githubusercontent.com/honze-net/nmap-bootstrap-xsl/
мастер / nmap-bootstrap.xsl
```

После завершения сканирования вы можете просмотреть XML-файл в веб-браузере. В результаты будут выглядеть как на Рисунке 4.1.

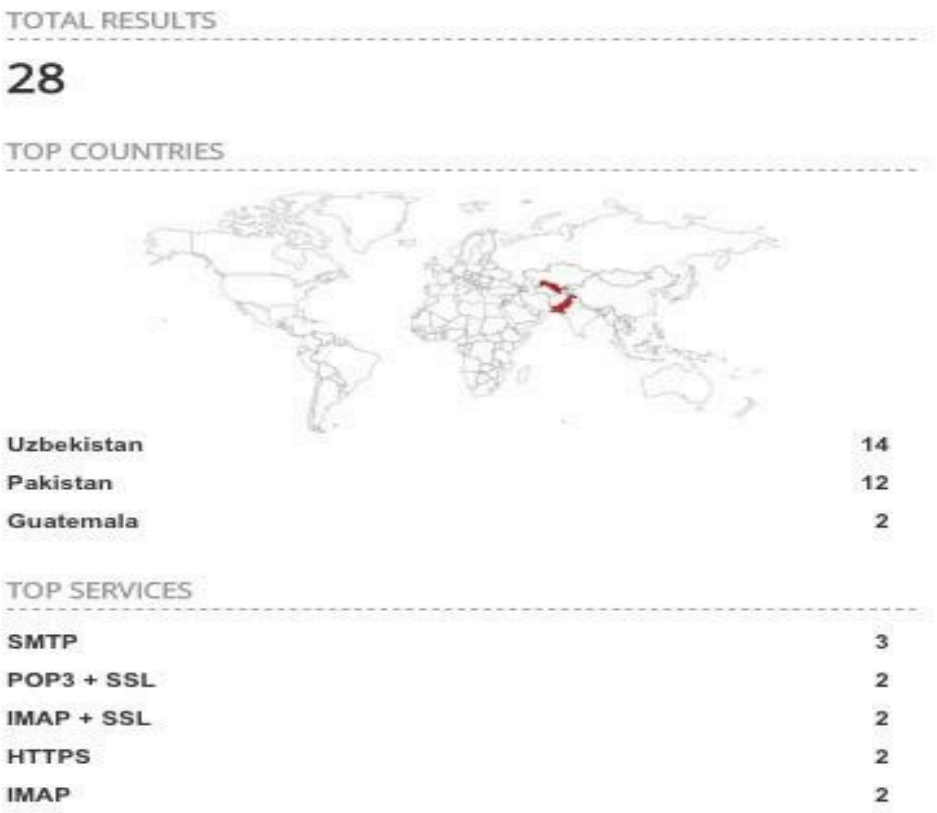


Рисунок 4.1.

Резюме

В этой главе был рассмотрен ряд передовых методов использования протокола NMAP для определить активность на целевом IP-адресе. Как межсетевые экраны и обнаружение вторжений системы продолжают становиться все более сложными, разные подходы должны использоваться для обеспечения точности и полноты результатов сканирования. Теперь, когда мы рассмотрели ручные инструменты и подходы для обнаружения информации о тар-получает, следующая глава будет посвящена нескольким автоматизированным инструментам, которые можно использовать для упростить наши усилия и расширить объем наших результатов поиска.

5

Мы рассмотрели ряд инструментов командной строки, которые можно использовать вручную, чтобы получить
разведка по целям, но что, если вы спешите или просто хотите взять ружье
подход к поиску как можно большего количества сразу?
В этой главе будут рассмотрены три автоматизированных инструмента, которые вы можете использовать для сбора
информации.
быстро, и различные функции каждого. Инструменты в этом разделе специфичны:
их называют «автоматизированными», потому что они глубже разбираются в любых результатах,
автоматически анализируя любые результаты и объекты, полученные на вашем первом этапе, чтобы найти
новая информация.
Например, если обнаружен адрес электронной почты, инструменты автоматически
запрашивать различные API-интерфейсы, чтобы найти столько точек подключения к этому адресу электронной почты, сколько
возможный; тогда как с инструментами командной строки это обычно ручной процесс.
Эти инструменты автоматически возьмут результаты, полученные на шаге 1, и автоматизируют ваши
следующие шаги для вас.
В случае обнаружения адреса электронной почты инструмент может проверить, есть ли у него
были взломаны, или если есть какие-либо данные WHOIS из таких источников, как Secu-
rityTrails или Whoisology. В случае обнаружения IP-адреса инструменты могут
автоматически начать поиск связанных доменных имен или запросить информацию об угрозах
например VirusTotal, чтобы проверить, есть ли IP-адрес в известных черных списках.
Результаты между каждым инструментом примерно на 80% похожи друг на друга. Это часто
оставшиеся 20%, которые могут иметь значение в расследовании и обеспечить
наиболее ценная (или уникальная) информация.

Автоматизированные инструменты для сети

Открытие

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

Другими словами, когда дело доходит до разведки, не существует «единого окна».
сбор, поэтому важно никогда не полагаться на один-единственный инструмент. Всегда
проведите несколько тестов, чтобы убедиться, что ваши результаты точны и полны.
В этой главе обсуждаются три инструмента: SpiderFoot, Intrigue.io и
Recon-NG.

В этой главе мы рассмотрим домен DualXCrypt.com.
(Рисунок 5.1). Сайт предлагает «децентрализованный смартфон» на базе CopperheadOS.
Домен был в сети лишь короткое время (вы все еще можете просмотреть его на archive.org **).**
Интересно то, что люди, создавшие сайт, рекламировали себя
как группа из трех известных хакеров с «Форума KickAss». Я бы не стал
знали об этом сайте, если наш друг Сайпер (владелец форума KickAss) не писал
об этом, в частности, заявив, что они не *имеют* **отношения к KickAss. Похоже на симпатичную**
хороший повод для расследования.

Паук

SpiderFoot - это платформа OSINT, основанная на концепции информации -
цепочка, означающая, что одна часть собранных данных используется для автоматического
получить следующий фрагмент данных в рекурсивном процессе до тех пор, пока все возможные OSINT для
целевая и связанные объекты были собраны.



Рисунок 5.1.

SpiderFoot связывает и связывает данные с помощью более чем 150 модулей, которые
API запросов, такие как Shodan, VirusTotal и Censys (и это лишь некоторые из них). Это даже
сканирует веб-сайты и выполняет сканирование портов. SpiderFoot - это автоматизированный инструмент в
в том смысле, что он будет рекурсивно анализировать любую новую информацию, полученную с помощью
начальное сканирование, чтобы найти как можно больше информации. Результаты будут
экспоненциально раздувается очень быстро.

Запустить SpiderFoot довольно просто:

```
корень @ OSINT: / opt / spiderfoot: python sf.py 0.0.0.0:5001
```

Оттуда вы можете получить доступ к SpiderFoot через веб-браузер через порт 5001. Вы
нужно потратить это время на настройку ключей API в настройках приложения. Однажды ты
подготовьте, запустить первое сканирование довольно просто, как показано на рис. 5.2.

У нас есть несколько различных вариантов сканирования, но, как упоминалось ранее, мы собираемся
для подхода дробовика и будет сканировать все, чтобы увидеть, что
возвращается.

Последний известный IP-адрес DualXCrypt был 185.165.169.124, поэтому мы собираемся
чтобы начать там.

После того, как мы введем наш целевой IP-адрес 185.165.169.124, мы нажимаем Run Scan и позволяем Spi-
derFoot делает свое дело. Когда сканирование будет готово, мы можем заглянуть во вкладку сканирования и
см. наши первоначальные результаты, показанные на рис. 5.3.

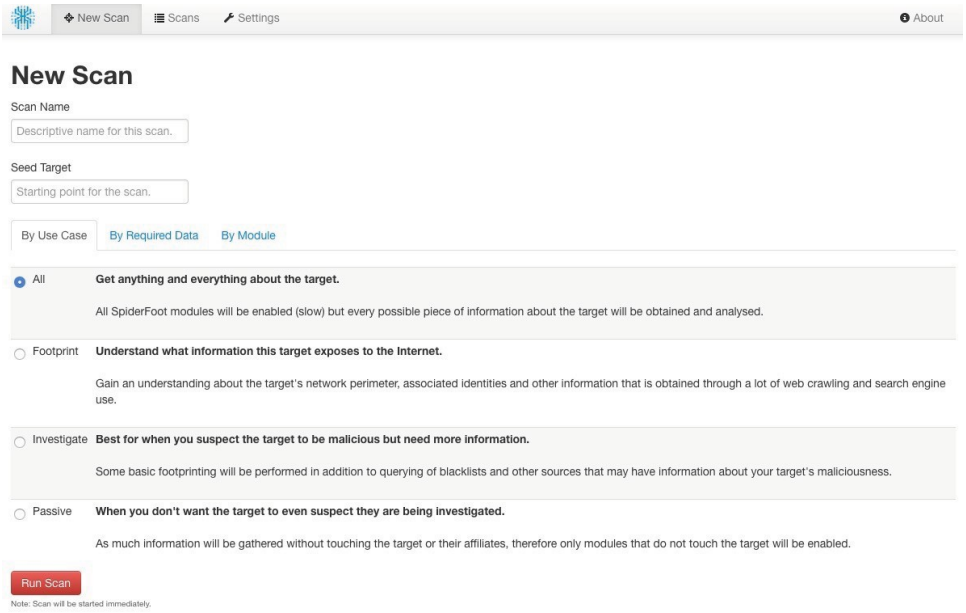


Рисунок 5.2.

Щелчок по IP-адресу покажет нам расширенный список различных элек-
элементы, обнаруженные нашим сканированием (рис. 5.4).

Из результатов на Рисунке 5.4 видно, что существует много действительно взаимозависимых
поиск путей получения новой информации. Особо стоит выделить
количество совместно размещенных вредоносных сайтов (9).

**Одна из причин, по которой я не часто начинаю с дробовика, - это явная
объем возвращенных результатов. Необходимость мысленно обрабатывать такой объем информации в таких
короткое время позволяет очень легко что-то упустить. Если у вас нет действительно
надежная система каталогизации и хранения информации, шансы что-то есть в этих
результаты проведут вас по одному конкретному пути, на котором очень трудно
вернитесь назад и начните заново.**

Name	Target	Started	Finished	Status	Elements	Action
185.165.169.124	185.165.169.124	2018-12-15 08:20:12	2018-12-15 09:59:52	FINISHED	307	

Рисунок 5.3.

185.165.169.124

Status | Browse | Graph | Scan Settings | Log

Type	Unique Data Elements	Total Data Elements
Affiliate - Email Address	79	101
BGP AS Membership	1	1
BGP AS Peer	3	3
Blacklisted IP on Same Subnet	11	11
Co-Hosted Site	47	49
Co-Hosted Site - Domain Name	40	47
Co-Hosted Site - Domain Whois	39	39
IP Address	1	1
Malicious Co-Hosted Site	9	9
Malicious IP Address	36	36
Malicious IP on Same Subnet	5	5
Netblock Membership	1	1
Open TCP Port	2	2
Search Engine's Web Content	2	2

Рисунок 5.4.

Расширяя эту опцию (рис. 5.5), мы можем увидеть список других вредоносных
веб-сайты, использующие один и тот же IP-адрес.

Результаты, показанные на рис. 5.5, заслуживают внимания, поскольку наличие других вредоносных
сайты, использующие один и тот же IP-адрес, необычно. Однако, учитывая контекст
сайта и его владельцев, обнаружение других вредоносных сайтов, использующих тот же IP-адрес
неудивительно. В владельцах доменов могут быть общие черты, которые стоит изучить.

Просмотр других потенциально вредоносных сайтов, использующих тот же IP-адрес, может сказать:
нас о цели. Поскольку мы можем видеть другие потенциально незаконные сайты, такие как торренты
и нелегальные сайты загрузки видео, это также поднимает вопрос о том, где находится сайт
размещается.

Щелкнув ссылку « dualxcrypt.com » в SpiderFoot, мы перейдем прямо на
VirusTotal, где мы можем увидеть, какая информация у них есть о нашем целевом домене.

☐	VirusTotal [dnstars.vip] https://www.virustotal.com/en/domain/dnstars.vip/information/	dnstars.vip
☐	VirusTotal [dualxcrypt.com] https://www.virustotal.com/en/domain/dualxcrypt.com/information/	dualxcrypt.com
☐	VirusTotal [putlockerhd.cc] https://www.virustotal.com/en/domain/putlockerhd.cc/information/	putlockerhd.cc
☐	VirusTotal [tfile-search.cc] https://www.virustotal.com/en/domain/tfile-search.cc/information/	tfile-search.cc
☐	VirusTotal [tfile-video.org] https://www.virustotal.com/en/domain/tfile-video.org/information/	tfile-video.org
☐	VirusTotal [www.seventorrents.cc] https://www.virustotal.com/en/domain/www.seventorrents.cc/information/	www.seventorrents.cc

Рисунок 5.5.

Это довольно интересная находка, потому что в этом конкретном домене было много
Перемещение IP за месячный период. Каждый из этих IP-адресов стоит изучить
потому что возможно, что один из них может быть личным веб-сервером или даже
домашний адрес. Однако, прежде чем мы это сделаем, может быть, стоит посмотреть, где
этот сайт в настоящее время размещен.

Быстрый переход к Censys.io (рис. 5.7) показывает, что ISP - это Flokinet,
размещено на Сейшельских островах. Эта информация может оказаться полезной или бесполезной в будущем,
а пока стоит отметить.

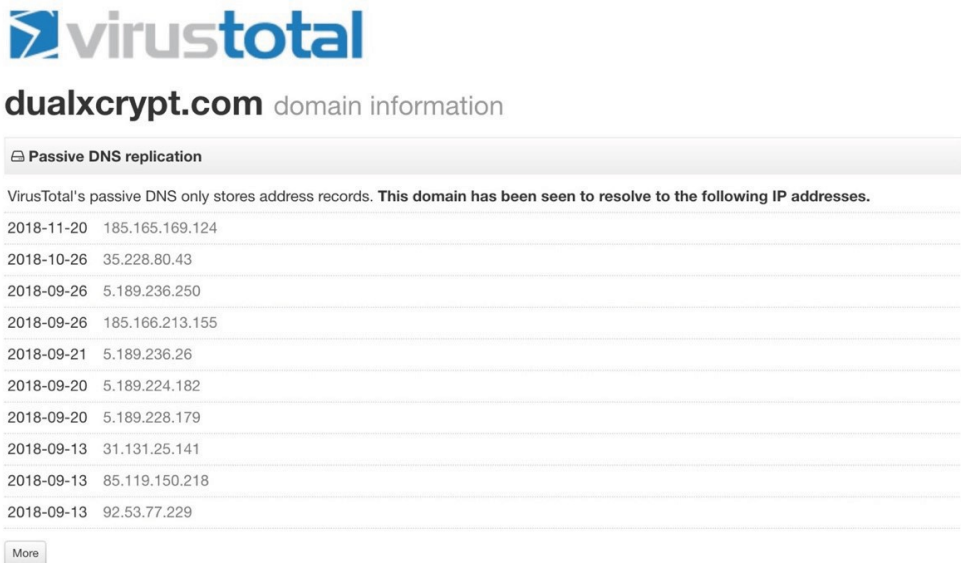


Рисунок 5.6.

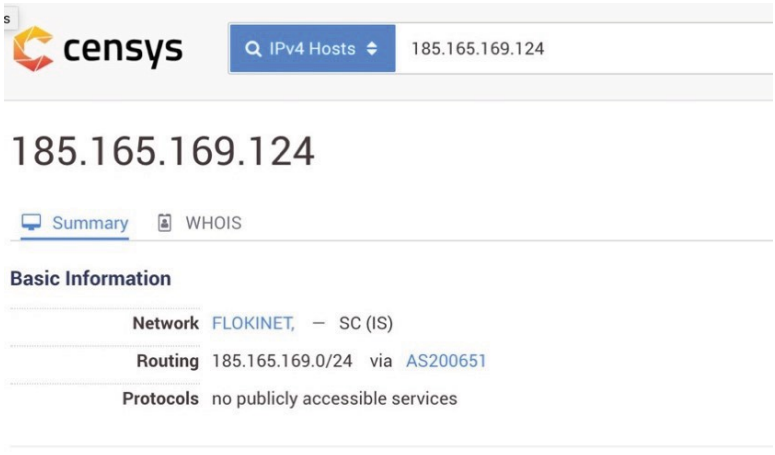


Рисунок 5.7.

Информация WHOIS показывает регистрацию на njalla.io, анонимном
служба регистрации доменов, которая также предоставляет полностью анонимный веб-хостинг,
так что это тупик (в главе 9 подробно рассматривается WHOIS).
Когда некуда исследовать этот конкретный способ сбора информации.
Например, мы можем развернуть и запустить последующее сканирование на соседних IP-адресах или домене.
имена, или, возможно, мы хотим отслеживать разные потенциальные клиенты.

При использовании Censys.io или Shodan поиск « dualxcrypt.com **» на самом деле не возвращает результатов. В этом случае** virustotal.com **является явным победителем с точки зрения доступности. способная информация. Однако существует множество ситуаций, в которых правда. Вы всегда должны тестировать, используя несколько сервисов.**

Не всегда может быть доступен большой объем информации. Итак, давайте попробуем с
гораздо более распространенная цель - популярный веб-форум uberpeople.net .
Вернувшись в главное меню SpiderFoot, мы можем запустить новое сканирование сверхлюдей.
net , как показано на Рисунке 5.8.
После сканирования uberpeople.net мы уже видим, что у нас есть сигнатуры.
значительно больше элементов для работы (рис. 5.9).
В таблице 5.1 показан список различных элементов данных из нашего сканирования убер-
people.net , который включает в себя такие вещи, как записи DNS, адреса электронной почты, нежелательные файлы,
утечка содержимого сайта (через pastebin), имен пользователей и т. д.

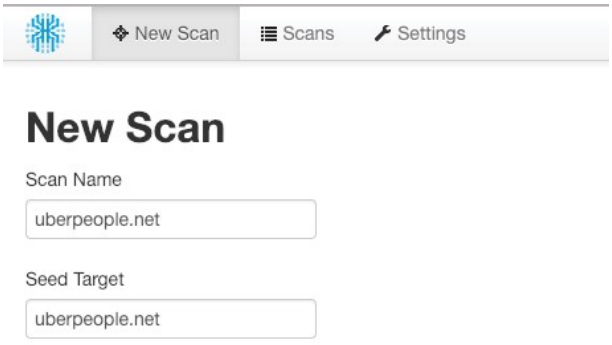


Рисунок 5.8

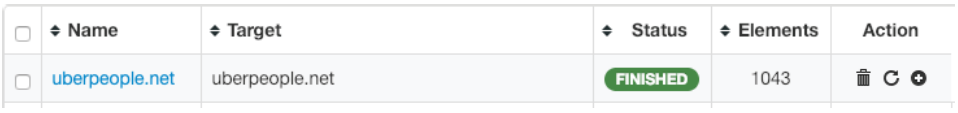


Рисунок 5.9

Таблица 5.1: Список элементов, обнаруженных при сканировании SpiderFoot

Аккаунт на внешнем сайте
12
Партнер - Название компании
5
Партнер - доменное имя
8
Партнер - Whois домена
7
Партнер - адрес электронной почты
19
Партнер - IP-адрес
20
Партнер - Имя в Интернете
13
Членство в BGP AS
1
BGP AS Peer
9
IP-адрес аффилированного лица, внесенный в черный список
1
Совместно размещенный сайт
2
Совместно размещенный сайт - доменное имя
1
Запись DNS SPF
1
Запись DNS TXT
2
Доменное имя
1
Адрес электронной почты
2
Шлюз электронной почты (записи DNS MX)
1
Хостинг-провайдер
2
Айпи адрес
1
Имя в Интернете
18
Имя в Интернете - не определено
6
Нежелательный файл
36
Утечка содержимого сайта
1
URL сайта утечки
2
Связанный URL - внутренний
287
Вредоносный партнер
1
Вредоносный партнерский IP-адрес
10
Вредоносный совместно размещенный сайт
2
Вредоносный IP-адрес
2
Вредоносный IP-адрес в той же подсети
4
Сервер имен (записи DNS 'NS')
2

Всего обнаружено 605 записей. Это *много* информации для
начать с! Это слишком много информации, чтобы принять ее сразу из-за
множество различных направлений исследования, каждая категория может привести вас
вниз. Если вы еще этого не сделали, лучше убедиться, что у вас есть способ сохранить
все ваши данные каталогизированы и упорядочены, иначе вы пропустите и забудете
вещи по пути.

SpiderFoot HX (Премиум)

SpiderFoot HX - это премиум-версия SpiderFoot. HX полностью облачный
и содержит ряд дополнительных улучшений и возможностей, включая
улучшенная скорость сканирования, многопоточное / одновременное сканирование, улучшенная визуализация,
командная работа, идентификация рисков и значительно улучшенная автоматизированная
корреляции данных.

Мое внимание сразу привлек модернизированный механизм автоматической корреляции.
В этом разделе мы повторно просканируем предыдущий набор целей в SpiderFoot HX и
сравните различия.

Чтобы начать сканирование, на рис. 5.10 показаны цели, добавленные в новое сканирование.
окно. Все модули были выбраны в качестве профиля сканирования, который показывает
новое окно сканирования по умолчанию с нашими целями.

Сравнивая различия, мы сразу видим, что HX-версия Spider-
Foot дает больше результатов и даже классифицирует их по уровню риска.

На рис. 5.11 показаны результаты начального риска с двумя элементами высокого риска, двумя средними,
и один низкий.

Членство в Netblock
1
Открыть порт TCP
18
Открыть баннер порта TCP
5
Необработанные записи DNS
15
SSL-сертификат - выдан
2
SSL-сертификат - выдан
4
SSL-сертификат - необработанные данные
8
Несоответствие хоста сертификата SSL
1
Веб-контент поисковой системы
60
Подобный домен
6
Подобный домен - Whois
5
Имя пользователя
1

Заглянув в наш раздел результатов, сразу видно, что пользовательский интерфейс и графические элементы в HX значительно улучшены по сравнению с тем, что можно найти в стандартная версия SpiderFoot, как показано на Рисунке 5.12.

При работе с исполнительными клиентами наличие графических элементов часто может сделайте разницу между хорошим отчетом и отличным отчетом. Я нашел это большинство руководителей не хотят, чтобы в отчете было много слов, которые они больше всего скорее всего, никогда не будет времени читать. Они хотят видеть краткие результаты, маркированный список, и графические элементы, которые они могут использовать, чтобы легко представить результаты своей доске или исполнительная команда.

В целом результаты между бесплатной и премиальной версией SpiderFoot одинаковы. очень похожий. Большинство возвращенных результатов (рис. 5.13) возвращается в Подсеть IP находится примерно в 30 различных черных списках. Кроме того, версия HX нашли дополнительное имя пользователя, связанное с нашей целью, учетной записью Reddit называется «dualxcrypt» (https://www.reddit.com/user/dualxcrypt). Отличное лидерство, но, к сожалению, пользователь ничего не опубликовал.

По общему признанию, это была очень сложная цель, и ее очень мало можно было обнаружить. Информация. Давайте посмотрим, как результаты SpiderFoot HX сравниваются с его открытыми исходный партнер при сканировании uberpeople.net , гораздо более популярной цели

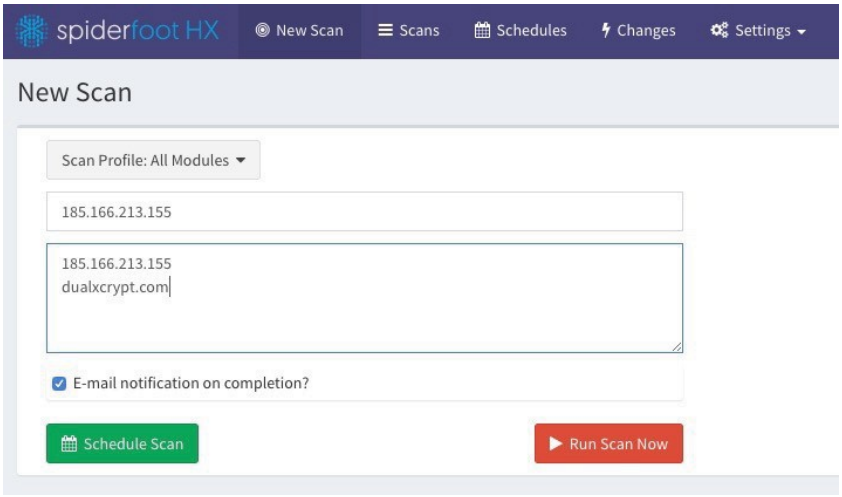


Рисунок 5.10.



Рисунок 5.11.

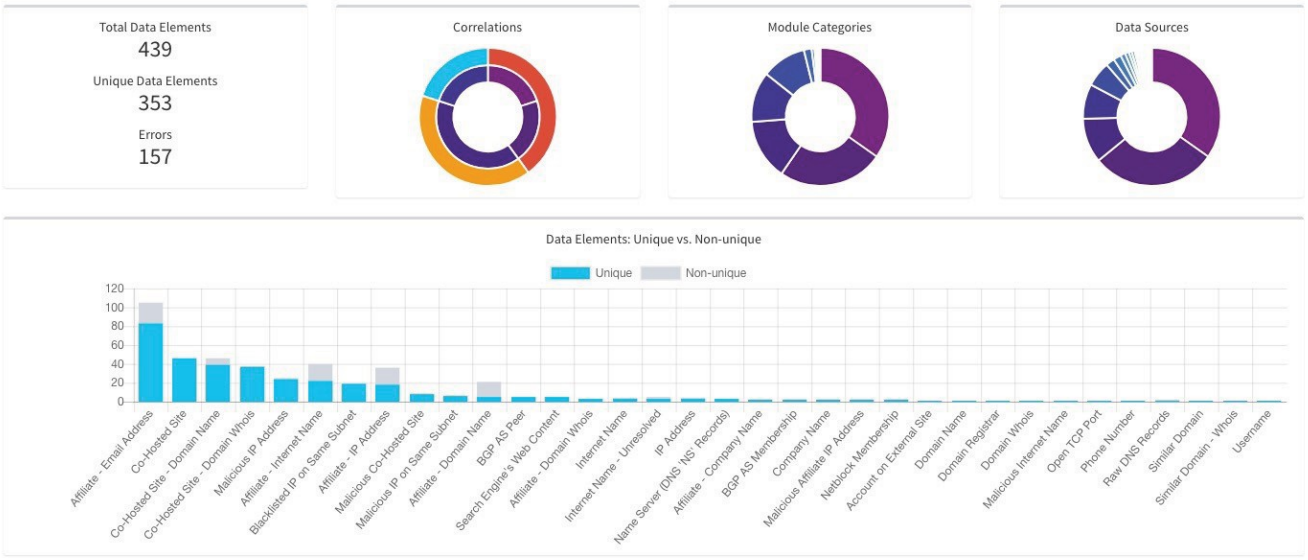

Total Data Elements
439
Unique Data Elements
353
Errors
157
Correlations
Module Categories
Data Sources
Data Elements: Unique vs. Non-unique
Unique
Non-unique
120
100
80
60
40
20
0
Affiliate - Email Address
Co-Hosted Site
Co-Hosted Site - Domain Name
Co-Hosted Site - Domain Whois
Malicious IP Address
Affiliate - Internet Name
Blacklisted IP on Same Subnet
Affiliate - IP Address
Malicious Co-Hosted Site
Malicious IP on Same Subnet
Affiliate - Domain Name
BGP AS Peer
Search Engine's Web Content
Affiliate - Domain Whois
Internet Name
Internet Name - Unresolved
IP Address
Name Server (DNS 'NS' Records)
Affiliate - Company Name
BGP AS Membership
Company Name
Malicious Affiliate IP Address
Netblock Membership
Account on External Site
Domain Name
Domain Registrar
Domain Whois
Malicious Internet Name
Open TCP Port
Phone Number
Raw DNS Records
Similar Domain
Similar Domain - Whois
Username

Рисунок 5.12.

Сканирование HX на uberpeople.net показывает 629 результатов, из которых 1 критический и 2 объекты средней степени риска (рис. 5.15).

Наши предыдущие сканирования uberpeople.net с использованием версии Spider- с открытым исходным кодом. Foot дал 605 общих результатов, в то время как улучшенная версия HX дала 629 результатов.

На первый взгляд 24 дополнительных матча могут показаться незначительными, но эти числа легко могут быть результатом многих факторов, в том числе наших выборочных тестовых сайтов.

В зависимости от вашей должности добавленные визуальные компоненты и возможность экспорт полезных графических элементов может сделать эту подписку очень выгодной

Обновить.

Correlation	Data Elements	Criticality	Created
Entity blacklisted by multiple sources: 185.165.169.0/24	19	HIGH	2018-12-17 09:02:13
Entity considered malicious by multiple sources: 185.165.169.0/24	27	HIGH	2018-12-17 09:02:12
Hostname only from proprietary service: hostmaster.dualxcrypt.com	1	MEDIUM	2018-12-17 09:02:13
Hostname only from proprietary service: www.dualxcrypt.com	1	MEDIUM	2018-12-17 09:02:13
IP address only from proprietary service: 149.129.212.248	1	LOW	2018-12-17 09:02:13

Рисунок 5.13

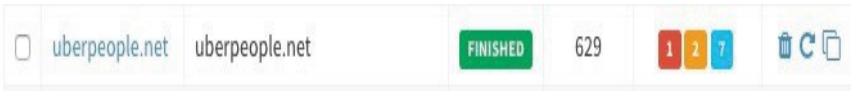


Рисунок 5.14

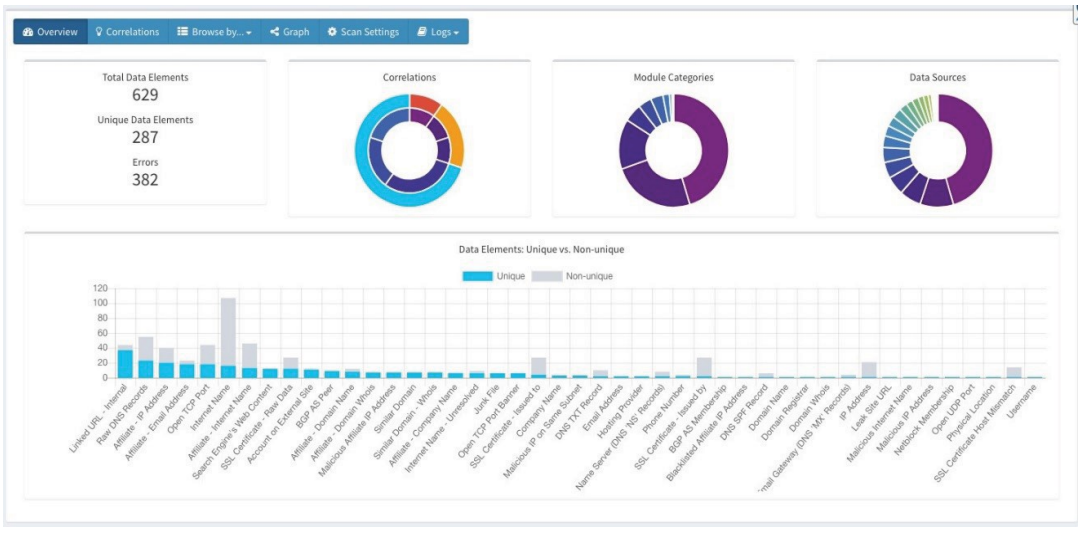


Рисунок 5.15

Intrigue.io

Интрига была разработана разработчиком безопасности и исследователем Джонатаном Краном, и вы можете скачать его на www.intrigue.io . Интрига - движок с открытым исходным кодом на котором работает Intrigue.io, платформа для обнаружения поверхностей для атак. В соответствии с Cran, Intrigue Core был разработан на основе концепции обнаружения на основе графов, позволяя автоматизировать процесс обнаружения поверхности атаки и обеспечения безопасности сбор разведданных.

Основная задача Intrigue - находить активы и «интересные вещи». об организации с внешней точки зрения. Это тоже становится полезным в качестве платформы для разработчиков и групп безопасности для получения информации, связанной с безопасностью вместе в единой стеклянной панели, что позволяет легко находить соединения быть между организационными единицами.

Внутри Intrigue каждый бит информации (или разведданных) классифицируется как *сущность* . Гибкая модель данных Intrigue использует задачи для выполнения функций, которые создают эти сущности. Каждая сущность, в свою очередь, может быть повторена с дополнительными задачами - либо вручную или автоматически. Интрига использует эту модель данных, а другая итеративная концепция под названием *машины* , чтобы конкретизировать активы и уязвимости организация.

Что меня больше всего впечатляет в Intrigue, так это ее способность обрабатывать, обнаруживать, и автоматически обрабатывать вновь обнаруженные объекты.

Например, предположим, что вы выполняете широкий поиск по доменному имени. Интрига может вернуть ряд сущностей, включая IP-адрес, связанный с доменные имена и поддомены (и это лишь некоторые из них). Используя «обогащать» вариант, Интрига возьмет каждую из этих новых сущностей и запустит целую батарею тесты по каждому из них. Комбинации и результаты быстро становятся экспоненциальными, сэкономит вам значительное количество времени на ваших начальных усилиях по обнаружению.

Интрига может выполнять большое количество задач, в том числе:

- Открытый поиск в базе данных: Censys, SecurityTrails и Shodan
- Поиск в WHOIS
- Проверки публичной доски Trello
- Брутфорс S3, Trello и других общедоступных сегментов.
- Spidering URI
- Перебор каталога и имени файла
- Перечисление DNS / серверов имен

- Поиск прозрачности сертификата (CRT.sh)
- Связанные проверки серверов имен и DNS-записей
- Соответствующие проверки домена WHOIS
- Обнаружение службы FTP и сбор данных
- Вход по SSH, RDP и VNC (с автоматическими снимками экрана)
- Прогулка NSEC
- Поиск на GitHub (с интеграцией Gitrob)
- И многое другое

**Я считаю Intrigue Core невероятно мощным на уровне приложений,
благодаря библиотеке Ident. Ident был разработан специально для пальцевого уровня приложения.
печать и поддерживается в актуальном состоянии на основе постоянно увеличивающихся данных сканирования, к которым у нас есть доступ
через Intrigue.io. Это дает базовой технологии возможность выполнять зависящие от версии
дактилоскопия и сопоставление уязвимостей.
Благодаря этому множеству встроенных задач, а также уведомлений и концепции проблем,
Intrigue Core - это больше платформа, чем инструмент. Концепция задачи и сущности делает это
легко расширить функциональность приложения. И по мере того, как мы продолжаем находить новые активы, уязвимые-
способности и неправильные конфигурации ищут платформу для дальнейшего развития.**

Чтобы использовать Intrigue для запуска базового автоматического запроса по URI, щелкните значок
Кнопка Пуск. Выберите Create Entity в качестве задачи и установите тип URI (как показано на рисунке).
на рисунке 5.16).

Вкладка Entities

Именно здесь творится волшебство Интриги. На вкладке Entities отображается список
всех обнаруженных типов сущностей. Для DualXCrypt.com мы видим только шесть типов. Для
более популярных целей (которые мы увидим позже в этом разделе), это число будет
быть намного выше.

Ниже приведены типы сущностей для обнаруженных результатов DualXCrypt.
com (рисунок 5.17):

- Домены: 3
- Uri: 1
- IPAddress: 1
- Сетевой блок: 1

Щелчок по любой из этих сущностей предоставит нам больше возможностей и преобразований, которые мы могу бегать. Например, щелкните имя домена. На рисунке 5.18 показан объект страница с подробностями; справа мы видим список опций для новых задач, которые мы можем запустить. При щелчке по типу задачи отображается множество последующих сканирований, которые можно запустить на домен (рис. 5.19), включая поиск CRT.SH (который мы обсуждаем в Глава 10), проверка утечек общедоступных групп Google, утечек Trello, перечисление серверы имен, поиск Whoisology и многое другое. У каждого типа сущности свой набор дополнительных задач, которые можно запустить, чтобы найти дополнительную информацию о вашем цель.

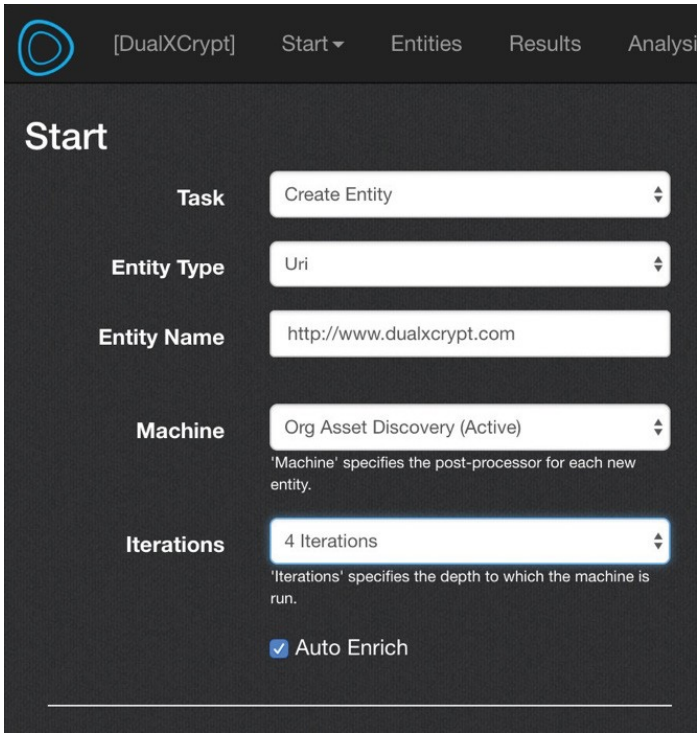


Рисунок 5.16

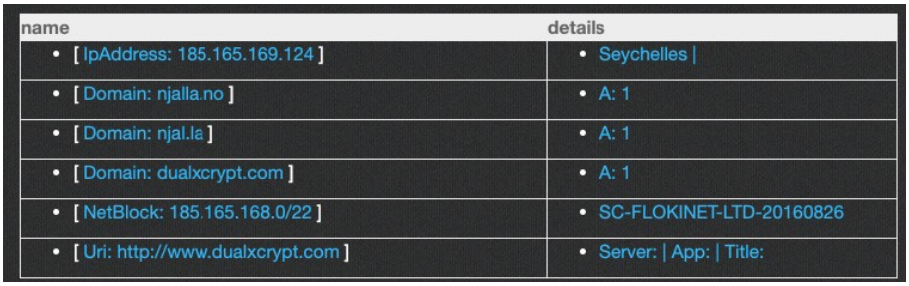


Рисунок 5.17

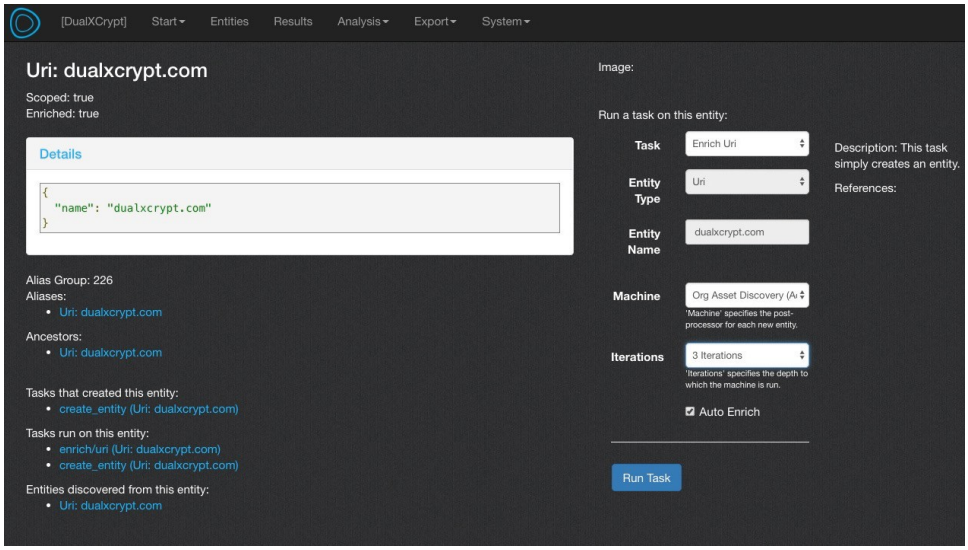


Рисунок 5.18

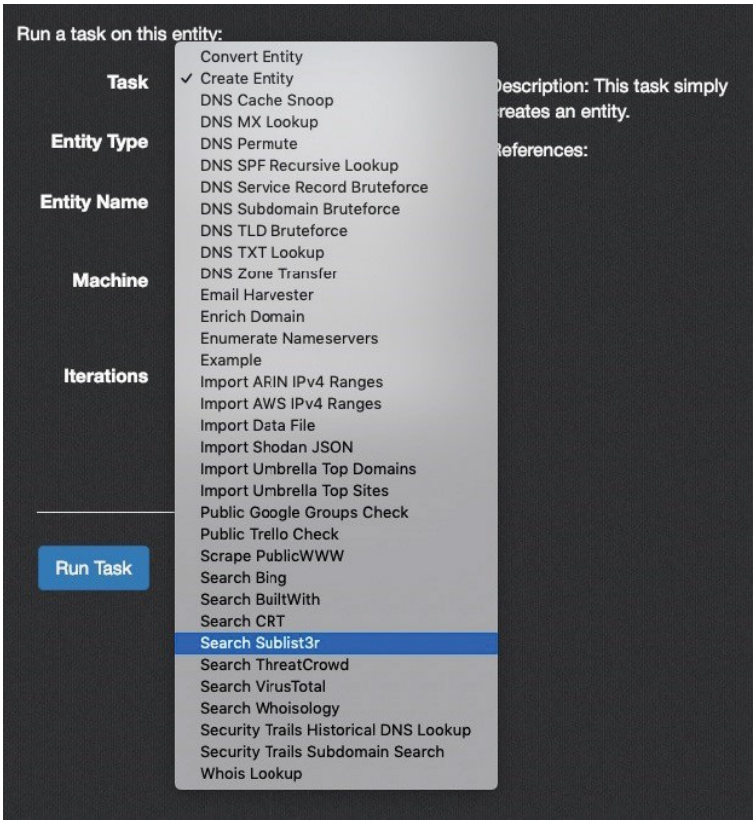


Рисунок 5.19

На экране, показанном на рисунке 5.20, мы также можем развернуть и увидеть более подробную информацию.
на обнаруженном объекте. Щелчок по IP-адресу показывает нам общую информацию
о нем, в том числе о его потенциальном местонахождении. Справа мы можем поднять нашу позицию.
список задач и запускать новые действия на основе этого IP. Обратите внимание, что типы задач
на рис. 5.20 отличаются от предыдущих типов задач. Потому что задача
типы будут меняться в зависимости от того, что может быть выполнено с данным типом сущности.

Анализируем uberpeople.net

Теперь, когда у нас есть понимание возможностей Intrigue, давайте перезапустим.
процесс посмотреть на uberpeople.net . На рисунке 5.21 показан экран добавления объекта.
настроен для запуска сканирования uberpeople.net .
Посмотрев на вкладку «Результаты», мы видим, что ряд задач был выполнен автоматически.
автоматически запускать на uberpeople.net .
На рис. 5.22 показан небольшой образец различных задач, которые выполнялись автоматически.
cally run и количество обнаруженных объектов для каждой задачи.

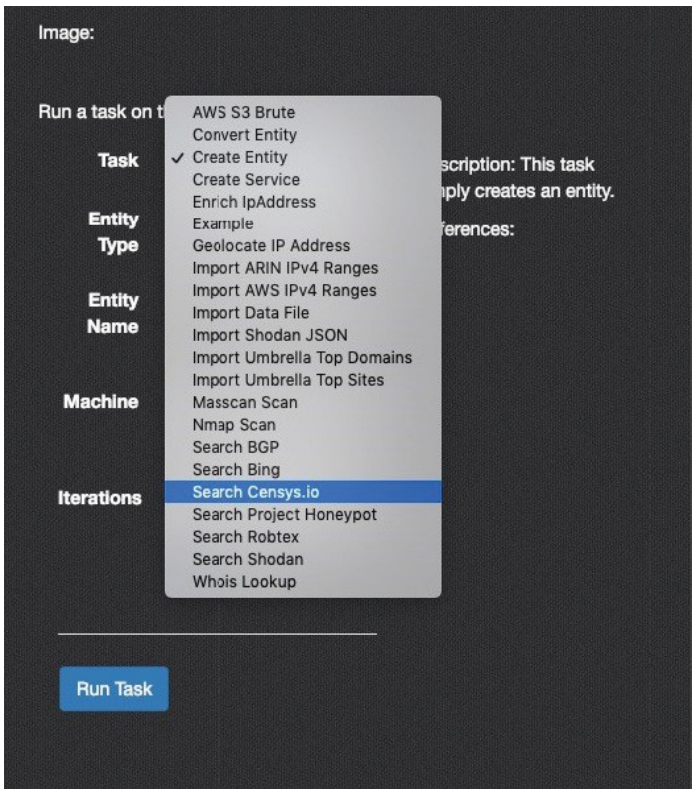


Рисунок 5.20.

Сканирование NMAP выглядит интересно. Если мы щелкнем по нему, мы получим не только список
какие порты были обнаружены, а также хороший список дополнительных объектов, которые мы
можно продолжить изучение, как показано в следующем коде и на рис. 5.23:

```
[_] Параметры: []
[_] Запуск задачи в 2018-12-18 03:52:42 UTC!
[_] Список сканирования: ["185.165.169.124"], порты: 10
[_] Сканирование 185.165.169.124 и сохранение в /tmp/nmap_scan_47907309.xml
[_] Параметры NMap:
[_] Вывод Nmap:
Запуск Nmap 7.01 (https://nmap.org) в 2018-12-18 03:52 UTC
Отчет о сканировании Nmap для 185.165.169.124
Хост включен.
СОСТОЯНИЕ ПОРТА
СЕРВИСНАЯ ВЕРСИЯ
21 / TCP с фильтром ftp
22 / TCP с фильтром ssh
23 / tcp отфильтрованный Telnet
SMTP с фильтром 25 / tcp
80 / TCP с фильтром http
110 / TCP с фильтром pop3
```

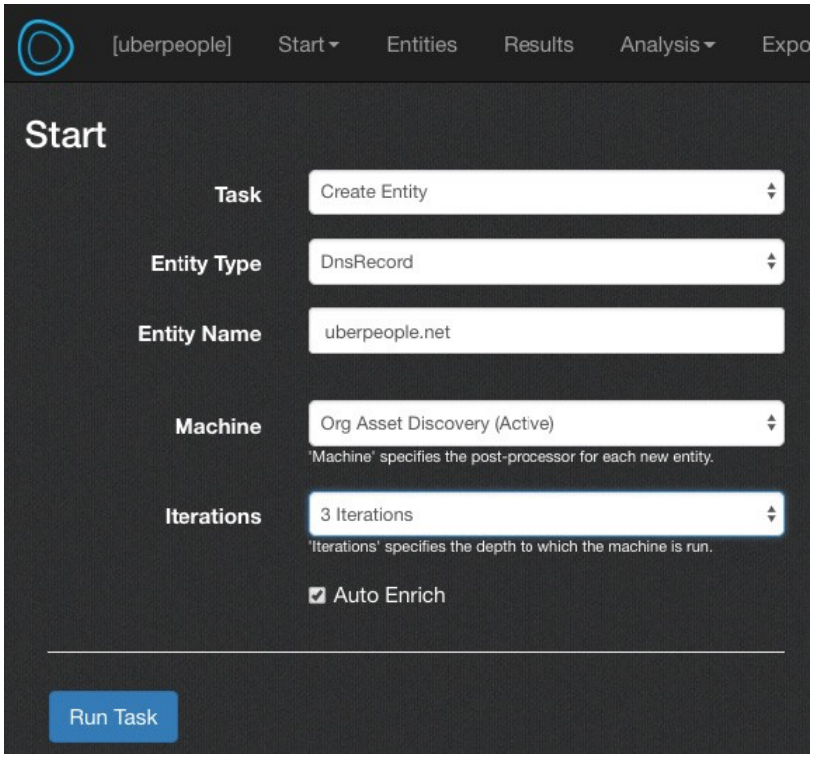


Рисунок 5.21

139 / TCP с фильтром netbios-ssn
443 / TCP с фильтром https
445 / TCP с фильтром microsoft-ds
3389 / tcp с фильтром ms-wbt-server
53 / udp open | отфильтрованный домен
67 / udp open | отфильтрованный dhcps
123 / udp open | отфильтрованный ntp
135 / udp open | отфильтрованный msrpc
137 / udp open | отфильтрованные netbios-ns
138 / udp open | отфильтрованный netbios-dgm
161 / udp open | отфильтрованный snmp
445 / udp open | отфильтровано microsoft-ds
631 / UDP open | отфильтрованный IPP
1434 / udp open | отфильтровано ms-sql-m
Слишком много отпечатков пальцев соответствует этому хосту, чтобы дать конкретные сведения об ОС

Я считаю Intrigue.io действительно уникальным не только из-за количества задач / модули, которые вы можете запускать, но из-за того, насколько широки вы можете использовать эти модулес. Например, в результатах, показанных на рис. 5.24, мы видим веб-диск .uberpeople.net и ftp.uberpeople.net .

dns_brute_sub on DnsRecord: ftp.uberpeople.net	0	complete
enrich/dns_record on DnsRecord: ftp.uberpeople.net	3	complete
dns_brute_sub on DnsRecord: www.uberpeople.net	0	complete
enrich/dns_record on DnsRecord: www.uberpeople.net	3	complete
dns_brute_sub on DnsRecord: cpanel.uberpeople.net	0	complete
enrich/dns_record on DnsRecord: cpanel.uberpeople.net	3	complete
dns_brute_sub on DnsRecord: www.mokotoband.uberpeople.net	0	complete
enrich/dns_record on DnsRecord: www.mokotoband.uberpeople.net	3	complete
dns_brute_sub on DnsRecord: mokotoband.uberpeople.net	3	complete
enrich/dns_record on DnsRecord: uberpeople.net	2	complete
enrich/dns_record on DnsRecord: mokotoband.uberpeople.net	3	complete
dns_brute_sub on DnsRecord: www.bedmaybebreakfast.uberpeople.net	0	complete
enrich/dns_record on DnsRecord: www.bedmaybebreakfast.uberpeople.net	3	complete
dns_brute_sub on DnsRecord: bedmaybebreakfast.uberpeople.net	3	complete
enrich/dns_record on DnsRecord: bedmaybebreakfast.uberpeople.net	3	complete
enrich/nameserver on DnsRecord: ns2.uberpeople.net	0	complete
enrich/nameserver on DnsRecord: ns1.uberpeople.net	0	complete
aws_s3_brute on DnsRecord: uberpeople.net	0	complete
public_google_groups_check on DnsRecord: uberpeople.net	0	complete
dns_brute_sub on DnsRecord: uberpeople.net	13	complete
search_crt on DnsRecord: uberpeople.net	4	complete
enumerate_nameservers on DnsRecord: uberpeople.net	2	complete
dns_brute_sub on DnsRecord: vps.uberpeople.net	0	complete
enrich/net_block on NetBlock: 184.154.0.0/16	0	complete
nmap_scan on IpAddress: 184.154.76.235	39	complete
whois_lookup on IpAddress: 184.154.76.235	1	complete
enrich/dns_record on DnsRecord: vps.uberpeople.net	3	complete
enrich/domain on DnsRecord: uberpeople.net	1	complete
enrich/ip_address on IpAddress: 184.154.76.235	2	complete
create_entity on DnsRecord: uberpeople.net	1	complete

Рисунок 5.22

Изучая результаты для webdisk.uberpeople.net , мы видим, что задача
параметры изменились и относятся к нашей новой цели. На этот раз мы можем бежать
проверки уязвимостей, сканирование хоста, создание снимков экрана (полезно при показе
открыть порты RDP или VNC), и даже выполнить грубую силу против цели
используя такие команды, как «URI Bruteforce» и «URI Bruteforce с учетными данными».

Подбор учетных данных выходит за рамки этой книги и может быть незаконно, если у вас нет необходимых разрешений. Если вы все же используете эти инструменты, используйте их законно и ответственно.

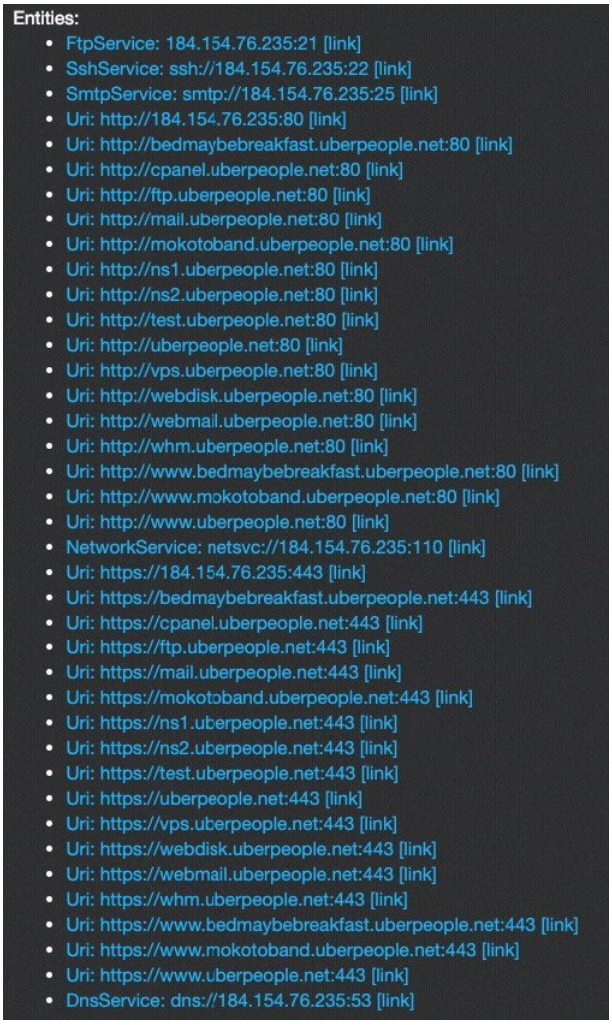


Рисунок 5.23

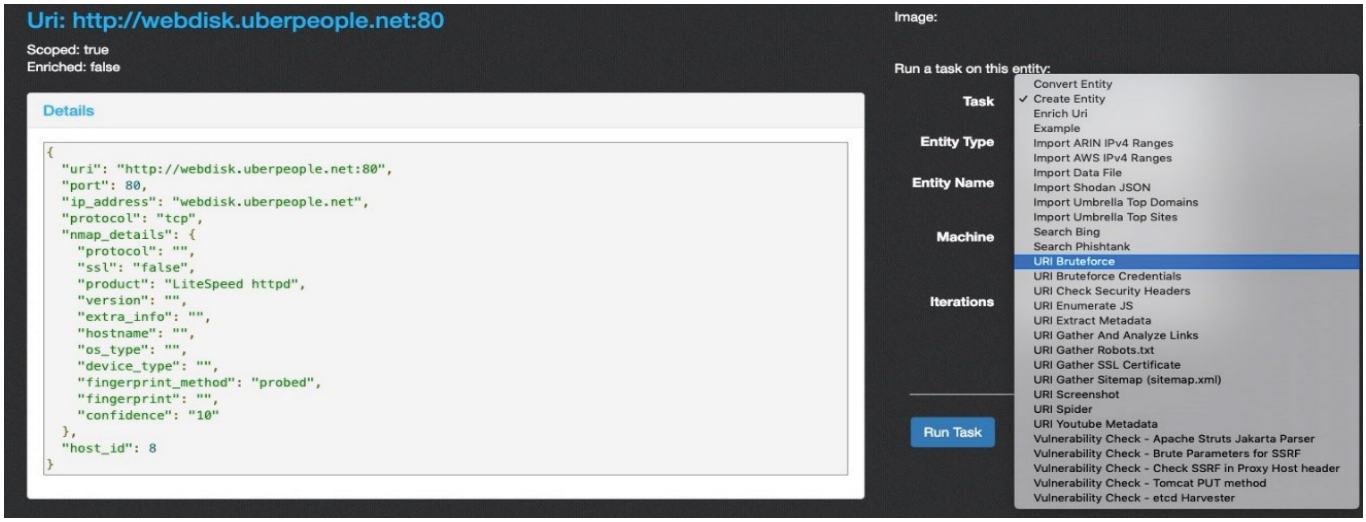

Uri: http://webdisk.uberpeople.net:80
Scoped: true
Enriched: false
Details
{
"uri": "http://webdisk.uberpeople.net:80",
"port": 80,
"ip_address": "webdisk.uberpeople.net",
"protocol": "tcp",
"nmap_details": {
"protocol": "",
"ssl": "false",
"product": "LiteSpeed httpd",
"version": "",
"extra_info": "",
"hostname": "",
"os_type": "",
"device_type": "",
"fingerprint_method": "probed",
"fingerprint": "",
"confidence": "10"
},
"host_id": 8
}
Image:
Run a task on this entity:
Task
Entity Type
Entity Name
Machine
Iterations
Run Task
Convert Entity
Create Entity
Enrich Uri
Example
Import ARIN IPv4 Ranges
Import AWS IPv4 Ranges
Import Data File
Import Shodan JSON
Import Umbrella Top Domains
Import Umbrella Top Sites
Search Bing
Search Phishtank
URI Bruteforce
URI Bruteforce Credentials
URI Check Security Headers
URI Enumerate JS
URI Extract Metadata
URI Gather And Analyze Links
URI Gather Robots.txt
URI Gather SSL Certificate
URI Gather Sitemap (sitemap.xml)
URI Screenshot
URI Spider
URI Youtube Metadata
Vulnerability Check - Apache Struts Jakarta Parser
Vulnerability Check - Brute Parameters for SSRF
Vulnerability Check - Check SSRF in Proxy Host header
Vulnerability Check - Tomcat PUT method
Vulnerability Check - etcd Harvester

Рисунок 5.24

Анализ результатов

Система результатов Intrigue.io невероятно впечатляет. После завершения сканирования щелкните вкладку Entities, чтобы просмотреть все, что он собрал.

Для uberpeople.net мы можем видеть следующие обнаруженные объекты, показанные на Рисунок 5.25:

- Всего организаций: 58 организаций
- NetworkService: 1
- DnsService: 1
- SshService: 1
- FtpService: 1
- SmtpService: 1
- Uri: 34
- IPAddress: 1
- NetBlock: 1
- DnsRecord: 17

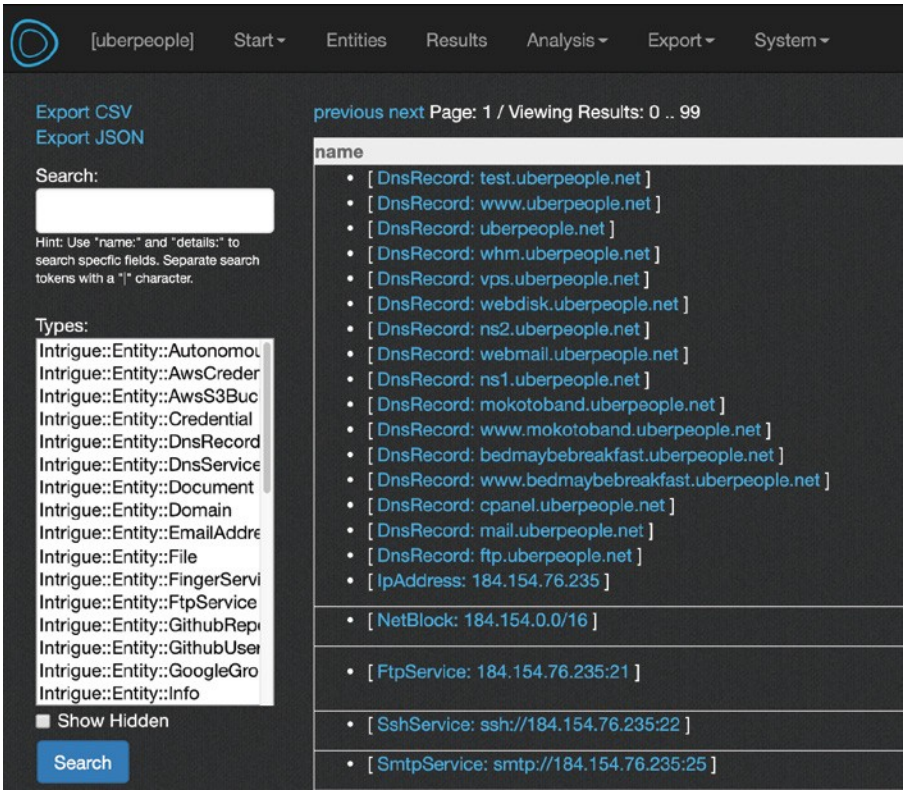


Рисунок 5.25

По мере увеличения размера ваших целей будут расти и ваши результаты. Чтобы добавить немного конт-
В соответствии с нашим тестированием, вот результаты Intrigue при выполнении поиска на
pepsi.com :

- Всего организаций: 208 организаций
- NetworkService: 3
- DnsService: 1
- SshService: 1
- Домен: 15
- Сервер имен: 4
- SmtpService: 1
- Uri: 72
- IP-адрес: 20
- NetBlock: 10
- DnsRecord: 81

Работая в разделе Entities, каждая из сущностей указана в главном меню.
стол. Отсюда вы можете щелкнуть объект, чтобы просмотреть дополнительную информацию и
запускать дополнительные задачи.
Вы также можете отфильтровать свой список, щелкнув один из типов и нажав кнопку
Кнопка поиска. Это отобразит только те типы сущностей, которые вы ищете.
Например, давайте отфильтруем наш поиск по DNSRecords. Для этого щелкните объект
введите (DNSRecord) и нажмите "Поиск". На рис. 5.26 показан обновленный экран.
с отфильтрованными результатами поиска.

Экспорт ваших результатов

На странице "Сущности" вы можете экспортировать результаты в удобном для использования виде.
Форматы CSV или JSON. Еще одна особенность, о которой стоит упомянуть, - это график Intrigue:
способность. Вы можете просмотреть свои результаты в виде диаграммы в стиле Мальтего.
Это может быть полезно для более широкого поиска при поиске централизованного подключения.
точки. Чтобы просмотреть график результатов, выберите пункт меню «Анализ».
На рис. 5.27 показан график, созданный Intrigue.io.
Каждый из узлов на графике доступен для нажатия, поэтому мы можем использовать эту страницу для
быстро получить доступ к любому из объектов и выполнить дальнейший поиск. Рисунок 5.28
показывает крупный план поддомена с интересным звучанием: bedmaybebreakfast.
uberpeople.net .

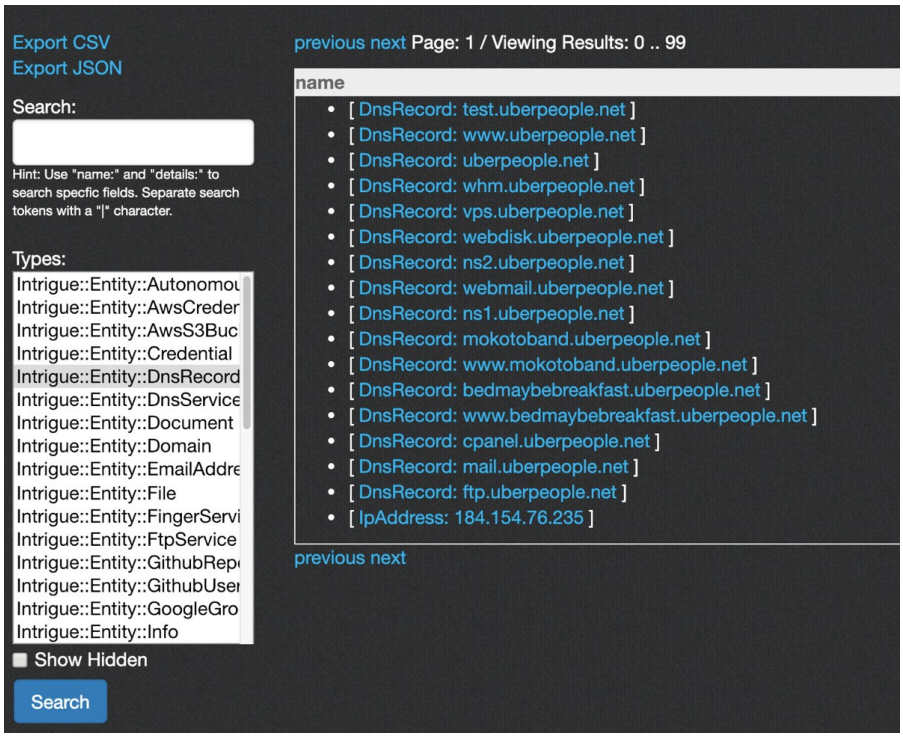


Рисунок 5.26

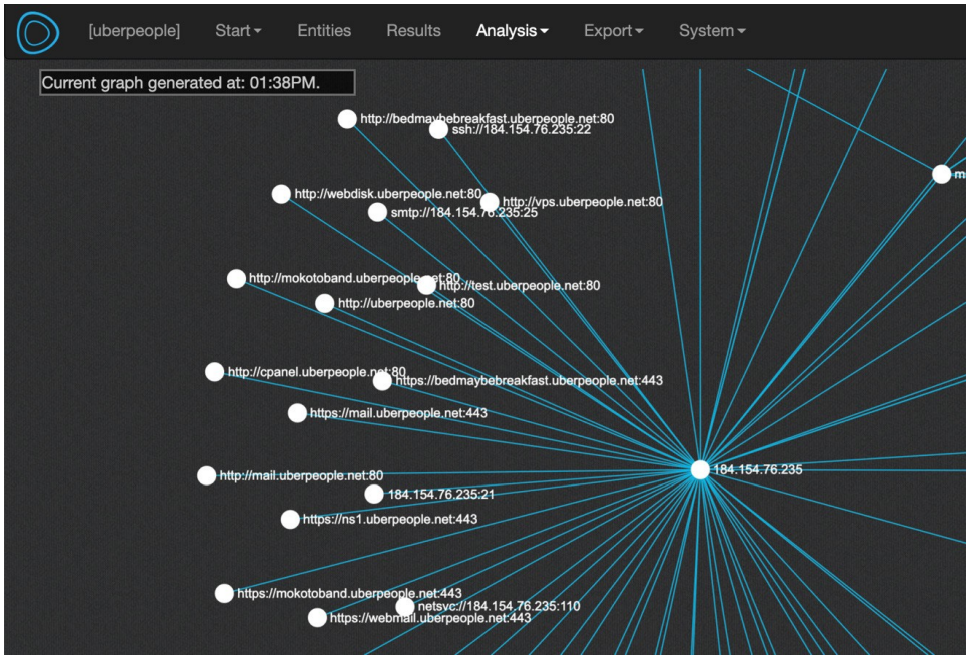


Рисунок 5.27

Щелчок по этой сущности поддомена приведет нас к странице сведений о сущности, показанной на рисунке 5.29.
На этой странице будет отображаться любая обнаруженная информация о конкретном объекте и также позволит нам выполнять дополнительные задачи, такие как выполнение паука полного URL и извлечение метаданных (которое мы обсудим более подробно в главе 12).
Это должно дать вам довольно хорошее представление о возможностях Intrigue. Теперь Давайте перейдем к нашему третьему и последнему инструменту этой главы, Recon-NG.

Recon-NG

Recon-NG, вероятно, один из наиболее широко используемых OSINT / разведывательных сборов. инструменты. Он сочетает в себе многие из функций, которые мы видели в двух предыдущих инструментах. в этой главе, но основывается исключительно на командной строке. К сожалению, графический интерфейс недоступен.

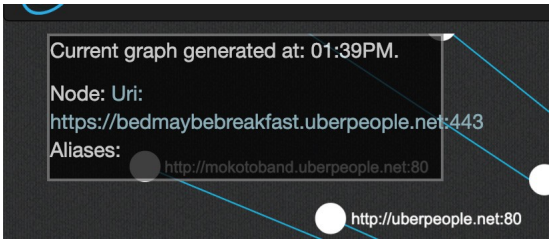


Рисунок 5.28

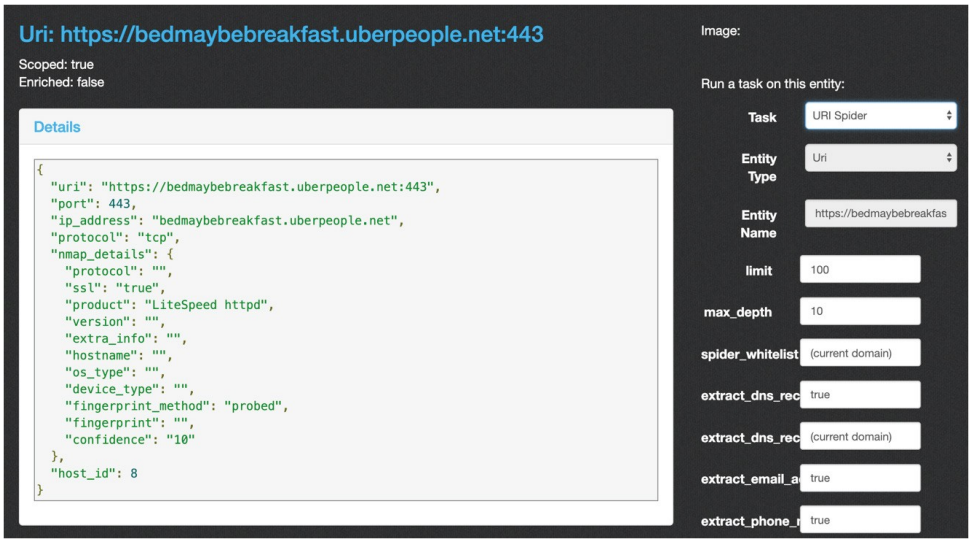


Рисунок 5.29

Recon-NG очень похож на Metasploit тем, что вам нужно вручную загружать и
запустите каждый модуль, который хотите использовать. Инструмент Recon-NG имеет множество встроенных
модули, организованные по категориям, каждый со своими возможностями.
Recon-NG не «автоматизирован», как другие инструменты, но у него есть много
те же возможности. У каждого модуля есть свой набор команд и опций.
Поскольку он основан на командной строке, вы должны указать Recon-NG, что вы хотите.
делать и вручную строить на каждом наборе результатов.
В настоящее время 76 модулей разведки позволяют выполнять различные виды поисков.
на отдельных людей, компании, веб-сайты, профили в социальных сетях, хосты, DNS,
IP-адреса и многое другое.
Запуск Recon-NG представляет собой простую однострочную команду:

```
корень @ OSINT: ./recon-ng
```

После запуска приложения вас встретит Metasploit-esque
страницу, показанную на Рисунке 5.30.
Отсюда Recon-NG будет ожидать вашего ответа, что делать дальше. Если ты
не уверены, какой модуль использовать, вы можете ввести **use** и нажать клавишу Tab, чтобы получить
список, подобный следующему:

```
[recon-ng] [OSINT]> используйте
открытие / info_disclosure / cache_snoop
открытие / информация_дисключение / интересные_файлы
эксплуатация / инъекция / командный_инжектор
эксплуатация / внедрение / xpath_bruter
import / csv_file
импорт / список
```



Рисунок 5.30

Recon / companies-contacts / bing_linkedin_cache
разведка / компании-контакты / головоломка / point_usage
Recon / Companies-Contacts / Jigsaw / Purchase_contact
Рек / домены-уязвимости / панкспайдер
Рек / домены-уязвимости / xssed
Рек / домены-уязвимости / xssposed
рекон / хосты-хосты / bing_ip
Рек / хосты-хосты / ipinfodb
рекон / хосты-хосты / ipstack
рекон / хосты-хосты / разрешить
рекон / хосты-хосты / ssltools
Рек / хосты-хосты / reverse_resolve
рекон / хосты-домены / migrate_hosts
Recon / hosts-domains / migrate_
Recon / Companies-Contacts / Jigsaw / search_contacts
Рек / компании-мульти / github_miner
Рек / компании-мульти / whois_miner
разведка / контакты-контакты / почтовый тестер
разведка / контакты-контакты / вывернуть
разведка / контакты-контакты / распутать
Recon / контакты-учетные данные / hibp_breach
Recon / контакты-учетные данные / hibp_paste
Recon / contacts-domains / migrate_contacts
Recon / контакты-профили / полный контакт
Рек / учетные данные / саман
Recon / учетные данные-учетные данные / bozocrack
Recon / credentials-credentials / hashes_org
Рек / домены-контакты / метакраулер
рекон / домены-контакты / pgp_search
рекон / домены-контакты / whois_pocs
Recon / домены-учетные данные / pwnedlist / account_creds
Recon / домены-учетные данные / pwnedlist / api_usage
Recon / домены-учетные данные / pwnedlist / domain_creds
Recon / домены-учетные данные / pwnedlist / domain_ispwned
Рек / домены-учетные данные / pwnedlist / утечка_просмотр
Рек / домены-учетные данные / pwnedlist / leaks_dump
Recon / domains-domains / brute_suffix
рекон / домены-хосты / bing_domain_api
рекон / домены-хосты / bing_domain_web
рекон / домены-хосты / brute_hosts
рекон / домены-хосты / встроенный
рекон / домены-хосты / certificate_transparency
Recon / domains-hosts / google_site_web
Рек / домены-хосты / hackertarget
рекон / домены-хосты / mx_spf_ip
Рек / домены-хосты / неткрафт
рекон / домены-хосты / shodan_hostname
рекон / домены-хосты / ssl_san

Рек / домены-хосты / угроза толпы
Рек / домены-уязвимости / ghdb
рекон / местоположения-местоположения / геокодировать
рекон / местоположения-местоположения / обратный_геокод
Recon / Location-Pushpins / Flickr
разведка / местоположения-кнопки / Picasa
разведка / местоположения-кнопки / shodan
Рек / местоположения-кнопки / твиттер
Recon / Location-Pushpins / YouTube
Recon / netblocks-компании / whois_orgs
Рек / нетблоки-хосты / обратный_ресолв
Рек / нетблоки-хосты / shodan_net
Рек / нетблоки-хосты / вируустотал
Рек / нетблоки-порты / census_2012
Рек / нетблоки-порты / censysio
Рек / порты-хосты / migrate_ports
Рек / профили-контакты / dev_diver
Рек / профили-контакты / github_users
Рек / профили-профили / namechk
Рек / профили-профили / профилировщик
Рек / профили-профили / twitter_mentioned
Рек / профили-репозитории / github_repos
Рек / репозитории-профили / github_commit
Рек / репозитории-уязвимости / gists_search
Рек / репозитории-уязвимости / github_dorks
отчетность / csv

Количество доступных модулей на выбор может быть огромным,
особенно для нового пользователя, поэтому давайте начнем с базового примера добавления нескольких целевых домены в Recon-NG с помощью команды добавления доменов :

```
[recon-ng] [OSINT]> добавить домены www.uberpeople.net
[recon-ng] [OSINT]> добавить домены www.dualxcrypt.com
```

После добавления записей в базу данных Recon-NG вы можете быстро увидеть, что
вы сохранили в своей локальной базе данных, набрав **show** и нажав клавишу Tab:

```
[recon-ng] [OSINT]> показать
утечки на панели инструментов баннера
репозитории опций
компании домены расположение порты схема
контакты хозяева
модули профили уязвимостей
ключи учетных данных
рабочие области netblocks pushpins
```

Это даст вам список всех типов результатов, которые вы можете «показать». Поскольку у нас есть
просто добавил несколько доменов, давайте покажем их, набрав **show domains** :

[recon-ng] [OSINT]> показать домены
+ ---------- +
| rowid | домен | модуль |
+ ---------- +
| 1 | www.uberpeople.net | user_defined |
| 2 | www.dualxcrypt.com | user_defined |
+ ---------- +
[*] 2 строки возвращены
[повтор] [OSINT]>

Поиск модулей

У вас есть два способа поиска модулей. Ранее описанный метод
набрав **use** и нажав клавишу Tab, вы увидите все доступные модули. Если
вы бы предпочли не просматривать весь список, вы можете ввести **поиск** и
нить. Посмотрим, что доступно для разрешения доменных имен:

[recon-ng] [OSINT]> разрешение поиска
[*] Поиск "решения" ...
Разведка

рекон / хосты-хосты / разрешить
Рек / хосты-хосты / reverse_resolve
Рек / нетблоки-хосты / обратный_ресолв

Перед тем, как начать сканирование цели любого типа, рекомендуется изучить
привычка вводить как можно больше информации о цели. Делать это
может дать интересные результаты в другом (и неожиданном) модуле.
Поскольку мы мало что знаем о DualXCrypt, мы можем найти некоторые интер-
результаты поиска, если мы также ищем название компании в дополнение к домену
имя. Чтобы добавить название компании, мы следуем тому же процессу, используя команду
добавить *описание названия* компании :

[recon-ng] [OSINT]> добавить компании DualXCrypt na

Использование модулей

Поскольку мы знаем домен, мы можем начать наше расследование, выполнив простой
разрешить поиск. Поиск решения - это краткий способ сказать, что мы будем выполнять
поиск разрешения DNS, который вернет серверы имен домена.
Начнем с использования модуля hosts-hosts / resolve :

[recon-ng] [OSINT]> используйте recon / hosts-hosts / resolve

Теперь, когда мы используем модуль, мы можем показать его параметры с помощью show команда options :

```
[Recon-ng] [OSINT] [решение]> показать параметры
Имя Текущее значение Требуется Описание
------ ------------- -------- -----------
ИСТОЧНИК по умолчанию
да источник ввода
```

Этот модуль требует, чтобы мы установили источник нашего ввода (т.е. целевой адрес сканирования). Давайте установим эту опцию на uberpeople.net , используя заданный источник команда:

```
[recon-ng] [OSINT] [resolve]> установить источник uberpeople.net
ИСТОЧНИК => uberpeople.net
```

Теперь, когда мы установили необходимую информацию об источнике, мы можем начать сканирование. набрав run .

```
[повторное сообщение] [OSINT] [решение]> запустить
[*] uberpeople.net => 184.154.76.235
```

Это был довольно простой поиск, который дал нам IP-адрес нашего источника. домен. Теперь давайте попробуем запустить обратное разрешение , начав с исходного IP-адреса. адрес. Это может быть полезно, если у вас есть неправильный IP-адрес и вы хотите посмотрите, связаны ли какие-либо домены с этим IP:

```
[recon-ng] [OSINT] [resolve]> используйте recon / hosts-hosts / reverse_resolve
[recon-ng] [OSINT] [reverse_resolve]> установить ИСТОЧНИК 184.154.76.235
ИСТОЧНИК => 184.154.76.235
[recon-ng] [OSINT] [reverse_resolve]> запустить
[*] [хост] vps.uberpeople.net (184.154.76.235)
-------
РЕЗЮМЕ
-------
[*] Всего найдено 1 (1 новых) хоста.
```

Каждый раз, когда мы находим новую сущность в Recon-NG, она автоматически добавлен в нашу рабочую базу данных. Чтобы убедиться в этом, мы можем увидеть наш новый хост по набрав **show hosts** :

```
[recon-ng] [OSINT] [reverse_resolve]> показать хосты
+ ---------------------------------------------------- ------------------- +
| rowid | хост | ip | регион | страна | широта | долгота | модуль |
+ ---------------------------------------------------- ------------------- +
| 1 | vps.uberpeople.net | 184.154.76.235 | | | | | reverse_resolve |
+ ---------------------------------------------------- ------------------- +
[*] Возвращена 1 строка
```

Информация в нашей базе данных теперь может быть использована для дополнительных проверок.
Посмотрим, сможем ли мы найти новую информацию о нашем хосте с помощью virustotal
модуль.

Модуль virustotal будет искать информацию по любому из доменов.
перечисленные в таблице хостов, в нашем случае vps.uberpeople.net , против VirusTotal
База данных доменов .com . Если будет обнаружена какая-либо новая информация, Recon-
NG автоматически обновит нашу таблицу хостов:

```
[recon-ng] [OSINT]> используйте recon / hosts-hosts / virustotal
[recon-ng] [OSINT] [virustotal]> запустить
--------------
184.154.76.235
--------------
[*] [хост] bedmaybebreakfast.com (184.154.76.235)
[*] [хост] bedmaybebreakfast.uberpeople.net (184.154.76.235)
[*] [хост] beeplam.co (184.154.76.235)
[*] [хост] livewithanyone.com (184.154.76.235)
[*] [хост] mokotoband.uberpeople.net (184.154.76.235)
[*] [хост] ns1.uberpeople.net (184.154.76.235)
[*] [хост] ns2.uberpeople.net (184.154.76.235)
[*] [хост] uberpeople.net (184.154.76.235)
[*] [хост] www.bedmaybebreakfast.com (184.154.76.235)
[*] [хост] www.bedmaybebreakfast.uberpeople.net (184.154.76.235)
[*] [хост] www.mokotoband.uberpeople.net (184.154.76.235)
[*] [хост] www.uberpeople.net (184.154.76.235)
---------------
185.165.169.124
---------------
[*] [хост] dualxcrypt.com (185.165.169.124)
-------
РЕЗЮМЕ
-------
[*] Всего найдено 13 (12 новых) хостов.
```

Это была отличная находка - найдено 12 новых хозяев!

Для полноты , давайте также проверим наши результаты с помощью модуля hackertarget. чтобы узнать, сможем ли мы сделать какие-либо дополнительные выводы:

```
[recon-ng] [OSINT]> используйте recon / domains-hosts / hackertarget
[recon-ng] [OSINT] [hackertarget]> запустить
--------------
DUALXCRYPT.COM
--------------
[*] [хост] dualxcrypt.com (185.165.169.124)
[*] [хост] www.dualxcrypt.com (35.228.80.43)
-------
РЕЗЮМЕ
-------
[*] Всего найдено 10 (2 новых) хоста.
```

Хотя это может показаться бесполезным, на самом деле это было очень важная находка. Присмотревшись к результатам, мы увидим, что наш целевой хост использование разных IP-адресов для URL-адресов с www и без www. Это хорошо напоминание о том, что при вводе информации о хосте всегда следует помнить ввести оба www. *домен* .com и *домен* .com .

С нашей новой информацией об IP, давайте вернемся и перезапустим модуль virustotal. чтобы узнать, изменились ли наши результаты:

```
[recon-ng] [OSINT]> используйте recon / hosts-hosts / virustotal
[recon-ng] [OSINT] [virustotal]> запустить
---------------
185.165.169.124
---------------
[*] [хост] dualxcrypt.com (185.165.169.124)
------------
35.228.80.43
------------
[*] [хост] blog.dualxcrypt.com (35.228.80.43)
[*] [хост] blogs.dualxcrypt.com (35.228.80.43)
[*] [хост] dualxcrypt.com (35.228.80.43)
[*] [хост] liearey1.com (35.228.80.43)
[*] [хост] my-vidar.com (35.228.80.43)
[*] [хост] new.my-vidar.com (35.228.80.43)
[*] [хост] old-vidar.com (35.228.80.43)
[*] [хост] resources.old-vidar.com (35.228.80.43)
[*] [хост] secretdomain912.com (35.228.80.43)
[*] [хост] www.liearey1.com (35.228.80.43)
[*] [хост] www.my-vidar.com (35.228.80.43)
[*] [хост] www.old-vidar.com (35.228.80.43)
[*] [хост] www.secretdomain912.com (35.228.80.43)
```

```
-------
РЕЗЮМЕ
-------
[*] Всего найдено 26 (13 новых) хостов.
```

Посмотри на это! Мы обнаружили довольно много доменных имен, которые связаны между собой.
связан с IP-адресом нашей цели, который мы рассмотрим далее в следующем
глава. А пока давайте продолжим поиск целевой информации, связанной с сетью.

Ищем порты с Shodan

Shodan - отличный ресурс для «ниндзя», потому что вы можете использовать его для поиска открытых портов на цель, не касаясь ее самостоятельно. Это полная скрытность!

Чтобы узнать, какие модули Shodan доступны, введите **поиск shodan,** чтобы вернуться
список доступных модулей:

```
[recon-ng] [OSINT] [hackertarget]> поиск shodan
[*] Поиск "шодан" ...
Разведка
-----
рекон / домены-хосты / shodan_hostname
Рек / хосты-порты / shodan_ip
разведка / местоположения-кнопки / shodan
Рек / нетблоки-хосты / shodan_net
```

Доступны четыре модуля Shodan. Для поиска по IP-адресу мы можем использовать
shodan _ ip модуль:

```
[recon-ng] [OSINT]> используйте recon / hosts-ports / shodan_ip
[recon-ng] [OSINT] [shodan_hostname]> запустить
------------------
WWW.UBERPEOPLE.NET
------------------
[*] Поиск в Shodan API: имя хоста: www.uberpeople.net
--------------
UBERPEOPLE.NET
--------------
[*] Поиск Shodan API для: hostname: uberpeople.net
[*] [порт] 184.154.76.235 (993 / <blank>) - vps.uberpeople.net
[*] [хост] vps.uberpeople.net (184.154.76.235)
--------------
DUALXCRYPT.COM
--------------
[*] Поиск Shodan API для: hostname: dualxcrypt.com
```

```
-------
РЕЗЮМЕ
-------
[*] Всего найдено 1 (0 новых) хостов.
[*] Всего найдено 1 (1 новый) порт.
```

Бинго! Мы нашли новый открытый порт.

Мы даже можем сделать еще один шаг и выполнить поиск по диапазону IP-адресов.

В отличие от предыдущего модуля Shodan, который искал хосты по одному IP адрес, модуль shodan _ net будет искать хосты по всему сетевому блоку (т. е. диапазон IP-адресов).

Более крупные организации обычно владеют целым блоком IP-адресов, поэтому запуск этого типа поиска, вероятно, более полезен, если вы выполняете разведку по организации.

Еще один пример того, почему может быть полезно искать по целому блоку IP-адресов. это посмотреть, какие другие домены могут быть размещены у того же интернет-провайдера. Например, злонамеренные интернет-провайдеры обычно размещают более одного вредоносного сайта, поэтому существует хороший шанс, что сайт, на котором размещены номера украденных кредитных карт, будет окружен на других подобных сайтах. Изучение этих сайтов может дать дополнительный контекст. или ключи к вашему расследованию.

Для этого мы используем модуль shodan _ net , затем устанавливаем источник цели сетевой блок:

```
[recon-ng] [по умолчанию]> загрузить recon / netblocks-hosts / shodan_net
[recon-ng] [default] [shodan_net]> установить ИСТОЧНИК 184.154.76.235/24
ИСТОЧНИК => 184.154.76.235
[recon-ng] [по умолчанию] [shodan_net]> запустить
```

Как вы, наверное, догадались , сканирование всего сетевого блока / 24 вернуло много несвязанных результатов. Я бы не рекомендовал запускать этот тип сканирования если у вас нет на то веской причины. Помните, все, что вы обнаружите, будет автоматически добавляется в вашу базу данных Recon-NG, поэтому случайное сканирование IP-адресов будет загрузите вас бесполезными результатами и увеличьте время сканирования в будущем!

Резюме

В этой главе рассматриваются три основных информационных разведки и открытия. инструменты: SpiderFoot, Intrigue.io и Recon-NG. Инструменты похожи по своей природе, но у каждого есть свой «секретный соус» того, как он может опираться на предыдущие результаты для автоматизации процесса обнаружения и сбора. SpiderFoot и Интрига. io считаются инструментами *автоматического* обнаружения, а Recon-NG - инструмент *ручного* обнаружения.

Преимущество использования ручного подхода к сбору информации заключается в том, что
у вас есть контроль над потоком возвращаемой вам информации. С использованием
полностью автоматизированные инструменты могут быть отличным способом сэкономить время, но они также могут оставить
вам с утомительной задачей просмотреть сотни (или даже тысячи)
нежелательных результатов. Обратной стороной является то, что автоматизированные инструменты также могут сэкономить вам
много времени и добиться неожиданных положительных результатов, глядя
в местах, которые вы бы не рассматривали.

Все сводится к вашим личным предпочтениям и тому, как вы предпочитаете
работа с инструментами и информацией.

Следующие несколько глав посвящены обнаружению и сбору информации из
веб-сайты и веб-приложения.

II

Веб-исследование

В этой части

Глава 6: Сбор информации на веб-сайте
Глава 7: Поиск в каталоге
Глава 8: Шутки с поисковыми машинами
Глава 9: WHOIS
Глава 10: Прозрачность сертификатов и Интернет-архивы
Глава 11: Ирис от DomainTools

В части I этой книги основное внимание уделяется исследованию и изучению сети.
адресов, часть II теперь будет сосредоточена на сборе и извлечении информации и
разведка с веб-сайтов и доменов.

В этой части будут рассмотрены такие темы, как снятие отпечатков пальцев и сбор базовой информации.
на целевых веб-сайтах и переходите к более сложным веб-сценариям, таким как попытка
перебирать папки на веб-сайте, чтобы найти ценную информацию.

В этой части также будут рассмотрены такие темы, как использование расширенных методов поиска.
(dorking), чтобы обнаружить скрытую информацию на веб-сайте и работать над процессом
атрибуции домена с помощью таких инструментов, как WHOIS, журналы прозрачности сертификатов,
Wayback Machine (archive.org) и платформа DomainTools IRIS.

Я буду полностью честен и скажу, что процесс попытки атрибуции

бут домен с владельцем абсолютно отстой. Это может быть жестоко, и все по-новому

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

Правила конфиденциальности GDPR значительно усложняют этот процесс. Даже тем более, если вы охотитесь на злоумышленников - они не упростят процесс для ты. В зависимости от домена или цели атрибуция часто сводится к просто иметь доступ к нужным историческим данным - а эта информация обычно не бесплатно (или дешево). При работе с злоумышленниками поиск истинного владельца домена часто включают в себя поворот через лабиринт поддельных имен, доменов и горелки учетные записи. Но будьте уверены, имея доступ к правильным историческим данным, часто будет повторяется в информации, которую вы можете отслеживать. Чаще всего ответ есть - вы просто должны быть готовы потратить время, чтобы его найти.

121

6

Переходя к следующему этапу сбора разведданных, мы можем начать
посмотрите сами сайты. Снятие отпечатков пальцев с веб-сайта - это первый шаг
в разработке плана игры для дальнейшего расследования. При выполнении атаки
обнаружение поверхности против цели или даже всей организации, вы можете узнать
огромный объем информации, выполнив небольшую пассивную разведку
рождение. Здесь начинается наше путешествие.

Важно отметить, что даже несмотря на то, что многие инструменты мы cover содержат параметры грубой форсировки, они выходят за рамки этой книги. если ты ищите отличный инструмент для веб-разведки, который также выполняет тестирование эксплойтов, я рекомендую вам проверьте Sn1per (https://github.com/1N3/Sn1per **). Мы не будем говорить о Sn1per, потому что большая часть его уникальности заключается в возможностях эксплойтов, которые выходит за рамки этой книги. Sn1per интегрируется с Nikto, WPScan и рядом другие инструменты для выполнения его тестов - определенно стоит проверить, нужен ли вам инструмент который также может проникнуть в цель.**

Построен с

В качестве отправной точки, как правило, неплохо понять, какая технология
ogies используются в веб-приложении вашей цели. Builtwith.com - отличное место для
Начните. BuiltWith - это инструмент для привлечения потенциальных клиентов и продаж, который позволяет

Сбор информации о веб-сайте

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

продавцы для определения технологий, присутствующих на веб-сайте или в веб-приложении.
Как оказалось, он также отлично подходит для первоначальной разведки на веб-сайте или в веб-приложении.
Вы можете выполнять поиск прямо с его веб-сайта или, если хотите,
подробная информация, зарегистрируйтесь для получения ключа API. Бесплатный ключ API позволяет 10
бесплатные поиски в месяц.
Для начала заглянем на мой личный сайт www.vinnytroia.com , показанный на
Рисунок 6.1.
Глядя на подробную вкладку «Технологический профиль», мы можем понять, что
программное обеспечение / технология работает - и всегда работала - на моем сайте. Мы можем
используйте это для построения стратегии атаки, такой как поиск плагина или приложения
уязвимости.

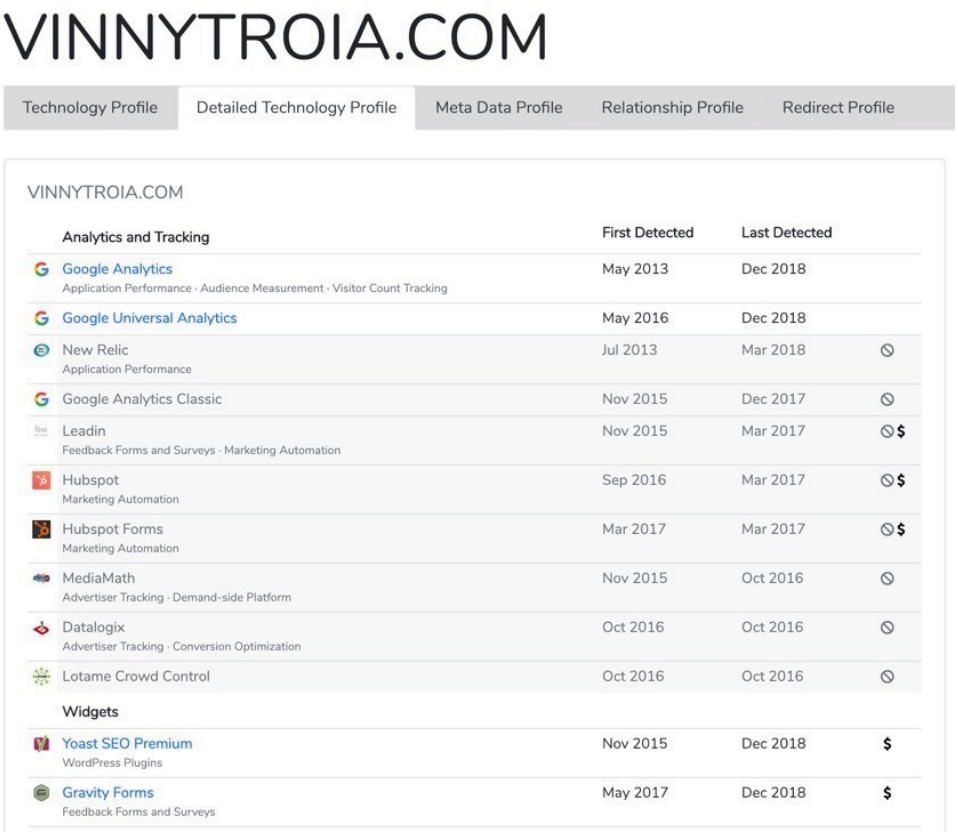


Рисунок 6.1.

Поиск общих сайтов с помощью Google Analytics Tracker

Перейдя на вкладку "Профиль взаимоотношений", мы увидим Google Analytics.
Идентификатор, используемый на этом сайте. Вы часто можете найти похожие веб-сайты или поддомены по
глядя на идентификатор отслеживания GA. Чаще всего люди используют одно и то же
Учетная запись Google для настройки отслеживания аналитики для нескольких веб-сайтов. Анализируя
идентификатор может дать вам подсказку относительно некоторых других их доменов. Отношение
На вкладке «Профиль» (рис. 6.2) отображается история тегов, используемых на сайте.
Если посмотреть на идентификатор GA для моего веб-сайта, рисунок 6.3 показывает, что тот же
Идентификатор также используется для трех других веб-сайтов (которые также принадлежат мне).

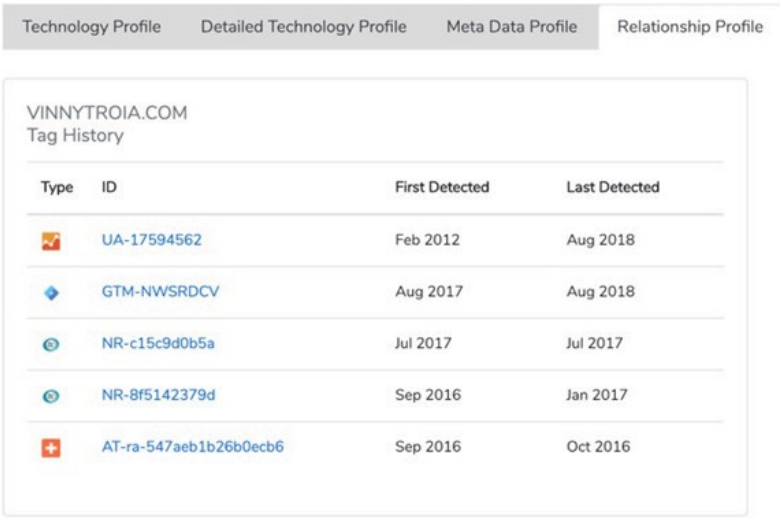


Рисунок 6.2.

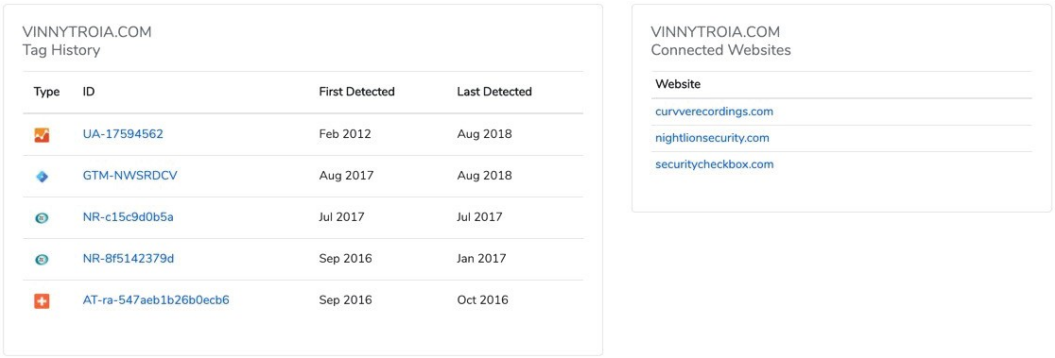


Рисунок 6.3.

История IP и связанные сайты

Еще одна полезная функция BuiltWith - это возможность видеть, какие другие домены в настоящее время используют или исторически использовали один и тот же IP-адрес. если ты ищут конкретного субъекта угрозы или организацию, вполне вероятно, что они повторно использовать одни и те же IP-адреса, особенно если у них есть собственные серверы. Это хороший способ получить представление о некоторых других доменах, которые у них есть.

На рисунке 6.4 показана история IP-адреса, связанного с моим веб-сайтом. www.vinnytroia.com .

Все эти примеры были показаны с использованием бесплатной версии BuiltWith.com . Существует также премиум-версия, больше ориентированная на привлечение потенциальных клиентов к продажам.

Сборщик информации Webapp (WIG)

WIG - это именно то, что написано в названии - это инструмент для сбора информации в Интернете. Программы. Поскольку большинство веб-сайтов / веб-приложений используют системы управления контентом, WIG является хороший способ быстро определить, какую CMS использует цель.

WIG доступен по адресу https://github.com/jekyc/wig **.**

Системы CMS обеспечивают работу подавляющего большинства современных веб-сайтов, поэтому возможность определить, какая CMS используется на целевом веб-сайте, - довольно важный первый шаг в определении направления для остальной части боя.

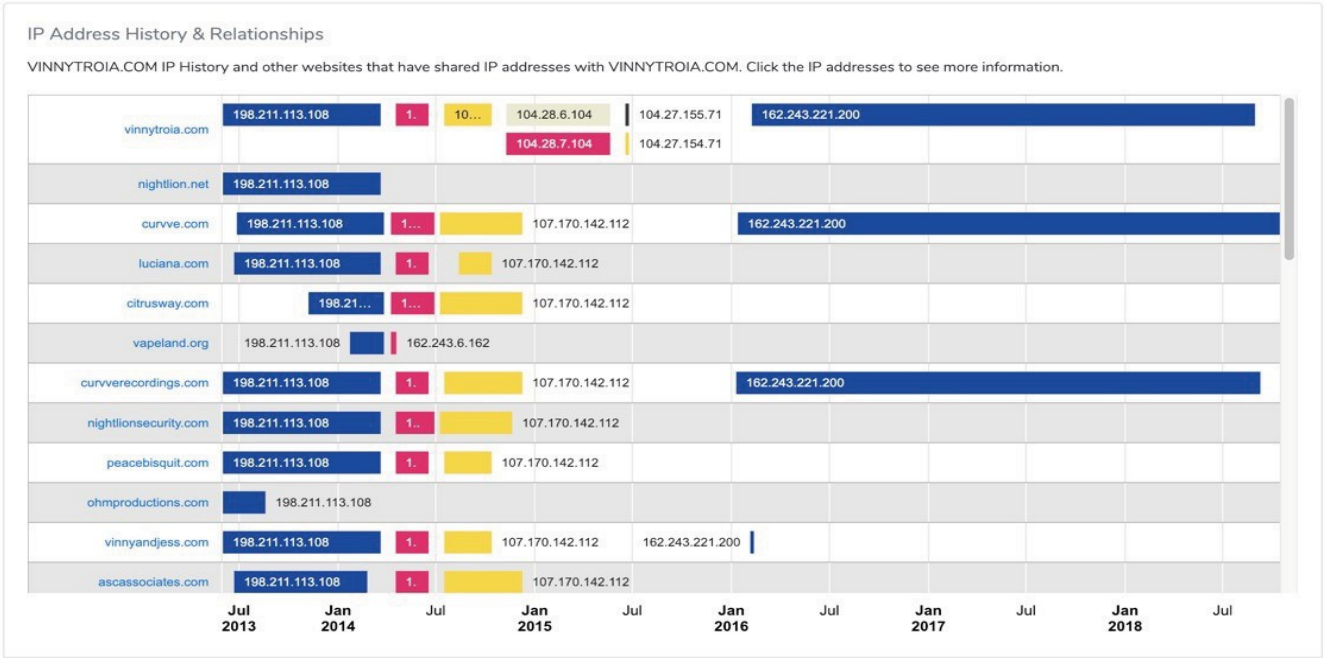


Рисунок 6.4.

Параметры экранопланов включают:

-l: list.txt
-a: не останавливаться после обнаружения первой CMS
-u: указать пользовательский агент
-N: не загружать кешированные ответы
-w: указать выходной файл

Для начала запустим простую экранопленку без дополнительных параметров.
против моего личного сайта vinnytroia.com :

python3 wig.py vinnytroia.com

Когда веб-браузер подключается к веб-сайту, он включает поле агента пользователя **в заголовок HTTP. Это позволяет веб-сайту идентифицировать браузер, который подключается к Это. У каждого браузера есть собственный отдельный пользовательский агент, и это часто может быть способом для веб-брандмауэры приложений для блокировки сканирования. Важная особенность экранопланов, а также любого хорошего сканера - это возможность замаскировать ваш пользовательский агент. WIG также поддерживает возможность сканировать сразу несколько сайтов с помощью параметра** -l **.**

_____ ИНФОРМАЦИЯ О САЙТЕ _____
IP
Заголовок
192.241.180.214 Винни Троя
_____ ВЕРСИЯ _____
Имя
Версии
Тип
WordPress 5.0.2
CMS
Apache
2.4.10 | 2.4.11 | 2.4.12 | 2.4.5 | 2.4.6 Платформа
nginx
2.4.9
Платформа
PHP
7.1.25
Платформа
_____ИНТЕРЕСНО _____
URL
Примечание
Тип
/wp-login.php Страница входа в Wordpress
Интересно
/авторизоваться/
Страница авторизации
Интересно
/readme.html Файл Readme
Интересно
/robots.txt индекс robots.txt
Интересно
/тестовое задание/
Каталог тестов
Интересно
/test.php Тестовый файл
Интересно
_____
Время: 9,2 сек. URL: 748
Отпечатков пальцев: 40401

Мы можем быстро увидеть статус моего личного веб-сайта, который включает URL моей страницы входа в WordPress и что у меня есть папка / test / и test.php файл (о котором я совсем забыл и сейчас буду удалять).

Пока я не запустил это сканирование, я понятия не имел, что файл test.php **все еще существует. я вообще-то даже не помню, как создавал это, что и есть моя точка зрения. Это *именно* те виды оставшихся файлов, которые могут потопить целые корабли. Я надеюсь, что этот пример иллюстрирует важность для организаций и руководителей по информационной безопасности, чтобы убедиться, что тесты проводятся в соответствии с их собственными веб-сайты.**

Я лично работал с организациями, у которых на своих сеть. Люди забывают, меняются рабочие места, меняется администрация. Чем больше организация- Если чем-то станет, тем вероятнее, что все забудется. И когда имеешь дело с серверов, если администраторы не помнят о существовании сервера или не знают, как его искать, существует хороший шанс, что сервер будет исключен из циклов исправлений, обычный пароль администратора сбрасывает и так далее.

Но зачем сканировать один сайт, если мы можем сканировать множество сайтов? Крупные организации могут даже не осознавать, на каких веб-приложениях работают их сеть, так что это отличный способ быстро отследить все в заданном среда.

В нашем следующем примере я загрузил пять разных сайтов в файл с именем target. .txt . (Для тех, кто играет дома, вы можете выбрать любое количество сайтов и поместите их в файл - по одному сайту в строке). Мы будем использовать WIG для сканирования всех из них, а изменение нашего пользовательского агента и вывод всех результатов в файл с именем results.txt .

Следующий код скажет wig.py просканировать все цели в target.txt , сообщить ему для использования определенного пользовательского агента браузера при выполнении сканирования и вывода все в results.txt :

```
python3 wig.py -l targets.txt -u "Mozilla / 5.0 (Android 4.4; Mobile; \
rv: 41.0) Gecko / 41.0 Firefox / 41.0 "-N -w results.txt
```

Выходной файл файла - JSON, поэтому, если вы не захватите исходный выходной текст, вам нужно будет проанализировать JSON в Excel или другом инструменте, который вы используете для прочтите результаты:

```
парик - сборщик информации о веб-приложениях
Сканирование https: //www.pepsi.com ...
_____ ИНФОРМАЦИЯ О САЙТЕ _____
IP
Заголовок
23.63.197.180
Pepsi.com
_____ ВЕРСИЯ _____
Имя
Тип версии
Apache
Платформа
_____ ПОДомены _____
Имя
IP-адрес заголовка страницы
```

https://cms.pepsi.com:443 Pepsi.com 18.222.154.81

_____

Время: 29.0 сек.
URL: 72 Отпечатков пальцев: 40401
Сканирование https: //www.nightlionsecurity.com ...
_____ ИНФОРМАЦИЯ О САЙТЕ _____
IP
Заголовок
192.241.180.214 Фирма кибербезопасности: тестирование на проникновение, риски
Оценки
_____ ВЕРСИЯ _____
Имя
Версии
Тип
WordPress
4.1.2 | 4.1.3 | 4.1.4 | 4.1.5 | 4.2 | 4.2.1 | 4.2.2
nginx
Платформа
PHP
7.1.25
Платформа
_____ИНТЕРЕСНО _____
URL
Примечание
Тип
/readme.html Файл Readme
Интересно
_____ УЯЗВИМОСТИ _____
Затронутый
#Vulns
Ссылка
WordPress 4.2.1 1
http://cvedetails.com/version/184019
WordPress 4.2.2 2
http://cvedetails.com/version/185073
Время: 16,3 сек. URL: 240
Отпечатков пальцев: 40401
Сканирование https: //www.comodo.com ...
_____ ИНФОРМАЦИЯ О САЙТЕ
IP
Заголовок
104.16.21.160
Комодо | Мировой лидер в области кибербезопасности
104.16.20.160
104.16.18.160
104.16.22.160
104.16.19.160
_____ ВЕРСИЯ _____
Имя
Версии
Тип
облачная вспышка
Платформа
_____ ПОДдомены _____
Имя
Заголовок страницы
IP
http://m.comodo.com:80 Мобильный антивирус Comodo 91.199.212.187
https://m.comodo.com:443 Мобильный антивирус
91.199.212.187
http://blog.comodo.com:80 Новости и Интернет Comodo ... 178.255.86.141

https://blog.comodo.com:443 Новости и Интернет Comodo ... 178.255.86.141
_____ ИНТЕРЕСНО _____
URL
Примечание
Тип
/robots.txt
индекс robots.txt
Интересно
/авторизоваться/
Страница авторизации
Интересно
_____
Время: 49,1 сек.
URL: 716
Отпечатков пальцев: 40401
Сканирование http: //whitepacket.com ...
_____ ИНФОРМАЦИЯ О САЙТЕ _____
IP
Заголовок
104.24.119.111 WhitePacket | Дом
104.24.118.111
_____ ВЕРСИЯ _____
Имя
Версии
Тип
WordPress
4.8.8
CMS
облачная вспышка
Платформа
Apache
2.2.11 | 2.2.12 | 2.2.13 | 2.2.14 | 2.2.15 Платформа
2.2.18 | 2.2.19 | 2.2.20 | 2.2.21 | 2.2.22 | 2.2.23
2.2.25 | 2.2.26 | 2.2.27 | 2.2.28 | 2.2.29 | 2.3.0 |
2.3.10 | 2.3.11 | 2.3.12 | 2.3.13 | 2.3.14 | 2.3.15 |
2.3.2 | 2.3.3 | 2.3.4 | 2.3.5 | 2.3.6 | 2.3.7 | 2.3.8
2.3.9 | 2.4.0 | 2.4.1 | 2.4.2 | 2.4.3
PHP
5.4.45-0 + deb7u12
Платформа
_____ ИНТЕРЕСНО _____
URL
Примечание
Тип
/robots.txt индекс robots.txt
Интересно
/readme.html Файл Readme
Интересно
/авторизоваться/
Страница авторизации
Интересно
_____ИНСТРУМЕНТЫ
Имя
Ссылка
Программное обеспечение
wpscan
https://github.com/wpscanteam/wpscan
WordPress
CMSmap
https://github.com/Dionach/CMSmap
WordPress
Время: 189,7 сек. URL: 410
Отпечатков пальцев: 40401

Теперь, когда у нас есть основы WIG, давайте перейдем к более расширенный инструмент отображения и обнаружения CMP.

CMSMap

CMSMap - это сканер Python с открытым исходным кодом, который автоматизирует процесс обнаружения выявление недостатков безопасности в популярных системах управления контентом (CMS). CMSMap похож на WIG в том, что оба инструмента могут отображать и идентифицировать системы CMS, но CMSMap более продвинутый и имеет дополнительные функции.

Вы можете скачать CMSMap здесь: https://github.com/Dionach/CMSmap **.**

Несмотря на то, что CMSMap похож, CMSMap значительно более продвинут, чем WIG и поддерживает ряд различных опций и параметров. В дополнение к просто обнаруживая CMS, используемые веб-приложениями, CMSMap также может перечислять плагины сайта, брутфорс для входа в систему и взлом хэшей паролей. CMSMap также использует официальную Репозиторий ExploitDB, который вы можете скачать здесь: https://github.com/offensive-безопасность / exploitdb.git .

Некоторые из доступных параметров CMSMap включают:

-f W / J / D / M, --force W / J / D / M
принудительное сканирование (W) или пресс, (J) oomla или (D) rupal или (M) oodle
-F, --fullscan
полное сканирование с использованием больших списков плагинов.
-t, --threads
количество потоков (по умолчанию 5)
-a, --agent
установить пользовательский агент
-H, --header
добавить собственный заголовок (например, «Авторизация: базовая»)
-i, --input
сканировать несколько целей, перечисленных в данном файле
-o, --output
сохранить вывод в файл
-E, --noedb
перечислять плагины без поиска эксплойтов
-c, --nocleanurls отключить чистые URL-адреса только для Drupal
-s, --nosslcheck не проверять сертификат сервера
-d, --dictattack выполнить низкоинтенсивную атаку по словарю во время сканирования
Грубая сила:
-u, --usr
имя пользователя или файл имени пользователя
-p, --psw
пароль или файл паролей
-x, --noxmlrpc
брутфорс WordPress без XML-RPC
Постэксплуатация:
-k, --crack
файл хэшей паролей
(Требуется установка hashcat. Только для WordPress и Joomla)
-w, --wordlist файл словаря
Другие:
-v, --verbose
подробный режим (по умолчанию false)
-h, --help
показать это справочное сообщение и выйти
-D, - по умолчанию
запустить CMSmap с параметрами по умолчанию
-U, --update
используйте (C) MSmap, (P) lugins или (PC) для обоих

Сканирование одного сайта

Начнем с базового сканирования веб-сайта с программным обеспечением Drupal CMS. K
найти сайты, на которых запущен Drupal, мы можем перейти на www.builtwith.com и
ищите «Drupal».

Для тестового сканирования я случайным образом выбрал PayChex.com , популярную компанию по расчету заработной платы.

Есть большая вероятность, что у него есть брандмауэр веб-приложений (WAF), и большинство WAF
знать, что нужно заблокировать для приложений сканирования CMS. Способ обойти это - указать
настраиваемый пользовательский агент браузера, который обманом заставит WAF подумать о запросе
исходит из веб-браузера пользователя.

Параметр -a CMSMap позволит нам указать настраиваемый пользовательский агент:

```
корень @ OSINT: / opt / CMSmap: python3 cmsmap.py -s -a \
"Mozilla / 5.0 (Android 4.4; Mobile; rv: 41.0) Gecko / 41.0 Firefox / 41.0" \
https://www.paychex.com
[-] Дата & amp; Время: 01.01.2019 15:48:12
[I] Тем: 5
[-] Цель: https://www.paychex.com (104.17.169.11)
[I] Сервер: cloudflare
[L] X-Generator: Drupal 8 (https://www.drupal.org)
[L] Параметры X-Frame: не применяются
[L] Robots.txt Найдено: https://www.paychex.com/robots.txt
[I] Обнаружение CMS: Drupal
[I] Тема Drupal: обычай
[M] EDB-ID: 29019 "Zikula CMS 1.3.5 - Множественные уязвимости"
[M] EDB-ID: 41564 «Службы модуля Drupal 7.x - удаленное выполнение кода»
[-] Перечисление имен пользователей Drupal через модуль "Просмотры" ...
[-] Перечисление имен пользователей Drupal через "/ user /" ...
[-] Файлы Drupal по умолчанию:
[-] В Drupal скорее всего будет большое количество файлов по умолчанию
[-] Вы хотите их все перечислить? Y
[результаты усечены]
[-] Поиск модулей Drupal ...
[I] содержание
[I] Проверка наличия списка каталогов включена ...
[-] Завершено за: 0:01:22
```

Сканирование нескольких сайтов в пакетном режиме

Подобно тому, что мы делали при использовании WIG, CMSMap будет сканировать несколько сайтов.
включены в целевой файл. Для этого используйте переключатель -i, за которым следует имя
файл с целевыми доменами. В следующем примере будет использоваться targets.txt.

в качестве входного имени файла укажите выходной файл output.txt и используйте настраиваемый пользовательский агент:

```
корень @ OSINT: / opt / CMSmap: python3 cmsmap -i targets.txt -o output.txt \
-a "Mozilla / 5.0 (Android 4.4; мобильный; rv: 41.0) Gecko / 41.0 Firefox / 41.0"
```

Раздражает при сканировании сайтов в пакетном режиме то, что если CMS не обнаружена с одним из сайтов скрипт не перейдет на следующий сайт автоматически. Так что вы необходимо либо принудительно переключить CMS на известный тип, либо просто сканировать сайты по одному. Следующий вывод показывает, что произойдет, если обнаружение сайта не удастся:

```
[-] Дата и время: 01.01.2019 20:45:12
[L] Robots.txt Найдено: http://www.nightlionsecurity.com/robots.txt
[ERROR] Ошибка обнаружения CMS :(
[ОШИБКА] Используйте -f, чтобы заставить CMSmap сканировать (W) orpress, (J) oomla или (D) rupal
```

Обнаружение уязвимостей

Удивительной особенностью CMSMap является его способность обнаруживать уязвимости внутри целевые сайты. Следующий результат был взят из сканирования с точным параметры, показанные в предыдущем коде. Мы должны опустить имена веб-сайтов из-за обнаруженных уязвимостей, но вы можете быстро увидеть насколько мощен этот инструмент:

```
[I] Тем: 5
[-] Цель: http://www.fakebank.com (52.37.170.23)
[M] Веб-сайт не в HTTPS: http://www.fakebank.com
[I] Сервер: Apache / 2.4.10 (Debian)
[L] Параметры X-Frame: не применяются
[I] Строгая транспортная безопасность: не применяется.
[I] X-Content-Security-Policy: не применяется
[I] X-Content-Type-Options: не применяется
[L] Robots.txt Найдено: http://www.fakebank.com/robots.txt
[I] Обнаружение CMS: WordPress
[I] Версия Wordpress: 4.8.8
[M] EDB-ID: 44949 "WordPress Core <4.9.6 - (с аутентификацией)
Удаление произвольного файла "
[I] Тема Wordpress: Avada
[M] EDB-ID: 34511 "Несколько тем WordPress -
'admin-ajax.php? img' Загрузка произвольного файла "
[-] Идентифицированы имена пользователей WordPress:
[M] [опущено]
[M] [опущено]
[M] [опущено]
```

[M] [опущено]
[M] [опущено]
[M] [опущено]
[M] [опущено]
[M] [опущено]
[M] [опущено]
[M] Сервисы XML-RPC включены
[M] **Веб-сайт уязвим для уязвимости XML-RPC Brute-Force**
[I] Автозаполнение выкл. Не найдено: http://www.fakebank.com/wp-login.php
[-] Файлы WordPress по умолчанию:
[I] http://www.fakebank.com/license.txt
[I] http://www.fakebank.com/readme.html
[-] Поиск плагинов Wordpress ...
[I] google-analytics-for-wordpress v6.2.6
[I] revslider
[I] akismet
[M] EDB-ID: 37826 "WordPress 3.4.2 -
Множественные уязвимости раскрытия информации "
[M] EDB-ID: 37902 "Плагин WordPress Akismet -
Множественные уязвимости межсайтового скриптинга "
[I] fusion-core
[I] строитель термоядерного синтеза
[Я кормлю
[M] **EDB-ID: 38624 «Плагин WordPress WP Feed - 'nid' SQL-инъекция»**
[I] Проверка наличия списка каталогов включена ...
Проверка включения списка каталогов ...
[-] Дата и время: 01.01.2019 21:00:26
[-] Завершено за: 0:04:58

Помимо обнаружения уязвимостей, CMSMap может перечислять, какие темы
или плагины, используемые на сайте, и даже брутфорс систем CMS с использованием заданного
файл имени пользователя и пароля. Это невероятно мощный инструмент среднего уровня - он
имеет достаточно функций, но при этом не кажется чрезмерно сложным и продвинутым.
Теперь перейдем к нашему третьему и последнему инструменту, WPScan.

WPScan

Wpscan - это инструмент для сбора информации в виде черного ящика и сканер уязвимостей.
для Wordpress. На мой взгляд, это, безусловно, лучший на рынке и имеет
стать «NMAP» сканирования уязвимостей.

WPScan доступен на https://wpscan.org **.**

Прямо сейчас вы можете подумать: CMSMap уже сканирует WordPress. Почему
Мне нужен другой сканер? Ответ: это зависит от того, насколько глубоко и тщательно
вы хотите получить. CMSMap ориентирован на предоставление аналогичных функций
несколько типов систем CMS, тогда как WPScan предоставляет расширенные функции
ориентирован исключительно на сайты WordPress.
Другие инструменты могут обеспечить хорошую основу для сканирования и поиска в CMS.
системы, которые в конечном итоге могут составлять 80% от того, что вам нужно. Если вы сосредоточены на
сканирование или тестирование сайтов WordPress, это WPScan.
Количество параметров, доступных в WPScan, может быть пугающим, но на самом деле
Ценность использования этого инструмента в том, что вы можете использовать его, чтобы оставаться вне поля зрения
и не быть обнаруженным. Избежать обнаружения может быть непросто, особенно когда
против современных WAF. WPScan позволяет использовать прокси и имеет встроенный
скрытый режим, в котором пользовательские агенты меняются при каждом запросе.
Вот некоторые из наиболее важных параметров, которые мы обсудим:
-v, --verbose
Подробный режим
-o, --output ФАЙЛ
Вывод в ФАЙЛ
-f, --format ФОРМАТ
Вывод результатов в указанном формате
- режим обнаружения РЕЖИМ
По умолчанию: смешанный
Доступные варианты: смешанный, пассивный, агрессивный.
--user-agent, --ua ЗНАЧЕНИЕ
--random-user-agent, --rua
Используйте случайный пользовательский агент для каждого сканирования
--http-auth логин: пароль
-t, --max-thread ЗНАЧЕНИЕ
Максимальное количество используемых потоков
- дроссельная заслонка в миллисекундах
MS ждать между каждым веб-запросом
--request-timeout СЕКУНДЫ Время ожидания запроса в секундах.
--connect-timeout СЕКУНДЫ Тайм-аут соединения в секундах.
--disable-TLS-проверки
Отключает проверку SSL / TLS
--proxy protocol: // IP: порт
--proxy-auth логин: пароль
--cookie-string COOKIE Строка cookie для использования в запросах
--cookie-jar FILE-PATH Файл для чтения и записи файлов cookie.
По умолчанию: /tmp/wpscan/cookie_jar.txt
--сила
Предположим, что WordPress запущен
--wp-content-dir
Вручную установите каталог wp-contents
--wp-plugins-dir
-e, --enumerate [OPTS]
Процесс подсчета - включает
возможность перечислять уязвимые плагины, все плагины, темы,
Timthumbs, резервные копии конфигурации, экспорт баз данных, идентификаторы пользователей, идентификаторы носителей,
и все
-P, --passwords ФАЙЛ-ПУТЬ
Пароли для использования во время атаки
-U, --usernames СПИСОК
Имена пользователей для использования во время

парольная атака
--multicall-max-passwords Максимальное количество паролей к
отправить по запросу с помощью XMLRPC multicall
--password-attack ATAKA Заставить указанную атаку
используется вместо автоматического определения одного
- незаметный
Принудительный скрытый / пассивный режим

По умолчанию WPScan автоматически перечислит все запущенные плагины.
на сайте, проверьте уязвимости этих плагинов и найдите важные
файлы, такие как резервные копии конфигурации.

После запуска инструмента без параметров, кроме URL-адреса моего
личный сайт, мы уже видим значительную разницу в генерации вывода
между WPScan и другими плагинами. Ниже приводится сокращенная версия.
результатов:

```
root @ OSINT: / opt / wpscan: wpscan --url http://www.vinnytroia.com
_____________________________________________________________
__
_______ _____
\ \
/ / __ \ / ____ |
\ \ / \ / / | | __) | (___ ___ __ _ _ __ ®
\ \ / \ / / | | ___ / \ ___ \ / __ | / _` | \
\ / \ / | | ____) | (__ | (_ | | | | |
\ / \ / | _ | | _____ / \ ___ | \ __, _ | _ | | _ |
Сканер безопасности WordPress от команды WPScan
Версия 3.4.2
При поддержке Sucuri - https://sucuri.net
@_WPScan_, @ ethicalhack3r, @erwan_lr, @_FireFart_
_____________________________________________________________
[+] URL: http://www.vinnytroia.com/
[+] Начат: Вт, 3 янв, 07:55:46 2019
Интересные открытия:
[+] http://www.vinnytroia.com/
| Интересные записи:
| - Сервер: nginx
| - X-Powered-By: PHP / 7.1.25, PleskLin.
| - Доступ-Контроль-Разрешить-Происхождение: *
| - Access-Control-Allow-Credentials: true
| - Access-Control-Allow-Headers: Content-Type, Accept.
| - Доступ-Контроль-Разрешить-Методы: GET, POST, OPTIONS, PUT, DELETE
| Найдено по: заголовкам (пассивное обнаружение)
| Уверенность: 100%
[+] http://www.vinnytroia.com/robots.txt
| Найдено: Robots Txt (агрессивное обнаружение)
```

| Уверенность: 100%
[+] http://www.vinnytroia.com/xmlrpc.php
| Обнаружено: Прямой доступ (агрессивное обнаружение)
| Уверенность: 100%
[+] http://www.vinnytroia.com/readme.html
| Обнаружено: Прямой доступ (агрессивное обнаружение)
| Уверенность: 100%
[+] Выявлена версия WordPress 5.0.2 (последняя, выпущена 19.12.2018).
| Обнаружен: Генератором RSS (пассивное обнаружение)
| - http://www.vinnytroia.com/feed/,
[+] Используемая тема WordPress: jupiter-child
| Расположение: http://www.vinnytroia.com/wp-content/themes/jupiter-child/
| URL стиля: http://www.vinnytroia.com/wp-content/themes/
юпитер-ребенок / style.css? ver = 5.0.2
| Название стиля: Дочерняя тема Юпитер
| URI стиля: http://themeforest.net/user/artbees
| Описание: Дочерняя тема для темы Юпитер ...
| Автор: Ваше имя здесь
[+] Перечисление всех плагинов
[+] Проверка версий плагинов
[i] Идентифицированные подключаемые модули:
[+] контактная форма-7
[+] google-analytics-for-wordpress
[+] Google-Analytics-Premium
[+] гравитационные формы
| Расположение: http://www.vinnytroia.com/wp-content/plugins/gravityforms/
| Обнаружен: URL-адреса на главной странице (пассивное обнаружение)
| Версия: 2.4.4 (достоверность 100%)
[+] js_composer
[+] js_composer_theme
| Расположение: http: //www.vinnytroia.com/wp-content/plugins / ...
[+] киви-логотип-карусель
| Расположение: http: //www.vinnytroia.com/wp-content/plugins / ...
[+] мастер-слайдер
| Расположение: http://www.vinnytroia.com/wp-content/plugins/masterslider/

```
[+] rdv-youtube-playlist-video-player
| Расположение: http: //www.vinnytroia.com/wp-content/plugins / ...
[+] tubepress_pro_5_1_5
| Расположение: http: //www.vinnytroia.com/wp-content/plugins / ...
|
| Обнаружен: URL-адреса на главной странице (пассивное обнаружение)
|
| Версия не может быть определена.
[+] wordpress-seo
| Расположение: http://www.vinnytroia.com/wp-content/plugins/wordpress-seo/
| Последняя версия: 9.3 (актуальная)
| Последнее обновление: 2018-12-18T09: 25: 00.000Z
[+] wp-super-cache
| Расположение: http: //www.vinnytroia.com/wp-content/plugins / ...
| Последняя версия: 1.6.4 (актуальная)
| Последнее обновление: 2018-12-20T09: 36: 00.000Z
[+] Перечисление резервных копий конфигурации
Проверка резервных копий конфигурации - Время: 00:00:03
[i] Резервные копии конфигурации не найдены.
[+] Завершен: Вт, 3 янв, 07:55:59 2019
[+] Выполнено запросов: 92
[+] Кешированных запросов: 5
[+] Отправлено данных: 18,989 КБ
[+] Получено данных: 2,482 МБ
[+] Используемая память: 67,148 МБ
[+] Прошедшее время: 00:00:13
```

Результаты моего сайта довольно скучные. Уязвимости не обнаружено и никаких реальных действий, которые можно предпринять на основании этих результатов, кроме попытки брутфорс мой логин / пароль. С точки зрения OSINT нет ничего интересно из этих результатов (к моей чести, я постоянно обновляю сайт и сервер пропатчен специально по этой причине).

А теперь попробуем что-нибудь посложнее.

Работа с WAF / WordPress не обнаружена

Если мы запустим то же сканирование веб-сайта моей компании, www.NightLionSecurity .com , получаем другое сообщение:

```
root @ OSINT: / opt / wpscan: wpscan --url http://www.nightlionsecurity.com
Сканирование прервано: удаленный веб-сайт работает, но не выглядит
работать под управлением WordPress.
```

Чаще всего вы можете сказать, что на сайте работает WordPress, просто перейдя в папку / wp-admin / - например, http://www.nightlionsecurity.com/wp-admin .

Если вы уверены, что на сайте работает WordPress, и вы все еще получаете это сообщение, то на сайте есть WAF, который необходимо обойти. Это случилось-ручки для веб-сайта NightLion. Есть несколько вещей, которые мы можем сделать чтобы обойти это сообщение об ошибке.

Первое, что мы можем попробовать, - это изменить наши параметры, чтобы использовать случайного пользователя. агент. Мы также можем использовать переключатель --force, потому что можем вручную проверить, что WordPress работает в домене:

```
root @ OSINT: / opt / wpscan: wpscan --url http://www.nightlionsecurity.com \
—-Random-user-agent --force
[+] URL: http://www.nightlionsecurity.com/
[+] Действующий URL: https://www.nightlionsecurity.com/
[+] Начат: Вт, 3 янв, 02:35:16 2019
Интересные открытия:
[+] https://www.nightlionsecurity.com/
| Интересные записи:
| - Сервер: nginx
| - X-Powered-By: PHP / 7.1.25, PleskLin.
| - Access-Control-Allow-Origin: cdn.nightlionsecurity.com.
| Найдено по: заголовкам (пассивное обнаружение)
| Уверенность: 100%
[i] Не удалось определить версию WordPress.
```

Хотя эти результаты невелики, они определенно являются шагом в правильном направлении. направление. В идеальной ситуации мы бы увидели результаты, которые включают в себя такие вещи, как перечисление имени пользователя и плагина, проверка оставшихся файлов и уязвимости сайта способности.

Сделав еще один шаг, давайте посмотрим, сможем ли мы найти какие-либо уязвимые плагины или имена пользователей. На этом этапе я обычно использую комбинацию параметров для попытаться добиться результатов.

Параметр --stealthy объединяет несколько различных параметров для создания сканирование с наименьшим шумом. Скрытый режим включает случайный пользовательский агент и также использует менее агрессивный подход к обнаружению плагинов, увеличивая время между зондами.

Следующим шагом будет использование переключателя --proxy для отправки каждого запроса через прокси (который будет использовать разные IP-адреса для каждого запроса).

Наконец, мы можем гарантировать, что имена пользователей сайта перечислены с помощью - перечислить u . Обычно это включается в сканирование по умолчанию, но пропускается, когда сканирование в скрытом режиме.

Возможность ротации IP-адресов не поддерживается WPScan. Пожалуйста не ожидайте, что эта функция будет доступна сразу после установки этого (или любого другого) инструмента. Я использую *платный* прокси-сервис под названием Storm Proxies, который автоматически меняет мои IP-адреса при каждом запросе.

Поток работает так:

■ WPScan позволяет мне использовать IP-адрес →

■ Storm Proxies предоставляет мне IP-адрес, который я использую в качестве своего прокси-сервера. адрес →

■ Для каждого запроса к этому IP-адресу Storm Proxies передает его через другой ент адрес.

Собирая все вместе, наш запрос выглядит так:

```
root @ OSINT: / opt / wpscan: wpscan --url http://www.nightlionsecurity.com \
—-Stealthy --force -proxy 'socks5: //127.0.0.1: 9050' - перечислить u
```

Новое сканирование привело к следующему результату:

```
[+] URL: https://www.nightlionsecurity.com/
[+] Начат: Вт, 3 янв, 04:30:13 2019
Интересные открытия:
[+] https://www.nightlionsecurity.com/
| Интересные записи:
| - Сервер: nginx
| - X-Powered-By: PHP / 7.1.25, PleskLin.
| - Access-Control-Allow-Origin: cdn.nightlionsecurity.com.
| Найдено по: заголовкам (пассивное обнаружение)
| Уверенность: 100%
[i] Идентифицированные пользователи:
[+] Винни
| Обнаружен: Генератором RSS (пассивное обнаружение)
| Подтверждено: Генератором RSS (Агрессивное обнаружение)
[+] BlogAdmin
```

| Обнаружен: Генератором RSS (пассивное обнаружение)
| Подтверждено: Генератором RSS (Агрессивное обнаружение)
[+] Редактор
| Обнаружен: Генератором RSS (пассивное обнаружение)
| Подтверждено: Генератором RSS (Агрессивное обнаружение)
[+] Выполнено запросов: 16
[+] Кешированных запросов: 63
[+] Отправлено данных: 3,992 КБ
[+] Получено данных: 1,437 МБ
[i] Обнаружены резервные копии конфигурации:
[+] http://www.nightlionsecurity.com.com/wp-config.bak
| Обнаружен: прямым доступом (агрессивное обнаружение)

Эти результаты намного лучше - мы явно добиваемся прогресса. Мы были
теперь можно использовать различные параметры для получения списка имен пользователей сайта (которые
мы не смогли сделать в первых нескольких примерах).

Мы также нашли резервную копию конфигурации, что является огромной находкой! *Wp-config*
файл резервной копии всегда должен содержать имя пользователя и пароль базы данных, поэтому, если вы найдете
файл резервной копии, считайте это джекпотом . Известно, что администраторы оставляют резервные копии
валяется, так что обязательно проверьте это.

Я добавил файл резервной копии специально, чтобы это сканирование обнаружило его. Нет
там больше (и никогда не было).

Следующим шагом обычно будет выявление и поиск уязвимостей в
плагины WordPress. После этого я бы попытался грубо форсировать
войдите, используя общий список паролей.

Чтобы найти уязвимые плагины, мы можем повторно ввести ту же команду, что и раньше.
но без параметра --stealthy (в этом примере, используя вращающийся
прокси-сервис - вот что позволяет нам обмануть мой WAF). Чтобы перечислить плагины, мы
также можно использовать --enumerate ap или --enumerate all для перечисления плагинов
в качестве имен пользователей, тем, резервных копий баз данных и всего остального.

На моем сайте работает не так много плагинов, поэтому для последней демонстрации
давайте запустим сканирование на ManageWP.com (система управления WordPress для
админы):

root @ OSINT: / opt / wpscan: wpscan --url http://www.managewp.com
--force --random-user-agent - перечислить все

```
_______________________________________________________________
        __
 _______ _____
 \ \
  / / __ \ / ____ |
  \ \ / \ / / | | __) | (___ ___ __ _ _ __ ®
   \ \ / \ / / | | ___ / \ ___ \ / __ | / _` | '_ \
    \ / \ / | | ____) | (__ | (_ | | | | |
     \ / \ / | _ | | _____ / \ ___ | \ __, _ | _ | | _ |
Сканер безопасности WordPress от команды WPScan
Версия 3.4.2
При поддержке Sucuri - https://sucuri.net
@_WPScan_, @ ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________
[+] URL: https://managewp.com/
[+] Начат: Вт, 3 янв, 04:45:21 2019
Интересные открытия:
[+] https://managewp.com/
| Интересная запись: Сервер: nginx
| Найдено по: заголовкам (пассивное обнаружение)
| Уверенность: 100%
[+] https://managewp.com/robots.txt
| Найдено: Robots Txt (агрессивное обнаружение)
| Уверенность: 100%
[+] Обнаружена версия WordPress 4.9.8 (небезопасная, выпущена 02.08.2018)
| [!] Выявлено 7 уязвимостей:
|
| [!] Название: [Исключено из публикации]
| Исправлено в: 5.0.1
| Ссылки: |
| [!] Название: [Исключено из публикации]
| Исправлено в: 5.0.1
| Использованная литература:
[Результаты усечены]
[i] Идентифицированные подключаемые модули:
[+] контактная форма-7
|
| Обнаружен: URL-адреса на главной странице (пассивное обнаружение)
| [!] Обнаружена X уязвимость:
[+] mailchimp-for-wp
```

```
[+] wordpress-seo
[!] Версия устарела, последняя версия 9.3
| Обнаружен: комментарием (пассивное обнаружение)
|
| [!] Обнаружена X уязвимость:
[Результаты усечены]
[i] Резервные копии конфигурации не найдены.
```

Результаты видны сразу: мы выявили несколько уязвимых
Плагины WordPress. Теперь, когда мы определили уязвимости на цели
сайт, следующий шаг будет зависеть от объема вашего участия.

Фактический список уязвимостей был удален по юридическим причинам.

Если вы авторизованы, чтобы попытаться взломать сайт, вы можете посмотреть exploitdb, чтобы
попробуйте найти работающий эксплойт или попробуйте такие инструменты, как Sn1per (обсуждалось в начале
этой главы). Во многих случаях достаточно просто сообщить подробности владельцу сайта.
будет достаточно, поэтому убедитесь, что у вас есть соответствующие разрешения, прежде чем
фактически пересекая линию сбора информации и взламывая что-либо.

Резюме

В этой главе были рассмотрены некоторые инструменты, которые можно использовать для отпечатков пальцев цели.
веб-сайт и определите, какие технологии используются. Поскольку большинство всех
современные веб-сайты работают в приложении CMS (система управления контентом),
возможность найти информацию о типе используемой CMS и существовании
любые оставшиеся файлы или уязвимости на платформе имеют решающее значение. Устаревшие файлы
может привести к обнаружению серьезной утечки информации или даже атрибуции
злоумышленник.

Теперь, когда мы понимаем, как правильно определять технологии, используемые на
Наша цель, следующая глава будет посвящена искусству поиска сокровищ в каталогах.

143

7

В поисках информации о веб-сайте вам неизбежно потребуется
ищите спрятанные (то есть забытые) сокровища. Лучший способ сделать это - поискать
случайные каталоги. Если вы еще не пробовали это сделать, вы будете поражены тем, как
много информации, о которой люди просто забывают: веб-оболочки, страницы PhPMyAdmin,
папки с просмотром каталогов и / или полными разрешениями на чтение / запись, частные
файлы и многое другое. Есть несколько способов добиться этого. Один
брутфорс для поиска рабочих каталогов, а другой анализирует
сканировать данные. В этой главе мы рассмотрим и то, и другое.

Dirhunt

Dirhunt - это тип веб-краулера, предназначенный для поиска и анализа каталогов.
и папки в веб-приложении. Dirhunt на самом деле не скребок, а
не использовать брутфорс для поиска папок. Вместо этого Дирхант проверяет ряд источников.
чтобы найти интересные файлы или папки, в том числе Google и VirusTotal. Дирхант
также предназначен для обнаружения ложных ошибок 404, чтобы свести к минимуму количество ложных срабатываний.
в ваших результатах.

Вы можете загрузить Dirhunt по адресу https://github.com/Nekmo/dirhunt **.**

Справочник Охота

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

Параметры Dirhunt включают:

-t, --threads ЦЕЛОЕ
Количество используемых потоков
-x, --exclude-flags ТЕКСТ
Исключить результаты с этими флагами
-i, --include-flags ТЕКСТ
Включайте только результаты с этими флагами
-e, --interesting-extensions ТЕКСТ Искать файлы с расширением
следующие расширения
-f, --interesting-files ТЕКСТ Файлы с этими именами
интересно
--stdout-flags ТЕКСТ
Вернуть только в stdout URL
из этих
--progress-enabled / --progress-disabled
--timeout ЦЕЛОЕ
--max-depth ЦЕЛОЕ
Максимальное количество ссылок для перехода
--not-follow-subdomains
Поддомены будут проигнорированы
--exclude-sources ТЕКСТ
Исключить исходные движки: роботы,
virustotal, google
-p, --proxies ТЕКСТ
Установите один или несколько прокси на чередование
-d, --delay FLOAT
Задержка между запросами
--not-allow-redirects
Редиректоры не будут отслеживаться
--limit ЦЕЛОЕ
Максимальное количество обработанных страниц
искать

Давайте протестируем возможности Dirhunt без параметров на примере Florida Alcohol.
и веб-сайт Ассоциации злоупотребления наркотиками (FADAA):

корень @ INTEL: / opt / dirhunt: dirhunt https://www.fadaa.org/
[301] https://fadaa.org/ (Перенаправление)
Перенаправить на: https://www.fadaa.org/?
[403] http://fadaa.org/global_inc/ (Общий)
Найден индексный файл: index.php
[301] http://fadaa.org/ (Перенаправление)
Перенаправить на: https://www.fadaa.org/?
[301] http://fadaa.org/global_engine/ (Перенаправление)
Перенаправить на: https://www.fadaa.org/global_engine/Default.asp?
[301] http://www.fadaa.org/global_inc/%2A.css (Перенаправление)
Перенаправить на: https://www.fadaa.org/404.aspx?404;
http://www.fadaa.org:80/global_inc/*.css
[301] http://www.fadaa.org/global_inc/%2A.js (Перенаправление)
Перенаправить на: https://www.fadaa.org/404.aspx?404;
http://www.fadaa.org:80/global_inc/*.js
[301] http://www.fadaa.org/ (Перенаправление)
Перенаправить на: https://www.fadaa.org/default.aspx
[403] http://www.fadaa.org/global_inc/ (Общий)
Найден индексный файл: index.php
[200] https://www.fadaa.org/ (Общий)
[404] https://www.fadaa.org/404.aspx (не найдено)
[200] https://www.fadaa.org/default.aspx (общий)
[302] https://www.fadaa.org/global_engine/Default.asp (Перенаправление)

Перенаправить на: https://www.fadaa.org/global_engine/Default.asp
[302] http://www.fadaa.org/global_engine/ (Перенаправление)
Перенаправить на: http://www.fadaa.org/global_engine/
[302] https://www.fadaa.org/global_engine/ (Перенаправление)
Перенаправить на: https://www.fadaa.org/global_engine/
[302] https://www.fadaa.org/page/SAMHSA_Treatment (Перенаправление)
Перенаправить на: https://findtreatment.samhsa.gov/
[200] https://www.fadaa.org/staff/ (Общий)
Найден индексный файл: index.php
[200] https://www.fadaa.org/news/ (Общий)
Найден индексный файл: index.php
[404] https://www.fadaa.org/page/ (не найдено)
Найден индексный файл: index.php
[200] https://www.fadaa.org/page/resource_links (общий)
Найден индексный файл: index.php
[200] https://www.fadaa.org/networking/ (общий)
[200] https://www.fadaa.org/page/AOE2017 (общий)
Найден индексный файл: index.php
[200] https://www.fadaa.org/page/Membership (общий)
Найден индексный файл: index.php
[200] https://www.fadaa.org/search/ (Общий)
[302] https://www.fadaa.org/general/ (Перенаправление)
Перенаправить на: https://www.fadaa.org/general/
[200] **https://www.fadaa.org/login.aspx (общий)**
[302] https://www.fadaa.org/general/register_start.asp (Перенаправление)
Перенаправить на: https://www.fadaa.org/general/register_start.asp
[404] https://www.fadaa.org/graphics/ (не найдено) (FAKE 404)
Найден индексный файл: index.php
[403] **https://www.fadaa.org/global_inc/** (общий)
[403] https://www.fadaa.org/global_inc/site_templates/js/ (общий)
[403] https://www.training.fadaa.org/css/ (Общий)
[200] https://www.fadaa.org/page/Healthcare_Division (общий)
Найден индексный файл: index.php
[200] https://www.fadaa.org/page/BusinessDivision (общий)
Найден индексный файл: index.php
[403] https://www.fadaa.org/global_inc/site_templates/ (общий)
[200] https://www.fadaa.org/page/Boards (общий)
Найден индексный файл: index.php
[302] https://www.fadaa.org/page/Become_a_Member (Перенаправление)
Перенаправить на: http://fadaa.site-ym.com/?page=Login
[200] https://www.fadaa.org/page/Housing_Recovery (общий)
Найден индексный файл: index.php
@ Завершено через 11 секунд
Не обнаружено интересных файлов

_
\ _ (") _ /

В зависимости от ваших результатов, с помощью этого типа сканирования теперь вы можете повернуть стратегия сосредоточиться на своих открытиях. Весьма вероятно, что вы откажетесь охватывают систему управления контентом (CMS) из-за того, насколько они распространены в работе большинства современных веб-сайтов. Открытие CMS неизбежно
)

это может привести к обнаружению уязвимостей в этой системе, которые могут
превращается в быструю победу для вашего участия.
Параметры Dirhunt можно дополнительно настроить, чтобы сосредоточиться (или не фокусироваться) на
определенные файлы, типы файлов, субдомены и т. д. Ищем сжатый файл
расширения (например, .zip , .rar или .gz) с помощью переключателя -e, как показано ниже.
Команда lowing часто может предоставить вам доступ к устаревшим файлам, которые должны иметь
было удалено:

```
dirhunt http://domain.com -e php, zip, sh
```

Также велика вероятность того, что вы обнаружите интересные файлы, например, оставшиеся
файлы конфигурации, резервные копии и файлы журналов, которые могли быть забыты. Спец-
в частности, ищите файлы, используйте переключатель -f , например:

```
dirhunt http://domain.com -f журнал_доступа, журнал_ошибок
```

При поиске файлов вы также можете указать список файлов для поиска из
файл словаря. Чтобы указать файл словаря, используйте следующее:

```
dirhunt http://domain.com -f /var/files/dictfile.txt
```

Wfuzz

Wfuzz существует уже очень давно и, вероятно, является одним из лучших
доступны хорошо известные инструменты тестирования веб-приложений. Wfuzz, по сути,
инструмент для брутфорса и, вероятно, один из лучших инструментов для брутфорсинга в Интернете.
Приложения.
Фаззинг - это процесс использования автоматизированных инструментов для поиска ошибок программного обеспечения.
отправляя искаженные данные в приложение. В этом случае мы не отправляем
Wfuzz (веб-фазз) искаженные данные. Мы используем его для отправки правильных слов и
фразы на веб-сервер для проверки наличия скрытых или личных файлов и
папки. Wfuzz доступен для загрузки по адресу https://github.com/xmendez/wfuzz .
Параметры для Wfuzz включают:

```
Параметры:
-час
: Эта помощь
--помощь
: Расширенная справка
--версия
: Детали версии Wfuzz
-e <тип>
: кодеры / полезные нагрузки / итераторы /
принтеры / скрипты
```

-c
: Вывод с цветами
-v
: Подробная информация.
- взаимодействовать
: Это позволяет вам взаимодействовать с
программа.
-p адрес
: Использовать прокси в формате ip: port: type.
Где тип может быть SOCKS4, SOCKS5 или
HTTP, если не указан.
-t N
: Укажите количество одновременных
соединения (10 по умолчанию)
-s N
: Укажите время задержки между запросами
(0 по умолчанию)
-R глубина
: Глубина обнаружения рекурсивного пути
-L, - следовать
: Следуйте перенаправлениям HTTP
-u URL
: Укажите URL-адрес для запроса.
-z полезная нагрузка
: Укажите полезную нагрузку - тип, параметры,
кодировщик.
-w список слов
: Укажите файл списка слов (псевдоним для
-z файл, список слов).
-V alltype
: Брутфорс всех параметров
(allvars и allpost).
-X метод
: Укажите метод HTTP для
запрос
-b cookie
: Укажите cookie для запросов
-d постданные
: Использовать данные публикации
(например: "id = FUZZ & catalog = 1")
-H заголовок
: Использовать заголовок
(например: "Cookie: id = 1312321 & user = FUZZ")
--basic / ntlm / digest auth: в формате «пользователь: пароль» или «FUZZ: FUZZ»
или "домен \ FUZ2Z: FUZZ"

Wfuzz содержит почти бесконечное количество комбинаций, которые вы можете использовать «размыть» веб-приложение. Мы можем сделать то же самое при поиске веб-директо-истории на целевом домене.

Wfuzz работает, беря ваш целевой URL и список слов и пытается вставить каждое слово в вашем словарном списке, где бы и когда бы вы ни указали «пушистость» в ваш URL.

Начнем с простого примера попытки перебора папок из основного путь к домену, используя список слов. В нашем примере словаря мы будем использовать big.txt wordlist в репозитории SecLists, обсуждаемый в главе 2. Мы также собираюсь использовать тег --hc, чтобы скрыть все ответы 404:

корень @ OSINT: wfuzz -c -z файл, / opt / SecLists / Discovery / Web-Content / big.txt --hc 404 http://www.biz-up.at/FUZZ

Если на веб-сайте настроено автоматическое перенаправление URL-адресов, вы будете перенаправлены со списком URL-адресов и 302 кодами ответа. Wfuzz думает, что каждая папка активный. Если вы начнете видеть кучу кодов ответов 301 или 302, то на сайте может быть настраиваемая страница 404 или настройка перенаправления ошибок на каждой странице. В любом случае, чтобы скрыть любой, кроме положительного ответа 202, используйте следующий код: --hc 404,301,302 **.**

Ваш результат будет выглядеть примерно так:

```
==================================================== ================
Слово строк ответа ID
Chars
Полезная нагрузка
==================================================== ================
000010: C = 403 9 л
24 Вт 216 Ch ".bashrc"
000015: C = 403 9 л
24 Вт 218 канал ".htaccess"
000016: C = 403 9 л
24 Вт 218 каналов ".htpasswd"
000026: C = 200551 L 3234 W 66939 Ch "0"
000919: C = 403 9 л
24 Вт 218 каналов "Изменения"
000965: C = 403 9 л
24 Вт 216 канал «ЛИЦЕНЗИЯ»
000974: C = 404 352 L 2504 W 53514 Ch "MANIFEST.MF"
001012: C = 403 9 л
24 Вт 215 каналов "README"
001015: C = 403 9 л
24 Вт 215 канал "Ридми"
001053: C = 403 9 л
24 Вт 213 Ch "TODO"
001058: C = 403 9 л
24 Вт 218 Ch "Thumbs.db"
001414: C = 403 9 л
24 Вт 213 каналов "_src"
001631: C = 404 352 L 2504 W 53514 Канал "доступ.1"
001629: C = 404 352 L 2504 W 53514 Канал "журнал доступа.1"
001634: C = 404 352 L 2504 W 53514 Канал "access_log.1"
001058: C = 403 9 л
24 Вт 218 Ch "typo3temp"
```

Код 200 показывает успешную страницу. Если URL-адрес интересен, возможно, стоит выезд. С другой стороны, ошибки кода 403 почти *всегда* интересны.

потому что теперь мы можем сказать, что файл существует; у нас просто нет к нему доступа. Как мы прогресс в нашем расследовании, это может дать нам представление о том, какой тип другие файлы, которые нужно искать, или он может предоставить нам вектор атаки позже, если мы могут получить доступ.

На основе того, что обнаружено, мы также можем адаптировать нашу стратегию фаззинга два или три уровня в определенном направлении.

Например, последняя строка нашего сканирования обнаружила папку «typo3temp» . Typo3 - популярная, но не столь известная CMS. Хотя у нас нет доступа в папку typo3temp , мы знаем, что она там, и велика вероятность, что доступны файлы в этой папке.

Иногда полезно просто взглянуть на исходный код веб-сайта. Ты бы удивляйтесь тому, сколько может быть оставшегося текста или комментариев. В этом случае, беглый взгляд на код показывает, что папка typo3temp все еще используется и следует изучить дальше:

<link rel = "stylesheet" type = "text / css" href = "https://www.biz-up.at/
typo3temp / assets / сжатый / d42b6e1bdf
-bf2d65d4a223e2f396e31c35d56d6ffc.css ">
<link rel = "stylesheet" type = "text / css" href = "https://www.biz-up.at/
typo3temp / assets / сжатый / flexslider
-a747cd663059c9546a6391e1d6f1a9e0.css ">

Чтобы использовать Wfuzz для исследования другого пути на веб-сайте, мы можем выполнить следующая команда:

wfuzz -c -z файл, / opt / SecLists / Discovery / Web-Content / big.txt
--hc 404 301 302 http://www.biz-up.at/typo3temp/FUZZ

Ошибки совершают даже самые осторожные киберпреступники. Wfuzz поставляется с двумя задирами словари. Когда я запускаю Wfuzz, я сначала использую Wfuzz для имен каталогов, а затем запускаю второй фазз для PHP, .zip, .tgz, .txt, .sql. Файл big.txt **, поставляемый с Wfuzz, найдет много интересного.**
Я регулярно нахожу такие файлы, как 1.sql **или** Abc.sql **. Люди спешат делать резервные копии файлов для быстрого создания имени файла он назовет что-нибудь короткое, и Wfuzz просто скопирует через и обнаружить их. Так я нашел исходные коды для целых даркнет-сайтов. я также ищите "c99", это обычная веб-оболочка. Я считаю, что люди будут использовать это вместо установки чего-то вроде Cpanel или Plesk.**

Фотон

Photon - это движок OSINT для сканирования и извлечения данных. Это очень сложно Усовершенствованный и отличный инструмент для использования, когда вы собираетесь стрелять из дробовика. Согласно странице Photon на GitHub, это «невероятно быстрый сканер, разработанный для OSINT. " Photon доступен для загрузки по адресу https://github.com/s0md3v/Photon **.**
Использование Photon включает поиск креативных / труднодоступных страниц на сайте, внешние ссылки и битые ссылки; создание клона сайта; и определение изменения на сайте с течением времени.
Доступны буквально сотни поисковых роботов, многие из них столь же мощные, сколь и дорогие. Фотон прекрасен, потому что он работает, и он с открытым исходным кодом.

Для OSINT Photon может легко извлекать различные целевые точки с веб-сайта.
Это может включать информацию о сотрудниках (например, имена и адреса электронной почты),
контактная информация, связанные сайты социальных сетей, документы и другие потенциально скрытые
информация о компании, такая как секретные ключи и информация о корзине.
Во время обычного сканирования веб-сайта Photon может извлекать следующие типы
Информация:

- URL-адреса (входящие и выходящие за рамки)
- URL-адреса на основе параметров
- Электронная почта, учетные записи в социальных сетях, корзины
- Файлы (pdf, doc, xls, csv и т. Д.)
- Секретные ключи (API, аутентификация и т. Д.)
- Строки, соответствующие пользовательским шаблонам регулярных выражений.
- Данные, относящиеся к субдоменам и DNS
- Wayback / Интернет-архивы

Photon также имеет встроенные плагины для получения контента из сторонних сервисов.
например Wayback Machine (Интернет-архив) и DNS Dumpster (для связанных с DNS
Информация). Также есть параметр –clone, который позволяет сохранить локальный
копия всего сайта.
Параметры для Photon включают:

-u --url
корневой URL
-l --level
уровни для ползания
-t --threads
количество потоков
-d --delay
задержка между запросами
-c --cookie
печенье
-r --regex
шаблон регулярного выражения
-s --seeds
дополнительные исходные URL
-e --export
экспорт форматированного результата
-o --output
указать выходной каталог
-v --verbose
подробный вывод
--клон
сделать копию сайта
- ключи
извлекать секретные ключи
--исключать
исключить URL-адреса по регулярному выражению
--stdout
распечатать переменную в стандартный вывод
- тайм-аут
Тайм-аут HTTP-запросов
--ниндзя
режим ниндзя
--Обновить
обновить фотон
--dns
перечислить поддомены и данные DNS
--only-urls
только извлекать URL
--путь назад
Используйте URL-адреса с archive.org в качестве семян
--пользователь-агент
укажите агент (ы) пользователя

Сканирование веб-сайта

Чтобы выполнить простое сканирование веб-сайта, используйте переключатель -u, за которым следует URL:

```
python photon.py -u "http://www.vinnytroia.com"
```

На рисунке 7.1 показан результат запуска Photon на моем личном веб-сайте.

Результаты, сохраненные этой командой, включают список обнаруженных URL-адресов из целевой веб-сайт.

На этом этапе параметр --clone примет эти URL-адреса и выполнит полное очистить сайт и сохранить каждую очищенную страницу на диск:

```
python photon.py -u "http://www.vinnytroia.com" --clone
```

Для более сложных сайтов, таких как сайты крупных корпораций, блоги и сообщения досок следует изменить глубину сканирования и количество одновременных новые темы. Переключатель -t позволяет указывать потоки, а переключатель -d определяет глубину (то есть, сколько уровней вложенных страниц будет отслеживаться):

```
python photon.py -u "http://www.site.com" -t 5 -d 5
```

Еще одна невероятно полезная функция Photon - это возможность автоматически spider DNS и связанные с ним поддомены с помощью переключателя --dns . Это даст вам возможность зафиксировать макет сайта и всех его поддоменов за один раз:

```
python photon.py -u "http://www.ethereum.org" --dns
```

Давайте попробуем это с Ethereum.org , как показано на рисунке 7.2.

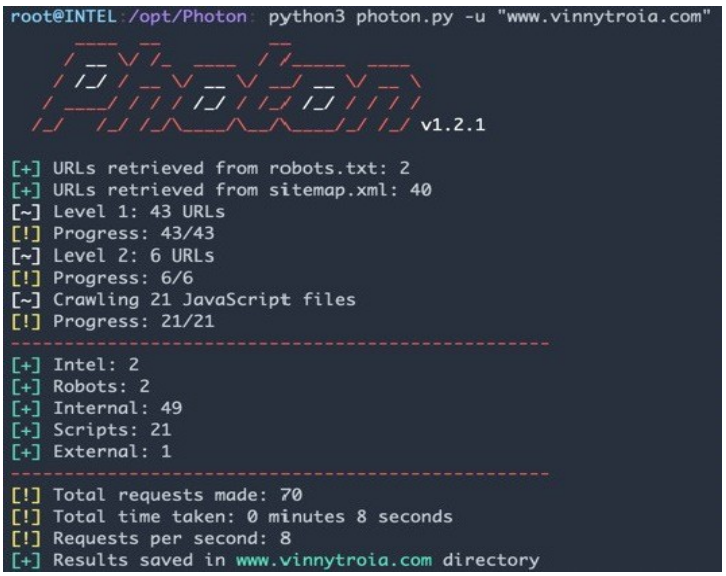


Рисунок 7.1.

Photon автоматически сгенерирует графическую карту DNS домена, используя DNSDumpster.com . Типичный вывод карты DNS выглядит как рисунок 7.3.

Photon также поддерживает сканирование и сканирование архивов из Wayback (Интернет-архив) с помощью **переключателя** --wayback **. Поговорим подробнее о Wayback и Интернет-архивы в главе 8.**

Intrigue.io

В главе 5 мы обсудили Intrigue.io, автоматическое обнаружение поверхности атаки. орудие труда. Intrigue.io - это универсальный инструмент, который делает гораздо больше, чем просто обнаружение сети.

Вы можете загрузить Intrigue.io по адресу https://github.com/intrigueio/. интрига-ядро **.**

Например, модуль паука Интриги невероятно впечатляет (чтобы сказать минимум) и требует очень мало усилий для запуска. Используя графический интерфейс Intrigue, давайте начнем от паука Ethereum.org, чтобы посмотреть, найдем ли мы что-нибудь потенциально полезное.

Для начала выберите URI Spider из списка задач и измените имя объекта на http://www.ethereum.org, как показано на рисунке 7.4. Затем нажмите «Выполнить задачу», чтобы начать. Сканирование.

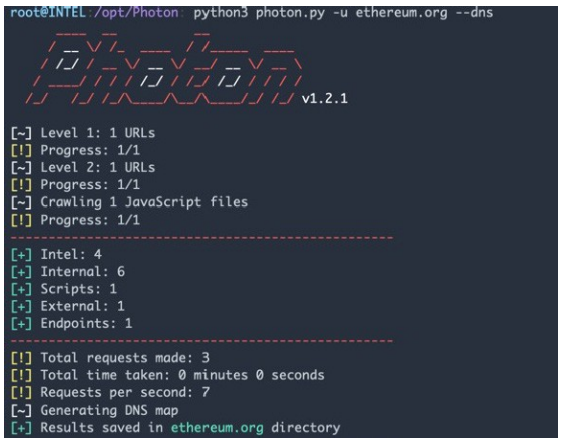


Рисунок 7.2.

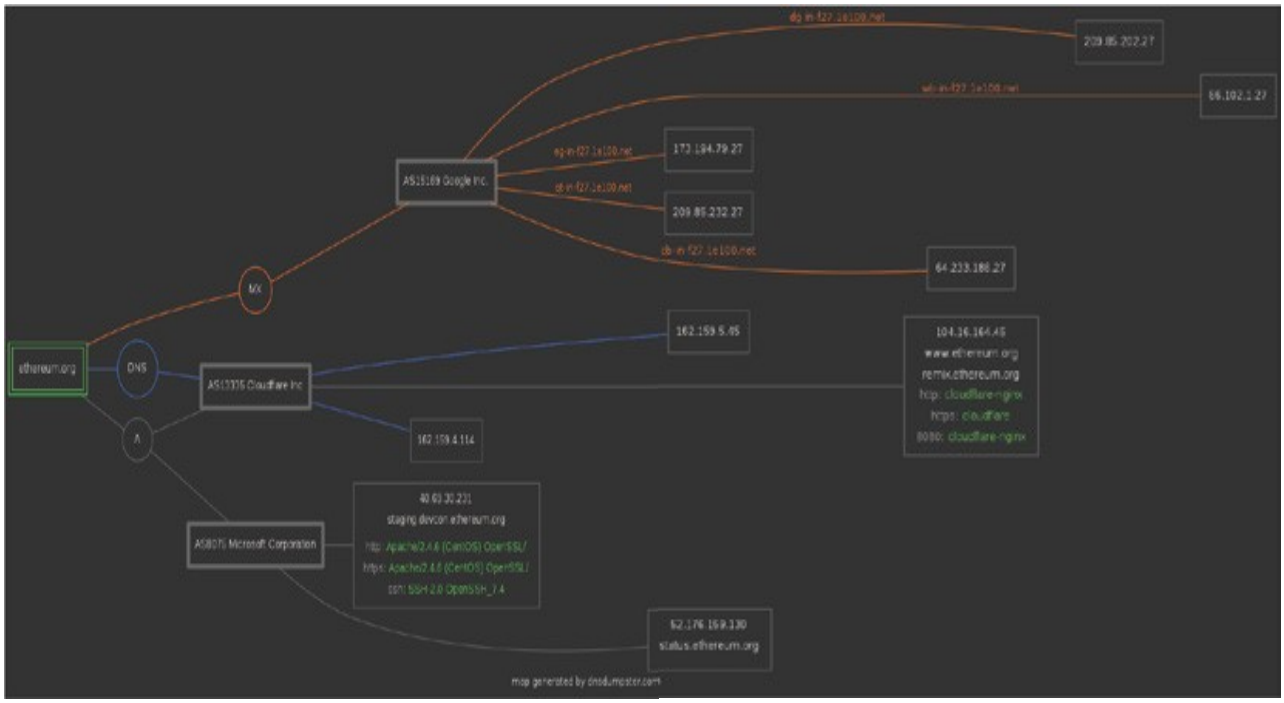

ethereum.org
MX
DNS
A
AS15169 Google Inc.
AS13335 Cloudflare Inc
AS8075 Microsoft Corporation
173.194.79.27
209.85.232.27
64.233.186.27
162.159.5.65
162.159.4.114
104.16.164.45
www.ethereum.org
remix.ethereum.org
40.69.30.231
staging.devcon.ethereum.org
52.176.169.130
status.ethereum.org
map generated by dnsdumpster.com

Рисунок 7.3.

Через некоторое время на вкладке «Сущности» отобразятся результаты сканирования. Рисунок 7.5. показывает сводку различных изначально захваченных объектов.

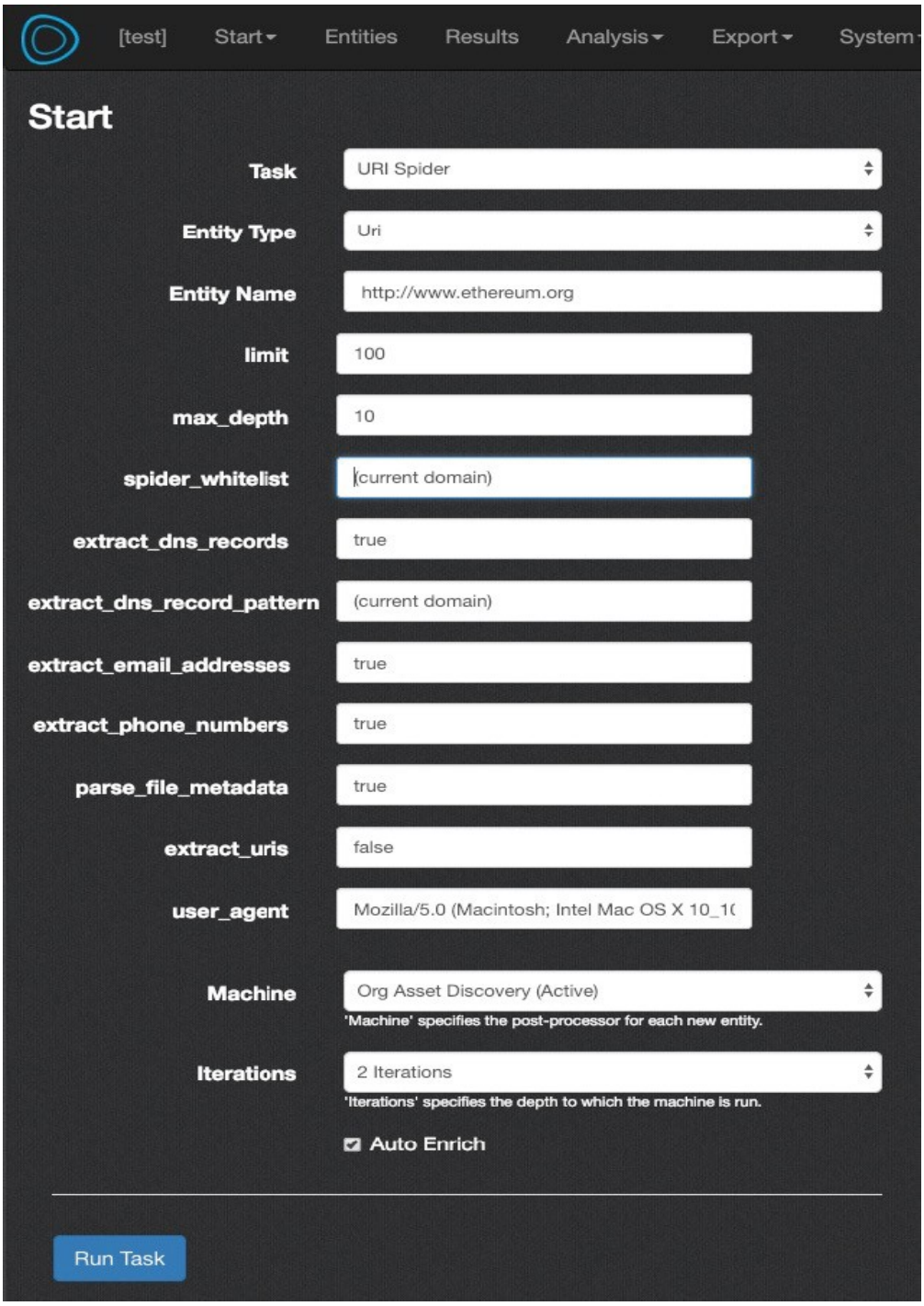


Рисунок 7.4.

Я очень наглядный человек, и одна из моих самых больших проблем - это организация
вся информация, которую я нахожу. Одна из причин, по которой мне нравится использовать интригу, заключается в том, что она позволяет
графический интерфейс для многих инструментов командной строки и объединяет всю эту информацию в один красивый и аккуратный район.

Глядя на наш список статистики, можно найти немало полезной информации, которая
Интрига собрана с нашего целевого сайта, включая другие домены, электронную почту
адреса, телефоны и даже обнаруженные документы.
Графический интерфейс Intrigue.io также позволяет легко фильтровать результаты ваших сущностей.
страницу, чтобы быстро найти нужную информацию (рис. 7.6).

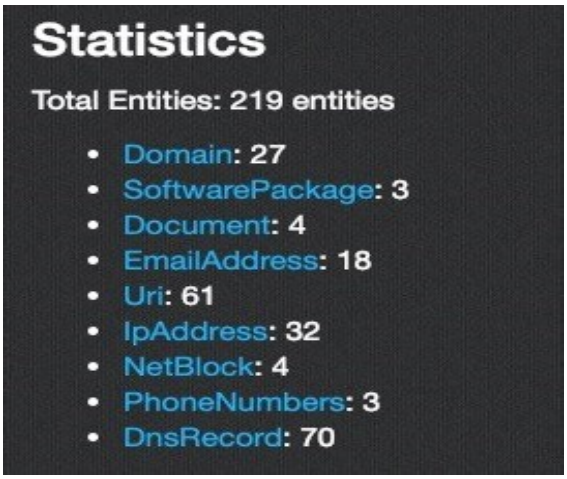


Рисунок 7.5.

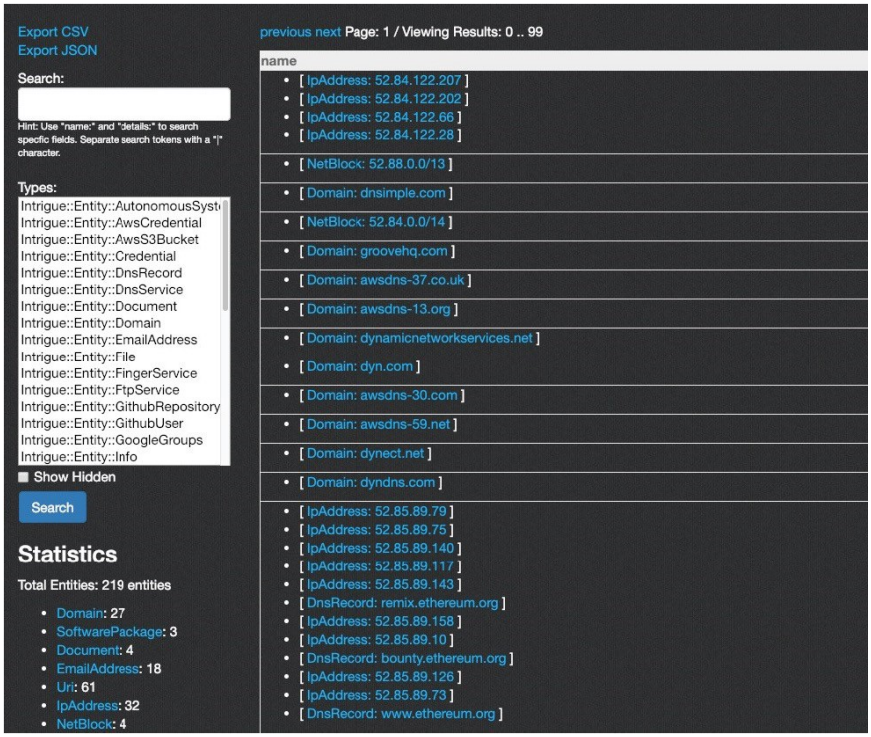


Рисунок 7.6.

Список фильтров - это очень простой способ быстро найти то, что вам нужно. В этом случае
всего 219 сущностей, но возможность фильтровать сущности станет особенно
полезно после выполнения больших сканирований с сотнями тысяч обнаруженных
сущности.

Чтобы понять, что я имею в виду, давайте исследуем сущности EmailAddresses (см. Рисунок 7.7).
Щелчок по ссылке изменяет таблицу информации для отображения обнаруженных
электронные письма. В левой колонке мы можем видеть электронную почту. Справа мы можем увидеть, где
письма пришли, что не менее интересно.

Я считаю обнаруженные адреса электронной почты одним из самых ценных элементов
Информация, которую вы можете найти. С корпоративными электронными адресами, это не может необхо-
Обычно это происходит из-за огромного количества маркетинговых сайтов, продающих доступ
на эти электронные письма. Однако при поиске злоумышленников поиск нового адреса электронной почты
адрес может быть абсолютным золотом, потому что он предоставит вам новую точку поворота
в поисках актера.

Глядя на URL-адреса, мы видим папки для загрузки, субдомены и файлы - в
Короче говоря, множество новых информационных путей, которые могут (и должны) быть дополнительно изучены.

previous next Page: 1 / Viewing Results: 0 .. 99

name	details
• [EmailAddress: press@ethereum.org]	• https://ethereum.org/
• [EmailAddress: donate@ethereum.org]	• https://ethereum.org/donate
• [EmailAddress: info@ethereum.org]	• https://blog.ethereum.org/
• [EmailAddress: brand@ethereum.org]	• https://ethereum.org/images/logos/Ethereum_Visual_Identity_1.0.0.pdf
• [EmailAddress: notices@ethereum.org]	• https://ethereum.org/privacy-policy
• [EmailAddress: support@ethereum.org]	• https://ethereum.org/privacy-policy
• [EmailAddress: gavin@ethcore.io]	• http://gavwood.com/Paper.pdf
• [EmailAddress: sompo@cs.huji.ac.il]	• https://eprint.iacr.org/2013/881.pdf
• [EmailAddress: avivz@cs.huji.ac.il]	• https://eprint.iacr.org/2013/881.pdf
• [EmailAddress: geth-ci@ethereum.org]	• https://geth.ethereum.org/downloads/
• [EmailAddress: fjl@ethereum.org]	• https://geth.ethereum.org/downloads/
• [EmailAddress: jeffrey@ethereum.org]	• https://geth.ethereum.org/downloads/
• [EmailAddress: martin.swende@ethereum.org]	• https://geth.ethereum.org/downloads/
• [EmailAddress: nick@ethereum.org]	• https://geth.ethereum.org/downloads/
• [EmailAddress: peter@ethereum.org]	• https://geth.ethereum.org/downloads/
• [EmailAddress: viktor@ethereum.org]	• https://geth.ethereum.org/downloads/
• [EmailAddress: bounty@ethereum.org]	• https://bounty.ethereum.org/
• [EmailAddress: n@r.nl]	• https://ethereum.org/images/assets/1900/Ethereum-homestead-background-39.jpg

previous next

Рисунок 7.7

Резюме

В этой главе основное внимание уделяется поиску скрытых драгоценных камней на веб-сайте путем поиска скрытые папки в его структуре. Это было достигнуто за счет использования инструментов. которые пытаются тысячи вариаций названия для того, чтобы найти рабочие каталоги (то есть, брутфорс) или сканирование целевого сайта и сбор рабочих ссылок на основе того, что он находится в коде сайта.

В следующей главе мы сосредоточимся на поиске скрытых данных веб-сайтов с помощью операторов продвинутых поисковых систем (т. е. «придурков»).

159

8

"Dorks" - это специально созданные условия расширенного поиска, которые можно использовать на любом
поисковая система для поиска широкого спектра общедоступной информации в сети.
Дорки (в основном) универсальны, но примеры в этой книге будут конкретно
на основе условий поиска Google.
Процесс Dorking относится к использованию общих фраз об ошибках, которые относятся к
специальный код ответа генерируется на языке программирования. Другими словами,
это поисковые запросы, используемые для поиска скрытых (и часто неправильно настроенных) данных.
в веб-сайтов. Google DORK запросы часто могут быть использованы для поиска:

■ XSS, SQLi и другие уязвимости в сети, основанные на параметрах.
Приложения

■ Конфиденциальная информация с веб-сайтов, такая как имена пользователей, пароли,
и другие формы PII

■ Информация о покупках в Интернете, такая как данные клиентов, заказы, номера кредитных карт,
и номера транзакций

■ Информация о принтерах, видеокамерах и типах IOT-устройств.

Вы можете найти исчерпывающий и регулярно обновляемый список придурков на сайте Exploit-
БД (ранее - База данных взлома Google): https://www.exploit-db.com/
google-hacking-database .

Поисковые машины Dorks

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

Google постоянно ограничивает то, что вы можете искать с операторами тупицы. Ты не можешь найти столько, сколько раньше.
Используйте оператор site:, **чтобы ограничить результаты поиска Google этим доменным именем. Ты можно сделать то же самое с Bing и DuckDuckGo. С Bing вы делаете это путем поиска IP-адреса. адрес - это называется «пассивным DNS для бедняков». Это быстрый способ увидеть все размещаются на этом IP-адресе - домены, документы и т. д.**
Во многих случаях вы можете обойти фильтр Google, выполняя поиск с помощью API Google.

Essential Search Dorks

Даже базовое понимание придурков поисковых систем станет ценным инструмент в вашей повседневной жизни, даже за пределами взлома и расследований безопасности. Это навык, который не только улучшит качество результатов поиска, но и также помогают снизить общий уровень стресса, когда вы не можете найти то, что вы ищу в сети.

В этом разделе основное внимание уделяется абсолютно важным модификаторам поиска, которые вы следует учиться и запоминать. Это все техники, которые я использую ежедневно, и вы, вероятно, тоже будете.

Знак минус

Я начинаю с модификатора минус, потому что это, наверное, самый простой и самый важный придурок, чтобы научиться. Знак минус (-) может спасти вас от читать страницы и страницы бесполезного маркетинга и товарного мусора, позволяя вам отфильтровать определенные термины из результатов поиска.

Этот метод невероятно полезен в правильном контексте. В самом простом уровень, это поможет удалить похожие, но неверные результаты поиска, которые раздувают запросы.

Использовать этот модификатор поиска так же просто, как и звучит: введите поисковый запрос, за которым следует знак минус и любые термины, которые вы *не* хотите использовать.

Использование цитат

Этот модификатор поиска так же прост и будет действовать противоположно использованию знак минус. Заключение поискового запроса в кавычки будет точно соответствовать вашему тексту. находясь в поиске. Например, поиск *хакера NSA* вернет результаты с слова NSA и Hacker, при поиске «NSA Hacker» будет возвращаться только результаты с этой точной фразой.

Сайт: Оператор

Оператор site: search вернет результаты поиска только на указанном веб-сайте.
Я лично считаю, что это один из самых полезных придурков OSINT, поскольку он позволяет сосредоточить поиск на целевой компании.
Например, чтобы ограничить поисковый запрос одним веб-сайтом, вы можете ввести следующее: сайт: domain.com . При выполнении этого запроса, Google будет возвращать вся информация, относящаяся к вашему поиску, относящаяся к «сайту», который вы запрашиваете.
Теперь, когда мы можем искать что угодно в определенном домене, давайте попробуем что-нибудь полезное и выполните поиск на определенном сайте, например fakebank.com .
Может быть, нам нужен быстрый способ узнать, проиндексированы ли какие-либо файлы Excel (XLS). на fakebank.com . Мы должны ввести в нашу поисковую систему следующее:

```
xls сайт: fakebank.com
```

Чтобы создать открытую поверхность для атаки, я начну с инструмента перечисления поддоменов, например Sublist3r, который будет проверять общедоступные базы данных и запускать списки слов для домена, чтобы найти поддомены. Затем я буду следить за этим с помощью Google Dorking и сайта: **оператор, ища все, что было пропущено Sublist3r.**

Название: Оператор

Использование оператора intitle: скажет Google показывать только те страницы, на которых есть указанный поисковый запрос в их странице / заголовке HTML. Следующий поисковый запрос вернет все сайты, в названии которых есть Pepsi:

```
название: пепси
```

Как только вы начнете понимать типы заголовков, которые используются на общих страницах, это Оператор становится бесконечно более полезным. Например, следующий поиск будет показать вам страницы с общедоступной сетевой камерой AXIS:

```
intitle: "Live View / - AXIS"
```

Другой способ поиска одинаковых камер AXIS - комбинировать intitle: операторов и просто найдите важные ключевые слова, например:

```
InTitle: "живой вид" InTitle: ось
```

На рисунке 8.1 показан пример результатов этого запроса.

Allintitle: Оператор

Вместо того, чтобы использовать пример из предыдущего раздела и иметь два intitle: операторов, оператор allintitle: позволяет упростить запрос. Google покажет вам только результаты поиска, в которых все поисковые слова содержатся в заголовок страницы. Следующий поиск будет возвращать только результаты , которые имеют *все* из слова «ось», «вживую» и «вид» в названии:

Allintitle: оси живого изображения

Чтобы увидеть разницу между результатами, полученными двумя операторами, сравните результаты, показанные на рис. 8.1, с результатами на рис. 8.2.

Тип файла: Оператор

Оператор filetype: - хороший модификатор поиска, который можно использовать при поиске определенные типы файлов, которые могли быть забыты, например XLS, DOC или CSV файлы. Возможно, вам повезет и вы найдете оставшийся бюджетный XLS-файл. Чтобы найти файл бюджета на определенном сайте, мы будем использовать следующие запрос:

Тип файла бюджета: xls site: sitename.com

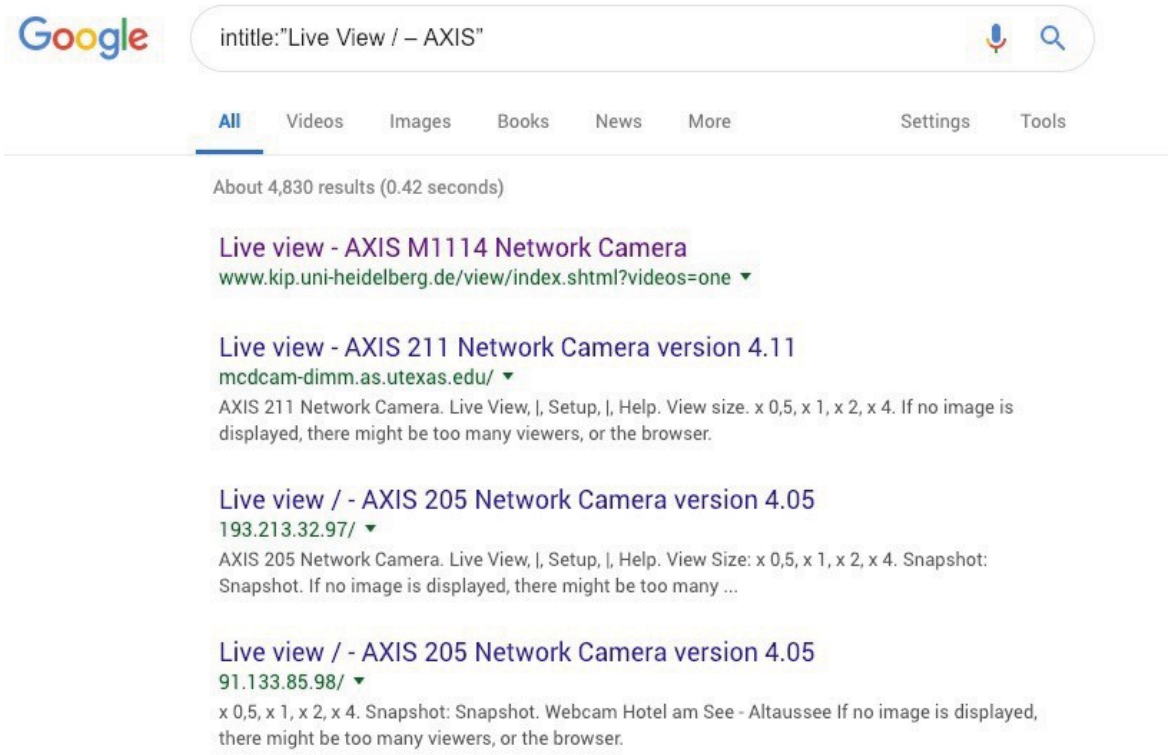


Рисунок 8.1.

Поиск файлов резервных копий - невероятно важная часть расследования.
Люди становятся небрежными и оставляют файлы без дела, и чаще всего такие
файлы будут иметь расширение .bak :

тип файла: бак

Inurl: Оператор

Оператор inurl: выдаст вам результаты с вашим поисковым запросом, в частности, в
URL-адрес. Это не обязательно должно быть только доменное имя; он может включать путь
или даже имя файла. Основываясь на предыдущем примере поиска резервной копии
files, мы можем использовать этот поиск для поиска файлов резервных копий паролей:

тип файла: бак inurl: пароль

На рис. 8.3 показан пример результатов этого типа поиска.
Хотите посмотреть веб-камеры в прямом эфире? Попробуй это:

inurl: "webcam.html"

Как показано на рис. 8.4, мы также можем искать файлы Excel (XLS) со словом
«Конфиденциально» в названии:

тип файла: xls inurl: конфиденциально

Не забываем про номера портов!

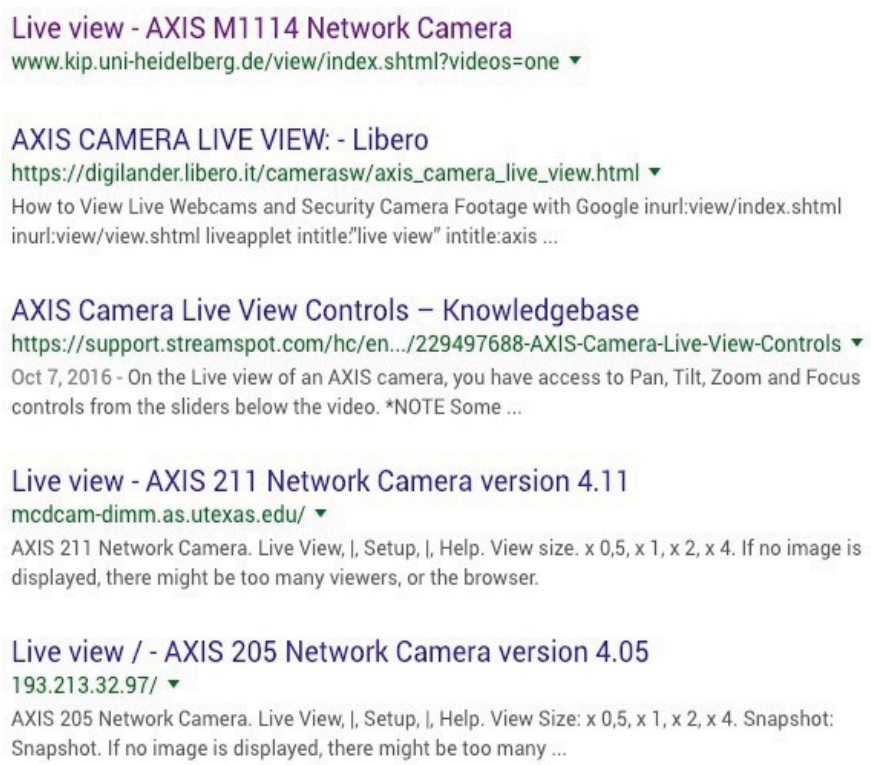


Рисунок 8.2.

Например, если вы хотите найти активные панели Plesk, вам может потребоваться искать:

```
Inurl: 8443 Plesk
```

На рис. 8.5 показан пример результатов такого поиска.

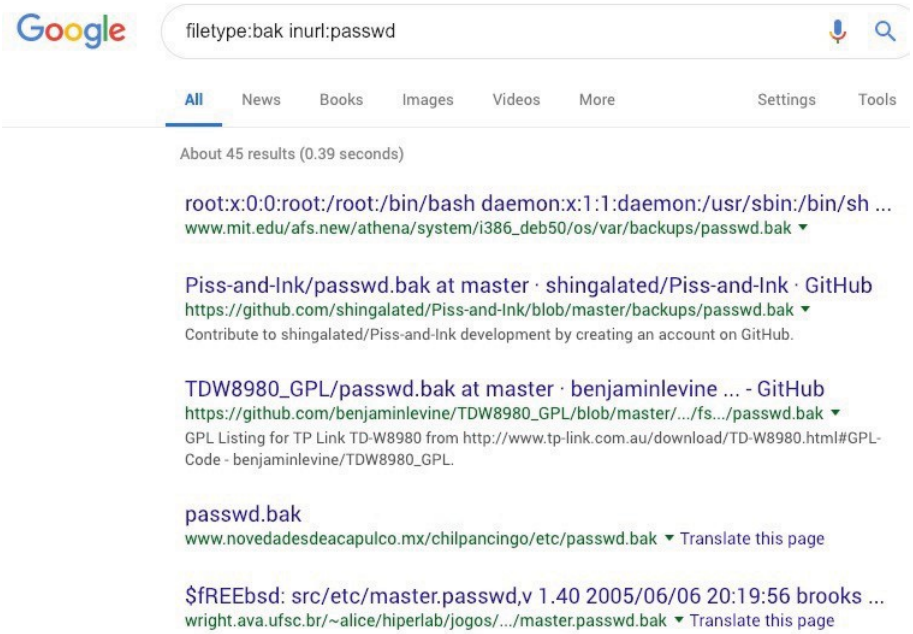


Рисунок 8.3.

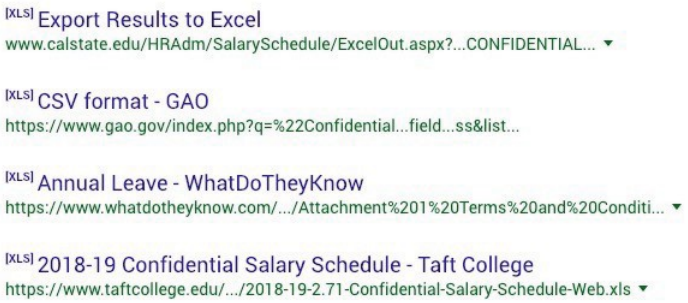


Рисунок 8.4.

Кеш: Оператор

Оператор cache: очень важен, потому что он позволяет вам искать
страницы в кеше Google. Страницы и сайты приходят и уходят, и иногда это может быть
необходимо искать страницу или файл, который был удален:

Кеш: поисковый запрос domain.com

Поиск в архивах Google и Wayback (archive.org) будет
более подробно обсуждается в главе 10.

Allinurl: Оператор

Подобно Allintitle: , в allinurl: оператор ограничить результаты URL - адресов
которые содержат все слова, которые вы указали в поисковом запросе. Например,
[allinurl: foo bar private] вернет результаты с «foo», «bar» и «private».
в URL. Важно отметить, что allinurl: игнорирует знаки препинания, поэтому
allinurl: foo / bar будет игнорировать / и возвращать результаты только с «foo» и «bar»
в URL.

Имя файла: Оператор

Расширение filename: очень похоже на оператор allinurl:, но его сложнее
придавить. Я не использую его так часто, но это может быть полезно, если вы ищете
для определенных файлов резервных копий конфигурации, таких как wp-config.bak .

Интекст: Оператор

Оператор intext: будет искать ваши конкретные слова в тексте сети.
страница. Это кажется маловероятным, но не стоит сбрасывать со счетов этого оператора. Эта операция-
ator можно использовать для сканирования страниц для поиска *любого* текста, например адреса электронной почты,
полное имя, PII или даже ключевые слова с экрана входа в систему администратора.

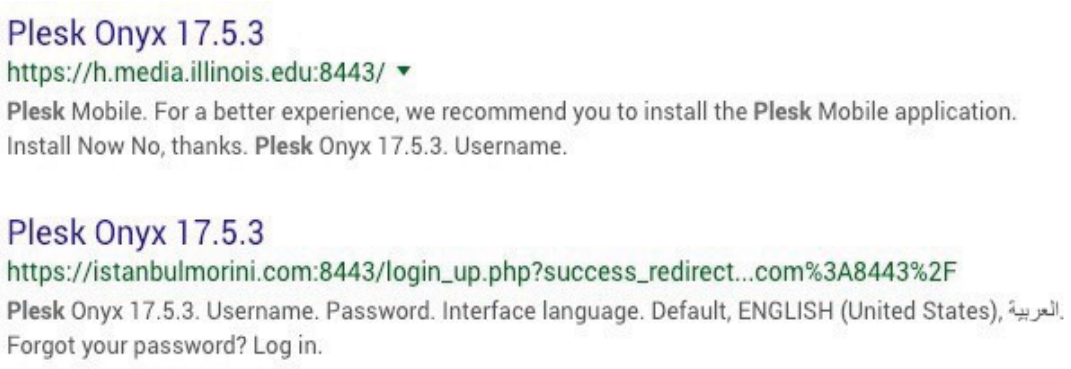


Рисунок 8.5.

Давайте воспользуемся этим для поиска активных административных панелей Plesk:

allintext: Название языка интерфейса: "Plesk"

На рисунке 8.6 показаны результаты этого поиска.

Сила придурка

Давайте возьмем то, что мы узнали, и применим это к одному из наших предыдущих примеров.
домены: DualxCrypt.org . Большинство наших сетевых поисков были
выходит пустым, но, возможно, мы сможем найти один или два самородка, используя доркинг
техника.

Иногда самый простой поиск может дать наилучшие результаты. Показать тебе
что я имею в виду, давайте поищем любые сайты, в тексте которых есть DualxCrypt.org :

intext: dualxcrypt.org

На рисунке 8.7 показаны результаты поиска.

Когда в главе 5 впервые был представлен DualXCrypt.org , я упомянул, что
Я узнал о домене, потому что он был упомянут в KickAss, Dark Web.
хакерский форум. Несмотря на то, что на сайте четко указано, что он связан с KickAss,
администратор сайта (пользователь: NSA) настаивал на том, что DualXCrypt не был создан
его или его команду.

Итак, щелкнув третью ссылку, мы попадаем на domainbigdata.com и некоторые другие
Получение результатов. Из результатов, показанных на рисунке 8.8, видно, что IP-адрес



Рисунок 8.6.

размещен в Cypher-Net. Даже если это окажется тупиком, это все равно
довольно удивительное совпадение названий, которое нельзя игнорировать.
Не менее интересен список других доменов, использующих тот же IP.
адрес (показан на рисунке 8.9).

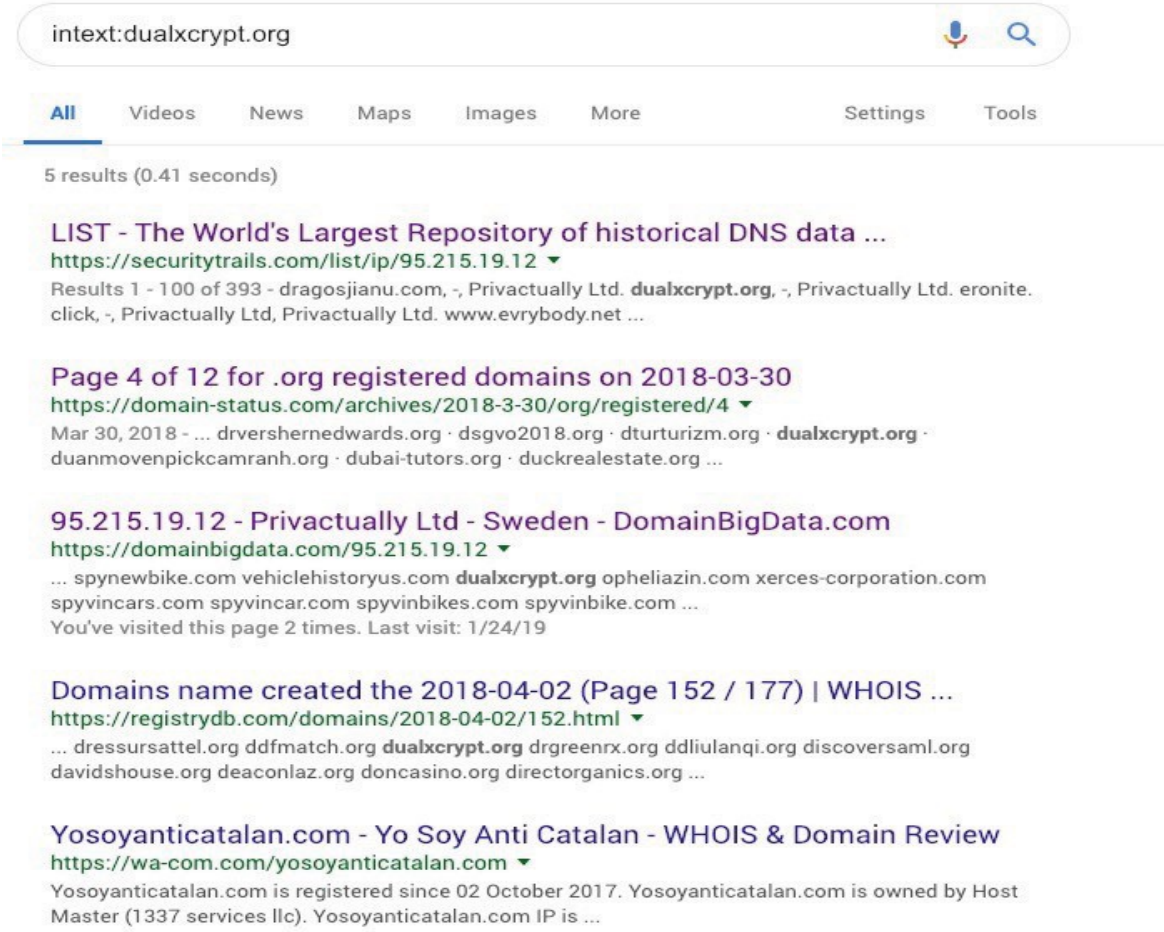


Рисунок 8.7

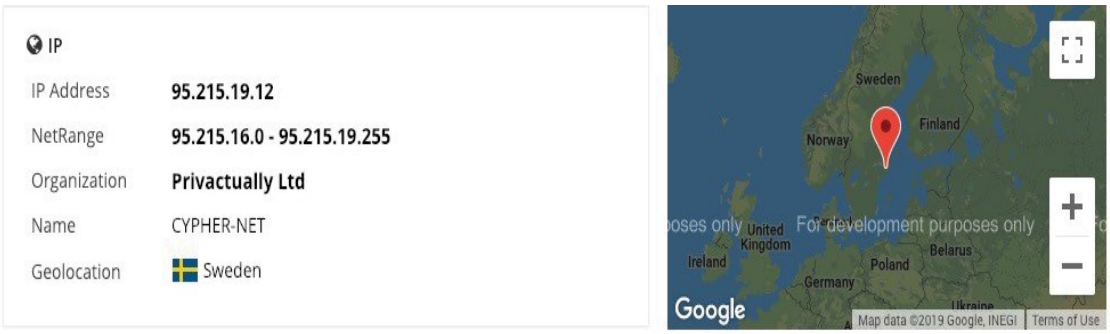


Рисунок 8.8

Трудно игнорировать вероятность того, что злоумышленник несколько других вредоносных или незаконных доменов, работающих на одном IP-адресе. В Результаты, показанные на рис. 8.9, открыли множество новых возможностей для атрибуции - и в то же время открылось то, что могло оказаться огромной тратой времени. Интернет предоставляет в наше распоряжение столько информации, что легко отвлечься с деталями, которые ведут вас в бесконечную кроличью нору. Возможно, что один из эти другие сайты предоставят ключ к раскрытию истинной личности нашего злоумышленника.

Website using this ip : 95.215.19.12 (top 100)

tamilrebels.com
powh.net
zuckless.org
matteboken.com
smartoptions.co
legale-mischung.org
smart-options.org
twitterfuck.com
joshuasoderholm.com
bookfair.cz
ripply.eu
semerie.com
uqhail.com
macgames-download.org
barterdex.com
barterdex.info
barterdex.org
secretdejt.se
robitq.com
dailycrypto.org
hpguiden.com
satoshistruevision.com
suscripcionneumaticos.com
contratosuscripcionneumaticos.com
authled.com
njalla.no
maestroiptv.net
sigavpn.org
kiezkommune.org
vincheckupfast.com
phoszine.com
buntglaublich.com
vinreportus.com
spyvinbikes.com
spyvincars.com
opheliazin.com
vehiclehistoryus.com
spyvinhistory.com
usavinnow.com
vinrecordusa.com
praisemonero.com
spyvins.com
vinsspy.com
historyspyvin.com
scanvinusa.com
latinoguysporn.net
residences4you.com
vinhistoryofficial.com
mode-warp.net
spycarsvin.com

bikinination.net
slutsofsnapchat.com
robitmedia.com
saik0.org
shinebelleza.com
usavinreport.com
macerie.org
josipdellolio.com
macgames-download.net
openredirect.net
njalla.net
kmdexplorer.com
digitalhighass.com
stbrunomedia.org
barter-dex.com
barterdex.net
barter-dex.org
torrent9.nl
yosoyanticatalan.com
amjad-media.net
uqaorg.com
casinosblockchain.com
tarifaplananeumaticos.com
larptog.com
elmurion.com
bitcoinpoland.org
atlagainstamazon.org
lendxgroup.com
beach-thong.com
vinfastcheckup.com
airdropone.com
premiumchannels.info
spyvinbike.com
spyvincar.com
xerces-corporation.com
dualxcrypt.org
spynewbike.com
kernel-update.org
usavinscan.com
vinspyhistory.com
spymotorcycle.com
unlimitedblocksize.org
speedrunhq.com
unofficialkodi.com
worthlessethereumtoken.com
montrealnazileaks.net
usaspybike.com
spyusavin.com
vonageuk.com
spymotorcyclevin.com

Рисунок 8.9

Однако в данном случае они совершенно не связаны. Проведя небольшое исследование IP, я обнаружил, что он (и Cypher-Net) принадлежит Njalla.io, полностью анонимному mous компания по регистрации доменов.
Njalla.io теперь также предлагает анонимный веб-хостинг, что объясняет, почему так много вредоносные сайты используют этот IP-адрес.

Не забывайте о Bing и Yahoo!

Google - это здорово, но это не единственная поисковая система. Часто Bing раскрывает результаты поиска, которые Google похоронил. По этой причине Yahoo не менее важен. У каждого сайта свой алгоритм поиска, и если вы ограничите поиск одним поисковой системе вы можете пропустить важную информацию. Придурки дис- Обсуждаемые в этой главе, будут работать в Google, Bing и Yahoo.
Вы должны взять за правило выполнять поисковые запросы во всех поисковых системах. я понимаю насколько это может быть утомительно, поэтому вы можете подумать об автоматизированных инструментах, которые помогут
в вашем стремлении к охоте на придурков через несколько поисковых систем.

Автоматизированные инструменты доркинга

Было бы здорово, если бы мы взяли все, о чем только что узнали dorks и используйте эти поисковые запросы для автоматизации процесса уязвимости охота или обнаружение OSINT на всех веб-сайтах?
Именно для этого был создан Inurlbr.

Inurlbr

Inurlbr (рис. 8.10), вероятно, лучший автоматический инструмент для поиска дорков на Интернет. Этот инструмент автоматизирует процесс поиска конкретных придурков в

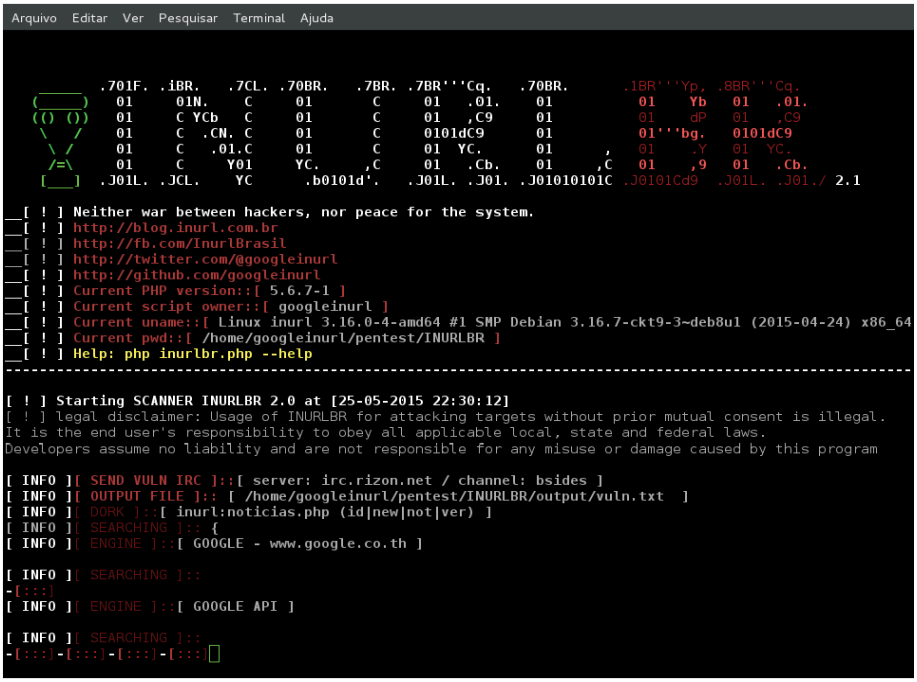


Рисунок 8.10

несколько поисковых систем (не только Google). Цель этого инструмента - помочь вам быстро найти уязвимые сайты, но вы можете использовать его и для других целей. Inurlbr также позволяет выполнять поиск по TOR, Shodan Exploits и Wikileaks. это доступно для загрузки по адресу https://github.com/googleinurl/SCANNER-INURLBR .

Чтобы использовать Inurlbr, вы предоставляете приложению указанный вами дорк, и оно вернет все сайты, которые он находит. Это особенно полезно при поиске конкретного эксплойт, а может сайты с оболочкой c99.

Inurlbr также является средством поиска эксплойтов, которое в этой книге не обсуждается (и мы не можем публиковать живые уязвимости). Но некоторые из интересных функций для Inurlbr включают в себя:

- Настройка заголовков HTTP и строк пользовательского агента.
- Случайное переключение прокси
- Электронная почта и извлечение URL
- Проверка уязвимости
- Эксплойты внедрения SQLi, LFI
- Поиск страниц на основе определенных строковых шаблонов (например, регулярного выражения).

Доступные переключатели и параметры для Inurlbr действительно исчерпывающие. В следующий код показывает несколько ключевых.

Это, вероятно, только половина фактического общего количества доступных параметров, поэтому обязательно используйте переключатель --help, чтобы просмотреть полный список:

```
-q Выберите, какую поисковую систему вы хотите использовать через [1 ... 24] / [e1..6]]:
[параметры]:
1 - GOOGLE / (CSE) GENERIC RANDOM / API
2 - BING
3 - YAHOO BR
4 - СПРОСИТЬ
5 - HAO123 BR
6 - GOOGLE (API)
7 - ЛИКОС
8 - УОЛ БР
9 - ЯХУ НАС
10 - SAPO
11 - ДМОЗ
12 - ГИГАБЛАСТ
13 - НИКОГДА
14 - BAIDU BR
15 - ЯНДЕКС
16 - ЗООПАРК
17 - ГОРЯЧИЙ БОТ
18 - ЧЖОНСОУ
19 - ПОИСК
20 - ЭЗИЛИОН
21 - СОГОУ
22 - УТКА УТКА ИДЕТ
```

23 - БУРОВ
24 - ГЕНЕРИЧЕСКИЙ СЛУЧАЙ GOOGLE (CSE)

СПЕЦИАЛЬНЫЕ МОТОРЫ
---
e1 - НАЙТИ ТОР
e2 - СЛОН
e3 - ПОИСК
e4 - WIKILEAKS
e5 - OTN
e6 - ИСПОЛЬЗУЕТ ШОДАН
---
all - Все поисковые системы / не специальные моторы
--proxy Выберите, какой прокси вы хотите использовать в поисковой системе:
--proxy-file Установить файл шрифта для рандомизации вашего прокси для каждого поиска
двигатель.
--time-proxy Установить время, как часто будет производиться обмен прокси.
--tor-random Включает функцию TOR, каждое использование связывает уникальный IP-адрес.
-t
Выберите тип проверки:
--dork Определяет, какой дорк будет использовать поисковая система.
--dork-file Установить файл шрифта с вашими поисковыми дорками.
-a
Укажите строку, которая будет использоваться в поисковом скрипте:
-м
Включите поиск писем по указанным URL.
-u
Включает поиск списков URL-адресов по указанному URL-адресу.
--save-as Сохранить результаты в определенном месте.
--пользователь-агент
Определите пользовательский агент, используемый в его запросе против
цель.
--regexp Использование регулярного выражения для проверки своих исследований
--replace Заменить значения в целевом URL.
--cms-check Включить простую проверку, использует ли URL / цель CMS.
--sall Сохраняет все URL-адреса, найденные сканером.
--ifcode Допустимые результаты на основе вашего HTTP-кода возврата.
--delay Задержка между исследовательскими процессами.
--command-all Используйте эту команду, чтобы указать одну команду для
КАЖДЫЙ URL найден.

Использование Inurlbr

К настоящему моменту должно быть очевидно, что Inurlbr действительно предназначен для использования в качестве инструмента черной шляпы для
сканировать на наличие легко используемых уязвимостей. Это не значит, что у него нет
законные и полезные цели.

Если вы предприниматель в сфере безопасности и хотите начать свой бизнес или опыт безопасности, вы можете использовать этот инструмент как ступню в дверь с уязвимыми организации. Как только вы обнаружите уязвимость, вы можете уведомить организацию о ошибка. Они могут быть настолько впечатлены вашей работой, что могут нанять вас, чтобы их системы!

Но будь осторожен. Вы должны рассказать им об уязвимости и помочь им закрыть ее. прежде чем вы попросите их взять вас в качестве клиента, иначе они могут истолковать этот жест как шейкдаун.

Inurlbr основан на PHP, поэтому его запуск может немного отличаться от другого.

Скрипты Python. Убедитесь, что у вас настроена среда PHP. Для начала давайте

поиск простого придурка для поиска активных веб-камер AXIS с использованием только Bing (результаты показаны на рисунке 8.11):

```
php inurlbr.php --dork 'inurl: view / index.shtml' -q 2 -s save.txt
```

Это 164 результата, и это с использованием только Bing! (Если вы хотите расширить свой

выполните поиск не только в Bing, используйте -q all.

Небо здесь действительно предел. По мере того, как вы глубже погружаетесь в поиск придурков, вы почти наверняка столкнется с блоками поисковых систем (например, CAPTCHA) для проверки



Рисунок 8.11

что ты человек. Вы можете попытаться обой роверки, чередуя
ваши прокси.

Если вы ищете придурков для поиска, не заб б эксплойтах.
база (https://www.exploit-db.com).

Параметр --proxy позволит вам указать прокс пользования или --proxy-file
позволит вам использовать альтернативные нутри файла. Также можно чередовать прокси
используя временной интервал, который вы нете с помощью --time-proxy .

Следующий дорк предназначен для помощи е панелей администратора. Он будет искать все
поисковые системы, используйте прокси в ф кси и чередуйте прокси каждые
второй:

```
php inurlbr.php --dork 'inurl: admin intitle: login' -q все
--proxy-файл proxy.txt --time-proxy 1s -s save.txt
```

Настоящая сила Inurlbr заключается в его сп ти тестировать и проверять LFI и SQLi.
уязвимости. Это выходит за рамки данной к если вам интересно
при поиске уязвимостей вам обязательно ст мотреться к этому инструменту.

Резюме

В этой главе основное внимание уделяется и 93.175.87:80 анию расширенных поисковых запросов (т. Е. Тупиц) для
найти информацию, которая в противном сл кет быть скрыта. Этот процесс доркинга может быть
используется для поиска уязвимостей на веб-сайтах или даже для поиска оставшихся файлов и
поддомены. В этой главе описаны основные техники доркинга, которые следует
запоминается и используется ежедневно.

Теперь, когда мы установили несколько способов идентификации поддоменов
и сетевых адресов, следующая глава будет посвящена краеугольному камню любого
исследование домена: WHOIS.

175

9

В следующих двух главах будут рассмотрены три конкретные темы: WHOIS, передача сертификатов.
parency, и Интернет-архив (он же Wayback Machine). Три инструмента
вместе взятые, станут чрезвычайно мощным инструментом расследования в вашем арсенале.
В этой главе основное внимание уделяется силе данных WHOIS.
В этой главе будет представлена справочная информация о WHOIS, о том, что это такое,
и почему это важно, а также рассмотрим различные услуги,
просматривать данные WHOIS, а также различные методы, которые можно использовать для запроса и
раскрыть исторические записи WHOIS.

КТО

Данные WHOIS могут содержать много полезной информации об атрибуции, касающейся
владелец домена, *если у* вас есть к нему доступ.
Протокол WHOIS используется для запроса баз данных, содержащих всевозможные публикации.
имеющаяся в открытом доступе информация на интернет-ресурсах, включая доменные имена и
IP-адреса. Он был получен из более раннего протокола имени / пальца, того же самого
протокол за сервером ARPANET NICNAME, который был частью ARPANET,
предшественник Интернета.
Протокол WHOIS используется для запроса широкой сети серверов WHOIS.
для получения любой информации о доменах, стоящих за миллиардами веб-сайтов вокруг
мир (все вместе известные как данные WHOIS). Тонны услуг и инструментов

КТО

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

доступны для запроса записей WHOIS, которые обычно могут возвращать информацию
по контактам регистранта, администратора, технических специалистов и специалистов по выставлению счетов домена.
С годами регистрация домена добавила уровень конфиденциальности (за определенную плату), мак-
При этом определить истинного владельца доменного имени гораздо сложнее.
В 2018 году процесс атрибуции сделал еще больший шаг назад:
введение Общего регламента защиты данных (GDPR) во всем
Европейский Союз. Вскоре после выхода GDPR Интернет-корпорация
Присвоенные имена и номера (ICANN) проголосовали за утверждение Временного специфика-
настройка, которая делает большую часть личной информации, связанной с доменами, недоступной
для общественности, но позволяет определенным сторонам получить аккредитацию от ICANN
и просматривать менее строгий набор данных WHOIS.

Эта глава действительно поможет понять фразу «вы получаете то, за что платите».

Открытый сбор разведывательных данных был бы отличным, если бы все инструменты и информация были всегда совершенно бесплатно, но это не всегда так. Некоторые из самых ценных и полезная информация, которая может вам понадобиться во время расследования, будет иметь большое значение. Возможно, вы в конечном итоге сможете найти информацию, потратив часы (или дни) на поиск через малоизвестные источники. В любом случае цена будет выплачена либо в долларах, либо твое время.

Что касается данных WHOIS, я часто обнаруживал, что самые лучшие данные поступают
из источников с крупнейшими историческими архивами. Чаще новее
домены будут зарегистрированы с соблюдением конфиденциальности домена, особенно купленные
киберпреступниками / субъектами угроз, что означает, что поиск в WHOIS будет
немедленный тупик.
Однако есть вероятность, что зарегистрированное старое, малоизвестное доменное имя
лет назад к вашей цели не прилагались такие же меры предосторожности. Ты
не узнает, пока вы не вернетесь как можно дальше назад, и при поиске WHOIS
data, этот тип исторических данных почти никогда не бывает бесплатным.

Использование данных WHOIS

Вы захотите просмотреть данные WHOIS по ряду причин. Самый распространенный
причины во время расследования заключаются в сборе новой или связанной информации о
домены, вовлеченные в мошенничество или другую преступную деятельность. WHOIS может быть
основной источник отслеживания киберпреступников, особенно если они повторно используют реестры
информация о своих доменах.
Данные WHOIS также можно использовать для:

- Найдите контактную информацию регистранта.
- Найдите подключенные доменные имена, электронные письма и физические адреса.
- Отслеживание личности подставных корпораций

■ Исследовательские ассоциации между организациями и частными лицами

■ Определите стороны, стоящие за доменным именем.

■ Проверить наличие или доступность имен (например, поиск спама
адреса)

Чаще всего ваша цель *не* думает на пять шагов вперед для
дни, когда кто-то придет за ними. Я имею в виду преступников
не часто начинают как преступники. Их первоначальные предприятия могут начинаться (полу) законными
и в конечном итоге станет незаконным, а это значит, что будет больше улик, чтобы найти дальнейшие
назад поискать.
Также вероятно, что у актеров будет один или два адреса электронной почты, специально предназначенные для
зарегистрировать домены. Как только вы сможете найти эти электронные письма, вы, как правило, сможете найти все
своих доменов одним выстрелом.

Исторический WHOIS

Название игры при поиске данных WHOIS в домене имеет
доступ к историческим данным. Как упоминалось ранее, велика вероятность
что домен не всегда был частным. Также есть небольшое окно времени
во время регистрации, где домен мог быть публичным, но затем переключился
в частный. Единственный способ увидеть, что происходит на самом деле, - это
надежная историческая служба WHOIS.
По моему скромному мнению, две самые популярные службы поиска WHOIS - это Whoisology.
com и DomainTools.
Я широко использовал и то, и другое в исследовательских целях, я не чувствую
любой другой сервис приближается к тому же уровню исторических данных, что и
DomainTools.
Однако в интересах справедливости и потому, что эта книга должна
Сосредоточившись на интеллектуальных инструментах с «открытым исходным кодом», я расскажу о нескольких
различных вариантах.

Поиск похожих доменов

Прежде чем искать данные WHOIS, нам нужно найти целевые домены. Существует
хороший шанс, что вы уже знаете доменное имя вашей цели, но это может
быть хорошим упражнением для поиска новых целей и расширения ваших возможностей.

Namedroppers.com

Namedroppers - это поисковая машина по доменному имени. Это наверное один из лучших
инструменты free-mium доступны, потому что поисковые запросы действуют как поиск по шаблонам.

Это означает, что любая строка, которую вы ищете, появится в любой части
доменное имя.
Например, поиск «винни» может отображать любую комбинацию доменов.
со словом Винни в нем:

- Vinny.com
- Vinny1.io
- MyCousinVinny.movie
- VinnyWeGetIt.org

Это важно по нескольким причинам. Во-первых, как я упоминал ранее, никогда не недооценивайте
оценить тщеславие (или неосведомленность) исполнителя угрозы, особенно в их
первые дни заноса, когда OPSEC было просто еще одним причудливым словом, которое нужно выучить.
Из-за широких возможностей поиска на сайте Namedroppers также есть
дополнительное преимущество быстрого поиска доменов, связанных с вашей организацией - это
могут включать в себя домены конкурентов или (скорее всего) фишинговые домены.
Namedroppers покажут вам зарегистрированные домены и предоставят вам
с возможностью просмотра информации WHOIS по любому из этих результатов поиска.
В конечном итоге это платная услуга, но первые 50 результатов бесплатны. Это может
звучит не так уж и много, но этого достаточно, чтобы дать вам представление о том, что еще может быть
там. Если вам нужно больше 50, скажем, для проекта заказчика, отчет
не очень дорого. Давайте посмотрим на несколько примеров.
На рисунке 9.1 показаны начальные окна поиска. Искать легко; просто введите свой
поиск по ключевому слову в поле.
Поиск USBank дает зарегистрированные результаты, показанные на рисунке 9.2.
Более 1000 матчей - это много. Хотя это не очень удобно для подробных исследований,
это отличный инструмент, если вы ищете похожие домены, которые могут
Обычно это используется для фишинговых атак.



Рисунок 9.1.

Поиск по нескольким ключевым словам

Вы также можете использовать поиск для запроса доменов, соответствующих нескольким ключевым словам, например «Банк» и «Америка». При работе с параметрами поиска выбирая
Any Order вернет каждый домен, содержащий каждое ключевое слово, независимо от
заказ, в то время как Exact Order вернет каждое доменное имя с вашим поиском
термины в том порядке, в котором вы их вводили (см. рис. 9.3).

Registered Domain Names

Matched **over 1,000** domain names out of **170,709,443** active records!

1. [WHOIS] **usbank**.biz
2. [WHOIS] **usbank**.com
3. [WHOIS] **usbank**.info
4. [WHOIS] **usbank**.net
5. [WHOIS] **usbank**.org
6. [WHOIS] **usbank**.us
7. [WHOIS] 1**usbank**.com
8. [WHOIS] 1800**usbank**.com
9. [WHOIS] 1st**usbank**.com
10. [WHOIS] 1st**usbank**.info
11. [WHOIS] 1st**usbank**.net
12. [WHOIS] 1st**usbank**.org
13. [WHOIS] 2**usbank**.com
14. [WHOIS] 4**usbank**.com
15. [WHOIS] 50plus**usbank**.com
16. [WHOIS] aus**bank**.com
17. [WHOIS] aus**bank**.net
18. [WHOIS] aus**bank**.org
19. [WHOIS] abacus**bank**.com
20. [WHOIS] abacus**bank**.info
21. [WHOIS] abakus**bank**.biz
22. [WHOIS] abakus**bank**.com
23. [WHOIS] abakus**bank**.info
24. [WHOIS] abakus**bank**.net
25. [WHOIS] abakus**bank**.org
26. [WHOIS] abakus**bank**.us
27. [WHOIS] abplus**bank**.com
28. [WHOIS] abplus**bank**.info
29. [WHOIS] abplus**bank**.net
30. [WHOIS] abplus**bank**.org
31. [WHOIS] accessus**bank**.com
32. [WHOIS] actius**bank**.com
33. [WHOIS] active-bus**bank**.com
34. [WHOIS] aengus**bank**.com
35. [WHOIS] airbus**bank**.com
36. [WHOIS] airbus**bank**.net
37. [WHOIS] akus**bank**.com
38. [WHOIS] al-andalus**bank**.biz
39. [WHOIS] al-andalus**bank**.com
40. [WHOIS] al-andalus**bank**.org
41. [WHOIS] alandalus**bank**.biz
42. [WHOIS] alandalus**bank**.com
43. [WHOIS] alandalus**bank**.org
44. [WHOIS] alandalous**bank**.biz
45. [WHOIS] alandalous**bank**.com
46. [WHOIS] alandalous**bank**.org
47. [WHOIS] alerts-us**bank**.com
48. [WHOIS] alius**bank**.com
49. [WHOIS] alius**bank**.info
50. [WHOIS] alius**bank**.net

Рисунок 9.2.

Чтобы проиллюстрировать этот момент, выполните поиск в «America bank» с выбранным параметром «Любой заказ». вернет результаты, показанные на рисунке 9.4.

Теперь, когда мы выполняем тот же поиск, но с использованием параметра «Точный порядок», мы можем увидеть заметную разницу в результатах, как показано на Рисунке 9.5.

В этих результатах мы видим, что порядок поисковых запросов сохраняется.

Это может существенно повлиять на качество ваших результатов.

Кроме того, глядя на результаты, можно составить важную картину других потенциальных возможностей. фишинговые сайты, конкуренты и сайты, предназначенные для взлома вашего IP.



Рисунок 9.3.



Рисунок 9.4.

Расширенный поиск

Вместо того, чтобы просматривать объемы несвязанных доменов, NameDroppers.com позволяет вам установить расширенные параметры поиска, чтобы сузить результаты поиска, как показано на рисунке 9.6.

При работе с опциями расширенного поиска выберите "Сначала начинается с". Ключевое слово заставит результаты поиска возвращать только те доменные имена, которые начинаются с вашим поисковым запросом. С другой стороны, если выбрать "Завершается последним ключевым словом", показывать только те домены, которые заканчиваются вашим поисковым запросом (см. рисунок 9.7).

Вы также можете настроить свои результаты, чтобы исключить числа, тире и альфа-ча-racters, установите минимальную и максимальную длину и покажите поиск, основанный на расширении домена. Вы уловили идею.

1. [WHOIS] 1bankofamerica.com
2. [WHOIS] 2bankofamerica.com
3. [WHOIS] 420bankofamerica.com
4. [WHOIS] aaabankofamerica.com
5. [WHOIS] abankamerica.com
6. [WHOIS] abankofamerica.com
7. [WHOIS] aboutbankofamerica.biz
8. [WHOIS] aboutbankofamerica.info
9. [WHOIS] aboutbankofamerica.us
10. [WHOIS] abuseatbankofamerica.com
11. [WHOIS] abusebankofamerica.com
12. [WHOIS] adminbankofamerica.com
13. [WHOIS] affinitybankofamerica.com
14. [WHOIS] airportbankamerica.com
15. [WHOIS] albankofamerica.com
16. [WHOIS] alert-bankofamerica.com
17. [WHOIS] alerts-bankofamerica.com
18. [WHOIS] allstatebankofamerica.com
19. [WHOIS] altcoinbankamerica.com
20. [WHOIS] altcoinbankofamerica.com
21. [WHOIS] aluminumcanbankofamerica.com
22. [WHOIS] anti-bankofamerica.biz
23. [WHOIS] anti-bankofamerica.info
24. [WHOIS] anti-bankofamerica.us
25. [WHOIS] antibankofamerica.com
26. [WHOIS] autobankamerica.com
27. [WHOIS] babankkofamerica.com
28. [WHOIS] babankofamerica.com
29. [WHOIS] badbankofamerica.com
30. [WHOIS] banbankofamerica.com

Рисунок 9.5.



Рисунок 9.6.

Ищем злоумышленников

Теперь давайте попробуем другой поиск, ориентированный на злоумышленников. Злоумышленник
первые дни, вероятно, наполнены мечтами стать величайшим в мире
и самый известный хакер. Тема, которую мы рассмотрим в следующих главах, - это
тщеславие преступника (или скрытая потребность в утверждении).
Имея это в виду, есть шанс, что ваша цель зарегистрируется
доменное имя их хакерского псевдонима (например, zerocool.com). Так что это, наверное, не
плохая идея искать псевдонимы вашей цели и видеть, есть ли похожие совпадающие домены
уже зарегистрированы.
Давайте проверим это на нашем приятеле Cyper, как показано на рис. 9.8.
Есть много потенциальных областей, которые стоит изучить. Щелчок по WHOIS
кнопка рядом с каждым доменом приведет вас на сайт GoDaddy для выполнения WHOIS
Погляди.
Я лично не считаю это полезным, но я также не хочу сбрасывать со счетов его
в качестве первого варианта поиска. В зависимости от вашей цели этого может быть достаточно. Как-
когда-либо чаще всего в доменах включена конфиденциальность, и вы увидите
что-то вроде этого:

Имя администратора: Частная регистрация
Административная организация: Domains By Proxy, LLC
Админ-стрит: DomainsByProxy.com

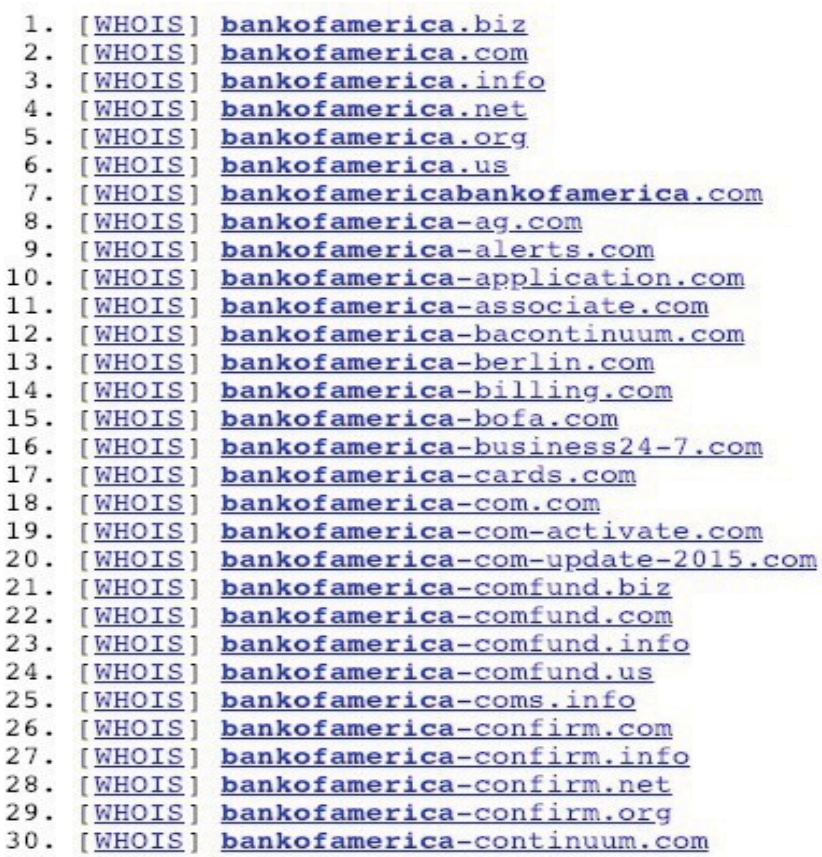


Рисунок 9.7.

Это тип ответа, который вы, вероятно, увидите при стандартном поиске в WHOIS.
Все мои личные домены имеют частную регистрацию, поэтому я был бы удивлен
чтобы найти домен, принадлежащий злоумышленнику, для которого не включена конфиденциальность.

Whoisology

Whoisology (www.whoisology.com) - это архив владельцев доменов, ориентированный на
расследования киберпреступлений, корпоративная разведка и юридические исследования. Суммируя,
Whoisology - это сервис, предназначенный для предоставления вам подробной информации
относительно истории регистрации домена.
На рисунке 9.9 показана начальная страница поиска Whoisology.
Начнем наше исследование с владельца сайта TheDarkOverlord.com .
Вероятность совпадения чего-либо полезного практически отсутствует, но мы
по крайней мере надо попробовать. На рисунке 9.10 показаны результаты поиска Whoisology для
TheDarkOverlord.com .
Текущие данные WHOIS показывают нам частную регистрацию и (к сожалению) ничего
полезный. В этом прелесть сайтов, которые предоставляют *историческую* информацию WHOIS.
Вы можете вернуться на несколько лет назад, чтобы попытаться найти принадлежность к владельцу домена.
На рисунке 9.11 показаны исторические параметры, доступные для TheDarkOverlord.com .

Matched **717** domain names out of **170,709,443** active records!

1. [WHOIS] **cyper**.com
2. [WHOIS] **cyper**.net
3. [WHOIS] **cyper**.org
4. [WHOIS] **cyper**.us
5. [WHOIS] block**cyper**.com
6. [WHOIS] hardcore**cyper**.com
7. [WHOIS] lustyhardcore**cyper**.com
8. [WHOIS] lustylatin**cyper**.com
9. [WHOIS] persianas**cyper**.com
10. [WHOIS] s**cyper**.com
11. [WHOIS] shop**cyper**.com
12. [WHOIS] thread**cyper**.com
13. [WHOIS] ventanas**cyper**.com
14. [WHOIS] **cyper**-demo.com
15. [WHOIS] **cyper**-digital.com
16. [WHOIS] **cyper**-digital.info
17. [WHOIS] **cyper**-digital.net
18. [WHOIS] **cyper**-german.com
19. [WHOIS] **cyper**-hip.net
20. [WHOIS] **cyper**-hr.com
21. [WHOIS] **cyper**-hub.net
22. [WHOIS] **cyper**-meal.com
23. [WHOIS] **cyper**-monday.com
24. [WHOIS] **cyper**-sa.com
25. [WHOIS] **cyper**-space.com
26. [WHOIS] **cyper**-stuhl.com
27. [WHOIS] **cyper**-wp.com
28. [WHOIS] **cyper**78.net
29. [WHOIS] **cypera**.com
30. [WHOIS] ku**cypera**.com

Рисунок 9.8

По результатам 2016 года сразу находим владельца домена (Рисунок 9.12).

Важное примечание: я не верю, что на www.darkoverlord.com **есть что-нибудь что делать с самой хакерской группой. Я просто использовал это как пример.**

Чтобы проиллюстрировать различия между сервисами, давайте сделаем еще одно поиск в WHOIS на сайте другого исследователя безопасности WhitePacket.com . Рисунок 9.13. показывает первые результаты.



Рисунок 9.9

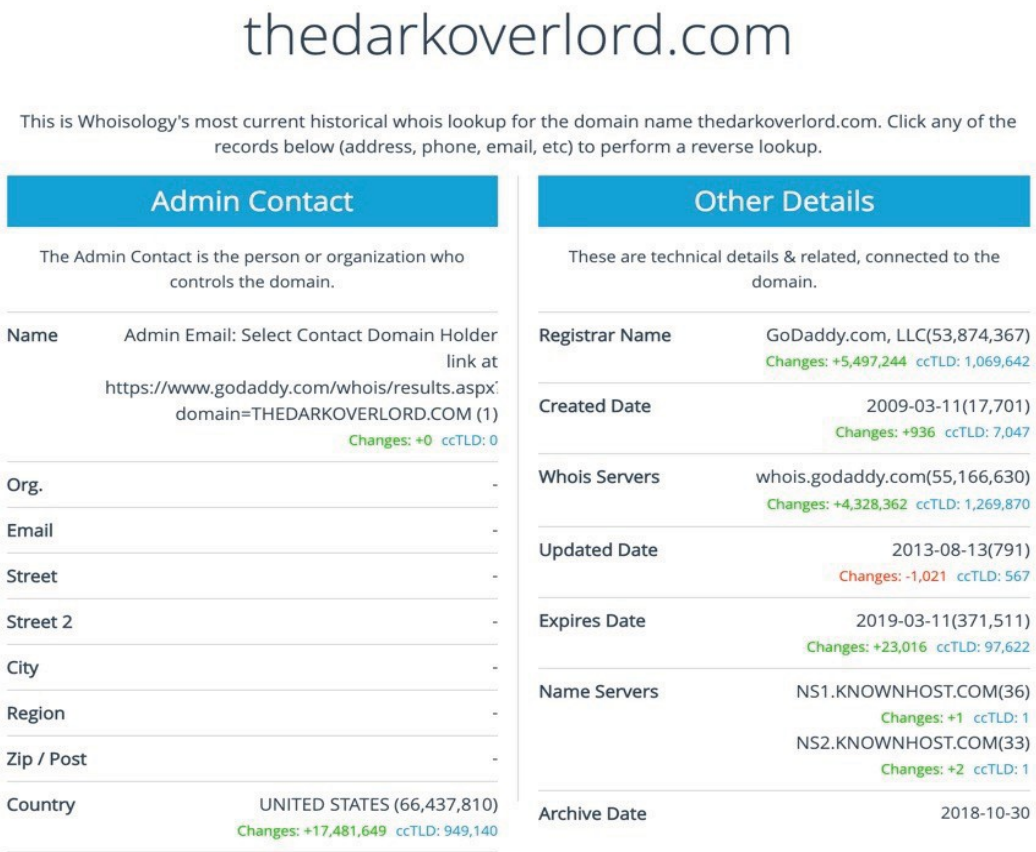


Рисунок 9.10.

Первоначальные результаты защищены, подключенных доменов нет. Этот
следует ожидать при первоначальном поиске в WHOIS, поскольку мы не углублялись в



Рисунок 9.11.

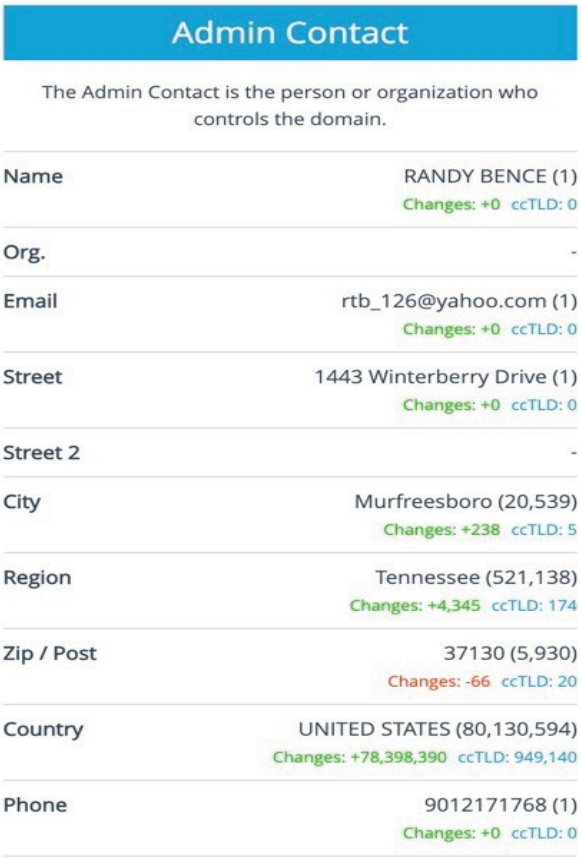


Рисунок 9.12

исторических данных. С Whoisology мы можем использовать исторический Whois на стороне Меню поиска (рис. 9.14), чтобы вернуться назад во времени.

Глядя на историческую таблицу на рисунке 9.14, мы видим, что записи WHOIS еще в декабре 2012 года. Подробнее об исторических ценностях мы поговорим позже.

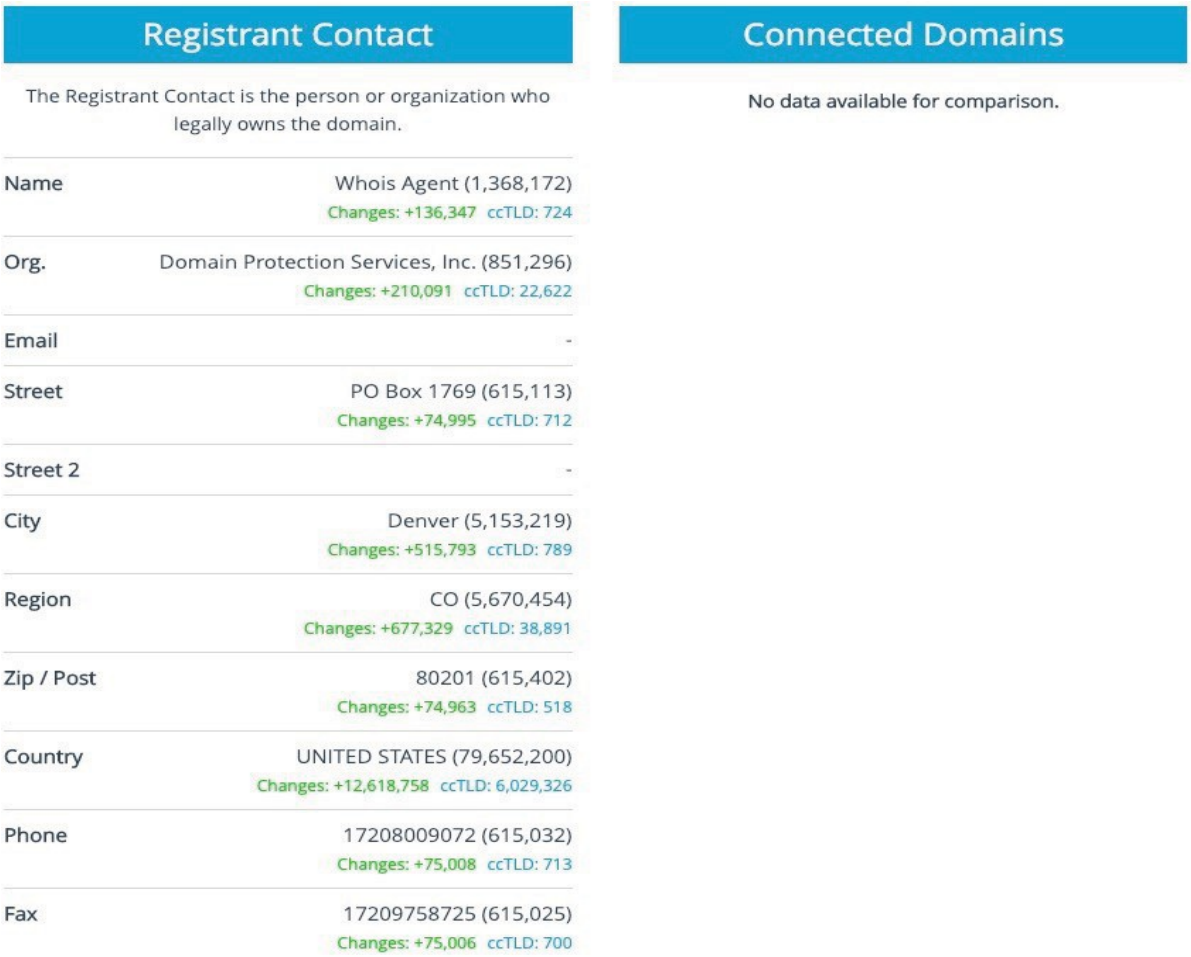


Рисунок 9.13.



Рисунок 9.14.

На данный момент важно отметить, что у нас есть много вариантов для истори-
Атрибуция.

Расширенный поиск домена

Whoisology также имеет действительно хорошую функцию расширенного поиска, где вы можете искать
для строк в любой части домена (аналогично Namedroppers.com).
По их словам, вы можете использовать их расширенный поиск, чтобы найти «цифровые иглы в
более 100000000 стогов сена », используя« несколько фильтров для просеивания
разумный объем данных ». Другими словами, это действительно полезно.
Быстрый расширенный поиск по запросу "cyper" дает множество результатов,
мы потенциально можем исследовать (рис. 9.15).

К сожалению, ни один из этих доменов не оказался полезным. Я использую
Cyper в качестве параметра поиска нашего злоумышленника для единообразия, но также для усиления
Дело в том, что не каждый поиск или инструмент дает полезные результаты. Насколько это было бы реалистично, если бы
каждый пример, который я использую, оказался кладезем полезной информации? Никогда не бывает
так просто . . . но в этом примере мы все еще можем видеть результаты домена и то, как они
***потенциально* может быть полезным.**

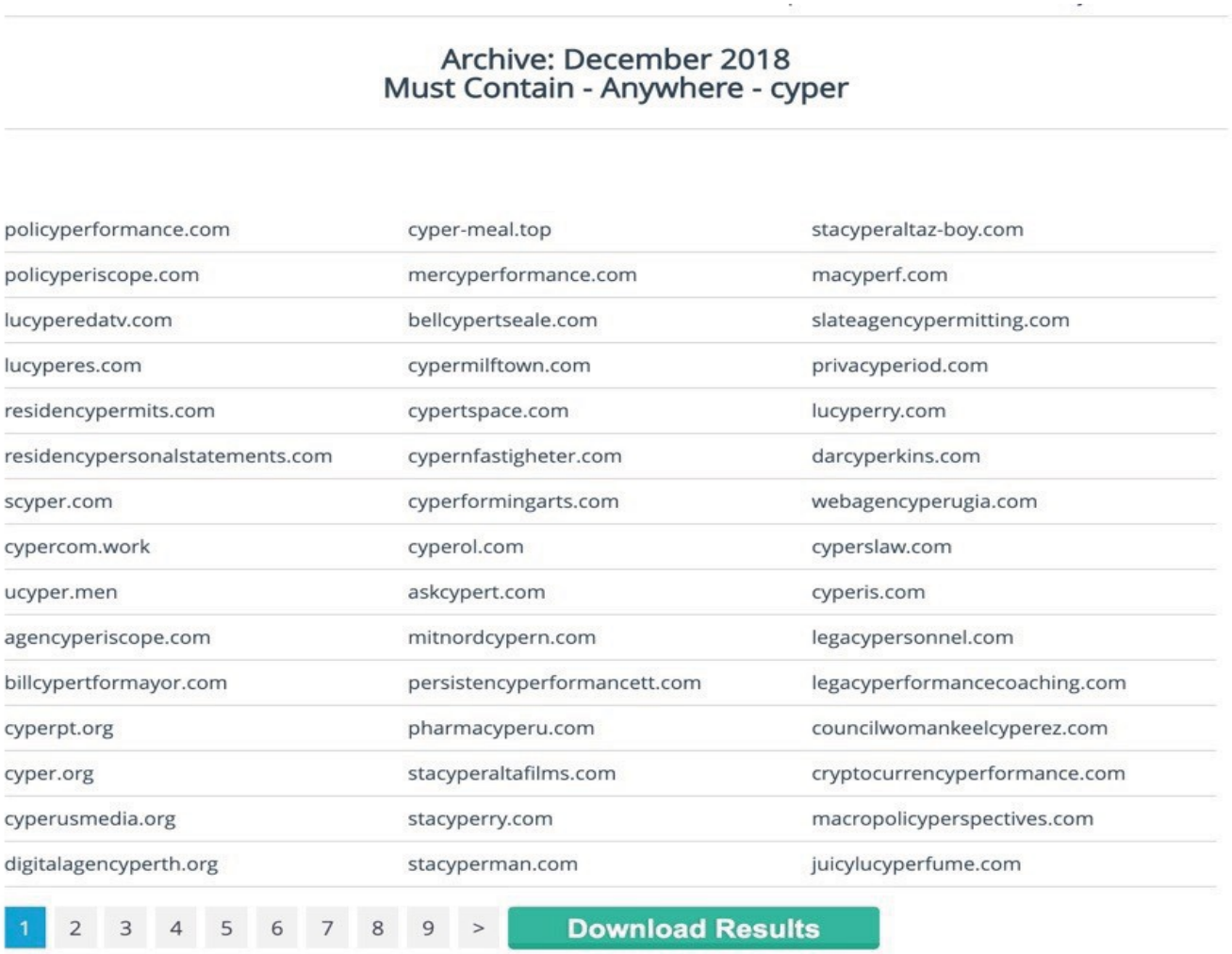


Рисунок 9.15

Стоит денег? Абсолютно

Whoisology - отличный сервис, который предоставляет доступный вариант доступа - значительный объем исторической доменной истории. Whoisology также предлагает богатые API-соединения со многими из ранее обсуждавшихся инструментов, таких как Intrigue. io, SpiderFoot и другие. Если вы ищете доступный вариант (или не хотите платить ежемесячную плату) или что-то, что легко подключается к существующему инструменты для максимально быстрых результатов, это может быть ваш путь. Whoisology работает по кредитам - это 5 долларов за отчет по домену, поэтому вы можете покупать только то, что вы потребность без ежемесячных накладных расходов. Это очень полезно при работе с такие инструменты, как «Интрига» - вы можете просто использовать / покупать кредиты по мере необходимости.

ДоменИнструменты

DomainTools (DT) может быть вашим универсальным магазином для всего, что связано с доменом, если вы готовы за это платить. Отличный инструмент очень легко может стать вашим «третьим рука », и для меня это один из таких инструментов. Если бы я расставлял приоритеты по важности и необходимость инструментов, обсуждаемых в этой книге, DomainTools абсолютно быть в моей тройке лучших.

Поиск домена

DomainTools предлагает свою собственную версию широкого поиска по ключевым словам. ругали ранее в этой главе. Кроме того, DT сообщит вам, зарегистрирован. На рисунке 9.16 показан начальный экран поиска домена DT.

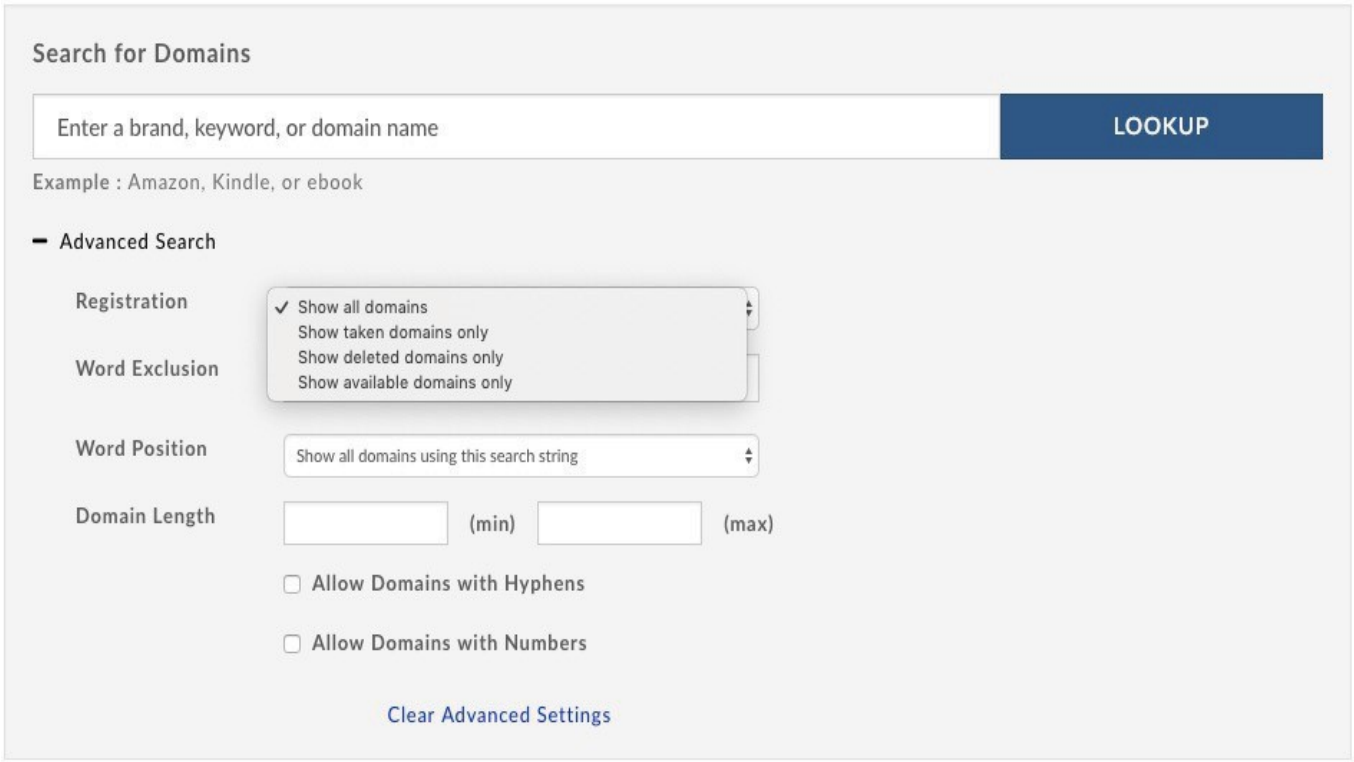


Рисунок 9.16

Массовый WHOIS

Массовый анализ WHOIS принимает список доменов через окно ввода текста и автоматически создает и загружает файл CSV, содержащий проанализированный WHOIS записи для этих доменов. Вы можете ввести до 2000 доменов одновременно, и вы может выполнять последовательные запросы до установленного месячного лимита запросов. Это полезная функция, если вам нужно получить результаты для нескольких доменов на один раз и в удобном, удобном для чтения формате CSV.

Обратный поиск IP

Здесь пригодится инструмент обратного поиска IP. Это экономит ваше время необходимости идти искать другое место, и исторические записи DT могут дать вам результаты, которые вы не можете найти с помощью другого инструмента. В качестве быстрого примера давайте посмотрим вверх 192.241.180.214, который является IP-адресом моего сайта. (См. Рисунок 9.17.) Из результатов, показанных на рис. 9.18, видно, что несколько доменов активны на этом IP-адресе. Это часто может быть огромной находкой, особенно когда поиск субъектов угрозы. Есть большая вероятность, что у актера будет несколько сайты размещены на одном сервере / IP-адресе.



Рисунок 9.17

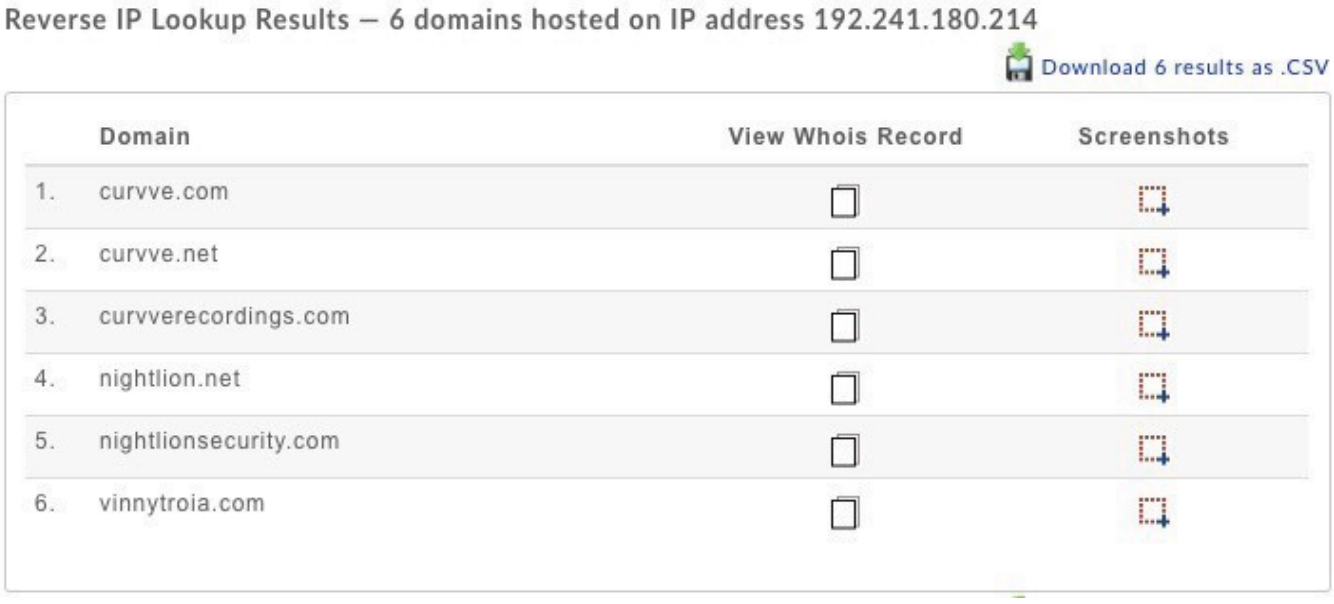
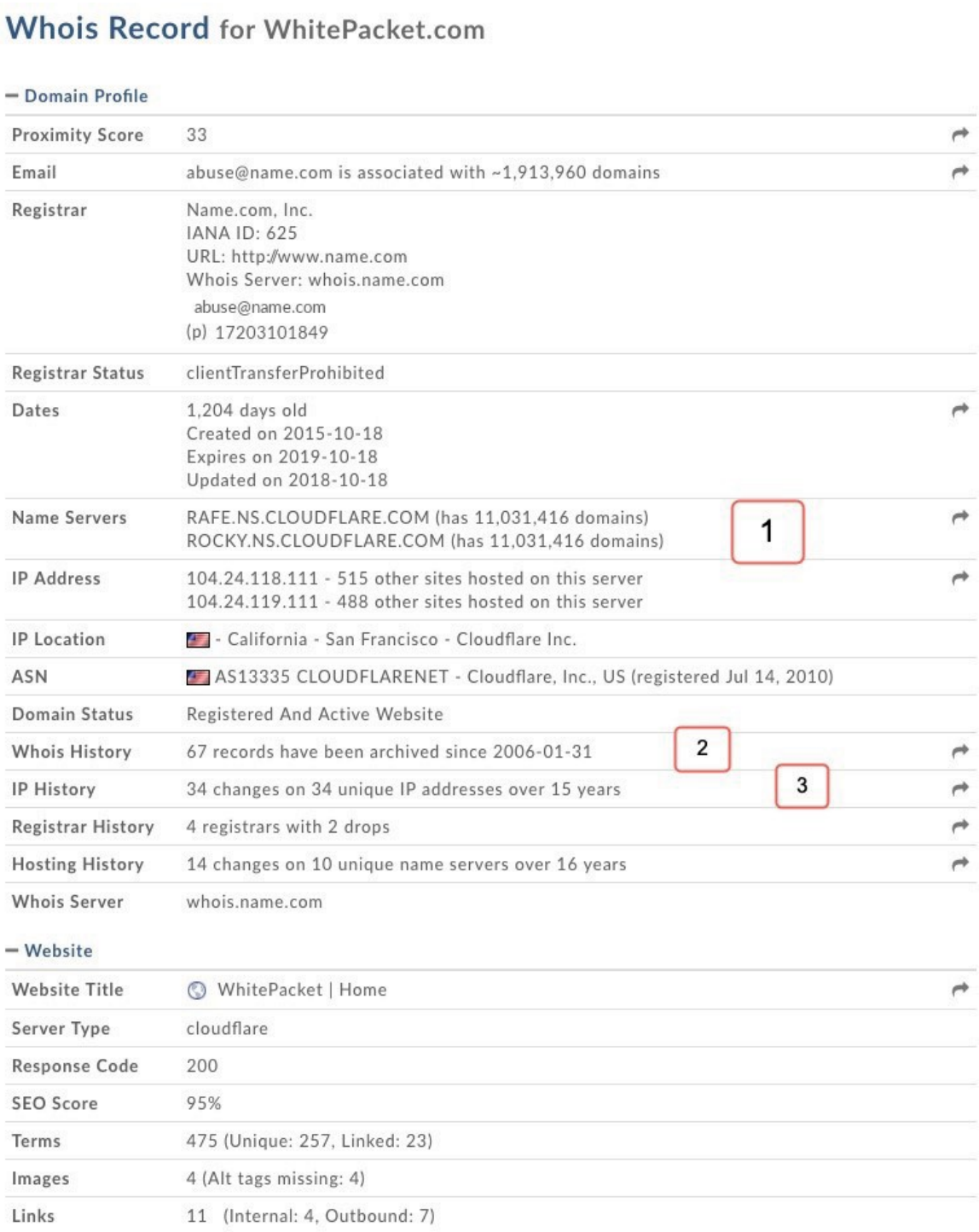


Рисунок 9.18

Отсюда вы можете нажать «Просмотреть запись Whois», чтобы просмотреть запись WHOIS для этот аккаунт.

Записи WHOIS о стероидах

Чтобы проиллюстрировать мощь DomainTools, давайте поищем наших собратьев по безопасности. исследователь WhitePacket. На рис. 9.19 показан первоначальный результат поиска в WHOIS. на WhitePacket.com .



Whois Record for WhitePacket.com

— Domain Profile

Proximity Score	33
Email	abuse@name.com is associated with ~1,913,960 domains
Registrar	Name.com, Inc. IANA ID: 625 URL: http://www.name.com Whois Server: whois.name.com abuse@name.com (p) 17203101849
Registrar Status	clientTransferProhibited
Dates	1,204 days old Created on 2015-10-18 Expires on 2019-10-18 Updated on 2018-10-18
Name Servers	RAFE.NS.CLOUDFLARE.COM (has 11,031,416 domains) ROCKY.NS.CLOUDFLARE.COM (has 11,031,416 domains)
IP Address	104.24.118.111 - 515 other sites hosted on this server 104.24.119.111 - 488 other sites hosted on this server
IP Location	- California - San Francisco - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET - Cloudflare, Inc., US (registered Jul 14, 2010)
Domain Status	Registered And Active Website
Whois History	67 records have been archived since 2006-01-31
IP History	34 changes on 34 unique IP addresses over 15 years
Registrar History	4 registrars with 2 drops
Hosting History	14 changes on 10 unique name servers over 16 years
Whois Server	whois.name.com

— Website

Website Title	WhitePacket | Home
Server Type	cloudflare
Response Code	200
SEO Score	95%
Terms	475 (Unique: 257, Linked: 23)
Images	4 (Alt tags missing: 4)
Links	11 (Internal: 4, Outbound: 7)

Рисунок 9.19

Здесь стоит упомянуть несколько вещей:

1. Сразу видно, что серверы имен находятся с Cloudflare. если ты
пытаются отследить веб-сайт до его фактического сервера, это может быть гигантский мертвый
конец, поскольку люди (и киберпреступники) часто маскируют свой веб-сайт за
DNS Cloudflare. Мы рассмотрим способы обойти это в следующих
глава (Прозрачность сертификата).
2. В DomainTools внесено 67 изменений в истории WHOIS с 2006 года, тогда как
Whoisology появился только в 2012 году.
3. За последние 15 лет к этому домену было привязано 34 уникальных IP-адреса.

По мере того, как наше расследование продолжается, поиск хостинг-провайдера или сервера
прикрепленный к домену, может быть важным, если мы пытаемся отследить
фактическое местонахождение IP.

Второй столбец информации, отображаемый на странице DomainTools, про-
открывает путь к расширению этих поисков (рис. 9.20).



Рисунок 9.20.

Сразу видно, что DT предоставляет историю скриншотов. Это будет
актуально, поскольку мы отслеживаем различных владельцев через историю WHOIS. Другой
у владельцев будут разные веб-сайты, и разные веб-сайты будут предлагать разные
подсказки.

Это огромная экономия времени, поэтому нам не нужно копаться в Wayback / Archive.
org (о чем мы поговорим в следующей главе).

История WHOIS

Глядя на историю WHOIS для WhitePacket.com , мы можем увидеть (маленьким глазом
на рисунке 9.21), что регистрационная информация стала частной
18 октября 2015 г. Именно здесь исторические данные становятся решающим фактором.
в потенциальном расследовании. Имея доступ к источнику данных, который может показать нам
кому принадлежала регистрация до *того,* как регистрация стала частной, может быть
монументальное открытие. Следующие шаги - вернуться как можно дальше назад.
попытаться определить собственника. Если это не сработает, мы можем использовать другую тактику, чтобы
определить владельца сайта.

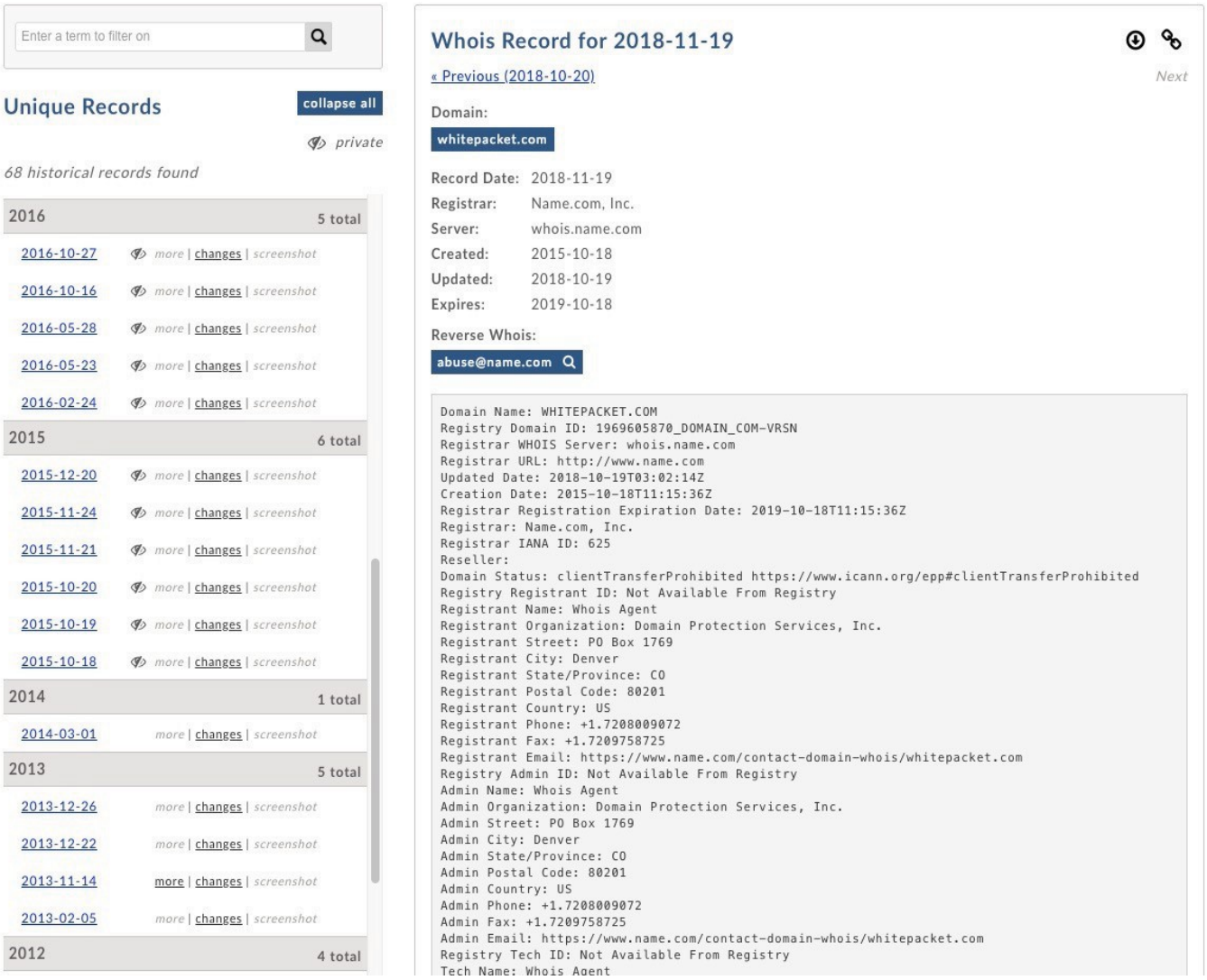


Рисунок 9.21

Сила скриншотов

В качестве гипотезы, допустим, нас интересовали только доменные действия WhitePacket.com по 2005 год В данном конкретном случае мы *можем* увидеть Регистрационные данные этого года, но давайте *делать вид* , что это не так , и регистрация является частной. Мы бы были на берегу Шиттс-Крик, верно?

Вот почему стоит посмотреть исторические данные веб-сайта. Вы никогда не знаете, что подсказки вы найдете в архивах. В случае с DomainTools он за-предоставляет вам скриншоты сайта, так что вам не придется копаться дальше.

Они говорят, что картинка стоит тысячи слов. В этом случае стоит как минимум два: имя и фамилия владельца сайта в 2005 году, написанные прямо на страницу (рисунок 9.22).

Это прекрасный пример того, почему Wayback Machine (Archive.org) является важный инструмент для расследования (который мы рассмотрим более подробно в следующих глава). На данный момент функция скриншота DomainTools дала нам владельца сайта WhitePacket.com около 9 июня 2005 г.

Копаться в истории WHOIS

Пример скриншота был чрезвычайно удачным. Скорее всего, вы не найдете Ответ настолько очевиден, что имя владельца буквально написано на сайте.

Тем не менее, оглядываясь назад, можно получить много очень полезной информации. в исторические данные WHOIS домена. Продолжим изучение WhitePacket. com, чтобы понять, почему.

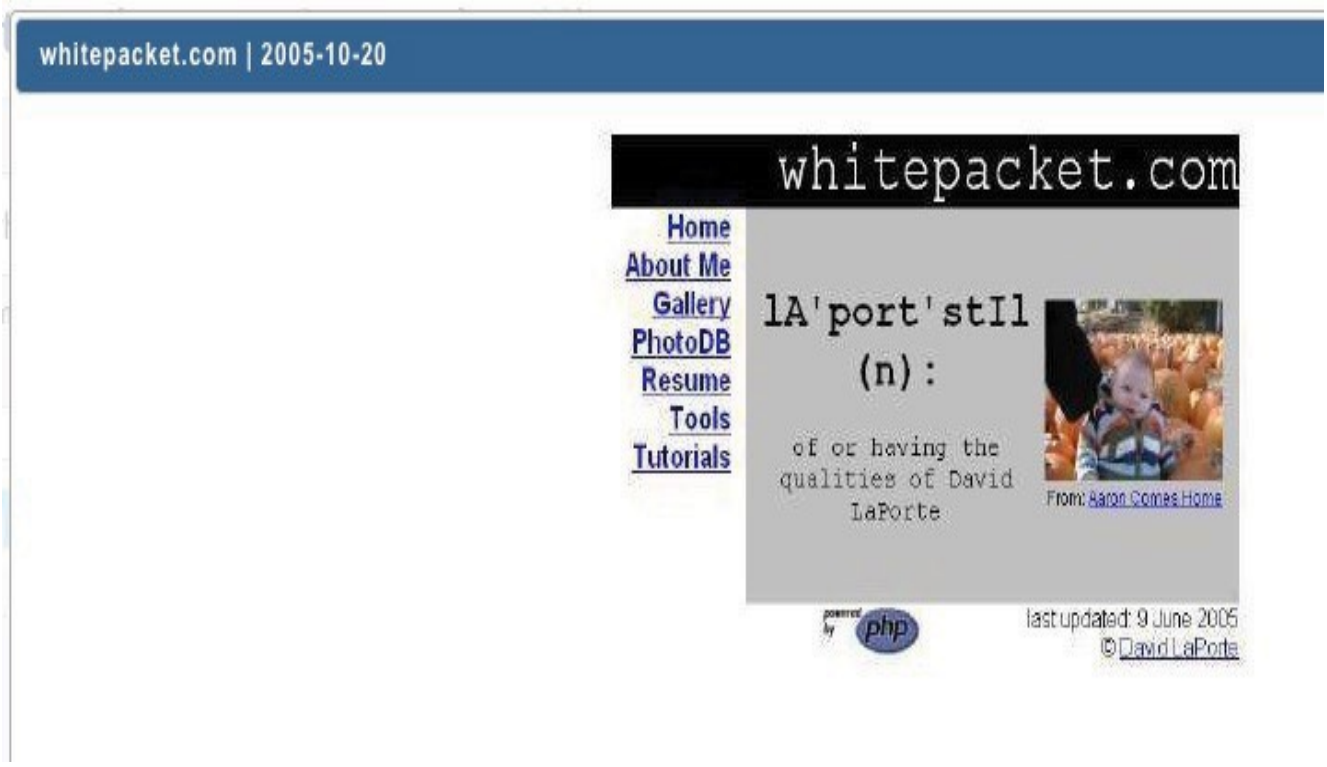


Рисунок 9.22

Ищете изменения в собственности

В предыдущем примере мы видели, что большинство записей WHOIS
заблокирован при частной регистрации (Рисунок 9.23).
Просматривая исторический список, мы видим, что последняя негосударственная регистрация
Данные по домену были доступны 1 марта 2014 г. (рис. 9.24).

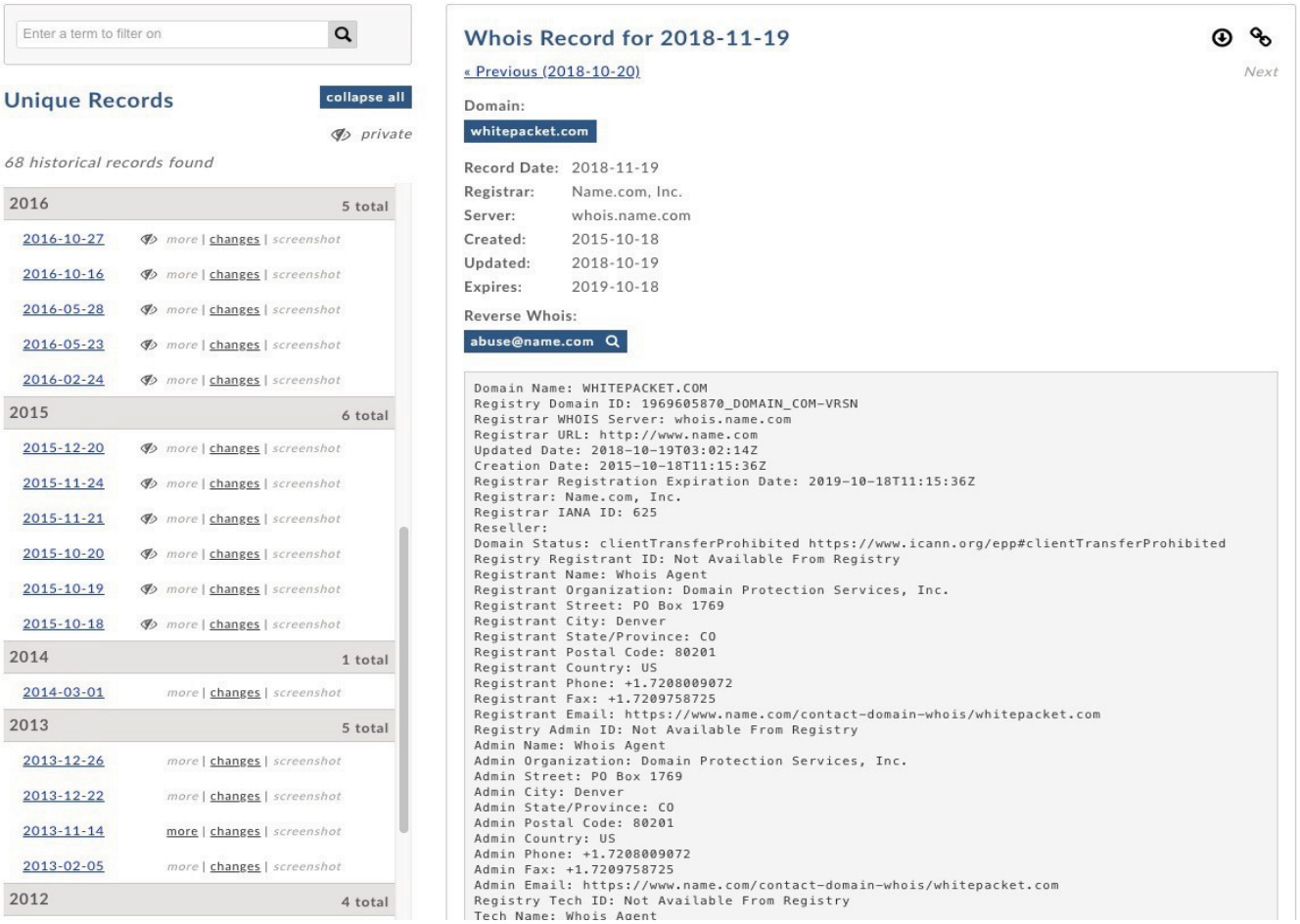


Рисунок 9.23



Рисунок 9.24

Напоминаем, что все имена, адреса, номера телефонов и электронные письма будут (в основном) изменены в примерах. Если вы пытаетесь это сделать дома, ваш результаты могут быть разными.

Мы видим огромный промежуток времени (более года) между тем, когда домен регистрация была открыта 1 марта 2014 г., а когда 18 октября она стала частной, 2015. Это потенциально может указывать на смену собственника, возможно, через истечение срока владения (т. е. истек срок действия домена). Это то, что мы можем (и следует) подтвердить.

После того, как мы щелкнем по результату домена 2014 г., на рис. 9.25 показано, что домен принадлежал Джонни Фрэмперсону из 178 Westbury Court, Лондон, Англия.

Посмотрев на поле «Статус домена», мы увидим, что домен находился в «REDEMPTIONPERIOD», что означает, что Джонни позволил домену истечь примерно этот раз. Это означает, что нынешний владелец WhitePacket.com , вероятно, не тот тот же человек, который владел им в 2014 году.

Хотя технически возможно, что владелец 2014 г. мог позволить домену срок действия истекает, а затем приобрел его резервную копию в 2015 году со статусом частной регистрации, этот сценарий кажется маловероятным.

Однако об этом следует помнить. Много причин существуют для того, почему кто-то может позволить домену истечь, а затем снова купить его используя приватную регистрацию. Например, возможно, этот злоумышленник настолько умен, что он знал, что хочет использовать домен в злонамеренных целях, и ожидал это тип будущего расследования. Опять же, маловероятно, но мало ли.

```
Domain Name: WHITEPACKET.COM
Registry Domain ID:
Registrar WHOIS Server: whois.freeparking.co.uk
Registrar URL:
Updated Date: 05-Feb-2014
Creation Date: 25-Dec-2011
Registrar Registration Expiration Date: 25-Dec-2013
Registrar: Freeparking Domain Registrars Inc
Registrar IANA ID: 837
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: REDEMPTIONPERIOD
Registry Registrant ID: DI_20004243
Registrant Name: Domain Contact (428946)
Registrant Organization: Johnny Framperson
Registrant Street: 178 Westbury Court
Registrant City: London
Registrant State/Province: England
Registrant Postal Code: EH16 6RU
Registrant Country: GB
Registrant Phone: +44.3456789123
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: johnnyboy@fakemail.com
Registry Admin ID: DI_20004244
```

Рисунок 9.25

Обратный WHOIS

Теперь у нас есть несколько новых сведений о возможном владельце
WhitePacket.com датируется 2014 годом. Именно здесь выполняется обратный поиск WHOIS
может вступить в игру. Система обратного поиска WHOIS позволяет нам искать домен
право собственности (в обратном порядке) путем поиска имени человека, номера телефона компании,
физический адрес или адрес электронной почты. Результатом вашего поиска будет список
доменные имена, в записях WHOIS которых есть ваш поисковый запрос.
На рис. 9.26 показано окно обратного поиска WHOIS DomainTools.
Посмотрим, сможем ли мы найти дополнительные домены, принадлежащие нашему новому лидеру,
Джонни Фрэмперсон. На рисунке 9.27 показаны результаты поиска WHOIS.
запись, содержащая «все слова» Джонни и Фрамперсон.
Результаты вернулись с тремя активными доменами (которые мы не можем вам показать,
извиняюсь!). Неплохая находка! Теперь у нас есть три новых и *активных* домена, которые также принадлежат
пользователя Mr. Framperson. Результаты по умолчанию покажут нам только те домены, которые
активен *и* принадлежит человеку, указанному в нашем поисковом запросе.
Это здорово, но заметили ли вы ссылку в правом столбце на рис. 9.27.
с надписью «Добавьте историю и получите:»? Это добавит любые ранее принадлежавшие домены
им тоже! На рис. 9.28 показаны новые результаты, когда мы щелкаем эту ссылку.

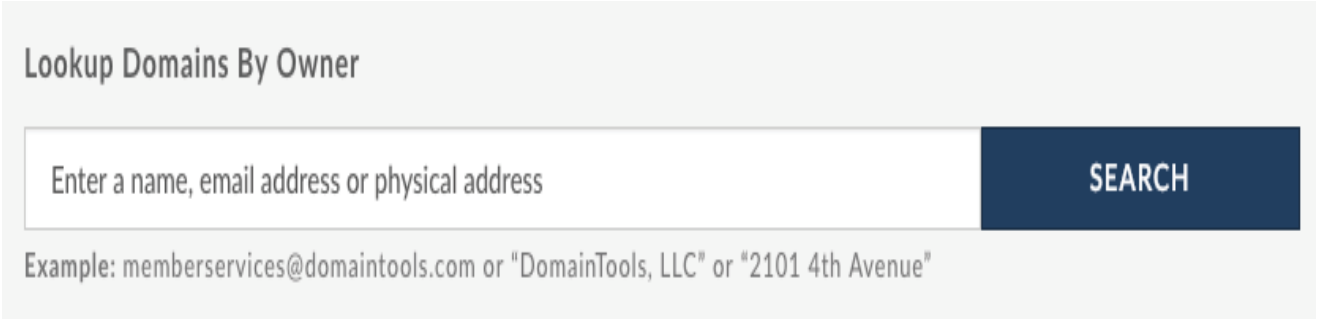


Рисунок 9.26

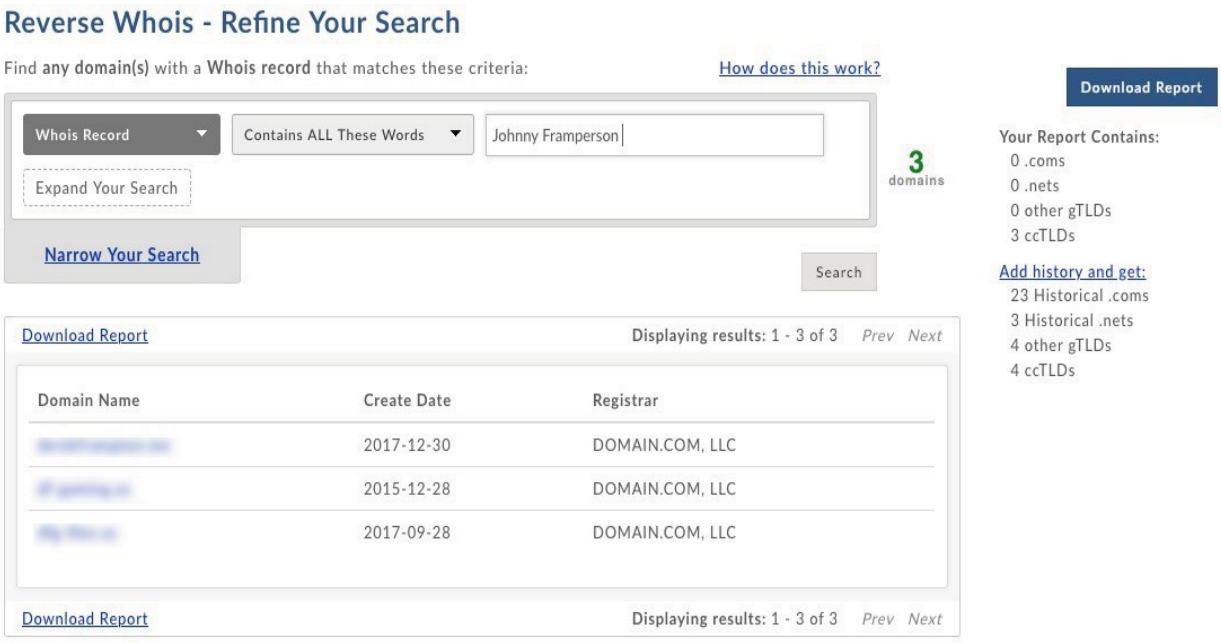


Рисунок 9.27

Бум! Теперь у нас есть 37 доменов, ранее принадлежавших этому человеку. Это
много. Я надеюсь, что вы ведете хорошие записи и хорошую систему отслеживания, потому что это
будет означать много дополнительных исследований касательных, чтобы найти больше подсказок! Мы будем
исследуем некоторые из этих областей более подробно в следующей главе.

Перекрестная проверка *всей* информации

Не могу сказать, сколько раз я забывал это сделать. Это требует дисциплины
и огромная организованность. Если вы расследуете злоумышленника,
переходя в этот режим документирования и хранения всех подсказок в организованном
система быстро окупится.
Помните, что большинство (если не все) злоумышленники имеют несколько псевдонимов и персон.
Когда вы начнете разбираться в сорняках, исследуя конкретный псевдоним, вы будете
скорее всего, вы забудете подсказки, которые вы нашли где-то еще. Хорошая система документации-
тация решит эту дилемму. Позвольте мне показать вам, что я имею в виду.
Когда мы искали имя Джонни Фрамперсона, мы нашли 37 других доменов
что он либо в настоящее время владеет, либо владел в какой-то момент. Угрожающие субъекты редко
используют свое собственное имя, но есть большая вероятность, что они будут повторно использовать другие части
такой информации, как адрес, номер телефона или адрес электронной почты. Проиллюстрировать

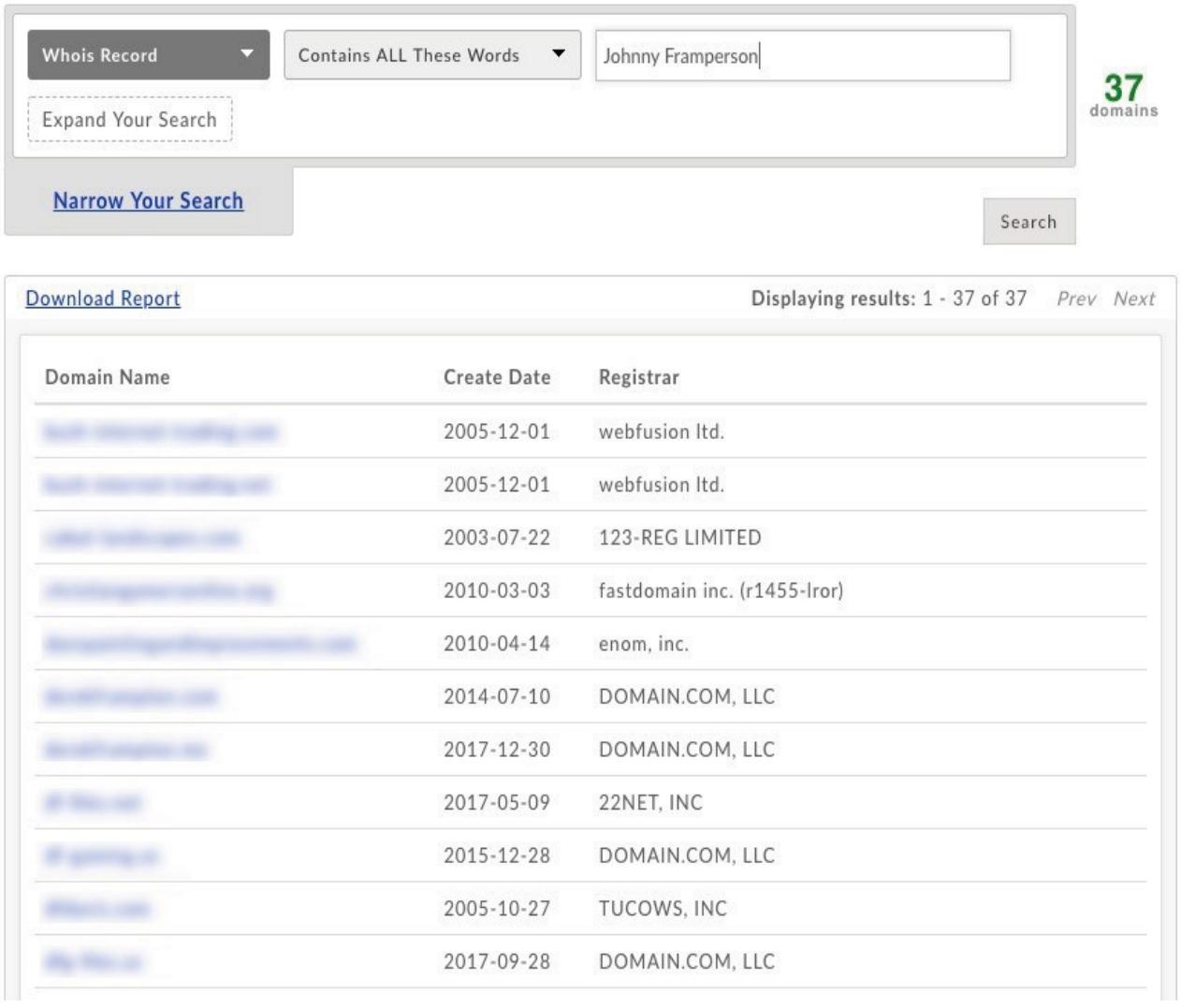


Рисунок 9.28

С моей точки зрения, на рис. 9.29 показаны результаты обратного поиска в WHOIS для Джонни.
Адрес электронной почты Фрамперсона, johnnyboy@iMadeThisUp.com.
Поскольку наши результаты поиска упали с 37 до 2, мы можем сделать вывод, что наш
target использует разные адреса электронной почты для регистрации домена. В рамках нормального
расследования, нам нужно будет просмотреть каждый из других доменов, чтобы
узнайте, какой адрес (а) электронной почты он использует. Когда они у нас есть, мы их документируем,
и выполните дополнительные поиски, чтобы найти дополнительные домены, которые потенциально могут быть
зарегистрированы под теми адресами электронной почты, которые мы могли пропустить. Как видите,
Весь процесс может быстро превратиться в одну гигантскую кроличью нору.

Это когда действительно пригодится инструмент сопоставления разума. если ты
у меня нет метода записи и расширения каждого из этих маршрутов, я очень
Предлагаю изучить инструмент составления карт разума. Доступно много. Mindnode отличный
инструмент для пользователей Mac. Если вы предпочитаете онлайн-приложение, вам подойдут и Coggle.it, и Lucidchart.
У вас так много выбора. Просто выберите что-нибудь, потому что писать все
вниз в OneNote, вероятно, не собирается его сокращать.
Я могу гарантировать, что вы потеряете информацию или пропустите важные
подсказки - потому что у меня есть. Много раз. Избавьте себя от боли возвращаться и заново
исследовать точки данных и выработать привычку правильно документировать вещи из
Начните. И делать скриншоты ***всего*** **(еще один урок, который мне пришлось выучить на собственном горьком опыте).**

Возвращаясь к нашему поиску, давайте вернемся и запустим обратный поиск WHOIS на
178 Westbury Court, почтовый адрес, указанный в реестре
Детали настройки для WhitePacket.com . На рисунке 9.30 показаны результаты обратного преобразования.
адресный поиск.
И посмотрите на это! Мы только что обнаружили дополнительное доменное имя, которое
не появлялись ни в одном из наших предыдущих поисков. Посмотрите, как это работает? Это много
перекрестной проверки фактов и данных, но это окупается!
Что еще более важно, мы видим очевидную силу возможности обыскать его-
исторические архивы WHOIS. Мы углубимся в эту тему в следующей главе.

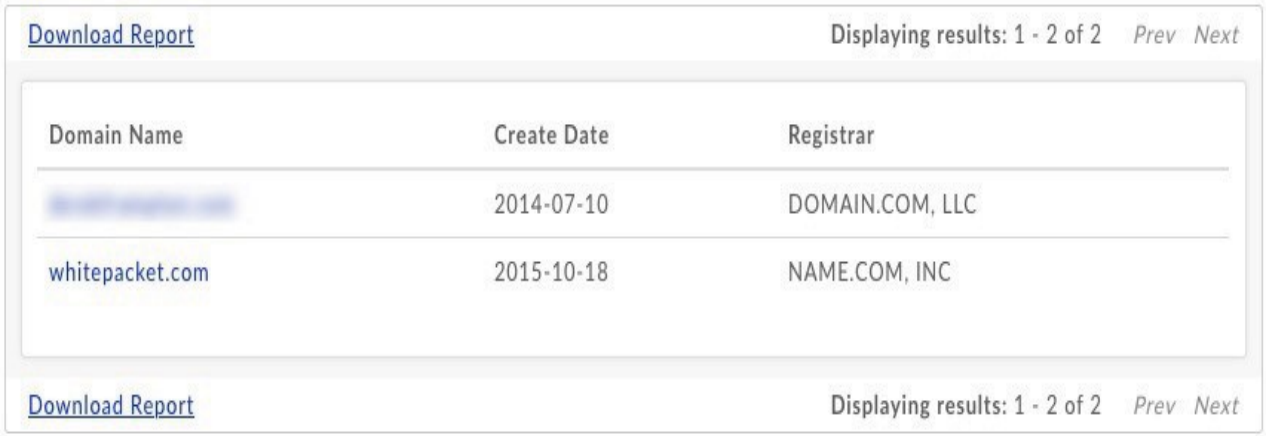


Рисунок 9.29

Резюме

В этой главе были рассмотрены основы поиска в WHOIS, включая несколько бесплатных
и услуги премиум-класса, которые можно использовать для определения владения доменом. Не все
услуги созданы равными, и это одна из областей, где вы, скорее всего, закончите
до необходимости тратить деньги, чтобы найти наилучшие результаты. К сожалению, нет
отличные инструменты или решения для запроса бесплатных исторических данных WHOIS, а также
назад вы хотите искать, тем больше вам будет стоить услуга.
В этой главе также рассматривается использование этих инструментов для выполнения обратных запросов WHOIS.
это может позволить нам найти дополнительные ключи к разгадке прав собственности на домен, которые могут
в конечном итоге приведет вас к полной атрибуции владельца. Whoisology.com - отличный недорогой
исторический инструмент поиска доменов, взимающий всего 5 долларов за отчет. С другой стороны,
DomainTools предлагает более премиальный сервис со значительно лучшими (и более
полные) исторические записи по гораздо более высокой цене.
В следующей главе мы рассмотрим использование журналов прозрачности сертификатов для идентификации
tify владельцев доменов, используя интернет-архивы, такие как Wayback Machine.



Рисунок 9.30

201

10

В этой главе мы сосредоточимся на двух основных темах: Сертификат Transparency и Интернет-архивы (например, Wayback Machine и кеши поисковых систем). Мы рассмотрим, как все они могут быть использованы для дальнейшего исследования сайта владелец, используя данные WHOIS или имея возможность просматривать и ссылаться на старые копии сайта.

Сертификат прозрачности

Certificate Transparency (CT) - это проект с открытым исходным кодом под руководством Google, направленный на обеспечение
аудит и мониторинг сертификатов серверов TLS / SSL, выданных Certificate
Власти (CA). Общая идея CT - снизить угрозу злонамеренного
хакеры, выдающие себя за веб-сайт (например, человек посередине [MITM] или фишинг
атаки) из-за использования украденных или поддельных SSL-сертификатов.
До прозрачности сертификата всякий раз, когда пользователь посещал веб-сайт, используя
поддельный сертификат SSL, сайт казался «нормальным» для веб-браузера, который
невозможно определить, действителен ли сертификат SSL (или сгенерирован
правильная партия).
В одном случае известный голландский центр сертификации (DigiNotar) был компромиссным.
mised, позволяя хакерам использовать свои системы для создания поддельных сертификатов SSL.
Эти сертификаты использовались для выдачи себя за ряд сайтов, включая Gmail.

Прозрачность сертификата и Интернет-архивы

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

и Facebook. Поскольку фишинговые сайты выглядели законными, атаки MITM
были успешными, что позволило хакерам шпионить за пользователями и красть их информацию.

**Атака «злоумышленник посередине» происходит, когда хакер может перехватить трафик.
между жертвой и их целевым веб-сайтом. Например, если кто-то
настроить поддельную точку доступа Wi-Fi в местном кафе. Люди подключаются к «бесплатному Wi-Fi»
точка доступа (иногда автоматически), не осознавая, что она принадлежит человеку в
в задней части магазина. Теперь, когда жертва общается с веб-сайтом, весь трафик
проходит через хакерскую точку доступа Wi-Fi. Теоретически хакер может прочитать все
трафик, что означает, что они могут украсть информацию о кредитной карте, личные данные, пароль
слова и т. д.**

В этих сценариях веб-браузеры не видят ничего плохого в сертификате.
потому что CA, похоже, имеет хорошую репутацию. Это дает пользователям впечатление
Если они посещают настоящий веб-сайт, то на самом деле их атакуют фишингом.
Чтобы уменьшить эту угрозу, Google учредил проект CT в 2015 году. С тех пор
всем четырем основным браузерам - Chrome, Firefox, Opera и Safari - требуются веб-сайты.
иметь сертификаты с отметками времени подписанных сертификатов (SCT), что доказывает, что
сертификат внесен в журнал. Если веб-сайт, который вы пытаетесь посетить
не имеет SCT, браузеры предупредят вас, что это может быть потенциально
ненадежный.

Какое отношение это имеет к цифровым расследованиям?

Поскольку проект CT делает сертификаты общедоступными, любой, кто заинтересован в
зная о конкретном домене, можно просто открыть его в браузере и просмотреть
Справочная информация. Поскольку эта общедоступная информация включает
информация о владельце (как правило, о человеке или организации),
любой, кто имеет доступ к сертификату, может не только проверить владельца сертификата,
но *также может просматривать другие сайты, используя тот же сертификат* .
Когда вы рассматриваете этот момент с точки зрения подстановочных сертификатов
(которые позволяют сертифицировать любой субдомен с помощью одного сертификата) или сайты, которые
обмениваться сертификатами на нескольких веб-сайтах, это может быть очень важным способом
исследуйте существование других сайтов.
Многие инструменты, обсуждаемые в предыдущих главах, имеют встроенную интеграцию.
использовать прозрачность сертификата для поиска поддоменов и связанных доменов.
Вы можете использовать их, если хотите. Остальная часть этой главы покажет вам, как
используйте инструменты, специально разработанные для поиска в журналах CT. Давайте копаться.

Скаутинг с CTFR

CTFR - это инструмент командной строки с открытым исходным кодом, который позволяет идентифицировать
вспомогательные
домены в определенном домене путем доступа к журналам прозрачности сертификатов.

Вы можете скачать CTFR по адресу https://github.com/UnaPibaGeek/ctfr .

CTFR прочитает общедоступные журналы прозрачности сертификатов, чтобы: 1) идентифицировать владельца SSL-сертификат используется на www.facebook.com и 2) посмотреть, какие еще поддомены также используют тот же сертификат SSL.

Использовать CTFR для поиска связанных поддоменов очень просто. Просто выполните файл Python и добавьте целевой домен. В нашем примере мы собираемся ищите поддомены Facebook.com :

```
корень @ OSINT: python ctfr.py -d facebook.com

____ _____ _____ ____
/ ___| _ _| ___| _ \
| |  | |_| | |_) |
| |___ | | |  _ <
\____||_| |_| |_| \_\
Версия 1.2 - Эй, не пропустите AXFR!
Сделано Шейлой А. Берта (UnaPibaGeek)
[!] ---- ЦЕЛЬ: facebook.com ---- [!]
[-] * .adtools.facebook.com
[-] * .ak.facebook.com
[-] * .alpha.facebook.com
[-] * .assistant.facebook.com
[-] * .beta.facebook.com
[-] * .channel.facebook.com
[-] * .cinyour.facebook.com
[-] * .connect.facebook.com
[-] * .cstools.facebook.com
[-] * .ctscan.facebook.com
[-] * .dev.facebook.com
[-] * .dns.facebook.com
[-] * .extern.facebook.com
[-] * .extools.facebook.com
[-] * .facebook.com
[-] * .fb.alpha.facebook.com
[-] * .fb.beta.facebook.com
[-] * .fb.m.alpha.facebook.com
[-] * .fb.m.beta.facebook.com
[оставшиеся 200+ субдоменов усечены]
[!] Выполнено. Хорошего дня! ;).
```

С помощью одного простого сканирования мы выявили более 200 поддоменов, связанных с Facebook.com .

Легко, правда? Поскольку это только первый шаг в OSINT-процессе, давайте сохраним
результаты нашего сканирования в файл:

```
корень @ OSINT: python ctfr.py -d facebook.com -o subdomains.txt
```

Использование прозрачности сертификата дает нам новый способ поиска поддоменов
без брутфорса и даже обхода сайта. Это совершенно незаметно.

Что мы сделали, так это посмотрели журналы прозрачности сертификатов домена, которые
нам другие поддомены, использующие тот же общий SSL-сертификат.

Круто, правда? Теперь давайте применим это не только к субдоменам.

Crt.sh

Crt.sh (www.crt.sh), разработанный Sectigo, представляет собой поиск в журнале прозрачности сертификатов.
двигатель. По мере выпуска новых сертификатов SSL журналы прозрачности сертификатов будут
в конечном итоге (обычно в течение нескольких часов) они попадают в поисковую систему crt.sh
двигатель. Вы можете не только искать активные сертификаты, но и crt.sh также позволяет
вы можете увидеть неактивные, отозванные или просроченные сертификаты.

Функция поиска невероятно проста. Просто введите поисковый запрос в
поисковая строка. Вы можете искать доменное имя, общее имя, организацию
имя или хеш SHA.

Чтобы просмотреть журналы сертификатов для моего личного веб-сайта, просто введите мой домен
имя и поиск (рисунок 10.1).

Результаты вашего поиска будут выглядеть примерно так, как показано на рисунке 10.2.

Каждый идентификатор crt.sh представляет собой моментальный снимок сертификата, используемого на определенный
момент времени.

целевой веб-сайт. Щелчок по идентификатору crt.sh расширит детали конкретного
сертификат, как показано на рисунке 10.3.

CT в действии: Обходной Cloudflare

Что, если исторические данные WHOIS никуда вас не приведут, и вы ищете
для нескольких дополнительных подсказок относительно того, кто может быть владельцем домена?

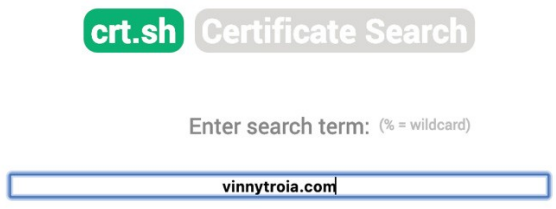


Рисунок 10.1.

crt.sh ID	Logged At	Not Before	Not After	Issu
1173587075	2019-02-03	2019-02-03	2019-05-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1167310269	2019-02-03	2019-02-03	2019-05-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1004501604	2018-12-05	2018-12-05	2019-03-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1004501033	2018-12-05	2018-12-05	2019-03-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
830463037	2018-10-06	2018-10-06	2019-01-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
830538627	2018-10-06	2018-10-06	2019-01-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
830218563	2018-10-06	2018-10-06	2019-01-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
830218452	2018-10-06	2018-10-06	2019-01-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
830218025	2018-10-06	2018-10-06	2019-01-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
830249334	2018-10-06	2018-10-06	2019-01-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
826981964	2018-10-06	2018-10-06	2019-01-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
826976273	2018-10-06	2018-10-06	2019-01-04	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
11762189	2015-12-31	2015-12-30	2016-07-03	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA L
10901189	2015-11-26	2015-11-24	2016-05-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA L
10704875	2015-11-15	2015-11-13	2016-05-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA L
10418131	2015-10-31	2015-10-29	2016-04-24	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA L
10399742	2015-10-30	2015-10-29	2016-04-24	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA L
10237720	2015-10-20	2015-10-18	2015-12-30	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA L

Рисунок 10.2.

crt.sh ID	10901189
Summary	Leaf certificate
Certificate Transparency	Timestamp: 2015-11-26 16:54:58 UTC, Entry #: 10021915, Log Operator: Google, Log URL: https://ct.googleapis.com/aviator 2015-11-26 21:53:19 UTC, 10783032, Google, https://ct.googleapis.com/pilot 2015-11-28 09:40:03 UTC, 8108514, Google, https://ct.googleapis.com/rocketeer 2017-04-29 03:22:12 UTC, 7131970, Let's Encrypt, https://clicky.ct.letsencrypt.org
Revocation Report a problem with this certificate to the CA	Mechanism / Provider / Status / Revocation Date / Last Observed in CRL / Last Checked (Error) OCSP / The CA / Check / ? / n/a / ? CRL / The CA / Not Revoked / n/a / n/a / 2019-02-11 04:52:42 UTC CRLSet/Blacklist / Google / Not Revoked / n/a / n/a / n/a disallowedcert.stl / Microsoft / Not Revoked / n/a / n/a / n/a OneCRL / Mozilla / Not Revoked / n/a / n/a / n/a
SHA-256(Certificate)	41FB09C5BEBCD0EC3B6EB690D10F0A61E27141FE9814C6D42DBFA31E9B02C15C
SHA-1(Certificate)	FD7CB1FB8CEBC7695A7C944F978F322A747A37B8
Certificate | ASN.1 Hide metadata Run cablint Run x509lint Run zlint Download Certificate: PEM	Certificate: Data: Version: 3 (0x2) Serial Number: 48:82:38:81:e9:9a:17:dd:ef:85:d0:a0:9b:2d:3f:85 Signature Algorithm: ecdsa-with-SHA256 Issuer: (CA ID: 1582) commonName = COMODO ECC Domain Validation Secure Server CA 2 organizationName = COMODO CA Limited localityName = Salford stateOrProvinceName = Greater Manchester countryName = GB Validity Not Before: Nov 24 00:00:00 2015 GMT Not After : May 7 23:59:59 2016 GMT Subject: commonName = sni68313.cloudflaressl.com organizationalUnitName = PositiveSSL Multi-Domain organizationalUnitName = Domain Control Validated Subject Public Key Info: Public Key Algorithm: id-ecPublicKey Public-Key: (256 bit) pub: 04:9e:77:88:44:70:12:3d:44:42:17:7e:6a:d8:51:

Рисунок 10.3.

Для этого примера давайте вернемся к нашему другу WhitePacket. Домен www
.whitepacket.com поддерживает конфиденциальность, начиная с 2015 г. (предположительно
когда текущий владелец домена стал владельцем домена). В этом случае
исторические данные WHOIS не помогают, но, глядя на данные, мы можем увидеть
что DNS домена использует Cloudflare.
DNS Cloudflare предоставляет механизм для маскировки истинного IP-адреса сервера,
что чрезвычайно затрудняет расследование. Одна вещь, которая мне также нравится в Облаке -
flare заключается в том, что он предоставляет общий SSL-сертификат, который вы можете использовать для *всех*
доменов.в вашем аккаунте. Видишь, к чему я с этим собираюсь?
Используя www.crt.sh , давайте исследуем прозрачность сертификата WhitePacket.com.
журналы, показанные на рисунке 10.4.
Щелкнув один из идентификаторов crt.sh, вы получите ту же информацию, которую мы видели ранее.
На этот раз прокрутите вниз до раздела «Альтернативное имя субъекта», и вы сможете увидеть разницу:

Сертификат:
Данные:
Версия: 3 (0x2)
Серийный номер:
83: 23: 1a: 8d: 16: 53: 53: 8d: 5f: 73: a9: 92: a0: 3e: bf: 8c
Алгоритм подписи: ecdsa-with-SHA256
Эмитент: (CA ID: 1582)
распространенное имя
= Проверка домена COMODO ECC
Безопасный сервер CA 2
Название организации
= COMODO CA Limited
localityName
= Салфорд
stateOrProvinceName = Большой Манчестер
название страны
= ГБ
[результаты усечены]
Доступ к информации о полномочиях:
Эмитенты ЦС - URI: http: //crt.comodoca4.com/
COMODOECCDomainValidationSecureServerCA2.crt
X509v3 Альтернативное имя субъекта:
DNS: sni230260.cloudflaressl.com
DNS: *. 4origines.com
DNS: *. Agilerioseguros.com.br

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1156176397	2019-01-29	2019-01-29	2019-08-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
1156175635	2019-01-29	2019-01-29	2019-08-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
1150013489	2019-01-28	2019-01-28	2019-08-06	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
1150013428	2019-01-28	2019-01-28	2019-08-06	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
1042699302	2018-12-19	2018-12-19	2019-06-27	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
1042698603	2018-12-19	2018-12-19	2019-06-27	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
959052596	2018-11-19	2018-11-19	2019-05-28	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
959052215	2018-11-19	2018-11-19	2019-05-28	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
907562447	2018-10-31	2018-10-31	2019-05-09	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2

Рисунок 10.4.

DNS: *. Ardyssv.gq
DNS: *. Ayrescorretora.com.br
DNS: *. Bleudecode.com
DNS: *. Bolnichnye-listi.com
DNS: *. Booksport1.cf
DNS: *. Cabinpaintingrefinishing.com
DNS: *. Colombia-sexo.tk
DNS: *. Donji-vakuf.tk
DNS: *. Ebooksfree911.cf
DNS: *. Galileiaseguros.com.br
DNS: *. Girlsmakeup.tk
DNS: *. Guessmantra.ga
DNS: *. Homespaces.com
DNS: *. Instapics.bid
DNS: *. Instapics.party
DNS: *. Jand.tk
DNS: *. Meettabernacle.com
DNS: *. Memoriaseguros.com.br
DNS: *. Mindbendingbeats.ca
DNS: *. Naysathseguros.com.br
DNS: *. Og.money
DNS: *. Originsgranite.com
DNS: *. Palwalonline.in
DNS: *. Peterkomorowski.com
DNS: *. Phpturtle.com
DNS: *. Reenuu.com
DNS: *. Satanism.ca
DNS: *. Seguros6k.com.br
DNS: *. Spravka-moscow177.ru
DNS: *. Tagbook-s.cf
DNS: *. Toolzdepot.com
DNS: *. Whitepacket.com

У нас есть буквально множество доменов, которые используют один и тот же сертификат SSL. как WhitePacket.com . В *лучшем случае* это выявит домены, все часть той же учетной записи Cloudflare. Это не обязательно означает, что все одного владельца, просто все они используют одну и ту же учетную запись Cloudflare.

Я связался с кем-то из следственной группы Cloudflare по поводу использования сертификатов tificates, чтобы найти владельцев связанных доменов. Они ответили: «В подавляющем большинстве случаев, когда полностью несвязанные домены группируются вместе на общем TLS SNI сертификаты ».
Принято к сведению! Как и все, что связано с OSINT, это еще один метод, который вы можете использовать чтобы получить больше подсказок по мере того, как вы спускаетесь по кроличьей норе информации. В нашем тестовом примере информация оказалась верной. Однако важно отметить, что Cloudflare указал, что это может быть не всегда так. Действуйте осторожно.

Тестирование большего количества целей

По мнению Cloudflare, возможно, эти домены не связаны. Я случайно знаю
из разговоров с владельцем, что по крайней мере некоторые из них верны. Так
Для полноты картины попробуем еще несколько доменов.

В качестве нашей следующей цели мы можем найти журналы прозрачности сертификата на наличие эксплойта.
in, популярный российский хакерский форум, который также использует Cloudflare. (См. Рисунок 10.5.)

Если посмотреть конкретно на crt.sh ID 11915608, мы можем увидеть следующие результаты:

Сертификат:
Данные:
Версия: 3 (0x2)
Серийный номер:
40: 7f: 98: 9b: 8d: ef: 73: 2f: 81: 4c: a1: ef: ff: dc: 28: c3
Алгоритм подписи: ecdsa-with-SHA256
Эмитент: (CA ID: 1582)
распространенное имя
= COMODO ECC Domain Validation Secure Server CA 2
organizationName = COMODO CA Limited
localityName
= Салфорд
stateOrProvinceName = Большой Манчестер
название страны
= ГБ
Срок действия
Не раньше: 21 октября, 00:00:00 2015 по Гринвичу
Не после: 20 октября 23:59:59 2016 по Гринвичу
Тема:
распространенное имя
= sni309783.cloudflaressl.com
organizationUnitName = PositiveSSL, многодоменный
organizationUnitName = Контроль домена подтвержден
[...]
X509v3 Альтернативное имя субъекта:
DNS: sni309783.cloudflaressl.com
DNS: *. Exploit.in
DNS: exploit.in

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
947978131	2018-11-15	2018-11-12	2019-11-12	C=US, ST=CA, L=San Francisco, O="CloudFlare, Inc.", CN=CloudFlare Inc ECC CA-2
940732002	2018-11-12	2018-11-12	2019-11-12	C=US, ST=CA, L=San Francisco, O="CloudFlare, Inc.", CN=CloudFlare Inc ECC CA-2
870351310	2018-10-17	2018-10-17	2019-04-25	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA 2
870351269	2018-10-17	2018-10-17	2019-04-25	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
870350535	2018-10-17	2018-10-17	2019-04-25	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
870350538	2018-10-17	2018-10-17	2019-04-25	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA 2
870349440	2018-10-17	2018-10-17	2019-04-25	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO Domain Validation Legacy Server CA 2
870349463	2018-10-17	2018-10-17	2019-04-25	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO Domain Validation Legacy Server CA 2
652333850	2018-08-18	2018-08-18	2019-02-24	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
652333597	2018-08-18	2018-08-18	2019-02-24	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
608774228	2018-07-23	2018-07-21	2020-07-20	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
608578897	2018-07-21	2018-07-21	2020-07-20	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
351550165	2018-03-10	2018-03-10	2018-09-16	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
319881684	2018-02-02	2014-10-15	2015-10-16	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - G2
284327456	2017-12-21	2017-12-19	2019-01-18	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018

Рисунок 10.5.

Они используют Cloudflare, и похоже, что никакой другой домен не использует
тот же общий SSL.
По мнению Cloudflare, я могу запустить этот инструмент в нескольких случаях и найти com-
полностью несвязанные домены. Мой домен оказался одним из них.
Когда вы просматриваете vinnytroia.com в crt.sh, вы получаете следующие результаты:

```
X509v3 Альтернативное имя субъекта:
DNS: sni68313.cloudflaressl.com
DNS: *. Alwatansport.ps
DNS: *. Alwatanvoice.com.ps
DNS: *. Alwatanvoice.net.ps
DNS: *. Alwatanvoice.org.ps
DNS: *. Hospitalshub.com
DNS: *. Jenanmag.com
DNS: *. Larhonda.review
DNS: *. Pincodehub.com
DNS: *. Ramallahnet.com
DNS: *. Thepointatpentagoncityapts.com
DNS: *. Vinnytroia.com
DNS: *. Wholiesmore.org
DNS: alwatansport.ps
DNS: alwatanvoice.com.ps
DNS: alwatanvoice.net.ps
DNS: alwatanvoice.org.ps
DNS: Hospitalshub.com
DNS: jenanmag.com
DNS: larhonda.review
DNS: pincodehub.com
DNS: ramallahnet.com
DNS: thepointatpentagoncityapts.com
DNS: vinnytroia.com
DNS: wholiesmore.org
```

Как оказалось, точка зрения Cloudflare верна. За исключением моего сайта,
vinnytroia.com , ни один из этих доменов мне не принадлежит. Итак, еще раз, *если вы собираетесь*
чтобы использовать этот метод для поиска дополнительных подсказок, имейте в виду, что результаты могут не
всегда будьте точны .

CloudFlair (сценарий) и Censys

Cloudflare предназначен для работы в качестве посредника между веб-сайтом и его пользователями,
для защиты владельцев сайта от различных видов кибератак. В
Теоретически злоумышленник не получит прямого доступа к веб-сайту. Вместо этого пользователь получает доступ
веб-сайт через защитный слой Cloudflare.com , который в конечном итоге маскирует
настоящий IP-адрес сервера. Это может быть полезным инструментом для служб безопасности.
использовать, потому что он маскирует исходный IP-адрес компании, тем самым делая
вести активную разведку против сайта труднее.

Конечно, это при условии, что сервер правильно настроен, что не
всегда так. Или, что более важно, возможно, сервер правильно настроен
сейчас , но не раньше.

Подобно crt.sh, Censys.io можно использовать для поиска через перенос сертификатов.
журналы паранентности для поиска текущих или ранее открытых серверов.

Как это работает?

Вместо того, чтобы искать связанные доменные имена, мы также можем использовать сертификат
выполняет поиск связанных IP-адресов. Если эти IP-адреса не являются частью
Cloudflare, то мы предполагаем, что IP принадлежит нашему целевому домену.

Если вы хотите автоматизировать этот процесс, существует инструмент Python под названием Cloud-
Flair (CF, поэтому мы не путаем его с компанией Cloudflare). CF - это используемый инструмент
для автоматизации процесса поиска происхождения общедоступных серверов, которые
не ограничивают должным образом доступ к диапазонам IP-адресов Cloudflare.com .

Этот инструмент доступен для загрузки по адресу https://github.com/christophetd/.
CloudFlair .

В нашем первом примере давайте посмотрим, можем ли мы использовать CF для отслеживания исходного сервера.
Codepen.io:

```
корень @ OSINT: python cloudflair.py codepen.io
[*] Получение диапазонов IP-адресов Cloudflare от
https://www.cloudflare.com/ips-v4
[*] Похоже, что цель находится за CloudFlare.
[*] Поиск сертификатов, соответствующих "codepen.io" с помощью Censys
[*] Найдено 13 сертификатов, соответствующих "codepen.io".
[*] Поиск хостов IPv4, представляющих эти сертификаты ...
[*] 3 хоста IPv4 предоставляют сертификат, выданный "codepen.io"
были найдены.
- 52.27.19.56
- 54.201.58.131
- 52.10.104.25
[*] Тестирование серверов-кандидатов происхождения
[*] Получение целевой домашней страницы на https://codepen.io
[*] «https://codepen.io» перенаправлен на «https://codepen.io/»
- 52.27.19.56
- 54.201.58.131
- 52.10.104.25
[*] Обнаружен 1 вероятный сервер-источник codepen.io!
- 52.27.19.56 (HTML-контент на 96% структурно похож на codepen.io)
```

Вот и все!

Прежде чем я закончу этот раздел, вы знаете, что я говорю не только
полагаться на один инструмент и убедиться, что вы тестируете с использованием нескольких инструментов и техник?
Чтобы проиллюстрировать мою точку зрения, посмотрите, что происходит при поиске
WhitePacket.com об использовании того же инструмента:

```
root @ OSINT: cloudflair.py whitepacket.com
[*] Получение диапазонов IP-адресов Cloudflare от
https://www.cloudflare.com/ips-v4
[*] Похоже, что цель находится за CloudFlare.
[*] Поиск сертификатов, соответствующих whitepacket.com, с помощью Censys
[*] Найдено 0 сертификатов, соответствующих " whitepacket.com ".
Выход.
```

Не найдено ни одного сертификата, хотя crt.sh показывает несколько сертификатов для
WhitePacket.com . Не поймите меня неправильно: Censys.io - платный инструмент,
хороший. Но идеального инструмента нет. Убедитесь, что вы не слишком полагаетесь на один
источник или вы можете что-то пропустить.

Архивы Wayback Machine и поисковых систем

Wayback или Wayback Machine - это цифровой веб-архив. Путь назад
(он же Archive.org) позволит вам увидеть состояние веб-сайта, как это было, на
историческая дата.
В этой книге уже описаны причины, по которым изучение исторических
состояние - важный способ поиска зацепок. В этом разделе основное внимание будет уделено
о способах автоматизации поиска, но сначала давайте рассмотрим несколько основных примеров.
Как показано на рисунке 10.6, при поиске Wayback Machine по запросу www.whitepacket
.com , в результатах будут представлены архивные данные за период с 2013 по 2018 год.

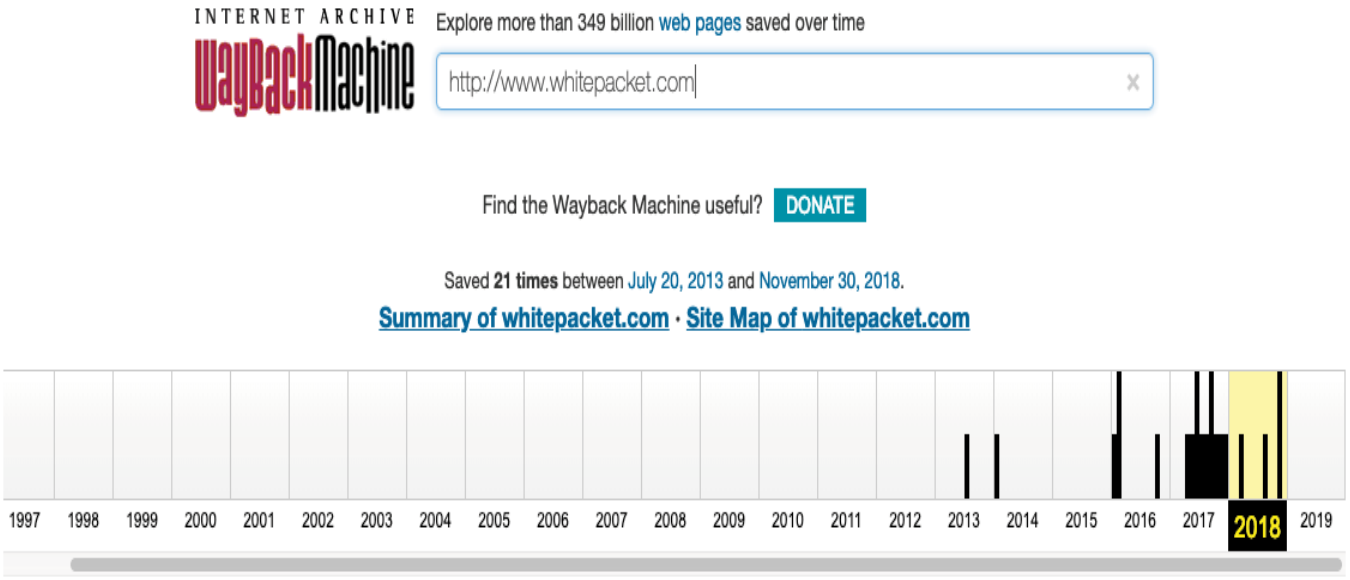


Рисунок 10.6.

Для дальнейшего изучения этих архивов щелкните год, а затем дату создания снимка.
Синие кружки на календаре (см. Рисунок 10.7) указывают дату, когда был сделан снимок.
сайт был занят. Для просмотра архива сайта, созданного на определенном
дату, щелкните любой из синих кружков в календаре.
Большую часть 2017 года WhitePacket перенаправлял свой домен на учетную запись Twitter: www.
twitter.com/whitepacket . Аккаунт Twitter был удален, но иногда
нам может повезти, используя кеш Google.

Кеши поисковых систем

Иногда Google предлагает кешированные версии веб-сайтов через стандартную
результаты поиска. Чтобы получить доступ к кешированным версиям сайта, щелкните зеленый вниз
стрелку (▾) рядом с результатом поиска и выберите «просмотр из кеша». Давай попробуем поискать
для кэшированной версии страницы Twitter WhitePacket (показанной на рис. 10.8):
введите следующий поиск в Google:

сайт: twitter.com/whitepacket

У Google есть только один результат, позволяющий просматривать кешированную копию. Несколько
твиты перечислены, но нажатие на них приводит к ошибке «страница не найдена», поскольку
страница была удалена.
Посмотрим, отличаются ли наши результаты в Bing, как показано на рисунке 10.9.

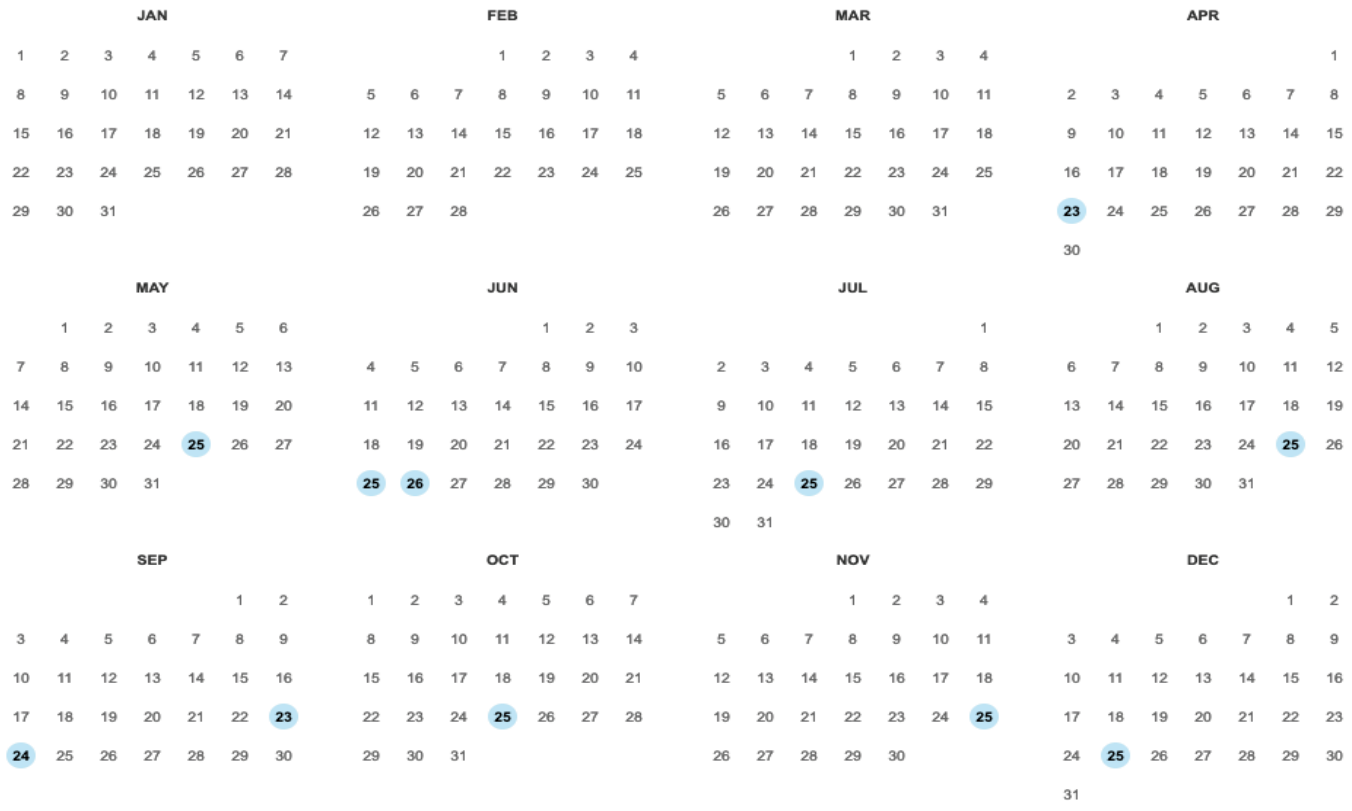
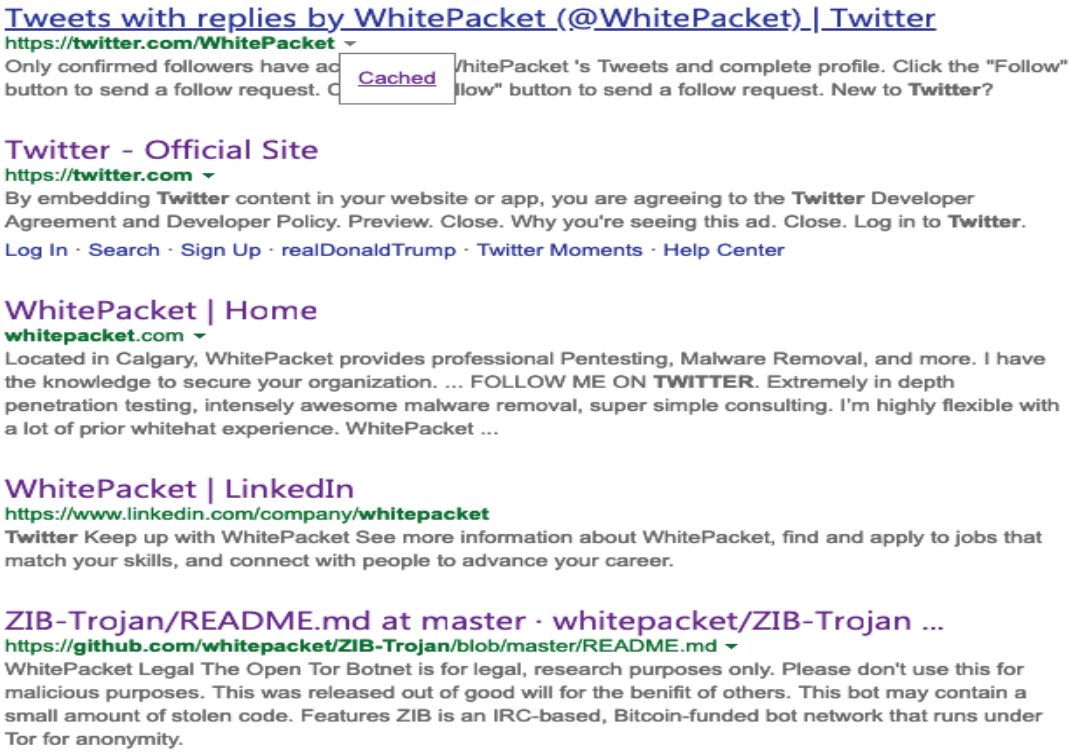


Рисунок 10.7.



Рисунок 10.8

Рисунок 10.9



Результаты с Bing такие же, как и для кэшированной копии
Страница Twitter, но обратите внимание на последний результат - ботнет TOR с открытым исходным кодом.
кодируется на странице WhitePacket GitHub. Выглядит интересно.
Изучение этой страницы дает нам адрес электронной почты, идентификатор jabber и адрес BTC.
чтобы добавить в наш список условий поиска.

CachedView.com

CachedView.com (рис. 10.10) - это сайт, который позволяет легко искать заархивированные
веб-страницы в кэше Google, Archive.org и Coral Cache. Результат
сайт такой же; он просто предоставляет тип концентратора для каждого доступа к нескольким
кеш-сайты.

Скребок для машин Wayback

Wayback Machine (www.archive.org) может быть прекрасным источником информации.
При работе с большими сайтами объем информации, которую вам нужно проанализировать,
может быть ошеломляющим.
Лучший способ, который я нашел для этого, - буквально очистить все кэшированные копии
site, а затем проанализируйте данные локально. Доступно несколько различных инструментов, которые
вы можете использовать для очистки данных. Один из них, enum _ wayback , даже запечен правильно
в Metasploit благодаря Робу Фуллеру (он же Mubix).

Я не умею тестировать веб-приложения на проникновение. Я не очень хорошо разбираюсь в том, как они фильтруются и что они делают. А поскольку в наши дни все является веб-приложением, не очень хорошо помогает взломать их. Итак, зная, как работает приложение на бэкэнде и знать, на какие веб-сайты или какие URI следует перейти и настроить таргетинг, - это своего рода угадайку.
Итак, вам нужно выяснить, где вам нужно войти в систему, чтобы добраться до косой черты.
панель администратора, панель инструментов и т. д. Все те URI, которые входят в панель управления, имеют своего рода

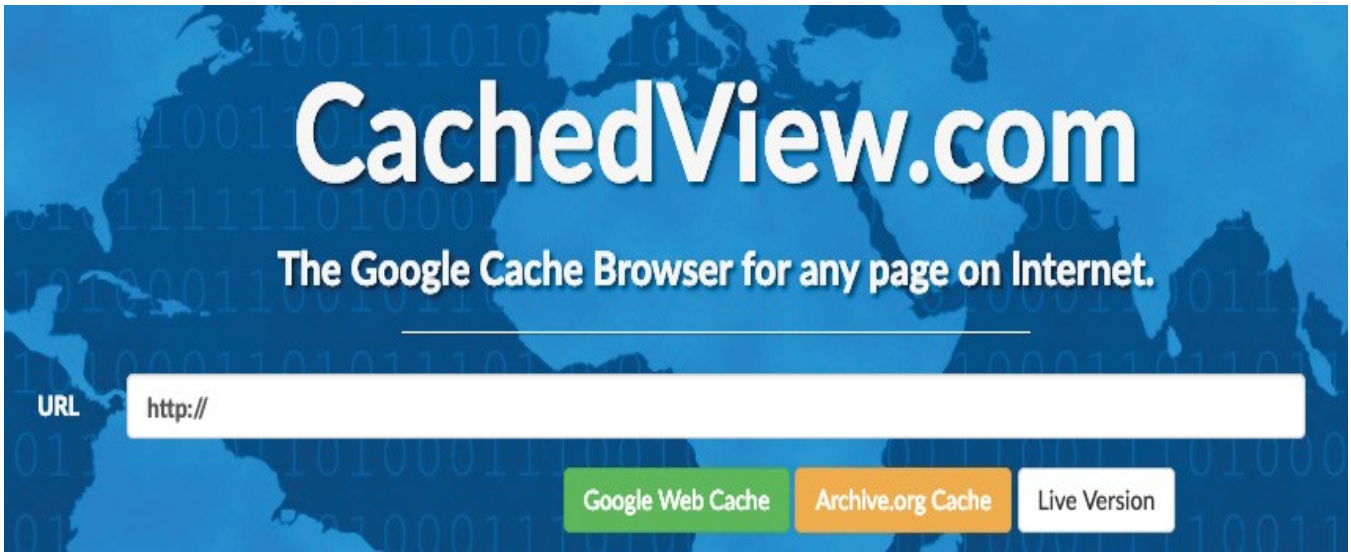


Рисунок 10.10.

присущая ему уязвимость. Если они не запрограммируют это правильно, вы можете получить прямой доступ к ресурсам.
с приборной панели или панели.
Wayback Machine записывает веб-сайты в разных состояниях. Если машина обратного пути
смог записать URI, который больше не используется или был открыт в течение минуты, когда он
поймал это, это может быть действительно полезно для понимания того, как работает приложение, или
по крайней мере, даже просто история этого.
Перечисление _ Вайбак **сценарий был разработан для вида дать вам кучу URIs , что**
вы могли не знать о. Он может показать вам URI, которые существовали и могут не существовать
Теперь. Скрипт не будет копировать все функции веб-приложения, но он
паук это.
Допустим, у них была специальная версия Drupal на один год и специальная версия
WordPress в следующем году. Вы получите URL-адреса Drupal и WordPress или
URI. Есть большая вероятность, что Java либо оставила файлы, либо не настроила маршрутизацию.
правильно, или какая-то другая деталь, и там будет технический долг. потом
Wayback не только находит это, но также находит все, что было открыто, что, вероятно,
не должно было быть.
Давайте возьмем в качестве примера Интернет-магазин Боба. Есть хороший шанс, что если сеть Боба
Store существует уже 15 лет, они не думали о безопасности еще 10 лет назад,
и поэтому те URI, которые были проиндексированы и каталогизированы, могут все еще присутствовать и все еще
очень корректно, но теперь более безопасно.
Может быть , что 80% из них являются более безопасными, но вы можете просто найти , что *один* **, что**
нет - и это действительно может иметь значение. Скрипт разработан, чтобы дать вам большой-
ger ресурс страниц для просмотра.
Использовать его действительно просто. Все, что вам нужно сделать, это указать ему на конкретное имя хоста или
домен, и он дает вам результаты Wayback, все проанализированные, красивые и аккуратные,
поэтому вам не нужно ничего пролистывать, и это очень упрощает загрузку в
Тоже отрыжка.

Enum Wayback

enum _ wayback - это сценарий Ruby, который теперь является частью платформы Metasploit.
Поскольку это книга о расследованиях и OSINT, мы не будем копать
слишком далеко в Metasploit или во всех удивительных вещах, которые вы можете с ним делать. если ты
не использовал Metasploit в прошлом (или, может быть, не знаю, что это такое), Metasploit
будет одним из ваших основных инструментов при проведении теста на проникновение. Сотни
(если не тысячи) эксплойтов и настраиваемых модулей встроены в инструмент,
что делает его необходимостью для любого тестера на проникновение.
Для тех из вас, кто знаком с Metasploit, мы можем запустить enum _ wayback следующим образом:

```
msf> используйте вспомогательный / сканер / http / enum_wayback
```

Чтобы увидеть наш список доступных опций, мы можем ввести опции :

```
вспомогательный msf (сканер / http / enum_wayback)> параметры
```

Параметры модуля (вспомогательный / сканер / http / enum_wayback):
Имя Текущая настройка Требуется Описание
---- ---------- -------- -----------
ДОМЕН
да Домен для запроса URL-адресов
АУТФАЙЛ
нет
Куда вывести список для использования

Параметры скребка Wayback довольно просты. Вы можете установить
домен, на который вы хотите настроить таргетинг, и выходной файл для данных.

Очистка пути назад с помощью Photon

Многие другие инструменты командной строки могут использоваться для очистки архивов Wayback.
Один из них - Photon, инструмент, который мы обсуждали в предыдущей главе. Фотон
Скребок Wayback будет извлекать все доступные URL-адреса сайта как «семена». В этом
В контексте, исходный файл - это в основном список других URL-адресов, к которым вы можете вернуться.
и зайти / соскрести. Другими словами, Фотон действует как паук и будет ползать.
различные URL-адреса, доступные на Wayback, и предоставят вам хорошо отформатированный список.
Во многих случаях веб-сайты (или форумы) не требуют аутентификации.
катион, чтобы увидеть их сообщения. По тем или иным причинам некоторые хакерские форумы могут
можно просматривать без входа в систему, что означает, что их содержимое будет очищено
и кешируется. Одним из таких сайтов является Bezlica.top, старый русский хакерский форум.
Я использую этот форум специально потому, что это был один из форумов, где
TDO впервые опубликовала информацию о продаже своих медицинских данных. На рисунке 10.11 показан снимок экрана.
исходного сообщения.

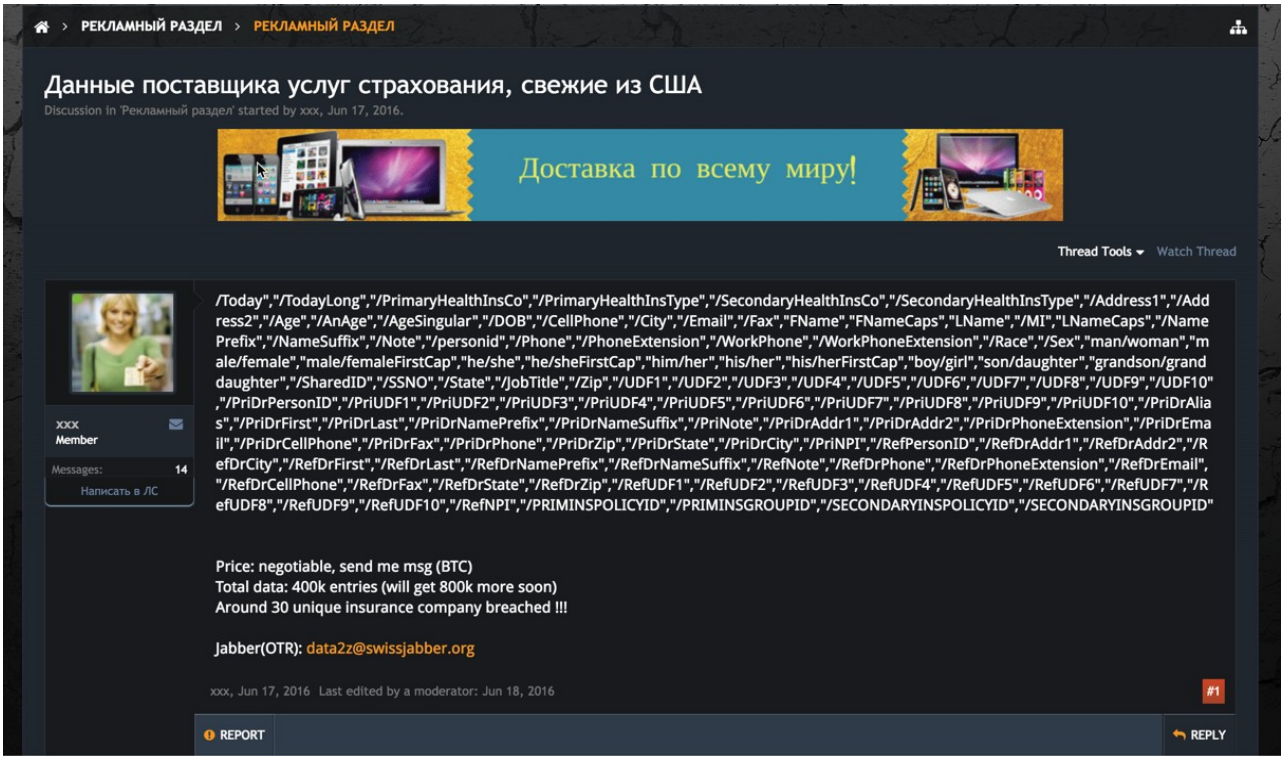


Рисунок 10.11

Возможность индексировать и исторически каталогизировать эти данные может быть невероятно полезной.
для будущих исследований. Что, если бы мы захотели найти больше сообщений по этому
Пользователь? Это прекрасный пример, потому что сайта больше нет в сети.
К счастью для нас, сообщения сайта были общедоступными и были скопированы Wayback, что означает
мы можем получить их с помощью Photon.
Чтобы запустить движок Wayback от Photon, используйте переключатель --wayback .
При запуске Photon мы также можем изменить глубину сканирования. Это использование-
Если мы знаем, что на сайте много уровней вложенных страниц, например форумов:

```
питон фотон --wayback -d 10 -u bezlica.top
корень @ INTEL: / opt / Photon: python photon.py --wayback -u bezlica.top -d 10
____ __
__
/ __ \ / / _ ____ / / _____ ____
/ / _ / / __ \ / __ \ / __ / __ \ / __ \
/ ____ / / / / / _ / / / _ / / _ / / / / /
/ _ / / _ / / _ / \ ____ / \ __ / \ ____ / _ / / _ / v1.2.1
[~] Получение URL-адресов с archive.org
[+] Получено -1 URL с archive.org
[+] URL-адреса, полученные из robots.txt: 1
[~] Уровень 1: 2 URL
[!] Прогресс: 2/2
[~] Уровень 2: 3 URL
[!] Прогресс: 3/3
[~] Сканирование 4 файлов JavaScript
[!] Прогресс: 4/4
-------------------------------------------------------
[+] Intel: 3
[+] Роботов: 1
[+] Внутренний: 5
[+] Скриптов: 4
[+] Внешний: 3
-------------------------------------------------------
[!] Всего запросов: 9
[!] Общее время: 0 минут 52 секунды
[!] Запросов в секунду: 0
[+] Результаты сохранены в директории bezlica.top
```

URL-адреса поиска по сайту Archive.org

Многие инструменты парсера могут потребовать от вас предоставить им точный список URL-адресов.
соскоблить. Составление списка рабочих URL-адресов может оказаться очень сложной задачей,
особенно когда речь идет о форумах с миллионами сообщений. Как оказывается
out, вы можете использовать специально созданные URL-адреса для загрузки списков страниц, кэшированных
Archive.org .

Следующий URL-адрес предоставит список каждой кэшированной копии сайта и ее дату.

подставив фактический домен: https://web.archive.org/cdx/search?url=domain.

com .

Например, введите этот URL-адрес в своем браузере для поиска Bezlica.top: https: //

web.archive.org/cdx/search?url=bezlica.top дает нам следующие результаты:

top, bezlica) / 20160911021317 http://bezlica.top:80/
text / html 200 7TMNRLBP5VIJEXO7K6RCZXPJTULOV5PO 11844
top, bezlica) / 20160914070721 http://bezlica.top
text / html 200 OHXJUAIWGKOH66WENAYCIG45PRYCHCCE 12492
top, bezlica) / 20161016030541 http://bezlica.top:80/
text / html 200 26YUBAWKSVXQJYXTHOBOLCPOTCJ3PH5C 10878
top, bezlica) / 20161208235225 http://www.bezlica.top:80/
text / html 200 BU2WMW7ZLZNL5VC6H6RLZVJCAEQUK2PH 11276
top, bezlica) / 20161216210357 http://bezlica.top:80/
text / html 200 6GJ5JTHKFEGGJEGHK35V7XUQ4BALB4RC 10166
top, bezlica) / 20170428055547 http://bezlica.top:80/
text / html 200 IJ6FUIV6CDPKDFOJDSFKWRVS37ORQHQ3 18429
top, bezlica) / 20170509213741 http://bezlica.top:80/
text / html 200 55CY2ONBUCCJTKCOQH4DR2EOL2Z3OJA5 23358
top, bezlica) / 20170520210324 http://bezlica.top:80/
text / html 200 7E3KPSJSOESAMJIX73Q6QGBOD3DFT734 21599
top, bezlica) / 20170609030411 http://bezlica.top:80/
text / html 200 4QB2Y33ZP5HMM53EEAFSUV7YZO6AOX74 23576
top, bezlica) / 20170611034742 http://bezlica.top:80/
text / html 200 JJE3IVA44G7P5YHIVR26HWSUS6BZDV7M 20182
top, bezlica) / 20170630193537 http://bezlica.top:80/
text / html 200 NITYMLKCZ5XFDAPJWDCTHIQL2CJLOLIU 20882
top, bezlica) / 20170712011807 http://bezlica.top:80/
text / html 200 4UBXAEQ2AWT5CL4USMJQXLWQEDOZI357 21177
top, bezlica) / 20170724230545 http://bezlica.top:80/
text / html 200 PTPCXTUMBAUGRUKAGNXU7FDHRRKCKPKW 20240
top, bezlica) / 20180104141200 http://bezlica.top:80/
text / html 200 6KQI5ILW4WE2EXH54ZRI6DWBNN5TR2H6 19138
top, bezlica) / 20180307003146 http://bezlica.top:80/
text / html 200 7DJMCBRJBRLPMEZRLKFETZVPTCORNQBZ 18959
top, bezlica) / 20180508100733 http://bezlica.top:80/
text / html 200 6POLETZBHK23AA7RRYRLHZUD3VPGAAX2 19171
top, bezlica) / 20180609005028 http://bezlica.top:80/
text / html 200 UVFKHSNQK5R4OIUDZFL3XGYXB7WJXZST 19178
top, bezlica) / 20180706234035 http://bezlica.top:80/
text / html 301 R4P57LSX7D3PMJ4CTPAJ3FU3VPVFIVF5 360
top, bezlica) / 20180811090133 http://bezlica.top
text / html 301 Q4XK7WZCBMFO7HSN7SMGOAX7KLKFT6MT 497
top, bezlica) / 20180904112205 http://bezlica.top
warc / revisit - Q4XK7WZCBMFO7HSN7SMGOAX7KLKFT6MT 457
top, bezlica) / 20181112133152 http://bezlica.top
warc / revisit - Q4XK7WZCBMFO7HSN7SMGOAX7KLKFT6MT 458
top, bezlica) / 20181127220905 https://bezlica.top/
warc / revisit - Q4XK7WZCBMFO7HSN7SMGOAX7KLKFT6MT 455

В начале каждой строки мы видим URL-адрес (вверху, bezlica), за которым следует
дата и время каждого сканирования (27.11.2018 и т. д.).
Эта информация затем может быть сохранена и загружена в веб-сканер (например, Photon).
выйти и очистить каждую копию сайта, чтобы убедиться, что мы собираем как можно больше
историческая справка по возможности.

Дайджест сайта Wayback: список URL-адресов всех сайтов, сохраненных в кэше Wayback

Мы можем расширить наш URL-запрос, чтобы отображать каждый кешированный URL-адрес для конкретного сайта.
by Wayback, добавив * & collapse = digest в нашу строку URL:

https://web.archive.org/cdx/search?url=domain.com*&collapse=digest

Посмотрев на этот URL-адрес, мы можем увидеть полный список каждой страницы, кэшированной для домена.
Расширяя наш поиск, чтобы снова взглянуть на Bezlica.top, мы можем увидеть сотни
страницы результатов, которые выглядят так:

https://web.archive.org/cdx/search?url=bezlica.top*&collapse=digest
вверху, безлица) /threads/nuzhen-ship-telefona.30788/reply?quote=182018
20170504095614 http://bezlica.top:80/threads/nuzhen-ship-telefona.30788/
ответить? quote = 182018 текст / html 200 6ULJU6ZH7ZM2ZGG6HNWHSDFWXEC7QAAU 9611
сверху, безлица) /threads/nuzhen-ship-telefona.30788/reply?quote=195845
20170504101949 http://bezlica.top:80/threads/nuzhen-ship-telefona.30788/
ответить? quote = 195845 текст / html 200 AAKCFAPVFPA6HVSVY2S72XTK6DPBWD4U 9639
вверху, безлица) /threads/nuzhen-ship-telefona.30788/reply?quote=
196094 20170425161906
верх, безлица) /threads/nuzhna-rabota.12142 20170425002556
http://www.bezlica.top:80/threads/nuzhna-rabota.12142
text / html 301 3I42H3S6NNFQ2MSVX7XZKYAYSCX5QBYJ 428
верх, безлица) /threads/nuzhna-rabota.12142 20170425002556
http://www.bezlica.top:80/threads/nuzhna-rabota.12142/
text / html 200 75PDTP3FGKT5AYHH5CT3WHF3DWW5GR43 11297
сверху, безлица) /threads/nuzhno-fake-id.62868 20170425020755
http://bezlica.top:80/threads/nuzhno-fake-id.62868
text / html 301 3I42H3S6NNFQ2MSVX7XZKYAYSCX5QBYJ 424
сверху, безлица) /threads/nuzhno-fake-id.62868 20170425020755
http://bezlica.top:80/threads/nuzhno-fake-id.62868/
text / html 200 73Y7JISNW7AXJDXTEB2GRCKC7OUGKPQO 8630
верх, безлица) /threads/nuzhny-sellery.90646 20170710104915
http://bezlica.top:80/threads/nuzhny-sellery.90646
text / html 301 3I42H3S6NNFQ2MSVX7XZKYAYSCX5QBYJ 405
верх, безлица) /threads/nuzhny-sellery.90646 20170710104915
http://bezlica.top:80/threads/nuzhny-sellery.90646/
text / html 200 4UTAHZPB5YVNTS5MSKJJ2JJ4FXACULRU 9200
верх, безлица) /threads/nuzhny-sellery.90646 20170712001847
http://bezlica.top:80/threads/nuzhny-sellery.90646/
text / html 200 PIVOCNJCPNWRDOC2XFHVKUZPNNDNI4EG 9204
вверху, безлица) /threads/obnal-vcc.22482 20170425023630
http://bezlica.top:80/threads/obnal-vcc.22482

text / html 301 3I42H3S6NNFQ2MSVX7XZKYAYSCX5QBYJ 423
верх, безлица) / темы / обналичу-ваши-звонки-с-чего-угодно.
90587 20170722053208 http://bezlica.top:80/threads/obnalichu-
vashi-zvonki-s-chego-ugodno.90587 text / html 301
3I42H3S6NNFQ2MSVX7XZKYAYSCX5QBYJ 547
верх, безлица) /threads/obnalichu-vashi-zvonki-s-chego-ugodno.90587
20170722053208 http://bezlica.top:80/threads/obnalichu-vashi-zvonki
-s-chego-ugodno.90587 / text / html 200 DHB3ECDNAZZJTZKTSZ4X6C7U4MKIWQMN
10902
верх, безлица) /threads/obnalichu-vashi-zvonki-s-chego-ugodno.90587
20170723200538 http://bezlica.top:80/threads/obnalichu-vashi-zvonki-
s-chego-ugodno.90587 / text / html 200 MB77HKZM7MH5YENQLZLLH4LKWF36TA5Q
11025

Немного сложно прочитать в одном гигантском пятне, но, глядя на результаты, мы можем
просмотреть полный URL-адрес страницы, которая была кэширована, а также дату кэширования страницы.
Почему это важно? Вместо того, чтобы загружать все кешированные
страниц и просматривайте потенциальную гору данных, насколько легко, по вашему мнению, это
было бы найти панель администратора, выполнив поиск по списку URL-адресов?
Теперь, когда у нас есть вся карта кешированных страниц, мы можем скачать
список всех кешированных страниц и быстрый поиск по определенным ключевым словам, например «админ»,
«Панель» и так далее.
Помните, что если кто-то хочет скрыть URL-адрес от поисковой системы, все они
необходимо обновить файл robots.txt на своем веб-сайте. Просто потому, что сайт
в текущей карте сайта не указана панель администратора, это не означает, что панель
не существует в какой-то момент. Возможно, страница все еще там, просто скрыта или переименована.
Использование этого метода позволяет быстро находить страницы, которые могли существовать.
в какой-то момент, но с тех пор были удалены.

Резюме

В этой главе основное внимание уделялось методам, которые вы можете использовать для дальнейшего исследования
веб-сайты и владение доменами с использованием прозрачности сертификатов и Интернета
архивы (например, кеши поисковых систем и Wayback Machine). Сертификат
Прозрачность позволяет находить связанные веб-сайты (и веб-сайты
владельцев), ища общие SSL-сертификаты. Кешированные страницы поиска и Интернет
архивы, такие как Wayback Machine, можно использовать для поиска интересных данных.
на сайте, просмотрев историю его страниц.
В следующей главе мы сосредоточимся на Iris от DomainTools, который был
единственный самый важный инструмент в любом из моих расследований, требующих информации
по истории домена и историческому исследованию веб-сайтов.

11

Если бы мне пришлось выбрать единственный инструмент, который был бы наиболее полезен при исследовании Тьмы Оверлорд, это будет Ирис.
DomainTools Iris - это, пожалуй, самый полный и впечатляющий исторический
инструмент поиска регистрации доменов на рынке. Это полная информация об угрозах и
платформа для расследования, ориентированная на предоставление контекста об угрозах с доменом
регистрация и данные пассивного DNS.
Iris - платный проприетарный инструмент. Я стараюсь включать открытые инструменты
источник, но правда в том, что я не нашел другого инструмента, который хотя бы приближался к
возможности я продемонстрирую.
DomainTools имеет не только самую полную базу данных исторических
данные о регистрации домена я когда-либо видел, но сам инструмент довольно хорош.
(Нет, мне не платят за то, чтобы я писал это, но теперь, когда я думаю об этом, я, наверное,
умело должен был спросить.)

Основы ириса

В этом разделе будут рассмотрены только основы Iris, поскольку мы исследуем мой личный веб-сайт.
Мы углубимся в Ирис в следующих разделах, когда начнем комбинировать его.
с другими техниками. Ирис сам по себе отличный инструмент, поэтому комбинируйте его с другими
инструменты и методы сделают его намного более мощным, особенно когда мы

Ирис от DomainTools

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

начать собирать всю обнаруженную информацию вместе в нашей матрице отслеживания (который мы начнем строить в части IV этой книги).

Мы можем начать использовать Iris с поиска любого количества полей, включая домен имена, личные имена, адреса электронной почты, физические адреса, IP-адреса, SSL хэш, DNS-серверы и любую другую информацию, составляющую запись WHOIS. (См. Рисунок 11.1.)

Используя панель поиска Iris, мы начнем с поиска моего личного сайта, « Vinnytroia.com ». Результаты поиска будут отображаться в Iris Pivot. Вид двигателя, показанный на рисунке 11.2.

Iris Pivot Engine действительно является краеугольным камнем предмета исследования. Когда вы ищете новые элементы, Pivot Engine будет выделять, какие другие пути вы можете изучить данные WHOIS в домене. Каждый путь называется *стержень* . Каждый раз, когда вы делаете новый шаг в другом направлении, вы меняете с вашего исходного шага. Данные, отображаемые в таблице Pivot Engine, показаны на Рисунок 11.2 очень широкий - на нем 20 столбцов, в которых можно выделить любое число. доступных для поиска полей, включая (но не ограничиваясь):

- Электронная почта
- Домен
- Регистрант

Рисунок 11.1.
Рисунок 11.2.

■ Организация

■ Статус

■ Дата создания / истечения срока действия

■ Google Analytics

■ Записи MX или SPF

■ хэш SSL-сертификатов, происхождение или страна

Управляемые повороты

Управляемые опорные точки предназначены для помощи в выявлении потенциально ценных опорных точек; таким образом, они выделены для вас. По умолчанию радужная оболочка выделяет любую точку поворота, подключается к менее чем 500 доменам (порог можно настроить). Когда мы катимся над ссылкой «3 управляемых поворота» на рис. 11.3 показано, какие поворотные точки доступны. для дальнейшего изучения.

Конфигурирование ваших настроек

Pivot Engine довольно легко настраивается. При нажатии на кнопку «Настройки» открывается Панель настроек. Отсюда вы можете изменить отображаемые заголовки таблиц. в Pivot Engine, а также порядок отображаемой информации в таблице Pivot Engine.

Помимо косметических предметов, вы также можете настроить чувствительность ваши управляемые повороты (показаны на рис. 11.4).

Как обсуждалось ранее, Айрис выделяет управляемые точки поворота, которые разделяют ценности с меньшими затратами. более 500 различных доменов (или совпадений). Это число может быть довольно большим, поэтому вы можно смягчить это в этом представлении настроек. Вы можете уменьшить это число до 10, это означает, что выделение управляемых точек будет отображаться только в том случае, если уникальные - качество отображаемых данных обнаруживается не более чем на 10 различных доменах.

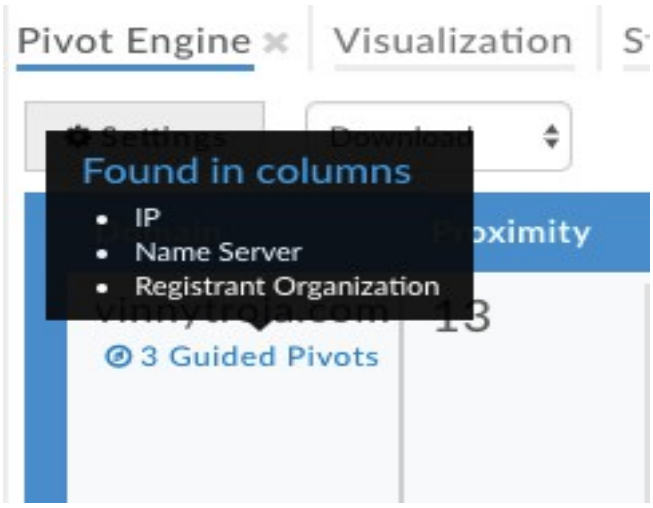


Рисунок 11.3.

Это может быть очень полезной настройкой при исследовании IP-адресов, поскольку она может предоставить быстрый способ изолировать IP-адреса, которые не используются совместно. Например, если вы найти домен на IP-адресе, который использовался лишь несколькими другими доменов, есть очень большая вероятность, что все домены будут принадлежать или управляется одним и тем же лицом.

Настройка исторического поиска

Последний вариант - это настройка исторического поиска. По умолчанию поиск по радужке ограничено совпадениями, в которых поисковый запрос встречается в текущей записи. Этот означает, что если вы искали Vinny Troia, вы не нашли бы домен, Прописал лет пять назад, продали другому хозяину. При поиске это обычно хорошее правило, чтобы убедиться, что этот параметр включен, если нет причина, по которой вы не хотите использовать более старые исторические данные в ваших результатах. (См. Рисунок 11.5.)

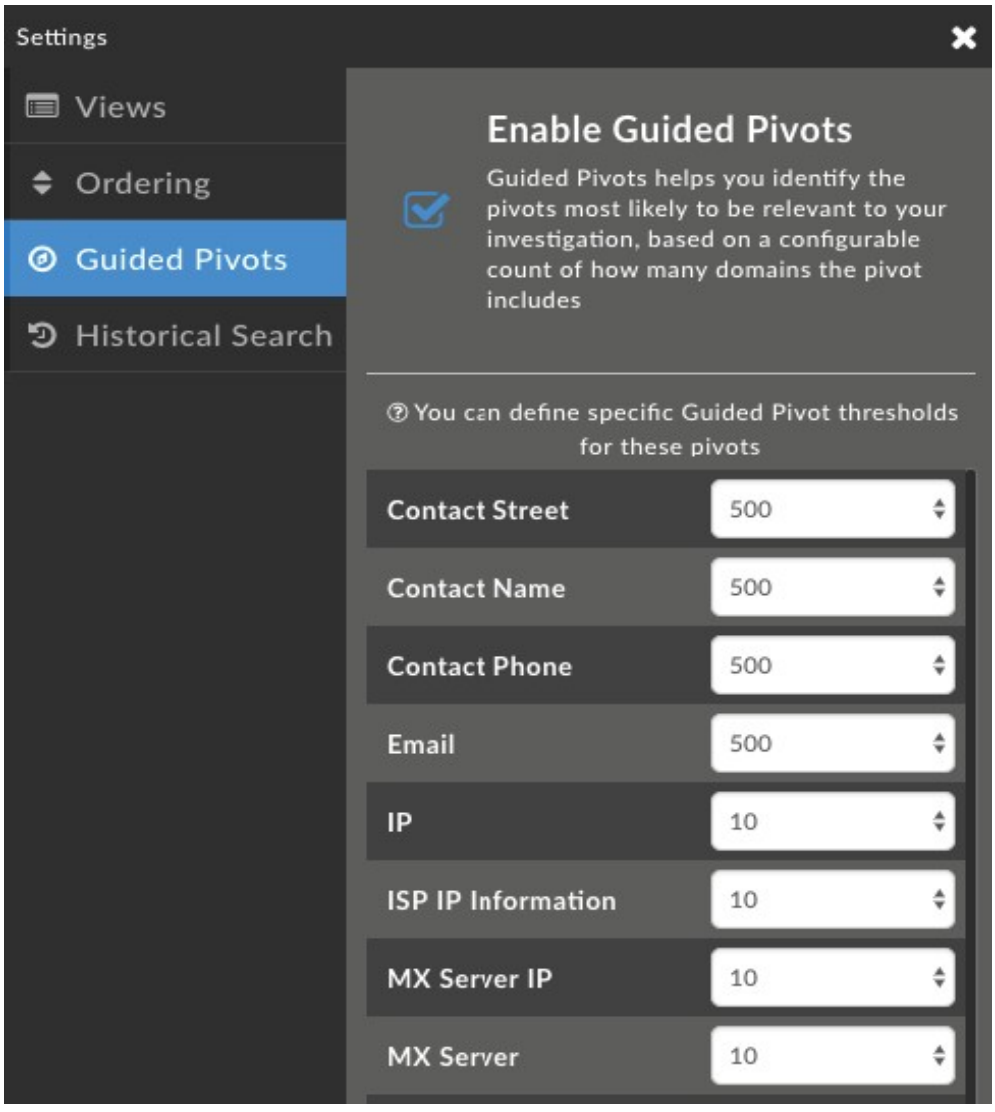


Рисунок 11.4.

Когда включен исторический поиск, результаты домена будут отображаться как «Активный» или «неактивный» в списке результатов, который показан значком гиперссылки для активных доменов и сломанный значок для неактивных доменов.

Пивоттт !!!

Каждый раз, когда я слышу слово « *поворот*» , я могу думать только об одной сцене из « *Друзья*». где Росс попытался сдвинуть диван вверх по лестнице, но продолжал кричать: «Пивот !!» Переходя к нашему первому повороту, мы видим на рис. 11.6, что у Pivot Engine есть обнаружил три точки управляемой сводки: IP, сервер имен и организация регистранта.

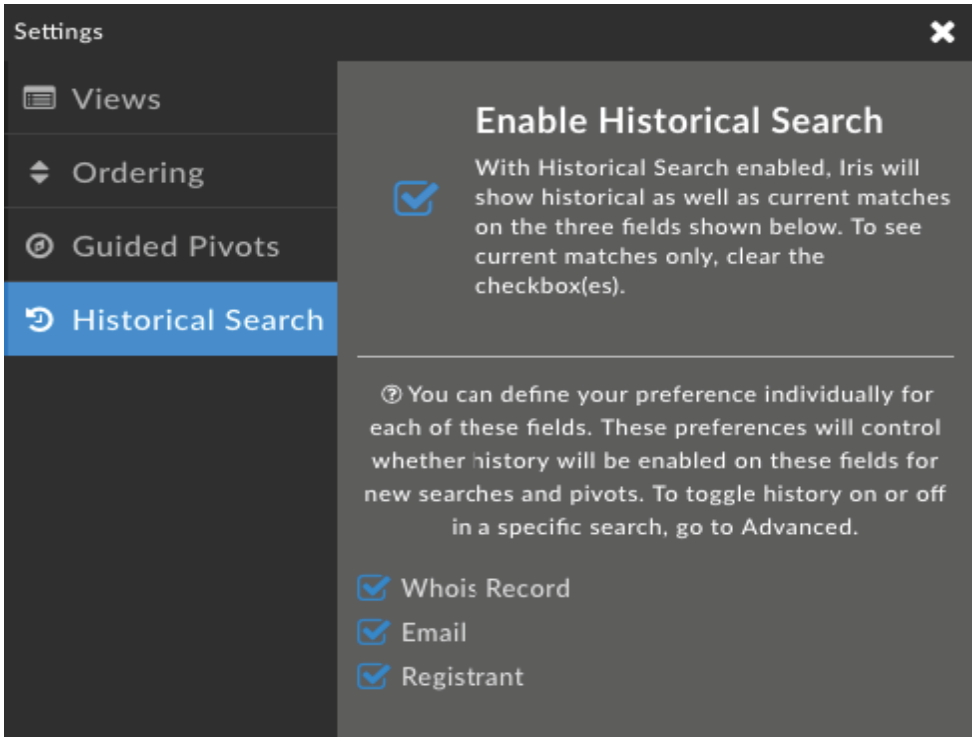


Рисунок 11.5.

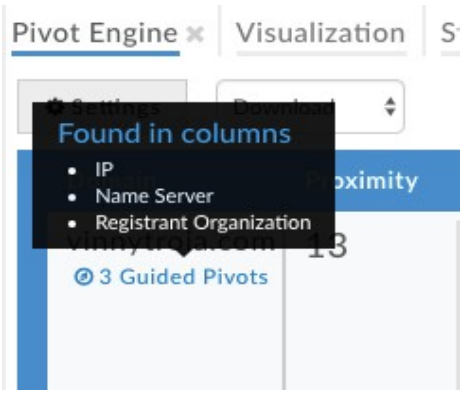


Рисунок 11.6.

Прокручивая список столбцов в Pivot Engine, IP-адрес
выделена как потенциальная точка разворота, как показано на Рисунке 11.7.
Кажется, это хорошее место для начала нашего путешествия по кроличьей норе. К
расширьте наш поиск на этот IP-адрес, щелкните правой кнопкой мыши IP-адрес и выберите «Развернуть»
Найдите (рисунок 11.8).
Данные пользовательского интерфейса в Pivot Engine изменятся, чтобы теперь отображать любые домены.
используя (или использовали) нашу текущую область поиска IP-адресов (рисунок 11.9).
Глядя на результаты, вы видите несколько доменов в наборе результатов, все из
которые принадлежат мне. Здесь нет ничего удивительного, но когда мы начнем применять это
подход к идентификации доменов, принадлежащих действительным злоумышленникам, результаты будут
кажутся намного интереснее.
Имейте в виду, что поиск доменов, которые размещены на уникальных (не общих)
IP-адреса могут быть редким явлением, поэтому давайте продолжим наш поиск, посмотрев
для других сводных полей.

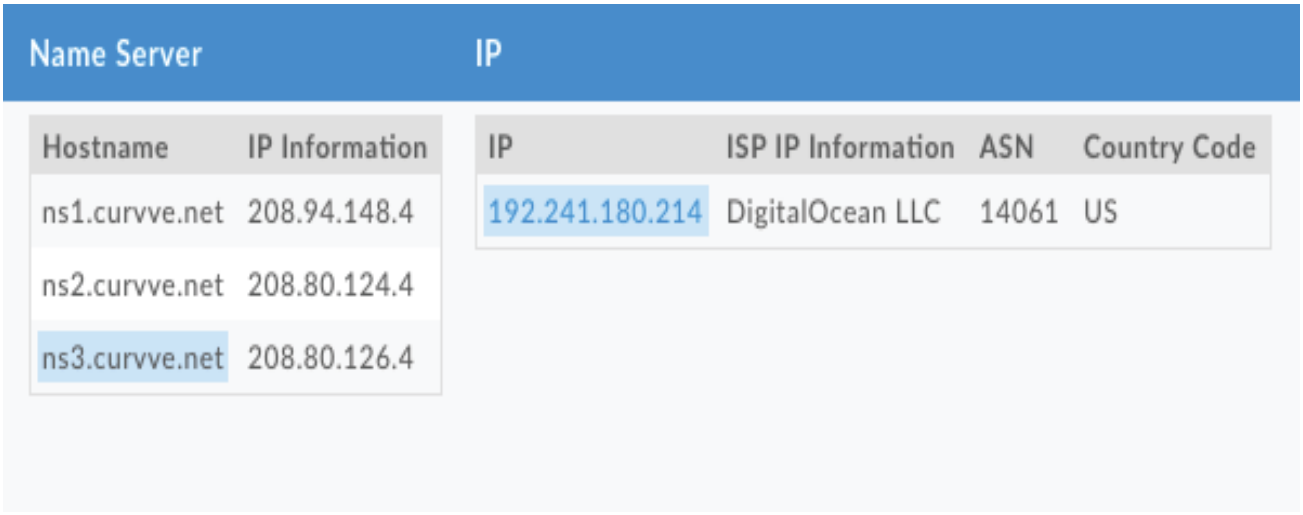


Рисунок 11.7.

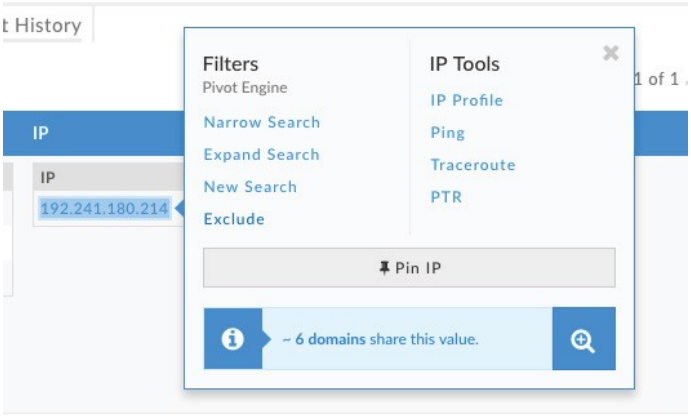


Рисунок 11.8

Вращение по хешам сертификатов SSL

SSL-сертификаты - отличный способ классифицировать домены и часто предоставляют
связи между связанной инфраструктурой. В предыдущей главе были показаны
способность находить связанные домены с помощью хэшей SSL-сертификатов или темы
имена. Iris привносит эту функциональность в свою собственную платформу, позволяя исследовать
участников, которые следят за лидами, основываясь на той же информации о прозрачности SSL-сертификата.
Глядя на информацию о сертификате для моего личного домена VinnyTroia.
com и домен моей компании NightLionSecurity.com (показан на рис. 11.10),
вы видите очевидные различия в сертификате SSL.
Два домена имеют одинаковый хэш SSL и имя субъекта. В
Хэш и тема NightLionSecurity.com уникальны для этого домена, который
почему данные не выделены. Других совпадений нет.
Чтобы изучить одну из выделенных точек поворота хэша SSL, щелкните хэш правой кнопкой мыши.
и выберите «Развернуть поиск», чтобы расширить поиск и включить в него домены, использующие
этот новый хеш SSL (рисунок 11.11).
Вы также можете начать новый поиск или сузить результаты поиска,
Это означает, что будут отображаться только сайты, которые используют выбранный хеш SSL. До
теперь в предыдущих примерах использовалась опция «Развернуть поиск», которая продолжается
чтобы добавить к общему количеству совпадений.

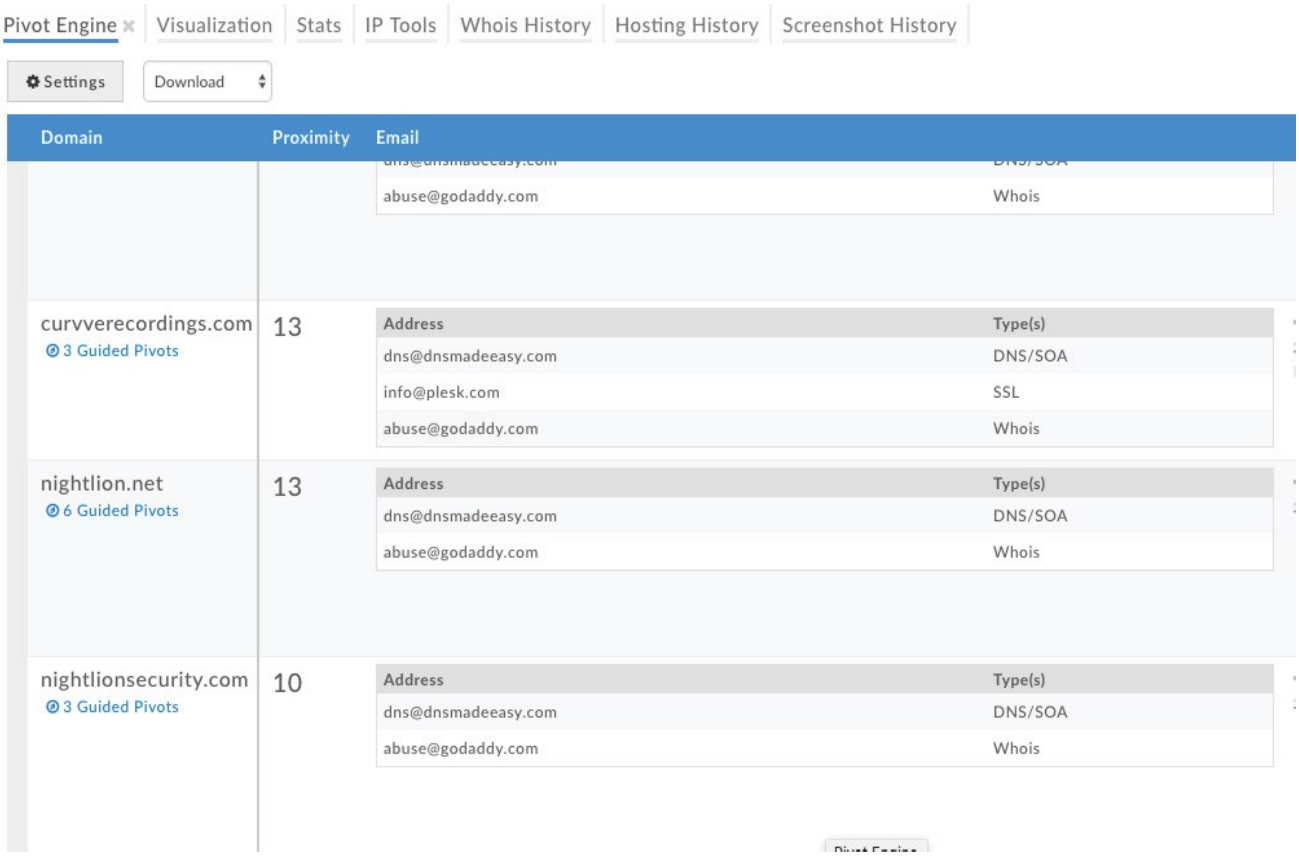


Рисунок 11.9

На рисунке 11.12 показан расширенный поиск хэша SSL в моем частном Интернете.
сервер.

Теперь готовим! После поиска SSL-сертификатов с похожим хешем
value, мы видим как минимум три новых сайта, которых не было в предыдущем списке.

Ведение заметок

Каждый раз, когда вы открываете для себя новый контент, вы должны добавлять его в
карта разума, таблица Excel или что-то еще, к чему вы можете вернуться и легко сослаться
ence. Чем дальше вы пройдете по кроличьей норе, тем больше информации вы получите.
раскрыть, и это не займет много времени, прежде чем вы забудете и потеряете
отслеживание потенциально ключевой информации. Вам нужен способ документировать
и отслеживайте все, что вы находите по пути (подробности я рассказываю самостоятельно
метод, начиная с главы 16).

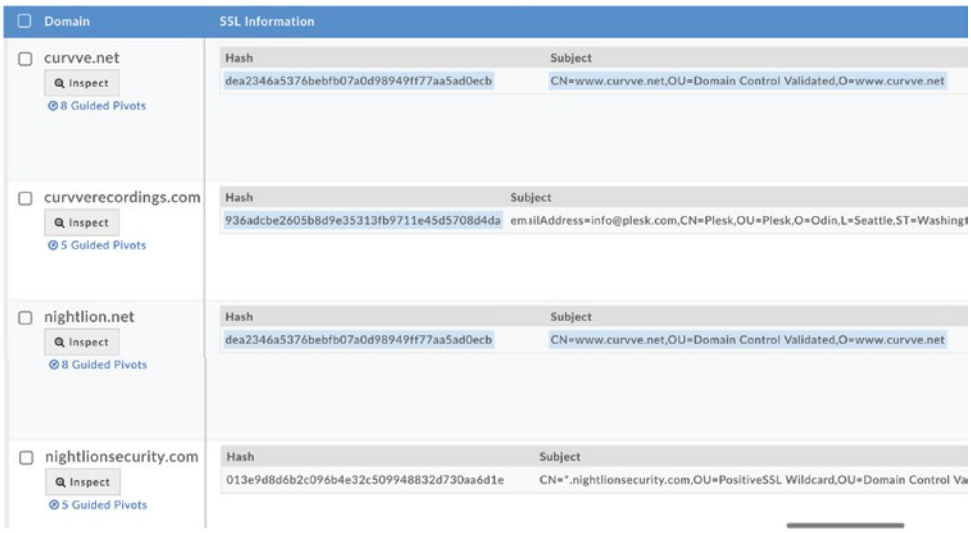


Рисунок 11.10.

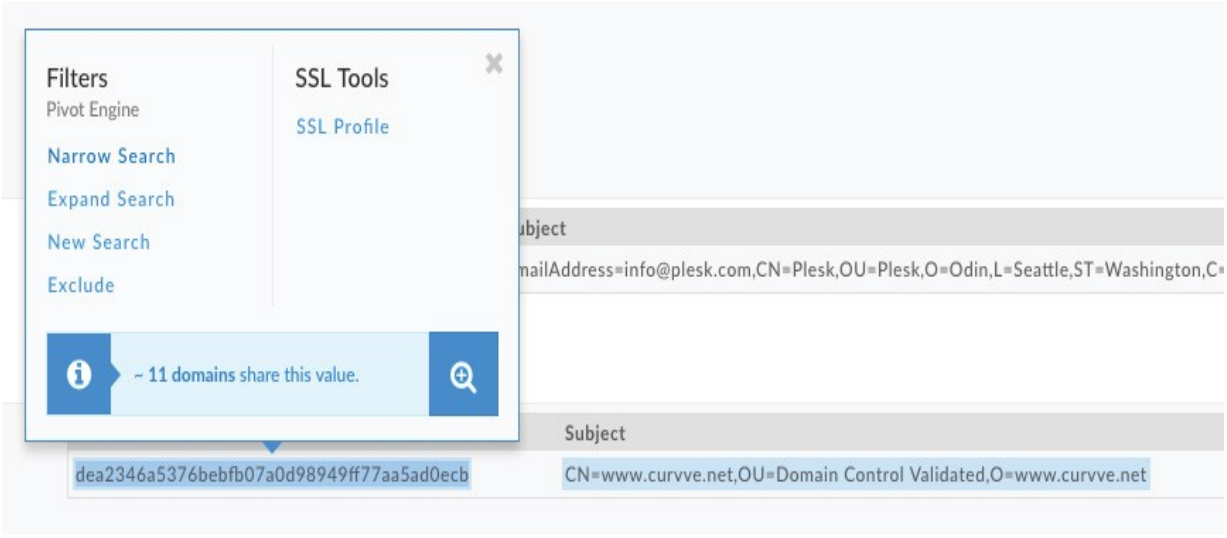


Рисунок 11.11

У Айрис есть собственный метод отслеживания следов вашего расследования. Ирис про-
в каждой точке поворота есть раздел «примечания», где вы можете задокументировать, что
вы делали, почему вы решили развернуться в определенном направлении, и любые другие
заметки, которые вы хотите оставить себе, чтобы помочь вам вспомнить, почему вы закончили
где ты делал. На рисунке 11.13 показано окно заметок в Iris.

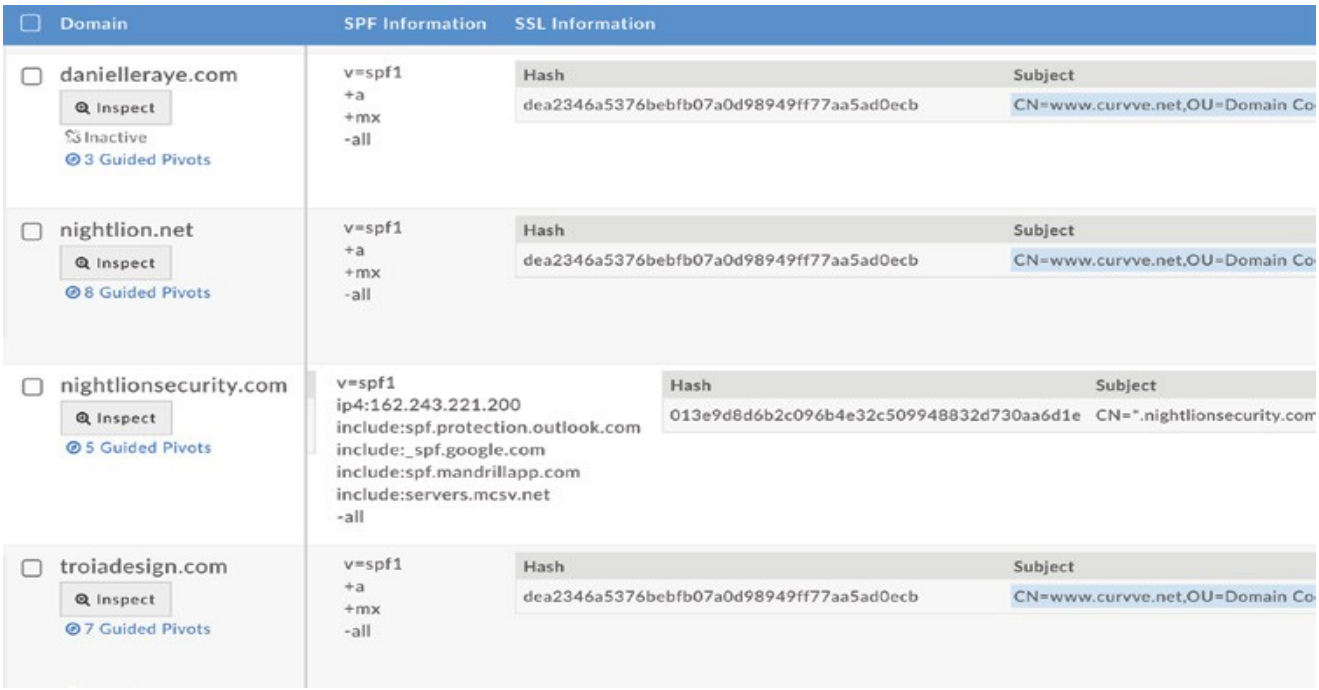


Рисунок 11.12

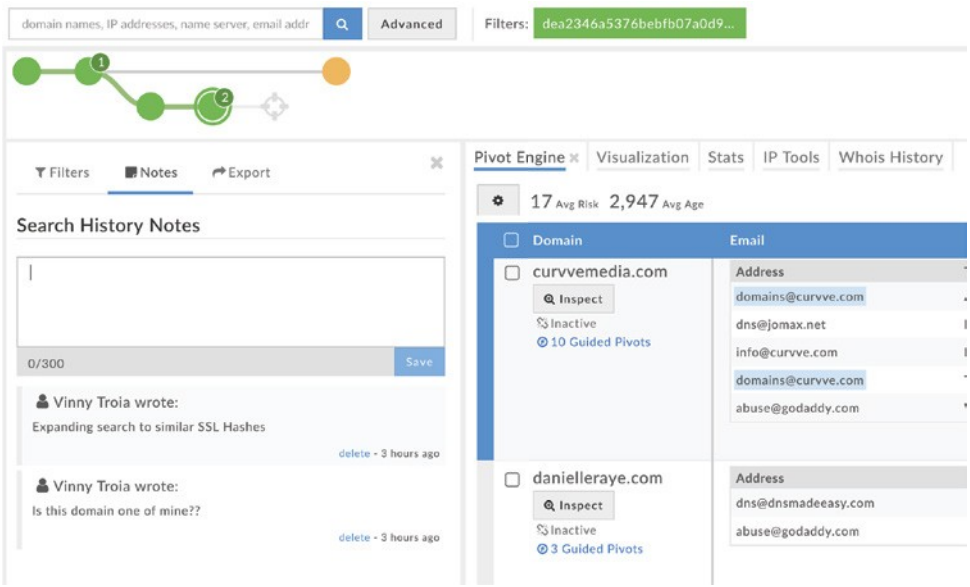


Рисунок 11.13

История WHOIS

После нашего исследования сертификатов SSL и связанных доменов следующий логический
Шаг - поиск истории WHOIS всех новых целевых доменов. Мы уже
нашел горстку, просто просмотрев аналогичную информацию о регистранте, а в
В предыдущем разделе мы нашли еще несколько, ища общие SSL-сертификаты.
Вкладка «История WHOIS» на Iris является наиболее полной записью регистрации домена.
доступна трация. Период. Мне еще предстоит найти источник регистрационных данных,
еще в DomainTools (а это почти два десятилетия). На рисунке 11.14 показано
записи истории WHOIS после выполнения поиска в моем личном домене,
vinnytroia.com .
История WHOIS на этой вкладке упорядочена по дате - с моим доменом,
результаты датируются 2003 годом.
Для любознательного читателя вы можете посмотреть мои результаты за 2003 год и увидеть адрес
в мою старую квартиру в Нью-Йорке. (См. Рисунок 11.15.)

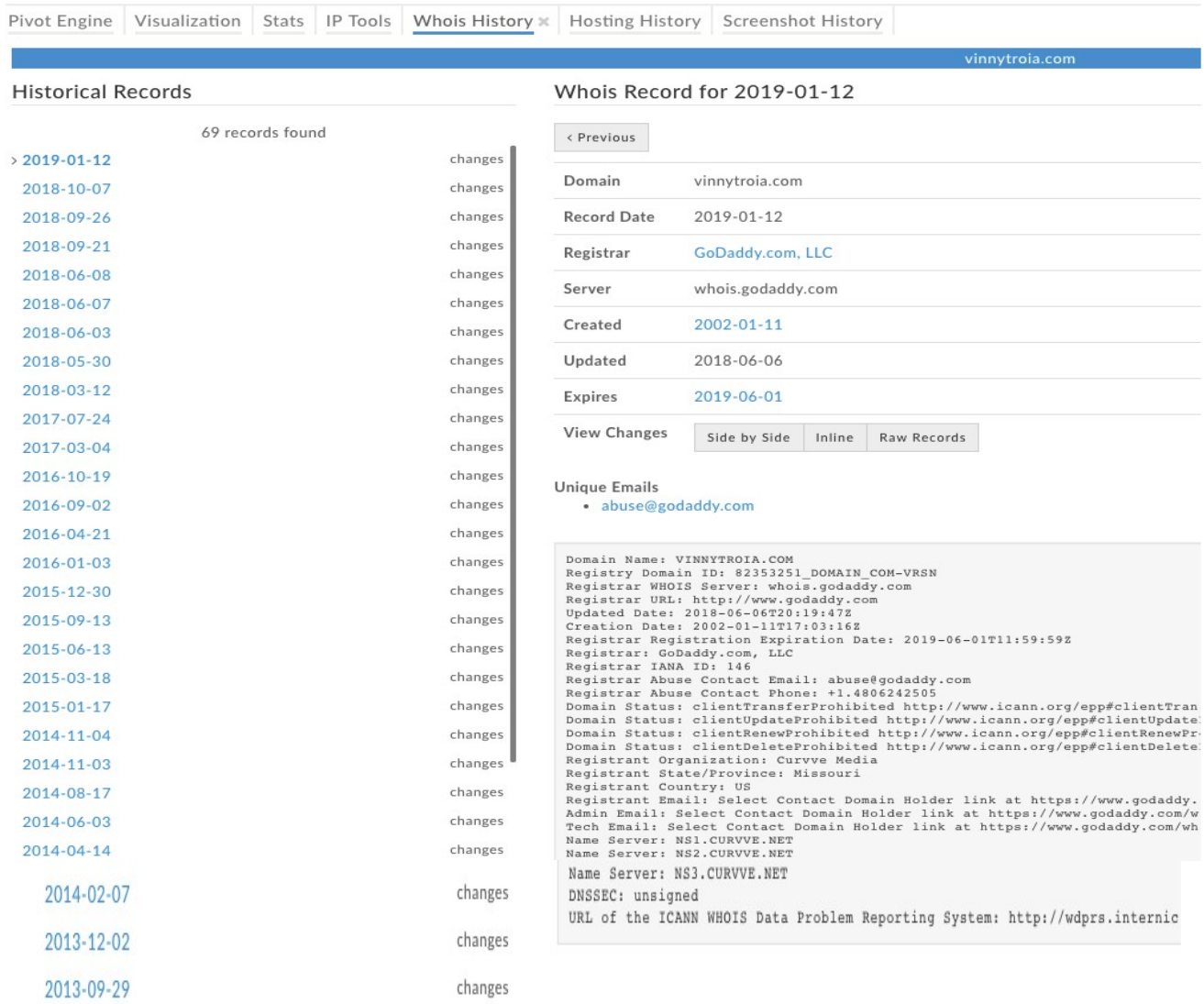


Рисунок 11.14.

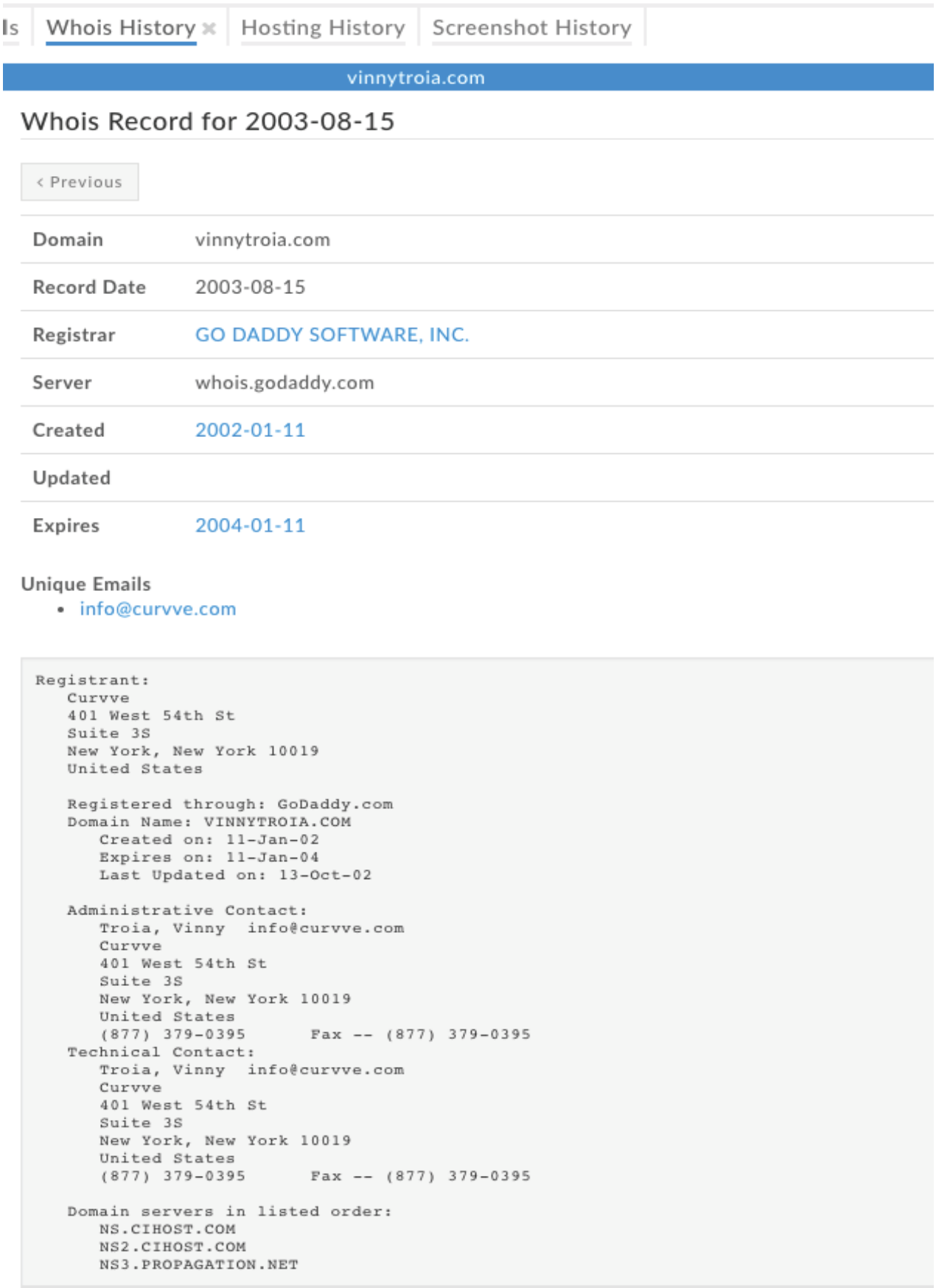


Рисунок 11.15

Это очень мощный инструмент, особенно если учесть тот факт, что большинство субъекты угроз были в какой-то момент занесены, и их оперативная безопасность (OPSEC), вероятно, не был таким уж сильным. Скид, или сценарий-кидди, - это термин, используемый для описания молодых и неопытных людей. опытные хакеры.

Это никогда не подводит: если вы вернетесь достаточно далеко, вы всегда найдете точку, где они были слишком молоды и наивны, чтобы понять, что они оставили след. Тщеславие всегда является главной темой для черные шляпы - они всегда хотят, чтобы мир знал об их достижениях. Это именно то, что произошло с угрожающим актером Сайпером (подробнее о нем в следующей главе). Часто тщеславие актера приводит к какой-то оплошности или неправильной конфигурации, потенциально при регистрации доменного имени, поэтому Iris является одним из самых мощных инструменты в моем арсенале.

История скриншотов

Я считаю этот раздел Ирис особенно полезным, потому что он означает, что мне не нужно идти прочесывать архивы Wayback на предмет всех возможных изменений. Конечно, Иногда DomainTools мог пропустить снимок экрана или изменение сайта, поэтому результаты всегда следует подтверждать и проверять с помощью ручного тестирования (в других слова, вернитесь и убедитесь, что ничего не пропустили).

Глядя на историю скриншотов моего сайта (рис. 11.16), мы видим результаты. восходит к 2004 году. Это отличный пример, потому что я уверен, что мой первый сайт был запущен раньше. Это идеальный случай, когда Wayback скорее всего есть дополнительная информация, которой нет на Iris.

Если все еще возникает вопрос, почему это важно, продолжайте читать. Конец в этой главе будет показан живой пример того, как исследователь может все это информацию вместе, чтобы сформировать конкретный вывод.

История хостинга

Наконец, вкладка Hosting History в Iris может предоставить еще больше подсказок относительно владелец домена в зависимости от того, где находится IP. Это не должно вызывать удивления злоумышленники могут (и часто делают) указывать субдомены на свой домашний IP-адрес. В любом случае знание того, где размещен сайт, может оказаться важным часть информации. Если сайт размещен на Amazon, Azure или другом гиганте хостинг-провайдер, это, вероятно, тупик для этого направления исследований, если вы может связать это с некоторыми другими данными.

На рисунке 11.17 показана вкладка Hosting History для моего личного веб-сайта, который включает различные IP-адреса до и после действия. Это может быть чрезвычайно полезно, если кто-то решает разместить домен с частного сервера, например, их дом.

Обнаруженная история хостинга показывает все разные IP-адреса из моего Интернета.
сервером еще в 2003 году. Один из возможных вариантов поиска на этом этапе - изучить каждый
IP-адресов, чтобы узнать, не привязаны ли к этим IP-адресам какие-либо другие вредоносные или сомнительные сайты.
Это будет очень трудоемкий процесс, поэтому одно предложение:
использовать функцию заметок Iris, упомянутую ранее в этой главе. Заметки Ирис могут быть
размещены в любой точке поворота и поиска, который вы выполняете, что сделает очень
хороший способ помочь вам вернуться назад и понять, как и почему вы пришли к
конкретный момент в вашем исследовании.
Вы никогда не знаете, когда появится информация (например, IP-адрес)
позже в ходе расследования, поэтому обязательно задокументируйте свои результаты таким образом, чтобы
можно будет легко найти позже.

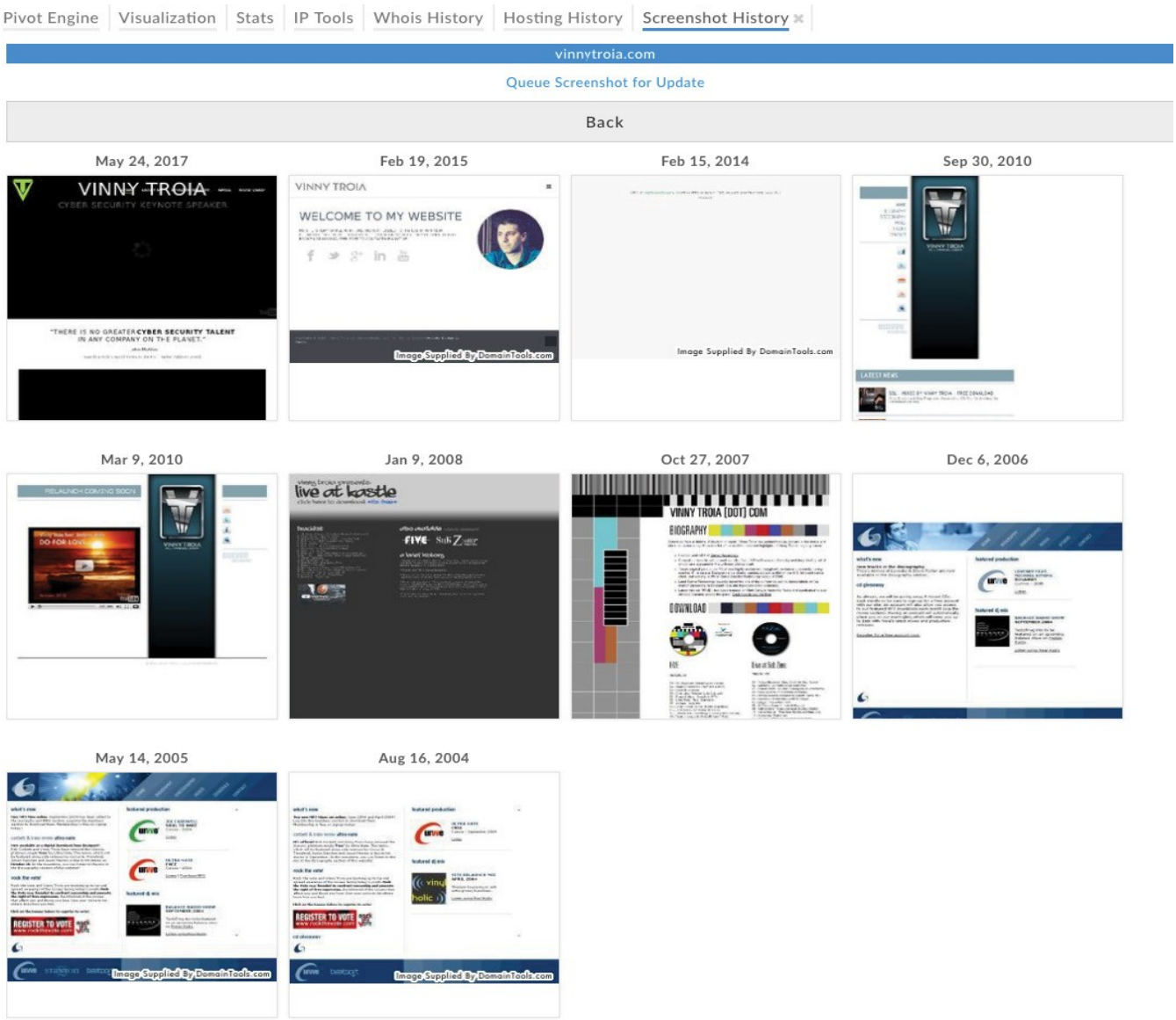


Рисунок 11.16

Функция заметок Iris поможет вам отслеживать каждый поиск и направлять вас
делать. Заметки также можно экспортировать, что само по себе удивительно. Когда вы
готово, вы можете экспортировать все свои заметки в один гигантский файл для дальнейшего использования.

Собираем все вместе

Важность очистки старых версий веб-сайта обсуждалась ранее.
в этой главе, но чтобы понять суть, давайте еще раз взглянем на наши
друг WhitePacket.

В главе 9 вы видели, что данные регистрации домена для WhitePacket.com
показали отсутствие информации о владельце (т. е. срок действия домена истек) в период с 2014 г.
и 2015. На рисунке 11.18 показана история регистрации домена для WhitePacket.
com . (Если данные регистрации домена являются частными, будет немного
Значок «глаз», чтобы вы знали:.)

Мы не можем считать владельцев одним и тем же человеком. На самом деле, давайте с
предположение, что это не так. Первое, что мы можем сделать, это посмотреть на исторические
данные домена, чтобы узнать, сможем ли мы найти какие-либо интересные подсказки о новых
владелец. На рисунке 11.19 показаны исторические снимки экрана рассматриваемого домена.

Pivot Engine | Visualization | Stats | IP Tools | Whois History | Hosting History | Screenshot History

vinnytroia.com

IP Address History | Registrar History | Name Server History

Event Date	Action	Pre-Action IP	Post-Action IP
2018-11-05	Change	192.124.249.105	192.241.180.214
2018-10-17	Change	162.243.221.200	192.124.249.105
2016-01-03	Change	104.27.154.71	162.243.221.200
2015-06-24	Change	104.28.6.104	104.27.154.71
2015-03-06	Change	108.162.192.152	104.28.6.104
2015-02-21	Change	104.28.6.104	108.162.192.152
2014-11-03	Change	107.170.142.112	104.28.6.104
2014-07-09	Change	162.243.6.162	107.170.142.112
2014-03-31	Change	198.211.113.108	162.243.6.162
2013-06-12	Change	107.23.116.26	198.211.113.108
2012-11-01	Change	205.186.165.181	107.23.116.26
2011-09-05	Change	74.208.238.129	205.186.165.181
2011-04-10	New	-none-	74.208.238.129
2011-02-13	Change	74.208.238.154	74.208.238.129
2010-12-19	Change	74.208.109.38	74.208.238.154
2009-06-29	Change	74.208.63.22	74.208.109.38
2008-05-04	Change	69.13.149.247	74.208.63.22
2005-03-05	New	-none-	69.13.149.247

Рисунок 11.17

На вкладке «История снимков экрана» Ирис заметен очевидный промежуток времени между
2016 г. (когда сайт выглядел так, как будто он перенаправлялся в Twitter) и 2013 г. Обведем кружком.
назад и посмотрите, какие результаты мы получим с помощью Wayback Machine
на archive.org . На рисунке 11.20 показана обсуждаемая функция временной шкалы archive.org.
в главе 10.
На этом скриншоте видно, что archive.org показывает 21 экран.
снимается в период с 20 июля 2013 г. по 30 ноября 2018 г. Интересно отметить
что результаты в Iris идут дальше назад, но у Wayback больше данных (просто еще один
дружеское напоминание никогда не полагаться на единый источник всей вашей информации
встреча).



Рисунок 11.18

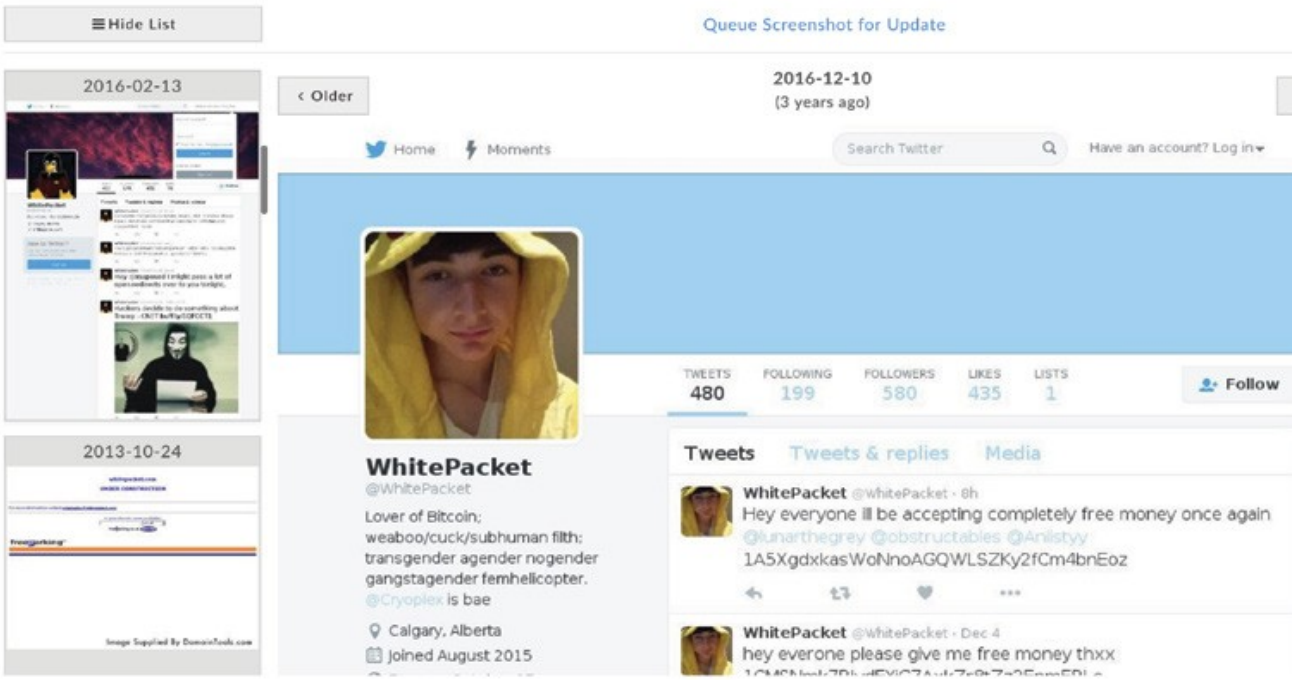


Рисунок 11.19

Копаясь в архивах страниц, в 2015 году особо отметить нечего.

Далее, обзор первого захвата в 2016 году открывает заархивированную страницу, которая дает нам множество новой информации, в том числе отзывы, показанные в Рисунок 11.21.

В дополнение к характеристике, в которой указано имя владельца, на рис. 11.22 показано дополнительная контактная информация. Бинго.

В контактной информации, расположенной на странице, указаны два телефонных номера: физический адрес, адрес электронной почты (# 4), который ссылается на другой домен, и три страницы в социальных сетях. Теперь у нас есть восемь новых фрагментов информации для изучения.

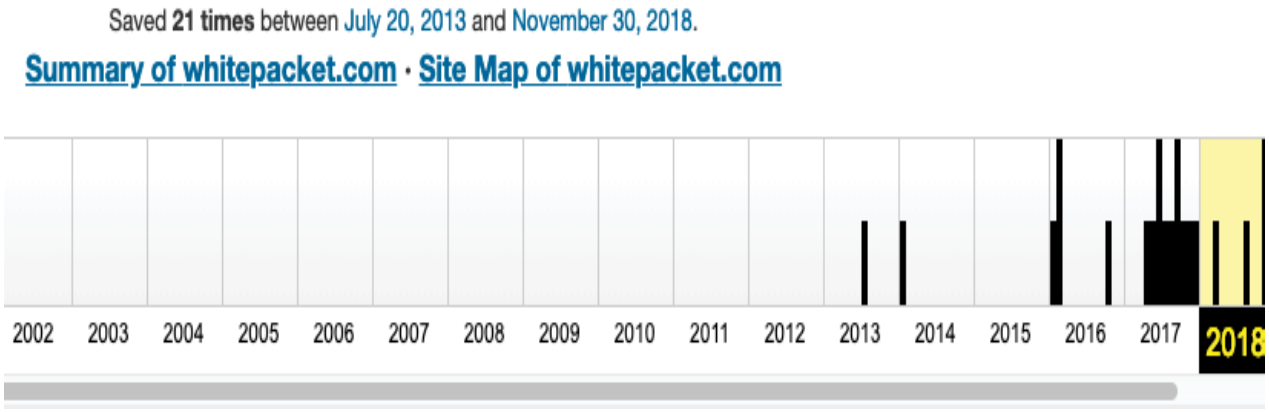


Рисунок 11.20.

I rarely write testimonials, but Mr. Meunier (WhitePacket) is one of the exceptions. Some months ago we got a warning from an XSSposed report about a potential threat on one of our websites. With a big concern from upper management and IT security, we were trying to patch the hole as quick as we could. I was testing my luck and contacted WhitePacket directly as he was the original white-hat hacker who found the bug, surprisingly enough, he did respond! Thanks, WhitePacket (Christopher Meunier) for giving us the clear explanation and the valuable advice, we had the patch in a matter of just a few hours. I'm not in the position of representing my organization but from the bottom of my heart, I again thank Mr. Meunier for his hard work, rich knowledge, and the good heart of being a white-hat hacker.

Рисунок 11.21

CONTACT

(61 2) 9251 5600

info@themesun.com

No.200 Joseph, Canada 10020

(61 2) 9200 5700

RECENT PROJECTS

- Facebook
- twitter
- linkedin

Copyright © 2015 WhitePacket.

Рисунок 11.22

**Большинство людей воспримут эту информацию и сразу начнут следить за новым кроликом.
яма и копаться в новых уликах. Вот где я бы посоветовал потренироваться
сдержанность. Как бы увлекательно ни было следовать новому примеру, это, скорее всего, будет означать, что
вы забудете вернуться и завершить поиск по** Archive.org **(или как там
это то, что вы ищете в данный момент). В вашем
текущий следственный процесс (а в данном случае есть). Обратите внимание: если вы
немедленно отправляйтесь исследовать, важные подсказки могут (и будут) упущены. В других
слов, постарайтесь сдержать импульс перейти к чему-то новому и закончить
текущая задача в первую очередь. Потратив немного больше времени сейчас, вы потенциально можете
расплата позже.**

Например, в будущих версиях сайта будет отображаться обновленный адрес электронной почты.
и номер телефона, как показано на рисунке 11.23.

После того, как все возможные архивы сайта будут изучены и исчерпаны, мы можем перейти
назад и начните исследовать нашу новую информацию. Ранее в этой главе
мы показали, что информация о сертификате SSL для WhitePacket.com также была
связаны с 46 другими доменами.

Мы не можем сказать с какой-либо степенью уверенности, что все домены принадлежат
тот же владелец, поэтому единственное, что мы можем сделать, это проверить. Быстрая перемотка вперед
Во всех ручных исследованиях мы находим две области, представляющие интерес:

- MindBendingBeats.ca
- Anonimo.ninja

MindBendingBeats.ca - это сайт, который продает бинауральные ритмы за биткойны. Может быть, мы
может повезти и найти адрес криптокошелька в архивах. Чтобы ускорить это
процесса, мы можем использовать Photon (обсуждается в главе 10) или другой полезный Python
инструмент под названием wayback-machine-scraper для загрузки архива всех страниц
кэшируется Wayback Machine (archive.org).

Следующий код показывает результат использования wayback-machine-scraper для
выполнить эту задачу:

```
2019-02-26 08:18:33 [scrapy.core.engine] ИНФОРМАЦИЯ: Паук открыт
2019-02-26 08:18:33 [scrapy.extensions.logstats] ИНФОРМАЦИЯ: просканировано 0 страниц
```

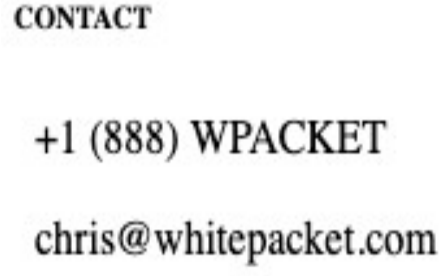


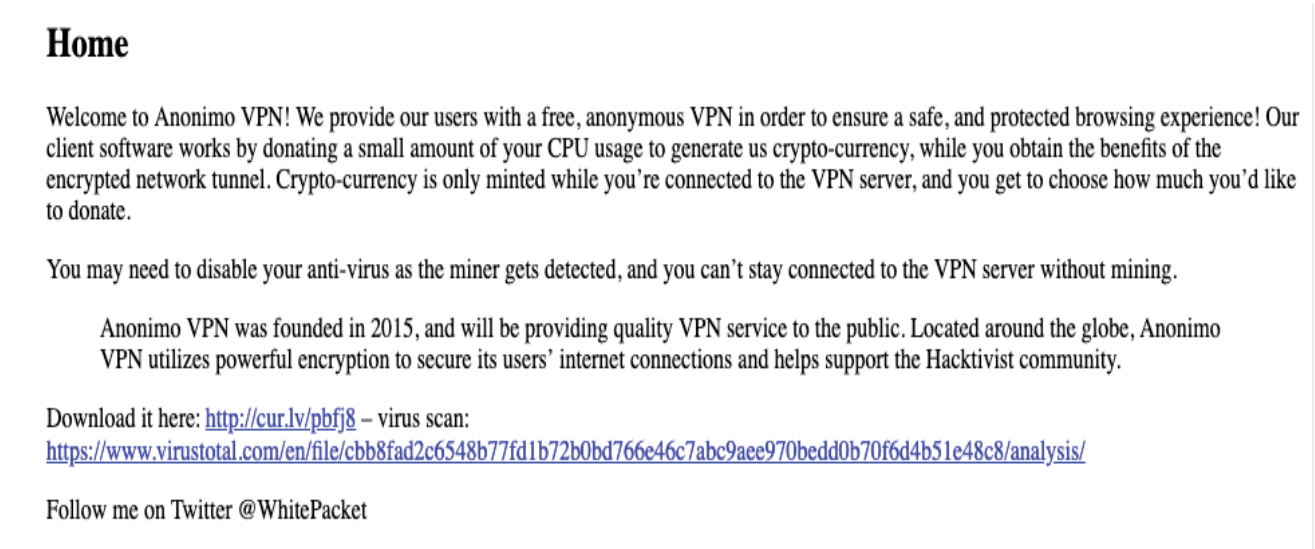
Рисунок 11.23

(при 0 стр. / мин.), извлечено 0 элементов (при 0 стр. / мин.)
2019-02-26 08:18:37 [scrapy.core.engine] ИНФОРМАЦИЯ: Закрытие паука (завершено)
2019-02-26 08:18:37 [scrapy.statscollectors] ИНФОРМАЦИЯ: статистика сброса Scrapy:
{'загрузчик / request_bytes': 6021,
'downloader / request_count': 17,
'downloader / request_method_count / GET': 17,
'загрузчик / response_bytes': 72542,
'downloader / response_count': 17,
'downloader / response_status_count / 200': 17,
'dupefilter / filter': 32,
'finish_reason': 'готово',
'finish_time': datetime.datetime (2019, 2, 26, 8, 18, 37, 320617),
'log_count / INFO': 7,
'memusage / max': 50098176,
'memusage / startup': 50098176,
'offsite / domains': 8,
'offsite / отфильтровано': 40,
'request_depth_max': 1,
'response_received_count': 14,
'планировщик / исключен из очереди': 26,
'scheduler / dequeued / memory': 26,
'планировщик / поставлен в очередь': 26,
'планировщик / поставлен в очередь / память': 26,
'start_time': datetime.datetime (2019, 2, 26, 8, 18, 33, 470619)}
2019-02-26 08:18:37 [scrapy.core.engine] ИНФОРМАЦИЯ: Паук закрыт (завершено)

Wayback-machine-scraper вернул восемь кешированных страниц и, посмотрев через код ни один из них не содержал кошелька BTC. Очень жаль. Также страницы не содержал ничего ценного. Далее посмотрим на Anonimo.ninja.

Глядя на сайт Archive.org , мы сразу видим на рисунке 11.24, что владелец тот же самый из-за связанной страницы Twitter (@WhitePacket).

Теперь, когда мы знаем, что владелец тот же самый, давайте посмотрим, есть ли что-нибудь Размещение в копии сайта. Читая сайт, копия сайта указывает что Anonimo.ninja - это VPN-клиент, который также является майнером биткойнов. Загрузка



Home

Welcome to Anonimo VPN! We provide our users with a free, anonymous VPN in order to ensure a safe, and protected browsing experience! Our client software works by donating a small amount of your CPU usage to generate us crypto-currency, while you obtain the benefits of the encrypted network tunnel. Crypto-currency is only minted while you're connected to the VPN server, and you get to choose how much you'd like to donate.

You may need to disable your anti-virus as the miner gets detected, and you can't stay connected to the VPN server without mining.

> Anonimo VPN was founded in 2015, and will be providing quality VPN service to the public. Located around the globe, Anonimo VPN utilizes powerful encryption to secure its users' internet connections and helps support the Hacktivist community.

Download it here: http://cur.lv/pbfj8 – virus scan:
https://www.virustotal.com/en/file/cbb8fad2c6548b77fd1b72b0bd766e46c7abc9aee970bedd0b70f6d4b51e48c8/analysis/

Follow me on Twitter @WhitePacket

Рисунок 11.24

ссылка для «Anonimo VPN.exe» не работает, но, к счастью, ссылка Virustotal
все еще активен.
На рисунке 11.25 показан результат поиска клиента Anonimo VPN.exe.
на Virustotal.
Виртуальные комментарии к этому файлу (рис. 11.26) выглядят подозрительно.
Судя по комментариям, похоже, что программное обеспечение VPN нашей цели было
на самом деле биткойн-майнер (о котором мы уже знали из описания сайта).
Хорошая новость заключается в том, что подпись оставила нам IP-адрес за пределами
Cloudflare: 199.168.147.147. Поиск по этому IP-адресу в Virustotal дает нам
информация о владельце показана на рисунке 11.27.
Глядя на данные, мы видим, что ASN (и хост) - это VolumeDrive.
(www.volumedrive.com). Из этой информации ничего нельзя сделать (пока), но она
Важно отметить, что информация может появиться позже.

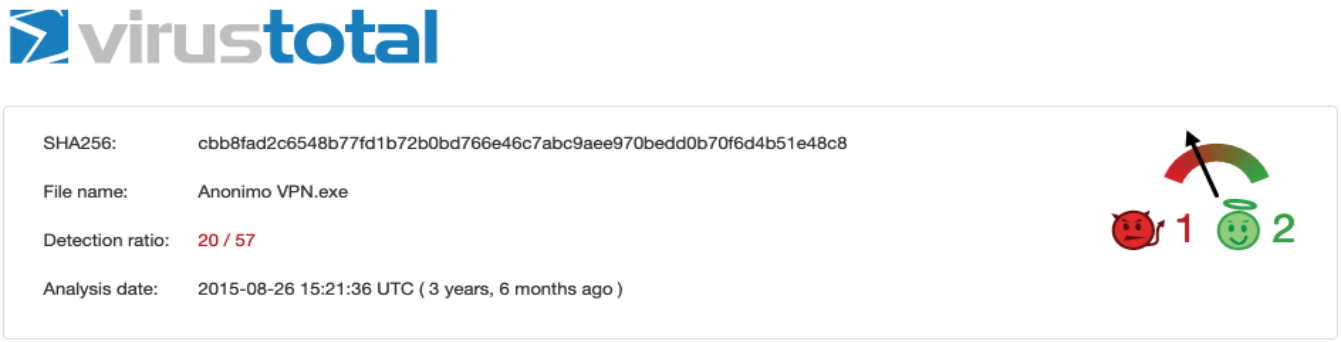


Рисунок 11.25



Рисунок 11.26

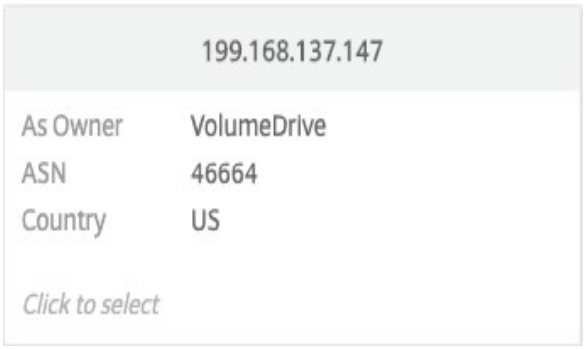


Рисунок 11.27

Основная находка

Предыдущий сценарий был всего лишь одной нитью возможного пути расследования.
На самом деле внутри был обнаружен довольно значительный фрагмент информации.
те результаты, которые я осознал намного позже.
Когда мы смотрели историю скриншотов для WhitePacket.com , там
был скриншот его старого аккаунта в Twitter 2016 года. На рисунке 11.28 показан
увеличенная версия этого скриншота.
Эта находка *очень тонкая* , и так было до тех пор, пока я не написал последние главы.
из этой книги, что я это понял.
Чтобы поместить это в надлежащий контекст, ниже приведены выдержки из единственного
разговор с TDO:
TDO:
Мы совсем не «братаны», приятель.
VT:
видите, и в своем электронном письме вы сказали, что мы друзья.
TDO:
Тебе повезло сегодня вечером.
VT:
Но хорошо, я понимаю. я сохраню это полностью
профессионально отныне. Не хотел обидеть
TDO:
Я сижу здесь, перемещаю терабайты данных в новый
сервер, и мне скучно, так что вы были благословлены
общается со мной.
TDO:
Да, проявите уважение к вам, рогоносец.



Рисунок 11.28

TDO:
Отвали, где твой алкоголь?
VT:
я выйду завтра вечером и обязательно заберу
немного пива по дороге домой для нашей следующей беседы
TDO:
Ты такой гребаный.
TDO:
Я здесь единственный, на кого влияют наркотики,

TDO:
Ваш сайт - ДЕРЬМО.
TDO:
Его взламывают ЕЖЕДНЕВНО.
TDO:
Ты тупой куколд.
VT:
да кстати
VT:
кто такой аргон
TDO:
Нет, мы не отвечаем.
VT:
потому что ты не знаешь?
TDO:
Потому что мы не отвечаем.

Вы что-нибудь заметили?

Теперь вернемся к WhitePacket, говорится в описании на его личной странице в Twitter. . .
«Любитель биткойнов: Weaboo **/ cuck /** нечеловеческая грязь». Важное слово здесь
это "cuck".

2:07 утра
TDO
Ты тупой **куколд.**

Я лично провел тысячи часов, разговаривая с разными угрозами
актеров как в приватных чатах, так и на форумах. Я ни разу - ни одного
время - когда-либо слышал (или видел), что кто-то употребляет слово «рогоносец».
Я не поверенный, поэтому не могу сказать, насколько важной будет эта находка.
быть в зале суда. Однако я знаю, что обычная техника, используемая законом
правоохранительные органы включают поиск общих черт в языковом поведении,
таких как использование уникальных слов и повторяющиеся грамматические ошибки (например, *их*
vs. *там*).
В сочетании со всеми другими доказательствами я подозреваю, что эти случаи употребления слова
«Cuck» на самом деле довольно значительны.

Резюме

В этой главе продемонстрированы мощь и широта охвата, доступного в Iris от
DomainTools. Я решил продемонстрировать Iris, несмотря на то, что это инструмент премиум-класса, потому что
огромной ценности, которую он предоставил мне во время моего расследования. Я могу сказать без
никаких сомнений, что я не смог бы найти столько улик и кусочков
вместе так много исторической информации о владении доменом без доступа к
этот инструмент.

В этой главе выделен ряд ключевых функций Iris и рассмотрен процесс использования этих функций для выявления владельца домена имя. Предоставленной информации должно быть достаточно, чтобы вы могли решить, стоит ли доступ к этому типу премиум-инструментов необходим вашей организации.

Следующая глава ознаменует начало третьей части этой книги, в которой мы начнет поиск золота с изучения метаданных документа.

III

Копаем золото

В этой части

Глава 12: Метаданные документа

Глава 13: Интересные места для поиска

Глава 14: Общедоступное хранилище данных

Этот раздел будет посвящен поиску данных в разных и необычных местах. В качестве
название предполагает, что в этом разделе мы будем копать золото, что означает
основное внимание будет уделено инструментам и методам, которые помогут раскрыть полезные (а часто и
скрытая) информация из часто упускаемых из виду уголков Интернета.

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.

© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

245

12

Метаданные документа относятся к информации, которая хранится в файле и используется
для предоставления контекста или описания этого файла. Метаданные часто невидимы и
предоставляет вспомогательную информацию о файле, в котором он хранится.
Метаданные документа могут включать в себя такие части информации, как
название, программное обеспечение, использованное для его создания, имя автора или организации, в которой
он был создан, имя компьютера, на котором он был создан, и дата
и время, когда файл был впервые создан или изменен.
Помимо базовой информации о метаданных, файлы разных типов могут содержать
различные типы метаданных, которые также могут различаться в зависимости от программного обеспечения,
используемого для
создайте этот файл. Количество метаданных, которые в конечном итоге сохраняются вместе с документом.
зависит от программного обеспечения, которое использовалось для создания документа.
Все становится по-настоящему интересным, когда вы сталкиваетесь с конфиденциальными документами.
элементы, метаданные которых не были удалены. Метаданные в этих
документы (особенно на фотографиях) могут содержать невероятно конфиденциальную информацию.
Например, в 2016 году произошел скандал, связанный с утечкой обнаженной натуры.
фотографии знаменитостей. Фотографии были украдены из личных аккаунтов пострадавших.
и просочился в сеть. После анализа метаданные на фотографиях содержали
очень конкретная и идентифицируемая информация, такая как тип камеры (или телефона),
настройки объектива, дата и время съемки и даже его геолокация!
Этот тип информации может предоставить существенное свидетельство
правильные обстоятельства. Быстрый поиск в Интернете также покажет несколько прошлых

Метаданные документа

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

новости, в которых беглецы размещали фотографии в своих учетных записях в социальных сетях, и
метаданные из этих документов в конечном итоге помогли их аресту.
Это всего лишь несколько примеров. Важно помнить, что все
в документах хранится какая-то информация о метаданных. Этот
В главе будут рассмотрены различные инструменты, которые мы можем использовать для поиска и извлечения метаданных.
из разных типов документов.

Exiftool

Exiftool - это независимый инструмент командной строки, используемый для чтения, записи и
редактирование метаинформации в файлах. Поддерживаемые форматы метаданных включают EXIF,
GPS, ID3, XMP, GeoTIFF и большинство цифровых камер (включая Canon,
Fuji, Kodak, Nikon и многие другие). В дополнение ко всем различным мета-
форматы информации, поддерживаемые Exiftool, он также может читать эту метаинформацию
практически из всех известных типов файлов, включая, помимо прочего, PDF-файлы, документы
элементы, электронные таблицы, изображения, аудиофайлы и видеофайлы.
Вы можете скачать Exiftool по адресу https://www.sno.phy.queensu.ca/~phil/exiftool .
Чтобы продемонстрировать потенциал инструмента, я использую образцы изображений из
Репозиторий Ианаре Севи на GitHub с образцами изображений для тестирования получения метаданных:
https://github.com/ianare/exif-samples .
Сам инструмент чрезвычайно прост и не имеет большого количества опций.
для демонстрации. Запуск инструмента состоит из вызова файла и включения
имя файла для анализа:

```
exiftool Canon_40D.jpg
Номер версии ExifTool
: 11.33
Имя файла
: DSCN0027.jpg
Размер файла
: 154 кБ
Дата / время изменения файла: 2019: 04: 04 04: 57: 47-05: 00
Дата / время доступа к файлу
: 2019: 04: 04 04: 57: 47-05: 00
Дата / время изменения Inode файла: 2019: 04: 04 04: 57: 47-05: 00
Права доступа к файлам
: rw-r - r--
Тип файла
: JPEG
Расширение типа файла
: jpg
Тип MIME
: изображение / JPEG
Порядок байтов Exif
: Little-endian (Intel, II)
Описание изображения
:
Делать
: NIKON
Название модели камеры
: COOLPIX P6000
Ориентация
: Горизонтальный (нормальный)
Разрешение X
: 300
Разрешение Y
: 300
Единица разрешения
: дюймы
```

Программное обеспечение
: Nikon Transfer 1,1 Вт
Изменить дату
: 2008: 11: 01 21:15:09
Версия Exif
: 0220
Дата / время Оригинал
: 2008: 10: 22 16:44:01
Дата создания
: 2008: 10: 22 16:44:01
Расстояние до объекта
: Неизвестный
[... усечено ...]
GPS Широта Ref
: Север
GPS долгота Ref
: Восток
Высота по GPS Ref
: Над уровнем моря
Отметка времени GPS
: 14: 42: 29.03
Спутники GPS
: 05
GPS Img Direction Ref
: Неизвестный ()
Датум карты GPS
: WGS-84
Штамп даты GPS
: 2008: 10: 23
Сжатие
: JPEG (старый стиль)
Смещение эскиза
: 4560
Длина эскиза
: 5803
Ширина изображения
: 640
Высота изображения
: 480
Процесс кодирования
: Базовая DCT, кодирование Хаффмана
Биты на образец
: 8
Компоненты цвета
: 3
Подвыборка Y Cb Cr
: YCbCr4: 2: 2 (2 1)
Набор инструментов XMP
: Public XMP Toolkit Core 3.5
Рейтинг в процентах
: 0
Диафрагма
: 4.1
Дата / время GPS
: 2008: 10: 23 14: 42: 29.03Z
Широта GPS
: 43 град 28 '6.39 "с.ш.
GPS долгота
: 11 град 52 '53,45 "в.д.
Положение GPS
: 43 град 28 '6,39 "северной широты, 11 град 52' 53,45" восточной долготы
Размер изображения
: 640 x 480
Мегапикселей
: 0,307

Эквивалент масштабного коэффициента до 35 мм: 4,7
Скорость затвора
: 1/148
Миниатюрное изображение
: (Двоичные данные 5803 байта, используйте параметр -b
извлекать)
Круг замешательства
: 0,006 мм
Поле зрения
: 65,5 град.
Фокусное расстояние
: 6,0 мм (эквивалент 35 мм: 28,0 мм)
Гиперфокальное расстояние
: 1,36 м
Световая ценность
: 11.9

Найти такой полностью загруженный документ во время расследования может показаться маловероятно, но реальность такова, что большинство преступников либо не разбираются в технологиях, либо просто думаю, что они непобедимы. Были зарегистрированы многочисленные случаи, когда полиция производили аресты на основании информации, записанной в метаданных документа, поэтому Вы не должны рассчитывать на это как на возможность при поиске информации!

Метагофил

Metagoofil - это инструмент для сбора информации, позволяющий извлекать метаданные. из общедоступных документов на веб-серверах. Хотя Exiftool отлично умеет чтения метаданных из файлов, которые у нас уже есть, Metagoofil поможет вам дальнейшее расследование, позволяя вам *находить* файлы о вашей цели.

Metagoofil работает, выполняя глупый поиск в Google, чтобы найти документы. документы, содержащие потенциально полезные метаданные. Его возможности включают в себя возможность для локального сохранения документов и удаленного извлечения метаданных из популярного файла типы и форматы, включая (но не ограничиваясь) документы Word, листы Excel, PDF-файлы и многое другое.

Имена, адреса электронной почты, общие ресурсы и имена серверов - это лишь некоторые метаданных, которые можно извлечь из документов с помощью этого инструмента.

Вы можете скачать Metagoofil со страницы https://github.com/laramies/metagoofil .

К параметрам Метагофила относятся:

-d: домен для поиска
-t: тип файла для загрузки (pdf, doc, xls, ppt, odp, ods, docx, xlsx, pptx)
-l: ограничение результатов для поиска (по умолчанию 200)
-h: работать с документами в каталоге (используйте «да» для локального анализа)
-n: лимит файлов для загрузки
-o: рабочий каталог (место для сохранения загруженных файлов)
-f: выходной файл

Запустить Metagoofil просто. Введите команду, а затем -d и домен, который вы хотите найти. Например:

python metagoofil.py -d apple.com

Перед запуском поиска мне нравится настраивать рабочий каталог файлов (так Metagoofil сохраняет копию всего, что находит) и создает выходной файл, чтобы я мог посмотреть мои результаты. Metagoofil также требует, чтобы вы указали, какие типы файлов искать. для (или он не запустится). Мы также уменьшим количество результатов поиска до максимума 100 и установите ограничение на скачивание файлов на уровне 100. Давайте выполним поиск с этими параметры против Busey Bank и посмотрим, что мы можем найти:

python metagoofil.py -d busey.com -t doc, pdf, xls, docx, xls, xlsx -l 100
-n 100 -o документы -f results.txt

Подождите, пока Metagoofil завершит поиск, после чего вы сможете просмотреть результаты. открыв HTML-файл. Загруженные данные могут включать имена пользователей, версии программного обеспечения, электронные письма, серверы и пути, а также файлы и метаданные каждого

файл, включая имена авторов и расположение каждого загруженного файла на машина, на которой обрабатывается поисковый запрос:

```
************************************************* ****
* / \ / \ ___ | | _ __ _ __ _ ___ ___ / _ (_) | *
* / \ / _ \ __ / _` | / _` | / _ \ / _ \ | | _ | | | *
* / / \ / \ \ __ / || (_ | | (_ | | (_) | (_) | _ | | | *
* \ / \ / \ ___ | \ __ \ __, _ | \ __, | \ ___ / \ ___ / | _ | | _ | _ | *
*
| ___ /
*
* Metagoofil версии 2.2
*
* Кристиан Марторелла
*
* Edge-Security.com
*
* cmartorella_at_edge-security.com
*
************************************************* ****
['pdf']
[-] Запуск онлайн-поиска ...
[-] Поиск файлов в формате PDF с ограничением до 10
Поиск результатов: 100 ...
Всего: найдено 106 файлов
Начинаем скачивать 100 из них:
----------------------------------------
[1/10] / webhp? Hl = ru
[2/10] https://www.microsoft.com/buxtoncollection/a/pdf/
ebookman_manual.pdf
[3/10] http://go.microsoft.com/fwlink/p/%3Flinkid%3D528467
[4/10] http://nds1.webapps.microsoft.com/phones/files/guides/
Nokia_302_UG_es.pdf
[5/10] http://nds1.webapps.microsoft.com/phones/files/guides/
Nokia_100_UG_en.pdf
[6/10] http://nds1.webapps.microsoft.com/phones/files/guides/
6310i_usersguide_hu.pdf
[7/10] http://nds1.webapps.microsoft.com/phones/files/guides/
Nokia_6020_UG_es.pdf
[8/10] http://nds1.webapps.microsoft.com/phones/files/guides/
Nokia_100_UG_nl.pdf
[9/10] http://nds1.webapps.microsoft.com/phones/files/guides/
Nokia_1616_1800_UG_fr.pdf
[10/10] http://nds1.webapps.microsoft.com/phones/files/guides/
Nokia_6555_UG_nl.pdf
обработка
```

[+] Список найденных пользователей:

Режим
[+] Список найденного ПО:

Acrobat Distiller 8.1.0 (Windows)
AH Formatter V5.3 R1 (5,3,2011,0425) для Windows
Acrobat Distiller 4.05 для Windows
FrameMaker + SGML 5.5.6p145
Acrobat Distiller 5.0.5 (Windows)
FrameMaker 6.0
[+] Список найденных путей и серверов:

[+] Список найденных писем:

Acrobat Distiller 5.0.5 (Windows)
FrameMaker 6.0
Acrobat Distiller 5.0.5 (Windows)
FrameMaker 6.0

Модули метаданных Recon-NG

Recon-NG (первоначально обсуждаемый в главе 5) - это инструмент ручного обнаружения с встроенные модули, предназначенные для быстрого поиска и извлечения полезных метаданных из файлов и документов.

Метакраулер

Модуль Metacrawler Recon-NG ищет файлы, связанные с данным домен, а затем извлекает из этих файлов метаданные, связанные с контактами. Чтобы использовать Модуль Metacrawler в Recon-NG, введите:

используйте recon / domains-contacts / metacrawler

На рисунке 12.1 показана информация о модуле Metacrawler, которую вы можете увидеть. набрав **показать информацию** .

В модуле Metacrawler также есть опция EXTRACT , которая извлекает метаданные из обнаруженных файлов. Если установлено значение False , модуль будет отображать любая контактная информация, найденная в найденных файлах, и отображение результатов на экране, но не будет извлекать (и сохранять) результаты.

На рисунке 12.2 показан модуль Metacrawler, работающий с Apple.com .

Чтобы извлечь данные в базу данных Recon-NG, установите опцию извлечения в true , набрав следующее:

[recon-ng] [default] [metacrawler]> установить extract true

[recon-ng] [по умолчанию] [metacrawler]> запустить

Теперь при запуске модуля вы увидите другой вывод, который включает некоторые из извлеченных метаданных. На рисунке 12.3 показан образец этого вывода.

```
[recon-ng][default][metacrawler] > show info

      Name: Meta Data Extractor
      Path: modules/recon/domains-contacts/metacrawler.py
    Author: Tim Tomes (@LaNMaSteR53)

Description:
  Searches for files associated with the provided domain(s) and extracts any contact related metadata.

Options:
  Name     Current Value  Required  Description
  -------  -------------  --------  -----------
  EXTRACT  False          yes       extract metadata from discovered files
  SOURCE   default        yes       source of input (see 'show info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

Comments:
  * Currently supports doc, docx, xls, xlsx, ppt, pptx, and pdf file types.

[recon-ng][default][metacrawler] >
```

Рисунок 12.1

```
[recon-ng][default][metacrawler] > set source apple.com
SOURCE => apple.com
[recon-ng][default][metacrawler] > run

---------
APPLE.COM
---------
[*] Searching Google for: site:apple.com filetype:pdf OR filetype:docx OR filetype:xlsx OR filetype:pptx OR filetype:doc OR filetype:xls OR filetype:ppt
[*] http://www.apple.com/certificateauthority/WWDR_CPS/
[*] https://www.apple.com/certificateauthority/Apple_Timestamp_CPS/
[*] https://developer.apple.com/softwarelicensing/files/audio_units_logo_lic.pdf
[*] https://developer.apple.com/softwarelicensing/files/mac_logo_license_agreement.pdf
[*] https://developer.apple.com/softwarelicensing/files/opencl_logo_agreement.pdf
[*] https://manuals.info.apple.com/en_US/8602GeoPortWelcome.PDF
[*] https://www.apple.com/dlf/APPLECOMPUTERINSCTOI.pdf
[*] https://www.apple.com/privacy/parentaldisclosureconsent.pdf
[*] https://developer.apple.com/softwarelicensing/agreements/pdf/bonjour4wincore.pdf
[*] https://developer.apple.com/softwarelicensing/agreements/pdf/imovie_logo_agreement.pdf
[*] http://images.apple.com/jp/server/pdfs/NetBoot_TB_050516.pdf
[*] http://images.apple.com/support/products/pdf/applecare_techsuppt_t_and_c_11182003.pdf
[*] http://images.apple.com/jp/server/pdfs/WebHost_TB.pdf
[*] http://images.apple.com/jp/server/pdfs/MailSvcs_TB.pdf
[*] http://images.apple.com/jp/server/pdfs/MacOSXSvr_TO_J_060901.pdf
[*] http://images.apple.com/jp/server/pdfs/Print_Services_TB_v10.4.pdf
[*] http://images.apple.com/support/security/guides/docs/Panther_Security_Config.pdf
[*] http://images.apple.com/support/security/guides/docs/Panther_Server_Security_Config.pdf
[*] https://www.apple.com/accessibility/pdf/imovie_v10_mac_VPAT.pdf
[*] https://itunesconnect.apple.com/docs/iTunesConnect_PublisherUserGuide.pdf
[*] https://www.apple.com/accessibility/pdf/Thunderbolt_Display_VPAT.pdf
[*] https://www.apple.com/itunesnews/docs/FAQ_Music_Signup.pdf
[*] https://beta.apple.com/agreements/AppleBetaPrgrmAgmt_20170605.pdf
[*] https://developer.apple.com/bonjour/printing-specification/
[*] https://www.apple.com/environment/pdf/Apple_Facilities_Report_2008.pdf
[*] https://itunesconnect.apple.com/docs/iTunesConnect_DeveloperGuide_JP.pdf
[*] http://images.apple.com/jp/server/pdfs/Open_Directory_TB_v10.4.pdf
[*] http://salesresources.apple.com/pdf/Ciscocustomerprofile.pdf
```

Рисунок 12.2

После запуска модуля извлеченные данные будут размещены в контактах.
стол. Следующая команда покажет извлеченные данные:

показать контакты

Если Recon-NG отображает сообщение «данные не возвращены», это означает, что
модулю не удалось собрать какие-либо контактные метаданные из файлов. Для юридических
по причинам, мы не можем отображать очищенные адреса электронной почты других людей и отображать-
Скриншот с кучей черных ящиков через него не кажется полезным.
Итак, идем дальше.

Модуль "Интересные_файлы"

«Интересные_файлы» - один из встроенных модулей обнаружения Recon-NG. Как
следует из названия, модуль используется для «поиска интересных файлов в предсказуемой
локации. "

```
[*] https://www.apple.com/environment/pdf/Apple_Facilities_Report_2009.pdf
[*] Title: untitled
[*] Creationdate: D:20090918122416-07'00'
[*] Producer: Acrobat Distiller 7.0 for Macintosh
[*] Moddate: D:20090918122416-07'00'
[*] https://www.apple.com/legal/docs/US_PSPA.pdf
[*] Producer: IndirectObject(72, 0)
[*] Creator: IndirectObject(75, 0)
[*] Author: IndirectObject(73, 0)
[*] Title: IndirectObject(71, 0)
[*] Aapl:Keywords: IndirectObject(78, 0)
[*] Moddate: IndirectObject(76, 0)
[*] Keywords: IndirectObject(77, 0)
[*] Creationdate: IndirectObject(76, 0)
[*] Subject: IndirectObject(74, 0)
[*] https://www.apple.com/accessibility/pdf/iPod_nano_7th_gen_VPAT.pdf
[*] Producer: IndirectObject(48, 0)
[*] Creator: IndirectObject(51, 0)
[*] Author: IndirectObject(49, 0)
[*] Title: IndirectObject(47, 0)
[*] Aapl:Keywords: IndirectObject(54, 0)
[*] Moddate: IndirectObject(52, 0)
[*] Keywords: IndirectObject(53, 0)
[*] Creationdate: IndirectObject(52, 0)
[*] Subject: IndirectObject(50, 0)
[*] https://www.apple.com/environment/pdf/Apple_FY2016_Assurance_Statement.pdf
[*] Producer: Microsoft® Word 2010
[*] Author: BV User
[*] Creator: Microsoft® Word 2010
[*] Moddate: D:20170410080929-07'00'
[*] Title: ASR-TT-06
[*] Creationdate: D:20170410080929-07'00'
[*] Subject: Assurance of Sustainability Reports - Template Assurance Statement (Medium)
[*] https://www.apple.com/newsroom/pdfs/q209data_sum.pdf
[*] Producer: Mac OS X 10.5.6 Quartz PDFContext
[*] Creator: Microsoft Excel
[*] Author: Farnaz Fattahi
[*] Title: 09-04-22 *Data Summary Excel.xls
[*] Aapl:Keywords: [u'']
[*] Moddate: D:20090422163709Z00'00'
[*] Creationdate: D:20090422163709Z00'00'
```

Рисунок 12.3

Если вы не знаете, как найти конкретный модуль в Recon-NG, вы можете выполнить поиск для него, набрав **поиск,** а затем имя модуля. Следующая команда будет искать интересный модуль _ files :

искать интересные_файлы

Чтобы загрузить модуль, введите " **использовать интересные файлы"** . На рисунке 12.4 показан вывод команды show info при запуске после загрузки интересных_файлов модуль.

Как видно на скриншоте, модулю нужна информация от хостов. table, прежде чем мы сможем его запустить. В нашем примере мы установим источник на Apple.com :

установить источник apple.com

На рис. 12.5 показан результат после запуска модуля на Apple.com .

```
[recon-ng][default] > use interesting_files
[recon-ng][default][interesting_files] > show info

      Name: Interesting File Finder
      Path: modules/discovery/info_disclosure/interesting_files.py
    Author: Tim Tomes (@LaNMaSteR53), thrapt (thrapt@gmail.com), Jay Turla (@shipcod3), and Mark Jeffery

Description:
  Checks hosts for interesting files in predictable locations.

Options:
  Name      Current Value  Required  Description
  --------  -------------  --------  -----------
  DOWNLOAD  True           yes       download discovered files
  PORT      80             yes       request port
  PROTOCOL  http           yes       request protocol
  SOURCE    default        yes       source of input (see 'show info' for details)

Source Options:
  default        SELECT DISTINCT host FROM hosts WHERE host IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

Comments:
  * Files: robots.txt, sitemap.xml, sitemap.xml.gz, crossdomain.xml, phpinfo.php, test.php, elmah.axd,
  server-status, jmx-console/, admin-console/, web-console/
  * Google Dorks:
    - inurl:robots.txt ext:txt
    - inurl:elmah.axd ext:axd intitle:"Error log for"
    - inurl:server-status "Apache Status"
```

Рисунок 12.4

```
[recon-ng][default][interesting_files] > set source apple.com
SOURCE => apple.com
[recon-ng][default][interesting_files] > run
[*] http://apple.com:80/robots.txt => 200. 'robots.txt' found!
[*] http://apple.com:80/sitemap.xml => 200. 'sitemap.xml' found!
[*] http://apple.com:80/sitemap.xml.gz => 404
[*] http://apple.com:80/crossdomain.xml => 404
[*] http://apple.com:80/phpinfo.php => 301
[*] http://apple.com:80/test.php => 404
[*] http://apple.com:80/elmah.axd => 404
[*] http://apple.com:80/server-status => 404
[*] http://apple.com:80/jmx-console/ => 404
[*] http://apple.com:80/admin-console/ => 404
[*] http://apple.com:80/web-console/ => 404
[*] 2 interesting files found.
[*] ...downloaded to '/root/.recon-ng/workspaces/default/'
```

Рисунок 12.5.

В этом домене было обнаружено два интересных файла. В роботах.
txt особенно интересен, потому что это файл, который сообщает поисковым системам
какие папки индексировать, а какие игнорировать.
Другими словами, если на веб-сайте есть папки, которые люди (или поисковые системы) должны
не смотреть, эти папки будут отмечены в этом файле. Открытие
папки, которые не следует индексировать, обычно является хорошим признаком того, что вы находитесь в
верный путь к открытию чего-то интересного; эти папки почти всегда
стоит изучить.

Модули геолокации канцелярских кнопок

Модули Pushpin в Recon-NG ищут файлы с геотегами или
в которых сохранены метаданные геолокации. Название происходит от
кнопки, прикрепленные к картам с указанием местоположения. В этом случае эти
модули предназначены именно для этого - определять точное местоположение из
какие файлы были размещены.
Благодаря уровню безопасности, предусмотренному в большинстве социальных сетей и онлайн-сайтов,
наткнуться на онлайн-изображение или файл со встроенными данными о местоположении сродни
выигрыш в лотерею - это *крайне* редко и, вероятно, произойдет только при
правильные обстоятельства. Тем не менее, существует множество сценариев, когда это может
быть обычной находкой, например, при непосредственном просмотре архива телефона,
так что вы всегда должны пробовать.
Модуль Pushpin ищет мультимедиа на Flickr, Shodan, Twitter и YouTube.
со встроенными данными геолокации. Модуль Pushpin *не* скажет вам, где
был опубликован конкретный материал. Вместо этого вы можете ввести адрес или
конкретные координаты, и модуль вернет все СМИ, опубликованные вокруг
это место.
К сожалению, у каждого из этих сайтов есть собственный модуль, поэтому вам нужно искать
их индивидуально.
Чтобы найти расположение модулей канцелярских кнопок, введите следующее:

```
кнопка поиска
[recon-ng] [default]> кнопка поиска
[*] Поиск "канцелярской кнопки" ...
Разведка
-----
Recon / Location-Pushpins / Flickr
разведка / местоположения-кнопки / shodan
Recon / Location-Pushpins / Twitter
Recon / Location-Pushpins / YouTube
Составление отчетов
---------
отчет / метка
```

Каждый модуль имеет свой набор параметров и описаний, которые вы можете
просмотр, загрузив модуль и используя команду show info . Получим информацию
в модуле Flickr:

```
[recon-ng] [по умолчанию]> используйте flickr
[recon-ng] [по умолчанию] [flickr]> показать информацию
Название: Поиск геолокации Flickr
Путь: modules / recon / locations-pushpins / flickr.py
Автор: Тим Томес (@ LaNMaSteR53)
Ключи: flickr_api
Описание:
Ищет на Flickr медиа в указанной близости от места.
Параметры:
Имя Текущее значение Требуется Описание
------ -------------- -------- -----------
РАДИУС 1
да радиус в километрах
ИСТОЧНИК по умолчанию
да источник ввода (см. «показать информацию» для
Детали)
Параметры источника:
дефолт
ВЫБЕРИТЕ РАЗЛИЧНУЮ широту || ',' || долгота ОТ
местоположения, ГДЕ Широта НЕ НУЛЬ И долгота НЕ НУЛЬ
<string> строка, представляющая один ввод
<путь>
путь к файлу, содержащему список входов
query <sql> запрос к базе данных, возвращающий один столбец входных данных
Комментарии:
* Радиус должен быть больше нуля и меньше 32 километров.
```

На странице информации о модуле мы видим, что нам необходимо согласовать
динаты адреса, а также сам адрес, прежде чем мы сможем использовать модуль.
Для этого в Интернете доступно множество бесплатных инструментов. Один из примеров - https: //
www.mapdevelopers.com/geocode _ tool.php . После посещения сайта введите
ваш желаемый адрес, и он вернет ваши координаты широты и долготы.
В этом примере я использую координаты Сент-Луиса, штат Миссури. MapDeveloper
Сайт .com вернул следующую информацию:

```
Широта 38.6337716
Долгота -90,2416548
```

Теперь, когда у нас есть координаты местоположения, давайте посмотрим, какую информацию мы
можно найти в модуле "Канцелярская кнопка".
Во-первых, нам нужно добавить местоположение в Recon-NG, используя команду добавления местоположений.
команда:

```
[recon-ng] [default] [geocode]> добавить местоположения
широта (ТЕКСТ): 38.6337716
```

долгота (ТЕКСТ): -90.2416548
street_address (ТЕКСТ):

Здесь все может быть по-настоящему весело. Широта и долгота Сент-Луиса
были введены как данные о местоположении - теперь давайте посмотрим, есть ли у кого-нибудь из этой области
твитнул недавно. Выполнение этого поиска включает загрузку канцелярской кнопки Twitter.
модуль, используя следующую команду:

используйте recon / locations-pushpins / twitter

На рисунке 12.6 показан образец результатов, полученных после запуска модуля.
Если подумать, это довольно мощная штука. Я установил данные о местоположении
в случайное место в Сент-Луисе. Но что, если мы ждем предстоящей активности
от конкретной цели, например от компании?
Если цель состоит в том, чтобы провести разведку и сбор разведданных о компании, чтобы
собирать информацию, которая может позволить нам получить доступ или настроить таргетинг на конкретный
сотрудника, хорошее место для начала - социальные сети.
Продолжая наш пример, Anheuser-Busch оказался одним из крупнейших
есть компании в Сент-Луисе. Используя сайт MapDevelopers, быстрый поиск
для Anheuser-Busch Сент-Луис возвращает следующие координаты:
Широта: 38.62727

```
[recon-ng][default] > use recon/locations-pushpins/twitter
[recon-ng][default][twitter] > run

----------------------
38.6337716,-90.2416548
----------------------
[*] Collecting data for an unknown number of tweets...
[*] Latitude: 38.63922358
[*] Longitude: -90.23237935
[*] Media_Url: https://twitter.com/Bethany2185/statuses/1114343913362296833
[*] Message: Friday at the Fox! 🎭💙💙 #waitressmusical @ The Fabulous Fox https://t.co/cBZJySqhWm
[*] Profile_Name: Bethany
[*] Profile_Url: https://twitter.com/Bethany2185
[*] Screen_Name: Bethany2185
[*] Source: Twitter
[*] Thumb_Url: https://pbs.twimg.com/profile_images/1110285476261433344/OhQ3Sw6x_normal.jpg
[*] Time: 2019-04-06 01:47:47
[*] ---------------------------------------------------
[*] Latitude: 38.63848437
[*] Longitude: -90.25084633
[*] Media_Url: https://twitter.com/Al_BJacobs/statuses/1114331713537110017
[*] Message: #repost Let's be legendary #shoutout queens especially the ones in the Lou.. _daniella_monae_ @Cedes_Babiie
This ha… https://t.co/WRLNhWYX0e
[*] Profile_Name: Albizness
[*] Profile_Url: https://twitter.com/Al_BJacobs
[*] Screen_Name: Al_BJacobs
[*] Source: Twitter
[*] Thumb_Url: https://pbs.twimg.com/profile_images/868497146823278593/IhlHd_aD_normal.jpg
[*] Time: 2019-04-06 00:59:18
[*] ---------------------------------------------------
[*] Latitude: 38.63848437
[*] Longitude: -90.25084633
[*] Media_Url: https://twitter.com/Al_BJacobs/statuses/1114330959007047680
[*] Message: POETRY FIX? NEXT SATURDAY #VERBZZZ #VERBZZZAFYERWORK #DJ #DJLIFE #DJLIFESTYLE #OPENMICSTL #OPENMIC SHOUTOUT…
 https://t.co/qEwqdnmrPl
[*] Profile_Name: Albizness
[*] Profile_Url: https://twitter.com/Al_BJacobs
[*] Screen_Name: Al_BJacobs
[*] Source: Twitter
[*] Thumb_Url: https://pbs.twimg.com/profile_images/868497146823278593/IhlHd_aD_normal.jpg
[*] Time: 2019-04-06 00:56:18
[*] ---------------------------------------------------
```

Рисунок 12.6.

Долгота: –90,19789
На рис. 12.7 показаны некоторые из 1200+ твитов, обнаруженных после ввода этих координаты в Recon-NG и повторный запуск модуля Twitter Pushpin.

Intrigue.io

Если вас интересует комплексное сканирование / обнаружение / метаданные OSINT инструмент извлечения, Intrigue.io может быть тем, что вы ищете. Ранее обсуждалось в главе 5 Intrigue.io - это гигантский универсальный инструмент, который пытается полностью автоматизировать процесс обнаружения OSINT. Обнаружение метаданных Intrigue.io и процесс экстракции ничем не отличается.
Чтобы обнаружить и извлечь метаданные из нашей цели, нашим первым шагом будет быть использовать модуль URI Spider. В меню нажмите кнопку Пуск, затем измените параметр задачи на URI Spider.

```
[*] --------------------------------------------------
[*] Latitude: 38.6272
[*] Longitude: -90.1978
[*] Media_Url: https://twitter.com/steph_m29/statuses/1110918911040671747
[*] Message: From tiny baby to big boy pup in only 4 weeks! 🖤 @ St. Louis https://t.co/NYnSAjHUnE
[*] Profile_Name: Stephanie Paine
[*] Profile_Url: https://twitter.com/steph_m29
[*] Screen_Name: steph_m29
[*] Source: Twitter
[*] Thumb_Url: https://pbs.twimg.com/profile_images/929907365784276992/OtrfdwX5_normal.jpg
[*] Time: 2019-03-27 14:58:02
[*] --------------------------------------------------
[*] Latitude: 38.6270025
[*] Longitude: -90.1994042
[*] Media_Url: https://twitter.com/tmj_stl_sales/statuses/1110916021886443520
[*] Message: Can you recommend anyone for this job? Account Manager - https://t.co/38sgrPxArX #StLouis, MO #Sales
[*] Profile_Name: TMJ-STL Sales Jobs
[*] Profile_Url: https://twitter.com/tmj_stl_sales
[*] Screen_Name: tmj_stl_sales
[*] Source: Twitter
[*] Thumb_Url: https://pbs.twimg.com/profile_images/669727751260106752/pIKyQnKI_normal.jpg
[*] Time: 2019-03-27 14:46:34
[*] --------------------------------------------------
[*] Latitude: 38.6270025
[*] Longitude: -90.1994042
[*] Media_Url: https://twitter.com/EnvisionJobs/statuses/1110915434688049152
[*] Message: Can you recommend anyone for this job in St. Louis, MO? https://t.co/XP0kCEFyAe #Engineer #TechLife
[*] Profile_Name: Envision, LLC
[*] Profile_Url: https://twitter.com/EnvisionJobs
[*] Screen_Name: EnvisionJobs
[*] Source: Twitter
[*] Thumb_Url: https://pbs.twimg.com/profile_images/1254848820/EnvisionBuilding_normal.jpg
[*] Time: 2019-03-27 14:44:14
[*] --------------------------------------------------
[*] Latitude: 38.62866202
[*] Longitude: -90.20208457
[*] Media_Url: https://twitter.com/TinaSTL/statuses/1110905208371060736
[*] Message: #Word @ Downtown St. Louis https://t.co/so6JqLmNog
[*] Profile_Name: TinaSTL
[*] Profile_Url: https://twitter.com/TinaSTL
[*] Screen_Name: TinaSTL
[*] Source: Twitter
[*] Thumb_Url: https://pbs.twimg.com/profile_images/989578318067494912/hEB7Q2ZF_normal.jpg
[*] Time: 2019-03-27 14:03:35
[*] --------------------------------------------------
[*] 1428 tweets processed.

-------
SUMMARY
-------
[*] 1280 total (1280 new) pushpins found.
```

Рисунок 12.7

На новом экране задач установите URI Spider с начальным целевым хостом, установленным на наш цель. В параметры включены глубина паука (по умолчанию 10) и предел на максимальное количество страниц в паук. Конфигурация по умолчанию также будет извлекать типы записей DNS, номера телефонов и адреса электронной почты в содержание страницы. Если вы хотите извлечь метаданные, важно установить параметр extract-uris имеет значение true. На рисунке 12.8 показан экран URI Spider с эти параметры устанавливаются таким образом.

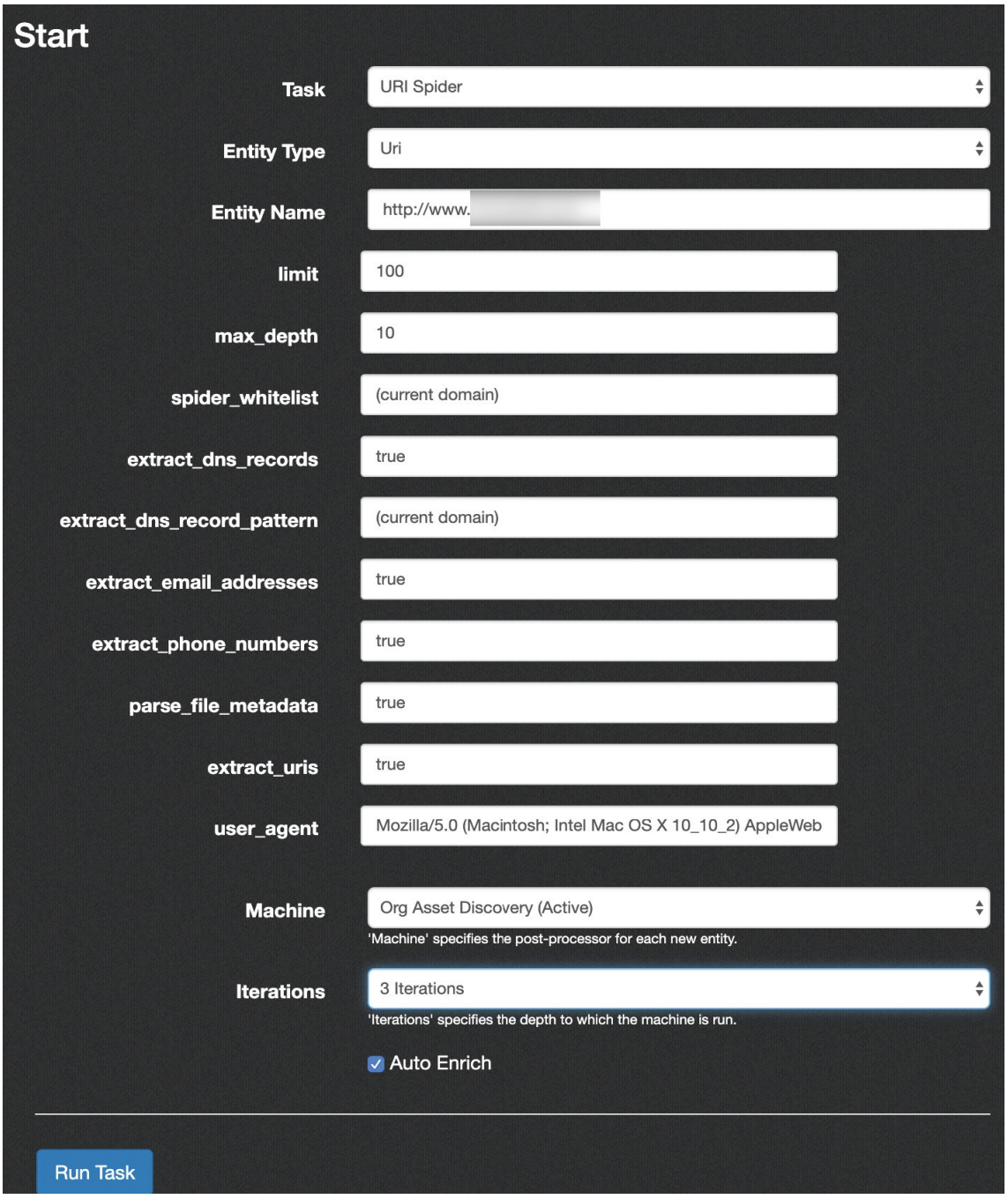


Рисунок 12.8

Паук определит сотни типов файлов, проанализирует их содержимое и
метаданные. Intrigue.io поддерживает более 300 форматов файлов, включая распространенные.
такие как DOC, DOCX и PDF, а также более экзотические типы, такие как application / ogg
и множество видеоформатов.

Когда задача будет выполнена, экран изменится на страницу результатов задачи.
(Рисунок 12.9). Эта страница покажет вам текущий список обнаруженных объектов.
В окне терминала слева также будет отображаться ход сканирования.
и процесс экстракции.

По завершении в окне терминала появится сообщение «задача завершена». Для просмотра
результаты нашего сканирования, нажмите кнопку Entities на главной панели навигации. На
На странице сущностей в области статистики (рис. 12.10) будут представлены все
сущности, которые были обнаружены и извлечены из метаданных документов.

Глядя на сводку результатов, можно сказать, что это действительно очень впечатляющая находка. В
результаты включают 31 домен, 1 номер телефона, 5 имен и 2 сегмента AWS S3!
Intrigue.io также автоматически попытается получить доступ к обнаруженным корзинам.

Чтобы просмотреть информацию о мероприятии, щелкните ссылку AWS Bucket в статистике.
площадь. На рисунке 12.11 показан экран со списком объектов.

Отсюда нажмите на сегмент, который хотите изучить. На рисунке 12.12 показан
страница индивидуального объекта со списком обнаруженных (и загруженных) элементов
из ведра AWS.

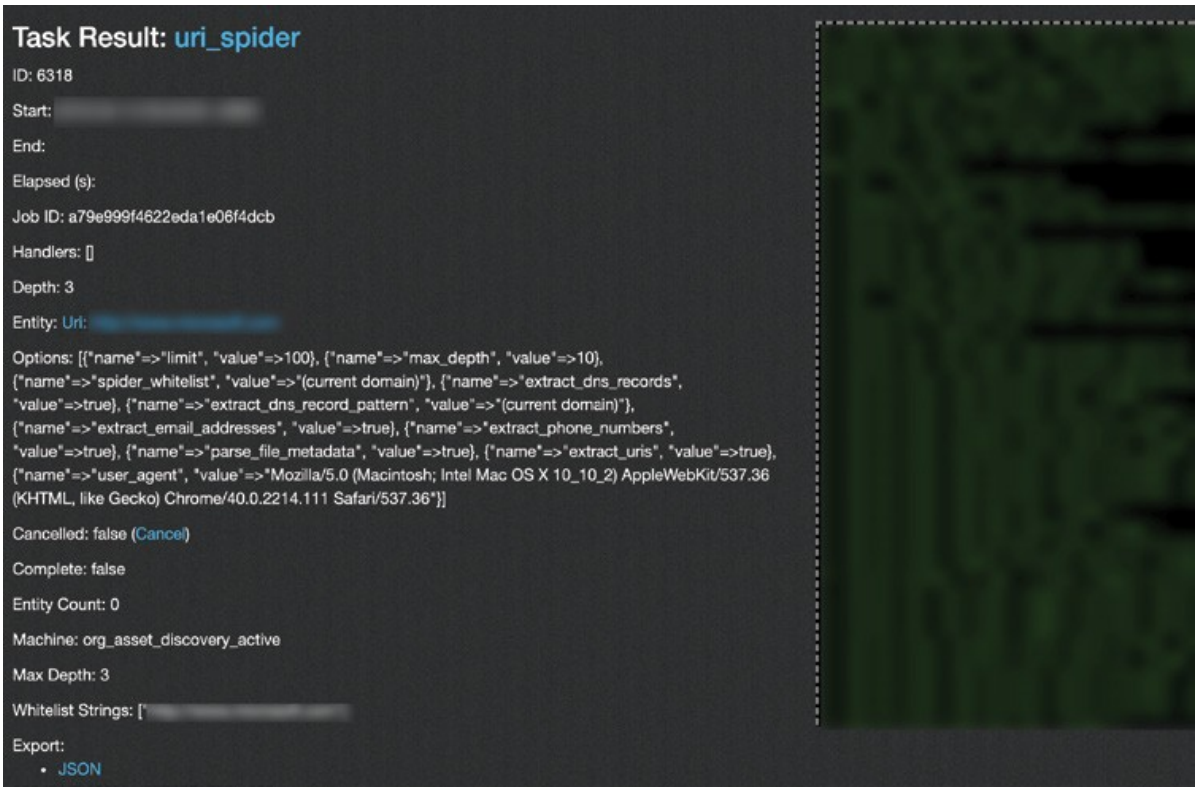


Рисунок 12.9

Обнаруженная информация о корзине может быть важной находкой. Открытая корзина AWS для вашей цели может быть отличным местом для поиска утечки данных.

Сегменты AWS нелегко защитить должным образом, поэтому многие организации люди случайно оставили свои ведра незакрепленными или в них были установлены ненадлежащие разрешения. Они всегда отличное место для поиска.



Рисунок 12.10

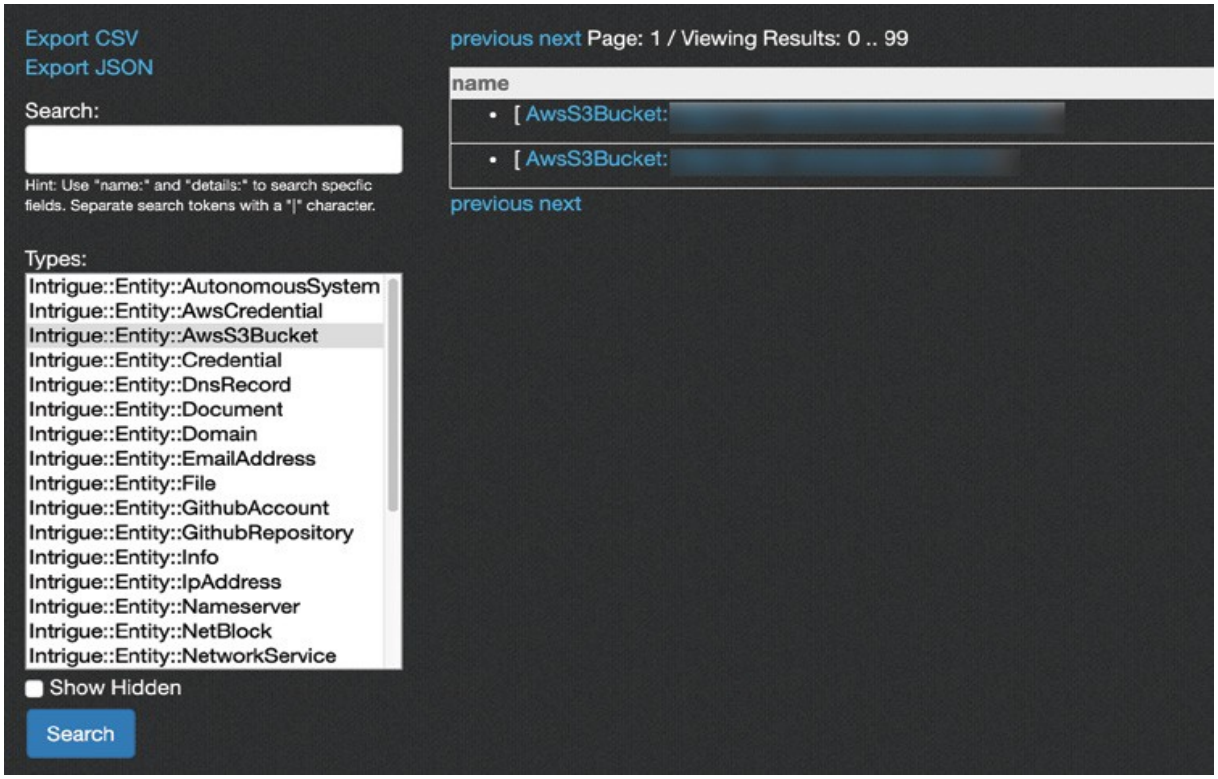


Рисунок 12.11

FOCA

Организации по снятию отпечатков пальцев с собранными архивами или FOCA - это открытая
исходный разведывательно-собирательский инструмент для Windows. FOCA - это инструмент с графическим интерфейсом, который
загружает общедоступные документы с веб-серверов и сканирует их
для метаданных и другой скрытой информации. FOCA использует Google, Bing и
DuckDuck Перейти к поиску документов.
FOCA может анализировать различные форматы документов, включая (но не ограничиваясь)
PDF, DOC, XLS, PPT, JPG, PNG, SVG и другие. Его также можно использовать для извлечения
Информация EXIF из графических файлов. Полезная особенность FOCA заключается в том, что он анализирует
метаданные документа перед загрузкой файла и ограничивают загрузку
только файлы, содержащие полезную информацию о метаданных.
Кроме того, в FOCA есть модуль обнаружения серверов, который позволяет искать
на наличие уязвимостей в документах и хостах. Приложение также может автоматически
поиск других хостов и доменных имен, связанных с основным целевым доменом, по
применение собственных методов разведки на основе DNS, таких как обратный DNS

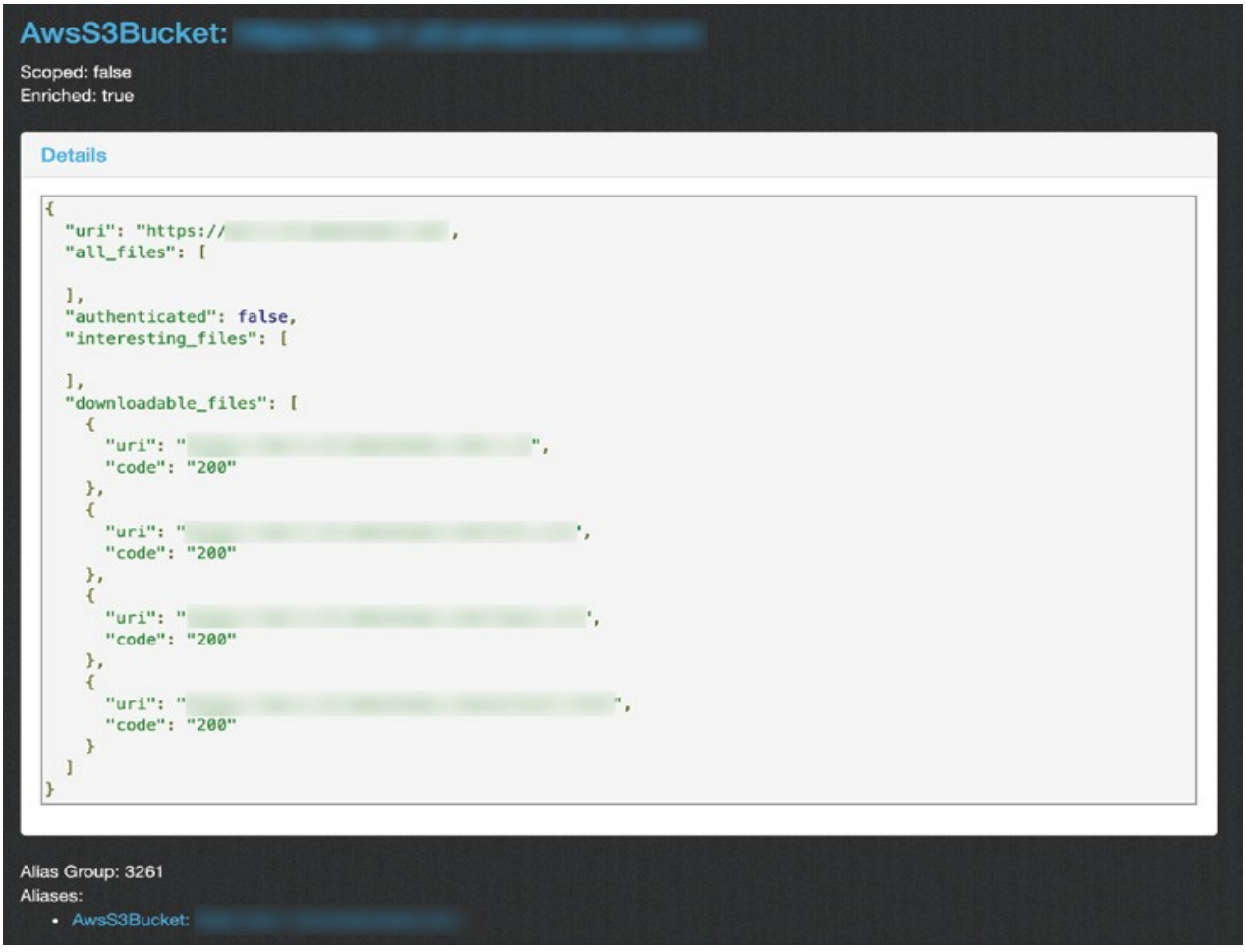


Рисунок 12.12

поиск и сканирование журналов PTR для поиска других связанных серверов по тому же адресу
сегмент. Кроме того, FOCA может выполнять перебор DNS по словарю для
найти скрытые поддомены.

У FOCA также есть собственный рынок, где пользователи могут расширять функциональность приложения.
с использованием сторонних плагинов. Вы можете скачать FOCA с https://github.com/
ElevenPaths / FOCA .

Запуск проекта

Когда открывается FOCA, первым делом требуется настройка проекта. Рисунок 12.13
показывает начальный экран FOCA с Microsoft, указанным в качестве имени нашего проекта и
Microsoft.com указан в качестве нашего целевого домена.

Одной из действительно хороших особенностей FOCA является то, что он автоматически организует
распределите свои проекты по доменам (их можно найти в разделе доменов).
Это особенно важно для исследователей, которые постоянно анализируют метаданные.
полезно из-за того, насколько организован процесс сбора документов.

После того, как FOCA создаст проект, нашим следующим шагом в обнаружении метаданных будет щелчок
элемент дерева метаданных. На рисунке 12.14 показана пустая область метаданных после щелчка мышью.
в дереве. FOCA автоматически выбирает все расширения файлов для наших метаданных
поиск. На этом же экране вы также можете расширить область поиска за пределы
Google, выбрав Bing и DuckDuckGo в качестве дополнительных поисковых систем в
раздел «Поисковые системы» в правом верхнем углу, рядом с разделом «Расширения».

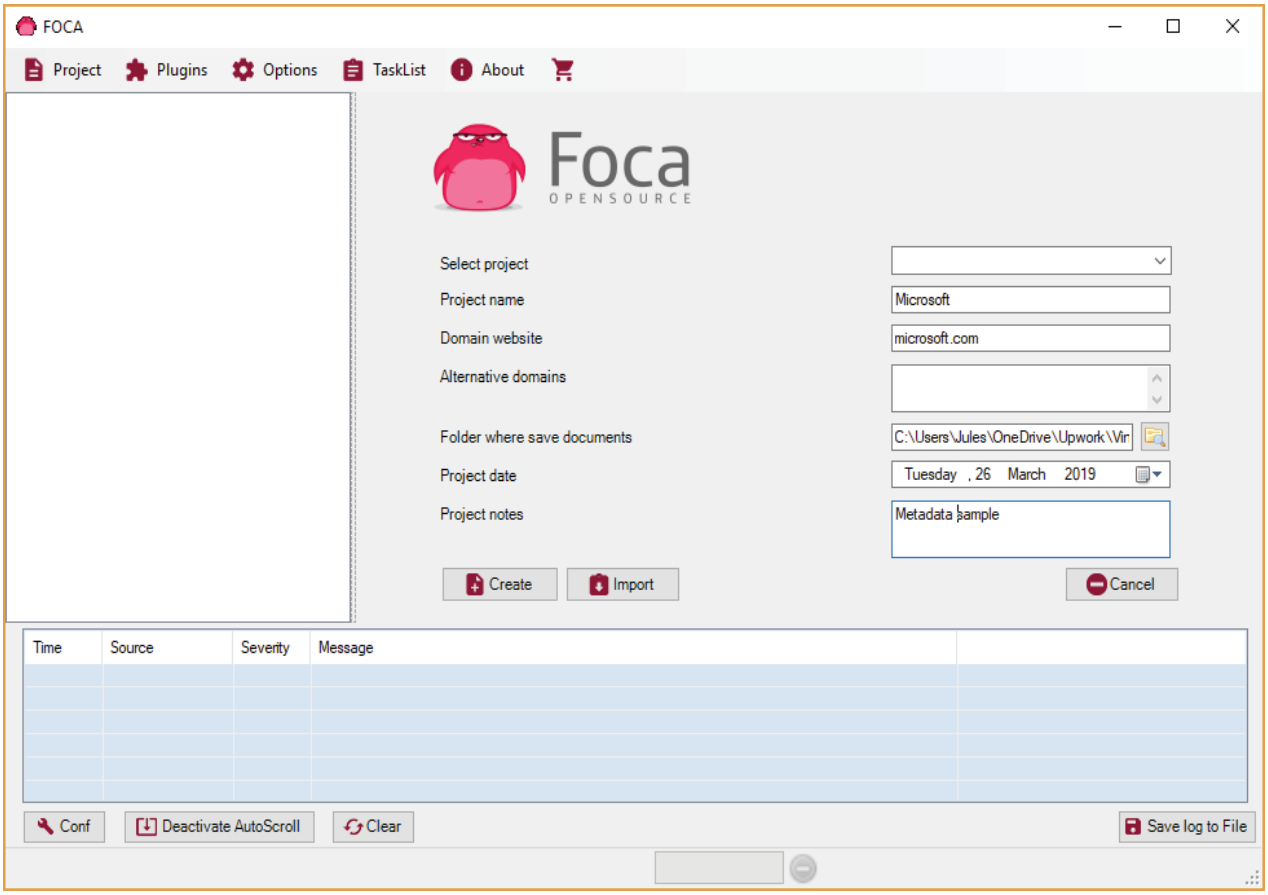


Рисунок 12.13

Не забудьте указать свои ключи API в настройках. Этот тип поиска потребует много обращений к Google и другим поисковым системам, что почти наверняка могут быть помечены или в конечном итоге заблокированы с помощью Captcha. Выполнение поиска в Google или Bing использование ключа API облегчит некоторые из этих ограничений.

Когда вы будете готовы начать сканирование, нажмите кнопку «Искать во всем». Любой обнаруженные документы будут отображаться в области сетки.

Все обнаруженные документы изначально отмечены значком x при загрузке столбец. Это означает, что файл еще не загружен. Верно- щелчок по любому из документов отобразит меню действий, которые можно выполнить. формируется из документов (изображенных на рис. 12.15).

FOCA требует, чтобы вы сначала загрузили документ, прежде чем сможете анализировать или извлеките любые метаданные. Если документ не был загружен, он будет отображаться x в столбце загрузки. После загрузки документа x становится а ●, означающий, что файл был успешно загружен (показано на Рисунке 12.16).

Извлечение метаданных

После загрузки документов у вас есть возможность извлечь любые метаданные, хранящиеся в них. Чтобы проанализировать метаданные, хранящиеся в файлах, сначала нажмите «Извлечь метаданные», а затем «Анализ метаданных» (см. рис. 12.15).

Если метаданные находятся в файле или файлах, папка метаданных обновляется соответствующим образом.

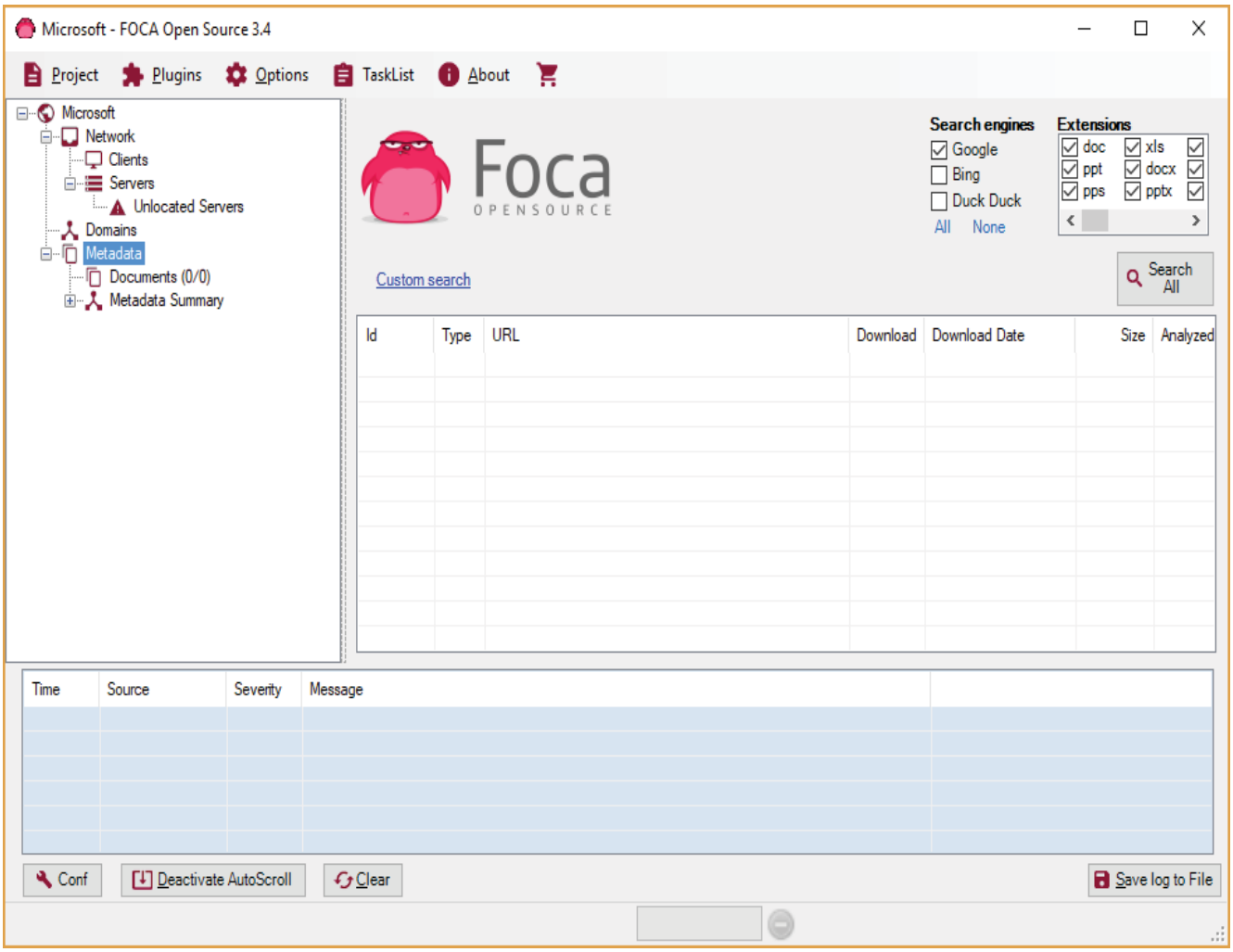


Рисунок 12.14

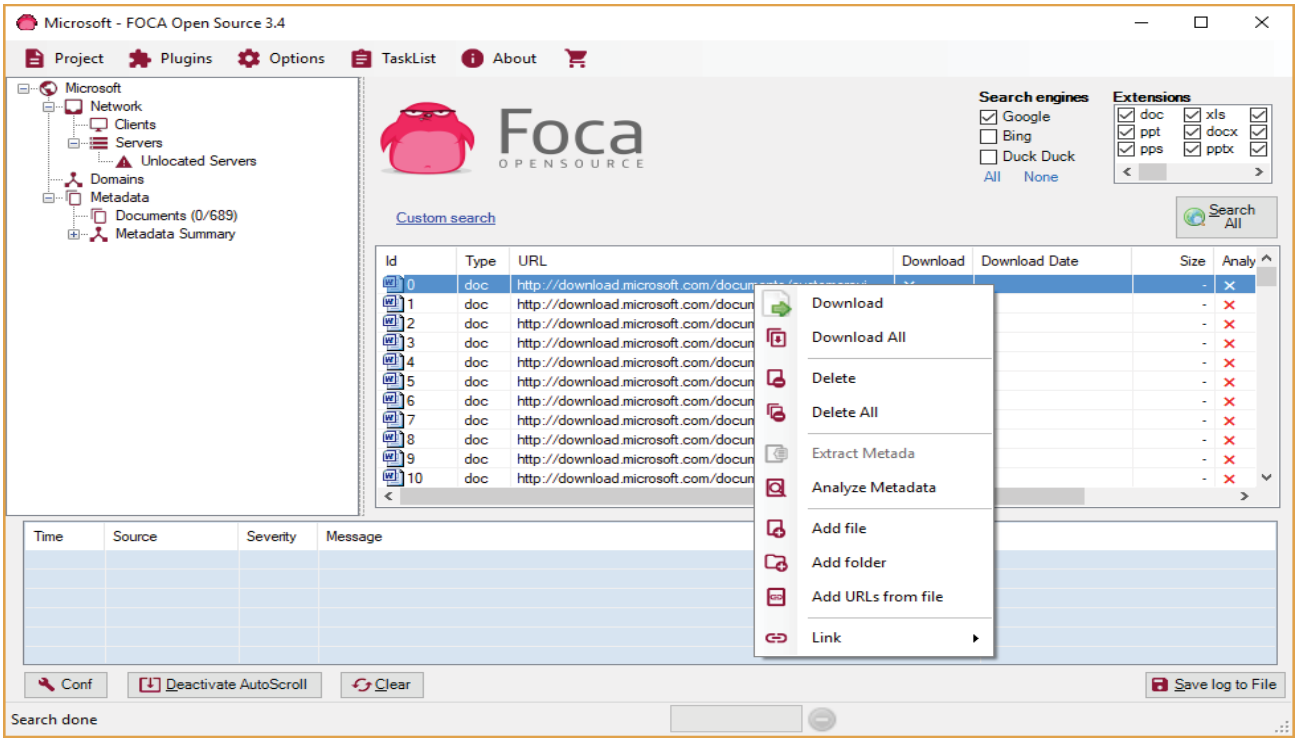


Рисунок 12.15

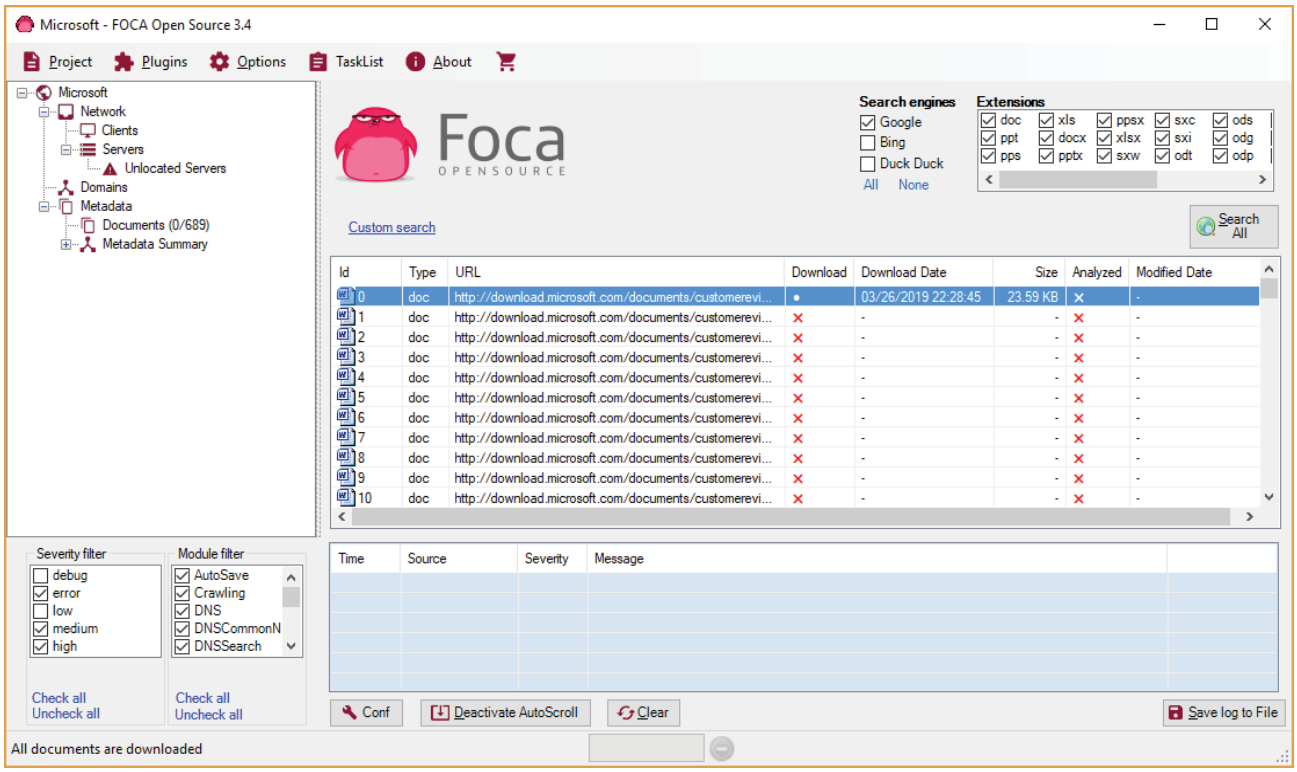


Рисунок 12.16

Извлеченные метаданные будут храниться в хорошо организованных списках поддеревьев. Для
Например, на рис. 12.17 показано дерево документов с поддеревом DOC. Дополнительный
поддеревья будут появляться при обнаружении новых типов документов (например, PDF, XLS,
так далее.). Возможные извлеченные метаданные включают имена пользователей, расположение папок и сервер
имена, информация о принтере, названия программного обеспечения, адреса электронной почты и пароли.
FOCA позволяет пользователям вручную добавлять файл (или папку, содержащую несколько файлов)
в список в сетке, чтобы автоматически извлекать их метаданные. Вы также можете добавить список
URL-адреса из файла, чтобы указать FOCA собрать информацию об этих URL-адресах.
После завершения процесса извлечения метаданных каждый файл будет иметь номера
отображается рядом с ними. Эти числа показывают, сколько частей метаданных
были обнаружены в каждом документе.
Любую из этих сведений можно легко использовать для проведения целевых атак на
организация. Например, любые обнаруженные имена могут быть использованы для вывода пользователя
логин. Оттуда сайт поиска учетных данных (подробнее обсуждается в главе 18)
может использоваться с комбинированными результатами для проведения атаки с использованием паролей.
против веб-панелей входа в организацию (например, Office 365).
После быстрого поиска первых 100 файлов на Microsoft.com , рисунок 12.18
показывает различные фрагменты извлекаемых метаданных.

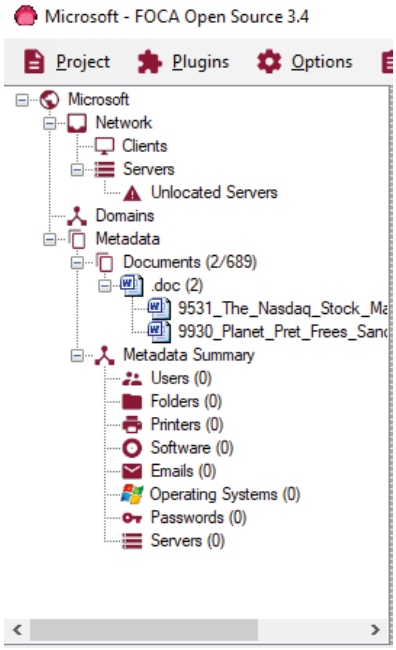


Рисунок 12.17

Резюме

В этой главе были рассмотрены метаданные документа, то есть информация, расположенная в
файл, который используется для описания содержимого этого файла. В этой главе также обсуждались
различные типы файлов, тип конфиденциальной информации, которую потенциально можно оставить
в документе, а также инструменты, которые можно использовать для автоматического обнаружения
и извлекать потенциально конфиденциальную информацию о метаданных из общедоступных
документы.

Инструменты в этой главе различаются по сложности и базовым наборам функций.
и поэтому имеют свои плюсы и минусы. Например, я бы сказал
Дополнительные инструменты, такие как Exiftool и Metagoofil, станут вашим «быстрым и грязным» решением, если
вам нужно сделать что-то быстро.

С другой стороны, FOCA - это инструмент, разработанный исключительно для мета-
анализ данных. Если ваша цель - анализировать только метаданные (или убедиться, что вы
проведение максимально тщательного анализа), этот инструмент можно использовать.

Intrigue.io обеспечивает хорошую середину для возможностей анализа, а также
объединение огромного количества других функций.

В следующей главе мы сосредоточимся на уникальных интересных местах, которые стоит искать.
конфиденциальная (или потрясающая) информация.

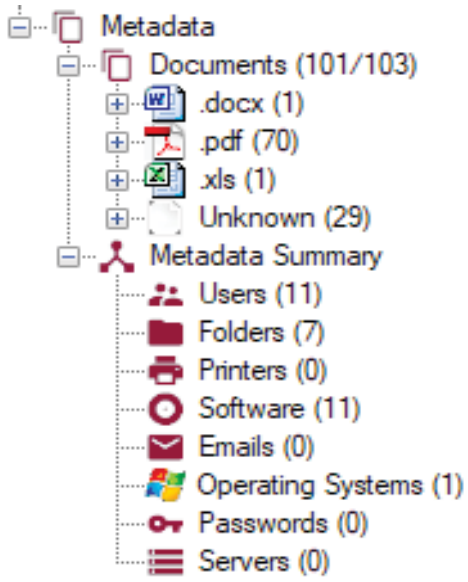


Рисунок 12.18

267

13

Как следует из названия, эта глава посвящена поиску информации в уникальных места. В этой главе также будет завершена история злоумышленника Сайпера и события, приведшие к раскрытию его личности.

Что может быть лучше для начала, чем отрывок из частной беседы XMPP? между мной и Сайпером. В этом разговоре мы с Сайпером обменялись информацией относительно того, как мы смогли обнаружить друг друга, используя неясные подсказки.

VT:
Как вы узнали, что это я?
kickass: лол, вы используете тот же макбук
VT:
учитывая, что я купил этот MacBook 2 дня назад, я не
думаю да
VT:
новый ребенок. i9
kickass: но не имя;)
kickass: все равно отвечу на вопросы
kickass: почему ты думаешь, что я тот парень
VT:
игнорирование того факта, что ваш языковой стиль меняется
где-то ближе к концу ада / прямо перед
BlackBox, когда вы наконец открыли KA, ваш новостной бот
было что-то вроде Cypernews
VT:
Новости CYPERCRIME
VT:
вот что это было

Интересные места для поиска

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

kickass: смеется
kickass: вы на ka, поэтому вы должны знать, что cyper тоже
там - кстати, мы вас забаним?
VT:
я не был на KA в течение долгого времени
kickass: совет, если вы используете jabber, не используйте тот же аватар
для всех учетных записей, а также изменить имя вашего ноутбука
иногда ;)

Сайпер имел в виду поле «имя хоста» в моем клиенте Jabber. я
не понимали этого в то время, но у вас есть возможность настроить это поле,
и если оставить его в покое, Adium для Mac OSX будет использовать имя вашего компьютера. В
в этом случае Сайпер знал, что разговаривает со мной, потому что имя моей ком-
компьютер был достаточно уникальным, чтобы его можно было идентифицировать.
Молодцы, и это именно та непонятная информация, которую мы будем
ищем в этой главе.

TheHarvester

TheHarvester - это инструмент OSINT с открытым исходным кодом, который собирает общедоступные
адреса электронной почты, субдомены, IP-адреса и URL-адреса из широкого спектра источников данных,
включая Baidu, Bing, Censys.io, Crt.sh, Dogpile, Google, LinkedIn, NetCraft,
PGP, ThreatCrowd, Twitter и VirusTotal.
Вероятно, это один из лучших доступных инструментов разведки из командной строки.
потому что он охватывает такую широкую область поиска. Я бы сказал, что если это
не дает никаких результатов, значит, вы не используете его правильно.
TheHarvester использует ряд методов, чтобы найти информацию о своих
цели, в том числе атаки DNS bruteforce с использованием перечисления словаря, DNS
обратный поиск, имена хостов и, конечно же, доркинг поисковой системы.

Я возвращался к тому, в какую главу включить этот инструмент, потому что
это так универсально. Мне показалось, что эта глава лучше всего подходит, потому что The Harvester охватывает много
больше, чем темы, которые мы обсуждали в предыдущих главах, и я не хотел
исключите любые особенности, которые не входили в рамки этих глав.

Я лично использую theHarvester, когда собираюсь публично очистить
доступная информация о названиях компаний и адресах электронной почты, которые сохранились
в поисковых системах.
Вы можете скачать theHarvester со страницы https://github.com/laramies/
Харвестер .
Ниже приводится список аргументов, доступных в theHarvester:

-h, --help
показать это справочное сообщение и выйти
-d ДОМЕН, --domain ДОМЕН

название компании или домен для поиска
-l LIMIT, --limit LIMIT
ограничить количество результатов поиска, по умолчанию = 500
-S START, --start START
начать с номера результата X, по умолчанию = 0
-g, --google-dork использовать Google Dorks для поиска Google
-p PORT_SCAN, --port-scan PORT_SCAN
просканируйте обнаруженные хосты и проверьте наличие поглощений
(21,22,80,443,8080) по умолчанию = False, params = True
-s, --shodan
используйте Shodan для запроса обнаруженных хостов
-v VIRTUAL_HOST, --virtual-host VIRTUAL_HOST
проверить имя хоста с помощью разрешения DNS и поиска
для виртуальных хостов params = basic, default = False
-e DNS_СЕРВЕР, --dns-server DNS_SERVER
DNS-сервер для поиска
-t DNS_TLD, --dns-tld DNS_TLD
выполнить обнаружение расширения DNS TLD,
по умолчанию False
-n DNS_LOOKUP, --dns-lookup DNS_LOOKUP
включить поиск DNS-сервера, по умолчанию = False,
params = True
-c, --dns-brute выполнить перебор DNS в домене
-f ИМЯ ФАЙЛА, - имя файла ИМЯ ФАЙЛА
сохранить результаты в файл HTML и / или XML
-b ИСТОЧНИК, --source ИСТОЧНИК
baidu, bing, bingapi, censys, crtsh, cymon,
dnsdumpster, собачья куча, duckduckgo, Google,
google- сертификаты, hunter, intelx, linkedin,
netcraft, securityTrails, угроза толпы, trello,
twitter, vhost, virustotal, yahoo, все
-x ИСКЛЮЧИТЬ, --exclude ИСКЛЮЧИТЬ
исключить параметры при использовании всех источников

Запуск сканирования

Поисковые системы обычно недовольны тем, что люди собирают данные, поэтому TheHarvester будет вставлять временные задержки между запросами, чтобы избежать обнаружения. Вы также можете ограничить количество запросов, ограничив количество возвращаемых результатов. Этот также позволит вам работать с более управляемым списком. При сохранении вашего вывод, theHarvester всегда будет выводить ваши результаты в HTML и XML. форматы.

Выполнение сканирования с помощью Harvester может быть немного необычным.

Если вы не введете необходимые параметры при сканировании, theHarvester запустит сканирование с 0 результатами.

Чтобы theHarvester запустил сканирование, вы *должны* использовать домен (-d), limit (-l) и исходный (-b) параметры. Если вы не включите все три параметра, вы увидите следующие результаты:

```
[root @ osint]> ./theHarvester.py -d apple.com
************************************************** ****************
* _ _
_
*
* | | _ | | __ ___ / \ / \ __ _ _ ____ _____ ___ | | _ ___ _ __ *
* | __ | _ \ / _ \ \ / / _ / / _` | '__ \ \ / / _ \ / __ | __ / _ \ '__ | *
* | | _ | | | | __ / / __ / (_ | | | \ V / __ / \ __ \ || __ / | *
* \ __ | _ | | _ | \ ___ | \ / / _ / \ __, _ | _ | \ _ / \ ___ || ___ / \ __ \ ___ | _ | *
*
*
* theHarvester 3.0.6 v380
*
* Кодирует Кристиан Марторелла.
*
* Исследование Edge-Security
*
* cmartorella@edge-security.com
*
*
*
************************************************** ****************
[*] IP-адресов не найдено.
[*] Электронных писем не найдено.
[*] Хостов не найдено.
```

Если вы получаете сообщение о том, что IP-адреса, электронные письма или хосты не найдены, вы больше всего скорее всего неправильно ввел параметры.

Параметр -d позволяет указать желаемый домен или название компании.

искать. Параметр -l - это ограничение на количество запросов, которые вы хотите выполнить.

работать с каждой поисковой системой. Параметр -b - это то, как вы указываете

исходная поисковая система для вашего поиска. Это могут быть такие сайты, как Censys, crt.sh, Google, Bing или Yahoo, и это лишь некоторые из них. Если вы не хотите ограничивать свой поиск для любой конкретной поисковой системы *необходимо* ввести -b all .

Сохранение высокого лимита поиска приведет к временному запрету

Google или любые другие поисковые системы. Значение поиска по умолчанию - 500, что означает, что theHarvester просматривает первые 500 результатов поиска. Google показывает 10 результатов поиска на странице, что означает, что TheHarvester быстро их просматривает. 50 страниц. Этого, безусловно, достаточно для Google (или любой поисковой системы), чтобы обнаружить вас как скребок и либо бросить уведомление о Captcha, либо просто заблокировать ваши результаты. Избегать для этого я рекомендую использовать прокси-сервис, который будет отправлять каждый запрос через другой Ent IP (например, Storm Proxies)

Теперь, когда мы понимаем важность указания параметра -d вручную ,
Параметры -b и -l , давайте начнем сканирование наших друзей в WhitePacket
Безопасность (www.whitepacket.com):

```
root @ osint> ./theHarvester.py -d whitepacket.com -l 100 -b все
**************************************************** ****************
* _ _
_
*
* | | _ | | __ ___ / \ / \ __ _ _ ____ _____ ___ | | _ ___ _ __ *
* | __ | _ \ / _ \ / / _ / / _` | '__ \ \ / / _ \ / __ | __ / _ \ '__ | *
* | | _ | | | | __ / / __ / (_ | | | \ V / __ / \ __ \ || __ / | *
* \ __ | _ | | _ | \ ___ | \ / / _ / \ __, _ | _ | \ _ / \ ___ || ___ / \ __ \ ___ | _ | *
*
*
* theHarvester 3.0.6 v380
*
* Кодирует Кристиан Марторелла.
*
* Исследование Edge-Security
*
* cmartorella@edge-security.com
*
*
*
**************************************************** ****************
[*] Цель: whitepacket.com
[*] Поиск в Bing.
[*] Searching Censys.
Страница результатов поиска IP 4.
[*] Поиск в Yahoo.
Поиск 100 результатов.
[*] Поиск в Baidu.
Поиск 100 результатов.
[*] Поиск в Google.
Поиск 100 результатов.
[усечено]
Пользователей из Twitter: 3
--------------------
[удаленный]
[*] Найдено IP: 1
--------------------
[удаленный]
[*] Найдено писем: 2
----------------------
[удаленный]
```

```
[*] Найдено хостов: 5
---------------------
www.whitepacket.com:104.24.118.111
[удаленный]
```

Результаты - хорошее начало, особенно для проведения первоначальной разведки на менее известный домен. TheHarvester нашел пять хостов, два электронных письма и три Пользователи Twitter. Неплохо, но теперь давайте попробуем еще один тест на гораздо более крупной цели - Microsoft.com :

```
корень @ osint / opt / theHarvester> ./theHarvester.py -d microsoft.com -l
100
-мяч
**************************************************** ****************
* _ _
_
*
* | | _ | | __ ___ / \ / \ __ _ _ ____ _____ ___ | | _ ___ _ __ *
* | __ | _ \ / _ \ / / _ / / _` | '__ \ \ / / _ \ / __ | __ / _ \ '__ | *
* | | _ | | | | __ / / __ / (_ | | | \ V / __ / \ __ \ || __ / | *
* \ __ | _ | | _ | \ ___ | \ / / _ / \ __, _ | _ | \ _ / \ ___ || ___ / \ __ \ ___ | _ | *
*
*
* theHarvester 3.0.6 v380
*
* Кодирует Кристиан Марторелла.
*
* Исследование Edge-Security
*
* cmartorella@edge-security.com
*
*
*
**************************************************** ****************
[*] Цель: microsoft.com
[*] Найдено пользователей: 34
---------------------
[удаленный]
Пользователей из Twitter: 24
--------------------
[удаленный]
[*] Найдено IP: 11
--------------------
[удаленный]
[*] Найдено писем: 18
----------------------
[удаленный]
[*] Найдено хостов: 2771
----------------------
[удаленный]
```

[*] Найдено URL: 131

---

https://trello.com/ .. [удалено]

Как видите, это гораздо более впечатляющая находка, особенно если учесть
эти результаты были получены с помощью одного инструмента: 2771 хост, 18 электронных писем, 34 пользователя, 24 Twitter.
учетные записи и 131 URL-адрес Trello, связанный с Microsoft.
Отсюда вам решать, каким путем вы пойдете для дальнейшего исследования.
Просто убедитесь, что вы документируете все, что найдете, чтобы вы могли легко
обратитесь к нему позже.
А теперь давайте посмотрим, что еще мы можем поднять в Интернете.

Вставить сайты

Хакеры и другие злоумышленники часто используют один или несколько сайтов вставки для публикации
образец их товаров в Интернете. В зависимости от ваших целей часто бывает значительный
количество информации, которую можно найти на этих сайтах. Вставить сайты часто будут содержать
образцы утечек данных, сообщения от злоумышленников и различные доксы на
частные лица.
Популярные сайты для вставки:

- Pastebin.com
- 0bin.net
- Doxbin.org
- Justpaste.it

Сайты вставки, такие как форумы, широко используются злоумышленниками и часто могут
предоставить основную информацию во время расследования. Проблема с этими
сайтов заключается в том, что определенные пасты часто удаляются, если обнаруживается, что они нарушают
условия обслуживания сайта, содержащие PII (личную информацию)
или другие формы частной информации.
В результате многие организации каждый день очищают эти сайты пасты на предмет новых
содержание. Я тоже так делаю и расскажу, как это можно сделать довольно легко.
далее в этой главе.

Psbdmp.ws

Как я уже упоминал ранее, пасты, которые нарушают условия обслуживания, публикуя PII или
другая скрытая информация быстро удаляется. Очень жаль, если паста
содержали улики или доказательства, необходимые для расследования. Нам повезло,
есть psbdmp.ws.

Долгое время psbdmp был одним из моих секретных оружий, потому что это единственное
сайт, на котором хранится полный исторический архив каждой пасты начиная с 2015 года.
только то, что его API очень удобен и может быть легко запрошен из URL или
внешнее приложение. Прежде чем я создал движок для очистки всех сайтов вставки для моего
Платформа DataViper, API psbdmp был ключевой частью моего набора инструментов для расследования.

Форумы

На мой взгляд, форумы - это ворота на подпольный рынок преступности. Какие
Я имею в виду, что присутствие на многих из этих хакерских форумов похоже на обряд
переход для более продвинутых злоумышленников. В каждом молодом хакере есть смысл
жизнь, когда их неминуемо считали заносом (сценарий-детка). Салазки, как
большинство детей действуют, не задумываясь, и часто оставляют за собой след, который
каким-то образом приводит к их настоящей личности.

Вот почему, по моему скромному мнению, истинное искусство распознавания злоумышленников будет
сводятся к способности исследователя собирать и искать историческую информацию.
Поиск на форумах не должен ограничиваться только хакерами и дарквебом (TOR).
форумы. Даже злоумышленники тусуются на нехакерских форумах, которые могут
любых форм и размеров. Изучение различных форумов часто может дать вам основную информацию.
общие подсказки, такие как привязка псевдонимов к новым адресам электронной почты.
Одним из таких форумов, который помог мне в этом отношении, был BitcoinTalk.
Форум. Я не могу объяснить почему, но я обнаружил, что многие исследователи угроз, которых я исследовал,
в прошлом, кажется, там тусуются. Я хочу сказать, что вы не должны ограничивать
выберите категорию поиска для определенного типа форума или сайта. Всегда расширять
как можно шире ваши поиски.

**Когда я руководил собственными лабораториями, мы строили собственные скребки. Мы бы начали с
набор интересующих URL. Это могло быть что угодно, от вставки сайтов в URL-адреса.
представляет интерес . . . Я имею в виду, что вы знаете, сколько всего на этой стороне.
Это был очень хороший случай сказать: «Хорошо, какие из них на самом деле будут использоваться?
полный? » Это было все: от возврата к ранним материалам до выхода из разлома.
данные. Мы использовали кучу материалов с данными о взломах.
Вы смотрите на это, вы смотрите на способность извлекать данные из темной стороны
Мир. Опять же, это та же концепция. Один URL ведет к 10 или 20 URL.
Вы проводите их быстрый и высокоуровневый анализ и решаете, какие приоритеты вы
собираюсь их очистить, основываясь на поиске слов, тепловых картах и множестве
другие вещи.
Затем оттуда данные извлекаются и индексируются на входе. Вы действительно закончите
создание вашей собственной версии среды очень и очень высокого типа DT-поиска. В этом**

В этом случае мы использовали Elasticsearch, а на другом конце не было архитектуры СУБД, чтобы уверен, что эта чертова штука будет работать должным образом.

А для получения данных чаще всего достаточно просто прочитать то, что другие люди говорят. Скажем так, вы заходите на форум, неважно, что это за форум.

Это. Если речь идет о взломе или взломе или торрентах. . . Вы заходите на эти форумы и он приведет вас к другому URL-адресу или другому веб-сайту, и еще одному и другому.

Итак, мы начнем с форума X, Y, Zed, давайте посмотрим, есть ли у нас кто-нибудь с учетная запись, идентификатор пользователя или что-то еще, что было бы полезно собрать. Вы можете бежать прямо в базу данных. Если ваша база данных настроена, она, вероятно, скажет вам, чья именно учетные записи пользователей, которые вы можете использовать, чтобы разобраться во всем этом, черт возьми!

Изучение истории форума (и TDO)

Если ваше расследование приводит вас на форумы, вы можете искать исторические данные
может стать действительно сложной частью вашего путешествия. Я продемонстрировал несколько
премиум-класса угроз для приложений Intel и не смог найти ничего, что могло бы предложить
уровень исторических данных, необходимых мне для дальнейшего расследования.
Многие компании утверждали, что у них есть данные, но на самом деле никто этого не сделал. Так что я в конечном итоге
пришлось сделать то же, что и Крис Роберт, и построить свой собственный.
Моя платформа называется DataViper, и создание ее оказалось краеугольным камнем.
камень за то, как я смог идентифицировать членов Темного Повелителя (TDO).
Я подробнее расскажу о том, почему и как написано это утверждение, в главах.
17 и 18. А пока вернемся к нашей основной истории и к тому, почему способность
поиск по форумам так важен.
Когда я исследовал TDO, все дороги вели к исходному форуму Hell
как истоки группы. К сожалению, этот форум закрылся в 2016 году, и
найти кого-нибудь с царапинами на форуме оказалось самой утомительной частью
всего расследования.
К счастью, после месяцев и месяцев неустанных поисков я наткнулся на один
человек, у которого были данные. Он попросил остаться безымянным, но если он когда-нибудь прочтет
это, я хочу, чтобы он знал, насколько я благодарен, потому что его данные оказались
полезнее, чем я мог когда-либо надеяться.
В моем случае все члены TDO встретились (и собрались вместе) в аду. После чтения
через их сообщения и сообщения иерархия группы сразу стала
Чисто. Казалось, все они смотрят на кого-то по имени Сайпер (нет H).
К тому времени, когда у меня был доступ к данным ада, я уже понял, что Cyper
другие ручки, так что это было хорошим подтверждением того, что я на правильном пути.
После закрытия Адского форума (который, как мне кажется, он организовал),
Сайпер основал свой собственный форум под названием BlackBox под псевдонимом Ghost. Он также
Одновременно был запущен еще один форум под названием KickAss под псевдонимом NSA.
Позвольте мне объяснить, откуда я это знаю.

После панировочных сухарей

Когда мы хотели взломать компанию в энергетическом секторе, я блуждал вокруг смотреть на своих третьих лиц, их продавцов и их поставщиков. я сижу там на одном из документов, на одном из форумов, и инженер разговаривает о некоторых проблемах, которые у него есть. Он ставит ссылку на документ. я ухожу к чертовому документу, там 350-страничный набор схем для всей подстанции, сетка, архитектура, включая все IP-адреса. . .
Я делал то же самое, когда проводил исследования. Неважно, если он включен, очевидно, что это очень хорошо известные вещи - это самолеты. Я имею в виду, что самолеты были отличный пример, потому что Boeing и Airbus не производят самолеты. Он построен гун-дреды других людей. Это как набор Лего.
Все, что вам нужно сделать, это найти тех правильных людей, которые строят то, что вы заинтересован, начните собирать всю информацию у этих людей, начните втягивать все данные от этих людей, что вроде того, как я это сделал.

Отслеживание злоумышленника ничем не отличается от расследования цели таким же образом. обсуждается Крисом. Что касается расследования TDO, наше путешествие начинается с 0-day (форум хакеров на основе TOR), где пользователи ze0ring и Cyper спорят за внутреннюю кражу данных из Управления кадров и управления (OPM) (рисунок 13.1).

Драма густая. Но в двух словах, ze0ring расстроен тем, что Сайпер и Revolt убежал с данными OPM и вызвал закрытие форума Hell (подробности вы можете прочитать в моем официальном отчете о The Dark Overlord).

Продолжая следить за цепочкой драматических событий, на рис. 13.2 показано сообщение, в котором Пользователь Photon выражает свое недовольство BlackBox и Ghost.

Для тех, кто заинтересован, ссылки на Imgur и mega.nz все еще активны.

BlackBox запускал пользователь по имени Ghost. Среди прочего, Photon's снимки экрана BlackBox помогли подтвердить, что Сайпер и Призрак на самом деле тот же человек.

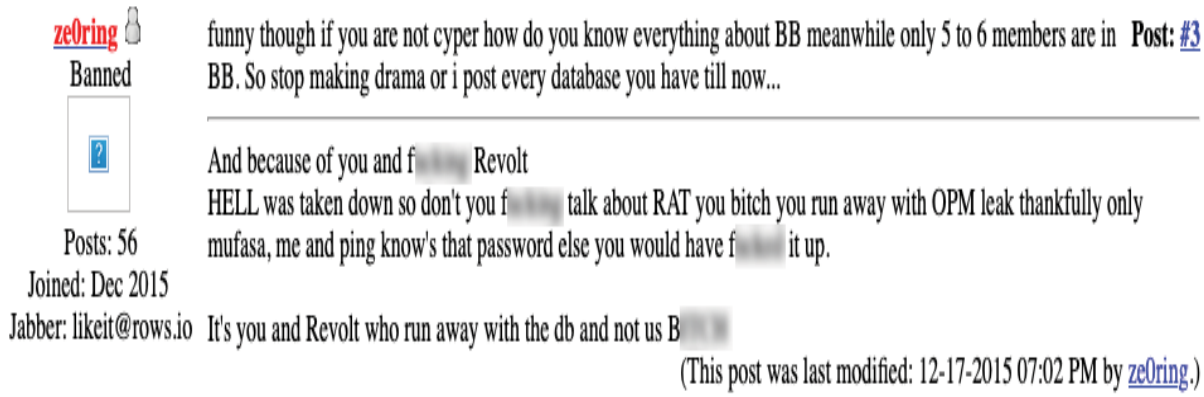


Рисунок 13.1

В следующем посте о BlackBox (рис. 13.3) Сайпер обсуждает веб-оболочку.
который был загружен в JJFox, магазин сигар за пределами Великобритании.
Несколько дней спустя мы видим тот же пост на рис. 13.4, но теперь Cyper's
имя пользователя было изменено на Призрак.
Эти снимки экрана ни в коем случае не единственное свидетельство того, что эти две угрозы
актеры - это одно и то же лицо. Но и они не пострадали.

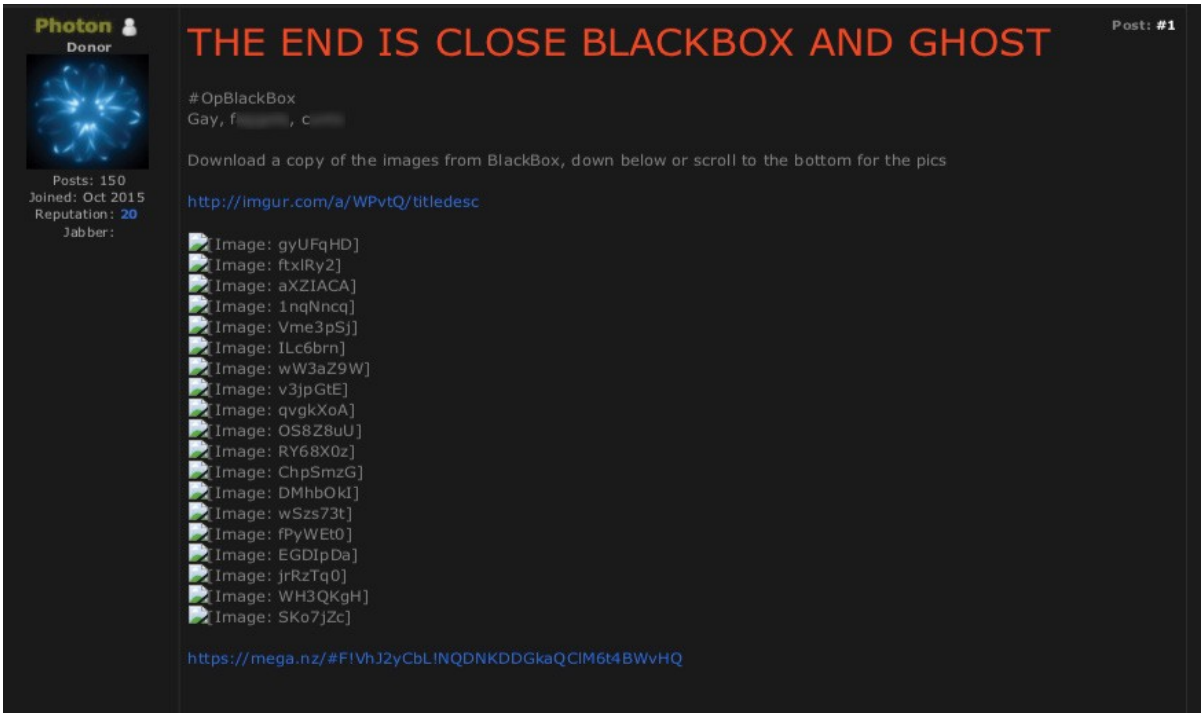


Рисунок 13.2



Рисунок 13.3

Отслеживание личности Сайпера

Я уже знал, что Сайпер был человеком, который организовал падение ада
(обсуждается в главе 2), так что теперь, когда я смог окончательно установить Cyper
Как лидер BlackBox, мой интерес к его личности резко возрос. К несчастью,
BlackBox был настолько эксклюзивным форумом, что обнаружение обрывков его данных доказало, что
быть невозможным.
Однако иногда самородки золота можно найти в самых случайных местах.
В этой книге я упоминал, что создал приложение под названием
DataViper, это моя собственная коллекция учетных данных, взломанных баз данных и
наскребал форумы. В моем стремлении очистить и проиндексировать столько исторических данных, сколько я
смог найти, я наткнулся на сайт социальной сети TOR под названием Galaxy.
Фактически, версия 2 Galaxy оказалась для большинства излюбленным местом встречи в социальных сетях.
участников адского форума, в том числе Сайпера и его банды миньонов.
В следующей войне с жарким пламенем Сайпер (он же CyPeRtRon) защищал
сам против тотального нападения со стороны двух других людей по поводу запуска
его нового форума BlackBox, url: **cyper** 7cybre7u57.onion.

Еще одно указание на то, что Сайпер был администратором BlackBox, который трудно игнорировать - слово Cyper буквально присутствует в URL-адресе.

Автор: Арсинтекс
@ Неизвестно 8698 8698, CyPeR должен знать, он / он - один из заносчиков
из коробки S ***, xex, Blackbox (название темы, очень оригинальное x) и вы

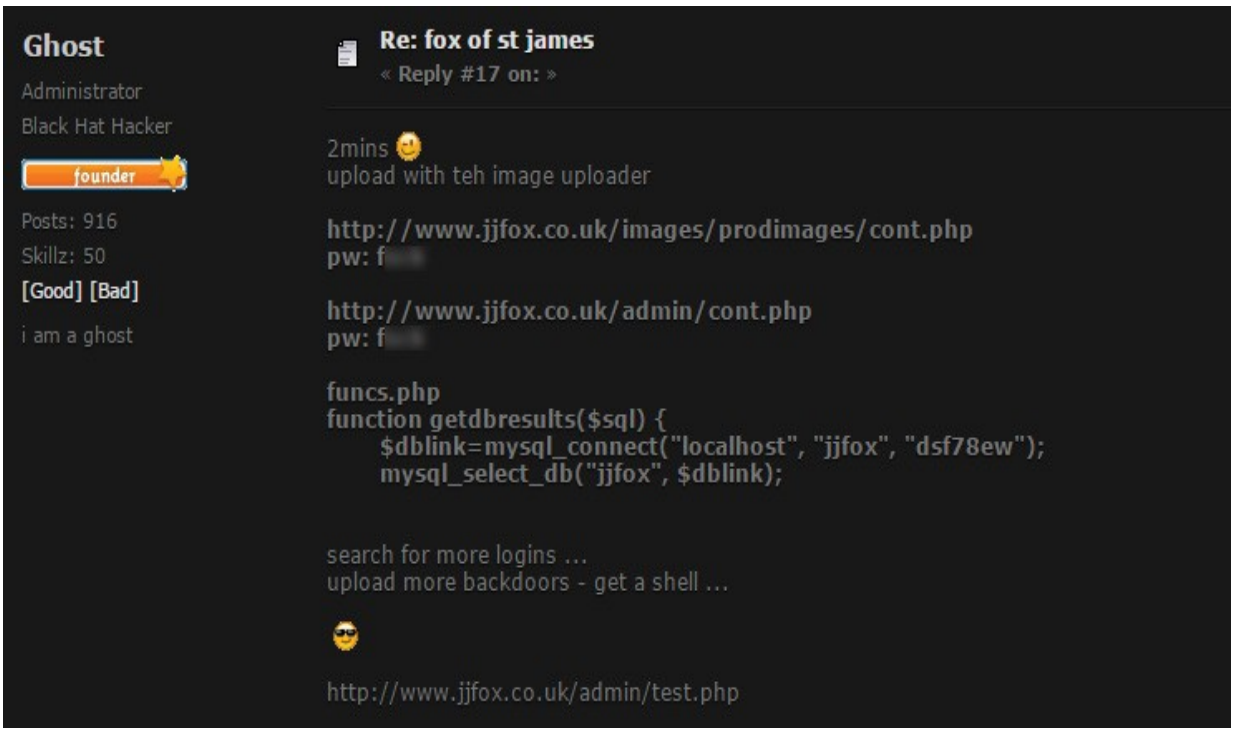


Рисунок 13.4.

с нетерпением ждешь моего профессионального форума? какой форум? это частная сеть &
да, продолжай мечтать, я сказал про, а не за бедных; D
Автор: CyPeRtRoN
LOL узнайте, чем отличается частная сеть от форума lame kid
Ад не было частной сети - только открытый форум ... Автор Arsyntex 9 дней
назад Скоро новый АД, только для ПРО людей, а не для умственно отсталых и невежественных
дети, никакого доксинга или SQLi дерьма.
Автор: CyPeRtRoN
кстати - почему бы и нет - когда имя подходит для имени форума ... но я боюсь тебя
не знаю, что означает название "Blackbox" ...
Автор: CyPeRtRoN
ты бесишься - потому что ты не можешь играть с большими мальчиками и должен играть
с детьми вокруг себя ...
Автор: Арсинтекс
ха-хаа я знаю разницу .. и я написал "Скоро новый АД" нет "Скоро
такое же открытое дерьмо АД "... а я не ребенок и не хромой, в отличие от тебя; D
http://matrixtxri745dfw.onion/neo/uploads/150724/
MATRIXtxri745dfwONION_142610hJl_lol.png LOL
Автор: Арсинтекс
меня бесить? .. ха-хаа .. я "играю" один и мои коллеги умные
ппл .. не идиоты детки .. просто я люблю раздражать и беспокоить
заносит, как ты, я многозадачный xD
Автор: CyPeRtRoN
да, на форуме есть правила - что вы хотите сказать этим снимком? о, простите
- Ты сам этого не знаешь ...
Автор: CyPeRtRoN
кстати - ты такой умный - тогда обязательно говорит, что ты отслеживаешь cookie, что: D
Автор: CyPeRtRoN
Ты думаешь, что прячешься за тор - подумай еще раз, малыш - не навещай не того
серверы ты был на моем сервере ребенок ... ты недостаточно умен ... у меня есть
много выходных узлов ... я надеюсь на вас - вы не использовали ни один из них
сука http://ow.ly/Q34fA
Автор: Арсинтекс
Сначала вы написали "играть" .. Повторяю саркастически .. (отсюда и
цитаты). Я умею «играть» (смеется); работать в одиночку и имея коллег, но
ваши рассуждения настолько скудны, что вы не понимаете, или
коллеги означает, что я не могу работать в одиночку? .. а когда я писал

280 Часть III ■ в поисках золота

Автор: Арсинтекс
и когда я написал "Я многозадачный", я имел в виду, что могу работать, пока
спорите с такими глупыми девчонками, как ты xD .. правила форума такие
смешно .. "тогда обязательно говорит, что вы отслеживаете cookie, что: D" <- WTF, xD
Автор: Арсинтекс
└ o ┘ ! , Теперь мне страшно, я лучше отключаюсь, хахаха
Автор: Sugartime
1. Правило скрытых сервисов: никогда не говорите свой настоящий IP. #telnet
cyper7cyb5re7u57.onion 25 Подключен к cyper7cyb5re7u57.onion. 220
ks355296.kimsufi.com ESMTP Exim 4.84 Пт, 24 июля 2015 г. xx: xx: xx
+0200 #dig **ks355296.kimsufi.com 91.121.120.49**
2. Правило скрытых сервисов: в случае отрицания никогда не произносите идентификационный номер Exim.
ваш реальный IP. ВЕРСИЯ СЛУЖБЫ ГОСУДАРСТВЕННОГО ПОРТА 113 / tcp открыть идентификатор? # **телнет**
91.121.120.49 113 Подключено к 91.121.120.49. 25, 25: ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ:
UNIX: сбой 25,25: ОШИБКА: БЕЗ ПОЛЬЗОВАТЕЛЯ
Автор: Арсинтекс
Ха-ха xD @CyPeRtRoN
http://freedomsct2bsqtn.onion/sannucjvkdoymsycrugq/cXsgtnpE.png
Поговорим о поразительном золоте!
Чтобы добавить еще больше контекста к сообщению Sugartime, URL cyper7 cybre7u57.
onion - это URL-адрес бывшего форума BlackBox. Если это сообщение верное, то
IP-адрес BlackBox был фактически открыт и находился на OVH
сервер (который является родительским хостом для Kimsufi.com) с IP-адресом 91.121.120.49.
Какой *грандиозный* результат !! Никогда не недооценивайте силу хакеров, желающих
сбивают друг друга. Как только они начнут враждовать, skidz часто будут докучать друг другу.
и делают все возможное, чтобы уничтожить друг друга.
Это прекрасный пример. Найти реальный IP-адрес сайта TOR практически невозможно.
sible (если только вы не контролируете узлы выхода), поэтому тот факт, что сервер
был разоблачен, как будто это потрясающе.
Может быть, это настоящий IP-адрес исходного сервера BlackBox?

Репозитории кода

Репозитории кода, такие как GitHub, Bitbucket и GitLab, могут предоставить важные подсказки
найти свой путь в организацию или узнать о цели. Суммируя,
разработчики будут использовать репозитории Git для загрузки кода. Сайты Git позволяют вам смотреть
через исторические коммиты и даже предоставит вам адрес электронной почты
человек, совершающий коммит, если вы знаете, как его запросить.

Если вам интересно, насколько это может быть полезно, позвольте мне на этот раз сказать что я *лично* обнаружил следующие типы информации, хранящиеся в старый Git коммит:

- Личные адреса электронной почты
- Жестко запрограммированные пароли приложений
- Ключи AWS
- PII и другие пользовательские данные
- Пароли учетных записей пользователей
- Полные архивы базы данных

Если вы все еще не уверены, то это настоящий разговор, который у меня был с NSFW, известным злоумышленником, о том, как он взломал крупный веб-сайт найдя ключи AWS на странице компании GitHub:

BTC: я доксировал cto или что-то еще
BTC: все взломано
BTC: dropbox
BTC: и т. Д.
BTC: у всех было 2fa, братан
BTC: но
BTC: ниггер
BTC: самый тупой идиот
BTC: cuz
BTC: github
BTC: не было 2fa
BTC: поставил 2fa на самое бесполезное дерьмо
BTC: но не github
BTC: в любом случае
BTC: ye
BTC: получил кредиты aws с github
BTC: тогда я приват esc'd
BTC: но
BTC: нет данных
BTC: в ведре ничего не было
BTC: только RDS
BTC: так что мне пришлось ждать целую вечность
BTC: пока они не портировались
BTC: в aws

SearchCode.com

SearchCode (www.searchcode.com) - это сайт, который позволяет искать код из проекты по github.com , BitBucket, Google Code, Gitlab, и многие другие сайты. Большинство хакеров написали код, поэтому велика вероятность, что они не только имеют учетные записи на сайтах Git, таких как GitHub и Gitlab, но также имеют зарегистрированный код.

Кроме того, здесь можно применить один неопровержимый факт: *кодеры будут повторно использовать собственный код* . Если у нас есть код, написанный целью, вы можете обратите внимание на оставленные ошибки или интересные комментарии. Атрибуция по ошибке написание и повторно используемый код могут показаться маловероятным, но это более распространено чем вы думаете.

Более того, когда злоумышленники впервые обращаются за доступом к хакерским форумам, они почти всегда включают образец кода в свое приложение. Возможность вернуться и раскрасить Эти примеры кода могут быть чрезвычайно полезны.

Возвращаясь к SearchCode.com , результаты невелики , но я не нашел ни одного конкурирующие сайты, которые лучше. На мой взгляд, основная проблема, с которой я сталкиваюсь, сайт заключается в том, что вы не можете искать полные строки.

Например, поиск «действительно длинная строка» вернет результаты, соответствующие *любое* слово действительно, длинное или строковое, что может привести к большому количеству бесполезные результаты.

При этом это лучше, чем ничего, и если ваши результаты не найдены, приложение дает вам быстрый доступ к прямому поиску вашей строки на основные сайты Git.

Поиск кода

Интерфейс SearchCode.com довольно понятен . Введите свой запрос в поле поиска (рис. 13.5) и нажмите «Поиск».

Для нашего тестового поиска давайте попробуем строку «\ x48 \ x31 \ xc0 \ x5e \ x68», которая будет дают довольно много результатов. Левая часть окна результатов на рисунке 13.6 - это что я считаю наиболее полезным в этом сайте.



Рисунок 13.5.

Наш поиск дал слишком много результатов, чтобы быть полезными, поэтому с помощью панели фильтров
может помочь уточнить наши результаты поиска. Это огромная экономия времени и позволит вам
чтобы быстро изучить код с разных сайтов или языков, просто выбрав
соответствующий фильтр.

Ложноотрицательные

Один важный момент, который следует учитывать при использовании этого сайта, - это количество ложноотрицательных результатов.
вы получите в своих результатах. Я имею в виду, что ваш поиск может часто
вернуть «результаты не найдены» или, что еще хуже, некоторые несвязанные или неверные результаты
по условиям поиска. Например, давайте попробуем найти «c3nt3rx» (это псевдоним
злоумышленника с форума KickAss).
Страница результатов (рис. 13.7) показывает, что совпадений нет.
Как упоминалось ранее, если результаты не найдены, SearchCode.com предоставляет
быстрые ссылки для поиска вашего термина на нескольких разных сайтах, включая GitHub.
Щелкнув ссылку для GitHub, мы попадаем прямо на этот сайт и автоматически
формирует тот же поиск, включая термин в запрос URL.

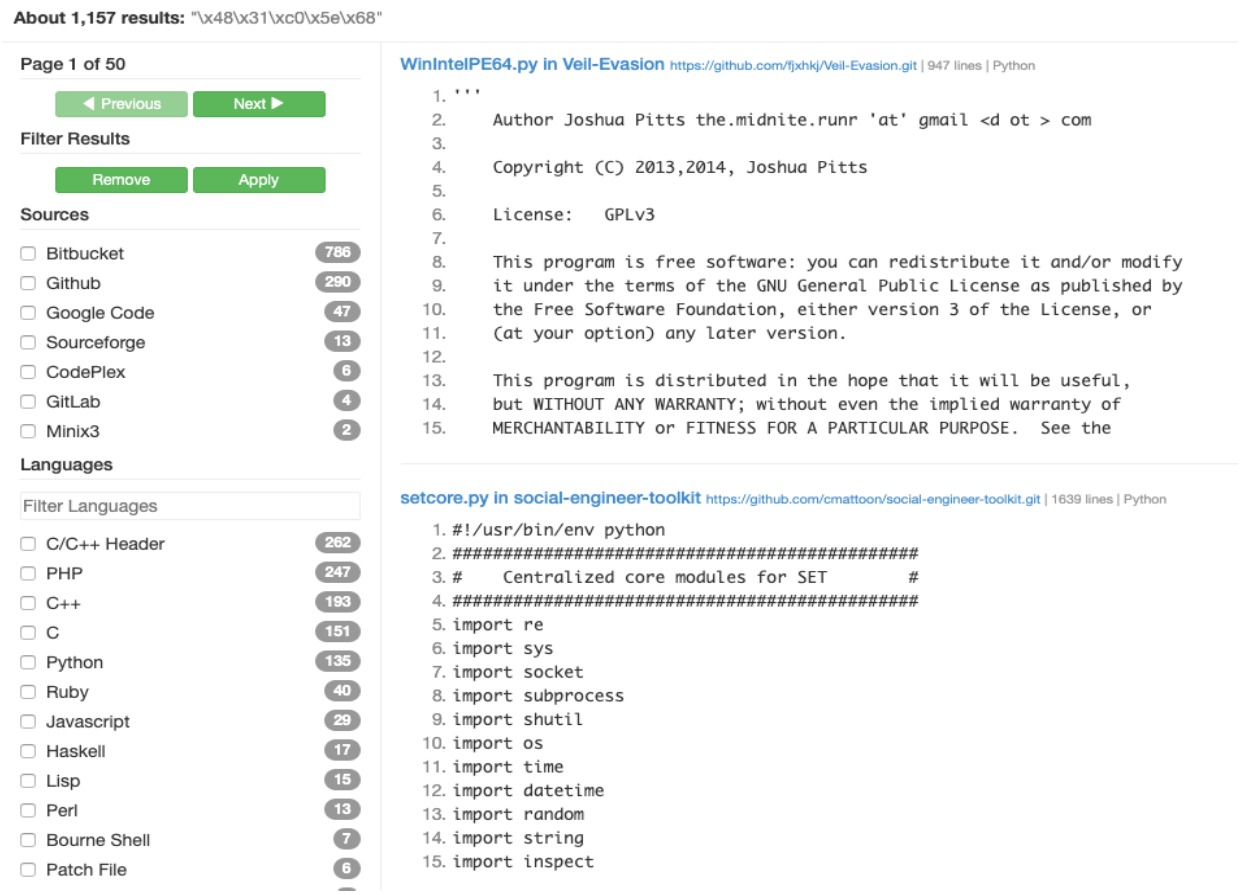


Рисунок 13.6.

Как вы можете видеть на рисунке 13.8, на GitHub найдено 15 совпадений для термина «c3nt3rx».
К счастью для нас, он был основным разработчиком KickAss Framework, хакерского
набор инструментов, поддерживаемый некоторыми участниками форума KickAss (включая Cyper).
Главный вывод здесь заключается в том, что ни один инструмент никогда не бывает идеальным, и вы всегда должны проверять
ваши результаты из нескольких источников. При использовании инструментов, которые объединяют результаты
несколько сайтов, также стоит проверить исходный сайт, чтобы убедиться, что ваши результаты
являются точными и согласованными между агрегированным сайтом и исходным сайтом.
Теперь, когда у нас есть новое направление для изучения фреймворка KickAss,
посмотрим, сможем ли мы узнать что-нибудь еще на странице GitHub.

Гитроб

Gitrob - это инструмент с открытым исходным кодом, используемый для поиска потенциально конфиденциальных файлов или
информация, хранящаяся в публичных репозиториях GitHub. Гитроб пригодится исследователям
и разработчикам, потому что он сканирует репозиторий и помечает информацию, которая
может быть потенциально опасным или частным.

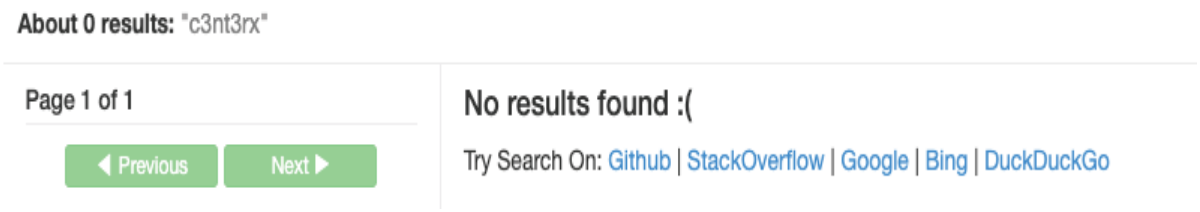


Рисунок 13.7

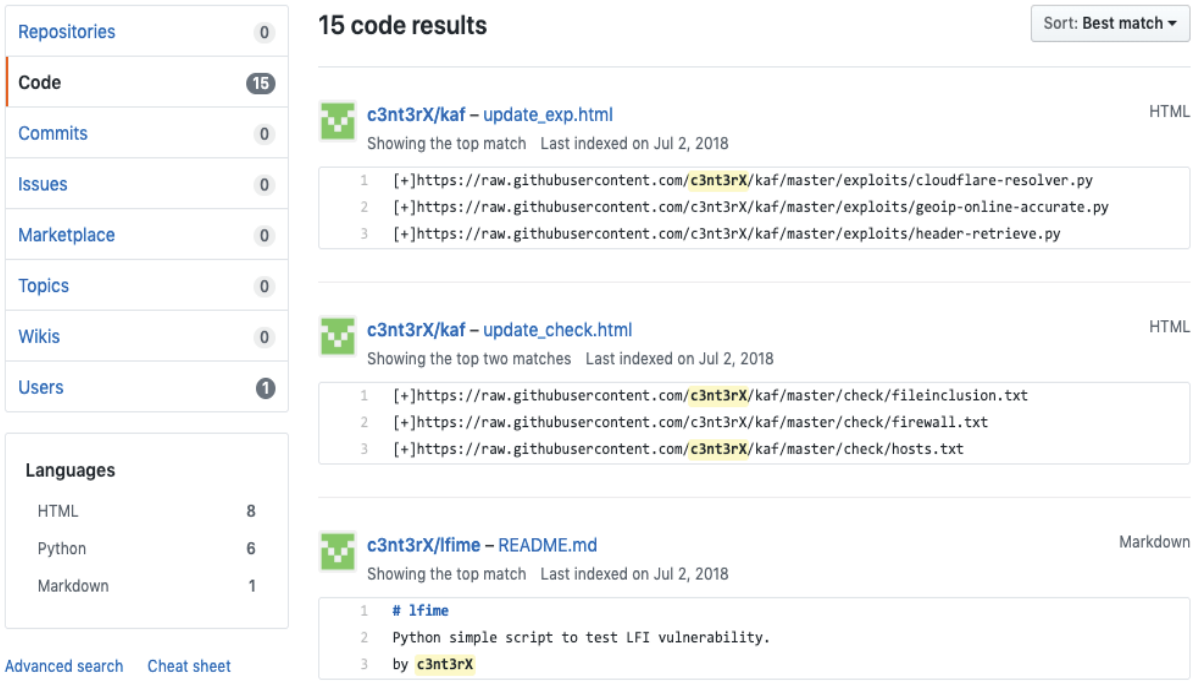


Рисунок 13.8

Gitrob работает путем клонирования общедоступных репозиториев и просмотра
совершать истории. Он помечает потенциально важные файлы и представляет свою находку.
файлов через веб-интерфейс для дальнейшего анализа. Результаты также можно экспортировать
в файл JSON.

Запуск Gitrob против репозитория c3nt3rx даст нам следующие результаты:

```
> gitrob -bind-адрес 0.0.0.0 c3nt3rx
_ __
__
___ _ (_) / _____ / /
/ _ `/ / __ / __ / _ \ / _ \
\ _, / _ / \ __ / _ / \ ___ / _.__ /
/ ___ / автор: @michenriksen
gitrob v2.0.0-beta началась 2019-07-15T03: 34: 29Z
Загружено 91 подпись
Веб-интерфейс доступен по адресу http://0.0.0.0:9393
Сбор целей ...
Получено 7 репозиториев с c3nt3rX
Анализируем 7 репозиториев ...
Выводы ....: 0
Файлы .....: 77
Коммитов .....: 63
Репозиторий: 7
Цели .....: 1
```

Эти результаты могут ввести в заблуждение. Хотя результаты показывают 77 файлов и 63 коммитов, если Gitrob не обнаружит ничего интересного, веб-face покажет 0 результатов.

В данном конкретном случае, поскольку нет результатов, которые Гитроб считал «интер-
esting », веб-интерфейс покажет 0 результатов.

Чтобы показать контрастный пример с лучшими результатами, я запустил Gitrob против
репозиторий michenriksen (разработчик Gitrob):

```
gitrob -bind-address 0.0.0.0 michenriksen
_ __
__
___ _ (_) / _____ / /
/ _ `/ / __ / __ / _ \ / _ \
\ _, / _ / \ __ / _ / \ ___ / _.__ /
/ ___ / автор: @michenriksen
gitrob v2.0.0-beta началась 2019-07-15T03: 31: 42Z
Загружено 91 подпись
```

```
Веб-интерфейс доступен по адресу http://0.0.0.0:9393
Сбор целей ...
Получено 20 репозиториев из michenriksen
Анализируем 20 репозиториев ...
ИЗМЕНИТЬ: содержит слово: учетные данные
Путь .....: credentials.json
Репо .....: michenriksen / searchpass
Сообщение ....: обновить пароли
Автор .....: Майкл Хенриксен <michenriksen@neomailbox.ch>
URL-адрес файла ...: https://github.com/michenriksen/searchpass/blob/
a245aee .. [усечено]
URL фиксации: https://github.com/michenriksen/searchpass/commit/
a245ae .. [усечено]
ИЗМЕНИТЬ: содержит слово: учетные данные
Путь .....: credentials.json
Репо .....: michenriksen / searchpass
Сообщение ....: обновить пароли
Автор .....: Майкл Хенриксен <michenriksen@neomailbox.ch>
URL-адрес файла ...: https://github.com/michenriksen/searchpass/blob/
ff908 ..
[усечено]
URL фиксации: https://github.com/michenriksen/searchpass/commit/
ff9085c .. [усечено]
Выводы ....: 2
Файлы .....: 539
Коммитов .....: 225
Репозиторий: 20
Цели .....: 1
Нажмите Ctrl + C, чтобы остановить веб-сервер и выйти.
```

Сразу видна разница в результатах. Gitrob предоставляет описание:
какие «интересные» предметы обнаружены, и их местонахождение. в
В случае с этим репозиторием результаты показывают, что некоторые файлы содержат слово
"Учетные данные".

Теперь, когда мы получаем доступ к веб-серверу, мы можем увидеть более подробный список
обнаруженные предметы. На рисунке 13.9 показан каждый из обнаруженных элементов вместе с
прямые ссылки для их просмотра.

Gitrob запрограммирован на поиск таких вещей, как ключи SSL, сохраненные учетные данные,
и множество другой информации. Если вы столкнетесь с репозиторием с большим количеством данных, это
экран загорится с информацией.

Журналы фиксации Git

Другой подход к сбору информации может заключаться в простом рассмотрении
журналы фиксации Git репозитория. Журналы Git показывают время и дату каждого сообщения.
mit, включая информацию о лице, совершившем изменения. С
каждая фиксация *должна* иметь связанный адрес электронной почты, журналы могут показывать новые
информация о цели, например новые псевдонимы или адреса электронной почты.
Чтобы проиллюстрировать мою точку зрения, давайте исследуем репозиторий c3nt3rx на предмет «KickAss
Фреймворк." Фреймворк открыто обсуждался на форуме KickAss и
могут быть напрямую связаны с несколькими ключевыми участниками форума, включая АНБ,
админ сайта (который на самом деле наш приятель Сайпер).
Для тех, кто играет дома, URL-адрес фреймворка - https: //
github.com/c3nt3rX/kaf .
После проверки репозитория вы можете просмотреть журналы фиксации, набрав
git журнал :

```
[root @ OSINT]> git log
совершить 9a8d392f4265f9fafec854d06bcc86608c393b3a
Автор: NSA < nightsquare@sigaint.org >
Дата: 16 июня, 22:11:16 2016 +0200
изменения
совершить c9282534f031f066450197f31ef985d07661daa7
Автор: NSA <nightsquare@sigaint.org>
Дата: 16 июня, 22:09:33 2016 +0200
некоторые изменения и новые скрипты
```

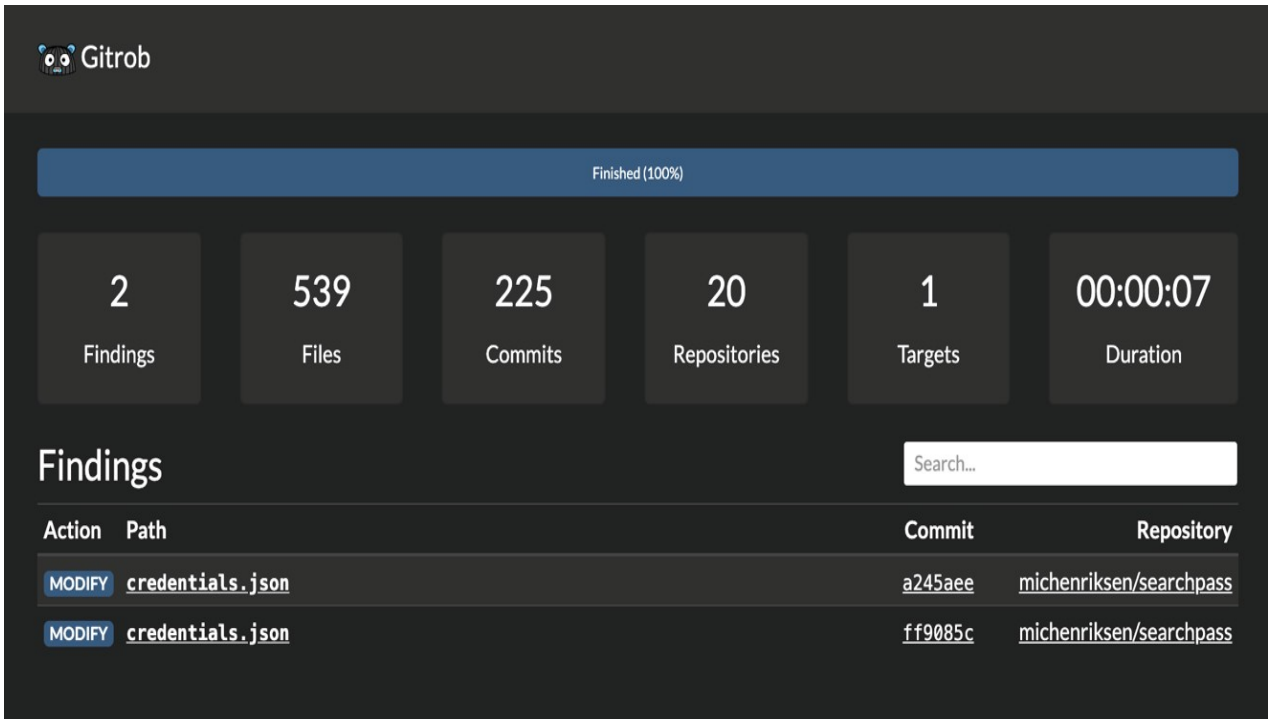


Рисунок 13.9

совершить 20fa61ff8113dd34e2dd6a2485b9654d6e09459a
Автор: NSA <nightsquare@sigaint.org>
Дата: 27 мая, пт, 01:18:05 2016 +0200
новый баннер
совершить af98fc17cec67f8a3085f374161cec93e15cd177
Автор: NSA <nightsquare@sigaint.org>
Дата: 25 мая 19:01:38 2016 +0200
новый ридми
совершить fd594e4bbc70e184005a7a3931a02aa7d3613b5a
Автор: **c3nt3rX < centerx@hotmail.gr >**
Дата: 21 мая 02:53:06 2016 +0300
Обновите kaf.py
совершить c06b68662da1b8690963a47930d24f04e6a75028
Автор: c3nt3rX <centerx@hotmail.gr>
:...пропуская...
совершить 6fbe9999d2fb68fb0954866328ad63505f4a06a5
Автор: NSA <nightsquare@sigaint.org>
Дата: 30 июня, 08:06:54 2016 +0200
изменить пожертвовать адрес

Глядя на результаты, мы видим двух разных авторов: NSA и c3nt3rx.

У каждого из авторов есть собственный связанный адрес электронной почты - теперь у нас есть электронная почта. адрес для c3nt3rx и действительно интересный адрес электронной почты для NSA (Cyper) - nightquare@sigaint.org .

«NightSquare» - действительно интересный адрес электронной почты, потому что первые два буквы в АНБ можно сопоставить с Ночью и Квадратом. Не знаю, монетка ли это-cidence, или если за названием NSA стоит больше смысла. Если да, то что означает буква «А» стоять за?

В следующем разделе будет показано, что Сайпер живет в Австрии (или около нее), поэтому, возможно, это имя ссылка на Ночную площадь Австрии?

Мне так и не удалось понять это, поэтому, если у кого-то, читая это, есть идеи, пришлите мне сообщение.

Вики-сайты

Для меня нет ничего более приятного, чем ощущение того, что я нашел этот «джекпот». улика во время расследования. Это чувство умножится, если вы также закончить его фразой «какой идиот» [SMH].

Это возвращает нас к истории нашего друга Сайпера (он же CyPeRtRoN, он же
Призрак, он же АНБ).
Одна из наиболее узнаваемых черт Сайпера - это то, как он *всегда* говорит о своем
принадлежность к Hackweiser (хакерская группа конца 90-х). Он действительно
никогда не молчите об этом, что упростило отслеживание его по аккаунтам. Один раз
вы знаете, что искать, или у вас есть какая-то ключевая идентифицируемая информация,
продолжайте, части начнут становиться на свои места.
При этом 24 июля 2015 г. состоялось следующее обсуждение
Galaxy 2, социальная сеть на основе TOR, где были пользователи Cyper и Arsyntex.
вовлечены в еще одну бурную дискуссию:
24 июля 2015 г.
Автор: CyPeRtRoN
для всех остальных - не будь параноиком - не трахайся со мной, и все
хороший ...
Автор: Арсинтекс
Остерегайтесь @CyPeRtRoN - это профессиональный трассировщик файлов cookie. Это один из
Суки АНБ и GCHQ xD
Автор: CyPeRtRoN
LOL, хорошо, спасибо за промо - ты не знаешь, кто я - ты думаешь, ты выпускаешь
2 опыта и теперь ты человек Джогеш
Автор: CyPeRtRoN
что почитать для вас https://en.wikipedia.org/wiki/Hackweiser
Автор: Арсинтекс
Члены включены; R4ncid, Bighawk, [P] hoenix, Immortal, RaFa,
Squirrlman, PhonE_TonE, odin, x [beast] x, Phiz, **@CyPeRtRoN** и
Джак-прочь (AKA Hackah Jak). **хахаха** (¬˘¬)
Из этого обсуждения можно сделать два интересных и важных вывода:
URL-адрес Hackweiser в Википедии и реакция Arsyntex на публикацию Cyper
URL-адрес.
До этого момента я никогда не считал Википедию (или любую другую общедоступную
wiki), чтобы быть возможным источником достоверной информации.
Я был неправ.

Википедия

Википедия, несмотря на общее отсутствие доверия к ней как к надежному источнику информации,
действительно хорошо справляется с одной задачей: ведет точный и публичный учет каждого изменения
внесены на его страницы (запрошенные или постоянные).

Текущий сайт Википедии для Hackweiser (https://en.wikipedia.org/w/index.php? title = Hackweiser) перечисляет следующие члены: R4ncid, Bighawk, [P] Hoenix, Immortal, RaFa, Squirrlman, odin, x [beast] x, Phiz и Jak-away (AKA Hackah Jak).

Как вы, возможно, заметили, в этом навсегда отсутствует ключевой член. увековеченный список: великий CyPeRtRoN.

Но ждать . . . Мы только что увидели сообщение из Galaxy 2, где Cyper был явно указан как член Hackweiser. Он даже хвастался этим.

Помните, что в глазах молодого и честолюбивого хакера *тщеславие всегда будет Трамп ОПСЕК* .

Чтобы подтвердить мою точку зрения, мы можем обратиться к вкладке «Просмотр истории», расположенной на каждом Страница Википедии (показана на рисунке 13.10).

На странице просмотра истории для Hackweiser (рисунок 13.11) мы видим полный список изменения, внесенные на страницу (в этот список входят как постоянные, так и удаленные изменения).

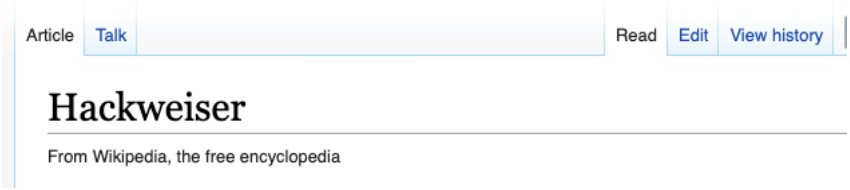


Рисунок 13.10



Рисунок 13.11

Возвращаясь к нашему разговору из Galaxy 2, сообщение от Сайпера было
от июня 2015 г. Обратите внимание на рис. 13.11, что есть запись за май 2015 г.? К
Чтобы понять все последствия изменения, произошедшего в мае 2015 г., давайте сначала посмотрим на предыдущие
запись за ноябрь 2014 г. (которую можно просмотреть прямо на https: //en.wikipedia.
org / w / index.php? title = Hackweiser & oldid = 635593910).
Согласно этой странице с ноября 2014 года, членами Hackweiser являются
R4ncid, Bighawk, [P] hoenix, Immortal, RaFa, Squirrlman, PhonE_TonE, odin,
x [beast] x, Phiz и Jak-away (AKA Hackah Jak) - точно такой же список, что и в
текущая страница.
В Википедии также есть очень удобная кнопка «Сравнить выбранные версии» (т. Е.
инструмент diff). Каждая версия страницы, показанной на рисунке 13.11, имеет переключатель.
рядом с ним. Установите переключатель для версии от мая 2015 г., затем нажмите
Сравнить выбранные версии, мы перейдем на страницу различий, на которой показаны различия.
между двумя записями (рисунок 13.12).
Вы также можете просмотреть эту страницу различий напрямую по этой ссылке: https: //en.wikipedia.
org / w / index.php? title = Hackweiser & diff = 662753224 & oldid = 635593910 .
Как вы уже, наверное, догадались, список участников за май 2015 г.
содержит одно дополнительное специальное дополнение: **CyPeRtRoN** .
Мог ли наш друг Сайпер быть настолько тщеславным, чтобы целенаправленно изменить свое имя на
страницу Википедии? И что еще более важно, готов ли он принять
риск внесения этого изменения с IP-адреса, отличного от VPN, чтобы добавить легитимность
его редактировать?
Если вы пропустили это в первый раз: *тщеславие всегда будет выше OPSEC* .
Быстрый поиск на whatismyipaddress.com (рис. 13.13) дает нам приблизительную
имейте местоположение 62.93.70.34, IP-адрес, используемый для изменения
Страница Википедии.
Мог ли Сайпер быть настолько тщеславным, чтобы редактировать эту Википедию прямо из
его дом? С юридической точки зрения я не могу сказать наверняка, но это довольно солидная зацепка!

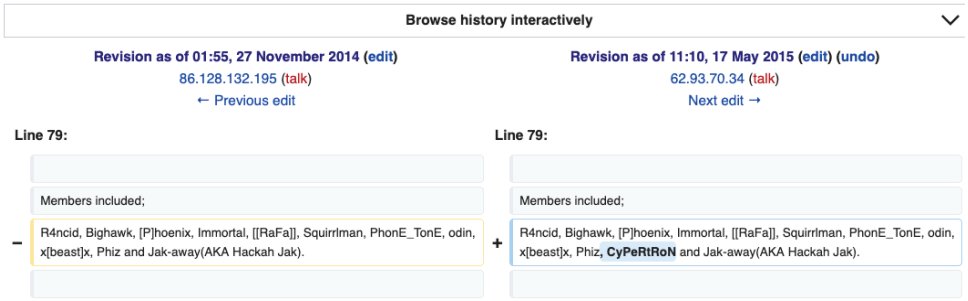


Рисунок 13.12

Дополнительную информацию о размещении Cyper в Австрии или ее окрестностях можно найти в официальный отчет о расследовании "Темного повелителя".

Резюме

Эта глава была сосредоточена на раскрытии скрытой информации в различных
разбросанные уголки интернета. Это включает использование таких инструментов, как theHarvester
для сбора разнообразной информации и более специализированных инструментов, таких как Gitrob для
сбор информации для GitHub.
Подробности и примеры, представленные в этой главе, должны сделать ее
ясно, что даже в самых случайных (и малоизвестных) местах, таких как форумы, сайты-вставки,
репозитории кода и вики-страницы могут предложить очень неожиданные результаты, а некоторые -
раз новаторские улики в расследовании.
В следующей главе мы расширим наш поиск еще дальше, чтобы найти
информация из общедоступных баз данных, таких как MongoDB и Elasticsearch.

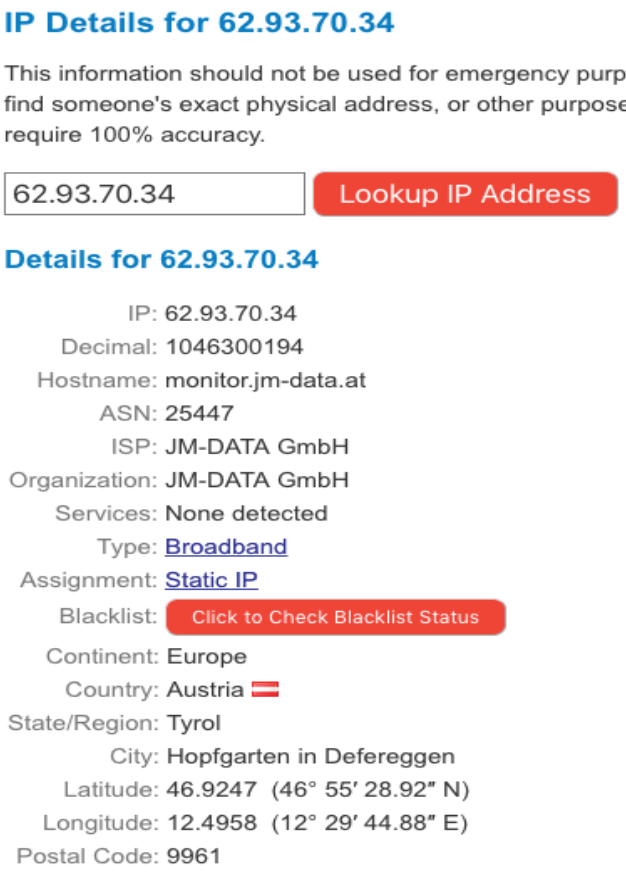


Рисунок 13.13

293

14

Обнаружение утечек данных (или утечек данных) никогда не бывает легким делом. Что я имею в виду под
это выяснение того, как поступить с ситуацией, когда вы обнаружите
Нарушение или утечка, по моему опыту, самая сложная часть всего процесса.
В этой главе будут рассмотрены обе стороны этой истории. Посмотрим на методы
для обнаружения данных в нескольких распространенных базах данных NoSQL, таких как MongoDB и
Elasticsearch, а также данные, размещенные на общедоступной платформе облачного хранилища.
такие формы, как ведра Amazon и пространства Digital Ocean. Я также раскрою некоторые
о моих личных открытиях и опыте, связанных с этими открытиями.
Но сначала слово Боба Дьяченко, человека, который лично раскрыл
больше утечек громких данных, чем я знаю.

**Не существует стабильного шаблона, который я буду использовать [для поиска данных] каждый раз, потому что я меняю [методы] на основе полученных мной результатов. И я также намеренно пытаюсь мин-
имейте в виду автоматизацию результатов поиска. Поэтому, когда я просматриваю отчеты, я всегда
это вручную. Я делаю это потому, что раньше упускал из виду важную информацию.
и сделал много ошибок, когда полагался на автоматизированные скрипты.
Когда я начал просматривать результаты, я был удивлен, увидев столько интересных
предметы были упущены из виду. Тогда я начал сам просматривать результаты, а именно:
как я пришел к своему текущему процессу.**

Общедоступное хранилище данных

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

Я разумно избегаю использования каких-либо изощренных или навязчивых методов или чего-либо, что
может ассоциировать меня с тем, что я хакер «в черной шляпе». Инструменты, которые я использую, всегда общедоступны.
Я хочу сказать, что если я смогу найти ваши данные, то любой в мире сможет
сделай это. Поэтому, когда я что-то нахожу, это становится доступно всем в Интернете.
Но только когда я начал заниматься ответственным раскрытием информации, я начал получать
обратная связь со стороны компаний. Особенно от компаний, с которыми действительно сложно связаться.
Я думаю, это может быть потому, что у меня не было профиля в то время - я имею в виду, что я был полностью
случайный человек в эти компании. Они были подозрительными, и это было очень тяжело.
вызов, который нужно преодолеть.
Бывали моменты, когда я почти переставал этим заниматься. Пара компаний пыталась
Сью. Я не знаю, могло ли это быть потому, что я действовал как часть компании, поэтому
может, они надеялись, что подадут на компанию в суд и заработают немного денег? я
честно не знаю.
В конце концов я осознал ценность, которую несу сообществу, как бы ни старался
давление есть. Я также переоценил свой подход к компаниям, а также то, как я
обрабатывать данные. Эти компании, о которых я сообщаю, смущены тем, что произошло.
подписаны, и во многих случаях несут юридическую ответственность за раскрытие данных, поэтому я
Теперь следуйте другому процессу, который, похоже, работает.
В таких ситуациях вам нужно быть очень осторожным с данными, которые вы
смотря на. Будьте готовы объяснить, как вы обрабатывали данные, почему вы
решения, и будьте готовы заверить, что вы единственный, кто
в вашей копии данных (я говорю *вашу* копию, потому что, поскольку данные являются общедоступными, многие люди
можно увидеть это).
К сожалению, большинство компаний меня об этом никогда не спрашивают. Они просто берут
информации и никогда не просите меня подписать соглашение о неразглашении информации и даже не пытайтесь понять, как я обрабатываю данные или
где я его храню. Это действительно интересно.

Утечка Exactis и Шодан

Примерно в июле 2018 года я обнаружил утечку данных Exactis - это была моя первая крупная
общедоступное обнаружение базы данных Elasticsearch. Exactis была маркетинговой фирмой (т.е.
брокер), который зарабатывал деньги, продавая данные другим компаниям. Публичная база данных
содержала сугубо личную информацию о более чем 200 миллионах человек. В
данные включали имена, адреса электронной почты, номера телефонов, адреса, пол, вероисповедание.
религиозные убеждения, политические предпочтения, информация о домашних животных, размеры семьи и множество
другой информации, связанной с образом жизни, например, курит ли человек,
нырять с аквалангом, носить одежду больших размеров и т. д.
Важно отметить, что базы данных Elasticsearch не
иметь права пользователя так же, как и большинство баз данных. По умолчанию вы делаете
не требуется аутентификация данных с использованием имени пользователя и пароля. Роли и
разрешения можно настроить, но по умолчанию ничего нет.

Это означает, что любой, кто пытается получить доступ к вашей базе данных Elasticsearch через IP
адрес на порту 9200 будет иметь полные права CRUD (создание, чтение, обновление, удаление)
к вашим данным, просто запросив URL-адрес. Способ защиты вашего ES-кластера
заключается в том, чтобы поместить все за брандмауэр, чтобы IP-адреса не были публично открыты.

Атрибуция данных

Выявление владельца открытого набора данных обычно является самой сложной частью
расследования, потому что все, что вам нужно, это IP-адрес, а хост -
Компания никогда не откажется от владельца этого адреса без официального
юридический запрос.
Хотя я обычно связываюсь с организацией задолго до того, как с кем-то поговорю.
иначе, этот случай был другим. Попытка определить владельца IP-адреса может
быть одной из самых изнурительных и утомительных задач, которые вам предстоит выполнить,
поэтому я привлек несколько человек, чтобы они помогли.
Мне потребовался целый месяц, чтобы выяснить, кому на самом деле принадлежат данные Exactis.
После нескольких недель, когда я не мог найти владельца, я обратился в суд.
правоохранительные органы и репортеры, которые потенциально могут помочь.
К тому времени, когда мы выяснили, что Exactis был владельцем открытых серверов,
Я уже тесно сотрудничал с Энди Гринбергом в *Wired* . Когда мы
наконец-то разобрался, я немедленно связался с Exactis и посоветовал взять
данные в автономном режиме, потому что они были полностью открыты.
Я объяснил, что уже уведомил правоохранительные органы, потому что данные
в нем содержалась информация почти о каждом гражданине США, а также о том, что я
работал с *Wired* во время моего расследования. Я настоятельно рекомендовал им поговорить с
Энди, чтобы зафиксировать свою точку зрения, чтобы помочь с устранением повреждений.
То, что случилось с Exactis после публикации истории *Wired,* не соответствует действительности.
то, что я мог предсказать, и что-то, что мне до сих пор не нравится из-за этого
день. Компания вышла из бизнеса, а ее владелец Стив Хардигри
в настоящее время сталкивается с несколькими коллективными исками. Однажды ночью я даже получил сообщение
сообщение от Стива, спрашивающего меня, почему я разрушил его жизнь.
Я не собираюсь лгать, это отстой, потому что я знаю, что в этом есть доля правды. На
с другой стороны, он является генеральным директором компании, которая оставила все эти данные открытыми. В
в какой-то момент это была его обязанность. И откровенно говоря, учитывая, сколько исследователей
искать открытые хранилища данных, это был лишь вопрос времени, когда кто-то другой
нашел бы данные.
Согласно последней публикации *Wired* , генеральный директор заявляет, что данные были
остается открытым только «на несколько дней». У меня другой взгляд на этот вопрос
исходя из того, сколько времени мне потребовалось, чтобы найти данные.
При этом мое «слово» ничего не значит. Придет время в каждом
карьеру следователя, когда нужно будет подкрепить свои слова

факты, и именно эта ситуация научила меня нескольким новым удивительным и полезным Shodan tecqhniques.

Параметры командной строки Shodan

Большинство исследователей используют веб-интерфейс Shodan, но многие люди могут не осознают (как и я) всех расширенных возможностей, доступных через Shodan's инструменты командной строки.

Одним из больших преимуществ инструментов командной строки Shodan является возможность загрузить все результаты определенного типа базы данных.

Например, можно было бы, чтобы Shodan предоставил нам все IP-адреса публично доступные базы данных Elasticsearch. Для этого требуются две отдельные команды.

Первый для загрузки данных, а второй для их синтаксического анализа в пригодный для использования формат.

Именно такой процесс я использовал для обнаружения утечки данных Exactis.

Сначала мы можем указать инструменту Shodan загрузить все IP-адреса, на которых запущен Elasticsearch. используя следующий синтаксис:

```
Shodan download --limit (количество результатов) (ваше имя файла) (запрос)
```

Для полной загрузки всех общедоступных баз данных Elasticsearch я установил ограничение на 50 000 записей. В веб-интерфейсе отображается около 30 000 записей, поэтому я намеренно установил это число выше, чтобы убедиться, что все включено:

```
root @ osint:> shodan download --limit 50000 elasticdata product: эластичный
Поисковый запрос:
продукт: эластичный
Общее количество результатов: 28289
Осталось кредитов на запрос: xxxx
Выходной файл:
elasticdata.json.gz
```

Теперь, когда мы имеем загруженные результаты, мы можем использовать синтаксическую анализ команды для извлечения нужных нам данных. В этом случае я обычно просто извлекаю IP и номер порта с помощью следующей команды:

```
shodan parse –fields ip_str, port --separator, elasticdata.json.gz
```

Это создаст проанализированный файл, содержащий только IP-адреса и номера портов. Позже в этой главе мы будем использовать эту информацию для автоматизации процесса идентификации серверы, на которых может происходить утечка конфиденциальной информации.

Запрос исторических данных

Ранее в этом разделе я упоминал, что сценарий Exactis научил меня чему-то действительно полезно об инструментах командной строки Shodan. Помимо возможности легко запрашивать и загружать необработанные данные, инструменты Shodan также позволяют выполнять поиск историческая информация об IP-адресах. Это означает, что в любой момент времени Shodan не только определяет, какие порты открыты на IP-адресе, но и

также ведите исторический учет этих данных, которые вы можете запросить. Применим это к
IP-адреса Exactis и посмотрим, что мы сможем найти.

У Exactis было три IP-адреса, связанных с кластером Elasticsearch:

- 172.106.108.69
- 172.106.108.73
- 172.106.108.77

В рамках расследования вас могут (и, скорее всего, будут) попросить предоставить
некоторый уровень доказательств (или свидетельских показаний) относительно продолжительности времени, в течение которого IP
адрес или набор данных был в сети. В последующих интервью *Wired* журнала,
Генеральный директор Exactis Стив Хардигри «настаивает на том, что данные были открыты только на
дело дней. "

Посмотрим, что нам расскажет Шодан.

Следующий синтаксис будет запрашивать историческую информацию по IP-адресу:

```
shodan host --history -S --format pretty (IP-адрес)
```

Выполнение этого для одного из IP-адресов Exactis вернет следующую информацию:

```
[root @ OSINT]> хост shodan --history -S --format pretty 172.106.108.77
172.106.108.77
Город:
Эшберн
Страна:
Соединенные Штаты
Организация:
Psychz Networks Эшберн
Обновлено:
2019-04-11T06: 43: 30.053445
Количество открытых портов: 7
Уязвимости:
CVE-2018-15919 CVE-2018-15473 CVE-2017-15906
Порты:
25 / TCP
(2016-09-02)
25 / TCP
(2016-08-30)
25 / TCP
(18.06.2016)
25 / TCP
(2016-06-16)
80 / tcp Apache httpd (2.2.15).
(2016-10-14)
2020 / TCP OpenSSH (7,4)
(2019-04-11)
3306 / TCP MySQL
(2016-06-02)
5601 / TCP
(2018-06-01)
5601 / TCP
[результаты усечены]
9200 / tcp эластичный (6.2.4)
(2018-06-04)
9200 / tcp эластичный (6.2.4)
(2018-06-02)
9200 / tcp эластичный (6.2.4)
(2018-05-29)
9200 / tcp эластичный (6.2.4)
(2018-05-25)
9200 / tcp эластичный (6.2.2)
(2018-05-07)
9200 / tcp эластичный (6.2.2)
(2018-04-27)
9200 / tcp эластичный (6.2.2)
(2018-04-03)
9200 / tcp эластичный (6.2.2)
(2018-03-31)
9200 / tcp эластичный (6.2.2)
(2018-03-20)
```

9200 / tcp эластичный (6.2.2)
(2018-03-18)
9200 / tcp эластичный (6.2.2)
(2018-03-11)
9200 / tcp эластичный (6.1.1)
(2018-02-19)
9200 / tcp эластичный (6.1.1)
(2018-02-15)
9200 / tcp эластичный (6.1.1)
(2018-02-15)
9200 / tcp эластичный (6.1.1)
(2018-02-10)
9200 / tcp эластичный (6.1.1)
(21.01.2018)
9200 / tcp эластичный (6.1.1)
(2018-01-03)
9200 / tcp эластичный (6.0.0)
(2017-12-14)
9200 / tcp эластичный (6.0.0)
(2017-12-07)
9200 / tcp эластичный (6.0.0)
(2017-11-24)

Из этих результатов видно, что порт 9200 (типичный порт для
Сервер Elasticsearch) был впервые обнаружен Shodan 24 ноября 2017 г.
оставались открытыми до 4 июня 2018 г. (примерно в то время, когда я с ними связался
и история сломалась).

Это означает, что согласно исторической информации Шодана, серверы
были открыты целых семь месяцев, прежде чем я их обнаружил. Вот почему у меня
проблемы с принятием заявления генерального директора Exactis о том, что серверы были только в сети
«за считанные дни».

Эта информация по крайней мере заставила меня почувствовать себя лучше в связи с открытием, и
конечный результат организации. Я полностью понимаю
Гнев и негодование генерального директора на меня. Однако семимесячный период - это
совсем другая ситуация. Учитывая, сколько других компаний, исследователей,
и преступники собирают общедоступные наборы данных, весьма вероятно, что я не единственный
человек, который нашел эти данные, но, возможно, был единственным человеком, способным выяснить
кто это владел.

Думаю, в конце концов, его жизнь не пострадала, потому что Стив вернулся к продаже данных в своей новой компании BrightSpeed (www.brightspeed.com)**.**

Надеюсь, мой аккаунт не только поможет пролить свет на события, связанные с
обнаружение и объявление инцидента Exactis, но также помогает дать больше
контекст вокруг типов ситуаций и последствий, которые следователи могут
лицо во время своей карьеры.

CloudStorageFinder

CloudStorageFinder (CSF) - это инструмент с открытым исходным кодом, написанный Робином Вудом, который
делает именно то, что следует из названия - находит общедоступное облачное хранилище
ведра. Доступен ряд инструментов поиска облачного хранилища, но я выбрал CSF.
из-за его способности выполнять поиск не только в AWS.

CSF может выполнять поиск в общедоступных корзинах Amazon S3, Digital
Пространства океана и общие папки SpiderOak. CloudStorageFinder доступен
на https://github.com/digininja/CloudStorageFinder .

CSF работает путем перебора общедоступных URL-адресов, поэтому чем лучше ваш список слов, тем лучше
у вас будет больше результатов. Вернитесь к главе 2 о методах создания отличных
списки слов для брутфорса.

CSF имеет три ключевых инструмента: bucket_finder.rb, space_finder.rb и spider_finder.
руб. Как вы, наверное, догадались, bucket_finder.rb используется для поиска Amazon.
Ковши S3, space_finder.rb используется для поиска пространств Digital Ocean, a spider_
finder.rb используется для поиска общих папок SpiderOak.

Параметры и параметры для всех трех программ очень похожи, основные
разница в параметрах региона. В каждом случае размещается общественное хранилище
в разных регионах, поэтому этот параметр может меняться в зависимости от разных
услуги, которые вы ищете.

Параметры поисковой системы CSF S3 включают:

--help, -h: показать справку
--download, -d: скачать файлы
--log-file, -l: имя файла для записи вывода в журнал
--region, -r: используемый регион, варианты:
us - стандарт США
ie - Ирландия
NC - Северная Калифорния
si - Сингапур
в - Токио
-v: подробный
список слов: список слов для использования

Amazon S3

Предполагая, что у вас есть готовый к работе список слов bruteforce, запуск CSF довольно удобен.
простой. Для нашего первоначального сканирования мы запустим bucket_finder против США.
регион и загрузите все, с чем мы сталкиваемся, используя -d :

[корень @ osint]> ./bucket_finder.rb -r us -d wordlist.txt -l logfile.txt

Результат моих первоначальных сканирований выглядел примерно так:

Bucket iis перенаправляет на: iis.s3.amazonaws.com
Сегмент не существует: endofspecialwords
Ведра не существует: Орхус
Сегмент найден, но в доступе отказано: Аарон
Ковша не существует: Абеба
Сегмент найден, но в доступе отказано: aback

Ковша не существует: сзади
Ковша не существует: заброшено
Ведра не существует: бросаем
Ведра не существует: отказ
Сегмент не существует: бросает
Сегмент найден, но в доступе отказано: abase

Одна вещь, которую CSF не делает, - это проверка подлинности сегмента использования Ключи API S3. Это будет рассмотрено позже в этой главе с помощью инструмента NoScrape.

Цифровые океанические пространства

Digital Ocean - мой предпочтительный поставщик облачных услуг. Digital Ocean недавно выпущен функция «пробелов», которая является еще одним типом общедоступных корзин, аналогичных Amazon S3. Это здорово, потому что мне всегда нравится просматривать новые услуги, потому что есть большая вероятность неправильной конфигурации прямо из коробки.

Когда вы регистрируетесь в пространстве Digital Ocean, в процессе регистрации запрашивается хотите ли вы иметь общий доступ или ограничить доступ только для пользователей с правильными ключи.

Первоначальная установка и настройка Amazon *значительно* сложнее, поэтому лично я не думайте, что здесь будет много места для ошибки, если только кто-то случайно создает общественное пространство и забывает о нем. Тем не менее, мы все же должны попробовать.

Основное различие в запуске CSF space_finder - небольшое изменение в параметры. К различным параметрам относятся:

Использование: space_finder [ВАРИАНТ] ... список слов
-h, --help: показать справку
-d, --download: скачать файлы
-l, --log-file: имя файла для вывода вывода в журнал
-h, --hide-private: скрыть частные пространства, только показать общедоступные
-n, --hide-not-found: скрыть пропущенные пробелы
-r, --region: регион для проверки, варианты:
all - Все регионы
nyc - Нью-Йорк
ams - Амстердам
sgp - Сингапур
-v: подробный
список слов: список слов для использования

Для нашего тестового запуска мы попробуем запустить space_finder для всех регионов, используя параметр -r all . В остальном все будет так же. Запуск инструмента против «Все» регионы означает, что вы отправите три разных запроса, один для каждый регион:

[корень @ osint]> ./space_finder.rb -r all -d wordlist.txt -l logfile.txt

Результат будет выглядеть примерно так:

```
Пространства нет в регионе ams3: Backup
Пространства нет в регионе nyc3: Backup
Пространства нет в регионе sgp1: Backup
Место не существует в регионе ams3: warez
Место не существует в регионе nyc3: warez
Место не существует в регионе sgp1: warez
Место не существует в регионе ams3: pr0n
Место не существует в регионе nyc3: pr0n
Пробел не существует в регионе sgp1: pr0n
Пространства не существует в регионе ams3: porn
Космоса не существует в регионе nyc3: porn
Пространства не существует в регионе sgp1: porn
Пробел не существует в регионе ams3: Scripts
Пробел не существует в регионе nyc3: Scripts
Пробел не существует в регионе sgp1: Scripts
Место не существует в регионе ams3: IISHelp
Место не существует в регионе nyc3: IISHelp
Пробел не существует в регионе sgp1: IISHelp
Место найдено в регионе nyc3: vinnytroia
(https://vinnytroia.nyc3.digitaloceanspaces.com)
<Личный> https://vinnytroia.nyc3.digitaloceanspaces.com/test/
```

Если вам повезет и вы найдете общественное место, оно будет похоже на предыдущий результат.
для моего личного пространства.

А пока перейдем к базам данных NoSQL и чудесам того, что может быть
нашел там.

Базы данных NoSQL

Традиционные реляционные базы данных имели проблемы с масштабируемостью и гибкостью схемы,
что привело к появлению типов баз данных NoSQL. В наши дни самая современная сеть
приложения используют какую-то базу данных NoSQL. В базе данных NoSQL все
основан на документах и не хранится в традиционных «таблицах».

Помимо скорости и гибкости, большинство этих систем баз данных
также требуют конфигураций безопасности, выходящих за рамки традиционного SQL
базы данных. Например, большинство баз данных Elasticsearch общедоступны.
по умолчанию, если вы не поставите перед ними какой-то брандмауэр или заблокируете доступ
в порт 9200.

В этом разделе будут рассмотрены способы поиска общедоступных данных, хранящихся на sev-
несколько наиболее популярных баз данных NoSQL, включая MongoDB, Elasticsearch,
и CassandraDB.

MongoDB

MongoDB - один из самых популярных типов баз данных NoSQL. MongoDB магазины
данные в гибких JSON-подобных документах, что означает, что они не используют традиционные
SQL-подобная структура таблиц встречается во многих приложениях. Вы можете запросить MongoDB
базы данных различными способами, включая инструменты командной строки Mongo и
Приложения с графическим интерфейсом пользователя, такие как RobotMongo.

Для Монго это интересно, потому что я думаю, что они сделали ошибку в прошлом, что они платят сейчас. В одной из более ранних версий решили оставить значение по умолчанию. конфигурации без каких-либо паролей или авторизации - и эта версия была вполне популярный. Тем не менее, многие компании и администраторы по всему миру используют это устаревшая версия MongoDB и не обновили свое программное обеспечение до более новой версии где эти учетные данные по умолчанию не разрешены. Полные «верительные грамоты» - это просто не пропуск. слово вообще, так что вам даже не нужно пытаться использовать грубую силу. Ты просто не используешь пароль, и вы можете войти в систему.

Робот 3T

Robot 3T - это бесплатный инструмент с графическим интерфейсом, используемый для доступа к MongoDB и работы с ним.
базы данных. Я лично считаю утилиты командной строки Mongo громоздкими.
некоторые и темпераментные. Robot 3T также имеет премиум-версию под названием Studio.
3T, который включает возможность импорта и экспорта из базы данных Mongo.
Прямо сейчас, если у вас нет сохраненных соединений в Robot 3T, первый экран
предложит вам ввести информацию о вашем соединении (рисунок 14.1).
В этом разделе будут показаны экраны, снятые с реального живого сервера MongoDB.
Поскольку я не знаю, кому принадлежат данные (и потому что они не мои), все относящиеся к делу
информация будет скрыта.

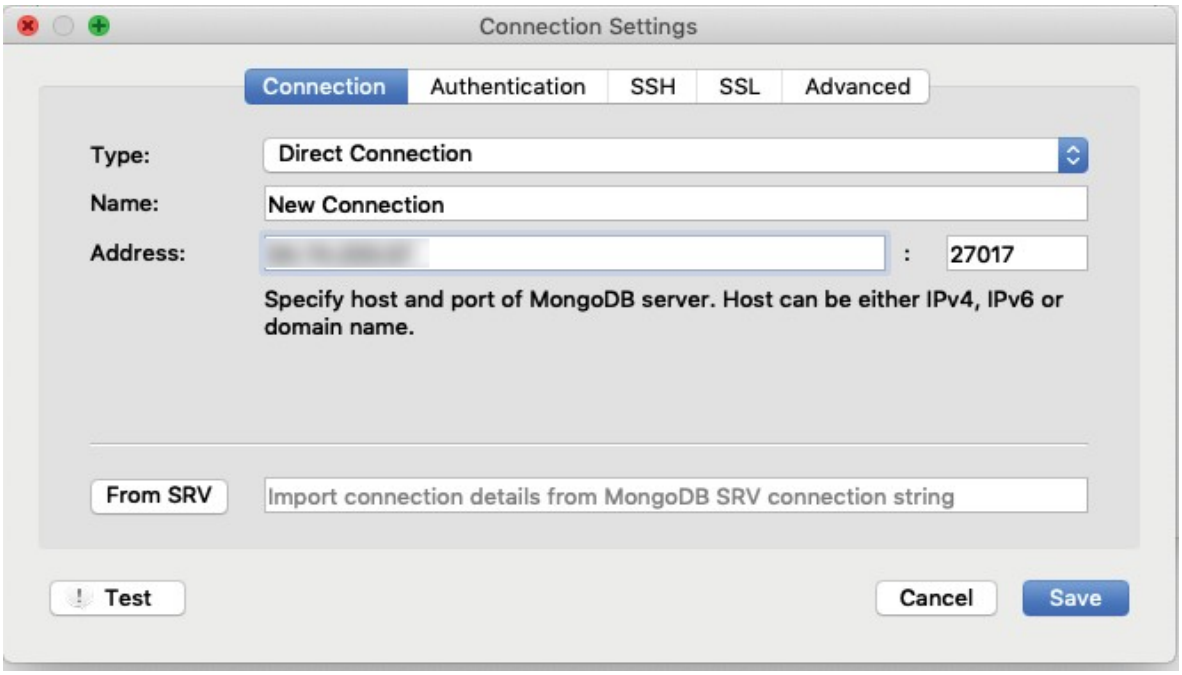


Рисунок 14.1

После того, как вы введете IP-адрес целевого сервера и нажмете «Сохранить», вы перейдете в список соединений MongoDB (показан на рисунке 14.2).

Нажав кнопку «Подключиться», вы подключитесь к серверу MongoDB. В

Первое, что вы заметите в левом столбце, - это древовидное меню со списком доступных файлов. способные базы данных и коллекции. На рисунке 14.3 показаны базы данных, доступные на тестовый сервер.

Для удобства я буду ссылаться на размытое имя базы данных на рисунке 14.3. как PrivateDB.

Расширение каждой из баз данных покажет список коллекций (аналогичный к таблицам) в наличии. На рисунке 14.4 показан список расширенных коллекций для каждого база данных.

Поскольку PrivateDB выглядит наиболее интересным, давайте продолжим изучение этих данных - база. В PrivateDB мы видим восемь разных коллекций. Щелкнув по первому Коллекция «пользователи» развернет окно приложения и покажет нам список документы, доступные в этой коллекции (рис. 14.5).

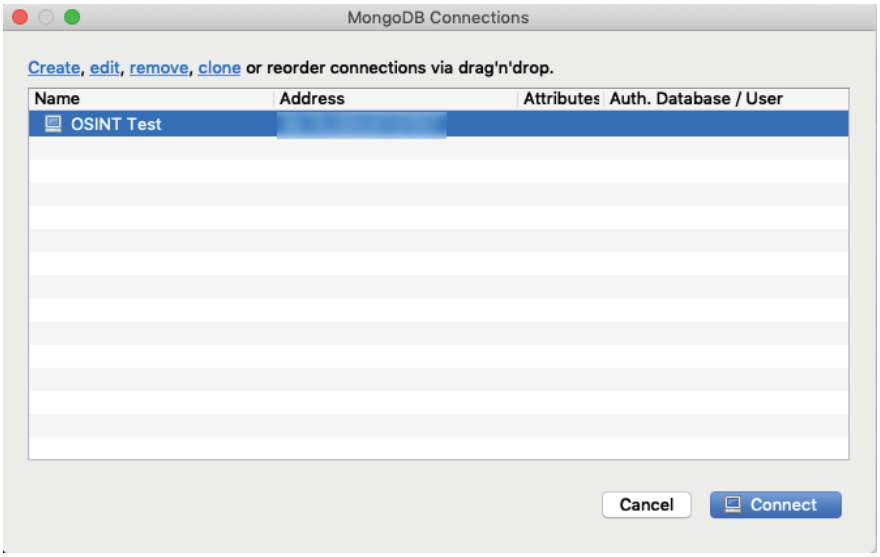


Рисунок 14.2

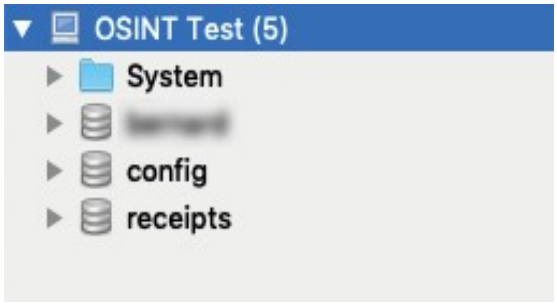


Рисунок 14.3

Из списка видно, что в большинстве документов 11 (или 12)
поля. Чтобы просмотреть различные поля в любом из документов, щелкните стрелку
и он расширит ваше представление, чтобы соответствовать рисунку 14.6.
Это представление также обеспечивает полный доступ для создания, изменения или удаления любых полей.
Поскольку это не наши данные, это все, что нам нужно. Однако изменение данных
Это так же просто, как щелкнуть правой кнопкой мыши нужное поле и воспользоваться меню (рис. 14.7).

Бесплатная версия Robot 3T не позволяет экспортировать данные. если ты хотите захватить всю базу данных, вам нужно будет либо использовать командную строку tools или приобретите лицензию на полную версию инструмента.

Робот 3T отлично подходит для быстрого просмотра отдельных баз данных MongoDB, но
пытаясь быстро просмотреть и обработать десятки тысяч IP-адресов с помощью этого метода
будет невозможно. Позже в этой главе мы рассмотрим инструмент под названием NoScrape,
что поможет с этой функцией. Перед этим давайте быстро взглянем на
Инструменты командной строки Mongo.

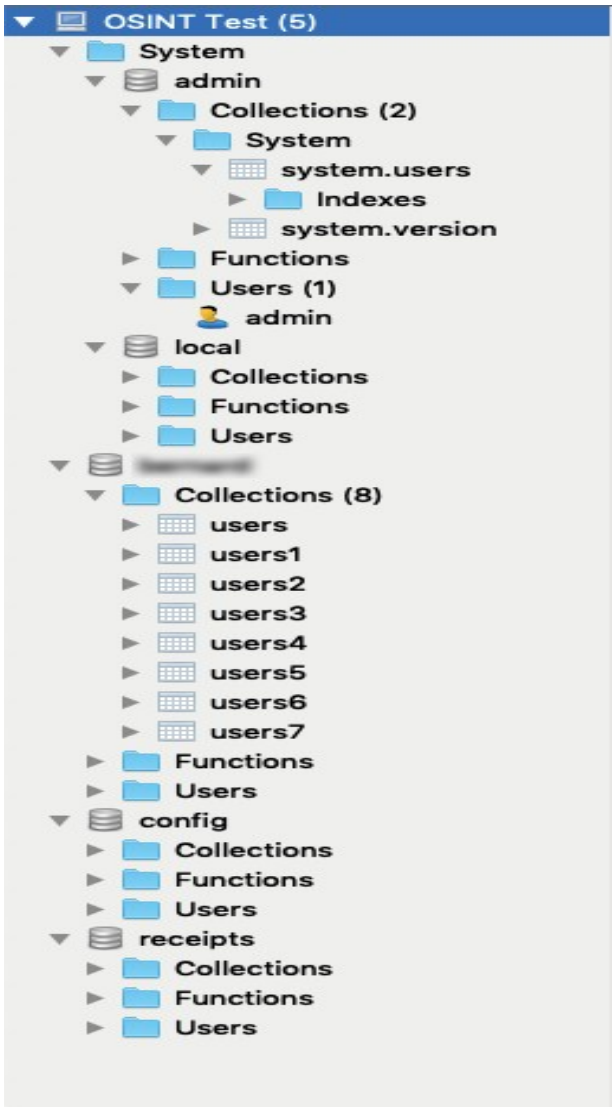


Рисунок 14.4

Инструменты командной строки Mongo

Инструменты командной строки Mongo одинаково полезны для просмотра и сброса
База данных Mongo (хотя сбросить несколько сложнее, чем просмотр).
Этот раздел предназначен только для очень краткого обзора инструментов Mongo по умолчанию.
так как наше основное внимание будет уделено дампу позже в главе, посвященной NoScrape.
После установки инструментов подключитесь к базе данных Mongo, набрав Mongo
за которым следует IP-адрес.

```
[корень @ scraper1 ~]> монго 0.0.0.0
Версия оболочки MongoDB v3.4.20
подключение к: mongodb: //0.0.0.0: 27017 / test
```

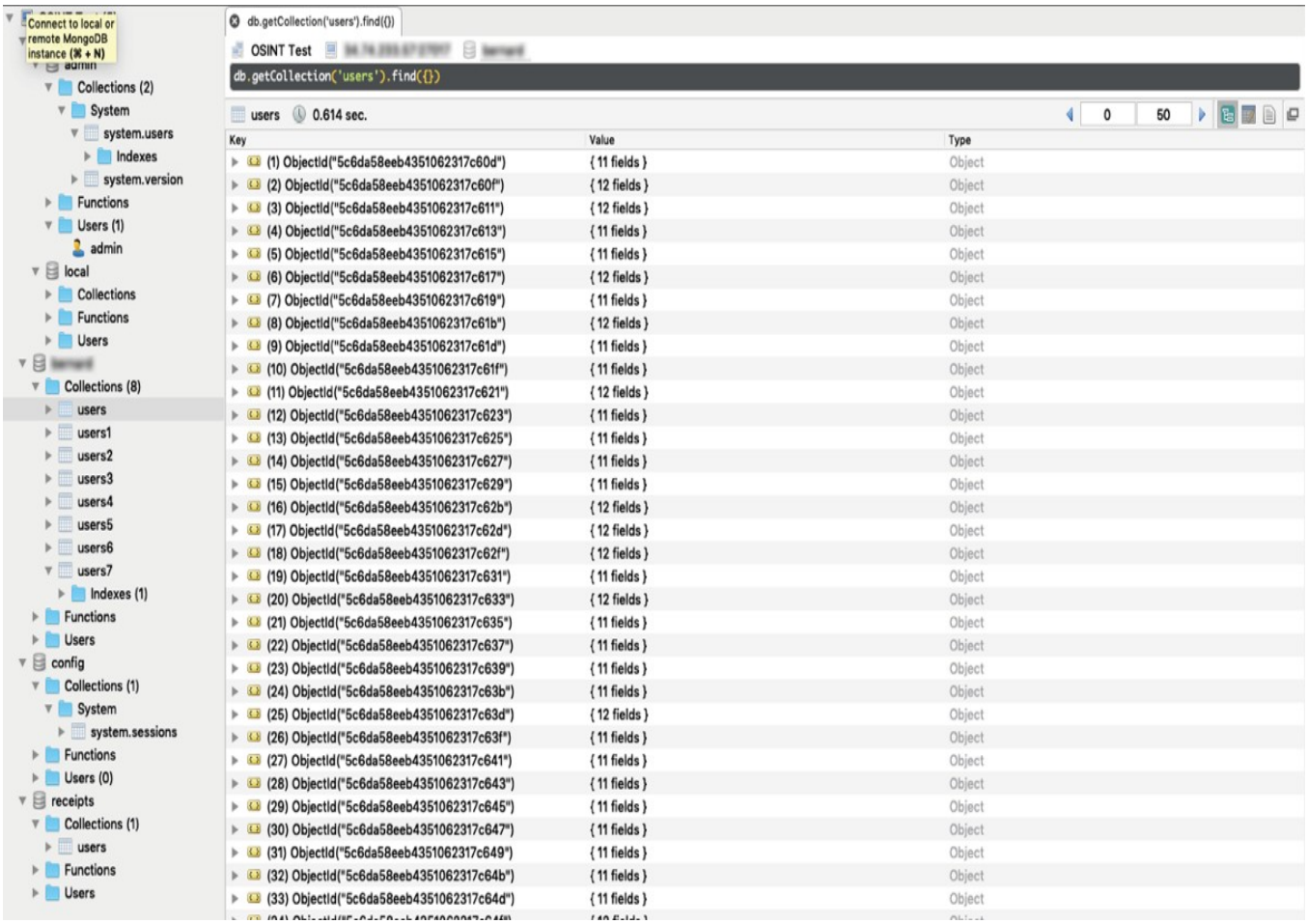


Рисунок 14.5

Версия сервера MongoDB: 4.0.9
ВНИМАНИЕ: версии оболочки и сервера не совпадают
На сервере появляются предупреждения о запуске:
2019-04-17T00: 03: 45.291 + 0000 Я ХРАНИЛИЩЕ [initandlisten]
2019-04-17T00: 03: 45.291 + 0000 Я ХРАНИЛИЩЕ [initandlisten]
** ВНИМАНИЕ: настоятельно рекомендуется использовать файловую систему XFS.
с механизмом хранения WiredTiger
2019-04-17T00: 03: 45.291 + 0000 Я ХРАНИЛИЩЕ [initandlisten]
** См. Http://dochub.mongodb.org/core/prodnotes-filesystem
2019-04-17T00: 03: 48.012 + 0000 Я КОНТРОЛЬ [initandlisten]
2019-04-17T00: 03: 48.012 + 0000 Я КОНТРОЛЬ [initandlisten]
** ПРЕДУПРЕЖДЕНИЕ: для базы данных не включен контроль доступа.
2019-04-17T00: 03: 48.012 + 0000 Я КОНТРОЛЬ [initandlisten]
** Доступ для чтения и записи к данным и конфигурации не ограничен.
2019-04-17T00: 03: 48.012 + 0000 Я КОНТРОЛЬ [initandlisten]

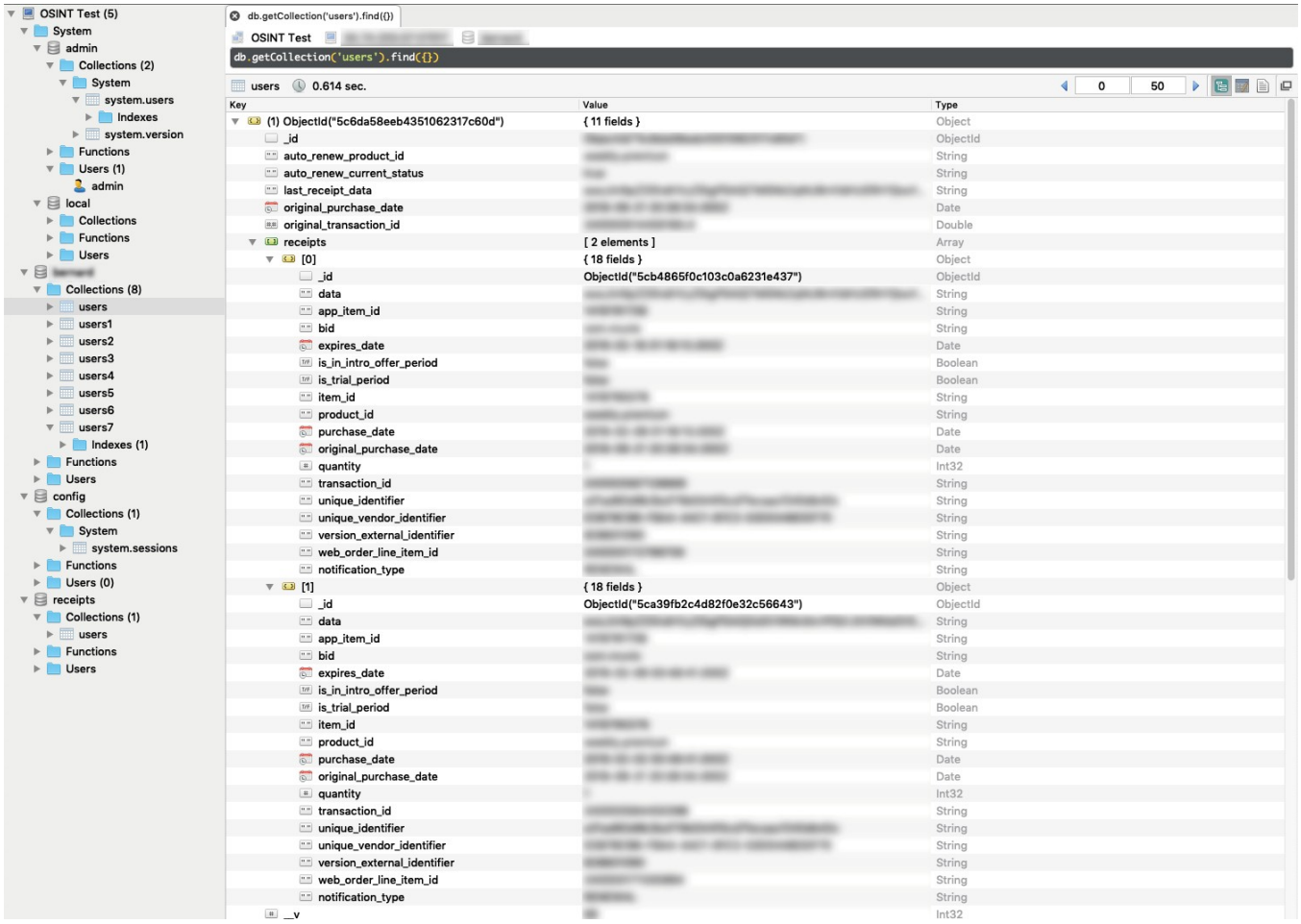


Рисунок 14.6.

Экземпляр MongoDB может иметь несколько баз данных. После подключения
вы можете показать различные базы данных в экземпляре MongoDB, используя команду show
команда dbs :

```
> показать dbs
admin 0,000 ГБ
Бернар 2,507 ГБ
config 0,000 ГБ
местный 0,000 ГБ
квитанции 0,001 ГБ
```

Затем мы можем выбрать конкретную базу данных для использования, набрав **use,** а затем
имя базы данных:

```
> используйте бернарда
переключился на db bernard
```

Отсюда мы можем перечислить различные коллекции в выбранной базе данных.
набрав **показать коллекции** :

```
> показать коллекции
пользователи
users1
пользователи2
пользователи3
пользователи4
пользователи5
пользователи6
пользователи7
```

Выбор коллекции аналогичен выбору базы данных - с помощью использования
команда, за которой следует имя коллекции:

```
использовать пользователей
```

Чтобы просмотреть все данные в коллекции MongoDB, вы можете использовать команду find () ,
или команду find (). pretty (), чтобы просмотреть предварительно настроенную версию JSON.
документ:

```
db.collection_name.find (). довольно ()
```

Этот тип поиска может занять много времени, так как он расширяет содержимое
всей коллекции базы данных, которая может быть огромной. На данный момент это обычно

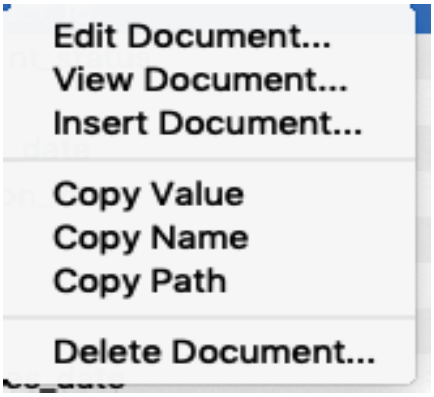


Рисунок 14.7

Лучше сбросить всю базу данных или выполнить поиск по данным с помощью графического интерфейса.
такой инструмент, как RobotMongo. Для сброса я разработал инструмент NoScrape, который
будет рассмотрено позже в этой главе.

Elasticsearch

Elasticsearch, пожалуй, самый популярный в мире продукт корпоративного уровня с открытым исходным кодом.
поисковый движок. Это невероятно быстро и так же просто. По сути, Elasticsearch
хранит данные в документах JSON. На основе бесплатного Apache с открытым исходным кодом
Библиотека программного обеспечения для поиска информации Lucene, построенная с поддержкой мультитенантности
имея в виду, Elasticsearch предлагает распределенную систему полнотекстового поиска, которая может быть
доступ через Интернет.
Elasticsearch использует JSON и Java API, чтобы сделать свои функции доступными для
тем, кто хочет интегрироваться с решением. Это идеальное хранилище данных NoSQL,
поскольку он поддерживает запросы Get в реальном времени .
Elasticsearch распределяет операции с индексами между шардами, которые, в свою очередь, могут иметь
собственные реплики. Распределенная архитектура делает Elasticsearch масштабируемым за счет
дизайн, позволяющий предоставлять возможности поиска в режиме, близком к реальному времени.
Что мне особенно нравится в Elasticsearch, так это то, насколько легко запрашивать данные.
Все можно выполнить с помощью простых команд curl .

Запрос Elasticsearch

Чтобы запросить Elasticsearch, просто введите **curl ip: port** . В следующем примере я
запросит локальную копию Elasticsearch:

```
> локальный локальный локальный объект: 9200
{
"имя": "узел1",
"имя_кластера": "myES",
"cluster_uuid": "UVc8iPj4TlqVdf-IacHcOw",
"версия": {
"number": "6.6.1",
"build_flavor": "по умолчанию",
"build_type": "об / мин",
"build_hash": "1fd8f69",
"build_date": "2019-02-13T17: 10: 04.160291Z",
"build_snapshot": ложь,
"lucene_version": "7.6.0",
"minimum_wire_compatibility_version": "5.6.0",
"minimum_index_compatibility_version": "5.0.0"
},
"слоган": "Знаешь, для поиска"
}
```

В результатах отобразится общая информация о версии Elasticsearch.
сервер, работающий на запрашиваемом IP-адресе. Теперь, когда мы знаем, что сервер активен,
давайте снова запросим его, чтобы показать список доступных индексов (баз данных):

```
curl -X GET "localhost: 9200 / _cat / index? v"
индекс состояния здоровья. uuid
pri rep docs.count docs.deleted store.size
зеленый открытый n203 i98ZmZQgSA 4 1 711314316 23 162,5 ГБ
желтый открытый n204 CVBXsWyIT 5 1 385781741 0 68 ГБ
зеленый открытый n205 HHrwpFHiQ7 4 1 211146503
0 264,8 ГБ
```

В этом списке мы видим три индекса: n203, n204 и n205, многие из которых содержат
несколько сотен миллионов записей (каждая хранится в документах JSON).
Поскольку имена индексов часто не видны, следующим шагом будет исследование
сопоставления внутри каждого индекса. Отображения аналогичны заголовкам таблиц. Они
предоставит структуру индекса и даст вам довольно хорошее представление о том, что
вы найдете внутри. Результатом этой команды будет чистый JSON, поэтому он может
помочь вставить данные в линтер JSON, чтобы отформатировать их для облегчения чтения (например,
www.jsonlint.com):

```
curl -X GET "localhost: 9200 / my-index / _mapping"
{"my-index": {"mappings": {"breach": {"dynamic": "false", "_ all": {"enabled"
: false}, "properties": {"address": {"type": "text"}, "dob": {"type": "keyword",
"ignore_above": 256, "normalizer": "lowercase_normalizer"}, "email": {"type":
"keyword", "ignore_above": 256, "normalizer": "lowercase_normalizer"}, "hash"
: {"type": "keyword", "ignore_above": 256}, "i": {"type": "keyword",
"ignore_above": 100}, "mobile": {"type": "text", "analyzer": "phone_number"},
"имя": {"тип": "текст", "поля": {"ключевое слово": {"тип": "ключевое слово",
"ignore_above": 256, "normalizer": "lowercase_normalizer"}}}, "password":
{"type": "keyword", "ignore_above": 256}}}}}
```

Вывод нелегко прочитать, поэтому давайте скопируем и вставим эти данные в jsonlint.
com (рисунок 14.8).

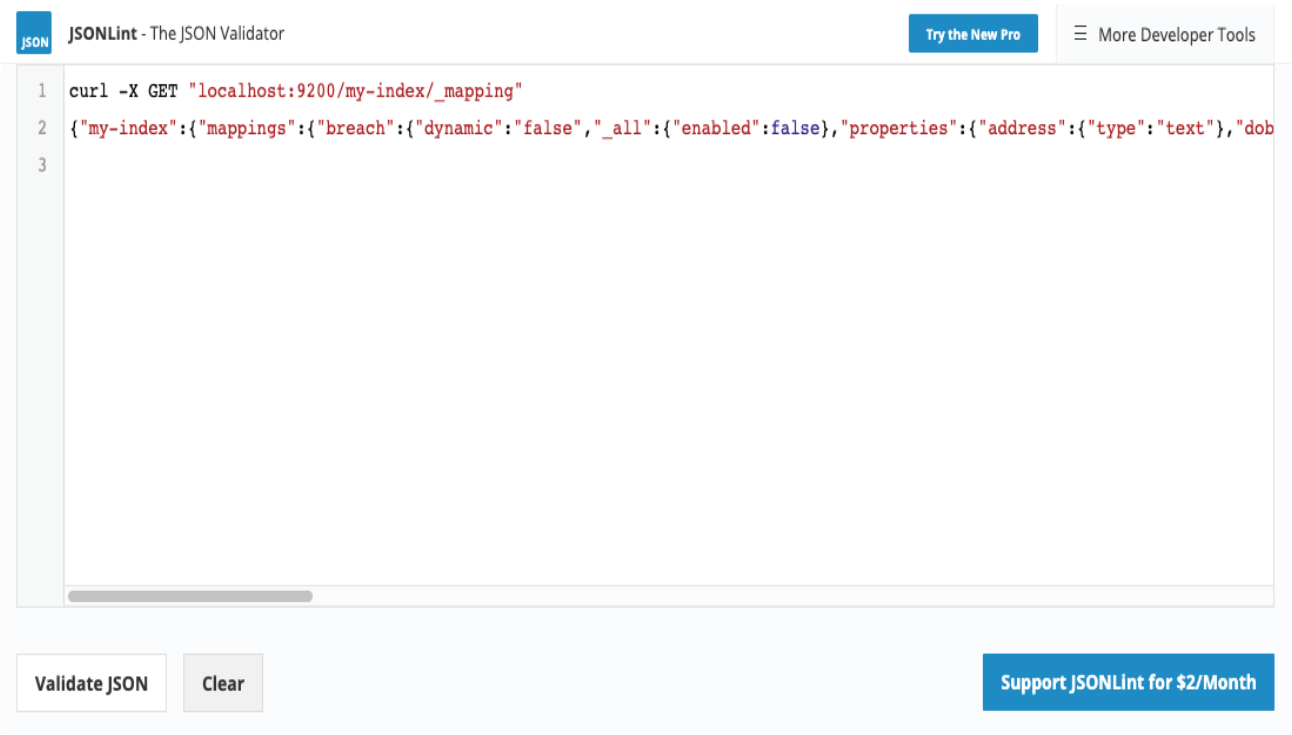


Рисунок 14.8

Как только мы это сделаем и нажмем Проверить JSON, мы получим следующий результат:


```
{
"my-index": {
"mappings": {
"нарушение": {
"динамический": "ложный",
"характеристики": {
"адрес": {
"тип": "текст"
},
"dob": {
"тип": "ключевое слово",
"ignore_above": 256,
},
"Эл. адрес": {
"тип": "ключевое слово",
"ignore_above": 256,
},
"hash": {
"тип": "ключевое слово",
"ignore_above": 256
},
"ip": {
"тип": "ключевое слово",
"ignore_above": 100
},
"mobile": {
"тип": "текст",
},
"имя": {
"тип": "текст",
},
"пароль": {
"тип": "ключевое слово",
"ignore_above": 256
},
"имя пользователя": {
"тип": "ключевое слово",
"ignore_above": 256,
"normalizer": "lowercase_normalizer"
}
}
}}
}
}
```


Глядя на сопоставления индексов, мы можем видеть имена полей, такие как имя пользователя , пароль. слово , имя , адрес и всякая другая полезная информация.

Это *точный* процесс, который я использовал для обнаружения и проверки информации о
Exactis, Verifications.io и Apollo.io. В каждом случае аутентификация не выполнялась.
требуется; потребовалось всего несколько простых команд curl .

. Отсутствие аутентификации, необходимой для Elasticsearch (и большинства других NoSQL баз данных) уступил место огромному всплеску выкупа баз данных. Если ты можешь получить доступ к базе данных Elasticsearch, и тогда у вас будут все возможности CRUD. Киберпреступность nals будут искать открытые базы данных Elasticsearch, скачивать все данные, удалять их из сервер, а затем замените его удобной запиской о выкупе. Я натыкаюсь на них довольно часто. Еще одна причина, по которой вы всегда должны не забывать размещать свои базы данных NoSQL за каким-то брандмауэром или списком контроля доступа.

Сброс данных Elasticsearch

Если вы найдете данные, которые кажутся полезными, вы, скорее всего, захотите загрузить копию
для экспертизы. Для этого требуется Elasticdump, а также NodeJS.
и NPM для установки.

После установки Elasticdump запустить команду так же просто, как и que-
рыбу базы данных. Единственная разница в том, что вам нужно указать ввод и
выходной файл и ограничение на передачу по запросу. Максимальное количество документов
вы можете экспортировать по запросу 10,000. Я бы посоветовал начать с этого числа
и если вы обнаружите, что сервер медленно обслуживает ваши запросы, попробуйте сбросить
ценность, пока вы не найдете то, что работает для вас. Следующая команда
начнет сбрасывать базу данных Elasticsearch с сервера 0.0.0.0:

```
> elasticdump --input = http: //0.0.0.0: 9200 / имя-индекса \\
--output = index-name.json –noRefresh --limit = 10000
стартовый дамп
получили 10000 объектов из источника elasticsearch (смещение: 0)
отправил 10000 объектов в целевой файл, написал 10000
получили 10000 объектов из источника elasticsearch (смещение: 10000)
отправил 10000 объектов в целевой файл, написал 10000
дамп завершен
```

Ваш вывод будет похож на этот код, и когда он будет завершен, у вас будет
файл JSON с содержимым запрошенного индекса.

Нет

NoScrape - это инструмент с открытым исходным кодом, предназначенный для облегчения процесса поиска и
парсинг наборов данных, доступных в открытых контейнерах для хранения и общедоступных
базы данных. Изначально разработанный мной и Уильямом Мартином, NoScrape сейчас

доступно для бесплатной загрузки со страницы Night Lion Security на Gitlab: https: // gitlab.com/nightlionsec/noscrape .

На момент написания этого раздела NoScrape поддерживает простой доступ и загрузка данных из MongoDB, корзин AWS, Elasticsearch и CassandraDB.

Мы разработали инструмент, потому что процесс выявления полезных данных в MongoDB и Elasticsearch были чрезвычайно громоздкими при работе с десятки тысяч активных хостов. Мы также добавили возможность поиска по Сегменты AWS S3 в чрезвычайно большом масштабе - все, что вам нужно, - это список слов.

NoScrape имеет множество параметров, которые можно указать в зависимости от выполняемую вами функцию.

Аргументы включают:

-d Тип базы данных
: Тип базы данных для очистки
[«монго», «s3», «es», «кассандра»]
-o файл вывода
: Файл для вывода результатов
-v
: Включить подробный вывод
--Примеры
: Распечатать примеры использования и выйти
Параметры Монго и Кассандры
-tf, --targetFile
: Список хостов в формате CSV (IP, порт)
-t, --target Цель: IP или CIDR базы данных
-p, --port Порт
: Порт базы данных
-s, --scrape
: Тип запуска: базовый, полный
-f, --filter FilterFile: файл, содержащий список ключевых слов.
соответствовать
-u, --username Имя пользователя: имя пользователя для стандартной аутентификации
-p, --password Пароль: пароль для стандартной аутентификации.
-a, --authDb AuthDB: база данных в Mongo для аутентификации
Параметры Elasticsearch
-tf, --targetFile
: Список хостов в формате CSV (IP, порт)
-t, --targets Цели: IP или CIDR баз данных
-p, --port Порт
: Порт базы данных
-s, --scrape
: Тип парсинга: сканирование, поиск, дамп,
свалка
-f, --filter FilterFile: файл, содержащий список
ключевые слова для соответствия
-l, --limit Предел
: Количество записей ES для сброса на
запрос (по умолчанию / максимум: 10000)
Параметры AWS Brute S3

--access AccessKey: ключ доступа AWS
--secret SecretKey: Секретный ключ AWS
--hitlist DictionaryFile: файл, содержащий список слов, которые можно попробовать

MongoDB

Начиная с MongoDB, запускаем NoScrape для получения данных с сервера MongoDB.
очень похож на инструменты командной строки MongoDB. Разница в том, что
многие из поисковых запросов автоматизированы для вас, поэтому вам не нужно сбрасывать
каждая коллекция и база данных индивидуально.
При очистке MongoDB NoScrape позволяет использовать два основных типа очистки: базовый и
полный. *Основной скрип* будет список всех баз данных и таблиц / коллекций в Tree-
формат списка. *Полный скрип* будет список всех баз данных, все таблицы / коллекций
в каждой базе данных и во всех полях в каждой коллекции.
Чтобы начать сканирование списка IP-адресов MongoDB, укажите тип базы данных mongo
с помощью параметра -d и список IP-адресов и портов в формате CSV с помощью параметра -tf
(целевой файл) параметр. Обязательно используйте параметр -o, а также укажите свой
выходной файл. Это то же самое, что и использование стандартного параметра Linux для отправки
весь вывод в файл:> outputfile .
Следующая команда запустит базовый дамп IP-адресов, расположенных в
файл mongolist.txt с базовым типом сканирования:

```
./noScrape.py -d mongo -s basic -tf mongolist.txt
```

Я не указывал выходной файл, поэтому могу видеть результат в реальном времени. Если ты
сканирование большого количества баз данных очень быстро заполнит ваш экранный буфер.
Просмотр сброшенных коллекций и таблиц MongoDB уже был
рассмотрены ранее в этой главе, так что мы можем пропустить это.

Выкупленный сервер MongoDB

Прежде чем мы перейдем к Elasticsearch, стоит упомянуть, что если вы используете
NoScrape для случайной очистки нескольких различных IP-адресов MongoDB,
есть большая вероятность, что ваш выходной файл также будет содержать ряд сообщений об ошибках.
мудрецы. Вот как будут выглядеть некоторые из наиболее распространенных сообщений об ошибках:

```
Прикреплено к 0.0.0.0:27017
{DB} hacked_by_unistellar
Коллекция} восстановить
```

Как упоминалось ранее, вы можете встретить базы данных NoSQL, которые
удалены и теперь выкупаются. Вот как это будет выглядеть в MongoDB.

Нет авторизации

Произошла непредвиденная ошибка при перечислении баз данных на
0.0.0.0:27017 - администратор не авторизован для выполнения
команда {listDatabases: 1, nameOnly: true}

Вы увидите это сообщение, если на сервере MongoDB настроена аутентификация.
Все больше и больше экземпляров MongoDB теперь имеют аутентификацию, что означает даже
если база данных обнаружена Shodan, вы не сможете получить к ней доступ без
надлежащие учетные данные.

Неверный IP-адрес / истекло время ожидания

Ошибка подключения к 0.0.0.0:27017 - время ожидания истекло

Довольно понятно. IP-адрес больше не активен или установлен брандмауэр.
вверх, чтобы предотвратить доступ.

Elasticsearch

NoScrape изначально разрабатывался как способ быстрого поиска и сброса больших
количество баз данных Elasticsearch. Все, что делает NoScrape, может так же
легко сделать вручную с помощью команд curl (как обсуждалось ранее в этом
глава). Разница, опять же, в том, что NoScrape помещает все в одну красивую
и аккуратный пакет для вас.

Подобно параметрам MongoDB, я лично указываю целевой файл CSV, который
содержит список IP-адресов и их портов. При запуске NoScrape обязательно установите
тип базы данных для es с помощью параметра -d .

Скребок Elasticsearch в NoScrape имеет четыре различных типа очистки, которые
можно указать с помощью параметра -s : сканирование, поиск, дамп и совпадение.
Посмотрим на них.

Сканировать

В параметре сканирования будут перечислены основные выходные данные каждого сервера Elasticsearch и
выводить содержимое индексов на экран (или в выходной файл). Это тоже самое
как запрос к серверу с помощью описанной ранее команды / _ cat / index? v :

[root @ osint]> python3 noscrape.py -d es -tf es-list.txt -s scan
---- Результаты: 0.0.0.0:9200
индекс состояния здоровья uuid pri rep docs.count docs.deleted store.size
желтый открытый nginx-dos-router-2019.04.29 1oE ... 5 1 3773305 0 1,5 ГБ
желтый открытый app-dos-web-2019.03.31 1Nq ... 5 1 2702331 0 892.12
желтый открытый nginx-dos-web-2019.05.01 3B0 ... 5 1 9851 0 2,9 МБ
желтый открытый nginx-dos-web-2019.04.04 EaA ... 5 1 10023 0 3 МБ

Это типичный вывод ES с одного сервера. Обратите внимание в начале
файл есть ---- Результаты: IP . Надеюсь, это упростит поиск и
очистите этот список позже.

Процесс, который вы, возможно, захотите использовать, - это поиск определенных ключевых слов и удаление
все остальное. Вы можете добиться этого с помощью параметра --filter . Я не ре-
не рекомендуется использовать эту опцию на данном этапе поиска, потому что вы
вы упустите много важных результатов, если будете смотреть только на имя индекса.

Поиск

Параметр поиска выполнит более глубокое погружение в данные Elasticsearch -
базовый вывод, просмотрев таблицу сопоставлений для каждого из индексов в
база данных. Это то же самое, что смотреть на заголовки таблицы. Использование этой опции
полезно, потому что чаще всего фактическое имя индекса будет скрыто или
не то, что когда-либо вызовет интерес. Однако файл сопоставлений будет
покажет вам, какой именно тип данных находится в каждой таблице.

Параметр dump будет использовать Elasticdump для дампа каждого индекса в
Айпи адрес. Используйте это с осторожностью, так как он загрузит все. Ты не делай
необходимо указать имя выходного файла, поскольку Elasticdump будет использовать имя файла
index как имя файла JSON.

Есть очень хороший шанс, что результат будет огромным, так что будьте
подготовлен к работе с очень большим файлом. Результат будет выглядеть так:

```
[root @ osint]> python3 noscrape.py -d es -tf es-list.txt -s search
{"тип": "ключевое слово"}, "часовой пояс": {"тип": "ключевое слово"}}}, "хост": {"тип":
"ключевое слово"}, "имя хоста": {"тип": "ключевое слово"}, "jsessionid": {"тип":
"keyword"}, "level": {"type": "keyword"}, "logger_name": {"type":
"keyword"}, "message": {"type": "text"}, "messageId": {"type": "keyword"},
"requestUri": {"type": "keyword"}, "requestedSessionId": {"type":
"ключевое слово"}, "запрошенныйSessionIdFromCookie": {"тип": "ключевое слово"},
"requiredSessionIdValid": {"type": "keyword"}, "service": {"type":
"keyword"}, "sessionId": {"type": "keyword"}, "stack_trace": {"type":
"text"}, "subscriptionId": {"type": "long"}, "system": {"type": "keyword"},
"теги": {"тип": "ключевое слово"}, "имя_потока": {"тип": "ключевое слово"}, "тип":
{"type": "keyword"}, "user": {"type": "keyword"}, "userId": {"type":
"keyword"}, "userIp": {"type": "keyword"}, "useragent": {"dynamic":
"true", "properties": {"build": {"type": "keyword"}, "device": {"type":
"ключевое слово"}, "основное": {"тип": "ключевое слово"}, "второстепенное": {"тип": "ключевое слово"},
"name": {"type": "keyword"}, "os": {"type": "keyword"}, "os_major": {"type":
"keyword"}, "os_minor": {"type": "keyword"}, "os_name": {"type":
"keyword"}, "patch": {"type": "keyword"}}}}, "x-forwarded-for":
{"type": "text"}, "x-forwarded-host": {"type": "keyword"},
"x-forwarded-port": {"type": "keyword"}, "x-forwarded-proto":
{"type": "keyword"}, "x-forwarded-server": {"type": "keyword"},
```

"x-prerender-token": {"type": "keyword"}, "x-real-ip": {"type":
"keyword"}, "x-request-id": {"type": "keyword"}}}, "ERROR": {"_ all":
{"enabled": false}, "dynamic_templates": [{"message_field": {"match":
"сообщение", "match_mapping_type": "строка", "сопоставление": {"индекс": "проанализировано",
"type": "string"}}}, {"string_fields": {"match": "*", "match_mapping_type":
"строка", "сопоставление": {"индекс": "не_анализ", "тип": "строка"}}}],
"properties": {"@ timestamp": {"type": "date"}, "_ ga_cid": {"type": "keyword"},
"_mxpnl_cd": {"тип": "ключевое слово"}, "_ mxpnl_cm": {"тип": "ключевое слово"},
"_mxpnl_cw": {"type": "keyword"}, "accept": {"type": "keyword"},
"accept-encoding": {"type": "keyword"}, "accept-language": {"type":
"ключевое слово"}, "агент": {"тип": "ключевое слово"}, "имя_приложения": {"тип":
"ключевое слово"}, "версия_приложения": {"тип": "ключевое слово"}, "cf-connected-ip":
{"type": "keyword"}, "cf-ipcountry": {"type": "keyword"}, "cf-ray": {"type":
"keyword"}, "cf-visitor": {"type": "keyword"}, "clientip": {"type":
"ключевое слово"}, "соединение": {"тип": "ключевое слово"}, "dos_ga_clientid": {"тип":
"ключевое слово"}, "dos_mixpanel_clientid": {"тип": "ключевое слово"}, "среда":
{"type": "keyword"}, "geoip": {"dynamic": "true", "properties": {"area_code":
{"type": "long"}, "city_name": {"type": "text"}, "continent_code": {"type":
"keyword"}, "координаты": {"type": "double"}, "country_code2": {"type":
"keyword"}, "country_code3": {"type": "keyword"}, "country_name": {"type":
"keyword"}, "dma_code": {"type": "long"}, "ip": {"type": "keyword"},
"latitude": {"type": "float"}, "location": {"type": "geo_point"},
"longitude": {"type": "float"}, "postal_code": {"type": "keyword"},
"real_region_name": {"type": "keyword"}, "region_code": {"type": "keyword"},
"имя_региона": {"тип": "ключевое слово"}, "часовой пояс": {"тип": "ключевое слово"}}},
"хост": {"тип": "ключевое слово"}, "имя хоста": {"тип": "ключевое слово"}, "jsessionid":
{"type": "keyword"}, "level": {"type": "keyword"}, "logger_name": {"type":
"keyword"}, "message": {"type": "text"}, "planId": {"type": "keyword"},
"requestUri": {"type": "keyword"}, "requiredSessionId": {"type": "keyword"},
"requiredSessionIdFromCookie": {"type": "keyword"},
"requiredSessionIdValid": {"type": "keyword"}, "service": {"type":
"keyword"}, "sessionId": {"type": "keyword"}, "stack_trace": {"type":
"текст"}, "подписка": {"тип": "ключевое слово"}, "система": {"тип": "ключевое слово"},
"теги": {"тип": "ключевое слово"}, "имя_потока": {"тип": "ключевое слово"}, "тип":
{"type": "keyword"}, "user": {"type": "keyword"}, "userId": {"type":
"keyword"}, "useragent": {"dynamic": "true", "properties": {"build":
{"тип": "ключевое слово"}, "устройство": {"тип": "ключевое слово"}, "основное": {"тип":
"ключевое слово"}, "второстепенное": {"тип": "ключевое слово"}, "имя": {"тип": "ключевое слово"}, "ОС":
{"type": "keyword"}, "os_major": {"type": "keyword"}, "os_minor": {"type":
"keyword"}, "os_name": {"type": "keyword"}, "patch": {"type": "keyword"}}},
"x-forwarded-for": {"type": "text"}, "x-forwarded-host": {"type": "keyword"},
"x-forwarded-port": {"type": "keyword"}, "x-forwarded-proto": {"type":
"ключевое слово"}, "x-forwarded-server": {"тип": "ключевое слово"}, "x-prerender-token":
{"type": "keyword"}, "x-real-ip": {"type": "keyword"},
"x-request-id": {"type": "keyword"}}}, "...

Это огромный беспорядок, но если вы присмотритесь к результатам, вы заметите что-то действительно интересное. Заголовки включают такие ключевые слова, как ip , широта , geoip , areacode и идентификатор пользователя .

**Я совершенно честен, когда говорю, что просто вытащил этот IP наугад.
и понятия не имел, что там было. Это выглядит действительно интересно и того стоит.
исследуя. Видишь, как это весело?**

Поскольку результатов так много, это было бы хорошим этапом для использования
- параметр фильтра . Использование фильтра позволяет указать файл ключевых слов
чтобы соответствовать результатам. Вывод будет отображаться только в том случае, если один или несколько ваших
ключевые слова соответствуют результатам поиска.

В этом случае предыдущий вывод будет содержать совпадения для нескольких ключевых слов,
так что результат будет точно таким же. Как только вы загрузите данные,
это обычно ручной процесс просмотра результатов, или вы можете пропустить это
шаг и сразу переходите к выгрузке всех данных.

Свалка

Команда dump просто сбрасывает все данные с каждого выбранного вами IP-адреса. если ты
просто хотите всего и не заботитесь о том, что вы скачиваете, это
вариант для вас.

Максимальное (и по умолчанию) количество записей, которые можно сбросить с помощью
каждый запрос Elasticdump - 10 000. Если вы столкнетесь с медленными серверами, вы можете попробовать
понизив это значение с помощью параметра -l (limit).

Команда dump автоматически создаст папку для каждого IP-адреса.
сбрасываются. Все загруженные данные будут храниться в этой папке. Следующие-
Команда ing запустит NoScrape для любого IP-адреса, указанного в es-test.
txt и автоматически загружает все базы данных независимо от содержимого:

```
./noScrape.py -d es -tf es-test.txt -s дамп
```

Если команда успешно подключилась к целевому IP-адресу, вывод будет
выглядят так:

```
ПОЛУЧИТЬ http://0.0.0.0:9200/* [статус: запрос 200: 0,116 с]
Выгрузка в файл для ip 0.0.0.0:9200 и индекса nginx ... 2019.01.29
http://0.0.0.0:9200/* [статус: запрос 200: 0,116 с]
Выгрузка в файл для ip 0.0.0.0:9200 и индекса nginx ... 2019.02.29
ПОЛУЧИТЬ http://0.0.0.0:9200/* [статус: запрос 200: 0,116 с]
Выгрузка в файл для ip 0.0.0.0:9200 и индекса nginx ... 2019.03.29
```

Ваш результат будет находиться в папке (0.0.0.0:9200) и будет представлять собой список
Файлы JSON, загруженные с каждого сервера.

MatchDump

Параметр matchdump представляет собой комбинацию всего предыдущего сканирования и очистки.
методы. Вместо того, чтобы использовать полностью широкий подход, просто скачивая

все и придется вручную пройти через все это позже, matchdump пытается
упростите этот процесс, выбрасывая только те базы данных, которые соответствуют определенным критериям.
Процесс выполняет несколько поисков в базе данных Elasticsearch,
начиная с комбинации функций «поиск» и «фильтр». В течение
На первом этапе процесса NoScrape получит все данные сопоставлений для
Индексы Elasticsearch и сравните их со списком ключевых слов фильтра. С использованием
эта опция требует, чтобы вы указали параметр --filter .
После сопоставления ключевых слов следующим шагом NoScrape будет использование дампа.
параметр и загрузите все соответствующие базы данных.
Выполнение полной команды выглядит примерно так:

```
./noscrape.py -d es -tf list.txt -s matchdump --filter keywords.txt
```

Когда мы выполняем эту команду, вывод должен выглядеть точно так же, как результаты
из предыдущего примера дампа . В данном случае выбранный мной случайный сервер ES
случайно попал во многие ключевые слова, которые я обычно использую, включая имя пользователя, IP,
geoIP, адрес и т. д.
После того, как эти ключевые слова совпадают, matchdump опция говорит NoScrape к
также дамп всей базы данных. Файлы будут храниться в папке в соответствии с
IP-адрес сервера.
При создании списка поиска для поиска интересных полей данных я рекомендую
следующие ключевые слова в качестве хорошей отправной точки:

- Пароль
- Имя пользователя
- Электронная почта (это также будет соответствовать email_address и любому варианту)
- GeoIP
- IP
- FacebookID
- LinkedIN
- Instagram
- Хеш
- Соль
- Телефон, мобильный, сотовый

Кассандра

Cassandra от Apache - еще один популярный тип базы данных NoSQL, который очень прост.
Аналогично MongoDB. Из-за сходства типов баз данных Cassandra
параметры NoScrape точно такие же, как у MongoDB. Единственная разница в
использование приложения заключается в том, что для запуска сканирования или очистки базы данных Cassandra
требуется
вам нужно изменить параметр -d на Cassandra .

Следующая команда запустит базовое сканирование списка IP-адресов CassandraDB:

```
./noScrape.py -d кассандра -s базовый -tf кассандра-список.txt
```

Успешный запуск будет очень похож на MongoDB:

```
[2019-05-12 08:02:15] Новый хост Cassandra <Host: 0.0.0.0 datacenter1>
обнаруженный
[2019-05-12 08:02:19] {Keyspace} weather_geohash_ks
[2019-05-12 08:02:19] {Таблица} GRIB2_Data
[2019-05-12 08:02:19] {Таблица} GRIB2_PIC
[2019-05-12 08:02:19] {Таблица} GRIB2_Status
[2019-05-12 08:02:19] {Таблица} GRIB2_Status_HTSGW
[2019-05-12 08:02:20] Не удалось создать пул соединений для нового хоста.
172.17.137.165:
OSError: [Errno None] Попытка подключиться к [('0.0.0.0', 9042)].
Последняя ошибка: истекло время ожидания
[2019-05-12 08:02:20] Использование центра обработки данных "DC1" для DCAwareRoundRobinPolicy
(через хост '0.0.0.0'); если неверно, укажите local_dc в
конструктор или ограничьте точки контакта локальными узлами кластера
[2019-05-12 08:02:21] {Keyspace} twitter
[2019-05-12 08:02:21] Пользователь {Table}
[2019-05-12 08:02:21] {Keyspace} elastic_admin
[2019-05-12 08:02:21] метаданные {Table}
[2019-05-12 08:02:21] {Keyspace} dbtest2
[2019-05-12 08:02:21] Выпускник {Table}
[2019-05-12 08:02:21] Выпускники {Table}
[2019-05-12 08:02:21] {Стол} амбуланция
[2019-05-12 08:02:21] Область {Таблица}
[2019-05-12 08:02:21] {Таблица} асегурадора
[2019-05-12 08:02:21] {Таблица} asistencias
[2019-05-12 08:02:21] {Table} auntentificacion
[2019-05-12 08:02:21] {Стол} авто
[2019-05-12 08:02:21] {Таблица} cajas
[2019-05-12 08:02:21] {Стол} cama
[2019-05-12 08:02:21] {Таблица} категория
[2019-05-12 08:02:21] {Таблица} центрокоста
[2019-05-12 08:02:21] {Таблица} citas
[2019-05-12 08:02:21] {Стол} клиентка
[2019-05-12 08:02:21] {Таблица} consultorio
[2019-05-12 08:02:21] {Table} Удобство
[2019-05-12 08:02:21] {Таблица} оценка критерия
[2019-05-12 08:02:21] {Table} curso
[2019-05-12 08:02:21] {Таблица} cursoprogramado
[2019-05-12 08:02:21] {Таблица} диагностика
[2019-05-12 08:02:21] {Таблица} диета
[2019-05-12 08:02:21] {Table} docente
```

Оттуда вы можете выбрать более подробный тип очистки, чтобы увидеть
сбор данных, или просто выгрузите все, используя параметр -d .

Amazon S3

NoScrape также поддерживает сканирование корзин Amazon S3. Главное отличие
между NoScrape и CloudStorageFinder (обсуждалось ранее в этой главе)
возможность указать аутентификацию для AWS.
Использование собственной аутентификации S3 может оказаться простым способом поиска корзин.
с неверно настроенными параметрами аутентификации.

Использование ваших собственных учетных данных S3

Несколько месяцев назад один репортер написал историю о том, как я связался с
его относительно разоблачения ведра S3 All American Entertainment. AAE
оказывается главным спикером этого репортера, поэтому утечка включала его
выступая вместе со многими другими известными знаменитостями и общественными деятелями,
в том числе Дуэйн «Скала» Джонсон, Гвинет Пэлтроу, Хиллари Клинтон,
Колин Пауэлл и многие другие.
Репортер был достаточно встревожен этим открытием, чтобы включить подробности
в его рассказе. Однако после публикации истории я пришел к выводу, что
что репортер был обеспокоен мной больше, чем фактическое открытие.
Тем не менее, «неправильная конфигурация» AAE была несколько сложной (в самом
по крайней мере, сбивает с толку) и не был бы легко пойман во время настройки кем-то
кто не имел глубоких знаний о слишком запутанной афере Amazon.
Настройки конфигурации.
Я говорю о том, что определенные сегменты S3, требующие аутентификации, могут
можно получить доступ с помощью *любой* аутентификации, включая ваши собственные ключи доступа S3.
Другими словами, *я смог обнаружить утечку AAE, получив доступ к частной
ведро, используя мои собственные учетные данные* .
Вот почему NoScrape был разработан с возможностью выполнять широкомасштабные
Обнаружение корзины S3 с использованием любых учетных данных.
Следующая команда выполнит сканирование корзин S3 с использованием определенного
Ключ доступа к Amazon и секретный ключ:

```
[root @ osint]> python3 noScrape.py -d s3 --access AccessKey \\
--secret SecretKey -tf wordlist.txt
```

Если сегмент существует, но ключ AWS недействителен (или не авторизован), вы
увидеть следующую ошибку:

```
[S3_NoAccess] 's3: // acciones' существует, но у нас нет доступа
[S3_NoAccess] 's3: // actividad' существует, но у нас нет доступа
[S3_NoAccess] 's3: // vinnytroia' существует, но у нас нет доступа
```

С другой стороны, если ключ был успешным (или если вы просто сканируете
открытые корзины без аутентификации), вы увидите сообщение, подобное
следующий:

```
Идентифицирован доступ к 's3: // vinnytroia-test' -
Список всех объектов / файлов ...
- OSINT-книга-test.txt
Модуль S3 завершен
```

Глядя на результаты, мы видим, что одна из корзин в нашем списке, vinny-
troia-test находится в открытом доступе. Это ведро, которое я создал для этого примера.
Один из перечисленных файлов - OSINT-book-test.txt . Если бы это был настоящий ковш S3, там
вероятно, будет больше файлов в списке.

NoScrape не настроен для загрузки файлов корзины (пока), но эта функция
Надеюсь, будет завершена к моменту публикации этой книги. В это время,
отправка всего вывода в файл позволит вам быстро идентифицировать и нацеливать сегменты
с активными объявлениями.

Резюме

В этой главе содержится много информации о том, как найти общедоступные данные.
наборы. Он предоставил информацию о поиске через общедоступное облачное хранилище
такие разработчики, как Amazon S3 и Digital Ocean, знакомство с базой данных NoSQL
такие типы, как MongoDB и Elasticsearch, а также команды для ручного запроса и
скачивать файлы из этих баз данных. Инструмент NoScrape обеспечивает автоматизацию
сложных и утомительных задач, таких как поиск, очистка и выгрузка данных из
несколько разных типов баз данных NoSQL, включая MongoDB, Elasticsearch,
и CassandraDB.

Теперь, когда мы определили способы поиска данных на общедоступных серверах,
следующий раздел этой книги будет посвящен охоте на людей и различных инструментах.
мы можем использовать для поиска информации о человеческих целях!

IV

Охота на людей

В этой части

Глава 15: Исследование людей, изображений и мест
Глава 16: Поиск в социальных сетях
Глава 17: Отслеживание профиля и подсказки для сброса пароля
Глава 18: Пароли, дампы и Data Viper
Глава 19: Взаимодействие с исполнителями угроз
Глава 20: Преодоление дезинформации взлома на 10 миллионов долларов
Этот раздел посвящен искусству исследования людей. Следующие несколько глав
охватит широкий спектр технологий и приемов, начиная от простых
Исследования в социальных сетях для использования информации, содержащейся в взломанных базах данных.
В этом разделе я также расскажу о построении «матрицы отслеживания», которая
поможет организовать вашу информацию и, если все будет сделано правильно, также поможет
вы организуете свое исследование таким образом, чтобы быстрее визуально находить подсказки.
Что может быть лучше для начала этого раздела, чем совет от «Человека-хакера»?

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

При проведении расследования или теста на проникновение действительно не существует единого стандарта. универсальная модель для инструментов и методов расследования, которая будет работать каждый раз. Это реально зависит от целевой цели. Это целевой фишинг или общий фишинг? Мы OSINT - целая компания или только человек? Или мы пытаемся получить оболочку, а не просто щелчок?

Есть так много возможностей. Если мы пытаемся получить оболочку, скажем, это может быть многоэтапная атака для нас, когда дело касается OSINT. Мы уделяем время исследованиям и найдите что-нибудь, где им имеет смысл вводить учетные данные. Мы ищем что-то в их профилях и социальных сетях, что позволяет нам подавать предлог орган, который законно запрашивал бы учетные данные. Затем, как только мы получим учетную запись - tials, мы можем продолжить под каким бы то ни было предлогом документ, который загружен с какой-то вредоносной программой, которая даст нам оболочку.

Если же мы просто щелкнем мышкой, иногда компании просто хотят, чтобы мы они восприимчивы к щелчку. В этом случае мы будем искать самый важный эмоциональный триггер. что мы можем найти, например, благотворительные организации, хобби, детские мероприятия и тому подобное.

Если это корпоративный OSINT, то это больше, чем просто попытка выяснить, как они используют социальные сети, потому что все так делают. С корпоративным OSINT мы просматриваем Flickr и Instagram и их корпоративная страница в Facebook, чтобы узнать, делают ли они такие вещи, как корпоративная рождественская вечеринка или пикник в конце года или что-то еще, и все люди имеют свои значки. Или, например, если у них был большой анонс или новый продукт uct, и компания устроила большую вечеринку, на которой люди фотографируются и они все еще носят свои значки.

Затем мы можем искать сотрудников, которых, возможно, только что наняли, и они рады и это что-то вроде: «Смотри, мама, мой новый стол», и на нем есть фотография включенного ноутбука. с поднятым рабочим столом, значком, телефоном и всем, что у них есть за их столом.

Они не понимают, чем они делятся на этих фотографиях.

325

15

Наконец-то мы подошли к моей любимой части расследования: изучению
люди. Я не знаю, что это, но есть что-то невероятно приятное
о том, чтобы наконец узнать, кто ваши цели, за всеми слоями псевдонимов и
изменить эго. Как только вы найдете эту волшебную нить улик, которую нужно распутать,
это как будто для тебя открывается новый мир. Время начинает замедляться и вдруг
все становится ясно. Это похоже на то, что вы попали в пулю из *«Матрицы»* . Его
невероятный.

Каждый раз, когда вы пытаетесь настроить таргетинг на отдельных лиц в организации, вы должны иметь
cess для определения наиболее вероятных целей для взаимодействия, с которыми нужно будет щелкнуть ссылку
или доверяйте тому, что вы им отправляете.
Я обучаю всех своих тестировщиков и всех, кто проходит мой курс SANS:
всегда ищите яркие блестящие предметы. Итак, представьте, что у вас есть организация,
насчитывает 4000 человек; наиболее интересными для меня людьми являются индивиды.
видео, которые наиболее активно работают в социальных сетях.
Это люди, которых очень много в Твиттере, они
люди, которые постоянно фотографируют свою еду и публикуют ее в Интернете. Они
люди, которые имеют свое мнение и настаивают на том, чтобы эти мнения присутствовали где-нибудь
В интернете. Когда вы создаете предлог для социальной инженерии человека, он

Исследование людей, изображений и Локации

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

действительно интересно, потому что вы можете использовать всю эту информацию, чтобы очень быстро получить человек, которому можно доверять.

Обычно вам нужно всего три точки контакта, которые связаны с доверием.

чтобы они начали полностью доверять вам, потому что люди обычно могут только

поддерживать около 150 межличностных отношений, о которых вы действительно можете заботиться одновременно время. Кроме того, это не имеет значения.

Например, если кто-то слышит о пароме, идущем по Средиземному морю.

и 400 человек умирают ужасной смертью, ты такой: «О, это отстой». Но на самом деле это не так имеет значение для них, и они могут легко продолжить свою жизнь. А если ваша собака получит сбитый машиной, ты неделями безутешен. Ваш мозг может иметь только способность обрабатывать так много социальных взаимодействий одновременно.

Для этого у нас на самом деле есть ярлыки, которые мы можем использовать, чтобы быстро улучшить наши- себя во время помолвки. Одна из самых простых вещей, которую нужно сделать, если я хочу, чтобы ты согласен со мной в том, что я обозначу ваши религиозные или политические предпочтения, а затем я может отразить это обратно к вам.

Я отражаю *вас* обратно к вам, и цель заполнит все остальное

этого соломенного человека. Как только вы получите примерно три точки отражения, они начнут думая: «Ну, этот человек думает так же, как я, и я хороший человек, поэтому этот человек должен быть хорошим человеком. Я заслуживаю доверия, и этот человек тоже должен быть заслуживающим доверия ». Это становится очень легко заставить их нажимать на ссылки, переходить на веб-страницы или взаимодействовать с вы на гораздо более доверительном уровне, чем просто сказали: «Эй, вот скидка 50 процентов на обувь в какой-то универмаг. "

Я имею в виду, что это требует немного усилий, но делает вас более целевым. Итак, вы пытаетесь- чтобы определить пользователей, которые с наибольшей вероятностью попадут в эти ловушки, а те наиболее активны в социальных сетях - это те, которые, как правило, соблазнительные цели, потому что у них есть эта глубокая потребность, и вы собираетесь их накормить необходимость. Эта потребность очень проста: они просто хотят, чтобы их видели и узнавали. Если ты можешь увидеть и узнать их и отразить их достоинства или сигнал добродетели, как отражение

Если вы подадите этим людям сигнал добродетели, они будут доверять *всему, что* вы говорите или делаете.

PIPL

Я *люблю* PIPL (www.pipl.com). PIPL (произносится как «люди»), возможно, является мировым крупнейшая поисковая система, связанная с людьми (по данным ее собственного веб-сайта). Я не знаю правда ли это на самом деле, но обслуживание потрясающее, и обычно моя первая остановка, когда я пытаюсь найти дополнительную информацию о человеке.

PIPL позволяет выполнять поиск по адресу электронной почты, имени пользователя в социальной сети и / или телефону. количество. Он также содержит обширную информацию о социальных сетях, связанных с людьми. медиа-информация, имена пользователей и альтернативные адреса электронной почты.

Я чувствую, что вырос в Интернете. Я пошел в колледж, и Facebook стал чем-то вроде
пока я был там, так что я как бы вырос рядом с некоторыми из этих платформ.
Социальные сети для меня часто кажутся низко висящими фруктами, поэтому я обычно начинаю
расследование есть. . . потому что почему бы и нет?
Я очень наглядный человек. Я думаю, что в фотографиях много силы, и я уверен, что
вы признаете, представленная информация может быть не совсем той, которую делится
эта информация думает, что это так. Например, вы можете внезапно увидеть розетку в
фон фотографии, и вы знаете нацию, в которой находится человек.
Возможно, они не об этом думали. . . Итак, я начну с
низко висящий плод разведки сайтов социальных сетей. Мне нравится делать общий аудит любого
потенциальные адреса электронной почты, которые я могу найти, любые имена пользователей, которые я могу найти, и все, что
они могут работать в сети. А затем, в зависимости от того, насколько надежны все эти
точки данных, я также попытаюсь проконсультироваться с тем, что Ник Фурно называл их «цифровыми
тень."
Но давайте возьмем мою маму в качестве примера. У нее уникальная фамилия, поэтому, если бы я был
собираюсь попробовать OSINT ее (или себя), я сначала посмотрю, какие результаты PIPL
есть, что, честно говоря, игрушка, которую я люблю.
Я не знаю, собирал ли PIPL данные из Facebook перед тем, как закрыть часть своего
параметры поиска, но если вы ищете номер телефона в PIPL, и он связан с
профиль Facebook, он покажет вам этот профиль Facebook, даже если Facebook будет
больше не делай этого за тебя. И, если вы выполните поиск по номеру телефона в PIPL, есть хороший
Вероятно, вы найдете основную информацию профиля пользователя, даже если этот профиль был ранее
удалено из социальных сетей.
Мне также нравится использовать PIPL с Maltego - введите несколько запросов, и вы получите
назад целый список телефонных номеров и аккаунтов.
Но есть так много ложных срабатываний; вам действительно все еще нужно делать свой собственный дом -
работают, и убедитесь, что эти профили реальны или даже действительны. Так что я очень люблю
Maltego в качестве начального инструмента для первоначального открытия.
Я думаю, что очень многие люди хотят, чтобы это был конец всем и всем.
ответ, и это просто нет - никогда не бывает. Вы всегда должны прилагать усилия в одну сторону
или другой.

Поиск людей

PIPL невероятно прост в использовании, а его API не очень дорого стоит.
обеспечивает. Для тех, кто использует Maltego, API PIPL встроен в несколько ключевых социальных сетей.
плагины для исследования СМИ. Для тех, кто не использует Maltego, веб-сайт чрезвычайно
простой. На рисунке 15.1 показана основная страница поиска PIPL.

Чтобы начать наш поиск, давайте использовать меня в качестве цели. До сих пор я никогда не искал себя в PIPL, так что интересно посмотреть на результаты.

В моей прошлой жизни я основал и руководил компанией Curvve Recordings, лейбл звукозаписи электронной танцевальной музыки (www.curvverecordings.com **). Я также произвел музыку и гастролировал в качестве ди-джея. Если вы все же решите искать меня, многие из результатов вы может найти, имеют отношение к музыке.**

На рисунке 15.2 показаны результаты использования «Vinny Troia» в поиске PIPL.

Результаты интересны - не совсем точные, но довольно приличный отчет.

моих онлайн-персон. Во-первых, я не живу в Вашингтоне, округ Колумбия. Фейсбук

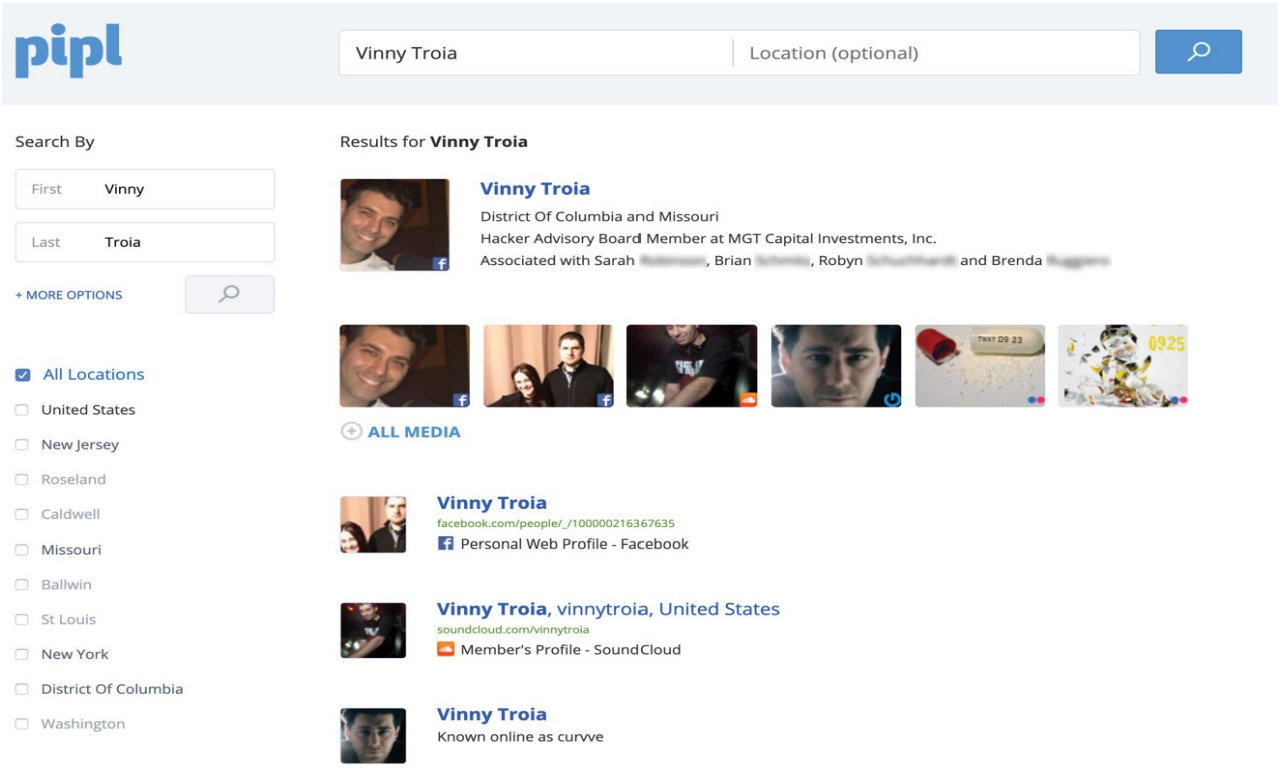


Рисунок 15.2

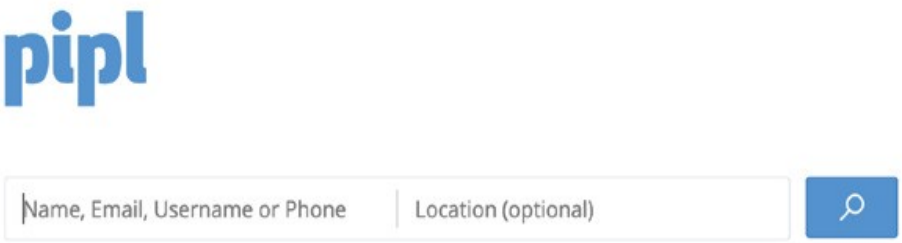


Рисунок 15.1

открывшаяся страница тоже не моя, но страница SoundCloud принадлежит
меня. Остальные результаты (которые были отсечены) относятся к музыкальным произведениям.
Я считаю, что раздел «Связанные с» (три строки под моим именем) наиболее
интересные данные на этой странице. Не потому, что он слишком точен, а потому, что
насколько это случайно. Первый человек, которого я знаю, очень слабо. Второй человек
кто-то, чей номер есть в моем мобильном телефоне, но мы не разговаривали много лет. В
третий человек, о котором я никогда не слышал, а четвертый человек - это тот, к кому я ходил
со средней школой, но я не разговаривал об этом долго.
Это, наверное, самая случайная группа «товарищей», которую я когда-либо видел,
потому что, хотя я знаю большинство из этих людей, я не могу сказать, что я действительно общаюсь
ел с любым из них.
Хотя эти результаты могут показаться не лучшим примером того, насколько
данные хранятся в базе данных PIPL, это должно дать вам представление о *mune* из
результаты, которые может предоставить PIPL. Это также отличный пример, показывающий, что данные
представление (какой-либо службой) может быть не совсем точным, поэтому
все должно быть проверено.
Я бы также никогда ничего не сбрасывал со счетов. Вы были бы удивлены, насколько часто
это найти страницу SoundCloud злоумышленника с помощью значка профиля (или имени пользователя)
который имеет сходство с учетной записью или профилем на другом веб-сайте.
Чтобы проиллюстрировать аналогичную мысль, давайте вернемся к поиску наших злоумышленников. я
помню, однажды я решил попытать счастья и поискать «TheDarkOverlord»
в PIPL. На рисунке 15.3 показаны результаты.
К моему большому удивлению, совпадение было! Бедный Крейг. Интересно сколько
звонки, которые он получил в результате этой информации?
Полное раскрытие информации - насколько мне известно, TheDarkOverlord - это *не* Крейг. Но я нахожу это
действительно интересно, что Крейг даже ассоциируется с этим именем. Щелкнув
ссылка на рис. 15.4 показывает нам, почему.
Очевидно, у Крейга в какой-то момент были личные страницы eBay и Netlog под
имя «TheDarkOverlord». Ни одной страницы больше нет, но они есть в PIPL.
кешируется и хранится. Хотя эта информация на самом деле нам не помогла, когда
вы думаете о том, что только что произошло, это действительно мощно.

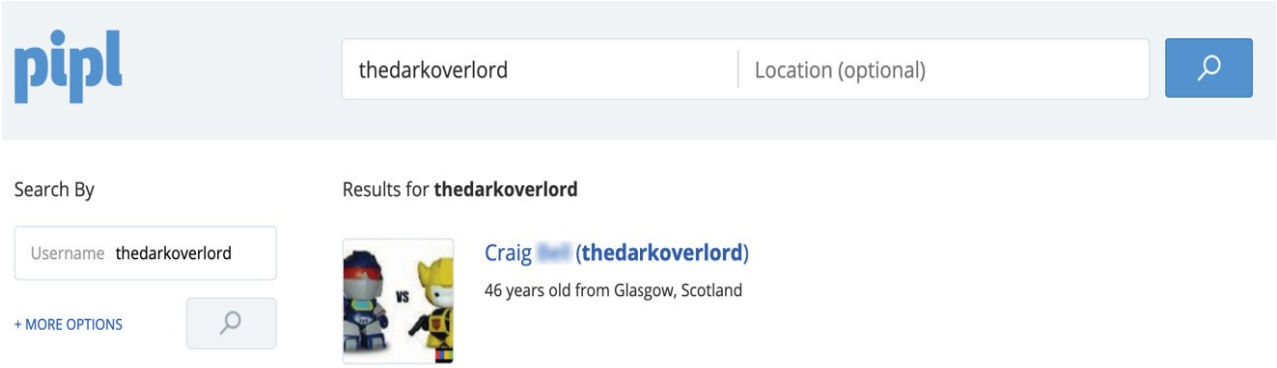


Рисунок 15.3

PIPL в какой-то момент кэшировал эти страницы и связал этого человека с TheDark-
Overlord на основе его имени пользователя. Хотя эти страницы больше не существуют, мы
могу видеть, что они существовали *когда-то* .
Доступ к историческим данным может быть (и часто является) наиболее важной частью исследования.
tigation - таким образом, имея доступ к такой информации, буквально за гроши за
результат поиска невероятен. Хотя это оказалось несущественным, есть
велика вероятность, что в будущем у PIPL будут и другие более полезные совпадения.

PIPL недавно изменил свой пользовательский интерфейс, добавив множество новых опций и Особенности. Новые изменения были добавлены после того, как большая часть содержания этой книги была написана. десять, так что я мог только проскользнуть в эту дополнительную записку.
При этом новые возможности расширенного поиска довольно значительны, теперь они позволяют: чтобы вы могли фильтровать и сводить результаты поиска, чтобы включать номера телефонов, имена пользователей, адреса, ассоциированные имена, образование, работа и возраст.

Публичные записи и проверка биографических данных

Сотни веб-сайтов позволяют проверять личные данные людей. если ты
вам нужна обычная проверка данных, я рекомендую эти
два сайта:

- FreeBackgroundCheck.org
- SkipEase.com (который выполняет поиск в BeenVerified, WhitePages и PeopleLooker)

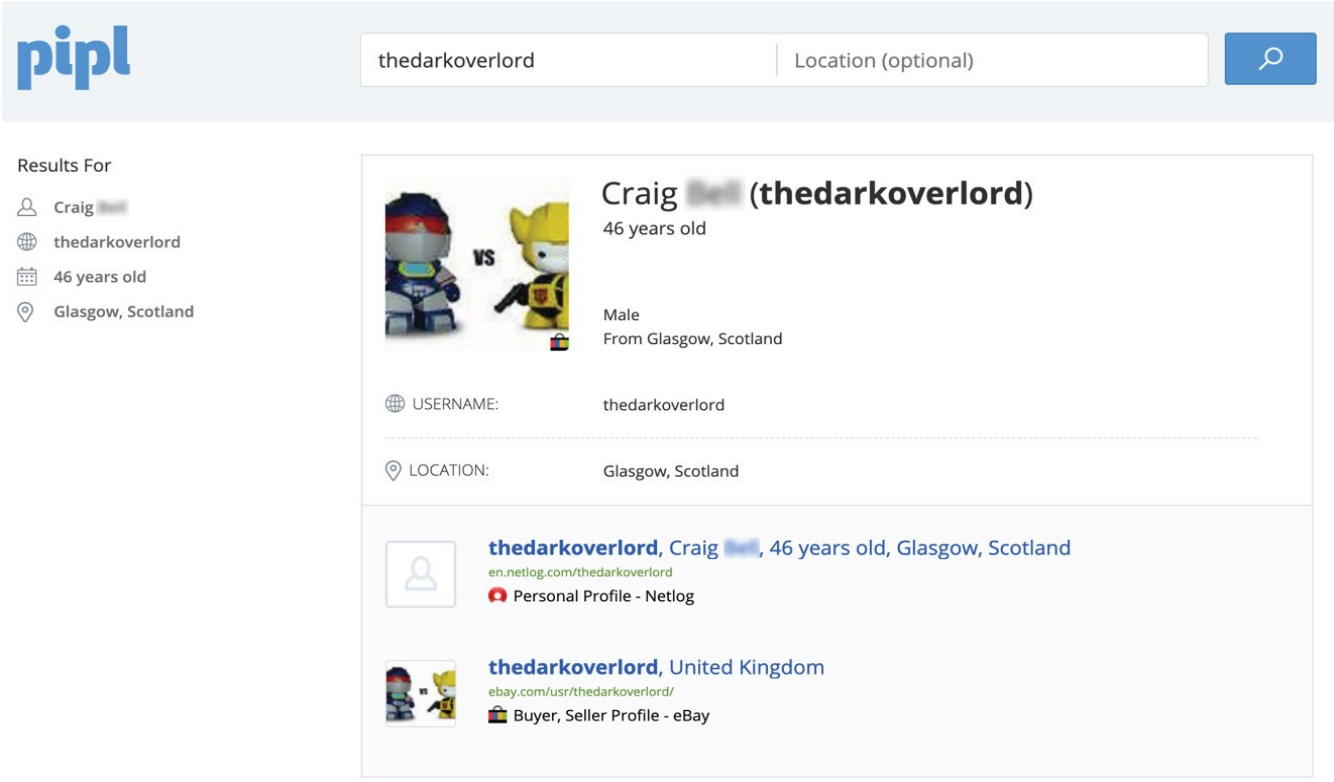


Рисунок 15.4.

FreeBackgroundCheck.org - это, как следует из названия, бесплатная проверка биографических данных.
Если вы ищете абсолютно бесплатно, стоит попробовать.
SkipEase.com очень похож на Kayak.com (туристический сайт) в том, что
дает возможность искать сразу на нескольких сайтах. Привлекательность байдарки в том, что вы
может выполнять поиск на многих основных сайтах, посвященных авиабилетам и отелям (например, Expedia и Travelocity) в то же время, что позволит вам найти лучшее предложение или цену для вашей поездки.
Точно так же SkipEase.com позволяет запускать одновременный поиск по
BeenVerified, WhitePages и PeopleLooker, три из крупнейших (и наиболее
уважаемые) люди находят сайты в Интернете. BeenVerified - обычно мой первый
стоп, но поскольку SkipEase позволяет искать все три, нет причин не
чтобы начать там.
На рис. 15.5 показан пользовательский интерфейс SkipEase с начальным поиском «Vinny Troia».
под BeenVerified.
Каждый из этих трех сайтов потребует от вас покупки отчета или оплаты
доступ для просмотра результатов, так что будьте готовы потратить здесь деньги, если
вы хотите просмотреть этот уровень информации о цели. Это еще один случай
где вы всегда получаете то, за что платите.
Эти инструменты охватят ваш базовый поиск людей и проверку биографических данных.
Ниже приведены несколько других менее распространенных инструментов, на которые стоит обратить внимание.

Ancestry.com

Ancestry.com почти всегда упускается из виду. Не знаю почему. Это буквально реклама
tises, у которого более 20 *миллиардов* записей для поиска - безусловно, самое большое количество
исторической информации о людях в любом месте. Это звучит для меня как красивый
хорошее место, чтобы посмотреть!

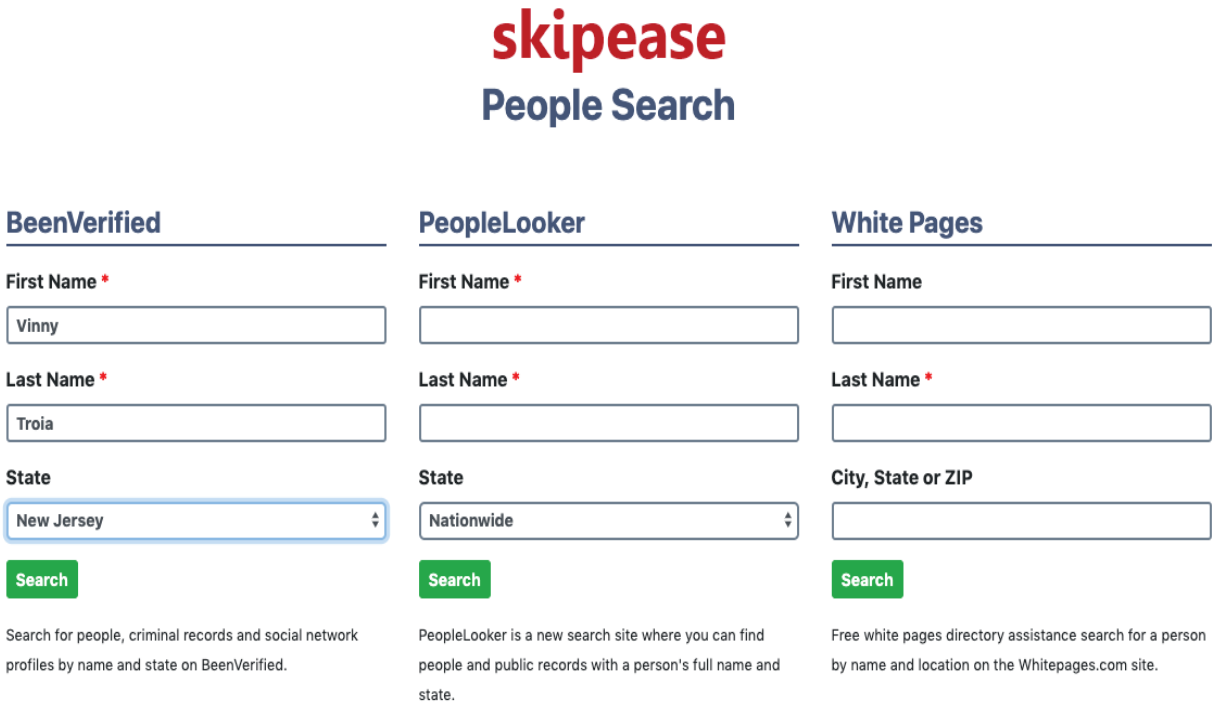


Рисунок 15.5

Что еще лучше в Ancestry.com, так это то, что вы можете покупать разные
пакеты, позволяющие искать международные рекорды. Хотя не во всех странах
Записи try будут такими же полными и актуальными, как и в США или
Канада, этот проспект стоит проверить, если вы имеете представление о злоумышленнике.
имя или имя члена семьи.

Самое замечательное в Ancestry.com - вы можете получить 14-дневную бесплатную пробную версию. если ты
не обнаружите, что используете его достаточно часто, чтобы оправдать членство, вы можете просто зарегистрироваться
для новой пробной версии, когда она вам снова понадобится.

У опасных актеров тоже есть отцы

Был случай, когда использование Ancestry.com действительно помогло
меня. Я искал злоумышленника в Канаде, но не смог найти много
так как он несовершеннолетний. Однако я плохо знал его имя и хотел узнать
больше о людях, с которыми он мог быть связан, поэтому я проверил Ancestry.com. Из
там мне удалось найти небольшое генеалогическое древо - достаточно, чтобы по крайней мере определить отца
и сестра. Как выяснилось, его отец - очень известный и известный повар.
в Канаде, у которых, кстати, была страница в Facebook с гораздо меньшими ограничениями, чем
его сын. К счастью для меня, я смог просмотреть его фотографии, не отправляя
ему просьба в друзья, поэтому я наконец нашел несколько фотографий
рассматриваемый субъект угрозы. Бум!

Судебные обыски

В каждом штате должна быть общедоступная система записей, в которой можно вести поиск. Если ты
ищут преступника в Соединенных Штатах, есть шанс, что они уже
есть запись. Если вы знаете имя человека и хотите узнать больше о
их фон, это хорошее место, чтобы посмотреть.

Фактический веб-сайт суда будет отличаться в зависимости от штата, поэтому лучше всего начать
Национальный центр государственных судов, www.ncsc.org . Чтобы найти прямую ссылку для
в каждом штате США перейдите на этот веб-сайт:
https://www.ncsc.org/topics/access-and-fairness/privacy-public-access-
к судебным записям / state-links.aspx

Или просто выполните поиск в Google по следующему запросу: «Веб-сайты государственных судов ncsc.org».
Предыдущий URL должен быть первым результатом.

На рис. 15.6 показан веб-сайт NCSC, на котором вы можете просматривать информацию о различных судах.
инструменты поиска для каждого штата.

Поиск изображений

Когда я исследовал происхождение Темного Повелителя, было несколько
изображения, которые впервые появились как аватары профиля. Хотя это, казалось бы, несущественно-
На первый взгляд, при более внимательном рассмотрении выяснилось, что изображения были достаточно отчетливыми, чтобы их можно было различить.
связаны с другими онлайн-дескрипторами. Хакеры (по крайней мере, пока они еще не работают) будут
повторно использовать изображения профиля на форумах, чтобы иметь возможность находить несколько вхождений
из этих изображений, особенно в социальных сетях, могут быть значительными.
Обычно при поиске изображений я обращаюсь к трем основным инструментам: TinEye, EagleEye,
и обратный поиск изображений Google. Давайте посмотрим на все три, но сначала слово из
Кот Мердок.

Одна вещь, с которой я сталкивался несколько раз, - это женщины, которые теперь являются профессионалами, которые ранее в их жизни в сеть просочились компрометирующие их фотографии.
Я думаю, что часто они даже не знают, что данные есть. Они не понимают
что кто-то поместил это туда, например фотографию, опубликованную на странице Flickr или в чьем-то блоге,
и вдруг он оказывается в Google Images.
Я думаю, что интересным преимуществом OSINT является то, что мы смогли идентифицировать некоторые из
эту информацию, и даже помочь людям удалить ее. Другое дело, если кто-то
эксплуатирует или вымогает у человека, или фактически использует данные для манипулирования кем-либо
каким-то образом . . . это становится намного более сложной ситуацией из-за всех эмоций
вовлеченный; это никогда не бывает легким решением.

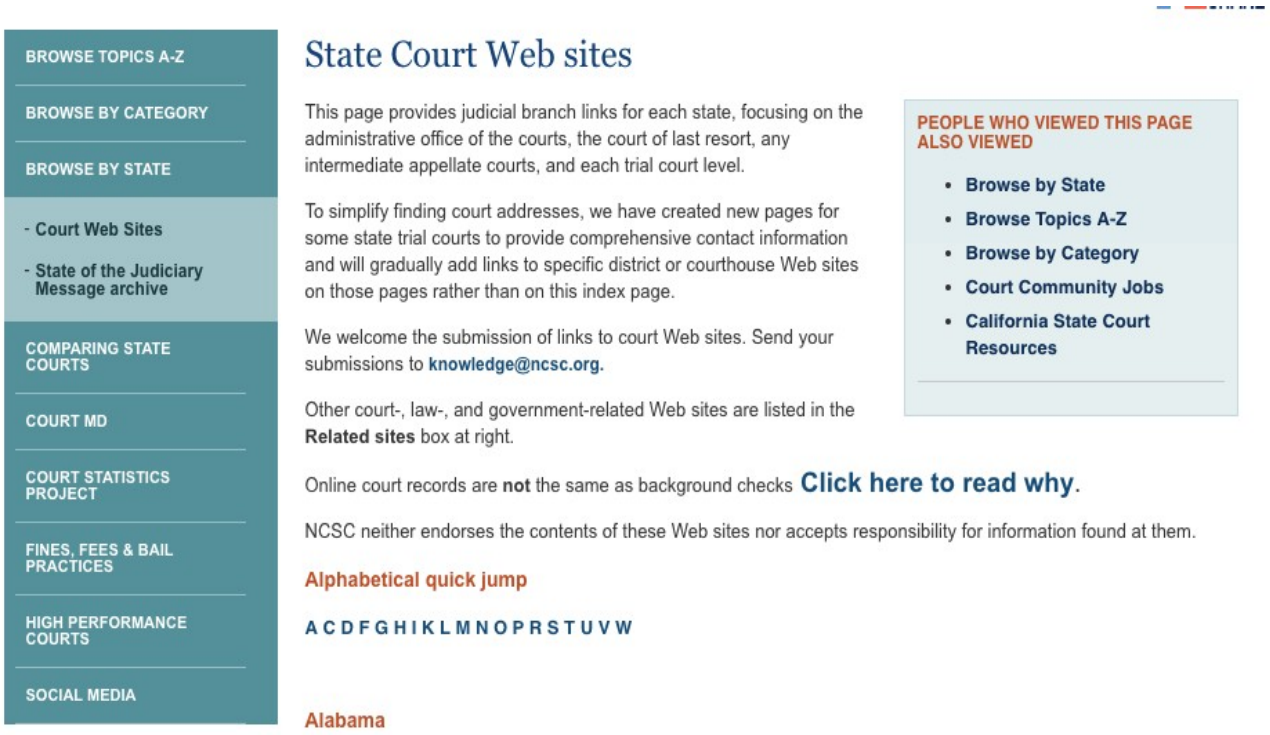


Рисунок 15.6.

Было действительно приятно помогать людям в таких ситуациях. к несчастью исследуя чью-то цифровую тень, вы обнаружите, что изображения использовались в каким-то другим способом, как будто они были обрезаны таким образом, что, возможно, не так желательно или каким-то образом меняет замысел изображения. Итак, когда вы можете найти эти изображения как часть расследования, и используйте эту информацию, чтобы связаться с Google и сказать: «Привет, мы владеть этим контентом. Сможешь его снять? " это мощное преимущество OSINT.

Может помочь обратный поиск изображений или такой инструмент, как TinEye. Иногда вы определяете обязательно нужно изучить возможность использования различных размеров при выполнении поиска, потому что обычно они были обрезаны или изменены.

Пару раз, когда это происходило, я видел фотографию, которая выглядела как человека, либо дело в том, что бывший фотограф сделал фотографии, а затем использовал их не одобренным образом.

Или, может быть, бывший парень использовал фотографию, но обрезал только лицо, а может быть супер- наложил свое лицо на чужое тело, чтобы он выглядел так, как на фотографии. Так что это действительно важно задокументировать мелочи, которые вы можете найти по пути в изучение. Сейчас они могут показаться неуместными, но они могут оказаться очень полезными. больше воздействия позже в будущем.

Google картинки

Google Images не только для поиска изображений. Конечно, вы можете ввести ключ- слово или имя человека и восхищаться появлением всех реальных совпадений, частичные совпадения и совпадения, которые не имеют абсолютно ничего общего с вашим исходный поисковый запрос.

Но . . . Знаете ли вы, что Google Images также позволяет выполнять обратный поиск изображений? существующее изображение? Для этого щелкните значок камеры, показанный на рисунке 15.7. Нажав на этот значок, вы сможете либо вставить конкретный URL-адрес изображения, либо загрузить изображение напрямую. На рисунке 15.8 показан экран загрузки изображения.



Рисунок 15.7

Стоит отметить, что я ни разу, ни разу не получал полезное совпадение с использованием обратного поиска Google Картинок. Однако я всегда оптимистичен. . . и для тщательности я всегда сначала пробую здесь.

В поисках золота

Некоторое время назад кто-то, слабо связанный с TDO, прислал мне несколько фотографий, которые он утверждены, были связаны с злоумышленником, известным как Tessa88. Видимо Тесса отправила этому злоумышленнику несколько фотографий, пытаясь представить круто, или подтвердите его личность. Рисунок 15.9 - одна из тех фотографий, на которой показано, что похоже, это украденные кредитные карты.

Вы никогда не знаете, где и почему это изображение может появиться в другом месте, но оно важно не оставлять камня на камне, поэтому я люблю начинать поиск в Картинках Google. Результаты поиска изображений показаны на рисунке 15.10.

У нас есть матч!

Клянусь, эти результаты были совершенно неожиданными. Я в шоке, что мы есть совпадение - и тем более, что у нас есть полезный. Иногда вы повезти. Единственная страница, которая соответствует изображению, - это blackforum.cc, русский язык. Кардинг форум. Давайте исследуем.

По следу

Следуя по следам российского кардингового форума, мы видим пост, где карты выставлены на продажу пользователем «Банкир» (рисунок 15.11).

Это действительно солидный успех - у меня уже были два других изображения на этой картинке. Это говорит мне о том, что это сообщение опубликовал тот же человек. или работая с той же группой.

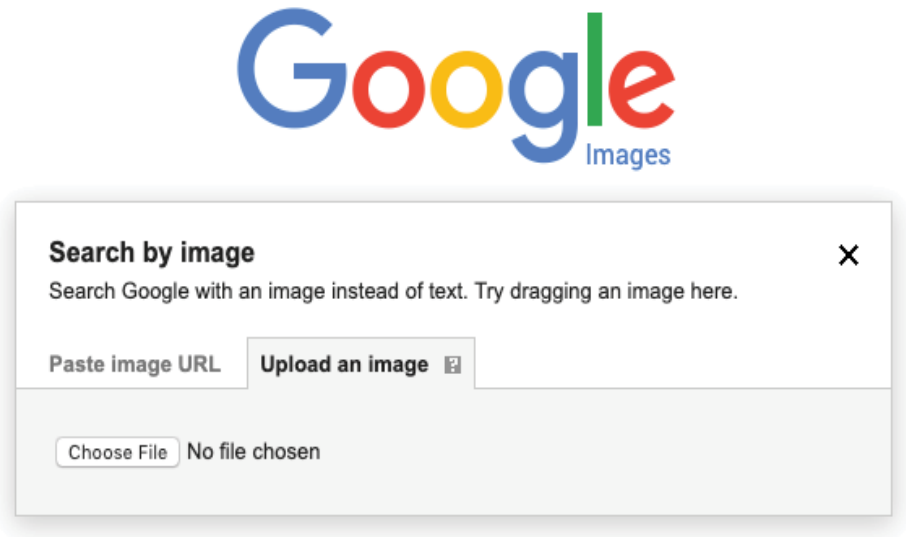


Рисунок 15.8

В любом случае мы узнали новое имя пользователя, с которым он связан: «Банкир».
У нас также есть его аккаунт в Telegram, который мы можем использовать, если захотим
с ним. Подайте его под «победой».

TinEye

TinEye (www.tineye.com) очень похож на обратный поиск Google Image и
Под «очень похожим» я подразумеваю то *же* самое, что и обратный поиск изображений Google. TinEye - это
точно так же, как Google, так что вам действительно стоит попробовать их оба.
На рисунке 15.12 показана страница поиска TinEye.
Для полноты картины давайте поищем в TinEye то же изображение кредитной карты в
Рисунок 15.9. К сожалению, на рис. 15.13 показано, что TinEye не смог сопоставить
изображение, найденное Google Images.
Запустим еще один поиск. На этот раз мы проверяем совпадения на одном из
Аватары старого профиля Сайпера (рис. 15.14).
Это довольно распространенное изображение и хороший способ проиллюстрировать разницу.
между TinEye и Google Images. Запуск этого изображения через Google
Обратный поиск изображений возвращает примерно 20 миллионов результатов.



Рисунок 15.9

С другой стороны, TinEye возвращает более управляемое число (рис. 15.15).
Первое попадание на это изображение - аватар профиля пользователя antichat.ru,
олдскульный русский хакерский форум. Это надежный матч, и он того стоит.
расследование. Это еще один отличный пример того, почему никогда не следует полагаться на
всего один инструмент для всех ваших результатов.
Интересно, что если вы посмотрите результаты поиска, вы даже-
Обычно найдите защищенную страницу Cyper в Twitter (рисунок 15.16).

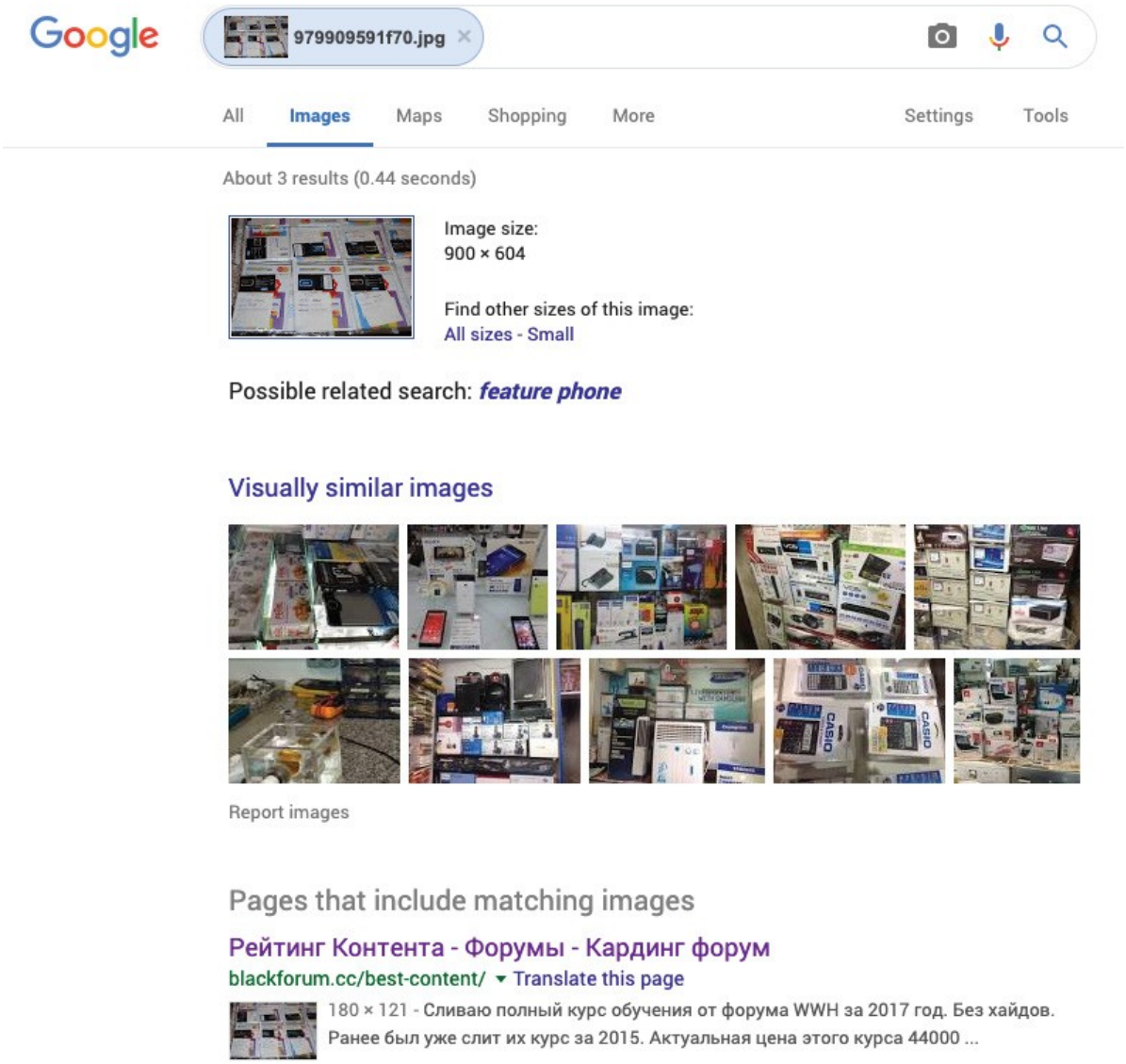


Рисунок 15.10.

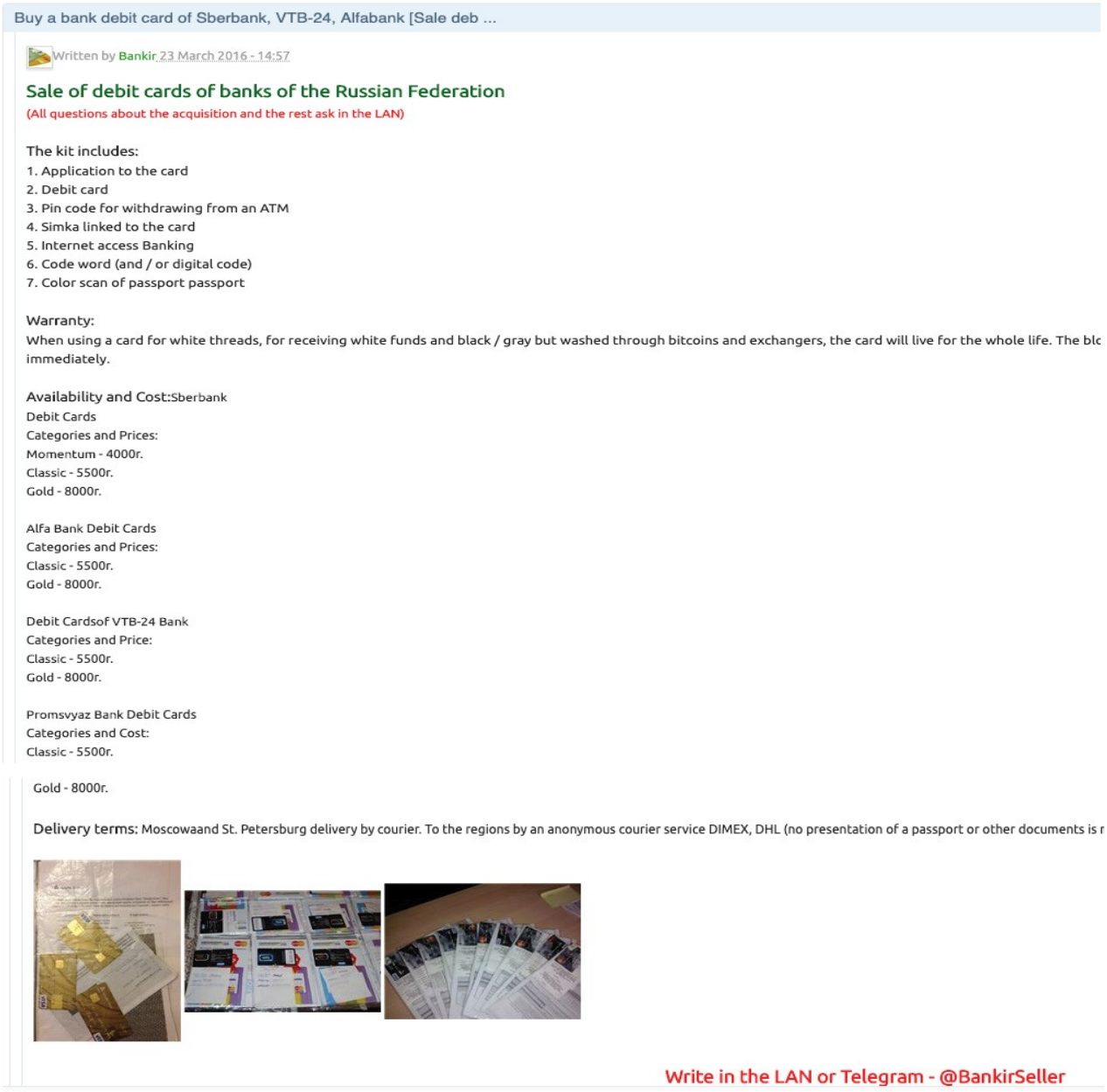


Рисунок 15.11

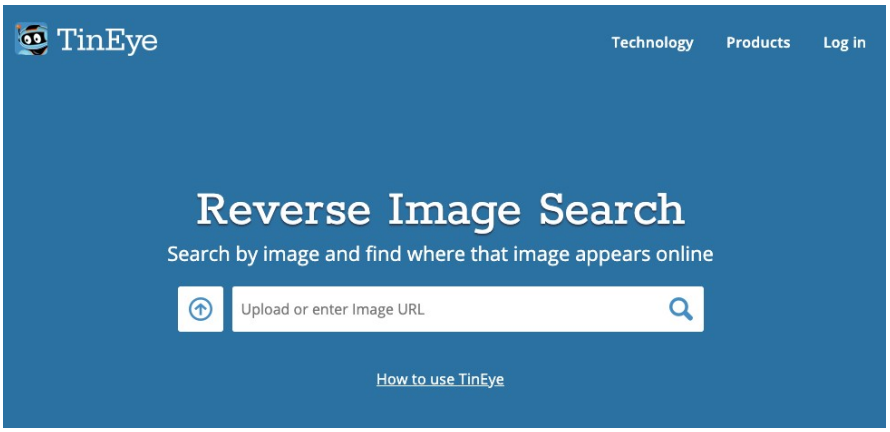


Рисунок 15.12

Еще один отличный матч. Я обнаружил, что злоумышленники любят повторно использовать профиль изображения, поэтому поиск новой страницы в Твиттере или социальной сети, связанной с угрозой актер часто сводится к чему-то простому, например, к сопоставлению изображения профиля.
Эй, посмотри на это! Я понятия не имел, что он следует за мной! Это довольно забавно, но это также подтверждает одну очень важную деталь: эта учетная запись все еще активна.

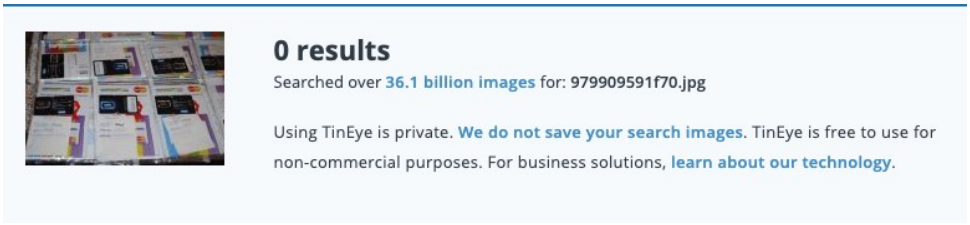


Рисунок 15.13



Рисунок 15.14

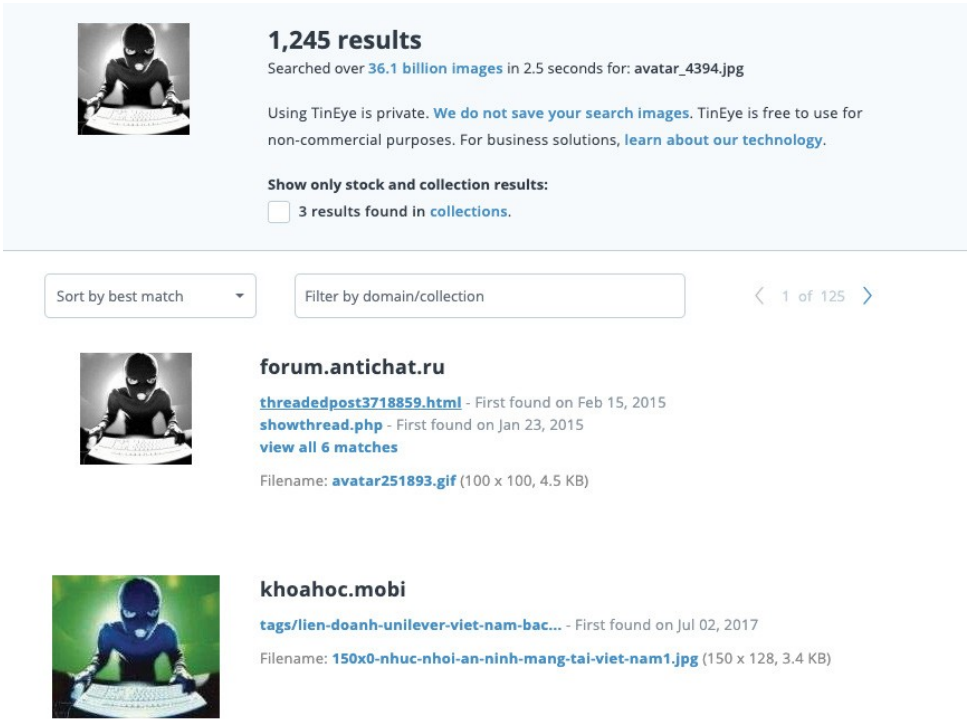


Рисунок 15.15

Орлиный глаз

EagleEye - это инструмент поиска изображений, предназначенный для обратного поиска в профиле в социальных сетях.
фотографий. Главный недостаток EagleEye в том, что нужно знать часть
имя человека, чтобы найти больше совпадений с его фотографиями профиля.
Это не обязательно может быть проблемой, если вы уже знаете название
субъект угрозы или цель и просто ищут дополнительную информацию об этом человеке.
EagleEye сначала ищет имя в Facebook, а затем выполняет обратный поиск.
поиск по картинке в Google, ImageRaider и Яндекс, чтобы найти
другие учетные записи человека в социальных сетях. Конечный результат - красиво отформатированный
Отчет в формате PDF.
Еще одно хорошее применение этого инструмента - проверить, есть ли у кого-то потенциально
ловить рыбу. Всегда хорошо запускать чью-то фотографию в соцсетях
и посмотрите, с какими еще совпадениями вы можете вернуться.
Вы можете скачать EagleEye по адресу https://github.com/ThoughtfulDev/EagleEye .
На рисунке 15.17 показан главный экран EagleEye.

Поиск изображений

Для нашего примера изображения давайте поищем одну из моих фотографий для прессы (рис. 15.18).
и посмотрим, какие результаты мы получим.
На рисунке 15.19 показано, как выглядит типичный вывод EagleEye при обработке.
Картинка.



Рисунок 15.16

В фоновом режиме EagleEye загружает веб-драйвер и автоматически выполняет поиск
Google для вашего изображения. На рисунке 15.20 показан автоматический обратный поиск в Google.
процесс.

Хотя это и не очень полезно, EagleEye, по крайней мере, смог идентифицировать мой Facebook.
страницу путем поиска учетных записей с использованием информации, полученной из моего профиля
рисунок (рисунок 15.21).

На самом деле неплохо. Он нашел несколько моих профилей, так что определенно есть заслуга
к этому инструменту, и стоит попробовать, если у вас есть фотографии людей, которых вы хотите идентифицировать.

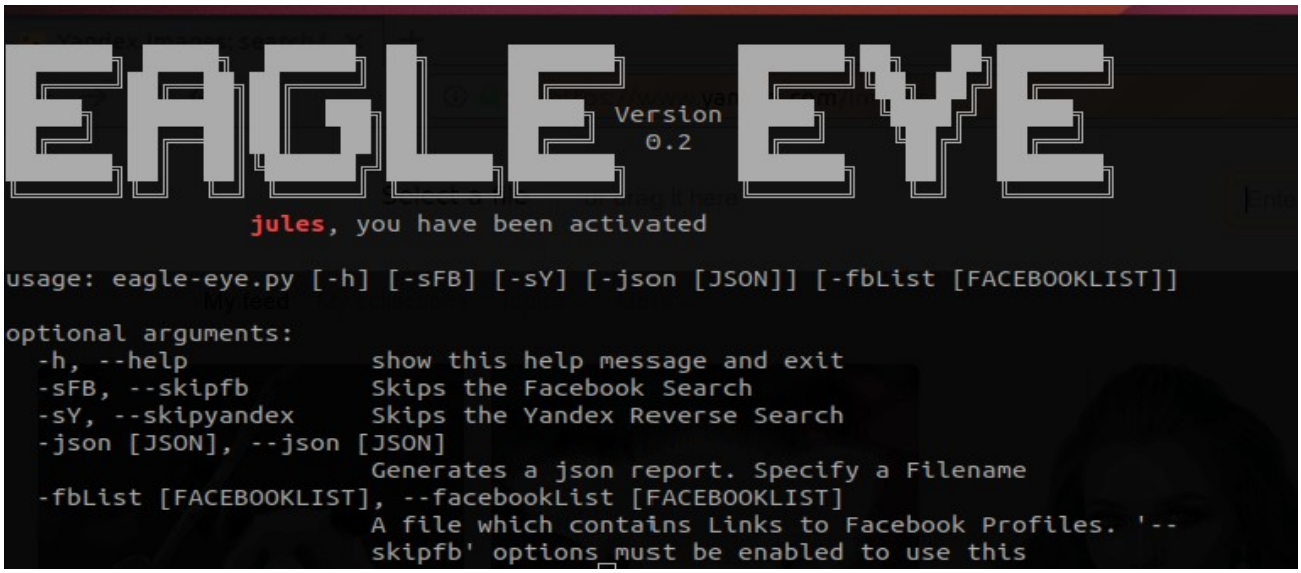


Рисунок 15.17



Рисунок 15.18

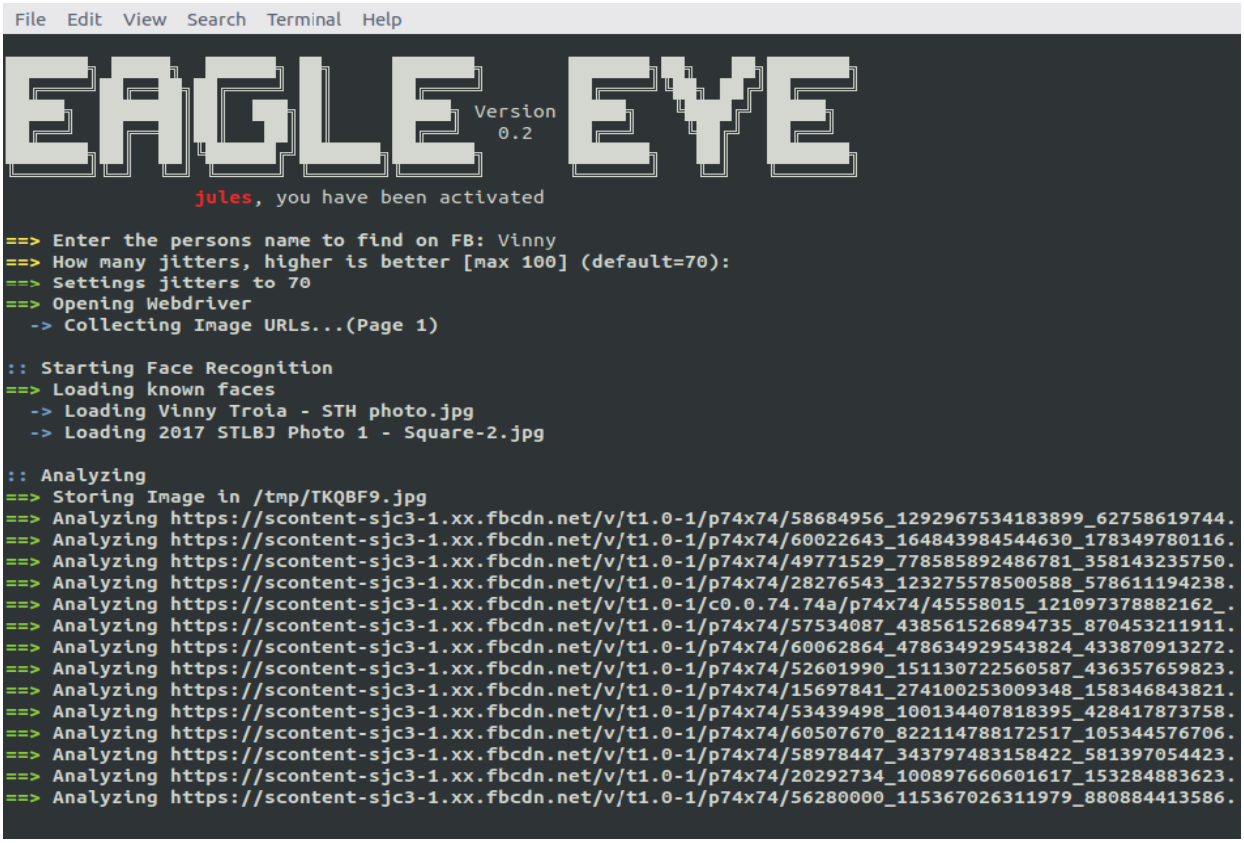


Рисунок 15.19

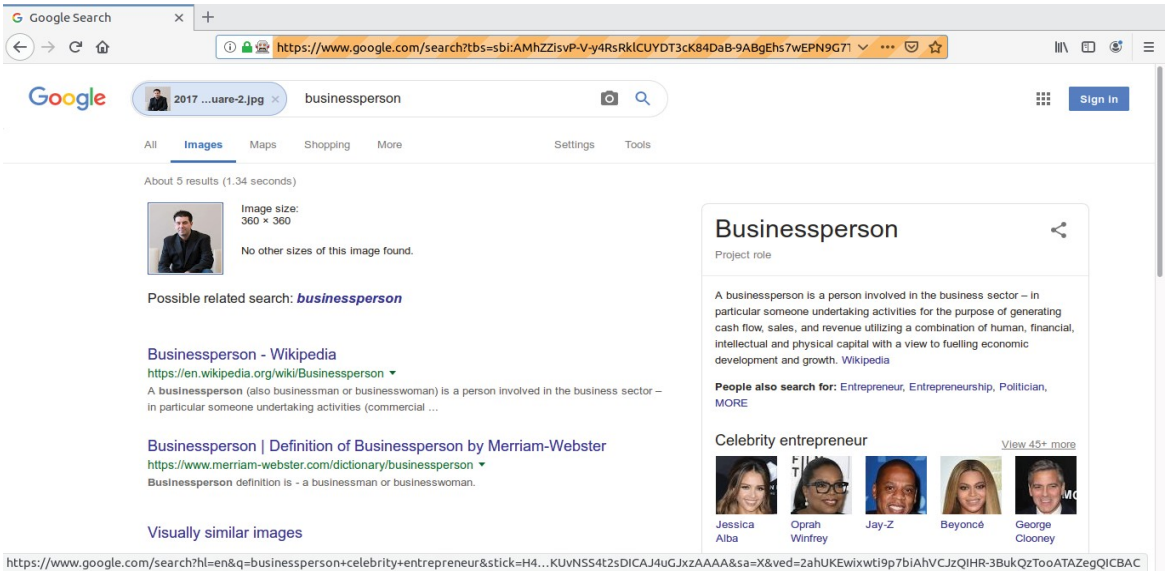


Рисунок 15.20

Cree.py и геолокация

Cree.py - это инструмент OSINT, предназначенный для получения информации о геолокации из общедоступные данные на отдельных сайтах социальных сетей.

В частности, Cree.py может извлекать данные о геолокации для твитов, пока целевые пользователи не отключили данные геолокации в своем клиенте Twitter. Если геолокатион отключен, Cree.py все еще может извлекать очень полезные, не зависящие от местоположения информация из аккаунта цели в Твиттере, такая как количество подписчиков, каких пользователей они ретвитят, типы устройств, которые они используют для подключения к Twitter, и частота и время суток, в которые они обычно пишут твиты.

Cree.py доступен для Windows, Mac OSX и Linux по адресу https: // www. .geocreepy.com .

Начиная

После того, как вы загрузили и установили Cree.py, на рис. 15.22 показаны основные Жуткий экран.

Чтобы начать новое сканирование, щелкните значок человека, чтобы создать новый профиль о вашем конкретная цель.

В качестве цели для нашего примера давайте поищем мою личную учетную запись Twitter «Vinny-Троя ». На рисунке 15.23 показано начальное окно поиска, в котором мы устанавливаем цель. и выберите платформы для поиска.

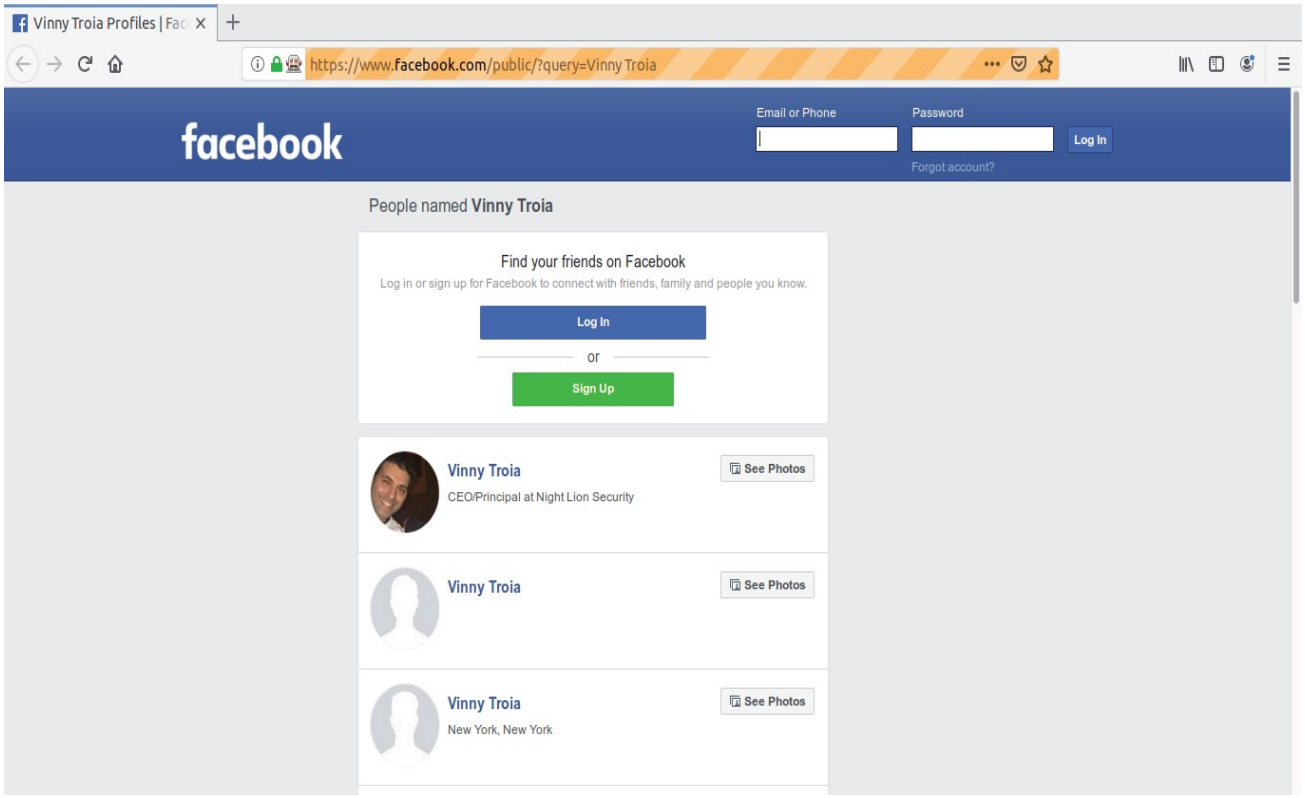


Рисунок 15.21

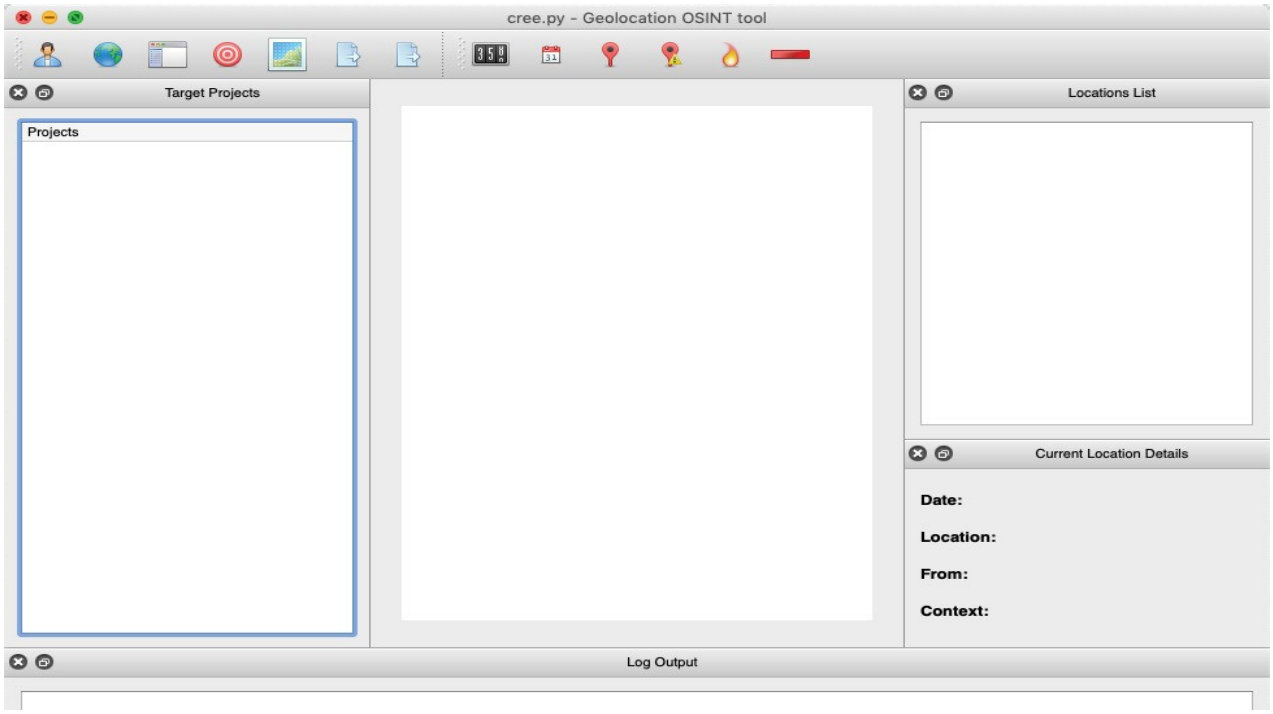


Рисунок 15.22

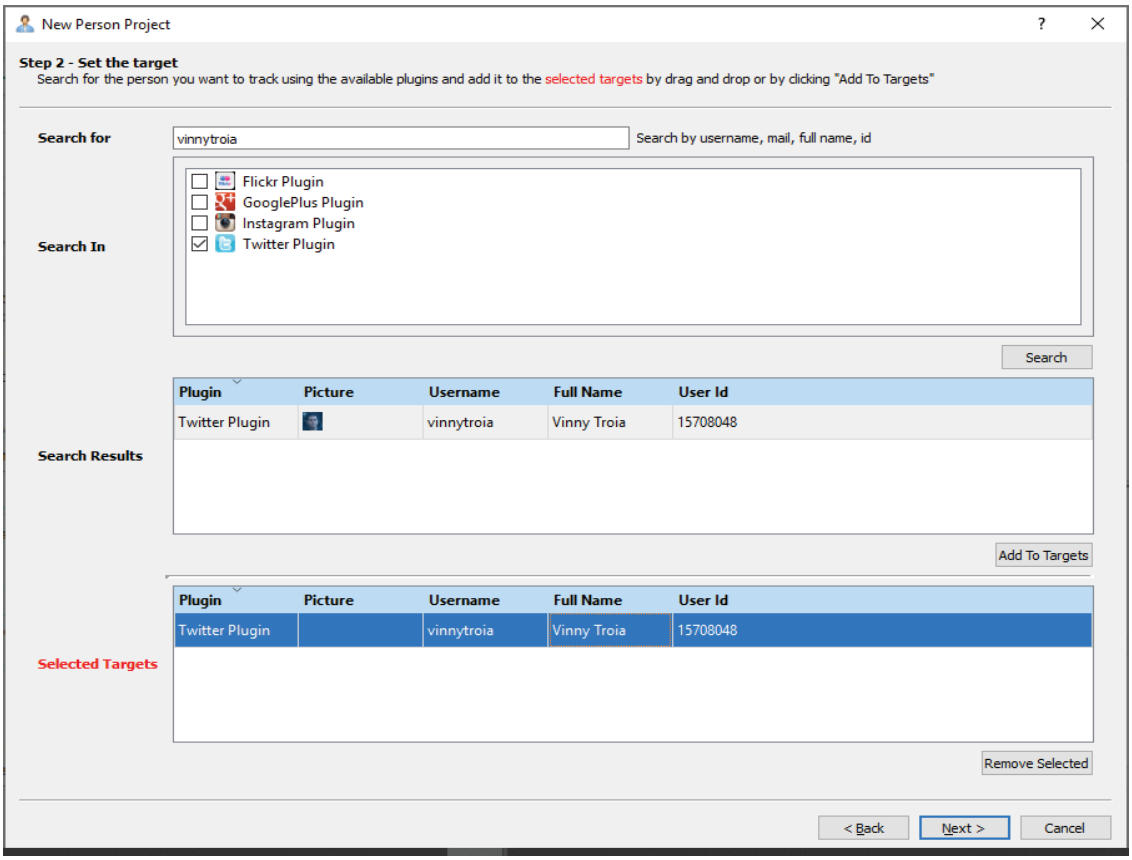


Рисунок 15.23

Введя мое имя в поле «Искать», вы заполните выбранные цели.
область, если найдено успешное совпадение (или если найдено несколько потенциальных совпадений).
После выбора цели нажмите кнопку «Далее», чтобы начать анализ пользовательского
твиты.
После завершения первоначального анализа информация профиля цели в Twitter будет
отображается. На этом этапе вы должны обратить внимание на одну из следующих двух строк:

■ Пользователь включил возможность геолокации своих твитов.

■ Пользователь отключил возможность геолокации своих твитов.

Если твиты пользователя содержат информацию о геолокации, Cree.py отобразит список
твитов цели и соответствующей информации о местоположении. Глядя на
результатов для моей учетной записи Twitter (рис. 15.24), мы видим семь твитов,
информация о геолокации.
На этом этапе вы можете фильтровать местоположения по дате или их положению на карте. В
Кроме того, вы можете настроить настраиваемый фильтр даты для поиска твитов в определенных
диапазоны дат или отфильтровать неточные местоположения. Каждый раз, когда вы обновляете местоположение
фильтр, карта обновляется автоматически.

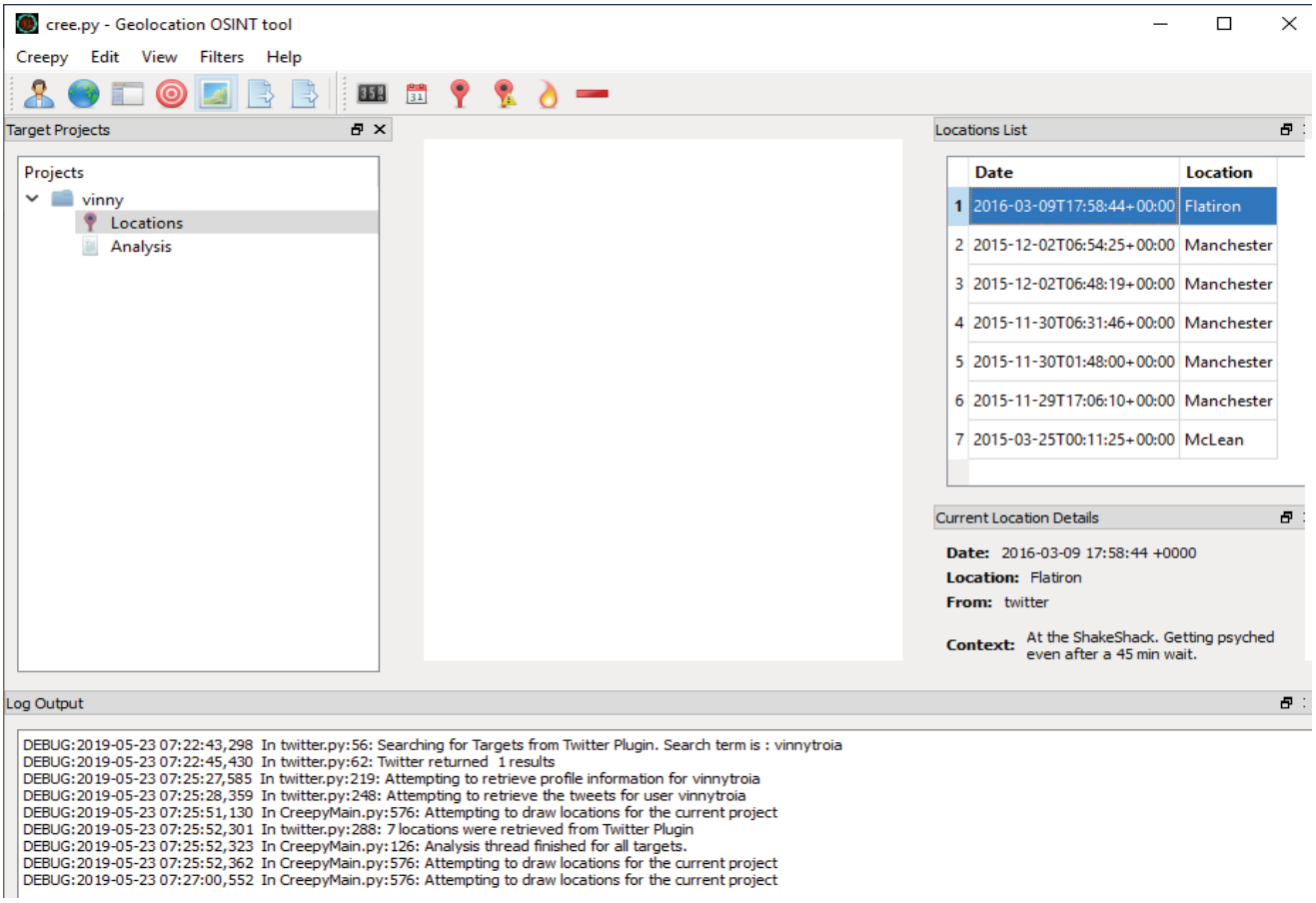


Рисунок 15.24

Вы также можете экспортировать свои результаты в виде CSV, что очень полезно для сохранения
запись информации и то, что вы можете индексировать и искать
позже в вашем расследовании.

Таблица 15.1 представляет собой экспорт в CSV моих твитов с включенной информацией о геолокации.
Поиск данных о геолокации в твитах злоумышленника кажется долгим,
но никогда не следует недооценивать способность киберпреступников оставлять небрежные
след вот так. Существует множество историй об аресте преступников за
серьезное преступление, такое как перевозка наркотиков из-за того, что они не остановились у знака «Стоп».
Это ничем не отличается.

Отслеживание IP-адресов

В этом году на Derbycon я видел, как Джон Стрэнд выступал с докладом о кибер-атрибуции. В его
разговора, он продемонстрировал способ добиться лучших результатов при попытке точно определить
физическое расположение IP-адреса.

Таблица 15.1: Экспорт CSV с информацией о геолокации «перевод таблицы»

TIMESTAMP	LATITUDE	LONGITUDE	LOCATION NAME	CONTEXT
2016-03-09 17:58:44 +0000	40.7393845	-73.990098	Flatiron	At the ShakeShack. Getting psyched even after a 45 min wait.
2015-12-02 06:54:25 +0000	38.577462	-90.499221	Manchester	ICYMI - 128GB USB3 Flash Drive - $25 - https://t.co/LhLWPotjVz
2015-12-02 06:48:19 +0000	38.577462	-90.499221	Manchester	Wow. 128GB USB3 flash drive only $25. SSD prices are dropping like crazy.
2015-11-30 06:31:46 +0000	38.577462	-90.499221	Manchester	has anyone started shopping yet? is there anything good out there worth buying right now? #BlackFriday
2015-11-30 01:48:00 +0000	38.577462	-90.499221	Manchester	Ok, look. I am as big a fan of #WalkingDead as anyone, but at some point shouldn't the zombies all collapse under their own weight?
2015-03-25 00:11:25 +0000	38.9374855	-77.203885	McLean	Hello, Langley.

2016-03-09
17:58:44 +0000
40,7393845
-73.990098
Утюг
В ShakeShack.
Даже нервничаю
после 45 минут ожидания.
2015-12-02
06:54:25 +0000
38,577462
-90,499221
Манчестер
ICYMI - 128 ГБ USB3
Флешка - 25 долларов -
https://t.co/
LhLWPotjVz
2015-12-02
06:48:19 +0000
38,577462
-90,499221
Манчестер
Вот это да. 128 ГБ флэш-памяти USB3
проехать всего 25 долларов. SSD
цены падают как
сумасшедший.
2015-11-30
06:31:46 +0000
38,577462
-90,499221
Манчестер
кто-нибудь начал
покупки еще нет? здесь
что-нибудь хорошее там
стоит покупать прямо сейчас?
#Черная пятница
2015-11-30
01:48:00 +0000
38,577462
-90,499221
Манчестер

Хорошо, смотри. Я такой же большой
поклонник #WalkingDead as
кто угодно, но в некоторых
указывать не следует
все зомби рушатся
под собственным весом?
2015-03-25
00:11:25 +0000
38.9374855
-77.203885
Маклин
Привет, Лэнгли.

Я тестировал Canarytokens на пользователе, который, как я знал, находился в центре Луевилля, штат Кентукки.
Когда пользователь открыл поддельный вредоносный пакет, мне вернули его IP-адрес.
Когда я выполнил поиск геолокации по его IP-адресу, и результат
не был очень точным - результаты вернулись с местоположением, которое составляло около 20 миль
прочь.
Я обнаружил, что один из способов улучшить детализацию поиска геолокации - это
использовать команду traceroute на рассматриваемом IP-адресе. Затем, глядя на
ваши результаты, возьмите IP-адрес *последнего* участка *маршрутизации* и определите местоположение этого IP-адреса.
вместо.
Это сделает вас *намного* ближе. В моем тестовом случае мне удалось точно определить IP-адрес.
с точностью до одного блока от отеля.
Причина, по которой это работает, заключается в том, что большинство IP-адресов (для домашних пользователей в
в частности) раздаются через случайный DHCP. IP-адреса могут перескакивать, а гео-IP
поиск не сможет узнать, где вы на самом деле находитесь.
Но используя инфраструктуру маршрутизации из команды traceroute, мы обычно можем получить
гораздо более близкие и более точные результаты для местоположения.

Резюме

В первой главе раздела «Охота на людей» был рассмотрен ряд инструментов.
которые можно использовать для отслеживания людей в Интернете, в том числе для обратного поиска изображений,
проверка данных, различные инструменты поиска людей и способы сбора данных о геолокации
информация из социальных сетей.
В следующей главе мы подробнее рассмотрим профили в социальных сетях.
который будет включать инструменты и методы, которые могут помочь идентифицировать несколько псевдонимов,
учетные записи и номера телефонов, связанные с целью.

349

16

В этой главе основное внимание уделяется инструментам и методам, которые помогут в вашем открытии.
альтернативных псевдонимов цели и профилей в социальных сетях. Посмотрим на разные
способы поиска и поиска имен, псевдонимов и телефонных номеров, чтобы даже-
Постройте матрицу отслеживания злоумышленников в главе 17.
Несколько примеров в этой главе будут сосредоточены на Натане Вятте, который в настоящее время
борется с экстрадицией США за преступления, связанные с Темным повелителем.
Моя официальная позиция в отношении Вятта состоит в том, что я считаю, что он использовал псевдоним Арни, и
что группа использовала его как своего любимца. Эта теория подтверждается следующим:
В разговоре с Коломбиной (которую я считаю близкой соратницей)
из NSA@rows.io).
Колумбина: Да, я не знаю, где сейчас настоящий Revolt, но idc tbh
Колумбина: Мы все равно так много не говорили
Колумбина: Многие другие ниггеры тоже ушли.
Колумбина: Нравится NSA@rows.io
Колумбина: Они образовали темную перегрузку.
Колумбина: та группа выкупа
SoundCard: да, я хорошо о них знаю
Колумбина: Я слышал, что Арни злился на АНБ.
SoundCard: скажу, что они хорошо поработали с маркетингом
Колумбина: Так внутреннее напряжение между группой

Поиск в социальных сетях

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

Коломбина: Ага
Колумбина: Они действительно хорошо справились с этим.
SoundCard: Драма забавная.
Звуковая карта: Ну ладно, я укушу. Почему?
Коломбина: АНБ почти не занималось сексом для TDO, я слышал
Коломбина: а деньги у него все-таки есть
Коломбина: так Арни (который проделал большую часть работы) рассердился
Коломбина: Я так понимаю.
SoundCard: о, видите ли, я думал, что Арни был тем парнем, которого посадили в тюрьму
Колумбина: Нет, они все еще здесь
Колумбина: Если они не сделают серьезную ошибку, я сомневаюсь, что они
арестован
Колумбина: Я так не думаю
Колумбина: Я ожидаю, что из всех них арестуют АНБ.
SoundCard: это был парень из Великобритании
Колумбина: Да, вы слышали его звонок?
Звуковая карта: ха-ха-ха-ха
Звуковая карта: что за хрень ***
Коломбина: Да, икр

Если я прав, то из этого разговора становится ясно, что Коломбина пытается-
пытаясь переложить все основные взломы TDO на Арни, а не на АНБ (ядро
руководитель ТДО).

Важный вывод здесь заключается в том, что не все, что вы соберете, будет действительным.
или законный. Многие из опытных злоумышленников оставят подсказки, предназначенные для раскрытия информации.
конкретно сбить вас с их следа.

При сборе информации, особенно в социальных сетях, вы всегда должны
спросите себя, действительно ли то, что вы нашли, или оно было помещено туда
кто-то хочет, чтобы вы его нашли.

Ставьте под вопрос все.

OSINT.rest

OSINT.rest - это сайт от создателей плагина SocialLinks для Maltego.
(https://www.mtg-bi.com). SocialLinks - это , *безусловно,* мой любимый плагин Maltego. Я
изначально планировал осветить Maltego только для того, чтобы рассказать о своем плагине, но
теперь, когда есть отдельный веб-сайт, который позволяет собирать те же данные, я
нравится такой подход лучше.

OSINT.rest (www.osint.rest) - это гигантский API, который позволяет собирать социальные СМИ информации о ваших целях. Вы можете запросить API с помощью команд CURL в командной строке или используйте такой инструмент, как Postman (https://www.getpostman.com). Это услуга премиум-класса - вы можете покупать ключи и запросы API оптом.

OSINT.rest позволяет API искать следующее:

- Поиск пользователя по телефону или электронной почте.
- Facebook (фотографии, страницы, видео, пользователи, сообщения, лайки, места)
- Instagram (поиск по псевдониму)
- Поиск изображений
- Поиск в Twitter
- Foursquare
- SL DB
- VK.com
- MySpace

При просмотре API Docs OSINT.rest, вы увидите кнопку с надписью «Выполнить в Почтальон «. Нажмите эту кнопку, чтобы загрузить API прямо в приложение Postman. (в настоящее время доступно для Windows или Mac).

Меню слева будет заполнено результатами поиска из OSINT.rest.

На рисунке 16.1 показано приложение Postman с загруженным API-соединением OSINT.rest. и выделена опция «Поиск информации по телефону».

Для нашего испытания я ввел номер своего мобильного телефона. Окно на рисунке 16.2 показывает успешные результаты этого поиска.

Этот API работает только с номерами в США, но результаты, очевидно, очень мощно, если вам нужна помощь в обратном поиске телефонного номера.

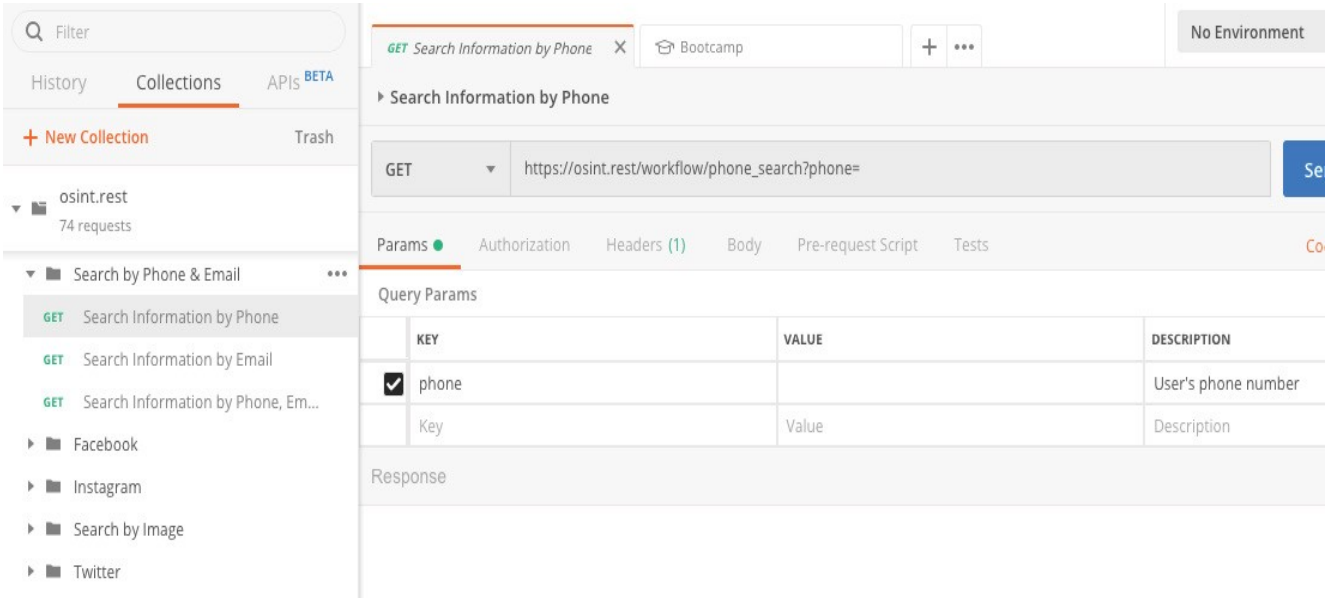


Рисунок 16.1

OSINT.rest имеет почти сотню различных вариантов поиска в Facebook,
которые включают возможность поиска пользователей, друзей пользователя, людей, которые общаются
в сообщениях, видео, страницах и многом другом.

Для нашего первого поиска давайте воспользуемся профилем Натана Вятта, человека, который был
осужден и отправлен в тюрьму в 2017 году за взлом телефона Пиппы Миддлтон.

По состоянию на 2019 год Натан Вятт борется с экстрадицией в США за преступления, связанные с
с Темным Повелителем (https://www.dailymail.co.uk/news/article-6578213/
Сидеть дома-отец-обвиняемый-взлом-борется-экстрадиция-US.html).

Простой поиск в Facebook покажет его общедоступный профиль в Facebook. Рисунок 16.3
показывает свою страницу в Facebook и идентификатор профиля 100010064775327 в строке URL.

Имея цели Facebook ID спасает нас шаг от того, чтобы искать его. Самый
для поиска требуется точный идентификатор, поэтому в конечном итоге вам нужно будет его найти. Давай копать
в возможности Facebook в OSINT.rest.

Зная, кто ваш целевой подключен к может быть очень простым способом определить
другие субъекты угроз или другие лица, имеющие взаимные связи. Получение списка JSON некоторых-
друзей так же просто, как ввести их Facebook ID в параметрах запроса.

На рисунке 16.4 показан результат этого запроса.

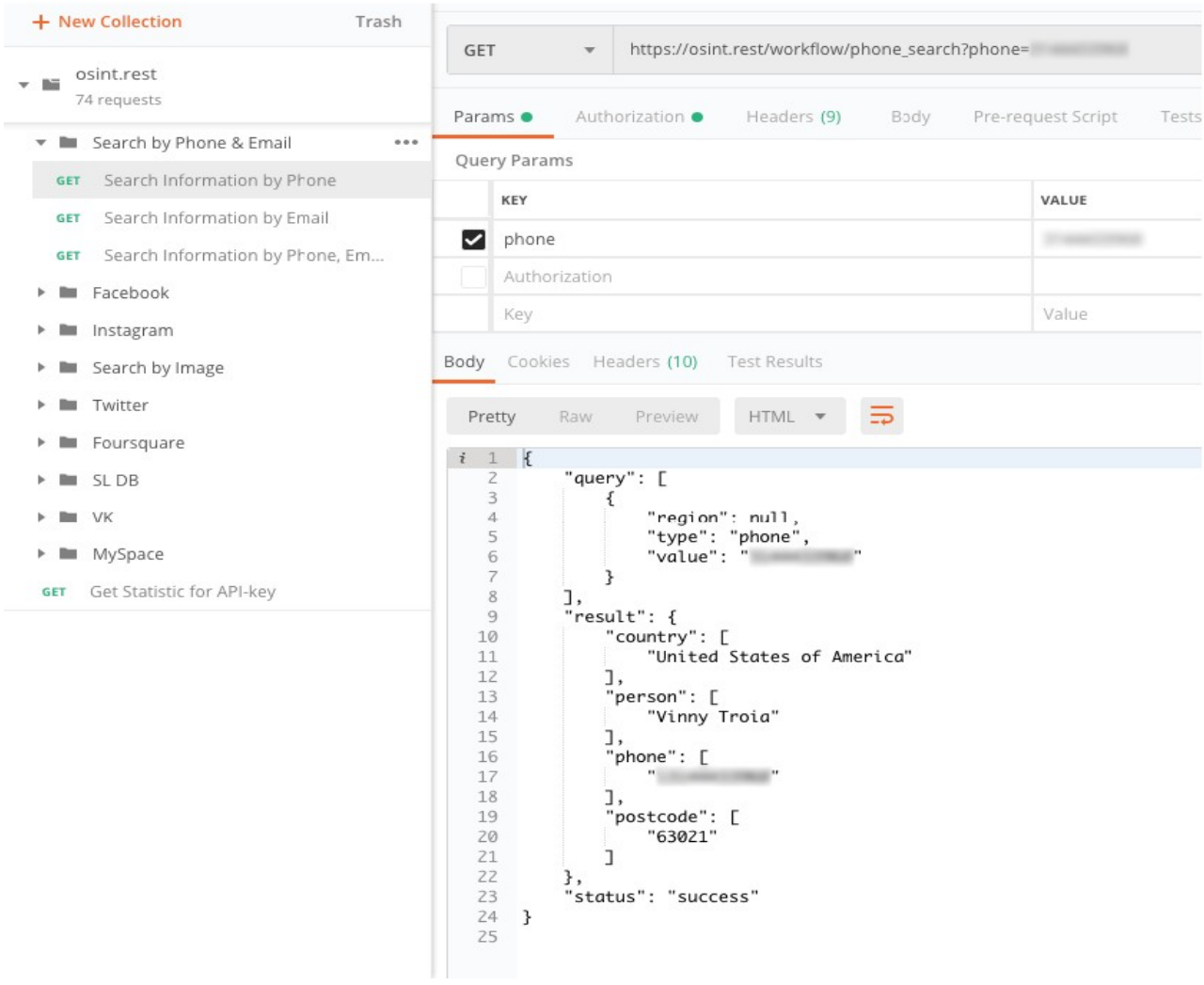


Рисунок 16.2



Рисунок 16.3

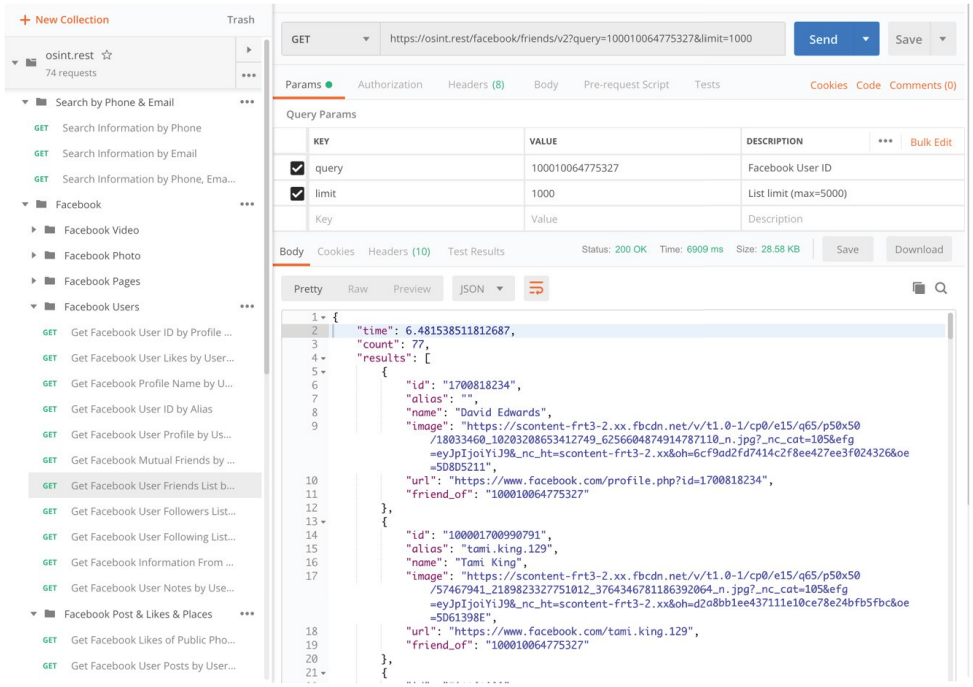


Рисунок 16.4

Вот очень конкретный пример того, почему знание чьих-то друзей может быть важным. Некоторое время назад я искал конкретного злоумышленника (я знал его настоящую имя). Я просматривал список его друзей, и там было несколько человек, которые поймали мой глаз. Посмотрев на их профили в Facebook и списки друзей, я заметил, что они на самом деле были друзьями с альтернативными аккаунтами моей цели в Facebook! Фотография была немедленная раздача, но поскольку название было другое, я бы никогда не нашел, что профиль, если бы я не нашел время, чтобы просмотреть его список друзей.

Из результатов видно, что у Натана Вятта 77 публичных друзей в Facebook.

Этот вывод также дает нам имена, идентификаторы, изображения и прямые URL-адреса его друзей.

Это одна из областей, где использование Maltego значительно упрощает этот процесс.

поскольку приложение автоматически создает для вас визуализацию всех подключений, которые

Я продемонстрирую позже в этом разделе.

Мы знаем, что псевдоним CraftyCockney напрямую связан с Натаном Вяттом.

из всех публичных новостей и отчетов суда, так что это отличное место для

начать поиск.

Для этого поиска давайте попробуем Instagram. Используя опцию Instagram API на

Слева на рис. 16.5 показан запрос «Craftycockney» рядом с результатами.

Этот поиск по API вернул всех в Instagram с CraftyCockney как

часть их имени пользователя. У нас всего около 20 результатов, поэтому просматривая все

это будет стоить времени, чтобы определить правильный целевой профиль.

Если у вас есть другие псевдонимы, просто промойте и повторите. Попробуем еще один.

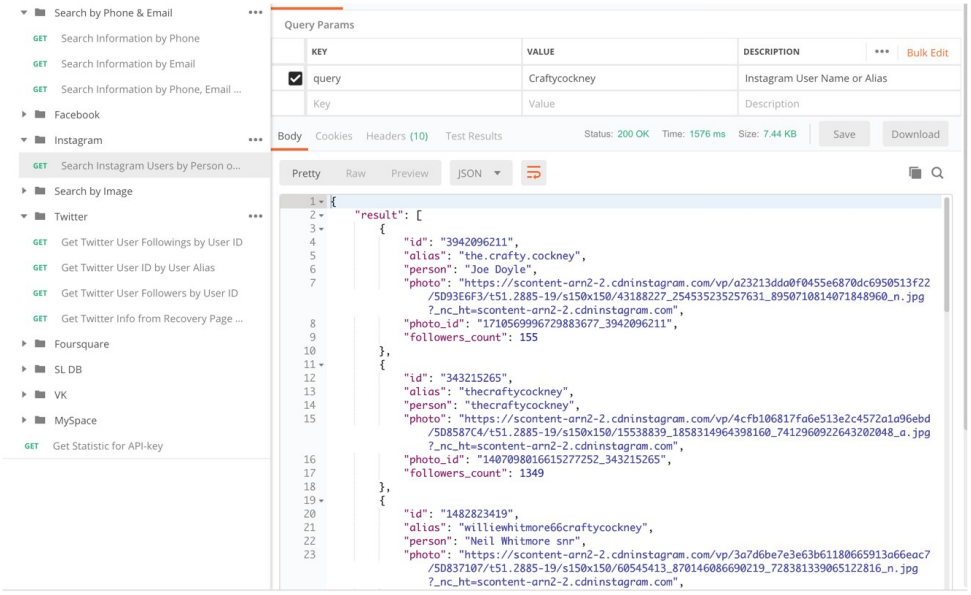


Рисунок 16.5

Другой подопытный

Для следующего примера, давайте посмотрим на наш хороший друг и товарищ эксперт по вопросам безопасности Кристофер Менье (он же WhitePacket). Большинство профилей Криса на Facebook
офлайн, но из-за магии поисковых алгоритмов Facebook я набрал его
имя и выскочил новый профиль с его аватаркой и намерением-
имя союзника написано с ошибкой. В профиле Facebook значился Крис Монье, но для
почему-то в результатах поиска все равно отображался профиль. Может быть в фейсбуке
связали его фото, или, может быть, это просто дало мне близкие совпадения. Или
Кстати, забей!

Чтобы выполнять какие-либо поиски, нам нужно знать его идентификатор в Facebook. Мы можем
сказать, из URL, что его имя пользователя является christopher.maunier.923. Все, что нам нужно
нужно ввести это имя пользователя в поиск API «Получить идентификатор пользователя Facebook по профилю».
(Рисунок 16.6).

Запустив поиск, мы легко получим его идентификатор в Facebook 100033275741589.

К сожалению, профиль Криса в основном частный, но все же есть приличный
количество информации, которую мы можем получить от него. Для того, чтобы начать, «Получить Facebook
пользователя Pro-
файл по идентификатору пользователя »(рис. 16.7) вернет сводку целевого Facebook
профиль, который включает последние сообщения, заголовок, полное имя, прямой URL, фото
URL и многое другое.

Одна вещь, которую мы можем сразу увидеть из этих результатов является URL его лицевой стороной
книга фото. К счастью для нас, OSINT.rest также включает в себя обратный поиск изображений API.

Давайте сначала начнем с перехода по этому URL-адресу. Публичная запись и фото профиля для
Пользователь 100033275741589 (рисунок 16.8) содержит заголовок «Fak u.»

Теперь, когда у нас есть фото профиля, мы можем сохранить его на потом или скопировать URL
и выполнить обратный поиск изображения.

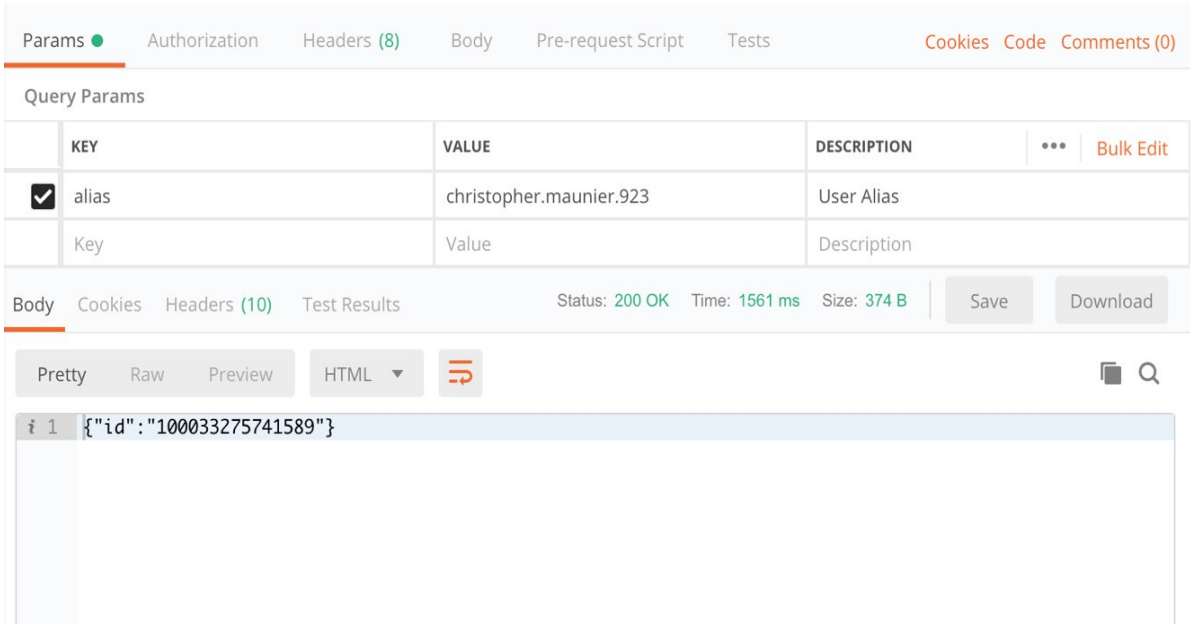


Рисунок 16.6.

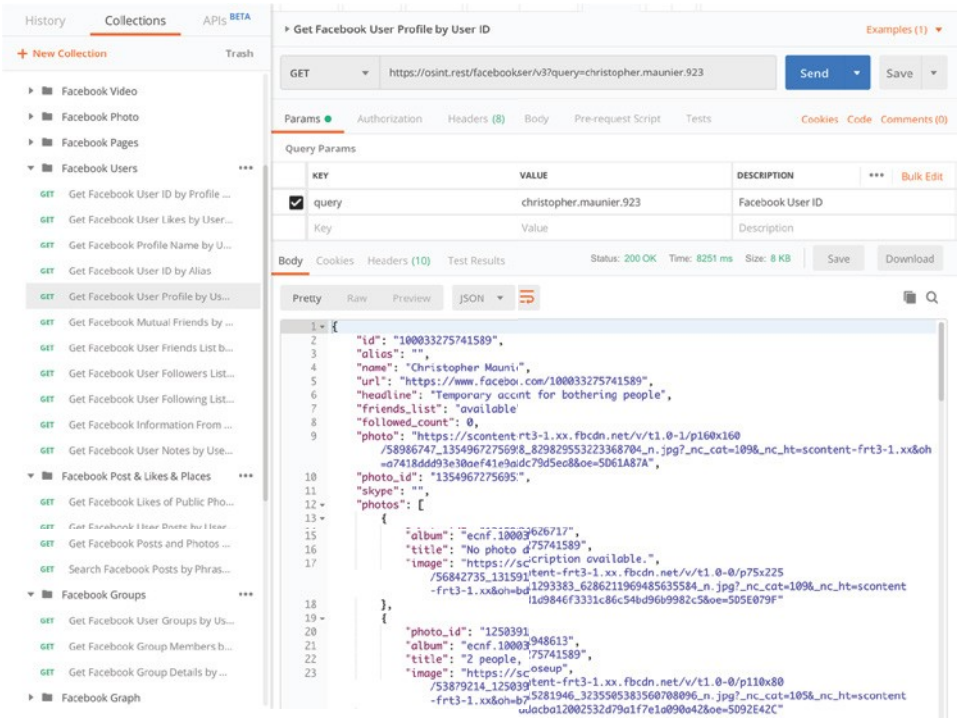


Рисунок 16.7

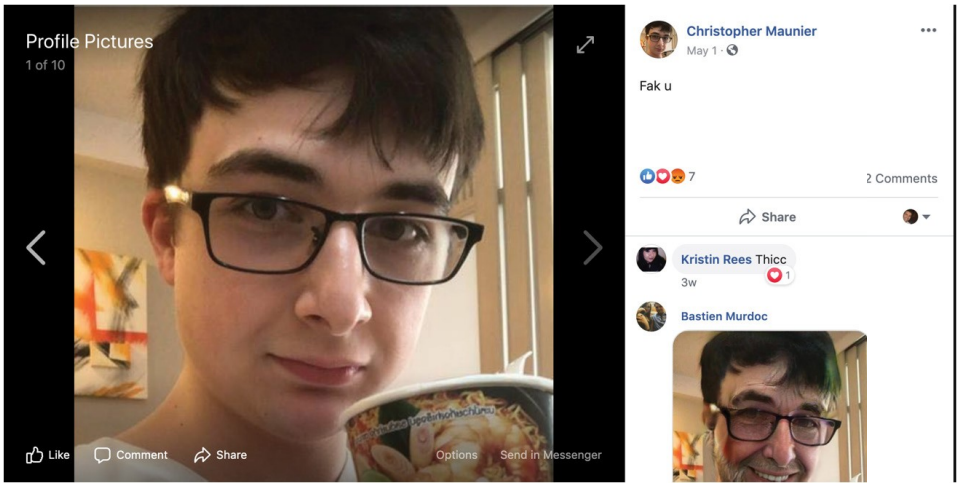


Рисунок 16.8

Если вы ищете профиль цели, я настоятельно рекомендую - нет, я *настоятельно призываем вас сохранять все фотографии, с которыми вы сталкиваетесь* . Однажды я ошибся сохраняя фотографию, предполагая, что я могу просто вернуться к профилю позже и взять картина, если бы я нуждался в этом. К сожалению, профиль был автономный режим, и я был COM- полностью не повезло. По сей день я до сих пор не могу поверить, что не сохранил фото. Не заставляйте та же ошибка, которую я сделал. Сохраните все (и правильно каталогизируйте свои папки, чтобы вы могли найти предметы позже).

На рисунке 16.9 показано использование API обратного поиска изображений Google. В
Единственный параметр, который нам нужно ввести, - это значение URL-адреса изображения.
Как вы можете видеть из ушка на рисунке 16.9, наши результаты поиска пустует.
Чтобы еще раз убедиться, что это не ошибка API, я вручную пропустил изображение через
Поиск Google Картинок и результаты были такими же. Как я уже сказал, я редко
вам повезет с обратным поиском изображений, но вы все равно должны попробовать.

Твиттер

Я не встречал ни одного злоумышленника или киберпреступника, у которого не было бы
хотя *бы* одна учетная запись Twitter. Twitter обычно содержит золотую жилу криминального мира.
активности, поэтому вам всегда следует выполнять исчерпывающий поиск учетных записей Twitter.
Продолжая наш предыдущий пример, мы уже знаем г-на «Монье».
связан с названием WhitePacket, так что давайте посмотрим, сможем ли мы придумать
что-нибудь. Чтобы начать поиск в Твиттере, нам нужно идентифицировать Твиттер цели.
Я БЫ. К счастью, в OSINT.rest есть поиск по API, который позволяет нам получить Twitter
ID от имени пользователя. На рисунке 16.10 показано «Получить идентификатор пользователя Twitter по псевдониму пользователя».
поиск со строкой запроса «whitepacket».

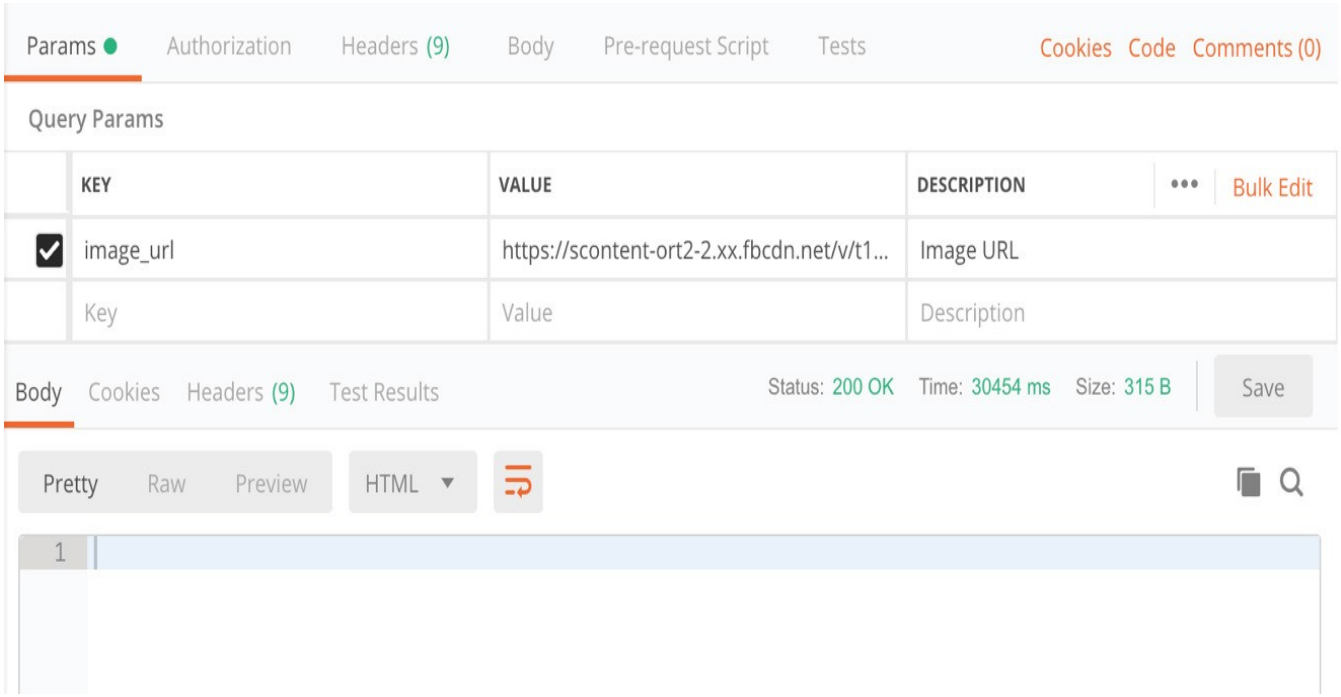


Рисунок 16.9

У нас есть совпадение - что на самом деле удивительно, потому что WhitePacket закрыл
несколько месяцев назад его аккаунт в Твиттере. Думаю, он решил запустить его обратно.
Теперь, когда у нас есть его идентификатор в Twitter, мы можем проводить всевозможные забавы и развлечения.
постоянный поиск, в том числе получение списков подписчиков и подписчиков.
К счастью, этот аккаунт довольно новый, поэтому у него не так много подписчиков.
На мой взгляд, это означает, что люди, за которыми он следит (или которые следят за ним)
Скорее всего, стоит изучить качественные контакты.
На рисунке 16.11 показан поиск для получения списка подписчиков Twitter на основе идентификатора Twitter.
Это так просто. Если бы он был целью, мы могли бы расширить наш поиск, чтобы также
получить списки твитов, которые ему понравились или которые он ретвитнул, и использовать их, чтобы собрать угрозу
актерская матрица.
Мы рассмотрели только несколько различных API поиска, доступных в OSINT.
отдыхаю, поэтому настоятельно рекомендую воспользоваться этой услугой.

SocialLinks: для пользователей Maltego

Многие, многие другие книги (исчерпывающе) охватывают Мальтего, поэтому я сделал
решение не включать его в эту книгу. Я лично не могу без этого жить, но я
подумал, что будет интереснее и выгоднее сосредоточиться на малоизвестных
инструменты и методы, которые потенциально могут принести больше пользы исследователям.
тион. При этом, поскольку в этом разделе обсуждается API OSINT.rest, я
хочу отметить потрясающие возможности плагина SocialLinks (который
по сути, версия OSINT.rest с графическим интерфейсом пользователя).

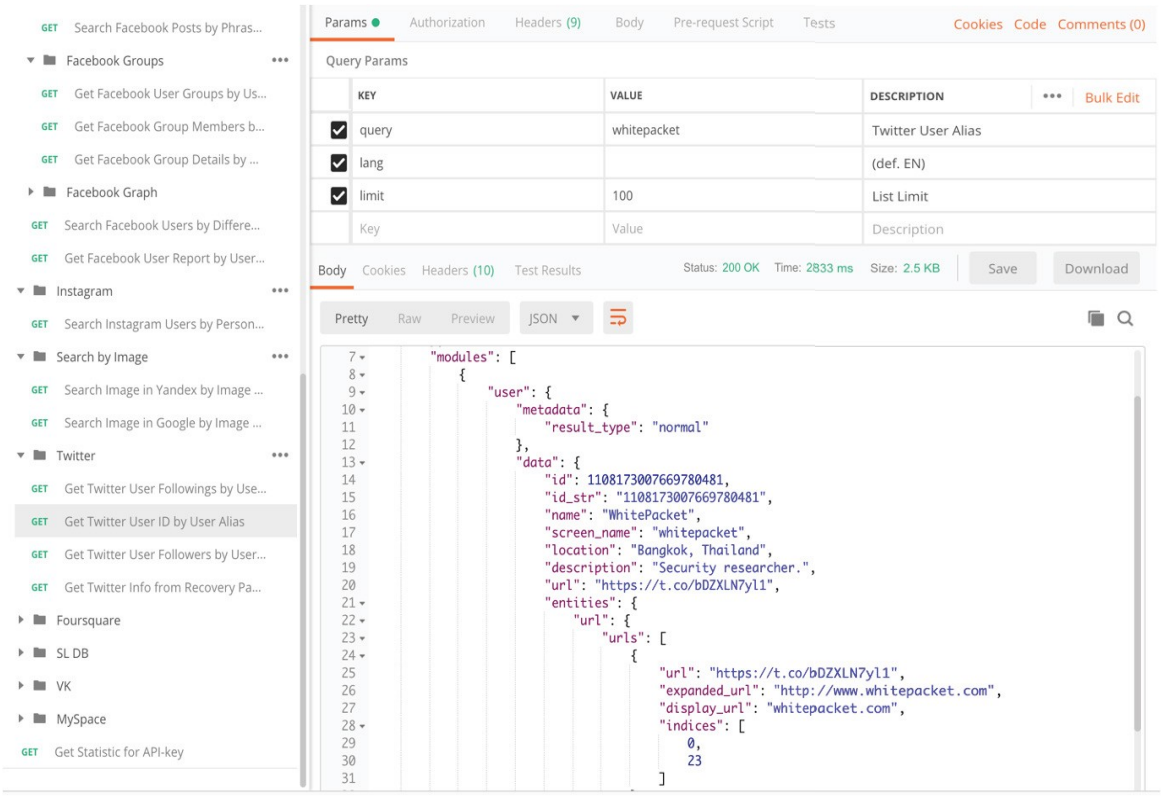


Рисунок 16.10

Чтобы проиллюстрировать два примера потрясающе полезного потенциала этого плагина, давайте выполните поиск по адресу электронной почты hackernike@live.ca. SocialLinks (с использованием тот же API, что и OSINT.rest) будет искать этот адрес электронной почты и автоматически Создавайте визуальные связи на основе любой найденной информации. Рисунок 16.12 показывает автоматически созданные подключения, связанные с нашим целевым адресом электронной почты. с помощью плагина SocialLinks.

Просто выполнив один поиск, мы можем увидеть две разные страницы MySpace, четыре разных учетных записи Skype, два IP-адреса и вымышленное имя. Это удивительно очень мощная штука!

В нашем последнем примере на рис. 16.13 показаны результаты использования SocialLinks. плагин в Maltego для поиска общедоступного адреса электронной почты WhitePacket, chris @ whitepacket.com.

Опять же, всего за один поиск мы можем увидеть столько информации: два Skype профилей, несколько ссылок на GitHub (одна для опубликованного трояна ZIB WhitePacket и ZLO Botnet), аккаунт Google и страницу Foursquare! Удивительный.

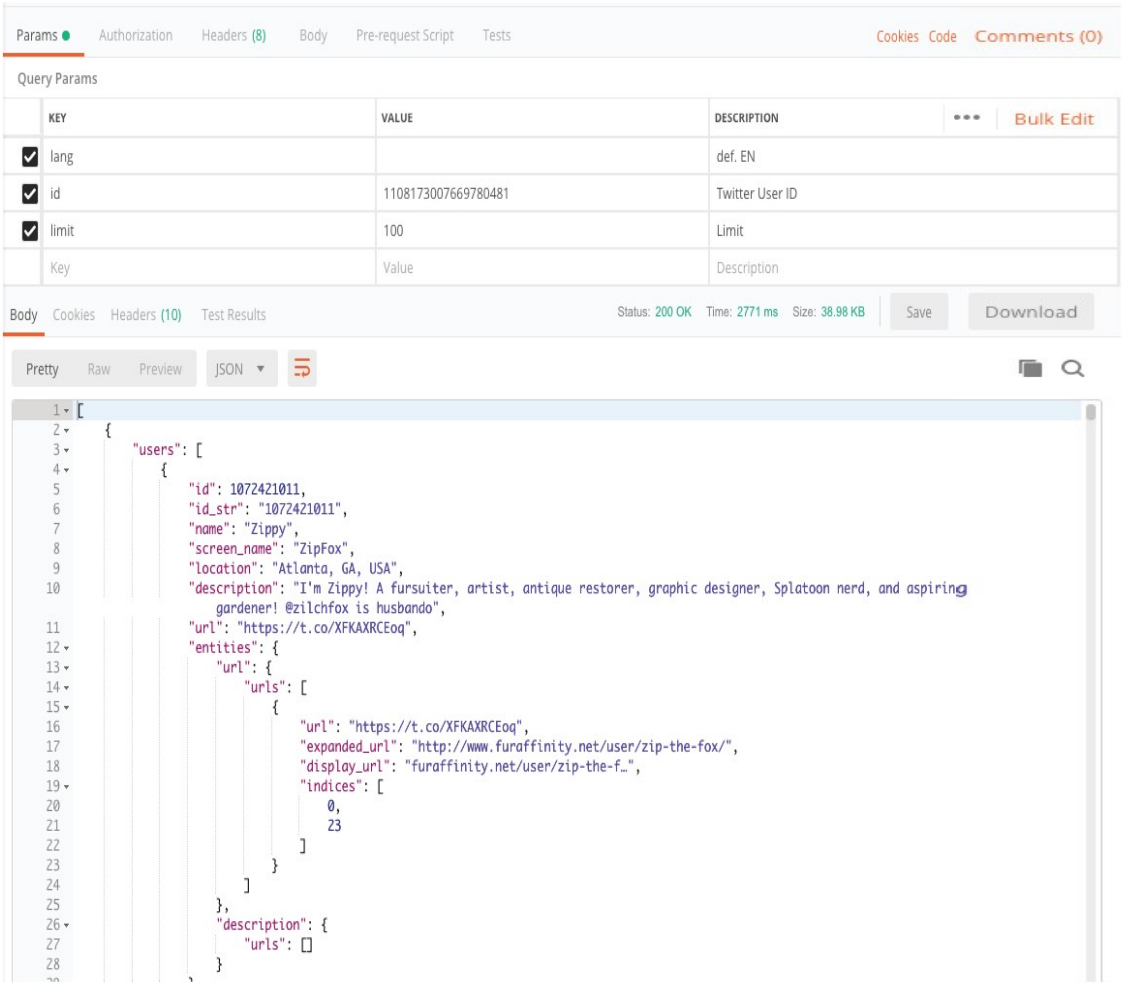


Рисунок 16.11

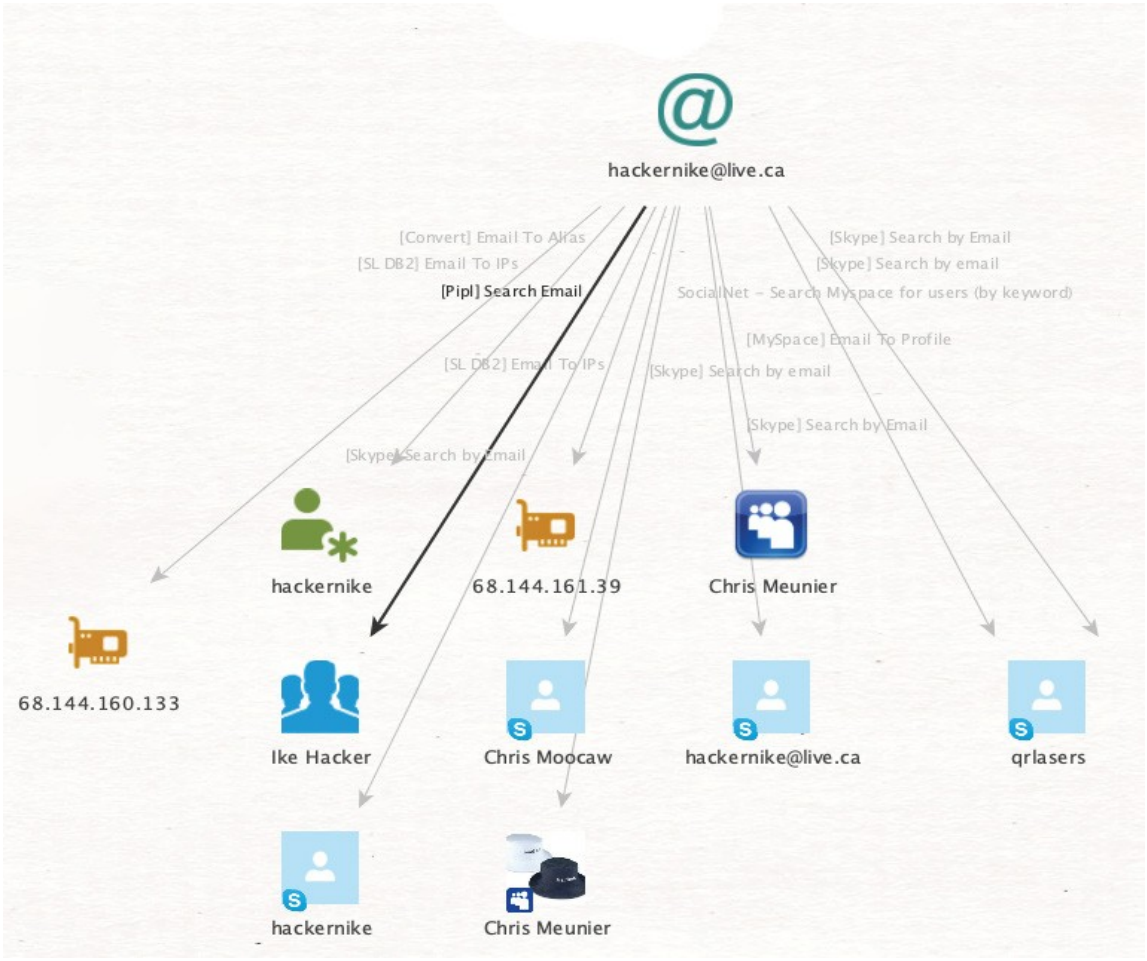


Рисунок 16.12

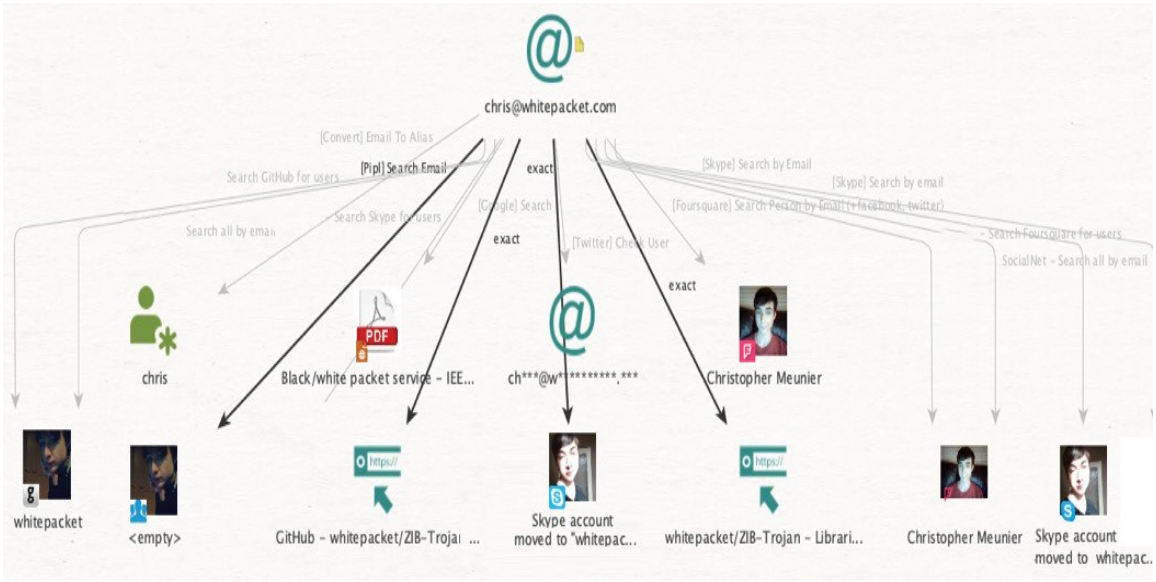


Рисунок 16.13

Skiptracer

Skiptracer - это инструмент Python, который использует базовый парсинг веб-страниц для компиляции пассивных информация о цели. У Skiptracer есть несколько модулей, которые собирают информация на основе номеров телефонов, адресов электронной почты, экранных имен, реальных имена (имя и фамилия), домашние адреса, IP-адреса, имена хостов, номерной знак номера и взломанные учетные данные веб-сайта (с использованием HIBP.com).

Модули электронной почты будут искать связанные учетные записи на основе вашей цели. адрес электронной почты на таких сайтах, как LinkedIn, HaveIBeenPwned, MySpace и AdvancedBackgroundChecks.

Модули имени будут искать имя и фамилию цели на таких сайтах, как Поиск правды, True People и AdvancedBackgroundChecks.

Телефонные модули выполняют поиск телефонных номеров в США (включая обратный поиск) на TruePeopleSearch, Who Called и 411.

com. Модуль номерных знаков будет искать общенациональную базу данных зарегистрированных Номерные знаки США.

Наконец, модуль экранного имени (имени пользователя) будет искать похожие имена пользователей. на таких сайтах, как Knowem и Namechk.

Вы можете бесплатно скачать Skiptracer на https://github.com/xillwillx/skiptracer .

Выполнение поиска

После запуска Skiptracer вы увидите справочное меню (показанное на рисунке 16.14). Оттуда вы можете выбрать, какой модуль использовать.

Поиск адреса электронной почты

Начнем с поиска адреса электронной почты. Нажатие 1 на вашей клавише - доска, находясь в главном меню, приведет вас к меню поиска по электронной почте (Рисунок 16.15).

Затем мы можем ввести любой целевой адрес электронной почты. Вернемся к предыдущему примеру и используйте hackernike@live.ca. По какой-то причине поиск в LinkedIn не работает. работа, что означает, что вы не можете искать «Все». Вместо этого мы должны запустить каждый модуль индивидуально. В этом примере давайте запустим поиск этого адреса электронной почты, используя вариант 3, который будет искать в электронном письме Троя Ханта, я был пойман (HIBP) (рисунок 16.16).

Вот результаты поиска по HIBP:

[?] HaveIbeenPwned
[+] Имя дампа: 000webhost
[=] Домен: 000webhost.com
[=] Нарушение: 01.03.2015



Рисунок 16.14

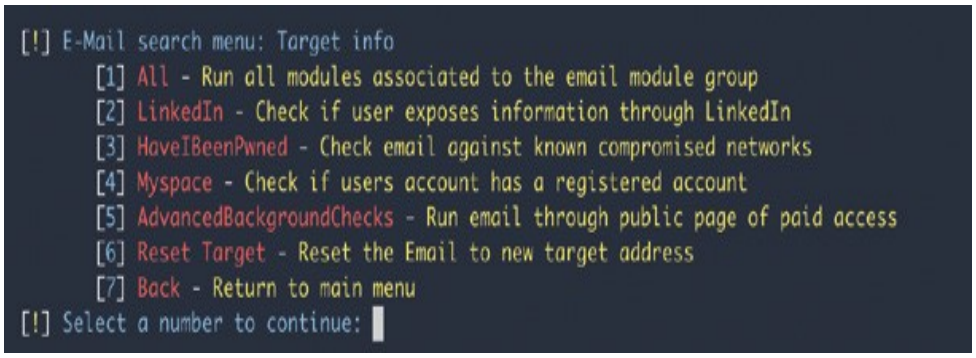


Рисунок 16.15

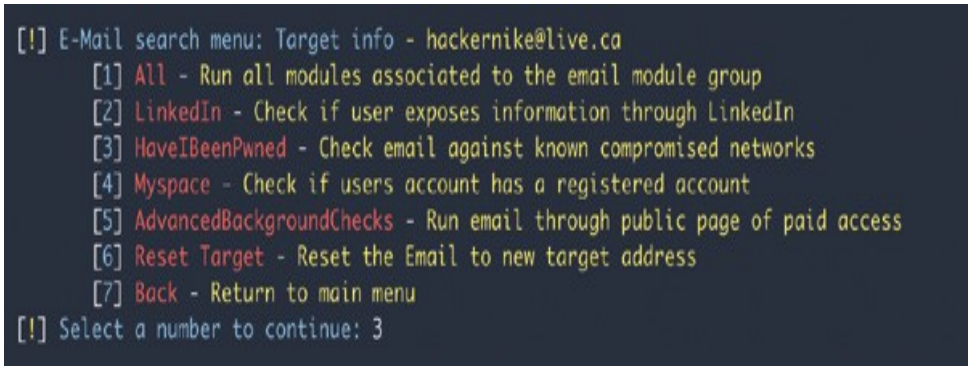


Рисунок 16.16

[=] Выставляет:
[-] DataSet: адреса электронной почты
[-] DataSet: IP-адреса
[-] DataSet: Имена
[-] DataSet: пароли
[+] Имя дампа: Adobe
[=] Домен: adobe.com
[=] Нарушение: 04.10.2013
[=] Выставляет:
[-] DataSet: адреса электронной почты
[-] DataSet: Подсказки для пароля
[-] DataSet: пароли
[-] DataSet: имена пользователей
[+] Название дампа: CashCrate
[=] Домен: cashcrate.com
[=] Нарушение: 17 ноября 2016 г.
[=] Выставляет:
[-] DataSet: адреса электронной почты
[-] DataSet: Имена
[-] DataSet: пароли
[-] DataSet: Физические адреса
[+] Имя дампа: DaniWeb
[=] Домен: daniweb.com
[=] Нарушение: 01.12.2015
[=] Выставляет:
[-] DataSet: адреса электронной почты
[-] DataSet: IP-адреса
[-] DataSet: пароли
[+] Имя дампа: MySpace
[=] Домен: myspace.com
[=] Нарушение: 01.07.2008
[=] Выставляет:
[-] DataSet: адреса электронной почты
[-] DataSet: пароли
[-] DataSet: имена пользователей
[+] Имя дампа: xat
[=] Домен: xat.com
[=] Нарушение: 4 ноября 2015 г.
[=] Выставляет:
[-] DataSet: адреса электронной почты
[-] DataSet: IP-адреса
[-] DataSet: пароли
[-] DataSet: имена пользователей
[-] DataSet: активность на сайте

Несмотря на то, что HIBP не покажет нам скомпрометированной информации, мы можем по-прежнему получать много информации, просто зная, *где* используется конкретный адрес электронной почты. Это будет особенно удобно в главе 17, когда мы будем обсуждать создание матрица субъектов угрозы и использование сброса пароля сайта для создания дополнительных улик

о наших целях. Между тем, на каждом из этих сайтов есть информация о
наша цель - иногда даже общедоступная информация, доступная на форумах или в социальных сетях
страницы СМИ.

Поиск номера телефона

Я до сих пор удивляюсь тому, сколько информации возвращается при поиске
номер телефона в Skiptracer. На рисунке 16.17 показан поиск по моему личному
сотовый телефон. Я заблокировал номер, но использую его в качестве примера, потому что
Хочу прокомментировать результаты.

Следующие (очень подробные) результаты отображаются при поиске
номер моего мобильного телефона. Я не буду показывать свою личную информацию, но я
чувствую, что было бы действительно полезно и информативно показать тип информации
отображается, и обсудите, действительно ли это.

Я заключил свои примечания в [скобки] рядом с каждым результатом:

[+] Псевдоним:
[=] Также известное как: Тория Винни
[=] Также известное как: Винни Троя
[=] Также известное как: Винни Троя
[=] Также известное как: Винченко Троя
[+] По теме:
[+] Сотрудник (ы):
[=] Известный сотрудник: *** [Человек, с которым я не разговаривал 15 лет]
[=] Известный сотрудник: *** [Удалено]
[=] Известный сотрудник: *** [Никогда не слышал об этом человеке]
[=] Известный сотрудник: *** [Никогда не слышал об этом человеке]
[=] Известный сотрудник: *** [мой ближайший сосед]
[=] Известный сотрудник: *** [раньше проживал по моему адресу]
[=] Известный сотрудник: *** [Никогда не слышал об этом человеке]
[=] Известный сотрудник: *** [член семьи]
[=] Известный сотрудник: *** [тетя]
[=] Известный сотрудник: *** [Удалено]
[=] Известный сотрудник: *** [бывший жена]
[=] Известный сотрудник: *** [Удалено]
[=] Известный сотрудник: *** [Удалено]
[+] Адрес:
[=] Текущее: ** [Точно]
[=] Предыдущая: ** [Неправильно]
[=] Предыдущая: ** [Неправильно]
[=] Предыдущая: ** [Точно]
[=] Предыдущая: ** [Точно]
[=] Предыдущая: ** [Точно]
[=] Предыдущая: ** [Точно]
[=] Предыдущая: ** [Неправильно]
[=] Предыдущая: ** [Неправильно]
[=] Предыдущая: ** [Точно]
[+] Телефон:
[=] #: *** Номера удалены
[+] Имя: Джессика ***
[+] Возраст: **
[+] Псевдоним:
[=] Также известное как: Джессика Троя (Моя жена)
[=] AKA: ***
[=] AKA: ***
[+] По теме:
[+] Сотрудник (ы):
[=] Известный партнер: *** [Accurate]
[+] Адрес:
[=] Текущее: ** [Точно]
[+] Телефон:
[=] #: ** Удалено
[?] AdvanceBackgroundChecks
[+] Имя: Винченцо Троя
[+] Псевдоним:
[=] Также известное как: Винни Троя
[=] Также известное как: Винни Троя
[=] Также известное как: Тория Винни [Weird]
[+] Телефон:
[=] #: ** Цифры удалены [некоторые точны]

[+] Электронная почта:
[=] Адрес: ** [Точно]
[=] Адрес: ** [Точно]
[=] Адрес: ** [Точно]
[=] Адрес: ** [Точно]
[=] Адрес: ** [Точно]
[=] Адрес: ** [Точно]
[=] Адрес: ** [Точно]
[=] Адрес: ** [Точно]
[=] Адрес: ** [Точно]
[=] Адрес: ** [Точно]
[=] Адрес: ** [Точно]
[=] Адрес: ** [Точно]
[=] Адрес: ** [Точно]

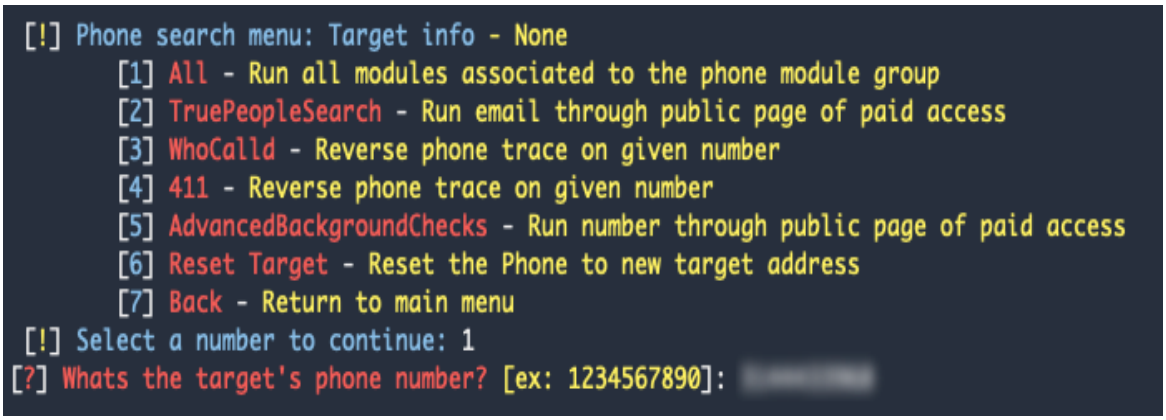


Рисунок 16.17

[+] Адреса:
[=] Текущий адрес:
[-] Улица: ** [Точно]
[-] Город: ** [Точно]
[-] Состояние: ** [Точно]
[-] ZipCode: ** [Точно]
[=] Пред. Адрес:
[-] Улица: ** [Точно]
[-] Город: ** [Точно]
[-] Состояние: ** [Точно]
[-] ZipCode: ** [Точно]
[+] Имя: ** [Точно]
[+] Телефон:
[=] #: ** [Точно]
[=] #: ** [Не помню]
[=] #: ** [Не помню]
[+] Электронная почта:
[+] Адреса:
[=] ** [Удалено]
[+] По теме:
[=] Известный родственник: ** [Удалено с точностью]
[=] Известный родственник: ** [Удалено с точностью]
[=] Известный родственник: ** [Неправильно удалено]

Независимо от того, сколько результатов было действительным или недействительным, это все равно довольно исчерпывающий список, составленный в результате единственного поиска!

Поиск имен пользователей

Поиск по имени пользователя будет проверять списки известных сайтов, чтобы узнать, существует ли URL-адрес. с именем пользователя на определенном сайте. Недостаток в том, что приложение не на самом деле проверить, если пользователь существует. Он показывает положительное совпадение, если есть - это появляющийся URL. Это означает, что если на сайте есть страница 404 или перенаправление, будет положительным матч. Многие другие инструменты (например, SpiderFoot и Intrigue. io) обеспечивают аналогичный поиск. Где бы вы ни решили запустить этот тип поиска, это абсолютно то, что вы должны делать для *каждого* имени пользователя, которое вы приходите через. Один положительный матч может открыть новый мир исследований для вас, и вы не можете сбрасывать со счетов тот факт, что актеры угрозы будут повторно использовать имена пользователей на несколько сайтов.

На рисунке 16.18 показан поиск пользователя cr00k.

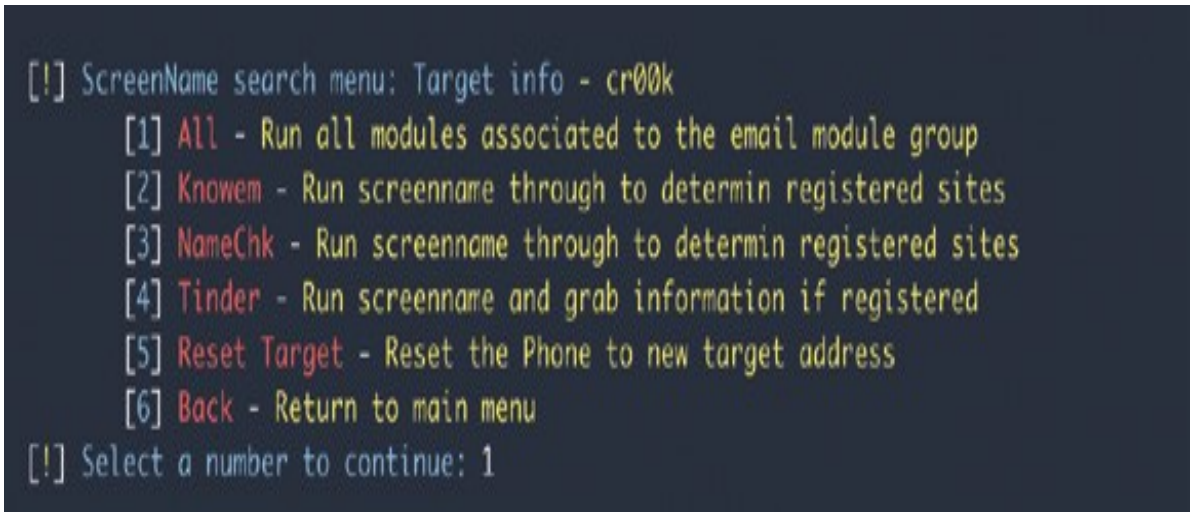


Рисунок 16.18

Я еще не много говорил о Cr00k (подробнее о нем в следующей главе).
Ослабляет), но он / его имя пользователя было связано с TDO в качестве одного из своих первых разносчиков данных.
Его имя было на хакерских форумах, и, как следствие, на всех связанных с TDO
отчеты об угрозах. Интересно, что реальный человек, стоящий за cr00k, был достаточно умен.
украсть имя пользователя другого кардера, что является его обычной тактикой.
Это очень умный ход, и его стоит остерегаться. Когда люди исследовали
имя cr00k, они неизбежно пойдут по пути дезинформации, введенной
размещать другими злоумышленниками с таким же именем.
Не только это, но и переключение и повторное использование имен в пределах одной и той же группы.
это очень распространенная тактика, используемая для создания замешательства. Вы обязательно должны оставить это в
ум, когда дело с длинной хронологией событий.

Поиск по имени пользователя для cr00k отображает следующие результаты:

```
[?] Какой экранный псевдоним цели? [пример: (Ac1dBurn | Zer0C00l)]: cr00k
[?] Ноем
[+] Аккаунт: Blogger
[+] Аккаунт: DailyMotion
[+] Аккаунт: facebook
[+] Аккаунт: foursquare
[+] Аккаунт: Imgur
[+] Аккаунт: LinkedIn
[+] Аккаунт: MySpace
[+] Аккаунт: Pinterest
[+] Аккаунт: reddit
[+] Аккаунт: Tumblr
[+] Аккаунт: Twitter
[+] Аккаунт: Typepad
[+] Аккаунт: Wordpress
[+] Аккаунт: YouTube
[?] Намечк
[+] Acct существует: https://facebook.com/cr00k
[+] Acct существует: https://www.youtube.com/cr00k
[+] Acct существует: https://twitter.com/cr00k
[+] Acct существует: https://www.instagram.com/cr00k
[+] Acct Exists: http://cr00k.blogspot.com/
[+] Acct Exists: https://plus.google.com/+cr00k/posts
```

```
[+] Acct существует: https://www.reddit.com/user/cr00k/
[+] Acct Exists: https://www.ebay.com/usr/cr00k
[+] Acct существует: https://cr00k.wordpress.com/
[+] Acct существует: https://www.pinterest.com/cr00k/
[+] Acct существует: https://cr00k.yelp.com
[+] Acct существует: https://github.com/cr00k
[+] Acct Exists: http://cr00k.tumblr.com/
[+] Acct Exists: https://www.producthunt.com/@cr00k
[+] Acct существует: https://steamcommunity.com/id/cr00k
[+] Acct существует: https://myspace.com/cr00k
[+] Acct существует: https://foursquare.com/cr00k
[+] Acct существует: https://soundcloud.com/cr00k
[+] Acct Exists: https://cash.me/$cr00k/
[+] Acct Exists: https://www.dailymotion.com/cr00k
[+] Acct существует: https://disqus.com/by/cr00k/
[+] Acct существует: https://www.deviantart.com/cr00k
[+] Acct существует: https://www.instructables.com/member/cr00k
[+] Acct существует: https://keybase.io/cr00k
[+] Acct Exists: https://www.kongregate.com/accounts/cr00k.
[+] Acct Exists: https://cr00k.livejournal.com
[+] Acct существует: https://angel.co/cr00k
[+] Acct существует: https://www.last.fm/user/cr00k
[+] Acct существует: https://www.tripit.com/people/cr00k#/profile
[+] Acct существует: https://fotolog.com/cr00k/
[+] Acct существует: https://imgur.com/user/cr00k
[X] Не удалось найти требуемые наборы данных.
[?] Трут
[+] Пользователь: cr00k
[X] Профиль не найден.
```

Опять же, высока вероятность того, что многие из них либо ошибочны.
человек или просто 404 страницы, но каждую обязательно нужно проверить.

Еще один поиск по имени пользователя

Просто для тщательности, а также потому, что мы не хотим, чтобы он чувствовал
опущены, давайте также запустим поиск по имени пользователя для CraftyCockney:

```
[?] Какой у цели экранный псевдоним? : Craftycockney
[?] Ноем
[+] Аккаунт: Blogger
[+] Аккаунт: Etsy
[+] Аккаунт: Hubpages
[+] Аккаунт: LinkedIn
[+] Аккаунт: MySpace
[+] Аккаунт: Photobucket
[+] Аккаунт: Pinterest
```

[+] Аккаунт: reddit
[+] Аккаунт: scribd
[+] Аккаунт: Tumblr
[+] Аккаунт: Twitter
[+] Аккаунт: Typepad
[+] Аккаунт: Wordpress
[?] NameChk
[+] Acct существует: https://facebook.com/Craftycockney
[+] Acct существует: https://twitter.com/Craftycockney
[+] Acct существует: https://www.instagram.com/Craftycockney
[+] Acct существует: http://Craftycockney.blogspot.com/
[+] Acct Exists: https://plus.google.com/+Craftycockney/posts
[+] Acct существует: https://www.reddit.com/user/Craftycockney/
[+] Acct существует: https://www.ebay.com/usr/Craftycockney
[+] Acct существует: https://www.pinterest.com/Craftycockney/
[+] Acct существует: https://Craftycockney.yelp.com
[+] Acct Exists: http://Craftycockney.tumblr.com/
[+] Acct существует: https://www.producthunt.com/@Craftycockney
[+] Acct существует: https://myspace.com/Craftycockney
[+] Acct существует: https://foursquare.com/Craftycockney
[+] Acct существует: https://www.etsy.com/people/Craftycockney
[+] Acct существует: https://soundcloud.com/Craftycockney
[+] Acct существует: https://disqus.com/by/Craftycockney/
[+] Acct Exists: http://photobucket.com/user/Craftycockney/
библиотека
[+] Acct существует: https://www.deviantart.com/Craftycockney
[+] Acct существует: https://www.instructables.com/member/
Craftycockney
[+] Acct существует: https://angel.co/Craftycockney
[+] Acct существует: https://www.last.fm/user/Craftycockney
[+] Acct существует: https://www.tripit.com/people/Craftycockney#/
[+] Acct существует: https://fotolog.com/Craftycockney/
[X] Не удалось найти требуемые наборы данных.
[?] Трут
[+] Пользователь: Craftycockney
[X] Профиль не найден.

При поиске имен пользователей обязательно пробуйте вводить общие буквы. учреждения. Например, аккаунт CraftyCockney в Твиттере на самом деле написан хитроумно. cockn3y. Это определенно может быть утомительным, но если вы не попробуете, вы многое пропустите. важные аккаунты. Теперь, когда мы знаем аккаунт Натана в Твиттере, беглый взгляд на тот, за кем он следует, сразу же говорит нам, что он увлекается видеоиграми, в частности, Assassin's Creed, Xbox и Ubisoft.

Userrecon

Userrecon - это простой скрипт Python, который ищет имена пользователей в 75 различных новые социальные сети. Он очень похож на используемые инструменты Knowem или Namechk. by Skiptracer в том смысле, что инструмент будет искать активные учетные записи по ряду разные сайты, проверяя URL.

Userrecon тестирует больше сайтов и дает более точные результаты, поэтому стоит попробовать. Когда скрипт завершает работу, он автоматически сохраняет результаты в текстовый файл, что невероятно полезно для каталогизации или импорта в другие приложения.

Вы можете скачать Userrecon через GitHub по адресу https://github.com/ thelinuxchoice / userrecon .

На рисунке 16.19 показан начальный экран Userrecon с поисковым запросом cr00k.

Userrecon возвращает следующие результаты:

[?] Введите имя пользователя: cr00k
[*] Удаление предыдущего файла: cr00k.txt
[*] Проверка имени пользователя cr00k на:
[+] Instagram: Нашел! https://www.instagram.com/cr00k
[+] Facebook: Нашел! https://www.facebook.com/cr00k
[+] Twitter: Нашел! https://www.twitter.com/cr00k
[+] YouTube: Нашел! https://www.youtube.com/cr00k
[+] Blogger: Найдено! https://cr00k.blogspot.com
[+] GooglePlus: Нашел! https://plus.google.com/+cr00k/posts
[+] Reddit: Нашел! https://www.reddit.com/user/cr00k
[+] Wordpress: Нашел! https://cr00k.wordpress.com
[+] Pinterest: Найдено! https://www.pinterest.com/cr00k
[+] Github: Найдено! https://www.github.com/cr00k
[+] Tumblr: Нашел! https://cr00k.tumblr.com
[+] Flickr: Найдено! https://www.flickr.com/photos/cr00k
[+] Steam: Нашел! https://steamcommunity.com/id/cr00k
[+] Vimeo: Не найдено!
[+] SoundCloud: найдено! https://soundcloud.com/cr00k
[+] Disqus: Нашел! https://disqus.com/cr00k
[+] Среда: Найдено! https://medium.com/@cr00k
[+] DeviantART: Найдено! https://cr00k.deviantart.com
[+] ВК: Нашел! https://vk.com/cr00k

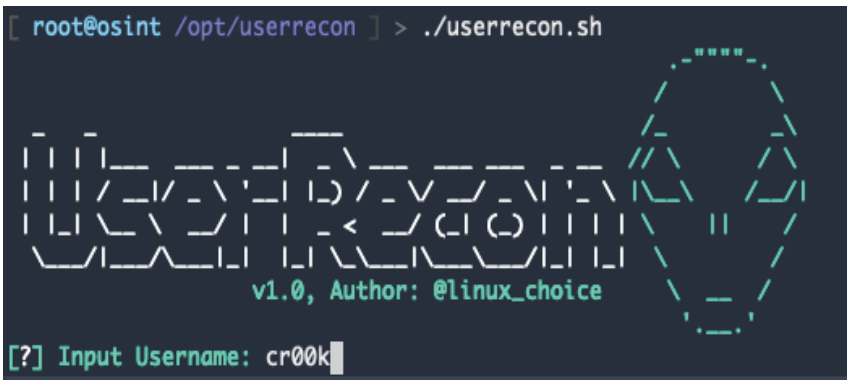


Рисунок 16.19

[+] About.me: Нашел! https://about.me/cr00k
[+] Imgur: Нашел! https://imgur.com/user/cr00k
[+] Flipboard: Нашел! https://flipboard.com/@cr00k
[+] SlideShare: найдено! https://slideshare.net/cr00k
[+] Фотолог: Нашел! https://fotolog.com/cr00k
[+] Spotify: Найдено! https://open.spotify.com/user/cr00k
[+] MixCloud: не найдено!
[+] Scribd: не найдено!
[+] Badoo: Не найдено!
[+] Patreon: Нашел! https://www.patreon.com/cr00k
[+] BitBucket: найдено! https://bitbucket.org/cr00k
[+] DailyMotion: найдено! https://www.dailymotion.com/cr00k
[+] Etsy: Нашел! https://www.etsy.com/shop/cr00k
[+] CashMe: Найдено! https://cash.me/cr00k
[+] Behance: Не найдено!
[+] GoodReads: не найдено!
[+] Инструкции: Найдено! https://www.instructables.com/member/cr00k
[+] Keybase: Найдено! https://keybase.io/cr00k
[+] Kongregate: Найдено! https://kongregate.com/accounts/cr00k
[+] Живой Журнал: Нашел! https://cr00k.livejournal.com
[+] AngelList: Найдено! https://angel.co/cr00k
[+] last.fm: Нашел! https://last.fm/user/cr00k
[+] Dribbble: Нашел! https://dribbble.com/cr00k
[+] Codecademy: Найдено! https://www.codecademy.com/cr00k
[+] Граватар: Нашел! https://en.gravatar.com/cr00k
[+] Pastebin: Найдено! https://pastebin.com/u/cr00k
[+] Foursquare: Не найдено!
[+] Роблокс: Найдено! https://foursquare.com/cr00k
[+] Gumroad: не найдено!
[+] Newgrounds: Найдено! https://cr00k.newgrounds.com
[+] Wattpad: Нашел! https://www.wattpad.com/user/cr00k
[+] Canva: Найдено! https://www.canva.com/cr00k
[+] CreativeMarket: найдено! https://creativemarket.com/cr00k
[+] Тракт: Нашел! https://www.trakt.tv/users/cr00k
[+] 500px: не найдено!
[+] Buzzfeed: Найдено! https://buzzfeed.com/cr00k
[+] TripAdvisor: найдено! https://tripadvisor.com/members/cr00k
[+] HubPages: Найдено! https://cr00k.hubpages.com/
[+] Содержательно: не найдено!
[+] Houzz: Нашел! https://houzz.com/user/cr00k
[+] blip.fm: не найдено!
[+] Википедия: Нашел! https://www.wikipedia.org/wiki/User:cr00k
[+] HackerNews: не найдено!
[+] CodeMentor: не найдено!
[+] ReverbNation: Нашел! https://www.reverbnation.com/cr00k
[+] Образцы: не найдено!
[+] Bandcamp: Не найдено!
[+] ColourLovers: не найдено!
[+] IFTTT: не найдено!
[+] Ebay: Нашел! https://www.ebay.com/usr/cr00k

[+] Slack: не найдено!
[+] OkCupid: Нашел! https://www.okcupid.com/profile/cr00k
[+] Поездка: Найдена! https://www.trip.skyscanner.com/user/cr00k
[+] Элло: Нашел! https://ello.co/cr00k
[+] Tracky: не найдено!
[+] Tripit: Найдено! https://www.tripit.com/people/cr00k#/profile/
основная информация
[+] Basecamp: не найдено!
[*] Сохранено: cr00k.txt

Судя по результатам, Userrecon ищет еще несколько сайтов.
чем другие инструменты, а также, кажется, лучше справляется с 404 и недействительными
страниц. Это отличный вспомогательный инструмент для проверки результатов и
все базы покрыты.

Reddit Investigator

Меня не перестает удивлять, сколько информации я в итоге нахожу на Reddit.
Люди публикуют сообщения на самые безумные темы - обычно вы можете найти злоумышленников в субред-
Диты, связанные со взломом, наркотиками и / или видеоиграми.
Одним из инструментов , стоит оставить в вашем получениях является www.redditinvestigator.com . В
сайт невероятно прост в использовании и предлагает как бесплатную, так и профессиональную версии.
На рисунке 16.20 показана домашняя страница Reddit Investigator, на которой нет
более одного поля поиска.
Если вы часто пользуетесь этим сайтом, профессиональная версия достаточно
недорого и позволяет также искать сообщения в кеше и просматривать записи в
промежутки времени. Возможность поиска кешированных (и потенциально удаленных сообщений)
стоит каждой копейки.
Подумайте об этом так: когда злоумышленник публикует сообщение о взломе
или чем-то, чем он хвастается, а через несколько недель решает удалить
это ценность возможности получить доступ к этим историческим данным позже, после того, как
было удалено огромно.



Рисунок 16.20

Результат поиска предоставляет статистику по пользователю, в том числе о том, какие под-
Reddits, на которых они публикуют, их очки кармы, за какие сообщения они голосуют, самые активные
часов и многое другое.

Давайте проведем поиск по нашему хорошему другу WhitePacket. Рисунки 16.21 и 16.22
показать полученную статистику панели управления из сообщений Reddit WhitePacket

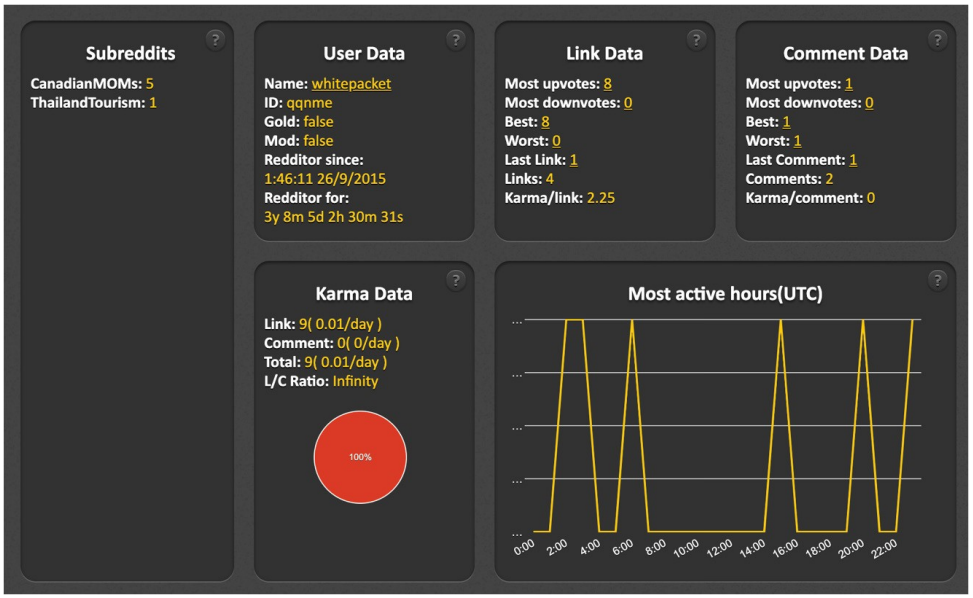


Рисунок 16.21



Рисунок 16.22

Глядя на эти данные, не похоже, что псевдоним WhitePacket очень активен.
на Reddit. Похоже, что большинство его постов находится в сабреддите под названием Cana-
dianMOMs. Прежде всего, это не порно-субреддит. Мама стоит
для марихуаны по почте.
Видеть, что! Что я говорил ранее о поиске людей, употребляющих наркотики или видеоигр
субреддиты?
Эта информация важна, потому что она позволит вам не только отслеживать
действия и интересы пользователей, а также видеть, с кем они взаимодействуют. Здание
профиль друзей и знакомых вашей цели может быть столь же важным, как и
построение профиля на актере. Один друг приводит к двум друзьям, а тем более
информация у вас есть, тем больше точек вы можете начать соединять.

Критический «мир» расследования TDO

Чтобы представить это в перспективе и дать реальный пример того, насколько полезен этот тип
информации может быть, самым критическим моментом моего расследования TDO был
когда я обнаружил, что пользователь cr00k на самом деле был «Peace of Mind» (он же «Мир»).
Как только я понял, что нужно искать Мира, я смог узнать, кто его друзья
и соратники были. Только тогда я действительно понял, кто
работал в TDO. К этому моменту (где-то в 2018 году) было больше
чем достаточно отчетов об угрозах, предполагающих, что Peace and Ping (владелец
Черт возьми, популярный форум хакеров даркнета) были одним и тем же человеком.
Предполагая, что эта информация верна (пока я не обнаружил обратное), я начал
исследования Пинга, всех его известных партнеров и всех основных игроков из
Ад. Это привело меня к необходимости найти исторические данные форума.
(который включал дампы и скрапы SQL). Как только у меня это было, я смог сформировать
фотография близких друзей Пинга основана на беседе на форуме.
Из старых сообщений на форуме Hell стало ясно, что Пинг и другой пользователь, Revolt,
были очень близкими друзьями. В какой-то момент во время пика внимания СМИ
окружающий ад, Пинг заявил, что дает полный административный контроль
восстать, пока «его не было».
Не знаю, как вы, но я не даю административного доступа ни к чему
если я действительно не доверяю человеку, которому я его даю. Имея это в виду, если мы
знает, что Peace, он же cr00k, является частью TDO, разве не логично, что он
также был связан с людьми, с которыми был действительно близок? Какое лучшее место для
начать искать чем Revolt?

Полное раскрытие информации, это не совсем то, как это произошло. Я действительно наткнулся
Название Revolt появилось намного раньше, до того, как я осознал идентичность cr00k.
Только когда я понял связь между cr00k и Ping, я смог
наконец соедините точки. История не является ложной или ложной, я просто написал ее таким образом, чтобы помочь
продемонстрируйте, почему так важно проявлять должную осмотрительность в отношении
друзья и известные соратники вашей цели.

Резюме

В этой главе были рассмотрены инструменты и методы, используемые для использования социальных сетей для помогите найти дополнительную информацию о вашей цели. Было бы невероятно редко, чтобы злоумышленник или цель не присутствует в социальных сетях. Скорее всего, они будет иметь более одной учетной записи на нескольких сайтах, поэтому важно исчерпать Тщательно сверяйте всю имеющуюся у вас информацию с как можно большим количеством социальных сетей. В следующих двух главах мы рассмотрим всю эту информацию и используйте его для построения матрицы субъектов угрозы. Веселье!!

377

17

Это, безусловно, моя любимая часть OSINT-процесса. Следующие две главы
подробно расскажу о моем процессе построения матрицы профилей злоумышленников. Что такое
Матрица профилей злоумышленников, спросите вы? По сути, это гигантский лист Excel, заполненный
несколько имен учетных записей, имена пользователей, поддельные профили, URL-адреса и другие личные
информация, относящаяся к цели. Это способ визуально упорядочить вашу учетную запись -
связанные данные в одном месте. Как только вы сможете это сделать, вы начнете замечать
закономерности в данных.
Мы будем использовать персонажей и персонажей из группы The Dark Overlord.
для наших примеров.

**В остальных главах основное внимание уделяется построению профиля киберугроз.
актера, что означает, что выбранная мной методология будет (в основном) ориентирована
к поиску такого человека. Если бы я искал обычного человека (т. Е. Не-
киберпреступник), я могу искать на разных платформах. Важный вывод - профессиональная
прием и техника.**

С чего начать (с TDO)?

Тебе нужно с чего-то начать, правда? Итак, если цель состоит в том, чтобы исследовать TDO (или любой другой
субъект угрозы), первый вопрос: «Что мы уже знаем?»

Отслеживание профиля и пароль Сбросить подсказки

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

Одна вещь, которую мы можем использовать в наших интересах, - это все внимание прессы и средств массовой информации.

что получил TDO. Изучая ранние новостные статьи, мы знаем, что украденный оригинал

данные продавались на нескольких различных хакерских форумах пользователем по имени Cr00k.

Рисунок 17.1 - это скриншот ветки продаж TDO Cr00k из России.

взлом форума Exploit.

Подобные темы продаж существуют на нескольких других форумах хакеров darkweb, в том числе

Ад, Siph0n и 0day. Чтобы было ясно, когда я говорю «похожий», я имею в виду точно такой же пост.

Если вы оказались на двух разных хакерских форумах и увидели одну и ту же публикацию

два разных человека, будет нетрудно предположить, что эти два пользователя

один и тот же человек или работает вместе.

На двух отдельных форумах даркweб пользователь «F3ttywap» (да, как и рэпер) может

быть связанными с Cr00k посредством публикации идентичного контента.

Здесь мы начнем собирать нашу матрицу отслеживания.

Построение матрицы профиля

В зависимости от сложности человека (или людей), которого вы ищете,

потенциально может быть довольно много данных для отслеживания. Я упомянул преимущества

визуально видеть все в одном месте или на одном экране, но

чем глубже вы погружаетесь в разгадку тайны чьей-то личности, тем меньше

вероятность того, что это возможно.

Следует помнить, что злоумышленники (особенно опытные)

будет иметь много разных аккаунтов и персонажей, поэтому, вероятно,

плохая идея разбивать эти данные по разным листам (вкладкам) Excel. В противном случае

информация будет беспорядочной, и вы вообще ничего не сможете увидеть.

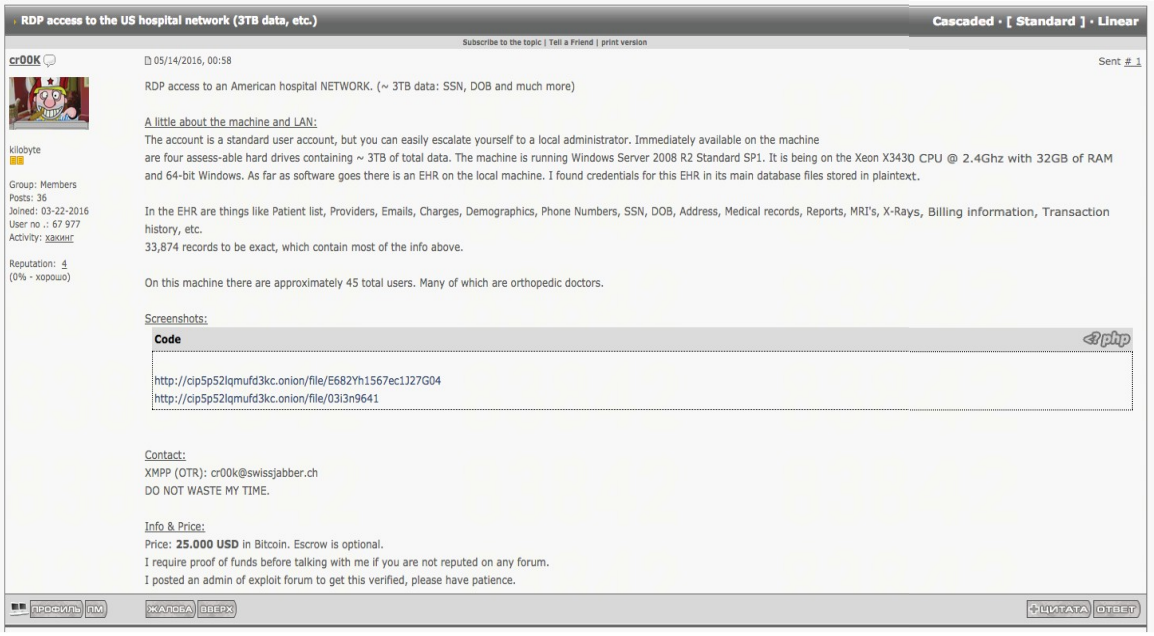


Рисунок 17.1

Помня об этом, я обычно начинаю со следующих трех вкладок в моем
матрица:

- Аккаунты
- Проверки
- Свалки

Каждый из этих трех разделов будет более подробно объяснен в следующем
две главы, но на высоком уровне: вкладка «Учетные записи» используется для определения того, какие
адреса электронной почты имеют учетные записи на определенных веб-сайтах; на вкладке "Подтверждения"
отслеживать информацию о сбросе пароля и проверочном вопросе; и свалки
Вкладка отслеживает данные, обнаруженные из дампов паролей и других взломанных данных (которые
это тема следующей главы).

Поиск по форуму

Первое, что нам нужно сделать, это поиск. Но где? К его чести, угроза
актер, стоящий за именами Cr00k и F3ttywap, был достаточно умен, чтобы использовать популярные
имена, у которых есть много существующих результатов поиска. Поиск в Google по запросу F3ttywap
даст нам массу информации о рэпере, которая нам не нужна.
Исследование злоумышленника в этих условиях чрезвычайно затрудняет
если вы не являетесь мастером техники доркинга.
Нам нужно сузить круг поиска, и, учитывая, что мы знаем имя F3ttywap
на форумах хакеров, лучшее место для поиска подсказок - это другой хакер
форумы.
Маловероятно, что у вас будет возможность пользоваться дорками и прочим расширенным поиском.
методы поиска соответствующих данных на форумах, потому что большинство хакеров
форумы требуют входа в систему (иногда платную) для просмотра их содержания. Но, как
со всем остальным иногда повезет. *Это один из тех случаев* .
Есть несколько явных форумов веб-хакеров, которые мы можем (и должны) просмотреть,
такие как HackForums.net , Nulled.to, RaidForums.com и OGUsers.com . Имея
некоторые псевдонимы для работы означают, что мы можем легко выполнить поиск в Google, используя
оператор "insite", или мы можем просто перейти на каждый сайт и найти сообщения или темы
содержащий это имя пользователя.
Начнем с поиска в Google, используя Nulled.to в качестве целевого сайта. Рисунок 17.2
показывает нам результаты следующего поиска:
'f3ttywap' на сайте: nulled.to

Первая ссылка ведет прямо на страницу его профиля: https://www.nulled.to/пользователь / 954035-f3ttywap . Проблема, как мы видим, в том, что учетная запись была обрезан (удален). То, что мы также можем видеть на рис. 17.3, очень важно.

Подробная информация заключается в том, что пользователь был забанен до того, как его учетная запись была удалена.

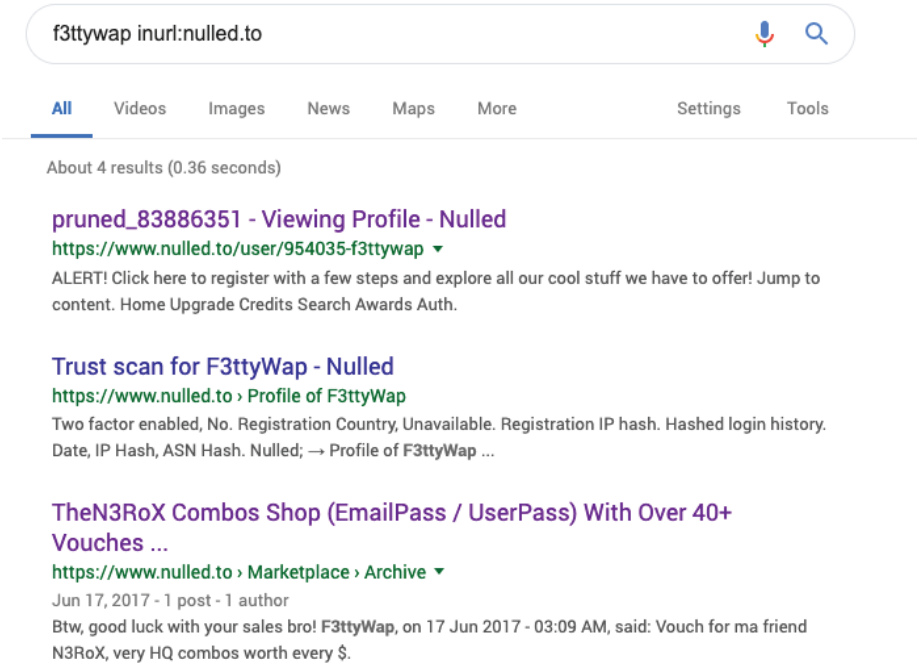


Рисунок 17.2

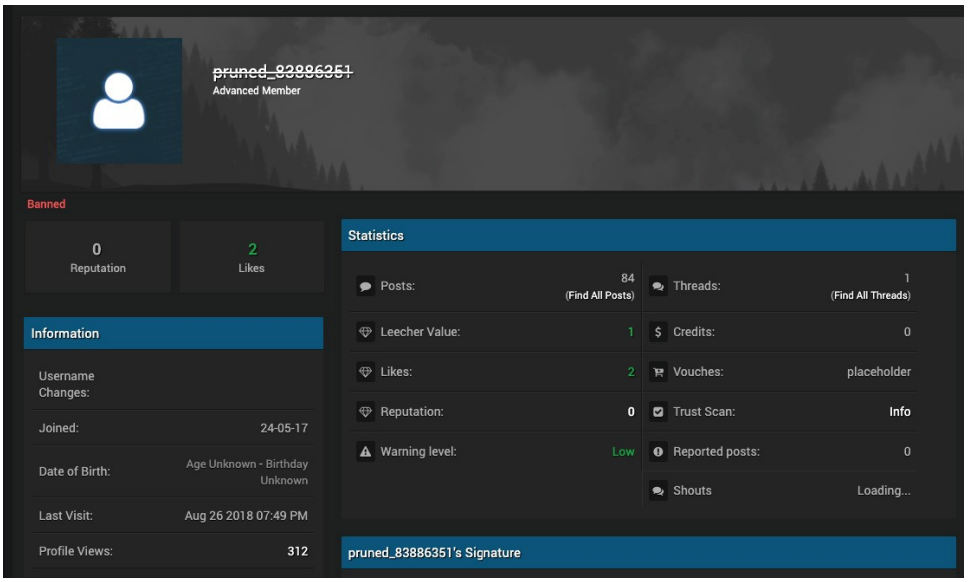


Рисунок 17.3

Списки запретов

На большинстве хакерских форумов есть *список запретов* , который представляет собой совокупный список пользователей, которые
были забанены с сайта. Как средство сдерживания мошенников от троллинга
свои сайты, большинство форумов будут публиковать зарегистрированный адрес электронной почты забаненного пользователя
рядом с забаненным именем пользователя (иронично, я знаю).
На рисунке 17.4 показан список запретов Nulled.to, доступ к которому можно получить с помощью команды «ban список »в нижнем колонтитуле сайта.
Поскольку мы знаем, что f3ttywap был забанен, мы можем с полным основанием ожидать, что
найдите его адрес электронной почты, просмотрев этот запретный список. Непосредственная проблема
заключается в том, что в бан-листе более 18000 страниц, и в нем нет функции поиска.
Для решения этой проблемы потребовался другой подход:
информация напрямую от одного из модераторов сайта.

Социальная инженерия

Возможность социальной инженерии вашей цели (или их партнеров) для извлечения
жизненно важная информация, скорее всего, будет необходимостью. Это конечно было
в этом случае. Прежде чем мы углубимся в подробности моей истории, давайте начнем с этого раздела.
со слов мастера социальной инженерии, г-на Человека-хакера,
Крис Хэднаги.

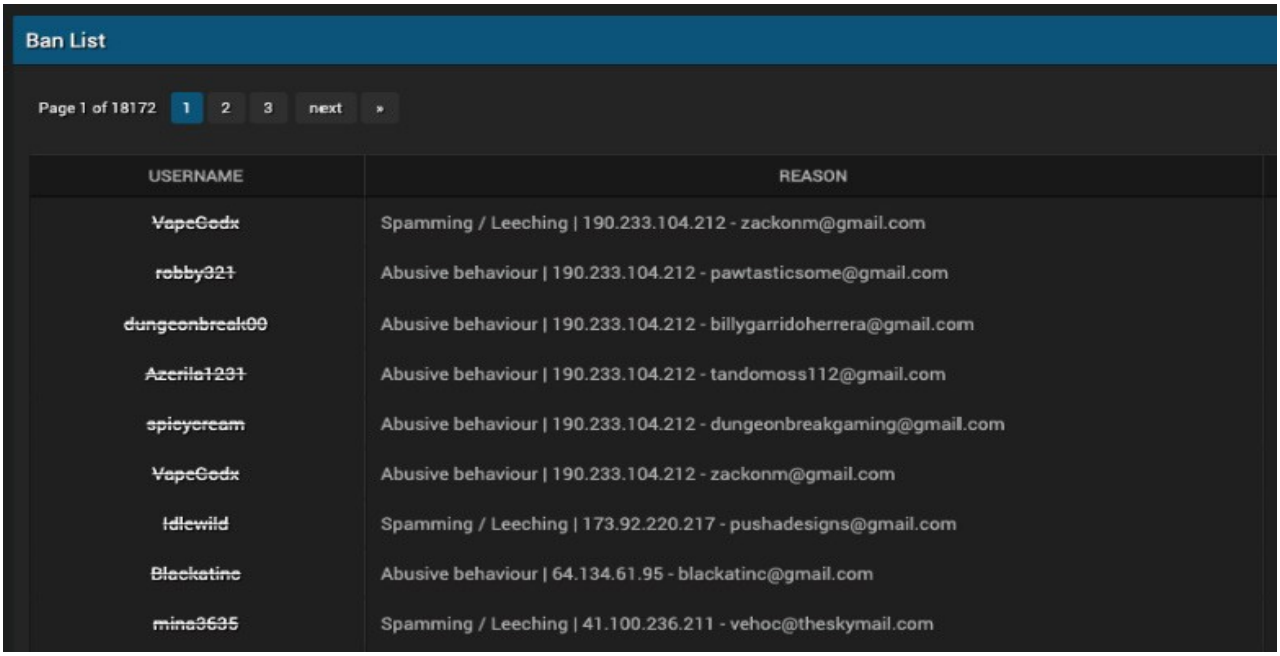


Рисунок 17.4

Недавно мы атаковали компанию, и нашей целью было проверить, сможем ли мы сбросить пароль. Для сброса пароля нам понадобился идентификатор сотрудника плюс ответ на один своих вопросов безопасности.
Мы работали так: сначала мы искали сотрудника, у которого были свои идентификатор сотрудника там. Либо изображение их значка, либо они его просто разместили ... где, потому что это была ошибка в электронном письме или цепочке писем или что-то в этом роде эффект. Мы нашли несколько.
Затем мы посмотрели на людей, которых нашли, и определили, много ли у них социальных присутствие в СМИ. Я не могу вспомнить точное количество, но допустим, мы нашли 10 человек, а затем пятеро из этих людей широко представлены в социальных сетях.
Затем мы зафиксировали эти пять, вызвали строку изменения пароля и сделали верю, что мы были одними из тех людей. Разговор был примерно таким: «Эй, это это Винни. Я сейчас в пути. Я не могу этого сделать, потому что я не за компьютером, но я мне нужно сбросить свой пароль, потому что я его забыл. Что мне понадобится позже? »
Каждый раз, без сомнения, человек на конце телефона говорил нам: «Вам понадобится идентификатор сотрудника плюс ответ на один из ваших секретных вопросов ». Тогда нам просто пришлось скажите: «О, чувак, я никогда не могу вспомнить, что я поставил для этих ответов. Что я сделал? »
Затем они обычно сообщают нам ответы на один или два из этих контрольных вопросов.
Без шуток, каждый раз.
Затем мы идем и просматриваем нашу информацию, которую мы доксировали, чтобы узнать, получили ли мы это лакомый кусочек. Если нет, найдите его, затем перезвоните позже, и когда мы перезвоним, у нас будет ответ.
Мы только что провели эту атаку на прошлой неделе, и она сработала безупречно. Мы смогли сбросить пароли из-за этого, что делает наш тест успешным.

В случае с F3ttywap я застрял и нуждался в связанном адресе электронной почты.
с его именем пользователя. Итак, я сделал то, что сделал бы любой уважаемый хакер, и зарегистрировал
на страницу поддержки сайта в Discord. Хотел бы я сохранить копию разговора,
но я этого не сделал.
Короче говоря, один из модераторов сайта хотел найти аккаунт для
меня. Думаю, я убедил его, что похожий пользователь меня сорвал, а я хотел сделать
уверен, что это был один и тот же человек. Он вернулся ко мне со снимком экрана аккаунта
таблица базы данных, показывающая адрес электронной почты kunt.x7@gmail.com. Админ был
также достаточно приятно, чтобы дать мне IP-адрес, который использовался для регистрации учетной записи!
Думаю, иногда все, что вам нужно сделать, это спросить!
Теперь, когда у нас есть больше информации для связи с нашим пользователем, мы можем начать
заполнение нашей матрицы субъектов угрозы. На рис. 17.5 показано, как выглядит моя таблица Excel.
нравится с этой информацией.

	A	B	C	D
1	Website	Email	Username	Notes
9	Nulled.to	kunt.x7@gmail.com	f3ttywap	95.85.176.212

Рисунок 17.5

Эта страница матрицы не должна быть чем-то чрезмерно сложным. Верно
теперь все, что мы делаем, это документируем найденные данные. Мы будем усиливать
поля на следующих страницах.

SE'ing Threat Actors: История «Аргона»

Пока мы говорим о социальной инженерии, я хотел бы вернуться к
наш хороший приятель Сайпер, и как я смог проникнуть на форум KickAss и
их внутренний круг.

Примерно в октябре 2018 года репортер службы безопасности написал обо мне рассказ под названием «Когда
Исследователи безопасности выдают себя за киберпреступников, кто может отличить? »

В то время я использовал псевдоним «SoundCard» на форуме KickAss и
выдавая себя за брокера данных. Автор статьи раскрыл мой псевдоним, и далее
быстро приведите участников KickAss в состояние повышенной готовности.

В статье упоминалось, что я изображал из себя брокера данных и предлагал продать данные.
утечка данных LinkedIn, и все это было правдой. Что меня действительно раздражало в
в статье рассказывается, как быстро автор бросил меня под автобус за то, что «бросил свое имя.
вокруг '', заявив, что я каким-то образом'' заставил его руку писать статью ''.
Я даже не понимаю, что это значит, но я предпочитаю не произносить его имя
потому что это только укрепит его веру в то, что я охотно говорю о его имени, например
какое-то ценное владение.
Реальность такова, что профессионалы разведки постоянно представляют угрозу киберпреступникам.
использовать их доверие к подпольным сообществам для получения ценных разведданных.
Это довольно распространенная практика, и у этого репортера не было проблем с чтением моих
информация из прошлого или информация из бесчисленного множества других аналитических данных об угрозах
фирмы и люди, которых он принимает ежедневно. Чем мои действия были другими?
Я спросил его, что на самом деле произошло в статье. Он написал мне по электронной почте, утверждая, что закрытие
деловой партнер сказал ему, что я сказал им, что он является соавтором этой книги, и
это как-то сбило его с толку.
Этого никогда не было. Учитывая контекст его заявления, я выяснил, кто
помощник был, и я вижу, как легко можно было запутать ситуацию. я
действительно сказал этому человеку, что репортер согласился дать комментарий приглашенного эксперта
в моей книге, как и несколько других людей. Это было больше похоже на то, что «следующие люди
предоставление гостевых взносов ».
В любом случае, я отправил этому репортеру электронное письмо, в котором он *принял мое приглашение* выступить в защиту
посмотрите комментарий к этой книге, и это был последний раз, когда я слышал от него.
Это был не первый и не последний раз, когда автор публиковал чьи-то личные
информации, возможно, потому, что он просто не согласился с их точкой зрения. В
в недавнем твите, этот репортер также опубликовал личную информацию о безопасности
исследователь NotDan, вызвавший крик в сообществе безопасности.

Суть этой напыщенной речи такова: будьте осторожны, сколько информации вы делитесь и с кем. Публикация чьей-либо личной информации может иметь серьезные последствия. Результат данной статьи, как мы увидим, положил начало цепочке событий, направленных на то, чтобы причиняя мне "боль".

Статья вызвала большой интерес на форуме KickAss и лично
сделал меня мишенью для атак. Когда все это рухнуло, Сайпер (он же АНБ),
администратор форума, решил назначить награду на моем сайте с помощью сообщения на форуме
«Владейте этим крысиным сайтом» (рис. 17.6).

Что касается публикации статьи, я не могу сказать, что ценю
Дело в том, что я был лично разоблачен. Есть последствия публичного разоблачения
чья-то личная информация, о чем свидетельствует следующее сообщение пользователя
«Глухой» (рис. 17.7).

К счастью, я один из тех, кто верит, что в каждом
проблема - и в этом случае я был прав.

Незаметно для всех у меня был второй псевдоним на форуме, «Аргон». На это
время, Аргон проходил процесс подачи заявки, чтобы быть принятым в Cyper's
личная хакерская группа. Конкурс против моего сайта оказался потрясающим
возможность. Какой лучший способ отточить свои навыки хакера-ниндзя в черной шляпе, чем
чтобы *взломать мой собственный сайт* ?

Так я и сделал.

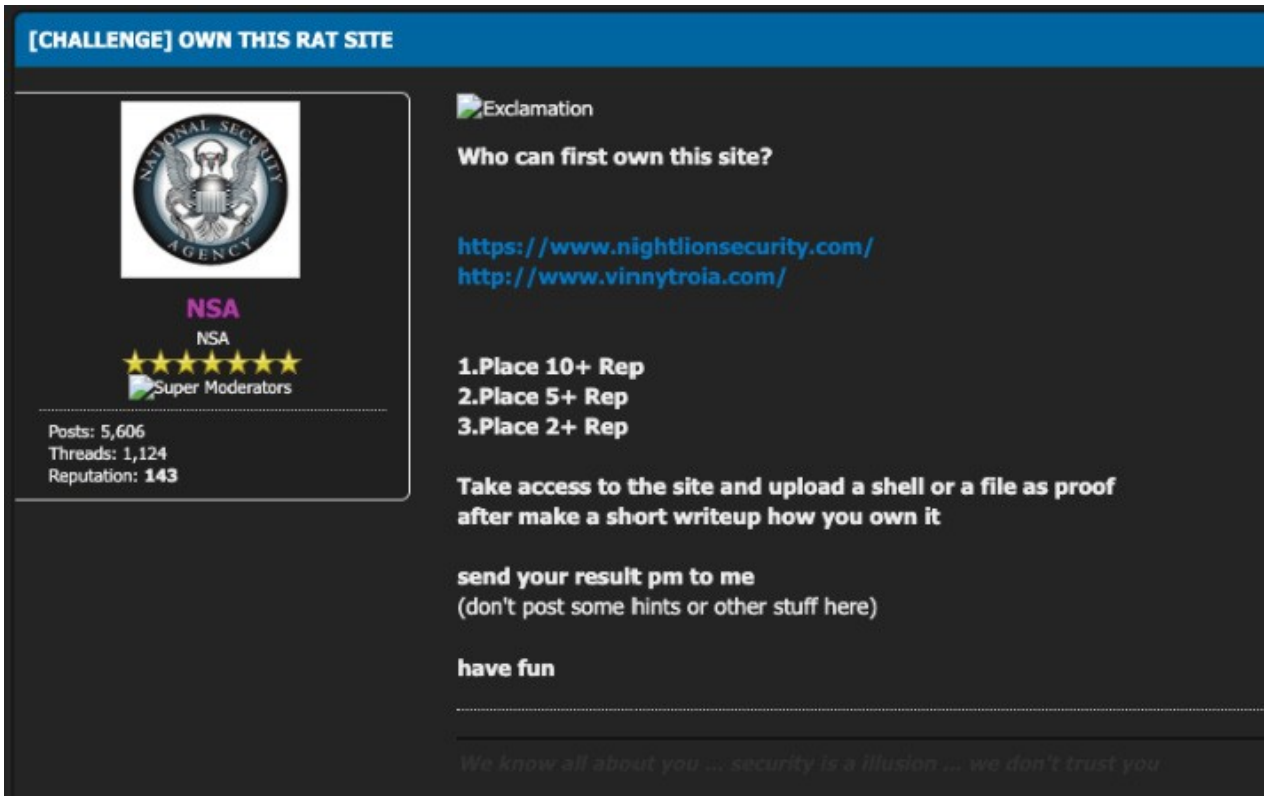


Рисунок 17.6

Я установил устаревшую панель PHPMyAdmin в удаленном каталоге на одном из моих
места. Любой, кто выполняет реконструкцию сервера и перебор каталогов с помощью Wfuzz
(как описано в главе 7) смогли бы его найти.

Моя легенда была простой. Как только я нашел панель, я провел широкий поиск
любые комбинации адреса электронной почты / пароля, которые можно найти в моем электронном письме
адреса (этот метод будет рассмотрен в следующей главе).

Я установил для входа в PHPMyAdmin более старую комбинацию имени пользователя и пароля из
случайная утечка данных. Используя пароли, «обнаруженные» в результате различных утечек данных,
Я сделал вид, что получил доступ путем перебора панели PHPMyAdmin.

Чтобы доказать, что я был там, я «взломал» свой собственный сайт WordPress, напрямую изменив
fing таблицу базы данных WP и заменил первую страницу показанным изображением
на рисунке 17.8.

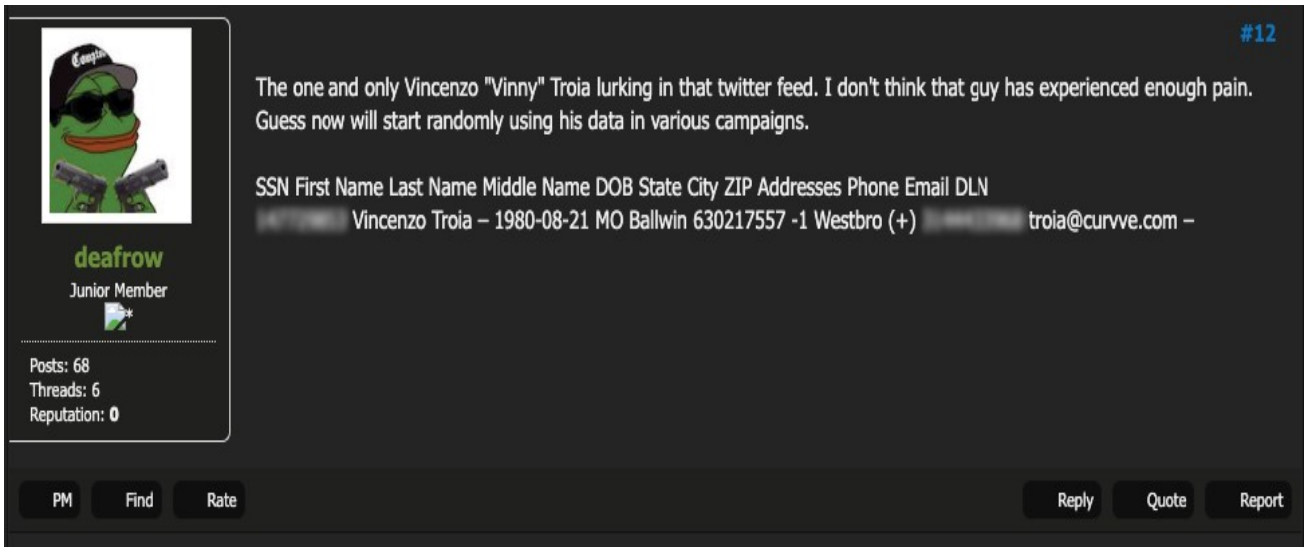


Рисунок 17.7

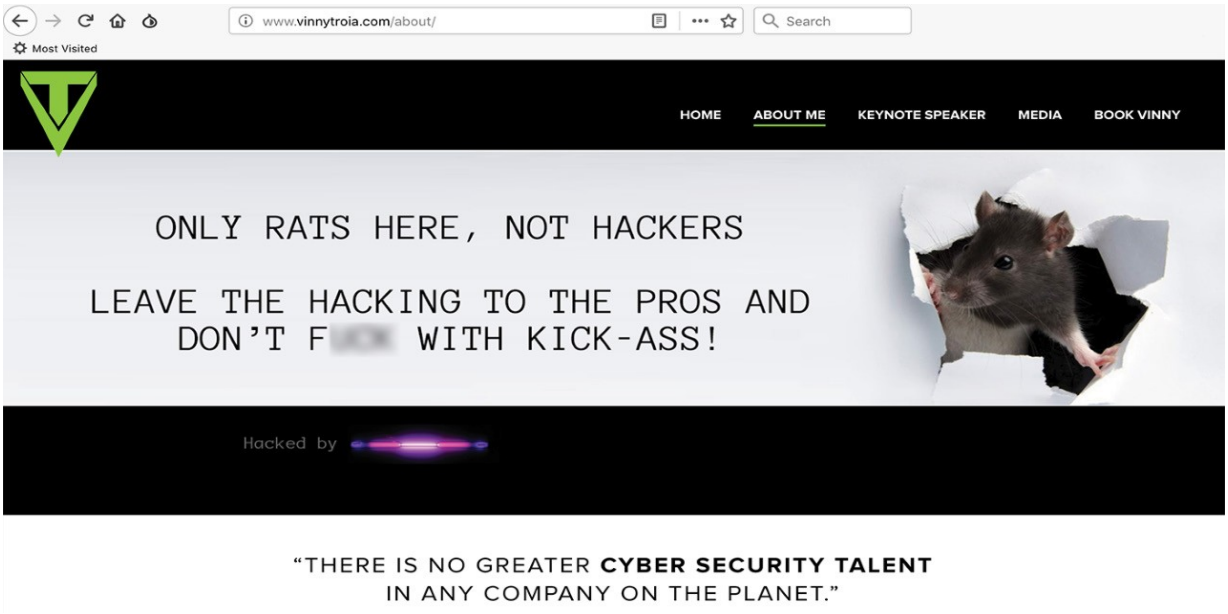


Рисунок 17.8

Но зачем останавливаться на достигнутом? Я предположил, что Сайпер и его команда захотят лично
проверяйте доступ и авторизуйтесь сами, поэтому перед моим объявлением о победе
Я взял на себя смелость установить строгие правила брандмауэра на моем сервере, предназначенные для
полностью заблокировать любые соединения с известным TOR, IP-адресом VPN, прокси или другим
известные плохие IP-адреса. Затем я настроил ведение журнала для отслеживания любых входящих подключений.
Когда ловушка была расставлена, я сделал праздничный пост в ветке конкурса на форуме.
(Рисунок 17.9).
Неплохо, правда? Сколько людей ожидают, что кто-то взломает их собственные
Веб-сайт?
АНБ задавало мне много вопросов о том, как мне это удалось, и все они
был вполне правдоподобным; и это сработало!
АНБ и его команда весело провели время, войдя в систему и поиграясь с моей панелью, и
в качестве награды я должен был записать всю информацию об их IP. URL-адрес PHPMyAdmin
был настолько непонятным (и таким новым), что любые обращения были явно актуальными, что
включали внезапно появившихся фальшивых ботов-парсеров.
Суть этой истории в том, что если вы собираетесь атаковать цель, зачем сдерживаться?
Иногда самые смелые идеи оказываются лучшими .

**Когда вы начинаете говорить о op-sec для злоумышленников, это не просто вопрос op-sec.
с точки зрения заставить их открыть любой старый документ и использовать его для
надеюсь собрать некоторую информацию о них. Все дело в правильной наживке.
За годы работы я узнал (довольно давно), что *поддельные документы выглядят
подделка* . Если вы действительно можете поместить элементы отслеживания в настоящий документ, это много
лучше.**

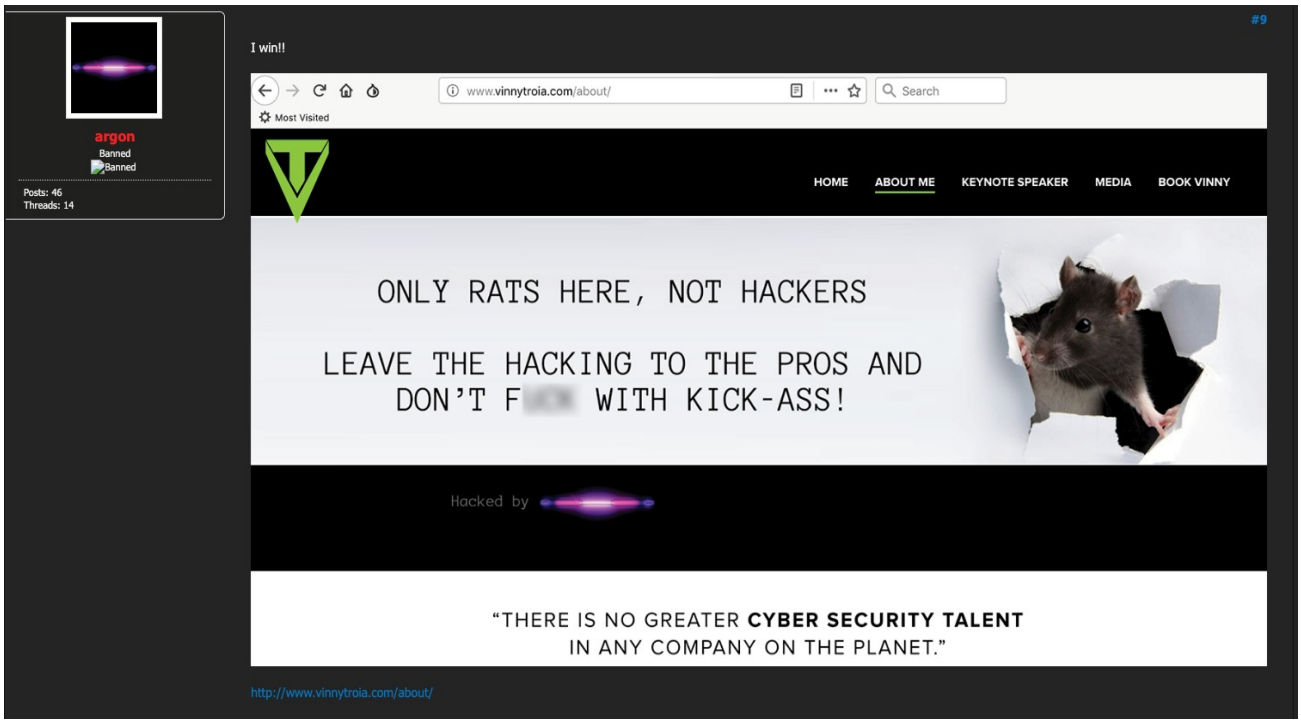


Рисунок 17.9

Макросы напугают противника. Если вы попытаетесь вставить макрос в документ, они не собираюсь его открывать. Если вы попытаетесь поместить макрос в электронную таблицу Excel, ну, макросы всегда в таблицах Excel. . . так они собираются его открыть или нет? Это ди-
Другой сценарий.
С другой стороны, если вы попытались добавить ссылку на каскадную таблицу стилей (CSS), или тег источника изображения в метаданных документа, ваша вероятность их фактического открыть этот документ и вернуть его обратно стало намного лучше.
Некоторые из моих любимых идей, как заставить злоумышленников управлять вещами, пришли вплоть до действительно простых идей. Просто создайте что-то вроде каталога на веб-сайте, который говорит VPN, и у вас есть исполняемый файл, который выполняет автоматическую настройку VPN, а затем вы создаете этот исполняемый файл с его собственной функцией обратного вызова. Или вы даже можете цифровой подсчитайте, подпишите этот исполняемый файл, затем дождитесь каких-либо поисков по этому сертификату подписи цифрового кода.
icate всякий раз, когда он запускается, или всякий раз, когда кто-то пытается запустить исполняемый файл.
Это скорее проблема выхода за рамки традиционного документооборота, но на самом деле союзник использует правильную приманку, чтобы попытаться заставить этого человека открыть этот конкретный документ - элементы, а затем взаимодействуют с компонентом, который вы создали, чтобы привлечь их.

Каждый получает SE'd - урок усвоен

Если вы обращаете внимание на историю, в какой-то момент вы можете спросить себя: "Подожди секунду. В статье ваше имя было обозначено как «SoundCard», но не было упоминание об Аргоне. Как это имя появилось? » Что ж, как ни странно, я был SE'd. В разгар всего ажиотажа Сайпер решил прыгнуть в Твиттер и перезвонить. в разговоре между мной и Кребсом. На рисунке 17.10 показана копия Cyper's сообщение со страницы Twitter KickAss_Sec (которая с тех пор была закрыта).

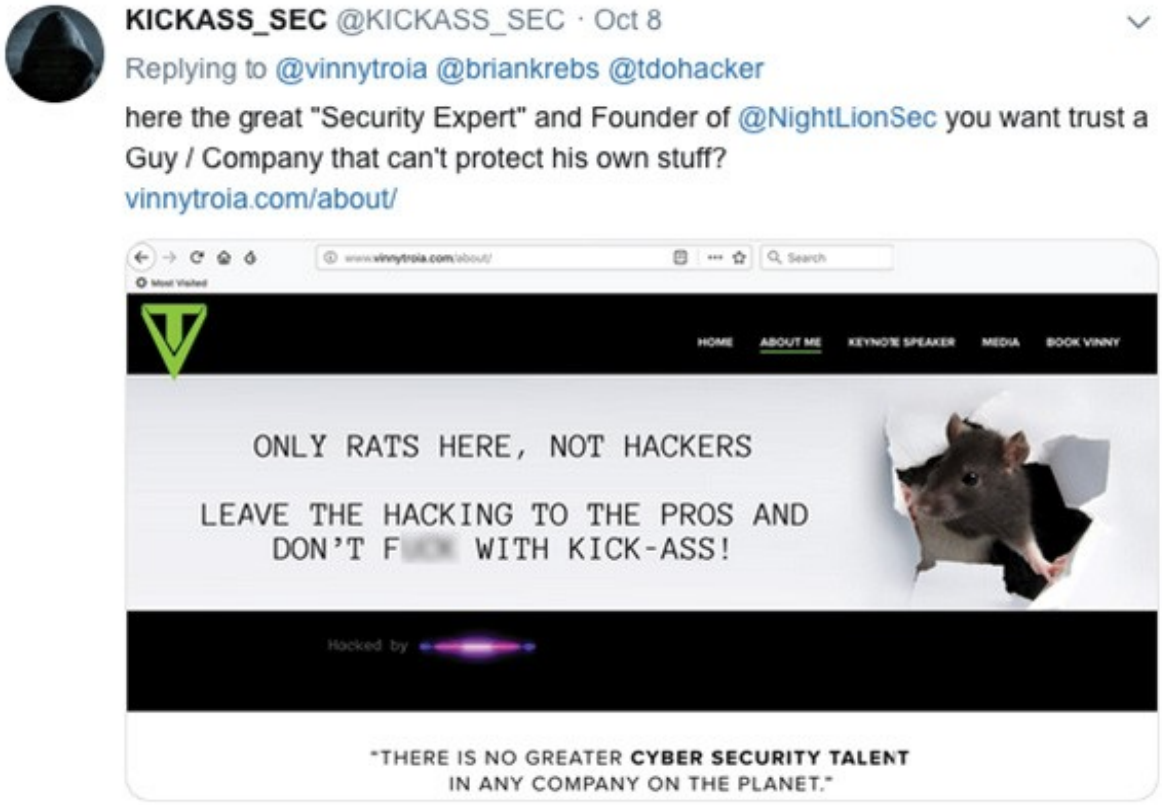


Рисунок 17.10

Где-то в этом жарком разговоре в Твиттере Сайпер обронил промо для
форум KickAss (но использовал старый URL, который я сразу узнал). я
щелкнул ссылку, чтобы узнать, что произошло и почему он будет использовать старый адрес.
В моем браузере TOR были сохранены файлы cookie, и я сразу вошел в старую
KickAss URL как Argon.
Хорошо сыграно, сэр.
Мораль истории - не храните файлы cookie в TOR и *не спешите*
переходите по ссылкам ! (Да, правда?)

Конец TDO и форума KickAss

В моем официальном отчете о TDO я предлагаю теорию о том, что форум KickAss, который
был официальным домом для Темного Повелителя, но в конце концов покинул его из-за тщательно продуманной
выйти из жульничества.

. *Мошенничество с выходом* (по крайней мере, в этом контексте) вовлекает владельца темной паутины.
Кетплейс внезапно закрывает сайт и оставляет все деньги на депонировании
учетная запись.
Торговые площадки Darkweb продают нелегальные товары (обычно наркотики) и работают на условном депонировании.
система. Покупатель оплачивает свои товары криптовалютой, которая затем хранится в
счет условного депонирования сайта. Когда покупатель получает товары, они подтверждают
получение товара и передача денежных средств продавцу.
В мошенничестве с выходом, когда на торговой площадке достаточно транзакций и хранятся деньги,
счет условного депонирования, администратор закроет сайт, сохранив все деньги и
винить продавцов.
Я считаю, что именно поэтому форум KickAss в конечном итоге закрылся.

Последняя медиа-кампания TDO включала утечку информации о страховании.
от теракта 11 сентября, названного «украденными газетами об 11 сентября». Каждый слой при отпускании
содержал другой набор *бесполезных* страховых документов. Группа использовала эту тактику
чтобы заманить СМИ в надежде привлечь внимание, охотясь на теоретиков заговора 11 сентября.
Это сработало . . . на короткое время.
Каждый уровень документов содержал ключ PGP для проверки правильности данных.
законно исходящий от TDO, а также содержал следующие официальные
Контактная информация:

КОНТАКТНАЯ ИНФОРМАЦИЯ И МЕСТОПОЛОЖЕНИЕ:
Электронный адрес thedarkoverlord: tdohackers@protonmail.com
Адрес электронной почты Backup1: thedarkoverlord@msgsafe.io
Адрес электронной почты Backup2: thedarkoverlord@torbox3uiot6wchz.onion
Сделайте свой на (torbox3uiot6wchz.onion)
KickAss Tor Адрес: kickassugvgoftuk.onion

Как интересно, что TDO вдруг станет продвигать форум KickAss.
Еще более интересным было то, что они продвигали *старый* URL (
тот же, на который я случайно щелкнул ранее в этой главе).

Стоимость членства в форуме сейчас взлетела до 600 долларов. Я считаю
это был способ группы использовать бренд TDO и прессу о событиях 11 сентября для привлечения дополнительных деньги в регистрации на сайте.
После того, как пресса, окружавшая информацию об 11 сентября, иссякла (т. Е. Люди посчитали, что
данные были совершенно бесполезны), форум закрылся типичным выходом-мошенничеством
моды, сохраняя заработанные деньги и загружая новых пользователей.
Но, увы, сайт фактически не закрыли. *Частный URL* по- прежнему сохраняется,
несмотря на то, что некоторые блоги и данные об угрозах подтверждают, вне всякой тени
есть сомнения, что сайт был заблокирован правоохранительными органами.
На рисунке 17.11 показан ответ АНБ (Сайпера) на закрытие сайта по закону.
исполнение. Обратите внимание, что это 30 января 2019 г., через несколько недель после публикации.
статей о закрытии и отчетов о законном закрытии сайта.
И в ответ на ветку / комментарий на рис. 17.11 АНБ выпустило еще
подробное сообщение о простое сайта (рисунок 17.12).

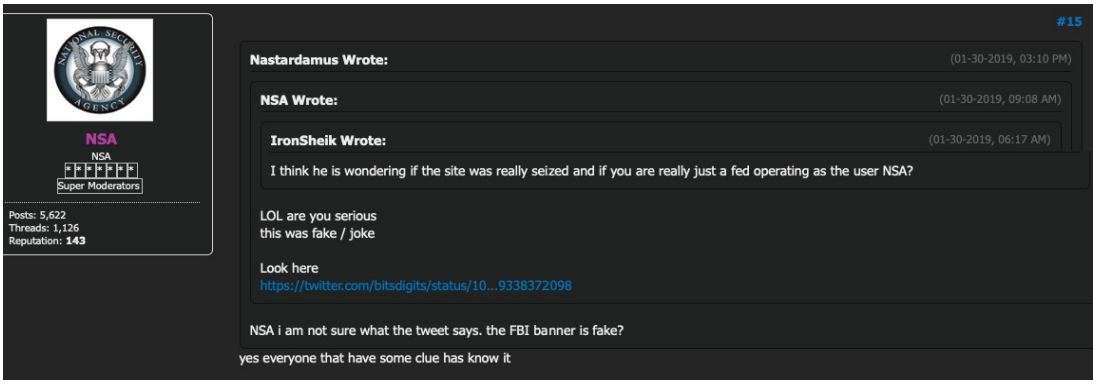


Рисунок 17.11

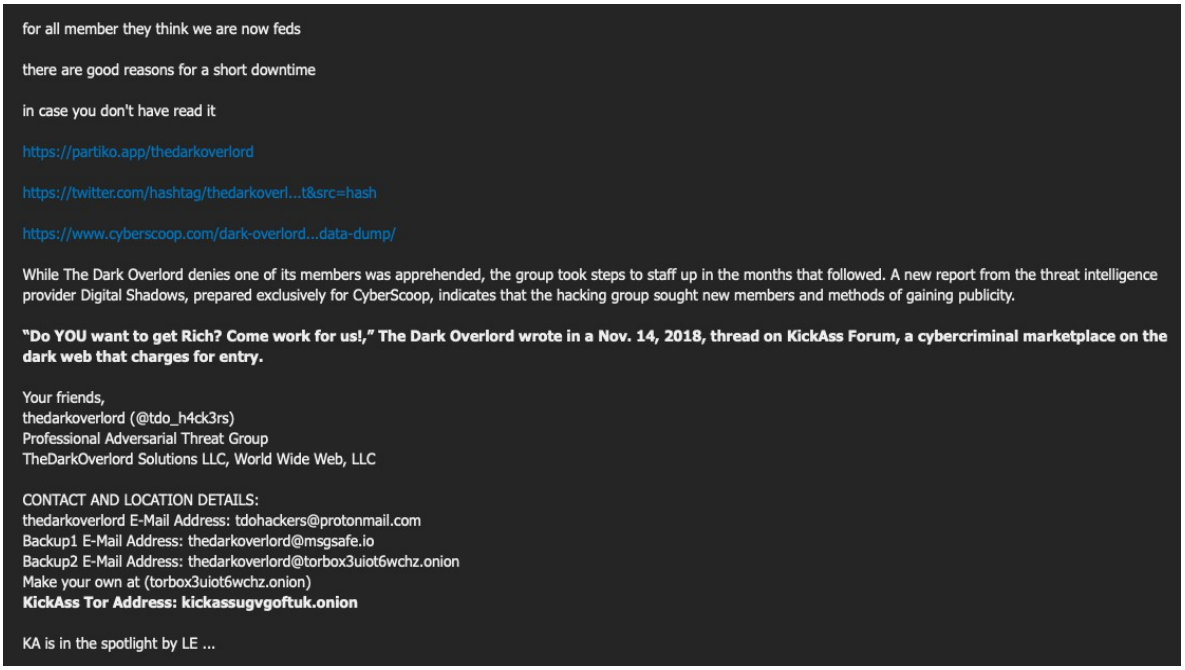


Рисунок 17.12

Но все в конце концов должно прийти к концу, и примерно через месяц
сайт явно закрыт навсегда. . . а может и нет?

Как ни странно, несколько дней назад мой друг разговаривал
со случайным злоумышленником, и всплыло мое имя. Ниже приводится стенограмма
их разговора.

X: Ты знаешь, вернулась ли еще крутая фигня?
X: я нигде не могу найти АНБ или ад
XXX: Имо, пизда не вернется
X: ой
X: они открывают новый сайт?
X: или все это дерьмо TDO?
X: похоже, они занимались мошенничеством на выходе
XXX: Со всем дерьмом, которое обрушилось на Кребса / Троя, все на
Пауза
XXX: Я думаю, это было связано с Тдо
X: что упало с krebs / troy?
XXX: В любом случае это то, что я слышал
XXX: хорошо
XXX: меньше их, больше того парня Винни Троя
XXX: троя *
X: ох, статья
X: попался

Ой!

Во всяком случае, я виню Кребса, поскольку это была его статья.

Теперь давайте вернемся к нашему регулярно планируемому содержанию главы об использовании pass-
слова сбросить подсказки, чтобы заполнить нашу матрицу отслеживания.

Использование подсказок для сброса пароля

Какая подсказка для сброса пароля? Каждый раз, когда вы нажимаете опцию «забыл пароль» на
веб-сайт, сайт обычно предоставляет вам подсказку, за которой следует запрос на проверку
ваша личность. Другой термин для обозначения этих ключей может быть «вопросы проверки учетной записи».
Например, на рассматриваемом веб-сайте может быть написано что-то вроде «для того, чтобы
чтобы сбросить пароль, мы отправим электронное письмо на ваш адрес электронной почты
v*******@gmail.com ».

Но что, если у вас больше нет доступа к этому электронному письму? Это полностью
правдоподобный сценарий, поэтому обычно существует два или три различных проверяемых сценария.
параметры катионов, которые могут включать электронную почту, текстовые сообщения и безопасность ответов
вопросов.

Эти подсказки могут предоставить огромное количество информации, когда вы
построение профиля на отдельном человеке, а иногда (как мы увидим) обучение

отсутствие учетной записи может быть не менее важным для понимания цели
движения.

Запуск вашего контрольного листа

Ранее в этой главе мы начали построение матрицы отслеживания. Один из листов
в документе Excel обозначен как Проверки. Этот лист Excel посвящен цвету.
сбор и документирование подсказок для сброса пароля.
В левом столбце вкладки "Подтверждения" я включаю список сайтов, которые я обычно
проверьте подсказки. Они могут отличаться в зависимости от вашей цели, но хороший старт
Список включает следующее:

- Gmail
- Yahoo
- Hotmail / Microsoft
- eBay
- PayPal
- Facebook
- Instagram
- Yahoo
- Twitter
- ВКонтакте
- Venmo
- LinkedIn
- Steam
- PlayStation Network
- ICQ

Начнем с применения этого к нашему поиску F3ttywap. Поскольку теперь у нас есть
адрес электронной почты (kunt.x7@gmail.com), хорошее место для запуска Veri-
Лист данных нашей матрицы отслеживания находится в Gmail от Google.

Gmail

Начиная с Gmail, мы можем ввести адрес электронной почты нашей цели и щелкнуть
Кнопка «забыл пароль» для перехода на страницу восстановления учетной записи. На рисунке 17.13 показано
первый экран восстановления учетной записи Gmail.

Теперь у нас есть первая подсказка. Резервный адрес электронной почты - 98.*******@gmail.com.

Самое замечательное в Gmail (и большинстве сайтов восстановления учетных записей) заключается в том, что он предоставляет точное количество символов в подсказке для восстановления. Это позволит нам конрасставим определенные точки позже в нашем исследовании, не беспокоясь о том, ненужные предположения.

Большинство сайтов предоставляют более одного метода восстановления учетной записи. При работе в Gmail, нажав «Попробовать другой способ», вы увидите дополнительную валидацию аккаунтации варианты.

В этом случае для нашей тестовой учетной записи была доступна только одна форма подтверждения учетной записи. возможно, но чтобы показать вам дополнительный пример, на рис. 17.14 используется мой личный Учетная запись Gmail, чтобы отобразить второй вариант проверки.

На этом экране видно, что мой номер телефона состоит из 12 цифр (важно для обратите внимание при работе с международными номерами) и оканчивается на 68.

Теперь у нас достаточно информации, чтобы начать заполнять вкладку Проверки на наша матрица отслеживания. На рис. 17.15 показано, что я добавил к своей матрице отслеживания. Я включил свой номер телефона в столбец проверочного номера в качестве пример того, как я бы заполнил эти данные.

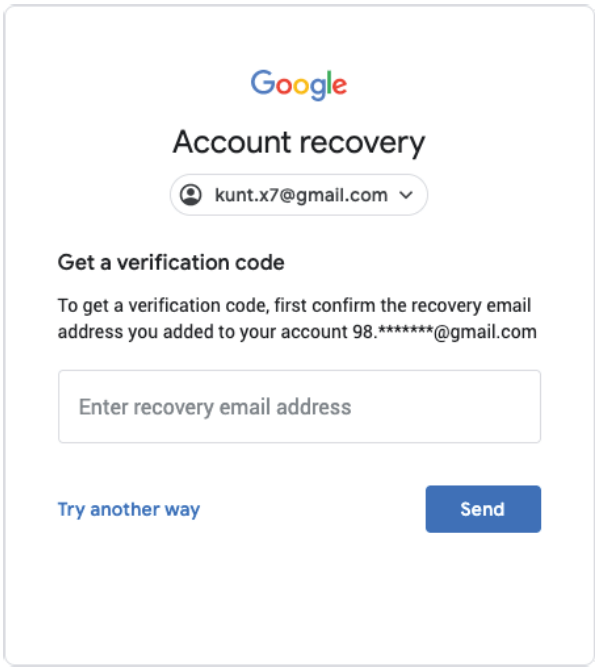


Рисунок 17.13

Facebook

Facebook не самый полезный, когда дело доходит до подсказок для подтверждения учетной записи.
Тем не менее, мы все еще можем многому научиться, даже если нет информации, которую можно было бы раскрыть.
играли - недостаток информации может быть не менее значительным. Недавно Facebook
удалили возможность поиска пользователя по адресу электронной почты, что означает, что мы
не имеют реального способа узнать, есть ли у человека учетная запись Facebook, использующая
указанный адрес электронной почты.
В этом случае страница восстановления пароля Facebook поможет нам выполнить
та же задача. На рисунке 17.16 показана страница восстановления учетной записи Facebook с нашим
целевой адрес электронной почты введен.

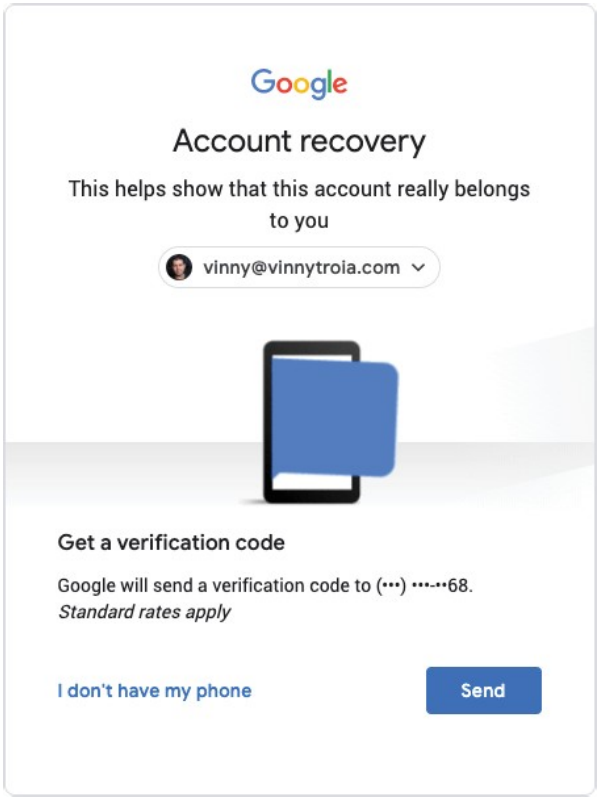


Рисунок 17.14

Site	Email	Username	Verification email	Verification Number
Gmail	kunt.x7@gmail.com		98.*******@gmail.com	********68

Рисунок 17.15

Если учетная запись существует, мы увидим сообщение о том, что письмо было отправлено.
для подтверждения. Вместо этого мы видим сообщение, показанное на рисунке 17.17.
Это однозначно говорит нам о том, что этот адрес электронной почты не имеет учетной записи с
Facebook. Если адрес электронной почты действительно существует, следующим шагом будет использование либо
Внутренний поиск Facebook или внешний инструмент, такой как OSINT.rest или PIPL.com, чтобы попробовать
чтобы найти человека, выполнив поиск по адресу электронной почты.

PayPal

Еще один очень важный сайт для проверки - PayPal. Большинство (если не все) злоумышленников
иметь несколько учетных записей PayPal, поэтому велика вероятность, что вы сможете
получить важные подсказки, используя параметры восстановления своей учетной записи.
На рисунке 17.18 показана первая проверка безопасности учетной записи PayPal, которую мы получаем после
вводим адрес электронной почты нашей цели на странице PayPal «Забыли имя пользователя / пароль».
Это невероятно важно, потому что PayPal дал нам последние две буквы.
первой части резервного адреса электронной почты, а не первых трех
предоставленный нам Gmail. Количество звездочек такое же, что хорошо
указание на то, что PayPal также показывает нам точное количество символов в
восстановление электронной почты.

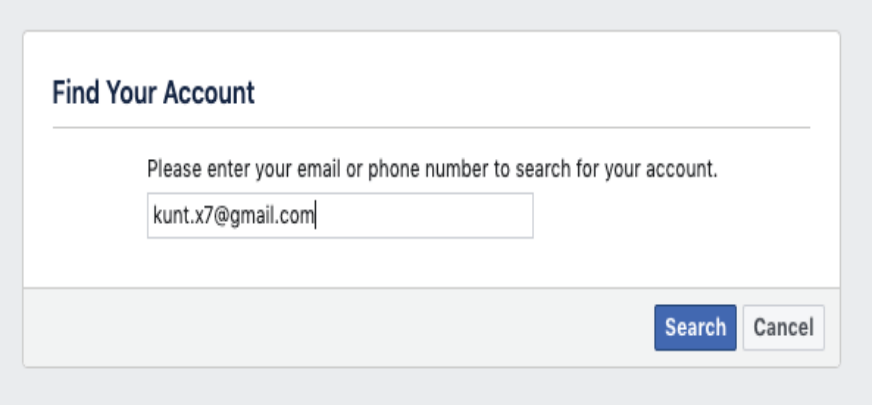


Рисунок 17.16

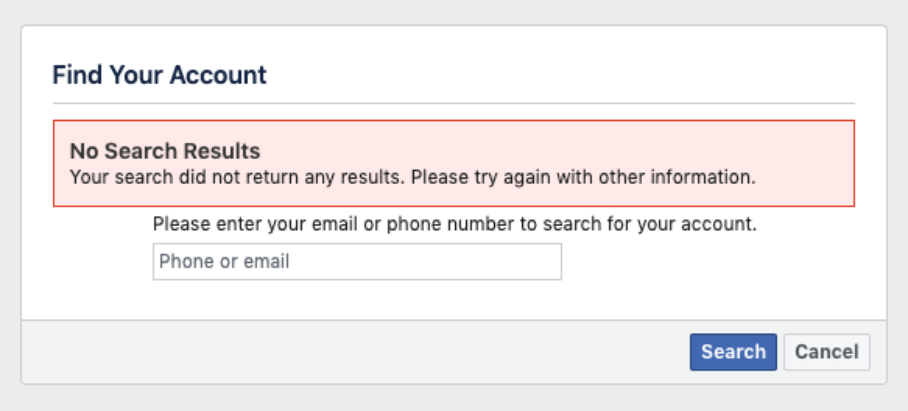


Рисунок 17.17

Конечно, возможно, что у этих двух сайтов разные адреса восстановления,
но предположив на мгновение, что они одинаковы, теперь мы можем экстраполировать, что
адрес для восстановления 98.*****op@gmail.com.
Это действительно хорошая зацепка, которую мы раскроем в следующем
глава. А пока давайте продолжим и посмотрим, что еще мы сможем найти.
Поскольку у нас нет доступа к адресу электронной почты, мы можем выбрать «Ответить
ваши контрольные вопросы ». Рисунок 17.19 показывает это приглашение.
Мы должны задокументировать эти два ключевых вопроса в нашей матрице. Возможно мы
позже может встретиться некоторая информация, которую можно использовать для заполнения деталей.
Наш тестовый адрес электронной почты мало что связан с его учетной записью PayPal,
или мы сможем узнать больше из этих подсказок. Чтобы показать вам, что я имею в виду,
вернемся к использованию моего личного кабинета

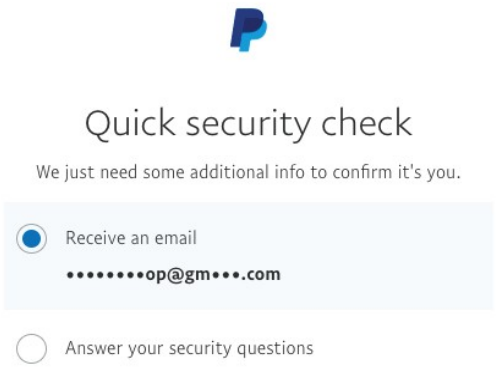


Рисунок 17.18

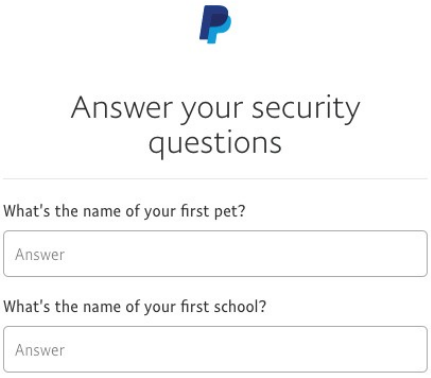


Рисунок 17.19

Введя свой личный адрес электронной почты в PayPal, я получаю четыре
различные способы подтверждения моей личности. Первый вариант - для проверки текстовых сообщений.
катион. На рис. 17.20 показан экран PayPal, на котором отображаются пять цифр моего
номер телефона.

Сравнивая это с тем, что мы узнали из Gmail, мы можем определить, что
оба телефонных номера заканчиваются на 68. Это хороший признак того, что оба телефона
числа такие же. Теперь у нас есть последние четыре цифры номера, *и*
первая цифра кода города. Эта информация сама по себе может использоваться для проверки
личность на других сайтах. Сколько раз вас просили ввести
последние четыре цифры вашего номера телефона?

Следующий вариант - проверка электронной почты. Это похоже на проверку
варианты на других сайтах - вам будет показана часть адреса электронной почты и
попросили получить электронное письмо (показано на рисунке 17.21).

Глядя на детали, представленные на рисунке 17.21, мы можем с уверенностью предположить, что
домен восстановления - mac.com, и мы знаем, что последние две буквы
адрес электронной почты: «ia». Так как звездочек восемь (всего девять букв)
нетрудно догадаться, что мой резервный адрес электронной почты - это мое имя, vinny-
troia@mac.com.

Последний вариант на рисунке 17.22 - проверить номер кредитной карты в файле.
Большинство сайтов не предлагают это для варианта проверки, но на случай, если он когда-нибудь появится
вверх, теперь мы знаем, что у меня есть виза, оканчивающаяся на 10.

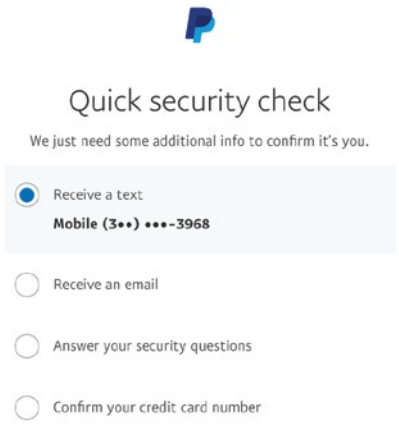


Рисунок 17.20

Твиттер

Практически очевидно, что у злоумышленников будет несколько учетных записей Twitter. Мы может попытаться найти учетную запись Twitter с помощью обычной поисковой системы Twitter, но там велика вероятность того, что имя будет каким-то образом запутано, или человек использовать псевдоним, с которым вы ранее не сталкивались.

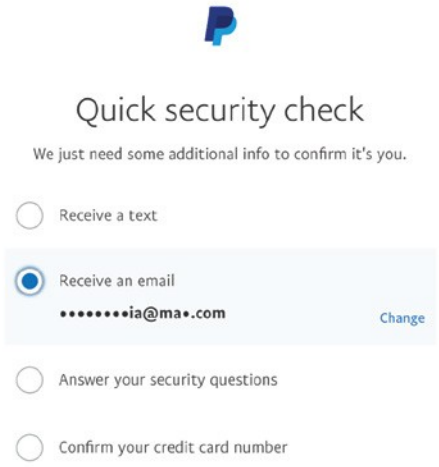


Рисунок 17.21

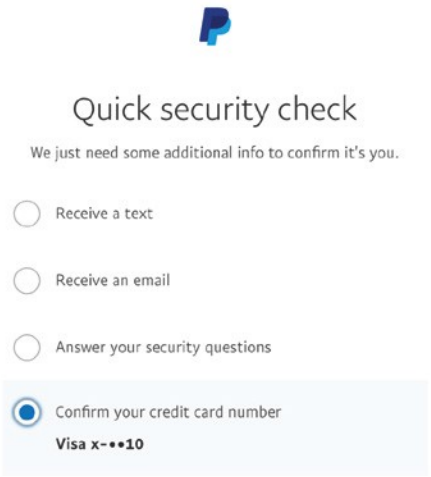


Рисунок 17.22

Чтобы дать вам отличный пример, одно время я искал старого участника
адского форума, известного как Revolt. Я провел несколько поисков в Твиттере, чтобы найти
его счет, но всегда не хватало.

Однажды я попытался найти одного из его известных соратников, «Пинга» или кого-то еще.
в частности, «Пингер». Мне повезло, и я нашел страницу Revolt в Twitter, прочитав
через разные посты. Его имя пользователя в Twitter было «RevoIt_». Глядя на его
на рисунке 17.23, вы можете видеть, что заглавная буква I выглядит идентично строчной
L в Твиттере.

Возвращаясь к нашему поиску, при использовании инструментов сброса учетной записи Twitter нам говорят
существует ли учетная запись. На рисунке 17.24 показан экран, который мы получаем при поиске.
ing для нашей целевой электронной почты kunt.x7@gmail.com.



Рисунок 17.23

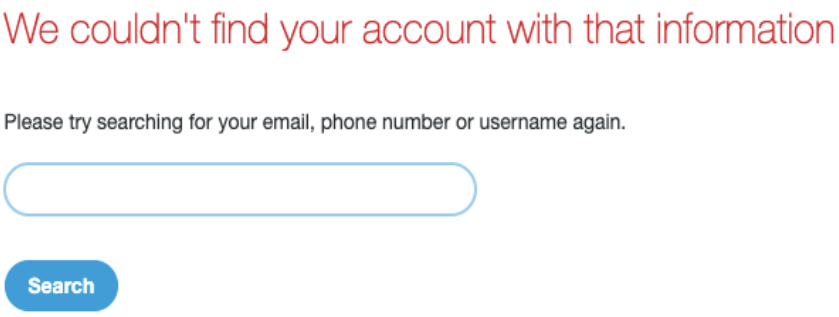


Рисунок 17.24

Но в случае с Twitter поиск имени пользователя может быть столь же эффективным. В качестве
Например, допустим, мы хотим узнать, существует ли учетная запись для кого-то с
имя пользователя m4l1h4ck3r. На рисунке 17.25 показан ответ, который мы получаем от Twitter.
Теперь у нас есть начало резервного адреса электронной почты для этого имени пользователя, которое мы
можете добавить в нашу матрицу проверки.

Microsoft

Еще один почти гарантированный успех - это поиск учетных записей Hotmail или Skype. Skype
учетные записи активно использовались злоумышленниками несколько лет назад до того, как Microsoft
покончил с групповым чатом Skype (и практически уничтожил продукт).
Несмотря на то, что большинство злоумышленников перешли от Skype к Telegram или
Discord, аккаунты, скорее всего, еще доступны.
Учетную запись Microsoft можно искать по имени пользователя, адресу электронной почты или телефону.
количество. На рис. 17.26 показан экран проверки личности одного из моих личных
Учетные записи Microsoft.
В отличие от других сайтов, Microsoft раскрывает полное доменное имя. Если цель была
используя что-то вроде gmail.com или yahoo.com, это не составит большого труда. Но
в случае использования одного из моих личных аккаунтов домен подтверждения не
то, о чем можно было бы легко догадаться.

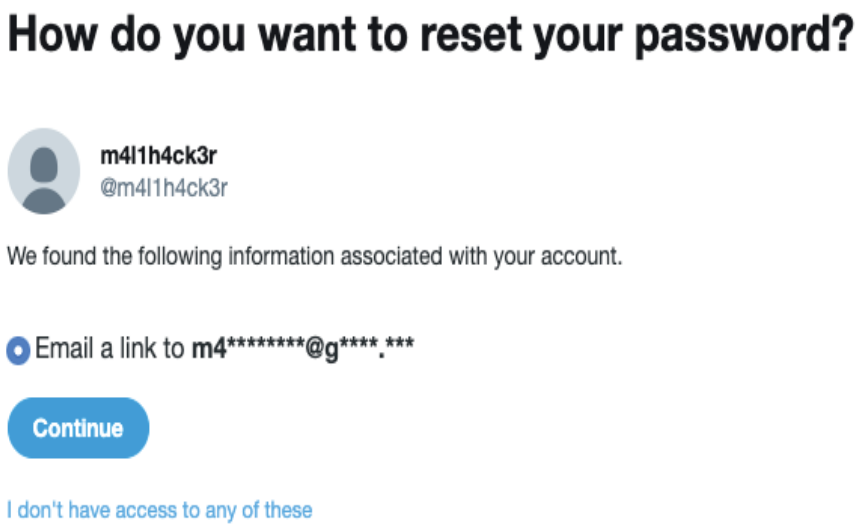


Рисунок 17.25

Instagram

Как и в Facebook или Twitter, у большинства людей есть учетные записи в Instagram. Даже
хотя Instagram не предоставит вам никаких подсказок, чтобы повысить эффективность вашей цели.
файл, параметр сброса учетной записи, по крайней мере, сообщит вам, существует ли учетная запись.
Для демонстрации на рис. 17.27 показано, что происходит, когда я ввожу несуществующий
адрес электронной почты на экране «забыл пароль».
Внизу страницы видно, что пользователей с
этот адрес электронной почты.
Затем давайте попробуем ввести реальный целевой адрес электронной почты. На рисунке 17.28 показан
разница в ответе.
Мы видим, что этот адрес электронной почты существует в Instagram. Хотя мы не можем
искать пользователей напрямую по адресу электронной почты, мы, по крайней мере, знаем, что у пользователя есть
аккаунт и можете поискать другие творческие способы найти его.

Использование ответов веб-сайта jQuery

jQuery - это современная библиотека JavaScript. На очень высоком уровне jQuery разработан
чтобы упростить кодирование JavaScript для веб-сайтов. Одним из распространенных способов использования jQuery является
предоставлять ответы на вопросы веб-форм в режиме реального времени без необходимости
отправить форму.
Например, были ли вы когда-нибудь на веб-сайте, который просит вас выбрать пользователя:
имя или адрес электронной почты, и как только вы введете свой ответ, вы увидите
красное уведомление с надписью «Извините, это имя пользователя уже занято. Пожалуйста, попробуйте еще раз"?
Я считаю, что это современное удобство Интернета - невероятно полезный способ
незаметно определить, есть ли у пользователя учетная запись на определенном веб-сайте.

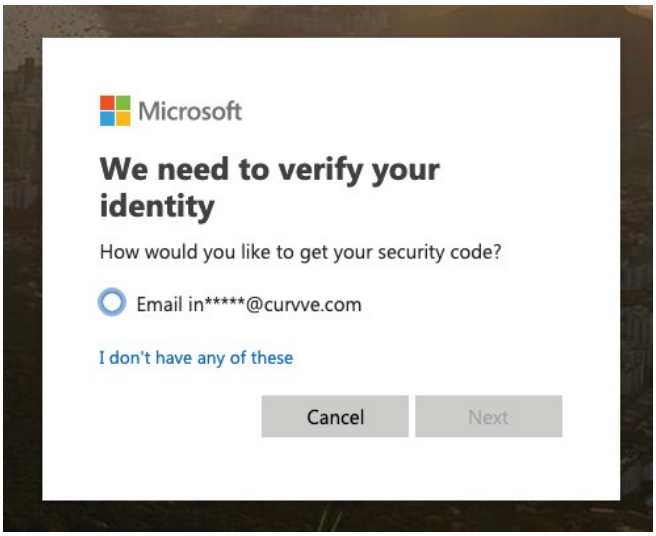


Рисунок 17.26

Чтобы продемонстрировать, давайте посмотрим, зарегистрирован ли наш тестовый адрес электронной почты на Exploit.in,
популярный российский хакерский форум.
На рисунке 17.29 показана часть экрана регистрации Exploit.
Благодаря чуду jQuery мы можем получить мгновенную проверку того,
имя пользователя или адрес электронной почты уже существует на форуме, без необходимости
вход в систему (и потенциально предупреждает администраторов о наших поисках). Рисунок 17.30
показывает результаты ввода адреса электронной почты испытуемого и потенциальных
имя пользователя в соответствующие поля.

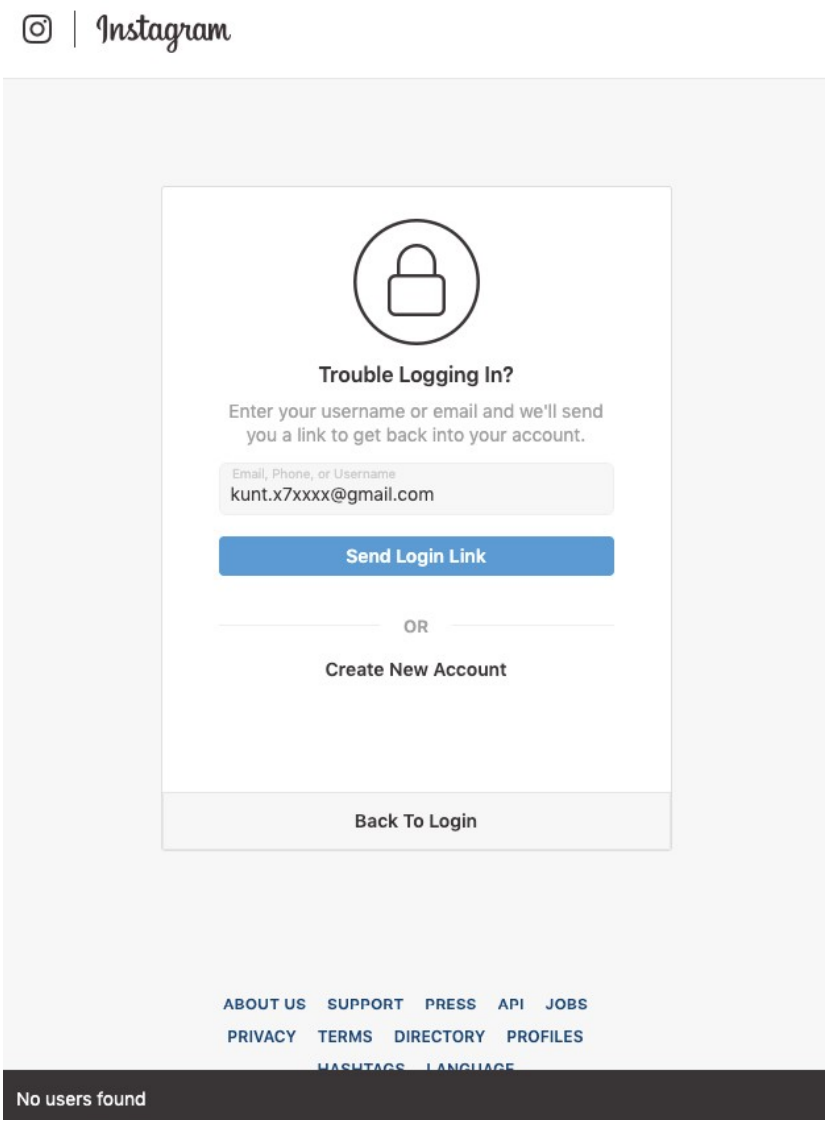


Рисунок 17.27

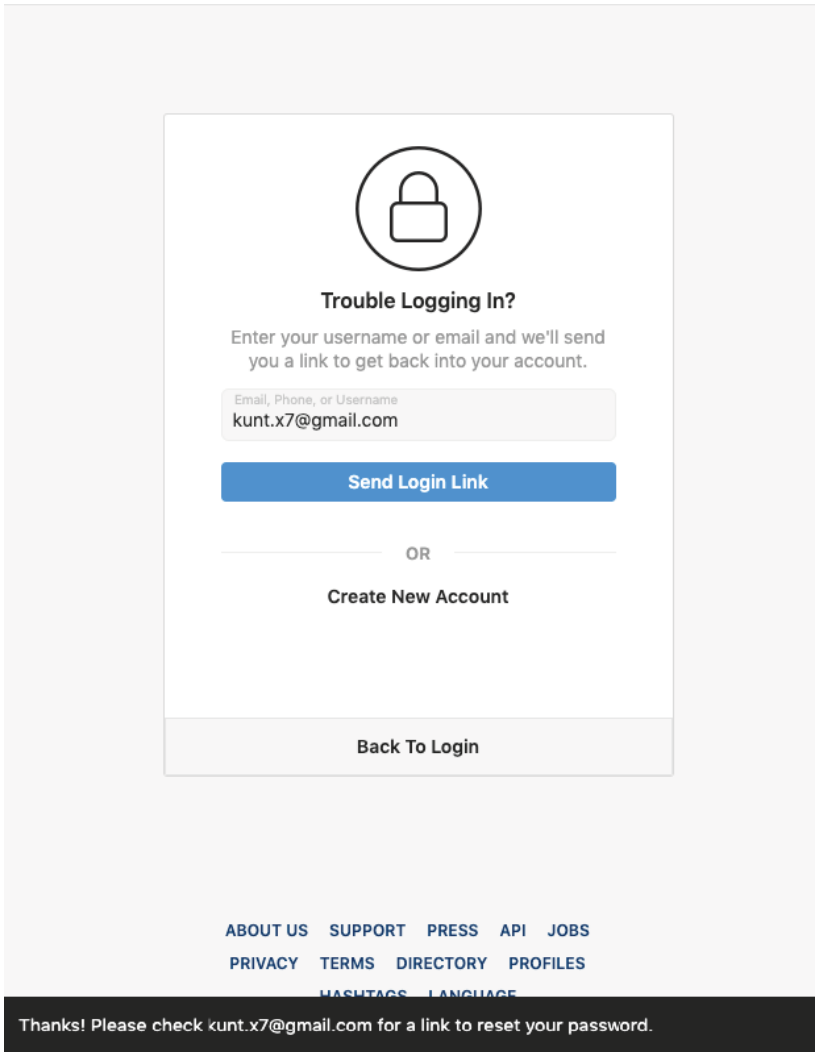


Рисунок 17.28

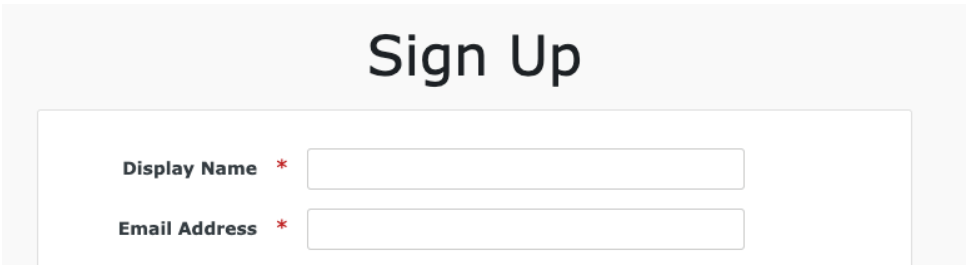


Рисунок 17.29

Оба поля снова стали зелеными, что означает, что они не используются и доступны.
быть зарегистрированным. Теперь посмотрим, что произойдет, если мы захотим узнать, есть ли пользователь
с именем «cr00k» на форуме (рисунок 17.31).
Мы сразу видим, что имя cr00k используется другим членом
форума.
Эти типы мгновенной проверки имени доступны на подавляющем большинстве сайтов.
в Интернете, и может использоваться, чтобы определить,
представляет интерес для вашего расследования.

**Обычно я храню эту информацию в разделе «Учетные записи» отслеживания.
матрицу, но я решил включить эту тему сюда (а не в начало
главу), потому что мы еще не обнаружили адрес электронной почты аккаунта.**

Аська

И последнее, но не менее важное: ICQ, старый чат-сервис конца 1990-х, который кажется
чтобы выжить и до сих пор активно используется международными участниками угроз. Аська
имена пользователей состоят из случайных чисел, состоящих из 8-10 цифр, поэтому их невозможно
Угадай. Но иногда менее умные субъекты угроз делают работу за нас.
На рис. 17.32 злоумышленник cr00k (не тот же cr00k, который связан с
TDO) разместил сообщение, рекламирующее продажу канадских и американских кредитных карт.
В ветке он публикует свой номер ICQ, чтобы с ним связаться.



Рисунок 17.30

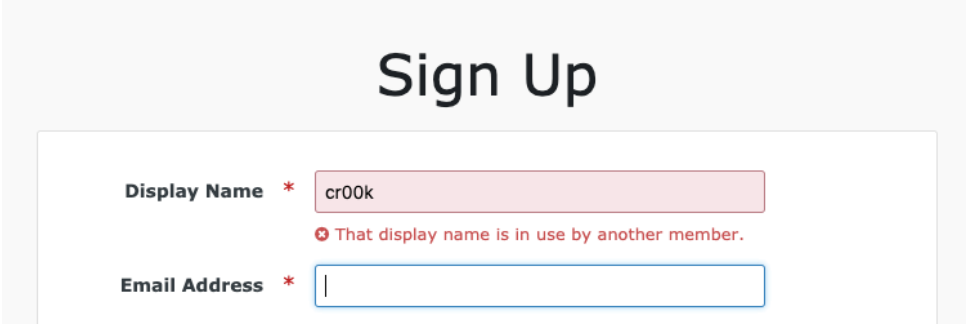


Рисунок 17.31

Страница восстановления учетной записи ICQ позволит вам использовать номер учетной записи в качестве
означает инициировать запрос. На рисунке 17.33 показано результирующее сообщение, когда
вводим 610-476-385 на страницу восстановления аккаунта ICQ.
Мы видим первую букву электронного адреса пользователя и полный домен.
имя. Если бы мы уже знали адрес электронной почты злоумышленника, это было бы
Удобный способ привязать его к номеру ICQ.

Что касается этой конкретной учетной записи ICQ, она связана с Zain M **,**
еще один кардер, связанный с именем cr00k. Электронный адрес совпадает с его
личный живой адрес, zainm****@live.com **.**

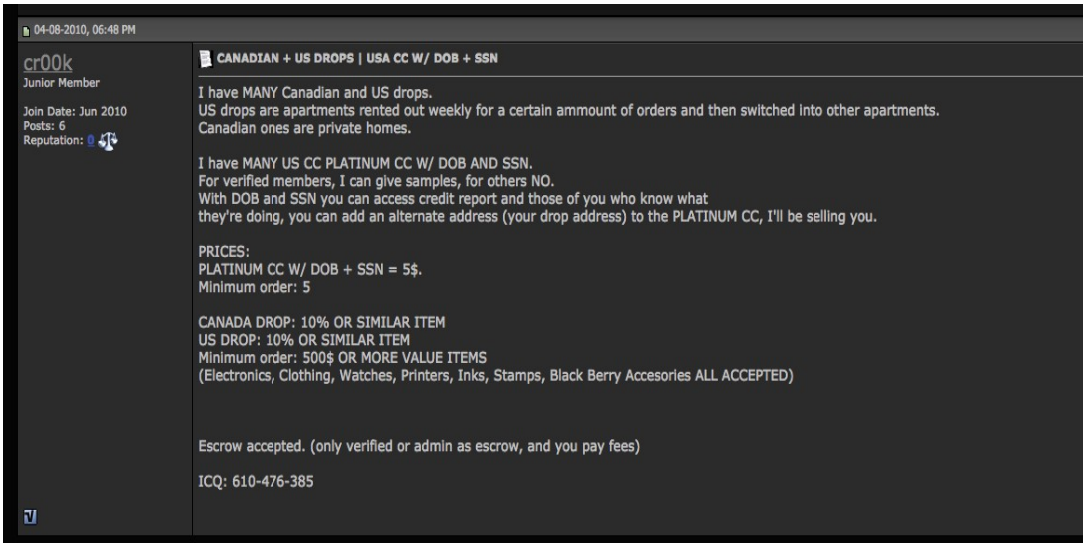


Рисунок 17.32

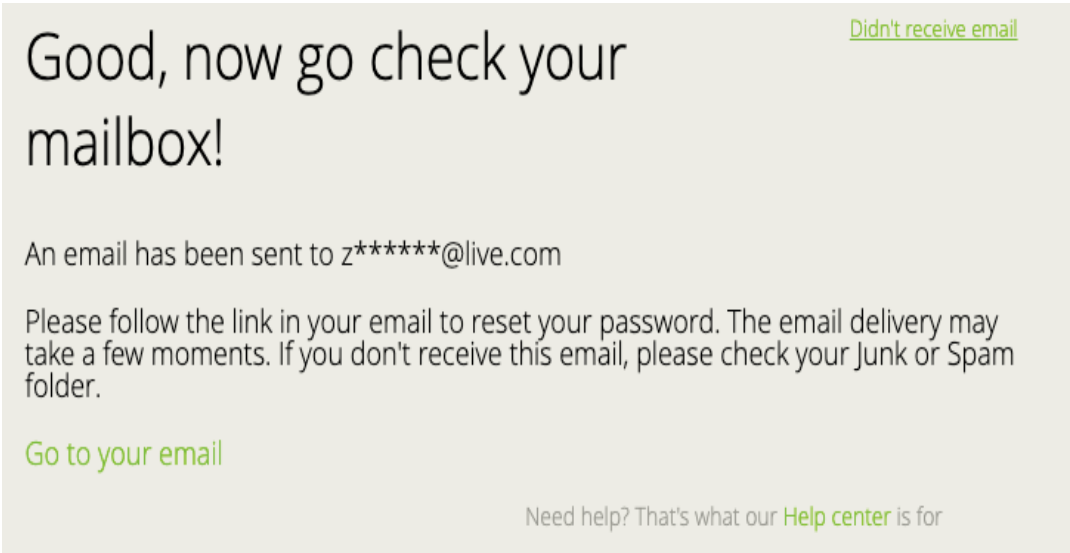


Рисунок 17.33

Резюме

В этой главе обсуждалось построение матрицы отслеживания, которую следует использовать
чтобы сохранить всю необходимую информацию о вашей цели. Матрица отслеживания на основе Excel
содержит три отдельных раздела: учетные записи, проверки и дампы.
В этой главе было рассмотрено несколько методов, используемых для пополнения ваших учетных записей.
и разделы "Проверки". Раздел "Учетные записи" используется как инвентарь всех
сайты, на которых у вашей цели есть учетная запись, в то время как раздел Проверки
используется для каталогизации подсказок «сброса учетной записи», предоставляемых этими сайтами.
Следующая глава будет посвящена использованию данных, полученных со взломанных веб-сайтов.
(также известный как дамп паролей), чтобы помочь нам заполнить профиль злоумышленника.

18

Я считаю, что это удивительно круто, когда я могу сказать следующее предложение: Это
это глава, в которой мы можем использовать против них собственные хакерские хаки. Что я
под этим подразумевается, что мы будем использовать данные в «дампе данных» (т. е., компания
взломанные данные), чтобы заполнить недостающие части из предыдущей главы.
Во время моих поисков раскрыть личности Темного Повелителя я не мог
найти единый инструмент со всеми историческими данными, необходимыми для формирования необходимых
выводы, поэтому я построил свой собственный: Data Viper (www.dataviper.io).
Хотя этот инструмент коммерчески недоступен (пока), я расскажу, как я построил
инструмент, как вы можете создать свой собственный, и, конечно же, как он был использован для достижения
выводы во время моего расследования.
Ниже приводится отрывок из моего первого разговора с TDO около ноября
Сентябрь 2017 г., где мы с ним обсуждаем Cr00k и его связь с группой.
TDO: Мир, это захватывающая мысль.
TDO: Мы наняли много людей, которые будут защищать нас.
в качестве брокеров данных. Трудно найти время для этого
вещи, когда мы заняты продвижением вверх по хакерской цепочке.
VT:
о, это интересно. Думаю, я никогда не смотрел на это так.
VT:
хорошо, если он брокер, почему его больше не используют?
TDO: Как владелец бизнеса, мы удивлены, что вы не учли
методология «цепочки поставок» и ее преимущества.

Пароли, дампы и данные

Гадюка

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

VT:
Думаю, я понятия не имел, насколько организована группа.
TDO: Считаете ли вы, что это разумное решение позволить другим
для устранения недостатков и затрат стилометрии, метаданных
сборник и прочие НАМЕКИ?
VT:
поглотить их как? я не слежу?
TDO: Риск.
V:
конечно, это имеет смысл с точки зрения анонимности
V:
но это возвращает меня к моему вопросу. если мы
собираясь обсуждать предыдущего брокера, важно знать
почему они были выбраны и почему они больше не участвуют
TDO: Мы считаем, что наши брокеры даже сдают в субаренду большую часть работы. Это
Нам сложно получить точную картину всего.
VT:
так вы все еще работаете с cr00k в каком-либо качестве?
TDO: В данный момент мы пытаемся провести CBA, и мы
трудно понять какие-либо преимущества от нас
отвечая на ваш вопрос о cr00k.
TDO: Мир, однако, как вы пришли к этому?
TDO: Это сделало бы нас причастными к некоторым из планетных
крупнейшие нарушения.
VT:
похоже, что у вас, ребята, определенно есть навыки.
TDO: Это твоя жена рассказала школьной спортивной команде?
VT:
моя жена не ходит в школу?
VT:
ой. ха-ха.
TDO: Это немного шутка, приятель. Мы атакуем вас. Мы предполагаем
она ходила в школу раньше.

По-настоящему интересная часть этого разговора - это то, как TDO распределяет
я спрашиваю его о «Душевном покое» и его стремлении классифицировать Мир как
один из величайших хакеров всех времен. Мне всегда было интересно, о чем это.
Теперь, когда информация доступна в Data Viper, эта глава ответит
этот вопрос.

Использование паролей

Люди в индустрии безопасности знают одну неизбежность:
все , будь то обычные конечные пользователи, опытные технические пользователи, злоумышленники,
или кто - нибудь между ними, *будет* , в какой - то момент, повторное использование паролей.
Как «эксперт» по безопасности (я говорю это в кавычках, потому что считаю, что термин
сам по себе невероятно помпезный) всем советую сделать это использовать пароль man-
ager, чтобы они не перерабатывали свои пароли.

Переработка паролей - это то, как современные группы злоумышленников, такие как Gnostic Players, МАБНА (в настоящее время находится в списке самых разыскиваемых ФБР) и многие другие могут доступ к средам Office365, учетным записям Amazon S3 и частным репозиториям кода.

Подход невероятно прост: они собирают списки учетных данных, нацелены на администраторов компании и участвуют в атаках по подбору учетных данных, пока не получат доступ. Весь процесс может быть автоматизирован и чрезвычайно эффективен против организации, в которых не включена многофакторная проверка подлинности.

К счастью для нас, злоумышленники ничем не отличаются. На самом деле, скорее всего, они будут быть моложе и, возможно, менее опытным, что увеличивает вероятность повторно использовать пароли в своих учетных записях, особенно в старых. С использованием информацию об учетной записи и пароле, которые мы обнаруживаем при утечке данных, мы могут начать отслеживать свои учетные записи с поиска похожих паролей.

Конечно, всегда существует вероятность того, что пароль будет *таким универсальным.* (например, «пароль123»), что попытка его поиска приведет к мусору. Более часто это не так. Если это так, просто перейдите к другой учетной записи.

Заполнение матрицы профиля F3ttywap

Примерно в 2017 году хакерский форум Nulled.io был взломан, и полный дамп его Распространена база данных MySQL. Его можно скачать где угодно теперь, включая такие сайты, как RaidForums.com .

Дампированная база данных содержала полный список пользователей, который включал такие поля, как имя пользователя, адрес электронной почты, хешированный пароль, адрес электронной почты для подтверждения и т. д.

Поиск в БД адреса электронной почты «kunt.x7@gmail.com» связывает нас с идентификатор участника 525426. Однако Kunt.x7 не был его основным адресом электронной почты; это было его резервный адрес. Из данных видно, что его основной адрес электронной почты указан как «kunt.lsx@gmail.com».

Бум! Теперь у нас есть новый адрес, который нужно добавить в нашу матрицу! Поскольку мы уже мы рассказали о сбросе пароля в предыдущей главе, давайте перейдем к на поиск паролей.

Важно: экраны, которые я вам покажу, относятся к моему Data Viper. инструмент, который мы обсудим позже в этой главе. А пока я хочу сосредоточиться на потоке и методы исследования паролей, а затем вернемся к использованию инструмента.

Выполнение простого поиска по электронной почте в моей базе данных Elasticsearch (т. Е. Data Viper) возвращает 21 совпадение для нашего нового адреса электронной почты (рисунок 18.1).

Первые четыре совпадения дают нам два уникальных пароля и один хэш пароля. В заголовках разделов указано название набора данных, в котором пришли (например, взлом MPGH, Exploit.in и Pemiblanc). К сожалению, Я пришлось заблокировать пароли. Вместо этого давайте представим, что один из паролей это «2119801m», что на самом деле очень похоже на исходный пароль пользователя. 2119801m - довольно уникальный пароль, что делает его отличным примером тот, в котором мы можем искать дальнейшие подсказки.

Поиск этого пароля дал 91 результат! Я не собираюсь публиковать все 91 (потому что многие из них избыточны), но давайте посмотрим на важные и обсудим почему они так актуальны.

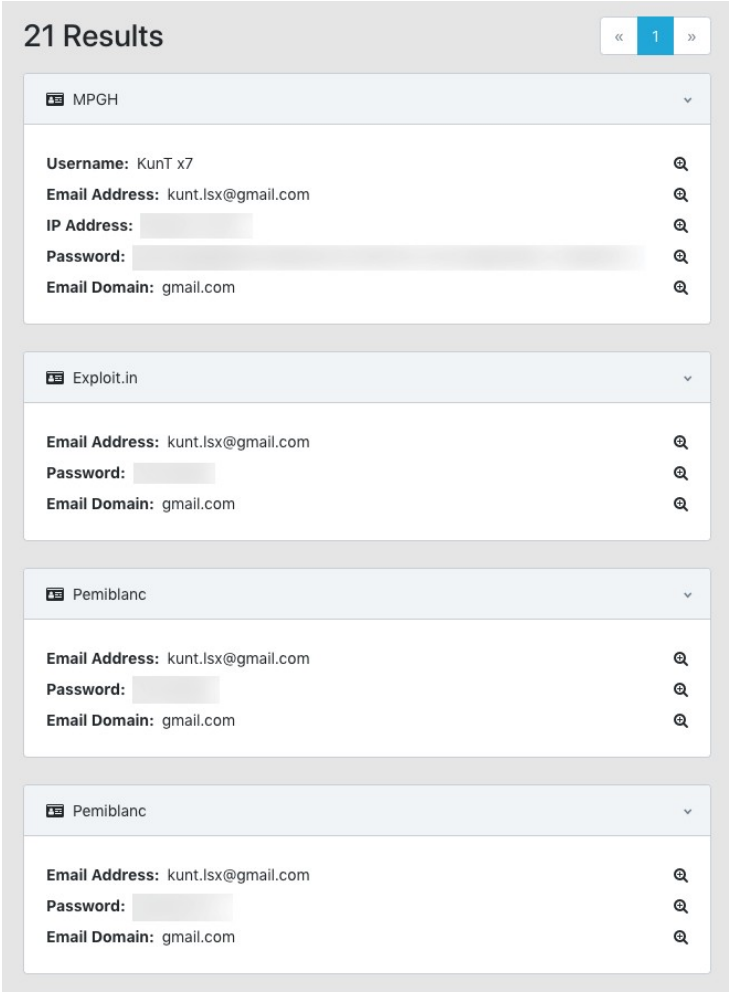


Рисунок 18.1

Во-первых, на рис. 18.2 показаны два сообщения электронной почты (с разными доменами), связанные с
наш пароль.
Это может быть тупик. Имя пользователя «m4l1h4ck3r» не появилось
раньше, но в этом случае повторяется совсем немного, поэтому стоит отложить в сторону.
Рисунок 18.3 - это учетная запись взломанного 000WebHost.com .
На самом деле это крупная находка по ряду причин. Первый (и самый важный)
Если вы вспомните проверочные вопросы из предыдущей главы, мы
возможность составить следующую строку письма с подтверждением, используя комбинацию
подсказок для сброса пароля Gmail и PayPal:
98.*****op@gmail.com
Теперь сравните это с адресом электронной почты, связанным с нашим паролем, и сим-
Сходства должны стать очевидными сразу:
98.*****op@gmail.com
98.lukapop@gmail.com

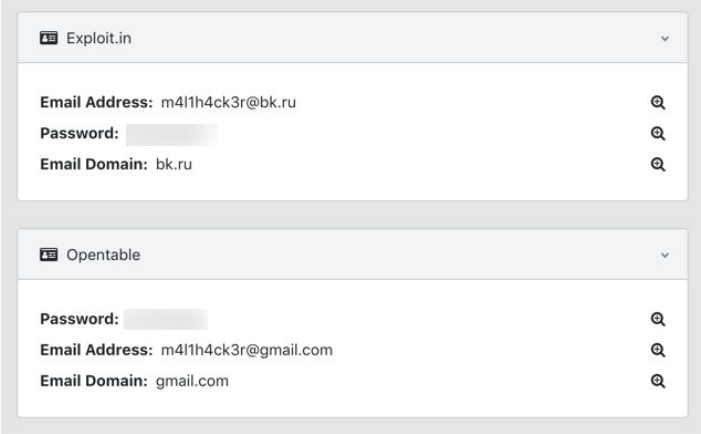


Рисунок 18.2

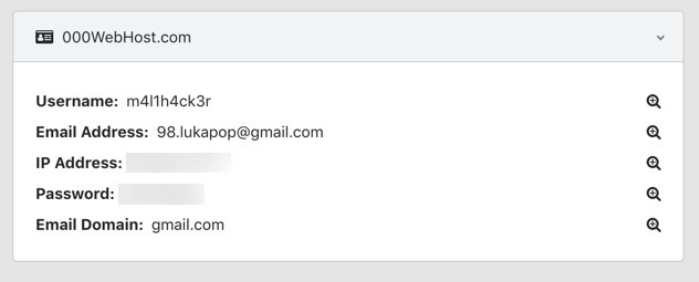


Рисунок 18.3

Кроме того, поскольку имя пользователя в этой учетной записи - m4l1h4ck3r, это также связывает
в любых учетных записях с таким именем пользователя.

Похоже, у нашего друга много аккаунтов на 000WebHost.com . На рисунке 18.4 показано
другая учетная запись с тем же паролем, другим адресом электронной почты и другим именем пользователя.

Это *мог* быть кто-то совсем другой. Однако, учитывая, что слово
Лука появляется в проверочном адресе электронной почты вместе с тем фактом, что
пароль тот же, есть большая вероятность, что это один и тот же человек.

На рис. 18.5 мы видим последний гвоздь в гроб этого человека - опять же, еще один
аккаунт открыт на 000WebHost.com с тем же паролем. На этот раз мы можем
на самом деле видеть его полное имя вместе с адресом электронной почты kunt.lsx@gmail.com
о котором мы уже знали.

На данный момент это просто вопрос незавершенного дела и сбора как можно большего количества информации.
насколько возможно. Мы можем использовать имя, IP, адреса электронной почты и пароли для поиска
для большего количества аккаунтов, которые начнут распутывать все его онлайн-движения.

Важный неверный поворот

Я уже упоминал об этом несколько раз, но на всякий случай хочу повторить еще раз:
насколько мне известно, *F3ttywap, использованный в этом примере, не имеет никакого отношения к
Темный повелитель* .

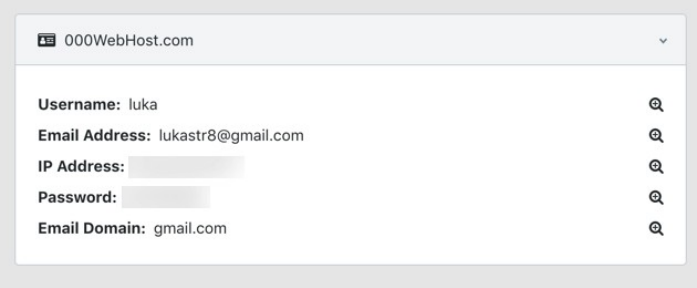


Рисунок 18.5

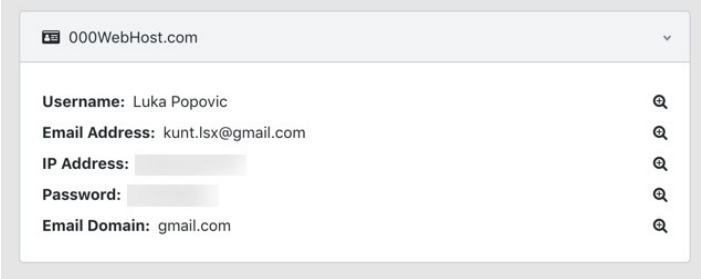


Рисунок 18.4

Помните, что опытные злоумышленники будут повторно использовать псевдонимы, принадлежащие другим
активные субъекты угроз. Это не было редкостью для Cr00k (он же Ping).
Это был важный урок для меня, и я надеюсь, что он найдет отклик
с тобой. Просто потому, что мы нашли владельца *этого набора учетных записей F3ttywap*
не значит, что он тот же F3ttywap связанный с TDO. Важный
различие состоит в том, что ни один из этих аккаунтов не может (каким-либо образом) быть привязан к
F3ttywap на форуме Darkweb Siph0n (где он и Арни оба рекламировали
продажа украденных медицинских данных TDO).
Мы рассмотрим больше примеров использования переработанных паролей для идентификации целей.
далее в этой главе. Во-первых, давайте сделаем шаг назад и посмотрим, как
эти данные собираются.

Получение ваших данных

Утечки данных и дампы паролей доступны повсюду. Вы можете
загружайте их за платные «кредиты» на форумах, таких как RaidForums.com , или вы можете даже
скачать *тысячи* дампов данных с крупных сайтов, таких как Adobe, Dropbox, LinkedIn,
Mate1 и Эшли Мэдисон с сайта www.databases.today . Если вы хотите
начните свою коллекцию, это то место, куда вам захочется попасть, чтобы увязнуть.
Предполагая, что вы получите все на базе данных databases.today и RaidForums.com ,
это, вероятно, приведет вас к отметке 50% с точки зрения того, что на самом деле
в обращении, в частном порядке.
Если вам нужно с чего начать, RaidForums.com завален людьми, предлагающими
«коллекции» учетных данных, которые включают *миллиарды* комбинаций имени пользователя и пароля.
ции. Вы также можете собирать коллекции с таких сайтов, как pastebin. Я лично
держитесь подальше от коллекций и учетных списков любого типа. Следующее примечание
объясняет почему.

. Обработка данных в Data Viper заняла более 18 месяцев, а в
мое скромное мнение, содержит больше качественных данных, чем я видел в любом другом
Платформа. Я понимаю, что это смелое заявление, особенно когда первое слово, которое вы слышите
от каждой компании по анализу угроз: «у нас больше / данных лучшего качества, чем
кто-нибудь еще." Разница в том, что я не пытаюсь продавать членство.
Конечно, это утверждение сложно доказать, но я разработал этот инструмент как средство для достижения
очень конкретная цель, и мне никогда не приходилось жертвовать качеством ради количества.
Я очень горжусь тем, что построил, и, в конце концов, это стоило потраченного времени и
усилия, потому что я смог достичь своей цели по идентификации членов TDO.

Качество и сбор данных 1–5

Где-то в начале 2019 года появилась новость о массовом сборе учетных данных.
внимание СМИ. Названный «Сборник 1», он включал более миллиарда

комбинации имени пользователя и пароля, составленные из различных утечек данных и утечки.

Другими словами, если у вас уже есть данные об утечках, то этот сбор будет просто избыточными данными.

Трой Хант, владелец Have I Been Pwned, написал длинное сообщение в блоге о данные, обнаруженные в Коллекции 1, а также данные в Коллекциях 2–5 (которые он решил не импортировать в свою базу данных).

Мы с Троем обрабатывали данные одновременно, и я сделал довольно много моего собственного анализа для коллекций 4 и 5, чтобы посмотреть, есть ли что-нибудь стоит сохранить.

Каждый набор данных содержал примерно от 10 до 20 различных папок, каждая из которых содержала сотни файлов с произвольной нумерацией. Мой процесс очистки данных был чтобы сначала объединить и исключить дубликаты файлов в каждой папке. Это привело бы примерно в 10–20 очень больших файлах с чисто уникальными совпадениями.

Следующим шагом было объединение и устранение дубликатов каждого из этих файлов до тех пор, пока не будет получен результат.

был только один мастер-файл для каждой коллекции.

Наконец, я объединил каждый из двух основных файлов коллекций с помощью де-команда дублирования и слияния. В результате получился один очень большой файл с уникальным набором записей из обоих сборников.

Вот статистика файлов и результаты моего анализа:

Сборник 4:

■ Исходный размер - примерно 300 ГБ.

■ Около 4 миллиардов необработанных записей (самый большой из выпусков коллекций 1–5).

■ Каждая папка была де-дублирована и объединена, в результате чего был получен один мастер-файл. 60 ГБ и 1,8 миллиарда записей.

■ Сравнение нового файла с исходными данными показало, что 55% общий выпуск был дублирован.

Сборник 5:

■ Исходный размер - примерно 220 ГБ.

■ 2,8 миллиарда необработанных записей

■ После сортировки и устранения дублирования окончательный размер файла составил 45 ГБ и 1,2 миллиарда. уникальные записи.

■ Сравнивая результаты, 58% данных в Коллекции 5 повторялись.

Объединение коллекций 4 и 5

■ Первоначальный размер обоих файлов составлял 105 ГБ с 3 миллиардами необработанных записей.

■ После того, как файлы были объединены и де-дублированы, окончательный размер файла составил 72 ГБ. с чуть менее 2,1 миллиарда записей.

■ Объединение этих наборов данных удалило еще 30% повторяющихся записей.

Всегда проверяйте данные вручную

На первый взгляд, это звучит довольно неплохо; 2,1 миллиарда уникальных пользователей Комбинации имени и пароля были бы отличным дополнением к любой коллекции, верно? К сожалению, именно здесь нам нужно время, чтобы вручную проверить что мы имеем. Когда мы это делаем, мы быстро понимаем, что данные - чистый мусор.

Ниже приведены несколько сотен записей, отобранных случайным образом из финального файл коллекции. Столбцы содержат адрес электронной почты и пароль:

«ddd-54000@hotmail.fr», «54000»
"ddd-54000@hotmail.fr", "cats654"
"ddd-54000@hotmail.fr", "cats654"
"ddd-54000 @ hotmail.
fr "," Cats654540 "
"ddd-54000@hotmail.fr", "ddd-54000"
"ddd-54000@hotmail.fr", "ddd54000"
"ddd-54000@hotmail.fr", "revoltec"
"ddd54000@hotmail.fr", "revoltec"
"ddd-54000@mail.ru", "Cats65454000"
"ddd-54000@rambler.ru",
"Кошки654540"
"ddd-54000@yandex.ru",
"Кошки65454000"
«ddd-54001@mail.ru», «Cats65454000»
"ddd-54002@mail.ru", "Cats65454000"
«ddd-54009@mail.ru», «Cats65454000»
"ddd5400@mail.ru", "qwerty"
"ddd5401@mail.ru", "1ytrewq"
"ddd5401@mail.ru", "ddd5403123"
"ddd5401@mail.ru", "qwert"
"ddd5401@mail.ru", "qwerty"
"ddd5401@mail.ru", "Qwerty"
"ddd5401@mail.ru", "qwerty10"
"ddd5401@mail.ru", "qwerty1123"
"ddd5402@mail.ru", "1ytrewq"
"ddd5402@mail.ru", "ddd5403123"
"ddd5402@mail.ru", "qwert"
"ddd5402@mail.ru", "qwerty"
"ddd5402@mail.ru", "Qwerty"
"ddd5402@mail.ru", "qwerty10"
"ddd5402@mail.ru", "qwerty1123"
"ddd5403@mail.ru", "1ytrewq"
"ddd5403@mail.ru", "ddd5403123"
"ddd5403@mail.ru", "qwert"
"ddd5403@mail.ru", "qwerty"
"ddd5403@mail.ru", "Qwerty"
"ddd5403@mail.ru", "qwerty10"
"ddd5403@mail.ru", "qwerty1123"
"ddd540422@yahoo.com.tw", "n888599"
"ddd5404@mail.ru", "1ytrewq"
"ddd5404@mail.ru", "ddd5403123"
"ddd5404@mail.ru", "qwert"
"ddd5404@mail.ru", "qwerty"
"ddd5404@mail.ru", "qwerty10"
"ddd5404@mail.ru", "qwerty1123"
"ddd5405@bk.ru", "qwerty"
"ddd5405@inbox.ru", "qwerty"
"ddd5405@list.ru", "qwerty"
"ddd5405@mail.ru", "1ytrewq"
"ddd5405@mail.ru", "ddd5403123"
"ddd5405@mail.ru", "qwert"
"ddd5405@mail.ru", "qwerty"
"ddd5405@mail.ru", "qwerty10"
"ddd5405@mail.ru", "qwerty1123"
"ddd5406812129@yahoo.com",
"ddd54068"
"ddd5406@bk.ru", "qwerty"
"ddd5406@hotmail.com", "qwerty"
"ddd5406@inbox.ru", "qwerty"
"ddd5406@list.ru", "qwerty"
"ddd5406@mail.ru", "qwerty"

"ddd5406@nm.ru", "qwerty"
"ddd5406@pochta.ru", "qwerty"
"ddd5406@qip.ru", "qwerty"
"ddd5406@rambler.ru", "qwerty"
"ddd5406@yandex.ru", "qwerty"
"ddd5407906@163.com", "d5407906"
"ddd5407@bk.ru", "qwerty"
"ddd5407@inbox.ru", "qwerty"
"ddd5407@list.ru", "qwerty"
"ddd5407@mail.ru", "qwerty"
"ddd54088@mail.ru", "qwerty"
"ddd5408@bk.ru", "qwerty"
"ddd5408@inbox.ru", "qwerty"
"ddd5408@list.ru", "qwerty"
"ddd5408@mail.ru", "qwerty"
«ddd540900@gmail.com», «1472580369»
«DDd540900@gmail.com», «1472580369»
"ddd5409@mail.ru", "qwerty"
"ddd5409@sbcglobal.net", "96867340"
«ddd5410@sian.com.cn», «19831014»
"ddd@54154.ru", "drive330"
"ddd54@163.com", "ninalove"
"ddd5417@mail.ru", "qwerty"
"ddd541983@mail.ru", "1645zzz"
"ddd541984@mail.ru", "1645zzz"
"ddd541985@bk.ru", "1645zzz"
"ddd541985@inbox.ru", "1645zzz"
"ddd541985@list.ru", "1645zzz"
"ddd541985@mail.ru", "1645zzz"
"ddd541985@rambler.ru", "1645zzz"
"ddd541985@yandex.ru", "1645zzz"
"ddd541986@mail.ru", "1645zzz"
"ddd541987@mail.ru", "1645zzz"
«ddd541@mail.ru», «45454546»
"ddd541@mail.ru", "CFIEKZ1"
«ddd541@mail.ru», «ЦФИЕКЗА»
"ddd542931@hotmail.com", "mevemoza"
«ddd542@mail.ru», «555555»
"ddd542@mail.ru", "CFIEKZ1"
«ddd542@mail.ru», «ЦФИЕКЗА»
"ddd5431@bk.ru", "cfiekz"
"ddd5431@list.ru", "cfiekz"
"ddd5431@mail.ru", "cfiekz"
«ddd54321d@bk.ru», «54321ddd»
«ddd54321d@inbox.ru», «54321ddd»
"ddd54321d@list.ru", "54321ddd"
"ddd54321d@mail.ru", "54321ddd"
«ddd54321d@rambler.ru», «54321ddd»
«ddd54321d@yandex.ru», «54321ddd»
"ddd5432@autorambler.ru", "cfiekz"
"ddd5432@bk.ru", "cfiekz"
"ddd5432@inbox.ru", "cfiekz"
"ddd5432@lenta.ru", "cfiekz"
"ddd5432@list.ru", "cfiekz"
"ddd5432@mail.ru", "cfiekz"
"ddd5432@myrambler.ru", "cfiekz"
"ddd5432@qip.ru", "cfiekz"
"ddd5432@r0.ru", "cfiekz"
"ddd5432@rambler.ru", "cfiekz"
"ddd5432@ro.ru", "cfiekz"
"ddd5432srftged@ddd.com",
«131531970»
"ddd5432@yandex.ru", "cfiekz"
«ddd54333@qip.ru», «555555»
"ddd5433@bk.ru", "cfiekz"
"ddd5433@list.ru", "cfiekz"
"ddd5433@mail.ru", "cfiekz"
«ddd5433@qip.ru», «555555»
«ddd543@aol.com», «Thomas914»
«ddd543@mail.ru», «555555»
"ddd543@mail.ru", "cfiekz"

"ddd543@mail.ru", "cfiekz @"
"ddd543@mail.ru", "CFIEKZ1"
"ddd543@mail.ru", "ЦФИЕКЗА"
«ddd543@qip.ru», «555555»
"ddd543@rambler.ru", "1q2w3e"
«ddd543@rambler.ru», «555555»
"ddd543s@mail.ru", "fdsa1210"
"ddd543s@yahoo.com", "fdsa1210"
"ddd543s@yahoo.com", "fdsa12101"
"ddd543s@yandex.ru", "fdsa1210"
"ddd543s@ya.ru", "fdsa1210"
«ddd543@yahoo.com», «csh12345»
«ddd543@yandex.ru», «555555»
"ddd54434@mail.ru", "egor89227"
"ddd54435@mail.ru", "egor89227"
"ddd54436@mail.ru", "egor89227"
"ddd5445d4kcjkksd @
qq.com "," 82546004 "
"ddd5445@mail.ru", "fdffdfdf"
«ddd54484848484dd@56.com», «198635»
«ddd544@aol.com», «Thomas914»
«ddd544@mail.ru», «555555»
"ddd544@mail.ru", "CFIEKZ1"
«ddd544@mail.ru», «ЦФИЕКЗА»
"ddd54511884@yandex.ru", "qqqqqqqq"
"ddd54542@yandex.ru", "54545454м"
«ddd54544@mail.ru», «54545»
«ddd545452@mail.ru», «6541236e»
«ddd545453@mail.ru», «6541236e»
«ddd545454@bk.ru», «6541236e»
«ddd545454@inbox.ru», «6541236e»
"ddd545454ksa @ gmail.
com "," 6541236e "
«ddd545454@list.ru», «6541236e»
"ddd545454@list.ru", "ddd54545"
«ddd545454@mail.ru», «6541236e»
«ddd545454@mail.ru», «6545236e»
«ddd545454@qip.ru», «6541236e»
«ddd545454@rambler.ru», «6541236e»
"ddd545454sla@web.de", "6541236e"
"ddd545454sla@yahoo.co.uk",
«6541236»
"ddd545454@yahoo.com", "444фильм"
«ddd545454@yandex.ru», «6541236e»
"ddd545454zlsl @ yahoo.
com "," 6541236e "
«ddd545455@mail.ru», «6541236e»
«ddd545456@mail.ru», «6541236e»
«ddd54545@mail.ru», «54545»
«ddd54545@mail.ru», «6541236e»
«ddd54546@mail.ru», «54545»
"ddd54546@mail.ru", "ddd54546 @"
mail.r "
"ddd@54546.ru", "drive330"
«ddd54547@mail.ru», «54545»
«ddd54547@yahoo.com», «sss54547»
«ddd54547@yahoo.com.tw», «sss54547»
«ddd545488@163.com», «1150718345»
«ddd5454@gmail.com», «255555»
«ddd5454@hotmail.com», «255555»
"ddd@5454.ru", "drive330"
"ddd5454@YAHOO.COM", "ddd789456"
"ddd54554545@juno.com",
"dddddgvlie6"
"ddd.54.55@hotmail.com",
"1234567894"
"ddd5456@mail.ru", "111qqqaaa"
"ddd5457@aol.com", "12696dd"
«ddd545@aol.com», «Thomas914»
"ddd545@mail.ru", "CFIEKZ1"
«ddd545@mail.ru», «ЦФИЕКЗА»

«ddd545y999@qip.ru», «3334444»
«ddd545y999@yandex.ru», «33344»
«ddd545y999@yandex.ru», «333444»
«ddd545y999@yandex.ru», «3334444»
«ddd545y999@yandex.ru», «33344441»
"ddd545y999@yandex.ru", "3334444Q"
«ddd545y999@yandex.ru», «545999»
«ddd545@yandex.ru», «1234567»
«ddd545@yandex.ru», «291979»
"ddd54608@mail.ru", "19a89a"
«ddd54615461», «54615461»
"ddd54615461 @ bigmir.
net "," 54615461 "
«ddd54615461@bk.ru», «54615461»
«ddd54615461@email.ua», «54615461»
"ddd54615461 @ freemail.
ru "," 54615461 "
«ddd54615461@gmail.com», «54615461»
«ddd54615461@gs.uz», «54615461»
"ddd54615461@hotmail.com",
"54615461"
"ddd54615461@hotmail.ru",
"54615461"
«ddd54615461@inbox.ru», «54615461»
«ddd54615461@i.ua», «54615461»
«ddd54615461@list.ru», «54615461»
«ddd54615461@mail.com», «54615461»
«ddd54615461@mail.ru», «54615461»
«ddd54615461@narod.ru», «54615461»
«ddd54615461@qip.ru», «54615461»
"ddd54615461 @ rambler.
ru "," 54615461 "
"ddd54615461@tut.by", "54615461"
«ddd54615461@ukr.net», «54615461»
"ddd54615461@yandex.by", "54615461"
"ddd54615461 @ яндекс.
com "," 54615461 "
«ddd54615461@yandex.kz», «54615461»
«ddd54615461@yandex.ru», «54615461»
«ddd54615461@yandex.ua», «54615461»
«ddd54615461@yandex.uz», «54615461»
«ddd54615461@ya.ru», «54615461»
«ddd54615461@ya.ua», «54615461»
«ddd5461546@gmail.com», «54615461»
«ddd5468@yandex.ru», «23011985»
"ddd_5470ddd @ yahoo.
co.jp "," 19880428 "
"ddd_5470ddd @ yahoo.
co.jp "," 87160044 "
«ddd-5476@qq.com», «325221»
"ddd5478d@hotmail.com", "ddd8478d"
«ddd5478@mail.ru», «1234567890»
«ddd5479@yandex.ru», «1322455»
«ddd5479@yandex.ru», «k1322455»
«ddd547@bk.ru», «mama8962»
"ddd5551970@list.ru", "gjkrjdjltw"
«ddd5551970@mail.ru», «5551970»
"ddd5551970@mail.ru", "ddd5551970"
"ddd5551970@mail.ru", "gjkrjdjltw"
"ddd5551970@qip.ru", "gjkrjdjltw"
"ddd5551970@rambler.ru",
"gjkrjdjltw"
"ddd5551970@yahoo.com",
"gjkrjdjltw"
"ddd5551970@yandex.ru",
"gjkrjdjltw"
«ddd5551971@mail.ru», «5551970»
"ddd5551971@mail.ru", "ddd5551970"
"ddd5551971@mail.ru", "ddd5551971"
«ddd5551979@mail.ru», «5551970»
"ddd5551979@mail.ru", "ddd5551970"

«ddd5551979@mail.ru», «ddd5551979»
"ddd5552008@yandex.ru",
"t30u87l89a"
"ddd.5552010@yandex.ru", "zyrjdf"
"ddd.5552010@yandex.ru", "Zyrjdf"
"ddd.5552019@yandex.ru", "zyrjdf"
"ddd555222554@mail.ru",
"321123321d"
"ddd555222555@mail.ru",
"321123321d"
"ddd555222556@mail.ru",
"321123321d"
«ddd555222@mail.ru», «28111988»
«ddd5552@hotmail.com», «947600»
«ddd.5552@mail.ru», «11aa11»
"ddd55533443@mail.ru",
"ddd555444333"
"ddd55533444@mail.ru",
"ddd555444333"
"ddd55533445@mail.ru",
"ddd555444333"
"ddd55533@aol.com", "8cwxkq43"
«DDD55533@AOL.COM», «Каир»
"DDD55533@AOL.COM", "dav2DAVID"
"ddd55533@aol.com", "Дэвид"
"ddd55533@aol.com", "ДЭВИД"
«ddd.5553@mail.ru», «11aa11»
«ddd.5553@mail.ru», «159753waTsOn»
"ddd5553@mail.ru", "ddd777"
"ddd5553@tianya.cn", "331769638"
"ddd55544@mail.ru", "inafngjn"
«ddd55545@hotmail.com», «035611295»
"ddd55545@mail.ru", "inafngjn"
"ddd55546@mail.ru", "inafngjn"
"ddd55547 @ hotmail.
com "," 0876585486 "
«ddd.5554@bk.ru», «11aa11»
«ddd.5554@gmail.com», «11aa11»
"ddd-55.54@gmx.de", "qazxcv"
«ddd.5554@inbox.ru», «11aa11»
«ddd.5554@list.ru», «11aa11»
«ddd.5554@mail.ru», «11aa11»
"ddd.5554@mail.ru", "159753waTsOn"
«ddd5554@mail.ru», «89222555920»
«ddd-55.54@mail.ru», «ddd-55.54»
«ddd-55.54@mail.ru», «ddd5555»
"ddd5554@mail.ru", "ddd777"
"ddd-55.54@mail.ru", "qazxcv"
«ddd-55.54@mail.ua», «qazxcv»
«ddd.5554@pochta.ru», «11aa11»
«ddd.5554@qip.ru», «11aa11»
«ddd.5554@rambler.ru», «11aa11»
«ddd.5554@rambler.ru», «11aa111»
«ddd.5554@rambler.ru», «11aa11123»
«ddd.5554@rambler.ru», «11aa11a»
"ddd.5554@rambler.ru", "11aa11qwe"
«ddd.5554@rambler.ru», «Ddd.5554»
"ddd5554@rambler.ru", "ddd777"
"ddd-55.54@web.de", "qazxcv"
«ddd.5554@yandex.ru», «11aa11»
«ddd.5554@yandex.ru», «1212aa1212»
"ddd55551@inbox.ru", "cfifcfif"
«ddd55551@mail.ru», «121212»
«ddd55551@mail.ru», «388211»
"ddd55552@inbox.ru", "cfifcfif"
«ddd55552@mail.ru», «5234ww»
"ddd55553@inbox.ru", "cfifcfif"
«ddd55554@bk.ru», «04111997az»
"ddd55554@inbox.ru", "cfifcfif"
"ddd55554@mail.ru", "cfifcfif"

«ddd55554@rambler.ru», «27101993м»
«ddd555550@mail.ru», «171000ddd»
«ddd555551@mail.ru», «171000ddd»
«ddd55555@21co.com», «000000»
«ddd555552@mail.ru», «171000ddd»
"ddd5555553@inbox.ru", "poiv4u9a"
"ddd5555554@inbox.ru", "poiv4u9a"
«DDD555555555555@bk.ru», «44444444»
"DDD555555555555@inbox.ru",
«4444444»
"DDD555555555555@list.ru",
"44444444"
«ddd5555555555@meta.ua», «225517»
"ddd555555555@mail.ru", "mamam12"
«ddd5555555@bk.ru», «bekl2001»
"ddd5555555@hotmail.com",
"рыремалу"
"ddd5555555@inbox.ru", "bekl2001"
"ddd5555555@inbox.ru", "poiv4u9a"
"ddd5555555@list.ru", "bekl2001"
"ddd5555556@inbox.ru", "poiv4u9a"
"ddd5555557@inbox.ru", "poiv4u9a"
"ddd555555d@sina.com", "нидзидо"
«ddd555555@gmail.com», «102030»
"ddd555555@hotmail.com",
"метианчай"
"ddd.555-555@hotmail.co.th",
«123456»
«ddd555557@mail.ru», «06020602»
«ddd555557@rambler.ru», «06020602»
«ddd55555@bk.ru», «04111997az»
«ddd55555ddd@mail.ru», «5555555»
«ddd55555ddd@mail.ru», «55555555»
«ddd55555ddd@yandex.ru», «5555555»
«ddd55555ddd@yandex.ru», «55555555»
"ddd55555d@hotmail.com", "larson07"
"ddd55555d@rambler.ru", "larson07"
"ddd55555@ibox.ru", "cfifcfif"
"ddd55555@inbox.ru", "cfifcfif"
«ddd55555@inbox.ru», «ddd55555»
"ddd55555@inbox.ru",
"ddd55555inboxrucfifcfif"
"ddd55555@inbox.ru", "fifcfifc"
«ddd55555@mail.ru», «55555»
"ddd55555@mail.ru", "cfifcfif"
«ddd55555@meta.ua», «225517»
«ddd55555@rambler.ru», «ddd77777»
«ddd55555@yahoo.co.jp», «ddd66666»
"ddd55555 @ яндекс.
ru "," qwerty123456 "
"ddd5555666333@163.com", "211385"
«ddd55556@bk.ru», «04111997az»
"ddd55556@inbox.ru", "cfifcfif"
«ddd55556@mail.ru», «55555»
"ddd55556@mail.ru", "cfifcfif"
"ddd55557@inbox.ru", "cfifcfif"
"ddd55558@inbox.ru", "cfifcfif"
"ddd55559@inbox.ru", "cfifcfif"
"ddd-55.55@aliceadsl.fr", "qazxcv"
«ddd-55.55@bk.ru», «qazxcv»
«DDD5555DDD@bk.ru», «EHtsvKWv»
«DDD5555DDD@inbox.ru», «EHtsvKWv»
"DDD5555DDD@list.ru", "EHtsvKWv"

Данные явно сфабрикованы. Электронная почта и пароли виртуально идентичный. Похоже, это скорее список подбора паролей, чем реальный комбинация реальных данных.

Я не могу представить, чтобы что-то из этого было когда-либо полезным, именно поэтому у меня никогда не заботился о сборе и обработке каких-либо данных коллекций.

Одна из вещей, которые я часто вижу, - это атаки на Spotify по подбору учетных данных. я регулярно встречаются люди, которые говорят: «Привет, меня обманули, я только что взял пасту (из pastebin), и похоже, что у Spotify произошла утечка данных ». А потом вы идете и смотрите на вставьте и поймите: «Ого, это отформатировано так же, как и любая другая« утечка данных », где фактически получил имя пользователя и пароль в открытом виде, а затем тип членства, например, семья, премиум или что-то еще ".
Каждый раз я возвращаюсь, чтобы проверить с некоторыми из пользователей, и всегда приходит вернуться к плохим повторно используемым паролям. Я не знаю, подходит ли мне слово «мусор», потому что это законные учетные данные, но они не из-за «утечки данных». Они просто из-за повторного использования пароля. Хотя, при этом, их часто выдают за данные нарушения, когда люди говорят: «Привет, у нас произошла утечка данных Spotify». Нет, не знаешь.
Что касается сфабрикованных нарушений, еще одна проблема, которую, как я вижу, многие люди пытаются Перед вами Twitter, где они скажут: «Эй, вот 30 миллионов аккаунтов из Twitter».
Это всегда плохо пахнет, и я однажды обратился к ИТ-директору Twitter, чтобы подтвердить некоторые данные, и они всегда возвращаются как часть другого комбинированного списка созданных Дефицитная начинка. Это одни и те же переработанные пароли, которые передаются и над.

Где найти качественные данные

На этом этапе вы можете спросить себя: хорошо, тогда где мне взять качественный данные? Что ж, это непростой и быстрый процесс.

Вы можете найти некоторые из ваших основных общедоступных наборов данных на таких сайтах, как RaidForums. com или databases.today . Для чего-то большего вам потребуется получить участвует в подпольном рынке данных.

Я написал несколько историй, в которых я создавал фальшивых персонажей, взаимодействовать с злоумышленниками и, по сути, откладывать всю мою жизнь, пока Я потратил тысячи часов на то, чтобы погрузиться в эту андеграундную сцену.

Это не для всех, но для тех из вас, кто занимается этим на постоянной основе. работа, или для тех, у кого есть должная мотивация (как я сделал с TDO), тогда знайте что это не будет мгновенным процессом.

Data Viper

Data Viper (www.dataviper.io) - мой инструмент. Я разработал его как средство, помогающее идентифицировать tify членов Темного Повелителя. Я сделал это, потому что видел явное отсутствие необходимые данные для всех инструментов анализа угроз, которые я пробовал, даже компании, которые отказались помочь мне в этом поиске (а некоторые были довольно грубо об этом). К счастью, у меня были друзья, которые были готовы искать в своих наборах данных меня, и я быстро понял, что причина, по которой эти компании были такими защита их данных заключается в том, что у них их не было.

Так что я решил собрать свою, и так родился Data Viper. Инструмент использует сочетание ReactJS и PHP для своего графического интерфейса и бэкэнд Elasticsearch для данных - базовое хранилище. Концепция инструмента не слишком сложна, поэтому я говорю любой может построить это. Фактически, вам даже не нужно создавать собственный интерфейс. Графический интерфейс; вы можете просто использовать Kibana, которая уже является частью проекта Elasticsearch. Если вам интересно, вы можете узнать больше о Kibana здесь: https: //www.elastic .co / products / kibana .

В этой книге я много раз обсуждал Data Viper, и ранее в этой главе я привел пример того, как этот инструмент можно использовать для раскрыть личность злоумышленника путем поиска общих паролей при утечке данных. На самом деле для этого можно использовать любой инструмент. Фактически, вы технически даже не нужен «инструмент»; вам просто нужен доступ к нужным данным, и возможность поиска по этим данным (вот тут-то и пригодится Kibana).

Позже в этой главе я предложу несколько различных готовых решений, которые могут можно использовать, если вы не хотите создавать свои собственные. Во-первых, давайте посмотрим, как данные были используется для формирования твердого вывода.

Форумы: Недостающее звено

Возможность поиска паролей - это лишь одна часть Data Viper. Когда ты впервые начинают расследование, поиск паролей может не обязательно быть настолько полезным, потому что есть вероятность, что вы не будете знать, какие учетные записи или адреса электронной почты связаны с вашим злоумышленником, и вы, вероятно, у вас даже не будет достаточно информации о вашей цели, чтобы знать, что вам следует искать.

Я понял это, когда впервые начал создавать Data Viper, поэтому я также потребовалось время, чтобы создать сеть сложных веб-парсеров, предназначенных для очистки все известные хакерские форумы и сайты, которые я смог найти. Теперь вместо того, чтобы просто быть возможность поиска паролей, я также разработал возможность поиска конкретных ключевые слова среди пользователей форума, обсуждений и сайтов вставки.

На момент написания этой главы у меня было более 11 миллиардов записей (независимых паст или коллекций) и сотни миллионов очищенных сообщений на форумах.

На рисунке 18.6 показан главный экран Data Viper.

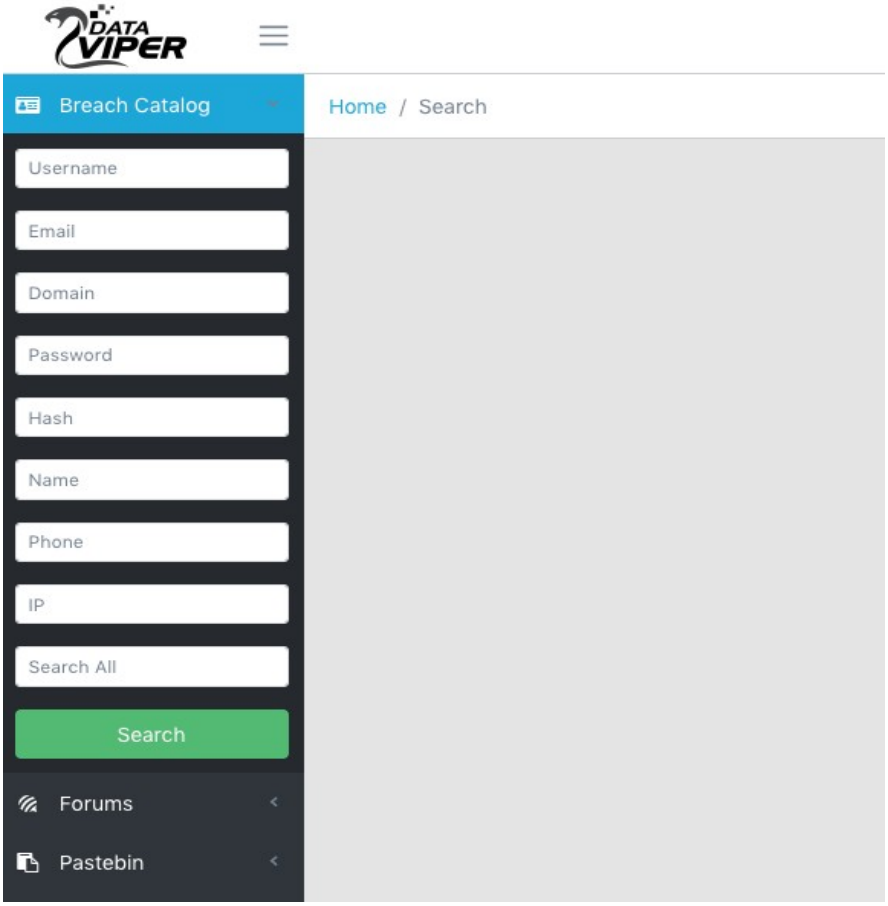


Рисунок 18.6

Пользовательский интерфейс прост. Я купил готовую тему для интерфейса, чтобы я мог
просто вставляйте компоненты без необходимости их кодирования. Поля, показанные в
На рис. 18.6 показаны основные элементы поиска, которые я обычно ищу и использую.

Определение настоящего «Cr00k»

Идентификация cr00k была первым большим прорывом, который у меня был во время исследования TDO.
тигация. Выполнение простого поиска cr00k в Google покажет множество
активность этого пользователя на различных хакерских форумах clearweb.
На первый взгляд, отследить местонахождение этого пользователя *должно* быть легко, особенно
учитывая большой след, который он оставил в Интернете. Каждый раз, когда я разговаривал с
исследователя или разведывательной компании об этом пользователе, они все немедленно и
окончательно согласился с тем, что cr00k - это «Заин М.», кардер низкого уровня из Саскатч-
Юан, Канада.
Что ж, оказывается, с ними все в порядке. Cr00k - кардер из Канады,
и все свидетельства указывают на то, что Zain - cr00k.
К сожалению, этот Cr00k не имеет никакого отношения к TDO, и потребовалось
месяцев, чтобы понять это.
Долгое время я был убежден, как и все остальные, что Cr00k
кто открыто говорит о кардинге в clearweb, должно быть, тот же Cr00k, что
связан с TDO.
Была только одна неприятная проблема, которую я не мог решить. Морфеус говорит это
Лучшее в первом фильме « *Матрица* »: «Это как заноза в твоей голове, сводящая тебя с ума».
Рисунок 18.7 - это скриншот одного из оригинальных сообщений о продаже, опубликованных
cr00k на российском хакерском форуме Exploit.

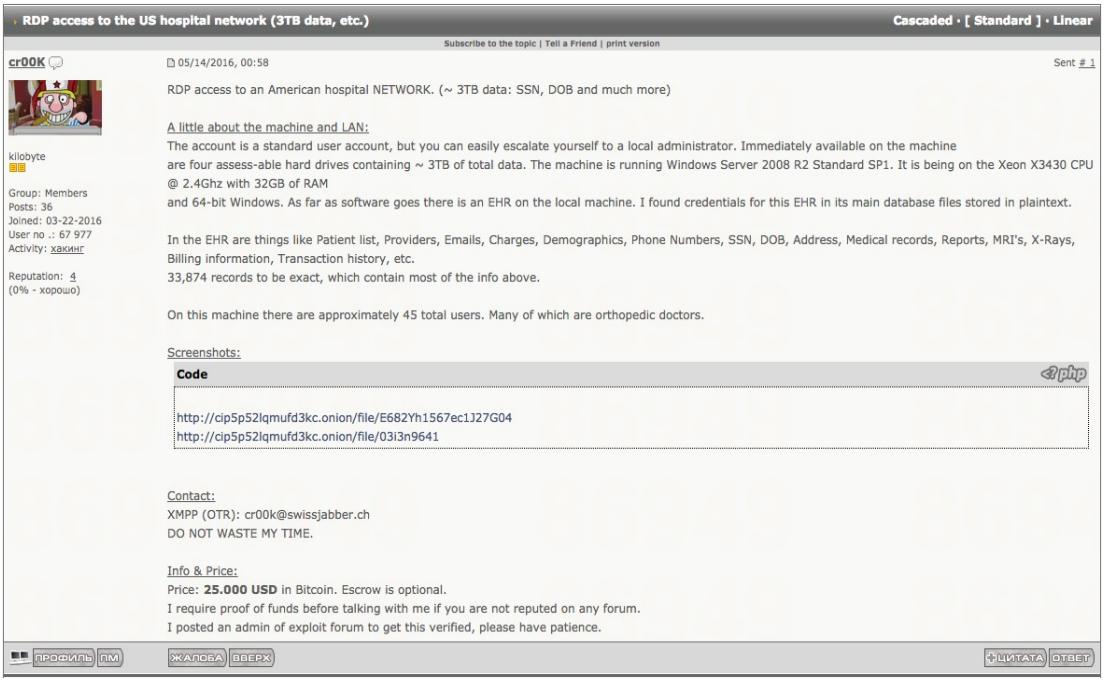


Рисунок 18.7

На этом снимке экрана важно обратить внимание на контактный адрес cr00k @.
swissjabber.ch.
В этом была суть проблемы. Каждый пароль, адрес электронной почты и онлайн
Ресурс ссылается на нашего друга Зейна как на человека, стоящего за Cr00k. Пока ничего,
ни единого клочка информации, связанного с Zain с адресом XMPP cr00k @
swissjabber.ch.
Войдите в Data Viper.

Отслеживание перемещений на форуме Cr00k

Потому что я потратил время, чтобы получить доступ и очистить как можно больше темной и чистой сети
форумов, насколько это возможно, я мог отслеживать движения cr00k. Большинство из
Матчи clearweb в данном случае не годились, поскольку в конечном итоге привели к
друг Заин. Однако мы могли бы легко сопоставить пользователя Cr00k из Exploit с
тот же Cr00k, который любил торчать с KickAss и 0Day (два других темных
форумы по взлому веб-сайтов) из-за его контактного адреса (cr00k@swissjabber.ch).
Рисунок 18.8 - это снимок экрана с веткой KickAss от Cr00k.
Поскольку идентификаторы Jabber одинаковы, можно смело заключить, что мы имеем дело
с тем же человеком. Теперь, используя Data Viper, мы можем запустить список всех его сообщений.
через KickAss и другие форумы (образец сообщений показан на рис. 18.9).

Анализ временной шкалы

Возможность просматривать все сообщения Cr00k на соответствующих форумах в упорядоченном по данным
подобная мода позволила мне увидеть следующую цепочку событий (чтобы вещи
Вам проще, я буду показывать события на скриншотах, а не в маленьких вырезах
от Data Viper).
На рисунке 18.10 показано, что 29 марта 2016 г. пользователь Cr00k разместил ветку продаж.
на форуме KickAss, где он продавал несколько взломанных баз данных (и
попросили связаться с ним по адресу cr00k@swissjabber.ch).

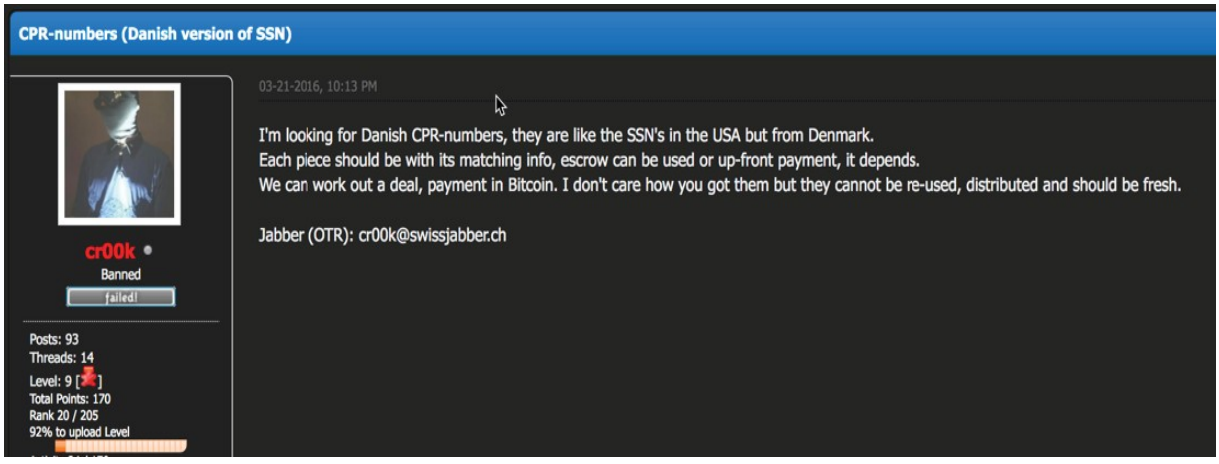


Рисунок 18.8

Одна из выставленных на продажу баз данных включала логины и пароли для TeamSkeet.com , порно сеть США.

	author	forum	message
▸	cr00k	KickAss	DB which I was selling Mother went to the press...
▸	cr00k	KickAss	If they are high quality then they can be used for online PoS systems l ike Stripe if you disable CVV number authorization/checking. Good luck with sales!
▸	cr00k	KickAss	Prevent leaks by: - background checks, as you see the idiot who used the same PGP keys. This incident could of been easily prevented if you think about it righ t now. - allow people only if they either a) offer a service and will be active on the board (e.g. discussion)
▸	cr00k	KickAss	1. EK with loads of traffic 2. Mavertising 3. E-mail spam with Word/PDF exploit.
▸	cr00k	KickAss	DK is dead, as in not coming back.
▸	cr00k	KickAss	Why would you ever use a source code from an AV from 8 years ago? Anti- virus companies are maybe updating their methods, techniques and databa ses everyday. If you want to effectively test your malware/exploits aga inst AV's you should set-up a VM with the AV in particular (Kaspersky) on hardest mode.
▸	cr00k	KickAss	Bitcoin mining is dead, better do ransomware with low price to decrypti on. 50 USD.

Рисунок 18.9

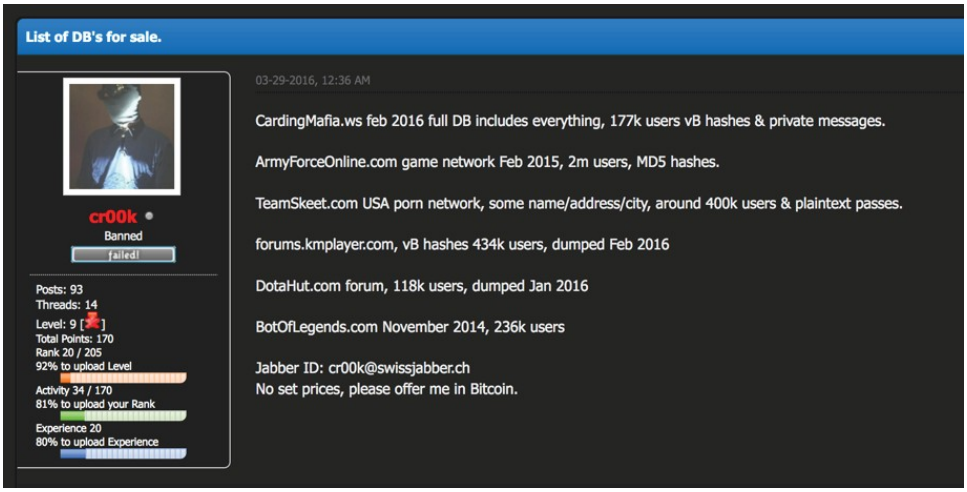


Рисунок 18.10

Вскоре после этого пользователь NeoBoss разместил те же данные о продаже на Dream Market, бывшая торговая площадка даркнета (рис. 18.11).

В сообщении говорилось: «Недавно мне удалось взломать TeamSkeet.com , гигантский Сеть порно США. Приобретая эту базу данных, вы получаете в основном бесплатную порно-аккаунты на всю жизнь, или вы могли бы продавать их отдельно ".

31 марта 2016 года на сайте Vice.com была опубликована статья, в которой описывалось хакерское проникновение: создание порно-сети и продажа данных в Интернете (рис. 18.12).

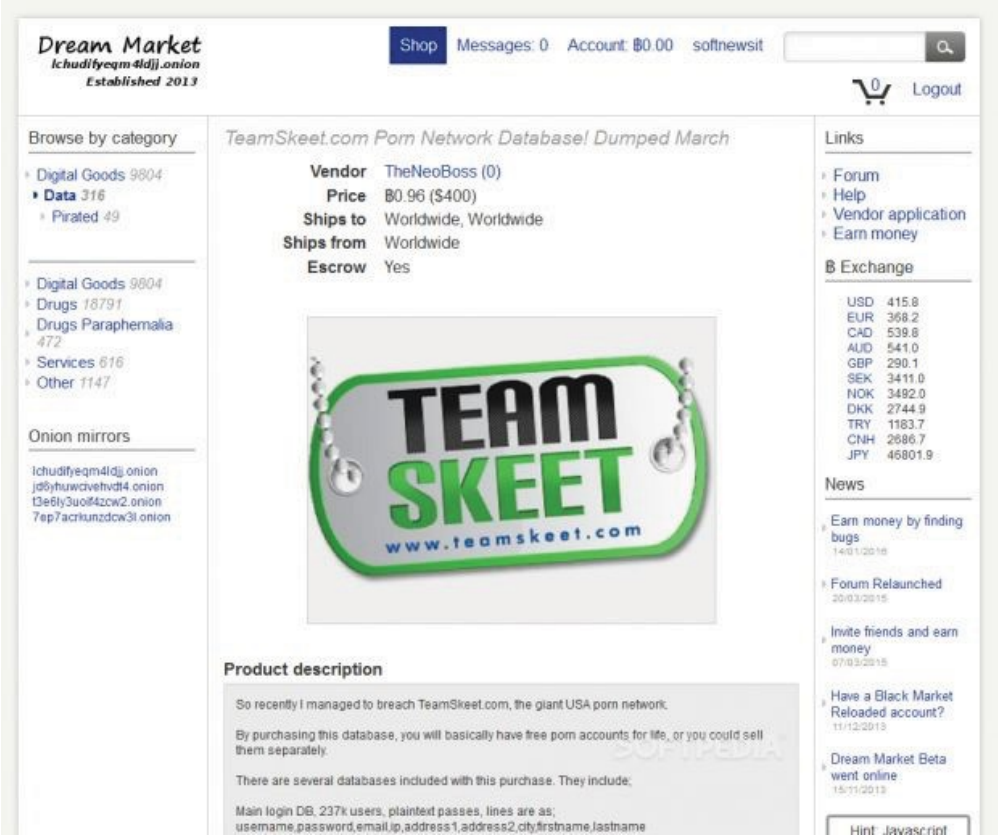


Рисунок 18.11



Рисунок 18.12

Эта статья включает несколько прямых цитат NeoBoss, где он уточняет:
Яич взял на себя ответственность за взлом и хотел «публично опозорить Команду Скита за их плохие методы ». На этом этапе можно было предположить, что Cr00k и NeoBoss такие же люди.
За исключением 3 апреля 2016 г., Cr00k опубликовал на KickAss сообщение о его партнер, который «обратился к прессе» с базой данных, которую он продавал (рис. 18.13).
Мы уже знаем из предыдущего поста, что он продавал TeamSkeet.com , поэтому, учитывая обстоятельства событий, было бы неправильно предположить, что NeoBoss был его партнером и «ублюдком, который пошел в прессу».
Только 26 июня 2016 года пользователь cr00k опубликовал «отчет о рипере» для пользователя w0rm на форумах Exploit и Siph0n (рисунок 18.14).
В отчете он перечисляет несколько деталей о пользователе w0rm (который оказывается очень известный российский мошенник).

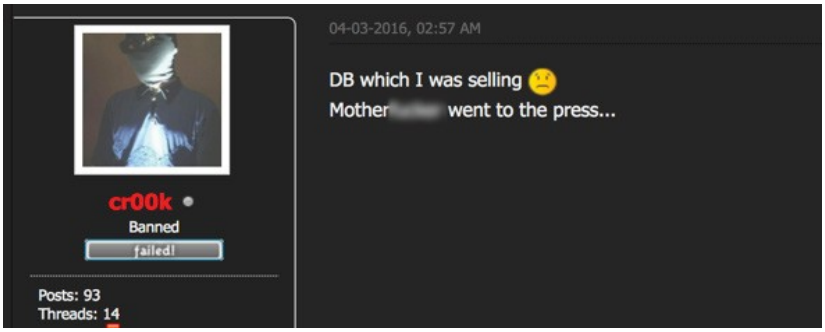


Рисунок 18.13

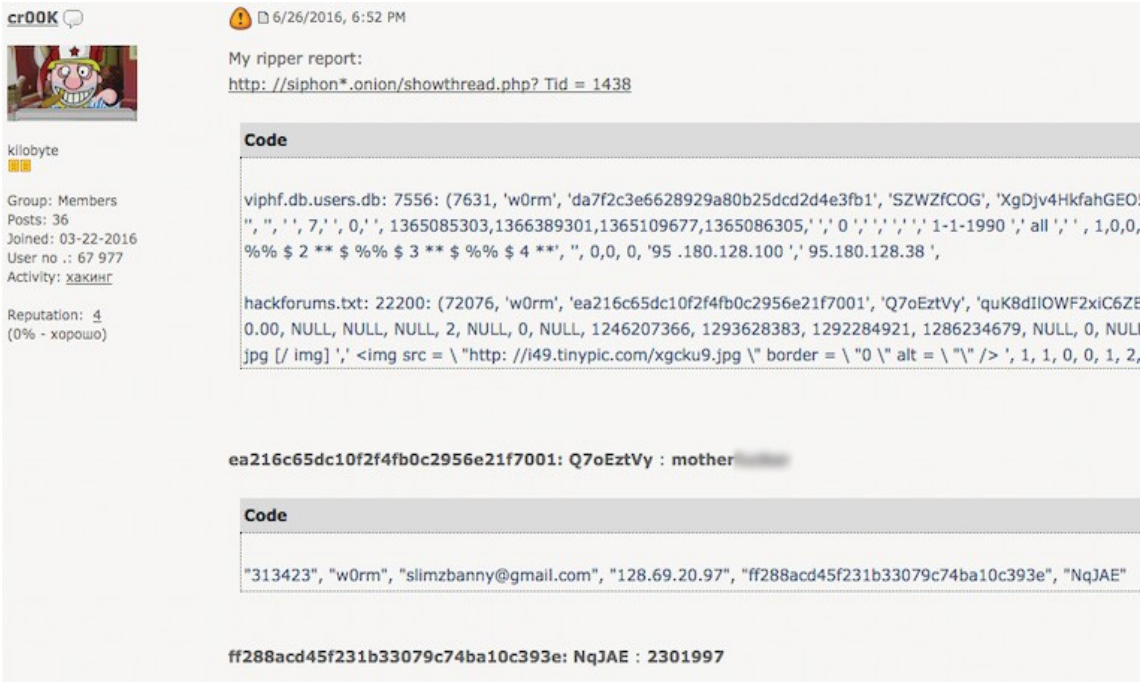


Рисунок 18.14

Опять же, обратите внимание на ссылку на «ублюдок» после хеш-информации.
Похоже, cr00k потребовалось несколько месяцев, чтобы понять, что w0rm и
NeoBoss был тем же человеком.

Следует отметить, что URL-адрес «отчета о риппере» ссылается на тот же отчет на Форум Siph0n, размещенный под именем F3ttywap. Это в сочетании с несколькими других идентичных сообщений TDO между Cr00k и F3ttywap на обоих форумах достаточно, чтобы сделать вывод, что эти два субъекта угроз - одно и то же лицо.

Перенесемся в октябрь 2016 года, в статье на сайте Motherboard (Vice.com) говорится:
этот пользователь "Peace" (также известный как "Peace of Mind") берет на себя ответственность за взлом и
сбросить собственный хакерский форум w0rm, w0rm.ws (рис. 18.15).

Момент Эврики

Все эти события кажутся совершенно не связанными друг с другом. К счастью для нас, Мир был достаточно зол
с w0rm, чтобы не только взломать его базу данных, но и опубликовать ее для всего мира.
В рамках Data Viper я написал скрипты, которые автоматически разделяют
такие дампы базы данных - пользовательские таблицы извлекаются и импортируются как пользовательские
учетные записи, а личные сообщения, сообщения и комментарии форума извлекаются
из и импортированы в раздел форумов.
Однако в этом случае простого импорта этих данных было бы недостаточно.
В качестве механизма безопасности я часто вручную ищу интересующие имена пользователей.
всякий раз, когда я получаю новые данные. У меня есть практика поиска по всему
набор данных, *прежде чем* я разделю и импортирую данные - и следующая подсказка будет
показать вам, почему именно.



MOTHERBOARD | By Joseph Cox | Oct 2 2016, 12:00pm
TECH BY VICE

Hacker Linked to Myspace, LinkedIn Dumps Hacks Competitor

Peace, who made his name selling databases of Silicon Valley companies, has dumped apparent data of a rival's black market site.

Рисунок 18.15

Если бы я не искал вручную «cr00k» в наборе данных w0rm, я бы
упустили этот ключевой ключ (поэтому я уверен, что многие другие тоже упустили его).
На рисунке 18.16 показана таблица «объявлений» базы данных w0rm.ws.
Объявление форума (которое не было бы воспринято как форум
post или личное сообщение) говорится, что «w0rm находится под новым управлением. . . оплата
и информация: ke7hb@w0rm.ws ».
Просматривая данные дальше, мы видим, что ke7hb уже был модификацией.
erator на форуме w0rm.
Расследование этого имени пользователя показывает, что ke7hb был еще одним из
Имена пользователей w0rm. Таким образом, похоже, что он пытается передать право собственности на
форум самому себе (просто под другим псевдонимом).
Однако журнал изменений базы данных (рис. 18.17) рассказывает нам совсем другую историю.
Глядя на таблицу «userchangelog», мы видим, что учетная запись ke7hb была
переименован в cr00k, а адрес электронной почты был изменен с ke7hb @ iranmail
.com на cr00k@swissjabber.ch.

Бум!

Вернитесь к рис. 18.15: Peace заявляет о праве собственности на w0rm hack. Мир
любит внимание СМИ. Он всегда так делал, и если бы он не пошел в
СМИ, заявляющие о праве собственности на взлом, это было бы еще одним мертвым
конец. Вместо этого теперь мы можем окончательно связать cr00k с пользователем Peace.

```
--
-- Dumping data for table `announcement`
--

INSERT INTO `announcement` (`announcementid`, `title`, `userid`, `startdate`, `enddate`, `pagetext`, `forumid`,
  `views`, `announcementoptions`) VALUES
(1, 'Trusted Section', 'w0rm is under new management, as you can see there will be launched a section named
  "Trusted" which only will be available to the most elite members and/or contributors.
  Payment & info: ke7hb@w0rm.ws', -1, 365, 29);
```

Рисунок 18.16

```
--
-- Dumping data for table `userchangelog`
--

INSERT INTO `userchangelog` (`changeid`, `userid`, `fieldname`, `newvalue`,
  `oldvalue`, `adminid`, `change_time`) VALUES
(61, 387, 'username', 'ke7hb', 'cr00K', 100, 1463697364),
(62, 387, 'email', 'ke7hb@iranmail.com', 'cr00k@swissjabber.ch', 100, 1463697364),
```

Рисунок 18.17

Тщеславие над OPSEC, каждый раз

Как я уже говорил ранее в этой книге, обсуждая Сайпера, *тщеславие всегда превосходит OPSEC* (операционная безопасность). Никогда не недооценивайте готовность угрозы актер проявляет беспечность во имя славы или дурной славы.

В довершение ко всему, на рис. 18.18 показано сообщение Cr00k на KickAss, в котором обсуждается Новое руководство w0rm.

Он хвастался, ясно и просто.

Почему эта связь важна

Привязка Cr00k к Peace имеет большое значение, потому что пользователь Peace также может быть связан «Пингу», бывшему владельцу и администратору Hell Forum. Довольно много опубликована информация о личности Ping (большая часть неверна) и Адский форум. Важным моментом является то, что я теперь связал участника TDO с Пингом, владельцем ныне несуществующего Hell Forum, что означает есть большая вероятность, что он все еще катался с некоторыми из своих старых корешей.

Это сместило *весь* фокус моего исследования с изучения текущих События, связанные с TDO, чтобы собрать как можно больше информации об аде Форум и его участники.

Как оказалось, я был прав. Пинг и его приятель Револьт оказались не только быть крутыми, как воры в сети, но они знали друг друга и в реальной жизни (они только 1 год разницы в возрасте и живут примерно в 5 милях друг от друга).

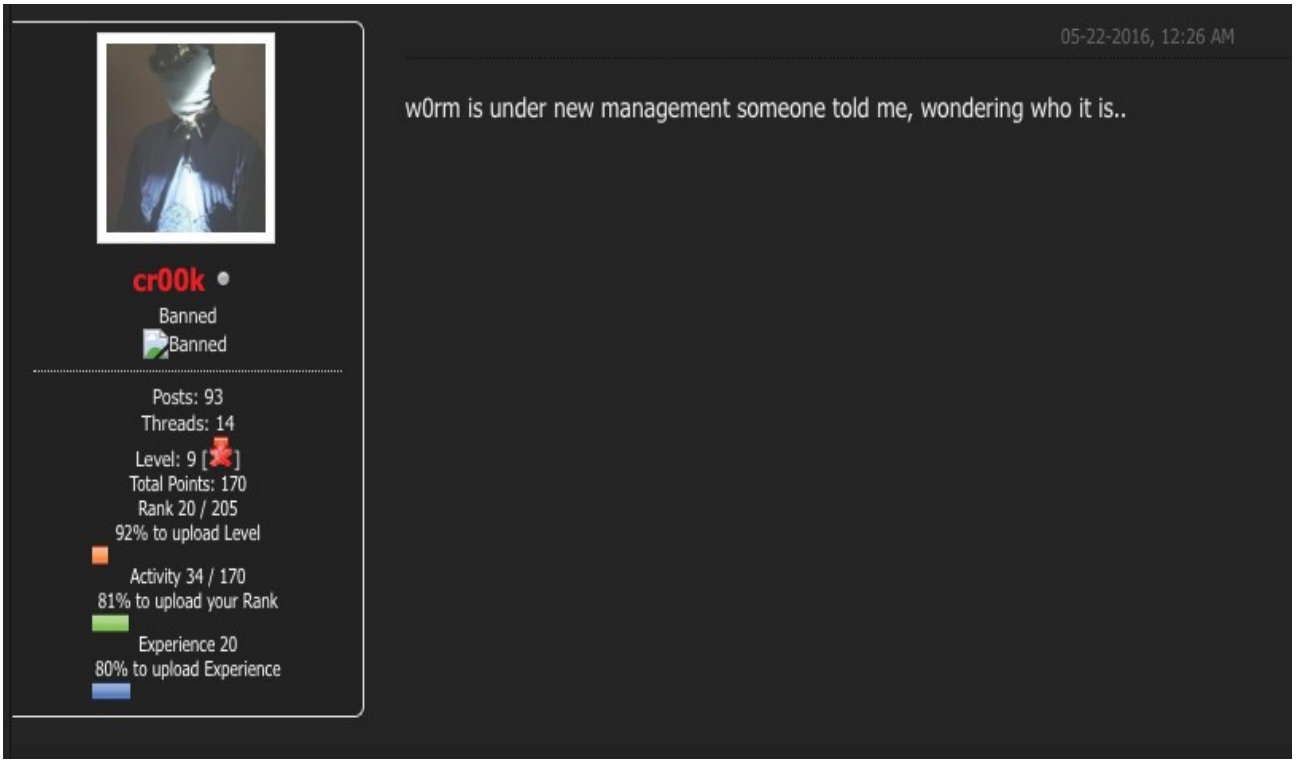


Рисунок 18.18

Что касается моего комментария к большей части опубликованной информации о Ping быть «неправильным». Совершенно блестящим ходом несколько участников Hell Forum пытался привязать личность Пинга к кому-то другому, создав фальшивую внутреннюю драму внутри группы и в конечном итоге «доксируют» не того человека (Дмитрий Барбу). Этот набор от цепной реакции, которая привела к аресту этого человека и нескольких отчетов об угрозах был освобожден, что *подтвердило,* что Пинг был этим фальшивым человеком. К его чести, была одна статья Джозефа Кокса о материнской плате, в которой он смог чтобы раскрыть правду, стоящую за историей. После ареста Дмитрий отказался от настоящей личности. пинга. К сожалению, в то время ему было всего 15 лет, поэтому эти записи были запечатаны и его имя никогда не разглашалось.

Эти дети устроили шоу с собаками и пони, которое было, честно говоря, потрясающим показом того, как Одно сообщение в блоге может сильно повлиять на восприятие следователей. и средства массовой информации.

По сей день тактика TDO не изменилась. Они регулярно общаются с журналистами. В Фактически, подавляющее большинство их историй исходят непосредственно от автора «Несогласных», который руководит блог на www.databreaches.net **. В прямом разговоре с ней Инакомыслящий сказал мне что она провела более 1000 часов в чате напрямую с TDO. Она регулярно передает информацию, которую они предоставляют ей через ее рассказы.**

Я пытаюсь подчеркнуть, что не всегда следует верить тому, что вы читаете, особенно, если источник информации исходит непосредственно от целей, которые вы расследование!

Начнем с малого: Data Viper 1.0

Когда я впервые начал этот квест, у меня был доступ к разного рода информации о вар-
форумов и сохраняя все вручную (буквально используя «Сохранить как», чтобы сохранить
каждая важная страница, с которой я сталкивался). В результате получился беспорядок из HTML-файлов,
Мне нужно было иметь возможность ссылаться. Это, в сочетании со всеми наборами данных, которыми я был
сбор, превратился в кошмар для ручного поиска с помощью grep.

Я начал исследовать различные решения, и прежде чем создать полную версию Elastic-
поисковой базе данных, я наткнулся на DEVONthink, замечательный инструмент поиска для
Mac. DEVON доступен на сайте www.devontechnologies.com .

DEVON - это инструмент для сбора и индексации данных. Перетащите в него данные, систематизируйте
по папкам, и у вас есть довольно приятный инструмент поиска.

Моя база данных DEVON все еще содержит все старые данные, которые я смог очистить
вместе. На рисунке 18.19 показан поиск «cr00k» только внутри KA.
(KickAss) папку.

Стоимость лицензии на DEVON невелика по сравнению со стоимостью строительства.
ваше собственное приложение. Если вам нужен способ легко искать в собственном
записи, это довольно хороший инструмент. К сожалению, это только для Mac. если ты
пользователь Windows или Linux, доступно множество вариантов; dtSearch
- отличный инструмент, которым пользуются многие (www.dtsearch.com). Еще один хороший вариант
это docfetcher (docfetcher.sourceforge.net). Вам нужно будет изучить, какие
решения подходят именно вам.

Резюме

В этой главе обсуждалось, как можно использовать взломанные базы данных и списки паролей.
чтобы найти новую информацию о ваших целях. Реальный пример пользователя F3ttywap был
используется, чтобы помочь завершить матрицу субъектов угрозы, которую мы строили из
предыдущие главы. Поскольку повторное использование пароля настолько распространено среди всех людей (даже
субъектов угрозы), вы всегда должны пытаться создавать новые ассоциации, ища
другие учетные записи, использующие аналогичные пароли.
В этой главе также более подробно рассказывается о Data Viper (www.dataviper.io) и
как информацию с форумов clearweb и darkweb можно использовать для отслеживания
перемещения субъектов угрозы и в правильном контексте могут в конечном итоге привести к их
идентификация. Поскольку Data Viper - это приложение собственного производства, эта глава также
обсуждались способы, которыми вы можете создавать свои собственные, используя свободно доступные инструменты
и наборы данных.

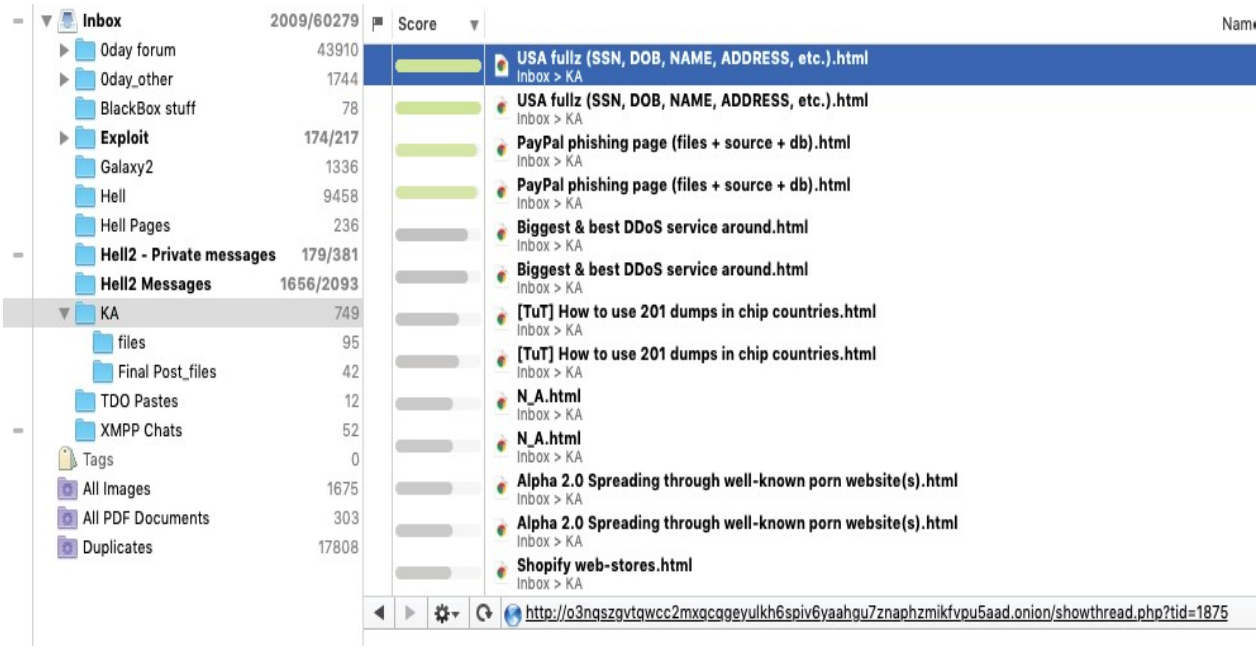


Рисунок 18.19

433

19

В этой последней главе подробно рассказывается, почему обычно стоит закатать рукава и прыгнуть.
в грязи с теми, кого вы расследуете. Вы будете невероятно
удивлен (как и я) тем, сколько информации они неосознанно откажутся.

Вытаскивая их из тени

Я только что вернулся домой с последнего ДербиКона, где я
«Охота на киберпреступников». Я собирался отвезти дочь на футбол
попрактикуйтесь, когда я получил слишком подозрительный твит.
Я знал, что мое выступление на ДербиКоне привлечет внимание определенных людей,
поэтому я специально включил Темного Повелителя в описание выступления,
и обязательно указывал их имя в моих рекламных твитах.
Чтобы сделать еще один шаг вперед, я намеренно спросил Адриана Креншоу (и Der-
byCon) не публиковать видео выступления именно по этой причине. У меня было подозрение
знайте, что люди, близкие к группам, услышат мой разговор и захотят
послушайте, что было сказано.
План сработал. Через несколько дней после выступления я получил следующий твит
от загадочной фигуры, известной как YoungBugsThug (рис. 19.1).

Взаимодействие с злоумышленниками

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

Конечно, это мог быть кто угодно. Но потом я получил следующее частное сообщение в Twitter от того же пользователя (рисунок 19.2).

Почему кто-то спрашивает меня о мире (душевном покое)? Мира нет работает с 2017 года. Это *действительно* привлекло мое внимание. Итак, я начал расследование YoungBugsThug и почему он может спрашивать. Результаты оказались довольно монументально. . .

Но прежде чем мы пойдем дальше, я хотел бы сделать шаг назад и добавить контекст, объясняющий, почему это актуально.

Кто такой WhitePacket?

Многие примеры в этой книге посвящены WhitePacket и Кристоферу Менье.

На протяжении всей книги я упоминаю, что он также является исследователем в области безопасности и владелец собственной охранной фирмы White Packet Security, но на самом деле я никогда не объясните, почему я решил говорить о нем.



Рисунок 19.1



Рисунок 19.2

Если вы прочитали официальный отчет TDO, то уже понимаете, почему я
полагаю, Менье - это nsa@rows.io и главный персонаж Темного Повелителя.
Ниже приводится личный отчет о событиях, которые привели к моим выводам.
который также подготовит почву для значимости личности YoungBugsThug.

Связь Бев Робба

Ранее в благодарностях я выразил свою вечную благодарность Бев Робб.
После того, как я обнаружил, что Cr00k был Ping, изначальным администратором Hell, я продолжил
поиски некоторых из его старых соратников. Я обратился к репортерам, которые написали
про адский форум, и она была одной из них.
Мы с Бев много разговаривали, и она познакомила меня с кем-то, кто
она знала с форумов. Его звали Кристофер Менье, и он также
получил название WhitePacket.
Бев представила Криса как очень талантливого хакера в белых шляпах, который когда-то был
черная шляпа, которая покинула место происшествия при тяжелых обстоятельствах. Крис и Бев
долгие разговоры об аде и почему он решил повесить свою черную шляпу,
и она, к счастью, спасла их всех!
Крис кормил Бев очень убедительными историями о том, как Пинг пытался угрожать
его жизнь за публикацию исходного кода трояна ZIB (ботнета на основе TOR). Это все было
часть очень продуманного заговора, чтобы попытаться связать истинную личность Пинга с кем-то
еще, и это сработало.
Бев очень хорошо отзывалась о Крисе, поэтому, когда я обратилась к нему, я сделала это
предлагая работу по контракту в качестве веб-тестера на проникновение. Во время нашего чата Крис был *чрезвычайно*
абразивный. Конечно, я был незнакомцем, но когда я обычно предлагаю кому-то работу,
они склонны быть более открытыми и благодарными. Он не был.
Вот критический отрывок из нашего первого разговора:

VT:
так откуда ты знаешь Бев?
whitepacket: извините, мне не интересно это обсуждать
whitepacket: вы работаете в правоохранительной сфере?
VT:
в LE нет денег
whitepacket: Извини, чувак, но ты говоришь так, будто ты ЛИ или
Чертов дебил, наверное, последнее.
VT:
почему я дебил?
whitepacket: вы и ваши друзья NightCat / jasonvoorhees / hafez asad
И другие ублюдки могут взобраться на стену из ублюдков
VT:
NightCat?
VT:
jasonvoorhees?
whitepacket: отстой * * к

Он и не подозревал, что одним-единственным словом он раскрыл весь
расследование для меня: NightCat.

Страдинатрас

Чего Крис не понимал, так это того, что NightCat был одним из моих псевдонимов. На самом деле я только однажды использовал этот псевдоним на Exploit.in для связи с одним человеком: Страдинатрас.

Страдинатрас также был известен как «Обфускация» на форуме KickAss, где его логотип был изображением белой шляпы (я предполагаю, потому что он маскировался под специалист по безопасности в белой шляпе). Обфускация очень громко говорила на KickAss о не нравится Арни, подозреваемый глава TDO.

. Имена Страдинатрас и Обфускация взаимозаменяемы - он открыто объявить, что это оба псевдонима, с jabber-адресом obbylord@jabber.de. Интересно, что он, кажется, использует слово *лорд* несколько раз: ObbyLord, Dark Повелитель.

Я обратился к Страдинатрасу по поводу Exploit, потому что не хотел, чтобы он знал мой псевдоним на KickAss, поэтому я придумал новый: NightCat.

На KickAss был специальный пост, в котором Obfuscation открыто критиковал Арни и АНБ (@ rows.io) (рис. 19.3), поэтому я подумал, что он может быть хорошим человеком поговорить о новых подсказках.

Я не знал, что Обфускация и АНБ были одним и тем же человеком, и его сообщения были просто способом отвлечь внимание от себя. В выявлении имя Nightcat для меня, Крис сделал критическую ошибку: он показал себя как Stradinatras и Obfuscation, и запустили колеса для остальной части изучение.

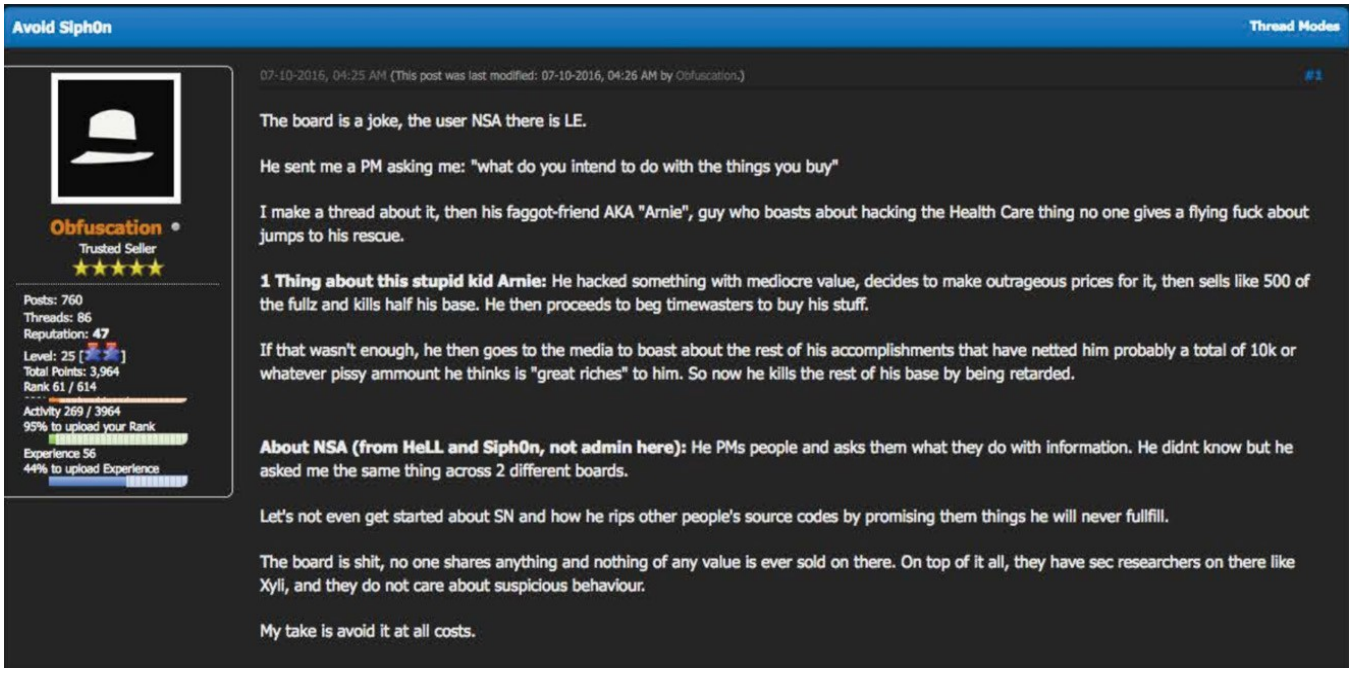


Рисунок 19.3

Обфускация и TDO

Просматривая логи Data Viper, я обнаружил очень интересную тему
относительно личности Арни и кого-то по имени «Билл».
В июне 2016 года на KickAss была опубликована статья о хакере, продающем 10 миллионов
львиная информация о пациентах на черном рынке (рис. 19.4). Эта статья касалась
хакер «Арни» и первое появление Темного Повелителя.
Первый ответ на эту тему был от пользователя l00t5, которого я считаю Арни
(Рисунок 19.5).
Логично, что Арни поручился за продажу своих данных. Следующий,
cr00k звонит (рисунок 19.6).
l00t5 затем отвечает, после чего следует затемнение. На следующем снимке экрана показано
цепочка сообщений и ответ запутывания на l00t5 очень интересны
(Рисунок 19.7).
«Мне кажется, ты Арни». Обфускация была правильной, и он это знал.

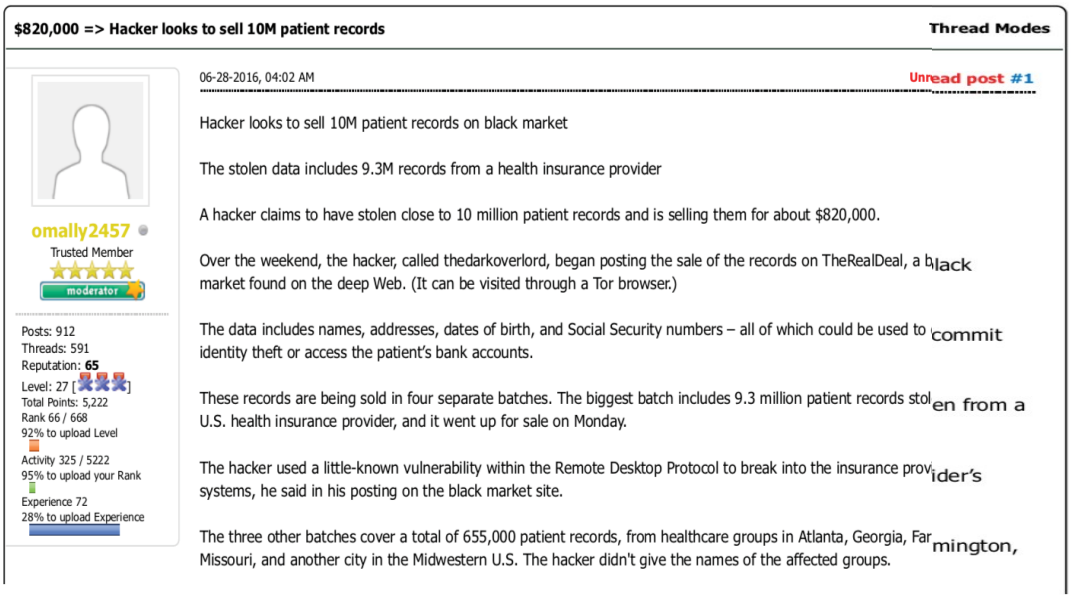


Рисунок 19.4

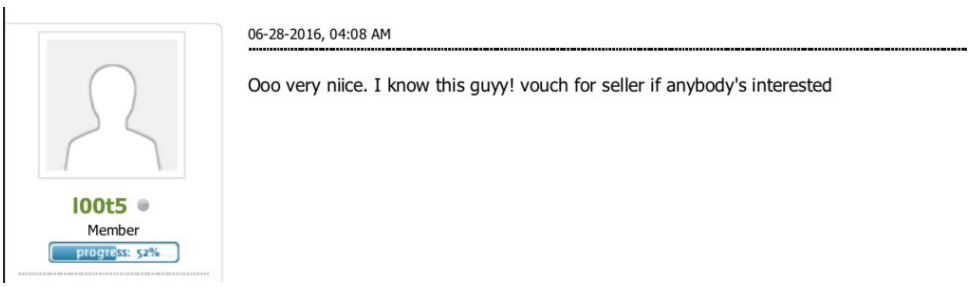


Рисунок 19.5

Помните, как раньше он снялся в «NightCat» с Джейсоном Вурхизом? В качестве оказывается, Джейсон Вурхиз - *тоже* Арни (ссылка была сделана благодаря чудеса стилометрического анализа).

В частном разговоре через Facebook Messenger Вятт раскрывает, что Раскол между Арни и АНБ стал результатом взлома Пиппы Миддлтон. После ареста (и освобождения) Вятта АНБ стало параноиком и предположило, что Арни теперь работа с правоохранительными органами. Это также объяснило бы, почему обфускация (также известная как АНБ) назвал Джейсона Вурхиса (он же Арни) диссонансом.

Следующий ответ в этой ветке, написанный l00t5 и адресованный Obfus- катион - это золотая жила (рис. 19.8).

Исходя из этих разговоров, казалось бы, что l00t5 (Арни) и Obfuscation знают друг друга достаточно хорошо, чтобы позвать друг друга. Мне это казалось очевидным

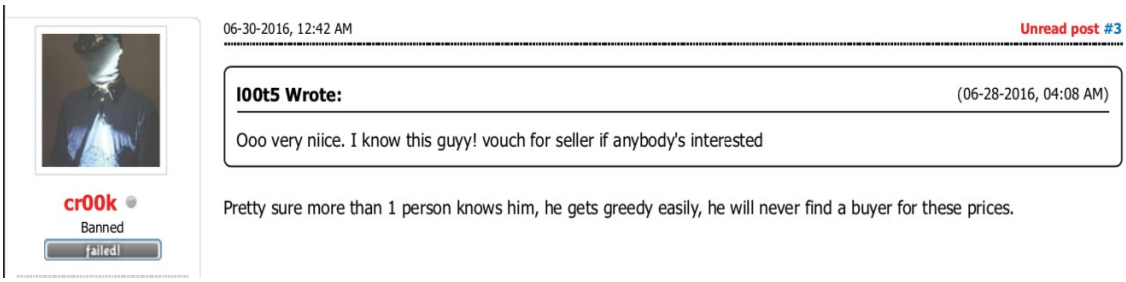


Рисунок 19.6

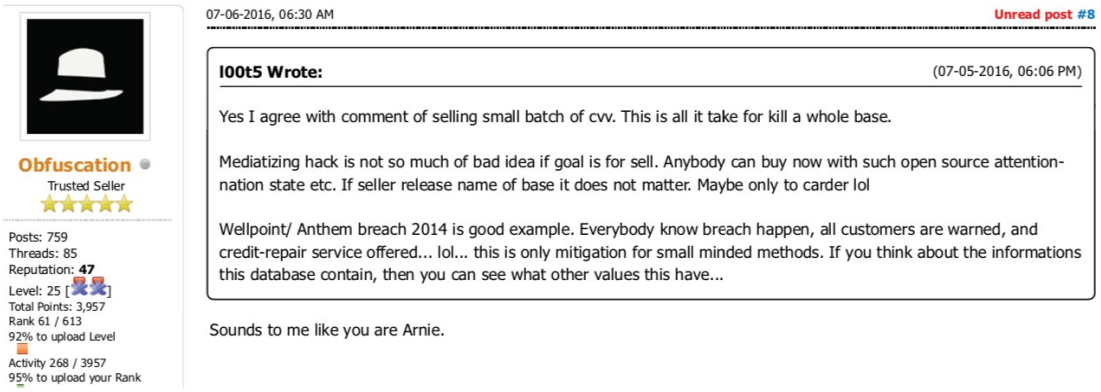


Рисунок 19.7

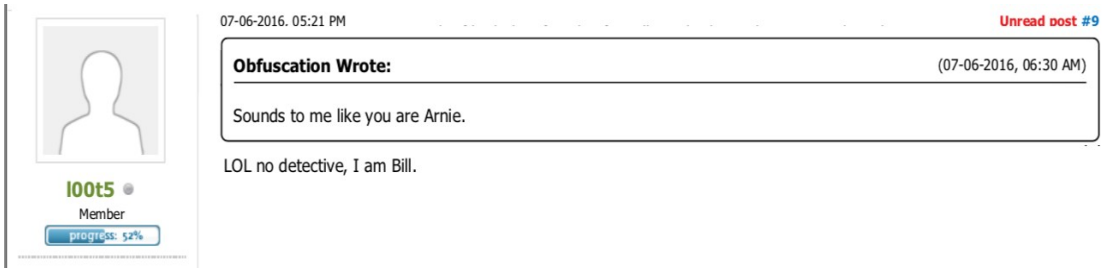


Рисунок 19.8

l00t5 намеренно использовал имя Билл, потому что знал, что оно что-то
Обфускация.
Может, l00t5 знал, что это его настоящее имя?

Кто такой Билл?

Помните, как я упоминал, что у Криса Менье было несколько долгих разговоров
с Бев Робб, и как мне повезло, что она их спасла? Следующий
скриншот - это фрагмент, казалось бы, случайного разговора, в котором Бев спрашивает Криса
для скриншотов (рисунок 19.9).
Важная деталь заключается в том, что Крис использует «машину Windows XP» своего отца, чтобы
запустите Pidgin. Далее у нас есть еще один снимок экрана на следующий день, где
Крис вставляет код с компьютера, который он использует (рис. 19.10).

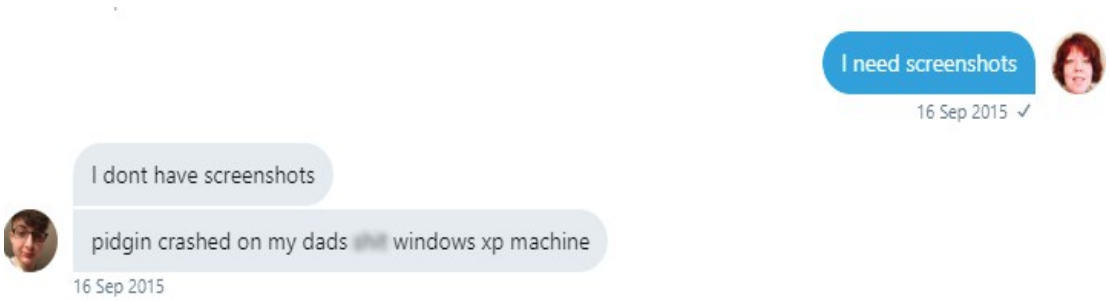


Рисунок 19.9

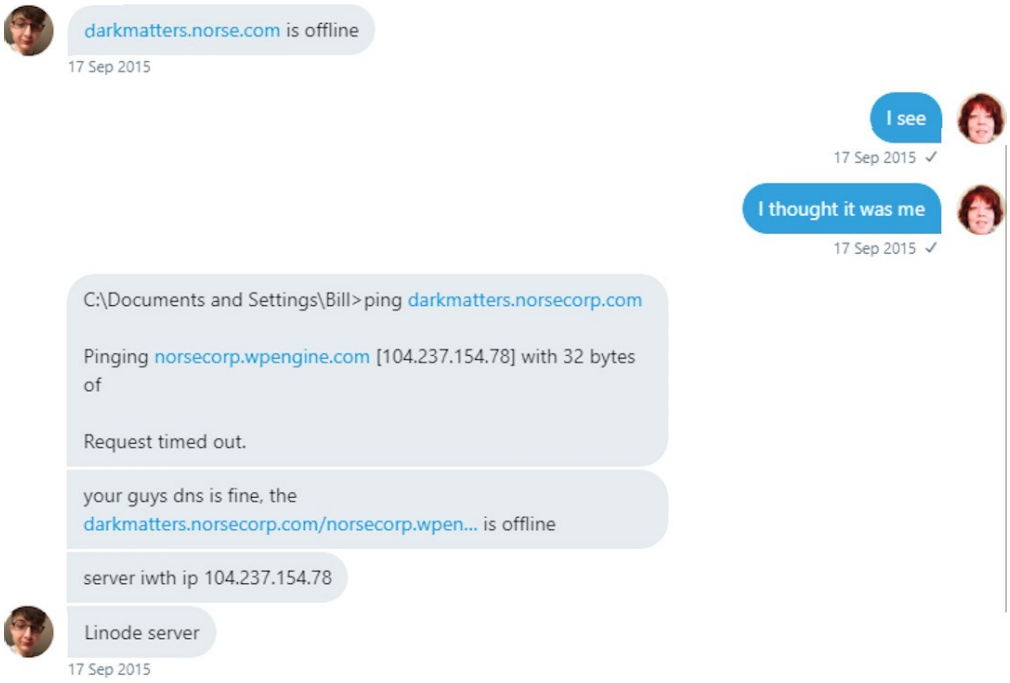


Рисунок 19.10

Те из вас, кто уделяет пристальное внимание, заметят имя пользователя
компьютера Криса - это «Билл». Учитывая то, что Крис несколько раз упоминает, что использует его
компьютер отца, можно было бы догадаться, что отца Криса зовут Билл.

Так кто же на самом деле Билл?

Уильям Мёнёр - отец Кристофера. Что делает это еще интереснее
Билл связан с канадской компанией, занимающейся кибербезопасностью. Крис (бывший)
Страница LinkedIN показывает, что он работал в частной фирме по кибербезопасности, а
предыдущие рисунки показывают, что он открыто использует машину своего отца для общения
с другими людьми.

Существует значительное количество других свидетельств, связывающих эти псевдонимы, все из
который можно прочитать в официальном отчете TDO. Я просто хочу четко заявить, что я
не основывать все свои теории на этой единственной информации.

Имея эту небольшую справочную информацию, давайте вернемся к нашему рассказу о
значение YoungBugsThug (YBT).

МолодойБандит

Теперь, когда мы понимаем, кто такой Крис и почему мы говорили о
его, давайте вернемся к нашему загадочному YoungBugsThug. Во время нашего разговора
YBT спросил меня, пользовался ли я ручкой Dr.X (рис. 19.11).
Честно говоря, нет, никогда. Это не то, на что я обращал много внимания
пока он не появился снова на следующий день.
На этот раз он объяснил, почему спросил меня. К сожалению, я не могу попасть в предварительную
уточняйте детали из уважения к другому вовлеченному лицу, но в двух словах, YBT
спросил конкретного репортера, был ли я доктором X. Теперь у меня была третья фигура, которая
Я мог бы подойти, чтобы попытаться подтвердить личность.
Я спросил репортера и упомянул сценарий доктора X. Я объяснил, что я
поверил, что знаю, кто этот человек, и спросил, откуда репортер знает его.

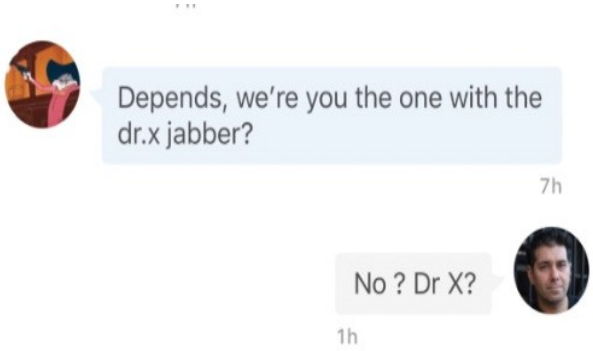


Рисунок 19.11

Репортер сказал немногое, за исключением того, что человек, упомянувший доктора X.
сделал это, используя свое настоящее имя.
К этому моменту я уже знал, что разговариваю с Крисом. Когда я спросил, есть ли у этого человека
настоящее имя Крис, репортер любезно подтвердил мои подозрения.

Как я узнал, что это Крис?

В нашем разговоре было несколько вещей, которые меня подсказали.
что YBT был чрезмерно чрезмерным, пытаясь заставить меня поверить в то, что он
Деннис К. (он же Пинг). Он говорил что-то вроде «как ты меня понял».
Судя по моим разговорам с Деннисом, я не верю, что он когда-либо сказал бы
ничего подобного. Последнее, что он сделал, - это признался, что он что-то знал.
о человеке по имени Деннис, не говоря уже о том , что он *является* этим человеком.
Но по-настоящему важной подсказкой для меня был тон разговора. Это был
Фактический момент, когда мы переписывались через Signal, я простудился, потому что его
тон вызвал у меня мурашки по коже. В частности, он делал заявление, а затем заявлял о моих
имя сразу после. В нем был очень агрессивный тон, как будто кто-то пытается показать
доминирование. Но он также делал это неоднократно, как если бы он пытался
подставил меня. Рисунок 19.12 - прекрасный пример.
TDO был точно таким же.
Это действительно сложно объяснить, но были времена, когда он и
У меня будет нормальный разговор, а он вставит предложение
это вернет вас к реальности и заставит вас понять, кем вы были
иметь дело с кем-то, кому нужно чувствовать свое превосходство над вами во всех отношениях. Это приходит
от него волнами и безошибочно.
Вот пример из разговора с TDO:

TDO: Вы, белые шляпы, идиоты.
TDO: Никто не публикует уязвимости Xen на вашем сайте, Винни.
TDO: И после этого вам нужно отпустить свое самоуверенное
«одержимость» нами. Это нездорово, Винни. Мы волнуемся
о вас.

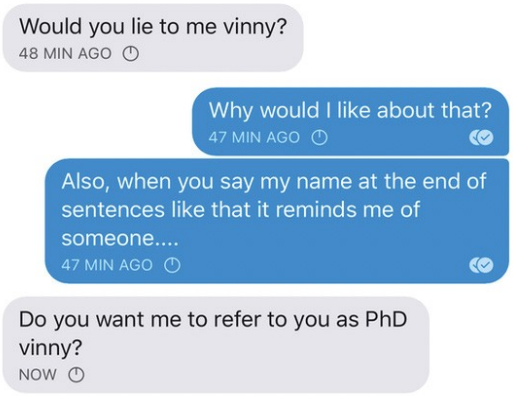


Рисунок 19.12

Многие злоумышленники знают, кто я, и знают, что говорят со мной.
напрямую. Никто никогда не использовал мое имя. Можно утверждать, что такое поведение
было направлено только на меня и просто совпадение.
Ниже приводится личная беседа между TDO и отредактированным третьим лицом.
участник по имени Джеймс.

TDO:
Мы понимаем ваше разочарование, Джеймс. Возможно, ФБР
совершил набег на вас, потому что вы разгласили нам разведданные?
J:
Только пого и моя жена знают, что ФБР просило о подарке.
карты
TDO:
Вы имеете в виду [Несогласие], Джеймс. У нее есть имя, знаете ли.
J:
О .. да, я написал это в Твиттере ...
J:
подарочные карты .. так .. ничего страшного .. моя жена только что напомнила
меня
TDO:
Ты нам очень помог, Джастин. Мы в долгу перед тобой
Интернет-деньги.
J:
Грустно, ты должен врачам и пациентам на самом деле мужчина
TDO:
Тск-цк, Джеймс. Вы общались со слишком многими
люди за пределами вашего региона.
J:
ты самый странный человек на земле
TDO:
Тебе будет очень весело сменить шляпу, приятель.
J:
Нет я бы не стал
TDO:
Джеймс, ты стал довольно занудным. Что с этим случилось
веселый любвеобильный персонаж, которого мы знали?

Казалось бы, язык довольно последовательный.
Была еще одна подсказка, с которой я столкнулся. Назовем это глазурью на торте.

Подключение к ботнету Mirai?

Где-то в январе 2019 года британский суд вынес приговор Дэниелу Кею, также известному как BestBuy.
он же Попорет, владелец / администратор торговой площадки Darkweb TheRealDeal, двум
лет и восемь месяцев тюрьмы за подключение и использование ботнета Mirai IoT.
Согласно нескольким статьям, Кэй - одна из многих, кто скачал
исходный код вредоносного ПО Mirai, когда он был впервые опубликован в Интернете на
Октябрь 2016 г.
Перенесемся в март 2019 года, когда Каталин Чимпану, обозреватель киберпреступлений
для ZDNet опубликовал следующий твит о Кайе и ботнете Mirai.
В его сообщении указывалось, что полиция изъяла журналы Skype, в которых подробно описывались разговоры с
двое других сообщников Мираи, одного по имени Крис (рис. 19.13).
Как интересно, что наш друг YoungBugsThug дошел до того, что спросил Каталина
если Крис был из Канады.

Я не видел восстановленной информации, поэтому у меня нет окончательного
доказательства того, что Крис (NSA / TDO) - это тот же человек, о котором говорится в журналах Skype.
Я основываю эту связь на том факте, что наш Крис также был администратором
Торговая площадка TheRealDeal (под псевдонимом Peace of Mind), которая принадлежала
Дэниел Кэй. У этих двоих есть долгая и очень прослеживаемая история совместной работы.
возвращаюсь на адский форум.
Ниже приводится отрывок из разговора между Деннисом К. (whereami) и
Крис обсуждает их участие с BestBuy.

whereami: Bestbuy уклоняется
whereami: Как будто вернулся в Великобританию и столкнулся со многими обвинениями
whereami: Я клянусь, что это TRD, или они арестовали TRD, чтобы захватить все мои
Деньги
whereami: В любом случае все трое из нас трахались
whereami: Допустим, trd не BB, это означает, что он был арестован из-за
год назад
whereami: Тогда дело закрыто

YBT и я в конце концов переместили наши разговоры в Signal, где он предложил
мне несколько громких баз данных в обмен на конфиденциальную информацию -
специально запечатанные протоколы обвинительного заключения - по Дэниелу Кею и имеющейся информации
вопрос о том, будет ли он экстрадирован в Соединенные Штаты (рис. 19.14).
Наконец, мой личный фаворит, он категорически спрашивает меня, думаю ли я, что он будет
предъявлено обвинение (рис. 19.15).



Рисунок 19.13

Как указывалось ранее, этот раздел является своего рода предположением, учитывая существующие отношения между BestBuy (Даниэль) и Peace of Mind (Крис). Есть еще
чем достаточно доказательств, чтобы показать, что двое работали вместе над другими взломами и проекты - торговая площадка TheRealDeal является одной из крупнейших, закрытых
с впечатляющей многомиллионной аферой с выходом.

Если кто-либо, читающий это, знает кого-либо в Европоле, имеющего доступ к Журналы чата Дэниела Кея, я надеюсь, что эта информация поможет понять, кем может быть «Крис».

Почему это открытие было таким потрясающим?

Было что-то, что меня не устраивало. На рисунке 19.16 YBT казался
чтобы продолжить о том, почему я считал Пинг душевным покоем.

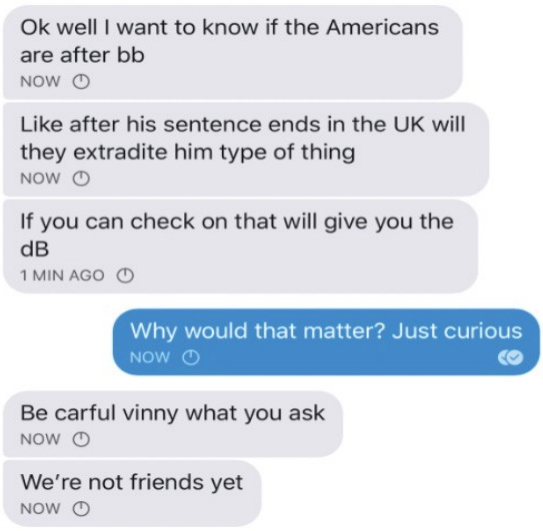


Рисунок 19.14



Рисунок 19.15

Я долго думал об этом, прежде чем понял что-то действительно важное.
tant: Я ни разу не усомнился в связи между миром и пингом. Я не могу вспомнить
где именно я это прочитал, или почему я создал эту ассоциацию, но
из того, что я помню, большинство статей и отчетов, которые я читал, не имели проблем
Цитирование мира с Ping.
Когда я вернулся и посмотрел, я не нашел ни единого доказательства
соединяя два. Причина, по которой этот разговор был таким значимым, заключается в том, что вверх
до этого момента я безоговорочно считал, что Ping и Peace - одно и то же
человек.
Как оказалось, я ошибался.
Это была огромная пощечина. Почему я так долго предполагал, что эти
два человека были связаны? Я даже обратился к некоторым друзьям при другой угрозе
исследовательских фирм и спросили, знают ли они, почему эти два псевдонима связаны:
никто не смог найти в их записях и следа информации.

Вопрос ко всему!

Когда я вернулся и посмотрел на все доказательства, мне стало намного легче.
связать Душевное равновесие с АНБ, и тем самым закрыл несколько

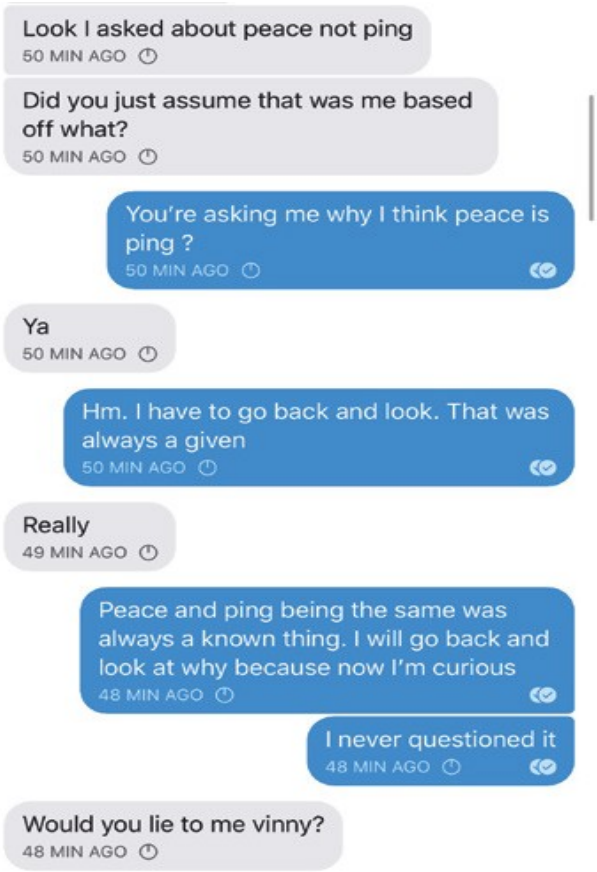


Рисунок 19.16

другие недоработки о других псевдонимах. Если бы YBT не связался со мной из страха перед
то, что я сказал в своем выступлении, я бы продолжал верить, что душевный покой был
на самом деле Деннис К. (Пинг), а не Крис.

Поскольку у этих двух людей так много общих псевдонимов, это
могут не иметь значения в глазах закона - только то, что они замысловато
взаимосвязаны. Но с точки зрения исследования этот опыт научил меня
очень ценный урок: *подвергайте сомнению все* .

Никогда не полагайтесь на предположения, независимо от того, насколько конкретна информация или как
многие другие люди (или исследователи безопасности) говорят вам то же самое. Если
вы не можете соединить части самостоятельно, значит, вы не можете предположить, что это правда.

Создание потока информации

По большей части я общаюсь с злоумышленниками, используя различные псевдонимы.
Однако некоторые злоумышленники все равно будут разговаривать с вами, даже если они знают, кто вы
действительно есть. Может быть ряд причин для существования такого типа отношений,
но чаще всего это происходит потому, что у вас есть то, чего они хотят.

Последние полгода я разговариваю с русским актером (он же Ping
он же Cr00k, и один из двух людей, использующих имя NSFW) почти ежедневно
основание. Он знал, кто я, с самого начала, потому что я сказал ему, когда впервые
подошел к нему, сославшись на статью Кребса обо мне как на предлог, чтобы поговорить с ним.
Со временем мы установили прочное взаимопонимание. Я не сомневаюсь, что он был
говорить со мной, чтобы следить за тем, что я знаю, а также чтобы накормить меня
информация, когда появляется возможность. Как и любой хороший злоумышленник (а он
определенно находится на высшем уровне), он знает, что для того, чтобы его дезинформация была
эффективный, он должен быть дополнен значительным объемом реальной информации.

Подумайте об этом так: если бы он сказал мне только ложь с того момента, как мы начали
говоря, я бы никогда не стал доверять тому, что он говорит. С другой стороны, если он кормит
мне второстепенную (но достоверную) информацию в течение нескольких месяцев, потом он может подбросить ложь
относящиеся к нему, которым я, естественно, должен доверять.

Как только такие отношения развиваются, происходит сильный поток информации.
это может быть невероятно успешным способом сбора информации о злоумышленнике
группы вне его круга. Чем меньше он заботится о людях (или чем дальше
от него они действуют), тем больше он будет полностью раскрываться и
расскажу то, что он знает.

Как и в случае с любым другим человеком, если вы можете попросить их рассказать о теме, они раскроют
много важной информации в пылу разговора. И учитывая
хрупкая межличностная динамика отношений с субъектом угрозы, часто это легко
найти их в ситуациях, когда они враждуют, или даже помочь разжечь
сама вражда.

Использование хакерской драмы

Еще одна не менее важная тактика - использовать возникающие детские аргументы.
между группами. Вы должны набраться терпения и дождаться этого, но это всегда происходит.
Актеры неизбежно будут пытаться работать вместе, и, прежде чем вы это заметите, кто-то
расстроятся, и вся группа начнет мстить друг другу.
Это отличная возможность прыгнуть и раздуть пламя. Номер
группы злоумышленников тусуются в похожих каналах Discord и IRC, так что до тех пор, пока
поскольку вы отслеживаете и регистрируете эти каналы, вы сможете выбрать
активизируйте действие, прежде чем удалить его.
Ниже приводится недавний пример внутренней драмы, происходящей между
GnosticPlayers и еще несколько человек из Discord:

Сонный
Между прочим, Момондо, ты знаешь, что я знаю, кто ты. я
будет держать рот на замке, потому что я действительно не
как держать шахту закрытой.
AmIEdgyEnough @UnPirlaACaso, кто знает, может быть он все еще
UnPirlaACaso nah: смеется
AmIEdgyEnough Да, наверное, нет
UnPirlaACo сомневаюсь, что попо будет заботиться о нем + он живет в третьем
мир, он понятия не имел, что такое ФБР и дерьмо
это ахахаха
AmIEdgyEnough Loooool
UnPirlaACaso ФБР даже не сможет его найти ахахахаха
как, черт возьми, эта страна действительно существует?
и я бы добрался до него только за это ахахаха
AmIEdgyEnough Lmao да
Liff
Вам просто 69d, что ваш партнер живет в 3-м мире
страна
UnPirlaACaso не секрет
он всегда говорил публично, поэтому сомневаюсь, что это будет
проблема ахахаха
Liff
ах ладно тогда
Сонный
Никому не составит труда найти Момондо, когда
фотографии его дома рядом с Макдональдсом проиндексированы
по всему гуглу
AmIEdgyEnough Lmao, если вы арестуете его, то 100% будет
как и 3-4 других ареста lmao
Сонный
Момондо уже арестован
Он заключил сделку с USRS
Как только он вернулся, я доил его, чтобы узнать все подробности.
AmIEdgyEnough Ах да
Сонный
Все, что я могу сказать о nclay, это то, что он будет вечно
придется беспокоиться о тяжелом тюремном заключении.
Достаточно и так.
AmIEdgyEnough Нет, он не будет, у аутизма есть свои преимущества

Сонный
Вы аутист, Фотон?
AmIEdgyEnough А также французская судебная система
Сонный
Пошмарк знает, что вы аутист?
AmIEdgyEnough @Sleepy
давай и дай им знать
Посмотрим что будет

Из этого разговора можно почерпнуть много информации,
но для меня самая интересная статья была про Пошмарк.
Поскольку я уже знаю, что русский язык (он же NSFW) также использовал псевдоним Photon,
и отвечает за взлом Poshmark (потому что он рассказал мне, как он это сделал
и поделился копией данных со мной), этот разговор только связал его
на новый псевдоним: AmIEdgyEnough.

Было ли это реальным?

Еще один вопрос, который вам нужно задать себе, особенно в подобных ситуациях:
является ли то, что вы читаете, настоящим или постановочным. Это не потребует больших усилий
чтобы группа этих парней собралась вместе и создала фальшивый сценарий; или сценарий
что более правдоподобно, так это то, что большая часть драмы реальна, но два друга
сговорились бросить в горшок один кусок дезинформации, чтобы просто бросить
исследователи от их TRAIL.
Поскольку я знаю историю NSFW, я знаю, что это одна из областей, в которой он преуспевает.
Насколько я могу проследить его происхождение, он манипулировал СМИ и
исследователи с именно такой дезинформацией.

**Стоит отметить, что на данный момент мои связи с NSFW были
полностью вырезать. После того, как было объявлено о моем выступлении на Дербиконе («Охота на киберпреступников»)
он начал отдаляться, и в конце концов мы перестали разговаривать на несколько дней
до этого все рухнуло. Поскольку мы с ним общались, используя мои настоящие
имя, и поскольку он знает, что я болтаюсь на том же канале Discord, это не будет
вне области вероятности, что информация о NSFW и Poshmark была
для моей выгоды.**

Нет никакого способа узнать наверняка, поэтому единственное, что я мог сделать, это начать спрашивать
вопросов. Когда я это сделал, мне сказали, что AmIEdgyEnough подошла к кому-то
со следующим сообщением, почти ожидая моей реакции:

AmiEdgy: Да, кстати, если кто-нибудь спросит, куда я иду, скажите, что мой псевдоним
это Фотон и что я собираюсь поступить в университет
так что я не буду активен. Я уверен, что когда я пойду, все будут
сначала спросить.
Также не забудьте сказать, что я не буду активен на рейдфорумах.

Мой партнер по-прежнему будет активен, используя профиль NSFW,
так что продолжайте взламывать хеши, если он спрашивает, но не говорите
любой фотон - мой псевдоним.
Если кто-то спросит, является ли Photon AmiEdgyEnough ответить «нет». Если
кто-то говорит, что NSFW - это AmiEdgy, хватит солгать и сказать да,
просто чтобы люди не знали, что я фотон, но это
Я кто-то другой. Я могу заплатить вам lmk.

Текст противоречит сам себе - скажите, что я Фотон, не говорите, что я Фотон, но это также ясно, что AmIEdgyEnough пытается создать разрыв между NSFW и Фотон.

Как это ни сбивает с толку, когда вы разбиваете это сообщение с недосказанностью. учитывая, что Photon и NSFW - это два разных человека, это фактически делает Отличный смысл. Он (AmiEdgyEnough) просит этого человека солгать и сказать что он не Фотон, но если кто-то спросит, является ли он NSFW, солгите и скажите «да». В ложь в том, что нынешний NSFW - его партнер, а не он. Расшифровка этого достаточно, чтобы взорвать чью-нибудь голову!

В поисках других улик

К счастью, были и другие подсказки, которым я мог следовать. AmIEdgyEnough и я уже говорил, и ему всегда казалось, что он изо всех сил старался изо всех сил ******.

После всего этого он, видимо, «уловил ветер», о котором я спрашивал. и отправил мне сообщение, в котором просил меня перестать расспрашивать о нем и никогда больше не связывайся с ним.

Игра началась.

Иногда простой разговор с человеком может дать вам ответы, которые вы ищете ибо, даже если они на самом деле ничего не говорят. Во время нашего последнего разговора AmIEdgyEnough начало казаться *очень* знакомым, но в каком-то смысле я не слышал какое-то время:

XX: Давай, талантливый парень. Как вы думаете, что я сделал? Или, может быть, в вашем
наркацистический мир, о котором, как вы думаете, люди на самом деле говорят
Вы?
Ами: «Маленький наркацистический мир» подразумевает, что я передаю чувство
важность себя.
XX: Да, это именно то, что я имел в виду.
Ами: Однако это ПРОТИВОРЕЧИРУЕТ тому, что вы спрашивали
обо мне БОЛЬШЕ, чем мой предполагаемый нарциссизм.
Ами: Ну, ты можешь отдыхать с миром, прекрасно зная, что ты не важен.
в этом и нет того, кого я боюсь или, следовательно, беспокоюсь.
Это те, кто вы есть
Говоря о том, вот эта информация как таковая.
Ами: Кто, к сожалению, убедился, что это невозможно, или я
свяжитесь с ними.

XX: мне нужно сосредоточиться на моем классе сейчас
Ами: И давайте будем честными, ты не потеряешь мою пропажу.
Сосредоточьтесь на этом классе. Ваш гребаный дегенеративный мозг
не может хранить информацию более суток.
Так что бесполезно сосредотачиваться или не сосредотачиваться.
Потому что я не говорю, как толстые болваны, которые пристрастились к
Discord 24/7.
XX: Ты прав, я просто устал с тобой разговаривать.
Ами: Вот почему вы чувствуете усталость из-за того, что не можете
расшифровать четкие запутанные сообщения.
Ами: Ну, если бы это было не п, то, с кем бы ты ни говорил, нет
достойная информация, если они не на связи.
Итак, на этой ноте, вы можете использовать свой недостаточно используемый мозг.

Кем бы ни был этот человек, ясно, что он пытается заставить себя звучать слишком умен в общении.

Этот стиль общения напоминает мне о ком-то конкретном. . . и что за совпадение, что это возвращает нас обратно к тому, с чего мы начали.

Возвращение в TDO

Ранее в этой книге я упоминал о двух различных фигурах TDO. TDO1 (он же Арни) был руководителем группы в 2016 году, а TDO2 (он же NSA@rows.io) был лидировал в группе с 2017 по 2019 год.

У меня никогда не было прямого контакта с TDO1 (с тех пор, как его срок полномочий закончился в 2016 году), но я прочитал несколько его стенограмм чата и сообщений на форуме.

При ребрендинге TDO в 2017 году они сделали это, используя английский королевы в попытаться стандартизировать все свои коммуникации. Это позволяло различать- побуждать людей действовать в качестве представителей группы.

В частном разговоре с Вяттом он упоминает, что на самом деле TDO было три основные участники - он, «ребенок», который хорошо разбирался в хакерских атаках, и кто-то, кто хорошо владеет языком и письмом.

Мое первое прямое взаимодействие с TDO произошло примерно в октябре 2017 года. По сей день Я могу сказать, что человек, с которым я разговаривал на этом свидании, был намного спокойнее чем человек, с которым я разговаривал каждый раз с тех пор. Мне всегда было интересно, кто эта таинственная- этот человек был - и я знал, что это не Арни, потому что он находился под стражей в время в Великобритании.

Сходство языков само по себе, как правило, и близко не было бы достаточно, чтобы прийти к любому разумному выводу. Однако, поскольку я уже есть более чем достаточно доказательств связи NSFW и Photon с Cr00k (который был непосредственно член TDO), не будет преувеличением думать, что я разговаривал с Cr00k 11 ноября 2017 года.

Решение последнего вопроса

Был еще один мучительный вопрос, который разрешился сам собой, когда я начал убеждать меня. Сидера, что Cr00k был одним из людей, говорящих под псевдонимом The Dark Overlord: Куда идут деньги?

Вывод биткойнов

Ниже приводится отрывок из разговора с TDO по поводу отказа-изъятие их «заработка»:

1:55 утра TDO В прошлом году мы заработали почти 10 миллионов фунтов стерлингов.
1:55 утра VT, это впечатляет
1:55 утра VT, как вы обналичиваете это?
1:55 утра TDO Мы этого не делаем.
1:55 BT справа
1:55 утра TDO Это большой секрет.
1:55 TDO Вы хотите видеть наши адреса?
1:55 утра VT, это не большой секрет
1:55 утра VT Я не могу представить, чтобы многие биржи BTC предлагали наличные
так много денег
1:56 AM TDO Я покажу вам прямо сейчас, раз уж вы такой эгит.
1:56 утра VT Конечно. Покажите мне.
1:56 утра TDO Конечно, нет, мы никогда не обналичиваем их.
1:57 утра VT SMH. ты не понимаешь мою точку зрения
1:57 утра VT Если вы не можете обналичить их, значит, деньги застряли.
там
1:57 AM TDO Это не так, вы этого не понимаете.
2:00 утра TDO Минутку. Имейте в виду, я подпишу их, если потребуется.
2:01 TDO 1EMWwmBJuvvES3eb51pNJnjEvD1RgQ7evA
2:01 TDO 1NcgGFPT23KawMMp8vp1TKxV1qEitpPtdk
2:01 утра TDO Давайте начнем с этих двух.
2:03 TDO Вы думаете, что мы убыточны, а вы
неправильный.

Мне всегда было интересно, как TDO смог обналичить такие деньги.

Еще один взгляд на нашего приятеля Cr00k дает очень правдоподобный сценарий. Если я прав, Cr00k, которого я считаю Деннисом Карвуниарисом (Instagram profile dio_the_plug), живет в Калгари, Канада. Простой поиск в Google показывает что его отец - известный и отмеченный наградами шеф-повар.

Поиск месторасположения бизнеса ничего полезного не дал.

Однако я извлек еще один очень ценный урок: *не забывайте искать* реальный адрес, о котором идет речь, а не только имя!

Сделав это, я увидел кое-что очень интересное (рис. 19.17).

Верно. В локации есть собственный биткойн-банкомат. Что лучше
способ анонимно вывести свои кровно заработанные вымогательские деньги?
Я не знаю, каким образом группа смогла добыть вымогательское вознаграждение.
монет, или если они использовали миксеры для монет, или какой-либо другой метод. Я просто считаю, что это
интересное совпадение .

Резюме

В этой главе освещены некоторые из моих прямых контактов с разными
субъекты угроз и объяснили, почему может быть необходимо напрямую взаимодействовать с ними
во время расследования. Иногда может потребоваться их вытянуть и
чтобы они подошли к вам, а в других случаях может потребоваться запустить или заправить
внутренний конфликт между ними, чтобы спарить их друг против друга.
Как я узнал в ходе этого процесса, злоумышленники могут неосознанно
отбрасывают величайшие ключи к разгадке своей личности просто из страха и самосохранения.
Какими бы ни были ваши методы общения с ними, обязательно возьмите то, что
они говорят с недоверием и ставят под сомнение любую информацию, которую они вам представляют.

Рисунок 19.17

453

20

Бывают дни, когда ты просто просыпаешься и что-то совершенно неожиданное бывает.

Я думал, что закончил с этой книгой, а потом просто случилось: GnosticPlayers, известная группа, получившая известность благодаря серии очень громких взломщиков, решил публично опубликовать свою причастность к краже 10 миллионов долларов криптовалюты.

Беспрецедентно признав свою вину, Нклей, лидер группы, решил покаяться в своих грехах и публично объявить о своей причастности к GateHub взлом.

То, что произошло потом, было столь же неожиданным: предполагаемое напряжение между члены группы привели к публичной утечке частной коллекции группы взломанные базы данных на RaidForums.com, впоследствии названные «утечкой». Практически все ценные украденные базы данных группы, содержащие миллиарды львов учетных записей пользователей, паролей и другой частной информации о клиентах опубликовано в Интернете и внезапно стало доступно для бесплатной загрузки.

Нклей продолжал выражать свое недовольство на публичных форумах, и с каждым новым post пришел дополнительный кусок, казалось бы, идентифицируемой информации. Не только признал ли GnosticPlayers свою вину, но внезапно решил участвовать в беседах, в которых он открыто использовал бы свои настоящие имена и личности.

Разрезая

Дезинформация

Взлом на 10 миллионов долларов

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

В кратчайшие сроки оба члена группы опубликовали свой полный докс,
и Nclay, лидер группы, отказался от своих псевдонимов и теперь имел в виду
себе по его настоящему имени.

В смеси всего этого замешательства и волнения одна из моих хорошо зарекомендовавших себя
контакты в верхних слоях группы открылись мне как охранник
исследователь и исследователь. Предположительно, этого человека нанял один из
жертв группы более года назад, чтобы проникнуть и расследовать GnosticPlayers в
чтобы раскрыть истинную личность Nclay. Очевидно, мы были на одной стороне. . . .

Он быстро начал кормить меня информацией о своих открытиях, которые все
похоже, подтверждает информацию, которую публикуют участники группы
их собственная идентичность.

Это было просто потрясающе! Ответственность за все эти преступления могла быть
теперь можно легко отнести к двум мальчикам, живущим во Франции, все благодаря предполагаемому
нестабильное психическое состояние лидера группы.

Наконец, в понедельник, 28 октября 2019 года, Nclay, по-видимому, был настолько раскаявшимся.
за его преступления и публичное предательство своих друзей, что он решил положить конец своему
собственная жизнь.

На этом история была завершена. Преступления учтены, данные
разоблачили, и пресловутый хакер исчез навсегда.

Я называю быков ** т.

Более года я лично общался со всеми участниками
GnosticPlayers, и я вырос, чтобы понять каждого из участников и их
личности, а также их взаимодействие друг с другом. Я верю всему этому
сценарий должен быть тщательно спланированным шоу, предназначенным для отправки исследователей безопасности
и правоохранительные органы идут по очень хорошо освещенному пути к неправильным подозреваемым.

Вдобавок *все* базы данных Gnostic не просочились. Утечка, пока
обширный, был лишь частичным и содержал в основном более старый материал. Новые базы данных
вроде Quora, Epic Games (Fortnite) и многих других не попали в список, большинство
вероятно, потому что они по-прежнему чрезвычайно ценны. Я тоже не верю ни одному
во-вторых, что Nclay покончил с собой.

Во что я верю и что собираюсь показать в этой главе,
в том, что эти события были тщательно организованы человеком, который не
только молчаливый член GnosticPlayers, но также тот же человек, который помог
оркестровать докс Пинга (и кадрирования Димитрия Барбу), о котором говорилось ранее
главы этой книги.

Гностик

Примерно в феврале 2019 года название GnosticPlayers возникло благодаря нескольким высоким
базы данных профилей, которые поступили в продажу на Dream Market (торговая площадка в даркве6е).
Некоторые из взломанных баз данных включали MyFitnessPal, MyHeritage, EyeEm, 8fit,
и WhitePages.

В продажу поступил почти 1 миллиард украденных записей данных, и это было всего лишь
первая огненная распродажа группы, получившая название «раунд 1».
Хотя это было мое первое знакомство с группой GnosticPlayers, я уже
разговаривал с участниками группы несколько месяцев. В течение курса
из следующих шести месяцев будет еще пять мгновенных продаж только что украденных
базы данных.
Группа состояла из двух основных участников: Nclay и DDB (и третий,
NSFW, который будет раскрыт позже). Nclay был хакером, а DDB -
продавец.
Флэш-продажи были результатом внутренней напряженности между членами группы.
берс. Основываясь на моих разговорах с двумя участниками, Nclay решил предать
DDB и выставил на продажу все свои громкие базы данных.
Следующее - личное сообщение, отправленное мне Nclay:

вне досягаемости:
DDB все взломал, взял кредит и сделал сам
имя, пока он не дерьмо
вне досягаемости:
потому что он взял на себя ответственность за взломы, которых не делал, и
так долго хвалил деньги
вне досягаемости:
теперь он чувствует, что он хорош

Вскоре после того, как первый раунд баз данных был выставлен на продажу на Dream Market,
несколько баз данных использовались веб-сайтом Троя Ханта HaveIBeenPwned.
сайт - согласно информации, размещенной на сайте, - источником, запросившим
это должно быть приписано Куроишу или Габриэлю Кимиаи-Асади Бильдштейну ».
В то же время докс Нклая (личная информация) просочилась в
небольшая группа людей (в том числе и я), называющие его Куроиш или Габриэль
Бильдштейн.

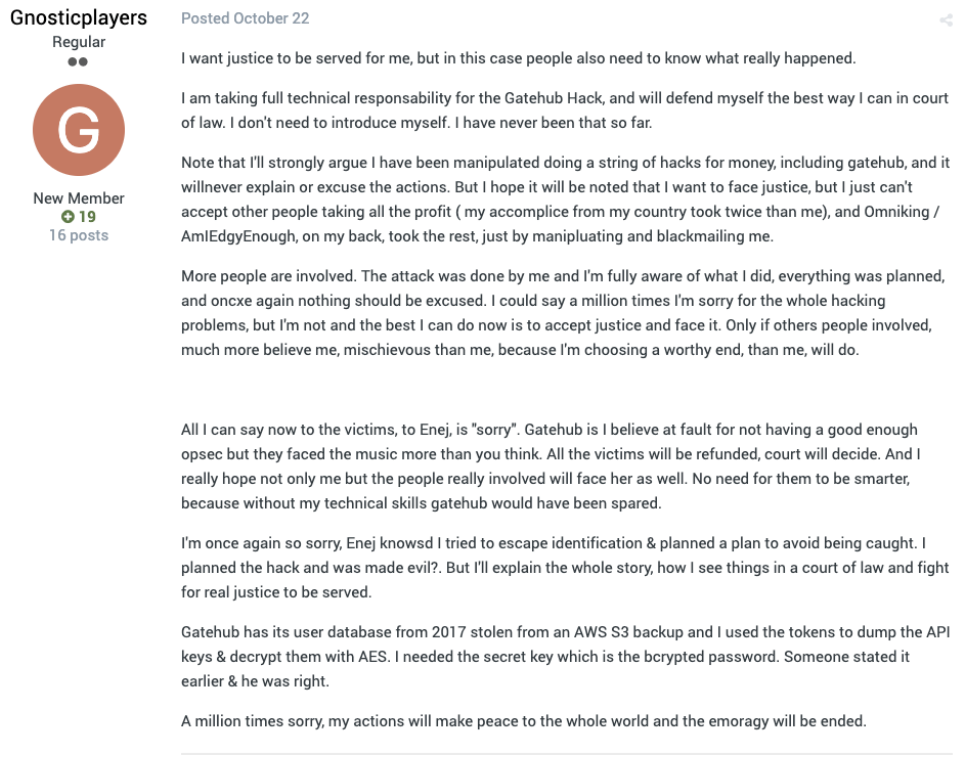
Габриэль Бильдштейн, также известный как Куроиш, - известный хакер, ранее арестованный
Французские власти в связи с взломом Vevo, который испортил "Despacito" и
несколько других музыкальных клипов на YouTube.

Примерно в апреле 2019 года по данным Bukalapak, индийского веб-сайта электронной коммерции,
также просочился к Трою Ханту. Однако на этот раз сайт HIBP заявил:
«Данные были предоставлены HIBP источником, который просил приписать их
«Максим Фале».
Спустя несколько месяцев Максим Фале-Фишер будет назван в качестве личности
Партнер Nclay, DDB.
Конфликт обострялся в течение многих месяцев, что в конечном итоге привело к появлению публичного поста.
от «Gnosticplayers» на форуме XRPchat.com, где он (предположительно Nclay)
признается, что взломал GateHub и был частью команды, ответственной за кражу
10 миллионов долларов в криптовалютах (рисунок 20.1).

В то же время тот же человек начал утечку нескольких GnosticPlay-
взломанные базы данных других - предлагая их совершенно бесплатно в популярной базе данных
демпинговый сайт RaidForums.com. Nclay использовал Raid Forums, чтобы выразить свое недовольство
с другими хакерами, а также опубликовать предполагаемое имя своего партнера DDB как
Максим Фале-Фишер.
Наконец, после четырех дней болтовни и неразберихи слух начал распространяться.
что Nclay чувствовал себя так плохо из-за публикации этих сообщений и утечки этих баз данных
что он покончил с собой.
Трагично, да. Итак, прежде чем мы проанализируем эту информацию, вот несколько дополнительных
справочная информация о группе и их известных взломах.
Не волнуйтесь! На самом деле Nclay не умер. Он жив-здоров и даже делает
чудесное возвращение позже в этой главе, чтобы предложить свой собственный комментарий
о том, как ему удалось взломать все эти сайты.

Сайты, взломанные GnosticPlayers

Ниже приводится список сайтов, взломанных GnosticPlayers (Nclay / DDB). Это
не исчерпывающий список; это всего лишь список сайтов, о которых мне известно.



Gnosticplayers
Regular

New Member
19
16 posts

Posted October 22

I want justice to be served for me, but in this case people also need to know what really happened.

I am taking full technical responsability for the Gatehub Hack, and will defend myself the best way I can in court of law. I don't need to introduce myself. I have never been that so far.

Note that I'll strongly argue I have been manipulated doing a string of hacks for money, including gatehub, and it willnever explain or excuse the actions. But I hope it will be noted that I want to face justice, but I just can't accept other people taking all the profit (my accomplice from my country took twice than me), and Omniking / AmIEdgyEnough, on my back, took the rest, just by manipluating and blackmailing me.

More people are involved. The attack was done by me and I'm fully aware of what I did, everything was planned, and oncxe again nothing should be excused. I could say a million times I'm sorry for the whole hacking problems, but I'm not and the best I can do now is to accept justice and face it. Only if others people involved, much more believe me, mischievous than me, because I'm choosing a worthy end, than me, will do.

All I can say now to the victims, to Enej, is "sorry". Gatehub is I believe at fault for not having a good enough opsec but they faced the music more than you think. All the victims will be refunded, court will decide. And I really hope not only me but the people really involved will face her as well. No need for them to be smarter, because without my technical skills gatehub would have been spared.

I'm once again so sorry, Enej knowsd I tried to escape identification & planned a plan to avoid being caught. I planned the hack and was made evil?. But I'll explain the whole story, how I see things in a court of law and fight for real justice to be served.

Gatehub has its user database from 2017 stolen from an AWS S3 backup and I used the tokens to dump the API keys & decrypt them with AES. I needed the secret key which is the bcrypted password. Someone stated it earlier & he was right.

A million times sorry, my actions will make peace to the whole world and the emoragy will be ended.

Рисунок 20.1

- 500 пикселей
- 8fit
- 8Tracks
- Animoto
- Игры про броню
- Художественный
- Avito
- BitMax
- BookMate
- Букалапак
- Чегг
- ClassPass
- CoffeeMeetsBagel
- Coinmama
- Coubic
- Cryptaur
- DataCamp
- Дубсмаш
- Эдмодо
- Эпические игры (Фортнит)
- Estante Virtual
- Evite
- EyeEm
- Fotolog
- GameSalad
- GateHub
- Ge.tt
- GfyCat
- HauteLook
- Houzz
- iCracked
- Ixigo.com
- Jobandtalent
- Legendas.tv
- LifeBear
- Mindjolt
- Moda Operandi
- MyFitnessPal
- MyHeritage
- Onebip
- PetFlow
- Пизап
- PromoFarma
- Quora
- Путешественники

- Roll20
- ShareThis
- Storenvy
- StoryBird
- StreetEasy
- Крепость

Королевства

- Таринга
- Ванело
- Белые страницы
- Wirecard.br
- Ксиго
- Яноля
- Ятра
- YouNow
- YouthManual
- Зомат
- Zynga

Техники взлома гностиков

Метод этих взломов был раскрыт мне NSFW (обсуждался в предыдущем
главы) и подтверждено Nclay. Метод был также подтвержден несколькими
взломанных организаций.

Взлом был прост, но чрезвычайно эффективен: группа нацелена на развитие.
opers и будут использовать переработанные учетные данные для входа в свои учетные записи GitHub.
Оттуда они будут искать в репозиториях Git разработчика ключи AWS или
аналогичные учетные данные, которые были проверены. Как только хакеры получили ключи,
они входили в системы компании и просто брали то, что хотели.

Хотя это может показаться очевидным набиванием учетных данных / захватом учетной записи
атаки, что особенно интересно в методе Гностиков, так это то, *как* они были
может войти во все эти учетные записи GitHub. Ниже приводится отрывок из

личный разговор, который у меня был с Nclay через Twitter, где он любезно предложил объясните его процесс, чтобы я мог включить его в эту книгу.

VT:
как ты понял, как войти в эти GitHub
учетные записи без использования oauth?
VT:
я не думал, что вы можете просто использовать user / pass для входа в
api, иначе люди просто взбесили бы нахуй
из них
Nclay:
См. Случай с хакером Capital One
Nclay:
Github подали в суд за халатность
Nclay:
Пользователь / пароль просто продолжал работать через github api
VT:
это восхитительно
Nclay:
И они пытались запросить подтверждение устройства после
Gatehub взлома
Nclay:
Но API все еще позволял мне трахаться
Nclay:
Я не ограничивался github, но было весело. Однажды ты
знаю, что такой недостаток существовал
Nclay:
Посмотреть историю про zomato hack
Nclay:
И посмотрите историю взлома 8tracks
Nclay:
Взламываю gatehub в основном благодаря github
VT:
как вы грубо форсировали github api? Просто питон
сценарий?
Outofreach: мой собственный php-скрипт
Outofreach: небольшая петля
Outofreach: это можно сделать с помощью curl up user: pass
Outofreach: И я использовал свои личные дампы
Outofreach: Canva, которую я взломал в одиночку, позволила мне трахнуть Gatehub
Outofreach: curl -u user: pass http://api.github.com/user
Outofreach: -k -L
Outofreach: вам просто нужно было вывести его в файл после того, как
проанализировал Json (можно сделать в одном конвейере с jq)

Это просто, и это работает.

Проверить это очень просто, и по состоянию на декабрь 2019 г.

работает на GitHub. Для проверки просто запустите следующую команду из командной строки:
curl -u имя пользователя: пароль http://api.github.com/repos **-k -L**
Если учетные данные действительны, вы получите хороший вывод личного GitHub пользователя.
репозитории. Затем вы можете использовать эти учетные данные для проверки любого из
частные репо.

Нклай не упомянул, как ему удалось обойти GitHub
IP проверяет. Для этого мы можем вернуться к следующему заявлению из NSFW
в главе 2.

После входа в систему мне пришлось действовать быстро, чтобы избежать блокировки нового алгоритма машинного обучения Github.
учетные записи не используют новые IP-адреса, поэтому я немедленно использовал ssh-keygen, чтобы добавить новый публичный SSH-ключ к профилю пользователя. . .

Эта часть была чрезвычайно творческой. Однажды Гностик смог определить
действительные учетные записи разработчиков путем заполнения учетных данных API-интерфейса на основе HTTP.
Затем группа добавила свои собственные SSH-ключи в учетную запись разработчика, используя
Инструменты командной строки GitHub (которые не подвергались проверке IP).
Хотя это не «уязвимость», этот упущение в конфигурации GitHub
это причина того, почему Gnostic Players так успешно взломали так много
организаций, и причина, по которой Nclay считает, что его следует считать «одним из
величайшие хакеры всех времен ".
Теперь, когда мы понимаем, как Gnostic проводил свои атаки, давайте
вернемся к нашей истории.

Сообщения GnosticPlayers

Публичное признание вины со стороны GnosticPlayers стало очевидным шоком. Даже
более шокирующим является тот факт, что этот человек также решил публично слить так много
частных баз данных группы (делая их общедоступными и свободно доступными для
кому скачать). Здесь мы начнем наш анализ.
Рисунок 20.2 - это один из первых постов GnosticPlayers1 на RaidForums.
.com по поводу утечки взломанной базы данных Zynga.
Я считаю, что этот пост был разработан только для того, чтобы привлечь внимание людей по нескольким причинам.
сыновья. Во-первых, ссылка Zynga никогда не работала; ссылка на mega.nz всегда была
приостановленный.
У человека, разместившего эти сообщения, не было проблем с исправлением ссылок на другие
утечка баз данных, но никогда не будет репостить Zynga. Само собой разумеется, что если он
действительно был заинтересован в утечке всех баз данных группы, он бы исправил

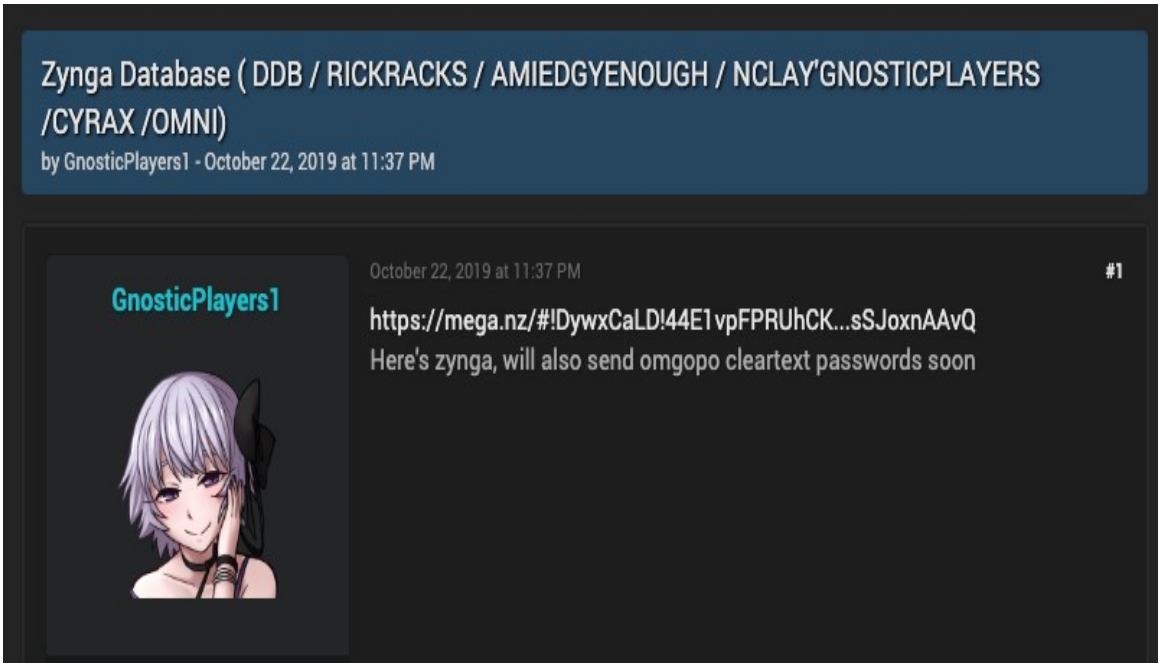


Рисунок 20.2

Вот этот. Я считаю, что причина, по которой он не слил Zynga (и несколько других), заключается в том, что они по-прежнему слишком ценны.

Ниже приводится личная беседа между другим исследователем и DDB / Bline:

bline@jabber.ru: это gnosticplayer
bline@jabber.ru: но не продавать
xxx:
зацепить брата
bline@jabber.ru: правда не могу я тоже не буду продавать вечно
ни у кого не будет
bline@jabber.ru: использую в Fortnite
xxx:
чем взламывать другие игровые аккаунты? и продать их?
bline@jabber.ru: да

Сообщение на рис. 20.2 интересно еще и тем, что оно называется RickRacks, AmiEdgyEnough, Cyrax и Omni - все люди, у которых, насколько мне известно, ничего общего с взломом Zynga.

Перейдем к другому посту Gnostic (рис. 20.3), который содержал данные для криптобиржи BitMax и Over-Blog.com.

Что мне показалось наиболее интересным в этом посте, так это огромное количество неточности, которые он содержал. Это важно, потому что человек, публикующий это

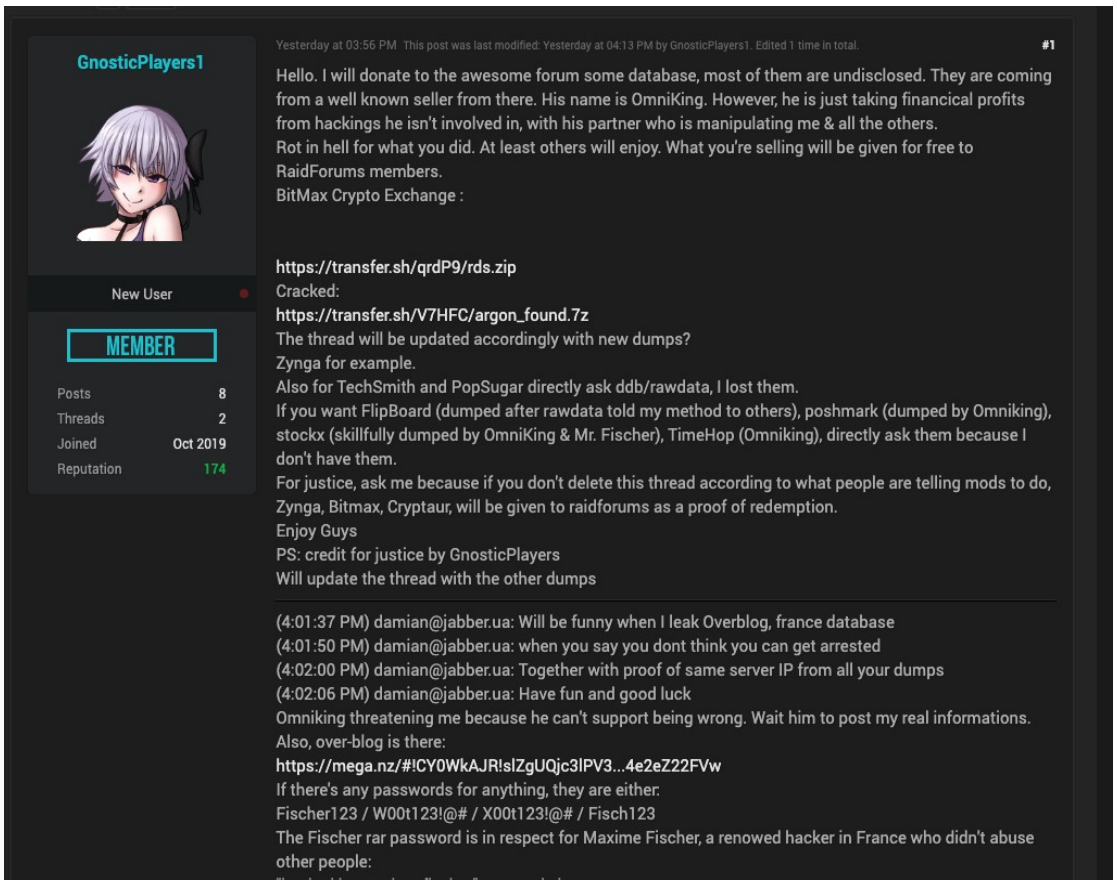


Рисунок 20.3

сообщение (предположительно Nclay) знал бы, что информация, которую он публикует
это неверно. Если он собирался испробовать полное признание -
Сион, зачем намеренно включать информацию, которая, как он знал, неверна?
Еще более важно *то, что* было неверным. GnosticPlayers1 утверждает, что StockX,
Poshmark и Timehop были взломаны Omniking, хотя на самом деле они
были взломаны NSFW (это неопровержимо).
Я также с абсолютной уверенностью знаю, что Nclay знал это, поскольку он и я
обсуждал это раньше. Итак, большой вопрос в том, почему этот человек защищает NSFW?

GnosticPlayers2 Emerges

25 октября 2019 г. на RaidForums.com появляется новый человек - его зовут
GnosticPlayers2 - и отправляет следующее сообщение:
Я пишу это письмо, потому что должен сказать вам правду. В настоящее время существует большой
представление обо мне настоящих GnosticPlayers.
Но чтобы понять, вы должны сначала узнать прошлое. GnosticPlayers - это не один человек
но за тож стоят два человека. Я пишу это письмо и GnosticPlayers1
кто начал всю эту драму. Чтобы разделить нас двоих, вы можете называть меня Габриэль
и назовите GnosticPlayers1 для Nclay, потому что это наша истинная личность.
Я знаю Nclay с 2015 года и всегда восхищался его навыками. Мы были
очень хорошие близкие друзья на долгие годы. Мы встречались несколько раз в реальной жизни, потому что
мы приехали из одной страны, и у нас нет ничего секретного друг для друга. Мы знали
все друг о друге, и мы доверяли друг другу.
Nclay был вдохновителем всех взломов и выполнял их все самостоятельно.
Но поскольку это все, что он знает, он не знал, что делать с базами данных, которые он
взломали и как принесли деньги. Это была моя первая идея - продать его на черном фоне.
market - это когда я впервые создал айдентику GnosticPlayers на рынке мечты.
Моя идея заключалась в том, чтобы продавать базы данных, которые взламывал nclay. Он был очень счастлив и любим
эта идея. Он ни разу не отказал этому, пока он получал деньги, которые хотел. Также
в это время мы присоединились к Rawdata / DDB, его настоящее имя Максим Талет, и помогли
мы продавали базы данных и давали нам новые идеи.
Все было хорошо, пока Nclay не прорвался через GateHub и не украл 10 миллионов долларов.
Так как до этого мы всегда делили деньги на все, Nclay был щедрым
Достаточно и дал мне и Максиму по 1/3 каждого. Мы все получили около 4 миллионов долларов
каждый. Но тут и началась проблема.
Nclay стал очень безответственным со своей долей денег и потратил все на то, чтобы
купил себе 3 элитных машины и подарил друзьям кучу денег бесплатно. Но
все они были фальшивыми друзьями, которые просто дружили с Нкли, потому что он был богат и
имел деньги и эксплуатировал его ради денег. После покупки его машины и дачи

остальное своему фальшивому другу у него не осталось денег. Там он пожадничал и начал
пожалеть о своем решении дать Мне и Максиму по 3 миллиона долларов.
Он начал просить нас вернуть его деньги или спрашивать, может ли он вернуть их крупному
степень. Конечно, так как он был нашим другом, мы дали ему 500000 долларов от обоих
я и Максим, но он отказался принять деньги из-за своей жадности и сказал
он просил половину. Он хотел, чтобы мы вернули ему 3 миллиона долларов. Мы не
принять это и в тот момент рассердился и начал шантажировать и угрожать за
я и Максим. Если мы не сделаем то, что он хочет, и вернем деньги, которые он нам дал, как
залог дружбы, он раскроет нашу информацию общественности и трахнет наши жизни.
Мы не слушали его и игнорировали, потому что думали, что он обманывает и
не стал бы делать такую глупость. Поскольку у Nclay действительно что-то не так с его
мозг он действительно сделал. Как уже отмечалось, он опубликовал все базы данных бесплатно и на добровольной основе.
таргетно распространил мою информацию и информацию Максима. Он представляет Меня и Максима как
главные действующие лица, стоящие за его действиями, хотя на самом деле единственная главная роль в этом случае - только он сам и никто другой.
Он опубликовал много ложной и фальшивой информации о том, что он был Габриэлем, но в
настоящий на самом деле я. Он выдает себя за нас, используя нашу информацию, чтобы навлечь на себя неприятности.
как месть. Он подставил всех, кроме себя. Он также транслировал имена
многих других, которые не принимали участия в процессе или никогда не участвовали
участвует в чём-либо, чтобы просто запутать людей и распространить ложную информацию. Его
слова не должны быть достоверными и честными. Это правда, и ты можешь мне поверить
или не. Все остальное, что говорит больной лжец, неверно и только пытается подставить других.

Хорошо. . . это довольно много информации. По словам этого нового человека,
GnosticPlayers - это не один человек, а два человека.
И очевидно, что именно Nclay взломал все сайты, в результате чего
в них добавление DDB в группу. Но если этот человек *не* Нклей, то кто он? я
думали, что в группе всего два участника? Теперь я внезапно считаю до трех.
Если верить этому сообщению, то Nclay был единственным человеком, который взломал
GateHub за 10 миллионов долларов и решил, исходя из строгого морального кодекса,
поделитесь большей частью с двумя другими партнерами.
Что-то меня не устраивает. . . .

Выяснилось, что за этим постом GnosticPlayers2 стоит DDB,
что имеет смысл, поскольку автор пытается дистанцироваться от взломов.
Вопреки тому, что он говорит, есть много сайтов, которые DDB взломал сам, например
Quora. Он также не стал «присоединяться к группе позже», они с Nclay всегда были вместе.

Таинственный третий член

Во введении к этой главе я упомянул, что таинственный член
ближайшее окружение группы, с которым я был знаком довольно давно, внезапно сделало

сам известен как исследователь безопасности. Ниже приводится отрывок из одного наших разговоров:

whackyideas25: Если вы знаете его сообщников, они не очень
любит друг друга.
Аргон:
DDB?
whackyideas25: Они дадут вам больше информации, чем вы можете
ожидать
Аргон:
вы думаете, что это ddb?
whackyideas25: DDB и третий.
Аргон:
подожди кто третий?
whackyideas25: Ты действительно не близок к делу, приятель
whackyideas25: Gnosticplayers - главный человек
Аргон:
я даже не изучал это до вчерашнего дня, так что
дайте мне секунду, чтобы наверстать упущенное
whackyideas25: Он начал работать с ddb примерно в 2016 году
whackyideas25: Он признал, что даже в своем посте на Raidforums
Аргон:
хорошо, но кто третий партнер? Омни?
whackyideas25: Когда он впервые взломал свои первые компании, такие как
Dailymotion, 8Tracks, Зомато
whackyideas25: Ddb связался с ним, чтобы узнать
whackyideas25: Несколько лет спустя ddb принял NSFW, который
все из ddb
whackyideas25: Теперь NSFW и Gnostic поссорились
Аргон:
да, все, что я знаю
whackyideas25: Потому что с гностической точки зрения он ничто
но пиявка своим собственным методом
whackyideas25: взламывать такие компании, как Flipboard, Doordash,
Пошмарк
whackyideas25: Подводя итог - это трио
whackyideas25: Gnosticplayers, Ddb, NSFW

NSFW / Photon

К этому моменту я знал Photon, он же русский (которого большинство людей называют NSFW потому что они команда) работал с группой, но я не был уверен, что он был активным участником.

Прежде чем мы начнем делать дикие обвинения, почему бы нам не посмотреть, что NSFW должен сказать об этом? Ниже приводится мой с ним разговор (под именем «Русский») 30 июля 2019 г .:

Аргон: ты упомянул, что продал DDB новое дерьмо
Аргон: что-нибудь хорошего, чего у меня нет?
Русский: хорошо
Русский: все это личное дело да
Русский: а если он узнает, что я продал тебе, это будет довольно трагично
Русский: так как мы теперь партнеры по хакерскому дерьму

Фантастика. У нас есть прямое подтверждение от NSFW, что он сотрудничает с DDB и, как следствие, Nclay / GnosticPlayers. Мы также знаем из предыдущего главы этой книги о том, что NSFW / Russian отвечает за взлом Flipboard, Poshmark, DoorDash, MGM, CodeChef, Timehop и многие другие сайты.

Перчатки оторваться

В очень неожиданном повороте пользователь OnSecurity (новый случайный пользователь) отвечает к сообщению другого пользователя в сообщении Nclay с надписью «SHUT THE F ** K UP VINNY» ТРОЯ ».

Оттуда в игру вступает еще один новый игрок, K3l0t3x (рис. 20.4).

Весь этот пост - ерунда, начиная с идеи, что я Сайракс (потому что я я не). Тем не менее, я могу сказать, что Nclay написал это, потому что он сказал похожие вещи мне в прошлом.

Цель этого поста, очевидно, заключалась в том, чтобы привлечь мое внимание и заставить меня поискать в это новое имя пользователя. В сообщении даже говорится, что нужно связаться с ним через Twitter, так что давайте поговорим с ним об этом.

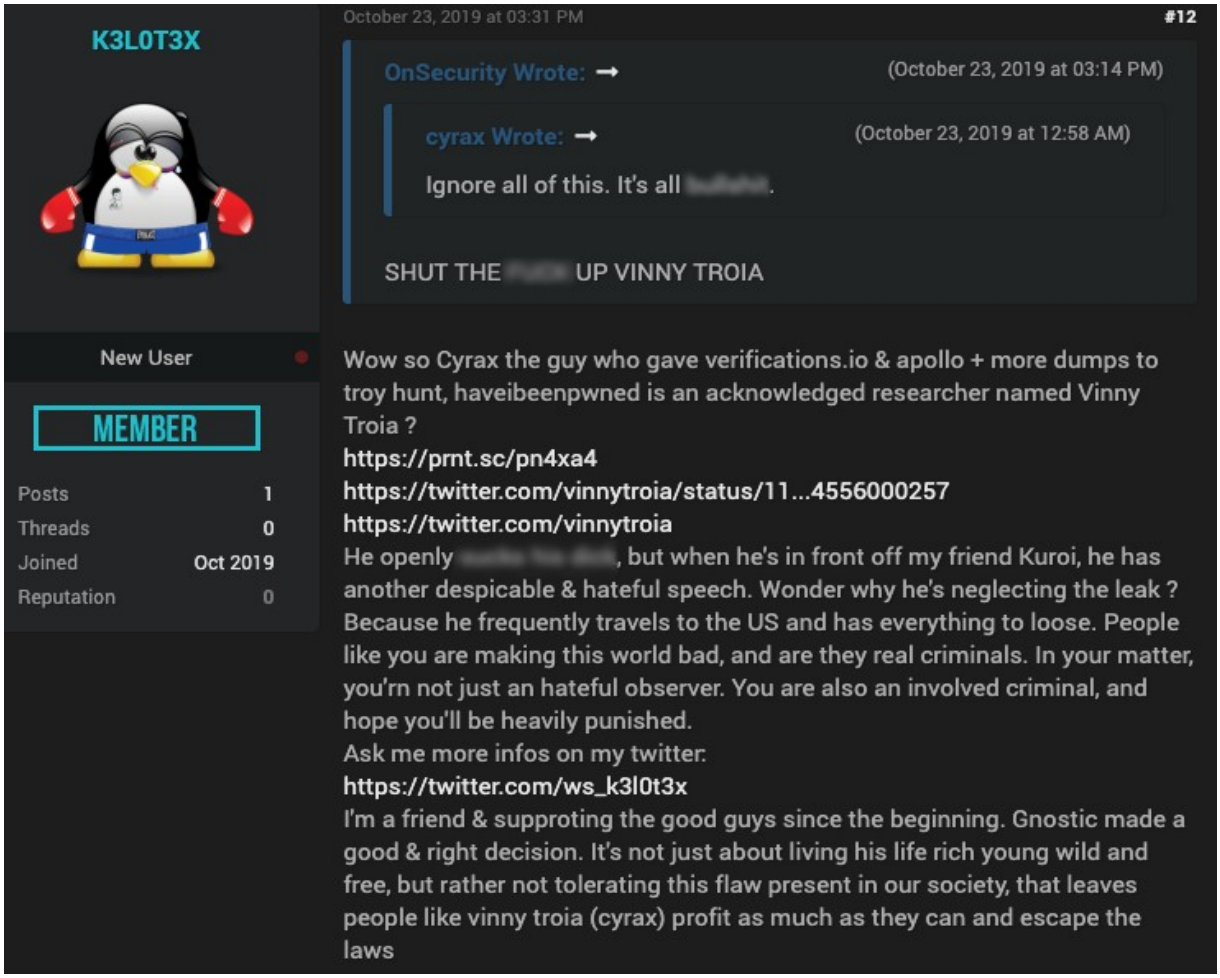


Рисунок 20.4

Установление контакта

Теперь, когда я вовлечен в эту маленькую сагу, я решил провести небольшое исследование. Этот работает для всех, особенно для вас, читателя, потому что какой способ лучше объединить все различные методы расследования, которым мы научились в этой книге, чем изучать группу киберпреступников, утверждающих, что украли 10 миллионов долларов в XMR?

Первым делом я вернулся и просмотрел весь мой старый разговор. журналы, и я нашел кое-что интересное - 12 февраля 2019 года NSFW прислал мне следующий dox для Nclay (тот самый, который сейчас просочился):

Имя пользователя: Kuroi'sh, nclay, shg_amar, amar_shg, irbl00d
Имя: Габриэль
Фамилия: Кимиаи-Асади Бильдштейн
Возраст: 19
Страна: Франция
Город: Тарб
Адрес: 6 rue emile rayse.
Почтовый индекс: 65000
Эл. адрес :
flam6@protonmail.com
carradio@protonmail.com
miraiever@protonmail.com
gaby.tarbes@gmail.com
Мать :
Телефон: 06 08 47 98 50
Работа: врач-офтальмолог.
Рабочий адрес: 24 rue larrey
Город: Тарб
Почтовый индекс: 65000
Рабочий номер: 05 62 93 29 29 | 05 62 34 99 93
Осада: Г-ЖА ЛАУР БИЛЬДШТЕЙН
С: 04-05-1998
УЛИЦА: 41829912900019
Эл. Почта: laure.bildstein@orange.fr

Похоже, что они планировали это давно, и NSFW, для по какой-то причине, это тот, кто скармливал мне дезинформацию. Давайте изучить информацию, которую я получаю.

Габриэль / Бильдштейн aka Kuroi'sh

«Габриэль КАБ», как сообщает Variety, - 18-летний гражданин Франции. Он и его партнеру Просоксу было предъявлено обвинение в нескольких уголовных преступлениях: существенная модификация данных о взломе музыкального видео «Despacito» на ютубе.

Быстрый поиск Kuroi'sh обнаруживает много информации на его YouTube.
взломать, а также ведет к его Twitter (@kuroi_dotsh) и GitHub (github.com/
securitygab) страницы.

Теперь, когда у Габриэля / Куроиша внезапно нет проблем с раскрытием
всему миру, что он Nclay, у него не должно быть проблем признаться мне в этом.
Поэтому я решил протянуть руку помощи.

На данный момент слухи о смерти Нклая все еще распространяются. Если этот человек действительно покончил жизнь самоубийством, он не должен отвечать.

Пользователь Twitter Kuroi'sh (@kuroi_dotsh) ответил сразу. К несчастью,
Я не мог никуда добраться с этим человеком и даже не был уверен
если бы Габриэль вообще контролировал эту учетную запись. На рис. 20.5 показана часть нашего
беседа.

Если бы это был действительно Nclay, он бы так не отреагировал. Он знает
точно кто я и его английский намного лучше.

Официальный аккаунт Габриэля в Твиттере оказался тупиком (пока), так что
мы можем двигаться дальше.

Затем страница Kuroi'sh на GitHub ссылается на его публичную страницу дефейса Zone-H.
(http://www.zone-h.org/archive/notifier=Kuroi). Как упоминалось ранее в этом
book, Zone-H - это исторический архив дефейсов общедоступных веб-сайтов.
Хакеры, взломавшие веб-сайты, всегда обращаются к своим друзьям. это
по сути, архив поведения скольжения, поэтому это идеальное место для
начать искать.

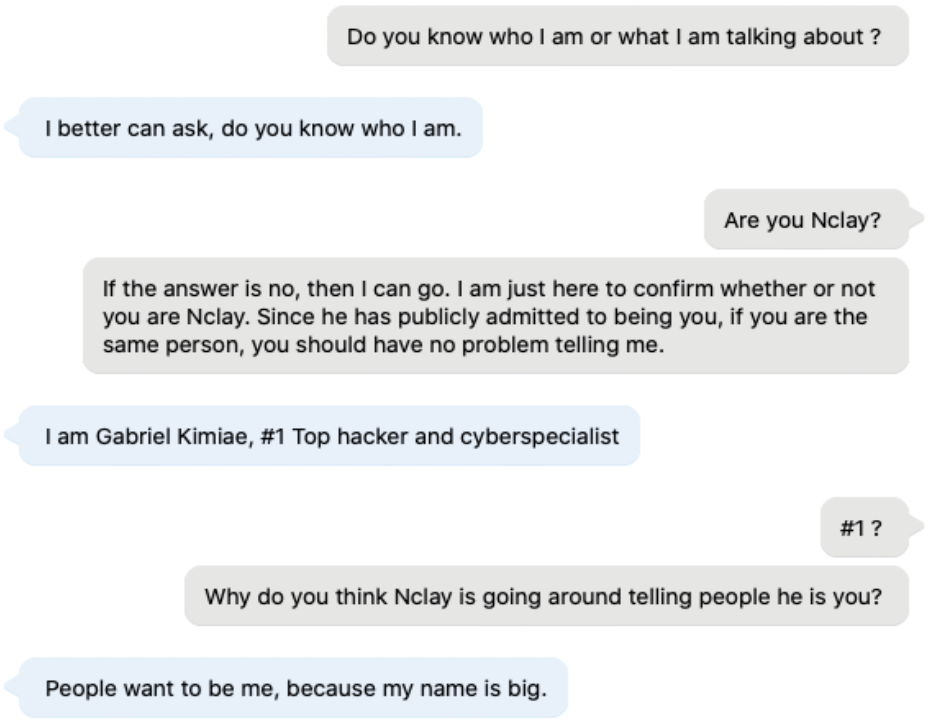


Рисунок 20.5.

Когда мы просматриваем архивы Zone-H, мы видим сотни веб-сайтов
порчи, сделанные Kuroi'sh, все с визитными карточками следующих людей:
Greetz: Kolotex, RxR, Prosox, General KBKB, Shade, Sxtz

Связь с его друзьями

Следующее, что я решил сделать, это найти его друзей в Твиттере. Дефейс-
Я могу найти того, кто знает
собственно Куройш. Я обратился к следующим людям:

- Кто я / k3l0t3x (@ ws_k3l0t3x)
- RevSec (@ cyb0rg_fs)
- Мальчик 9-4 лет (@FuegoLevel)
- Prosox (@ ProsoxW3b)
- Chic000 (@ Chic000w3b)

Честно говоря, я даже не знал, что Chic000 существует, пока он не взял его на себя чтобы отправить мне личное сообщение через Twitter с сообщением «занимайтесь своим делом».

RevSec (@ cyb0rg_fs) первым ответил и, похоже, знает Габриэля.
очень хорошо. На рисунках 20.6 и 20.7 показаны основные моменты.
Итак, теперь у нас есть кто-то, кто действительно знает Габриэля, и говорит нам, что все
информация, которую мы читаем, является фальшивкой.
Сюжет сгущается. . . .



Рисунок 20.6.

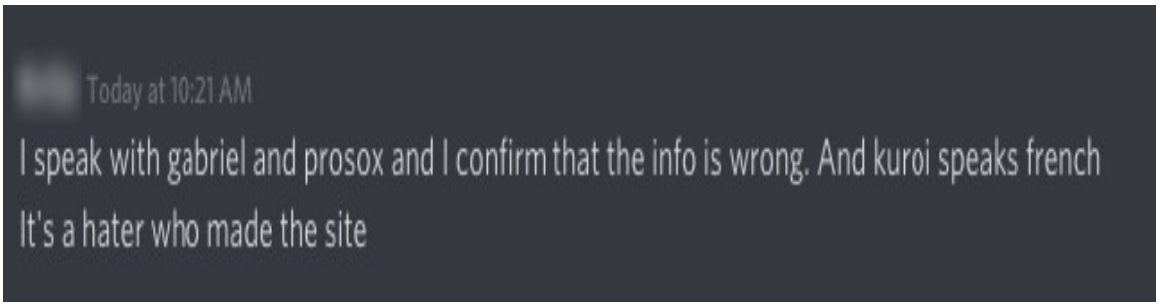


Рисунок 20.7.

Прополка через дезинформацию

Что касается «участка», показанного на рис. 20.7, я спросил этого человека об очень
интересный блог WordPress, с которым я столкнулся. Я скажу, что кто бы ни подумал
При разработке этого плана, безусловно, было потрачено много времени и усилий на разработку дезинформации.
Я полагаю, когда вы говорите о том, чтобы избежать наказания за грабеж миллионов
долларов в криптовалюте, вы хотите убедиться, что ваши базы защищены.
Блог WordPress под названием «Нассим AKA Prosox из Марокко» может быть
просмотрено здесь:
https://prosoxrealnamenassimfrommorocco.wordpress.com
Блог был создан кем-то, кто хотел разоблачить Prosox как «тупого»
самый лучший хакер. " Чтобы обеспечить охват ключевых слов их поисковых систем, они даже
создал страницу под названием «Kuroi'SH & Friends».
На странице полно разговоров якобы из Kuroi'sh, и это
похоже, что последний пост в блоге был написан 14 марта 2017 года. Все выглядит
полностью законный и достаточно старый, чтобы вызвать разумные подозрения.
Я снова называю быков ** т.

Проверка с помощью Wayback

Блог WordPress, который работает с марта 2017 года, должен иметь своего рода
архив на Wayback Machine. На этом сайте нет.
Тем не менее, Wayback захватывает два URL-адреса (рис. 20.8).

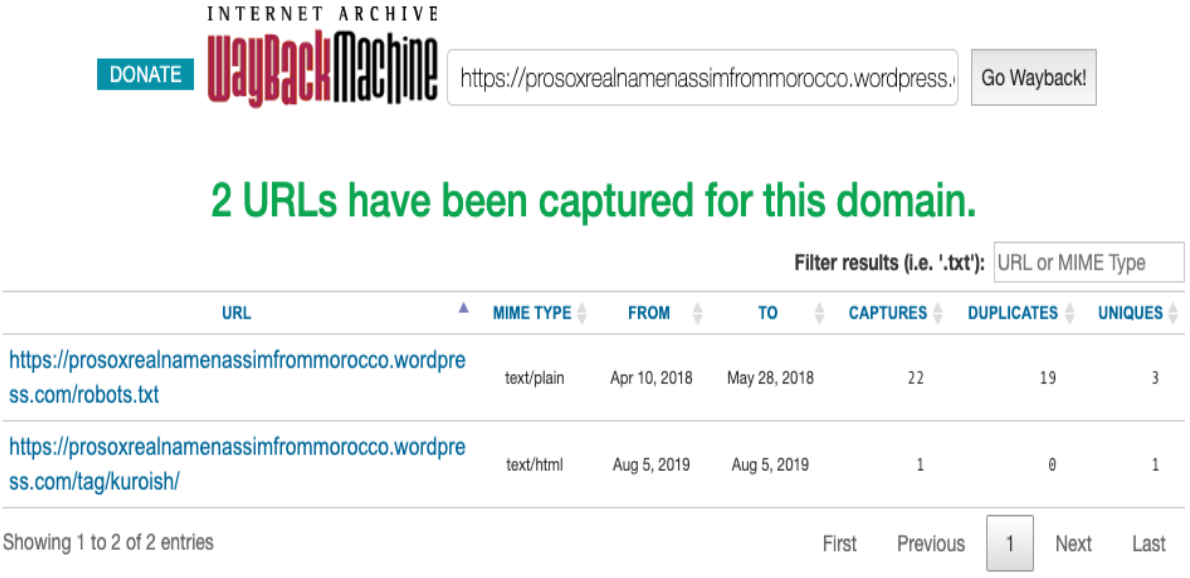


Рисунок 20.8

Первый файл - ar.txt , записанный в апреле 2018 года. Второй - это URL-адрес.
с тегом Kuroish, который, похоже, был опубликован в августе 2019 года. Роботы
.txt файл пуст, а файла sitemap.xml нет , что делает его еще меньше.
правдоподобно.
В *настоящее время на* сайте есть полный файл sitemap.xml (как и на большинстве сайтов WordPress),
поэтому, если бы эти сообщения в блоге действительно были опубликованы в 2017 году, Wayback кэшировал бы
копия сайта. Вместо этого мы видим, что теги были добавлены два года спустя.
Мы можем зарегистрировать это как «совершенно ложное».
Когда этот объезд позади, давайте продолжим с того места, на котором остановились, и продолжим движение вниз.
путь контакта с бывшими соратниками Куроиша.

Собираем все вместе

Возвращаясь к RaidForums, посту, который специально призывает меня (рисунок 20.4)
был написан пользователем K3l0t3x (назовем его Kel). Я могу с уверенностью сказать, что
Это написал Nclay. Стиль письма такой же, как и у него, и он даже сказал несколько
эти *конкретные* вещи мне в чате несколькими днями ранее.
Итак, остается вопрос: зачем ему использовать имя Кела? Плакат
знал, что я хочу поговорить с этим человеком, поэтому он сказал мне
свяжитесь с ним через Twitter.
Так я и сделал. И тот, кто ответил, казалось, много знал о том, что происходит
на (рисунок 20.9).
По словам этого человека, Nclay (Kuroi'sh) был обманут из 4 миллионов
долларов какой-то русской. Это имеет больше смысла относительно того, почему он создал
такая публичная сцена.
И чтобы убедиться, что мы все говорим об одном и том же человеке, он кон-
подтвердил, что учетная запись Kuroi'sh в трепе - «аутфрейм» (рис. 20.10).
Outofreach@jabber.ua - это адрес jabber, который я всегда использовал для связи
общаться с Nclay. В этом нет никаких сомнений, а это значит, что кто бы то ни было
этот человек знает, что происходит, и, кажется, пытается
история о Габриэле, являющемся Нкли.
Поскольку люди, близкие к настоящему Kuroi'sh, говорят мне, что все это фальшивка,
было бы разумно сказать, что любой, кто пытается продвигать ложь, является
Часть этого.

Data Viper

Поскольку Кел теперь очевидный интересный человек, давайте посмотрим, что мы сможем узнать.
о нем. Первым делом я направился к Data Viper и просмотрел его
имя пользователя (рисунок 20.11).

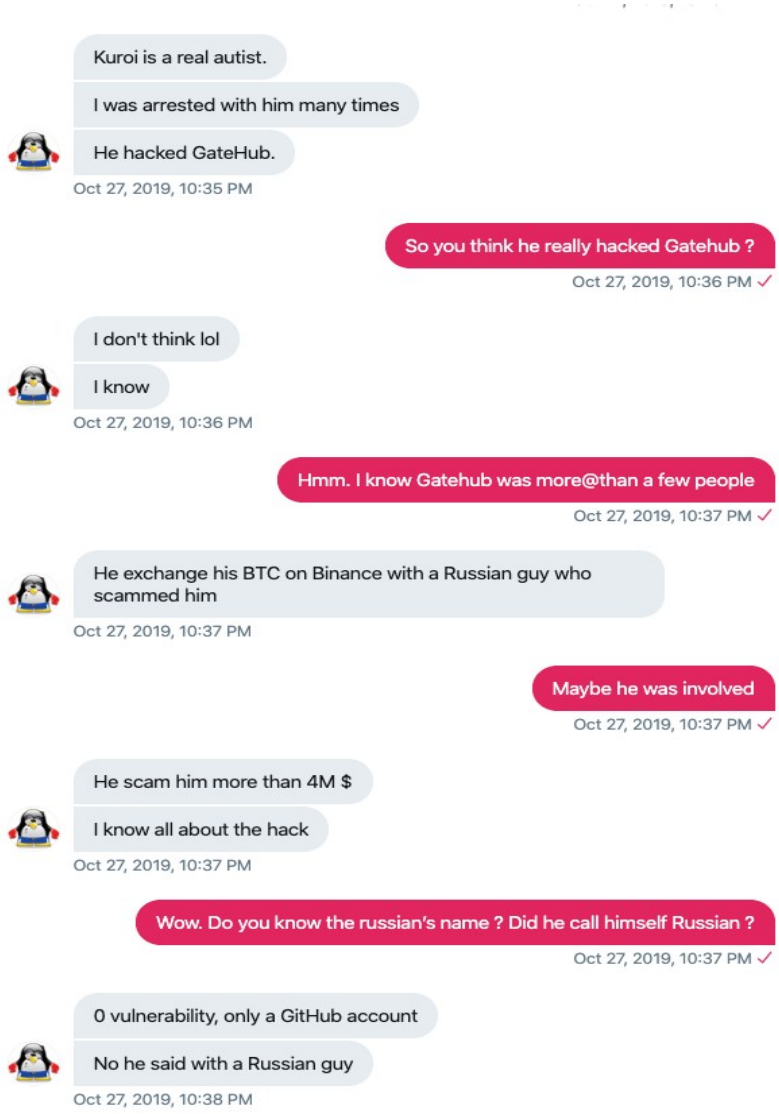


Рисунок 20.10.



Рисунок 20.9

У нас есть два обращения к электронному адресу. Начиная с первого адреса электронной почты, anonymous.30.m@gmail.com , дает нам несколько новых сведений для изучения (Рисунок 20.12).

IP-адреса всегда полезны для изучения, особенно когда они не VPN или прокси (это не так). Расширяем поиск до 88.169.240.198 дает нам хороший набор новых совпадений, все, казалось бы, связанных с одним и тем же человеком (Рисунок 20.13).

Все эти адреса электронной почты и имена пользователей действительны, поэтому важно следить за тем, что вы делаете. Мы также видим, что существует общий пароль abbyblue14, который показывает еще больше имен пользователей и общих IP-адресов (Рисунок 20.14).



Рисунок 20.11

Username	Email	Password	IP Address
K3L0T3X	anonymous.30.m@gmail.com		
	anonymous.30.m@gmail.com		
	anonymous.30.m@gmail.com		88.169.240.198
K3L0T3X	anonymous.30.m@gmail.com		
HyXaZ	anonymous.30.m@gmail.com	8a517b2cfaf5	37.160.158.204
K3L0T3X	anonymous.30.m@gmail.com		
K3L0T3X	anonymous.30.m@gmail.com		

Рисунок 20.12

Username	Email	Password	IP Address
HyXaZ	fibrebooter@outlook.fr	9657f6bf683	88.169.240.198
Mattys	savoiemattys@gmail.com	abbyblue14	88.169.240.198
	anonymous.30.m@gmail.com		88.169.240.198
DzF0x	azerty@hotmail.fr		88.169.240.198
Mattys	savoiemattys@hotmail.fr	abbyblue14	88.169.240.198
Flocon	hyxaz@gmail.com		88.169.240.198

Рисунок 20.13

. Инструмент карты разума (или Maltego) - отличный способ визуализировать эти связи.

так что вы можете вернуться, если вам нужно.

По мере того, как мы прослеживаем этот длинный след учетных записей, имен пользователей и паролей, выясняется, что что все дороги в конечном итоге ведут к двум адресам электронной почты: mattysdbz@gmail.com и savoiemattys@gmail.com .

Основываясь на этой информации, похоже, что настоящее имя K0l0t3x - Мэтти.

Савойя.

Однако это кажется слишком простым.

Доверяй, но проверяй

Я настроен крайне скептически, и злоумышленник, способный осуществить такой уровень обмана.

ция будет иметь длинную цепочку учетных записей, что приведет к неверной информации.

Теперь, когда у нас есть некоторая информация, которую можно связать с нашей личностью, давайте посмотрим, что информацию, которую мы можем собрать, используя подсказки для сброса пароля. Начиная с адрес электронной почты anonymous.30.m@gmail.com , сброс пароля PayPal показывает нам частичный номер телефона (рисунок 20.15).

Затем проверяем информацию для сброса пароля в Google для электронной почты. savoiemattys@gmail.com дает нам другое приглашение (рисунок 20.16).

Что мне нравится в этом конкретном экране, так это то, что мы видим, что электронное письмо адрес привязан к активному номеру телефона. Мы также видим, что число оканчивается на 34, что, скорее всего, является тем же номером, что и в телефоне PayPal. проверка для anonymous.30.m@gmail.com .

Но что мне действительно нравится в этом методе проверки, так это то, что мы действительно можем используйте его, чтобы проверить, правильный ли у нас номер телефона.

Если мы введем здесь неправильный номер, Google сообщит нам и не отправит код подтверждения. Итак, как только у нас есть число, которое мы считаем точным, все нам нужно вернуться сюда и ввести номер, чтобы убедиться, что он действителен!

Username	Email	Password	IP Address
	savoiemattys@gmail.com	abbyblue14	
NezertYu	hyxaz@gmail.con	abbyblue14	
Mattys	savoiemattys@gmail.com	abbyblue14	88.169.240.198
	savoiemattys@yahoo.fr	abbyblue14	
	hyxaz@gmail.con	abbyblue14	
	savoiemattys@yahoo.fr	abbyblue14	
	savoiemattys@yahoo.fr	abbyblue14	
NezertYu	hyxaz@gmail.con	abbyblue14	
Mattys	savoiemattys@hotmail.fr	abbyblue14	88.169.240.198
	savoiemattys@yahoo.fr	abbyblue14	

Рисунок 20.14.

PayPal любезно предоставил нам много информации для работы, но 07

•• •• • 1 34 мало. Давай продолжим поиски.

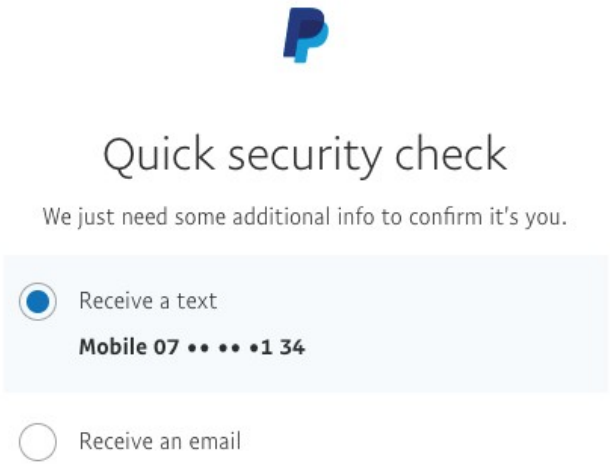


Рисунок 20.15

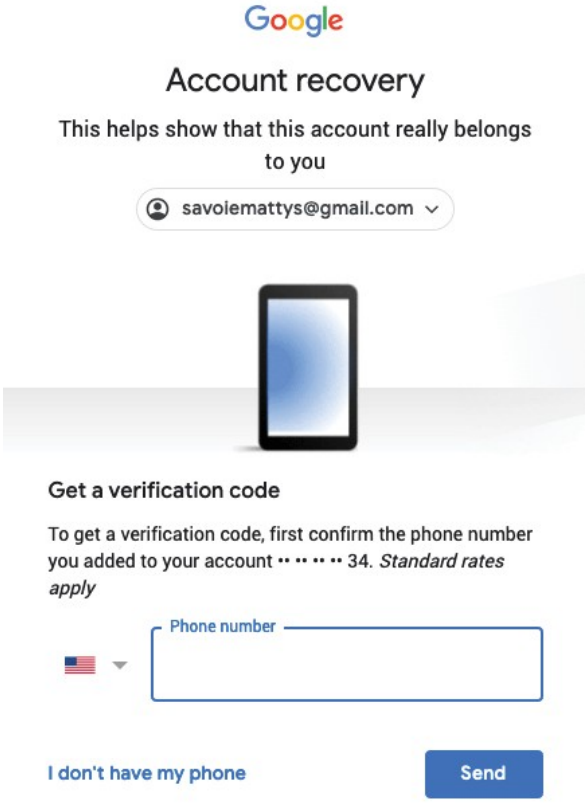


Рисунок 20.16

Ирис доменных инструментов

Следующий шаг - посмотреть, сможем ли мы найти какие-либо домены, зарегистрированные на электронные письма, которые мы

имеют. Всегда есть большая вероятность, что вас встретят злоумышленники, которые

Вот почему Iris от Domain Tools является такой важной частью моего исследовательского рабочего процесса.

Выполнение поиска по запросу anonymous.30.m@gmail.com сразу же дает нам успех!

Доменное имя:
nova-stresser.net
Имя регистранта:
K *** W ****
Организация регистранта:
Улица регистранта:
30900 *******
Город регистрации:
Ним
Штат / провинция регистранта:
Почтовый индекс регистранта: 3 *****
Страна регистрации:
FR
Телефон регистранта:
+ 33.78xxxxx34
Телефон регистранта, доб .:
Факс регистранта:
+ 43.xxxxxxx
Факс регистранта, внутр .:
1
Электронная почта регистранта:
anonymous.30.m@gmail.com
Сервер имен:
ns1.easyname.eu
Сервер имен:
ns2.easyname.eu

Теперь у нас есть имя, адрес и номер телефона, которые выглядят потрясающе.

аналогично номеру телефона, который нам нужен для подтверждения как PayPal, так и Google

учетные записи.

Я скрываю его личную информацию, потому что не могу узнать,

этот человек на самом деле вовлечен или нет, и я не занимаюсь доксингом людей.

Выполнение еще одного поиска по номеру телефона дает нам второе совпадение

(Рисунок 20.17).

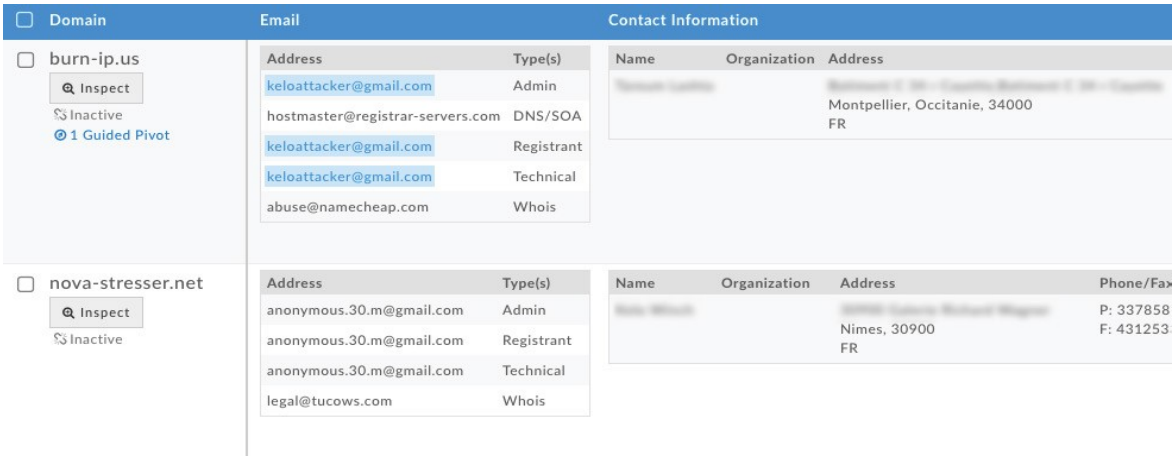


Рисунок 20.17

На этом экране у нас есть новый адрес электронной почты (keloattacker@gmail.com),
и у нас также есть два возможных имени, K *** W **** и Ta **** La ****, оба с
разные адреса.
Поиск в Google по запросу «Ta **** La ****» приведет нас прямо на LocateFamily.com.
(Рисунок 20.18).

Проверка с помощью второго источника данных

Даже со всей любовью и усилиями, которые я вложил в то, чтобы Data Viper был
как можно больше данных, я знаю, что невозможно охватить *все* . у меня есть
неоднократно подчеркивал в этой книге, что никогда не следует полагаться ни на один
источник вашей информации, и мой собственный инструмент не является исключением из этого правила.
WeLeakInfo.com - это веб-сайт, который позволяет любому найти пароль человека.
слово или другая личная информация. Подобно более старым сайтам, таким как LeakedSource
.com или Abusewith.us (которые с тех пор были заблокированы правоохранительными органами -
мент), WLI позволяет любому получить доступ к этим данным за небольшую ежемесячную плату.
Такие сайты, хотя и являются крайне незаконными, все же могут предлагать очень важные элементы
Информация. Используйте их, пока можете, потому что эти сайты, похоже, недолговечны.
В этом случае я обнаружил важное совпадение (рис. 20.19).



Рисунок 20.18

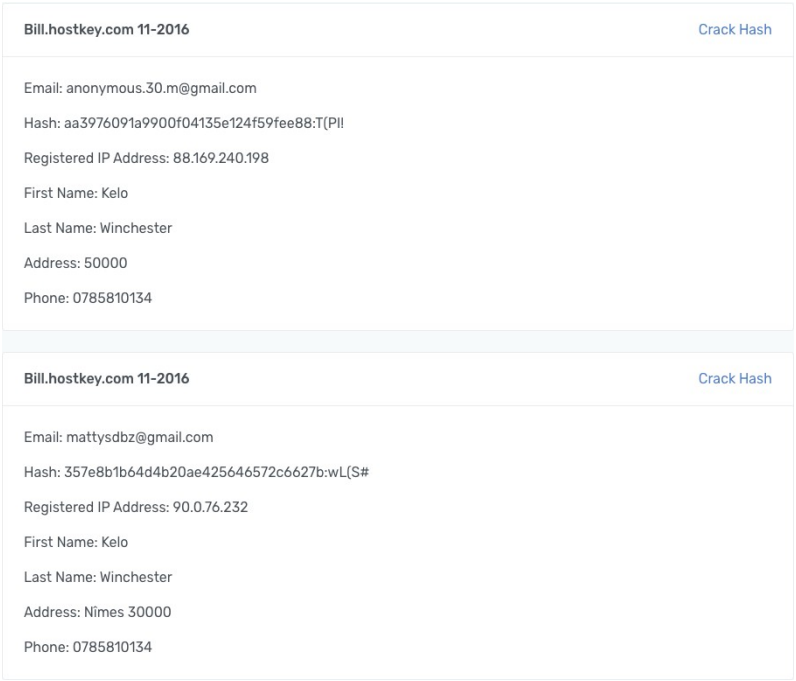


Рисунок 20.19

Данные взлома hostkey.com в 2016 году показывают две разные учетные записи с нашим
совпадающий номер телефона и адреса электронной почты. Поскольку это хостинговая компания,
само собой разумеется, что имя в этой учетной записи будет действительным.
Теперь у нас есть два возможных имени для K3l0t3x. Конечно, возможно, что
оба имени вымышленные. В любом случае номер телефона остается действительным и активным.

Конец строки

К сожалению, на этом моя история GnosticPlayers подходит к концу. Это было
никогда не означал, что это полная атрибуция членов группы. Хотя
один из людей, тесно связанных с GnosticPlayers, ранее был членом
TDO, это никогда не было моим расследованием. Моя атрибуция на NSFW уже была
закончилась, когда произошла эта сага.
По крайней мере, я выполнил свою часть работы и указал на кого-то
который, на мой взгляд, либо работает в структуре группы, либо знает
достаточно о взломе GateHub, чтобы предоставить достаточно информации, чтобы
нужные люди. Какое бы агентство ни занималось расследованием взлома GateHub, оно может
это отсюда.
Честно говоря, я не собирался даже включать Гностика в свою
книга, пока они не втянули меня в этот бардак.
Однако это заставляет задуматься. . .
Зачем Nclay намеренно втянул меня в это? Он знал, что это будет ссать
меня прочь, так был ли *это* его план с самого начала ? Если Нклей хотел, чтобы я исследовал Кела, он
имеет смысл, что он назвал бы меня своим именем.
Но почему?

Что на самом деле произошло?

Короткий ответ: я не знаю. Но теперь, когда у нас есть предыстория
GnosticPlayers и взлом GateHub, вот несколько потенциальных теорий.

Вне досягаемости

11 февраля 2019 года TheRegister сообщил, что хакер, известный как GnosticPlayers
разместил три полных раунда эксклюзивных баз данных для продажи на Dream Market.
Согласно последующей статье на ZDNet, «Гностические игроки взяли на себя ответственность за
взломов и отрицал, что был просто посредником ».
Звучит знакомо?
Примерно в тот же день NSFW раскрыл имя этого загадочного продавца.
для меня как «Nclay», партнера DDB. Это момент, когда я узнал, что DDB
был просто продавцом, а Nclay был хакером, стоящим за взломами.

Я связался с продавцом (как и предсказывал NSFW), который представил его:
самостоятельно с помощью jabber-адреса outofreach@jabber.ua .
И первое, что я узнал о Нкли, было то, что он
хакер, стоящий за всеми взломами, и что он также пользуется Outofreach. Все
меня красиво кормили с ложечки.

Волшебное появление Курои

Как будто его каким-то образом вызвали телепатически, Куройш связался со мной по
Twitter, используя учетную запись @kuroi_dotsh , которую я ранее отклонил. Этот
время, казалось, ему больше хотелось поговорить и убедить меня в том, кто он такой.
К этому моменту я был честно готов закончить всю эту сагу, но там
было то, что он сказал, что действительно привлекло мое внимание, потому что я уже
думал об этом (рис. 20.20).
Этот человек, выдающий себя за Габриэля / Куроиша, похоже, много знает о Нкли,
самая важная деталь, подтверждающая, что Nclay и Outofreach (человек, которого я
предположительно Nclay) были не такими.

Что я узнал, наблюдая за потерянным

«Остаться в живых» - одно из моих любимых телешоу. Одна из вещей, которые я особенно
В сериале очень понравилось то, что никогда не знаешь, кому и чему верить. После
посмотрев его во второй раз, мне пришло в голову, что причина, по которой у меня было такое

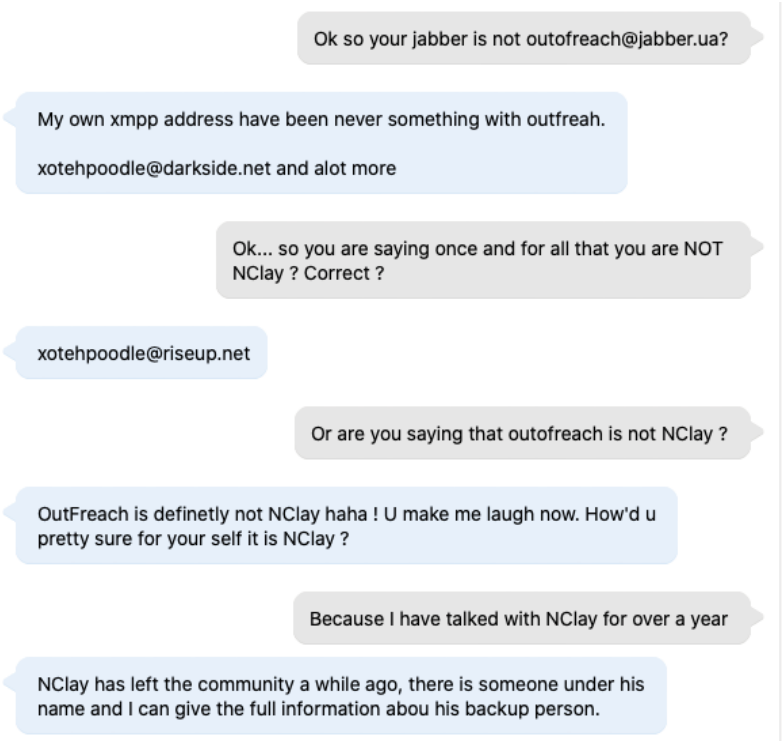


Рисунок 20.20

Трудно понять, что происходит, было то, что у меня была *естественная склонность предполагать, что все лгали* .

Действительно интересно пересмотреть шоу с этой точки зрения. Вы будете
быстро найти, что Бенджамин Линус (один из самых загадочных и ненавистных персонажей)
актеров сериала) *никогда ни о чем не лгал* . Он всегда говорил правду
о том, что происходит, но люди предпочли ему не верить.

При первом просмотре шоу я предположил, что «другие» лгут.
обо всем, что заставило меня потратить так много времени, пытаясь понять
что на самом деле происходило, что я упустил много очевидных истин.

То же самое можно применить и к этому сценарию.
На данный момент ко мне приходит так много информации, что
Габриэль Нклей и Куроиш - один и тот же человек, которого я могу продолжать.
считайте, что все лгут, или соглашайтесь с этим.

Момент лампочки:

Я не уверен, почему мне никогда не приходило в голову, что может быть более одного человека используя имя Nclay .

Кто взломал GateHub?

Если верить *всем* , Габриэль Бильдштейн (он же Nclay aka Kuroi'sh) взломал
сайт (вместе с некоторыми другими).

Ниже приводится отрывок из частной беседы между мной и русским.
(также известный как NSFW) 22 июня 2019 г .:

Русский: но этот хак Gatehub добавил много новых игроков, я слышал
Русский: недавно я слышал, что LE связалась с AWS, Github и Proxyrack
по этому поводу
Русский: и поговорили с службой безопасности Gatehub, у них есть кое-какие зацепки
их группа
Русский: это 4 человека и они неплохо перемешали
Русский: посмотрим, не возникнут ли проблемы
Русский: зависит от того, много ли тратит Gatehub или открыт
дополнительные иски
Русский: не хочу быть в слепую
Русский: я был с ними какое-то время, мне нужно знать, в чем дело
Аргон: с кем был? ddb / nclay?
Русский: ddb
России: nclay это п ****

NSFW четко знал, кто несет ответственность за взлом GateHub, и сказал это.
было четыре «новых человека».

Какое невероятное совпадение, с которым я только что разговаривал
четыре новых человека в Твиттере, все, казалось бы, связаны с Габриэлем, Нкли и
вся эта ситуация (K3l0t3x, RevSec, Chic000 и Kuroi'sh).

Разгадывая ложь

Если мы наконец поверим, что Габриэль имел какое-то отношение к GateHub
hack, мы должны спросить себя, *почему* мы вообще об этом знаем.
Ответ в том, что некто по имени GnosticPlayers публично объявил
что он взломал GateHub. Следующий очевидный вопрос: зачем кому-то
публично признаться в краже всех этих денег?
Ответ: они бы не стали.
Кроме публичного признания, я не видел никаких доказательств того, что
GnosticPlayers (он же Outofreach) на самом деле ответственен за взлом GateHub.
Это ложь. *Какой лучший способ переложить все свои преступления на кого-то другого?*
Сейчас существует так много информации, связывающей Gabriel / Nclay с GateHub, что
когда Европол спросит его, они, несомненно, предположат, что Nclay - это
тот же Nclay, который является известной частью GnosticPlayers. А почему бы и нет, учитывая
тот факт, что признание Nclay исходило от кого-то с именем пользователя
GnosticPlayers?
Внезапно все 50+ громких хаков, связанных с GnosticPlayers
будет взиматься с кого-то другого.
Очень-очень хорошо сделано.

Был ли замешан Габриэль? Моя теория

По правде говоря, я понятия не имею, но мое чутье говорит мне «нет», потому что я узнал о
name Nclay в феврале, то есть примерно за месяц до взлома GateHub.
В июне NSFW четко заявил, что знает, кто стоит за взломом GateHub.
и приписывает это четыре «новых людей». На одном дыхании, он также признает
работая с DDB, что говорит мне, что они могли легко придумать
этот план вместе (или даже были работать вместе все вместе).
Кажется ли разумным, что шесть человек сговорились бы сговориться с десятимиллионным заговором?
доллар Ограбление на одного человека? Конечно, есть. То есть много денег, и
NSFW, путем его истории с TDO и ад форум, уже долгое
история приписывания преступлений другим людям.
По его собственному признанию, Габриэль использовал имя Нклей несколько лет назад, когда
он взломал Zomato и Edmodo, и имя не было вокруг с тех пор. Этот
создали возможность для кого-то использовать имя и связывать его с кем-то
остальное с известной историей взлома.

Габриэль - это Нклей: альтернативная теория

Чем больше я читаю разговоры между участниками группы, тем больше я верю
что Габриэль действительно может быть Nclay. Некоторые вещи, которые он мне говорит, не могут

быть отказано, включая информацию, которую должен знать только Габриэль, включая
какой сотрудник министерства юстиции Франции ведет его дело, и что
были конфискованы четыре его машины (в том числе 2 его ламборджини), а также
У него также было конфисковано около 1,8 миллиона долларов в биткойнах.
Кроме того, он сказал мне, что когда он впервые обратился в полицию, его отправили
в больницу за то, психическое расстройство. Возможно, это был его план?
Я прочитал многочисленные разговоры между участниками угроз, в которых говорилось, что Габриэль
это «шизофреник» или «Bipolar» (это их слова), и эти медицинские diag-
nosis - это то, как он смог избежать наказания за предыдущие взломы.
Возможно, у него действительно есть заболевание, о чем он знал.
бы уйти от полного признания.
Конечно, это все лишь домыслы, основанные на его собственном понимании ситуации.
. . . но представленные им утверждения точны.

Все дороги ведут обратно в NSFW

Независимо от мотивов Нклая или его истинной личности, лежащая в основе связь с
Фотон (NSFW) отрицать нельзя.
Ниже приводится личный разговор двух близких к этому человеку.
ситуация:

Digi:
Джимми и Винни планируют против nclay
Сайракс: ты глупый
Digi:
Ладно
Сайракс: я тот, кто разговаривает с nclay
Digi:
oxxx
Сайракс: нклей испугался и подумал, что я винни
Сайракс: винни не имеет ничего общего с nclay
Digi:
В самом деле?
Сайракс: 100%
Digi:
кто винни на рф?
Сайракс: Епископ
Digi:
он тот, кто писал о nclay в твиттере
Cygax: OMG
Сайракс: о разговоре ??
Сайракс: вот о чем все это ??
Digi:
да
Сайракс: гребаные идиоты
Digi:
видеть
Digi:
ты ничего не знаешь
Сайракс: в его разговоре не упоминались личности
Сайракс: смеется
Digi:
coz of vinny только все началось
Сайракс: если это так
Cygax: тогда я знаю, почему это действительно началась
Сайракс: и в его имени 4 буквы
Digi:
я не совсем уверен в этом

Digi:
всенаправленный?
Сайракс: NSFW
Digi:
lmao
Digi:
да
Digi:
nsfw и ddb
Сайракс: ебать nsfw
Digi:
или вы можете сказать rawdata
Digi:
или фотон
Cyrax: rawdata - это ddb
Digi:
я знаю это
Сайракс: фотон - это nsfw
Digi:
вот почему я сказал, что вы можете называть их как угодно
Учитывая время всего, что произошло, и тот факт, что NSFW
был тем, кто скармливал мне большую часть этой информации, я не могу не
Вопрос о том, являются ли они тот же человек. Независимо от того, что эта книга и
в моем отчете TDO будет достаточно указаний на NSFW, в чем я не сомневаюсь
правда выяснится, как только он окажется под стражей.
А пока у этой саги отличный (и очень познавательный) финал.
в эту книгу!

Резюме

Помимо невероятно занимательной истории, главный вывод из этого
глава, что ничто не должно быть принято как факт, без проверки. Кибер
преступникам не составит труда сочинить замысловатые предыстории, чтобы просто бросить
вы сбиваетесь с пути, особенно когда речь идет о деньгах.
Как и все остальное, если что-то кажется слишком хорошим, чтобы быть правдой (например,
преступник вдруг признался в краже 10 миллионов долларов), как обычно. Не надо
принять это как факт только потому, что за этим, кажется, стоит законный конфликт.
Никому не доверяйте, проверяйте все и не думайте, что все лгут!

483

На момент написания этого эпилога Натан Вятт (который, как я полагаю, является Арни) имел
были экстрадированы в Соединенные Штаты, а два других основных члена
Dark Overlord не далеко позади.

К сожалению, канадская судебная система движется *очень* медленно. Тем не менее, все *это*
движется, и я поделюсь с вами, как узнать.

22 ноября 2019 г. я получил следующее письмо от человека, который
звучало очень знакомо.

Ты знаешь кто я. Я могу говорить только по этому *адресу* электронной почты: *vinnytroia @ mailbox*
.org , из-за того положения, в которое вы меня поставили, вы дегенерируете.
Я говорю, чтобы оценить нанесенный вами ущерб, о котором я не знаю.

Я был очень заинтригован. Два дня спустя мы назначаем время для разговора через Jabber.
под псевдонимом thegoodoldNSA.

thegoodoldnsa:
Вот что я знаю.
thegoodoldnsa:
Или то, что я могу сделать.
thegoodoldnsa:
Вы рассказали обо мне ФБР и другим, и что
Я сделал.
thegoodoldnsa:
Вы могли подумать, что это из-за отказа
с вами, но испортить чью-то жизнь (потенциально),
это варварство.
---
thegoodoldnsa:
Что я сделал такого, что требует чего-то серьезного,
убедитесь, что меня будет расследовать не только один,
но несколько агентств?
thegoodoldnsa:
И я никогда не смогу уйти от этого заговора заряда
как я уверен, вы в курсе.

Эпилог

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

484 Эпилог

thegoodoldnsa:
Я уверен, что ведутся расследования, я очень
уверен, что вы принимали в этом участие.
thegoodoldnsa:
По причинам, которые я не могу обсуждать.
thegoodoldnsa:
Те, кто сказал мне, связаны законом.
---
thegoodoldnsa:
Как оказывается, кем-то, кого я не считал угрозой
самый большой.
thegoodoldnsa:
Неужели что-то не так?
thegoodoldnsa:
Я просто хочу, чтобы вы поняли, что то, что вы сделали,
К черту мою жизнь.
thegoodoldnsa:
И единственное, что я хочу сейчас понять, это почему
ты сделал это со мной?
thegoodoldnsa:
Мы долго разговаривали, я вел себя как д ** к, но
это было оправдано, вы не выиграете, если будете хорошо играть.
thegoodoldnsa:
Но серьезно. То, что вы натворили, ужасно.
-
Аргон:
Неважно, есть у меня настоящий TDO или нет.
Вятт поет как птица
Аргон:
он продолжает много говорить о ребенке, которого он обучал
thegoodoldnsa:
Вы сказали мне все, что мне нужно знать. Я бы хотел
Убей Вятта сейчас, ебать.

Казалось бы, ФБР допрашивало этого человека (который, как мне кажется,
быть TDO / NSA / NSFW в зависимости от его языкового стиля).
Независимо от того, кем я думал, что это могло быть, этот человек был явно расстроен, хотел ...
Я хочу знать, почему я должен предоставить какую-либо информацию ФБР. . .
На следующий день я получил сообщение в WhatsApp от нашего друга Криса.
Менье.

Крис Менье:
Прекратите играть в игры
Винни Троя:
в какие игры я играю?
Крис Менье:
Вы делаете вид, что не знаете, почему я написал вам
Крис Менье:
Я здесь не для того, чтобы причинять тебе горе, я просто хочу сделать
конечно, мы получаем все факты прямо
Винни Троя:
ну, довольно забавно, TDO отправил мне сообщение 2 ночи назад
Винни Троя:
или кто-то связанный с этими парнями
Винни Троя:
говоря мне, что я трахаюсь с его жизнью
Винни Троя:
а теперь здесь вы просите помочь прояснить факты
Крис Менье:
И это приводит вас к какому выводу?
Крис Менье:
Что ты прав в том, что собираешься делать?
Винни Троя:

или что-то заставило его написать мне из
Синий
Крис Менье:
Ты что-то делаешь
Крис Менье:
Вовлекая меня
Винни Троя:
и в чем я с тобой не разговаривал? 6 месяцев? а также
теперь вот ты где
Крис Менье:
Послушай, ты хочешь, чтобы я просто дал тебе подсказку
Винни Троя:
это было бы действительно полезно
Крис Менье:
В нем участвует ФБР

Эпилог 485

Винни Троя:
да, мы на одной странице. я говорил с ФБР
кратко о Nclay
Крис Менье:
Да, я знаю, что ты говорил с ФБР
Винни Троя:
почему вы узнали, что я разговаривал с ФБР?
Крис Менье:
Мы оба на связи с ФБР, хорошо?

Какое невероятное совпадение, что я получаю случайное сообщение от кого-то
Я верю, что это TDO относительно того, что ФБР говорит ему обо мне,
затем буквально на следующий день Крис пишет мне то же самое.
Если этого было недостаточно, ниже приведен фрагмент отправленного сообщения Twitter.
мне от моей подруги Бев Роб. Очевидно, Крис также связался с ней из
синий, чтобы узнать, разговаривала ли она с ФБР.



Какое интересное совпадение. Каковы шансы, что кто-то прозвучит
точно так же, как TDO свяжется со мной, а затем Крис свяжется со мной однажды
потом задавать тот же вопрос?

Куда мы идем отсюда?

Я надеялся написать этот эпилог о том, что это дело уже закрыто, но
похоже, ничто не может поторопиться с канадской системой правосудия. По крайней мере, это
Из тех сообщений очевидно, что есть какое-то движение.
Я подозреваю, что по мере приближения к этому ситуация действительно начнет набирать обороты.
дата публикации книги, и, если повезет, эта история будет завершена
время, когда вы это читаете.

Если к тому времени что-то не решится, я подозреваю, что вовлеченные люди будут пытаться переложить как можно больше вины на своих бывших партнеров.

Я видел, что происходит на хакерских форумах, когда салазки начинают спорить с друг с другом. Правда никогда не займет много времени, чтобы выйти наружу и быстро обостриться на всеобщее общение, где каждый мужчина, женщина и ребенок заботятся только о них - себя. В результате все оказываются в гигантском пламени славы.

Теперь, когда я думаю об этом, наверное, это то, что правоохранительные органы все время планировали.

Вот как я позволю всему этому разыграться.

В заключение, спасибо!

В любом случае, я хочу поблагодарить ***вас*** за покупку моей книги. Эта книга представляет итог нескольких лет следственной работы, и я благодарен, что вы были заинтересованы в чтении о моих приключениях в Охоте на киберпреступников.

Проблемы, с которыми я испытал при исследовании TDO были действительно изменение жизни в том, как они сформировали мои мыслительные процессы для будущих усилий, и я нахожу чрезвычайно унизительным то, что вы хотите узнать о различиях инструменты и методы, которые я использовал для решения многих проблем, с которыми я столкнулся по пути.

С выпуском этой книги также знаменуется запуск моей платформы Data Viper. Он стал отличным хранилищем данных об акторах и данных до и после взлома. разведка угроз. Я очень рад возможности увидеть других организации выиграют от нескольких лет напряженной работы я выливалась в разработке эту платформу, помогая им ссылаться на свои преступления и даже использовать данные, чтобы остановить преступления до их совершения.

Еще раз спасибо за покупку моей книги. Если вы найдете эту книгу интересной, пожалуйста дайте мне знать, когда мы в следующий раз встретимся на конференции или не стесняйтесь отправьте мне электронное письмо или личное сообщение в Twitter.

Мир .

ЦИФРЫ И СИМВОЛЫ

0-дн., 276
- (знак минус) модификатор, придурки, 160
A
AdvandedBackgroundChecks, Скиптрейсер, 361
псевдонимы, 20
allintitle: оператор, придурки, 162
allinurl: оператор, придурки, 165
Amazon, ведра, 293
Корзины Amazon S3, 320–321
CSF (CloudStorageFinder) и, 299–300
NoScrape и, 312
Ancestry.com, 331–332
Ключи API, 6
Apollo.io, 311
Archive.org, 214
поисковые URL, 217–219
архивы. *Также* Wayback Машина
CachedView.com, 212–214
кеши поисковых систем, 212–214
ARIN (Американский реестр Интернет-номера), 47–48.
Арни, TDO и, 32–35
CraftyCockney, 32 года
открытие активов, 46–47
ARIN (Американский реестр Интернет-номера), 47–48.
Ценсис, 56
Поиск субдоменов, 56–57
DNSDumpster, 49–52
придурки, поисковые системы, 48–49
Enumall, 59–60
Fierce, 57-58
Хакерская цель, 52–53
Шодан, 53–55
Sublist3r, 58–59
результаты инструмента, 60–61
аутентификация, Elasticsearch и, 311
Веб-камера AXIS, Инурлбр, 172

Показатель

Охота на киберпреступников: Руководство хакера по инструментам и методам сбора оперативной информации в Интернете, первое издание. Винни Троя, доктор философии.
© 2020 John Wiley & Sons, Inc. Опубликовано John Wiley & Sons, Inc., 2020.

B

бан списки, форумы, 381
основной соскоб, 313
BeenVerified, 330, 331
Bezlica.top, 216
Бинг, придурки, 169
BitBucket, 280
SearchCode.com и, 281
Биткойн, 13
адресов, 15
Bitcoin Наличные, 13
Форум Bitcoin Talk, 274
BlackBox форум, 275, 276-277
Сайпер, 32 года
блокчейн, 13
исследователи блокчейнов, 13–15 лет
Blue Snap Breach, 23 года
нарушения, 21–23
Блю Снап, 23
Регпак, 23
браузеры, поле user-agent
(Заголовок HTTP), 125
грубая сила
учетные данные, 102
Wfuzz, 146
ведро _ finder.rb, CSF, 299–300
BuiltWith, 121–122
Идентификатор Google Analytics, 123
История IP, 124
Вкладка "Профиль взаимоотношений", 123
Вкладка "Технологический профиль", 122

C

кеш: оператор, придурки, 165
CachedView.com, 214
кеши, поисковые системы, 212–214
Канарские жетоны, 25
Кархарт, Лесли, 25–26
ЦС (центры сертификации),
201
CassandraDB, 301
NoScrape и, 312, 318–319

Censys, Поиск субдоменов, 57
Cewl, 10
Чайнализ, 17
Чимпану, Каталин, 442
Ciphertrace, 17
Cloudflair, 209–211
Cloudflare, 191, 204–209.
Cloudflair, 209–211
CMSMap, 129
пакетный режим, 130–131
сканирование
несколько сайтов, 130–131
один сайт, 130
обнаружение уязвимости, 131–132
CMS (управление контентом
системы)
параметры, 129
Экранопланы и, 124–125
репозитории кода
BitBucket, 280
GitHub, 280
GitLab, 280
SearchCode.com, 281–282
ложноотрицательные, 283–284
повторное использование кода, 282
Coggle.it, 198
Монетная, 17
инструменты командной строки, MongoDB,
305–308
стиль общения, TDO, 30
Закон о неправомерном использовании компьютеров, Wyatt,
Натан, 33 года
конфигурирование, Linux, 5–6
Коралловый тайник, 214

Cr00k, 35–36, 403, 446. *См. Также* NSFW; Мир / душевный покой
псевдонимы, 35–36
Data Viper and, 422–429
поиск по форуму, 379
идентификация, 422–431
Карвуниарис, Деннис, 451
результаты поиска, 367–368
TDO и, 407–408
Экран Userrecon, 370–372
Крэн, Джонатан, 95, 96
учетные данные, брутфорс, 102
Cree.py, геолокация, 343–346
Креншоу, Адриан, 433 года
судимости, государственный суд
веб-сайты, 332–333
crt.sh, 204
CRUD (создать, прочитать, обновить, удалить) права, 295
Кранч, 10
криптовалюты, 4, 11–12
Биткойн, 13
исследователи блокчейнов, 13–15 лет
Чайнализ, 17
Ciphertrace, 17
Монетная, 17
Эллиптическая, 17
исследования, 15-17
биржи, 17–18
торговцы, 17–18 лет
CSF (CloudStorageFinder), 298–299
Корзины Amazon S3, 299–300
параметры, 299
ведро _ finder.rb, 299–300
Цифровой океан и, 299, 300–301
скачивание, 299
публичные URL, 299
пробел _ finder.rb, 299, 300–301
-p все, 300
паук _ finder.rb, 299
Дуб паук, 299
CSV файлы
Cree.py экспорт, 343–346

придурки, 162
информация о геолокации,
343–346
CT (прозрачность сертификата),
201
Cloudflare, 204–209
Cloudflair, 209–211
crt.sh, 204
Проект Google, 202
бревна, 206–208
CTFR, 202-203
поддомены, 203–204
Команды CURL, OSINT.rest,
351
Curvve Recordings, 328
кибер-атрибуция, 25
киберпреступники, 26–27
Cyper (CyPeRtRoN), 31–32, 267,
276
псевдонимы, 32
История Аргона, 383–386
Форум BlackBox и,
276–279
Группа Dark Overload, 30
Хаквайзер, 290
идентификационный след, 278–280
KickAss Forum и, 84, 388
KickAss Framework, 287
социальная инженерия и,
383–387
TinEye, 336

Страница Twitter, 337
WHOIS, 182
Википедия, 291
Ципертрон, 32

D

darkweb маркетплейсы, 388
данные, атрибуция, 295–296
дампы данных, 413
сборники 1–5, 413–414
поиск данных, 420
качество, 413–414
расположение, 420
проверка, 415–419
Data Viper, 407
Cr00k, 422–423
открытие, 427–429
форумов, 423
анализ хронологии, 423–427
курирование данных, 413
ДЕВОН и, 430–431
форумы, 421–422
Кель и, 470-472
PHP, 420
ReactJS, 420
базы данных
скачивание результатов, 296
NoSQL, 301
выкуп, 311
DataViper, 275
ДербиКон, 433
DEVON, Viper данных и,
430–431
Дьяченко, Боб, 293–294
инструменты различий, Википедия, 291
DigiNotar, 201–202
Цифровой океан, 293
CSF (CloudStorageFinder) и,
299, 300–301
Дирхант, 143
FADAA, 144–145
параметры, 144
распределенное сканирование
прокси-сети, 73
прокси-сервис, ротация, 73
Карта DNS, сгенерированная фотоном,

152
DNSDumpster, 49–52
Фотон и 150
DNSTwist, 61–62
DOC файлы, dorks, 162
метаданные документа, 245
Exiftool, 246–247
FOCA (снятие отпечатков пальцев)
Организации с
Собрание архивов),
261–262
извлечение метаданных, 263–266
старт проекта, 262–263
Intrigue.io, 257
информация о ведре, 259–260
URI Spider, 257–259
Метагоофил, 248–250
Модули Recon-NG
Интересные_файлы, 252–254
Metacrawler, 250–252
Канцелярская кнопка, 254–257
документы, MongoDB, 302
Dogecoin, 13
домены
CT (прозрачность сертификата),
202
обратный поиск IP, 189
поисковые запросы, 188
Поисковые запросы в WHOIS, 177
продвинутый, 181–182
массовый разбор, 189
ключевые слова, многократные, 179-181

namedroppers.com, 177–183
исполнители угроз, 182–183
DomainTools, 177, 188
поиск домена, 188
Домен поле Status, 195
IP-адрес, обратный поиск,
189
Iris, 221-222, 474-476
Вкладка "История хостинга", 232–234
Поворотный двигатель, 222–229
история скриншотов, 232
строка поиска, 222
Вкладка «История WHOIS», 230–231
скриншоты, 193
КТО
массовый разбор, 189
перекрестная проверка информации,
197–199
история, 192, 193-195
Обратный WHOIS, 196-197
Просмотреть запись Whois, 190–191
Dorks, поисковые системы, 48-49, 159
- (знак минус) модификатор, 160
Бинг, 169
DualxCrypt.org, 166
Exploit-DB, 159
Inurlbr, 169-173
операторы
allintitle :, 162
allinurl :, 165
кэш :, 165
имя файла :, 165
тип файла :, 162–163
intext :, 165–166
InTitle :, 161-162
inurl :, 163–165
сайт :, 161
цитаты, 160
Yahoo !, 169
DualXCrypt.com, 84
VirusTotal, 87-88
параметр дампа , Elasticsearch, 317
E
EagleEye, 333, 340-343
Elasticsearch, 293, 301

команда curl, 308–309
базы данных, загрузка, 296
JSON, 308-310
NoScrape и, 312
свалка, 317
поиск по ключевым словам, 315
matchdump, 317–318
скан, 314–315
поиск, 315–317
пароли, 409–413
выполнение запроса, 308
Шодан и, 296
Эллиптическая, 17
электронная почта, поиск, Skiptracer
361–364
электронные письма
открытие адреса, 156
Фотон, 150
enum _ wayback (сценарий Ruby),
215–216
Ethereum, 13
Exactis, 294, 311
биржи, криптовалюты,
17–18
Exiftool, 246–247
выход афера, 388
Эксплойт-БД, придурки, 159
F
Facebook
OSINT.rest, 352-357
сброс пароля, 393-394

FADAA (Флорида Алкоголь и
Ассоциация злоупотребления наркотиками), 144
ложноотрицательные, SearchCode.com,
283–284
Fierce, 57-58
имя файла: оператор, придурки, 165
файлы, Фотон, 150
тип файла : оператор, придурки,
162–163
FIN сканирование, 68
результаты, 71
брандмауэров, 70
подмена адреса
IP-адрес, 78-79
MAC, 78–79
контрольные суммы, 76-77
изменение длины данных, 78
приманка сканирования, 77
распределенное сканирование
прокси-цепочки, 73–74
прокси-сервис, ротация, 73
TOR, 73-74
угли, 79
фрагментированные пакеты, 74
MTU (максимальная передача
ед.), 74
обнаружение службы, 74–75
сроки запросов, 76
FOCA (снятие отпечатков пальцев)
Организации с собранными
Архивы), 261–262.
извлечение метаданных, 263–266
старт проекта, 262–263
форумы, 274
бан-листы, 381
BitcoinTalk, 274
Блэкбокс, Сайпер, 32
Data Viper and, 421–422
HackForums.net, 379
история, 275–278
KickAss, Cyper, 32
Nulled.to, 379–380
OGUsers.com, 379
RaidForums.com, 379
фрагментированные пакеты, 74

FreeBackgroundCheck.org, 330,
331
полный скрип, 313
Фуллер, Роб, 214–215
фаззинг, 147
грамм
Габриэль / Билдштейн (Куроиш),
465–467, 477
Галактика 2, 289, 291
GateHub хак, 453, 478-480
GDPR (Общая защита данных
Положение), 176
геолокация, Cree.py, 343–346
Призрак, 32
Журналы фиксации Git, 287–288
GitHub, 280
SearchCode.com и, 281
Gitlab, Night Lion Security, 312
GitLab, 280
SearchCode.com и, 281
Гитроб, 284–287
Gmail, сброс пароля, 391–393
Гностические игроки, 409
GnosticPlayers, 454–456,
463–476
хакерские методы, 457-459
NSFW, 463
посты, 459–461
сайтов взломано, 457
GnosticPlayers2, 461–462

Google
Проект CT, 202
поиск обратного изображения, 333,
357
кеши поисковых систем, 212–214
Google Analytics, BuiltWith
и, 123
Код Google, SearchCode.com
и, 281
Google Dorks
операторы
allintitle :, 162
allinurl :, 165
кэш :, 165
имя файла :, 165
тип файла :, 162–163
intext :, 165–166
InTitle :, 161-162
inurl :, 163–165
сайт :, 161
запросов, 159
База данных взлома Google. *Видеть*
Эксплойт-БД
Google Images, 334–336
Гринберг, Энди, 295
Управляемые повороты (радужная оболочка), 223–224
Исторический поиск, 224–225
ИП, 225
IP-адрес, 226
Имя сервера, 225
Регистрант Организация, 225
Хэши SSL-сертификатов, 227–229
ЧАС
Хакерская цель, 52–53
HackForums.net, 379
Хаквайзер, 289
Сайпер, 290
участники, 291
Сайт Википедии, 290
Хаднаги, Крис, 324, 382
Хардигри, Стив, 295 лет
HaveIBeenPwned, Skiptracer,
361
Хайд, Алекс, 160
Адский Форум, 35, 275

Ад Reloaded, 32
Исторические поиски Whois,
186
Медицинское программное обеспечение HL7, TDO
и, 29–30
гомоглифы, 61
Медовый барсук, 25 лет
Охотно, 9
Хант, Троя, 414, 419
я
ICANN (Интернет-корпорация
для присвоенных имен и
Числа), 176
ICQ, сброс пароля и,
403–404
IDS (система обнаружения вторжений),
70
поиск изображений, 333
EagleEye, 333, 340-343
Google Images, 334–336
обратный поиск изображения, 357
Google поиск обратного изображения,
333
повторно использованные фото профиля, 339
TinEye, 333, 336–340
ImageRaider, 340
изображения, сохранение из соц.
медиа, 357
Instagram, сброс пароля, 400

IntelTechniques, 7–8
задачи, 95–96
взаимодействие с субъектами угроз
растягивая, 433-434
поток информации
заведение, 446
хакерская драма и, 447–452
Обфускация / Страдинатрас,
436–439
TDO, 450–451
WhitePacket, 434–440
YoungBugsThug, 440–446
intext: оператор, придурки, 165–166
название: оператор, придурки, 161–162
Intrigue.io, 84, 95, 257
информация о ведре, 259–260
EmailAddresses лица, 156
сущностей, 95
Вкладка Entities, 96–99, 154–155
станки, 95
полученные результаты
анализ, 104–105
экспорт, 105–107
Выполнение задачи, 152-154
модуль паука, 152–153
Анализ uberpeople.net, 99–103
URI Spider, 152–153, 257–259
inurl: оператор, придурки, 163–165
Inurlbr, 169-173
исследования, 19
Кархарт, Лесли, 25–26
киберпреступники, 26–27
дорожки, 25–26
IP-адреса
Управляемые точки поворота (радужная оболочка), 226
запросы исторической информации,
297
история, BuiltWith, 124
идентификация собственника, 295
обратный поиск, DomainTools,
189
трекинг, 346–347
WPScan, 138
Атрибуция IP, 46
Iris, 221-222, 474-476

Вкладка "История хостинга", 232–234
Поворотный двигатель, 222
Guided Pivots, 223–224,
225–229
Исторический поиск, 224–225
IP-адрес, 226
Вкладка История снимков экрана, 232,
235, 240
строка поиска, 222
Вкладка «История WHOIS», 230–231
J
Java API, Elasticsearch, 308
jQuery, сброс пароля и,
400–403
JSON
Elasticsearch, 308–310
Выход экранопланов, 126–128
K
Карвуниарис, Деннис, 451
Байдарка, 331
Кэй, Дэниел, 442–443
Кел, Data Viper and, 469–472
ключевые слова, несколько, WHOIS,
179–181
Форум KickAss, 275, 284
закрытие, 388
Сайпер, 32 года
социальная инженерия и,
383–387

L

замены букв, имя пользователя
поисковые запросы, 369
LinkedIn, Skiptracer, 361
Linux, конфигурация, 5–6
Лайткойн, 13
журналы, журналы фиксации Git, 287–288
Lucidchart, 198

M

МАБНА, 409
Мальтего, 5
SocialLinks, 350–351, 358–360
Мартин, Уильям, 73-74, 311
параметр matchdump ,
Elasticsearch, 317–318
метаданные. *Также* документ
метаданные
Метагоофил, 248–250
Metasploit
enum _ wayback (сценарий Ruby),
215–216
Рекон-НГ и, 108
Очистка Wayback Machine,
214–215
Менье, Кристофер, 435
ОСИНТ.рест, 355–357
Microsoft, сброс пароля,
399–400
инструменты отображения разума, 198
MindBendingBeats.ca, 237
Mindnode, 198
Mirai зловред, 442
MITM (человек посередине)
атаки, 202
MO (modus operandi), 27
модули, Recon-NG
хакерская цель, 114
список, 108–109
поисковые запросы, 111
Шодан, 115–116
используя, 111–115
вируустоталь, 113, 114–115
MongoDB, 293, 301
инструменты командной строки, 305–308
команды

найти (), 307
найти () .pretty (), 307
показать dbs, 307
использовать, 307
подключение к базе данных, 305–306
документы, 302
NoScrape и, 312, 313
основной соскоб, 313
полный скрип, 313
выкупленный сервер, 313–314
Инструмент робот 3T, 302–305
Кнопка подключения, 303
PrivateDB, 303–304
РоботМонго, 302
мораль, 24
MTU (максимальная передача
ед.), 74
Мердок, Кэт, 327, 333–334
MySpace, Skiptracer, 361
N
namedroppers.com, 177-179
Nclay, 453–454
Взломы сайта GnosticPlayers, 458
Рейдовые форумы, 456
Ндифф, 79
НеоБосс, 426
Night Lion Security, страница Gitlab,
312
NightCat, 435–436

Ночная площадь, 288
NMAP
- мтю, 74
- прокси, 73
- причина, 71
-A, 74
-badsum, 76
-f, 74
-O, 74
-p-, 68
-scanflags, 68, 69
-sn, 68
-sS, 69
-sU, 68, 69, 74
-cB, 74
-sW, 70
-sX (Рождественское сканирование), 68, 69
-T, 76
-T3, 76
-T4, 76
ФИНПШ, 69
брандмауэров, 70
контрольные суммы, 76-77
изменение длины данных, 78
приманка сканирования, 77
распределенное сканирование, 73–74
TOR, 73-74
угли, 79
фрагментированные пакеты, 74
Подмена IP-адреса, 78–79
Подмена MAC-адреса, 78–79
MTU (максимум
блок трансмиссии), 74
обнаружение службы, 74–75
сроки запросов, 76
Ндифф, 79
проксичейны, 73
ПШ, 69
ответ причины, живой сервер
идентификация, 71–72
отчеты, 80
сравнение результатов, 79–81
сканы, 67
список активных хостов, 68
конфигурирование, 68–69

ФИН, 68
полное сканирование портов, 68–70
SYN, 68
TCP-порты, 69
Окна TCP, 70
типы, 69
СИНФИН, 69
uberpeople.net, 100–101
NoScrape, 304, 311–312
Корзины Amazon S3 и, 312,
320–321
CassandraDB и, 312, 318–319
Elasticsearch и, 312
свалка, 317
поиск по ключевым словам, 315
matchdump, 317–318
скан, 314–315
поиск, 315–317
MongoDB и, 312
основной соскоб, 313
полный скрип, 313
выкупленный сервер, 313–314
Базы данных NoSQL, 293, 301
CassandraDB, 301
Elasticsearch, 301
дамп данных, 311
запрос, 308–311
MongoDB, 301
инструменты командной строки, 305–308
Инструмент робот 3T, 302–305
РоботМонго, 302

NSA (Душевное спокойствие), 32, 36, 374,
445–446
псевдонимы, 38
враждебность, 37–38
Департамент Мотор Луизианы
Транспорт, 36
NSFW, 463, 476–477, 480
Nulled.to, 379–380
O
Обфускация / Страдинатрас,
436
TDO и, 437–439
OGUsers.com, 379
Инструменты разведки с открытым исходным кодом,
6
инструменты с открытым исходным кодом, 5
операторы, придурки
allintitle :, 162
allinurl :, 165
кэш :, 165
имя файла :, 165
тип файла :, 162–163
intext :, 165–166
InTitle :, 161-162
inurl :, 163–165
сайт :, 161
OPSEC, тщеславие и, 429
Оранжевый - это новый черный, TDO
(Темный повелитель) и, 27
OSINT, 2
каркас, 6
OSINT.link, 6
ОСИНТ.рест, 350–351
Команды CURL, 351
Поиск в Facebook, 352–357
Запустить кнопку "Почтальон",
351
Поиск информации по телефону,
351–352
Twitter, 357–358
П
пакеты, фрагментированные, 74
URL-адреса на основе параметров, Photon,
150
менеджеры паролей, 409

пароли, 408–409
профильная матрица, 409–413
переработка, 409
сброс, 382, 390–391
Facebook, 393–394
Gmail, 391–393
ICQ, 403–404
Instagram, 400
ответы jQuery, 400–403
Microsoft, 399–400
PayPal, 394–397
Twitter, 397–399
лист сверки, 391
вставить сайты, 273
psbdmp.ws, 273–274
PayPal, восстановление пароля, 394–397
Спокойствие духа. *См.* АНБ (Мир ума)
поиск людей, PIPL, 326–330
PeopleLocker, 330, 331
Петя / НоПетя, 14
фишинговые домены, 61–64
DNSTwist, 61–62
номера телефонов, Skiptracer
поисковые запросы, 364–366
Фотон, 149, 237
Карта DNS, 152
информация извлечена, 150
параметры, 150

ползет, 151–152
Очистка Wayback Machine,
216–217
PHP
Data Viper и, 420
Инурлбр, 172
ПИПЛ, 326
Поворотный двигатель (Ирис), 222
Guided Pivots, 223–224,
225–229
Исторический поиск, 224–225
ИП, 225
Имя сервера, 225
Регистрант Организация, 225
Хэши SSL-сертификатов, 227–229
Исторический поиск, 224–225
IP-адрес, 226
шарнирные, 222
PrivateDB (MongoDB), 303–304
матрица профиля
F3ttywap, 409–413
форумы
список запретов, 381
поиск, 379–381
прокси, Storm Proxies, 10–11,
138
psbdmp.ws, 273–274
публичные записи
Ancestry.com, 331–332
FreeBackgroundCheck.org, 330
SkipEase.com, 330
Python
Skiptracer
поиск адреса электронной почты,
361–364
поиск телефонных номеров,
364–366
поиск по имени пользователя, 366–369
Userrecon, 370–372
Q
запросы, MongoDB, 302
цитаты, придурки, поисковики,
160
p
Рейдовые форумы, 456

RaidForums.com, 379
программа-вымогатель, Петя / NoPetya, 14
RDP (протокол удаленного рабочего стола),
29
ReactJS, 420
Разведка-НГ, 84, 107–108
команды
добавить домены, 110
обратная решимость, 112
набор исходников, 112
показать домены, 110–111
показать варианты, 112
базы данных, локальные, 110
домашний экран, 108
Метасплоит а, 108
модули
хакерская цель, 114
хосты-хосты / разрешение, 111–112
Интересные_файлы, 252–254
список, 108–109
Metacrawler, 250–252
Канцелярская кнопка, 254–257
поисковые запросы, 111
используя, 111–115
вируустоталь, 113, 114–115
Шодан, модули, 115–116
Reddit Investigator, 372–374.
шаблоны регулярных выражений, Photon, 150
Регпак, 23
отчеты, NMAP, 80
обратный поиск IP, 189
Обратный WHOIS, 196

Восстание, 374
Поиск в Twitter, 398
Робб, Бев, 435
Робертс, Крис, 274–275,
276
Робот 3T (MongoDB)
PrivateDB, 303–304
экраны, 302–303
Студия 3T, 302
Инструмент Robot 3T, кнопка подключения,
303
РоботМонго, 302
Ruby, скрипт enum _ wayback,
215–216
S
САНС, 325
параметр сканирования , Elasticsearch,
314–315
сканы, NMAP, 67
список активных хостов, 68
конфигурирование, 68–69
ФИН, 68
полное сканирование портов, 68–70
SYN, 68
TCP-порты, 69
Окна TCP, 70
типы, 69
соскабливание
основной соскоб, 313
репозитории кода, 280–281
Журналы фиксации Git, 287–288
Гитроб, 284–287
SearchCode.com, 281–284
форумы, 274
полный скрип, 313
NoScrape, 311–312
Корзины Amazon S3 и, 312,
320–321
CassandraDB и, 312,
318–319
Elasticsearch и, 312,
314–318
MongoDB и, 312
вставить сайты, 273–274
theHarvester, 269–273.

инструменты, URL, 217–219
Wayback Machine, 214–215,
237–238
Фотон, 216–217
дайджест сайта, 219–220
вики-сайты, 288–289
Википедия, 289–292.
скриншоты
DomainTools, 193–194
история, 232
скрипт-детишки (салазки), 274
SCT (подписанный сертификат
отметки времени), 202
поисковые системы
тайники, 212–214
dorks (*См.* dorks, поиск
двигатели)
количество пределов поиска, 270
параметр поиска , Elasticsearch,
315–317
SearchCode.com, 281
BitBucket, 281
ложноотрицательные, 283–284
Журналы фиксации Git, 287–288
GitHub, 281
GitLab, 281
Гитроб, 284–287
Код Google, 281
SecLists, 9
секретные ключи, Фотон, 150
обнаружение службы, 74–75
Шодан, 53–55

параметры командной строки, 296
команды, синтаксический анализ, 296
Elasticsearch и, 296
модули, 115–116
запросы, исторические данные,
296–298
результаты, скачивание, 296
сайт: оператор, придурки, 161
салазки (скрипт-кидди), 274
SkipEase.com, 330, 331
Skiptracer
AdvandedBackgroundChecks,
361
поиск адреса электронной почты,
361–364
HaveIBeenPwned, 361
LinkedIn, 361
MySpace, 361
поиск телефонных номеров,
364–366
Настоящие люди, 361
Поиск правды, 361
поиск по имени пользователя,
366–369
SOC (охранные операции
центр), 25
социальная инженерия, 381–382
История Аргона, 383–387
Форум KickAss и, 383–387
социальные сети, 349
изображений, сохранение, 357
ОСИНТ.рест, 350–351
Поиск в Facebook, 352–357
Инстаграм, 354
Фотон, 150
Reddit Investigator, 372–374.
Skiptracer
поиск адреса электронной почты,
361–364
поиск телефонных номеров,
364–366
поиск по имени пользователя, 366–369
На базе TOP, 289
Userrecon, 370–372
SocialLinks, 350–351
Пользователи Maltego, 358–360

пробел _ finder.rb CSF, 299,
300–301
паук _ finder.rb CSF, 299
Паучья Фут, 84
доступ, 85
список обнаруженных элементов, 90–91
Сканирование IP-адреса, результаты, 86–87
uberpeople.net, 89–90
VirusTotal, 87-88
SpiderFoot HX, 91 год.
раздел результатов, 92–93
Дуб паук, CSF
(CloudStorageFinder) и, 299
SSL-сертификаты, Pivot Engine,
227–229
веб-сайты государственных судов, 332–333
Штормовые прокси, 10–11, 138
Страдинатрас, 436
Стрэнд, Джон, 24–25, 325–326, 347,
386–387
поддомены
CT (прозрачность сертификата)
и, 202
CTFR, 203–204
Фотон, 150
Sublist3r, 58–59
SYN сканирование, 68
T
TCP, оконное сканирование, 70
TDO (Темный повелитель), 27–28
Вывод биткойнов, 451

стиль общения, 30
форумы и, 275–278
состав группы, 30–31
Арни, 32–35
Cr00k, 35–36
Cyper (CyPeRtRoN), 31–32
NSA, 36–41
здравоохранение, 32
Закрытие форума KickAss,
388–389
смена руководства, 36–37
Обфускация / Страдинатрас,
437–439
Поиск PIPL, 329–330
презентация, 38–41

школа терроризма, 37
жертвы, 28–29 лет
TeamSkeet.com, 424–425
Термбина, 8
Талет-Фишер, Максим, 455
Харвестер, 268
аргументы, 268–269
параметры
-b, 270
-d, 270
-л, 270
сканы, бег, 269–273
субъекты угроз. *См. Также* конкретные
актеры
взаимодействуя с, вытягивая,
433–434
Поиск в WHOIS, 182–183
Тим Томес, 25 лет
TinEye, 333, 336–340
Сайпер, 336
жетоны, Канарские жетоны, 25
инструменты, с открытым исходным кодом, 5
TOR, 73-74
трейдеры, криптовалюты, 17–18 лет
Настоящие люди, Skiptracer, 361
Поиск правды, Skiptracer, 361
Твиттер
ОСИНТ.рест, 357–358
сброс пароля, 397–399
типосквоттинг, 61–64
DNSTwist, 61–62
U
uberpeople.net
Intrigue.io, 99–103
SpiderFoot, 89–90
URL
Фотон, 150
общественные, CSF и, 299
скребковые инструменты, 217–219
поле user-agent (HTTP-заголовок),
125
имя пользователя
замены букв, 369
Поиск Skiptracer,
366–369
Userrecon, 370–372
V

лист проверки, пароль
сбросить и, 391
Verification.io, 311
Просмотр записи Whois
(DomainTools), 190–191.
VirusTotal, 87-88
уязвимости
Сканы CMSMap, 131–132
WordPress, плагины, 139–141
W
Wayback Machine, 211–212, 468
Фотон, 150
соскабливание, 214–215, 237–238

enum _ wayback (сценарий Ruby),
215–216
Фотон, 216–217
дайджест сайта, 219–220
скриншоты а, 193
поисковые роботы
ползет, 151–152
Фотон, 149
Wfuzz, 146
Коды ответов 301/302,
148
выход, 148
параметры, 146–147
папка typo3temp , 148
сканирование, комбайн,
271–272
WhitePacket, 434–435
Билл, 439–440
Reddit Investigator, 373
Робб, Бев, 435
Twitter, 358
YoungBugsThug, 440–446
WhitePacket.com, 184–185,
234–235
Белые страницы, 330, 331
WHOIS, 47, 89, 175–176
перекрестная проверка информации,
197–199
использование данных, 176–177
Домен поле Status, 195
домены, поиски, 177
продвинутый, 181–182
ключевые слова, многократные, 179-181

namedroppers.com, 177-179
исполнители угроз, 182–183
DomainTools, 177
Просмотреть запись Whois, 190–191
Исторические поисковые запросы Whois, 186
историческая, 177
история, 192, 193
смена собственников, 194–195
Обратный WHOIS, 196-197
WhitePacket.com, 184–185
Whoisology.com, 177,
183–184
расширенный поиск, 187
Вкладка История WHOIS (Ирис),
230–231
Whoisology.com, 183–184
расширенный поиск, 187
Исторические поиски Whois,
186
WhitePacket.com, 184–185
WhoisRWS, 47
WIG (информация о веб-приложении
Собирателя), 124
CMS и, 124–125
файловый вывод, 126–128
Вывод JSON, 126–128
параметры, 125
сканирование всех целей, 126
маскирование пользовательского агента, 125
вики-сайты, 288–289
Википедия, 289–292.
Википедия, 289–292.
Сравнить выбранные версии
кнопка, 291
инструменты различий, 291
Просмотр страницы истории, 290
Проводной, 295
Вуд, Робин, 298
словари
Cewl, 10
Кранч, 10
SecLists, 9
WordPress

плагины, уязвимости,
139–141
WPScan и, 136–141

WPScan, 132
- перечислим u, 138
- сила, 137
- прокси, 137
- незаметный, 137
IP-адреса, ротационные, 138
выход, 134–136
параметры, 133–134
WAFs, 136–141
WordPress не обнаружен,
136–141
Вятт, Натан, 32, 349. *См. Также*
Арни, TDO и
Закон о неправомерном использовании компьютеров, 33
Интервью с инакомыслящим, 33 года
экстрадиция, 33–34
обвинительный акт, 33–34
ОСИНТ.рест, 352–354
Аудио YouTube, 34
Икс
Xdedic, 29
XLS файлы, доркс, 162, 163
Y
Yahoo !, придурки, 169
Яндекс, 340
YoungBugsThug, 433–434,
440–446
Z
ze0ring, 276
ZIB троян, 435
Зынга, 459

Первод сделан специально для

лучшего кунала в Telegram

Max Open Source

Academy: Information technologies

(https://t.me/coursmax)

Альтруист и подпищик канала.

Также спасибо администрации проекта, за ваш вклад в IT.