Аннотация – В документе представлен анализ ситуации вокруг AlphaV (программы-вымогатели), связанного с группой BlackCat, который охватывает технические детали программы-вымогателя, включая её механизмы шифрования, векторы начального доступа, методы бокового перемещения и методы эксфильтрации данных.

Выводы, полученные в результате этого анализа, важны для практиков кибербезопасности, ИТ-специалистов и политиков. Понимание особенностей программ-вымогателей AlphV/BlackCat позволяет разрабатывать более эффективные механизмы защиты, совершенствовать стратегии реагирования на инциденты.

I. Введение

Сайт-вымогатель AlphV, связанный с группой BlackCat, подвергся серии сбоев и блокировок со стороны ФБР, за которыми последовали попытки группы восстановить контроль. 19 декабря 2023 года ФБР в рамках скоординированных усилий с международными правоохранительными органами наложило арест на веб-сайт группы и опубликовало соответствующее уведомление. Это действие было частью кампании по уничтожению деятельности группы вымогателей BlackCat, которая нацелилась на компьютерные сети более 1000 жертв по всему миру, включая те, которые поддерживают критически важную инфраструктуру США.

ФБР также разработало инструмент расшифровки, который был предоставлен сотням жертв программ-вымогателей по всему миру, позволяющий предприятиям, школам, здравоохранению и экстренным службам восстанавливаться и возвращаться в Сеть. Однако официальные лица AlphV быстро отреагировали, восстановив временный контроль над своим сайтом и разместив новое уведомление, в котором говорилось о преуменьшении значения действий ФБР и объявили, что "VIP" филиалы получат частную поддержку в отдельных изолированных центрах обработки данных.

Несмотря на первоначальный успех ФБР, сайт AlphV снова заработал, но без всех ссылок на жертв, ранее опубликованных в рамках их стратегии вымогательства. Группа также утверждала, что у ФБР были ключи дешифрования только для около 400 компаний, в результате чего более 3000 жертв получили зашифрованные данные. В отместку AlphV сняла свой добровольный запрет на атаки на критически важные сектора инфраструктуры, включая здравоохранение и ядерные объекты.

«Перепалка» между ФБР и AlphV привела к многочисленным случаям захвата веб-сайта, а затем его "отмены", демонстрируя перетягивание каната за контроль над сайтом. Несмотря на эти события, ФБР и его партнёры продолжают расследование и преследование лиц, стоящих за BlackCat, с целью привлечения их к ответственности.

II. AlphV ransomware

Программа-вымогатель работает с токеном доступа, который поставляется с зашифрованной конфигурацией, которая содержит список служб / процессов, список каталогов / файлов / расширений файлов, внесённых в белый список, и список украденных учётных данных из среды жертвы. Программа-вымогатель сканирует тома на локальном компьютере, монтирует все размонтированные тома и начинает шифровать файлы. Он также удаляет все теневые копии томов, затрудняя жертвам восстановление своих данных.

Программа-вымогатель эволюционировала и стала использовать более сложные конструкции, что затрудняет её обнаружение. Например, конфигурационные данные больше не имеют формат JSON; вместо этого используются бинарные структуры, и они содержат ненужный код и тысячи зашифрованных строк для затруднения статического анализа.

Было замечено, что программа-вымогатель ALPHV использует уязвимости в открытых сервисах или слабые учётные данные для первоначального доступа. Он также использует такие инструменты, как ExMatter, для кражи конфиденциальных данных перед развёртыванием программы-вымогателя.

III. Тактика AlphV

ALPHV использует несколько тактик распространения для компрометации систем:

- **Фишинговые электронные письма**: вводящие в заблуждение сообщения создаются для того, чтобы заманить жертв к открытию вредоносного контента, часто замаскированного под законные сообщения
- **Вредоносная реклама**: использование вредоносной рекламы для распространения вредоносного ПО. Известно, что группа программ-вымогателей ALPHV манипулирует рекламой Google, чтобы привести ничего не подозревающих пользователей на вредоносные сайты

- **Установщики заражённого ПО**: использование заражённых установщиков для доставки программ-вымогателей. Сюда входят клонированные веб-страницы законных организаций, которые используются для распространения вредоносного кода по заражённым ссылкам или файлам
- **Использование уязвимостей ПО**: Группа использует уязвимости в операционных системах Windows, серверах Exchange и продуктах защищённого мобильного доступа для получения доступа к сетям жертв
- **Метод тройного вымогательства**: Эта возникающая угроза включает кражу данных с локальных компьютеров и облачных серверов, запуск программы-вымогателя, а затем оказание дополнительного давления на жертву посредством DDoS-атак или утечки данных

IV. Точки входа AlphV

ALPHV была идентифицирована как один из самых распространённых вариантов программы-вымогателя "как услуга" в мире, затрагивающий различные секторы, включая производство, технологии, розничную и оптовую торговлю, финансы, здравоохранение и общественную сферу, госсектор и энергетику, и профессиональные услуги.

Первоначальными точками проникновения программы-вымогателя ALPHV в сети жертв являются, прежде всего, скомпрометированные учётные данные пользователей и использование уязвимостей программного обеспечения. Например, было замечено, что дочерние компании ALPHV нацеливались на общедоступные установки Veritas Backup Exec, которые были уязвимы для определённых CVE, для получения первоначального доступа к среде жертвы.

В секторе здравоохранения атаки программ-вымогателей часто используют множество возможных точек входа, включая фишинговые электронные письма, уязвимости программного обеспечения, атаки по протоколу удаленного рабочего стола и несанкционированные загрузки с вредоносных веб-сайтов.

В финансовом секторе атаки ALPHV подчеркнули необходимость расширения возможностей обнаружения инцидентов и надёжной своевременной отчётности перед лицом развивающихся киберугроз.

В технологическом секторе известно, что ALPHV компрометирует поставщиков технологий цифрового кредитования, что видно из атаки на MeridianLink.

В государственном секторе сбои затронули критически важную инфраструктуру США и госучреждения.

В энергетическом секторе было замечено, что программа-вымогатель нацелена на сети, поддерживающие критически важную инфраструктуру США.

В секторе профессиональных услуг ALPHV нацелена на юридические, IT-, промышленные и финансовые услуги.

В дополнение к этим методам ALPHV также использует инструменты администрирования Windows и инструменты Microsoft Sysinternals для компрометации. Также стоит отметить, что некоторые филиалы ALPHV осуществляют фильтрацию данных и вымогательство у жертв, даже не внедряя программы-вымогатели.

V. Шифрование и выкупы

ALPHV использует сложные методы шифрования для блокировки данных жертв: комбинацию симметричного и асимметричного шифрования, хотя конкретные детали этих алгоритмов публично не разглашаются. Более конкретно, программа-вымогатель ALPHV использует либо AES, либо ChaCha20, в зависимости от его конфигурации. Программа-вымогатель генерирует случайный ключ для каждого файла, который затем шифруется с помощью открытого ключа RSA, хранящегося в конфигурации BlackCat. Затем файл шифруется с помощью AES.

Что касается способов оплаты, ALPHV обычно запрашивают выплаты выкупа в криптовалютах, в частности в биткоинах и Monero. Эти криптовалюты пользуются спросом из-за их децентрализованного характера и анонимности, которую они предоставляют получателям. Суммы выкупа, требуемые ALPHV, часто непомерны и варьируются от пяти до шести цифр в долларах США. Однако стоит отметить, что известно, что субъекты угрозы вели переговоры и принимали платежи ниже первоначального требования о выкупе

VI. Цели AlphV

Было обнаружено, что ALPHV нацелена на организации различных размеров. Согласно данным с сайтов утечек с требованием выкупа, больше всего жертв приходится на компании с 51–200 сотрудниками, что составляет 20,57% от общего числа. За ними следуют компании с численностью менее 50 сотрудников, на долю которых приходится 16,91% жертв:

- Компании с численностью сотрудников 501–1000 человек: 7,12%
- Компании с численностью сотрудников от 1000 до 5000 человек: 9,92%
- Компании с численностью 5,000-10,000 сотрудников: 2,38%
- Компании с численностью сотрудников более 10 000 человек: 4,46%

Однако важно отметить, что существует категория с пометкой "неизвестно", на долю которой приходится 27,87% от общего числа, что указывает на то, что точный размер компании некоторых жертв не известен.

В четвёртом квартале 2022 года успешные атаки BlackCat были нацелены в первую очередь на малые предприятия, составив 38,9% от общего числа, за которыми следовали компании среднего размера (28,6%).

ALPHV нацелена на широкий круг организаций в различных секторах:

- **Организации здравоохранения**: ALPHV был связан с атаками на организации здравоохранения, включая утечку конфиденциальных изображений

пациентов с раком молочной железы. Norton Healthcare также стала жертвой атаки ALPHV

- **Финансовые учреждения**: Fidelity National Financial стала мишенью ALPHV. Группа заявила о взломе систем поставщика программного обеспечения для бухгалтерского учёта Tipalti с планами вымогательства у клиентов поставщика
- **Нефтяные компании**: Две немецкие нефтяные компании стали мишенью группы BlackCat
- **Гостиничный бизнес**: Громкие атаки были связаны с ALPHV, в т.ч. MGM Resorts и Caesars Entertainment
- **Производство**: ALPHV нацелилась на производителя и поставщика складских услуг
- **Государственные учреждения и службы экстренной помощи**: Министерство юстиции США связало ALPHV с атаками на критически важную инфраструктуру США, включая госучреждения и службы экстренной помощи
- **Школы**: Школы также стали мишенью ALPHV
- **Компании оборонно-промышленной базы**: Эти компании стали мишенью ALPHV в рамках её атак на критически важную инфраструктуру США

A. Здравоохранение

AlphV шифровал конфиденциальные данные, включая информацию о пациентах, и требовал выкуп за ключи расшифровки. Эти атаки не только привели к финансовым потерям, но и создали серьёзные риски для ухода за пациентами и их безопасности. Агрессивные действия правоохранительных органов, включая разработку инструментов дешифрования, принесли некоторую помощь жертвам.

Известные атаки и воздействия

Атака программ-вымогателей McLaren HealthCare: Крупная атака программ-вымогателей на McLaren HealthCare, крупного поставщика медицинских услуг в Мичигане, выявила уязвимость систем здравоохранения к киберугрозам.

- **Атаки на больницы и медицинские сети**: Группа атаковала больницы, раскрывая конфиденциальные данные пациентов и подвергая риску уход за пациентами и их жизни. Эти атаки были частью более широкой схемы атаки на сети критически важной инфраструктуры США
- **Влияние на уход за пациентами и безопасность данных**: Атаки на организации здравоохранения имели серьёзные последствия, включая перебои в предоставлении медицинских услуг, раскрытие конфиденциальной медицинской информации и финансовые потери.

Реакция правоохранительных органов

- **Кампания по подрыву деятельности Министерства юстиции США**: Министерство юстиции (DOJ) в сотрудничестве с ФБР и международными партнёрами запустило кампанию против группы ALPHV/BlackCat, направленную на снижение угрозы для критически важной инфраструктуры, включая сектор здравоохранения
- **Инструмент дешифрования ФБР**: в рамках усилий по предотвращению сбоев ФБР разработало инструмент дешифрования для жертв ALPHV, включая организации здравоохранения. Этот инструмент помог спасти жертв от требований выкупа на общую сумму около 68 миллионов долларов, позволив пострадавшим предприятиям и медицинским учреждениям восстановиться и возобновить деятельность

B. Индустрия финансовых институтов

ALPHV представляет серьёзную угрозу для индустрии финансовых учреждений, применяя эффективную тактику нападения на банки, страховые компании и других поставщиков финансовых услуг, включая шифрование файлов, кражу конфиденциальных данных и требование выкупа, часто с использованием двойного вымогательства (шифрование и угроза разглашения данных).

Известные атаки и воздействия

- **Атака на Fidelity National**: Один из самых громких инцидентов был связан с компанией Fidelity National Financial, поставщиком титульного страхования, входящей в список Fortune 500. Группа ALPHV / Black Cat взяла на себя ответственность за эту кибератаку, которая привела к сбоям в страховании титула, условном депонировании и других сопутствующих услугах.
- **Рост угроз программ-вымогателей**: В финансовой отрасли наблюдается всплеск атак программ-вымогателей, при этом заметно возросла как частота, так и эффективность этих инцидентов. Финорганизации являются привлекательной мишенью из-за огромного количества хранящихся у них конфиденциальных данных о клиентах и партнёрах, что делает их идеальными для атак с двойным вымогательством.
- **Влияние на финансовые операции**: Атаки на финучреждения имеют серьёзные последствия, включая нарушение работы важнейших финансовых услуг и торговой деятельности. Например, атака на американское торговое подразделение Промышленно-коммерческого банка Китая нарушила торги на рынке казначейских облигаций США, что подчёркивает потенциальное влияние программ-вымогателей на финансовую стабильность

C. Нефтяные компании, промышленность

Группа работает по модели "программа-вымогатель как услуга" (RaaS) и нацелена на организации по всему миру

Известные атаки и воздействия

ALPHV раскрыла 400 ГБ данных, которые, как утверждается, были украдены у Encino Energy, основного производителя нефти в Огайо. Несмотря на это, Encino Energy сообщила, что атака не повлияла на их деятельность. В Европе ALPHV была замешана в нападении на немецкие нефтяные компании Mabanaft и Oiltanking, которое нарушило работу их систем погрузки и разгрузки и вынудило энергетического гиганта Shell перенаправить поставки. Эти атаки демонстрируют способность ALPHV нацеливаться на критически важную энергетическую инфраструктуру и разрушать её.

Реакция правоохранительных органов

Правоохранительные органы приняли меры против инфраструктуры группы ALPHV. ФБР и международные правоохранительные органы проникли в инфраструктуру группы и закрыли её, жертвами которой за 18 месяцев стали более 1000 человек. Хотя в рамках демонтажа не было объявлено ни о каких арестах, операция представляет собой значительную попытку пресечь деятельность групп программ-вымогателей, нацеленных на критически важные секторы, такие как нефтяная промышленность.

D. Индустрия гостеприимства и развлечений

AlphV совершила несколько громких атак на индустрию гостеприимства и развлечений, которые характеризуются кражей конфиденциальных данных, включая личную и финансовую информацию клиентов, за которой следуют требования выкупа. Используемая группой тактика включает социальную инженерию и недобросовестную рекламу.

Известные атаки и воздействия

- **Атака LBA Hospitality**: LBA Hospitality управляет отелями крупных сетей, таких как Marriott и Hilton. Группа утверждала, что скомпрометировала около 200 ГБ "строго конфиденциальных" внутренних данных компании, включая личные данные клиентов и сотрудников, финансовые отчёты, информацию о кредитных картах и многое другое
- **Международная атака MGM Resorts**: ALPHV была ответственна за кибератаку на MGM Resorts, вызвавшую значительные сбои в работе, вывела из строя системы онлайн-бронирования, цифровые ключи от номеров, игровые автоматы и веб-сайты. Группа использовала тактику социальной инженерии, чтобы получить доступ к системам MGM, и внедрила программу-вымогатель в более чем 100 гипервизорах ESXi в сети MGM.
- **Атака Caesars Entertainment**: Caesars Entertainment стала ещё одной жертвой ALPHV, в результате которой был нанесён ущерб по меньшей мере в 100 миллионов долларов и, как сообщается, был выплачен выкуп в размере 15 миллионов долларов
- **Westmont Hospitality Group**: Группа заявила, что взломала Westmont Hospitality Group, один из крупнейших в мире частных гостиничных бизнесов
- **Утечка данных Motel One**: Группа атаковала сеть отелей Motel One и угрожала утечкой 6 ТБ украденных данных, включая контактные данные клиентов, внутренние документы и данные кредитной карты

Технологические подходы

Группа злоупотребляла поисковой рекламой Google для распространения программ-вымогателей, используя крупные бренды в качестве приманки, чтобы перенаправлять пользователей на вредоносные сайты. Также используются тактику социальной инженерии, такую как шпионский фишинг и звонки в службы поддержки для получения доступа к сетям.

E. Производственная и складская промышленность

AlphV связан с серией атак в различных секторах, включая производство. За последние 18 месяцев под атаку попало более 1000 жертв.

Известные атаки и воздействия

Формально сюда можно упомянутую ранее атаку на MGM Resorts International и использование Google Ads. ALPHV/BlackCat часто выдают себя за ИТ-специалистов компании и / или сотрудников службы поддержки и используют телефонные звонки или SMS-сообщения для получения доступа к системам.

Ещё одна атака совершена на Clarion, мирового производителя аудио- и видеооборудования для автомобилей и других транспортных средств. Группа утверждала, что произошла утечка конфиденциальных данных об их бизнесе и партнёрах, включая техническую информацию клиентов компании.

Организациям также следует знать, что группа нацелена как на устройства Windows, так и на Linux, а также на устройства хранения данных с сетевым подключением (NAS), которые часто используются для хранения резервных копий и конфиденциальных данных.

F. Государственные учреждения

AlphV оказала влияние на государственные учреждения и отрасль экстренных служб как разновидность критически важной инфраструктуры, вызывая сбои в работе и создавая угрозы национальной и общественной безопасности.

Известные атаки и воздействия

- **Нарушение работы критически важной инфраструктуры**: ALPHV была связана с атаками на критически важную инфраструктуру США, включая госучреждения и службы экстренной помощи.
- **Глобальный масштаб операций**: ALPHV/BlackCat стала вторым по распространённости вариантом программы-вымогателя "как услуга" в мире (RaaS). Её деятельность привела к значительным глобальным последствиям, в результате чего группа поставила под угрозу деятельность более 1000 юридических лиц по всему миру.
- **Финансовые последствия и выплаты выкупа**: Группа потребовала выкуп в размере более $500M и получила выплаты в размере почти $300M. Это финансовое воздействие подчёркивает прибыльный характер операций с программами-вымогателями,

нацеленных на критически важные сектора, включая госучреждения и службы экстренной помощи

Реакция правоохранительных органов

- **Кампания по дезорганизации Министерства юстиции**: Министерство юстиции в сотрудничестве с ФБР и международными партнёрами запустило кампанию по дезорганизации деятельности группы. Эта кампания была направлена на снижение угрозы, которую представляет программа-вымогатель для критически важной инфраструктуры, включая госучреждения и экстренные службы
- **Инструмент для расшифровки данных**: ФБР разработало инструмент для расшифровки данных, предоставляемый жертвам ALPHV, который помог сэкономить около $68M, позволив пострадавшим организациям восстановиться и возобновить операционную деятельность

G. Школьная индустрия

ALPHV нацелена на сектор образования, включая школы K-12, университеты и другие учебные заведения. Эти атаки нарушили образовательные процессы и поставили под угрозу конфиденциальные данные учащихся и персонала. Восприимчивость сектора к киберугрозам из-за часто ограниченных ресурсов и большого количества потенциальных противников кибербезопасности.

Известные атаки и воздействия

- **Участились атаки программ-вымогателей**: резко увеличилось количество атак на школы, число таких инцидентов увеличилось на 17%. Атаки включали шифрование файлов и угрозы утечки украденных данных, если не будет выплачен выкуп
- **Пострадали крупные школьные округа**: Школьные округа, такие как государственные школы Далласа и Миннеаполиса, были в числе крупных жертв атак программ-вымогателей.
- **Глобальный охват**: Атаки на школы не ограничивались США; образовательные учреждения в Соединенном Королевстве, Австралии, Германии, Франции и Бразилии также столкнулись с атаками программ-вымогателей
- **Влияние на образовательные операции**: Атаки на школы могут привести к значительным сбоям в работе, включая прерывание процесса подачи заявок, операций и занятий. В некоторых случаях нападения были достаточно серьёзными, чтобы привести к закрытию школ

Тактика и приемы

- **Двойное вымогательство**: операторы ALPHV часто используют тактику двойного вымогательства, при которой они шифруют файлы, а также угрожают утечкой украденных данных. Такой подход оказывает дополнительное давление на жертв, требуя выплатить выкуп
- **Использование уязвимостей**: Основной причиной атак в секторе образования является использование уязвимостей в устройствах, и отсутствие ресурсов для принятия надёжных мер кибербезопасности, что делает их восприимчивыми к таким атакам

H. Оборонно-промышленные предприятия

Особое внимание к оборонной промышленности подчёркивает стратегический подход группы к компрометации организаций, жизненно важных для национальной безопасности и экономической стабильности.

Известные атаки и воздействия

- **Атаки на критическую инфраструктуру**: Министерство юстиции (DOJ) определило компании оборонно-промышленной базы как один из секторов критической инфраструктуры, на которые нацелен вариант программы-вымогателя ALPHV.
- **Финансовые и операционные последствия**: Глобальные потери, связанные с ALPHV, которая использует модели атак с множественным вымогательством, привели к финансовым затратам.