Аннотация – В этом документе представлен анализ группы вымогателей Mallox, которая быстро развивалась с момента своего первого выявления в июне 2021 года.

Анализ посвящён различным аспектам деятельности группы, включая её отличительную практику добавления названий целевых организаций к зашифрованным файлам, эволюцию её алгоритмов шифрования и тактику обеспечения постоянства и обхода средств защиты.

Выводы, полученные в результате этого анализа, имеют решающее значение для разработки стратегий защиты и повышения готовности к таким развивающимся киберугрозам.

I. Вредоносное ПО и тактика предотвращения обнаружения

Ransomware-группа TargetCompany, или Mallox, известна своими целенаправленными атаками программ-вымогателей, в первую очередь нацеленными на незащищённые серверы Microsoft SQL, работающие в Интернете. Программа-вымогатель шифрует данные жертв и требует выкуп, как правило, в криптовалюте, за ключ расшифровки.

Группа добавила в свой арсенал такие инструменты, как Remcos RAT, BatCloak и Metasploit, демонстрирующие передовые методы обфускации, позволяющие избежать обнаружения. Они используют полностью необнаруживаемые программы-обфускаторы (FUD) для шифрования своих программ-вымогателей, что затрудняет обнаружение и блокировку вредоносного ПО. Также – сбор конфиденциальных данных с использованием таких инструментов, как MIMIKATZ, и выполнение атак с помощью Trojan.BAT.TARGETCOMP*. Они также используют методы предотвращения обнаружения, такие как GMER, расширенное завершение процесса и YDArk

II. Смягчение последствий и дешифрование

Mallox добавляет уникальное расширение зашифрованного файла к именам файлов целевой организации. Было замечено, что для поддержания работоспособности заражённой системы следует избегать шифрования определённых папок и типов файлов. Программа-вымогатель помещает записку в каждый каталог на диске жертвы, содержащий инструкции по оплате

Компания Avast выпустила бесплатные дешифраторы для программ-вымогателей TargetCompany, которые при определённых обстоятельствах могут расшифровывать файлы. Важно отметить, что выплата выкупа не гарантирует, что злоумышленники предоставят ключ дешифрования, и это может стимулировать дальнейшую преступную деятельность

III. Программа-вымогатель как услуга (RaaS)

Mallox работает по модели RaaS, используя подпольные форумы для рекламы своих услуг. Группа поддерживает сайт на базе TOR, где публикует объявления о недавно скомпрометированных данных

A. Распространение

Mallox, распространяется различными способами. Программа-вымогатель в первую очередь нацелена на компании, а не на отдельных пользователей.

Одним из первоначальных методов доступа является фишинг, при котором для получения доступа к системе жертвы используются вредоносные файлы Microsoft OneNote. Другой метод заключается в атаках методом перебора на серверы Microsoft SQL, т.е. недостаточно защищённые серверы MS-SQL, используя атаки по словарю в качестве точки входа для проникновения в сети жертв.

Оказавшись внутри системы, программа-вымогатель использует команду PowerShell для извлечения полезной нагрузки программы-вымогателя с удалённого сервера. Полезная нагрузка пытается остановить и устранить службы, связанные с SQL, удалить теневые копии томов, очистить журналы системных событий и завершить процессы, связанные с безопасностью. После этих шагов он инициирует процесс шифрования и впоследствии оставляет записку с требованием выкупа в каждом каталоге.

Программа-вымогатель также собирает системную информацию и передаёт её на C2C-сервер. Программа-вымогатель шифрует файлы жертвы с помощью алгоритма шифрования ChaCha20 и генерирует ключ шифрования с использованием ECDH, примера криптографии с эллиптическими кривыми, и AES-128. К зашифрованным файлам добавляются расширения, которые соответствуют названию затронутой компании.

B. Симптомы атаки вымогателей нацелевую компанию

Симптомы атаки могут варьироваться в зависимости от конкретного варианта программы-вымогателя и тактики, однако общие признаки включают:

- **Невозможность доступа к файлам**: наиболее заметным симптомом атаки программ-вымогателей является невозможность открыть файлы, хранящиеся на компьютере, или получить к ним доступ. Файлы зашифрованы и их расширения изменены на название затронутой компании, такое как ".artiis", ".brg", ".mallox", ".architek", ".tohnichi", ".herrco" и другие
- **Повышенная активность процессора и диска**: Повышенная активность диска или основного процессора может указывать на то, что программа-вымогатель работает в фоновом режиме
- **Записка с требованием выкупа**: после процесса шифрования программа-вымогатель оставляет в каждом каталоге записку с требованием выкупа, озаглавленную "How to decrypt files.txt" или “RECOVERY FILES.txt”. Это примечание обычно содержит инструкции о том, как заплатить выкуп, чтобы получить ключ расшифровки
- **Сетевые аномалии**: используется сканирование сети для сбора информации о сетевом подключении, что может привести к необычной активности в сети
- **Завершение определённых процессов и служб**: Программа-вымогатель пытается остановить и устранить службы, связанные с SQL, удалить теневые копии томов, очистить журналы системных событий и завершить процессы, связанные с безопасностью

C. Методология

- **Первоначальный доступ**: Группа часто получает первоначальный доступ к системам жертв с помощью фишинговых кампаний, в которых задействованы вредоносные файлы OneNote. Они также используют слабые SQL-серверы на начальном этапе развертывания
- **Выполнение**: Полезная нагрузка программы-вымогателя выполняется с использованием различных методов. Например, группа внедряет исполняемый файл программы-вымогателя в AppLaunch.exe. Они также используют командные строки и PowerShell для загрузки полезной нагрузки программы-вымогателя с удалённого сервера
- **Постоянство**: Группа стремится к постоянству с помощью различных методов, включая изменение URL-адресов или путей до тех пор, пока выполнение Remcos RAT (вредоносное ПО удалённого доступа) не завершится успешно
- **Предотвращения обнаружения**: Группа использует полностью необнаруживаемые упаковщики-обфускаторы (FUD), чтобы избежать обнаружения решениями безопасности. Они также удаляют разделы реестра и теневые копии, чтобы повредить службам восстановления
- **Повышение привилегий**: присваивает своему процессу привилегии SeTakeOwnershipPrivilege и SeDebugPrivilege, чтобы облегчить свою собственную вредоносную работу
- **Обнаружение**: используется сканирование сети
- **Сбор**: Группа использует такие инструменты, как MIMIKATZ, для сбора данных
- **Командование и контроль (C&C)**: Группа устанавливает соединение с сервером C&C с помощью “/ap.php” точки
- **Шифрование**: Программа-вымогатель получает маски всех логических дисков в системе, используя GetLogicalDrives() Win32 API. Тип каждого диска проверяется с помощью GetDriveType(). Если этот диск действителен (стационарный, съёмный или сетевой), шифрование диска продолжается
- **Воздействие**: после шифрования программа-вымогатель оставляет записку с требованием выкупа. Группа использует метод двойного вымогательства, угрожая утечкой украденных данных, если выкуп не будет выплачен

D. Точки входа и Способы доставки

Атаки программ-вымогателей могут проникать в систему через различные точки входа:

- **Скомпрометированные учётные данные**: украденные или скомпрометированные учётные данные – это может произойти, когда сотрудники становятся жертвами фишинговых атак или когда учётные данные приобретаются в темной Сети
- **Неуправляемые устройства или принесите своё собственное устройство (BYOD)**: Неуправляемые устройства или персональные устройства, используемые в рабочих целях, могут стать точкой входа для программ-вымогателей, если они не защищены должным образом
- **Приложения с уязвимостями, подключённые к Интернету**: Уязвимости в приложениях, подключённых к Интернету, могут быть использованы злоумышленниками для получения доступа к сети. Сюда входят такие приложения, как VPN SSL, серверы Microsoft Exchange и веб-интерфейсы на основе пользовательского интерфейса Telerik
- **Фишинг**: Фишинговые атаки часто нацелены на конечных пользователей, обманом заставляя их раскрывать конфиденциальную информацию или загружать вредоносное программное обеспечение. Сотрудники играют жизненно важную роль в защите от этой угрозы, поэтому организациям крайне важно инвестировать в обучение своих сотрудников навыкам распознавания попыток фишинга и предотвращения таких попыток
- **Заражённые программные пакеты или исправления**: Скомпрометированные исправления или программные пакеты могут стать точками входа

для преступников-вымогателей. Эта тактика основана на том факте, что пользователи часто быстро загружают и устанавливают обновления для обеспечения безопасности своих систем, непреднамеренно позволяя вымогателям проникать

- **Атаки методом "грубой силы" на внешние шлюзы**: Киберпреступники все чаще используют такие методы, как атаки методом "грубой силы", для получения доступа к системам. Это включает в себя систематическое перебирание всех возможных комбинаций паролей до тех пор, пока не будет найден правильный
- **Протокол удалённого рабочего стола (RDP) и злоупотребление учётными данными**: Злоумышленники часто используют уязвимости в удалённых службах, таких как RDP или VPN-серверы. Они могут прибегать к фишинговым действиям, чтобы завладеть учётными данными, или использовать дампы учётных данных, доступные на форумах dark web
- **Электронная почта**: Электронная почта является распространённой точкой входа для атак программ-вымогателей. Злоумышленники часто прикрепляют к электронным письмам вредоносные файлы. Когда ничего не подозревающие жертвы открывают эти документы, выполняются макросы, запускающие полезную нагрузку программы-вымогателя

Mallox, использует различные точки входа для проникновения в системы:

- **Бэкдор Remcos**: Группа использует бэкдор Remcos в качестве начальной точки доступа. Remcos - который позволяет злоумышленникам удалённо управлять заражённой системой
- **Незащищённые серверы Microsoft SQL**: Группа нацелена на незащищённые серверы Microsoft SQL, используя их в качестве точек входа в инфраструктуру ИКТ жертв
- **BatLoader**: Группа использует BatLoader для запуска полезных программ-вымогателей. BatLoader – это вредоносное ПО, которое загружает и устанавливает дополнительные вредоносные программы в заражённую систему
- **Сканирование сети**: Группа использует сканирование сети в качестве метода обнаружения для выявления потенциальных целей в сети
- **Trojan.BAT.TARGETCOMP**: Это вредоносная программа, используемая группой для выполнения. Он предназначен для того, чтобы поставить под угрозу безопасность заражённой системы
- **GMER**: Группа использует GMER, детектор и средство для удаления руткитов, для предотвращения обнаружения. Это позволяет группе скрывать свои действия и закрепляться в заражённой системе

1) Точки входа в отрасли

Промышленное производство:

- **Промышленные системы управления (ICS) и устройства промышленного Интернета вещей (IIoT)**: уязвимости в этих системах используются для нарушения операций на производстве
- **Атаки на цепочку поставок**: Компрометация цепочки поставок, включая сторонних поставщиков, может стать отправной точкой для программ-вымогателей

Розничная торговля

- **Системы торговых точек (POS)**: Вредоносное ПО может заразить эти системы для кражи информации о кредитной / дебетовой карте
- **Серверы Microsoft SQL**: нацелены на незащищённые серверы MS-SQL, используемые в розничных операциях

Телекоммуникации

- **Уязвимости удалённого выполнения кода (RCE)**: Использование уязвимостей, таких как CVE-2019–1069 и CVE-2020–0618, для выполнения произвольного кода
- **Серверы Microsoft SQL**: использование функции xp_cmdshell в Microsoft SQL для удалённого выполнения

Бизнес-услуги

- **Устаревшие и не исправленные системы**: использование устаревших систем облегчает получение преступниками доступа
- **Функциональная зависимость от ИТ**: невозможность работать без ИТ стимулирует быстрые выплаты выкупа.

Здравоохранение

- **Фишинг и социальная инженерия**: использование ложных электронных писем для обмана медицинского персонала с целью установки программ-вымогателей
- **Скомпрометированные учётные данные**: использование украденных учётных данных для доступа к сетям здравоохранения

Финансы

- **Атаки на доступ к серверу и неправильные настройки**: использование уязвимостей сервера и ошибок конфигурации
- **Фишинг и кража учётных данных**: нацелены на ценные аккаунты, такие как аккаунты генеральных директоров и CFOS

Госсектор

- **Фишинг и социальная инженерия**: использование ложных электронных писем для обмана государственных служащих
- **Программа-вымогатель как услуга (RaaS):** использование моделей RaaS для нацеливания на государственные организации

Образование

- **Фишинг и социальная инженерия**: использование ложных электронных писем для обмана педагогического персонала и студентов
- **Скомпрометированные учётные данные**: использование украденных учётных данных для доступа к образовательным сетям

Информационные технологии

- **Эксплойты уязвимостей ПО**: Использование известных уязвимостей в ИТ-инфраструктуре
- **Учётные записи**: получение доступа к ИТ-системам через скомпрометированные учётные записи

Транспорт

- **Фишинг и социальная инженерия**: нацеливание сотрудников на фишинговые электронные письма с целью получения доступа к сети
- **Скомпрометированные учётные данные**: использование украденных учётных данных для доступа к транспортным сетям

IV. География и отраслевые цели

В поле зрения Mallox попали компании различных размеров, в т.ч. малый и средний бизнес. В 37% компаний, пострадавших от программ-вымогателей, работало менее 100 сотрудников, а 82% атак программ-вымогателей в 2021 году были направлены против компаний с численностью менее 1000 сотрудников. В то время как доля крупных организаций была выше в первом полугодии 2022 года, доля малых и средних организаций была выше в первом полугодии 2023 года, что указывает на тенденцию к увеличению числа целевых показателей малого и среднего бизнеса. Средний размер целевой компании, подвергшейся атаке вымогателей, составил 275 сотрудников, что на 10% больше, чем в предыдущем квартале

Группа в первую очередь нацелена на предприятия в Азиатско-Тихоокеанском регионе, за которыми следуют Европа и Ближний Восток (США, Индия, Саудовская Аравия, Канада, Германия, Австралия, Бразилия, Болгария, Китай, Вьетнам) и проявила интерес к организациям, работающим в промышленных отраслях, госсекторе, отраслях образования, розничной торговли, ИТ, здравоохранение, бизнес-услуг, телекоммуникаций, финансовой автомобильной и транспортной отрасли

A. Промышленное производство

В этом секторе атаки программ-вымогателей часто используют уязвимости в промышленных системах управления (ICS) и устройствах промышленного Интернета вещей (IIoT). Эти системы являются неотъемлемой частью производственных операций, и их компрометация может привести к значительным сбоям.

Эти атаки выходят за рамки непосредственных финансовых потерь, приводя к значительным затратам на реагирование на нарушения, возможному контакту с третьими сторонами, уменьшению доли рынка и нанесению ущерба корпоративной репутации. В некоторых случаях злоумышленники могут также потребовать выкуп в обмен на разрешение компании восстановить доступ к своим компьютерным системам. Более того, атаки программ-вымогателей могут привести к потере конфиденциальной и личной информации, что может иметь долгосрочные последствия для затронутых компаний и их клиентов

Сбой в работе

Атаки нарушают производственные операции, часто приводя к существенным потерям в производстве и разрозненным операциям. Когда программа-вымогатель выводит из строя производство, операции могут быть приостановлены на несколько дней или недель, что приводит к финансовым потерям, остановке производственных линий, что означало невозможность выполнения заказов клиентов.

Финансовые последствия

Финансовые последствия атак программ-вымогателей на производственный сектор огромны. В период с 2018 по 2023 год 478 производственных компаний подверглись атаке программ-вымогателей, что привело к потере примерно 46,2 миллиарда долларов только из-за простоев. Затраты на простой значительны, поскольку это сказывается на повседневной работе, а производственные линии иногда останавливаются.

Репутационный ущерб

Атаки также могут нанести значительный репутационный ущерб, который может быть длительным и иногда приводить к тому, что бизнес так и не оправится от репутационных последствий.

Проблемы конфиденциальности

Утечка данных является распространённым следствием атак программ-вымогателей. В 32% атак злоумышленники не только шифровали данные, но и крали их. В результате этих атак было взломано более 7,5 миллионов индивидуальных записей.

Правовые и нормативные последствия

Атаки программ-вымогателей могут иметь правовые и нормативные последствия, особенно когда они приводят к утечке данных. Компаниям могут грозить штрафы за неспособность должным образом защитить данные клиентов, и они также могут столкнуться с судебными исками от клиентов или деловых партнёров, пострадавших от нарушения.

Долгосрочные эффекты

Долгосрочные последствия атак программ-вымогателей могут включать незапланированное сокращение персонала и даже полное закрытие бизнеса. В некоторых случаях атаки программ-вымогателей приводили к тому, что компании просили передать их в конкурсное управление с сокращением рабочих мест.

Повышенная частота атак

В 2023 году производственный сектор пострадал сильнее всего, что свидетельствует о значительных уязвимостях в этом секторе. Количество атак на производственные предприятия также выросло примерно на 107% по сравнению с предыдущим годом

B. Розничная торговля

В сфере розничной торговли одной из распространённых точек входа для атак программ-вымогателей являются системы торговых точек (POS). Злоумышленники часто используют вредоносное ПО для заражения этих систем и кражи информации о кредитных / дебетовых картах. Кроме того, были замечены группы программ-вымогателей, нацеленные на серверы Microsoft SQL (MS-SQL), которые часто используются в операциях розничной торговли, и атакующие их

Атаки могут нанести ущерб розничному бизнесу, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному ущербу репутации и юридическим последствиям. Зависимость сектора розничной торговли от цифровых систем и обработки конфиденциальных данных клиентов делает его прибыльной мишенью для атак.

Сбой в работе

- **Потеря продаж**: атака может привести к упущенным возможностям для продаж, особенно в пиковые сезоны
- **Непрерывность бизнеса**: атаки могут нарушать критически важные бизнес-операции, предотвращая или ограничивая доступ к системам продаж
- **Время простоя**: даже несколько часов простоя интернет-магазина могут иметь огромные финансовые последствия, и потерей клиентов

Финансовые последствия

- **Потеря доходов**: Организации розничной торговли сообщают о значительной потере доходов в результате атак программ-вымогателей
- **Выплаты выкупа**: Розничные торговцы могут чувствовать себя вынужденными платить выкупы, особенно в периоды высоких продаж, и доля розничных организаций, выплачивающих более высокие выкупы, увеличилась
- **Затраты на восстановление**: у розничных продавцов-жертв, которые платят выкуп, средние затраты на восстановление в четыре раза выше, чем у тех, которые этого не делают

Репутационный ущерб

- **Доверие клиентов**: атаки подрывают доверие клиентов, особенно в случаях, когда личная информация была скомпрометирована
- **Ущерб бренду**: Восприятие "небезопасного" бизнеса может нанести больший ущерб, чем непосредственные финансовые потери, и повлиять на репутацию розничного продавца
- **Общественное мнение**: Успешные атаки могут рассматриваться как признак слабых методов обеспечения безопасности, что вынуждает клиентов вести бизнес в другом месте

Утечка данных

- **Конфиденциальная информация**: Розничные продавцы обрабатывают данные кредитных карт и личную информацию, которая может быть раскрыта в результате атаки программ-вымогателей
- **Утечки данных**: атаки представляют значительный риск утечки данных, что может привести к потере доверия потребителей

Влияние на сотрудников

- **Увольнения**: половина розничных продавцов столкнулись с увольнениями сотрудников после того, как стали жертвами программ-вымогателей
- **Приостановление деятельности**: трети розничных торговцев пришлось временно приостановить или приостановить свою деятельность

Риски, связанные с цепочкой поставок и третьими сторонами

- **Цепочки поставок**: злоумышленники могут заразить многие организации, нацеливаясь на конкретных поставщиков
- **Зависимость от сторонних производителей**: Розничные продавцы зависимы от сторонних производителей, которые могут создавать ИБ-риски

Правовые и нормативные последствия

Розничные продавцы могут столкнуться с юридическими последствиями в случае компрометации данных клиентов, включая штрафы за несоблюдение правил защиты данных.

C. Телекоммуникации

В телекоммуникационной отрасли для атак используют уязвимости удалённого выполнения кода (RCE), такие как CVE-2019–1069 и CVE-2020–0618, которые позволяют злоумышленникам выполнять произвольный код. Злоумышленники также могут использовать удалённое выполнение с помощью функции xp_cmdshell в MS SQL

Атаки могут нанести ущерб телекоммуникационному бизнесу, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному репутационному ущербу и юридическим последствиям.

Сбой в работе

- **Прерывание обслуживания**: атаки нарушают работу телекоммуникационных служб, затрагивая индивидуальные и корпоративные коммуникации
- **Проникновение в сеть**: созависимый характер телекоммуникационных сетей увеличивает риск проникновения, потенциально обеспечивая доступ через различные подключённые системы

Финансовые последствия

- **Потеря доходов**: атака может серьёзно повлиять на операционную способность организации, приведя к снижению доходов или полной остановке операций на время восстановления
- **Выплаты выкупа и затраты на восстановление**: компании могут столкнуться со значительными расходами, связанными с выплатами выкупа, усилиями по восстановлению, судебными издержками и другими сопутствующими расходами

Репутационный ущерб

- **Доверие клиентов**: успешная атака может нанести ущерб репутации телекоммуникационной компании из-за предполагаемых слабых методов обеспечения безопасности.
- **Ущерб бренду**: восприятие "небезопасного" бизнеса может нанести больший ущерб, чем немедленные финансовые потери

Проблемы конфиденциальности

- **Раскрытие конфиденциальных данных**: телекоммуникационные компании хранят обширные данные о клиентах, и атаки программ-вымогателей могут привести к утечке конфиденциальных данных
- **Двойное вымогательство**: злоумышленники могут угрожать разглашением конфиденциальных данных организации, если выкуп не будет выплачен, что приводит к атакам с двойным вымогательством

Правовые и нормативные последствия

- **Нарушения комплаенса**: Компании могут столкнуться с юридическими последствиями в случае компрометации данных клиентов, включая штрафы и неустойки за несоблюдение правил защиты данных

Риски, связанные с цепочкой поставок и третьими сторонами

- **Атаки на цепочки поставок**: злоумышленники могут заразить многие организации, нацеливаясь на поставщиков
- **Зависимость от сторонних производителей**: телекоммуникационные компании полагаются на расширенные цепочки поставок и зависимости от сторонних производителей, которые могут создавать риски кибербезопасности

Кража интеллектуальной собственности

Ценная интеллектуальная собственность телеком компаний находится под угрозой кражи или компрометации, что потенциально наносит ущерб конкурентным преимуществам и инновационным усилиям

Долгосрочный шпионаж

Некоторые атаки на операторов связи проводятся высокоразвитыми группами угроз, нацеленными на долгосрочный шпионаж

D. Транспторт

Атаки могут нанести ущерб транспортному сектору, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному репутационному ущербу и юридическим последствиям.

Сбой в работе

- **Остановка производства**: Атаки могут привести к остановке заводов-производителей, вызывая задержки в производстве и доставке
- **Уязвимость цепочки поставок**: цепочка поставок сложна и взаимосвязана, что делает её уязвимой для атак, которые могут иметь каскадный эффект

Финансовые последствия

- **Выплаты выкупа**: были зафиксированы одни из самых высоких выплат за вымогательство: промышленные компании потратили в 2019 году 6,9 миллиона долларов, что составило 62% от всех выплат за вымогательство
- **Потеря доходов**: атаки могут серьёзно повлиять на операционную способность организаций, приводя к снижению доходов или полной остановке операций на время восстановления

Репутационный ущерб

- **Доверие клиентов**: успешные атаки могут нанести ущерб репутации автомобильных компаний, вынуждая клиентов вести бизнес в других местах из-за предполагаемых слабых методов обеспечения безопасности
- **Ущерб бренду**: восприятие "небезопасного" бизнеса может нанести больший ущерб, чем немедленные финансовые потери

Проблемы конфиденциальности

- **Раскрытие конфиденциальных данных**: компании хранят обширные данные о клиентах, и атаки программ-вымогателей могут привести к утечке конфиденциальных данных
- **Двойное вымогательство**: злоумышленники могут угрожать разглашением конфиденциальных данных организации, если выкуп не будет выплачен, что приводит к атакам с двойным вымогательством

Правовые и нормативные последствия

Компании могут столкнуться с юридическими последствиями в случае компрометации данных клиентов, включая штрафы и неустойки за несоблюдение правил защиты данных

Кража интеллектуальной собственности

Интеллектуальная собственность автомобильных компаний находится под угрозой кражи или компрометации, что потенциально наносит ущерб конкурентным преимуществам и инновационным усилиям

Долгосрочный шпионаж

Некоторые атаки на поставщиков автомобильных услуг проводятся высокоразвитыми группами угроз, нацеленными на долгосрочный шпионаж

E. Бизнес-услуги

Атаки программ-вымогателей могут нанести ущерб бизнесу в сфере услуг, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному ущербу репутации и юридическим последствиям.

Сбой в работе

- **Время простоя**: атаки могут привести к остановке операций, что приведёт к значительному простою и нарушению деловой активности
- **Потеря бизнеса**: если важные файлы зашифрованы, предприятия могут оказаться неспособными работать, что приведёт к потере доходов

Финансовые последствия

- **Выплаты выкупа**: Предприятия могут почувствовать необходимость заплатить выкуп, чтобы быстро восстановить доступ к своим данным, особенно если резервные копии недоступны или также скомпрометированы
- **Затраты на восстановление**: помимо выплаты выкупа, предприятия сталкиваются со затратами на усилия по исправлению, включая ИТ-услуги, судебные издержки и потенциальные штрафы регулирующих органов
- **Потеря доходов**: невозможность работать во время и после атаки может привести к значительному снижению доходов

Репутационный ущерб

- **Доверие клиентов**: атака может серьёзно повредить репутации компании, в результате чего клиенты потеряют доверие и, возможно, перенесут свой бизнес в другое место
- **Ущерб бренду**: восприятие неадекватных мер безопасности может запятнать имидж бренда, влияя на долгосрочные перспективы бизнеса

Проблемы конфиденциальности

- **Раскрытие конфиденциальных данных**: Фирмы, предоставляющие бизнес-услуги, часто обрабатывают конфиденциальные данные клиентов. Атака может привести к утечке данных, раскрыв конфиденциальную информацию
- **Двойное вымогательство**: злоумышленники могут не только шифровать данные, но и угрожать их обнародованием, если выкуп не будет выплачен, что усугубляет последствия

Правовые и нормативные последствия

При компрометации клиентских данных предприятия могут столкнуться с юридическими последствиями и штрафами за несоблюдение правил защиты данных

Риски, связанные с цепочкой поставок и третьими сторонами

Атаки могут выходить за рамки затронутого бизнеса, затрагивая клиентов, партнёров и поставщиков

Кража интеллектуальной собственности

Для фирм, которые полагаются на запатентованные методы или данные, атаки программ-вымогателей представляют риск кражи интеллектуальной собственности

Долгосрочный шпионаж

Некоторые атаки могут быть частью долгосрочных шпионских усилий, направленных на сбор стратегической информации с течением времени

F. Здравоохранение

Атаки программ-вымогателей могут нанести ущерб организациям здравоохранения, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному ущербу репутации и юридическим последствиям.

Сбой в работе

- **Прерывание обслуживания**: Атаки могут нарушать работу здравоохранения путём шифрования или недоступности медицинских записей и систем, что приводит к задержкам в оказании помощи пациентам и потенциально может привести к смерти пациентов
- **Повышенная смертность пациентов**: атаки увеличивают внутрибольничную смертность пациентов, госпитализированных во время атаки, со значительным повышением риска смерти

Финансовые последствия

- **Потеря дохода и затраты на восстановление**: Организации здравоохранения могут столкнуться с финансовыми потерями, связанными с потерей дохода, выплатами выкупа, затратами на восстановление, а также ущербом для бренда и судебными издержками. Средняя стоимость атаки программы-вымогателя в сфере здравоохранения составила 4,82 миллиона долларов в 2021 году
- **Потери, связанные с простоями**: Атаки программ-вымогателей на здравоохранение привели к

потерям, связанным с простоями, в размере более 77 миллиардов долларов для экономики США

Репутационный ущерб

Успешные атаки могут серьёзно подорвать репутацию поставщиков медицинских услуг, что приведёт к потере доверия пациентов и потенциально вынудит пациентов обращаться за медицинской помощью в другое место

Проблемы конфиденциальности

- **Раскрытие конфиденциальных данных**: организации здравоохранения хранят обширные данные о пациентах. Атаки программ-вымогателей могут привести к утечке конфиденциальных данных, включая личную медицинскую информацию (PHI), подвергая миллионы пациентов рискам конфиденциальности
- **Двойное вымогательство**: злоумышленники могут угрожать разглашением конфиденциальных данных, если выкуп не будет выплачен, что усугубляет последствия атаки

Правовые и нормативные последствия

В случае компрометации данных пациентов медицинские организации могут столкнуться с юридическими последствиями и штрафами за несоблюдение правил защиты данных

Риски, связанные с цепочкой поставок и третьими сторонами

Атаки программ-вымогателей могут выходить за рамки непосредственно затронутого поставщика медицинских услуг, затрагивая клиентов, партнёров и поставщиков

Кража интеллектуальной собственности

Атаки программ-вымогателей создают риск кражи интеллектуальной собственности, потенциально нанося ущерб конкурентным преимуществам и инновационным усилиям

Долгосрочный шпионаж

Некоторые атаки на медицинских работников осуществляются высокоразвитыми группами угроз, нацеленными на долгосрочный шпионаж

G. Финансы

Атаки программ-вымогателей могут нанести ущерб финансовым учреждениям, что приведёт к прямым финансовым потерям, остановкам работы, долгосрочному ущербу репутации и юридическим последствиям. Зависимость финансового сектора от цифровых систем и обработки конфиденциальных данных клиентов делает его прибыльной мишенью для киберпреступников.

Сбой в работе

- **Прерывание обслуживания**: Атаки нарушают финансовые операции, шифруя или делая недоступными финансовые записи и системы, что приводит к задержкам в финансовых транзакциях и потенциально вызывает значительные операционные сбои
- **Сетевое проникновение**: Взаимосвязанный характер финансовых сетей увеличивает риск проникновения, потенциально обеспечивая доступ к информации через различные связанные системы

Финансовые последствия

- **Потеря дохода и затраты на восстановление**: Финансовые организации могут столкнуться с финансовыми потерями, связанными с потерей дохода, выплатами выкупа, затратами на восстановление, а также ущербом для бренда и судебными издержками. Средняя стоимость атаки финансового вымогателя составила 5,9 миллиона долларов за киберинцидент в 2023 году
- **Потери, связанные с простоями**: Атаки на финансовые сервисы привели к значительным финансовым потерям, включая затраты, связанные с серьёзностью атаки и степенью раскрытия данных

Репутационный ущерб

- **Потеря доверия**: успешные атаки программ-вымогателей могут серьёзно повредить репутации финансовых учреждений, в результате чего клиенты теряют доверие и, возможно, переводят свой бизнес в другое место
- **Ущерб бренду**: восприятие неадекватных мер безопасности может запятнать имидж бренда, влияя на долгосрочные перспективы бизнеса

Проблемы конфиденциальности

- **Раскрытие конфиденциальных данных**: Финансовые учреждения хранят обширные данные о клиентах. Атаки программ-вымогателей могут привести к утечке конфиденциальных данных, подвергая миллионы клиентов рискам конфиденциальности
- **Двойное вымогательство**: злоумышленники могут угрожать разглашением конфиденциальных данных, если выкуп не будет выплачен, что усугубляет последствия атаки

Правовые и нормативные последствия

: В случае компрометации клиентских данных финансовые учреждения могут столкнуться с юридическими последствиями и штрафами за несоблюдение правил защиты данных

Риски, связанные с цепочкой поставок и третьими сторонами

Атаки могут распространяться за пределы непосредственно затронутого финансового учреждения, затрагивая клиентов, партнёров и поставщиков

Кража интеллектуальной собственности

Атаки создают риск кражи интеллектуальной собственности, потенциально нанося ущерб конкурентным преимуществам и инновационным усилиям

Долгосрочный шпионаж

Атаки на финансовые учреждения проводятся группами, нацеленными на долгосрочный шпионаж

H. Госсектор

Атаки на государственные учреждения могут нарушить жизненно важные операции, привести к значительным финансовым потерям, подорвать общественное доверие и иметь долгосрочные последствия для сообщества.

Сбой в работе

- **Прерывание обслуживания**: возможно отключение цифровые активы, такие как платёжные платформы или гражданские порталы, что приводит к остановке муниципальных операций
- **Службы экстренной помощи**: Атаки, приводящие к отключению систем диспетчеризации 911 или 311, могут поставить жизни людей под угрозу
- **Время простоя системы**: Госслужащие могут остаться без систем, прибегая к ручным процессам

Финансовые последствия

- **Затраты**: В период с 2018 по декабрь 2023 года атаки на правительственные организации США обошлись примерно в 860,3 миллиона долларов
- **Выплаты выкупа**: Правительства могут быть вынуждены платить выкупы или столкнуться с дорогостоящим решением о перестройке систем

Репутационный ущерб

- **Общественное доверие**: атака может нанести ущерб репутации государственных структур, потенциально приводя к потере доверия общественности
- **Восприятие безопасности**: Успешные атаки рассматриваются как свидетельство слабых методов обеспечения безопасности, что заставляет общественность сомневаться в способности правительства защищать конфиденциальную информацию

Проблемы конфиденциальности

- **Конфиденциальная информация**: Правительства рискуют потерять контроль над секретной и личной информацией, такой как номера социального страхования или данные кредитной карты
- **Потеря данных**: Программа-вымогатель может привести к непригодности данных и систем, что приведёт к потенциальной потере данных, если резервные копии недоступны или скомпрометированы

Правовые и нормативные последствия

Правительства могут столкнуться с юридическими последствиями и штрафами за несоблюдение правил защиты данных, если данные граждан будут скомпрометированы

Долгосрочные эффекты

- **Обучение и денежные потери**: например, атаки программ-вымогателей на школы могут привести к потере знаний, а также к денежным потерям
- **Психосоциальное воздействие**: могут наблюдаться значительные краткосрочные и долгосрочные социальные и психологические последствия для лиц, пострадавших от нападений

Повышенная частота атак

Значительно увеличилось количество атак программ-вымогателей на правительственные организации, при этом на 313% увеличилось количество зарегистрированных инцидентов со службами безопасности

I. Образование

Атаки программ-вымогателей могут нанести ущерб учебным заведениям, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному ущербу репутации и юридическим последствиям.

Сбой в работе

- **Прерывание обслуживания**: Программа-вымогатель может отключать цифровые активы, такие как платёжные платформы или гражданские порталы, что приводит к остановке муниципальных операций
- **Службы экстренной помощи**: Атаки, приводящие к отключению систем диспетчеризации 911 или 311, могут поставить жизни людей под угрозу
- **Время простоя системы**: Государственные служащие могут остаться без своих систем, прибегая к ручным процессам

Финансовые последствия

- **Затраты**: В период с 2018 по декабрь 2023 года атаки программ-вымогателей на правительственные организации США обошлись примерно в 860,3 миллиона долларов; Средняя стоимость образовательной атаки программ-вымогателей составила 2,73 миллиона долларов за киберинцидент в 2023 году.
- **Выплаты выкупа**: Правительства могут быть вынуждены платить выкупы или столкнуться с дорогостоящим решением о перестройке систем

Репутационный ущерб

- **Общественное доверие**: атака программ-вымогателей может нанести ущерб репутации государственных структур, потенциально приводя к потере доверия общественности

- **Восприятие безопасности**: Успешные атаки могут рассматриваться как свидетельство слабых методов обеспечения безопасности, что заставляет общественность сомневаться в способности правительства защищать конфиденциальную информацию

Проблемы конфиденциальности

- **Конфиденциальная информация**: Правительства рискуют потерять контроль над секретной и личной информацией, такой как номера социального страхования или данные кредитной карты
- **Потеря данных**: Программа-вымогатель может привести к непригодности данных и систем, что приведёт к потенциальной потере данных, если резервные копии недоступны или скомпрометированы

Правовые и нормативные последствия

Правительства могут столкнуться с юридическими последствиями и штрафами за несоблюдение правил защиты данных, если данные граждан будут скомпрометированы

Долгосрочные эффекты

- **Обучение и денежные потери**: например, атаки программ-вымогателей на школы могут привести к потере знаний, а также к денежным потерям
- **Психосоциальное воздействие**: могут наблюдаться значительные краткосрочные и долгосрочные социальные и психологические последствия для лиц, пострадавших от нападений

Повышенная частота атак

Значительно увеличилось количество атак программ-вымогателей на правительственные организации, при этом на 313% увеличилось количество зарегистрированных инцидентов со службами безопасности конечных точек

J. Информационные технологии

Атаки программ-вымогателей могут нанести ущерб ИТ-компаниям, что приведёт к прямым финансовым потерям, остановкам в работе, долгосрочному ущербу репутации и юридическим последствиям.

Сбой в работе

- **Прерывание обслуживания**: Программы-вымогатели могут нарушать работу ИТ-служб, шифруя или делая системы и данные недоступными, что приводит к задержкам в обслуживании и потенциально вызывает значительные сбои в работе
- **Проникновение в сеть**: Взаимосвязанный характер ИТ-сетей увеличивает риск проникновения, потенциально обеспечивая доступ к информации через различные подключённые системы

Финансовые последствия

- **Потеря доходов**: Организации могут столкнуться со снижением доходов или полной остановкой операций во время восстановления после атаки программ-вымогателей, даже если у них есть функциональные резервные копии
- **Выплаты выкупа и затраты на восстановление**: Компании могут столкнуться со значительными расходами, связанными с выплатой выкупа, восстановлением системы, судебными издержками и другими сопутствующими расходами

Репутационный ущерб

- **Доверие клиентов**: успешная атака может нанести ущерб репутации ИТ-компаний, вынудив клиентов вести бизнес в других местах из-за предполагаемых слабых методов обеспечения безопасности
- **Ущерб бренду**: Восприятие "небезопасного" бизнеса может нанести больший ущерб, чем непосредственные финансовые потери, и повлиять на репутацию компании

Утечка данных и проблемы конфиденциальности

- **Раскрытие конфиденциальных данных**: ИТ-компании хранят обширные данные о клиентах и операционной деятельности. Атаки программ-вымогателей могут привести к утечке конфиденциальных данных, подвергая клиентов рискам для конфиденциальности
- **Двойное вымогательство**: злоумышленники могут угрожать разглашением конфиденциальных данных, если выкуп не будет выплачен, что приводит к атакам с двойным вымогательством

Правовые и нормативные последствия

В случае компрометации данных клиентов ИТ-компании могут столкнуться с юридическими последствиями и штрафами за несоблюдение правил защиты данных

Цепочка поставок и риски третьих сторон

Атаки программ-вымогателей могут распространяться за пределы непосредственно затрагиваемой ИТ-компании, затрагивая клиентов, партнёров и поставщиков

Кража интеллектуальной собственности

Атаки создают риск кражи интеллектуальной собственности, потенциально нанося ущерб конкурентным преимуществам и инновационным усилиям

Долгосрочный шпионаж

Некоторые атаки на ИТ-компании проводятся группами, нацеленными на долгосрочный шпионаж