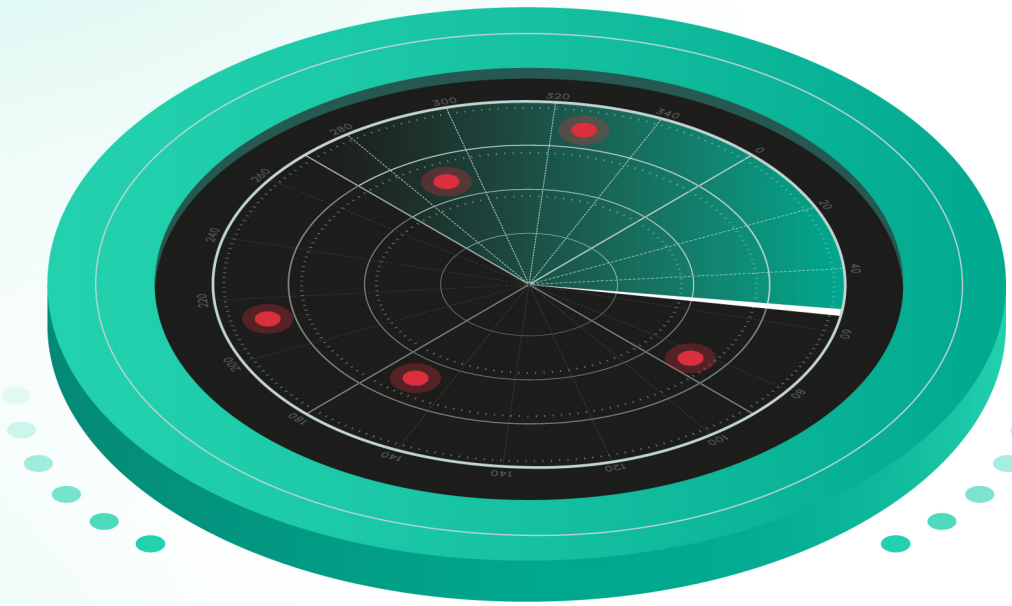
Реагирование на инциденты: аналитический отчет

2021



kaspersky

Основные выводы

В отчете использованы статистические данные, полученные на основе инцидентов, которые были обработаны в рамках сервиса по расследованию инцидентов за 2020 год.

Общие сведения об атаке

Вектор проникновения

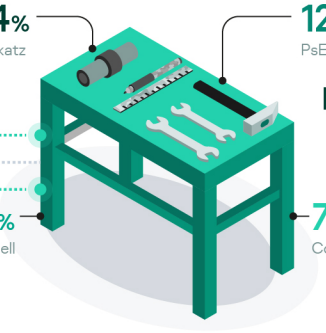
31,6% Атаки с перебором паролей (bruteforce)

31,5% Эксплуатация уязвимостей на периметре сети

23,7% Атаки через электронную почту

- Внедрить надежную парольную политику и многофакторную аутентификацию
- Исключить общедоступные сервисы удаленного управления в сети Интернет
- Устанавливайте обновления ПО или используйте компенсационные меры для сервисов на периметре сети
- Развивайте осведомленность сотрудников в вопросах информационной безопасности

Инструментарий атакующих



13,4% Mimikatz

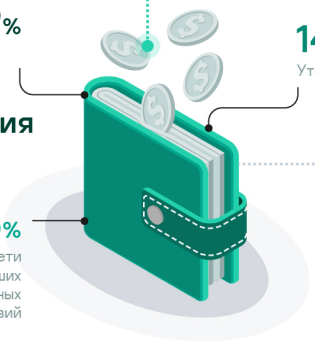
12,3% PsExec

8,2% PowerShell

7,2% Cobalt Strike

- Использовать правил обнаружения инструментов, используемых атакующими
- Используйте решения класса EDR
- Регулярно проводите киберучения с применением распространенных техник и тактик злоумышленников
- Откажитесь от использования внутренними командами ИТ инструментов, часто используемых атакующими

Последствия атаки



37,9% Зашифрованные данные

14,7% Утечка данных

10,5% Закрепление в сети с целью дальнейших злонамеренных действий

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

Индустрии

22% Промышленные предприятия

19% Государственный сектор

13% Финансовые организации

13% Телекоммуникации

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

Регионы

27,8% СНГ

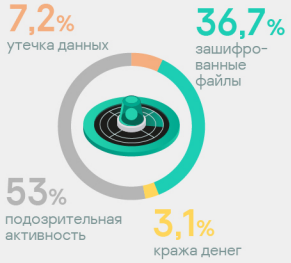
26,8% Ближний Восток и Африка

24,7% Европа

16,5% Америки

Операционные метрики

Как обнаружили инцидент



7,2% утечка данных

36,7% зашифрованные файлы

53% подозрительная активность

3,1% кража денег

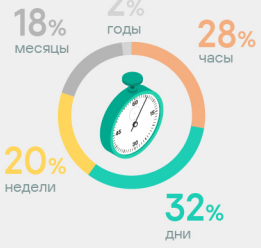
Обнаружение до или после последствий атаки

17% нет информации*

32% до обнаружения последствий атаки

51% после обнаружения последствий атаки

Продолжительность атаки



18% месяцы

2% годы

28% часы

20% недели

32% дни

Продолжительность реагирования на атаку

37% месяцы

22% часы

4% дни

37% недели

* Информации о последствиях атаки отсутствует, когда эксперты «Лаборатории Касперского» действуют как вспомогательная команда для другой основной команды, ведущей расследование

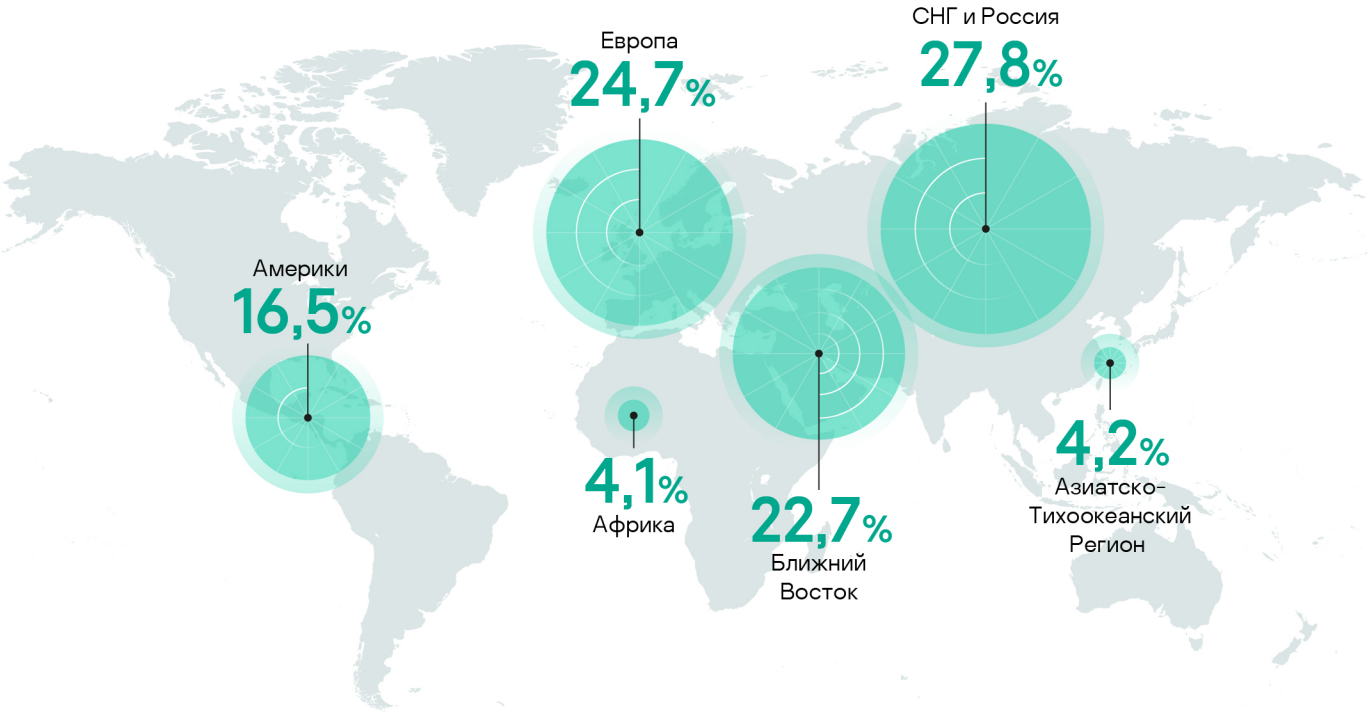
Введение

Аналитический отчет содержит информацию об атаках, расследованных «Лабораторией Касперского» в 2020 году. Мы предоставляем широкий спектр сервисов (реагирование на инциденты, цифровая криминалистика, анализ вредоносных программ) для оказания помощи пострадавшим от инцидентов информационной безопасности организациям. 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 .

В 2020 году пандемия вынудила компании приспособиться к подходу «работа из дома» (WFH), что оказало сильное влияние на работу отделов ИБ. Хотя основные тенденции с точки зрения угроз остались прежними, 97% наших сервисов стали проводиться в удаленном формате.

Сервисы цифровой криминалистики (Kaspersky Digital Forensics) и реагирования на инциденты (Kaspersky Incident Response) оказывают эксперты нашей Глобальной группы реагирования на чрезвычайные ситуации (GERT). Подразделения по расследованию компьютерных инцидентов (CIIU) и Глобального центра исследований и анализа угроз (GReAT) с экспертами в России и странах СНГ, Европе и Азии, Южной и Северной Америке, на Ближнем Востоке и в Африке.

География реагирования на инциденты

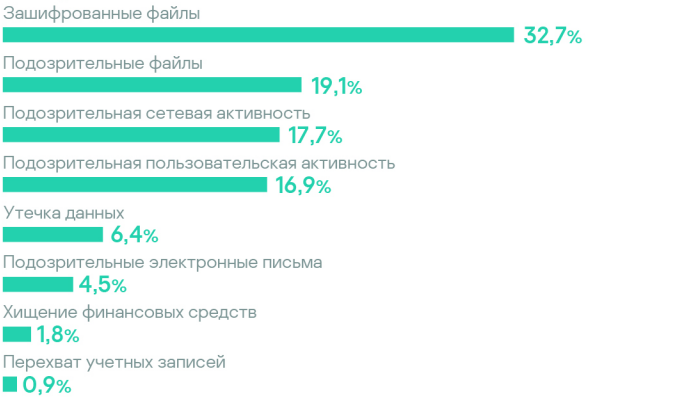


Вертикали и отрасли промышленности

Причины обращений к сервису реагирования на инциденты

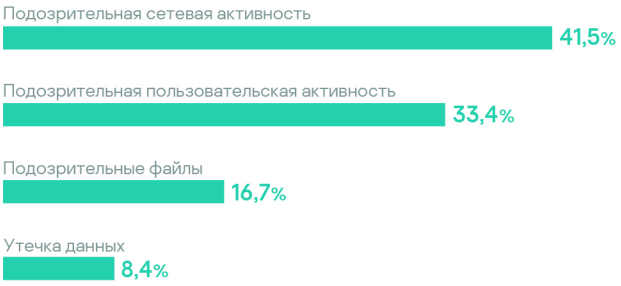
Доля инцидентов с программами-вымогателями (ransomware) превышает количество инцидентов с хищением денежных средств или любыми другими последствиями, так как атаки с шифрованием данных имеют простую схему монетизации и распространены во всех отраслях (не только финансовой). Большинство инцидентов с причинами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

Обращения с инцидентами (True positives)



10% от всех запросов были ложными срабатываниями. 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.

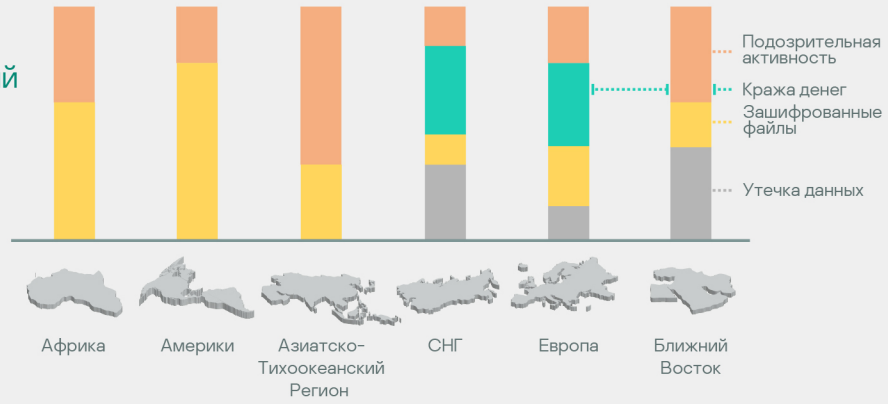
Ложные срабатывания (False positives)



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 публикаций, проекта NoRansom и отчетов об угрозах.

Статистика причин обращений по основным регионам

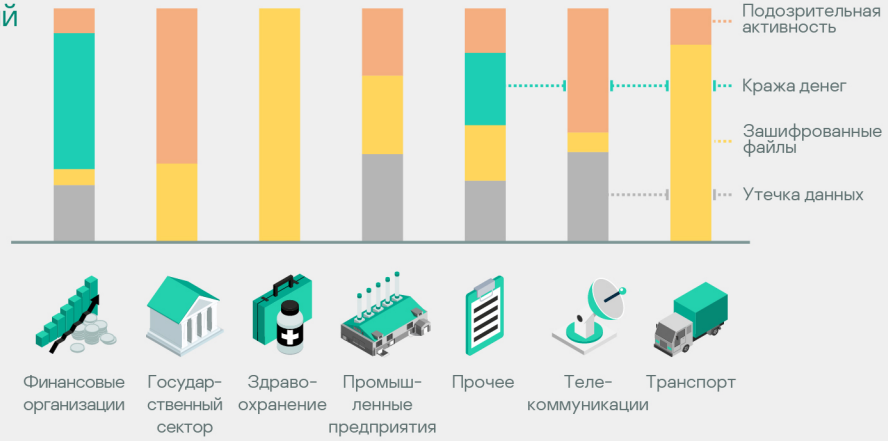
Америка и Африка в основном сталкиваются с атаками программ-вымогателей, в то время как в других регионах наблюдается более широкий спектр атак и очевидные проблемы с персональными данными (ПДн).



Статистика причин обращений по отдельным индустриям

В то время как здравоохранение, транспорт и промышленность сильно пострадали от программ-вымогателей, в финансовом секторе все еще продолжают использоваться прежние методы монетизации.

Отсутствие утечек данных в государственном секторе, скорее всего, связано с тем фактом, что государственные системы с ПДн обычно располагаются у телекоммуникационных и ИТ-провайдеров.

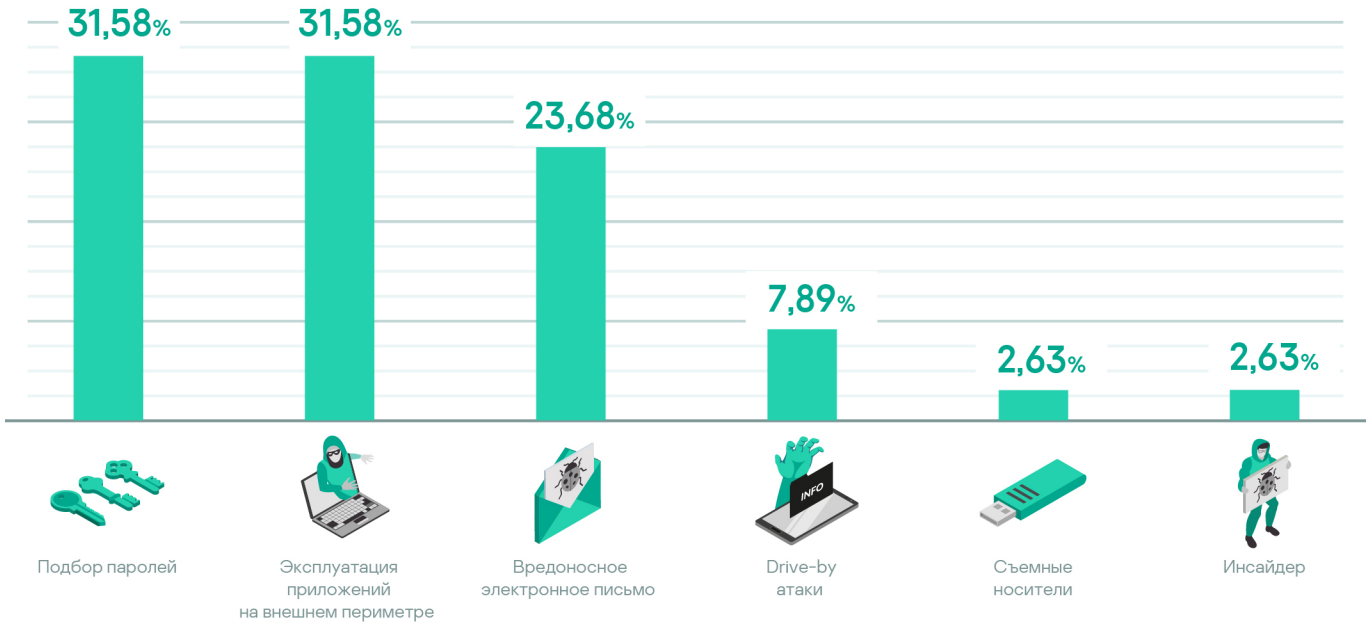


* Подозрительная активность является категорией событий генерируемых средствами выявления аномалий в сетевом и пользовательском поведении с точки зрения информационной безопасности.

Начальный вектор атаки

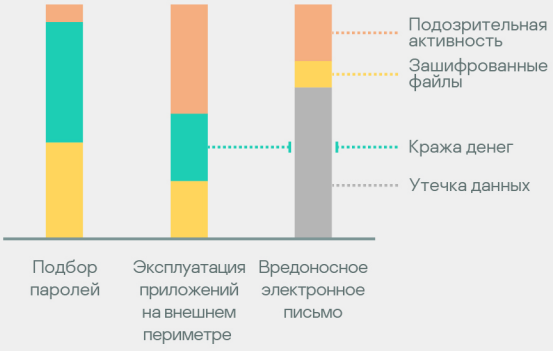
Как атакующие проникают внутрь организаций

Из года в год подавляющее большинство первоначальных векторов атаки – это проблемы безопасности с паролями, 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 30%, а внедрение надежной политики паролей снижает эту вероятность на 60% .



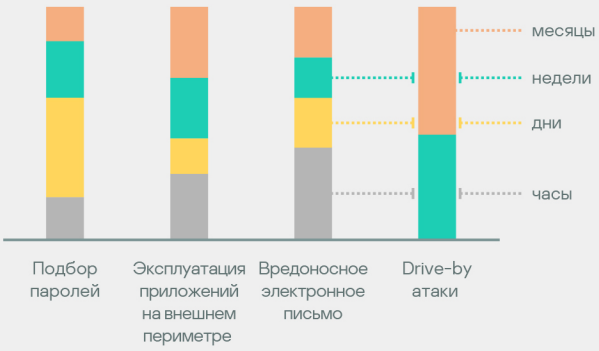
Самые популярные векторы начала атаки и методы их обнаружения

Злоумышленники-вымогатели используют почти все широко распространенные сценарии первоначальной компрометации инфраструктуры. Атаки с перебором паролей (bruteforce) легко обнаружить в теории, но на практике только часть из них была идентифицирована до наступления последствий атаки.



Продолжительность атаки в зависимости от вектора начала атаки

Большинство случаев, в которых не удалось установить начальный вектор атаки, оставались незамеченными более года, прежде чем были обнаружены – отсутствие артефактов для анализа (перезапись журналов). Более половины всех атак, которые начинались со вредоносных электронных писем, брутфорс-атак и эксплуатации уязвимости внешних приложений, были обнаружены в течение нескольких часов или дней.



* Мы установили начальный вектор в 55% обращений. Продолжительные атаки оставляют пострадавших без следов для исследования из-за перезаписи журналов или часть доказательств становятся недоступными из-за (не)намеренных действий ИТ-команд организаций. Атаки на подрядные организации также были среди многочисленных причин того, почему не удалось определить начальный вектор проникновения в сеть

** Согласно имеющимся статистическим данным

Инструменты атакующих и эксплойты

44% всех инцидентов содержали известный инструментарий

Почти в половине от всех инцидентов было обнаружено использование пользовательских инструментов уже присутствующих в системах пользователей (подобно LOLbins), хорошо известных инструментов с GitHub (например Mimikatz, AdFind, Masscan), а также коммерческих фреймворков (Cobalt Strike).

Используемые инструменты в случае инцидентов

Часто используемые

11–13%

Mimikatz, PsExec, Advanced IP Scanner

Умеренно используемые

4–8%

PowerShell, Cobalt Strike, Process Hacker, ProcDump

Редко используемые

2–3%

TeamViewer, Impacket, WMIC, PowerTool, Nmap, fgdump, Masscan, CScript, NetScan, WINrar, AdFind, NBTScan, PuTTY, RDP

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 — Execution — 26,2%
- Cobalt Strike
- CScript
- Impacket
- PowerShell
- PsExec

Обход защиты — Defense Evasion — 7,3%
- ProcessHacker
- PowerTool

Доступ к учетным данным — Credential access — 18,8%
- fgdump
- Mimikatz
- PowerTool
- ProcDump

Обнаружение — Discovery — 20,5%
- AdFind
- Advanced IP Scanner
- Masscan
- NBTScan
- NetScan
- Nmap
- WMIC

Горизонтальное перемещение — Lateral movement — 18,1%
- Cobalt Strike
- Impacket
- PsExec

Сбор данных — Collection — 1,7%
- WINrar

Управление и контроль — Command and control — 7,4%
- PuTTY
- RDP
- TeamViewer

Использование эксплойтов было обнаружено в 13% всех инцидентов

Только в небольшой части инцидентов эксплуатировались уязвимости 2020-го года. В других случаях были злоумышленники эксплуатировали старые уязвимости. Это позволяет говорить о том, что своевременные обновления безопасности могли бы предотвратить десятую часть расследованных инцидентов.

CVE-2020-0796

SMB сервис в Microsoft Windows

Уязвимость в сервисе SMBv3 позволяет удаленно исполнять произвольный код без предварительной аутентификации. Наследник уязвимости MS17-010.

CVE-2020-0787

Windows Background Intelligent Transfer Service (BITS)

Уязвимость позволяет повысить привилегии. Широко используется шифровальщиками.

CVE-2019-11510

Pulse Secure SSL VPN

Атакующие без аутентификации может получить учетные данные пользователя VPN-сервера. Мгновенный доступ к организации-жертве по легитимному каналу.

CVE-2019-0604

Microsoft SharePoint

Уязвимость позволяет удаленно исполнять произвольный код без предварительной аутентификации в Microsoft SharePoint.

CVE-2018-8453

Компонент Win32k Microsoft

Уязвимость позволяет повысить привилегии во время обработки объектов в памяти. Использовалась группой FruityArmor.

CVE-2017-0144

SMB сервис в Microsoft Windows

Уязвимость в сервисе SMBv1, позволяющая атакующим исполнять код через отправку сетевых пакетов. Используется в эксплойте EternalBlue.

CVE-2017-11317

Telerik.Web.UI

Уязвимость использует ошибку в функции шифрования RadAsyncUpload, которая позволяет применить удаленные загрузку файлов и исполнение кода.

CVE-2017-8464

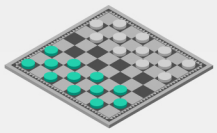
Microsoft Windows Shell

Позволяет локальным пользователям или удаленному атакующему исполнять код путем специально подготовленных .LNK файлов, обрабатываемых Windows Explorer или другими приложениями при отображении иконок. Применяется при атаках LemonDuck..

* Использование каждой из утилит было обнаружено в 11-13% инцидентов

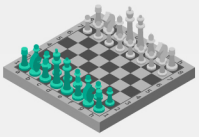
Продолжительность атак

Все инциденты можно сгруппировать по трем категориям с различными временем пребывания злоумышленника в сети, продолжительностью реагирования на инцидент, начальным вектором и последствиями атаки.



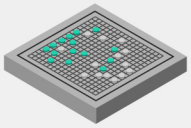
Быстрые

часы и дни



Средней продолжительности

недели



Продолжительные

месяцы и дольше

Продолжительность атаки

Быстрые	Средней продолжительности	Продолжительные
1,5 дней	18,1 дней	90,4 дней

Типовая угроза

Быстрые	Средней продолжительности	Продолжительные
Программы-вымогатели (ransomware)	Программы-вымогатели и хищения денежных средств	Программы-вымогатели и утечки данных

Стандартный вектор атаки (рейтинг по частоте)

Быстрые	Средней продолжительности	Продолжительные
▪ Атаки с перебором паролей (bruteforce) ▪ Эксплуатация уязвимостей на периметре сети ▪ Целенаправленный фишинг с вредоносными ссылками	▪ Эксплуатация уязвимостей на периметре сети ▪ Атаки через перенаправление (Drive-By) ▪ Атаки с перебором паролей ▪ Съемные устройства хранения данных ▪ Целенаправленный фишинг с вредоносными ссылками	▪ Эксплуатация уязвимостей на периметре сети ▪ Целенаправленный фишинг с вредоносными вложениями ▪ Атаки с перебором паролей ▪ Атаки через перенаправление (Drive-By) ▪ Инсайдер

Продолжительность инцидентов (затраты в часах на расследование инцидентов)

Быстрые	Средней продолжительности	Продолжительные
34,4 часов ▪ Атаки, которые продолжались до недели ▪ Масштабные быстрые атаки программ-вымогателей, которые представляют большую проблему даже для организаций со зрелой ИБ. Как правило, инциденты связаны с общедоступными и легко идентифицируемыми проблемами безопасности	48,9 часов ▪ Атаки, которые продолжались до месяца ▪ 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	105,6 часов ▪ Атаки, которые продолжались больше месяца ▪ Неравномерные периоды активной и пассивной фаз во время атаки. Продолжительность активных фаз очень похожа на предыдущую группу (Средней продолжительности)

Контакты

Запросы на расследование инцидентов

intelligence@kaspersky.com

Вопросы по отчету

gert@kasperksy.com

kaspersky