I. Введение

Ниже подробно проанализируем публичных материалы о программах-вымогателях за третий квартал 2023, углубляясь в различные аспекты текущей ситуации, меняющиеся тенденции в атаках, отрасли и географию явления. Материалы позволяют оценить как количественные факторы инцидентов, так и качественный синтез данных применяемых тактик, и последствия для стратегий кибербезопасности в будущем. Цель анализа – предоставить читателям полезную информацию и более глубокое понимание феномена программ-вымогателей в его нынешнем виде и прогнозов на 2024.

II. Отличительные особенности за 2023 год

- **Рост количества атак программ-вымогателей**: Количество известных атак, при которых жертва не платила выкуп, составило 457 только в ноябре; общее количество зарегистрированных атак составило 1900, а нераскрытых массовых атак было 1815 за первые полгода. Количество сообщений, связанных с программами-вымогателями, составило 4082, в среднем 371,1 сообщения в месяц.
- **Атаки программ-вымогателей на сектор здравоохранения**: за последние четыре года количество атак на сектор здравоохранения увеличилось на 278%. Крупные нарушения, о которых сообщалось, затронули более 88 миллионов человек (на 60% больше чем в 2022).
- **Успех программ-вымогателей**: 2023 год отмечен как самый успешный год для групп программ-вымогателей за всю историю: в общей сложности 4368 жертв, что на 55,5% больше, чем в предыдущем году. Только за второй и третий кварталы 2023 года общее число жертв превысило 2022 год и составило 2903 человека.
- **Всплеск числа программ-вымогателей**: Во втором квартале 2023 года количество случаев вымогательства увеличилось на 67% по сравнению с предыдущим кварталом, жертвами стали 1386 человек по всему миру. Ведущими группами программ-вымогателей в этот период были LockBit3.0, ALPHV и Cl0p.
- **Кампания MOVEit**: Кампания MOVEit была признана самой успешной в этом году, что подчёркивает важность chain-атак и необходимость надёжного контроля версий и понимания поверхности атаки. Основной мишенью были США, где было зарегистрировано примерно 64% случаев.
- **Рекордный третий квартал**: Третий квартал 2023 года стал самым успешным кварталом в истории программ-вымогателей, поскольку на отрасль сильно повлияла эксплуатация критических уязвимостей и появление новых групп и семейств программ-вымогателей.
- **Рост отрасли в целом**: несмотря на глобальные усилия правоохранительных органов по борьбе с программами-вымогателями, отрасль быстро расширяется.
- **Новые программы-вымогатели**: было ликвидировано множество программ-вымогателей, включая Hive, RansomedVC и ALPHV. Однако появились и новые игроки, такие как Hunters International, Dragon Force и WereWolves.
- **Выкупы вымогателям**: Средний размер корпоративного выкупа превысил 100 000 долларов при среднем требовании в размере 5,3 миллиона долларов. 80% организаций придерживаются политики "Не платить", и только 41% организаций заплатили выкуп.
- **Страхование от программ-вымогателей**: 77% организаций обнаружили, что программы-вымогатели специально исключены из их страхования безопасности.
- **Цели программ-вымогателей**: в США промышленный сектор подвергся атакам 48 различных групп программ-вымогателей.
- **Атаки на крупные компании**: ряд атак были проведены на Toyota, Boeing и другие компании с использованием уязвимости Citrix Bleed (CVE-2023–4966).
- **Программа-вымогатель как услуга (RaaS)**: Распространение RaaS стало заметной тенденцией, упростив киберпреступникам выполнение атак.

III. Особенности кампании MOVEit

Кампания MOVEit относится к инциденту 2023 года, связанному с использованием уязвимости нулевого дня в

программном обеспечении для передачи файлов MOVEit, разработанном Progress Software. Кампания была организована группой программ-вымогателей Clop, которая использовала уязвимость для кражи данных многочисленных организаций в различных секторах, включая правительство, финансы и здравоохранение.

Ключевые артефакты:

- **Уязвимость и эксплуатация**: уязвимость CVE-2023–34362 затронула как локальные, так и облачные версии MOVEit и связана с SQL-инъекциями для манипулирования данными и получения доступа к базе данных.
- **Исполнители**: ответственность за атаки несла группа Clop, которая в том же году была связана с инцидентами GoAnywhere и PaperCut.
- **Влияние**: Кампания оказала значительное влияние, затронув более 1062 организаций и примерно 65 435 641 человека к концу августа 2023 года. Жертвы охватывали целый ряд отраслей и включали как частные организации, так и организации государственного сектора.
- **Реакция**: Progress Software оперативно отреагировала на обнаружение уязвимости, выпустив исправление. Однако спустя месяцы число жертв продолжало расти, что наводит на мысль о том, что многие организации, вероятно, подверглись взлому в первые несколько дней и недель кампании.
- **Последствия**: Кампания MOVEit подчеркнула важность упреждающей кибербезопасности и управления уязвимостями. Это также говорит, что потенциальный ущерб может быть нанесён в рамках chain-атак, поскольку многие организации были скомпрометированы не потому, что напрямую они использовали MOVEit, а потому, что наняли сторонних подрядчиков или субподрядчиков.

IV. География

Ключевые моменты географии покрытия атак:

- **Глобальное распространение программ-вымогателей**: киберпреступники расширили географию своего присутствия в 2023 году, распространив проверенные вредоносные инструменты на новые страны и регионы.
- **Наиболее пострадавшие страны**: США были наиболее пострадавшей страной с большим количеством взломанных учётных записей, далее Великобритания, Канада, Мозамбик, Ангола и Гана.
- **Сектора**: главные цели включали сектора образования, строительный и недвижимость, центральное и федеральное правительство, средства массовой информации, развлечения а также местные органы власти.
- **Тенденции в области программ-вымогателей**: появились новые группы программ-вымогателей, такие как Rhysida, BianLian, IceFire, Sparta и Bl00dy, что подчёркивает развивающийся характер отрасли.

V. Результаты третьего квартал 2023 года

Результаты деятельности программ-вымогателей:

- **Рекордная активность**: наблюдался значительный всплеск активности программ-вымогателей: частота глобальных атак вымогателей выросла на 11% по сравнению со вторым кварталом и на 95% в годовом исчислении (г/г).
- **Жертвы**: Количество жертв программ-вымогателей в 2023 году уже превысило то, что наблюдалось в 2021 и 2022 годах.
- **Новые игроки**: такие программы-вымогатели как MalasLocker, 8base и Nokoyawa, привлекли внимание, так как за первый квартал своей деятельности эти группы в совокупности заявили о 305 жертвах.
- **Отрасли**: Атаки программ-вымогателей затронули производство, правительственные учреждения, нефтегазовый сектор, транспорт, логистику и складирование.
- **Тенденции на будущее**: Исходя из активности в конце 3-го и начале 4-го квартала, ожидается, что цифры превзойдут все, что наблюдалось в предыдущие годы

VI. Прогноз на 2024 год

Исходя из фактов за 2023 год ожидается, что программы-вымогатели останутся серьёзной угрозой в 2024 году, и организациям необходимо будет адаптировать и усилить меры кибербезопасности для снижения рисков:

- **Chain-атаки**: группы программ-вымогателей воспользуются преимуществами инфраструктуры ориентированной на подрядчиков и субподрядчиков, по-прежнему придерживаясь традиционных методов, таких как использование утёкших учётных данных и использование методов социальной инженерии
- **Тенденции**: ожидается, что индустрия программ-вымогателей будет развиваться с появлением новых групп и тактик.
- **Усилия правоохранительных органов и отрасли**: вероятно, усилия продолжатся с упором на закрытие основных групп киберпреступности и предотвращение атак
- **Страхование от программ-вымогателей**: по мере роста числа атак программ-вымогателей роль страхования в кибербезопасности будет становиться все более важной, поскольку организациям необходимо ориентироваться в сложностях покрытия инцидентов с вымогателями

- **Технологические разработки**: кибербезопасность будет продолжать развиваться с переходом к более комплексным стратегиям защиты, которые включают предотвращение, обнаружение, устранение последствий и судебную экспертизу
- **Глобальное воздействие**: ожидается, что географическое влияние программ-вымогателей останется значительным, поскольку киберпреступники по-прежнему нацелены на широкий круг стран и отраслей
- **Разновидности программ-вымогателей**: Появление новых разновидностей и дальнейшая активность существующих, вероятно, сохранятся, создавая постоянные проблемы для защиты от кибербезопасности.

VII. Заключение

В качестве заключения хотелось бы подчеркнуть важность надёжных мер кибербезопасности и необходимость постоянной бдительности и адаптации перед лицом растущих угроз программ-вымогателей:

- **Атаки программ-вымогателей в 2023 году**: год стал рекордным для индустрии программ-вымогателей, поскольку количество атак значительно увеличилось. Наиболее целевым сектором был сектор деловых услуг, за которым следовали секторы розничной торговли и производства.
- **Рост индустрии программ-вымогателей**: несмотря на усилия правоохранительных органов, индустрия программ-вымогателей продолжала быстро расти. Появились новые группы, а существующие, такие как LockBit3.0, ALPHV и Cl0p, нанесли ущерб организациям по всему миру
- **Усилия правоохранительных органов**: правоохранительные органы по всему миру работают над тем, чтобы остановить рост индустрии программ-вымогателей. Они добились определённого успеха в закрытии нескольких крупных киберпреступных группировок, таких как HIVE
- **Прогноз на 2024 год**: индустрия программ-вымогателей продолжит расти, при этом новые и существующие группы будут представлять серьёзную угрозу для организаций по всему миру