Аннотация – Анализ тенденций в области программ-вымогателей за 4 квартал 2023 года направлен на понимание многогранного ландшафта угроз, связанных с программами-вымогателями и произошедших изменений.

С учётом специфики можно определить особенности операций, совершаемых с использованием программ-вымогателей, включая идентификацию доминирующих групп программ-вымогателей, их целевых секторов и географического распределения атак.

Кроме того, анализ выявит важные тенденции, такие как рост числа инцидентов с программами-вымогателями, эволюция тактики вымогательства и последствия этих изменений для стратегий кибербезопасности.

Эти знания будут полезны как для специалистов в области технической, так и стратегической безопасности, предлагая информацию, которая может направлять разработку надёжных механизмов защиты, информировать о решениях по управлению рисками и, в конечном счёте, повышать устойчивость организаций к постоянно присутствующей угрозе программ-вымогателей.

I. Введение

2023 год стал самым успешным годом для групп программ-вымогателей в истории: в общей сложности 4368 жертв, что на 55,5% больше, чем в предыдущем году. Только в четвёртом квартале число жертв составило 1386 человек, что указывает на постоянное влияние программ-вымогателей на отрасль.

В 4 квартале 2023 года наиболее распространённые типы атак программ-вымогателей в основном осуществлялись тремя группами: LockBit 3.0, Clop Ransomware и ALPHV / BlackCat ransomware. LockBit 3.0 оставалась самой активной группой программ-вымогателей, заявляя в среднем о 23 жертвах в неделю.

В ежеквартальном отчёте Air IT об угрозах подчёркивается, что атаки программ-вымогателей, фишинг и инсайдерские угрозы по-прежнему представляют значительные риски, при этом резкий рост объёма данных и расширение уязвимостей глобальной сети. В отчёте ISACA о состоянии кибербезопасности за 2023 год указано, что 48% организаций столкнулись с ростом кибератак в 4 квартале 2023 года.

В отчёте TechTarget о тенденциях в области программ-вымогателей на период до 2024 года говорится, что атаки на цепочки поставок и использование облачной и VPN-инфраструктуры по-прежнему будут оставаться ключевыми тенденциями. В отчёте также упоминается, что с 2020 года было обнаружено более 130 различных штаммов программ-вымогателей, причём наиболее распространённым является семейство GandCrab family being the most prevalent.

Отчёт Trend Micro о программах-вымогателях за первую половину 2023 года показал, что LockBit, BlackCat и Clop были ведущими группами RaaS, при этом число организаций-жертв значительно увеличилось по сравнению со второй половиной 2022 года.

Исследование Check Point Research описало 2023 год как год масштабных атак программ-вымогателей с переходом от тактики шифрования к использованию украденных данных для вымогательства. Сектор образования и исследований в наибольшей степени пострадал от атак программ-вымогателей в 2023 году.

II. Воздействие на отрасли

В 4 квартале 2023 года отраслями, наиболее пострадавшими от атак программ-вымогателей, были сектор бизнес-услуг, сектор образования / исследований и сектор розничной / оптовой торговли.

Сектор бизнес-услуг США был наиболее уязвимым сектором по данным Cyberint.

Сектор образования и исследований также сильно пострадал от атак программ-вымогателей, на долю которых, по данным Check Point Research, пришлось 22% всех атак в 2023 году.

По данным Check Point Research, еженедельный рост числа атак в секторе розничной и оптовой торговли составил 22% по сравнению с 2022 годом.

Другие отрасли, которые были заметно затронуты, включают ИТ, здравоохранение и производственный сектор, которые, по данным Trend Micro, были наиболее уязвимыми с точки зрения обнаружения файлов-вымогателей в первой половине 2023 года. В отчёте TechTarget также перечислены несколько отраслей в качестве приоритетных целей, включая строительство и недвижимость, правительственны учреждения, СМИ, развлечения и досуг, местные и федеральные органы власти, энергетическую и коммунальную инфраструктуру, транспорт, финансовые услуги, а также профессиональные и отдельно юридические услуги.

III. Ключевые моменты Q4

Основные выводы из тенденций в области программ-вымогателей в 4 квартале 2023 года заключаются в следующем:

- **Рекордное количество жертв**: 2023 год стал самым успешным годом для групп программ-вымогателей в истории: в общей сложности 4368 жертв, что на 55,5% больше, чем годом ранее. Только в четвёртом квартале было зафиксировано 1386 жертв
- **Доминирующие группы программ-вымогателей**: LockBit 3.0 оставалась самой активной группой программ-вымогателей, заявляя в среднем о 23 жертвах в неделю. Также были заметны программы-вымогатели Clop и ALPHV / BlackCat, жертвами которых стали 104 и 81 человек соответственно
- **Громкие инциденты**: Известные инциденты включали атаку LockBit на Royal Mail и отключение программы-вымогателя Hive
- **Влияние на отрасль**: Сектор бизнес-услуг, сектор образования / исследований и сектор розничной / оптовой торговли были одними из наиболее пострадавших от атак программ-вымогателей
- **Географический фокус**: главной мишенью стали США, за ними следуют Великобритания и Канада
- **Тенденции в методах атак**: Произошёл сдвиг в тактике от шифрования к использованию украденных данных для вымогательства, при этом злоумышленники больше внимания уделяли краже данных и кампаниям по вымогательству, которые не обязательно включали шифрование данных
- **Программа-вымогатель как услуга (RaaS)**: RaaS остаётся ключевым фактором атак, и такие группы, как LockBit, работают по этой модели
- **Тактика вымогательства**: Двойные и тройные атаки с целью вымогательства становятся все более распространёнными и потенциально более результативными, и дорогостоящими для пострадавших компаний
- **Chain-Атаки**: chain-атаки стали неотъемлемой частью ландшафта угроз, связанных с программами-вымогателями, распространяя воздействие атак не только на отдельных жертв

IV. Платёжные инструменты программ-вымогателей

В 4 квартале 2023 года наиболее распространёнными способами оплаты, используемыми при атаках программ-вымогателей, по-прежнему оставались криптовалюты, причём наиболее распространённым был биткоин. На биткойн приходилось примерно 98% платежей программ-вымогателей из-за его предполагаемой анонимности и простоты использования. Однако появились первые признаки того, что цифровые валюты, более ориентированные на конфиденциальность, такие как Monero, набирают популярность в качестве предпочтительного способа оплаты для киберпреступников. Этот сдвиг произошёл из-за возрастающей простоты обнаружения потока и источников биткоина.

Несмотря на распространённость выплат с целью получения выкупа, доля жертв, которые платили выкупы, снижалась. Только 37% жертв программ-вымогателей заплатили выкуп в 4 квартале 2023 года, что является рекордно низким показателем. Снижение было связано с улучшением мер безопасности и инвестициями в непрерывность резервного копирования, что позволило большему количеству организаций восстанавливаться после атак без выплаты выкупов.

Средний платёж за выкуп в 4 квартале 2023 года был значительно высоким: средний платёж составил 408 643 доллара, что на 58% больше, чем в 3 квартале 2022 года, а средний платёж составил 185 972 доллара, что на 342% больше, чем в 3 квартале 2022 года. Увеличение сумм платежей было расценено киберпреступниками как тактика компенсации сокращающегося числа жертв, готовых платить выкупы.

V. Точки входа программ-вымогателей

В 4 квартале 2023 года наиболее распространёнными точками входа для атак программ-вымогателей были:

- **Фишинговые атаки**: Фишинговые атаки были основным методом доставки программ-вымогателей, при этом 62% успешных атак программ-вымогателей использовали фишинг в качестве точки входа в систему жертвы. Число фишинговых атак выросло на 173% в третьем квартале 2023 года. Злоумышленники использовали все более изощренные методы социальной инженерии, чтобы обманом вынудить сотрудников предоставлять конфиденциальную информацию
- **Использование уязвимостей**: Уязвимости в программном обеспечении и системах были ещё одной распространённой точкой входа. Например, группа программ-вымогателей CL0P использовала программное обеспечение для передачи файлов GoAnywhere. Два новых вида программ-вымогателей, CACTUS и 3AM, появились в четвёртом квартале 2023 года, причём CACTUS использовал известные уязвимости в устройствах VPN
- **Кража учётных данных и атаки методом грубой силы**: Кража учётных данных использовалась в 44% успешных атак программ-вымогателей, а учётные данные методом грубой силы, такие как подбор пароля, использовались в 17% атак
- **Атаки на цепочки поставок**: Злоумышленники нацеливались на сторонних поставщиков, чтобы получить доступ к сети организации.

- **Инсайдерские угрозы**: Инсайдерские угрозы продолжали представлять значительные риски для организаций
- **Атаки социальной инженерии**: Атаки социальной инженерии, включая компрометацию деловой электронной почты (BEC), также были распространёнными

VI. Методы шифрования программ-вымогателей

Методы шифрования, используемые в этих атаках, эволюционировали с течением времени, и злоумышленники используют сочетание симметричных и асимметричных методов шифрования для повышения эффективности своих атак. При таком подходе программа-вымогатель генерирует два набора ключей, и для повышения эффективности атаки используется цепочка шифрования.

В дополнение к этим методам шифрования произошёл заметный сдвиг в стратегиях выполнения атак программ-вымогателей. Киберпреступники все чаще сосредотачиваются на краже данных, за которыми следуют кампании по вымогательству, которые не обязательно включают шифрование данных.

VII. Способы Доставки программ-вымогателей

В 4 квартале 2023 года наиболее распространёнными методами доставки, используемыми при атаках программ-вымогателей, были атаки по цепочке поставок, методы двойного вымогательства и воздействия "Программа-вымогатель как услуга" (RaaS).

Атаки на цепочки поставок стали надёжным методом для зрелых и опытных групп программ-вымогателей. В этих атаках вместо прямого нападения на единственную жертву злоумышленники нацеливаются на сторонних поставщиков, чтобы получить доступ к сети организации.

Двойное вымогательство было ещё одним распространённым методом. С помощью этого метода злоумышленники не только шифруют данные жертвы, но и угрожают утечкой украденных данных, если выкуп не будет выплачен.

Операции с программами-вымогателями как услугой (RaaS) также сыграли значительную роль. В RaaS разработчики создают программное обеспечение-вымогатель и продают доступ к этому инструменту преступникам, которые затем распространяют его среди потенциальных целей. Доступ осуществляется на основе подписки, поэтому он называется RaaS.

Фишинг с вредоносными вложениями и эксплуатация уязвимостей, таких как уязвимости нулевого дня, также использовались в качестве методов начального доступа к целевой системе

VIII. Уязвимости, используемые при атаках программ-вымогателей

В четвёртом квартале 2023 года злоумышленники-вымогатели продолжали использовать ряд уязвимостей для компрометации организаций. Одной из наиболее заметных эксплуатируемых уязвимостей была уязвимость двухлетней давности, для которой примерно в то же время было доступно исправление. Это подчёркивает важность своевременного управления исправлениями и контроля версий в организациях.

Кроме того, злоумышленники использовали уязвимость в программном обеспечении MagicLine4NX, затрагивающую версии до 1.0.026, для инициирования своих атак. Уязвимость MOVEit также была значительной, составляя значительный процент жертв в предыдущих кварталах, и вполне вероятно, что такие уязвимости оставались мишенью для групп программ-вымогателей.

В 2023 году также произошёл всплеск использования эксплойтов нулевого дня при атаках программ-вымогателей, которые представляют собой уязвимости, неизвестные поставщику программного обеспечения или не имеющие доступного исправления на момент атаки. Эта тенденция использования уязвимостей нулевого дня подчёркивает адаптивность субъектов киберугроз и необходимость для организаций укреплять свою защиту от таких возникающих угроз.

IX. Способы предотвращения атак программ-вымогателей

В 4 квартале 2023 года наиболее эффективные способы предотвращения атак программ-вымогателей были многогранными, включающими сочетание технических мер, обучения пользователей и упреждающих стратегий:

- **Резервное копирование данных**: Регулярное резервное копирование данных является важным шагом в смягчении последствий атаки программ-вымогателей. Решение для резервного копирования данных может гарантировать, что даже если данные зашифрованы программой-вымогателем, организация сможет восстановить свои системы без необходимости платить выкуп
- **Обучение кибератакам**: Обучение сотрудников распознавать потенциальные угрозы вымогателей и избегать их, такие как фишинговые электронные письма и вредоносные вложения, может значительно снизить риск успешных атак
- **Управление исправлениями**: Регулярное обновление и исправление программного обеспечения может устранить известные уязвимости, которые могут использовать программы-вымогатели
- **Расширенное предотвращение угроз**: Автоматизированные системы обнаружения и предотвращения угроз могут выявлять и устранять большинство атак программ-вымогателей до того, как они нанесут значительный ущерб
- **Защита конечных устройств**: Надёжные решения для обеспечения безопасности конечных устройств, включая антивирус и программное обеспечение для защиты от вредоносных программ, могут

обнаруживать и блокировать угрозы, связанные с программами-вымогателями

- **Сегментация сети**: Разделение сети на отдельные сегменты может предотвратить распространение программ-вымогателей по всей системе
- **Модель безопасности с нулевым доверием**: Внедрение модели с нулевым доверием, при которой доступ к ресурсам предоставляется только после успешной проверки пользователем своей личности, может снизить вероятность атаки программ-вымогателей
- **Многофакторная аутентификация (MFA)**: Внедрение MFA может повысить уровень безопасности, затрудняя злоумышленникам доступ к системам
- **Доступ с наименьшими привилегиями**: Обеспечение пользователям минимальных уровней доступа, необходимых для выполнения их задач, может ограничить потенциальный ущерб от атаки программ-вымогателей
- **Белый список приложений**: Разрешение запускать в системе только одобренные приложения может предотвратить выполнение программ-вымогателей.