НИЧТО ТАК НЕ ГОВОРИТ О ИБ, КАК СОТНИ ИБ-ПРОДУКТОВ И БИОМЕТРИЧЕСКИЙ СКАНЕР

ХРОНИКИ БЕЗОПАСНИКА

ДАЙДЖЕСТ. 2024 / 05

Добро пожаловать в очередной выпуск ежемесячного сборника материалов, который является вашим универсальным ресурсом для получения информации о самых последних разработках, аналитических материалах и лучших практиках в постоянно развивающейся области безопасности. В этом выпуске мы подготовили разнообразную подборку статей, новостей и результатов исследований, рассчитанных как на профессионалов, так и на обычных любителей. Цель нашего дайджеста - сделать наш контент интересным и доступным. Приятного чтения!

Больше контента:

BOOSTY.TO

SPONSR.RU

TELEGRAM

Рубрика: Новичок

Для новичков в мире ИБ или для тех, кто предпочитает работать с контентом без финансовых обязательств.

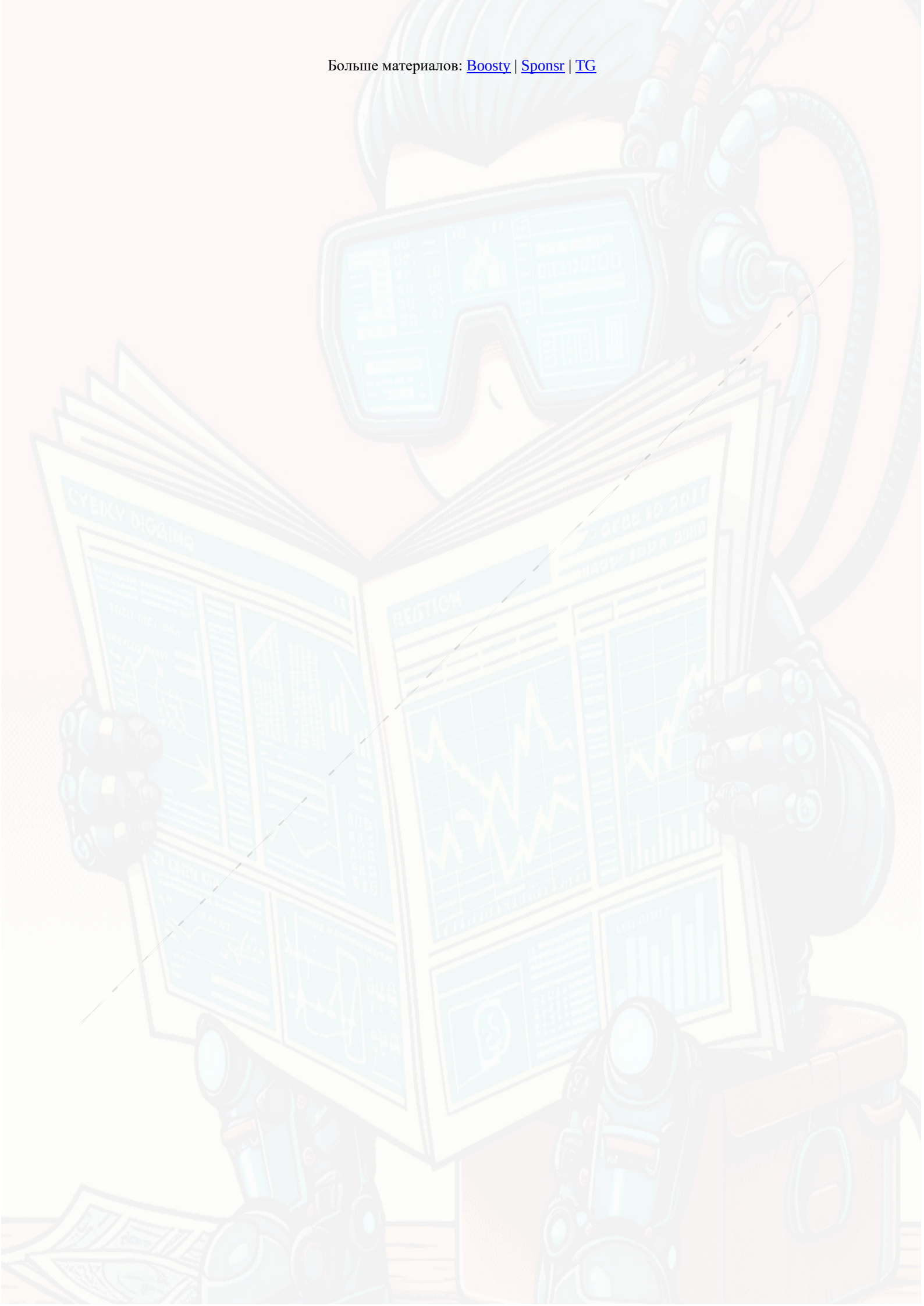
Рубрика: Специалист

Для постоянных читателей, которые заинтересованы быть в курсе последних тенденций в мире кибербезопасности

Рубрика: Профессионал

Для ИТ-специалистов, экспертов, и энтузиастов, которые готовы погрузится в сложный мир ИБ.

Больше материалов: Boosty | Sponsr | TG



Новости

Больше материалов: Boosty | Sponsr | TG

BatBadBut

📌 **Идентификация уязвимости:** Критическая уязвимость идентифицируется как "BatBadBut" CVE-2024–24576

📌 **Уязвимое ПО:** Уязвимость существует в стандартной библиотеке Rust и, в частности, затрагивает системы Windows

📌 **Степень критичности:** присвоена наивысшая оценка по шкале CVSS, равная 10,0, что указывает на максимальную степень тяжести

📌 **Подробная информация**: Уязвимость возникает из-за того, что стандартная библиотека Rust неправильно экранирует аргументы при вызове пакетных файлов в Windows с использованием командного API. Это может позволить злоумышленнику выполнять произвольные команды оболочки, обходя экранирующий интерфейс.

📌 **Условия:** выполнение команды в Windows, команда не указывает расширение файла или использует .bat или .cmd, команда содержит управляемый пользователем ввод в качестве части аргументов команды, а среда выполнения не может должным образом обработать аргументы команды для cmd.exe

📌 **Уязвимые версии:** Все версии Rust для Windows до версии 1.77.2 подвержены этой уязвимости

📌 **Воздействие:** Уязвимость также затрагивает другие языки программирования, включая Erlang, Go, Haskell, Java, Node.js, PHP, Python и Ruby, хотя исправления выпущены не для всех из них

📌 **Рекомендации по устранению:** Пользователям рекомендуется перемещать пакетные файлы в каталог, не указанный в переменной среды PATH, чтобы предотвратить непредвиденное выполнение. Разработчикам следует перейти на версию Rust 1.77.2, чтобы устранить уязвимость

📌 **Обнаружение и отчётность**: Уязвимость была обнаружена инженером по безопасности из Flatt Security, известным как RyotaK, и передана в Координационный центр сертификации (CERT/CC).

📌 **Ответ от Rust:** Rust признала проблему и с тех пор улучшила надежность экранирующего кода и модифицировала командный API, чтобы возвращать ошибку InvalidInput, если аргумент не может быть безопасно экранирован

📌 **Реакция разработчиков других языков:** Разработчики Haskell, Node.js, PHP и yt-dlp выпустили исправления для устранения ошибки, связанной с внедрением команд

Уязвимости LG's WebOS / LG SmartTV

Исследователи из Bitdefender выявили множество уязвимостей в WebOS от LG, влияющих на различные модели смарт-телевизоров компании. Использование этих уязвимостей может позволить злоумышленникам получить несанкционированный root-доступ к устройствам.

Уязвимые версии и модели:

📌 Уязвимости затрагивают телевизоры LG, работающие под управлением WebOS версий с 4.9.7 по 7.3.1, в таких моделях, как LG43UM7000PLA, OLED55CXPUA, OLED48C1PUB и OLED55A23LA

Конкретные уязвимости:

📌 **CVE-2023-6317:** Позволяет обойти проверку PIN-кода и добавить профиль привилегированного пользователя без участия пользователя

📌 **CVE-2023-6318:** Позволяет повысить свои привилегии и получить root-доступ

📌 **CVE-2023-6319**: Позволяет внедрять команды операционной системы, манипулируя библиотекой для отображения музыкальных текстов

📌 **CVE-2023-6320**: Позволяет вводить команды, прошедшие проверку подлинности, используя com.webos.конечная точка API service.connectionmanager/tv/setVlanStaticAddress

Масштабы воздействия:

📌 Более 91 000 устройств были идентифицированы как потенциально уязвимые в Южной Корее, Гонконге, США, Швеции и Финляндии

Меры по устранению уязвимостей и действия пользователей:

📌 Компания LG выпустила исправления для этих уязвимостей, которые доступны в меню настроек телевизора в разделе "Обновление программного обеспечения"

📌 Пользователям рекомендуется включить автоматическое обновление ПО, чтобы обеспечить получение на свои устройства последних исправлений безопасности

Потенциальные риски:

📌 Эти уязвимости позволяют получить контроль над телевизором, получить доступ к конфиденциальным пользовательским данным и потенциально использовать скомпрометированное устройство как часть ботнета или для других вредоносных действий

Рекомендации по безопасности:

📌 Помимо применения последних обновлений встроенного ПО, пользователи должны использовать надежные уникальные пароли для своих устройств и защищать свои сети Wi-Fi, чтобы еще больше снизить риск их использования

Больше материалов: Boosty | Sponsr | TG

TA547 ФИШИНГОВАЯ КАМПАНИЯ

Фишинговая кампания TA547 с использованием Rhadamanthys stealer представляет собой эволюцию в тактике киберпреступников, в частности, благодаря интеграции сценариев, созданных с помощью ИИ.

Детали

📌**Имитация и содержимое электронной почты:** Фишинговые электронные письма были созданы для того, чтобы выдавать себя за немецкую компанию Metro AG, и сообщения, связанные со счетами. Эти электронные письма содержали защищённый паролем ZIP-файл, который при открытии запускал удалённый сценарий PowerShell

📌**Способ выполнения:** Скрипт PowerShell выполняется непосредственно в памяти, развёртывая Rhadamanthys stealer без записи на диск. Этот метод помогает избежать обнаружения традиционным антивирусным программным обеспечением

📌**Использование ИИ при создании вредоносных программ:** Есть явные признаки того, что скрипт PowerShell был создан или, по крайней мере, доработан с использованием большой языковой модели (LLM). Скрипт содержал грамматически правильные и очень специфичные комментарии, что нетипично для скриптов вредоносных программ, созданных человеком

TTPs

📌 **Инновационные приманки и методы доставки:** В рамках кампании также были опробованы новые тактики фишинга, такие как уведомления о голосовых сообщениях и встраивание изображений в формате SVG, для повышения эффективности атак по сбору учётных данных

📌**ИИ:** Использование технологий ИИ, таких как ChatGPT или CoPilot, при написании сценариев вредоносного ПО указывает на значительный сдвиг в тактике киберпреступности, предполагая, что киберпреступники все чаще используют ИИ для совершенствования своих методов атаки

📌**Последствия:** кампания не только подчёркивает адаптивность и техническую сложность TA547, но и подчёркивает тенденцию к внедрению инструментов ИИ в свою деятельность. Эта интеграция потенциально может привести к повышению эффективности и сложности обнаружения кибер-угроз

Рекомендации по защите

📌**Обучение сотрудников**: Организациям следует повысить уровень кибербезопасности, обучив сотрудников распознавать попытки фишинга и подозрительный контент электронной почты

📌**Технические меры предосторожности:** Внедрение строгих групповых политик для ограничения трафика из неизвестных источников и рекламных сетей может помочь защитить конечные точки от таких атак.

📌**Обнаружение, основанное на поведении:** Несмотря на использование искусственного интеллекта при разработке атак, механизмы обнаружения, основанные на поведении, остаются эффективными при выявлении и смягчении таких угроз

FBI IC3

Злоумышленники используют различные методы, включая фишинговые электронные письма с вредоносными вложениями, обфусцированные файлы сценариев и Guloader PowerShell, для проникновения в системы жертв и их компрометации. Мошенничество с выставлением счетов, форма взлома деловой электронной почты (BEC), является одним из популярных методов, используемых злоумышленниками для обмана жертв. В этом типе мошенничества третья сторона запрашивает оплату обманным путём, часто выдавая себя за законного поставщика

Мошенничество со счетами-фактурами представляет серьёзную угрозу для бизнеса, поскольку может привести к значительным финансовым потерям и непоправимому ущербу. Согласно отчёту ФБР IC3, в 2022 году атаки BEC нанесли ущерб жертвам в США на сумму 2,7 миллиарда долларов, что сделало их наиболее распространённой формой компрометации деловой электронной почты

Некоторые признаки мошеннических электронных счетов-фактур включают запросы на предоставление личной информации (PII), запросы на изменение банковской или платёжной информации, и счета-фактуры с необычными суммами. Кроме того, злоумышленники часто используют методы обфускации, чтобы обойти защиту и затруднить обнаружение своих вредоносных действий.

TELETRACKER

TeleTracker предлагает набор инструментов для анализа данных об угрозах, ориентированных на каналы Telegram, используемые во вредоносных целях. Его функции облегчают мониторинг и пресечение активных вредоносных кампаний, что делает его ценным ресурсом для специалистов в области кибербезопасности. Эти скрипты особенно полезны для аналитиков по анализу угроз или исследователей, стремящихся отслеживать, собирать и выслеживать злоумышленников, используя Telegram для C2-целей.

Особенности

📌**Просмотр сообщений канала и загрузка содержимого:** позволяет просматривать сообщения в канале и загружать содержимое непосредственно во вновь созданную папку "загрузки" в текущем рабочем каталоге. Программа поддерживает загрузку различных типов файлов, включая документы, фотографии и видео.

📌**Отправка документов через Telegram**: Пользователи могут дополнительно отправлять сообщения и документы через Telegram, поддерживая все типы файлов Telegram с автоматическим определением типа MIME.

📌**Выбор сообщения:** предоставляет возможность выбрать указанное количество сообщений или определённый идентификатор сообщения для загрузки, при этом загрузка всегда происходит от самого нового к самому старому сообщению.

📌**Сохранение логов:** сохраняет логи в удобном текстовом формате с основной информацией в файле с именем <имя_бота>.txt.

Больше материалов: Boosty | Sponsr | TG

Использование

📌 Чтобы отправить сообщение в Telegram-канал: python TeleTexter.py -t YOUR_BOT_TOKEN -c YOUR_CHAT_ID -m "сообщение"

📌 Для непрерывной отправки сообщений (рассылки спама) флаг --spam.

📌 TeleViewer.py это новейший инструмент, позволяющий пользователям просматривать и загружать все сообщения и медиафайлы из контролируемого Telegram-канала, контролируемого threat actor. Доступ к этой функции можно получить, выбрав цифру 6 в начальном меню после запуска TeleGatherer.py.

WSUS: ADCS ESC8 атака через MITM

Статья служит техническим руководством о том, как сочетание сетевого перехвата, MITM-атак и использования ADC-систем может привести к значительным нарушениям безопасности, подчёркивая необходимость принятия надёжных мер безопасности в сетевых конфигурациях и процессах обработки сертификатов.

📌 **Конфигурация и уязвимости WSUS:** В статье подробно описывается, как можно использовать сервер служб обновления Windows Server (WSUS), настроенный для работы по протоколу HTTP. Доступ к конфигурации протокола WSUS-сервера можно получить, запросив определённый раздел реестра. Эта настройка позволяет потенциально перехватывать трафик с помощью таких инструментов, как Wireshark, которые могут перехватывать связь между клиентами и сервером WSUS.

📌 **Выполнение MITM-атаки:** В основе атаки лежит подход "Человек посередине" (MITM), при котором злоумышленник перехватывает и ретранслирует запросы с клиентского компьютера на сервер WSUS. Во время этого процесса злоумышленник может манипулировать сообщениями, перенаправляя запросы на сторонний сервер или манипулируя ответами.

📌 **Эксплойт ADCS ESC8:** Перехваченное сообщение затем используется для проведения атаки на службы сертификации Active Directory (ADCS) ESC8. Это включает в себя передачу перехваченных запросов на веб-страницу регистрации Центра сертификации для запроса сертификата с использованием учётных данных скомпрометированного компьютера. Успешное выполнение этой атаки может позволить злоумышленнику получить несанкционированные сертификаты, которые могут быть использованы для дальнейших атак в сети.

📌 **Набор инструментов:** PKINITtools и скрипты для управления запросами Kerberos и их экспорта помогают извлекать и использовать учётные данные из перехваченного трафика для проверки подлинности с помощью ADC и запроса сертификатов.

📌 **Рекомендации по обеспечению безопасности:** Атака демонстрирует значительный риск для безопасности, связанный с использованием незащищённых протоколов (HTTP) для критически важной инфраструктуры, такой как WSUS и ADCS. В статье предполагается, что защита этих коммуникаций с помощью HTTPS и внедрение строгого контроля доступа и мониторинга могут снизить вероятность таких атак.

Разбитые мечты о ключах доступа

В статье представлен критический взгляд на реализацию и удобство использования ключей доступа, особенно в контексте WebAuthn (веб-аутентификации). Автор делится личным анекдотом, чтобы осветить проблемы, с которыми сталкиваются пользователи, что приводит к более широкой критике паролей доступа.

📌 **Личный опыт, связанный с отказом ключа доступа:** Автор начинает с личной истории, в которой его партнёр не смог получить доступ к своей домашней системе управления освещением, потому что с брелка Apple был удалён ключ доступа, который она использовала. Этот инцидент служит примером практических проблем, с которыми сталкиваются пользователи при использовании ключей доступа.

📌 **Критика эволюции WebAuthn:** Автор размышляет об их участии в WebAuthn, начиная с первых дней его существования. Они рассказывают о своем оптимизме и вкладе в работу рабочей группы WebAuthn, направленной на улучшение стандарта. Однако они выражают разочарование тем, как развивалась технология, особенно критикуя концепцию и реализацию паролей доступа.

📌 **Пароли доступа как инструмент блокировки платформы:** В статье утверждается, что пароли доступа, вместо того чтобы быть решением для безопасной и удобной аутентификации, стали для платформ средством привязки пользователей к своим экосистемам. Невозможность извлечения или экспорта учётных данных выделяется как существенный недостаток, приводящий к тому, что автор описывает как "долгосрочное заманивание пользователей в ловушку".

📌 **Проблемы, связанные с работой пользователей:** Автор делится негативным опытом своей партнёрши по работе с паролями доступа, отмечая, что она предпочитает вернуться к традиционным паролям из-за их простоты и надёжности. Это мнение разделяет автор, который неохотно признает, что менеджеры паролей обеспечивают лучший пользовательский опыт, чем пароли доступа.

📌 **Заключение и размышления:** В заключение автор выражает чувство разочарования в паролях доступа, предполагая, что первоначальное обещание безопасного и удобного для пользователя метода аутентификации было нарушено. Они намекают на иронию ситуации с выпуском новой версии своей библиотеки WebAuthn для Rust на фоне этих размышлений.

Lock Bit и конфиденциальные данные, украденные из больницы в Каннах во Франции

📌 LockBit является самой опасной программой-вымогателем в мире и несёт ответственность за значительное количество атак во Франции в период с апреля 2022 по март 2023 года.

📌 За этот период на LockBit пришлось 57% известных атак во Франции, что значительно выше, чем на его ближайшего конкурента, ALPHV.

Больше материалов: Boosty | Sponsr | TG

📌 Количество ежемесячных атак во Франции было крайне нестабильным, и большая часть этой волатильности приходилась на LockBit.

📌 Французская экономика достаточно велика, чтобы стать благодатной почвой для киберпреступников, и вполне возможно, что некоторые из филиалов LockBit решили специализироваться на атаках на французские объекты.

📌 В июле 2022 года оператор мобильной связи La Poste Mobile, принадлежащий французской почтовой компании La Poste, подвергся атаке программы-вымогателя LockBit, в результате которой была опубликована личная информация более полутора миллионов человек во Франции.

📌 В августе 2022 года злоумышленники потребовали 10 миллионов долларов после атаки программы-вымогателя на Center Hospitalier Sud Francilien (CHSF), больницу на 1000 коек недалеко от Парижа, что привело к сбоям в работе компьютерных систем и привело к тому, что пациентов пришлось отправлять в другое место, а операции были отложены.

📌 В середине ноября 2022 года французская оборонная и технологическая группа Thales подтвердила утечку данных, повлиявшую на контракты и партнёрские отношения в Малайзии и Италии, при этом злоумышленники использовали программу-вымогатель LockBit.

📌 В период с апреля 2022 по март 2023 года Франция занимала пятое место в мире по числу нападений, причём государственный сектор подвергался нападениям чаще, чем в аналогичных странах.

📌 Причины доминирования LockBit во Франции неясны, но это может быть связано со способностью группы использовать возможности за пределами Англосферы и возможностью того, что некоторые из её филиалов специализировались на атаках на французские объекты.

📌 LockBit работает по модели "Программа-вымогатель как услуга" (RaaS), при этом атаки осуществляются независимыми преступными группировками, называемыми "аффилированными лицами", которые платят банде LockBit 20% от получаемого ими выкупа.

📌 Истинное количество атак LockBit, вероятно, намного превышает количество известных атак, поскольку многие жертвы предпочитают заплатить выкуп, а не рисковать публикацией своих данных в даркнете.

📌 LockBit был связан с атаками на больницы, правительства и предприятия по всему миру, которые нанесли значительный ущерб тысячам жертв.

📌 Правоохранительные органы работают над пресечением деятельности LockBit, и несколько человек, предположительно связанных с бандой, были арестованы в Украине и Польше.

📌 Несмотря на эти усилия, LockBit продолжает действовать и совершать нападения, а предполагаемый лидер группы клянётся продолжать свою деятельность.

📌 Государственный департамент США объявил о денежном вознаграждении в размере до 15 миллионов долларов за информацию, которая может привести к выявлению ключевых лидеров группы вымогателей LockBit и аресту любого лица, участвующего в операции.

📌 С января 2020 года злоумышленники LockBit совершили более 2000 атак на жертв в США и по всему миру, что привело к дорогостоящим сбоям в работе и уничтожению или утечке конфиденциальной информации.

📌 Было выплачено более 144 миллионов долларов в качестве выкупа за восстановление после событий, связанных с программой-вымогателем LockBit.

📌 В ответ на требование о выкупе CHC-SV заявила: "Государственные учреждения здравоохранения никогда не платят выкуп перед лицом атак такого типа".

📌 Больница также пообещала уведомить пациентов и заинтересованные стороны, если банда вымогателей решит опубликовать какие-либо украденные данные.

📌 На момент подготовки настоящего отчёта от Каннской больницы не поступало никаких заявлений относительно якобы опубликованных данных.

Genzai - IoT инструментарий

Репозиторий Genzai на GitHub, разработанный umair9747, направлен на повышение безопасности Интернета вещей путём выявления связанных с IoT информационных панелей и сканирования их на наличие паролей по умолчанию и уязвимостей.

📌 **Назначение и функциональность:** Genzai предназначен для повышения безопасности устройств Интернета вещей путём идентификации информационных панелей Интернета вещей, доступных через Интернет, и сканирования их на наличие распространённых уязвимостей и паролей по умолчанию (например, admin:admin). Это особенно полезно для защиты административных панелей устройств автоматизации и других IoT-продуктов.

📌 **Fingerprint и сканирование:** инструментарий делает fingerprint с продуктов Интернета вещей, используя набор подписей из файла signatures.json. После идентификации продукта он использует шаблоны, хранящиеся в его базах данных (vendor-logins.json и vendor-vulns.json) для поиска паролей по умолчанию для конкретного поставщика и потенциальных уязвимостей.

📌 **Поддерживаемые устройства и функции:** По состоянию на последнее обновление, Genzai поддерживает снятие отпечатков пальцев с более чем 20 различных информационных панелей на базе Интернета вещей. В него также включены шаблоны для проверки на наличие проблем с паролями по умолчанию в этих информационных панелях. Кроме того, доступно 10 шаблонов уязвимостей, и в будущих обновлениях планируется расширить это число. Некоторые из устройств Интернета вещей, которые можно сканировать, включают беспроводные маршрутизаторы, камеры наблюдения, человеко-машинные интерфейсы (HMI), интеллектуальные системы управления питанием, системы контроля доступа в здания, климат-контроль, системы промышленной автоматизации, домашней автоматизации и системы очистки воды.

📌 **Обновления и контактная информация:** В репозитории указано, что Genzai является активно поддерживаемым проектом, в ближайшие обновления планируется добавить больше шаблонов уязвимостей.

Больше материалов: Boosty | Sponsr | TG

UserManagerEoP / CVE-2024-21447

Эксплойт UserManager EoP нацелен на уязвимость, идентифицированную как CVE-2023–36047, которая позже была отслежена как CVE-2024–21447 после дополнительных исправлений Microsoft.

Эксплойт UserManager EoP

📌 **Обнаружение уязвимости:** Эксплойт был обнаружен владельцем репозитория в прошлом году и влияет на работу службы UserManager в Windows.

📌 **Характер уязвимости:** Уязвимость заключается в том, что служба UserManager неправильно копирует файлы из каталога, которым может управлять пользователь, что приводит к повышению уровня привилегий (EoP).

📌 **Частичное исправление и повторное использование:** Изначально Microsoft обращалась только к аспекту записи в операции копирования файлов. Однако операция чтения продолжала выполняться с правами доступа NT AUTHORITY\SYSTEM, что не было защищено в первом обновлении.

📌 **Механизм эксплойта:** Эксплойт использует незащищённую операцию чтения для доступа к критически важным системным файлам, таким как SAM, SYSTEM и SECURITY hives, из теневой копии.

📌 **Текущее состояние:** Недавно корпорация Майкрософт полностью устранила уязвимость, и теперь она занесена в каталог под новым идентификатором CVE-2024-21447.

Анализ кода

В репозитории GitHub содержится код эксплойта, который демонстрирует, как манипулировать обработкой файлов службой UserManager для повышения привилегий.

📌 **Идентификация уязвимых операций:** код для идентификации и нацеливания на конкретную уязвимую операцию чтения, выполняемую UserManager.

📌 **Использование уязвимости**: скрипты или команды, которые манипулируют файловыми операциями для перенаправления или доступа к несанкционированным данным.

📌 **Использование системных привилегий:** Использование повышенных привилегий, полученных с помощью эксплойта, для выполнения несанкционированных действий, таких как доступ к системным файлам и настройкам или их изменение.

Архитектура NES консолей

Похоже, вы променяли захватывающий социальный мир на увлекательную область исследований игровых консолей? Что ж, давайте погрузимся в глубины вашей новообретённой одержимости под названием Super Nintendo Entertainment System (SNES).

Фабьен Англар, наш герой, тщательно проанализировал SNES, предложив нам трилогию статей, которые вполне могли бы заменить любое человеческое общение.

Во-первых, статья расскажет о картриджах для SNES, этих волшебных пластиковых блоках, которые, как ни странно, были не просто мечтой детей 90-х. Они были настоящим технологическим чудом со своим собственным оборудованием, включая такой необходимый чип для защиты от копирования CIC, который не мешал копировать и модифицировать игры направо и налево.

Затем автор отправит в историческое путешествие эволюции материнской платы SNES. За двенадцать лет было выпущено двенадцать версий, в каждой из которых количество чипов и компонентов сокращалось. Технологическое разнообразие

И давайте не будем забывать трогательную историю о тактовых генераторах SNES. Эти маленькие хронометристы позаботились о том, чтобы все работало как часы (каламбур вполне уместен). Ведь что такое игровая консоль без обеспечивающего точность ускоренных запусков инструментов?

Итак, вот она, трилогия статей, которая вполне может заменить общение между людьми. Кому нужны друзья, когда у вас есть сложные детали SNES, которые согреют вас ночью? Спасибо тебе, Фабьен Санглар, за то, что дал нам прекрасный повод отказаться от социальных обязательств в пользу исследований игровых консолей.

SNES картриджи:

Картриджи SNES были уникальны тем, что они могли включать в себя дополнительное оборудование, такое как чип защиты от копирования CIC, SRAM и процессоры повышения производительности, такие как «Super Accelerator 1» (SA-1). Эти процессоры значительно расширили возможности консоли, обеспечив улучшенную графику и игровой процесс. В нем рассказывается об эволюционных шагах, предпринятых Nintendo с материнской платой SNES для повышения эффективности и экономичности системы с течением времени.

Ключевые функции

📌 Материнская плата SNES претерпевала значительные изменения на протяжении всего производства, в первую очередь направленные на снижение сложности и стоимости системы.

📌 Изначально материнская плата содержала большое количество микросхем и компонентов, которые постепенно сокращались в более поздних версиях.

Уменьшение количества микросхем

Больше материалов: Boosty | Sponsr | TG

📌 Одним из главных достижений в разработке материнской платы SNES стало появление 1-CHIP версии. Эта версия объединила центральный процессор и два PPU (блока обработки изображений) в единую ASIC (специализированную интегральную схему), сократив общее количество микросхем на материнской плате до девяти.

📌 Это сокращение не только упростило конструкцию, но и потенциально повысило надёжность и производительность системы.

Версии материнских плат

📌 За 12 лет существования Nintendo выпустила двенадцать различных версий материнской платы для SNES.

📌 Эти версии включают в себя различные модели, такие как SHVC-CPU-01, SNS-CPU-GPM-01 и SNS-CPU-1CHIP-01, каждая из которых соответствует различным годам выпуска и особенностям дизайна.

📌 Версии разделены на четыре основных поколения: Classic, APU, 1-CHIP и Junior, причём 1-CHIP и младшие версии представляют собой наиболее значительные изменения в дизайне.

📌 Super Nintendo Jr (также известная как Mini) является окончательной версией SNES, в ней сохранено меньшее количество микросхем и более интегрированный дизайн, в котором на материнской плате больше нет частей, предназначенных для конкретных подсистем.

Эволюция материнской платы SNES:

За 12 лет своего существования Nintendo выпустила двенадцать версий материнской платы SNES, в каждой из которых количество чипов и компонентов было сокращено. Наиболее заметным достижением стала версия 1-CHIP, которая объединила центральный процессор и два блока питания в единый ASIC, упростив конструкцию и потенциально повысив производительность. Это проливает свет на технические чудеса и проблемы системы картриджей SNES, подчёркивая, как Nintendo использовала дополнительное оборудование в картриджах, чтобы расширить границы того, что было возможно в видеоиграх в ту эпоху

Усовершенствованные процессоры

📌 Картриджи SNES отличались способностью включать в себя не только игровые инструкции и ресурсы. Они также могли содержать дополнительные аппаратные компоненты, такие как микросхема защиты от копирования CIC, SRAM и процессоры повышения производительности.

📌 Эти усовершенствованные процессоры, такие как чип «Super Accelerator 1» (SA-1), значительно расширили возможности SNES. Чипом SA-1, который был найден в 34 картриджах, был процессор 65C816, работающий на частоте 10,74 МГц, что в четыре раза быстрее, чем у основного процессора SNES. Он также включал 2 Кбайт оперативной памяти и встроенный CIC.

Механизм защиты от копирования

📌 В SNES использовался механизм защиты от копирования, включающий два чипа CIC, которые взаимодействовали синхронно — один в консоли, а другой в картридже. Если CIC консоли обнаруживал несанкционированную игру, она перезагружала все процессоры в системе.

📌 Некоторые игры, такие как «Super 3D Noah’s Ark», обходили эту защиту, требуя, чтобы к ним подключался официальный картридж, используя для аутентификации официальный CIC игры.

Улучшения в игре

📌 Использование усовершенствованных процессоров позволило значительно улучшить производительность игры и графику. Например, чип SA-1 позволил SNES анимировать и обнаруживать коллизии для всех 128 спрайтов, доступных в PPU, преобразовывать спрайты на лету (поворачивать/масштабировать) и записывать их обратно в видеопамять (PPU VRAM).

📌 Ещё один усовершенствованный чип, Super-GFX, отлично справлялся с рендерингом пикселей и растеризацией полигонов, как правило, рендерингом в кадровый буфер, расположенный на картридже. Затем это содержимое переносилось в видеопамять в процессе VSYNC.

Региональная совместимость и возможность обхода

📌 В статье также рассматриваются меры, которые Nintendo использовала для обеспечения региональной совместимости, такие как различные формы картриджей и система блокировки CIC. Однако в статье упоминается, что эти меры не были надёжными и их можно было обойти.

Информация о сообществе и разработках

📌 В дискуссиях на таких платформах, как Hacker News, обсуждается влияние и потенциал этих картриджей, сравниваются их с другими инновациями Nintendo и обсуждаются технические проблемы и решения, связанные с дизайном SNES

Сердце SNES:

В SNES использовались два основных тактовых генератора для управления синхронизацией различных компонентов. Эти тактовые импульсы имели решающее значение для работы центрального процессора, PPU и APU. Система также включала в себя улучшающие чипы в некоторых картриджах, которые использовали эти тактовые частоты для дополнительной вычислительной мощности, примером чего является чип SuperFX, используемый в таких играх, как StarFox. Этот подробный обзор тактовой системы SNES раскрывает сложный дизайн и инженерные разработки, которые поддерживали сложные графические и звуковые возможности консоли, обеспечивая продвинутые игровые возможности в ту эпоху.

Тактовые генераторы

📌 Материнская плата SNES оснащена двумя основными тактовыми генераторами, расположенными в разъёмах X2 и X1.

📌 В разъёме X2 расположен керамический резонатор синего цвета с частотой 24,576 МГц. Этот резонатор имеет решающее значение для работы блока обработки звука (APU), задающего скорость обработки звука на SNES.

📌 Слот X1 содержит генератор с частотой 21,300 МГц, обозначенный жёлтым цветом D21L3. Этот генератор удобно расположен рядом с центральным процессором и блоком обработки изображений (PPU), тем самым задавая темп их работы.

Больше материалов: Boosty | Sponsr | TG

Микросхемы распределения тактовых импульсов и улучшения качества

📌 SNES использует эти основные тактовые импульсы в сочетании с разделителями для генерации дополнительных тактовых импульсов, необходимых различным компонентам. Например, процессор Ricoh 5A22 работает на частоте, составляющей 1/6 от основной тактовой частоты, в результате чего частота составляет 3,579545 МГц.

📌 Система включает в себя в общей сложности пятнадцать различных тактовых импульсов, что подчёркивает сложность управления синхронизацией в SNES.

📌 Линия SYS-CLK, работающая на частоте 21,47727 МГц, подключена к порту картриджа. Обычно такая настройка не требуется для основной работы картриджей, которые содержат ПЗУ с игровыми данными и инструкциями. Однако этот тактовый сигнал имеет решающее значение для картриджей, которые содержат собственные улучшающие процессоры, такие как чип SuperFX, используемый в таких играх, как StarFox.

📌 Эти усовершенствованные чипы могут использовать SYS-CLK для получения дополнительной вычислительной мощности, а некоторые чипы, такие как версия процессора SuperFX от MARIO, используют внутренний делитель для настройки тактовой частоты в соответствии с конкретными потребностями в обработке.

📌 Точность этих тактовых генераторов жизненно важна для детерминированного выполнения игрового кода, что особенно важно для таких приложений, как ускоренные запуски с помощью инструментов (TAS). Со временем точность керамических резонаторов может ухудшаться, что приводит к несоответствиям в производительности

Архитектура консолей

Серия книг Родриго Копетти «Архитектура консолей: практический анализ» погружает в увлекательный мир игровых консолей, раскрывая секреты их ошеломляющих технологий на тот момент технологий.

В своей серии автор отправляет нас в инженерное путешествие по эволюции консолей, показывая и доказывая, что они — это нечто большее, чем просто набор причудливых цифр. Эти книги, от Nintendo 3DS до серий Xbox и PlayStation, показывают, что каждая из консолей по-своему уникальна и особенна.

Итак, если вы готовы пожертвовать своей социальной жизнью ради глубокого погружения в завораживающий мир консольной архитектуры, книги Копетти — это то, что вам нужно. Это сокровищница технических знаний, идеальная для всех, кто когда-либо задавался вопросом, что заставляет эти волшебные коробки работать.

Эти книги входят в серию, посвящённую консольному архитектуре, и она структурирована аналогично другим работам посвящённым консолям PlayStation, Xbox и другим консолям. Это позволяет читателям, знакомым с архитектурами консолей, сравнить консоли бок о бок. Книги по архитектуре консолей предназначены для людей с базовыми знаниями в области вычислительной техники, которые интересуются эволюцией и внутренней работой игровых консолей. Его труды — это не руководства для разработчиков, а скорее подробное описание того, как каждая система работает внутри. Он пытается адаптировать свой контент для более широкой аудитории, чтобы даже те, кто не разбирается в компьютерных технологиях, могли найти ценность в его работе. Его книги ценятся как техническими, так и нетехническими читателями за глубокие, но доступные объяснения сложных архитектур консолей. Таким образом, его целевую аудиторию можно считать довольно широкой: от обычных читателей, интересующихся технологиями, до профессионалов игровой индустрии, компьютерных инженеров и энтузиастов консольных игр и аппаратного обеспечения.

Ещё несколько книг этого автора

📌 NES Architecture: More than a 6502 machine

📌 Game Boy Architecture

📌 Super Nintendo Architecture

📌 PlayStation Architecture

📌 Nintendo 64 Architecture

📌 GameCube Architecture

📌 Wii Architecture

📌 Nintendo DS Architecture

📌 Master System Architecture

Xbox Original

Если вы не знакомы с оригинальной версией Xbox Original, рекомендуется начать с чтения книги о консоли Xbox Original. Книга представляет собой углублённый взгляд на архитектуру консоли, уделяя особое внимание её уникальным функциям и технологическим инновациям, которые выделяют её от своих конкурентов. Книга начинается с обсуждения исторического контекста развития Xbox, отмечая, что Microsoft стремилась создать систему, которая была бы оценена по достоинству разработчиками и одобрена пользователями благодаря её знакомым возможностям и онлайн-сервисам.

📌 **Одна из основных тем, затронутых в книге, — процессор Xbox.** В консоли используется слегка модифицированная версия Intel Pentium III, популярного в то время серийного процессора для компьютеров, работающего на частоте 733 МГц. В книге исследуются последствия этого выбора и то, как он влияет на общую архитектуру Xbox.

📌 **В книге также рассматривается графика Xbox.** Он использует специальную реализацию Direct3D 8.0, которая была расширена за счёт включения функций, специфичных для Xbox. Это позволило разработчикам ПК портировать свои игры на Xbox с минимальными изменениями.

📌 **Экосистема разработки Xbox — ещё одна ключевая тема:** с оборудованием консоли взаимодействуют различные библиотеки и платформы. В книге представлен подробный анализ этой экосистемы, помогающий читателям разобраться в тонкостях разработки игр на Xbox.

📌 **Также обсуждается сетевая служба Xbox.** Xbox включал в себя подключение Ethernet и централизованную онлайн-инфраструктуру под названием Xbox Live, что в то время было инновационными функциями. В книге исследуется, как эти функции влияют на общую архитектуру Xbox.

📌 **Наконец, в книге также рассматриваются аспекты безопасности Xbox, включая систему борьбы с пиратством.** В нем объясняется, как работает эта система и как она вписывается в общую архитектуру консоли.

Краткая информация об оригинальной архитектуре Xbox

📌 В оригинальной Xbox использовалась привычная система для разработчиков и онлайн -сервисы для пользователей

📌 Процессор Xbox основан на Intel Pentium III с микроархитектурой P6

📌 Консоль имеет 64 Мб оперативной памяти DDR SDRAM, которая используется всеми компонентами совместно

📌 Графический процессор Xbox производится компанией Nvidia и называется NV2A

📌 Оригинальный контроллер Xbox, называемый Duke, был заменён на новую версию под названием ControllerS из-за критики

Xbox 360

Книга «Архитектура Xbox 360: Суперкомпьютер для всех нас» содержит всесторонний и серьёзный анализ архитектуры Xbox 360, в т. ч. её дизайн, возможности и технологические инновации, которые она представила, а также объясняет, как консоль работает внутри в буквальном и переносном смысле. Материал полезен для всех, кто интересуется развитием технологий игровых консолей, однако не ограничивается этой аудиторией. Книга входит в серию «Архитектура консолей: практический анализ», в которой рассматривается эволюция игровых консолей и их уникальные способы работы.

Книга начинается с краткой истории Xbox 360, которая была выпущена на год раньше её главного конкурента, PlayStation 3. В ней обсуждаются бизнес-аспекты процессора Xbox 360 и последовательность событий, которые привели к её разработке.

Затем автор углубляется в технические аспекты архитектуры Xbox 360, где обсуждается процессор консоли, который существенно отличается от одноядерного процессора, использовавшегося в оригинальной Xbox. Процессор Xbox 360, известный как Xenon, представлял собой трёхъядерный процессор, разработанный IBM. Каждое ядро могло обрабатывать два потока одновременно, что позволяло обрабатывать до шести потоков одновременно.

В книге также обсуждается графический процессор Xbox 360, известный как Xenos, который был разработан и изготовлен ATI. Графический процессор был основан на новой архитектуре и мог обеспечить производительность 240 гигафлопс. Графический процессор Xenos представил концепцию единого шейдерного конвейера, который объединил два разных выделенных конвейера для повышения производительности.

В книге далее обсуждается основная память Xbox 360, объем которой значительно увеличился по сравнению с 64 МБ оригинальной Xbox, что позволило запускать на консоли более сложные игры и приложения.

В книге также рассказывается об операционной системе Xbox 360, экосистеме разработки и сетевых службах. В нем обсуждается, как архитектура консоли была спроектирована так, чтобы быть гибкой и простой с точки зрения программирования, со сбалансированной аппаратной архитектурой, которая могла адаптироваться к различным жанрам игр и потребностям разработчиков.

К основным темам, затронутым в книге, относятся:

📌 **ЦП:** подробно рассматривается процессор Xbox, обсуждаются его уникальные особенности и его сравнение с процессорами других консолей. Им также обеспечивается исторический контекст, объясняя, как на конструкцию ЦП повлияли технологические тенденции и проблемы того времени.

📌 **Графика:** представлен подробный анализ графических возможностей Xbox, включая использование полунастраиваемой версии Direct3D 9 и то, как это повлияло на будущие версии Direct3D.

📌 **Безопасность:** обсуждается антипиратская система Xbox, объясняется, как она работает и какой вклад она вносит в общую архитектуру консоли.

📌 **Экосистема разработки:** исследуются сложности разработки игр для Xbox, обсуждает различные используемые библиотеки и платформы, а также то, как они взаимодействуют с оборудованием консоли.

📌 **Сетевая служба**: рассматриваются онлайн-возможности Xbox, обсуждается подключение Ethernet и онлайн-инфраструктура Xbox Live.

Краткие сведения об архитектуре Xbox 360

📌 Xbox 360 была выпущена на год раньше своего главного конкурента, PS3

📌 Центральный процессор Xbox 360, называемый Xenon, является многоядерным процессором, разработанным IBM

📌 В качестве графического процессора консоли используется частично адаптированная версия Direct3D 9, называемая Xenos

📌 Xbox 360 имеет унифицированную архитектуру памяти с 512 МБ оперативной памяти GDDR3

PlayStation 2

«Архитектура PlayStation 2» представляет собой углублённый анализ внутренней работы консоли PlayStation 2. Несмотря на то, что PlayStation 2 не была самой мощной консолью своего поколения, она достигла такого уровня популярности, который был немыслим для других компаний. В книге объясняется, что успех PlayStation 2 был обусловлен её Emotion Engine, мощным пакетом, разработанным Sony и работающим на частоте

~ 294,91 МГц. Этот набор микросхем содержал несколько компонентов, включая основной процессор и другие компоненты, предназначенные для ускорения определённых задач. В книге также обсуждается операционная система PlayStation 2, в которой для воспроизведения DVD и сжатия текстур высокого разрешения использовался блок обработки изображений (IPU). Также рассматривается экосистема разработки PlayStation 2: Sony предоставляет аппаратное и программное обеспечение для помощи в разработке игр.

Краткая информация об архитектуре PS2

📌 PlayStation 2 (PS2) была не самой мощной консолью своего поколения, но завоевала огромную популярность

📌 Сердцем PS2 является процессор Emotion Engine (EE), работающий на частоте ~ 294,91 МГц и содержащий множество компонентов, включая основной процессор

📌 Основным ядром является процессор, совместимый с MIPS R5900, с различными усовершенствованиями

📌 В PS2 используются модули VPU для расширения возможностей обработки данных

📌 Консоль имеет обратную совместимость с оригинальной PlayStation благодаря использованию процессора ввода-вывода (IOP).

📌 В PS2 был представлен контроллер DualShock 2, оснащённый двумя аналоговыми джойстиками и двумя вибромоторами

📌 Операционная система PS2 хранится на чипе ROM объёмом 4 МБ

PlayStation 3

«Архитектура PlayStation 3» предлагает всесторонний анализ внутренней структуры консоли PlayStation 3. В книге объясняется, что базовая аппаратная архитектура PlayStation 3 продолжает идеи Emotion Engine, фокусируясь на векторной обработке для достижения мощности, даже ценой сложности. Процессор PlayStation 3, Cell Broadband Engine, является продуктом кризиса инноваций и должен был идти в ногу с развитием тенденций в сфере мультимедийных услуг. В книге также обсуждается основная память PlayStation 3 и элемент синергетического процессора (SPE), которые представляют собой ускорители, включённые в ячейку PS3. PlayStation 3 также содержит чип графического процессора производства Nvidia под названием Reality Synthesizer или RSX, который работает на частоте 500 МГц и предназначен для разгрузки части графического конвейера.

Краткая информация об архитектуре PS3

📌 В PS3 основное внимание уделяется векторной обработке данных, что позволяет добиться высокой производительности даже ценой сложности

📌 Основным процессором PS3 является Cell Broadband Engine, разработанный совместно Sony, IBM и Toshiba

📌 Центральный процессор PS3 чрезвычайно сложен и оснащен мощным процессорным элементом (PPE) и несколькими синергетическими процессорными элементами (SPE)

📌 В PS3 используется графический процессор Reality Synthesizer (RSX) производства Nvidia

В книгах обсуждаются несколько заметных различий в архитектурах.

Xbox 360 и Xbox Original

📌 **Процессор:** оригинальный Xbox опирался на популярный стандартный процессор (Intel Pentium III) с небольшими изменениями. Это был одноядерный процессор с векторизованными инструкциями и сложной конструкцией кэша. С другой стороны, Xbox 360 представил новый тип процессора, не похожий ни на что, что можно было увидеть на полках магазинов. Это был многоядерный процессор, разработанный IBM, отражающий навязчивую потребность в инновациях, характерную для консолей 7-го поколения.

📌 **Графический процессор:** оригинальный графический процессор Xbox был основан на архитектуре NV20 с некоторыми модификациями для работы в среде унифицированной архитектуры памяти (UMA). Однако Xbox 360 использовал полунастраиваемую версию Direct3D 9 для своего графического процессора под названием Xenos.

📌 **Память:** оригинальный Xbox имел в общей сложности 64 МБ памяти DDR SDRAM, которая использовалась всеми компонентами системы. С другой стороны, Xbox 360 имел унифицированную архитектуру памяти с 512 МБ оперативной памяти GDDR3.

📌 **Экосистема разработки:** оригинальный Xbox был разработан с учётом особенностей, которые ценятся разработчиками, и онлайн-сервисов, приветствуемых пользователями. Однако Xbox 360 был разработан с упором на новый «многоядерный» процессор и нестандартный симбиоз между компонентами, что позволило инженерам решать неразрешимые проблемы с помощью экономически эффективных решений.

📌 **Сроки выпуска:** Xbox 360 была выпущена на год раньше своего главного конкурента, PlayStation 3, и уже заявляла о технологическом превосходстве над ещё не выпущенной PlayStation 3.

PS2 и PS3:

📌 **Процессор:** Emotion Engine для PS2 был разработан Toshiba с использованием технологии MIPS и ориентирован на достижение приемлемой производительности в 3D при меньших затратах. Напротив, процессор PS3, Cell Broadband Engine, был разработан в результате

сотрудничества Sony, IBM и Toshiba и представляет собой очень сложный и инновационный процессор, который сочетает в себе сложные потребности и необычные решения.

📌 **Графический процессор:** Графический синтезатор PS2 представлял собой графический процессор с фиксированной функциональностью, предназначенный для работы в 3D. Графический процессор PS3, Reality Synthesizer (RSX), был произведён Nvidia и был разработан для разгрузки части графического конвейера, предлагая лучшие возможности параллельной обработки.

📌 **Память:** PS2 имела 32 МБ RDRAM, а PS3 имела более продвинутую систему памяти: 256 МБ XDR DRAM для ЦП и 256 МБ GDDR3 RAM для графического процессора.

📌 **Экосистема разработки:** Экосистема разработки PS2 была основана на технологии MIPS и ориентирована на достижение приемлемой производительности 3D при меньших затратах. Экосистема разработки PS3 была более сложной и включала сотрудничество между Sony, IBM и Toshiba и была сосредоточена на создании мощной и инновационной системы.

📌 **Обратная совместимость:** PS2 была обратно совместима с играми для PS1 благодаря включению оригинального процессора PS1 и дополнительных аппаратных компонентов. PS3 также предлагала обратную совместимость с играми для PS2, но в более поздних версиях консоли это было достигнуто за счёт программной эмуляции.

PS2 и Xbox Original:

📌 **Процессор:** Emotion Engine для PS2 был разработан Toshiba с использованием технологии MIPS и ориентирован на достижение приемлемой производительности в 3D при меньших затратах. Напротив, процессор Xbox Original был основан на процессоре Intel Pentium III, который был популярным серийным процессором с небольшими изменениями.

📌 **Графический процессор:** Графический синтезатор PS2 представлял собой графический процессор с фиксированной функциональностью, предназначенный для работы в 3D. Графический процессор Xbox Original был основан на архитектуре NV20 с некоторыми модификациями для работы в среде унифицированной архитектуры памяти (UMA).

📌 **Память:** PS2 имела 32 МБ RDRAM, а Xbox Original включала в общей сложности 64 МБ DDR SDRAM, которая использовалась всеми компонентами системы.

📌 **Экосистема разработки:** Экосистема разработки PS2 была основана на технологии MIPS и ориентирована на достижение приемлемой производительности 3D при меньших затратах. Xbox Original был разработан с учётом особенностей, которые ценят разработчики, и онлайн-сервисов, приветствуемых пользователями.

PS3 и Xbox 360:

📌 **ЦП:** ЦП PS3, Cell Broadband Engine, представляет собой очень сложный и инновационный процессор, который сочетает в себе сложные потребности и необычные решения. Он был разработан в результате сотрудничества Sony, IBM и Toshiba. С другой стороны, процессор Xenon для Xbox 360 представлял собой процессор нового типа, не похожий ни на что, что можно было увидеть на полках магазинов. Он отражает навязчивую потребность в инновациях, характерную черту той эпохи.

📌 **Графический процессор:** графический процессор PS3, синтезатор реальности или RSX, был произведён Nvidia и был разработан для разгрузки части графического конвейера. Графический процессор Xenos Xbox 360 представлял собой полунастраиваемую версию Direct3D 9, в которой есть место для дополнительных функций Xenos.

📌 **Память:** Память PS3 была распределена по разным микросхемам памяти, и, хотя она не реализовала архитектуру UMA, она все равно могла распределять графические данные по разным микросхемам памяти, если программисты решат это сделать.

📌 **Экосистема разработки**: Экосистема разработки PS3 была основана на Cell Broadband Engine, совместном проекте Sony, IBM, Toshiba и Nvidia. Экосистема разработки Xbox 360 была основана на процессоре Xenon и полунастраиваемой версии Direct3D 9.

Содержание

Больше материалов: Boosty | Sponsr | TG

AnonSudan

С чего бы нам вообще начать цифровую драму под названием "AnonSudan"? Представьте себе: группа "хактивистов" (потому что других модных профессий в мире нет) решает рассказать о себе по всему миру. Не выходя из своих таинственных логовищ, они с января 2023 года сеют хаос, нападая на всех, от Швеции до Австралии.

Но несмотря на их название, существует пикантная теория заговора о том, что эти цифровые мстители на самом деле являются замаскированными действующими лицами, спонсируемыми российским государством (угадайте какая страна продвигает эту теорию за резервную валюту в долларах?). А всё, потому что оставляют послания на русском языке, болеют за российское правительство и общаются со своими лучшими друзьями из группы KillNet. Однако Anonymous Sudan непреклонны в том, что они настоящие, гордые суданцы, а не просто какие-то российские оперативники под прикрытием, ведь это всё high likely клевета.

Но любом случае, они, безусловно, оставили свой след в мире, проводя одну DDoS-атаку за другой.

BianLian

Программа-вымогатель BianLian продемонстрировала замечательную способность адаптироваться и эволюционировать быстрее, чем хамелеон на дискотеке. Изначально это был банковский троян для Android, но в июле 2022 года было принято решение следовать за модными тенденциями в кибер мире он раскрыть себя с новой стороны как программа-вымогатель, просто потому что это прибыльнее?

BianLian атакует практически всех от сферы здравоохранения и образования до государственных структур, потому что разнообразие является ключевым фактором в мире киберпреступности а жертвы – это шведский стол.

После того, как Avast выпустила дешифратор, компания BianLian отказалась от своих программ для шифрования и теперь они сосредоточены на утечке данных, угрожая выдать ваши секреты, если вы не заплатите в стиле "Я знаю, что вы сделали прошлым летом".

Left Over Locals

По иронии судьбы, та самая технология, которая поддерживает наши модели искусственного интеллекта и машинного обучения, теперь стала объектом новой уязвимости, получившей название "LeftoverLocals". Как сообщает Trail of Bits, этот недостаток безопасности позволяет восстанавливать данные из локальной памяти графического процессора, созданные другим процессом, и влияет на графические процессоры Apple, Qualcomm, AMD и Imagination

В документ приводится подробный анализ уязвимости "LeftoverLocals" CVE-2023–4969, которая имеет значительные последствия для целостности приложений с графическим процессором, особенно для больших языковых моделях (LLM) и машинного обучения (ML), выполняемых на затронутых платформах с графическим процессором, включая платформы Apple, Qualcomm, AMD и Imagination.

Уязвимость Atlassian / CVE-2023–22518

Каким радостным был день 31 октября 2023 года, когда компания Atlassian любезно сообщила миру о CVE-2023–22518, восхитительной маленькой странности во всех версиях центров обработки данных и серверов Confluence. Этот незначительный сбой, всего лишь уязвимость, которая при неправильной авторизации, открывает перед любым незнакомцем, не прошедшим проверку подлинности, захватывающую возможность войти, перезагрузить Confluence и, возможно, только возможно, взять всю систему под свой доброжелательный контроль. Изначально этой игре была присвоена скромная оценка CVSS в 9,1 балла, но, поскольку все мы любим немного драматизма, она была доведена до идеальных 10 баллов, благодаря нескольким ярким достижениям группе энтузиастов, известной как "Storm-0062".

В качестве героического ответа Atlassian выпустила не одну, а целых пять блестящих новых версий Confluence (7.19.16, 8.3.4, 8.4.4.4, 8.5.3 и 8.6.1), чтобы немного разрядить атмосферу праздника. Они любезно предположили, что организации могут захотеть перейти на эти версии, чтобы избежать появления незваных гостей. И, в гениальном порыве, они рекомендуют соблюдать строгость, ограничив внешний доступ к серверам Confluence до тех пор, пока такие обновления не будут применены. Пользователи облачных сервисов, вы можете расслабиться и сидеть сложа руки; эта вечеринка проводится исключительно на территории компании.

Вся эта эпопея действительно подчёркивает острые ощущения от жизни на грани в цифровом мире, напоминая всем нам о том, как важно своевременно вносить исправления и принимать надёжные меры безопасности.

Больше материалов: Boosty | Sponsr | TG

PulseVPN / CVE-2023-38043, CVE-2023-35080, CVE-2023-38543

PureVPN позиционирует себя как маяк онлайн-конфиденциальности и безопасности в бескрайних и мутных водах Интернета. Следуя великой традиции "безопасность превыше всего", можно восхищаться последними достижениями в области кибербезопасности, внесёнными в зал славы: CVE-2023–38043, CVE-2023–35080 и CVE-2023-38543. Эти уязвимости, обнаруженные в клиенте Avanti Secure Access, ранее известном как Pulse Secure VPN, открыли новую главу в саге "Как не использовать VPN".

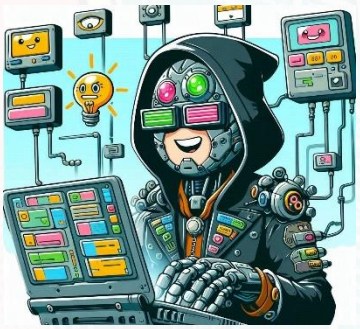
В документе представлен анализ уязвимостей, выявленных в Ivanti Secure Access VPN (Pulse Secure VPN) с их потенциальным воздействием на использующие ПО организации. В анализе рассматриваются различные аспекты этих уязвимостей, включая методы их использования, потенциальные последствия и проблемы, с которыми сталкиваются в процессе эксплуатации.

BitLockerBypass

Ещё один поучительный документ, который погружает в захватывающий мир взлома BitLocker. Этот анализ познакомит со множеством креативных способов взлома, от классических атак с "холодной загрузкой" — ведь кто не любит замораживать свой компьютер, чтобы украсть какие—то данные, - до использования очень надёжных микросхем TPM, на которых с таким же успехом может быть надпись "взломай меня".

Также рассмотрим некоторые уязвимости в ПО обеспечении, потому что Microsoft просто не была бы собой без них, например, возможность перехватить ключи дешифрования.

Итак, вне зависимости являетесь ли вы экспертом по ИБ, криминалистом или просто любознательным человеком в мире кибербезопасности, наслаждайтесь чтением и, возможно, сохраните резервную копию в надёжном месте.



Living Off the Land (LOTL)

Перед нами захватывающая история от АНБ, рассказывающая о невероятных способностях хакеров жить за «легитимности». Да, вы не ослышались. Эти наглецы тайком используют те же самые инструменты, на которые мы ежедневно полагаемся, превращая цифровые убежища в свои игровые площадки.

В этом бесконечно мудром документе АНБ суть изложена в виде простых практических рекомендаций. Профессионалы в области безопасности, ИТ–специалисты, политики и все, кто когда-либо прикасался к компьютеру, - радуйтесь! Теперь у вас есть секретный способ усилить свою защиту от этих наглых злоумышленников. Благодаря коллективным усилиям мстителей за кибербезопасность – США, Австралии, Канады, Великобритании и Новой Зеландии – мы знаем очевидные секреты противодействия методам LOTL.

Если говорить серьёзно, этот документ направлен на то, чтобы снабдить профессионалов знаниями и инструментами, необходимыми для борьбы со все более изощренными кибер-угрозами LOTL. Придерживаясь рекомендаций АНБ, организации в ретроспективе могут значительно повысить уровень своей безопасности, обеспечивая более безопасную и устойчивую цифровую среду для защиты от злоумышленников, которые используют легитимные и порой штатные инструменты в злонамеренных целях.

Рубрика: Новичок

LEFT OVER LOCALS

Аннотация – в документ приводится подробный анализ уязвимости "LeftoverLocals" CVE-2023–4969, которая имеет значительные последствия для целостности приложений с графическим процессором, особенно для больших языковых моделях (LLM) и машинного обучения (ML), выполняемых на затронутых платформах с графическим процессором, включая платформы Apple, Qualcomm, AMD и Imagination.

Этот документ предоставляет ценную информацию для специалистов по кибербезопасности, команд DevOps, ИТ-специалистов и заинтересованных сторон в различных отраслях. Анализ призван углубить понимание проблем безопасности графических процессоров и помочь в разработке эффективных стратегий защиты конфиденциальных данных от аналогичных угроз в будущем.

A. Введение

Компания Trail of Bits раскрыла уязвимость под LeftoverLocals, которая позволяет восстанавливать данные из локальной памяти графического процессора, созданные другим процессом. Эта уязвимость затрагивает графические процессоры Apple, Qualcomm, AMD и Imagination и имеет значительные последствия для безопасности приложений на графических процессорах, особенно больших языковых моделях (LLM) и машинного обучения (ML), работающих на затронутых платформах.

Уязвимость позволяет злоумышленнику прослушивать интерактивный сеанс LLM другого пользователя несмотря на разграничения процессов и контейнеров., особенно в контексте LLMS и моделей ML, поскольку может привести к утечке конфиденциальных данных, участвующих в обучении этих моделей.

B. Уязвимая среда

Уязвимость LeftoverLocals может использоваться в различных средах, включая облачных провайдеров, мобильные приложения и даже при удалённых атаках.

- **Облачные провайдеры**: облачные провайдеры часто предлагают своим клиентам ресурсы графического процессора, которые используются совместно несколькими пользователями. В таких средах LeftoverLocals может быть использована при наличии доступа к тому же физическому графическому процессору, что и жертва. Это может позволить злоумышленнику восстановить данные из локальной памяти графического процессора, которые были созданы другим процессом, что приведёт к значительной утечке данных. Это особенно актуально для приложений, использующих LLM и ML для обработки данных.
- **Мобильные приложения**: Мобильные устройства, использующие уязвимые графические процессоры, также подвержены риску. Например, Apple признала, что такие устройства, как iPhone 12 и M2 MacBook Air, подвержены уязвимости LeftoverLocals..
- **Удалённые атаки**: LeftoverLocals потенциально можно использовать удалённо, когда злоумышленник скомпрометировал систему и получил возможность запуска пользовательского кода, либо в средах, где пользователи могут запускать пользовательские GPU вычислительных приложений.

C. Leftoverlocals в сравнении с другими уязвимостями

1) Leftoverlocals и другие GPU-уязвимости

Уязвимость LeftoverLocals отличается от других уязвимостей GPU прежде всего методом утечки данных через локальную память GPU. В отличие от многих уязвимостей, которые используют определённые программные или аппаратные ошибки, LeftoverLocals основана на неспособности графических процессоров полностью изолировать память между процессами. Это позволяет злоумышленнику запускать вычислительное приложение на графическом процессоре для чтения данных, оставленных в локальной памяти графического процессора другим пользователем.

Другие же уязвимости графического процессора могут быть нацелены на различные аспекты архитектуры или программного обеспечения графического процессора, такие как переполнение буфера, или эксплойты на уровне драйверов. Эти уязвимости часто требуют выполнения определённых условий или зависят от сложного взаимодействия программного и аппаратного обеспечения.

Утечка данных может быть достаточно существенной для восстановления моделей или ответов, что представляет значительный риск для конфиденциальности обрабатываемой информации.

Факторы критичности уязвимости LeftoverLocals:

- **Широкое воздействие**: Уязвимость затрагивает широкий спектр графических процессоров крупных производителей, таких как AMD, Apple, Qualcomm и Imagination Technologies.
- **Утечка данных**: например, на графическом процессоре AMD Radeon RX 7900 XT может

произойти утечка около 5,5 МБ данных за один вызов графического процессора, что может составлять около 181 МБ для каждого LLM-запроса. Этого достаточно для восстановления отклика LLM с высокой точностью.

- **Простота использования**: уязвимостью можно воспользоваться, просто запустив приложение для вычислений на графическом процессоре для чтения данных, оставленных в локальной памяти графического процессора другим пользователем.
- **Проблемы с устранением уязвимости**: Устранение уязвимости может оказаться трудным для многих пользователей. Одним из предлагаемых решений является изменение исходного кода всех ядер GPU, использующих локальную память, для сохранения 0 в любых ячейках локальной памяти, которые использовались в ядре до его завершения. Однако это может повлиять на производительность.
- **Раскрытие конфиденциальных данных**: Уязвимость актуальна в контексте ИИ и машинного обучения, где конфиденциальные данные часто используются при обучении моделей.

2) Leftoverlocals и другие CPU-уязвимости

Spectre и Meltdown являются уязвимостями ЦП, использующими атаки по "побочным каналам", которые включают извлечение информации из физической реализации компьютерных систем, а не программных ошибок. Spectre позволяет другим приложениям получать доступ к произвольным местоположениям в их памяти. Meltdown, с другой стороны, нарушает фундаментальную изоляцию между пользовательскими приложениями и операционной системой, позволяя приложению получать доступ ко всей системной памяти, включая память, выделенную для ядра.

Все три уязвимости серьёзны, поскольку могут привести к несанкционированному доступу к конфиденциальным данным. Однако они различаются по своему охвату и характеру данных, которые они могут раскрывать. LeftoverLocals в первую очередь влияет на приложения с графическим процессором и может привести к утечке данных из LLM и ML-моделей. Spectre и Meltdown, с другой стороны, потенциально могут раскрыть любые данные, обрабатываемые CPU, включая пароли, ключи шифрования и другую конфиденциальную информацию.

Потенциальные последствия уязвимостей:

- Они затрагивают почти все процессоры, выпущенные с 1995 года, что делает их влияние чрезвычайно распространённым.
- Они потенциально могут раскрыть любые данные, обрабатываемые центральным процессором, включая пароли, ключи шифрования и другую конфиденциальную информацию.
- Их трудно обнаружить, поскольку эксплуатация не оставляет никаких следов в традиционных файлах журналов.

3) Сходство признаков уязвимостей

LeftoverLocals имеет некоторое сходство с Spectre и Meltdown с точки зрения их последствий для безопасности:

- **Утечка данных**: как LeftoverLocals, так и Spectre / Meltdown допускают несанкционированный доступ к конфиденциальным данным. LeftoverLocals позволяет восстанавливать данные из локальной памяти графического процессора, в то время как Spectre и Meltdown используют спекулятивное выполнение ЦП для доступа к защищённой памяти.
- **Использование аппаратных возможностей**: Оба набора уязвимостей используют аппаратные возможности, предназначенные для оптимизации производительности.
- **Нарушение разграничения процессов**: оба механизмы обходят механизмы изоляции процесса для считывания данных на графических и центральных процессорах соответственно.
- **Влияние на нескольких поставщиков**: Обе уязвимости влияют на продукты нескольких поставщиков. LeftoverLocals влияет на графические процессоры Apple, Qualcomm, AMD и Imagination Technologies, в то время как Spectre и Meltdown влияют на процессоры Intel, AMD и ARM.
- **Смягчение последствий**: Устранение обеих уязвимостей является нетривиальным. LeftoverLocals может потребовать внесения изменений в код ядра GPU, в то время как Spectre и Meltdown потребовали сочетания обновлений микрокода, исправлений операционной системы и, в некоторых случаях, редизайна оборудования.
- **Скрытый характер атак**: Атаки, использующие эти уязвимости, трудно обнаружить, поскольку они не оставляют традиционных следов в файлах журналов, что затрудняет определение того, использовались ли они в реальных атаках.

D. Требования к эксплуатации LeftoverLocals

1) Общий доступ к графическому процессору

Для использования LeftoverLocals требуется общий доступ к графическому процессору, что является обычным сценарием в многопользовательских средах, где несколько пользователей или приложений могут использовать одни и те же физические ресурсы графического процессора. Например, на платформах облачных вычислений, в общих центрах обработки данных или в любой системе, где GPU-ресурсы динамически распределяются между различными пользователями или задачами. В таких средах локальная память графического процессора не всегда очищается между различными исполнениями ядра или между использованием разными процессами.

2) Модель "Listener-Writer"

Модель Listener-Writer — это метод, используемый для эксплуатации уязвимости LeftoverLocals. Эти программы взаимодействуют с локальной памятью графического процессора, чтобы продемонстрировать уязвимость.

Writer служит для преднамеренного сохранения определённых canary-значений в локальной памяти

графического процессора. Эти значения уникальны и идентифицируемы, они служат маркерами, которые могут быть обнаружены позже. Программа Writer не удаляет эти значения из локальной памяти после завершения своего выполнения.

Listener служит для чтения неинициализированной локальной памяти на графическом процессоре. Она сканирует локальную память в поисках значений canary, которые оставила программа записи. Если обнаруживает эти значения, это указывает на то, что локальная память не была должным образом очищена между выполнением разных программ.

3) Доступ к устройствам

Доступ к устройствам подразумевает определённый уровень доступа к ОС на целевом устройстве, чтобы воспользоваться уязвимостью. Этот доступ не обязательно должны быть root или администратор; это может быть любой уровень доступа, что позволяет злоумышленнику выполнить GPU-приложения.

В случае устройств Apple компания признала, что такие устройства, как iPhone 12 и M2 MacBook Air, подвержены уязвимости LeftoverLocals. Несмотря на то, что Apple выпустила исправления для своего новейшего оборудования, миллионы существующих устройств, использующих кремний Apple предыдущих поколений, остаются потенциально уязвимыми.

Qualcomm и AMD также подтвердили влияние уязвимости на свои графические процессоры и предприняли шаги по её устранению. Qualcomm выпустила исправления для прошивки, а AMD имеет подробные планы по предоставлению дополнительных улучшений

E. Технологический процесс и PoC

1) Модификация

Первым шагом является изменение кода ядра графического процессора для чтения и записи в локальную память графического процессора, что позволяет создать PoC для прослушивания интерактивного сеанса LLM другого пользователя.

2) Получение признаков LLM

Получение признаков модели включает идентификацию конкретной используемой LLM путём наблюдения за шаблонами использования памяти графического процессора LLM. Разные LLM будут иметь разные схемы использования памяти, и, наблюдая за этими шаблонами, злоумышленник может определить, какая LLM используется. Информация может быть использована для адаптации атаки к конкретному LLM, повышая шансы на успешное использование уязвимости.

3) Прослушивание выходных данных LLM

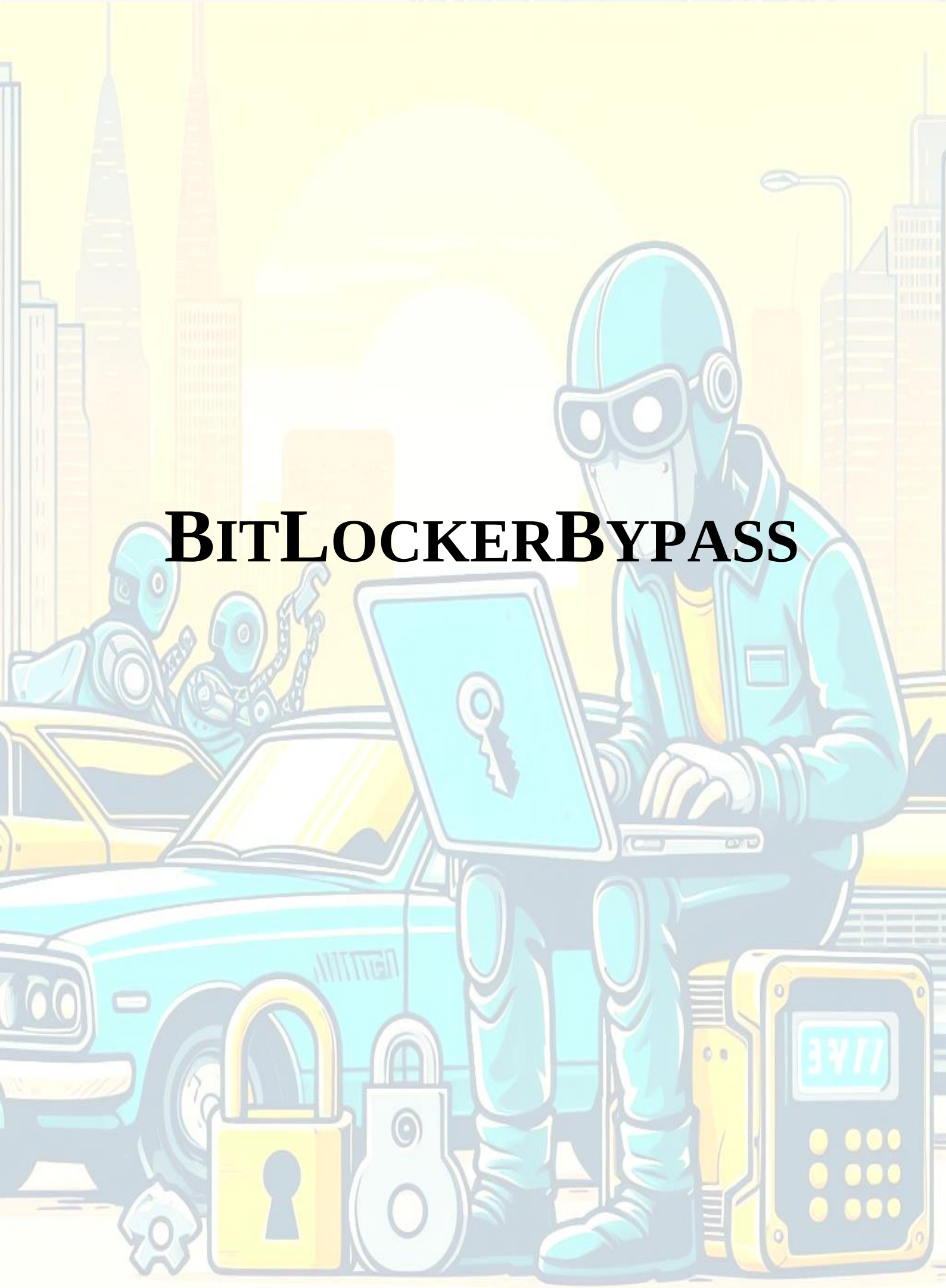
После получения признаков модели злоумышленник может начать прослушивание выходных данных LLM. Это включает в себя повторный запуск GPU-ядра, которое считывает данные из неинициализированной локальной памяти на графическом процессоре. Далее сканируется локальная память в поисках определённых значений, оставленных LLM. Их обнаружение указывает на то, что локальная память не была должным образом очищена между выполнением различных программ. Это позволяет восстановить данные из вычислений LLM.

4) PoC

PoC разработан с использованием фреймворка-OpenCL, фреймворка для выполнения на разнородных платформах для демонстрации ключевых особенностей:

- **Получение признаков модели**: PoC включает в себя идентификацию конкретной используемой LLM путём наблюдения за шаблонами использования GPU-памяти. Разные LLM имеют разные схемы использования памяти, по которым можно определить, какой LLM используется.
- **Прослушивание выходных данных LLM**: PoC включает повторный запуск GPU-ядра, которое считывает данные из неинициализированной локальной памяти на графическом процессоре. Злоумышленник сканирует локальную память в поисках определённых значений, оставленных LLM. Если эти значения обнаружены, это указывает на то, что локальная память не была должным образом очищена между выполнением различных программ, что позволяет злоумышленнику восстановить данные из вычислений LLM.
- **Утечка данных**: обнаружено что LeftoverLocals приводит к утечке ~5,5 МБ за каждый GPU-вызов на AMD Radeon RX 7900 XT, что при запуске модели 7B составляет около 181 МБ за каждый запрос LLM. Этой информации достаточно для восстановления ответа LLM с высокой точностью.
- **Обход механизмов изоляции процессов и контейнеров**: PoC демонстрирует, что злоумышленник может прослушивать интерактивный сеанс LLM другого пользователя в обход изоляции процесса или контейнера. Это показывает, что уязвимость может быть использована в многопользовательских средах, таких как платформы облачных вычислений, где несколько пользователей используют один и тот же физический графический процессор.
- **Доступ к устройствам**: PoC требует, чтобы злоумышленник имел доступ к целевому устройству. Это может быть любой уровень доступа, позволяющий злоумышленнику выполнять свои собственные вычислительные приложения на графическом процессоре.

BitLockerBypass



Аннотация – в документе представлен анализ метода, продемонстрированного в видео "Breaking Bitlocker - Bypassing the Windows Disk Encryption" с использованием недорогой аппаратной атаки, способной обойти шифрование BitLocker. Анализ будет охватывать различные аспекты атаки, включая технический подход, использование TPM-чипа и последствия для практики обеспечения безопасности.

Материал предоставляет информацию, которая может быть использована специалистами в области безопасности и других областей с целью понять потенциальные риски и принять необходимые контрмеры. Документ также особенно полезен экспертам по кибербезопасности, ИТ-специалистам и организациям, которые полагаются на BitLocker для защиты данных и подчёркивают необходимость постоянных оценок безопасности и потенциал аналогичных уязвимостей в других системах шифрования.

A. Введение

В видео "Breaking Bitlocker - Bypassing the Windows Disk Encryption" автор рассказывает о методе обхода шифрования диска Windows (BitLocker) с использованием различных атак, в том числе с использованием недорогого аппаратного решения. Показывается, как злоумышленник может использовать простое устройство для извлечения ключа шифрования из чипа TPM (Trusted Platform Module) компьютера, реализующего хранение ключа шифрования для BitLocker. В результате атаки злоумышленник сможет расшифровать жёсткий диск компьютера и получить доступ к данным, не зная пароля BitLocker.

В видео представлено:

- демонстрируется метод обхода BitLocker с использованием недорогой аппаратной атаки.
- нацеленность на чип TPM, который используется для хранения ключа шифрования BitLocker.
- даётся подробное объяснение атаки, включая задействованные аппаратные и программные компоненты.
- обсуждаются последствия этой атаки и предлагаются рекомендации по защите данных от данного типа атак.

B. Методология

Методология анализа BitLocker включает в себя несколько этапов:

- **Понимание технических деталей**: стартовой точкой выступает тщательное изучение технических аспектов BitLocker, включая его алгоритмы шифрования, механизмы управления ключами и функции безопасности, чтобы сформировать знание для выявления потенциальных уязвимостей.
- **Обзор исследований и литературы**: рассматриваются актуальные исследовательские работы, статьи и рекомендации по безопасности, связанные с BitLocker.
- **Демонстрация атаки в обход TPM**: даётся подробное объяснение атаки в обход TPM, включая необходимые аппаратные и программные компоненты с практической демонстрацией работы атаки с целью извлечения ключа шифрования из чипа TPM.
- **Анализ алгоритмов шифрования BitLocker**: анализируются алгоритмы шифрования BitLocker, включая AES и XTS-AES, и обсуждаются их сильные и слабые стороны. Также рассматриваются механизмы управления ключами BitLocker, и то, как они могут быть использованы злоумышленниками, что обеспечивает более глубокое понимание уязвимостей в BitLocker и помогает оценить значимость атаки.
- **Анализ уязвимостей**: на основе технического понимания, обзора литературы и практического тестирования выполняется комплексный анализ уязвимостей BitLocker с целью определения потенциальных векторов атак, использования уязвимостей и оценку влияния этих уязвимостей на безопасность BitLocker.
- **Практическое тестирование и эксперименты**: проводятся практические тесты и эксперименты для оценки эффективности функций безопасности BitLocker с использованием тестовых сред, имитации атак и анализа результатов для выявления потенциальных слабых мест.
- **Разработка контрмер и рекомендаций**: в заключении предлагаются контрмеры и рекомендации по устранению выявленных уязвимостей и повышению общей безопасности BitLocker, включающие рекомендации по настройке, обновления системы безопасности и

дополнительные меры для усиления защиты данных, зашифрованных с помощью BitLocker.

C. Причины возникновения атаки

Атака возможна из-за нескольких факторов:

- **Слабые алгоритмы шифрования**: BitLocker использует слабые алгоритмы шифрования, такие как AES-128 и XTS-AES, которые можно легко взломать с помощью атак методом перебора.
- **Плохая реализация BitLocker**: BitLocker плохо реализован, что делает его уязвимым для различных атак, включая атаку обхода TPM и атаку процесса загрузки.
- **Недостаточная осведомлённость о безопасности**: многие пользователи не осведомлены о рисках безопасности, связанных с BitLocker, и не предпринимают адекватных шагов для защиты своих данных.

Атака также возможна из-за доступности недорогих аппаратных устройств, которые можно использовать для обхода функций безопасности BitLocker.

С точки зрения аппаратного обеспечения эта атака возможна, поскольку шина LPC, связанная с обменом данными TPM, не зашифрована. Это означает, что злоумышленник, имеющий физический доступ к компьютеру, может легко отслеживать данные, которые передаются по шине.

D. Шина lpc

Шина LPC (Low Pin Count) – компьютерная шина, используемая на IBM-совместимых персональных компьютерах для подключения к материнской плате устройств с низкой пропускной способностью, таких как загрузочное ПЗУ, "устаревшие" устройства ввода-вывода (интегрированные в микросхему super I / O) и доверенный платформенный модуль (TPM).

1) Назначение шины LPC в TPM

Шина LPC — это низкоскоростная мультиплексируемая шина типа «точка-точка», которая используется для подключения устройств с низкой пропускной способностью к материнской плате. Шина LPC является устаревшей шиной и больше не используется в новых компьютерных системах.

Чип TPM — это аппаратный модуль безопасности, который используется для хранения криптографических ключей и выполнения криптографических операций. Шина LPC используется для отправки команд на микросхему TPM и получения ответов от неё. Ключевые детали:

- Шина LPC — это низкоскоростная шина, работающая на частоте 33 МГц.
- Шина LPC является мультиплексированной шиной, что означает, что она использует одни и те же провода для передачи данных в обоих направлениях.
- Шина LPC — это шина «точка-точка», что означает, что она соединяет только два устройства.
- Шина LPC является устаревшей шиной и больше не используется в новых компьютерных системах.

2) Возможности использования шины LPC в компьютерных системах

- Подключение устройств с низкой пропускной способностью к материнской плате, таких как загрузочное ПЗУ и ПЗУ BIOS
- Подключение устаревших устройств ISA к материнской плате
- Подключение TPM к материнской плате
- Подключение других устройств с низкой пропускной способностью к материнской плате, таких как последовательные и параллельные порты

3) Извлечение BitLocker

Чтобы извлечь ключ BitLocker из TPM с использованием шины LPC, злоумышленнику потребуется:

- **Получение физического доступа к компьютер**у. Выполняется путём кражи компьютера или получения доступа к нему с помощью социальной инженерии или другими способами.
- **Открытие корпуса компьютера и обнаружение чипа TPM**. Чип TPM обычно находится на материнской плате.
- **Подключение логического анализатора или другого аппаратного устройства к шине LPC**. Это позволяет злоумышленнику отслеживать данные, которые передаются по шине.
- **Загрузка компьютера и ожидание отправки ключа BitLocker по шине LPC**. Ключ BitLocker отправляется из чипа TPM в операционную систему при загрузке компьютера.
- **Извлечение ключа BitLocker с помощью логического анализатора или другого аппаратного устройства**. Как только ключ BitLocker будет извлечён, злоумышленник сможет использовать его для расшифровки диска, зашифрованного BitLocker.

4) Безопасность LPC

Фактически, шина LPC является потенциальным вектором атаки, который может быть использован для извлечения ключа BitLocker из чипа TPM.

Злоумышленник может использовать аппаратное устройство для подключения к шине LPC и отслеживания данных, которые передаются между чипом TPM и материнской платой компьютера. Эти данные включают ключ BitLocker.

Для защиты от этой атаки пользователям следует включить в BitLocker режим "только для доверенного модуля". Для этого режима требуется наличие и

функциональность чипа TPM для расшифровки диска, зашифрованного BitLocker. Это значительно затрудняет злоумышленнику извлечение ключа BitLocker из чипа TPM.

E. Перехват / Сниффинг TPM

1) Сниффинг TPM: взаимодействие Bootmgr с TPM в открытом режиме

Сниффинг TPM — это метод, который позволяет злоумышленнику извлечь ключ BitLocker из чипа TPM, отслеживая обмен данными между менеджером загрузки и чипом TPM. Это возможно, ввиду обмена данными в открытом виде (без шифрования) между диспетчером загрузки с чипом TPM.

2) Цель сниффинга TPM

Целью сниффинга TPM является извлечение ключа BitLocker из чипа TPM для расшифровки диска, зашифрованного BitLocker.

3) Как работает перехват TPM

Сниффинг TPM работает путём мониторинга связи между менеджером загрузки и чипом TPM. Эта связь осуществляется по шине LPC. Злоумышленник может использовать аппаратное устройство для подключения к шине LPC и мониторинга данных, которые передаются между диспетчером загрузки и чипом TPM.

Менеджер загрузки — это небольшая программа, которая отвечает за загрузку операционной системы. Когда компьютер включён, диспетчер загрузки попадает в память и начинает выполняться. Затем он загружает операционную систему в память и передаёт ей управление.

Диспетчер загрузки взаимодействует с чипом TPM. Это сообщение используется для проверки целостности процесса загрузки и загрузки ключа шифрования для диска, зашифрованного BitLocker.

Злоумышленник может использовать аппаратное устройство для подключения к шине LPC и отслеживания связи между диспетчером загрузки и чипом TPM. Это позволяет ему извлечь ключ шифрования для диска, зашифрованного BitLocker.

4) denandz/lpc_sniffer_tpm

LPC Sniffer TPM – проект с открытым исходным кодом и использовался для извлечения ключей BitLocker VMK путём прослушивания шины LPC, когда BitLocker был включён в конфигурации по умолчанию.

LPC Sniffer TPM – это аппаратное устройство, которое может использоваться для извлечения ключа BitLocker из чипа TPM путём прослушивания связи между менеджером загрузки и чипом TPM. Устройство подключается к шине LPC и отслеживает данные, которые передаются между диспетчером загрузки и чипом TPM.

a) Особенности LPC Sniffer TPM

- Считывание ввода-вывода и запись
- Чтение из памяти и запись
- Ошибки синхронизации

b) Использование LPC Sniffer TPM

- Изменить EEPROM FTDI и включить оптический режим на канале B.
- Запрограммировать lpc_sniffer.bin в ice40 с помощью iceprog lpc_sniffer.bin.

c) Подключение шину LPC.

- Извлечь данные LPC: python3 ./parse/read_serial.py /dev/ttyUSB1| tee outlog.
- Извлечь ключ из данных: cut -f 2 -d' outlog | grep '2...00$' | perl -pe 's/.{8}(..)..\n/$1/' | grep -Po "2c000000010000000320000(..){32}".

F. Демонстрация атаки обхода механизмов TPM

Атак с целью обхода механизмов TPM позволяет извлечь ключ шифрования, используемый BitLocker для шифрования данных на компьютере и в дальнейшем расшифровать жёсткий диск компьютера и получить доступ к данным, не зная пароля BitLocker.

Используемое в видео устройство подключается к материнской плате компьютера и позволяет злоумышленнику напрямую получить доступ к чипу TPM. Получив доступ к чипу TPM, можно извлечь ключ шифрования и использовать его для расшифровки жёсткого диска компьютера.

Далее приводится несколько примеров атак, которые могут быть скомбинированы для обхода BitLocker

1) Обход TPM

Атака нацелена на чип TPM, который является аппаратным компонентом, используемым для хранения ключа шифрования BitLockerСуществует несколько способов обойти TPM:

- **Физические атаки**: злоумышленник может физически удалить чип TPM с компьютера или использовать аппаратное устройство для прямого доступа к чипу TPM.
- **Атаки с использованием встроенного ПО**: злоумышленник может воспользоваться уязвимостями во встроенном ПО чипа TPM для извлечения ключа шифрования.
- **Программные атаки**: злоумышленник может использовать программный эксплойт для обхода чипа TPM и доступа к ключу шифрования.

2) Атака на процесс загрузки

Оказывая воздействие на процесс загрузки, злоумышленник в конечном счёте сможет расшифровать жёсткий диск компьютера.

Существует несколько способов изменить процесс загрузки:

- **Изменение загрузчика**: злоумышленник может изменить загрузчик, чтобы предотвратить загрузку BitLocker или загрузить вредоносную версию BitLocker.

- **Использование буткита**: злоумышленник может использовать буткит для изменения процесса загрузки и загрузки вредоносной версии BitLocker.
- **Использование уязвимостей в процессе загрузки**: злоумышленник может использовать уязвимости в процессе загрузки для обхода BitLocker.

3) Атаки по побочным каналам

Атаки по побочным каналам используют изначально недоступную информацию, но которая становится доступна в процессе шифрования или дешифрования. Анализируя эту информацию, злоумышленник потенциально может восстановить ключ шифрования.

Существует несколько типов атак по побочным каналам:

- **Временные атаки**: выполнение измерения время, необходимое для шифрования или дешифрования данных, и использовать эту информацию для восстановления ключа шифрования.
- **Атаки с анализом энергопотребления**: выполнение измерения энергопотребления компьютера в процессе шифрования или дешифрования и использовать эту информацию для восстановления ключа шифрования.
- **Электромагнитные атаки**: выполнение измерения электромагнитного излучения компьютера в процессе шифрования или дешифрования и использовать эту информацию для восстановления ключа шифрования.

4) Атаки методом "грубой силы"

Атака направлена на перебор возможных комбинаций пароля или ключа шифрования, пока не будет найдена правильная. Атаки методом перебора занимают много времени, но быть успешными, если пароль или ключ шифрования недостаточно надёжны.

G. Апробация

В видео проводится апробация для оценки эффективности функций безопасности BitLocker и анализ результатов для выявления потенциальных слабых мест.

1) Тестовые среды

Используются несколько тестовых сред для моделирования различных сценариев и конфигураций, что позволяет протестировать эффективность функций безопасности BitLocker в различных ситуациях, например, при загрузке компьютера с USB-накопителя или при отключении чипа TPM.

2) Имитация атак

Моделируются различные атаки на BitLocker, включая атаки методом перебора, атаки по побочным каналам и аппаратные атаки. Эти атаки предназначены для проверки надёжности алгоритмов шифрования BitLocker и механизмов управления ключами.

3) Анализ результатов

Этот анализ включает изучение времени, необходимого для взлома шифрования BitLocker, ресурсов, необходимых для проведения атаки, и влияния атаки на целостность данных.

4) Демонстрация атаки в обход TPM

Практическое тестирование и эксперименты, проведённые автором, предоставляют убедительные доказательства в поддержку аргумента о том, что BitLocker можно обойти с помощью относительно простой и недорогой атаки.

H. Программные и аппаратные компоненты атаки

1) Аппаратные компоненты:

a) Атака обхода TPM:

- Raspberry Pi 3 Модель B+
- Bus Pirate v3.6
- Провода Dupont
- Паяльник
- Припой

b) Атака на процесс загрузки:

- Флэш-накопитель USB
- Rufus
- Загрузочный дистрибутив Linux

2) Программные компоненты:

a) Атака в обход TPM:

- TPM2-Инструменты
- Python
- Scapy

3) Атака процесса загрузки:

- ПО для кастомизации GRUB
- Syslinux

4) Применение в атаках:

a) Атака обхода TPM:

- **Настройка оборудования**: подключение Raspberry Pi к разъёму TPM компьютера с помощью проводов Dupont.
- **Настройка программного обеспечения**: установка TPM2-Tools, Python и Scapy на Raspberry Pi.
- **Извлечение ключа шифрования**: использование TPM2-Tools для извлечения ключа шифрования из чипа TPM.

b) Атака на процесс загрузки:

- **Создание загрузочного USB-накопитель**: использование Rufus для создания загрузочного USB-накопителя с дистрибутивом Linux.
- **Изменение загрузчика**: использование GRUB Customizer, чтобы изменить загрузчик на USB-накопителе для загрузки вредоносной версии BitLocker.
- **Загрузка с USB-накопителя**: загрузка компьютера с USB-накопителя.

- **Расшифровка жесткого диска**: вредоносная версия BitLocker расшифровывает жесткий диск компьютера.

5) *Шаги по извлечению ключа BitLocker*

- Подключение Raspberry Pi к TPM-header. Использование провода Dupont для подключения выводов GPIO Raspberry Pi к разъёму TPM компьютера.
- Установка TPM2-Tools, Python и Scapy на Raspberry Pi с использованием авторских инструкций.
- Загрузка Raspberry Pi.
- Выполнение команды для извлечения ключа шифрования из чипа TPM: **python tpm2_extractkey.py -d /dev/tpm0 -o key.bin**
- Ключ шифрования будет сохранен в файле key.bin.

I. Последствия атаки

- **Потеря данных**: атака позволяет злоумышленникам расшифровать данные на компьютере жертвы и получить к ним доступ, включая личные файлы, финансовую информацию и коммерческие секреты. Это может привести к значительным финансовым потерям, репутационному ущербу и юридической ответственности жертвы.
- **Заражение вредоносным ПО**: злоумышленники могут использовать атаку для установки вредоносного ПО на компьютер жертвы, такого как программы-вымогатели, шпионское ПО или ботнеты. Это может дать удалённый контроль над компьютером жертвы, позволяя им красть данные, запускать атаки на другие системы или шпионить за действиями жертвы.
- **Отказ в обслуживании**: атака может быть превращена в атаку типа отказа в обслуживании компьютера жертвы, не позволяя ей получить доступ к своим данным или использовать свой компьютер в рабочих или личных целях. Это приведёт к потере производительности, финансовым потерям и репутационному ущербу.
- **Компрометация конфиденциальной информации**: атака может быть использована для компрометации конфиденциальной информации, такой как государственные секреты, военные планы или корпоративные коммерческие секреты. Это имеет серьёзные последствия для национальной безопасности, общественного спокойствия и экономической стабильности.

J. Контрмеры

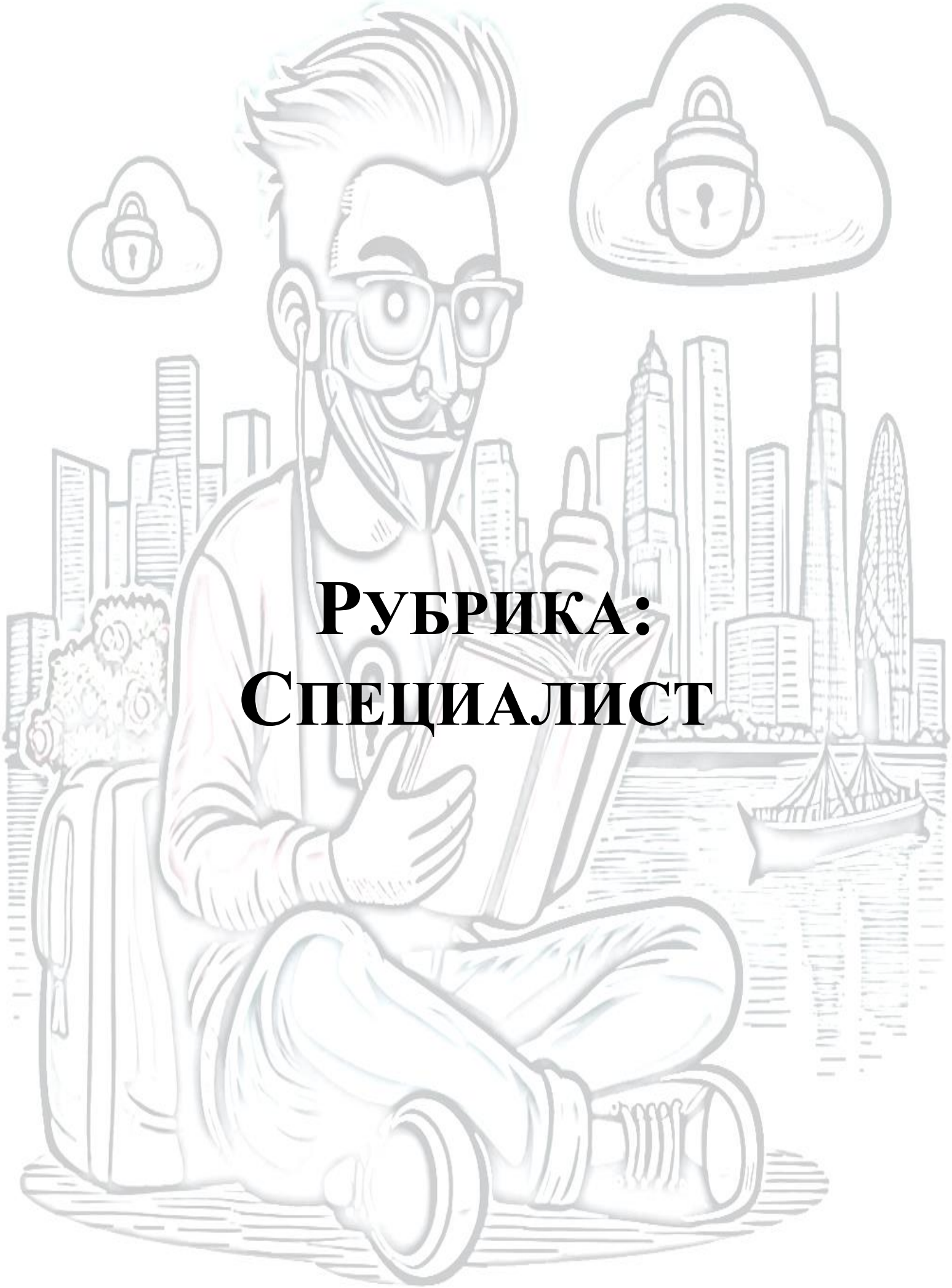
Несколько контрмер и рекомендаций по устранению выявленных уязвимостей и повышению общей безопасности BitLocker:

- **Использование надёжного пароля BitLocker**: надёжный пароль затрудняет злоумышленнику принудительное использование ключа шифрования.
- **Включение дополнительных функций безопасности**: BitLocker предлагает несколько дополнительных функций безопасности, таких как двухфакторная аутентификация и безопасная загрузка, которые могут помочь защитить от атак.
- **Поддержание актуальности операционной системы и программного обеспечения компьютера**: обновления программного обеспечения часто включают исправления безопасности для защиты от уязвимостей.
- **Использование аппаратного TPM-чипа**: аппаратные TPM-чипы более безопасны, чем программные TPM-чипы.

1) *Предотвращение сниффинга TPM*

Есть несколько вещей, которые можно сделать, чтобы предотвратить перехват TPM, в том числе:

- **Включение режима BitLocker "только для доверенного модуля"** значительно затрудняет извлечение ключа BitLocker из чипа TPM.
- **Поддержание операционной системы и встроенного ПО компьютера в актуальном состоянии** помогает защититься от уязвимостей, которые могут быть использованы для получения доступа к шине LPC.
- **Использование надёжного пароля или кодовой фразы для ключа шифрования BitLocker** затруднит злоумышленнику принудительное использование ключа шифрования.



Рубрика: Специалист


ANONSUDAN

Аннотация – В этом документе представлен анализ группы Anonymous Sudan и различным аспектам деятельности группы, включая их происхождение, мотивацию, методы и последствия их действий.

Выводы, полученные в результате этого анализа, полезны экспертам по кибербезопасности, ИТ-специалистам и правоохранительным органам. Понимание методов работы Anonymous Sudan дает этим заинтересованным сторонам знания, позволяющие предвидеть потенциальные атаки, укреплять свою защиту и разрабатывать эффективные контрмеры против аналогичных хакерских угроз.

A. Особенности группы и мотивация

Anonymous Sudan – хактивистская группа, получившая известность благодаря серии распределённых атак типа "отказ в обслуживании" (DDoS) на различные глобальные цели. Группа представляет собой уникальное сочетание политических и религиозных мотиваций, используя цифровые инструменты для продвижения своих целей и создания сбоев. Они нацелены на организации, связанные с инфраструктурой и ключевыми услугами, в том числе в государственном и частном секторах.

Группа работает с января 2023 года, с тех пор постоянно попадая в заголовки газет по всему миру, отдавая предпочтение таким странам как Швеции, Нидерландам и Дании. Они также нацелились на такие страны, как Израиль, ОАЭ, Франция и Австралия. Что касается недавних действий – атака на телекоммуникационного провайдера Sudachad и ChatGPT из-за поддержки сотрудником OpenAI Израиля

Однако до сих пор ведутся серьёзные споры об истинном происхождении и принадлежности к Anonymous Sudan, а использование русского языка в сообщениях, что с точки зрения всех западных стран однозначно говорит об истинном происхождение (или скорее умственном развитии).

Группа набирает членов через онлайн-платформы, используя влияние других групп, предлагая финансовые стимулы и внедряя процесс предварительного отбора для обеспечения определённого уровня квалификации среди новобранцев в отличие от более широкого коллектива Anonymous, который известен тем, что приветствует любого независимо от уровня квалификации. Эти методы помогают группе поддерживать операционную безопасность и эффективность. Группа часто набирает новых участников через онлайн-платформы, хакерские форумы и каналы социальных сетей, Telegram. Эти платформы позволяют им охватить широкую аудиторию, интересующихся кибербезопасностью, хакерством и активизмом.

Anonymous Sudan утверждает, что её мотивами являются как политические, так и религиозные убеждения. Например, они ссылались на геополитические события, которые они воспринимают как антимусульманские, в качестве катализатора своих действий. Атаки на шведские и датские организации и объекты критической инфраструктуры были в ответ на сожжение копии Корана в Швеции.

B. Тактика

Группа в основном использует DDoS-атаки, используя комбинацию веб-DDoS-атак и чередующихся потоков UDP / SYN для нарушения работы сервисов. Они также компрометируют учётные записи электронной почты. Группа часто доводит дело до конца, атакуя цели, которым они публично угрожают, и пагубное воздействие этих атак часто демонстрируется с использованием инструментов достижимости. Они также часто ретроспективно берут на себя ответственность за несвязанные перебои в обслуживании.

Группа использует стандартные услуги DDoS-атак по найму и аренду ботнетов, отходя от традиционного менталитета и возможностей и ведя себя скорее как APT-группа. Они используют инфраструктуру общедоступных облачных серверов для генерации трафика и проведения атак. Атаки группы происходят с десятков тысяч уникальных IP-адресов источников, при этом трафик UDP достигает 100 Гбит /с.

Перед началом атаки группа часто заранее угрожает целям. Обычно это делается с помощью публичных постов в социальных сетях или других онлайн-платформах, где они объявляют о своих намерениях и причинах своих действий. Такой подход не только служит предупреждением для намеченной цели, но и помогает привлечь внимание к делу и действиям группы.

Группа использует разные подходы к DDoS-атакам:

- **Атаки с высокой пропускной способностью**: отправляются большие сетевые пакеты / большие объёмы сетевого трафика для увеличения числа TCP-атак; максимальная наблюдаемая пропускная способность атаки составила 284 Гбит / с и 57 Mpps

- **Флуд-атаки**: комбинация различных UDP, DNS, SSDP SYN-атак для «подавления» цели.
- **Веб-DDoS-атаки**: нарушают работу веб-сервисов, перегружая цель потоком интернет-трафика.
- **Инфраструктура серверов публичного облака**: облачные сервисы для формирования трафика и потоков атак, что обеспечивает анонимность и затрудняет точное определение источника атак.

C. Целевой профиль

Операционные схемы группы и секторы, на которые они нацелены, предполагают стратегический подход к их хактивизму, направленный на то, чтобы вызвать сбои и привлечь внимание к их причинам. Вот несколько ключевых моментов, характеризующих жертв.

Период активности – группа была наиболее активна в феврале и апреле, и за эти месяцы произошло значительное количество атак.

Целевые страны и секторы

- Наиболее упоминаемые страны: Швеция, Израиль, США, Нидерланды, Дания, Австралия, Франция, Германия, ОАЭ, Иран
- Израиль был главной мишенью, более 70 нападений, на долю которых приходится более 20% от общего числа жертв, особенно во время кампании " OpIsrael"
- Скандинавские компании, включая Scandinavian Airlines (SAS), подверглись атаки после антиисламской акции протеста сожжения Корана
- К числу важнейших целевых секторов относятся финансы, авиация, здравоохранение и государственные организации

Публичность и вовлечение сообщества

Группа жаждет публичности и общественного признания, активно взаимодействуя со своей аудиторией и привлекая подписчиков к целевому отбору

1) Пострадавшие компании

В число крупнейших пострадавших компаний входят:

- Технологический гигант Microsoft
- Авиакомпания Air France
- Система онлайн-платежей PayPal
- Корпорация финансовых услуг American Express:
- Компания Cloudflare, занимающаяся веб-инфраструктурой и безопасностью веб-сайтов, подверглась DDoS-атаке, в результате которой её веб-сайт был отключён на несколько минут
- Государственная дубайская авиакомпания Flydubai:
- Информационное агентство Associated Press (AP)

2) Отрасли

- **Транспорт**: системы бронирования, базы данных клиентов и другие сетевые системы.
- **Госсектор**: общедоступные веб-сайты, системы электронной почты и другая сетевая инфраструктура.
- **Образование**: информационные системы для учащихся, платформы онлайн-обучения и системы электронной почты.
- **Здравоохранение**: системы электронной медицинской документации, системы записи на приём и другие сетевые медицинские устройства.
- **Финансы**: системы онлайн-банкинга, базы данных клиентов и системы электронной почты.
- **Производство**: системы промышленного контроля, системы управления цепочками поставок и другие сетевые системы.
- **Технология**: общедоступные веб-сайты, базы данных клиентов и облачные сервисы.

3) Последствия

- **Нарушение работы сервисов**: Основным методом атаки группы является DDoS, который может нарушить работу сервисов в различных секторах, включая финансы, авиацию, здравоохранение и государственные структуры. Это может привести к значительным перебоям в обслуживании, затрагивающим как предприятия, так и потребителей
- **Экономический эффект**: Затраты на смягчение последствий DDoS-атак могут быть значительными. Сюда входят затраты на дополнительную полосу пропускания, аппаратное и программное обеспечение для предотвращения атак, а также потенциальная потеря доходов из-за перебоев в обслуживании
- **Общественное восприятие и доверие**: огласка, вызванная этими атаками, может повлиять на общественное восприятие и доверие к объектам, которым они подвергаются, и на способность страны защищаться от кибер-угроз
- **Распределение ресурсов**: реагирование на эти атаки и смягчение их последствий требует значительных ресурсов, что может отвлечь ресурсы от других критически важных областей
- **Потенциал эскалации**: риск того, что со временем группа может ужесточить свою тактику, потенциально перейдя от DDoS-атак к более разрушительным формам кибер-атак
- **Политическое воздействие**: Нападения группы часто носят политический характер, что может усугубить существующую напряжённость и конфликты

4) Последствия [Транспортная отрасль]

- **Перебои в обслуживании**: Атаки могут привести к нарушению работы критически важных служб, таких как выполнение рейсов, продажа билетов и обслуживание клиентов, что доставит неудобства пассажирам и может вызвать проблемы с безопасностью.
- **Экономические потери**: Авиакомпании и другие транспортные организации могут понести экономические потери из-за простоев в

обслуживании, затрат на смягчение последствий атак и потенциальной компенсации пострадавшим клиентам.

- **Репутационный ущерб**: Повторяющиеся атаки могут нанести ущерб репутации компаний-мишеней, что приведёт к потере доверия клиентов и потенциально повлияет на будущий бизнес.
- **Оперативная нагрузка**: Реагирование на DDoS-атаки и восстановление после них может привести к перегрузке операционных возможностей целевых объектов, требуя значительных ресурсов и потенциально отвлекая внимание от других важных задач

5) *Последствия [Государственная промышленность]*

- **Нарушение работы государственных служб**: правительственные веб-сайты и онлайн-сервисы могут быть переведены в автономный режим, что повлияет на доступ граждан к важной информации и услугам
- **Экономические издержки**: Финансовые последствия включают затраты на устранение последствий атак и потенциальную потерю производительности из-за простоя службы
- **Подрыв общественного доверия**: повторяющиеся атаки могут подорвать доверие общественности к способности правительства обеспечить безопасность своей цифровой инфраструктуры
- **Нагрузка на ресурсы**: Государственным учреждениям, возможно, потребуется выделить значительные ресурсы для реагирования на эти атаки и восстановления после них, которые в противном случае могли бы быть использованы для оказания государственных услуг.
- **Последствия для безопасности**: если правительственные сети будут восприниматься как уязвимые, это может подтолкнуть других злоумышленников к дальнейшим атакам

6) *Последствия [Индустрияобразования]*

- **Нарушение работы образовательных служб**: DDoS-атаки могут нарушить доступность образовательных онлайн-ресурсов, включая веб-сайты, системы управления обучением и виртуальные классы. Это может затруднить доступ учащихся к образованию и повлиять на их успеваемость.
- **Экономические издержки**: Финансовые последствия включают затраты на устранение последствий атак и потенциальную потерю производительности из-за простоя службы.
- **Подрыв общественного доверия**: повторяющиеся атаки могут подорвать доверие персонала, семей и студентов к способности учреждения обеспечить безопасность своей цифровой инфраструктуры.
- **Нагрузка на ресурсы**: образовательным учреждениям, возможно, потребуется выделить значительные ресурсы для реагирования на эти атаки и восстановления после них.
- **Последствия для безопасности**: если образовательные сети будут восприниматься как уязвимые, это может подтолкнуть других злоумышленников к дальнейшим атакам.

7) *Последствия [Индустрияздравоохранения]*

- **Нарушение работы критически важных служб**: DDoS-атаки могут нарушить доступность основных медицинских услуг, таких как электронные медицинские карты, телемедицина и онлайн-порталы для пациентов. Это может затруднить оказание медицинской помощи пациентам и повлиять на важнейшие медицинские операции
- **Нарушение безопасности пациентов**: если системы здравоохранения нарушены, безопасность пациентов может быть поставлена под угрозу, поскольку доступ к медицинской информации и своевременная помощь пациентам имеют решающее значение
- **Экономические издержки**: Учреждения здравоохранения могут столкнуться со значительными расходами, связанными со смягчением последствий атак, восстановлением услуг и потенциальной юридической ответственностью, если данные пациента будут скомпрометированы
- **Потеря конфиденциальности**: Кибер-атаки могут привести к раскрытию конфиденциальной информации о пациентах, что приведёт к нарушению конфиденциальности и потенциальной краже личных данных или мошенничеству
- **Ущерб репутации**: Повторяющиеся атаки могут нанести ущерб репутации медицинских работников, что приведёт к потере доверия среди пациентов и общественности
- **Перенаправление ресурсов**: Реагирование на DDoS-атаки и восстановление после них может потребовать значительных ресурсов, отвлекая внимание от ухода за пациентами и других важных услуг

8) *Последствия [Финансовая отрасль]*

- **Нарушение работы финансовых служб**: Атаки могут нарушить доступность онлайн-банкинга, обработки платежей и других финансовых услуг, затрагивая как предприятия, так и потребителей
- **Экономические издержки**: Финансовые учреждения могут столкнуться со значительными расходами, связанными со смягчением последствий атак, восстановлением услуг и потенциальной юридической ответственностью, если данные клиентов будут скомпрометированы
- **Потеря доверия клиентов**: повторяющиеся атаки могут нанести ущерб репутации финансовых

учреждений, что приведёт к потере доверия среди клиентов и потенциально повлияет на будущий бизнес
- **Перенаправление ресурсов**: Реагирование на DDoS-атаки и восстановление после них может потребовать значительных ресурсов, отвлекая внимание от других важных служб
- **Последствия для безопасности**: DDoS-атаки могут служить прикрытием для более разрушительной кибер-деятельности, такой как проникновение в системы и утечка данных, создавая дополнительную нагрузку на и без того ограниченные ресурсы

9) *Последствия [Обрабатывающая промышленность]*
- **Нарушение работы**: DDoS-атаки могут нарушить доступность основных производственных служб, таких как системы производственного контроля, управление цепочками поставок и порталы обслуживания клиентов
- **Экономические издержки**: Производственные предприятия могут столкнуться со значительными расходами, связанными с устранением последствий атак, восстановлением служб и потенциальной потерей производительности из-за простоя служб
- **Потеря интеллектуальной собственности**: Многие атаки в производственном секторе включают кражу интеллектуальной собственности, которая может привести к потере доли рынка или прекращению производственной деятельности
- **Ущерб репутации**: Повторяющиеся атаки могут нанести ущерб репутации компаний-производителей, что приведёт к потере доверия среди клиентов и потенциально повлияет на будущий бизнес
- **Перенаправление ресурсов**: Реагирование на DDoS-атаки и восстановление после них может потребовать значительных ресурсов, отвлекающих внимание от производства и других важных услуг

10) *Последствия [Технологическая отрасль]*
- **Нарушение работы сервисов**: DDoS-атаки могут привести к отключению веб-сайтов и онлайн-сервисов, что повлияет на доступность цифровых продуктов и услуг
- **Экономические издержки**: Компании могут столкнуться со значительными расходами, связанными с устранением последствий атак, восстановлением служб и потенциальной потерей доходов из-за простоя служб
- **Ущерб репутации**: Повторяющиеся атаки могут нанести ущерб репутации технологических компаний, что приведёт к потере доверия среди клиентов и потенциально повлияет на будущий бизнес
- **Перенаправление ресурсов**: Реагирование на DDoS-атаки и восстановление после них может потребовать значительных ресурсов, отвлекая внимание от инноваций и других важных услуг
- **Последствия для безопасности**: DDoS-атаки могут служить прикрытием для более разрушительной кибер-деятельности, такой как проникновение в системы и вывоз данных

BIANLIAN

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.

A. 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 кибер-угроз 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

B. 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, причём 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.

C. 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.

D. 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

E. 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

F. 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

G. 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

H. 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, что программа-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.

I. 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.

1) 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.

2) Atera

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

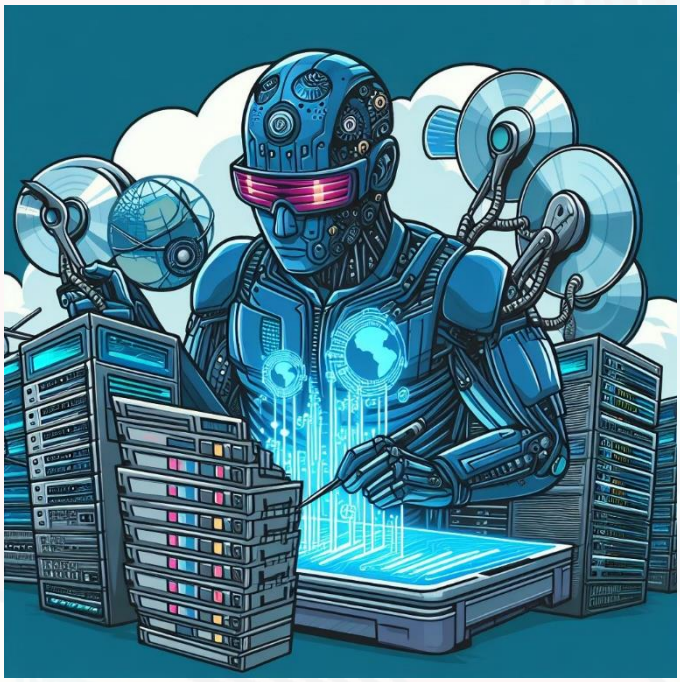
- **Удалённый мониторинг и управление (RMM)**: Atera обеспечивает мониторинг и оповещения в режиме реального времени, автоматизацию ИТ, управление исправлениями и расширенное удалённое обслуживание. Это позволяет BianLian group отслеживать взломанные системы и управлять ими в режиме реального времени.
- **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

3) 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

Уязвимость Atlassian / CVE-2023-22518



Аннотация – В этом документе представлен анализ уязвимости CVE-2023–22518, связанной с неправильной авторизацией в Atlassian Confluence Data Center and Server. Анализ будет охватывать различные аспекты уязвимости, включая её обнаружение, воздействие, методы эксплуатации и стратегии смягчения последствий.

Специалисты по безопасности найдут этот анализ особенно полезным, поскольку он предоставляет оперативную информацию, включая показатели компрометации и подробные шаги по смягчению последствий. Понимая первопричины, методы эксплуатации и эффективные контрмеры, эксперты по безопасности могут лучше защитить свои организации от подобных угроз в будущем.

A. Введение

CVE-2023-22518 – уязвимость неправильной авторизации, которая затрагивает все версии Confluence Data Center. Эта уязвимость позволяет злоумышленнику, не прошедшему проверку подлинности, перезагрузить Confluence и получить контроль над уязвимой системой.

Изначально уязвимости был присвоен критический балл серьёзности 9,1 в CVSS, но позже он был повышен до 10, что является наивысшим показателем критичности, из-за изменения масштаба атаки и наблюдения за активными эксплойтами и сообщениями об исполнителях угроз, использующих программы-вымогатели.

Atlassian выпустила исправленные версии Confluence для решения CVE-2023-22518. Исправленными версиями являются 7.19.16, 8.3.4, 8.4.4, 8.5.3 и 8.6.1. Кроме того, рекомендуется ограничить внешний доступ к серверам Confluence до тех пор, пока не будет применено обновление. Эта уязвимость не затрагивает пользователей Atlassian Cloud.

B. Подробности атак

Уязвимость была обнаружена из-за разницы в исправлениях между исправленной и не исправленной версиями ПО и заключается в конечных точках "восстановления настроек" в экземплярах Confluence, которые были доступны пользователям, не прошедшим проверку подлинности. Конечные точки являются частью функций восстановления системы и предназначены для использования администраторами для восстановления экземпляра Confluence из резервной копии. Конечные точки, к которым должен иметь доступ только пользователь-администратор, включают /json/setup-restore.action, /json/setup-restore-local.action и /json/setup-restore-progress.action. Используя их, возможно загрузить специально созданный zip-архивный файл через HTTP Post-запрос. Zip-файл может содержать веб-шелл для выполнения произвольных команд.

1) Схема атаки

Процесс атаки CVE-2023–22518 включает в себя несколько этапов, которые позволяют злоумышленнику, не прошедшему проверку подлинности, использовать уязвимости неправильной авторизации:

- **Использование параметров "Восстановления настроек"**: конечные точки "setup restore" в Confluence предназначены для администраторов для восстановления экземпляра Confluence из резервной копии. Из-за уязвимости эти конечные точки доступны для не прошедших проверку подлинности пользователей
- **Загрузка вредоносного zip-файла**: злоумышленник создаёт специально разработанный zip-файл, который при загрузке на уязвимый сервер Confluence через скомпрометированные конечные точки может либо уничтожить экземпляр Confluence, что приведёт к потере данных, либо содержать веб-шелл для удалённого выполнения кода (RCE) на сервере
- **Получение несанкционированного доступа**: если атака включает загрузку веб-шелла, злоумышленник может выполнять произвольные команды на сервере. Этот уровень доступа позволяет злоумышленнику выполнять все административные действия, доступные администраторам экземпляра Confluence, эффективно получая контроль над системой
- **Развёртывание программ-вымогателей**: в некоторых случаях злоумышленники использовали эту уязвимость для развёртывания программ-вымогателей, таких как Cerber ransomware. При запуске программа-вымогатель шифрует файлы на локальных дисках и общих сетевых ресурсах, добавляя к зашифрованным файлам определённое расширение файла (например, LOCK3D) и требует выкуп за расшифровку данных
- **Последствия**: Успешное использование CVE-2023–22518 может привести к несанкционированному управлению системой, потере данных, сбоям в работе и финансовым затратам из-за развёртывания программ-вымогателей, нарушения работы, получения доступа к конфиденциальной информации, а также манипулированию данными или их удалению.

2) PoC

exploit.py выполняет следующие действия (GitHub https://github.com/ForceFledgling/CVE-2023-22518):

- **Идентификация цели**: скрипт предложит ввести URL уязвимого экземпляра Confluence.
- **Выполнение эксплойта**: затем скрипт использует предоставленный URL-адрес для отправки обработанных запросов точкам "setup restore", таким как /json/setup-restore.action, которые обычно доступны только администраторам, но в уязвимых версиях – обычным пользователям, не прошедшим проверку подлинности, из-за уязвимости.
- **Загрузка вредоносной полезной нагрузки**: эксплойт включает загрузку вредоносного zip-файла, который может содержать веб-шелл или другой вредоносный код, на сервер через скомпрометированные конечные точки.
- **Удалённое выполнение кода (RCE)**: если загруженный zip-файл содержит веб-шелл, злоумышленник может выполнять произвольные команды на сервере, что приведёт к несанкционированному управлению системой.
- **Результат**: административный доступ к экземпляру Confluence, который может быть использован для выполнения дальнейших вредоносных действий, таких как эксфильтрация данных, уничтожение данных или развёртывание программ-вымогателей.

Входящие данные для скрипта будут включать URL целевого экземпляра Confluence и путь к вредоносному zip-файлу. Исходящие данные будут состоять из HTTP-запросов к уязвимым конечным точкам и потенциально загруженной вредоносной полезной нагрузки.

xmlexport-20231109-060519-1.zip – файл предназначен для загрузки в уязвимый Confluence и экземпляр сервера для использования уязвимости неправильной авторизации. При загрузке в уязвимый экземпляр Confluence это может привести к несанкционированной загрузке файлов, потенциально позволяя удалённое выполнение кода или другие уязвимости в системе безопасности.

CVE-2023–22518 в контексте использования файла .jar, например **atlplug.jar** может служить в качестве приложения-бэкдора Confluence для выполнения определённых действий на уязвимом сервере Confluence.

C. Отрасли

Atlassian Confluence используется в ряде отраслей промышленности благодаря своей универсальности в качестве ПО для командной работы:

- **Информационные технологии и услуги**: Confluence широко используется в ИТ-секторе для управления знаниями, документации и совместной работы над проектами по разработке ПО
- **Программное обеспечение**: компании-разработчики ПО используют Confluence для управления документацией по своему продукту, отслеживания прогресса проекта и облегчения общения между членами команды
- **Финансовые услуги**: Финансовая индустрия использует Confluence для систематизации конфиденциальной информации, ведения документации по соблюдению нормативных требований и поддержки внутреннего делопроизводства
- **Образование**: Образовательные учреждения могут использовать Confluence в качестве базы знаний для ИТ-поддержки, а также для управления образовательными материалами и исследованиями и совместного использования с ними
- **Госсектор**: Госучреждения могут использовать Confluence для управления проектами, документацией и создания централизованного хранилища институциональных знаний
- **Здравоохранение**: Организации здравоохранения могут использовать Confluence для управления информационными системами пациентов, документацией исследований и в качестве базы знаний для медицинского персонала

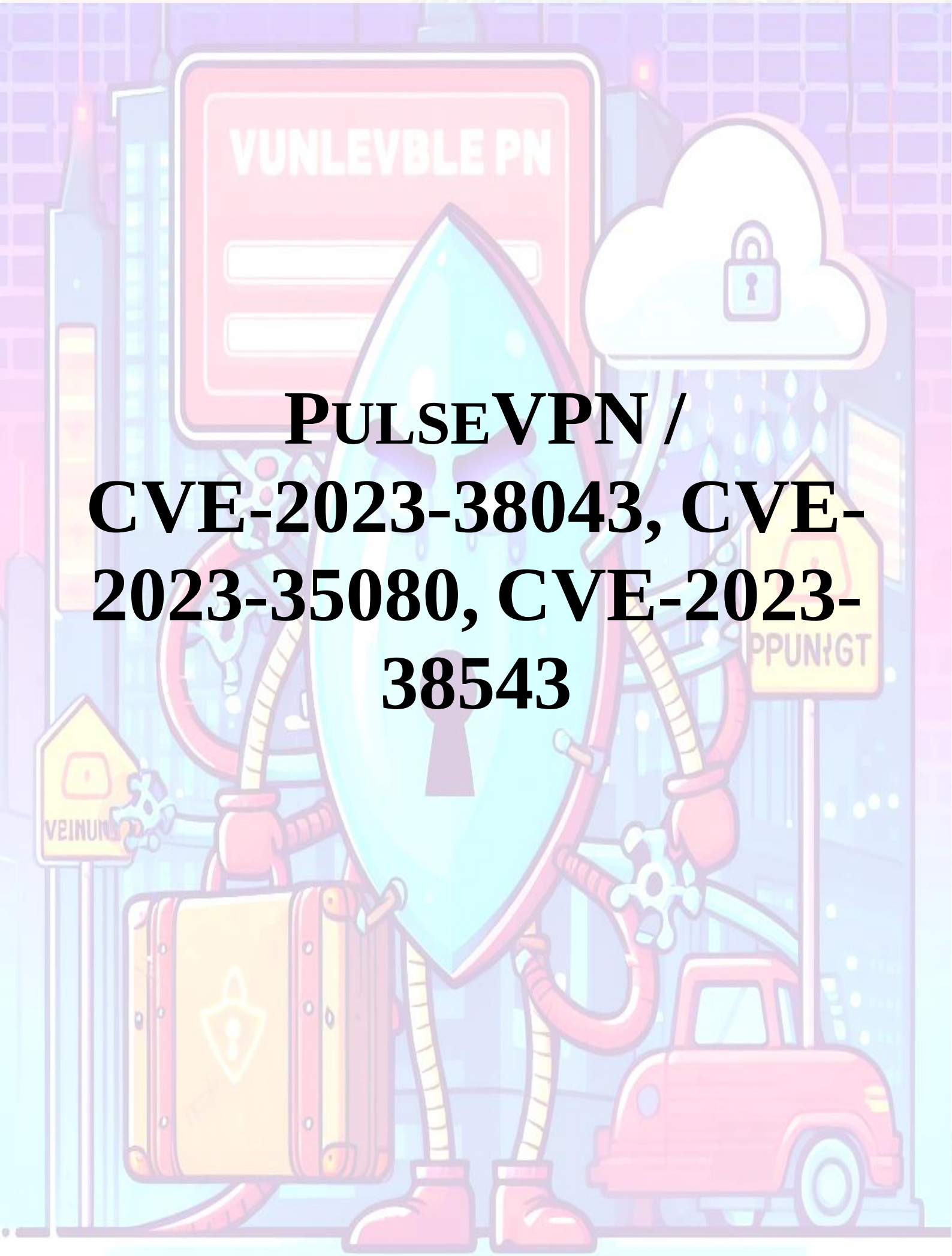
1) Воздействие

Эксплуатация CVE-2023–22518 может привести к:

- **Несанкционированный контроль системы**: Злоумышленники могут получить административный доступ, позволяющий им выполнять любые действия внутри экземпляра Confluence, которые могут нарушить работу и поставить под угрозу конфиденциальные данные
- **Развёртывание программы-вымогателя**: были случаи, когда уязвимость использовалась для развёртывания программы-вымогателя Cerber, что приводило к шифрованию данных и требованиям выкупа, что могло остановить ИТ-операции и привести к финансовым потерям
- **Сбой в работе**: Сброс экземпляра Confluence может нарушить текущие проекты и усилия по совместной работе, что приведёт к задержкам и потенциальной потере данных

2) Последствия

- **Потеря данных**: несанкционированный доступ и потенциальное внедрение программ-вымогателей могут привести к необратимой потере данных, что особенно опасно в отрасли, которая полагается на целостность данных
- **Финансовые затраты**: Затраты, связанные с запросами программ-вымогателей, восстановлением системы и потенциальными штрафами регулирующих органов, могут быть существенными
- **Ущерб репутации**: Нарушения безопасности могут нанести ущерб репутации поставщиков ИТ-услуг, что приведёт к потере доверия и потенциальной потере бизнеса
- **Перераспределение ресурсов**: ИТ-отделам может потребоваться перенаправление ресурсов для устранения уязвимости и её последствий, что может отвлечь внимание от других важных ИТ-инициатив



PULSEVPN / CVE-2023-38043, CVE-2023-35080, CVE-2023-38543

Аннотация – В документе представлен анализ уязвимостей, выявленных в Ivanti Secure Access VPN (Pulse Secure VPN) с их потенциальным воздействием на использующие ПО организации. В анализе рассматриваются различные аспекты этих уязвимостей, включая методы их использования, потенциальные последствия и проблемы, с которыми сталкиваются в процессе эксплуатации.

Документ предоставляет ценную информацию специалистам по кибербезопасности, ИТ-администраторам и другим заинтересованным сторонам в различных отраслях. Понимая технические нюансы, методы эксплуатации и стратегии смягчения последствий, становится возможно повысить уровень безопасности своей организации от подобных угроз.

Этот анализ особенно полезен специалистам по безопасности, стремящимся разобраться в тонкостях уязвимостей VPN и их последствиях для безопасности предприятия. Он также служит ресурсом для ИТ-администраторов, ответственных за поддержание безопасных конфигураций VPN, и для заинтересованных сторон отрасли, заинтересованных в более широком влиянии таких уязвимостей на цифровую безопасность и соответствие требованиям.

A. Введение

Northwave Cybersecurity выявила несколько уязвимостей в Ivanti Secure Access VPN (Pulse Secure VPN). Было обнаружено, что эти уязвимости, в частности CVE-2023–38043, CVE-2023–35080 и CVE-2023–38543, затрагивают программное обеспечение VPN, используемое более чем 40 000 организациями по всему миру. Основная обсуждаемая уязвимость позволяет повысить привилегии из-за драйвера ядра, установленного ПО VPN, который создаёт устройство, доступное для чтения и записи любому пользователю. Это потенциально может привести к повреждению ядра или повышению привилегий.

B. Уязвимости

Уязвимости CVE-2023-38043, CVE-2023-35080, CVE-2023-38543 обнаружены во всех версиях клиента Ivanti Secure Access Client ниже 22.6R1.1 и может позволить злоумышленнику, прошедшему локальную аутентификацию, использовать уязвимую конфигурацию, что потенциально может привести к отказу в обслуживании (DoS) или раскрытие информации. Успешная эксплуатация уязвимости может позволить злоумышленнику получить повышенные привилегии в уязвимой системе. Серьёзность этой уязвимости оценивается как высокая: базовый балл CVSS 3.x составляет 7,8 от NIST и 8,8 от HackerOne, что указывает на значительное влияние на конфиденциальность, целостность и доступность.

1) Схема атаки

- **Первоначальный доступ:** злоумышленник должен сначала получить возможность выполнять код в целевой системе, что достигается различными способами, такими как фишинг, использование другой уязвимости или получение легитимного доступа к учётной записи пользователя в системе.
- **Эксплуатация:** как только злоумышленник получит возможность выполнить код в целевой системе, он использует уязвимую конфигурацию клиента безопасного доступа Ivanti путём отправки специально созданного запроса компоненту клиента Ivanti Secure Access Client.
- **Отказ в обслуживании.** Успешная эксплуатация уязвимости может привести к DoS-состоянию, при котором затронутая машина перестанет отвечать на запросы или выйдет из строя.
- **Компрометация системы.** В некоторых сценариях уязвимость может быть использована для получения повышенных привилегий или выполнения произвольного кода, что приводит к полной компрометации системы.

2) Затронутые отрасли

CVE затрагивают различные отрасли, которые используют VPN клиент для безопасного удалённого доступа к своим сетям.

- **Здравоохранение.** Больницы и поставщики медицинских услуг используют VPN-клиенты, для безопасного удалённого доступа к записям пациентов и внутренним системам, что делает их потенциальными целями.
- **Финансовые услуги.** Банки, страховые компании и другие финансовые учреждения полагаются на безопасный VPN-доступ для удалённых сотрудников и защиту конфиденциальных финансовых данных.
- **Государственный сектор:** Государственные учреждения используют VPN-клиенты для обеспечения безопасной связи и удалённого

доступа к конфиденциальным правительственным ресурсам.

- **Образование.** Университеты и учебные заведения используют VPN-клиенты для безопасного доступа к академическим ресурсам, а также для обеспечения удалённого обучения и администрирования.
- **Технологии и ИТ-услуги.** Компании технологического сектора, включая поставщиков ИТ-услуг, используют VPN-клиенты для безопасного удалённого доступа к сетевым ресурсам и клиентским средам.
- **Производство и критическая инфраструктура.** Производственные компании и поставщики критической инфраструктуры используют VPN-клиенты для безопасного подключения к системам промышленного управления и сетям операционных технологий.
- **Розничная торговля и потребительские товары.** Розничные торговцы используют VPN-клиенты для безопасного удалённого доступа к управлению запасами, системам торговых точек и другим критически важным бизнес-приложениям.

a) Здравоохранение

В текущей отрасли последствия использования такой уязвимости могут включать:

- **Нарушение предоставления медицинских услуг.** Атака типа «отказ в обслуживании» может нарушить доступ к критически важным системам здравоохранения и данным пациентов, что повлияет на уход за пациентами и потенциально приведёт к задержкам в лечении или диагностике.
- **Компрометация конфиденциальных данных.** Повышенные привилегии могут позволить злоумышленникам получать доступ, изменять или удалять конфиденциальные данные пациентов, нарушая конфиденциальность пациентов и потенциально приводя к краже личных данных или мошенничеству.
- **Нарушения нормативных требований и нормативных требований.** На медицинские организации распространяются строгие нормативные требования по защите данных пациентов, поэтому последствия уязвимости могут привести к штрафам со стороны регулирующих органов и юридическим последствиям.
- **Ущерб репутации.** Инцидент безопасности может нанести ущерб репутации затронутой организации здравоохранения, что приведёт к потере доверия среди пациентов и партнёров.
- **Финансовые затраты:** Реагирование на нарушение безопасности и восстановление после него может быть дорогостоящим, включая расходы, связанные с расследованием, исправлением ситуации, судебными издержками и потенциальными выплатами или штрафами.

b) Индустрия финансовых услуг

В текущей отрасли последствия использования такой уязвимости могут включать:

- **Нарушение финансовых операций.** Атака типа «отказ в обслуживании» может нарушить доступ к критически важным финансовым системам, повлиять на транзакции, торговлю и другие срочные операции, что потенциально может привести к финансовым потерям.
- **Кража конфиденциальных финансовых данных.** Повышенные привилегии могут позволить злоумышленникам получить доступ, изменить или украсть конфиденциальные финансовые данные, включая учётные записи клиентов, истории транзакций и собственные торговые алгоритмы, что приведёт к финансовому мошенничеству и конкурентному ущербу.
- **Нарушения нормативных требований и требований:** к финансовым учреждениям предъявляются строгие нормативные требования в отношении защиты данных и кибербезопасности. Нарушение безопасности, вызванное этой уязвимостью, может привести к штрафам со стороны регулирующих органов, санкциям и усилению контроля.
- **Репутационный ущерб:** инциденты безопасности могут серьёзно подорвать репутацию финансовых учреждений, подрывая доверие клиентов и потенциально приводя к потере бизнеса, поскольку клиенты перемещают свои активы в кажущиеся более безопасными учреждения.
- **Финансовые затраты.** Затраты, связанные с реагированием на нарушение безопасности и восстановлением после него, могут быть значительными, включая криминалистические расследования, исправление системы, судебные издержки и потенциальную компенсацию пострадавшим клиентам.

c) Государственный сектор

В текущей отрасли последствия использования такой уязвимости могут включать:

- **Нарушение предоставления основных услуг:** госучреждения предоставляют населению основные услуги, включая службы экстренной помощи, социальные услуги и управление инфраструктурой. DoS-атака может нарушить работу этих критически важных служб, что повлияет на общественную безопасность и благосостояние.
- **Раскрытие конфиденциальной информации.** Правительственные учреждения обрабатывают конфиденциальную информацию, включая личные данные граждан, секретную информацию

национальной безопасности и данные критической инфраструктуры. Полная компрометация системы может привести к раскрытию такой информации с серьёзными последствиями для национальной безопасности и конфиденциальности личности.

- **Потеря общественного доверия.** Любое нарушение или сбой в работе государственных служб из-за инцидента в области кибербезопасности может привести к значительной потере общественного доверия к государственным учреждениям. Восстановление этого доверия может оказаться долгим и трудным процессом.
- **Нормативно-правовые последствия:** Государственные учреждения подчиняются строгим нормативным и правовым нормам в отношении защиты данных и кибербезопасности. Нарушение, вызванное этой уязвимостью, может привести к судебным разбирательствам, расследованиям и наложению штрафов.
- **Финансовые последствия:** Реагирование на инциденты кибербезопасности и восстановление после них может оказаться дорогостоящим. Сюда входят затраты, связанные с криминалистическими расследованиями, восстановлением системы, потенциальными юридическими обязательствами и мерами по предотвращению будущих инцидентов.

d) Образовательная индустрия

В текущей отрасли последствия использования такой уязвимости могут включать:

- **Нарушение образовательных услуг.** Атака может нарушить доступ к системам управления обучением, виртуальным классам и другим онлайн-образовательным ресурсам.
- **Раскрытие конфиденциальных данных.** Если уязвимость приведёт к компрометации системы, конфиденциальные данные, такие как записи студентов, данные исследований и личная информация преподавателей и студентов, могут стать публично доступными.
- **Вопросы регулирования и соответствия:** образовательные учреждения часто подчиняются правилам, касающимся защиты данных учащихся. Нарушение безопасности может привести к несоблюдению этих правил, что приведёт к юридическим и финансовым последствиям.
- **Репутационный ущерб:** Инцидент безопасности может нанести ущерб репутации учебного заведения, что потенциально может повлиять на набор студентов и партнёрские отношения с другими организациями.
- **Финансовые затраты.** Затраты, связанные с реагированием на нарушение безопасности, включая расследования, исправление системы и потенциальную юридическую ответственность, могут быть значительными для образовательных учреждений.

e) Отрасль технологий и ИТ-услуг

В текущей отрасли последствия использования такой уязвимости могут включать:

- **Нарушение ИТ- и технологических услуг.** Атака может нарушить доступ к критически важной ИТ-инфраструктуре и услугам, затрагивая как поставщиков услуг, так и их клиентов. Это может привести к простоям, снижению производительности и нарушению соглашений об уровне обслуживания (SLA).
- **Компрометация конфиденциальных данных.** Уязвимость потенциально может привести к полной компрометации системы, обеспечивая несанкционированный доступ к конфиденциальным данным, таким как интеллектуальная собственность, исходный код, данные клиентов и внутренние коммуникации. Это может иметь серьёзные последствия для конфиденциальности и целостности данных.
- **Регуляторные риски и риски, связанные с соблюдением требований.** Многие компании, занимающиеся технологиями и ИТ-услугами, подчиняются нормативным требованиям, касающимся защиты данных и кибербезопасности. Атака может привести к несоблюдению требований, что приведёт к штрафам, судебным искам и усилению контроля со стороны регулирующих органов.
- **Репутационный ущерб.** Репутация компаний, предоставляющих технологические и ИТ-услуги, во многом зависит от их способности защитить свои собственные данные и данные своих клиентов. Инцидент безопасности может подорвать доверие, что потенциально может привести к потере клиентов и трудностям в приобретении нового бизнеса.
- **Финансовые затраты.** Финансовые последствия реагирования на нарушения безопасности и восстановления после них могут быть существенными. Затраты могут включать криминалистические расследования, восстановление системы, судебные издержки и компенсации пострадавшим сторонам.

f) Отрасль производства и критической инфраструктуры

В текущей отрасли последствия использования такой уязвимости могут включать:

- **Нарушение операционной деятельности.** DoS-атака может нарушить доступ к критически важным системам и сетям, затрагивая производственные линии, управление цепочками поставок и среду операционных технологий.

- **Компрометация конфиденциальных данных.** Повышенные привилегии могут позволить злоумышленникам получить доступ, изменить или украсть конфиденциальные данные, включая запатентованные производственные процессы, данные систем управления инфраструктурой и информацию о сотрудниках.
- **Риски безопасности.** В критически важных секторах инфраструктуры, таких как энергетика, водоснабжение и транспорт, нарушение системы может создать прямые риски для безопасности населения и окружающей среды.
- **Нарушения нормативных требований и требований.** Многие производственные организации и организации критической инфраструктуры подчиняются нормативным требованиям в отношении кибербезопасности. Нарушение безопасности может привести к несоблюдению требований, что приведёт к штрафам и судебным искам.
- **Репутационный ущерб.** Инцидент безопасности в этих отраслях может привести к потере доверия со стороны клиентов, партнёров и регулирующих органов, что потенциально повлияет на будущие возможности бизнеса.
- **Финансовые затраты.** Финансовые последствия нарушения безопасности могут быть значительными, включая затраты на реагирование на инциденты, восстановление системы и потенциальную юридическую ответственность.

g) Розничная торговля и производство потребительских товаров

В текущей отрасли последствия использования такой уязвимости могут включать:

- **Нарушение операций розничной торговли.** Атака типа «отказ в обслуживании» может нарушить доступ к критически важным системам розничной торговли, что повлияет на продажи, управление запасами и обслуживание клиентов, потере дохода.
- **Компрометация конфиденциальных данных.** Если уязвимость приводит к компрометации системы, конфиденциальные данные и платёжная информация клиентов, конфиденциальные бизнес-данные и информация о сотрудниках, могут стать доступными.
- **Вопросы регулирования и соответствия.** Розничные торговцы часто подчиняются правилам, касающимся защиты данных потребителей. Нарушение безопасности может привести к несоблюдению этих правил, что приведёт к юридическим и финансовым последствиям.
- **Репутационный ущерб.** Инцидент безопасности может нанести ущерб репутации ритейлера, что потенциально повлияет на лояльность клиентов и ценность бренда.
- **Финансовые затраты.** Затраты, связанные с реагированием на нарушение безопасности, включая расследования, исправление системы и потенциальную юридическую ответственность, могут быть значительными для организаций розничной торговли.

C. Детали

IOCTL 0x80002018 связан с уязвимой функцией в callback'е IRP_MJ_DEVICE_CONTROL драйвера ядра. Эта функция предназначена для обработки кодов управления вводом-выводом (IOCTL), которые отправляются из приложений пользовательского режима драйверу. Код, обрабатывающий этот IOCTL, содержит уязвимость повышения привилегий из-за следующей последовательности операций:

- Загружается указатель на входные данные, переданные из пользовательского режима (системного буфера).
- Первое значение внутри этого ввода принимается как указатель на структуру, специфичную для драйвера.
- Внутри этой структуры загружается указатель по смещению +28h.
- Указатель на смещение +50h внутри памяти, на которое указывает предыдущий указатель, передаётся API ядра IoCsqRemoveIrp.
- Кроме того, второй аргумент, предоставляемый вызову IoCsqRemoveIrp, который находится в регистре RDX, также находится под контролем пользователя.

Функция IoCsqRemoveIrp — это API ядра, который удаляет IRP (пакет запроса ввода-вывода) из очереди с помощью указателей функций (callback), содержащихся в первом аргументе, переданном API. Уязвимость возникает потому, что пользователь контролирует этот первый аргумент, что означает, что он может манипулировать указателями функций, используемыми IoCsqRemoveIrp, для выполнения произвольного кода с привилегиями ядра.

Сама функция IoCsqRemoveIrp относительно проста и использует процедуры диспетчеризации очереди для удаления, указанного IRP из очереди. Однако критическая проблема безопасности здесь заключается в том, что пользователь может управлять регистрами RCX и RDX, которые используются в качестве аргументов функции. Внутри функции есть несколько мест, где указатель загружается из первого аргумента (RCX) и затем передаётся в _guard_dispatch_icall. Эта внутренняя функция предназначена для вызова любого указателя функции в регистре RAX, но у нее есть существенное ограничение: указатель в RAX должен находиться в начале допустимой функции, которая является частью образа ядра. Это

означает, что функции шеллкода или не-изображения ядра не могут быть вызваны напрямую.

Таким образом, уязвимость в коде обработки IOCTL позволяет злоумышленнику контролировать указатели функций, используемые IoCsqRemoveIrp, что потенциально может привести к выполнению произвольного кода с привилегиями ядра. Это серьёзный недостаток безопасности, который можно использовать для повышения привилегий, позволяя злоумышленнику с локальным доступом к системе получить полный контроль над ней.

Ограничения, описанные в сценарии с уязвимой обработкой IOCTL в драйвере ядра, иллюстрируют сложность и проблемы разработки надёжного эксплойта для уязвимости ядра. Давайте разберём эти ограничения и их последствия для разработки эксплойтов:

1) Ограничение 1: гарантированный синий экран

Автоматическое освобождение предоставленного пользователем указателя через ExFreePoolWithTag в конце процедуры обработки IOCTL представляет собой серьёзную проблему. Для этой операции требуется действительный указатель ядра. Даже если злоумышленнику удастся предоставить действительный указатель, его освобождение может привести к нестабильности или повреждению ядра, что, вероятно, приведёт к сбою системы (синий экран). Это ограничение значительно усложняет разработку стабильного эксплойта, поскольку требует, чтобы эксплойт либо избегал запуска этого освобождения, либо гарантировал, что освобождение не приведёт к неблагоприятному воздействию на стабильность системы.

2) Ограничение 2: Сильно ограниченный контроль аргументов

Ограниченный контроль над аргументами, передаваемыми функциям, вызываемым IoCsqRemoveIrp через _guard_dispatch_icall, создаёт ещё одну проблему. Эксплойт контролирует регистр RCX (указывающий на область памяти с указателями функций) и, в одном случае, регистр RDX (указывающий на контролируемую область памяти). Однако для других вызовов RDX указывает на область стека, находящуюся вне контроля злоумышленника, а регистр R8, который потенциально может содержать дополнительные данные, не используется в контексте этих вызовов функций. Это ограничение серьёзно влияет на возможности эксплойта манипулировать потоком выполнения вызываемых функций, что затрудняет выполнение произвольного кода без сбоя системы.

3) Ограничение 3: защищенные вызовы

Использование _guard_dispatch_icall в качестве защитной меры со стороны Microsoft ещё больше усложняет разработку эксплойтов. Этот механизм гарантирует, что могут быть вызваны только указатели на легитимные функции в образе ntoskrnl.exe, эффективно предотвращая выполнение произвольного шеллкода или функций вне образа ядра. Найти в ядре последовательность из трех функций, которую можно вызвать с ограниченным доступным управлением аргументами, не вызывая при этом сбоя, является серьёзной проблемой. Это ограничение требует глубокого понимания внутреннего устройства ядра и доступных функций, чтобы определить жизнеспособную цепочку, которая может привести к успешной эксплуатации.

4) Обход синего экрана

Чтобы решить проблему обхода синего экрана после использования уязвимости, предполагается использование последнего вызова функции перед сбоем системы. Идея состоит в том, чтобы предотвратить продолжение выполнения после последнего вызова функции, не вызывая при этом сбоя системы. Предлагаемое решение включает использование функций синхронизации и блокировки, в частности, нацеленных на функцию синхронизации ядра, которая может блокировать весь поток на неопределённый срок, предотвращая тем самым его доступ к вызову ExFreePoolWithTag, который приводит к появлению синего экрана.

Для этой цели выбрана функция KxWaitForSpinLockAndAcquire. Эта функция принимает указатель в регистре RCX и проверяет, не равно ли значение в начале памяти, на которую он указывает, нулю. Если это так, функция входит в цикл, многократно проверяя значение, пока оно не станет нулевым. Установив для первых 8 байт памяти, на которые указывает RCX, ненулевое значение, поток можно заблокировать в бесконечном цикле, эффективно предотвращая появление синего экрана без сбоя системы.

Однако блокировка потока ядра в бесконечном цикле может существенно повлиять на производительность системы, вызывая замедление работы компьютера после многократного выполнения эксплойта. Чтобы решить проблему, эксплойт может установить минимально возможный приоритет потока через API SetThreadPriority() с параметром THREAD_PRIORITY_LOWEST. Это гарантирует, что заблокированный поток получит наименьшее количество процессорного времени, сводя к минимуму его влияние на производительность системы.

Стратегия обхода синего экрана включает в себя:

- Использование функции KxWaitForSpinLockAndAcquire для блокировки потока в бесконечном цикле, не позволяя ему достичь вызова ExFreePoolWithTag.
- Установка минимально возможного приоритета заблокированного потока, чтобы минимизировать его влияние на производительность системы.

5) Уязвимый код

Чтобы добраться до уязвимого кода и правильно настроить входной буфер IOCTL для вызова IoCsqRemoveIrp, в предоставленном фрагменте кода выполняются следующие шаги:

- HANDLE устройства получается путём вызова CreateFile с DEVICE_NAME.
- Входной буфер выделяется и инициализируется нулем с помощью calloc.

- Первые 8 байт входного буфера указывают на начальный_буфер.
- Затем в Initial_buffer устанавливаются указатели со смещениями 0x28 и 0x30, указывающие на buff_28h и buff_30h соответственно.
- Функция DeviceIoControl вызывается с кодом VULN_IOCTL и подготовленным входным буфером.

Фрагмент кода предназначен для выполнения проверок, выполняемых драйвером входного буфера перед вызовом IoCsqRemoveIrp. В частности, это гарантирует, что:

- Первое значение во входном буфере — это ненулевой указатель на другой буфер (initial_buffer).
- Initial_buffer содержит указатели, отличные от NULL, по смещениям +0x28 и +0x30.
- Эти указатели используются для передачи указателя на смещение +0x50 в буфере, на которое указывает buff_28h в качестве первого аргумента IoCsqRemoveIrp.
- Указатель, загруженный со смещения +0x28 (buff_28h), передаётся в качестве второго аргумента функции.

Настраивая таким образом входной буфер и вызывая DeviceIoControl, код достигает уязвимой области кода драйвера, где вызывается IoCsqRemoveIrp, что подтверждается попаданием точки останова в отладчике.

Функция IoCsqRemoveIrp — это API ядра, который удаляет IRP (пакет запроса ввода-вывода) из очереди с помощью указателей функций (callback), содержащихся в первом аргументе, переданном API. Уязвимость в коде обработки IOCTL позволяет злоумышленнику контролировать указатели функций, используемые IoCsqRemoveIrp, что потенциально может привести к выполнению произвольного кода с привилегиями ядра.

6) Управление IoCsqRemoveIrp

Чтобы управлять функцией IoCsqRemoveIrp и подготовить входные данные для выполнения всех внутренних проверок, выполняются следующие шаги:

- Входной буфер настроен на доступ к вызову IoCsqRemoveIrp, гарантируя, что первые 8 байтов входного буфера интерпретируются как указатель на другой буфер и что этот указатель не равен NULL.
- Буфер, на который указывают первые 8 байтов входного буфера, затем устанавливается с помощью указателей со смещениями +0x28 и +0x30, указывающих на buff_28h и buff_30h соответственно.
- Буфер buff_28h подготовлен с указателями функций для трех вызовов функций, которые выполнит IoCsqRemoveIrp. Эти указатели размещаются по соответствующим смещениям внутри buff_28h:
  - Первый указатель вызова функции размещается по смещению +0x20.
  - Второй указатель вызова функции размещается по смещению +0x10.
  - Третий указатель вызова функции размещается по смещению +0x28.
- Выделяется отдельный буфер iocsq_rsi_plus_8h, а ненулевое значение помещается по смещению +0x68, чтобы обеспечить проверку внутри IoCsqRemoveIrp.
- Буфер buff_30h настроен так, чтобы указывать на iocsq_rsi_plus_8h по смещению +0x08, а ненулевое значение также помещается по смещению +0x68 в пределах buff_30h.
- Чтобы предотвратить появление синего экрана после использования уязвимости, для третьего вызова функции установлено значение KxWaitForSpinLockAndAcquire, которое заблокирует поток на неопределённый срок и не позволит ему достичь вызова ExFreePoolWithTag, который мог бы вызвать синий экран.
- Первые два вызова функции настроены на HalMakeBeep, безвредную функцию ядра, которая не дает сбоя и не принимает аргументов.
- Буферу buff_28h по смещению +0x50 присваивается ненулевое значение, чтобы предоставить заблокированный объект спин-блокировки KxWaitForSpinLockAndAcquire.

Настраивая таким образом входной буфер и вызывая DeviceIoControl с кодом VULN_IOCTL, эксплойт может достичь уязвимой области кода драйвера, где вызывается IoCsqRemoveIrp, и контролировать указатели функций, используемые IoCsqRemoveIrp, что потенциально может привести к выполнению произвольного кода с привилегии ядра

7) Повышение привилегий

Чтобы повысить привилегии и получить полный контроль над системой, злоумышленник может использовать соответствующие уязвимости. Одним из распространённых методов является манипулирование токенами доступа, которые представляют собой объекты, описывающие контекст безопасности процесса или потока, включая личность и привилегии учётной записи пользователя, связанной с процессом. Получив токен с более высокими привилегиями, злоумышленник может создать новый процесс с повышенными правами или заменить токен существующего процесса. Условие записи «что-где» — это уязвимость, которая позволяет злоумышленнику записать произвольное значение в произвольное место в памяти. Это можно использовать для перезаписи критических структур данных или указателей функций, что приводит к выполнению произвольного кода.

В контексте уязвимостей Ivanti Secure Access VPN, CVE-2023–38043, CVE-2023–35080 и CVE-2023–38543, процесс

эксплуатации включает остановку VPN-клиента во избежание повреждения памяти, а затем использование уязвимостей для повышения привилегий. Уязвимости позволяют повысить привилегии из-за драйвера ядра, установленного программным обеспечением VPN, который создаёт устройство, доступное для чтения и записи любому пользователю, что потенциально может привести к повреждению ядра или повышению привилегий.

Процесс эксплуатации может включать поиск указателя ядра для объекта токена с использованием класса SystemExtendedHandleInformation в API NtQuerySystemInformation, а затем использование примитива записи для перезаписи полей TOKEN->_SEP_TOKEN_PRIVILEGES->Enabled и TOKEN->_SEP_TOKEN_PRIVILEGES->Present для предоставления системного уровень привилегий для процесса. За этим может последовать создание оболочки с повышенными привилегиями.

8) Включение уязвимого драйвера

Чтобы включить уязвимый драйвер в Ivanti Secure Access VPN, который обычно отключён по умолчанию, злоумышленник может воспроизвести поведение, которое автоматически запускает драйвер, когда пользователь подключается к VPN-серверу с включённым аварийным переключением TDI. Это можно сделать, установив мошеннический VPN-сервер Ivanti Secure Access и настроив его на использование аварийного переключения TDI:

- **Загрузить VM образ:** необходимо скачать образ виртуальной машины сервера Ivanti Secure Access VPN с официального сайта.
- **Установить сервер:** установить загруженный образ виртуальной машины на виртуальный частный сервер (VPS) или локально и указать на него доменное имя, например vpn.rogue-server.com.
- **Завершить настройку виртуальной машины:** после загрузки VM-образа и завершить настройку и получить доступ к порталу администрирования.
- **Настроить действительный сертификат.** Необходимо получить действительный сертификат для домена «мошеннического» сервера (например, vpn.rogue-server.com), используя службу Let's Encrypt и загрузить файлы fullchain.pem и privkey.pem на портал администрирования в разделе «Система» -> «Конфигурация» -> «Сертификаты» -> «Сертификат устройства» с удалением предварительно настроенных самоподписанных сертификатов.
- **Ограничить VPN и настроить TDI-Failover:** на портале администрирования в разделе «Пользователи» -> «Роли пользователей» -> «Пользователи» снять флажки со всех функций доступа, кроме подпункта «Диспетчер безопасных приложений и версия для Windows/Mac». Затем включите «Включить аварийное переключение на TDI для подключения Pulse SAM» на вкладке SAM -> «Параметры».
- **Создать пользователя VPN:** «Аутентификация» -> «Аутентификация». Серверы -> Локальная система -> вкладка Пользователи и создать нового пользователя со статическим именем пользователя и паролем. Этот пользователь будет использоваться для подключения к мошенническому VPN.
- **Подключение к мошенническому серверу.** Необходимо что жертва выполнила подключение к мошенническому серверу, указав URL-адрес, имя пользователя и пароль созданного пользователя, а также область, в которой находится этот пользователь (по умолчанию — «Пользователи»). Для подключения:

  "%programfiles(x86)%\Common Files\Pulse Secure\Integration\pulselauncher.exe" -url YOUR_DOMAIN -u YOUR_USER -p YOUR_PASS -r Users

  Например:

  "%programfiles(x86)%\Common Files\Pulse Secure\Integration\pulselauncher.exe" -url vpn.rogue-server.com -u steve -p Welcome01! -r Users
- Остановить VPN-клиент. Прежде чем запускать эксплойт повышения привилегий, необходимо остановить VPN-клиент, чтобы предотвратить повреждение памяти, с помощью команды:

  "%programfiles(x86)%\Common Files\Pulse Secure\Integration\pulselauncher.exe" -stop

Выполнив эти шаги, злоумышленник может включить уязвимый драйвер и потенциально использовать уязвимости CVE-2023–38043, CVE-2023–35080 и CVE-2023–38543 в Ivanti Secure Access VPN для повышения привилегий.

D. PoC «main.c»

Код предназначен для использования уязвимости в VPN-клиенте, позволяющей повысить привилегии, отказ в обслуживании или раскрытие информации.

1) Как работает код

- **Настройка приоритета потока.** Код начинается с попытки установить приоритет текущего потока в фоновый режим, чтобы минимизировать его влияние на производительность системы.
- **Распределение и настройка памяти:** он выделяет память для различных буферов (input_buffer, Initial_buffer, buff_30h, iocsq_rsi_plus_8h) и настраивает их для создания вредоносной полезной нагрузки. Сюда входит настройка указателя (buff_28h) для хранения значения байта, предназначенного для записи в уязвимый компонент в пространстве памяти драйвера.
- **Получение базового адреса ядра:** код извлекает базовый адрес ядра (ntoskrnl_base) для вычисления адресов конкретных функций или смещений внутри

ядра, которыми эксплойт намеревается манипулировать.

- **Настройка указателей функций:** он устанавливает указатели функций в подготовленных буферах, чтобы они указывали на вредоносные или контролируемые сегменты кода или вызывали уязвимость в драйвере клиента Ivanti Secure Access Client.
- **Запуск уязвимости.** Эксплойт запускает уязвимость, выполняя вызов DeviceIoControl с подготовленным input_buffer, который содержит вредоносную полезную нагрузку, предназначенную для использования уязвимости.
- **Повышение привилегий:** в случае успеха эксплойт изменяет привилегии токена текущего процесса или выполняет другие несанкционированные действия, что приводит к повышению привилегий, DoS или раскрытию информации.

2) Входные данные:

- **Путь к целевому устройству:** путь к уязвимому устройству или драйверу, на который нацелен эксплойт.
- **Значение байта (что):** конкретное значение байта, которое эксплойт намеревается записать в целевую ячейку памяти.
- **Целевой адрес памяти (где):** адрес памяти внутри уязвимого компонента или драйвера, куда эксплойт намеревается записать значение байта.

3) Выходные данные/результат

- **Сообщения о состоянии эксплойта:** код выдает сообщения о состоянии, указывающие на успех или неудачу различных шагов, таких как установка приоритета потока, создание потоков и выполнение эксплойта.
- **Привилегированный доступ:** если эксплойт успешен, он получает повышенные привилегии для текущего процесса, позволяя ему выполнять действия, которые ранее были ограничены.
- **Потенциальная модификация системы:** в зависимости от цели эксплойта он может изменить настройки системы, отключить меры безопасности или выполнить другие несанкционированные действия в результате повышения привилегий.

E. PoC «kernel.c»

Код является частью эксплойта, нацеленноого на уязвимость в системном драйвере, написан на C и включает в себя несколько функций, которые взаимодействуют с операционной системой Windows на низком уровне для управления дескрипторами устройства и памятью.

1) Как работает код

- **BuildDevicePath:** создаёт строку пути к устройству для уязвимого драйвера.
- **OpenDevice:** открывает дескриптор устройства с помощью функции CreateFileW, которая позволяет выполнять чтение и запись на устройство.
- **CloseDevice:** закрывает дескриптор устройства и освобождает связанную память.
- **GetFunctionOffset:** извлекает смещение функции в файле ntoskrnl.exe, который является ядром Windows NT.
- **GetKernelBase:** определяет базовый адрес ядра путём запроса системной информации.
- **GetObjectPointedByHandle:** извлекает объект ядра, на который указывает данный дескриптор, который можно использовать для манипулирования или чтения информации из этого объекта.

2) Входные данные

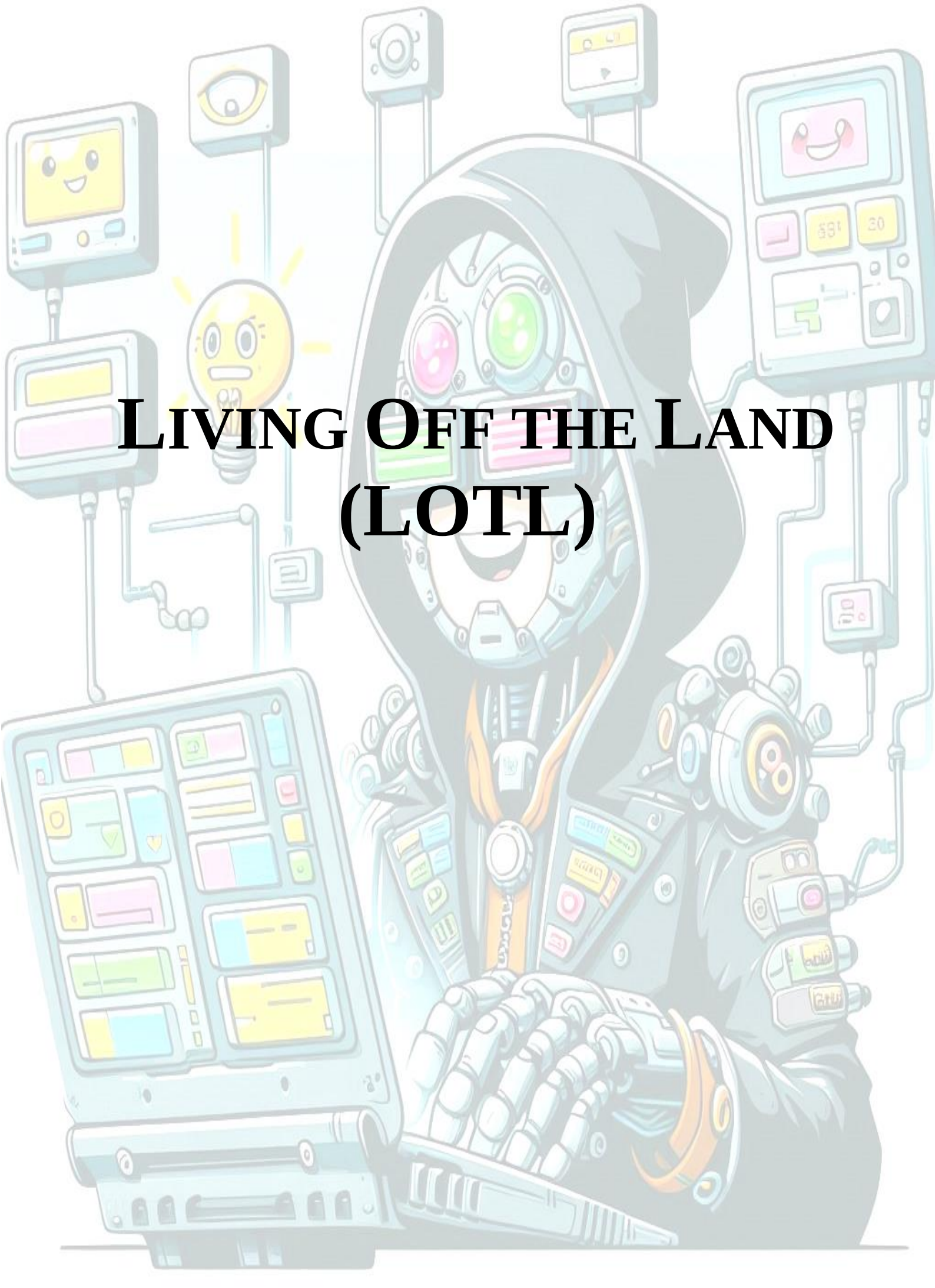
- DevicePath: строка, представляющая путь к уязвимому устройству или драйверу.
- DEVICE_NAME_W: имя устройства, которое используется для построения пути к устройству.
- hDevice: указатель на дескриптор, который будет использоваться для взаимодействия с устройством.
- fnName: имя функции, смещение которой извлекается.

h: Дескриптор, чей указанный объект извлекается.

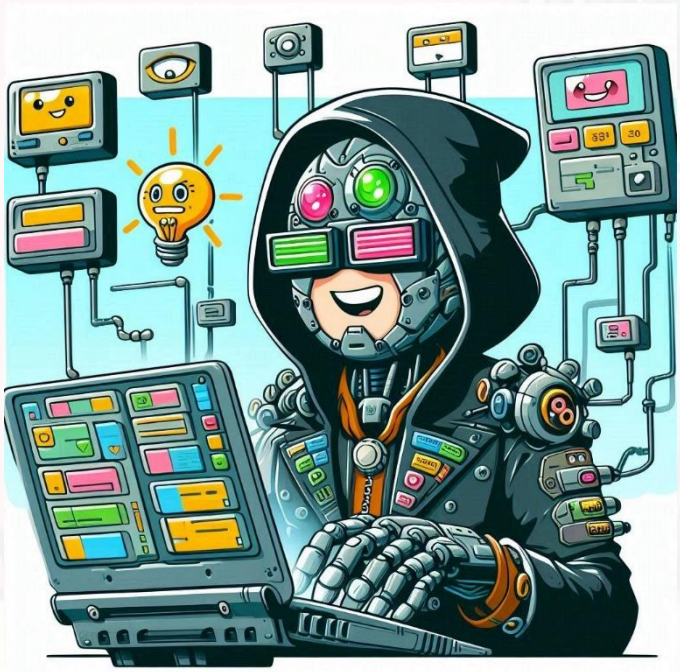
3) Выходные данные/результат

- **DevicePath:** полная строка пути к устройству, которая создаётся и используется для открытия дескриптора устройства.
- **hDevice:** ручка, получаемая при открытии устройства, которую можно использовать для дальнейшего взаимодействия с устройством.
- **FnOffset:** смещение указанной функции в исполняемом образе ядра.
- **KernelBase:** базовый адрес ядра, полученный из системной информации.
- **Объект:** объект ядра, на который указывает указанный дескриптор, которым можно манипулировать или читать.

Код предназначен для выполнения низкоуровневых операций, которые обычно являются частью цепочки эксплойтов. Эти операции включают в себя открытие дескриптора уязвимого драйвера, определение местоположения определённых функций или данных в ядре и потенциальное использование этой информации для манипулирования системой таким образом, чтобы использовать уязвимость.



LIVING OFF THE LAND (LOTL)



Аннотация – В документе представлен анализ рекомендаций Агентства национальной безопасности (АНБ) по борьбе с LOTL-атаками. Анализ включает в себя изучение подхода к тактике LOTL, подразумевающей использование легитимных инструментов в различных целях.

Анализ предлагает качественное изложение рекомендаций АНБ и служит ценным ресурсом для специалистов по безопасности, ИТ-персонала, политиков и заинтересованных сторон в различных отраслях, предоставляя им знания для защиты от сложных LOTL-угроз.

A. Введение

Документ, озаглавленный "Joint Guidance: Identifying and Mitigating LOTL Techniques", содержит рекомендации о том, как организации могут лучше защитить себя от методов известных как Living Off The Land (LOTL). Эти методы предполагают, что атакующие используют легитимные инструменты и программное обеспечение, присутствующие в среде объекта, для осуществления вредоносных действий, что усложняет обнаружение. Этот подход направлен на сокращение таких легитимных инструментов операционной системы и приложений для нецелевого применения.

Руководство основано на практических результатах, оценках red team, отраслевых практиках и практиках по реагированию на инциденты. Также подчёркивается важность создания и поддержания инфраструктуры, которая собирает и систематизирует данные, помогающие правозащитникам выявлять методы LOTL, адаптированные к ландшафту рисков каждой организации и её ресурсным возможностям.

1) Ключевые моменты

- Руководство составлено крупнейшими агентствами кибербезопасности и национальной безопасности США, Австралии, Канады, Соединённого Королевства и Новой Зеландии и посвящено распространённым методам LOTL и пробелам в возможностях киберзащиты.
- LOTL применяется для компрометации и поддержания доступа к критически важной инфраструктуре, путём использования легитимных системных инструментов и процессов, чтобы «вписаться в обычную активность» и избежать обнаружения.
- Многим организациям трудно обнаружить вредоносную активность LOTL из-за неадекватных методов обеспечения безопасности и управления сетью, отсутствия общепринятых индикаторов компрометации и сложности отличить вредоносную активность от легитимного поведения.
- Рекомендации включают использование детализированного журнала событий, установление базовых показателей активности, использование автоматизации для непрерывного анализа, снижение количества оповещений и использование аналитики поведения пользователей и объектов (UEBA).
- Усиление безопасности включают применение рекомендаций поставщика по усилению безопасности, внедрение списка разрешённых приложений, улучшение сегментации сети и мониторинга, а также усиление контроля аутентификации и авторизации.
- Производителям программного обеспечения рекомендуется применять принципы secure-by-design, чтобы уменьшить количество уязвимостей, которые позволяют использовать методы LOTL, что включает в себя отключение ненужных протоколов, ограничение доступности сети, ограничение повышенных привилегий, включение по умолчанию защищённого от фишинга MFA, обеспечение защищённости журнала событий, устранение паролей по умолчанию и ограничение динамического выполнения кода.

2) Вторичные моменты

- Направленность на смягчение последствий использования LOTL-методов, когда нецелевым образом применяются легитимные инструменты.
- Поставщики должны нести ответственность за настройки своего программного обеспечения по умолчанию и соблюдение принципа наименьших привилегий.
- Производителям ПО рекомендуется сокращать количество уязвимостей, которыми можно воспользоваться, и брать на себя ответственность за обеспечение безопасности своих клиентов.
- Стратегии сетевой защиты включают мониторинг необычных системных взаимодействий, повышения

привилегий и отклонений от обычных административных действий.

- Организациям следует создать и поддерживать инфраструктуру для сбора и систематизации данных для обнаружения методов LOTL, адаптированную к их конкретному ландшафту рисков и ресурсным возможностям

B. Преимущества и недостатки

В анализируемом документе излагается комплексный подход к усилению защиты кибербезопасности от тактики LOTL. Этот подход включает рекомендации по обнаружению, централизованному протоколированию, поведенческому анализу, обнаружению аномалий и упреждающему поиску.

Несмотря на то, что предлагаемые решения обладают значительными преимуществами, организации также должны учитывать потенциальные недостатки и ограничения. Эффективное внедрение требует тщательного планирования, распределения ресурсов и постоянной корректировки с учётом меняющегося ландшафта угроз.

1) Преимущества

- **Расширенные возможности обнаружения**: внедрение комплексной и детализированной системы регистрации событий наряду с централизованным управлением событиями значительно повышает способность организации обнаруживать вредоносные действия. Такой подход позволяет анализировать поведение, обнаруживать аномалии и осуществлять упреждающий поиск, обеспечивая надёжную защиту от методов LOTL.
- **Улучшенная система безопасности**: рекомендуются различные меры, предоставляемые поставщиком или отраслевыми стандартами, сведение к минимуму запущенных служб и защита сетевых коммуникаций с целью сокращения векторов атаки.
- **Повышенная прозрачность**: централизованное управление событиями позволяет выявлять закономерности и аномалии с течением времени. Такой подход в отношении сетевых и системных действий способствует упреждающему обнаружению потенциальных угроз.
- **Эффективное использование ресурсов**: автоматизация анализа журналов и поиска информации повышает эффективность этих процессов, позволяя организациям лучше использовать свои ресурсы. Автоматизированные системы могут сравнивать текущие действия с установленными показателями поведения, с учётом особого внимания привилегированным учётным записям и критически важным активам.
- **Стратегическая сегментация сети**: улучшение сегментации сети и мониторинга ограничивает возможности распространения угрозы, уменьшая "радиус поражения" доступных систем в случае компрометации. Такой стратегический подход помогает сдерживать угрозы и сводит к минимуму потенциальный ущерб.

2) Недостатки/Ограничения

- **Ресурсоёмкость**: реализация рекомендуемых мер по обнаружению и усилению защиты может требовать значительных инвестиций в технологии и обучение персонала. Небольшим организациям будет сложно выделить необходимые ресурсы.
- **Сложность реализации**: создание и поддержание инфраструктуры для детальной регистрации событий и анализа является сложной задачей. Организации могут столкнуться с трудностями при эффективной настройке этих систем и управлении ими, особенно в разнообразных и динамичных ИТ-средах.
- **Снижение эффективности от систем оповещения**: хотя целью предлагаемых решений является снижение избытка оповещений, их огромный объем, генерируемых комплексными системами регистрации и обнаружения аномалий, может привести к переутомлению сотрудников службы безопасности и пропуску важных оповещений.
- **Ложноположительные и отрицательные результаты**: системы анализа поведения и обнаружения аномалий могут формировать ложноположительные и отрицательные результаты, что приводит к ненужным расследованиям инцидентов или пропущенным угрозам. Точная настройка этих систем для сведения к минимуму неточностей требует постоянных усилий и опыта.
- **Зависимость от поддержки поставщиков**: эффективность мер по усилению защиты и безопасных конфигураций часто зависит от поддержки и рекомендаций, предоставляемых поставщиками программного обеспечения. Организации могут столкнуться с ограничениями, если поставщики не уделяют приоритетного внимания безопасности или не предоставляют адекватных рекомендаций по усилению защиты.

C. LIVING OFF THE LAND

Методы LOTL представляют собой стратегию кибер-угроз, при которой злоумышленники используют нативные инструменты и процессы, уже присутствующие в среде атакуемой цели. Такой подход позволяет органично сочетаться с обычной деятельностью системы, значительно снижая вероятность обнаружения. Эффективность LOTL заключается в её способности использовать инструменты, которые не только уже развёрнуты, но и пользуются доверием в среде, тем самым обходя традиционные меры безопасности, которые могут блокировать или помечать незнакомое или вредоносное программное обеспечение.

Методы LOTL не ограничены каким-либо одним типом среды; они эффективно используются в локальных,

облачных, гибридных средах Windows, Linux и macOS. Такая универсальность отчасти объясняется тем, что злоумышленники предпочитают избегать затрат и усилий, связанных с разработкой и развёртыванием пользовательских инструментов. Вместо этого упор делается на повсеместное применение и доверие к типовым, популярным и нативным инструментам.

1) Среды Windows

В корпоративных Windows-средах, методы LOTL особенно распространены из-за широкого использования нативных инструментов, служб и функций операционной системы и доверия к ним.

2) macOS и гибридные среды

В этом случае злоумышленники используют нативные скрипт-среды, встроенные инструменты, системные конфигурации и бинарные файлы. Стратегия аналогична стратегии в средах Windows, но адаптирована к уникальным аспектам macOS. В гибридных средах, сочетающих физические и облачные системы, злоумышленники все чаще применяют сложные методы LOTL для использования преимуществ систем обоих типов.

3) Известные Эксплойты

Применение эксплоитов хорошо представлено на ресурсах:

- Репозиторий проекта LOLBAS на GitHub предлагает информацию о том, как жить за счёт обычных бинарных файлов, скриптов и библиотек.
- Такие веб-сайты, как gtfobins.github.io, loobins.io и loldrivers.io, предоставляют списки бинарных файлов Unix, macOS и Windows соответственно, которые используются в методах LOTL.

4) ПО удалённого доступа сторонних производителей

Помимо нативных инструментов, атакующие также используют ПО удалённого доступа сторонних производителей в следующих категориях: удалённый мониторинг и управление, управление конфигурацией конечных устройств, EDR, управление исправлениями, системы управления мобильными устройствами и инструменты управления базами данных. Эти инструменты, предназначенные для администрирования и защиты доменов, обладают встроенной функциональностью, которая может выполнять команды на всех клиентских узлах в сети, включая такие важные, как контроллеры домена. Также стоит обратить внимание на наборы привилегий, которые требуются этим инструментам для системного администрирования.

D. Параметры безопасности и избыток уведомлений систем оповещения

Одной из основных выявленных проблем является отсутствие базовых параметров безопасности в организациях, что приводит к выполнению LOLBin без обнаружения аномальной активности. Кроме того, организациям часто не удаётся корректно настроить инструменты обнаружения, что приводит к огромному количеству оповещений, которыми трудно управлять и на которые трудно реагировать. Это усугубляется автоматизированными системами, выполняющими действия с высокими привилегиями, которые могут завалить аналитиков событиями журнала, если их не классифицировать должным образом.

1) Проблемы с распознаванием вредоносной активности

Даже организациям со зрелыми передовыми практиками бывает трудно отличить вредоносную активность LOTL от легитимного поведения:

- LOLBins обычно используются ИТ-администраторами и поэтому являются доверительными, что может приводить к заблуждению безопасности для всех пользователей.
- Существует ошибочное представление о том, что легитимные инструменты ИТ-администрирования безопасны априори, что приводит к политикам "разрешения", которые расширяют возможности атаки.
- Исключения для таких инструментов, как PsExec, из-за их регулярного использования администраторами могут быть использованы злоумышленниками для скрытого распространения.

2) Разрозненные операции и ненастроенные системы EDR

Информация складывается из опыта redteam и групп реагирования на инциденты в отношении специалистов по сетевой безопасности:

- Обособленная работа от других ИТ-команд препятствует формированию поведенческих пользовательских признаков, устранению уязвимостей и расследования аномального поведения.
- Использование ненастроенных систем обнаружения и EDR и индикаторов компрометации (IOCs), которые могут приводить к отсутствию оповещений о действиях злоумышленников для предотвращения обнаружения.

3) Конфигурации системы регистрации событий и политики внесения в разрешенные списки

Недостатки в конфигурациях систем регистрации событий и политиках управления списками разрешений ещё больше усложняют обнаружение действий LOTL:

- Конфигурации систем регистрации событий по умолчанию часто не позволяют фиксировать все соответствующие действия, и журналы из многих приложений требуют дополнительной обработки.
- Политика списков разрешений для диапазонов IP-адресов, принадлежащих хостинг-провайдерам и

облачным провайдерам, может непреднамеренно обеспечить «прикрытие для злоумышленников».

4) Защита устройств macOS

Несмотря на то, что устройства macOS изначально считаются безопасности, они также требуют настройки:

- В macOS отсутствуют стандартизированные рекомендации по повышению надёжности системы, что приводит к развёртываниям с настройками по умолчанию, которые могут быть небезопасными.
- Презумпция безопасности macOS может привести к отмене приоритетов стандартных мер безопасности и внесение приложений в списки разрешённых.
- В средах со смешанными операционными системами низкая представленность устройств macOS может привести к недостаточному вниманию к их безопасности, что делает их более уязвимыми для вторжений.

E. Возможности для детектирования

1) Детализированные журналы событий

- **Внедрение комплексной системы регистрации событий**: решающее значение имеет создание механизмов регистрации всех ИБ-событий на разных платформах и обеспечение агрегирования журналов в централизованном хранилище для предотвращения.
- **Ведение журнала в облачной среде**: для облачных сред важно регистрировать различные события ввиду их большего количества и настроить политики управления журналами событий для всех облачных служб, особенно редко используемых с целью обнаружения действий злоумышленников.
- **Детализация событий безопасности**: включение детализации событий, таких как командные строки, действия PowerShell и отслеживание событий WMI, обеспечивает более глубокое представление об использовании инструмента в среде, помогая обнаруживать вредоносные действия LOTL.

2) Установление поведенческих ориентиров

- **Отслеживание отклонений в параметрах**: отслеживание параметров установленных инструментов, программного обеспечения, поведения учётной записи и сетевого трафика позволяет защитникам выявлять отклонения, которые могут указывать на вредоносную активность.
- **Мониторинг сети и поиск угроз**: улучшение мониторинга сети, расширение хранилища журналов и углубление тактики поиска угроз жизненно важны для выявления длительного присутствия атакующих.

3) Автоматизация и эффективность

- **Использование автоматизации**: использование автоматизации для постоянного изучения журналов и сравнения текущих действий с установленными параметрами поведения повышает эффективность поиска, особенно с акцентом на привилегированные учётные записи и критически важные активы.

4) Снижения «шума» от системы оповещения

- **Совершенствование инструментов мониторинга**: важно совершенствовать инструменты мониторинга и механизмы оповещения, чтобы проводить различие между типичными административными действиями и поведением, связанным с угрозой, сосредоточив внимание на предупреждениях, которые с наибольшей вероятностью указывают на подозрительные действия.

5) Использование UEBA

- **Аналитика поведения пользователей и организаций (UEBA)**: использование UEBA для анализа и сопоставления действий в нескольких источниках данных помогает выявлять потенциальные инциденты безопасности, которые могут быть пропущены традиционными инструментами, и профилировать поведение пользователей для обнаружения внутренних угроз или скомпрометированных учётных записей.

6) Особенности облачных технологий

- **Проектирование облачной среды**: проектирование облачной среды для обеспечения надлежащего разделения основных и дополнительных журналов позволяет лучше отслеживать потенциальные действия LOTL.

F. Hardening-Стратегии

Hardening-стратегии направлены на сокращение количества возможных атак и повышение уровня безопасности критически важной инфраструктуры.

1) Рекомендации

Рекомендации по усилению защиты от вендоров и отраслей: организациям следует усиливать конфигурации программного обеспечения и систем на основе рекомендаций по защите от поставщиков или от отрасли, сектора или правительства, например, от NIST, чтобы уменьшить количество векторов атаки.

a) Для конкретной платформы:

- **Windows**: применение обновления и исправления для системы безопасности от Microsoft, руководства по базовым показателям безопасности Windows или тестам CIS, ужесточение часто используемых служб, такие как SMB и RDP, и отключение ненужных служб и функций.
- **Linux**: контроль за разрешениями для работы с бинарными файлами и использование стандартов Red Hat Enterprise Linux.
- **macOS**: регулярные обновления и применение исправлений системы, а также встроенных

функций безопасности, такие как Gatekeeper, XProtect и FileVault, и рекомендаций macOS Security Compliance Project.

b) Повышение надежности облачной инфраструктуры:

- **Microsoft Cloud**: применение руководств CISA по настройкам безопасности Microsoft 365 в различных облачных службах Microsoft.
- **Google Cloud**: применение руководств по настройке безопасности Google Workspace Security от CISA для настройки облачных сервисов Google.
- **Универсальные меры защиты**: сведение к минимуму количество запущенных служб, применение принципа наименьших привилегий и защитите сетевые коммуникации.
- **Защита критически важных активов**: применение мер по усилению защиты критически важных активов, таких как ADFS и ADCS, и ограничение приложений и служб, которые могут использоваться или к которым они могут получить доступ.
- **Средства администрирования**: применение предотвращающих повторное использование скомпрометированных учётных данных средств.

2) Список разрешенных приложений

Ограничение выполнения: внедрение списка разрешений приложений как для пользователей, так и администраторов с целью улучшения мониторинга и уменьшения объёма оповещений.

a) Список разрешений для конкретной платформы:

- **macOS**: использование параметров Gatekeeper для предотвращения выполнения неподписанных или неавторизованных приложений.
- **Windows**: использование AppLocker и Windows Defender Application Control для управления исполняемыми файлами, скриптами, MSI-файлами, библиотеками DLL и другими упакованными приложениями.

3) Сегментация сети и мониторинг

- **Ограничение распространения**: реализация сегментации сети для ограничения доступа пользователей минимально необходимыми приложениям и службам, в т.ч. снижения влияния скомпрометированных учётных данных.
- **Анализ сетевого трафика**: применение инструментов для мониторинга трафика между сегментами и размещение сетевые датчики в критических точках для всестороннего анализа трафика.
- **Анализ метаданных сетевого трафика**: применение анализаторов трафика, например Zeek, и интеграция с NID-решениями, например Snort или Suricata.

4) Элементы управления аутентификацией

- **Защита от фишинга**: использование MFA во всех системах, особенно для привилегированных учётных записей.
- **Управление привилегированным доступом (PAM)**: развёртывание надёжных PAM-решений с доступом и элементами управления на основе временного фактора, дополненных ролевым управлением доступа (RBAC).
- **Облачное управление идентификацией и доступом к учётным данным (ICAM)**: применение строгих политик ICAM, аудит конфигураций и смена ключей доступа.
- **Проверка файла Sudoers File Review**: для macOS и Unix регулярная проверка файла sudoers на наличие некорректных настроек в рамках принципа наименьших привилегий.

5) Архитектура нулевого доверия

В качестве долгосрочной стратегии внедряется архитектура с нулевым доверием, чтобы гарантировать, что бинарные файлы и учётные записи не являются доверенными и привилегированными по умолчанию.

6) Дополнительные рекомендации

- **Комплексная проверка при выборе поставщика**: выбор поставщиков с надёжными принципами проектирования и привлечение их к ответственности за конфигурации их программного обеспечения по умолчанию.
- **Аудит ПО удалённого доступа**: аудирование ПО удалённого доступа и применение лучших практик для обеспечения безопасности удалённого доступа.
- **Ограничение исходящего подключения к Интернету**: ограничение доступа к Интернету для внутренних серверов и контроля исходящих подключений для основных служб.

G. Рекомендации по обнаружению угроз

В рамках рекомендаций предлагаются регулярные проверки инвентаризации системы для выявления поведения злоумышленников, которое может быть пропущено журналами событий из-за некорректных конфигураций. Организациям рекомендуется включить регистрацию всех событий, связанных с безопасностью, включая действия командной строки, системные вызовы и журналы аудита на всех платформах, чтобы улучшить обнаружение вредоносной активности LOTL.

1) Сетевые журналы

Обнаружение LOTL-методов с помощью сетевых журналов представляет собой проблемы из-за преходящего характера сетевых артефактов и сложности распознавания вредоносной активности от легитимного поведения. В отличие от артефактов хоста, которые часто можно обнаружить, если только атакующий намеренно не удалит их, сетевые артефакты являются производными от сетевого трафика, временными и требуют надлежащей настройки

систем управления событиями для их отслеживания. Без соответствующих датчиков для регистрации сетевого трафика невозможно наблюдать за активностью LOTL.

2) Показатели активности LOTL

Обнаружение активности LOTL включает в себя поиск набора возможных индикаторов для формирования связанных поведенческих сетевых признаков в трафике.

- **Просмотр журналов брандмауэра**: Заблокированные попытки доступа в журналах брандмауэра могут сигнализировать о компрометации, особенно в должным образом сегментированной сети. Попытки обнаружения сети и сопоставления внутри неё также могут указывать на активность LOTL. Важно различать обычное поведение инструмента управления сетью и аномальное.
- **Исследование аномальных признаков в трафике**: изучение определённых типов трафика, такие как запросы LDAP от хостов Linux, не присоединённых к домену, запросы SMB из разных сегментов сети или запросы доступа к базе данных с рабочих станций пользователей, которые должны выполняться только внешними серверами, с конечной целью отличить легитимное приложения от вредоносных запросов.
- **Изучение журналов сетевых служб на хост-машинах**: журналы таких служб, как Sysmon и IIS, на хост-машинах могут предоставить информацию о взаимодействиях веб-сервера, транзакциях FTP и других сетевых действиях. Эти журналы содержат ценный контекст и детали, которые могут быть недоступны традиционным сетевым устройствам.
- **Объединение журналов сетевого трафика с журналами на базе хоста**: этот подход позволяет включать дополнительную информацию, такую как учётная запись пользователя и сведения о процессе. Расхождения между артефактами назначения и внутри сети могут указывать на вредоносный трафик.

3) Журналы событий приложений, безопасности и системных событий

Системы регистрации событий по умолчанию часто не позволяют фиксировать все необходимые события, потенциально оставляя пробелы в видимости вредоносных действий. Определение приоритета журналов и источников данных, которые с большей вероятностью выявят вредоносную активность LOTL, имеет решающее значение для эффективного обнаружения и реагирования.

4) Журналы аутентификации

Журналы аутентификации играют важную роль в выявлении попыток несанкционированного доступа и отслеживании действий пользователей по сети. Регистрация всех операций, включая вызовы API и входы конечных пользователей, с помощью таких сервисов, как Amazon Web Services CloudTrail, Azure Activity Log и Google Cloud Audit Logs. Эти журналы могут предоставить ценную информацию о потенциальных действиях LOTL, выявляя необычные схемы доступа или попытки использования механизмов аутентификации.

Надёжная стратегия разграничения привилегий необходима для идентификации методов LOTL по журналам аутентификации. Такие практики, как ограничение доступа учётных записей администраторов домена только к контроллерам домена и использование рабочих станций привилегированного доступа (PAWs) и наличие MFA могут свести к минимуму доступ к учётным данным и усилить сегментацию сети.

5) Регистрация событий на хосте

Sysmon и другие инструменты регистрации хостовых событий обеспечивают детальную визуализацию системных действий о создании процессов, сетевых подключениях и изменениях файловой системы, эти инструменты с целью обнаружения и расследования подозрительных активностей и поведенческих признаков.

a) Установление исходных условий и обеспечение защиты журнала

Основополагающим шагом в обнаружении аномального или потенциально вредоносного поведения является установление условий запуска инструментов и событий. Это включает в себя понимание механизмов безопасности операционных систем для выявления отклонений, которые могут указывать на угрозу безопасности. Также важно полагаться на защищённые журналы, которые менее подвержены подделке злоумышленниками. Например, в то время как файлы Linux .bash_history могут быть изменены непривилегированными пользователями, журналы аудита системного уровня более безопасны и обеспечивают надёжную запись действий.

b) Использование Sysmon в средах Windows

Sysmon, инструмент мониторинга системы Windows, предоставляет детальную информацию о таких действиях, как создание процессов, сетевые подключения и модификации реестра. Подробное протоколирование имеет неоценимое значение для служб безопасности при поиске и выявлении случаев неправильного использования легитимных инструментов. Ключевые стратегии включают:

- Использование свойства OriginalFileName для идентификации переименованных файлов, которые могут указывать на вредоносную активность (для большинства утилит Microsoft исходные имена файлов хранятся в заголовке PE).
- Внедрение методов обнаружения для выявления использования утилит командной строки и скриптов, особенно использующих альтернативные потоки данных (ADS) - мониторинг определённых аргументов командной строки или синтаксиса, используемых для взаимодействия с ADS.

c) Стратегии обнаружения

Усовершенствование конфигураций Sysmon для анализа с упором на шаблоны, указывающие на обфускацию, может помочь выявить попытки обойти средства мониторинга

безопасности, например использование управляющих символов, объединение команд и использование кодировки Base64.

d) Мониторинг подозрительных цепочек процессов

Мониторинг подозрительных цепочек процессов, например связанных с Microsoft Office и процессами создания скриптов, является ключевым показателем активности LOTL, т.к. приложения Office редко запускают процессы (cmd.exe, PowerShell, wscript.exe или cscript.exe).

e) Интеграция журналов с SIEM-системами

Интеграция журналов Sysmon с SIEM-системами с целью применения правил корреляции может значительно улучшить обнаружение атак путём автоматизации процесса обнаружения и применения аналитики для выявления сложных поведенческих моделей вредоносной активности.

f) Рекомендации по работе с Linux и macOS

На компьютерах с Linux использование Auditd или Sysmon и интеграция этих журналов с платформой SIEM могут значительно улучшить обнаружение аномальных действий. Для macOS использование таких инструментов, как Santa, система авторизации с открытым исходным кодом, может помочь отслеживать выполнение процессов и обнаруживать аномальное поведение производительных приложений

6) Просмотр Конфигураций

Регулярный анализ и обновление системных конфигураций необходимы для обеспечения того, чтобы меры безопасности оставались эффективными против возникающих угроз. Это включает проверку того, что параметры систем регистрации событий надлежащим образом настроены для сбора соответствующих данных и что средства контроля безопасности соответствуют современным передовым практикам. Организациям также следует оценить использование списков разрешений и других механизмов контроля доступа для предотвращения злоупотребление легитимными инструментами злоумышленниками.

Регулярные проверки конфигураций хостов на соответствие установленным базовым показателям необходимы для выявления признаков компрометации, и включают изменения в установленном программном обеспечении, конфигурации брандмауэра и обновления основных файлов, таких как файл Hosts, который используется для разрешения DNS. Проверки могут выявить несоответствия, которые сигнализируют о несанкционированных модификациях или присутствии вредоносного программного обеспечения.

- **Обход стандартных журналов событий**: известно, что атакующие обходят стандартные журналы событий, напрямую внося изменения в реестр для регистрации служб и запланированных задач. Такой подход не регистрируется в стандартных системных событиях, что делает его способом сокрытия активностей.
- **Системные инвентаризационные аудиты**: проведение регулярных системных инвентаризационных аудитов является упреждающей мерой для выявления поведения злоумышленников, которое могло быть пропущено журналами событий по различным причинам, а также гарантирует, что любые изменения в системе санкционированы и учтены.

7) Поведенческий анализ

Сравнение активности с обычным поведением пользователя позволяет говорить об обнаружении аномалий. Необычное поведение, на которое следует обратить внимание, например включает нетиповое время входа в систему, доступ вне ожидаемого рабочего графика или праздничных перерывов, быструю последовательность или большое количество попыток доступа, необычные пути доступа, одновременные входы в систему из нескольких мест.

8) NTDSUtil.exe и PSExec.exe

Особое внимание уделяется выявлению неправомерного использования NTDSUtil.exe и PSExec.exe инструментов, которые, хотя и являются легитимными, часто используются злоумышленниками в злонамеренных целях, например попытки сбросить учётные данные или распространяться по сети в направлении. Сосредоточив внимание на поведенческом контексте использования этих инструментов, организации могут более эффективно проводить различие между легитимными и вредоносными действиями.

a) Процесс эксплуатации

Обычная тактика заключается в создании теневой копии системного диска на томе, обычно с помощью vssadmin.exe с помощью таких команд, как Create Shadow /for=C:. Это действие создает моментальный снимок текущего состояния системы, включая базу данных Active Directory. После этого ntdsutil.exe используется для взаимодействия с этой копией с помощью определённой последовательности команд (ntdsutil snapshot “activate instance ntds” create quit quit). Затем злоумышленники получают доступ к теневой копии, чтобы извлечь файл ntds.dit из указанного каталога. Эта последовательность предназначена для извлечения конфиденциальных учётных данных, таких как хэшированные пароли, из Active Directory, что позволяет полностью скомпрометировать домен.

b) Обнаружение и реагирование

Для обнаружения такого использования и реагирования на него крайне важно понимать контекст ntdsutil.exe действий и проводить различие между легитимным административным использованием и потенциальным злонамеренным использованием. Основные источники журналов и стратегии мониторинга включают:

- **Журналы командной строки и создания процессов**: журналы безопасности (**идентификатор события 4688**) и журналы Sysmon (**идентификатор события 1**) предоставляют информацию о выполнении ntdsutil.exe команд.

Необычное или нечастое использование ntdsutil.exe для создания моментальных снимков может указывать на подозрительную активность.

- **Журналы создания файлов и доступа к ним**: мониторинг событий создания файлов (**идентификатор события Sysmon'a 11**) и попыток доступа к конфиденциальным файлам, таким как NTDS.dit (**идентификатор события 4663**), могут предоставить дополнительный контекст для процесса создания моментальных снимков и доступа.
- **Журналы использования привилегий**: идентификатор события 4673 в журналах, указывающий на использование привилегированных служб, может говорить о потенциальном злоупотреблении, когда оно связано с выполнением ntdsutil.exe команд.
- **Журналы сетевой активности и аутентификации**: журналы могут содержать информацию о одновременных удалённых подключениях или передачах данных, потенциально указывая на попытки эксфильтрации данных. Журналы аутентификации также важны для идентификации исполнителя команды ntdsutil.exe и оценки того, соответствует ли использование типичному поведению администратора.

c) Комплексный анализ PSExec.exe

PSExec.exe, компонент пакета Microsoft PsTools, представляет собой мощную утилиту для системных администраторов, предлагающую возможность удалённого выполнения команд в сетевых системах, часто с повышенными привилегиями. Однако его универсальность также делает его излюбленным инструментом у APT-групп.

d) Роль PSExec.exe в кибер-угрозах

PSExec.exe обычно используется для удалённого администрирования и выполнения процессов в разных системах. Его способность работать с системными привилегиями делает его особенно привлекательным для вредоносного использования, например для выполнения одноразовых команд, направленных на изменение системных конфигураций, таких как удаление конфигураций прокси-порта на удалённом хосте с помощью команд типа:

"C:\pstools\psexec.exe" {REDACTED} -s cmd /c "cmd.exe /c netsh interface portproxy delete v4tov4 listenaddress=0.0.0.0 listenport=9999"

e) Стратегии обнаружения

Для эффективного противодействия злонамеренному использованию PSExec.exe сетевые защитники должны использовать различные журналы, которые дают представление о выполнении команд и более широком контексте операции:

- **Журналы командной строки и создания процессов**: Журналы безопасности (**идентификатор события 4688**) и журналы Sysmon (**идентификатор события 1**) полезны для отслеживания выполнения PSExec.exe и связанных с ними команд. В этих журналах подробно описывается использованная командная строка, определяющая природу и «намерения» процесса.
- **Журналы использования привилегий и явных учётных данных**: журналы безопасности **Идентификатор события 4672**) документируют случаи, когда новым входам в систему назначаются особые привилегии, что крайне важно, когда PsExec выполняется с переключателем -s для системных привилегий. Идентификатор события 4648 фиксирует явное использование учётных данных, указывая, когда PsExec запускается с определёнными учётными данными пользователя.
- **Sysmon регистрирует сетевые подключения и изменения реестра**: идентификатор события 3 Sysmon регистрирует сетевые подключения, что является центральным элементом функции удалённого выполнения PsExec. Идентификаторы событий 12, 13 и 14 отслеживают изменения реестра, включая удаления (Идентификатор события 14) разделов реестра, связанных с выполненной командой Netsh, предоставляя доказательства изменений конфигурации системы.
- **Журналы аудита реестра Windows**: в журналы записываются изменения разделов реестра, содержащие информацию, такую как временная метка изменений, учётная запись, под которой были внесены изменения (часто системная учётная запись из-за переключателя PsExec -s), и конкретные изменённые или удалённые значения реестра.
- **Журналы сети и брандмауэра**: анализ сетевого трафика, особенно трафика SMB, характерного для использования PsExec, и журналов брандмауэра в целевой системе может выявить подключения к общим ресурсам администрирования и изменения конфигурации сети системы. Журналы коррелируют со временем выполнения команды, предоставляя дополнительный контекст для действия.

H. Стратегии для скомпрометированных сетей

В случае обнаружения факта компрометации необходимо применение защитных контрмер.

1) Действия немедленного реагирования

- Сброс учётных данных для привилегированных и непривилегированных учётных записей в пределах границ доверия каждой скомпрометированной учётной записи.
- Принудительный сброс пароля, отзыв и выдача новых сертификатов для всех учётных записей и устройств.

2) Действия, относящиеся к среде Windows:

- При подозрении на доступ к Контроллеру домена (DC) или Active Directory (AD) сброс паролей всех

локальных учётных записей, включая Guest, HelpAssistant, DefaultAccount, System, Administrator и krbtgt. Учётную запись krbtgt, которая обрабатывает запросы на регистрацию Kerberos, следует дважды сбросить для обеспечения безопасности из-за истории с двумя паролями.

- Если есть подозрение, что файл ntds.dit подвергался эксфильтрации, требуется сброс пароля всех пользователей домена.
- Просмотр и коррекция политики доступа для временного отзыва или уменьшения права доступа для затронутых учётных записей и устройств.
- Сброс учётных данных учётной записи без повышенных прав доступа: если доступ атакующего ограничен правами, сброс соответствующих учётным данным ключа доступа и отслеживание дальнейших признаков несанкционированного доступа, особенно к учётным записям администраторов.

3) Аудит конфигурации сети и устройств

- **Аудит сетевых устройств и пограничных устройств**: проверка наличия признаков несанкционированных или вредоносных изменений конфигурации. Если изменения обнаружены:
  - Требуется изменения всех учётных данных, используемых для управления сетевыми устройствами, включая ключи и строки, обеспечивающие функции сетевого устройства.
  - Обновление всех прошивок и программного обеспечения до последних версий.

4) Использование инструмента удалённого доступа

Минимизация удалённого доступа и контроль: следование рекомендациям по обеспечению безопасности средств и протоколов удалённого доступа, включая рекомендации по безопасности программного обеспечения удалённого доступа и безопасному использованию PowerShell.

I. Рекомендации для производителей ПО

1) Минимизация векторов атаки

Производителям ПО настоятельно рекомендуется минимизировать возможности атаки путём выполнения различных действий: отключение ненужных протоколов по умолчанию, ограничение количества процессов и программ, запущенных с повышенными привилегиями, и принятие упреждающих мер по ограничению возможностей участников использовать нативные функциональные возможности для вторжений.

2) Внедрение системы безопасности в SDLC

Безопасность должна быть встроена в архитектуру продукта на протяжении всего жизненного цикла разработки программного обеспечения (SDLC). Такая упреждающая интеграция гарантирует, что соображения безопасности станут не второстепенной задачей, а фундаментальным компонентом продукта от начала разработки до развертывания.

3) Обязательная многофакторная аутентификация (MFA)

Производителям следует установить MFA, в идеале защищенный от фишинга, для привилегированных пользователей и сделать его функцией по умолчанию, а не необязательной. Этот шаг значительно повышает безопасность учётных записей пользователей, особенно тех, которые имеют повышенный доступ.

4) Уменьшение hardening-действий

Объём действий, прилагаемых к объектам защиты, следует отслеживать и уменьшать. По мере выпуска новых версий программного обеспечения целью должно быть уменьшение размера этих руководств с течением времени путем интеграции их компонентов в качестве конфигурации продукта по умолчанию.

5) Учёт пользовательского опыта

Необходимо учитывать влияние настроек безопасности на работу пользователя. В идеале наиболее безопасная настройка должна быть интегрирована в продукт по умолчанию, а при необходимости настройки опция должна быть защищена от распространённых угроз. Такой подход снижает когнитивную нагрузку на конечных пользователей и обеспечивает широкую защиту.

6) Удаление паролей по умолчанию

Пароли по умолчанию следует полностью исключить, или сформировать, или установить при первой установке, а затем периодически менять. Такая практика предотвращает использование паролей по умолчанию в качестве удобной точки входа для злоумышленников.

7) Ограничение динамического выполнения кода

Динамическое выполнение кода, хотя и обеспечивает универсальность, представляет собой уязвимое место для атаки. Производителям следует ограничить или удалить возможность динамического выполнения кода из-за высокого риска и сложности обнаружения связанных с ним индикаторов компрометации (IoC).

8) Удаление фиксированных учётных данных

Приложения и скрипты, содержащие информацию об учётных данных в виде открытого текста (hardcode), представляют значительный риск для безопасности. Удаление таких учётных данных важно для предотвращения использования их злоумышленниками для доступа к ресурсам и расширения своего присутствия в сети.