Аннотация – В этом документе представлен анализ программы-вымогателя Bian Lian и охватывает множество аспектов программы-вымогателя, включая её оперативную тактику, технические характеристики и последствия её деятельности для кибербезопасности.

Анализ BianLian полезен специалистам по безопасности, ИТ-персоналу и организациям в различных отраслях. Он даёт им знания, необходимые для понимания ландшафта угроз, прогнозирования потенциальных векторов атак и внедрения надёжных механизмов безопасности для снижения рисков, связанных с атаками программ-вымогателей.

I. Введение

BianLian – это группа программ-вымогателей, которая действует с июня 2022 года в отношении организаций из критически важных секторов инфраструктуры в США и Австралии и известна разработкой, развёртыванием и использованием программ-вымогателей.

Агентство по кибербезопасности и инфраструктурной безопасности (CISA), Федеральное бюро расследований (ФБР) и Австралийский центр кибербезопасности (ACSC) выпустили рекомендации по снижению киберугроз от BianLian, включающие тактики, приёмы и процедуры (TTP), а также индикаторы компрометации (IoC), помогающие организациям защититься от атак.

Средний размер требований о выкупе, выдвигаемых BianLian, варьируется. Согласно отчёту BeforeCrypt, среднее требование о выкупе – в районе от 100 000 до 350 000 долларов. В отчёте Halcyon говорится, что требования о выкупе могут составлять в среднем около 3 миллионов долларов, и достигают 20 миллионов долларов. Coveware, консалтинговая фирма по безопасности, обнаружила, что средняя сумма выкупа за третий квартал 2023 года составила 850 700 долларов США

II. Профилирование

Известно, что группа нацелена на широкий спектр отраслей, включая финансовые учреждения, здравоохранение, производство, образование, развлечения и энергетический сектор. BianLian обычно атакует важные цели из самых разных областей. К ним относятся здравоохранение, финансы, государственное управление, образование, юриспруденция и профессиональные услуги. Группа также уделяет большое внимание сектору образования. Группа ориентирована на различные отрасли, включая, но не ограничиваясь ими: здравоохранение, образование, госструктуры, профессиональные услуги, производство, СМИ и развлечения, банковские и финансовые услуги, энергетический сектор.

В секторе здравоохранения распространёнными точками входа для BianLian являются серверы, ПК, базы данных и медицинские записи. Растущую озабоченность вызывает нацеленность на медицинские устройства, а не только на сети. Это связано с конфиденциальными данными, хранящимися в этих устройствах, включая интеллектуальную собственность, коммерческую тайну, личные данные и медицинские записи. В 2023 году в секторе здравоохранения по всему миру произошло более 630 инцидентов с программами-вымогателями, причем более 460 из них затронули США

В сфере образования часто используют устаревшее ПО с известными проблемами безопасности в качестве точки входа. Это связано с неадекватным управлением исправлениями, что делает системы уязвимыми для атак. Поэтому BianLian нацелена на образовательные учреждения, используя эти уязвимости для получения несанкционированного доступа к их системам.

Для государственных организаций точки входа в BianLian аналогичны. Они используют уязвимости для перемещения по взломанным сетям незамеченными, используя специально разработанное вредоносное ПО. Они также нацелены на протокол удалённого рабочего стола (RDP) и другие инструменты удалённого доступа.

Для производственных BianLian обычно использует известные уязвимости в системах, подключённых к Интернету. Для этих организаций крайне важно уделять приоритетное внимание исправлению этих уязвимостей, чтобы предотвратить атаки. BianLian также нацелен на системы с использованием учётных RDP.

В организациях, оказывающих профессиональные услуги, BianLian часто получает первоначальный доступ через профессиональные услуги и действительные учётные данные RDP в качестве общей точки входа. Кроме того, было замечено, что группа использовала компрометацию электронной почты (BEC) в качестве средства доставки.

В энергетических организациях BianLian использует различные тактики, включая фишинговые кампании и использование уязвимостей, для получения несанкционированного доступа и шифрования файлов с целью получения выкупа. Также было замечено, что группа использует уязвимость Netlogon (CVE-2020–1472) для подключения к Active Directory.

III. Как работает BianLian

Группа обычно проникает, используя актуальные учётные данные RDP. Затем эксплуатируются известные уязвимости и используются инструменты для обнаружения и сбора учётных данных. Оказавшись внутри, отключаются антивирусное программное обеспечение, и изменяют настройки системы.

Программа-вымогатель шифрует файлы и добавляет к ним расширение .bianlian, оставляя в каждом затронутом каталоге записку с требованием выкупа под названием "Look at this instruction.txt". Первоначально группа следовала модели двойного вымогательства, при которой они шифровали системы жертв после извлечения данных. Однако с января 2023 года они перешли к модели вымогательства, основанной в основном на эксфильтрации (через протокол передачи файлов (FTP), Rclone или Mega file-sharing services).

Однако в январе 2023 года группа изменила свою тактику. Вместо систем шифрования они перешли к модели вымогательства, основанной на эксфильтрации. Этот сдвиг совпал с выпуском Avast дешифратора для программы-вымогателя. В этой новой модели группа продолжает красть данные, но больше не шифрует системы жертвы. Затем они угрожают обнародовать украденные данные, если не будет выплачен выкуп.

IV. Признаки BianLian атаки

- **Сообщение о выкупе**: Жертвы обычно получают сообщение о шифровании или эксфильтрации данных с требованием выкупа (файл «Look at this instruction»)
- **Расширения файла**: Расширения файлов в заражённой системе изменены на ".bianlian"
- **Звонки с угрозами**: Сотрудники компаний-жертв сообщали о получении телефонных звонков с угрозами от лиц, связанных с группой
- **Криптовалютные кошельки**: BianLian получает платежи в уникальных криптовалютных кошельках для каждой компании-жертвы
- **Быстрое шифрование**: BianLian известна своей исключительной скоростью шифрования файлов
- **Эксфильтрация данных**: группа крадёт данные жертвы по протоколу передачи файлов (FTP), Rclone или Mega, а затем вымогает деньги, угрожая разглашением данных, если оплата не будет произведена
- **Spearphishing Emails**: Первоначальный доступ к целевой системе часто достигается с помощью электронных писем, содержащих вредоносные вложения или ссылки.
- **Использование протокола удалённого рабочего стола (RDP)**: Группа часто получает доступ к системам-жертвам с помощью действительных учётных данных RDP
- **Системные изменения и низкая производительность**: BianLian может вызывать заметные системные изменения и снижать производительность заражённой системы

V. Начальные векторы доступа

- **Разведка**: для выполнения сетевой разведки BianLian использует такие инструменты, как Advanced Port Scanner, SoftPerfect Network Scanner, SharpShares и PingCastle.
- **Скомпрометированные учётные данные RDP**: Группа использует скомпрометированные учётные данные RDP для получения начального доступа к сетям. Они используют эти действующие учётные записи для доступа к сетям целей через RDP
- **Spearphishing Emails**: Первоначальный доступ к целевой системе часто достигается с помощью электронных писем, содержащих вредоносные вложения или ссылки.
- **Использование уязвимостей**: В ландшафте угроз произошёл сдвиг: операторы программ-вымогателей, включая BianLian, все чаще используют известные уязвимости для получения первоначального доступа
- **Внешние удалённые службы**: BianLian использует слабые места в доступных извне удалённых службах, таких как RDP, чтобы закрепиться в целевых сетях
- **Использование недостатков ProxyShell**: известно, что группа использовала уязвимости ProxyShell для получения первоначального доступа к сетям
- **Использование брокеров начального доступа (IAB)**: были случаи, когда компания BianLian использовала брокеров, которые специализируются на получении начального доступа к сетям и последующей продаже этого доступа другим субъектам угроз

VI. IoCs

Индикаторы компрометации (IoC), связанные с BianLianскими атаками программ-вымогателей, могут предоставить ценную информацию для обнаружения этих угроз и реагирования на них. Хотя конкретные IOC могут различаться в зависимости от конкретной атаки, некоторые общие IOC, связанные с программой-вымогателем BianLian, включают:

- **Хэши SHA-256**: идентифицированы конкретные хэши, связанные с BianLian (например, anabolic.exe (46d340eaf6b78207e24b6011422f1a5b4a566e493d72365c6a1cace11c36b28b 64-разрядный исполняемый файл, скомпилированный с Golang версии 1.18.3.)
- **IP-адреса**: Определённые IP-адреса были связаны с атаками BianLian с помощью программ-вымогателей, например 104.207.155[.]133

- **Изменения файлов**: изменяются расширения всех зашифрованных файлов, добавляя .bianlian
- **Записка с требованием выкупа**: Наличие записки с требованием выкупа в каждом уязвимом каталоге
- **Сетевой трафик**: Необычный сетевой трафик, поступающий на известные вредоносные IP-адреса или домены, связанные с BianLian, например использовался netsh для добавления правила брандмауэра для открытия 3389 на RDP
- **Системные изменения**: Изменения в системных настройках или отключение антивирусного программного обеспечения, в т.ч. встроенного

VII. C2C ИНФРАСТРУКТУРА

- **Использование легитимного программного обеспечения удалённого доступа**: было замечено, использование ПО удалённого доступа, такое как TeamViewer, Atera и AnyDesk для установления интерактивных каналов командования и контроля
- **Расширение инфраструктуры**: Группа быстро расширяет свою инфраструктуру уровня C2, что свидетельствует об увеличении темпов работы
- **Пользовательский бэкдор на основе Go**: после получения доступа к сети группа развёртывает пользовательский бэкдор на основе Go, специфичный для каждой жертвы
- **Использование сценариев PowerShell**: Группа использует сценарии PowerShell для различных действий, включая эксфильтрацию данных
- **Использование инструментов с открытым исходным кодом и сценариев командной строки**: Группа использует инструменты с открытым исходным кодом для обнаружения и сбора данных
- **Использование IP-адресов**: Группа использует различные IP-адреса для своей инфраструктуры C2. Например, IP-адрес 104.207.155[.]133 был связан с деятельностью группы

VIII. СЕТЕВЫЕ УЯЗВИМОСТИ

BianLian использует уязвимости в сетях с помощью различных методов. Первоначальный доступ часто достигается с помощью электронных писем, содержащих вредоносные вложения, или путём использования известных уязвимостей в системах и сервисах. Известно, что группа использовала действительные учётные данные протокола удалённого рабочего стола (RDP) и эксплойты для уязвимостей, таких как CVE-2020–1472. Это критическая уязвимость в удалённом протоколе Netlogon от Microsoft, который используется для различных задач, связанных с аутентификацией пользователей и компьютеров. Было замечено, чтопрограмма-вымогатель BianLian использует эту уязвимость для получения несанкционированного доступа к доменам Windows. Они также используют разведывательные вредоносные программы и пользовательские бэкдоры.

Оказавшись внутри сети, BianLian использует такие инструменты, как PsExec и RDP, наряду с действительными учётными записями для распространения. Они используют командную оболочку и собственные инструменты Windows для добавления учётных записей пользователей на локальный удалённый рабочий стол, изменения пароля добавленной учётной записи и настройки правил брандмауэра Windows для разрешения входящего трафика RDP.

Группа также развёртывает пользовательский бэкдор на основе Go, специфичный для каждой жертвы, и устанавливает инструменты удалённого управления, такие как AnyDesk, SplashTop и TeamViewer. Они используют сценарии PowerShell для сбора данных, которые затем передаются по FTP и через Rclone.

IX. ПО УДАЛЁННОГО ДОСТУПА, ИСПОЛЬЗУЕМОЕ BIANLIAN

BianLian использует различные программы для создания инфраструктуры C2 поскольку эти инструменты обычно используются в легитмных целях, таких как предоставление удалённой технической поддержки.

- **TeamViewer**: широко используемое программное обеспечение для удалённого доступа и удалённого управления, которое позволяет пользователям удалённо управлять компьютерами через Интернет
- **Atera**: платформа удалённого ИТ-управления, разработанная для поставщиков управляемых услуг (MSP), которая обеспечивает удалённый мониторинг и управление (RMM), автоматизацию профессиональных услуг (PSA) и возможности удалённого доступа
- **SplashTop**: инструмент удалённого доступа, который позволяет пользователям подключаться к компьютерам и управлять ими с любого устройства
- **AnyDesk**: программное обеспечение для удалённого рабочего стола, которое обеспечивает удалённый доступ к персональным компьютерам, на которых запущено основное приложение

Использование ПО RDP позволяет группе удалённо управлять скомпрометированными системами, выполнять команды и совершать вредоносные действия. В обоих случаях группа развёртывает пользовательский бэкдор на основе Go, специфичный для каждой жертвы, после получения доступа к сети. Этот бэкдор позволяет субъекту угрозы устанавливать инструменты удалённого управления, и закрепления. Группа также создаёт или активирует учётные записи администраторов и меняет их пароли для дальнейшей защиты доступа.

A. TeamViewer и AnyDesk

TeamViewer и AnyDesk пользуются популярностью у BianLian благодаря своим надёжным функциям, облегчающим удалённый доступ и контроль, которые могут быть использованы в вредоносных целях.

- **Широкое использование и простота доступа**: TeamViewer и AnyDesk установлены на сотнях миллионов устройств по всему миру, более чем на

400 миллионах устройств работает программное обеспечение, из которых 30 миллионов подключены к TeamViewer в момент времени.

- **Удалённая поддержка и доступ**: обеспечивается удалённую поддержку, совместная работу и доступ к конечным устройствам. Эта функция позволяет злоумышленникам удалённо получить контроль над окружением жертвы.
- **Управление активами**: TeamViewer и AnyDesk предлагают возможности управления активами, позволяющие удалённо управлять обновлениями программного обеспечения, системы и развёртыванием исправлений.
- **Интеграция с другими инструментами удалённого доступа**: TeamViewer и AnyDesk интегрируются с другими инструментами удалённого доступа, такими как Splashtop и AnyDesk, предоставляя дополнительные пути доступа к скомпрометированным системам и контроля над ними.
- **Меры безопасности**: несмотря на меры безопасности AnyDesk и TeamViewer, злоумышленники нашли способы использовать инструмент даже несмотря на аспекты сложных паролей, двухфакторной аутентификации, списков разрешений и обновлений ПО для предотвращения несанкционированного доступа.

B. Atera

Atera пользуется популярностью у гр BianLian из-за его надёжных функций и возможностей, которые могут быть использованы во вредоносных целях:

- **Удалённый мониторинг и управление (RMM)**: Atera обеспечивает мониторинг и оповещения в режиме реального времени, автоматизацию ИТ, управление исправлениями и расширенное удалённое обслуживание. Это позволяет BianLian group отслеживать взломанные системы и управлять ими в режиме реального времени.
- **Встроенный удалённый доступ**: Atera интегрируется с Splashtop и AnyDesk, предоставляя возможности удалённого доступа. Это позволяет BianLian group получать удалённый доступ к скомпрометированным системам и управлять ими.
- **Управление активами и товарно-материальными запасами**: Atera предоставляет возможности управления активами и товарно-материальными запасами. Это может предоставить ценную информацию о взломанных системах.
- **Автоматизация профессиональных услуг (PSA)**: Atera включает в себя такие возможности, как оформление билетов, выставление счетов и создание отчётов. Хотя эти функции предназначены для ИТ-специалистов, они могут быть злонамеренно использованы BianLian.
- **Возможности искусственного интеллекта**: Atera включает в себя возможности искусственного интеллекта. Хотя конкретное использование этих возможностей группой BianLian неясно, они потенциально могут быть использованы в злонамеренных целях.
- **Создание сценариев**: Atera позволяет создавать сценарии, которые могут быть очень полезны для BianLian group для автоматизации определённых задач в скомпрометированных системах

C. Splashtop

Splashtop является популярным выбором BianLian благодаря надёжным функциям безопасности, часть из которых напрямую используется для управления устройством, обхода механизмов, закрепления, сокрытия и обеспечения защиты на уровне канала:

- **Меры безопасности**: используется шифрование, аутентификация пользователей и устройств, а также множество других мер безопасности. Все удалённые сеансы шифруются сквозным способом с помощью TLS и 256-битного AES. Он также включает в себя такие функции, как двухфакторная аутентификация, многоуровневая защита паролем, пустой экран, автоматическая блокировка экрана, время ожидания сеанса и уведомление об удалённом подключении
- **Простота настройки и использования**: Splashtop прост в настройке и использовании, что делает его удобным инструментом для удалённого доступа. Он работает независимо от устаревшей ИТ-инфраструктуры, его настройка занимает всего несколько минут.
- **Splashtop Connector**: функция обеспечивает удалённый доступ к компьютерам, которые обычно доступны только в локальной сети. Это позволяет пользователям подключаться к компьютерам, поддерживающим протокол RDP, непосредственно из Splashtop, без использования VPN или установки какого-либо агента удалённого доступа
- **Детализированные разрешения**: Splashtop предлагает детализированные разрешения, позволяющие ИТ-подразделениям иметь полный контроль над защитой данных
- **Аутентификация устройства**: Эта функция добавляет дополнительный уровень безопасности, гарантируя, что только аутентифицированные устройства могут получить доступ к сети
- **Единый вход (SSO)**: Эта функция упрощает процесс входа в систему, облегчая пользователям безопасный доступ к своим системам
- **Модуль доступа по расписанию**: Эта функция позволяет ИТ-подразделениям управлять расписаниями и политиками, определяющими, когда пользователи и группы пользователей могут получить доступ к определённым конечным точкам