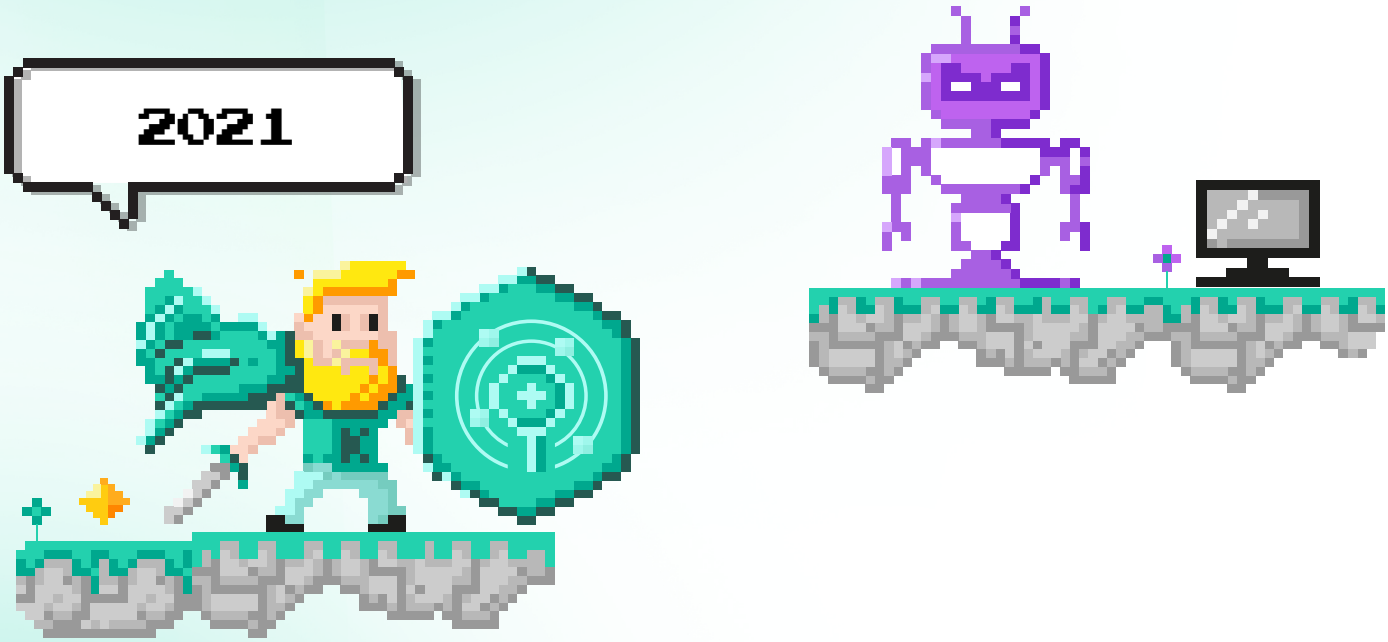
Managed Detection and Response: Аналитический отчет



kaspersky

Основные выводы

Managed Detection and Response

до 2 критических инцидентов ежедневно

41 мин. среднее время обнаружения инцидента

77 % инцидентов успешно остановлены после первого оповещения

Ключевые регионы (% клиентов)

Европа	Россия и СНГ	АТР
47 %	23 %	16 %

Ключевые европейские заказчики (% клиентов)

Италия	Германия	Австрия
30 %	25 %	11 %

Наиболее атакуемые индустрии (% клиентов)

Производство	Финансы	ИТ
17 %	16 %	12 %

Профили атакующих	Техники и тактики	Инструменты
41 % Целевая атака	T1566: Фишинг TA0001: Первичный доступ	powershell.exe
18 % Анализ защищенности	T1210: Использование уязвимостей удаленных служб TA0008: Горизонтальное перемещение	rundll32.exe
14 % Криминал	T1204: Запуск пользователем TA0002: Выполнение	certutil.exe
...		...

Критичность инцидентов

14,3 % Высокая — **65,4 %** Средняя — **20,3 %** Низкая

Рекомендации

- С каждым годом увеличивается количество целевых атак, реализуемых при непосредственном участии человека. Для их эффективного обнаружения необходимо внедрить активный поиск угроз (threat hunting) в сочетании с классическим мониторингом событий безопасности[1]
- Целевые атаки хорошо воспроизводятся в рамках киберучений с участием Red team[2], поэтому последние являются отличным способом тренировки команд по обнаружению атак и оценке безопасности организации
- Более 14% инцидентов высокого уровня критичности связаны с вредоносными программами, что доказывает необходимость многоуровневого подхода к защите[3]
- Использование базы знаний MITRE ATT&CK[4] способствует эффективности обнаружения. Самые сложные атаки состоят из простых шагов, техник, и обнаружение одного шага может позволить выявить всю атаку

[1] https://www.kaspersky.com/enterprise-security/managed-detection-and-response
[2] https://www.kaspersky.com/enterprise-security/security-assessment
[3] https://www.kaspersky.com/enterprise-security/wiki-section/products/multi-layered-approach-to-security
[4] https://attack.mitre.org/

Введение

О сервисе Kaspersky MDR

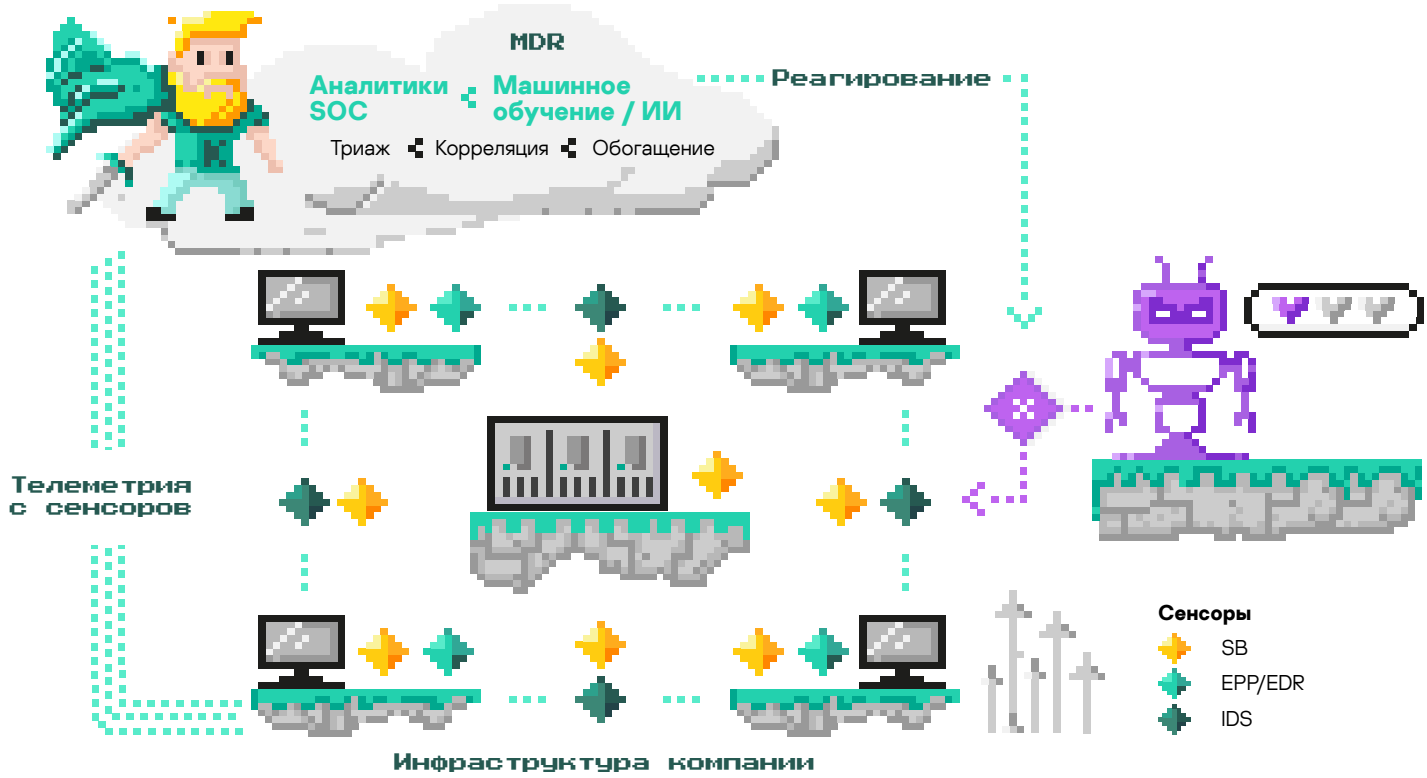
Kaspersky Managed Detection and Response (MDR) позволяет организациям дополнить существующие возможности обнаружения, а также усилить внутреннюю команду безопасности, чтобы в режиме реального времени 24x7 защищать корпоративную сеть от растущего количества сложных угроз. Мы собираем телеметрию и анализируем ее с использованием технологий машинного обучения при непосредственном участии экспертов по обнаружению атак.

Аналитики Kaspersky SOC расследуют события безопасности и оповещают клиента о вредоносной активности, предоставляя инструментальное реагирование и рекомендации.

5/5 рейтинг "Лаборатории Касперского"

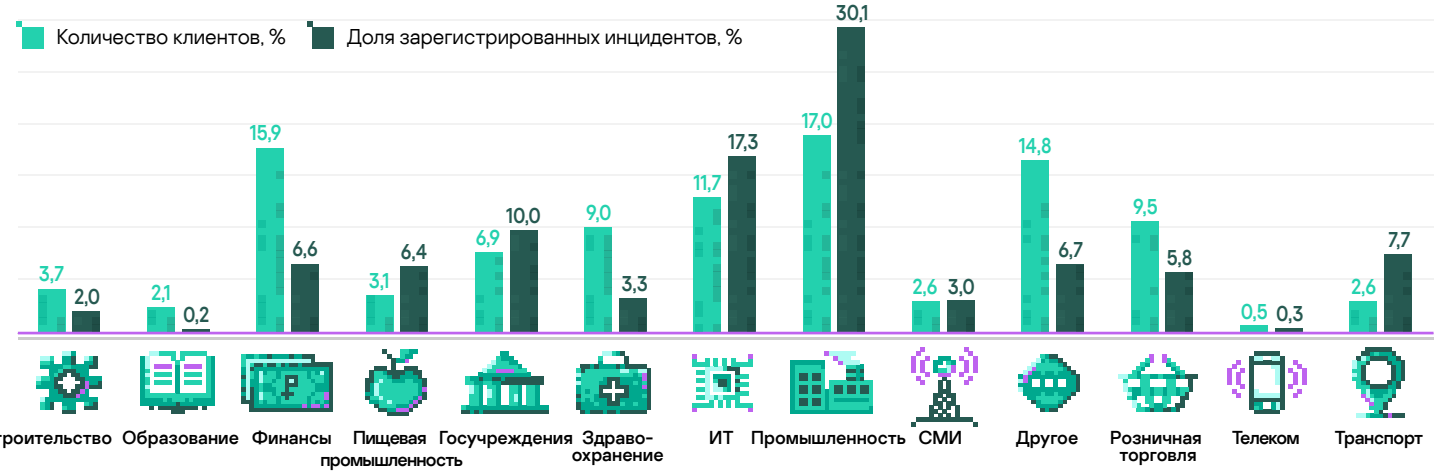
в MDR

на основе отзывов реальных клиентов в Gartner Peer Insights™ (по состоянию на 9 февраля 2022 г.)[1]



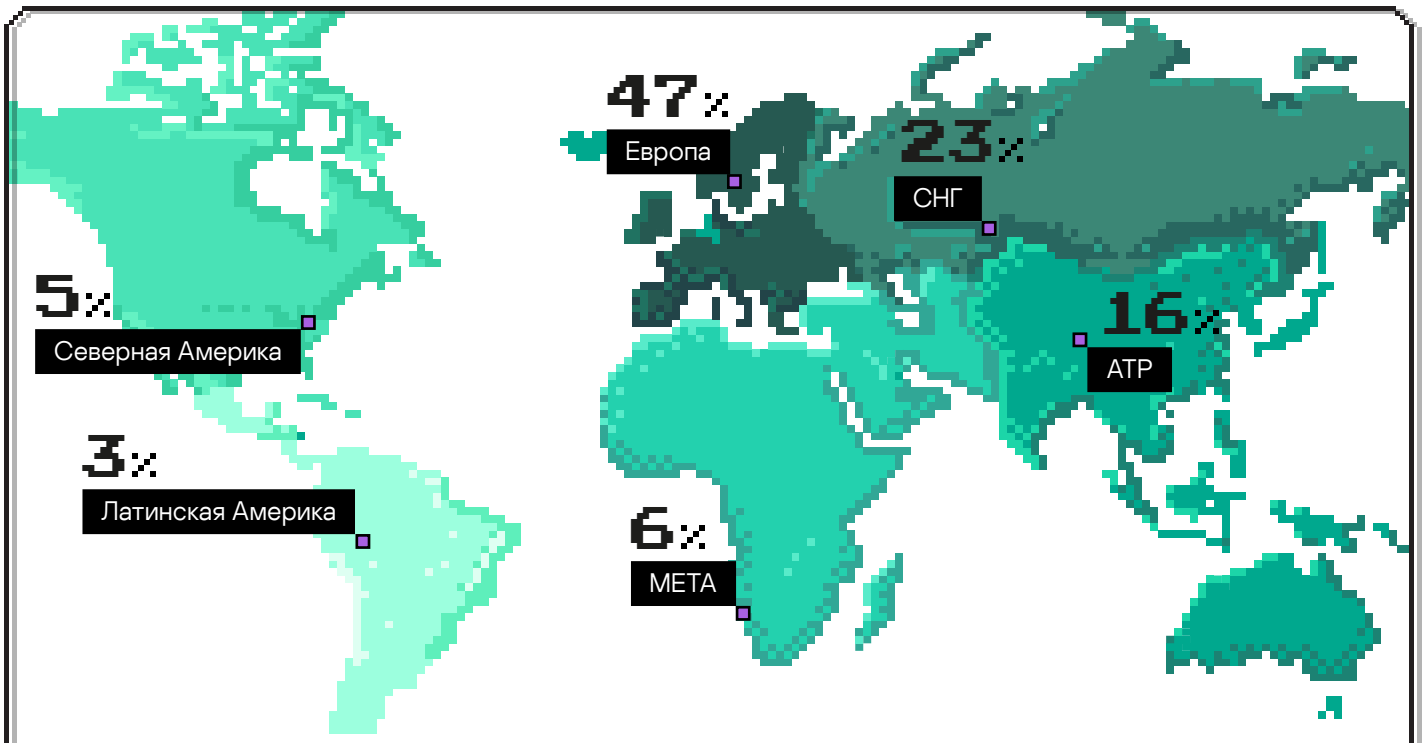
Охват Kaspersky MDR: отрасли

В 2021 году сервис MDR использовался в разных отраслях. Большинство наших клиентов относятся к промышленным, финансовым или ИТ-организациям.

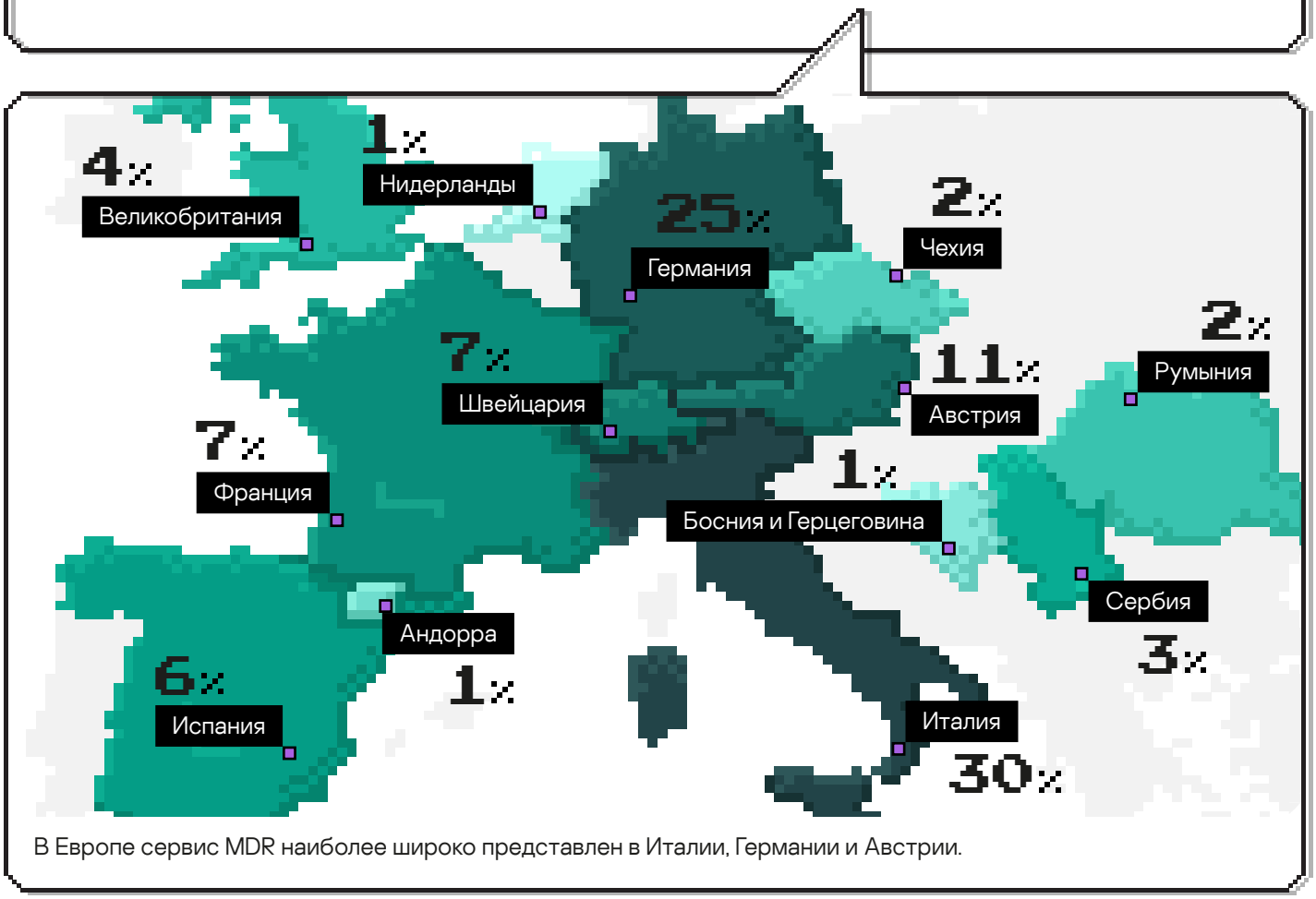


[1] https://www.kaspersky.com/about/press-releases/2022_kaspersky-managed-detection-and-response-gets-highest-rating-in-gartner-peer-insightstm

Охват услуги MDR: регионы



Чтобы правильно понять имеющуюся информацию об угрозах, необходимо уточнить распространённость услуги в различных регионах: природа инцидентов, тактики и техники имеют географическую специфику.



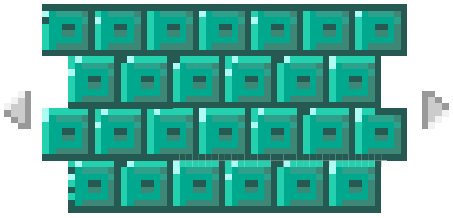
В Европе сервис MDR наиболее широко представлен в Италии, Германии и Австрии.

Режим использования MDR

В 2021 году MDR каждый день получал огромное количество телеметрии, в результате чего формировались события безопасности. 36,26% сформированных событий безопасности были обработаны роботом на основе машинного обучения. 6,67% событий безопасности, обработанных аналитиками SOC, были следствием реальных инцидентов, о которых сообщалось клиентам через портал MDR.

Ежедневные события от одного хоста

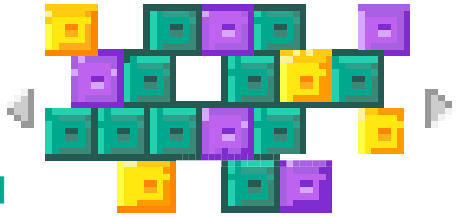
~15 тыс.



Этот показатель может значительно меняться в зависимости от активности хоста

Из которых были обработаны

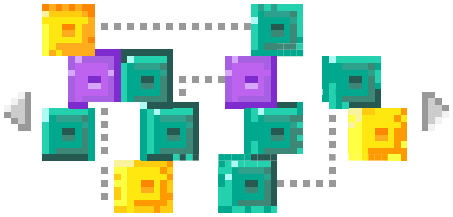
414 тыс. событий безопасности



Более 150 тыс. событий безопасности было обработано автоматически с помощью ИИ, а более 264 тыс. были проанализированы аналитиками SOC

В результате клиентам сообщили о

8 479 инцидентах

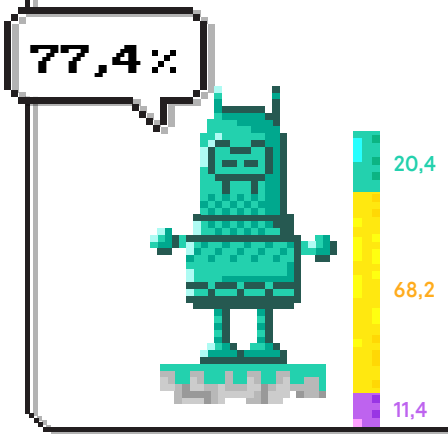


~18 тыс. событий безопасности свидетельствовали об инцидентах, что составляет ~7% от общего количества событий

Эффективность реагирования

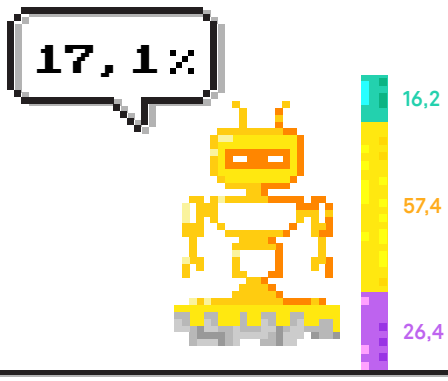
1 событие безопасности

77,39% инцидентов остановлены после первого оповещения. Это свидетельствует о высокой эффективности реакции.
В эту категорию попадают и типовые инциденты с четкими сценариями реагирования[1]. Доля критичных инцидентов здесь самая низкая – 11,38%



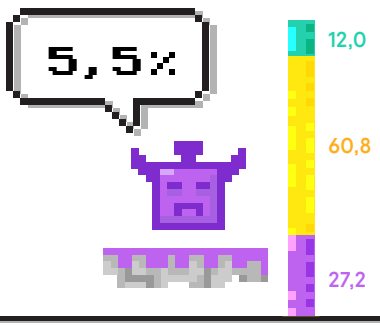
2-4 события безопасности

17,13% инцидентов выявлены на основе 2-4 событий безопасности. Для предотвращения обхода обнаружения для одной угрозы мы используем разные технологии, создающие разные события безопасности. Эта категория демонстрирует нам будущие возможности по улучшению обработки событий безопасности



5+ событий безопасности

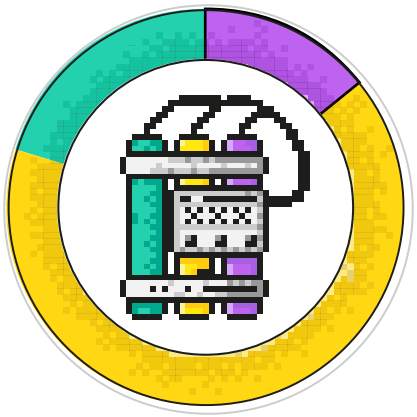
5,48% инцидентов связаны с 5 и более событиями безопасности. Это случаи, когда реакция была отклонена клиентом или наблюдалась новая целевая атака, требующая тщательного расследования перед реагированием, или клиент запросил мониторинг атаки без активного противодействия. Доля инцидентов высокой критичности здесь самая большая и превышает 27%, а низкой критичности – составляет всего ~12%



[1] Примерами могут являться: подмена файлов функционала специальных возможностей Windows (T1546.008), обнаружение дампа памяти процесса LSASS (T1003.001), обнаружение дампа реестра Windows (T1003.004), обнаружение Rootkit (T1014), атака грубой силы (T1110) и многие другие

Критичность инцидентов

Мы сообщаем заказчикам только об инцидентах, на которые возможна эффективная реакция с их стороны.



14% высокая критичность

атака с участием человека или вирусное заражение, оказывающее серьезное воздействие на бизнес

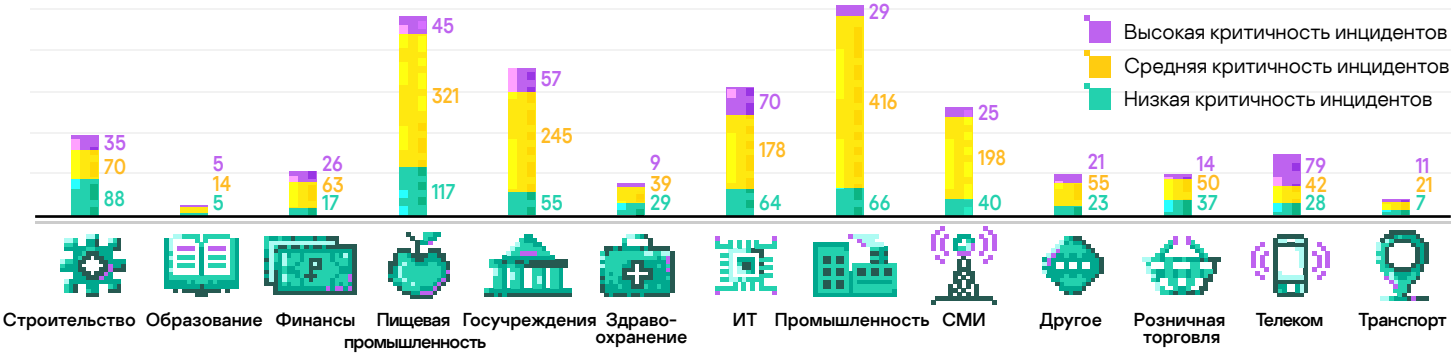
66% средняя критичность

нет подтверждений участия человека, степень воздействия на бизнес – средняя

20% низкая критичность

без существенного воздействия на бизнес, тем не менее существуют мероприятия, которые повысят уровень безопасности

В 2021 году мы ежедневно обнаруживали более одного критичного инцидента.
На приведенной ниже диаграмме отражено количество инцидентов в отношении к 10 000 конечных точек в мониторинге, распределенное по индустриям.



Сколько времени требуется для обнаружения инцидента?

Жизненный цикл события безопасности начинается в очереди, откуда аналитик SOC берет его в работу, исходя из критичности и времени до нарушения метрик SLA[1]. Если анализ показывает ложное срабатывание[2], событие безопасности игнорируется, создаются клиентские и/или глобальные фильтры[3]. В противном случае событие безопасности импортируется в инцидент, который или может быть закрыт как ложное срабатывание, или о нем будет отправлена информация клиенту через портал MDR вместе с рекомендуемой реакцией. Одобрение клиентом рекомендаций по реагированию через портал приведет к автоматическому их выполнению агентами на конечных точках.

41,4 мин. высокая критичность

Самые сложные инциденты, требующие больше времени на дополнительное обогащение данных и проверки. По сравнению с предыдущими периодами[4] нам удалось сократить это время за счет большей автоматизации работы аналитика и введения новых полей телеметрии, существенно ускоряющих триаж

34,8 мин. средняя критичность

Наиболее распространенный уровень критичности. В сравнении с предыдущими периодами это время увеличилось за счет выявления новых типов инцидентов, для которых еще не реализована автоматическая обработка. Другая причина – это увеличение числа критичных инцидентов, приводящее к сокращению ресурсов аналитиков, выделяемых на обработку инцидентов средней и низкой критичности

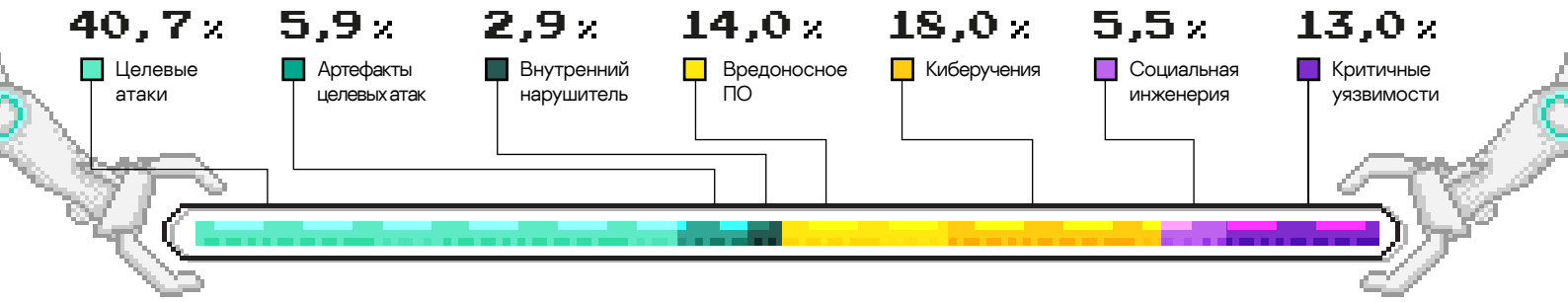
40,2 мин. низкая критичность

Инциденты самой низкой критичности провели больше времени в очереди

[1] SLA – соглашение об уровне сервиса (Service Level Agreement)
[2] 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
[3] 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
[4] https://media.kaspersky.com/ru/business-security/mdr-analyst-report-2020.pdf

Природа критичных инцидентов

Каковы причины критичных инцидентов?



Более 40% всех выявленных в 2021 критичных инцидентов были связаны с целевыми атаками

Почти 6% инцидентов связаны с обнаруженными следами ранее активных атак с участием человека (целевые атаки или киберучения)

Немногим менее 3% инцидентов были связаны с внутренними нарушителями[1]

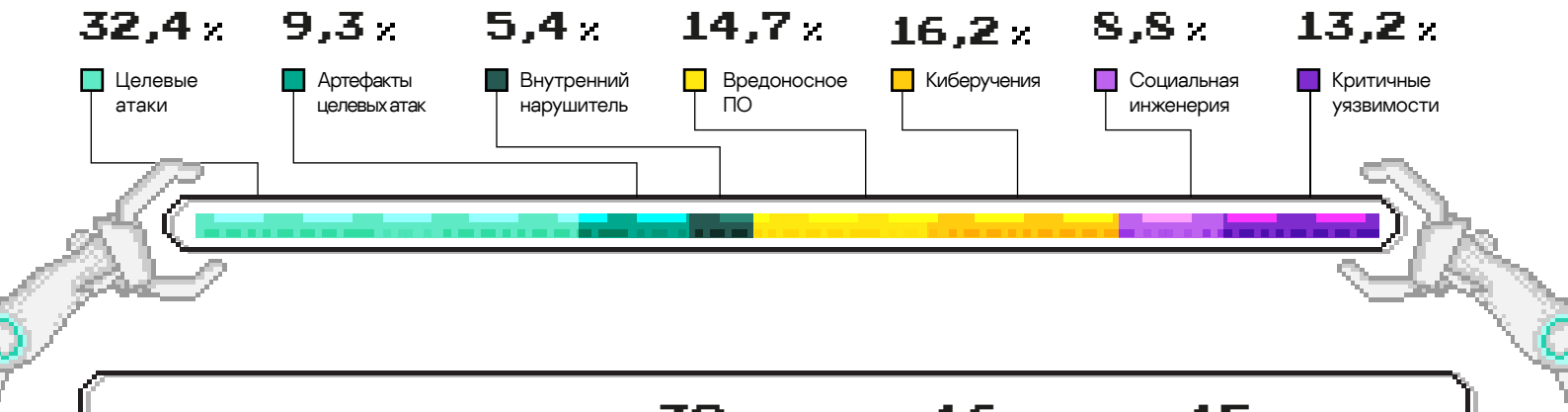
Атаки вредоносного ПО с серьезными последствиями – 14%

Киберучения (тестирование на проникновение, учения с участием Read team и т. п.) составили 18%.

Около 5,5% инцидентов – результат успешного использования социальной инженерии с последующим развитием, приведшим к серьезным последствиям

Чуть менее 13% инцидентов связаны с публично доступными критичными уязвимостями

Как много организаций столкнулись с критичными инцидентами?



Результаты по заказчикам сервиса Kaspersky MDR в значительной степени повторяют статистику по количеству инцидентов.

Лидеры аналогичны:

~32 % Целевые атаки

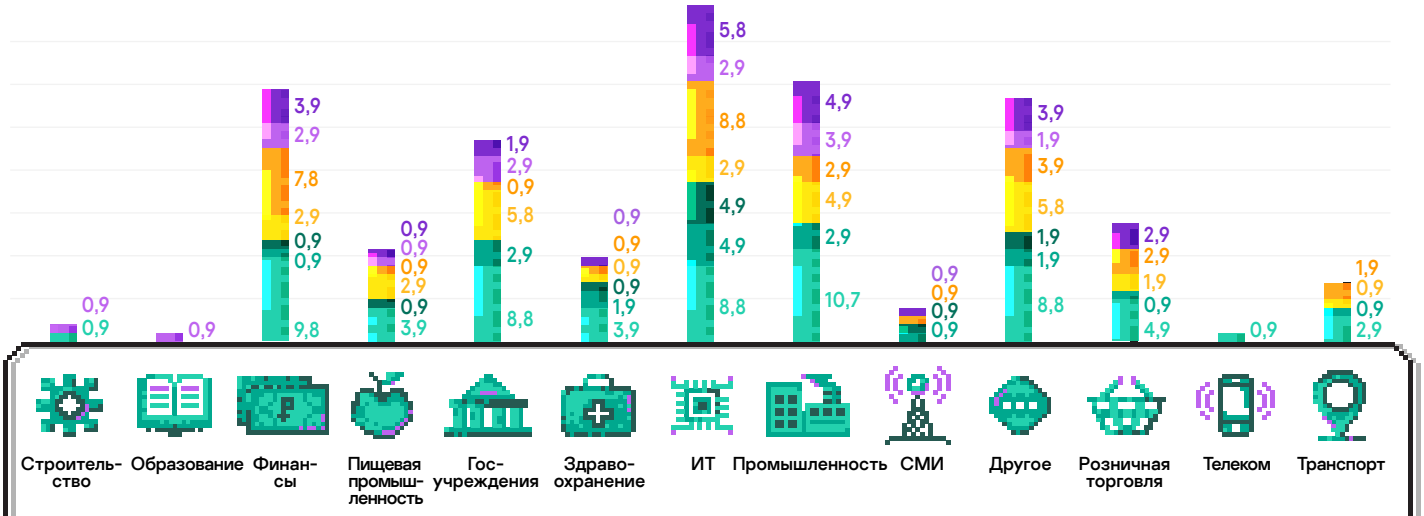
~16 % Киберучения

~15 % Вредоносное ПО с дальнейшим воздействием на бизнес

[1] В инцидентах такого типа нам не удалось обнаружить каких-либо признаков внешних злоумышленников, и подозрительные действия выполнялись от имени действительных привилегированных учетных записей. Мы запрашивали, была ли обнаруженная активность легитимной или нет, но не получали ответа, поэтому у нас нет оснований классифицировать эти инциденты как ложноположительные (например, это могли быть попытки проверить работоспособность MDR или действительно незаконные действия ИТ-персонала, о которых заказчики предпочли нам не сообщать)

Природа критичных инцидентов

Количество организаций по отраслям, столкнувшихся с критичными инцидентами, %

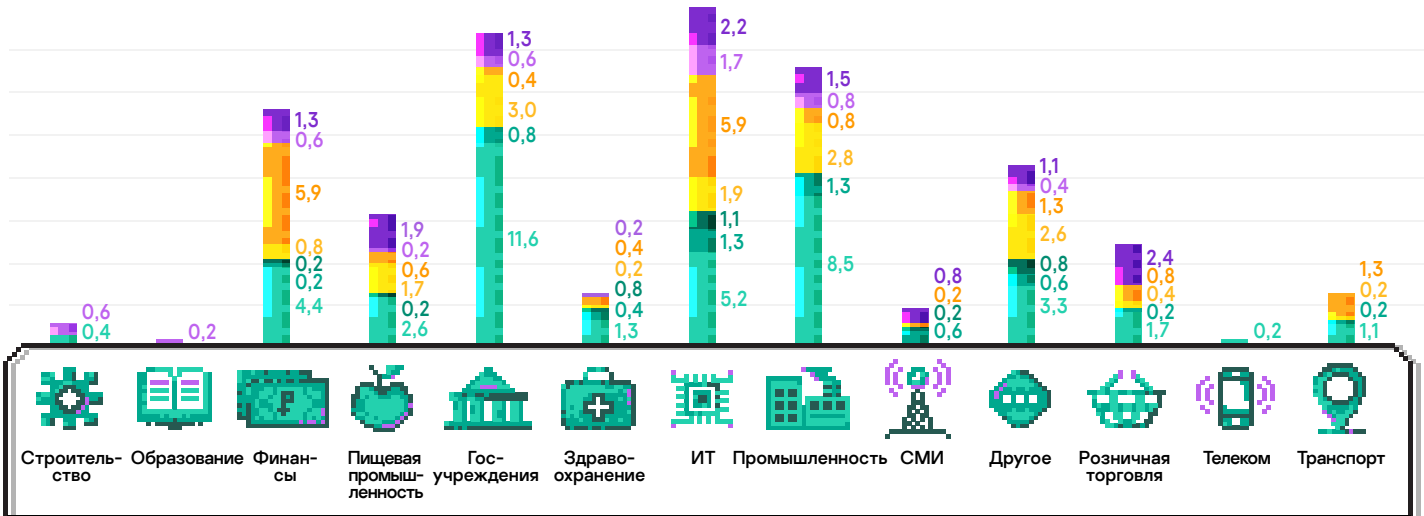


Основные выводы из статистики:

- Большинство отраслей столкнулись со всеми типами критичных инцидентов
- Целевые атаки были обнаружены во всех индустриях, за исключением Образования и СМИ
- В отрасли СМИ обнаруживались инциденты, связанные со следами прошлых взломов
- Практически все отрасли, кроме Строительства, Образования и Телекома, практиковали те или иные виды киберучений
- Социальная инженерия по-прежнему крайне популярна и эффективна

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

Количество критичных инцидентов по отраслям, %



Из статистики можно сделать следующие выводы:

- Наибольшее количество инцидентов, связанных с целевыми атаками, было выявлено в государственных, промышленных, ИТ и финансовых учреждениях
- Финансы и ИТ лидируют по количеству киберучений
- Строительство и Телеком сталкивались с целевыми атаками, но не проводили киберучения
- Успешная социальная инженерия и публично доступные уязвимости коррелируют с инцидентами, связанными с целевыми атаками
- Обнаруженные целевые атаки обычно повторяют статистику инцидентов, связанных с обнаружением артефактов прошлых атак с участием человека

Технологии обнаружения. Тактики, техники и процедуры злоумышленников

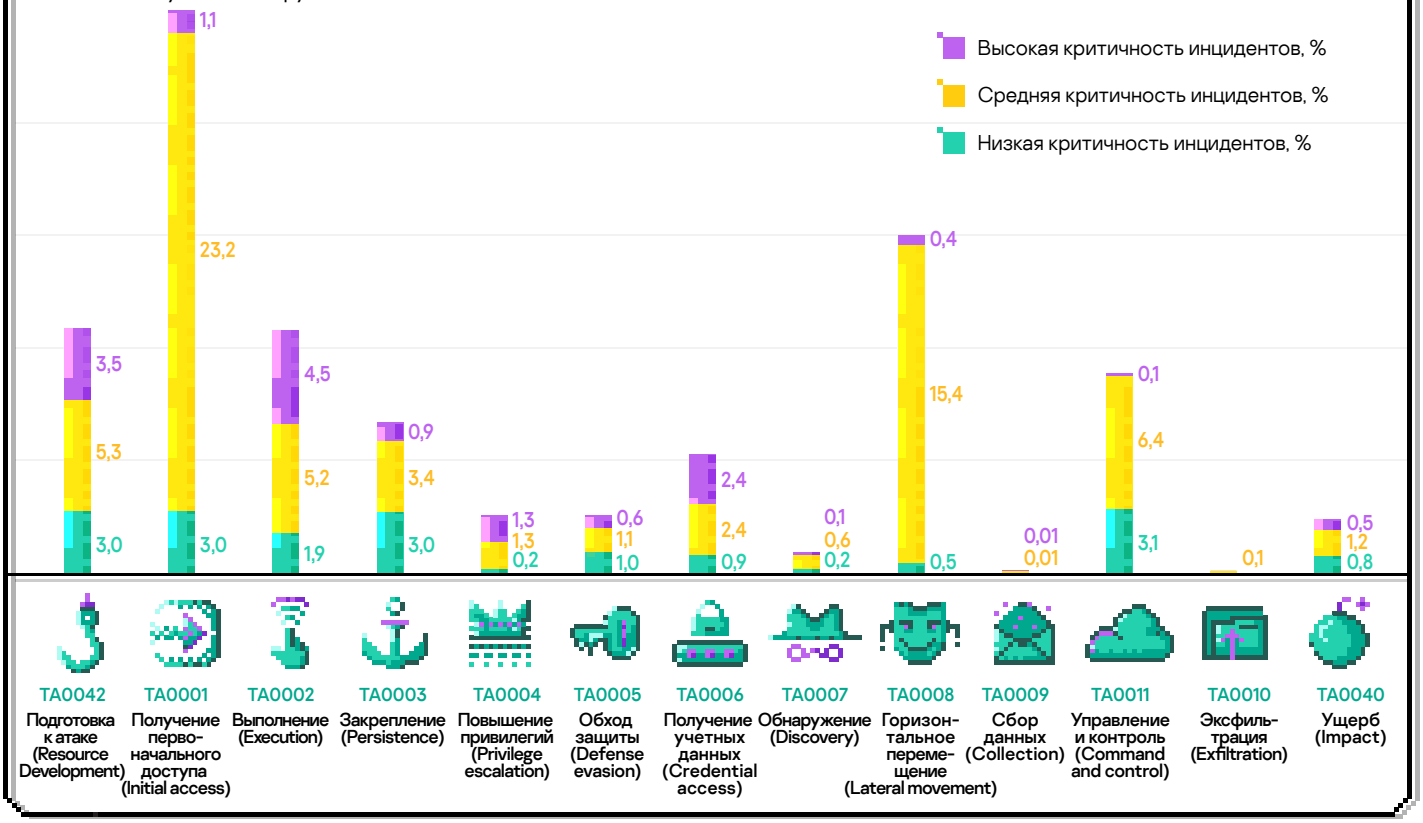
Тактики злоумышленников

MDR позволяет обнаруживать инциденты на разных этапах атаки. Обычно инцидент проходит через все стадии (тактики MITRE ATT&CK), но на диаграмме ниже мы отображаем тактику в момент обнаружения инцидента ...

Подробнее

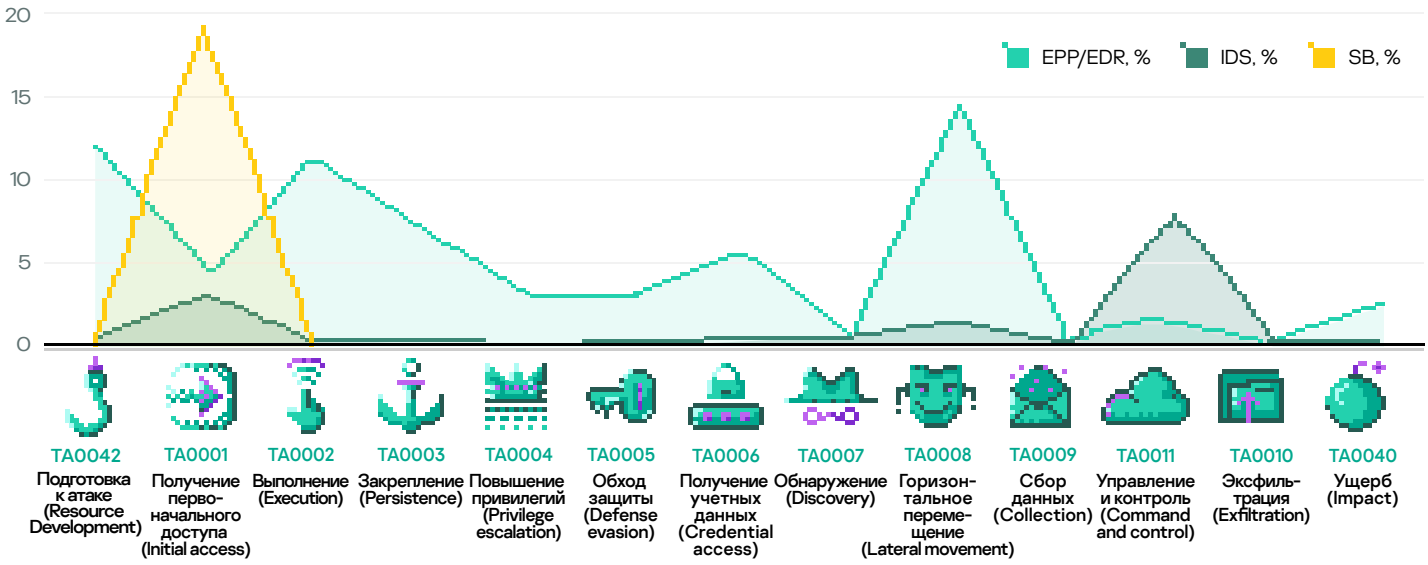
Основные тактики, с помощью которых мы обнаруживаем инциденты:

- Первоначальный доступ в основном покрывается платформой Kaspersky Anti Targeted Attack на сетевом периметре: обнаруживается фишинг и социальная инженерия
- Обнаружение на этапе Подготовки к атаке может показаться странным. Но это инциденты типа «обнаружен подозрительный файл», когда потенциально опасный инструмент наблюдался без каких-либо признаков запуска. Часто это связано с киберучениями, но иногда позволяет выявить реального атакующего, еще не перешедшего в активную фазу
- Обнаружение на этапе Выполнение очень похоже на предыдущее, но здесь мы наблюдали запуск инструмента. Выполнение тяжело скрыть, поэтому наибольшее количество критичных инцидентов было обнаружено на этом этапе. Часто атакующие используют готовые наборы инструментов, и это подтверждает все еще высокую эффективность выявления атак на основе используемых инструментов
- Горизонтальное перемещение обычно хорошо заметно, но количество обнаруженных здесь критичных инцидентов меньше
- На этапе Управление и контроль также выявлено много атак, но в основном это инциденты низкой и средней критичности
- На этапе Обнаружение было выявлено очень мало инцидентов. Это связано со сложностью создания детектирующей логики с приемлемым количеством ложных срабатываний
- Наиболее успешно выявляются атаки на этапах Получение учетных данных, Закрепление и Повышение привилегий, причем с наименьшим количеством ложных срабатываний
- Попытки Обхода защиты также часто приводят к успешному обнаружению



Тактики и технологии обнаружения

В MDR мы анализируем телеметрию с разных типов сенсоров: конечная точка, сетевая система обнаружения вторжений (СОВ) и песочница. Сетевые СОВ и песочница являются частью платформы Kaspersky Anti Targeted Attack (KATA). Доли инцидентов, обнаруженных различными типами сенсоров, представлены на диаграмме ниже.



Получение первоначального доступа

EPP/EDR SB IDS T1566.001
Фишинговое вложение

EPP/EDR T1078
Использование действительных учетных записей

EPP/EDR IDS T1190
Использование уязвимостей публично доступного приложения

EPP/EDR IDS T1133
Использование внешних служб удаленного доступа

EPP/EDR SB IDS 1566.002
Фишинговая ссылка

Выполнение

EPP/EDR SB T1204.002
Запуск вредоносного файла

EPP/EDR T1059.001
Использование PowerShell

EPP/EDR T1053
Вмешательство в работу планировщиков

EPP/EDR T1047
Вмешательство в Windows Management Instrumentation (WMI)

EPP/EDR IDS T1569.002
Вмешательство в Windows service control manager

Закрепление

EPP/EDR T1098
Манипуляции с учетной записью

EPP/EDR T1547.001
Добавление в разделы реестра Run или папку автозагрузки (Startup)

EPP/EDR T1546.008
Запуск через функции для людей с ограниченными возможностями

Повышение привилегий

EPP/EDR T1055.002
Внедрение PE в процесс

EPP/EDR T1055
Внедрение кода в процесс

EPP/EDR T1068
Использование уязвимостей для повышения привилегий

Обход защиты

EPP/EDR T1036.005
Маскировка под легитимное местоположение

EPP/EDR T1036.003
Переименование системных утилит

EPP/EDR T1562.001
Отключение или модификация средств защиты

Получение учетных данных

EPP/EDR T1003
Доступ к учетным данным ОС

EPP/EDR IDS T1110
Атака грубой силы

EPP/EDR IDS T1110.001
Подбор пароля

Обнаружение

EPP/EDR T1033
Обнаружение владельца/пользователя системы

EPP/EDR T1007
Обнаружение системных служб

EPP/EDR T1016
Раскрытие параметров конфигурации сети

Горизонтальное перемещение

EPP/EDR IDS T1210
Использование уязвимостей удаленных служб

EPP/EDR IDS T1021
Использование служб удаленного доступа

EPP/EDR T1021.006
Использование WinRM

Сбор данных

EPP/EDR T1119
Автоматизированный сбор данных

EPP/EDR T1560.001
Архивирование с помощью утилит

EPP/EDR T1005
Сбор данных о локальной системе

Разведка

EPP/EDR IDS T1595.002
Сканирование уязвимостей

EPP/EDR T1592
Сбор информации о хосте жертвы

EPP/EDR T1590.005
Сбор данных об IP-адресах

Управление и контроль

EPP/EDR SB IDS T1071.001
Коммуникации с помощью Web протоколов

EPP/EDR IDS T1095
Использование протоколов не прикладного уровня

EPP/EDR IDS T1071.004
Коммуникации с помощью DNS

Ущерб

EPP/EDR IDS T1496
Захват ресурсов

EPP/EDR IDS T1486
Шифрование данных как цель атаки

EPP/EDR T1485
Уничтожение данных

Подготовка к атаке

EPP/EDR SB T1587.001
Создание вредоносных программ

EPP/EDR IDS T1588.002
Получение инструментов

Эксфильтрация

IDS T1048
Выгрузка данных через альтернативный протокол

EPP/EDR T1020.001
Дублирование трафика

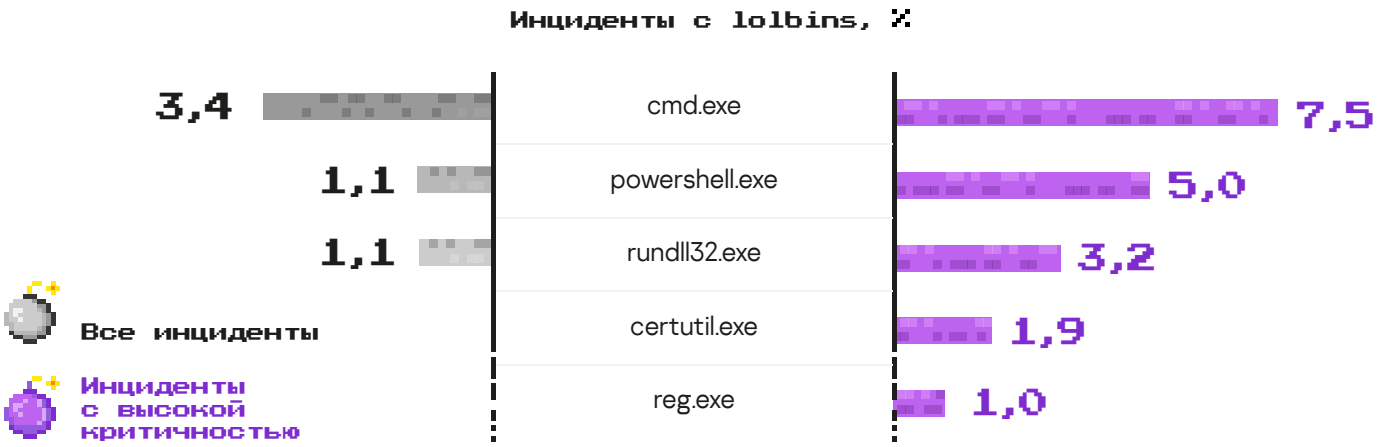
Высокая эффективность песочницы и сетевых СОВ на этапе Первоначального доступа обусловлена распространенным сценарием использования KATA для обнаружения фишинговых атак. Также сетевая СОВ эффективна на этапе Горизонтальных перемещений, а на этапе Управление и контроль она просто незаменима.

На этапах Выполнения, Закрепления, Повышения привилегий, Обхода защиты, Получения учетных данных и Ущерба сенсор конечной точки является основным. Интересно отметить, что тактика Горизонтальных перемещений им также хорошо покрывается.

Техники злоумышленников

Инструменты, применяемые в атаках

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



Самые популярные LOL-утилиты[1], которые наблюдались практически в любом инциденте, это cmd.exe и powershell.exe. rundll32.exe также довольно популярен в инцидентах всех уровней критичности.

Критичные инциденты отличаются большим разнообразием используемых инструментов LOL. В дополнение к вышеупомянутым LOL-утилитам в критичных инцидентах часто встречались reg.exe, te.exe и certutil.exe.

Классификация инцидентов по MITRE ATT&CK

Наша логика обнаружения поддерживает классификацию MITRE ATT&CK. Для каждого правила обнаружения мы рассчитываем конверсию и вклад, поэтому мы можем поделиться ими и для техник MITRE ATT&CK. Ниже перечислены восемь техник, показавших наибольшую конверсию, а следующая тепловая карта демонстрирует вклад обнаруженных нами техник в 2021 [2].

80,0%
T1003: Доступ к учетным данным ОС
Доступ к памяти LSASS, секретам LSA и атака DCSync наблюдались практически в каждом случае взлома домена Windows на этапе Получения учетных данных

55,8%
T1569: Вмешательство в системные службы
Системные службы очень популярны для запуска вредоносного контента

52,4%
T1021: Использование удаленных служб
Различные типы внешних сервисов, таких как RDP, сетевые административные папки Windows, DCOM или SSH, широко использовались на этапе Горизонтальных перемещений

50,6%
T1110: Атака грубой силы
Еще одна популярная техника доступа к учетным данным, демонстрирующая низкий уровень ложных срабатываний

47,3%
T1558: Кража или подделка билетов Kerberos
Эта техника и ее подтехники наблюдались при каждом взломе инфраструктуры Active Directory

38,2%
T1078: Использование действительных учетных записей
Доменные и локальные учетные записи использовались злоумышленниками для обхода защиты и последующего закрепления в системе

38,1%
T1190: Использование уязвимостей публично доступных приложений
В 2021 году мы сталкивались с несколькими критическими уязвимостями, что привело к результативности этой техники

34,9%
T1049: Обнаружение сетевых подключений системы
Техники рекогносцировки всегда наблюдаются в инцидентах, вызванных действиями человека, но обычно демонстрируют самый высокий уровень ложных срабатываний. Однако в 2021 эта техника была исключением

[1] https://lolbas-project.github.io/
[2] 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

<0,5% <5% <10% <20%

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1590.005: IP Addresses	T1583.005: Botnet	T1078: Valid Accounts	T1047: Windows Management Instrumentation	T1037: Boot or Logon Initialization Scripts	T1055: Process Injection	T1014: Rootkit
T1592: Gather Victim Host Information	T1583.006: Web Services	T1091: Replication Through Removable Media	T1053.005: Scheduled Task	T1098: Account Manipulation	T1068: Exploitation for Privilege Escalation	T1027: Obfuscated Files or Information
T1595: Active Scanning	T1587.001: Malware	T1133: External Remote Services	T1053: Scheduled Task/Job	T1136: Create Account	T1134: Access Token Manipulation	T1036: Masquerading
T1598.003: Spearphishing Link	T1588.001: Malware	T1189: Drive-by Compromise	T1059: Command and Scripting Interpreter	T1137: Office Application Startup	T1548.002: Bypass User Account Control	T1070: Indicator Removal on Host
	T1588.002: Tool	T1190: Exploit Public-Facing Application	T1064: Scripting	T1176: Browser Extensions		T1112: Modify Registry
	T1588.003: Code Signing Certificates	T1195: Supply Chain Compromise	T1106: Native API	T1197: BITS Jobs		T1127.001: MSBuild
	T1588.005: Exploits	T1566.001: Spearphishing Attachment	T1129: Shared Modules	T1205.001: Port Knocking		T1140: Deobfuscate/ Decode Files or Information
	T1588.006: Vulnerabilities	T1566.002: Spearphishing Link	T1203: Exploitation for Client Execution	T1505.003: Web Shell		T1202: Indirect Command Execution
	T1608.002: Upload Tool		T1204: User Execution	T1542: Pre-OS Boot		T1207: Rogue Domain Controller
			T1569: System Services	T1543: Create or Modify System Process		T1211: Exploitation for Defense Evasion
				T1546.002: Screensaver		T1218: Signed Binary Proxy Execution
				T1546.003: Windows Management Instrumentation Event Subscription		T1220: XSL Script Processing
				T1546.007: Netsh Helper DLL		T1222.001: Windows File and Directory Permissions Modification
				T1546.008: Accessibility Features		T1497: Virtualization/ Sandbox Evasion
				T1546.010: AppInit DLLs		T1550.002: Pass the Hash
				T1546.012: Image File Execution Options Injection		T1550.003: Pass the Ticket
				T1546.015: Component Object Model Hijacking		T1553.002: Code Signing
				T1547: Boot or Logon Autostart Execution		T1553.004: Install Root Certificate
				T1554: Compromise Client Software Binary		T1562.001: Disable or Modify Tools
				T1556.002: Password Filter DLL		T1564.001: Hidden Files and Directories
				T1574.002: DLL Side-Loading		T1564.002: Hidden Users
						T1564.004: NTFS File Attributes

<0,5% <5% <10% <20%

TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1003: OS Credential Dumping	T1007: System Service Discovery	T1021: Remote Services	T1005: Data from Local System	T1001: Data Obfuscation	T1020.001: Traffic Duplication	T1485: Data Destruction
T1040: Network Sniffing	T1012: Query Registry	T1210: Exploitation of Remote Services	T1113: Screen Capture	T1071: Application Layer Protocol	T1048: Exfiltration Over Alternative Protocol	T1486: Data Encrypted for Impact
T1056: Input Capture	T1016: System Network Configuration Discovery	T1570: Lateral Tool Transfer	T1119: Automated Collection	T1090: Proxy	T1052: Exfiltration Over Physical Medium	T1496: Resource Hijacking
T1110: Brute Force	T1018: Remote System Discovery		T1560.001: Archive via Utility	T1095: Non-Application Layer Protocol		T1561.001: Disk Content Wipe
T1212: Exploitation for Credential Access	T1033: System Owner/User Discovery			T1102: Web Service		T1561.002: Disk Structure Wipe
T1555: Credentials from Password Stores	T1046: Network Service Scannin			T1104: Multi-Stage Channels		T1565: Data Manipulation
T1558: Steal or Forge Kerberos Tickets	T1049: System Network Connections Discovery			T1105: Ingress Tool Transfer		
	T1069: Permission Groups Discovery			T1219: Remote Access Software		
	T1082: System Information Discovery			T1568.002: Domain Generation Algorithms		
	T1083: File and Directory Discovery			T1571: Non-Standard Port		
	T1087: Account Discovery			T1572: Protocol Tunneling		
	T1124: System Time Discovery					
	T1135: Network Share Discovery					
	T1482: Domain Trust Discovery					
	T1518.001: Security Software Discovery					