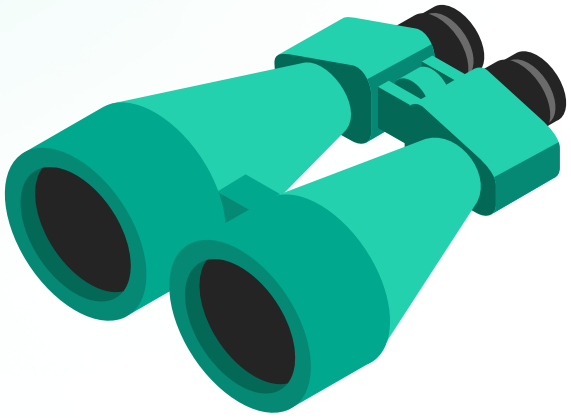
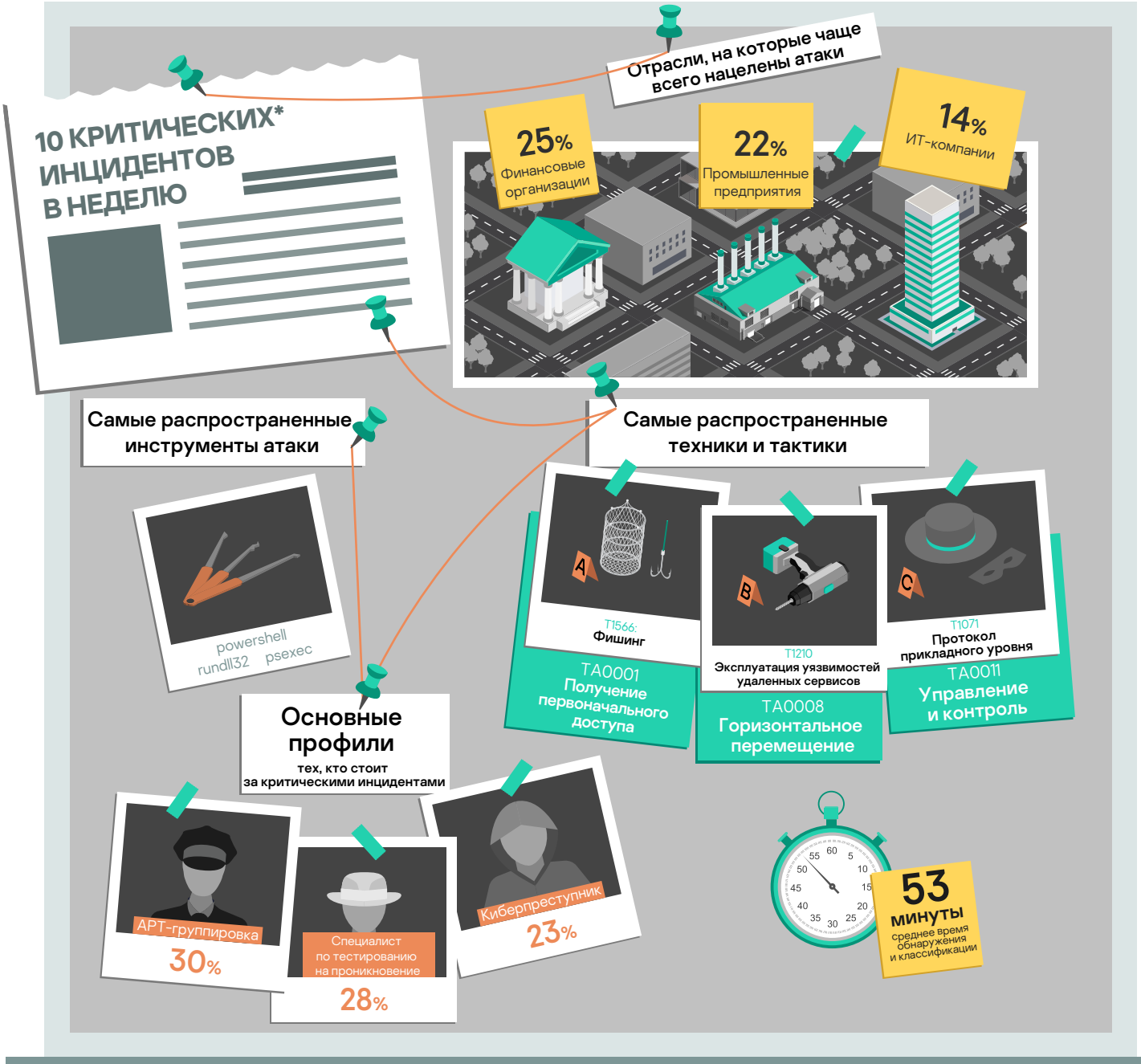
Managed Detection and Response: Аналитический отчёт

Q4 2020



kaspersky

Основные выводы



* Критические – наиболее опасные инциденты, связанные с активной работой злоумышленников в скомпрометированной инфраструктуре, которые составляют 9% от общего числа обнаруженных атак

Рекомендации

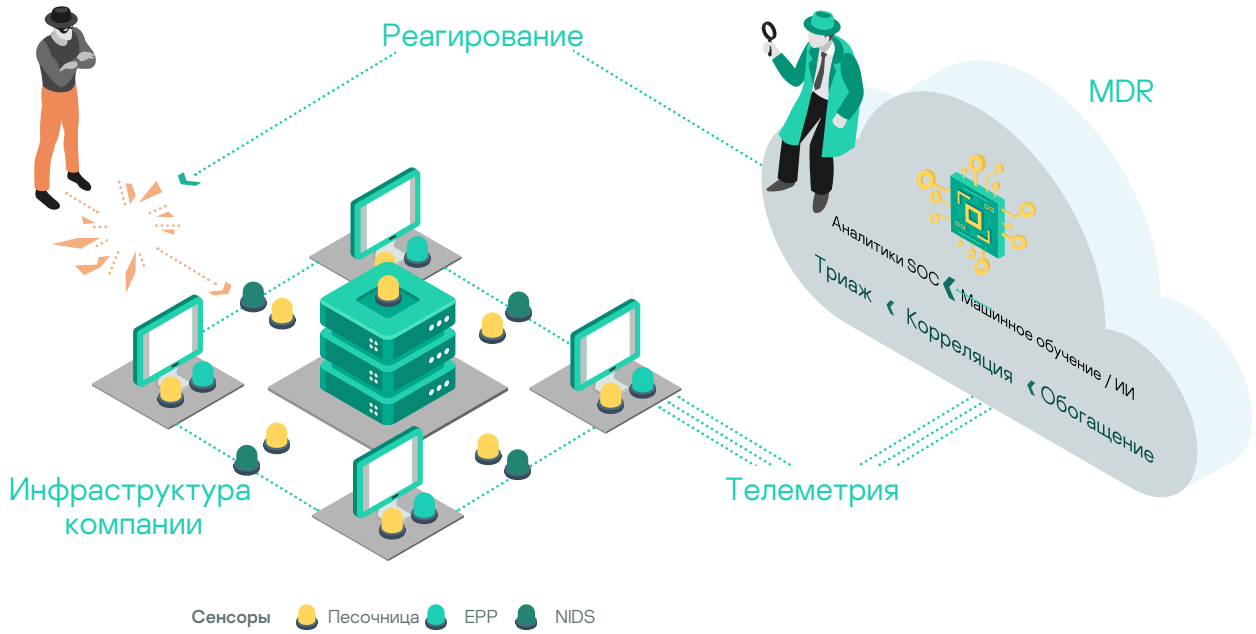
- Треть выявленных критичных инцидентов составляют целевые атаки, реализованные с непосредственным участием атакующих. Для эффективного обнаружения подобных атак недостаточно исключительно автоматических инструментов – необходима комбинация классического мониторинга и активного поиска угроз (threat hunting)[1].
- Продвинутые атаки достаточно точно моделируются во время киберучений с участием red team[2] – это отличный способ оценки операционной эффективности организации.
- Девять процентов серьезных инцидентов связаны с использованием методов социальной инженерии, что в очередной раз демонстрирует необходимость повышения осведомленности сотрудников о киберугрозах[3].
- Необходимо иметь возможность обнаружения всех тактик MITRE ATT&CK (этапов цепочки атаки). Даже комплексные атаки включают в себя простые техники. Возможность распознавать эти техники позволит обнаруживать атаки целиком.
- Разные средства защиты демонстрируют разную эффективность при обнаружении разных техник. Использование различных систем безопасности значительно повышает вероятность обнаружения сложных атак[4].

[1] www.kaspersky.ru/enterprise-security/managed-detection-and-response
[2] www.kaspersky.ru/enterprise-security/security-assessment
[3] www.kaspersky.ru/enterprise-security/security-awareness
[4] www.kaspersky.ru/enterprise-security/wiki-section/products/multi-layered-approach-to-security

Введение

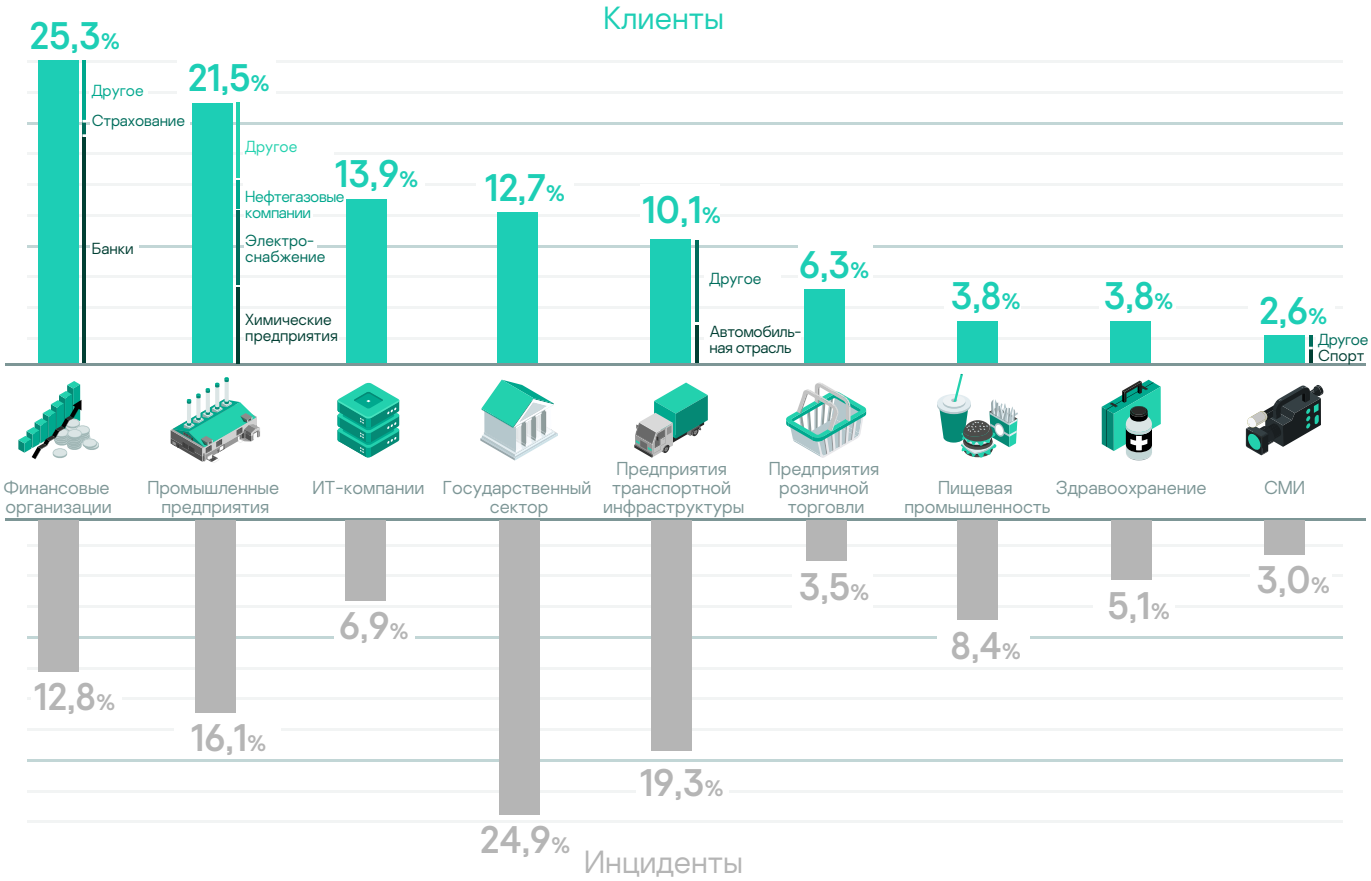
Кибератаки становятся все более изощренными, и защитным решениям требуются дополнительные ресурсы для анализа огромного объема данных, которые поступают ежедневно. Поэтому компаниям необходимы технологии, которые будут непрерывно обнаруживать и обезвреживать усложняющиеся угрозы.

Согласно данным компании Gartner (2020 MDR Service Market Guide), к 2025 году 50% организаций будут пользоваться MDR-сервисами не только для мониторинга, обнаружения угроз и реагирования на них, но и для сдерживания угроз.



Где используется MDR: отрасли и вертикали

На диаграмме представлены распределения по отраслям количества клиентов сервиса Kaspersky MDR и количества выявленных инцидентов. В этом отчете представлены данные за IV квартал 2020 года[1].



[1]В этом отчете использовались анонимизированные метаданные, предоставленные клиентами начиная с IV квартала 2020 г., когда сервис появился на указанных рынках. Сервис был запущен в глобальном масштабе в I квартале 2021 г.

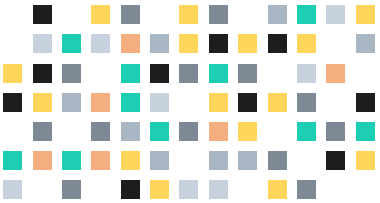
Режим использования MDR

Сервис Kaspersky MDR получает огромное количество телеметрии от сенсоров и обрабатывает их, в результате чего формируются события безопасности (алерты), которые далее обрабатываются сотрудниками Центра мониторинга. Это позволяет специалистам по активному поиску угроз быстрее реагировать на атаки, а также использовать информацию об инцидентах при работе с другими защитными инструментами.

~15 тысяч событий телеметрии с одного хоста ежедневно

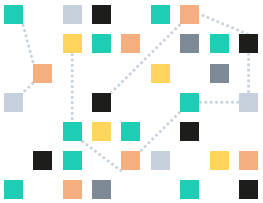
Этот показатель может существенно меняться в зависимости от активности хоста

Из них
65 тыс. событий безопасности от всех сенсоров
были обработаны
за 3 месяца



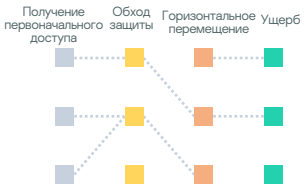
- 22 тысячи событий безопасности были обработаны в автоматическом режиме с помощью технологий машинного обучения и ИИ
- 43 тысячи были проанализированы аналитиками Центра мониторинга (SOC) «Лаборатории Касперского»

1506 переданных заказчикам инцидентов



- Количество событий безопасности по зарегистрированным инцидентам: 2566
- Количество зарегистрированных инцидентов составляет 5,9% от числа оповещений, то есть 94,1% срабатываний оказались ложноположительными

92,9%
обогащены данными из базы MITRE ATT&CK



- 1400 инцидентов можно сопоставить с базой MITRE ATT&CK
- Остальные включают инциденты, связанные с проблемами покрытия сервисом инфраструктуры заказчика или низким уровнем критичности, поэтому в сопоставлении таких инцидентов с базой MITRE ATT&CK нет практической необходимости

Эффективность устранения инцидентов

Сколько событий безопасности потребовалось для решения инцидента?

1 событие безопасности

80,1% инцидентов

Показатель демонстрирует общую эффективность обнаружения и разрешения инцидентов.

2–4 события безопасности

15,3% инцидентов

Этот показатель позволяет выявить области, в которых необходимо улучшить процессы управления инцидентами. При каждом новом инциденте создается новый алгоритм, который позволяет обнаружить этот инцидент уже после первого события безопасности.

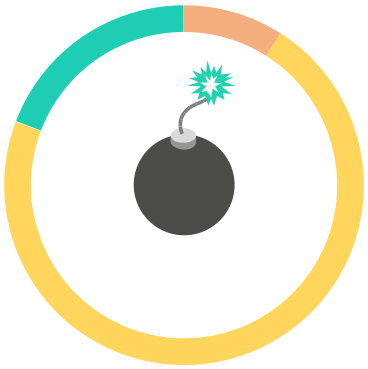
5 и более событий безопасности

4,6% инцидентов

Большое число срабатываний происходит в тех случаях, когда быстрое устранение угрозы недопустимо или неэффективно:

- Новые целевые атаки и APT-угрозы
- Мониторинг атак по запросу клиента без реагирования
- Анализ защищенности без реагирования (например, тестирование на проникновение)

Критичность инцидентов



9% **высокий уровень**

Влекут за собой несанкционированный доступ к ресурсам клиента, находящимся под защитой MDR, или к серьезным сбоям в их работе.

Выявляются признаки целевой атаки или неизвестной угрозы, требующие дальнейшего расследования при помощи методов цифровой криминалистики.

72% **средний уровень**

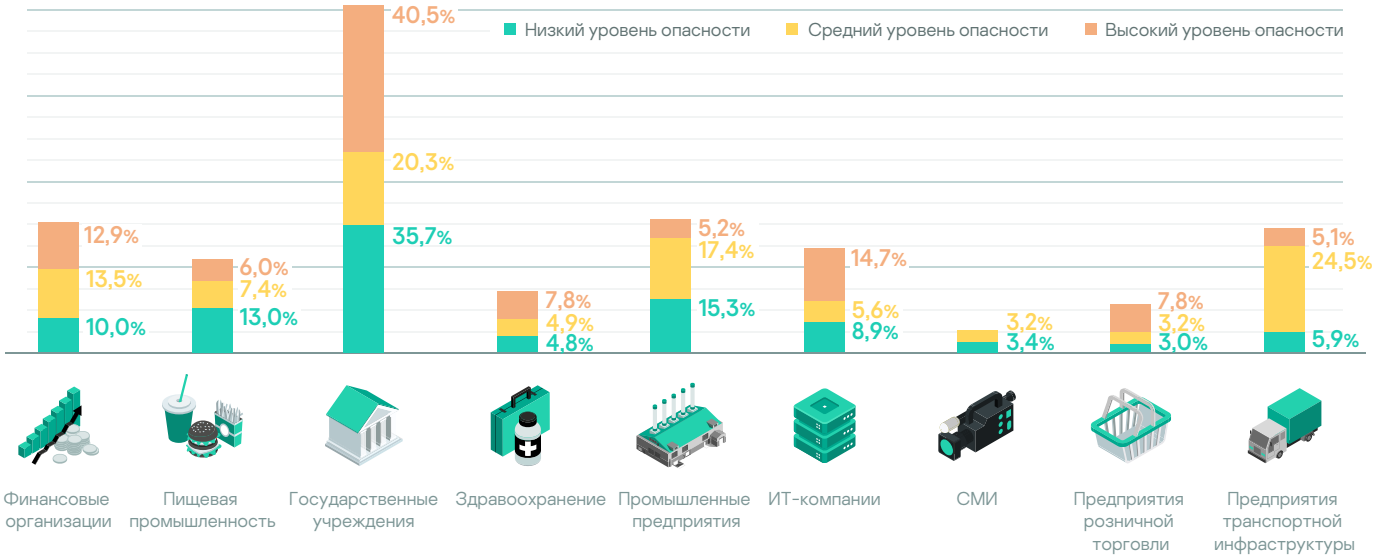
Могут сказаться на эффективности или производительности ресурсов клиента, находящихся под защитой MDR, и в некоторых случаях привести к повреждению данных.

19% **низкий уровень**

Не оказывают существенного влияния на эффективность или производительность ресурсов клиента, находящихся под защитой MDR, и, как правило, не приводят к повреждению данных.

Выявление потенциально нежелательного ПО – adware, riskware, not-a-virus и т. д.

Каждый день мы обнаруживаем 1-2 инцидента с высоким уровнем критичности. В IV квартале 2020 года избежать таких инцидентов удалось только сектору СМИ. С самыми серьезными атаками столкнулись государственные учреждения, финансовые организации и ИТ-компании.



Сколько времени требуется на обнаружение инцидента?

Событие безопасности появляется в очереди, ожидая сортировки аналитиком в ручном режиме (около 33% оповещений обрабатываются за считаные секунды с использованием технологий ИИ и машинного обучения и в очереди не появляются).

События безопасности, являющиеся следствием реальной атаки, регистрируются как инциденты. Для каждого инцидента аналитиком формируется карточка инцидента, которая передается клиенту через Портал MDR. Ниже представлены сроки полной обработки событий безопасности (включая время ожидания в очереди) до момента передачи заказчикам карточки инцидента.

52,6 мин. **высокий уровень критичности**

Наиболее значимые инциденты, требующие дополнительного сбора данных и дополнительного времени на расследование

21,1 мин. **средний уровень критичности**

Инциденты этого уровня критичности происходят чаще остальных. Кратчайшие сроки обнаружения свидетельствуют об эффективности шаблонизации карточек наиболее распространенных инцидентов

30,2 мин. **низкий уровень критичности**

Низкий приоритет инцидентов означает, что большую часть указанного времени они находятся в очереди на обработку аналитиком

Природа инцидентов с высоким уровнем опасности

Каковы источники инцидентов с высоким уровнем опасности?

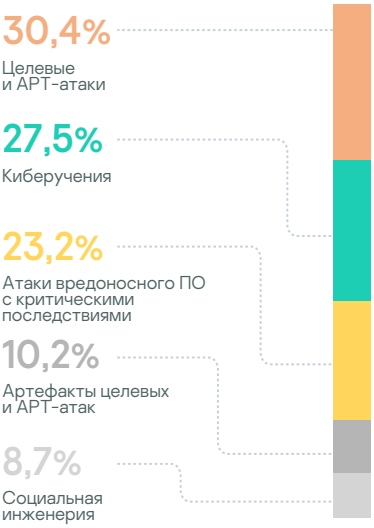
Треть серьезных инцидентов (30,4%) приходится на долю целевых и APT-атак

Каждый 4-й инцидент с высоким уровнем критичности – следствие киберучений (тестирование на проникновение, учения с участием red team, эмуляция действий злоумышленников и т. д.)

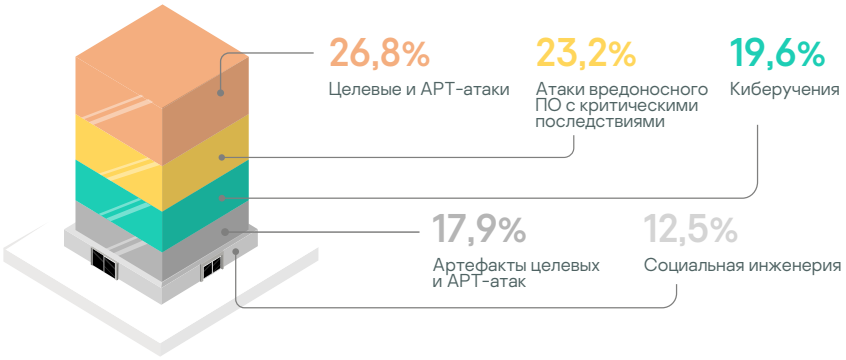
Каждая 5-я атака использовала вредоносное ПО, такое как программы-вымогатели; они причинили компаниям серьезный ущерб, но осуществлялись без участия человека

10% инцидентов остались неклассифицированными и имели явные признаки ранее совершенных атак, в том числе в ходе киберучений (например, дамп процесса Lsass, файлы kirbi, признаки успешного закрепления в ОС и т. д.). Чаще всего такие инциденты обнаруживались у новых клиентов, либо на хостах, для которых ранее не был активирован мониторинг

В 9% случаев злоумышленники получили первоначальный доступ с помощью методов социальной инженерии, но атаки были предотвращены и, следовательно, не были классифицированы



Сколько организаций пострадало от серьезных инцидентов?



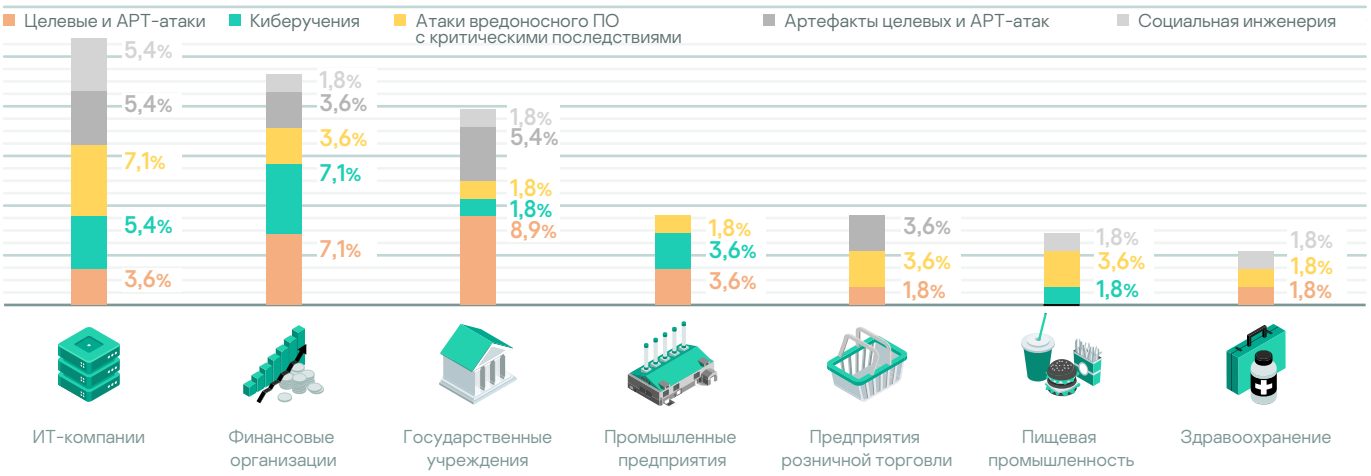
27% организаций стали жертвами целевых или APT-атак

23% стали жертвами серьезных атак с использованием вредоносного ПО (например программ-вымогателей)

20% наших клиентов проводили киберучения в той или иной форме

Количество организаций (по отраслям), которые столкнулись с инцидентами высокого уровня критичности

За три месяца исследования почти во всех отраслях наблюдались различные типы инцидентов высокого уровня критичности.



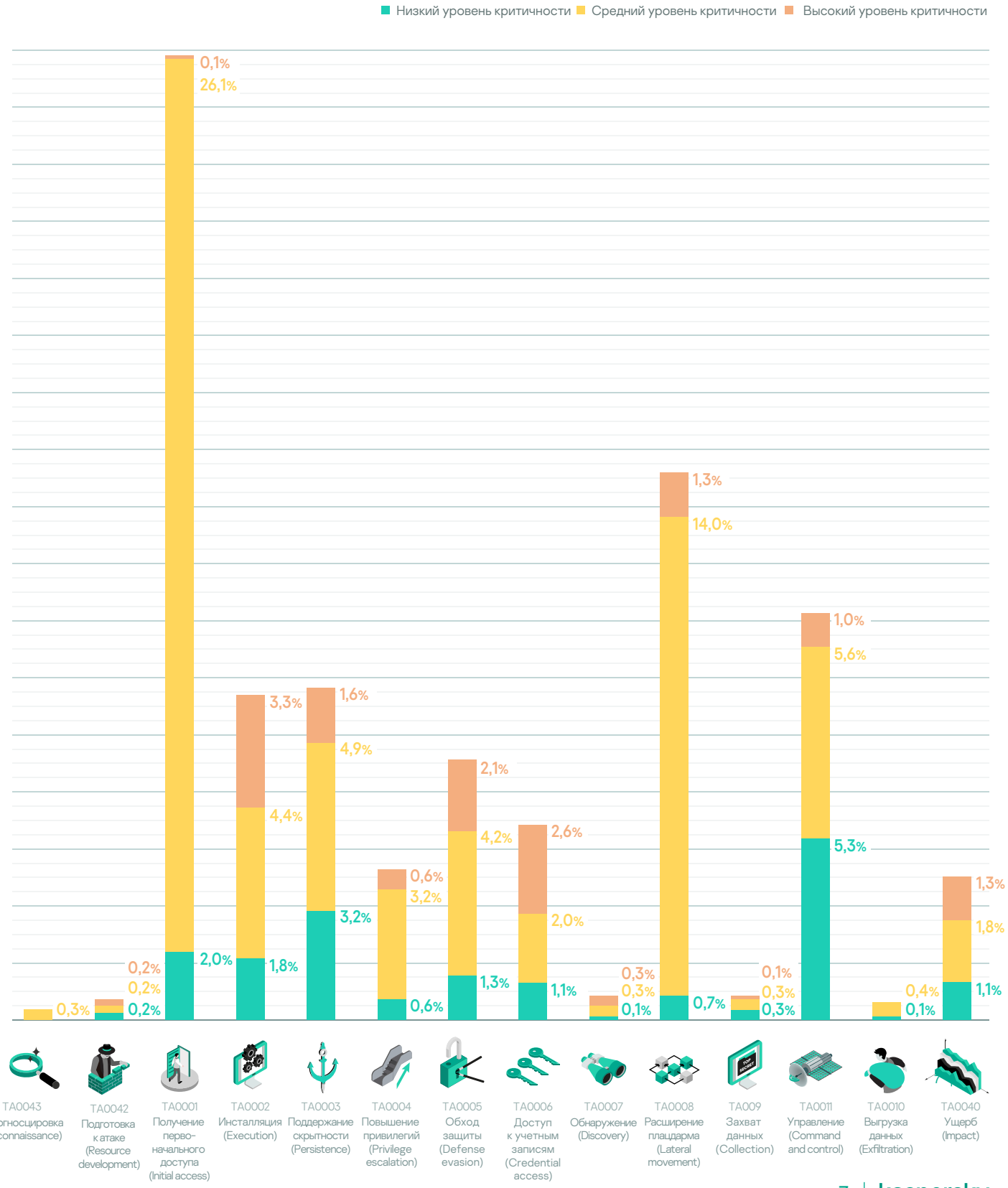
При расследовании активных целевых атак часто обнаруживаются артефакты предыдущих успешных APT-атак. Это говорит о том, что после того как организация восстановит ресурсы, она наверняка будет атакована снова и, вероятно, теми же лицами.

В отраслях, являющихся частой жертвой целевых атак, как правило, проводятся и киберучения, что демонстрирует корректно работающий процесс оценки рисков безопасности.

Технологии обнаружения атак. Тактики, техники и процедуры, используемые злоумышленниками

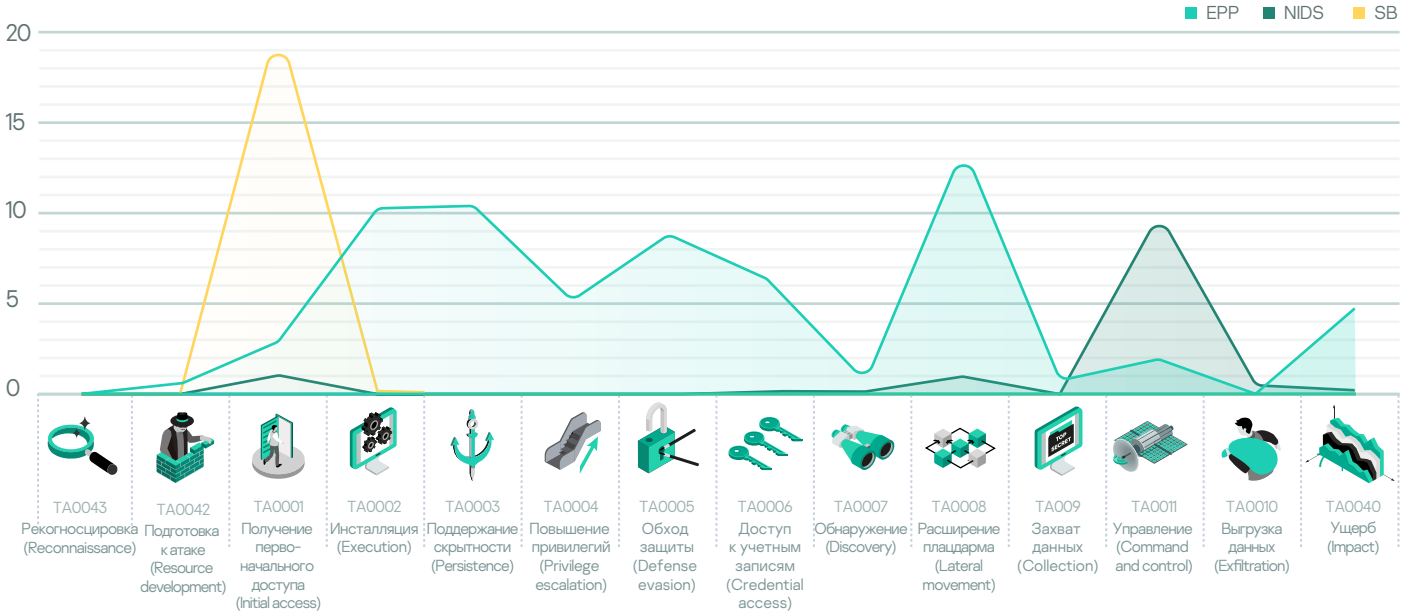
Тактики злоумышленников

Большинство инцидентов было обнаружено на этапе первоначального доступа. Кроме того, злоумышленники достаточно часто обнаруживались на этапах: Инсталляция (Execution), Поддержание скрытности (Persistence), Обход защиты (Defense evasion), Доступ к учетным записям (Credential Access), Расширение плацдарма (Lateral movement), Управление (Command and Control). На этапе выгрузки данных (Exfiltration) и захвата данных (Collection) было обнаружено меньше инцидентов, что подтверждает эффективность мероприятий по обнаружению и реагированию. Все инциденты, обнаруженные на более поздних этапах, подвергаются тщательному анализу с целью последующей доработки детектирующей логики, чтобы обнаруживать как можно больше угроз на ранних этапах.



Тактики и технологии обнаружения

Kaspersky MDR получает телеметрические данные от различных сенсоров (технологий обнаружения): платформ для защиты рабочих мест (EPP), песочницы (SB) и сетевой системы обнаружения вторжений (NIDS). Сетевая система обнаружения вторжений и песочница – это компоненты Kaspersky Anti Targeted Attack (KATA)[1]. NIDS на уровне хоста – часть Kaspersky Security для бизнеса, комплексного решения для защиты рабочих мест[2]. На диаграмме показаны тактики, используемые злоумышленниками в момент обнаружения инцидента.



Далее приведены наиболее часто встречавшиеся в переданной клиентам информации об инцидентах техники MITRE ATT&CK с указанием, какая технология обнаружения позволила их выявить.

Получение первоначального доступа (Initial access)

- EPP, Песочница — T1566.001 Целевой фишинг через вложения
- Песочница, NIDS — T1566.002 Целевой фишинг через ссылки
- NIDS — T1190 Эксплуатация уязвимости общедоступного приложения
- NIDS — T1133 Внешние службы удаленного доступа

Инсталляция (Execution)

- EPP, Песочница — T1053 Плановые задачи
- EPP, Песочница — T1204 Запуск пользователем
- EPP — T1059.001 PowerShell
- EPP — T1059 Интерпретатор команд и сценариев
- Песочница — T1204.001 Вредоносные ссылки

Поддержание скрытности (Persistence)

- EPP, SB — T1053 Плановые задачи
- EPP — T1547.001 Записи в разделе автозапуска реестра / папка автозагрузки
- EPP — T1546.008 Функции доступа
- NIDS — T1133 Внешние службы удаленного доступа

Повышение привилегий (Privilege escalation)

- EPP, SB — T1053 Плановые задачи
- EPP — T1547.001 Записи в разделе автозапуска реестра / папка автозагрузки
- EPP — T1546.008 Специальные возможности операционной системы
- EPP — T1055 Инъекция кода в процессы

Обход защиты (Defense evasion)

- EPP — T1036 Маскировка
- EPP — T1055 Инъекция кода в процессы

Доступ к учетным записям (Credential access)

- EPP — T1003 Создание дампа учетных данных ОС

Обнаружение (Discovery)

- NIDS — T1083 Поиск файлов и директорий

Расширение плацдарма (Lateral movement)

- EPP, NIDS — T1210 Эксплуатация уязвимостей удаленных сервисов
- EPP — T1021 Удаленные сервисы

Управление (Command and control)

- NIDS — T1071 Протокол прикладного уровня
- NIDS — T1095 Не протокол прикладного уровня
- NIDS — T1102 Веб-сервис

Выгрузка данных (Exfiltration)

- NIDS — T1048 Эксфильтрация через альтернативный протокол

Ущерб (Impact)

- EPP — T1496 Захват ресурсов

EPP

- Защищает от большинства атак, независимо от тактики их проведения
- Обнаруживает большинство атак на самых активных стадиях: между первоначальным доступом и компрометацией ресурсов, приводящей к ущербу

Песочница

- Ускоряет расследование событий безопасности и предоставляет аналитикам дополнительный контекст
- Полезное дополнение для покрытия тактик первоначального доступа

NIDS

- Обнаружение атак, которые еще не привели к ущербу
- Полезное дополнение для отражения тактик получения первоначального доступа

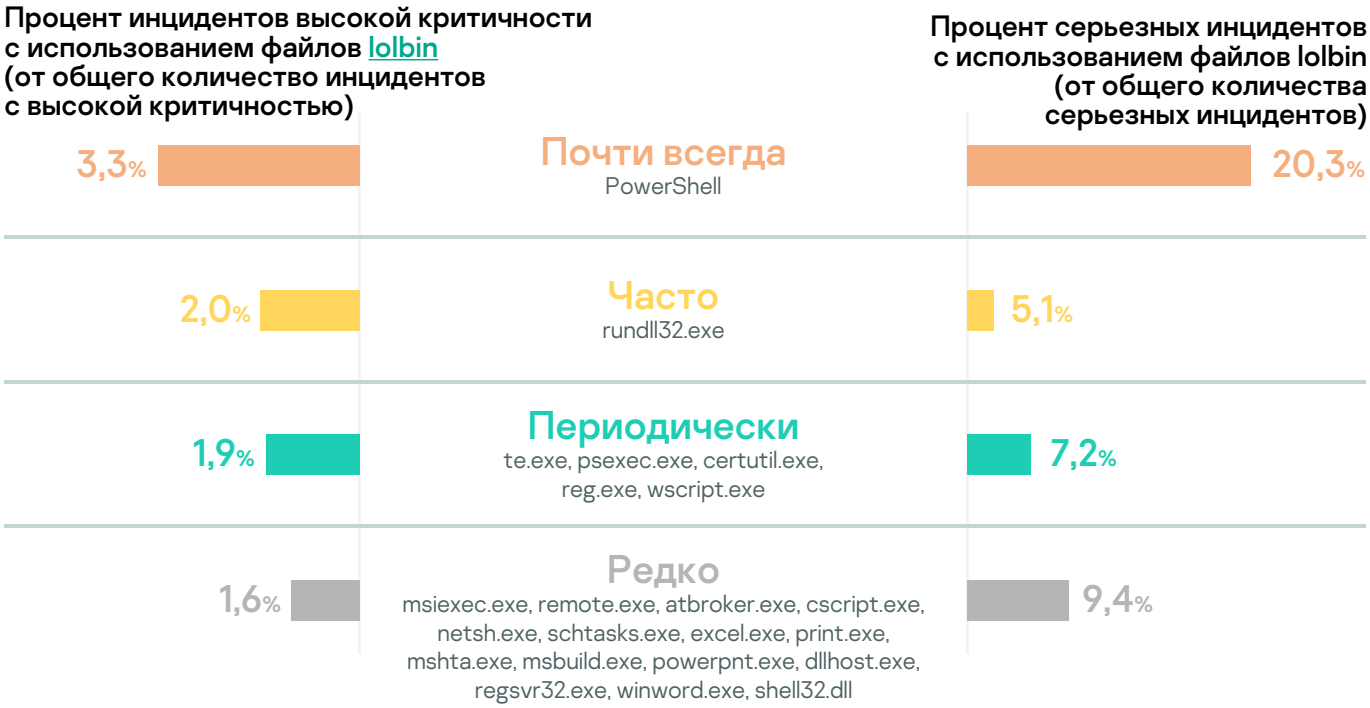
[1] KATA – www.kaspersky.ru/enterprise-security/anti-targeted-attack-platform
[2] KESB – www.kaspersky.ru/enterprise-security/endpoint

Техники злоумышленников

Инструменты, используемые в атаках

Злоумышленники используют интегрированные в ОС средства, чтобы оставить как можно меньше следов в системе, снизить стоимость разработки инструментов для атаки и, самое главное, замаскировать свои действия под работу легитимных программ, усложнив обнаружение.

Сведения о легитимных инструментах, которые используются для атаки, доступны на сайте проекта LOLBin. Несмотря на то что компания Microsoft существенно повысила защиту и улучшила контроль PowerShell, эта оболочка остается самым популярным инструментом злоумышленников.



Сопоставление инцидентов с базой знаний MITRE ATT&CK

При оценке эффективности детектирующей логики, основанной на техниках MITRE ATT&CK, подсчитывается процент всех зарегистрированных инцидентов, выявленных с помощью правил, которые базируются на той или иной технике MITRE ATT&CK.

33%

T1566: Фишинг для доступа к целевой системе (Phishing)

Этот показатель демонстрирует и эффективность сервиса MDR, позволяющего обнаружить эту технику на этапе получения первоначального доступа, и ее популярность среди злоумышленников

16,5%

T1210: Использование уязвимостей удаленных служб (Exploitation of Remote Services)

Связана с попытками удаленной эксплуатации служб (например, частым использованием эксплойта EternalBlue и т. п.)

10,6%

T1071: Коммуникации с помощью протоколов прикладного уровня (Application Layer Protocol)

Коммуникации с помощью протоколов прикладного уровня часто используют для связи с инфраструктурой командных центров. Для сравнения техника T1095 встречалась только в 3,79% инцидентов

5,3%

T1021: Использование удаленных сервисов (Remote Services)

Широко используется атакующими для горизонтальных перемещений (например, T1021.002: Использование общих ресурсов SMB/Windows и T1021.001: Использование Remote Desktop Protocol

4,4%

T1036: Маскировка под легального пользователя или инструмент (Masquerading)

Часто используются бэкдоры на базе специальных возможностей операционной системы Windows, когда утилиты sethc.exe, narrator.exe, magnify.exe, utilman.exe и т. п. заменяют на cmd.exe. По статистике такие инциденты редко бывают высокого уровня критичности. Реже встречаются случаи, когда злоумышленники переименовывают вредоносные файлы по аналогии с системными инструментами или создают плановые задачи, напоминающие легитимные, – такие случаи часто имеют отношение к инцидентам высокого и среднего уровней критичности

3,3%

T1204: Выполнение пользователем определенных действий (User Execution)

В случае успешной реализации методов социальной инженерии пользователь открывает фишинговое вложение или запускает загруженное из интернета ПО

6,6%

T1059: Вмешательство в интерпретатор команд и скриптов для запуска команд, скриптов или исполняемых файлов (Command and Scripting Interpreter)

Чаще всего включает T1059.001: PowerShell и T1059.004: Использование Unix Shell

>0% >5% >10% >20%

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1595: Active Scanning	T1587: Develop Capabilities	T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1098: Account Manipulation	T1548: Abuse Elevation Control Mechanism	T1140: Deobfuscate/ Decode Files or Information
	T1588: Obtain Capabilities	T1133: External Remote Services	T1203: Exploitation for Client Execution	T1547: Boot or Logon Autostart Execution	T1134: Access Token Manipulation	T1564: Hide Artifacts
		T1566: Phishing	T1559: Inter-Process Communication	T1037: Boot or Logon Initialization Scripts	T1546: Event Triggered Execution	T1562: Impair Defenses
		T1091: Replication Through Removable Media	T1053: Scheduled Task/Job	T1554: Compromise Client Software Binary	T1068: Exploitation for Privilege Escalation	T1070: Indicator Removal on Host
		T1078: Valid Accounts	T1569: System Services	T1136: Create Account	T1574: Hijack Execution Flow	T1036: Masquerading
			T1204: User Execution	T1505: Server Software Component	T1055: Process Injection	T1112: Modify Registry
			T1047: Windows Management Instrumentation			T1027: Obfuscated Files or Information
						T1542: Pre-OS Boot
						T1218: Signed Binary Proxy Execution

TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1110: Brute Force	T1087: Account Discovery	T1210: Exploitation of Remote Services	T1123: Audio Capture	T1071: Application Layer Protocol	T1048: Exfiltration Over Alternative Protocol	T1485: Data Destruction
T1555: Credentials from Password Stores	T1482: Domain Trust Discovery	T1570: Lateral Tool Transfer	T1005: Data from Local System	T1001: Data Obfuscation		T1486: Data Encrypted for Impact
T1556: Modify Authentication Process	T1083: File and Directory Discovery	T1021: Remote Services	T1056: Input Capture	T1105: Ingress Tool Transfer		T1565: Data Manipulation
T1003: OS Credential Dumping	T1046: Network Service Scanning	T1550: Use Alternate Authentication Material		T1095: Non-Application Layer Protocol		T1561: Disk Wipe
T1552: Unsecured Credentials	T1135: Network Share Discovery			T1090: Proxy		T1496: Resource Hijacking
	T1069: Permission Groups Discovery			T1219: Remote Access Software		
	T1012: Query Registry			T1102: Web Service		
	T1018: Remote System Discovery					
	T1033: System Owner/User Discovery					
	T1497: Virtualization/ Sandbox Evasion					