kaspersky

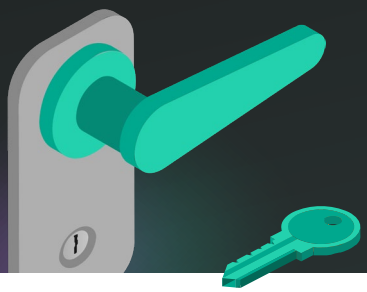
Природа инцидентов информационной безопасности

Основано на данных, полученных командой реагирования «Лаборатории Касперского» в результате расследований компьютерных инцидентов.

2022

Как атакующие получают первоначальный доступ

2019 2020 2021



Эксплуатация уязвимостей в публично доступных приложениях

37,0% 31,5% 53,6%

Скомпрометированные учетные данные

13,0% 31,6% 17,9%

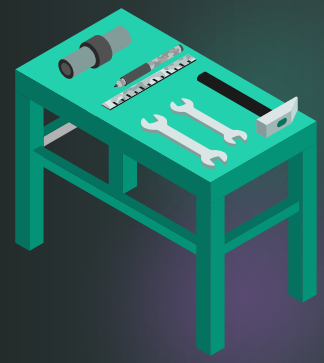
Вредоносные письма

30,0% 23,7% 14,3%

Инструменты атакующих

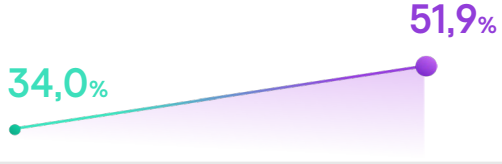
Тренд на использование LOLBins сохраняется. PowerShell остается одним из самых популярных инструментов среди атакующих на стадии Lateral Movement.

PsExec, Mimikatz и Cobalt Strike остаются основными популярными инструментами атакующих в последние годы. В 2021 году использование вышеупомянутых инструментов было отмечено в **10,8%, 9,7%** и **9,7%** всех случаев соответственно.



Масштаб атак

За последние три года шифрование данных было основной проблемой, с которой встречались компании. Число компаний, атакованных шифровальщиками (программами-вымогателями), возросло с 34% в 2019 году до 51,9% в 2021 году.

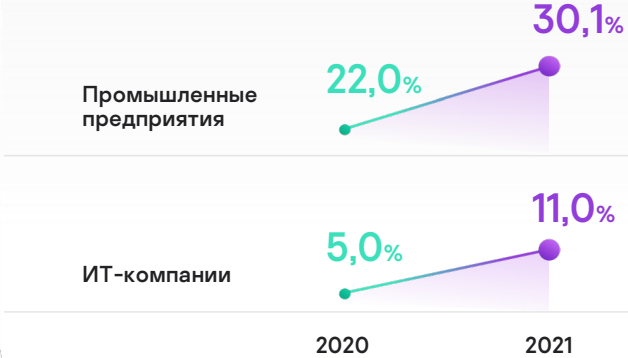


Наиболее атакуемые отрасли

Промышленные предприятия, государственные и финансовые учреждения остаются самыми атакуемыми организациями

- **Промышленные предприятия**
- **Государственные учреждения**
- **Финансовые организации**

В 2021 году мы отмечаем значительный рост инцидентов на промышленных предприятиях и в ИТ-компаниях



Наиболее атакуемые регионы

Бóльшая часть всех запросов на сервис Incident Response была получена в трех регионах

Европа	первое место в 2021 г. (**30,1%**)
Россия и СНГ	первое место в 2020 г.
Ближний Восток	первое место в 2019 г.

Тренды в 2021 году

Программы-вымогатели

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

Начальный вектор атаки	Часы	Недели	Месяцы	Общее количество
Эксплуатация уязвимостей в публично доступных приложениях	12,5%	0,0%	25,0%	37,5%
Вредоносные письма	0,0%	0,0%	25,0%	25,0%
Скомпрометированные учетные данные	12,5%	12,5%	12,5%	37.5%
Общее количество	25,0%	12,5%	62,5%	100%

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 данных пользователей было отмечено в **37,5%** случаев, в то время как вредоносная почта использовалась в каждом четвертом случае.

Однако в ряде атак целью злоумышленников было не вымогательство или шифрование данных, а данные компании - личные данные сотрудников и клиентов, интеллектуальная собственность и другая конфиденциальная информация. Полностью устранить ущерб от такого рода атак практически невозможно. Это может привести к ущербу для репутации компании, а также к потенциальным штрафам со стороны регулирующих органов и судебным искам. Понимая это, злоумышленники получают дополнительный стимул для шантажа. В атаках с шифровальщиками мы наблюдали утечку данных в **10%** случаев.

Кроме того, целью использования шифровальщиков иногда является сокрытие первоначальных следов атаки для усложнения расследования инцидента.

Анализируя продолжительность атак с использованием шифровальщиков, можно сделать вывод, что между начальной компрометацией сети и заключительной стадией атаки проходит значительный промежуток времени. В **62,5%** атак злоумышленники проводят внутри сети более месяца, прежде чем зашифровать данные. Правильно организованный процесс обнаружения инцидентов и реагирования на них сокращает время, необходимое для выявления злоумышленников в сети, и позволяет предотвратить крупный ущерб.

После первоначального проникновения злоумышленники используют PowerShell для сбора данных, Mimikatz для повышения привилегий, PsExec для удаленного выполнения команд, или фреймворки, такие как Cobalt Strike, для всех этапов атаки.

Эксплуатация уязвимостей

Во всех случаях когда в качестве исходного вектора использовалась эксплуатация уязвимостей, основной ущерб был связан с шифрованием данных.

Наиболее распространенной уязвимостью в нашем наборе данных является уязвимость **CVE-2021-26855 Microsoft Exchange SSRF в Microsoft Exchange Server**, которая позволяет злоумышленникам отправлять произвольные HTTP-запросы и проходить аутентификацию на сервере Exchange (использовалась Hafnium group). Она использовалась в 22,7% случаев, когда эксплуатировались уязвимости.

Несмотря на то, что есть простое средство защиты от этого вектора атаки — своевременная установка обновлений безопасности — тем не менее 1-дневные уязвимости намного опережают другие методы первоначального проникновения.

Обзор статистики за 2021 год

Основные выводы и рекомендации экспертов

Основные сведения об атаках

Статистика получена на базе инцидентов, обработанных в рамках сервиса Kaspersky Incident Response в 2021 году

Начальный вектор атаки

1. Внедряйте надежную парольную политику и многофакторную аутентификацию
2. Не используйте общедоступные сервисы удаленного управления в интернете
3. Устанавливайте обновление ПО или используйте компенсационные меры для сервисов на периметре сети
4. Развивайте осведомленность сотрудников в вопросах информационной безопасности

53,6% Эксплуатация уязвимостей в публично доступных приложениях

14,3% Вредоносные письма

17,9% Скомпрометированные учетные данные

5. Используйте правила обнаружения инструментов, используемых атакующими
6. Используйте решения класса EDR
7. Регулярно проводите киберучения с применением распространенных техник и тактик злоумышленников
8. Откажитесь от использования внутренними командами ИТ-инструментов, часто используемых атакующими

Инструменты атакующих

Легитимное ПО было использовано атакующими в 39,7% расследуемых инцидентов

9,7%	9,7%	8,6%	10,8%
Cobalt Strike	Mimikatz	PowerShell	PsExec

Последствия атаки

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

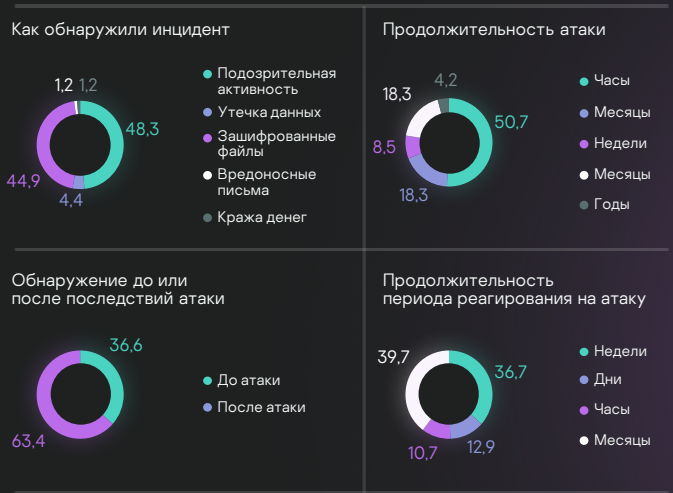
16,0% Утечка данных

51,9% Зашифрованные данные

11,1% Скомпрометированные службы Active Directory

Промышленные предприятия, %

Показатели операционной деятельности, %



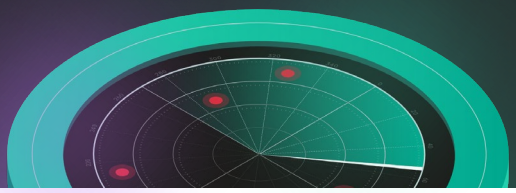
Изучайте профили злоумышленников, атакующих вашу отрасль и регион, с целью приоритизации мер по развитию ИБ

Введение

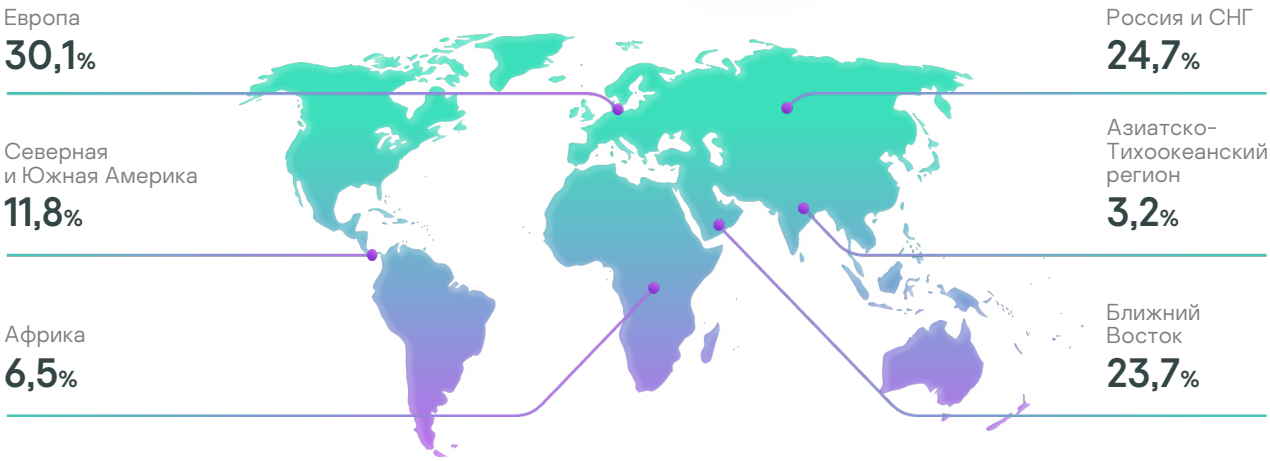
Аналитический отчет содержит информацию об атаках, расследованных «Лабораторией Касперского» в 2021 году. Мы предоставляем широкий спектр сервисов (реагирование на инциденты, цифровая криминалистика, анализ вредоносных программ) для оказания помощи организациям, постарадавшим от индидентов информационной 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[1].

В 2021 году, хотя основные тенденции в области угроз сохранялись, наша команда реагирования почти полностью (98% всех случаев) перешла к удаленному формату работы. Услуги по расследованию и реагированию на инциденты оказывает наше подразделение GERT[2] с экспертами в Европе, Азии, Южной и Северной Америке, на Ближнем Востоке и в Африке.

В 2020 году пандемия COVID-19 вынудила компании реструктурировать свои методы обеспечения информационной безопасности, чтобы приспособиться к удаленной работе.



География сервиса Kaspersky Incident Response



Отрасли, %

1. Аналитика основана на случаях реагирования на инциденты, выполненных "Лабораторией Касперского"
2. https://www.kaspersky.com/enterprise-security/incident-response

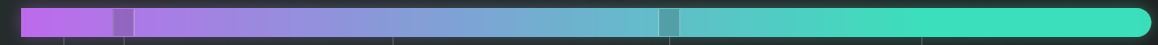
Причины обращений к сервису реагирования на инциденты

Доля инцидентов с программами-вымогателями (ransomware) превышает количество инцидентов с хищением денежных средств или любыми другими последствиями, так как атаки с шифрованием данных имеют простую схему монетизации и распространены во всех отраслях (не только финансовой). Большинство инцидентов с причинами обращений, связанных с подозрительными событиями, можно с уверенностью классифицировать как инциденты с программами-вымогателями.

Причины обращений с инцидентами

12,9% от всех запросов были ложными срабатываниями[3].

Подозрительные активности, обнаруженные сетевыми сенсорами (NIDS, межсетевые экраны) и сенсорами на рабочих станциях (EPP), генерируют основную часть ложных срабатываний. Каждое четвертое обращение с подозрительной активностью от сетевых сенсоров или рабочих станций в дальнейшем было квалифицировано как ложное срабатывание. Ложные обнаружения утечек данных были вызваны утечками в других организациях.



5,1% Утечка данных

1,3% Вредоносное письмо

50,6% Зашифрованные данные

1,3% Хищение финансовых средств

41,7% Подозрительная активность

Ложные обращения

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

18,2% Оповещение средств безопасности

9,1% Подозрительное электронное письмо

9,1% Подозрительный файл

27,3% Подозрительная сетевая активность

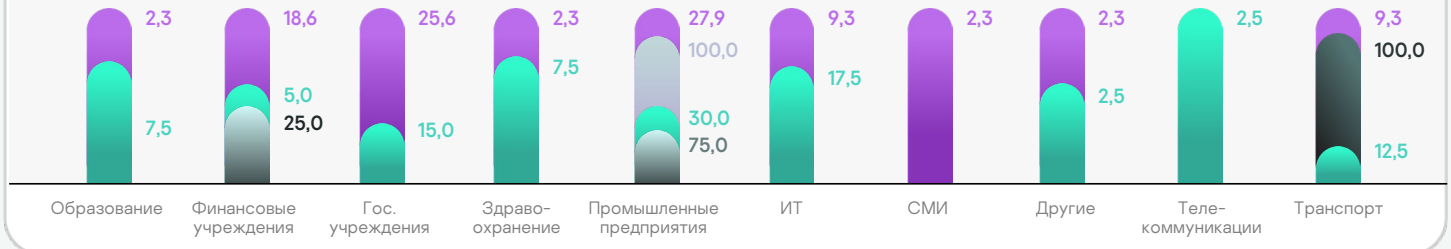
36,3% Подозрительная активность на рабочей станции

Статистика причин обращений по основным регионам

Абсолютно все регионы сталкиваются с атаками программ-вымогателей, также подозрительные активности являются наиболее распространенной причиной для начала расследования.

Статистика причин обращений по основным отраслям

Деньги больше не являются главной целью злоумышленников, даже когда они нацелены на финансовый сектор. Основная цель - данные. Утечка данных - причина половины наших расследований в этом секторе.



Утечка данных · Зашифрованные данные · Вредоносное письмо · Хищение финансовых средств · Подозрительная сетевая активность

3. Подозрительная активность - это категория предупреждений, генерируемых стеком средств безопасности, или сообщения пользователей об аномальном поведении

Начальный вектор атаки

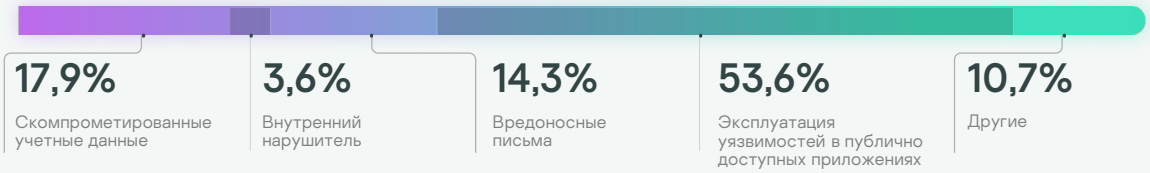
Как атакующие проникают внутрь организации

Из года в год подавляющее большинство первоначальных векторов атаки[4] — это недостаточно защищенные пароли, уязвимости программного обеспечения и социальная инженерия. Настройка и контроль политик паролей, управление обновлениями безопасности, повышение осведомленности сотрудников в вопросах ИБ, а также меры по борьбе с фишингом могут значительно снизить возможности злоумышленников. Когда злоумышленники готовят свою вредоносную кампанию, они в первую очередь рассматривают легко достижимые цели, такие как общедоступные серверы с хорошо известными уязвимостями и известными эксплойтами.

Внедрение политики управления обновлениями само по себе снижает вероятность стать жертвой атаки на 50%.

В 2021 году в MS Exchange были обнаружены несколько уязвимостей. Поскольку MS Exchange имеет широкое распространение в индустрии, использование общедоступных эксплойтов для этих уязвимостей приводит к огромному количеству инцидентов. Ниже в отчете приведены описания встречавшихся в расследованиях уязвимостей.

Причины обращений с инцидентами

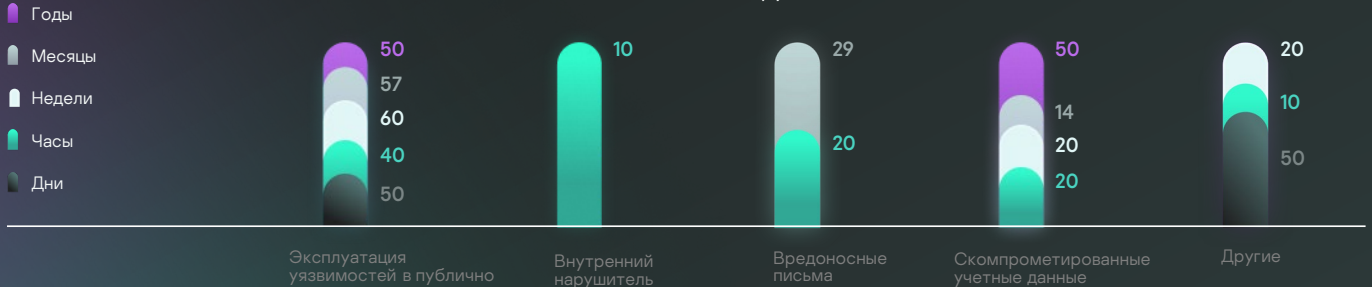


Самые популярные векторы начала атаки и методы их обнаружения

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.

Продолжительность атаки в зависимости от начального вектора

Большинство случаев, в которых не удалось установить начальный вектор атаки, оставались незамеченными более года, прежде чем были обнаружены — на это указывает отсутствие артефактов для анализа (перезапись журналов). Более половины всех атак, которые начинались с вредоносных электронных писем, украденных учетных данных и эксплуатации уязвимостей во внешних приложениях, были обнаружены в течение часов или дней с момента начала атаки.

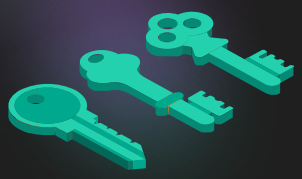


4. Мы определили начальный вектор атаки в 30% случаев. Очень старые инциденты, недоступные журналы, (не) преднамеренное уничтожение доказательств организацией-жертвой и атаки по цепочке поставок являются одними из многочисленных причин невозможности раскрыть, как злоумышленники изначально проникли в сеть.

Инструменты атакующих и эксплойты

40,0%

всех инцидентов использовали различные утилиты



Почти в половине от всех инцидентов было обнаружено использование **существующих средств ОС**[5], таких как PowerShell, известных вредоносных программ с GitHub (например, Mimikatz, AdFind, Masscan), а также специализированных коммерческих фреймворков (Cobalt Strike).

Поскольку их очень трудно обнаружить с помощью традиционных средств контроля безопасности, требуется другой подход. Например, сервис Kaspersky Managed Detection and Response обнаруживает использование такого программного обеспечения.

Используемые инструменты в случае инцидентов

Часто используемые

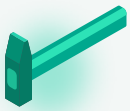
5–8%[6]

Cobalt Strike, Mimikatz, PowerShell, PsExec

Умеренно используемые

3–4%

Advanced IP Scanner, Bitlocker, ProcDump, ProcessHacker



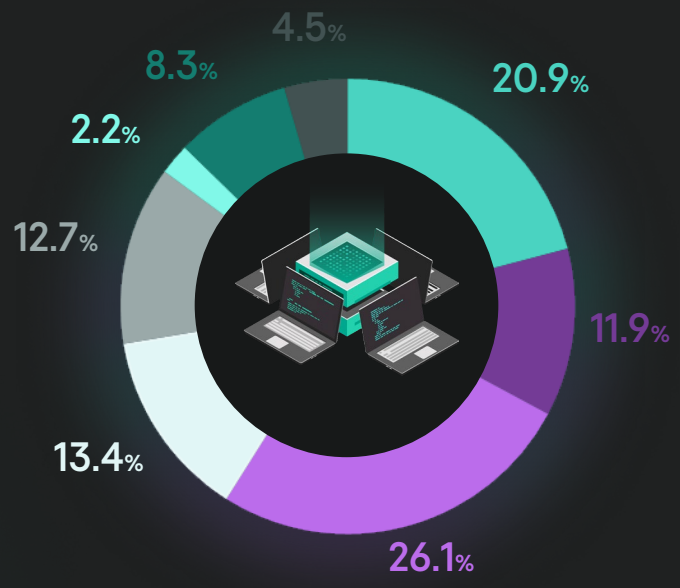
Редко используемые

1–2%

AnyDesk, DiskCryptor, Everything, Fast Reverse Proxy FRP, Meterpreter, reg.exe, RMS, SMBExec WebBrowserPassView.exe

Распределение и частота использования инструментов атакующих при сопоставлении с матрицей MITRE ATT&CK показывают, что злоумышленники чаще всего используют инструменты на этапах между получением первоначального доступа (Initial Access) и ущерба (Impact). Эти инструменты — хорошие индикаторы, которые могут помочь обнаружить атаку быстрее – пока атакующие исследуют сеть.

- **Выполнение**
  PowerShell
  PsExec
  SmbExec
- **Обход защиты**
  ProcessHacker
  PCHunter
  PowerTool
- **Доступ к учетным данным**
  Mimikatz
  PowerTool
  ProcDump
- **Обнаружение**
  Advanced IP Scanner
  nbtscan wmic
- **Сбор данных**
  Everything
  7zip
- **Горизонтальное перемещение**
  Cobalt Strike
  Impacket
  PowerSploit
  Empire_Powershell
- **Управление и контроль**
  RDP
  AnyDesk
  RMS
- **Воздействие**
  DiskCryptor
  BitLocker



5. https://lolbas-project.github.io
6. Использование каждой утилиты было обнаружено в 5-8% инцидентов

Эксплуатация уязвимостей была обнаружена в 14% всех инцидентов

В 2021 году уязвимости были опубликованы в очень популярном ПО, и таким образом это затронуло многие организации. Управление обновлениями остается очень важным инструментом для обеспечения информационной безопасности.

Microsoft Exchange — CVE-2021-34523

Уязвимость с повышением привилегий (EoP).Уязвимость позволяет злоумышленникам повышать свои привилегии.Часть цепочки уязвимостей ProxyShell.

Microsoft Exchange — CVE-2021-34473

Уязвимость удаленного выполнения кода (RCE). Из-за недостатка в службе автоматического обнаружения Exchange Server злоумышленники, не прошедшие аутентификацию, могут получить доступ к его ограниченным ресурсам и использовать это в сочетании с другими уязвимостями для выполнения произвольного кода.Часть цепочки уязвимостей ProxyShell.

Microsoft Exchange — CVE-2021-31207

Security Feature Bypass уязвимость. Уязвимость позволяет злоумышленникам обойти процесс аутентификации. Часть цепочки уязвимостей ProxyShell.

Microsoft Exchange — CVE-2021-27065

Уязвимость для записи произвольных файлов после аутентификации. Злоумышленникам необходимо пройти аутентификацию с использованием других эксплойтов или украденных учетных данных. Уязвимость позволяет злоумышленникам выполнять произвольный код и записывать произвольные файлы. Используется группой Hafnium.

Microsoft Exchange — CVE-2021-26858

Уязвимость для записи произвольных файлов после аутентификации. Злоумышленникам необходимо пройти аутентификацию, используя другие эксплойты или используя украденные учетные данные. Уязвимость позволяет злоумышленникам выполнять произвольный код и записывать произвольные файлы. Используется группой Hafnium.

Microsoft Exchange — CVE-2021-26857

Небезопасная уязвимость десериализации в службе единой системы обмена сообщениями в Microsoft Exchange. Злоумышленникам необходимо пройти аутентификацию с использованием других эксплойтов или украденных учетных данных. Уязвимость позволяет злоумышленникам выполнять произвольный код и записывать произвольные файлы. Используется группой Hafnium.

Microsoft Exchange — CVE-2021-26855

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

Apache Solr — CVE-2019-17558

Уязвимость удаленного выполнения кода позволяет злоумышленникам выполнять произвольный код без аутентификации в Apache Solr через VelocityResponseWriter.

Gigabyte Drivers — CVE-2018-19320

Уязвимость низкоуровневого драйвера GDrv. Злоумышленники используют открытые функции в gdrv.sys, которые позволяют пользователю низкого уровня выделять и записывать данные в память для повышения привилегий SYSTEM.

Fortinet FortiOS — CVE-2018-13379

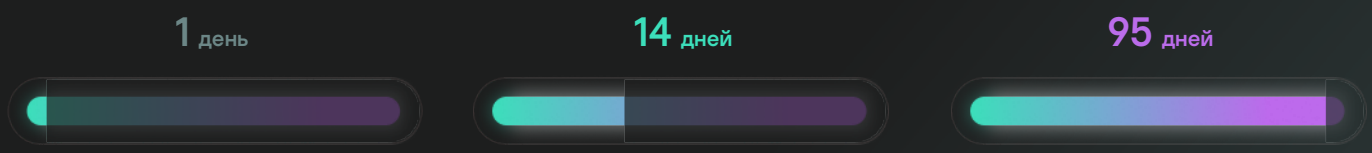
Уязвимость в FortiOS Web portal SSL VPN позволяет злоумышленникам, не прошедшим проверку подлинности, загружать системные файлы с помощью специально созданных HTTP-запросов к ресурсам.

Продолжительность атаки

Все инциденты можно разбить на три категории: продолжительность атаки, скорость реагирования на инцидент и ущерб от инцидента.

Быстрые	Средней продолжительности	Долгосрочные
52,7%	6,5%	17,2%
Часы и дни	Недели	Месяцы и дольше

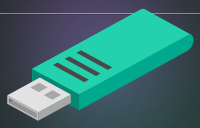
Средняя продолжительность атаки



Типовая угроза

Программы-вымогатели (ransomware)

Программы-вымогатели и хищения денежных средств



Программы-вымогатели и утечки данных

Продолжительность инцидентов

затраты в часах на расследование инцидента

Атаки, которые продолжались до недели	Атаки, которые продолжались до месяца	Атаки, которые продолжались больше месяца
29,4 часа	48,3 часа	60,13 часов
Масштабные быстрые атаки программ-вымогателей, которые представляют большую проблему даже для организаций со зрелой службой ИБ. Как правило, инциденты связаны с общедоступными и легко идентифицируемыми проблемами безопасности.	Несмотря на то, что из-за вымогателей многие атаки сходны с более быстрыми, случаи в этой группе имеют более значительный промежуток времени между первоначальным проникновением и следующими стадиями атаки.	Неравномерные периоды активной и пассивной фаз во время атаки. Продолжительность активных фаз очень похожа на предыдущую группу (средней продолжительности).

Контакты

По вопросам подписки на сервис:

intelligence@kaspersky.com

Для оказания помощи в экстренных случаях:

gert@kaspersky.com

kaspersky