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

ХРОНИКИ БЕЗОПАСНИКА

ДАЙДЖЕСТ. 2024 / 06

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

SPONSR

TELEGRAM

Рубрика: Ключевые факты

сжатая редакция других разделов для быстрого и всестороннего обзора.

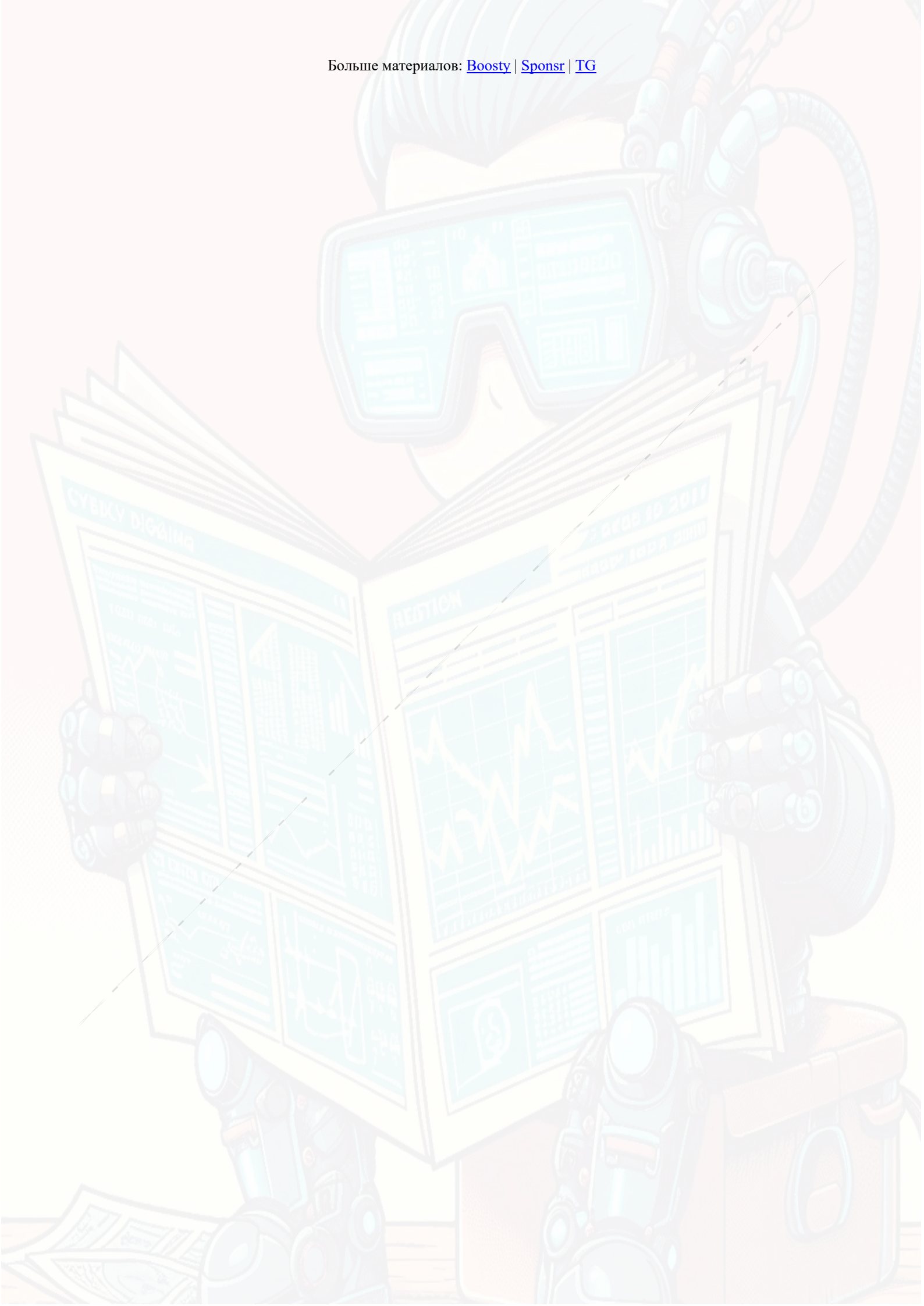
Рубрика: Разбор

критические обзоры и анализ статей, включая научно-практические статьи и отраслевые отчёты

Рубрика: Исследование

оригинальные исследования, отчёты и выводы, способствующие пониманию проблем кибербезопасности

Больше материалов: Boosty | Sponsr | TG



Новости

Ботнет, нацеленный на старые непропатченные D-Link устройства

Ботнет под названием "Goldoon" нацелен на уязвимость десятилетней давности в незащищённых устройствах D-Link.

📌 **Уязвимость:** Goldoon использует CVE-2015-2051, критический дефект безопасности с оценкой CVSS 9,8, который затрагивает маршрутизаторы D-Link DIR-645. Эта уязвимость позволяет злоумышленникам удалённо выполнять произвольные команды с помощью специально созданных HTTP-запросов.

📌 **Действия ботнета:** Как только устройство скомпрометировано, злоумышленники получают полный контроль, что позволяет им извлекать системную информацию, устанавливать связь с сервером управления (C2) и использовать устройства для проведения дальнейших атак, таких как распределённые атаки типа "отказ в обслуживании" (DDoS).

📌 **Методы DDoS-атак:** Ботнет Goldoon способен запускать различные DDoS-атаки, используя такие методы, как TCP-флудинг, ICMP-флудинг, и более специализированные атаки, такие как Minecraft DDoS.

📌 **Распространение и скрытность:** Ботнет инициирует атаку, используя CVE-2015-2051 для развёртывания скрипта-"дроппера" с вредоносного сервера. Этот скрипт предназначен для самоуничтожения, чтобы избежать обнаружения, и работает в различных архитектурах систем Linux. Программа загружает и запускает файл, "подготавливая почву" для дальнейших вредоносных действий.

📌 **Меры по снижению и предотвращению:** Пользователям настоятельно рекомендуется своевременно обновлять устройства D-Link. Кроме того, внедрение решений для мониторинга сети, установление строгих правил брандмауэра и постоянное информирование о последних бюллетенях по безопасности и исправлениях являются важными шагами, позволяющими опережать возникающие угрозы.

📌 **Влияние и критичность:** Использование CVE-2015-2051 ботнетом Goldoon представляет собой малозатратную атаку, но оказывает критическое воздействие на безопасность, которое может привести к удалённому выполнению кода. Активность ботнета резко возросла в апреле 2024 года почти вдвое.

📌 **Рекомендации:** Fortinet рекомендует по возможности использовать исправления и обновления в связи с постоянным развитием и внедрением новых ботнетов. Организациям также рекомендуется пройти бесплатный обучающий курс Fortinet по кибербезопасности, который поможет конечным пользователям научиться распознавать фишинговые атаки и защищаться от них.

Затронутые отрасли промышленности

📌 **Домашние сети и сети малого бизнеса:** они подвергаются непосредственному воздействию, поскольку в этих средах обычно используются маршрутизаторы D-Link. Компрометация этих маршрутизаторов может привести к сбоям в работе сети и несанкционированному доступу к сетевому трафику.

📌 **Интернет-провайдеры (ISP):** Интернет-провайдеры могут столкнуться с повышенным давлением, требуя от клиентов помощи в обновлении или замене уязвимых устройств, и они могут испытывать повышенную нагрузку на сеть в результате DDoS-атак от скомпрометированных маршрутизаторов.

📌 **Компании, занимающиеся кибербезопасностью:** Эти организации могут столкнуться с повышенным спросом на услуги в области безопасности, включая обнаружение угроз, повышение надёжности систем и реагирование на инциденты, связанные со взломанными маршрутизаторами.

📌 **Электронная коммерция и онлайн-сервисы:** Компании в этом секторе могут стать объектами DDoS-атак, запущенных со взломанных устройств, что потенциально может привести к перебоям в обслуживании и финансовым потерям.

📌 **Здравоохранение:** С ростом числа медицинских служб, использующих подключение к Интернету, скомпрометированные маршрутизаторы могут представлять угрозу целостности данных пациентов и доступности критически важных услуг.

Последствия

📌 **Компрометация сети и утечка данных:** Злоумышленники могут получить полный контроль над скомпрометированными маршрутизаторами, что потенциально может привести к краже данных, включая конфиденциальную личную и финансовую информацию.

📌 **Распределённые атаки типа "Отказ в обслуживании" (DDoS):** Ботнет может запускать различные DDoS-атаки, которые могут нанести ущерб сетевой инфраструктуре, нарушить работу служб и привести к значительному простою в работе затронутых организаций.

📌 **Увеличение эксплуатационных расходов:** Организациям может потребоваться инвестировать в усиленные меры безопасности, проводить широкомасштабные проверки и заменять или обновлять уязвимые устройства, что приведёт к увеличению эксплуатационных расходов.

📌 **Ущерб репутации:** Компании, пострадавшие от атак, связанных со взломанными маршрутизаторами, могут понести репутационный ущерб, если будет сочтено, что они недостаточно защищают данные клиентов или не обеспечивают доступность услуг.

📌 **Нормативно-правовые последствия:** Организации, которые не обеспечивают надлежащую защиту своих сетей, могут столкнуться с проверкой со стороны регулирующих органов и потенциальными юридическими проблемами, особенно если данные потребителей будут скомпрометированы из-за небрежности при устранении известных уязвимостей.

QEMU для эмуляции IoT прошивок

В статье приводится руководство по использованию QEMU для эмуляции встроенного по IoT, в частности, с акцентом на практический пример, связанный с эмуляцией встроенного ПО маршрутизатора. Автор делится идеями и подробными шагами о

том, как эффективно использовать QEMU для исследований и тестирования безопасности.

Обзор QEMU

📌 QEMU используется для эмуляции различных аппаратных архитектур, что делает его ценным инструментом для ИБ-исследователей, которым необходимо тестировать программное обеспечение в контролируемой среде без физического оборудования.

📌 В руководстве особое внимание уделяется использованию Ubuntu 18.04 для настройки QEMU из-за простоты управления интерфейсами в этом конкретном дистрибутиве.

Первоначальная настройка и установка

📌 В документе описаны начальные шаги по установке QEMU и его зависимостей от Ubuntu 18.04, включая установку библиотек и инструментов, необходимых для создания сетевых мостов и отладки с помощью pwndbg.

Анализ и подготовка встроенного ПО

📌 Binwalk используется для анализа и извлечения содержимого встроенного ПО. В руководстве подробно описано, как использовать Binwalk для идентификации и распаковки компонентов встроенного ПО, уделяя особое внимание файловой системе squashfs, которая имеет решающее значение для процесса эмуляции.

Процесс эмуляции

📌 **Среда Chroot:** Для этого необходимо скопировать двоичный файл qemu-mips-static в каталог встроенного ПО и использовать chroot для непосредственного запуска веб-сервера встроенного ПО.

📌 **Эмуляция системного режима:** Этот метод использует скрипт и дополнительные загрузки (например, vmlinux и образ Debian) для создания более стабильной и интегрированной среды эмуляции.

Отладка и настройка сети

📌 Приведены подробные инструкции по настройке сетевых мостов и интерфейсов, которые позволят эмулируемому микропрограммному обеспечению взаимодействовать с хост-системой.

📌 В руководстве также описывается установка различных каталогов (/dev, /proc, /sys) для обеспечения доступа эмулируемой системы к необходимым ресурсам.

Запуск и взаимодействие с эмулируемым встроенным ПО

📌 После завершения настройки микропрограммное обеспечение запускается, и пользователь может взаимодействовать с эмулируемым веб-сервером через браузер. В руководстве содержатся советы по устранению распространённых проблем, таких как неправильные пути или отсутствующие файлы, которые могут привести к сбою сервера.

Тестирование безопасности и обратное проектирование

📌 Документ завершается описанием использования программы эмуляции для тестирования безопасности и обратного проектирования. В нем упоминаются такие инструменты, как Burp Suite для сбора веб-запросов и Ghidra для анализа двоичных файлов.

Практическая демонстрация

📌 Представлена практическая демонстрация поиска и использования уязвимости, связанной с внедрением команд, в эмулируемом микропрограммном обеспечении, демонстрирующая, как QEMU можно использовать для тестирования и разработки доказательств концепции уязвимостей в системе безопасности.

Уязвимость TP-Link TDDP (Buffer Overflow)

В статье представлен подробный анализ конкретной уязвимости в устройствах TP-Link, о которой сообщалось в 2020 году, но которой до настоящего момента не был присвоен индикатор и статус CVE.

📌 **Причины возникновения уязвимости переполнения буфера TDDP в TP-Link:** Уязвимость TDDP-протокола TP-Link (протокол отладки устройств TP-LINK), связанная с переполнением буфера, в первую очередь связана с обработкой протоколом UDP-пакетов. TDDP, двоичный протокол, используемый для целей отладки, обрабатывает пакеты с помощью одного UDP-пакета, который при неправильной обработке может представлять угрозу безопасности. Конкретной причиной переполнения буфера является отсутствие надлежащей проверки длины данных во время анализа этих UDP-пакетов. Эта приводит к переполнению памяти, что приводит к повреждению структуры памяти устройства

📌 **Последствия уязвимости:** Основной причиной уязвимости, связанной с переполнением буфера TDDP в TP-Link, является отказ в обслуживании (DoS). Это происходит, когда переполнение приводит к повреждению структуры памяти, в результате чего устройство выходит из строя или перестаёт отвечать на запросы. Кроме того, существует вероятность удалённого выполнения кода, что может позволить злоумышленнику выполнить произвольный код на устройстве. Это может привести к несанкционированному доступу к сети, краже данных или дальнейшему использованию сетевых ресурсов

📌 **Методы использования:** Использование уязвимости переполнения буфера TDDP в TP-Link связано с отправкой созданных UDP-пакетов, которые превышают установленные протоколом пределы буфера. Этого можно достичь, манипулируя длиной данных пакета, чтобы она превышала то, что может обработать буфер, что приводит к переполнению. Такие инструменты, как Shambles, могут использоваться для выявления, устранения, эмуляции и проверки таких условий переполнения буфера. Успешное использование может позволить злоумышленникам вызвать отказ в обслуживании или потенциально выполнить произвольный код на устройстве.

Стратегии смягчения последствий

📌 **Обновления встроенного ПО:** Регулярное обновление встроенного по устройств TP-Link до последней версии может помочь устранить уязвимости и повысить безопасность.

📌 **Сегментация сети:** Размещение критически важных устройств в отдельных сегментах сети может ограничить распространение потенциальных атак.

📌 **Правила брандмауэра:** Настройка брандмауэров для ограничения входящего трафика через UDP-порт 1040, который

используется TDDP, может предотвратить несанкционированный доступ.

📌 **Сканеры уязвимостей:** Регулярное сканирование уязвимостей средствами безопасности может помочь выявить их и устранить до того, как они будут использованы.

Обзор TDDP

📌 **Протокол отладки устройств TP-Link (TDDP):** Двоичный протокол, используемый в основном для целей отладки, который работает с помощью одного UDP-пакета. Этот протокол описан в патенте CN102096654A.

📌 **Структура пакета:** Пакет TDDP содержит такие поля, как версия, тип, код, ReplyInfo, PktLength, PktID, подтип, Резерв и дайджест MD5, которые имеют решающее значение для работы протокола.

Анализ уязвимых функций:

📌 **tddpEntry (sub_4045f8 0x004045F8):** Эта функция постоянно проверяет входящие данные с помощью функции recvfrom и передаёт данные в функцию TddpPktInterfaceFunction без проверки размера полученных данных.

📌 **GetTddpMaxPktBuff (sub_4042d0 0x004042D0):** Возвращает размер буфера, равный 0x14000.

📌 **tddp_versionTwoOpt (sub_404b40 0x00405990) и tddp_deCode (sub_404fa4 0x00405014):** функции, участвующие в обработке и декодировании пакета TDDP. Они обрабатывают расшифровку данных с помощью DES и проверяют целостность расшифрованных данных.

Механизм использования

📌 **Триггер переполнения буфера:** Уязвимость срабатывает, когда длина пакета, указанная в пакете TDDP, превышает размер буфера (0x14000), что приводит к переполнению буфера.

📌 **Расшифровка и проверка MD5:** Для расшифровки используется функция des_min_do, и дайджест пакета MD5 сверяется с дайджестом данных MD5. Если длина пакета превышает размер буфера, это приводит к повреждению памяти и отказу в обслуживании (DoS).

Проверка концепции (PoC)

📌 **Настройка:** PoC включает в себя настройку виртуальной машины (ВМ) с встроенным ПО и запуск службы tddpd.

📌 **Код эксплойта:** Документ содержит код на Python, который создает пакет TDDP с определёнными полями, манипулируемыми для запуска переполнения буфера.

📌 **Результат:** Выполнение PoC приводит к сбою программы tddpd, что подтверждает уязвимость.

Вывод:

📌 **Последствия:** Уязвимость приводит к отказу в обслуживании и потенциально позволяет выполнять удаленный код при дальнейшем использовании.

📌 **Рекомендации:** Для устранения таких уязвимостей рекомендуется регулярно обновлять и исправлять, сегментировать сеть и надлежащим образом проверять поступающие данные.

QCSuper: Подслушивание устройства становится увлечением

QCSuper – универсальный инструмент, предназначенный для различных целей. Его функциональные возможности перехвата и анализа радио-сетевых данных с устройств на базе Qualcomm делает его незаменимым для операторов связи, исследователей в области безопасности, разработчиков сетей.

Основные возможности QCSuper

📌 **Поддержка протоколов:** перехват сырых радио-фреймов для сетей 2G (GSM), 2,5G (GPRS и EDGE), 3G (UMTS) и 4G (LTE). Для некоторых моделей доступна частичная поддержка 5G.

📌 **Совместимость с устройствами:** Работает с телефонами и модемами на базе Qualcomm, включая рут Android-устройства и USB-донглы

📌 **Вывод данных:** Формирует файлы PCAP с инкапсуляцией GSMTAP, которые можно проанализировать с помощью Wireshark.

📌 **Простота использования:** простые команды для начала сбора данных

📌 **Кроссплатформенная поддержка:** поддерживается установка как на Linux, так и на Windows, с подробными инструкциями для обеих платформ

📌 **Исследования и анализ:** Широко используется исследователями в области телекоммуникаций, мобильной связи и безопасности для анализа радиосвязи

Аппаратные требования QCSuper

📌 **Устройства на базе Qualcomm:** Основным требованием является наличие телефона или модема на базе Qualcomm. Это связано с тем, что QCSuper использует протокол Qualcomm Diag для перехвата данных

📌 **Рут Android-телефон или USB-модем:** Рут доступ требуется для доступа к необходимым диагностическим интерфейсам

📌 **Совместимость с операционной системой:** QCSuper протестирован на Ubuntu LTS 22.04 и Windows 11.

📌 **Wireshark:** Wireshark необходим для анализа файлов PCAP, сформированных QCSuper. В зависимости от типа снимаемых кадров требуются различные версии Wireshark (например, Wireshark 2.x - 4.x для кадров 2G/3G, Wireshark 2.5.x для кадров 4G и Wireshark 3.6.x для кадров 5G).

Ограничения

🚫 QCSuper нельзя использовать с телефонами, отличными от Qualcomm. Этот инструмент специально использует протокол Qualcomm Diag, который является фирменным протоколом, доступным только на устройствах на базе Qualcomm. Поэтому он несовместим с телефонами или модемами, которые не используют чипсеты Qualcomm

🚫 QCSuper не может перехватывать радио-фреймы 5G на всех устройствах. Возможность захвата радиокадров 5G

ограничена некоторыми моделями устройств на базе Qualcomm. Инструмент частично поддерживает 5G, и эта функциональность была протестирована в определённых условиях с помощью Wireshark 3.6.x . Поэтому не все устройства на базе Qualcomm обязательно будут поддерживать захват кадров 5G, и пользователям может потребоваться проверить совместимость для конкретной модели устройства.

Применение QCSuper

Телекоммуникационная отрасль:

📌 **Анализ сети:** QCSuper позволяет операторам связи фиксировать и анализировать обмен радиосигналами между мобильными устройствами и сетью. Это помогает лучше понять производительность сети, диагностировать проблемы и оптимизировать сетевые конфигурации.

📌 **Соответствие протоколам:** Фиксируя исходные радиокадры, телекоммуникационные компании могут гарантировать соответствие своих сетей отраслевым стандартам и протоколам, таким как те, которые определены в 3GPP для сетей 2G, 3G, 4G и 5G.

Безопасность мобильной связи:

📌 **Исследование безопасности:** Исследователи могут использовать QCSuper для изучения уязвимостей в мобильных сетях и выявления потенциальных недостатков в системе безопасности и разрабатки стратегии их устранения.

📌 **Тестирование на проникновение:** QCSuper полезен для проведения тестов на проникновение в мобильные сети. Это позволяет специалистам по безопасности моделировать атаки и оценивать устойчивость сети к различным угрозам.

Сетевые исследования и разработки:

📌 **Анализ протоколов:** Исследователи могут использовать QCSuper для сбора и анализа сигнальной информации и пользовательских данных на разных уровнях стека мобильной сети. Это имеет значение для разработки новых протоколов и улучшения существующих.

📌 **Исследование 5G:** Благодаря частичной поддержке 5G QCSuper играет важную роль в изучении достижений в области мобильных технологий, чтобы понять новые возможности и проблемы, связанные с сетями 5G.

Образовательные и обучающие цели:

📌 **Учебные программы**: QCSuper используется в учебных программах для обучения специалистов в области телекоммуникаций и безопасности протоколам и безопасности мобильных сетей, предоставляя практический опыт сбора и анализа реального сетевого трафика.

📌 **Академические исследования:** Университеты и исследовательские институты могут использовать QCSuper для академических проектов и исследований, помогая студентам и исследователям получить практическое представление о работе мобильных сетей.

Incident Response Made Easy: Using BucketLoot for Cloud Storage Forensics

BucketLoot, универсальный в работе с облачными платформами и обширный набор функций делают его ценным дополнением к инструментам специалистов по безопасности, команд DevOps и организаций, стремящихся повысить уровень своей облачной безопасности и защитить конфиденциальные данные, хранящиеся в облачных хранилищах объектов.

Ключевые функции

📌 **Автоматическая проверка облачных хранилищ:** BucketLoot может автоматически сканировать и проверять облачные хранилища, совместимые с S3, на нескольких платформах, включая Amazon Web Services (AWS), Google Cloud Storage (GCS), DigitalOcean Spaces и пользовательские домены/URL-адреса.

📌 **Извлечение ресурсов:** Инструмент может извлекать ресурсы, хранящиеся в корзинах, такие как URL-адреса, поддомены и домены, которые могут быть полезны для управления объектами атаки и разведки.

📌 **Обнаружение секретных данных:** BucketLoot может обнаруживать и помечать потенциальные секретные данные, такие как API-ключи, токены доступа и другую конфиденциальную информацию, помогая организациям выявлять и снижать риски безопасности.

📌 **Пользовательский поиск по ключевым словам и регулярным выражениям:** пользователи могут выполнять поиск по определённым ключевым словам или регулярным выражениям в файлах корзины, что позволяет осуществлять целенаправленный поиск конфиденциальных данных или определённых типов информации.

📌 **Эффективное сканирование:** BucketLoot специализируется на сканировании файлов, в которых хранятся данные в текстовом формате, оптимизируя процесс сканирования и повышая производительность.

📌 **Гибкие режимы сканирования:** Инструмент предлагает гостевой режим для первоначального сканирования без необходимости использования учётных данных, а также режим полного сканирования с использованием учётных данных платформы для более всестороннего анализа.

📌 **Вывод в формате JSON:** BucketLoot предоставляет свои выходные данные в формате JSON, что упрощает анализ и интеграцию результатов в существующие рабочие процессы или другие инструменты обеспечения безопасности.

Полезность для различных отраслей и экспертов в области безопасности

📌 **Профессионалы в области кибербезопасности:** BucketLoot - это инструмент для специалистов в области кибербезопасности, таких как пентестеры, багхантеры и исследователи безопасности, т.к. он помогает выявлять потенциальные уязвимости и проблемы доступа к данным в конфигурациях облачных хранилищ.

📌 **Поставщики облачных услуг:** Организации, предлагающие облачные сервисы, могут использовать BucketLoot

для обеспечения безопасности данных своих клиентов, хранящихся в облачных хранилищах, и поддержания соответствия отраслевым стандартам.

📌 **Команды DevSecOps и DevOps:** Интегрируя BucketLoot в свои рабочие процессы, команды DevSecOps и DevOps могут проактивно выявлять и снижать риски безопасности, связанные с облачными хранилищами, продвигая безопасные методы разработки программного обеспечения.

📌 **Реагирование на инциденты и криминалистика:** В случае утечки данных или инцидента BucketLoot может помочь группам реагирования на инциденты и судебным следователям быстро идентифицировать уязвимые данные и потенциальные векторы атак, связанные с неправильной конфигурацией облачного хранилища.

📌 **Соответствие требованиям и управление рисками:** Организации, на которые распространяются требования нормативных актов, такие как GDPR, HIPAA или PCI-DSS, могут использовать BucketLoot для обеспечения безопасной обработки конфиденциальных данных, хранящихся в облачных хранилищах, и демонстрации соблюдения стандартов защиты данных.

📌 **Программы вознаграждения за ошибки:** Багхантеры и исследователи могут использовать BucketLoot для выявления потенциальных уязвимостей и доступа к данным в конфигурациях облачных хранилищ, что способствует повышению общей безопасности организаций и получению вознаграждений.

FIDO2: Устойчив к фишингу, но не к токенам

В статье рассказывается о том, как MITM-атаки могут обойти защиту FIDO2 от фишинга; подробно описывается процесс аутентификации в FIDO2, освещаются уязвимости в обработке токенов сеанса и приводятся реальные примеры, связанные с использованием единого входа Entra ID, PingFederate и Yubico Playground, а также стратегии устранения неполадок для повышения безопасности.

📌 FIDO2 – это современный стандарт аутентификации без пароля, разработанный Альянсом FIDO Alliance для замены паролей

📌 Он предназначен для защиты от фишинга, атак типа "человек посередине" (MITM) и перехвата сеанса

📌 Процесс аутентификации включает в себя регистрацию устройства и аутентификацию с использованием криптографии с открытым ключом

Функции безопасности FIDO2

📌 FIDO2 разработан для предотвращения фишинговых атак, MITM и перехвата сеанса

📌 Однако исследование показало, что реализации FIDO2 часто не защищают токены сеанса после успешной аутентификации

Атака на FIDO2 с помощью MITM

📌 Автор исследовал атаки MITM на поставщиков идентификационных данных (IDP), которые ретранслируют сообщения между устройствами

📌 Хотя MITM сложнее использовать с помощью TLS, такие методы, как подмена DNS, отравление ARP и кража сертификатов, могут помочь в этом

📌 Выполнив MITM для IdP, злоумышленник может перехватить токен сеанса после проверки подлинности FIDO2

EntraID SSO (Microsoft)

📌 **Обзор:** Entra ID SSO - это решение для единого входа, которое поддерживает различные протоколы единого входа и современные методы аутентификации, включая FIDO2.

📌 **Уязвимость**: Исследование показало, что злоумышленник может перехватывать сеансы, используя способ, которым Entra ID обрабатывает токены сеанса.

📌 **Метод атаки:** Злоумышленнику не нужно ретранслировать весь процесс аутентификации. Вместо этого он может использовать подписанный токен, предоставленный IdP, срок действия которого составляет один час. Этот токен может быть повторно использован в течение допустимого периода времени для создания файлов cookie состояния на более длительный период.

📌 **Пример:** Собственное приложение портала управления Azure не проверяет токен, предоставленный службой единого входа, что позволяет злоумышленнику использовать украденный токен для получения несанкционированного доступа.

PingFederate

📌 **Обзор:** PingFederate - это решение для единого входа, которое использует сторонние адаптеры для выполнения аутентификации. Эти адаптеры могут быть объединены в поток политики аутентификации.

📌 **Уязвимость:** Исследование показало, что если разработчик, которому доверяют, не проверит токен OIDC (или SAML-ответ), атака MITM может быть успешной.

📌 **Метод атаки:** Атака использует самое слабое звено в цепочке аутентификации. Поскольку протоколы единого входа основаны на предоставлении токенов, которые могут быть повторно использованы различными устройствами, злоумышленник может перехватить сеанс, украв эти токены.

📌 **Пример:** Адаптер PingOne можно использовать с поддержкой FIDO2. Если токен OIDC не будет подтверждён, злоумышленник может обойти защиту FIDO2 и получить несанкционированный доступ.

Yubico Playground

📌 **Обзор:** Yubico Playground - это среда тестирования функций и ключей безопасности FIDO.

📌 **Уязвимость:** Исследование показало, что можно использовать простой сеансовый файл cookie, сгенерированный после аутентификации FIDO2.

📌 **Метод атаки:** На устройстве, запросившем сеансовый файл cookie, отсутствует проверка подлинности. Любое устройство может использовать этот файл cookie до истечения срока его действия, что позволяет злоумышленнику обойти этап аутентификации.

📌 **Пример:** Получив файл cookie сеанса, злоумышленник может получить доступ к личному кабинету пользователя и удалить ключ

Трассировка лучей на ZX Spectrum: Зачем нужны современные GPU, когда можно потратить выходные на рендеринг одного кадра, чтобы доказать, что мазохизм отличное хобби?

Проект ZX Raytracer не только демонстрирует возможность внедрения трассировщика лучей в ZX Spectrum, но и служит образовательным ресурсом, посвящённым истории вычислительной техники, и источником вдохновения для будущих проектов в области ретро-вычислений, встраиваемых систем и методов оптимизации

Ключевые моменты и потенциальные области применения

📌 **Реализация Raytracer на устаревшем оборудовании:** Проект демонстрирует возможность реализации raytracer, технологии рендеринга графики, требующей больших вычислительных затрат, на ZX Spectrum, домашнем компьютере 1980-х годов с очень ограниченными аппаратными возможностями (процессор Z80A с частотой 3,5 МГц и часто всего 16Кб оперативной памяти).

📌 **Преодоление аппаратных ограничений:** Несмотря на серьезные аппаратные ограничения, проект преодолел такие проблемы, как цветовые ограничения, низкое разрешение 256x176 пикселей и низкую производительность (начальное время рендеринга 17 часов на кадр) благодаря продуманной оптимизации и приближениям.

📌 **Образовательный инструмент:** Проект может быть использован в качестве учебного пособия на курсах информатики, особенно тех, которые посвящены компьютерной графике, методам оптимизации или низкоуровневому программированию.

📌 **Выставки ретро-игр и демосцены**: Raytracer можно демонстрировать на ретро-компьютерных мероприятиях, вечеринках-демосценах или выставках, посвящённых достижениям винтажного оборудования и программирования.

📌 **Разработка встраиваемых систем:** Методы оптимизации и аппроксимации, использованные в этом проекте, могут вдохновить разработчиков, работающих над встраиваемыми системами или устройствами с ограниченными ресурсами, где решающее значение имеет эффективное использование ограниченных ресурсов.

📌 **Знакомство с историей вычислительной техники:** Проект может быть представлен в музеях или на выставках, посвящённых истории вычислительной техники, демонстрируя изобретательность и творческий подход первых программистов, работавших с ограниченными аппаратными ресурсами.

📌 **Вдохновение для будущих проектов:** Успех этого проекта может побудить других изучить возможности устаревшего оборудования или взяться за аналогичные сложные проекты, расширяя границы возможного на старых системах.

ICSpector: Решение Forensics-проблем, о которых вы и не подозревали

Microsoft ICS Forensics Tools (ICSpector) - инструмент с открытым исходным кодом, предназначенный для криминалистического анализа промышленных систем управления (ICS), в частности, программируемых логических контроллеров (PLC).

Технические характеристики

Состав и архитектура

📌 **Модульная конструкция:** ICSpector состоит из нескольких компонентов, что обеспечивает гибкость и индивидуальную настройку в зависимости от конкретных потребностей. Пользователи могут также добавлять новые анализаторы.

📌 **Сетевой сканер:** Идентифицирует устройства, взаимодействующие по поддерживаемым протоколам OT, и обеспечивает их работоспособность. Он может работать с предоставленной IP-подсетью или с определённым списком IP-адресов.

📌 **Извлечение данных и анализатор:** Извлекает метаданные и логику ПЛК, преобразуя необработанные данные в удобочитаемую форму, чтобы выделить области, которые могут указывать на вредоносную активность.

Криминалистические возможности

📌 **Идентификация скомпрометированных устройств:** помогает идентифицировать скомпрометированные устройства с помощью ручной проверки, автоматизированного мониторинга или во время реагирования на инциденты.

📌 **Создание моментальных снимков:** Позволяет создавать моментальные снимки проектов контроллеров для сравнения изменений с течением времени, что помогает обнаруживать несанкционированное вмешательство или аномалии.

📌 **Поддержка ПЛК Siemens:** В настоящее время поддерживаются семейства Siemens SIMATIC S7-300 и S7-400, в будущем планируется поддержка других семейств ПЛК.

Интеграция с другими инструментами

📌 **Microsoft Defender для Интернета вещей:** Может использоваться совместно с Microsoft Defender для Интернета вещей, который обеспечивает безопасность на сетевом уровне, непрерывный мониторинг, обнаружение активов, угроз и управление уязвимостями в средах Интернета вещей/OT.

Примеры использования

📌 **Реагирование на инциденты:** активности по реагированию на инциденты позволяют обнаружить скомпрометированные устройства и понять, был ли взломан код ПЛК.

📌 **Проактивная защита:** Помогает в проактивном реагировании на инциденты, сравнивая программы ПЛК на инженерных рабочих станциях с программами на реальных устройствах для обнаружения несанкционированных изменений.

Отрасли

📌**Атомные, тепловые и гидроэлектростанции:** Электростанции в значительной степени зависят от промышленных систем управления для управления критически важными операциями. ICSpector можно использовать для обеспечения целостности программируемых логических контроллеров, которые управляют этими процессами. Обнаруживая любые аномальные индикаторы или скомпрометированные конфигурации, ICSpector помогает предотвратить сбои в работе, которые могут привести к отключению электроэнергии или угрозе безопасности.

📌**Водоочистные сооружения:** На этих объектах используются микросхемы управления процессами очистки, обеспечивающие безопасность воды. ICSpector может помочь в мониторинге и проверке целостности ПЛК, гарантируя, что процессы очистки воды не будут нарушены, что имеет решающее значение для здоровья и безопасности населения.

📌**Промышленное производство:** В производственных условиях микросхемы используются для управления оборудованием и производственными линиями. ICSpector можно использовать для обнаружения любых несанкционированных изменений или аномалий в ПЛК, обеспечивая стабильное качество продукции и предотвращая дорогостоящие простои из-за отказа оборудования.

📌**Сектора критической инфраструктуры:** сюда входят такие отрасли, как энергетика, водоснабжение, транспорт и системы связи. ICSpector можно использовать для защиты систем управления этими критически важными инфраструктурами от кибератак, обеспечивая их непрерывную и безопасную работу.

📌**Предприятия химической промышленности:** На этих предприятиях используются микросхемы для управления сложными химическими процессами. ICSpector может помочь в обеспечении безопасности ПЛК, управляющих этими процессами, и их исправности, что жизненно важно для предотвращения опасных инцидентов.

📌**Нефтегазовая промышленность:** Системы ICS широко используются в нефтегазовом секторе для процессов бурения, переработки и распределения. ICSpector можно использовать для мониторинга и проверки целостности этих систем, предотвращая сбои, которые могут привести к значительным финансовым потерям и ущербу окружающей среде

Взлом реестра для чайников: Удаление рекламы сложным способом с помощью OFGB (Oh Frick Go Back)

OFGB (Oh Frick Go Back) предназначен для удаления рекламы из различных частей операционной системы Windows 11 путём изменения определённых разделов в реестре Windows.

Основные возможности и функционал

📌**Удаление рекламы:** Основная функция OFGB заключается в отключении рекламы, появившейся в обновлении Windows 11 от 23 апреля 2024 года. Эта реклама появляется в различных частях операционной системы, включая проводник и меню "Пуск".

📌**Модификация реестра:** Инструмент работает путём изменения определённых разделов в реестре Windows. Этот метод используется для эффективного отключения рекламы.

📌**Написано на C# и WPF:** OFGB разработан с использованием C# и Windows Presentation Foundation (WPF), которая предоставляет графический пользовательский интерфейс для этого инструмента.

📌**Ссылки:** Разделы реестра и комментарии к их функциям были вдохновлены сценарием Шона Бринка. Кроме того, на тематику приложения повлиял проект Aldaviva под названием DarkNet.

📌**Создание инструмента:** Для создания OFGB пользователям потребуется Visual Studio и .NET 8.0 SDK. Репозиторий можно клонировать или загрузить в виде ZIP-файла, а решение можно создать в Visual Studio, используя сочетание клавиш Ctrl + Shift + B или пункт меню "Сборка" > "Создать решение".

📌**Безопасность и распространение:** Разработчик подчёркивает, что GitHub является единственной официальной платформой распространения OFGB. Безопасность загрузок с других веб-сайтов не гарантируется.

📌**Альтернативное предложение:** Для пользователей, которые хотят вообще не сталкиваться с подобной рекламой, разработчик в шутку предлагает попробовать Linux.

Преимущества OFGB:

📌**Простой и понятный интерфейс:** OFGB предоставляет простой графический интерфейс пользователя (GUI) с флажками для различных типов рекламы, что позволяет пользователям, не обладающим техническими знаниями, легко отключать рекламу, не обращаясь напрямую к реестру Windows.

📌**Комплексное удаление рекламы:** OFGB охватывает широкий спектр рекламных объявлений, включая те, что находятся в меню "Пуск", проводнике, на экране блокировки, в приложении "Настройки" и т. д., предоставляя универсальное решение для удаления рекламы.

📌**Открытый исходный код и бесплатно:** Поскольку OFGB является проектом с открытым исходным кодом, доступным на GitHub, его можно использовать бесплатно, и дорабатывать под свои нужды.

Недостатки OFGB:

📌**Ограниченная функциональность:** В отличие от более комплексных инструментов, таких как Shutup10 или Wintoys, OFGB ориентирован исключительно на удаление рекламы и не предлагает дополнительных функций для обеспечения конфиденциальности, телеметрии или других настроек Windows.

📌**Возможные проблемы с совместимостью:** Поскольку сторонний инструмент изменяет реестр Windows, существует риск возникновения проблем с совместимостью или конфликтов с будущими обновлениями Windows, что потенциально может нарушить настройки удаления рекламы.

📌**Отсутствие автоматических обновлений:** в OFGB отсутствует механизм автоматического обновления, поэтому пользователям может потребоваться вручную проверять и устанавливать новые версии, поскольку Microsoft вводит новые типы объявлений или изменяет разделы реестра.

Для сравнения, такие инструменты, как Shutup10, Wintoys и Tiny11 Builder, предлагают более полную функциональность, включая средства управления конфиденциальностью и телеметрией, параметры настройки и возможность создания пользовательских образов Windows. Однако эти инструменты могут оказаться более сложными в использовании, особенно для пользователей, не обладающих техническими знаниями.

Перезапись встроенного ПО: новая модная тенденция атак на маршрутизаторы

Вредоносная кампания Chalubo RAT была нацелена на конкретные модели маршрутизаторов Actiontec и Sagemcom, в первую очередь затронув сеть Windstream. Вредоносная программа использовала атаки методом перебора для получения доступа, выполняла загрузку данных в память, чтобы избежать обнаружения, и взаимодействовала с серверами C2 по зашифрованным каналам. Атака привела к значительному сбою в работе, потребовавшему замены более 600 000 маршрутизаторов, что подчеркивает необходимость принятия надежных мер безопасности и регулярного обновления для предотвращения подобных инцидентов.

Последствия для интернет-провайдеров:

📌 **Windstream**: Пострадал интернет-провайдер, более 600 000 маршрутизаторов были выведены из строя в период с 25 по 27 октября 2023 года.

📌 **Модели**: Actiontec T3200, T3260 и Sagemcom F5380.

📌 **Последствия**: Примерно 49% модемов интернет-провайдера были отключены, что потребовало замены оборудования.

Глобальные последствия:

📌 **Активность ботнета**: С сентября по ноябрь 2023 года панели ботнета Chalubo взаимодействовали с 117 000 уникальными IP-адресами в течение 30 дней.

📌 **Географическое распределение**: Большинство заражений произошло в США, Бразилии и Китае.

📌 **Особенности**: 95% ботов взаимодействовали только с одной панелью управления.

Уязвимые маршрутизаторы

📌 **Целевые модели:** маршрутизаторы бизнес-класса с истекшим сроком службы.

📌 Actiontec T3200 и T3260 - это беспроводные маршрутизаторы VDSL2, одобренные компанией Windstream.

📌 Sagemcom F5380 - это маршрутизатор WiFi6 (802.11ax).

📌 Модели DrayTek Vigor 2960 и 3900

Вредоносное ПО: Chalubo RAT

📌 Впервые обнаружен Sophos Labs в августе 2018 года.

📌 **Основные функции:** DDoS-атаки, выполнение Lua-скриптов и методы обхода с использованием шифрования ChaCha20.

📌 **Первоначальное заражение:** Использует атаки методом перебора на SSH-серверы со слабыми учётными данными (например, root:admin).

📌 **Доставка полезной нагрузки:**

📌 **Первый этап:** скрипт bash ("get_scrpc") запускает второй скрипт ("get_strtriush"), который извлекает и выполняет основную полезную нагрузку бота ("Chalubo" или "mips.elf").

📌 **Выполнение:** Вредоносная программа запускается в памяти, удаляет файлы с диска и изменяет имя процесса, чтобы избежать обнаружения.

📌 **Взаимодействие:**

📌 **Серверы C2:** выполняется циклический просмотр фиксированных C2s, загрузка следующего этапа и его расшифровка с помощью ChaCha20.

📌 **Закрепление:** Новая версия не поддерживает закрепление на зараженных устройствах.

Вредоносная программа Hiatus RAT

📌 **Порт 8816**: HiatusRAT проверяет наличие существующих процессов на порту 8816, отключает все существующие службы и открывает прослушиватель на этом порту.

📌 **Сбор информации:** Собирает информацию о хосте и отправляет её на сервер C2 для отслеживания статуса заражения и регистрации информации о скомпрометированном хосте.

📌 **Первоначальный доступ:** использование уязвимостей во встроенном ПО маршрутизатора или ненадёжных учётных данных.

📌 **Закрепление:** используется скрипт bash для загрузки и выполнения HiatusRAT и двоичного файла для перехвата пакетов

Лаборатория Black Lotus обнаружила новые вредоносные кампании на маршрутизаторах

📌 Black Lotus Labs, исследовательская группа по изучению угроз в Lumen Technologies (ранее CenturyLink), недавно обнаружила две крупные кампании вредоносных программ, нацеленных на маршрутизаторы и сетевые устройства разных производителей. Эти открытия свидетельствуют о растущих угрозах, с которыми сталкивается инфраструктура Интернета, и о необходимости совершенствования методов обеспечения безопасности.

Кампания Hiatus

📌 В марте 2023 года Black Lotus Labs сообщила о проведении комплексной кампании под названием "Hiatus", которая с июня 2022 года была нацелена на маршрутизаторы бизнес-класса, в первую очередь на модели DrayTek Vigor 2960 и 3900.

📌 Злоумышленники использовали маршрутизаторы DrayTek с истекшим сроком службы для обеспечения долговременного сохранения без обнаружения.

📌 В Интернете было опубликовано около 4100 уязвимых моделей DrayTek, при этом Hiatus скомпрометировал примерно 100 из них в Латинской Америке, Европе и Северной Америке.

📌 После заражения вредоносная программа перехватывает данные, передаваемые через заражённый маршрутизатор, и внедряет троянскую программу удалённого доступа (RAT) под названием "HiatusRAT", которая может передавать вредоносный трафик в дополнительные сети.

📌 Black Lotus Labs отключила маршрутизацию серверов управления и разгрузки (C2) на глобальной магистрали Lumen и

добавила индикаторы компрометации (IOCs) в свою систему быстрой защиты от угроз, чтобы блокировать угрозы до того, как они достигнут сетей клиентов.

Кампания Pumpkin Eclipse

📌 В конце октября 2023 года лаборатория Black Lotus Labs исследовала массовый сбой, затронувший определённые модели шлюзов ActionTec (T3200s и T3260s) и Sagemcom (F5380) в сети одного интернет-провайдера.

📌 Более 600 000 устройств отображали красный индикатор, указывающий на вероятную проблему с повреждением встроенного ПО.

📌 Атака была ограничена определённым номером автономной системы (ASN), затронув около 49% устройств в этой сети, подвергшихся воздействию.

📌 Лаборатории Black Lotus обнаружили многоступенчатый механизм заражения, который позволил установить Chalubo RAT - ботнет, нацеленный на шлюзы SOHO и устройства Интернета вещей.

📌 Black Lotus Labs добавила IOC в свою аналитическую ленту threat intelligence, пополнив портфель подключённых средств безопасности Lumen.

Переход по ссылкам электронных писем - лучший способ подружиться с IT

В статье Google Security Blog "On Fire Drills and Phishing Tests" рассказывается о важности тестов на фишинг и тренингов для повышения безопасности организации.

Важность тестов на фишинг

📌 **Фишинговые тесты как инструмент обучения**: Фишинговые тесты используются для обучения сотрудников распознавать попытки фишинга и реагировать на них. Они имитируют реальные фишинговые атаки, чтобы помочь сотрудникам выявлять подозрительные электронные письма и ссылки.

📌 **Анализ поведения**: Эти тесты дают представление о поведении сотрудников и эффективности текущих программ обучения. Они помогают определить, какие сотрудники или отделы более подвержены фишинговым атакам.

Тренинги по реагированию на инциденты

📌 **Имитация инцидентов**: тренингов включают в себя имитацию инцидентов безопасности для проверки возможностей организации по реагированию на инциденты. Это включает в себя то, насколько быстро и эффективно команда может обнаруживать угрозы безопасности, реагировать на них и устранять их.

📌 **Готовность и совершенствование**: Регулярные учения помогают обеспечить готовность группы реагирования на инциденты к реальным инцидентам безопасности. Они также указывают на области, требующие улучшения в плане реагирования на инциденты.

Интеграция тестов на фишинг и проведения треннингов

📌 **Комплексное обучение безопасности**: Сочетание тестов на фишинг с тренингами обеспечивает комплексный подход к обучению безопасности. Это гарантирует, что сотрудники будут не только осведомлены о фишинговых угрозах, но и знают, как эффективно на них реагировать.

📌 **Реалистичные сценарии**: Объединяя эти два метода, организации могут создавать более реалистичные и сложные сценарии, которые лучше подготовят сотрудников к реальным угрозам.

Показатели и оценка

📌 **Измерение эффективности**: Как тесты на фишинг, так и треним должны оцениваться с использованием показателей для измерения их эффективности. Это включает в себя отслеживание количества сотрудников, которые поддаются тестированию на фишинг, и времени реагирования во время тренингов.

📌 **Постоянное совершенствование**: Данные, собранные в ходе этих учений, следует использовать для постоянного совершенствования программ обучения безопасности и планов реагирования на инциденты.

Организационная культура

📌 **Продвижение культуры, ориентированной прежде всего на безопасность**: Регулярные тесты на фишинг и тренинги помогают продвигать культуру безопасности в организации. Они подчёркивают важность осведомлённости сотрудников о безопасности и готовности к ней.

📌 **Поощряющие сообщения**: Эти упражнения побуждают сотрудников сообщать о подозрительных действиях и потенциальных инцидентах безопасности, способствуя созданию активной среды безопасности.

Обнаружение Android-угроз в режиме реального времени: 200 миллиардов сканирований в день не позволят выявить все угрозы

Обновления для системы безопасности, анонсированные на выставке Google I/O 2024, призваны значительно повысить безопасность и конфиденциальность устройств Android, оказывая влияние на различные отрасли за счёт снижения уровня мошенничества, защиты конфиденциальных данных и укрепления доверия к мобильным технологиям.

Ключевые аспекты

Google Play защита в режиме реального времени:

📌 **Функциональность**: Ежедневно сканирует 200 миллиардов приложений для Android с помощью искусственного интеллекта на устройстве для обнаружения и устранения вредоносных программ и мошеннических приложений.

📌 **Реализация**: Использует частное вычислительное ядро для анализа с сохранением конфиденциальности.

📌 **Установка**: Доступно на устройствах таких производителей, как Google Pixel, Honor, Lenovo, Nothing, OnePlus, Oppo, Sharp и Transsion.

Более надёжная защита от мошенничества:

📌 **Обнаружение мошеннических звонков**: использует искусственный интеллект Gemini-Nano для обнаружения и оповещения пользователей о потенциальных мошеннических звонках в режиме реального времени.

📌 **Защита от совместного использования экрана**: Расширенные средства контроля для предотвращения атак социальной инженерии во время совместного использования экрана.

📌 **Усовершенствованная система безопасности сотовой связи**: новые средства защиты от поддельной сотовой связи для предотвращения слежки и SMS-мошенничества.

Функция приватного пространства:

📌 **Функциональность**: Позволяет пользователям создавать защищённую изолированную часть операционной системы для конфиденциальной информации, аналогичную режиму инкогнито.

📌 **Доступ для разработчиков**: доступен для экспериментов разработчиков, и в ближайшее время ожидается исправление выявленных ошибок.

Расширенные инструменты разработчика:

📌 **Play Integrity API**: Обновлён чтобы разработчики могли обнаруживать и предотвращать мошеннические или рискованные действия.

📌 **Средство выбора фотографий**: Улучшено для поддержки облачных сервисов хранения данных и обеспечения более строгих разрешений на доступ к фотографиям и видео.

Влияние на отрасли промышленности

Финансовые услуги:

📌 **Предотвращение мошенничества**: Улучшенное обнаружение мошеннических звонков и расширенные функции безопасности сотовой связи значительно снизят риск финансового мошенничества и аферисток, защищая как потребителей, так и финансовые учреждения.

📌 **Конфиденциальность данных**: Функция "Личное пространство" обеспечивает сохранность конфиденциальных финансовых данных, повышая доверие к мобильному банкингу и финансовым приложениям.

Здравоохранение:

📌 **Безопасность данных пациентов**: Усовершенствованные меры безопасности, включая оперативное обнаружение угроз и защиту личного пространства, помогут защитить конфиденциальную информацию о пациентах, хранящуюся на мобильных устройствах.

📌 **Телемедицина**: Расширенные возможности совместного использования экрана обеспечат безопасность сеансов телемедицины, предотвращая несанкционированный доступ к данным пациента во время удалённых консультаций.

Электронная коммерция:

📌 **Безопасность транзакций**: Обнаружение мошеннических звонков и расширенная система безопасности сотовой связи защитят пользователей от попыток фишинга и мошенничества, обеспечивая более безопасные онлайн-транзакции.

📌 **Доверие пользователей**: Усовершенствованный контроль конфиденциальности и безопасная среда приложений повысят доверие пользователей к мобильным торговым платформам.

Телекоммуникации:

📌 **Сетевая безопасность**: Усовершенствованные средства защиты сотовой связи помогут операторам связи защитить свои сети от имитаторов сотовой связи и других средств наблюдения.

📌 **Безопасность клиентов**: Функции обнаружения мошенничества в режиме реального времени повысят безопасность клиентов, снизив количество жалоб, связанных с мошенничеством.

Разработка приложений:

📌 **Интеграция в систему безопасности**: Разработчики могут использовать обновлённый API Play Integrity и другие инструменты безопасности для создания более безопасных приложений, снижая риск их эксплуатации и злоупотреблений.

📌 **Конфиденциальность пользователей**: Более строгие разрешения на фотосъёмку и функция личного пространства помогут разработчикам обеспечить соблюдение правил конфиденциальности и завоевать доверие пользователей.

Содержание

AntiPhishStack

В мире, где переход по ссылке сродни переходу по минному полю, фишинг становится главным злодеем. Представляем наших героев: исследователей, написавших эту статью, вооружённых своим новым блестящим оружием - антифишстеком. Это не просто какая-то модель; это чудо борьбы с киберпреступностью на базе LSTM, которому не нужно ничего знать о фишинге, чтобы поймать его.

Они разработали настолько действенный продукт, что традиционные системы обнаружения фишинга могут устареть до слез. Используя мистические возможности сетей LSTM и алхимию функций TF-IDF, они создали эликсир для обнаружения фишинга, которому, как предполагается, могут позавидовать специалисты по кибербезопасности во всем мире.

Fuxnet

На этот раз мы погружаемся в мутные воды вредоносной программы Fuxnet, детища хакерской группы Blackjack.

Место действия: Москва, город, который, ни о чем не подозревая, занимается своими делами, что он вот-вот станет звездой социальный драмы Blackjack.Суть атаки – ничего особенного, просто классический ход "давайте отключим сенсорные шлюзы".

Стремясь к беспрецедентной прозрачности, Blackjack решает транслировать свои киберпреступления на сайте ruexfil.com. Потому что ничто так не кричит о "секретной операции", как публичная демонстрация хакерского мастерства, сопровождаемая скриншотами для особо внимательных пользователей.

Но тут-то интрига и обостряется: первоначальное утверждение о 2659 вышедших из строя сенсорных шлюзах? Кажется, это небольшое преувеличение. Реальное число? Чуть больше 500. Это сродни провозглашению мирового господства для тех сфоткался после пересечения границы в аэропорту.

Создатели, как всегда, намекают на продолжение, утверждая, что их результаты были всего лишь намёком на грядущий хаос. Ведь что такое кибератака без намёка на продолжение, дразнящее аудиторию обещанием новых цифровых разрушений?

АНБ в истерике. AdaptTactics

Приготовьтесь к очередному эпизоду "Кибербезопасности", в котором будут показаны наши любимые кибер-злодеи, и их громкие облачные выходки! На этот раз АНБ и ФБР объединились, чтобы рассказать захватывающую историю о том, что атакующим уже не интересны локальные сети и сервера, когда есть бескрайние просторы облачных сервисов.

Этот документ больше похож на практическое руководство для начинающих киберпреступников, чем на предупреждение. В нем подробно описывается хитроумная смена тактики, когда наглым образом воруются токенов от учётных записей, особенно неиспользуемых, но всё ещё активных, чтобы обойти разом все облачные механизмы защиты.

Если вы думали, что ваши данные в облаке будут в большей безопасности, подумайте ещё раз. А потом, обновите свои пароли, защитите свои учётные записи и, возможно, купите кибер-страховку, этот рынок кибер-продуктов популярнее ИБ-продуктов.

АНБ в истерике. Ubiquiti EdgeRouters

ФБР, АНБ и их международные партнёры порадовали ещё одним рекомендацией по безопасности на этот раз с участием очень популярных пользователей Ubiquiti EdgeRouters и их главной роли в глобальной кибер-драме, срежиссированной APT28.

В этом последнем выпуске блокбастера от экспертов в области кибербезопасности мы узнаем, как Ubiquiti EdgeRouters, эти удобные в использовании устройства, стали невольными соучастниками схем APT28… с их то учётными данными по умолчанию и защитой "зачем вам firewall".

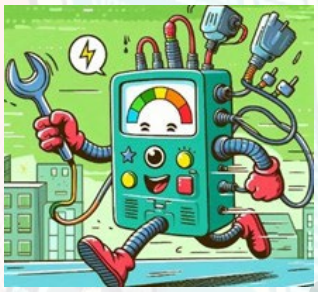
Если вы пользуетесь Ubiquiti EdgeRouters и вас ещё не взломали, поздравляем! Но, возможно, стоит проверить настройки, обновить прошивку и сменить пароли. Или, что ещё лучше, просто отправьте свой маршрутизатор в отпуск в такое место, где APT28 не сможет его найти. Удачной защиты роутера!

АНБ в истерике. SOHO

Ещё один захватывающий документ о невероятно безопасном мире маршрутизаторов для малого и домашнего офиса (SOHO). На этот раз нас ждёт восхитительный анализ, который глубоко погружает в пучину дефектов безопасности, эксплойтов и катастрофических последствий для критически важной инфраструктуры.

В этом документе содержится подробное описание того, как эти устройства, по сути, являются открытыми дверями для спонсируемых государством кибер-вечеринок. Это обязательное к прочтению пособие для всех, кто интересуется проблемами кибербезопасности, а также руководство о том, как не следует проектировать маршрутизатор. А ещё вы узнаете, что производителям делают строгий выговор о внедрении принципов безопасности с занесением в личное дело ФБР.

Итак, если вы ищете руководство по защите вашего маршрутизатора SOHO, то этот документ – идеальный вариант. Это своего рода практическое руководство, но для всего, что вам не следует делать



Обнаружение кибератак на интеллектуальные устройства с учётом потребляемой энергии

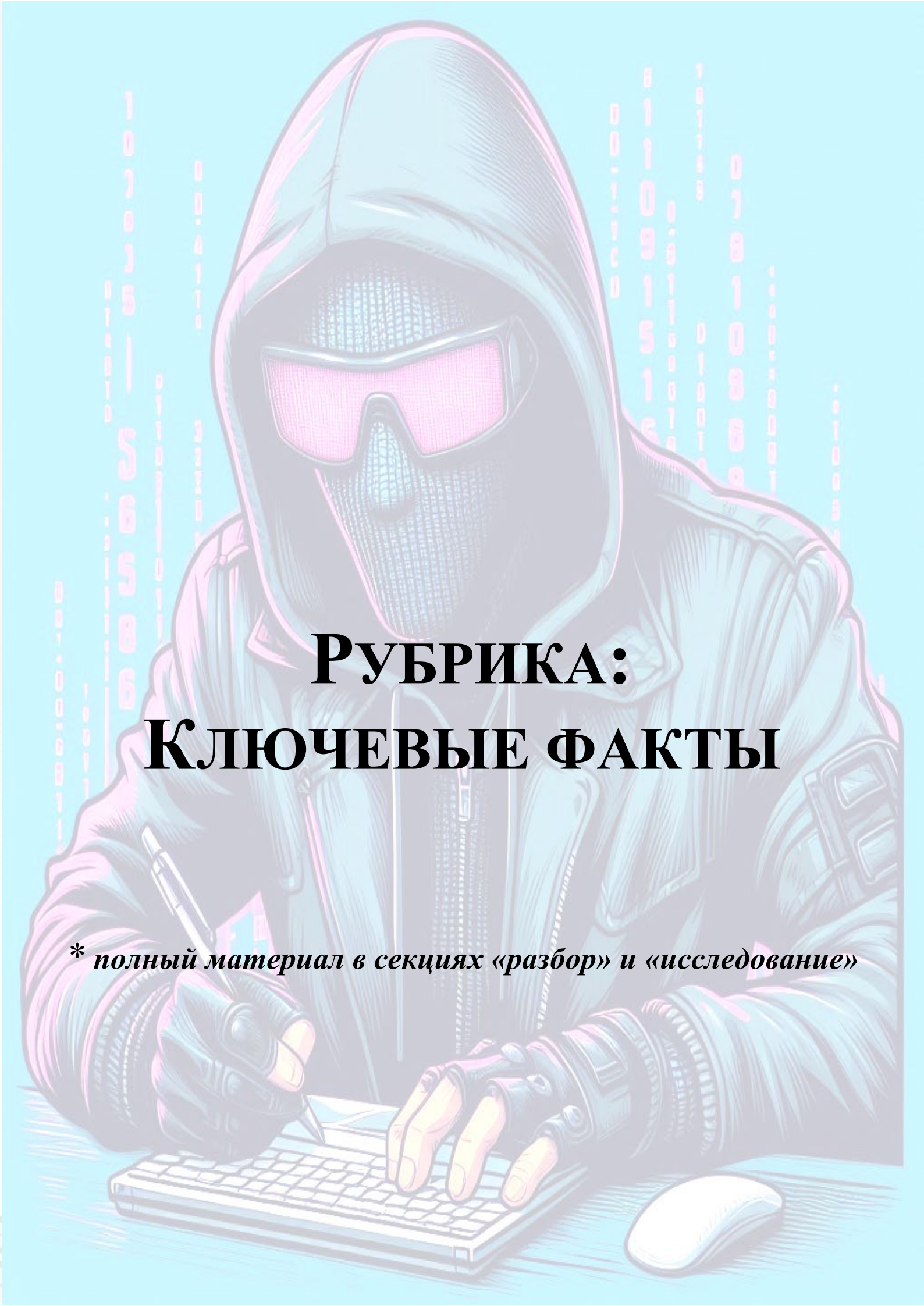
В мире, где умные устройства призваны облегчить нашу жизнь, научная статья "Обнаружение кибератак на интеллектуальные устройства с учётом потребляемой энергии" – это захватывающая история о том, как эти гаджеты могут быть использованы против нас. Представьте, что ваш "умный" холодильник планирует сократить ваши счета за электроэнергию, пока вы спите, или ваш термостат сговорился с вашим тостером совершить кибератаку. В этой статье героически предлагается простая система обнаружения, которая спасёт нас от этих опасных бытовых приборов, проанализировав их энергопотребление. Потому что, очевидно, лучший способ перехитрить интеллектуальное устройство — это следить за тем, сколько электроэнергии оно потребляет вас нет дома. Итак, в следующий раз, когда ваша интеллектуальная лампочка начнёт мигать, не волнуйтесь — это просто алгоритм (обнаружения атаки на ваш холодильник) выполняет свою работу.

MediHunt

Статья "MediHunt: A Network Forensics Framework for Medical IoT Devices" – это настоящий прорыв. Она начинается с рассмотрения насущной потребности в надёжной сетевой криминалистике в среде медицинского Интернета вещей (MIoT). Вы знаете, что среды, в которых используются сети передачи телеметрии с использованием MQTT (Message Queuing Telemetry Transport), являются любимыми для умных больниц из-за их облегчённого протокола связи.

MediHunt – это платформа автоматической сетевой криминалистики, предназначенная для обнаружения атак на сетевой трафик в сетях MQTT в режиме реального времени. Она использует модели машинного обучения для расширения возможностей обнаружения и подходит для развёртывания на устройствах MIoT с ограниченными ресурсами. Потому что, естественно, именно из-за этого мы все потеряли сон.

Эти аспекты – отличная почва для подробного обсуждения фреймворка, его экспериментальной установки и оценки. Вам уже не терпится погрузиться в эти захватывающие подробности?



Рубрика:
Ключевые факты

** полный материал в секциях «разбор» и «исследование»*

A. *AntiPhishStack*

В документе под названием "Модель многоуровневого обобщения на основе LSTM для оптимизации фишинга" обсуждается растущая зависимость от революционных онлайновых веб-сервисов, что привело к повышенным рискам безопасности и постоянным проблемам, создаваемым фишинговыми атаками.

Фишинг, вводящий в заблуждение метод социальной и технической инженерии, представляет серьёзную угрозу безопасности в Интернете, направленный на незаконное получение идентификационных данных пользователей, их личного счета и банковских учётных данных. Это основная проблема преступной деятельности, когда атакующие преследуют такие цели, как продажа украденных личных данных, извлечение наличных, использование уязвимостей или получение финансовой выгоды.

Исследование направлено на улучшение обнаружения фишинга с помощью AntiPhishStack, работающего без предварительного знания особенностей фишинга. Модель использует возможности сетей долгой краткосрочной памяти (LSTM), типа рекуррентной нейронной сети, которая способна изучать зависимость порядка в задачах прогнозирования последовательности. Он симметрично использует изучение URL-адресов и функций TF-IDF на уровне символов, повышая его способность бороться с возникающими фишинговыми угрозами.

1) *Методология и значимость исследования*

В документе представлена новая модель обнаружения фишинговых сайтов. Важность этого исследования заключается в совершенствовании методов обнаружения фишинга, в частности, за счёт внедрения обобщённой двухфазной стековой модели, названной AntiPhishStack.

Эта модель предназначена для обнаружения фишинговых сайтов, не требуя предварительного знания особенностей, специфичных для фишинга, что является значительным улучшением по сравнению с традиционными системами обнаружения, которые полагаются на машинное обучение и ручные функции.

Это исследование вносит вклад в продолжающийся дискурс о симметрии и асимметрии в информационной безопасности и предоставляет перспективное решение для повышения сетевой безопасности перед лицом развивающихся киберугроз.

Источник данных, использованный в исследовании, включает два контрольных набора, содержащих доброкачественные и фишинговые или вредоносные URL-адреса. Эти наборы данных используются для экспериментальной проверки модели. В документе наборы данных обозначены как DS1 и DS2, причём DS1 включает доброкачественные сайты Яндекса и фишинговые сайты PhishTank, а DS2 состоит из доброкачественных сайтов из common-crawl, базы данных Alexa и фишинговых сайтов из PhishTank.

2) *Ключевые компоненты*

Антифиш-стековая модель работает в два этапа (обобщённая модель двухфазного стека):

- **Этап I**: модель симметрично запоминает URL-адреса и функции TF-IDF на уровне символов. Эти функции обучаются на базовом классификаторе машинного обучения, использующем K-кратную перекрёстную проверку для надёжного прогнозирования среднего значения.
- **Этап II**: для динамической компиляции используется двухуровневая многоуровневая сеть LSTM с пятью адаптивными оптимизаторами, обеспечивающими превосходное прогнозирование этих функций.
- Кроме того, симметричные прогнозы на обоих этапах оптимизированы и интегрированы для обучения мета-классификатора XGBoost, что способствует получению окончательного надёжного прогноза.

3) *Преимущества и ограничения исследования*

Для сравнения, традиционные фишинговые системы, основанные на машинном обучении и ручных функциях, борются с эволюционирующими тактиками. Другие модели, такие как модель CNN-LSTM и архитектура сквозного глубокого обучения, основанная на методах обработки естественного языка, показали ограничения в их обобщении тестовых данных и их зависимости от существующих знаний об обнаружении фишинга. Модель AntiPhishStack, напротив, демонстрирует высокую способность к обобщению и независимость от предыдущих знаний функций, что делает её надёжным и эффективным инструментом для обнаружения фишинга.

Преимущества исследования по сравнению с традиционными фишинговыми системами включают:

- **Независимость от предварительного знания функций**: AntiPhishStack не требует предварительного знания функций, специфичных

для фишинга, что позволяет ему адаптироваться к новым и развивающимся тактикам более эффективно, чем традиционные системы, которые полагаются на предопределённые функции.

- **Независимость от экспертов по кибербезопасности и сторонних сервисов**: модель автономно извлекает необходимые функции URL, уменьшая зависимость от экспертов по кибербезопасности и сторонних сервисов, таких как рейтинг страницы или возраст домена, от которых могут зависеть традиционные системы.
- **Высокая точность**: Модель продемонстрировала исключительную производительность, достигнув заметной точности 96,04% для контрольных наборов данных, что является значительным улучшением по сравнению с традиционными системами.
- **Адаптивность к развивающимся угрозам**: Конструкция модели позволяет ей извлекать уроки из обрабатываемых данных, что потенциально делает её более адаптируемой к постоянно меняющимся тактикам, используемым атакующими, в отличие от традиционных систем, которые могут требовать обновления вручную для сохранения эффективности.

Ограничения исследования включают:

- **Применение в реальном мире**: в документе не обсуждается производительность модели в реальных сценариях, где фишинговые тактики постоянно развиваются.
- **Производительность на других наборах данных**: производительность модели была проверена на двух контрольных наборах данных, но неясно, как она будет работать на других наборах или в других контекстах.
- **Зависимость от функций**: зависимость модели от функций TF-IDF на уровне URL и символов может ограничить её способность обнаруживать попытки фишинга, использующие другие тактики.
- **Вычислительные ресурсы**: в документе не обсуждаются вычислительные ресурсы, необходимые для реализации модели, что может быть потенциальным ограничением для некоторых пользователей.

Предлагаемая модель имеет ряд ограничений с точки зрения масштабируемости и производительности.

- Во-первых, зависимость модели от сетей долгой краткосрочной памяти (LSTM) может привести к неэффективности вычислений. Сети LSTM известны своими высокими требованиями к вычислениям и памяти, что может ограничивать масштабируемость модели при работе с большими наборами данных или в приложениях реального времени.
- Во-вторых, двухэтапный подход модели, который включает в себя обучение функций в базовом классификаторе машинного обучения, а затем использование двухуровневой многоуровневой сети на основе LSTM, может потребовать много времени и вычислительных ресурсов. Это потенциально может ограничить производительность модели в сценариях обнаружения фишинга в реальном времени.
- Наконец, хотя модель предназначена для работы без предварительного знания специфических функций фишинга, это также может быть ограничением. Модели может быть сложно точно обнаруживать новые или изощренные попытки фишинга, которые используют функции, не учтённые при обучении.

B. АНБ в истерике. AdaptTactics

Документ под названием «cyber actors adapt tactics for initial cloud access», опубликованный Агентством национальной безопасности (АНБ) предупреждает, об адаптации тактики для получения первоначального доступа к облачным сервисам, а не для использования уязвимостей локальной сети.

Переход от локальных решений к облачным является ответом на то, что организации модернизируют свои системы и переходят на облачную инфраструктуру. Также кибер-кампании расширяются в сторону таких секторов, как авиация, образование, секторов, связанных региональными и федеральными, а также госучреждениями, правительственными финансовыми департаментами и военными организациями.

1) Ключевые выводы

- **Адаптация к облачным сервисам:** сместился фокус с эксплуатации уязвимостей локальной сети

на прямое воздействие на облачные сервисы. Это изменение является ответом на модернизацию систем и миграцию инфраструктуры в облако.

- **Аутентификация как ключевой шаг**: чтобы скомпрометировать облачные сети, необходимо успешно пройти аутентификацию у поставщика облачных услуг. Предотвращение этого первоначального доступа имеет решающее значение для предотвращения компрометации.
- **Расширение таргетинга:** расширена сфера воздействия на сектора, такие как, как авиация, образование, правоохранительные органы, региональные и федеральные организации, правительственные финансовые департаменты и военные организации. Это расширение указывает на стратегическую диверсификацию целей сбора разведывательной информации.
- **Использование служебных и неактивных учётных записей:** подчёркивается, что за последние 12 месяцев использовались брутфорс-атаки для доступа к служебным и неактивным учётным записям. Эта тактика позволяет получить первоначальный доступ к облачным средам.
- **Профессиональный уровень атакующих:** выявлена возможность осуществления компрометациии глобальной цепочки поставок, как, например, инцидент с SolarWinds в 2020 году.
- **Первая линия защиты:** подчёркивается, что первая линия защиты включает предотвращения возможности первичного доступа к сервисам.

2) *Детали TTP:*

- **Доступ к учётным данным / подбор пароля T1110**: используются password-spray и подбор паролей в качестве начальных векторов заражения. Подход предполагает попытку ввода нескольких паролей для разных учётных записей или многочисленные попытки для одной учётной записи для получения несанкционированного доступа.
- **Первоначальный доступ / T1078.004 Действительные учётные записи: Облачные учётные записи:** получение доступа к облачным сервисам, используя скомпрометированные учётные данные: как системные учётные записи (используемые для автоматизированных задач и служб), так и неактивные учётные записи, учётные которые все ещё остаются в системе.
- **Доступ к учётным данным / T1528 Кража токена доступа к приложению:** злоумышленники используют украденные токены доступа для входа в учётные записи без необходимости ввода паролей. Токены доступа — это цифровые ключи, которые позволяют получить доступ к учётным записям пользователей. Их получение позволяет обойти традиционные механизмы входа в систему.
- **Доступ к учётным данным / Формирование запроса многофакторной аутентификации T1621:** метод «бомбардировка MFA» предполагает, что злоумышленники неоднократно отправляют запросы MFA на устройство жертвы. Цель состоит в том, чтобы жертва приняла запрос и таким образом предоставила злоумышленнику доступ.
- **Командование и контроль / T1090.002 Прокси: Внешний прокси:** чтобы поддерживать «тайные операции и сливаться с обычным трафиком», используются открытые прокси, расположенные в частных диапазонах IP-адресов, т.к. вредоносные соединения сложнее отличить от легальной активности пользователей в журналах доступа.
- **Постоянство / T1098.005 Манипулирование учётными записями: Регистрация устройств:** после получения доступа к учётным записям предпринимаются попытки зарегистрировать свои собственные устройства в облачном клиенте. Успешная регистрация устройства может обеспечить постоянный доступ к облачной среде.

C. АНБ в истерике. Ubiquiti

Документ под названием “Cyber Actors Use Compromised Routers to Facilitate Cyber Operations”, опубликованный ФБР, АНБ, киберкомандованием США и международными партнёрами предупреждает об использовании скомпрометированных маршрутизаторов Ubiquiti EdgeRouters для облегчения вредоносных кибероперациий по всему миру.

Популярность Ubiquiti EdgeRouters объясняется удобной в использовании ОС на базе Linux, учётными данными по умолчанию и ограниченной защитой брандмауэром. Маршрутизаторы часто поставляются с

небезопасными конфигурациями по умолчанию и не обновляют прошивку автоматически.

Скомпрометированные EdgeRouters использовались APT28 для сбора учётных данных, дайджестов NTLMv2, сетевого трафика прокси-сервера и размещения целевых страниц для фишинга и пользовательских инструментов. APT28 получила доступ к маршрутизаторам, используя учётные данные по умолчанию, и троянизировала серверные процессы OpenSSH. Наличие root-доступ к скомпрометированным маршрутизаторам, дало доступ к ОС для установки инструментов и сокрытия своей личности.

APT28 также развернула пользовательские скрипты Python на скомпрометированных маршрутизаторах для сбора и проверки украденных данных учётной записи веб-почты, полученных с помощью межсайтовых скриптов и кампаний фишинга "браузер в браузере". Кроме того, они использовали критическую уязвимость с повышением привилегий на нулевой день в Microsoft Outlook (CVE-2023–23397) для сбора данных NTLMv2 из целевых учётных записей Outlook и общедоступные инструменты для оказания помощи в атаках с ретрансляцией NTLM

1) Ключевые моменты

- APT28 (известные как Fancy Bear, Forest Blizzard и Strontium) использовали скомпрометированные серверы Ubiquiti EdgeRouters для проведения вредоносных кибероперациий по всему миру.
- Эксплуатация включает сбор учётных данных, сбор дайджестов NTLMv2, проксирование сетевого трафика, а также размещение целевых страниц для фишинга и пользовательских инструментов.
- ФБР, АНБ, киберкомандование США и международные партнеры выпустили совместное консультативное заключение по кибербезопасности (CSA) с подробным описанием угрозы и рекомендациями по ее устранению.
- Рекомендации включают наблюдаемые тактики, методы и процедуры (TTP), индикаторы компрометации (IoC) для сопоставления с системой MITRE ATT&CK framework.
- В рекомендациях содержится настоятельный призыв к немедленным действиям по устранению угрозы, включая выполнение заводских настроек оборудования, обновление встроенного ПО, изменение учётных данных по умолчанию и внедрение стратегических правил брандмауэра.
- APT28 использует скомпрометированные EdgeRouters как минимум с 2022 года для содействия операциям против различных отраслей промышленности и стран, включая США.
- EdgeRouters популярны благодаря своей удобной операционной системе на базе Linux, но часто поставляются с учётными данными по умолчанию и ограниченной защитой брандмауэром.
- В рекомендациях содержатся подробные TTP и IOC, которые помогут сетевым защитникам идентифицировать угрозу и смягчить ее последствия.
- Рекомендация также включает информацию о том, как сопоставить вредоносную киберактивность с платформой MITRE ATT&CK framework.
- Организации, использующие Ubiquiti EdgeRouters, должны принять немедленные меры для защиты своих устройств от использования APT28.
- Рекомендуемые действия включают сброс оборудования к заводским настройкам, обновление до последней версии прошивки, изменение имен пользователей и паролей по умолчанию и внедрение стратегических правил брандмауэра.

D. АНБ в истерике. SOHO

Эксплуатация небезопасных маршрутизаторов SOHO злоумышленниками, особенно группами, спонсируемыми государством, представляет значительную угрозу для отдельных пользователей и критически важной инфраструктуры. Производителям настоятельно рекомендуется применять принципы security by-design, privacy-by-design и методы повышения прозрачности для снижения этих рисков, в то время как пользователям и безопасникам рекомендуется внедрять передовые методы обеспечения безопасности маршрутизаторов и сохранять бдительность в отношении потенциальных угроз.

1) Проблема небезопасных маршрутизаторов soho

- **Распространённые уязвимости**: Значительное количество уязвимостей, общее число которых составляет 226, было выявлено в популярных брендах маршрутизаторов SOHO. Эти уязвимости

различаются по степени серьёзности, но в совокупности представляют существенную угрозу.

- **Устаревшие компоненты**: Основные компоненты, такие как ядро Linux, и дополнительные службы, такие как VPN, в этих маршрутизаторах устарели. Это делает их восприимчивыми к известным эксплойтам уязвимостей, которые уже давно стали достоянием общественности.
- **Небезопасные настройки по умолчанию**: Многие маршрутизаторы поставляются с простыми паролями по умолчанию и отсутствием шифрования соединений, чем пользуются злоумышленники.
- **Отсутствие security-by-design**: Маршрутизаторам SOHO часто не хватает ряда функций безопасности, например возможностей автоматического обновления и отсутствия эксплуатируемых проблем, особенно в интерфейсах веб-управления.
- **Доступность интерфейсов управления**: Производители часто создают устройства с интерфейсами управления, с доступом через Интернет по умолчанию, часто без уведомления клиентов об этой небезопасной конфигурации.
- **Отсутствие прозрачности и подотчётности**: производители не обеспечивают прозрачность путём раскрытия уязвимостей продукта с помощью программы CVE и точной классификации этих уязвимостей с использованием CWE
- **Пренебрежение безопасностью в пользу удобства и функциональных возможностей**: Производители отдают предпочтение простоте использования и широкому спектру функций, а не безопасности, что приводит к созданию маршрутизаторов, которые "недостаточно безопасны" прямо из коробки, без учёта возможности эксплуатации.
- **Небрежность пользователей**: Многие пользователи, включая ИТ-специалистов, не соблюдают базовые правила безопасности, такие как смена паролей по умолчанию или обновление встроенного программного обеспечения, оставляя маршрутизаторы уязвимыми для атак.
- **Сложность идентификации уязвимых устройств**: Идентификация конкретных уязвимых устройств является сложной из-за юридических и технических проблем, усложняющих процесс их устранения.

2) *Сектора / Отрасли*

a) *Коммуникации*

- **Утечки данных и перехват данных**: небезопасные маршрутизаторы могут привести к несанкционированному доступу к сетевому трафику, позволяя злоумышленникам перехватывать конфиденциальные сообщения.
- **Нарушение работы служб**: скомпрометированные маршрутизаторы могут использоваться для запуска распределённых атак типа "Отказ в обслуживании" (DDoS), нарушающих работу служб связи.

b) *Транспорт и Логистика*

Уязвимость инфраструктуры: транспортный сектор в значительной степени полагается на сетевые системы для выполнения операций. Скомпрометированные маршрутизаторы могут позволить злоумышленникам нарушить работу систем управления трафиком и логистических операций.

c) *Водоснабжение*

Операционные технологии (OT): небезопасные маршрутизаторы предоставляют злоумышленникам шлюз для атак на системы OT в секторе водоснабжения, что потенциально влияет на системы очистки и распределения воды.

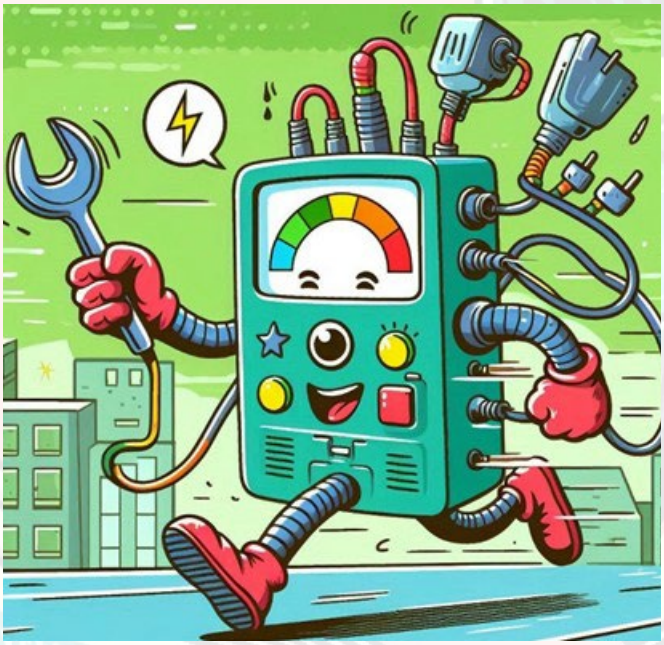
d) *Энергетика*

Сетевая безопасность: Энергетический сектор, особенно предприятия электроэнергетики, подвержены риску целенаправленных атак через небезопасные маршрутизаторы. Злоумышленники могли получить доступ к системам управления, создавая угрозу стабильности электросети.

e) *Другие отрасли*

- **Здравоохранение**: Небезопасные маршрутизаторы могут скомпрометировать данные пациентов и нарушить работу медицинских служб, предоставляя злоумышленникам доступ к сетям здравоохранения.
- **Розничная торговля и гостиничный бизнес**: Эти сектора уязвимы для утечки данных, связанных с информацией о клиентах и финансовыми транзакциями, из-за небезопасных сетевых устройств.
- **Промышленность**: Промышленные системы управления могут быть взломаны через небезопасные маршрутизаторы, что влияет на производственные линии и производственные процессы.
- **Образование**: Школы и университеты подвержены риску утечки данных и сбоев в предоставлении образовательных услуг.
- **Государственный и общественный сектор**: небезопасные маршрутизаторы могут привести к несанкционированному доступу к правительственным сетям, подвергая риску конфиденциальную информацию и критически важные услуги

E. Обнаружение кибератак на интеллектуальные устройства с учётом потребляемой энергии



В научной статье "Detection of Energy Consumption Cyber Attacks on Smart Devices" подчёркивается влияние интеграции технологии Интернета вещей в умные дома и связанные с этим проблемы безопасности.

- **Энергоэффективность**: подчёркивается важность энергоэффективности в системах Интернета вещей, особенно в средах "умного дома" для комфорта, уюта и безопасности.
- **Уязвимости**: уязвимость устройств Интернета вещей к кибератакам и физическим атакам из-за ограниченности их ресурсов подчёркивает необходимость защиты этих устройств для обеспечения их эффективного использования в реальных сценариях.
- **Предлагаемая система обнаружения**: Авторы предлагают систему обнаружения, основанную на анализе энергопотребления интеллектуальных устройств. Цель этой платформы – классифицировать состояние атак отслеживаемых устройств путём изучения структуры их энергопотребления.
- **Двухэтапный подход**: Методология предполагает двухэтапный подход. На первом этапе используется короткий промежуток времени для грубого обнаружения атаки, в то время как второй этап включает в себя более детальный анализ.
- **Облегчённый алгоритм**: представлен облегчённый алгоритм, который адаптирован к ограниченным ресурсам устройств Интернета вещей и учитывает протоколы: TCP, UDP и MQTT.
- **Анализ скорости приёма пакетов**: Метод обнаружения основан на анализе скорости приёма пакетов интеллектуальными устройствами для выявления аномального поведения, указывающего на атаки с использованием энергопотребления.

1) Преимущества

- **Облегчённый алгоритм обнаружения**: Предлагаемый алгоритм разработан таким образом, чтобы быть облегчённым, что делает его подходящим для устройств Интернета вещей с ограниченными ресурсами. Это гарантирует, что механизм обнаружения не будет нагружать устройства, которые он призван защищать.
- **Универсальность протокола**: Алгоритм учитывает множество протоколов связи (TCP, UDP, MQTT), что повышает его применимость к различным типам интеллектуальных устройств и конфигурациям сетей.
- **Двухэтапное обнаружение подход**: использование двухэтапного обнаружения подход позволяет повысить точность определения потребления энергии ударов при минимальном количестве ложных срабатываний. Этот метод позволяет как быстро провести первоначальное обнаружение, так и детальный анализ.
- **Оповещения в режиме реального времени**: Платформа оповещает администраторов об обнаружении атаки, обеспечивая быстрое реагирование и смягчение потенциальных угроз.
- **Эффективное обнаружение аномалий**: измеряя скорость приёма пакетов и анализируя структуру энергопотребления, алгоритм эффективно выявляет отклонения от нормального поведения, которые указывают на кибератаки.

2) Недостатки

- **Ограниченные сценарии атак**: Экспериментальная установка ориентирована только на определённые типы атак, что ограничивает возможность обобщения результатов на другие потенциальные векторы атак, не охваченные в исследовании.
- **Проблемы с масштабируемостью**: хотя алгоритм разработан таким образом, чтобы быть лёгким, его масштабируемость в более крупных и сложных средах "умного дома" с большим количеством устройств и различными условиями сети может потребовать дальнейшей проверки.
- **Зависимость от исходных данных**: Эффективность механизма обнаружения зависит от точных базовых измерений скорости приёма пакетов и энергопотребления. Любые изменения в нормальных условиях эксплуатации устройств могут повлиять на исходные данные, потенциально приводя к ложноположительным или отрицательным результатам.
- **Ограничения ресурсов**: несмотря на легковесность, алгоритм по-прежнему требует вычислительных ресурсов, что может стать проблемой для устройств с крайне ограниченными ресурсами. Постоянный мониторинг и анализ также могут повлиять на срок службы батареи и производительность этих устройств.

F. MediHunt

В документе "MediHunt: A Network Forensics Framework for Medical IoT Devices" рассматривается необходимость надёжной сетевой криминалистики в медицинских средах Интернета вещей (MIoT), особенно с упором на сети MQTT. Эти сети обычно используются в интеллектуальных больничных средах благодаря их облегчённому протоколу связи. Освещаются проблемы обеспечения безопасности устройств MIoT, которые часто ограничены в ресурсах и обладают ограниченной вычислительной мощностью. В качестве серьёзной проблемы упоминается отсутствие общедоступных потоковых наборов данных, специфичных для MQTT, для обучения систем обнаружения атак.

1) Преимущества

- **Обнаружение атак в режиме реального времени**: MediHunt предназначен для обнаружения атак на основе сетевого трафика в режиме реального времени для уменьшения потенциального ущерба и обеспечения безопасности сред MIoT.
- **Комплексные возможности криминалистики**: Платформа предоставляет комплексное решение для сбора данных, анализа, обнаружения атак, представления и сохранения доказательств. Это делает его надёжным инструментом сетевой криминалистики в средах MIoT.
- **Интеграция с машинным обучением**: Используя модели машинного обучения, MediHunt расширяет свои возможности обнаружения. Использование пользовательского набора данных, который включает данные о потоках как для атак уровня TCP/IP, так и для атак прикладного уровня, позволяет более точно и эффективно обнаруживать широкий спектр кибератак.
- **Высокая производительность**: решение показало высокую производительность, получив баллы F1 и точность обнаружения, превышающую 0,99 и указывает на то, что она обладает высокой надёжностью при обнаружении атак на сети MQTT.
- **Эффективность использования ресурсов**: несмотря на свои широкие возможности, MediHunt разработан с учётом экономии ресурсов, что делает его подходящим для развёртывания на устройствах MIoT с ограниченными ресурсами (raspberry Pi).

2) Недостатки

- **Ограничения набора данных**: хотя MediHunt использует пользовательский набор данных для обучения своих моделей машинного обучения, создание и обслуживание таких наборов данных может быть сложной задачей. Набор данных необходимо регулярно обновлять, чтобы охватывать новые и зарождающиеся сценарии атак.
- **Ограничения ресурсов**: хотя MediHunt разработан с учётом экономии ресурсов, ограничения, присущие устройствам MIoT, такие как ограниченная вычислительная мощность и память, все ещё могут создавать проблемы. Обеспечить бесперебойную работу фреймворка на этих устройствах без ущерба для их основных функций может быть непросто.
- **Сложность реализации**: Внедрение и поддержка платформы сетевой криминалистики на основе машинного обучения может быть сложной задачей. Это требует опыта в области кибербезопасности и машинного обучения, который может быть доступен не во всех медицинских учреждениях.
- **Зависимость от моделей машинного обучения**: Эффективность MediHunt в значительной степени зависит от точности и надёжности его моделей машинного обучения. Эти модели необходимо обучать на высококачественных данных и регулярно обновлять, чтобы они оставались эффективными против новых типов атак.
- **Проблемы с масштабируемостью**: хотя платформа подходит для небольших развёртываний на устройствах типа Raspberry Pi, ее масштабирование до более крупных и сложных сред MIoT может вызвать дополнительные проблемы. Обеспечение стабильной производительности и надёжности в более крупной сети устройств может быть затруднено

G. Fuxnet

Хакерская группа Blackjack, предположительно связанная с украинскими спецслужбами, взяла на себя ответственность за кибератаку, которая якобы поставила под угрозу возможности обнаружения чрезвычайных ситуаций и реагирования на них в прилегающих районах РФ. Группа была связана с предыдущими кибератаками, направленными против интернет-провайдеров и военной инфраструктуры. Их последнее заявление касается нападения на компанию, отвечающую за строительство и мониторинг инфраструктуры подземных вод, канализации и коммуникаций. Основные выводы из анализа Fuxnet, в т.ч. из материалов Team82 и Claroty:

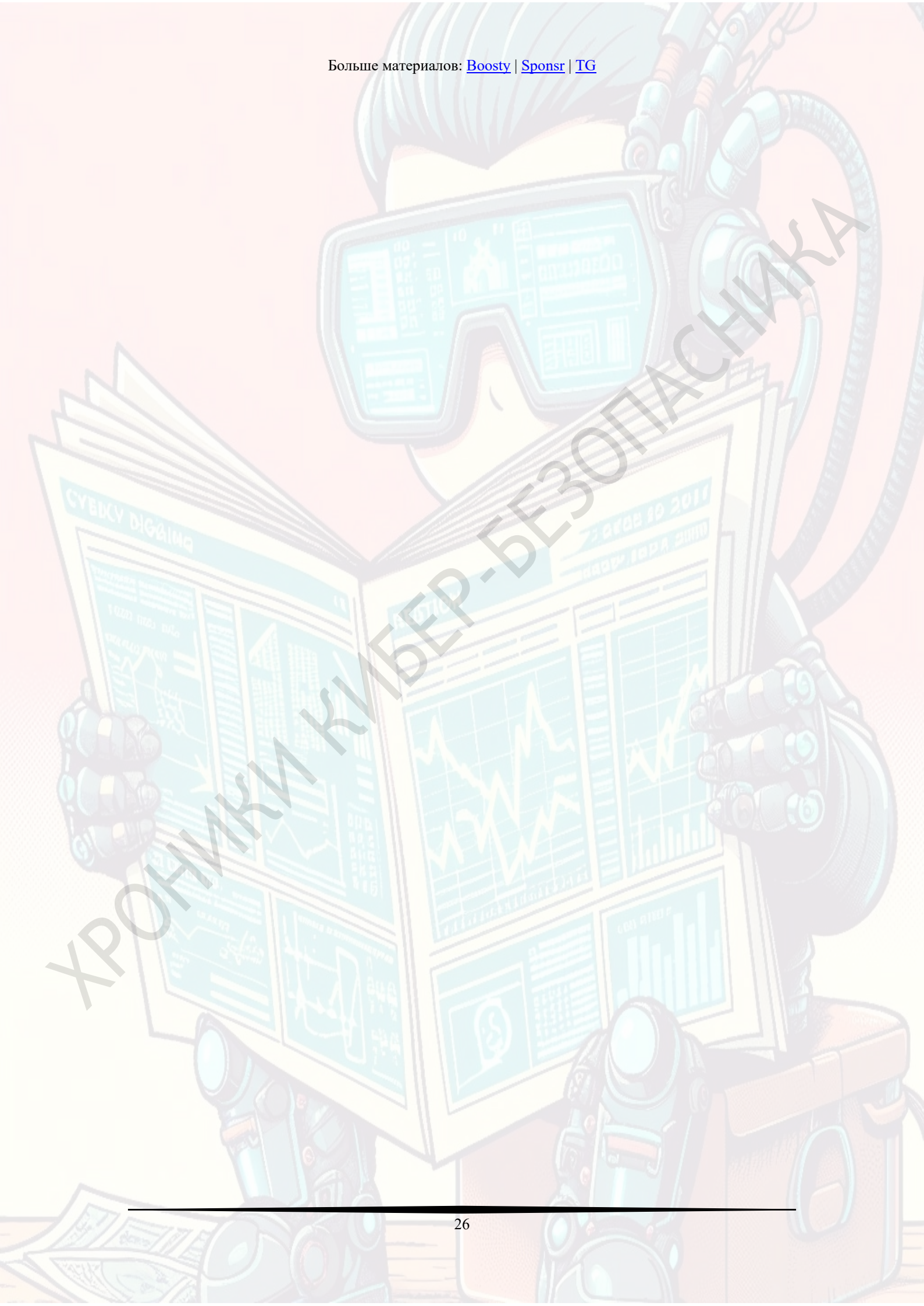
- **Неподтверждённые заявления**: Team82 и Claroty не смогли подтвердить заявления относительно влияния кибератаки на возможности правительства по реагированию на чрезвычайные ситуации или степени ущерба, причинённого Fuxnet.
- **Несоответствие в сообщениях о воздействии**: первоначальное утверждение о 2659 сенсорных шлюзов не совпали с информацией об атаке 1700. А проведённый Team82 анализ показывает, что только немногим более 500 были фактически затронуты Fuxnet. На это последовали заявление Blackjack об выведено из строя 87000 датчиков также было разъяснено, заявив, что они отключили датчики, «уничтожив шлюзы путём фаззинга», а не физическое уничтожение датчиков.
- **Фаззинг M-Bus**: метод был направлен на отключение датчиков, но точное количество датчиков оказалось невозможно установить ввиду их недоступности извне.
- **Отсутствие прямых доказательств**: отсутствуют прямые доказательства, подтверждающие масштабы ущерба или влияние на возможности обнаружения ЧС и реагирования на них.
- **Разъяснение от Blackjack**: после публикации первоначального анализа Team82 Blackjack обратилась с просьбой предоставить разъяснения, в частности, оспорив утверждение о том, что было затронуто только около 500 сенсорных шлюзов и обнародованные файлы JSON были лишь примером полного объёма их деятельности.

1) Возможные отрасли:

- **Коммунальные службы**: Основной целью Fuxnet был сектор коммунальных услуг, в частности сенсорные шлюзы, управляющие системами водоснабжения и канализации. Это может иметь последствия для предоставления этих основных услуг и мониторинга за ними.
- **Службы экстренной помощи**: Группа утверждала, о получении доступ к службе экстренной помощи 112, что могло повлиять на способность эффективно реагировать на чрезвычайные ситуации.
- **Транспорт**: Группа также утверждала, что вывела из строя датчики и контроллеры в критически важных объектах инфраструктуры, включая аэропорты и метро, что могло нарушить транспортное обслуживание и безопасность.
- **Энергетика**: В качестве ещё одной цели были упомянуты газопроводы, что указывает на потенциальный риск для систем распределения энергии и мониторинга.

2) Возможные последствия:

- **Нарушение работы служб**: Разрушение или неисправность сенсорных шлюзов может привести к нарушению работы систем мониторинга и управления коммунальными службами, что потенциально может привести к перебоям в обслуживании.
- **Нарушение безопасности**: В транспортном и энергетическом секторах потеря функциональности датчиков может представлять угрозу безопасности, поскольку эти датчики часто имеют решающее значение для обнаружения опасных условий.
- **Экономический эффект**: Потенциальные простои и затраты на ремонт, связанные с заменой или перепрошивкой повреждённых шлюзов датчиков, могут иметь значительные экономические последствия для затронутых отраслей.
- **Задержки с реагированием на чрезвычайные ситуации**: может привести к задержкам в реагировании на чрезвычайные ситуации, что повлияет на общественную безопасность.
- **Утечка данных**: возможная компрометация сетевые системы потенциально может привести к утечке данных и утечке конфиденциальной информации.
- **Потеря общественного доверия**: может привести к потере общественного доверия к сервисам и организациям, ответственным за их безопасность.



Рубрика:
Разбор

AntiPhishStack

Аннотация – Анализ документа "AntiPhishStack: модель многоуровневого обобщения на основе LSTM для оптимизированного обнаружения фишинговых URL", будет охватывать различные аспекты, включая методологию, результаты и последствия для кибербезопасности. В частности, будет рассмотрен подход документа к использованию сетей с долгой краткосрочной памятью (LSTM) в рамках многоуровневой структуры обобщения для обнаружения фишинговых URL-адресов. Будет изучена эффективность модели, стратегии её оптимизации и её производительность по сравнению с существующими методами.

В ходе анализа также будут рассмотрены практические применения модели, способы её интеграции в существующие меры кибербезопасности и её потенциальное влияние на сокращение числа фишинговых атак. Подчёркнута актуальность документа для специалистов по кибербезопасности, ИТ-специалистов и заинтересованных сторон в различных отраслях, а также важность передовых методов обнаружения фишинга в современном цифровом ландшафте.

Это изложение послужит ценным ресурсом для экспертов по кибербезопасности, ИТ-специалистов и других лиц, интересующихся последними разработками в области обнаружения и предотвращения фишинга.

A. Введение

В документе под названием "Модель многоуровневого обобщения на основе LSTM для оптимизации фишинга" обсуждается растущая зависимость от революционных онлайновых веб-сервисов, что привело к повышенным рискам безопасности и постоянным проблемам, создаваемым фишинговыми атаками.

Фишинг, вводящий в заблуждение метод социальной и технической инженерии, представляет серьёзную угрозу безопасности в Интернете, направленный на незаконное получение идентификационных данных пользователей, их личного счета и банковских учётных данных. Это основная проблема преступной деятельности, когда атакующие преследуют такие цели, как продажа украденных личных данных, извлечение наличных, использование уязвимостей или получение финансовой выгоды.

Исследование направлено на улучшение обнаружения фишинга с помощью AntiPhishStack, работающего без предварительного знания особенностей фишинга. Модель использует возможности сетей долгой краткосрочной памяти (LSTM), типа рекуррентной нейронной сети, которая способна изучать зависимость порядка в задачах прогнозирования последовательности. Он симметрично использует изучение URL-адресов и функций TF-IDF на уровне символов, повышая его способность бороться с возникающими фишинговыми угрозами.

B. Методология и значимость исследования

В документе представлена новая модель обнаружения фишинговых сайтов. Важность этого исследования заключается в совершенствовании методов обнаружения фишинга, в частности, за счёт внедрения обобщённой двухфазной стековой модели, названной AntiPhishStack.

Эта модель предназначена для обнаружения фишинговых сайтов, не требуя предварительного знания особенностей, специфичных для фишинга, что является значительным улучшением по сравнению с традиционными системами обнаружения, которые полагаются на машинное обучение и ручные функции.

Это исследование вносит вклад в продолжающийся дискурс о симметрии и асимметрии в информационной безопасности и предоставляет перспективное решение для повышения сетевой безопасности перед лицом развивающихся киберугроз.

Источник данных, использованный в исследовании, включает два контрольных набора, содержащих доброкачественные и фишинговые или вредоносные URL-адреса. Эти наборы данных используются для экспериментальной проверки модели. В документе наборы данных обозначены как DS1 и DS2, причём DS1 включает доброкачественные сайты Яндекса и фишинговые сайты PhishTank, а DS2 состоит из доброкачественных сайтов из common-crawl, базы данных Alexa и фишинговых сайтов из PhishTank.

C. Ключевые компоненты

Антифиш-стековая модель работает в два этапа (обобщённая модель двухфазного стека):

- **Этап I**: модель симметрично запоминает URL-адреса и функции TF-IDF на уровне символов. Эти функции обучаются на базовом классификаторе машинного обучения, использующем K-кратную перекрёстную проверку для надёжного прогнозирования среднего значения.
- **Этап II**: для динамической компиляции используется двухуровневая многоуровневая сеть LSTM с пятью адаптивными оптимизаторами,

обеспечивающими превосходное прогнозирование этих функций.

- Кроме того, симметричные прогнозы на обоих этапах оптимизированы и интегрированы для обучения мета-классификатора XGBoost, что способствует получению окончательного надёжного прогноза.

1) URL-особенности

- **Структура URL-адресов**: в документе подчёркивается, что злоумышленники часто создают фишинговые URL-адреса, которые кажутся пользователям законными. Они используют тактику блокирования URL-адресов, чтобы обманом заставить пользователей раскрыть личную информацию.
- **Легкие функции**: исследование направлено на обнаружение фишинговых веб-сайтов с использованием облегчённых функций, в частности системы маркеров URL с весовым коэффициентом, которые позволяют быстро обнаруживать их без доступа к содержимому веб-сайта.
- **Вычисление веса**: приводится формула для вычисления весаt W_i for i-th d неопределённого слова в URL-адресе, которая используется для присвоения значения веса каждому URL-адресу для прогнозирования фишинга.
- **Компоненты URL**: описываются компоненты URL-адреса, включая протокол, IP-адрес хоста или местоположение ресурса, основные домены, домены верхнего уровня (TLD), номер порта, путь и необязательные поля, такие как запрос.
- **Индикаторы фишинга**: несколько дополнительных признаков идентифицируются как индикаторы фишинга, такие как использование IP-адреса вместо доменного имени, наличие символа "@", символа "//", префиксов и суффиксов доменных имён, разделённых знаком "-", и использование нескольких поддоменов.
- **HTTPS и возраст сертификата**: отмечается, что большинство законных сайтов используют HTTPS, и возраст сертификата имеет решающее значение. Требуется сертификат, заслуживающий доверия.
- **Favicon**: favicon может использоваться для перенаправления клиентов на сомнительные сайты, когда он находится во внешнем пространстве.
- **Анализ вспомогательных функций**: в документе представлен анализ вспомогательных функций, таких как IP-адрес, символ "@", символ "//", префиксы и суффиксы доменных имён, HTTPS и значок, объясняющий, как эти функции можно использовать для идентификации фишинговых веб-сайтов

2) Символьные особенности

- **TF-IDF**: используется термин, обратный частоте документа (TF-IDF) на уровне символов, чтобы определить относительную важность символов в URL-адресах по всему корпусу анализируемых URL-адресов.
- **Расчёт TF-IDF**: оценка TF-IDF состоит из двух частей: частоты использования термина (TF), которая представляет собой нормированное количество терминов в документе, и обратной частоты использования документа (IDF), которая состоит из логарифмов отношения общего количества документов к количеству документов, содержащих термин.
- **Уровни TF-IDF**: упоминается, что векторы TF-IDF могут генерироваться на разных уровнях, таких как уровень слова, уровень символа и уровень n-граммы, причём уровень символа особенно важен для данного исследования.
- **Ограничения TF-IDF**: хотя TF-IDF полезен для извлечения важных ключевых слов, у него есть ограничения, такие как невозможность извлечения терминов с орфографическими ошибками, что может быть проблематичным, поскольку URL-адреса могут содержать бессмысленные слова.
- **Символьный TF-IDF**: чтобы устранить ограничения TF-IDF для URL-адресов, которые могут содержать орфографические ошибки или бессмысленные слова, в исследовании используется подход TF-IDF на уровне символов с максимальным количеством функций 5000.
- **Естественное изучение функций**: модель обрабатывает строки URL как последовательности символов, которые считаются естественными функциями, не требующими предварительного знания функций для эффективного изучения моделью.
- **Обобщение стека для извлечения объектов**: модель использует обобщение стека для извлечения локальных объектов URL из последовательностей символов, а для окончательного прогнозирования разработан метаклассификатор.
- **Преимущества подхода**: подход позволяет предлагаемой модели обучаться на последовательностях символов URL как естественных признаках, что упрощает процесс обучения и потенциально улучшает способность модели обнаруживать фишинговые URL-адреса без предварительного знания особенностей

3) Модель обобщения стека

- **Двухфазный подход**: модель разделена на две фазы. На этапе I используются классификаторы машинного обучения для генерации среднего прогноза, в то время как на этапе II используется двухуровневая стековая обобщённая модель на основе LSTM, оптимизированная для наилучшего

прогнозирования при обнаружении фишинговых сайтов.

- **Интеграция прогнозов**: средний прогноз из фазы I объединяется с основным прогнозом из фазы II. Затем для получения окончательного прогноза используется метаклассификатор, в частности XGBoost.
- **Метод обобщения стека**: в модели используется обобщение стека, методология коллективного обучения, которая объединяет различные алгоритмы машинного обучения и модели глубокого обучения для повышения эффективности обнаружения.
- **Model Flow**: включает в себя сбор наборов данных, разделение их на обучающие и тестовые наборы, построение этапов модели обобщения стека и объединение прогнозов для получения окончательного.
- **Важность функции**: модель подчёркивает важность функций TF-IDF на уровне URL и символов, которые используются симметрично для обнаружения фишинговых веб-страниц.
- **Существенные преимущества**: модель обладает рядом преимуществ, включая независимость от предварительного знания функций, высокую способность к обобщению и независимость от экспертов по кибербезопасности и сторонних сервисов.
- **Улучшенное обнаружение фишинга**: модель предназначена для интеллектуального выявления новых фишинговых URL-адресов, ранее не идентифицированных как мошеннические, демонстрируя надёжную работу на контрольных наборах данных.

4) Эксперименты

Представлена экспериментальная проверка предложенной модели. Она была протестирована на двух контрольных наборах данных, которые включали доброкачественные и фишинговые или вредоносные URL-адреса.

- Модель продемонстрировала исключительную производительность при обнаружении фишинговых сайтов, достигнув точности 96,04%. Этот результат был заметно выше по сравнению с существующими исследованиями.
- Модель оценивалась с помощью различных матриц, включая кривую AUC-ROC, точность, отзыв, F1, среднюю абсолютную ошибку (MAE), среднеквадратичную ошибку (MSE) и точность.
- Сравнительный анализ с базовыми моделями и традиционными алгоритмами машинного обучения, такими как метод опорных векторов, дерево решений, наивный байесовский алгоритм, логистическая регрессия, метод K-ближайших соседей и последовательная минимальная оптимизация, выявил превосходную эффективность обнаружения фишинга в модели.
- Было установлено, что эта модель эффективна при выявлении новых фишинговых URL-адресов, которые ранее не были идентифицированы как мошеннические.
- Модель работает без предварительного знания особенностей фишинга, что является значительным преимуществом в достижении прогресса в области кибербезопасности

5) Оценка оптимизатора в LSTM

- **Производительность оптимизатора**: в статье оценивается производительность пяти различных адаптивных оптимизаторов: AdaDelta, Adam, RMSProp, AdaGard и SGD (Stochastic Gradient Descent), чтобы определить, какой из них лучше всего подходит для предлагаемой модели защиты от фишинга.
- **Эпохи и скорость обучения**: для реализации двухуровневого LSTM с разными оптимизаторами рассматривается разное количество эпох. Скорость обучения, важнейший параметр, настраивается для каждого оптимизатора, для контроля модели.
- **Точность, MSE и MAE**: в документе указаны точность, среднеквадратичная ошибка (MSE) и средняя абсолютная ошибка (MAE) для каждого оптимизатора с использованием модели обобщения стека на основе LSTM на двух наборах данных (DS1 и DS2).
- **Результаты для наборов данных**: оптимизатор AdaGard обеспечил высочайшую точность при минимальных значениях MSE и MAE в DS1, в то время как оптимизатор Adam достиг наивысшей точности в DS2.
- **Кривые точного воспроизведения**: кривые точного воспроизведения представлены для каждого набора функций, указывая на компромисс между точностью и повторным воспроизведением для различных оптимизаторов.
- **Выбор оптимизатора**: анализ показывает, что скорость обучения в значительной степени способствует успеху предлагаемой модели с адаптивными оптимизаторами. Оптимизатор Adam выделяется своей производительностью с определённой скоростью обучения при использовании двухуровневого LSTM со 100 эпохами.
- **Сравнительный анализ**: сравнивается средняя производительность оптимизаторов на DS1 и DS2, при этом DS2 показывает несколько лучшую точность.
- **Значимость оптимизаторов**: оценка оптимизаторов имеет решающее значение для

точности модели, которая является ключевым компонентом машинного обучения и искусственного интеллекта, отвечающим за формирование модели для получения наиболее точных результатов из возможных

D. Ключевые выводы

Конструкция модели позволяет эффективно идентифицировать новые фишинговые URL-адреса, ранее не идентифицированные как мошеннические, тем самым снижая вероятность ложноотрицательных результатов. Использование K-кратной перекрёстной проверки и двухуровневой сети LSTM помогает предотвратить переоснащение и улучшить способность модели правильно классифицировать фишинговые сайты, тем самым снижая вероятность ложных срабатываний.

- **Разработка модели**: новый режим, внедрённый с помощью обобщённой модели двухфазного стека, предназначенной для эффективного обнаружения фишинговых сайтов.
- **Симметричное изучение URL-адресов и функций TF-IDF на уровне символов**: в модели симметричное изучение URL-адресов и функций TF-IDF на уровне символов. Это повышает способность модели бороться с возникающими фишинговыми угрозами.
- **Двухфазная работа**: на этапе I функции обучаются на базовом классификаторе машинного обучения с использованием K-кратной перекрёстной проверки для надёжного прогнозирования среднего значения. На этапе II используется двухуровневая многоуровневая сеть LSTM с пятью адаптивными оптимизаторами для динамической компиляции, обеспечивающими превосходное прогнозирование этих функций.
- **Интеграция прогнозов (Мета-классификатор XGBoost)**: симметричные прогнозы на обоих этапах оптимизированы и интегрированы для обучения мета-классификатора XGBoost, что способствует получению окончательного надёжного прогноза.
- **Независимость от предварительного знания функций, специфичных для фишинга**: модель работает без предварительного знания функций, специфичных для фишинга, что является значительным достижением в его обнаружении, которое демонстрирует сильную способность к обобщению и независимость от экспертов по кибербезопасности и сторонних сервисов.
- **Высокая производительность**: проверка (экспериментальная) на двух контрольных наборах данных, включающих «доброкачественные» и фишинговые или вредоносные URL-адреса, демонстрирует производительность модели, достигая заметной точности 96,04% по сравнению с существующими исследованиями
- **Независимость от экспертов по кибербезопасности и сторонних сервисов:** модель самостоятельно извлекает необходимые функции URL, устраняя зависимость от экспертов по кибербезопасности. Она также демонстрирует независимость от функций сторонних производителей, таких как рейтинг страницы или возраст домена
- **Независимость от предварительного знания функций**: подход, использованный в этой работе, рассматривает строки URL как последовательности символов, выступающие в качестве естественных функций, которые не требуют предварительного знания для эффективного изучения предлагаемой моделью
- **Повышение сетевой безопасности**: исследование добавляет ценности продолжающемуся обсуждению симметрии и асимметрии в информационной безопасности и предлагает перспективное решение для повышения сетевой безопасности перед лицом развивающихся киберугроз.

E. Преимущества и ограничения исследования

Для сравнения, традиционные фишинговые системы, основанные на машинном обучении и ручных функциях, борются с эволюционирующими тактиками. Другие модели, такие как модель CNN-LSTM и архитектура сквозного глубокого обучения, основанная на методах обработки естественного языка, показали ограничения в их обобщении тестовых данных и их зависимости от существующих знаний об обнаружении фишинга. Модель AntiPhishStack, напротив, демонстрирует высокую способность к обобщению и независимость от предыдущих знаний функций, что делает её надёжным и эффективным инструментом для обнаружения фишинга.

Преимущества исследования по сравнению с традиционными фишинговыми системами включают:

- **Независимость от предварительного знания функций**: AntiPhishStack не требует предварительного знания функций, специфичных для фишинга, что позволяет ему адаптироваться к новым и развивающимся тактикам более эффективно, чем традиционные системы, которые полагаются на предопределённые функции.
- **Независимость от экспертов по кибербезопасности и сторонних сервисов**: модель автономно извлекает необходимые функции URL, уменьшая зависимость от экспертов по кибербезопасности и сторонних сервисов, таких как рейтинг страницы или возраст домена, от которых могут зависеть традиционные системы.
- **Высокая точность**: Модель продемонстрировала исключительную производительность, достигнув заметной точности 96,04% для контрольных наборов данных, что является значительным

улучшением по сравнению с традиционными системами.

- **Адаптивность к развивающимся угрозам**: Конструкция модели позволяет ей извлекать уроки из обрабатываемых данных, что потенциально делает её более адаптируемой к постоянно меняющимся тактикам, используемым атакующими, в отличие от традиционных систем, которые могут требовать обновления вручную для сохранения эффективности.

Ограничения исследования включают:

- **Применение в реальном мире**: в документе не обсуждается производительность модели в реальных сценариях, где фишинговые тактики постоянно развиваются.
- **Производительность на других наборах данных**: производительность модели была проверена на двух контрольных наборах данных, но неясно, как она будет работать на других наборах или в других контекстах.
- **Зависимость от функций**: зависимость модели от функций TF-IDF на уровне URL и символов может ограничить её способность обнаруживать попытки фишинга, использующие другие тактики.
- **Вычислительные ресурсы**: в документе не обсуждаются вычислительные ресурсы, необходимые для реализации модели, что может быть потенциальным ограничением для некоторых пользователей.

Предлагаемая модель имеет ряд ограничений с точки зрения масштабируемости и производительности.

- Во-первых, зависимость модели от сетей долгой краткосрочной памяти (LSTM) может привести к неэффективности вычислений. Сети LSTM известны своими высокими требованиями к вычислениям и памяти, что может ограничивать масштабируемость модели при работе с большими наборами данных или в приложениях реального времени.
- Во-вторых, двухэтапный подход модели, который включает в себя обучение функций в базовом классификаторе машинного обучения, а затем использование двухуровневой многоуровневой сети на основе LSTM, может потребовать много времени и вычислительных ресурсов. Это потенциально может ограничить производительность модели в сценариях обнаружения фишинга в реальном времени.
- Наконец, хотя модель предназначена для работы без предварительного знания специфических функций фишинга, это также может быть ограничением. Модели может быть сложно точно обнаруживать новые или изощренные попытки фишинга, которые используют функции, не учтённые при обучении.

F. Значение для будущих исследований

- **Обобщение модели**: способность модели работать без предварительного знания особенностей фишинга предполагает, что будущие исследования могут быть направлены на разработку более обобщённых моделей, которые могут адаптироваться к различным типам киберугроз без обширной переподготовки.
- **Методы глубокого обучения**: успех модели на основе LSTM указывает на то, что методы глубокого обучения обладают значительным потенциалом в приложениях кибербезопасности. Будущие исследования могли бы дополнительно изучить интеграцию различных архитектур нейронных сетей и их эффективность в обнаружении угроз.
- **Извлечение признаков**: использование функций TF-IDF на уровне символов и анализа URL-адресов в модели демонстрирует важность извлечения признаков для обнаружения фишинга. Исследования могли бы быть сосредоточены на выявлении новых признаков и методов извлечения для повышения уровня обнаружения.
- **Стековое обобщение**: двухфазный подход, используемый в модели, которая объединяет классификаторы машинного обучения и сети LSTM, демонстрирует преимущества многоуровневого обобщения. В будущих исследованиях можно было бы изучить другие комбинации алгоритмов и моделей для повышения эффективности прогнозирования.
- **Эталонные наборы данных**: использование эталонных наборов данных для проверки модели подчёркивает необходимость всеобъемлющих и актуальных наборов данных в исследованиях кибербезопасности. Будущая работа может включать создание и поддержание наборов данных, отражающих последние тенденции в области угроз.

G. Основной вклад в кибербезопасность

- **Независимость от предварительного знания функций**: способность модели извлекать информацию из строк URL в виде последовательностей символов без необходимости предварительного знания функций упрощает процесс обнаружения и делает его более адаптируемым к новым и неизвестным фишинговым атакам.
- **Высокая способность к обобщению**: использование в модели функций на основе символов URL для надёжного обобщения и точности проверки в сочетании с интеграцией многоуровневых функций в нейронной сети повышает её эффективность при обобщении различных фишинговых угроз.
- **Независимость от экспертов по кибербезопасности и сторонних сервисов**:

благодаря автономному извлечению необходимых функций, URL модель снижает зависимость от экспертов по кибербезопасности и сторонних сервисов, что делает её самодостаточным инструментом для обнаружения фишинга.

- **Повышенная точность обнаружения**: экспериментальная проверка модели на контрольных наборах данных продемонстрировала исключительную производительность с заметной точностью 96,04%, что выше, чем в существующих исследованиях.
- **Вклад в симметрию в информационной безопасности**: исследование дополняет дискурс о симметрии и асимметрии в информационной безопасности, предоставляя модель, которая может симметрично изучать и обнаруживать фишинговые URL-адреса, тем самым повышая безопасность сети от возникающих киберугроз.

H. Предполагаемые направления будущих исследований

- **Улучшение способности к обобщению**: модель обладает сильной способностью к обобщению, используя функции на основе символов URL для надёжного обобщения и точности проверки. Будущие исследования могли бы быть сосредоточены на дальнейшем повышении этой способности, особенно в контексте развития тактики и методов фишинга.
- **Повышение независимости от экспертов по кибербезопасности и сторонних сервисов**: модель автономно извлекает необходимые функции URL, устраняя зависимость от экспертов по кибербезопасности и сторонних сервисов. В будущих исследованиях можно было бы изучить способы дальнейшего повышения этой независимости, возможно, за счёт разработки более сложных методов выделения признаков.
- **Оптимизация модели многоуровневого обобщения**: используется двухфазная модель многоуровневого обобщения, при этом на первом этапе генерируется прогноз среднего значения, а на втором этапе используется двухуровневая обобщённая модель стека на основе LSTM, оптимизированная для наилучшего прогнозирования при обнаружении фишинговых сайтов. Будущие исследования могли бы быть сосредоточены на оптимизации этой модели, возможно, с помощью различных алгоритмов или методов машинного обучения.
- **Повышение точности**: хотя модель продемонстрировала высокую точность обнаружения фишинговых сайтов, будущие исследования могут быть сосредоточены на способах дальнейшего повышения этой точности, особенно в контексте атак нулевого дня и других передовых методов фишинга.
- **Распространение модели на другие приложения кибербезопасности**: модель потенциально может быть адаптирована для других приложений кибербезопасности, помимо обнаружения фишинга.

АНБ в истерике. AdaptTactics

Аннотация. В документе представлен всесторонний анализ публикации, в которой подробно описаны известные тактики, методы и процедуры (TTP), используемые кибер-профессионалами для получения первоначального доступа к облачным системам. Анализ охватывает различные аспекты, включая выявление и использование уязвимостей, различные методы использования облачных технологий, развёртывание специального вредоносного ПО.

Представлены ключевые моменты и полезная информация, которую могут использовать ИБ и ИТ специалисты и специалисты в различных отраслях для улучшения своих защитных стратегий, против спонсируемых государством киберугроз. Понимая адаптированную тактику субъекта для первоначального доступа к облаку, заинтересованные стороны могут лучше предвидеть и снижать потенциальные риски для своей облачной инфраструктуры, тем самым укрепляя свою общую безопасность.

A. Введение

Документ под названием «cyber actors adapt tactics for initial cloud access», опубликованный Агентством национальной безопасности (АНБ) предупреждает, об адаптации тактики для получения первоначального доступа к облачным сервисам, а не для использования уязвимостей локальной сети.

Переход от локальных решений к облачным является ответом на то, что организации модернизируют свои системы и переходят на облачную инфраструктуру. Также кибер-кампании расширяются в сторону таких секторов, как авиация, образование, секторов, связанных региональными и федеральными, а также госучреждениями, правительственными финансовыми департаментами и военными организациями.

Реальность такова, что для взлома облачных сетей нужно только пройти аутентификацию у поставщика облачных услуг, и в случае успеха, защита будет преодолена. Другими словами, «неожиданный» аспект облачных сред: меньшая уязвимость сети по сравнению с локальными системами парадоксальным образом делает преодоление первоначального доступа наиболее эффективным.

За последний год наблюдаемые TTPs были простыми, и вместе с тем эффективными так как использовались служебные и бездействующие учётные записи. В целом публикация вызывает прохладное утешение, предполагая, что прочная основа основ безопасности всего лишь гонка на опережение специалистов по безопасности с атакующими.

B. Ключевые выводы

- **Адаптация к облачным сервисам:** сместился фокус с эксплуатации уязвимостей локальной сети на прямое воздействие на облачные сервисы. Это изменение является ответом на модернизацию систем и миграцию инфраструктуры в облако.
- **Аутентификация как ключевой шаг**: чтобы скомпрометировать облачные сети, необходимо успешно пройти аутентификацию у поставщика облачных услуг. Предотвращение этого первоначального доступа имеет решающее значение для предотвращения компрометации.
- **Расширение таргетинга:** расширена сфера воздействия на сектора, такие как, как авиация, образование, правоохранительные органы, региональные и федеральные организации, правительственные финансовые департаменты и военные организации. Это расширение указывает на стратегическую диверсификацию целей сбора разведывательной информации.
- **Использование служебных и неактивных учётных записей:** подчёркивается, что за последние 12 месяцев использовались брутфорс-атаки для доступа к служебным и неактивным учётным записям. Эта тактика позволяет получить первоначальный доступ к облачным средам.
- **Профессиональный уровень атакующих:** выявлена возможность осуществления компрометациии глобальной цепочки поставок, как, например, инцидент с SolarWinds в 2020 году.
- **Первая линия защиты:** подчёркивается, что первая линия защиты включает предотвращения возможности первичного доступа к сервисам.

C. Адаптация к облачным сервисам

Адаптация атак к облачным сервисам знаменует собой эволюцию в сфере кибершпионажа и кибервойны и представляет собой более глубокую стратегическую адаптацию к меняющейся технологической среде и растущей зависимости правительств и корпораций от облачной инфраструктуры. Переход организаций к облачным сервисам обусловлен преимуществами масштабируемости, экономической эффективности и возможности быстрого развёртывания и обновления

сервисов. Однако этот переход также создаёт новые уязвимости и проблемы для кибербезопасности.

1) Стратегический переход к облаку

По мере того, как организации модернизировали свои системы и переходили на облачную инфраструктуру, участники адаптировали свои тактики, методы и процедуры (TTP) к новой среде. Эта адаптация обусловлена осознанием того, что облачные сервисы, централизуя огромные объёмы данных и ресурсов, представляют собой выгодную цель для шпионажа и сбора разведывательной информации. Облачная архитектура, предлагая организациям многочисленные преимущества, также требует переоценки стратегий безопасности для устранения уникальных уязвимостей.

2) Тактика, методы и процедуры (TTP)

Адаптация участников к облачным сервисам включает в себя ряд сложных TTP, предназначенных для использования конкретных характеристик облачных сред. Один из основных методов получения первоначального доступа к облачным сетям включает аутентификацию у поставщика облачных услуг, что достигается различными способами, включая подбор пароля и password-spray для доступа к служебным и неактивным учётным записям. Эти учётные записи, часто используемые для запуска приложений и управления ими без прямого контроля со стороны человека, особенно уязвимы, поскольку они могут быть не защищены многофакторной аутентификацией (MFA) и обладать высокими уровнями привилегий.

Кроме того, было замечено, что использование для аутентификации выданных системой токенов позволяет убрать необходимость в паролях. Дополнительно использовался процесс регистрации новых устройств в облаке с обходом механизмов безопасности MFA, в частности, с помощью таких методов, как «бомбардировка MFA», с целью случайного одобрения пользователем одного из этих запросов как легитимного. Кроме того, использование резидентных прокси-серверов для сокрытия своего присутствия в Интернете и затруднения обнаружения вредоносной деятельности представляет собой ещё один уровень профессионального подхода.

3) Последствия

Адаптация участников к целевым облачным сервисам имеет серьёзные последствия для кибербезопасности. Это подчёркивает необходимость внедрения надёжных мер безопасности, адаптированных к облачной среде. Сюда входит применение политик надёжных паролей, внедрение MFA, управление и мониторинг служебных и неактивных учётных записей, а также настройка политик регистрации устройств для предотвращения несанкционированного доступа. Кроме того, корректировка срока действия токенов, выпущенных системой, и использование средств защиты на уровне сети для обнаружения и предотвращения использования резидентных прокси-серверов являются важными шагами в защите от этих угроз.

D. Детали TTP:

- **Доступ к учётным данным / подбор пароля T1110**: используются password-spray и подбор паролей в качестве начальных векторов заражения. Подход предполагает попытку ввода нескольких паролей для разных учётных записей или многочисленные попытки для одной учётной записи для получения несанкционированного доступа.
- **Первоначальный доступ / T1078.004 Действительные учётные записи: Облачные учётные записи:** получение доступа к облачным сервисам, используя скомпрометированные учётные данные: как системные учётные записи (используемые для автоматизированных задач и служб), так и неактивные учётные записи, учётные которые все ещё остаются в системе.
- **Доступ к учётным данным / T1528 Кража токена доступа к приложению:** злоумышленники используют украденные токены доступа для входа в учётные записи без необходимости ввода паролей. Токены доступа — это цифровые ключи, которые позволяют получить доступ к учётным записям пользователей. Их получение позволяет обойти традиционные механизмы входа в систему.
- **Доступ к учётным данным / Формирование запроса многофакторной аутентификации T1621:** метод «бомбардировка MFA» предполагает, что злоумышленники неоднократно отправляют запросы MFA на устройство жертвы. Цель состоит в том, чтобы жертва приняла запрос и таким образом предоставила злоумышленнику доступ.
- **Командование и контроль / T1090.002 Прокси: Внешний прокси:** чтобы поддерживать «тайные операции и сливаться с обычным трафиком», используются открытые прокси, расположенные в частных диапазонах IP-адресов, т.к. вредоносные соединения сложнее отличить от легальной активности пользователей в журналах доступа.
- **Постоянство / T1098.005 Манипулирование учётными записями: Регистрация устройств:** после получения доступа к учётным записям предпринимаются попытки зарегистрировать свои собственные устройства в облачном клиенте. Успешная регистрация устройства может обеспечить постоянный доступ к облачной среде.

1) Доступ через сервисные и спящие учётные записи

Одна из ключевых стратегий, применяемых злоумышленниками, предполагает нацеливание на сервисные и неактивные учётные записи в облачных средах. Учётные записи служб используются для запуска приложений и служб и управления ими без прямого взаимодействия с человеком. Эти учётные записи особенно уязвимы, поскольку их часто невозможно защитить с помощью многофакторной аутентификации (MFA), и они могут иметь высокопривилегированный доступ в зависимости от их роли в управлении приложениями и службами. Получив доступ к этим учётным записям, злоумышленники могут получить привилегированный

первоначальный доступ к сети, которую они используют в качестве стартовой площадки для дальнейших операций.

Кампании нацелены на неактивные учётные записи, пользователи которых больше не активны в организации-жертве, но не были удалены из системы. Эти учётные записи могут быть использованы для восстановления доступа к сети, особенно после мер реагирования на инциденты, таких как принудительный сброс пароля. Было замечено, что субъекты входили в эти неактивные учётные записи и следовали инструкциям по сбросу пароля, что позволяло им сохранять доступ даже после того, как группы реагирования на инциденты пытались их «выселить».

2) Аутентификация токена на основе облака

Ещё один TTP — это использование аутентификации на основе облачных токенов. Замечено, что злоумышленники использовали выданные системой токены доступа для аутентификации в учётных записях жертв без необходимости ввода пароля. Этот метод позволяет обходить традиционные методы аутентификации на основе учётных данных и может быть особенно эффективным, если срок действия этих токенов длительный, или если токены не защищены должным образом.

3) Брутфорс и password-spray

Использование злоумышленниками атаки (T1110) применяется в качестве начальных векторов заражения. Метод включают попытку доступа к учётным записям путём перебора множества паролей или использования общих паролей для многих учётных записей соответственно. Метод часто бывает успешен из-за использования слабых или повторно используемых паролей для разных учётных записей.

4) Роль токенов доступа

Токены доступа являются неотъемлемой частью современных систем аутентификации, особенно в облачных средах. Они предназначены для упрощения процесса входа в систему для пользователей и обеспечения безопасного метода доступа к ресурсам без повторного ввода учётных данных. Токены выдаются после того, как пользователь входит в систему с именем и паролем, и их можно использовать для последующих запросов аутентификации.

5) Риски, связанные с аутентификацией токенов

Хотя аутентификация на основе токенов может обеспечить удобство и безопасность, она также создаёт определённые риски, если ею не управлять должным образом. Если злоумышленники получат эти токены, они смогут получить доступ к учётным записям без необходимости знания пароли, особенно если токены имеют длительный срок действия.

6) Настройка срока действия токена

Отмечается, что время действия токенов, выпущенных системой, по умолчанию может варьироваться в зависимости от используемой системы. Однако для облачных платформ крайне важно предоставить администраторам возможность регулировать время действия этих токенов в соответствии с их потребностями в безопасности. Сокращение срока действия токенов может уменьшить окно возможностей для несанкционированного доступа, если токены будут скомпрометированы.

7) Обход аутентификации по паролю и MFA

Отмечается, что обход аутентификации по паролю в учётных записях с помощью повторного использования учётных данных и password-spray. Метод предполагает попытку получить доступ к большому количеству учётных записей с использованием часто используемых паролей, в то время как повторное использование учётных данных позволяет пользователям повторно использовать одни и те же пароли для нескольких учётных записей

Также применяется техника «бомбардировка MFA» (T1621), для обхода систем MFA. Метод предполагает повторную отправку запросов MFA на устройство жертвы до тех пор, пока жертва, перегруженная постоянными уведомлениями, не примет запрос. Метод эффективно использует человеческую психологию и неудобство повторных уведомлений для обхода надёжных мер безопасности.

8) Регистрация новых устройств в облаке

После преодоления первоначальных барьеров выполняется регистрация собственных устройств в качестве новых (T1098.005). Этот шаг имеет решающее значение для сохранения доступа к облачной среде и облегчения дальнейших вредоносных действий. Успех тактики зависит от отсутствия строгих правил проверки устройств в конфигурации безопасности арендатора облака. Без надлежащих мер проверки устройств крайне легко добавить неавторизованные устройства в сеть, предоставив им доступ к конфиденциальным данным и системам.

9) Защита от несанкционированной регистрации устройств

Внедряя строгие правила проверки устройств и политики регистрации, организации могут значительно снизить риск несанкционированной регистрации устройств. Известны случаи, когда эти меры были эффективно применены, успешно защитили от злоумышленников, лишив их доступа к арендатору облака.

10) Резидентные прокси и их использование

Резидентные прокси — это промежуточные службы, которые позволяют пользователям маршрутизировать трафик через IP-адрес, предоставленный интернет-провайдером (ISP), который обычно присваивается резидентному адресу. Из-за этого трафик выглядит так, как будто он исходит от обычного пользователя, что может быть особенно полезно для целей слиться с обычным трафиком и избежать раскрытия.

Использование резидентных прокси-серверов служит целью сокрытия истинного местонахождения и источника их вредоносной деятельности. Создавая впечатление, что их трафик исходит из диапазонов легитимных провайдеров. Тактика усложняет обеспечение безопасности, которые полагаются на репутацию IP-адреса или геолокацию как на индикаторы компрометации.

11) Проблемы, создаваемые резидентными прокси

Эффективность резидентных прокси-серверов в сокрытии источника трафика представляет собой проблему для сетевой защиты. Традиционные меры безопасности, которые отслеживают и блокируют известные вредоносные IP-адреса, неэффективны против использующих резидентные прокси-серверы, поскольку эти IP-адреса могут не иметь предыстории вредоносной активности и неотличимы от IP-адресов законных пользователей.

E. Аутентификация как ключевой шаг

1) Аутентификация как ключевой шаг в облачной безопасности

В изменяющемся кибер-ландшафте адаптация к целевым облачным сервисам подчёркивает кардинальный сдвиг в тактике кибершпионажа. Переход от использования уязвимостей локальной сети к прямому нацеливанию на облачные инфраструктуры знаменует собой значительную эволюцию киберугроз. В основе этого лежит решающая роль аутентификации как ключевого шага в защите облачных сетей от кибер-профессионалов.

2) Важность аутентификации в облачных средах

Аутентификация служит шлюзом к облачным сервисам, определяя, следует ли предоставить доступ пользователю или системе. В облачных средах, где ресурсы и данные размещаются за пределами предприятия и доступны через Интернет, невозможно переоценить важность надёжных механизмов аутентификации. В отличие от традиционных локальных систем, где есть меры физической безопасности и внутренняя сетевая защита, облачные сервисы по своей сути более подвержены воздействию Интернета. Такая уязвимость делает начальный этап аутентификации не просто мерой безопасности, а критически важным механизмом защиты от несанкционированного доступа.

3) Проблемы облачной аутентификации

Переход к облачным сервисам приносит с собой уникальные проблемы в реализации эффективных стратегий аутентификации. Пользователи получают доступ к облачным сервисам из разных мест, устройств и сетей, что требует эффективных механизмов аутентификации.

Масштабируемость облачных сервисов означает, что механизмы аутентификации должны быть в состоянии обрабатывать большое количество запросов на доступ без значительных задержек и ухудшения пользовательского опыта. Это требование масштабируемости и удобства для пользователя часто противоречит необходимости строгих мер безопасности, создавая хрупкий баланс, который должны соблюдать организации.

4) Стратегии усиления облачной аутентификации

- **Многофакторная аутентификация (MFA).** MFA добавляет дополнительный уровень безопасности, требуя от пользователей предоставления двух или более факторов проверки для получения доступа. Подход снижает риск несанкционированного доступа, поскольку значительно сложнее получить несколько факторов аутентификации.
- **Адаптивная аутентификация.** Механизмы адаптивной аутентификации корректируют требования в зависимости от контекста запроса доступа. Такие факторы, как местоположение, устройство и поведение пользователя, могут влиять на процесс аутентификации, что позволяет применять более строгий контроль в сценариях повышенного риска.
- **Архитектура нулевого доверия.** Принятие подхода нулевого доверия к облачной безопасности, при котором ни один пользователь или система не пользуется доверием по умолчанию, может повысить эффективность аутентификации. Эта модель требует строгой проверки личности каждого кто пытается получить доступ к ресурсам, независимо от их местоположения или сети.
- **Использование биометрии.** Методы биометрической аутентификации, такие как сканирование отпечатков пальцев или распознавание лиц, обеспечивают высокий уровень безопасности за счёт использования уникальных физических характеристик пользователей. Эти методы могут быть особенно эффективными для предотвращения несанкционированного доступа в облачных средах.
- **Шифрование данных аутентификации.** Шифрование данных аутентификации (паролей, токенов аутентификации и другой конфиденциальной информации), как при передаче, так и при хранении, может защитить от перехвата и использования злоумышленниками.

F. Первоначальный доступ

1) Возросшая важность первоначального доступа в облачной безопасности

Смещение акцента кибер-профессионалов на облачные сервисы вывело важность обеспечения первоначального доступа на передний план. В облачных средах первоначальный доступ представляет собой критический момент, когда безопасность всей системы становится наиболее уязвимой. В отличие от традиционных локальных сетей, доступ к облачным сервисам осуществляется через Интернет, что делает начальную точку входа основной целью для злоумышленников.

2) Первоначальный доступ как плацдарм для злоумышленников

Получение первоначального доступа к облачным сервисам позволяет злоумышленникам закрепиться в целевой среде с последующим повышением привилегий, распространения по сети и получения доступа к конфиденциальным данным. Распределённый характер облачных сервисов также означает, что компрометация одной учётной записи может потенциально предоставить доступ к широкому спектру ресурсов и данных.

3) Проблемы в обеспечении первоначального доступа

- **Удалённый доступ.** Облачные сервисы предназначены для удалённого доступа, что увеличивает поверхность атаки.

- **Управление идентификацией и доступом (IAM).** В облачных средах IAM становится важнейшим компонентом безопасности. Организации должны обеспечить надёжность политик IAM и предоставление разрешений на основе принципа наименьших привилегий, чтобы минимизировать риск первоначального доступа со стороны неавторизованных лиц.

- **Фишинг и социнженерия.** используются методы фишинга и социальной инженерии для получения первоначального доступа. Эти методы используют человеческий фактор, а не технические уязвимости, что затрудняет защиту от них с помощью традиционных мер безопасности.

4) Примеры методов первоначального доступа

- **Credential Stuffing.** Метод предполагает использование ранее взломанных пар имени пользователя и пароля для получения несанкционированного доступа к учётным записям, делая ставку на вероятность того, что люди будут повторно использовать учётные данные в нескольких службах.

- **Использование некорректных конфигураций.** Облачные сервисы сложно настроить правильно, и используются некорректные конфигурации: открытые сетевые сегменты или ошибки в настройке управления доступом.

- **Компрометация сторонних сервисов.** Злоумышленники могут атаковать сторонние сервисы, которые интегрируются с облачными средами, например приложения SaaS, чтобы получить первоначальный доступ к облачной инфраструктуре.

5) Снижение рисков первоначального доступа

- **Комплексные политики доступа.** Установление и соблюдение комплексных политик доступа может помочь контролировать, кто и на каких условиях имеет доступ к облачным ресурсам.

- **Регулярные аудиты и проверки.** Проведение регулярных аудитов и проверок журналов доступа и разрешений может помочь выявить и устранить потенциальные уязвимости до того, как они будут использованы.

- **Обучение по вопросам безопасности.** Обучение сотрудников рискам фишинга и социальной инженерии может снизить вероятность компрометации учётных данных.

- **Endpoint Security.** Обеспечение безопасности и актуальности всех устройств с доступом к облачным сервисам, может помешать злоумышленникам использовать уязвимости конечных точек для получения первоначального доступа.

- **Обнаружение аномалий.** Внедрение систем обнаружения аномалий помогает выявить необычные модели доступа или попытки входа в систему, которые могут указывать на попытку взлома.

G. Расширение сферы деятельности

1) Расширение таргетинга

Стратегическое расширение деятельности на более широкий круг секторов является тревожным событием в сфере глобальной безопасности. Такая диверсификация целей отражает расчётливый подход к использованию взаимосвязанного характера современных отраслей и растущей зависимости от облачных сервисов в различных секторах.

2) Расширение сферы шпионажа

Расширение таких секторов, как авиация, образование, правоохранительные органы, местные и федеральные учреждения, правительственные финансовые ведомства и военные организации, демонстрирует их намерение собирать разведданные из широкого спектра источников. Широкая стратегия таргетинга предполагает, что они заинтересованы не только в традиционной информации, связанной с национальной безопасностью, но также в получении разнообразного набора данных, которые могут обеспечить экономические, политические или технологические преимущества.

3) Последствия для различных секторов

- **Авиация.** Авиационная отрасль включает в себя сложную экосистему авиакомпаний, аэропортов, производителей и служб поддержки, каждая из которых обрабатывает конфиденциальные данные, связанные с национальной безопасностью и запатентованными технологиями.

- **Образование.** Университеты и исследовательские институты являются источниками передовых исследований и интеллектуальной собственности. Их часто таргетируют за новаторскую работу в области науки, технологий и обороны.

- **Правоохранительные органы.** организации хранят конфиденциальные данные об уголовных расследованиях, вопросах национальной безопасности и личную информацию граждан, что делает их ценной целью для шпионажа.

- **Местные и федеральные учреждения.** Органы местного и федерального самоуправления управляют критически важной инфраструктурой, госуслугами и имеют доступ к огромным объёмам персональных данных, которые могут быть использованы для различных злонамеренных целей.

- **Государственные финансовые департаменты.** департаменты обрабатывают конфиденциальные экономические данные и имеют представление о национальных финансовых стратегиях и политике, что может быть ценным для иностранных разведывательных служб.

- **Военные организации.** представляют большой интерес из-за их стратегической важности и доступа

к секретной информации об оборонных возможностях, операциях и технологиях.

4) Проблемы защиты широкого круга целей

- **Разнообразие подходов к обеспечению безопасности.** Разные отрасли имеют разные уровни зрелости и ресурсов кибербезопасности, что делает некоторые из них более уязвимыми для сложных киберугроз.
- **Взаимосвязь.** Взаимосвязанный характер этих секторов означает, что нарушение в одной области может иметь каскадные последствия для других, как это видно в атаках на цепочки поставок.

5) Стратегии снижения рисков

- **Секторальные механизмы кибербезопасности.** Разработка и внедрение механизмов кибербезопасности, адаптированных к уникальным потребностям и рискам каждого сектора, может повысить общую безопасность.
- **Обмен информацией.** Обмен информацией об угрозах и лучшими практиками внутри секторов и между ними может помочь организациям опережать возникающие угрозы и координировать реагирование на инциденты.
- **Регулярные оценки безопасности.** Проведение регулярных оценок безопасности и тестирования на проникновение может помочь организациям выявлять и устранять уязвимости до того, как они будут использованы.
- **Безопасность цепочки поставок.** Укрепление безопасности цепочки поставок имеет решающее значение, поскольку злоумышленники часто нацелены на менее защищённые элементы в цепочке поставок, чтобы получить доступ к более крупным организациям.
- **Планирование реагирования на инциденты.** Наличие чётко определённого плана реагирования на инциденты может гарантировать, что организации готовы быстро и эффективно реагировать на нарушения.

H. Использование Сервисных и неактивных учётных записей

1) Использование сервисных и неактивных учётных записей в кибератаках

Эксплуатация сервисных и неактивных учётных записей кибер-профессионалами представляет собой изощренный и часто упускаемый из виду вектор кибератак. Эти учётные записи, созданные для различных операционных целей в облачных и локальных средах организации, могут предоставить злоумышленникам доступ, необходимый им для достижения своих целей, если они не управляются и не защищаются должным образом.

2) Понимание сервисных и неактивных учётных записей

Учётные записи служб — это специализированные учётные записи, используемые приложениями или службами для взаимодействия с операционной системой или другими службами. Они часто имеют повышенные привилегии для выполнения определённых задач и могут не быть привязаны к личности отдельного пользователя. С другой стороны, неактивные учётные записи — это учётные записи пользователей, которые больше не используются либо потому, что пользователь покинул организацию, либо потому, что цель учётной записи была достигнута. Эти учётные записи особенно опасны, поскольку о них часто забывают, им оставляют больше привилегий, чем необходимо, и они не контролируются так тщательно, как активные учётные записи пользователей.

3) Почему служебные и неактивные учётные записи подвергаются атаке

- **Повышенные привилегии.** Учётные записи служб имеют повышенные привилегии, необходимые для системных задач, которые можно использовать для получения широкого доступа к сети организации.
- **Отсутствие мониторинга.** Неактивные учётные записи используются нерегулярно, что снижает вероятность их отслеживания на предмет подозрительной активности делает их привлекательной целью для злоумышленников.
- **Слабые учётные данные или учётные данные по умолчанию.** Учётные записи служб могут быть настроены со слабыми учётными данными или учётными данными по умолчанию, которые проще найти с помощью атак методом перебора.
- **Обход аналитики поведения пользователей.** Поскольку учётные записи служб выполняют автоматизированные задачи, их модели поведения могут быть предсказуемыми, что позволяет вредоносным действиям сливаться с обычными операциями и уклоняться от обнаружения.

4) Угроза, которую представляют скомпрометированные учётные записи

- **Распространение:** использование привилегий учётной записи для дальнейшего распространения в сети, получая доступ к другим системам и данным.
- **Повышение привилегий:** использование учётной записи для повышения привилегий и получения административного доступа к критически важным системам.
- **Закрепление:** обеспечение постоянного присутствия в сети, что затрудняет обнаружение и устранение злоумышленника.
- **Эксфильтрация данных:** доступ к конфиденциальным данным и их удаление, что приводит к утечке данных и краже интеллектуальной собственности.

5) Снижение рисков, связанных с сервисными и неактивными счетами

- **Регулярные проверки.** Проведение регулярных проверок всех учётных записей для выявления и деактивации неактивных учётных записей и обеспечения того, чтобы учётные записи служб имели минимально необходимые привилегии.
- **Строгий контроль аутентификации.** Применение политики надёжных паролей и использование MFA для учётных записей служб, где это возможно.
- **Мониторинг.** Внедрение механизмов мониторинга и оповещения для обнаружения необычных действий, связанных со службами и неактивными учётными записями.
- **Разделение ролей.** Применение принципа разделения ролей к учётным записям служб, чтобы ограничить объем доступа и снизить риск неправомерного использования.
- **Инструменты автоматического управления.** Использование инструментов автоматического управления учётными записями, чтобы отслеживать использование и жизненный цикл учётной записи, гарантируя, что учётные записи будут деактивированы, когда они больше не нужны.

I. Изощрённость атак

1) Сложность кибероперaций

Отмечался высокий уровень сложности атак, что отражает глубокое понимание киберландшафта и способность адаптироваться в условиях меняющихся мер безопасности. Эта изощрённость очевидна не только в технических возможностях, но и в их стратегическом подходе к кибершпионажу, который включает в себя тщательный выбор целей, планирование и использование передовых тактик, методов и процедур (TTP).

2) Техническое мастерство и инновации

Кибероперации характеризуются использованием специального вредоносного ПО и уязвимостей нулевого дня. Эксплуатация этих уязвимостей позволяет эффективно проникать, например chain-атака SolarWinds, в результате которой был нарушен процесс разработки ПО путём внедрения вредоносного кода в обновление ПО, что затронуло клиентов, включая правительственные учреждения и компании из списка Fortune 500.

3) OpSec и скрытность

OpSec является отличительной чертой операций, и атакующие делают все возможное, чтобы замести следы и сохранить скрытность в скомпрометированных сетях. Это включает в себя использование зашифрованных каналов для кражи данных, тщательное управление серверами управления и контроля во избежание обнаружения, а также использование легитимных инструментов и услуг (LOTL), чтобы гармонировать с обычной сетевой деятельностью. Способность вести себя сдержанно в целевых сетях часто позволяет им проводить долгосрочные шпионские операции без обнаружения.

4) Тактика психологической и социальной инженерии

Помимо технических возможностей, он продемонстрировал искусность в тактике психологической и социальной инженерии. Эти методы предназначены для манипулирования людьми с целью разглашения конфиденциальной информации или выполнения действий, ставящих под угрозу безопасность. Фишинговые кампании, целевой фишинг и другие формы социнженерии часто используются для получения первоначального доступа к целевым сетям или для повышения привилегий внутри них.

5) Выбор цели и сбор разведданных

Процесс выбора цели носит стратегический характер и соответствует национальным интересам России. Цели тщательно выбираются на основе их потенциала предоставления ценной разведывательной информации, будь то политическая, экономическая, технологическая или военная. Как только цель скомпрометирована, участники сосредотачиваются на долгосрочном доступе и сборе разведданных, отдавая предпочтение скрытности и закреплению вместо немедленной выгоды.

6) Адаптируемость к ландшафту кибербезопасности

Одним из наиболее определяющих аспектов является его адаптивность. Переход в сторону облачных сервисов и использования сервисных и неактивных учётных записей является свидетельством такой адаптивности.

7) Базовые механизмы защиты

- **Контроль доступа:** обеспечение того, чтобы только авторизованные пользователи имели доступ к информационным системам и данными чтобы они могли выполнять только те действия, которые необходимы для их роли.
- **Шифрование данных:** защита данных при хранении и передаче посредством шифрования, что делает их нечитаемыми для неавторизованных пользователей.
- **Управление исправлениями:** регулярное обновление программного обеспечения и систем для устранения уязвимостей и снижения риска эксплуатации.
- **Брандмауэры и системы обнаружения вторжений (IDS):** внедрение брандмауэров для блокировки несанкционированного доступа и IDS для мониторинга сетевого трафика на предмет подозрительной активности.
- **Многофакторная аутентификация (MFA):** требование от пользователей предоставления двух или более факторов проверки для получения доступа к системам, что значительно повышает безопасность.
- **Обучение по вопросам безопасности:** обучение сотрудников рискам кибербезопасности и передовым методам предотвращения атак социальной инженерии и других угроз.
- **Планирование реагирования на инциденты:** подготовка к потенциальным инцидентам безопасности с помощью чётко определённого плана реагирования и восстановления.

8) Роль механизмов в защите от сложных угроз

Многие из кибер-стратегий по-прежнему используют основные недостатки безопасности, такие как плохое управление паролями, необновленное ПО и недостаточный контроль доступа. Придерживаясь базовых механизмов безопасности, организации могут устранить эти уязвимости, значительно усложняя злоумышленникам первоначальный доступ или распространение внутри сети.

Например, реализация MFA может предотвратить несанкционированный доступ, даже если учётные данные скомпрометированы. Регулярное управление исправлениями может закрыть уязвимости до того, как они смогут быть использованы в ходе атаки нулевого дня. Обучение по вопросам безопасности может снизить риск того, что сотрудники станут жертвами фишинга или других тактик социальной инженерии.

9) Проблемы в поддержании механизмов безопасности

Несмотря на очевидные преимущества, поддержание «прочного фундамента безопасности» может оказаться непростой задачей для организаций. Это связано с множеством факторов, включая ограниченность ресурсов, сложность современной ИТ-среды и быстрые темпы технологических изменений. Кроме того, по мере того, как организации все чаще внедряют облачные сервисы и другие передовые технологии, среда становится более сложной, что требует постоянной адаптации фундаментальных методов обеспечения безопасности.

10) Стратегии усиления защиты

- **Непрерывная оценка рисков:** регулярная оценка состояния безопасности организации для выявления уязвимостей и определения приоритетности усилий по их устранению.
- **Использование структур безопасности:** принятие комплексных структур безопасности, таких как NIST Cybersecurity Framework, для руководства внедрением лучших практик и средств контроля.
- **Автоматизация процессов безопасности:** использование автоматизации для оптимизации процессов безопасности, таких как управление исправлениями и мониторинг, для повышения эффективности и результативности.
- **Формирование культуры безопасности:** создание культуры безопасности внутри организации, где кибербезопасность рассматривается как общая ответственность всех сотрудников.
- **Сотрудничество и обмен информацией:** участие в сотрудничестве и обмене информацией с коллегами по отрасли и государственными учреждениями, чтобы оставаться в курсе возникающих угроз и передового опыта.

J. Меры по смягчению последствий

- **Внедрение многофакторную аутентификацию (MFA).** MFA — это один из наиболее эффективных способов защиты учётных записей пользователей от компрометации. Требуя несколько форм проверки, MFA значительно затрудняет злоумышленникам получение несанкционированного доступа, даже если они получили учётные данные пользователя.
- **Регулярная установка исправлений и обновлений.** Поддержание актуальности программного обеспечения и систем с использованием последних исправлений имеет решающее значение для устранения брешей в безопасности, которыми могут воспользоваться злоумышленники. Должен быть установлен регулярный процесс управления исправлениями, чтобы обеспечить своевременное применение обновлений.
- **Сегментация сети.** Разделение сети на более мелкие контролируемые сегменты ограничивает возможность злоумышленника перемещаться внутри сети и получать доступ к конфиденциальным областям. Сегментация также помогает сдерживать потенциальные нарушения в меньшем подмножестве сети.
- **Защита конечных точек.** Развёртывание расширенных решений для защиты конечных точек может помочь обнаружить и предотвратить вредоносные действия на устройствах, имеющих доступ к сети организации. Это включает в себя использование антивирусного программного обеспечения, систем предотвращения вторжений на базе хоста и инструментов обнаружения и реагирования на конечных точках (EDR).
- **Обучение по вопросам безопасности.** Обучение сотрудников рискам и передовым методам кибербезопасности имеет важное значение для предотвращения атак социальной инженерии, таких как фишинг. Регулярное обучение может помочь создать культуру осведомлённости о безопасности внутри организации.
- **Контроль доступа с наименьшими привилегиями.** Обеспечение пользователей только правами доступа, необходимыми для их роли, помогает минимизировать потенциальное воздействие компрометации учётной записи. Средства контроля доступа должны регулярно пересматриваться и корректироваться по мере необходимости.
- **Планирование реагирования на инциденты.** Наличие чётко определённого и проверенного плана реагирования на инциденты позволяет организациям быстро и эффективно реагировать на инциденты безопасности, сводя к минимуму ущерб и восстанавливая операции как можно скорее.
- **Непрерывный мониторинг и обнаружение.** Реализация возможностей непрерывного мониторинга и обнаружения может помочь выявить подозрительные действия на раннем этапе. Сюда входит использование систем управления информацией о безопасности и событиями (SIEM), систем обнаружения вторжений (IDS) и анализа сетевого трафика.

- **Безопасная конфигурация и усиление защиты.** Системы должны быть надёжно настроены и защищены от атак. Это включает в себя отключение ненужных служб, применение параметров безопасной конфигурации и обеспечение включения функций безопасности.
- **Резервное копирование и восстановление.** Регулярное резервное копирование критически важных данных и систем, а также надёжные процедуры восстановления необходимы для устойчивости к программам-вымогателям и другим разрушительным атакам. Резервные копии следует регулярно проверять, чтобы гарантировать, что на них можно положиться в чрезвычайной ситуации.

1) Проблемы в реализации мер по смягчению последствий

Хотя эти меры по смягчению последствий теоретически эффективны, организации часто сталкиваются с проблемами при их реализации. Эти проблемы могут включать ограниченность ресурсов, сложность ИТ-среды, потребность в специализированных навыках и сложность балансировки безопасности с бизнес-требованиями. Кроме того, быстро меняющаяся природа киберугроз означает, что стратегии смягчения их последствий должны постоянно пересматриваться и обновляться.

2) Совместные усилия и обмен информацией

Чтобы преодолеть эти проблемы и повысить эффективность мер по смягчению последствий, организации могут участвовать в совместных усилиях и обмене информацией с отраслевыми партнёрами, государственными учреждениями и сообществами кибербезопасности. Такое сотрудничество обеспечивает доступ к общим знаниям, информации об угрозах и передовым практикам, которые могут информировать и улучшать усилия организации по смягчению последствий.

K. Преимущества и недостатки документа

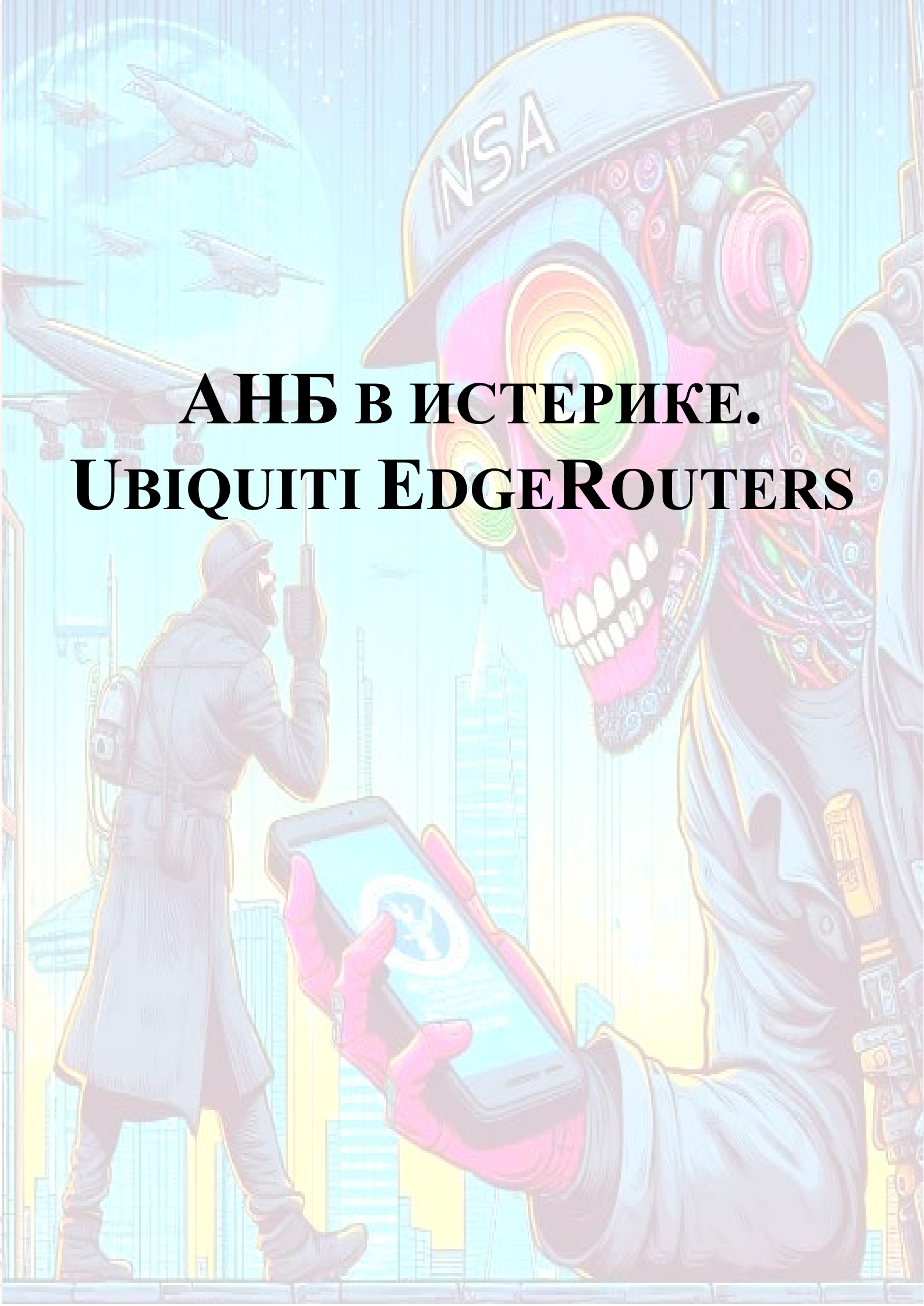
Документ содержит ценную информацию и рекомендации для организаций по защите от кибер-профессионалов, нацеленных на облачные сервисы. Однако динамичный характер киберугроз и сложность облачных сред означают, что организации должны постоянно обновлять свои методы обеспечения безопасности, а не полагаться исключительно на статические рекомендации.

1) Преимущества:

- **Осведомлённость**: документ повышает осведомлённость об изменении тактики в сторону облачных сервисов, что имеет решающее значение для понимания организациями текущего ландшафта угроз.
- **Подробные TTP**: он предоставляет подробную информацию о тактиках, методах и процедурах (TTP), используемых участниками, включая использование сервисных и неактивных учётных записей, что может помочь организациям выявить потенциальные угрозы и уязвимости.
- **Секторальная информация**: описывается расширение охват таких секторов, как авиация, образование, правоохранительные органы и военные организации, предлагая отраслевую информацию, которая может помочь этим отраслям укрепить свою обороноспособность.
- **Стратегии смягчения последствий:** предлагает практические стратегии смягчения последствий, которые организации могут реализовать для усиления своей защиты от первоначального доступа со стороны субъектов, таких как внедрение MFA и управление системными учётными записями.

2) Недостатки:

- **Ресурсоёмкость**: реализация рекомендуемых мер по снижению рисков может потребовать значительных ресурсов, что может оказаться затруднительным для небольших организаций с ограниченными бюджетами и персоналом в области кибербезопасности.
- **Сложность облачной безопасности**: в документе указываются проблемы, присущие обеспечению безопасности облачной инфраструктуры, которые могут потребовать специальных знаний и навыков, которыми обладают не все организации.
- **Развивающаяся тактика:** хотя в документе представлены текущие TTП, тактика участников постоянно развивается, а это означает, что защита, основанная исключительно на этих рекомендациях, может быстро устареть.
- **Потенциал чрезмерного акцента на конкретных угрозах:** слишком большое внимание к таким субъектам может привести к тому, что организации пренебрегут другими векторами угроз, которые столь же опасны, но не описаны в документе.
- **Модель общей ответственности:** документ подразумевает модель общей ответственности за облачную безопасность, что может привести к путанице в разделении обязанностей по обеспечению безопасности между поставщиками облачных услуг и клиентами.
- **Ложное чувство безопасности:** у организаций может возникнуть ложное чувство безопасности, полагаясь на предложенные меры по смягчению последствий, не принимая во внимание необходимость динамической и адаптивной системы безопасности для реагирования на новые угрозы.



АНБ в истерике. Ubiquiti EdgeRouters

Аннотация –представлен анализ документа, опубликованного на официальном сайте Минобороны США, описывающего использование скомпрометированных маршрутизаторов Ubiquiti EdgeRouters по всему миру.

Этот анализ предоставляет качественную выжимку документа, делая его доступным для широкой аудитории, включая специалистов по кибербезопасности, сетевых администраторов и руководителей ИТ-отделов. Он позволяет понять угрозы APT28, что даёт возможность разработать эффективные стратегии защиты, методы идентификации и реагирования в сетевом оборудовании), а также стратегический взгляд на управление рисками и необходимость внедрения рекомендаций по смягчению угрозы для защиты организационной инфраструктуры.

A. Введение

Документ под названием “Cyber Actors Use Compromised Routers to Facilitate Cyber Operations”, опубликованный ФБР, АНБ, киберкомандованием США и международными партнёрами предупреждает об использовании скомпрометированных маршрутизаторов Ubiquiti EdgeRouters для облегчения вредоносных кибероперацій по всему миру.

Популярность Ubiquiti EdgeRouters объясняется удобной в использовании ОС на базе Linux, учётными данными по умолчанию и ограниченной защитой брандмауэром. Маршрутизаторы часто поставляются с небезопасными конфигурациями по умолчанию и не обновляют прошивку автоматически.

Скомпрометированные EdgeRouters использовались APT28 для сбора учётных данных, дайджестов NTLMv2, сетевого трафика прокси-сервера и размещения целевых страниц для фишинга и пользовательских инструментов. APT28 получила доступ к маршрутизаторам, используя учётные данные по умолчанию, и троянизировала серверные процессы OpenSSH. Наличие root-доступ к скомпрометированным маршрутизаторам, дало доступ к ОС для установки инструментов и сокрытия своей личности.

APT28 также развернула пользовательские скрипты Python на скомпрометированных маршрутизаторах для сбора и проверки украденных данных учётной записи веб-почты, полученных с помощью межсайтовых скриптов и кампаний фишинга "браузер в браузере". Кроме того, они использовали критическую уязвимость с повышением привилегий на нулевой день в Microsoft Outlook (CVE-2023–23397) для сбора данных NTLMv2 из целевых учётных записей Outlook и общедоступные инструменты для оказания помощи в атаках с ретрансляцией NTLM

B. Ключевые моменты

- APT28 (известные как Fancy Bear, Forest Blizzard и Strontium) использовали скомпрометированные серверы Ubiquiti EdgeRouters для проведения вредоносных кибероперацій по всему миру.
- Эксплуатация включает сбор учётных данных, сбор дайджестов NTLMv2, проксирование сетевого трафика, а также размещение целевых страниц для фишинга и пользовательских инструментов.
- ФБР, АНБ, киберкомандование США и международные партнеры выпустили совместное консультативное заключение по кибербезопасности (CSA) с подробным описанием угрозы и рекомендациями по ее устранению.
- Рекомендации включают наблюдаемые тактики, методы и процедуры (TTP), индикаторы компрометации (IoC) для сопоставления с системой MITRE ATT&CK framework.
- В рекомендациях содержится настоятельный призыв к немедленным действиям по устранению угрозы, включая выполнение заводских настроек оборудования, обновление встроенного ПО, изменение учётных данных по умолчанию и внедрение стратегических правил брандмауэра.
- APT28 использует скомпрометированные EdgeRouters как минимум с 2022 года для содействия операциям против различных отраслей промышленности и стран, включая США.
- EdgeRouters популярны благодаря своей удобной операционной системе на базе Linux, но часто поставляются с учётными данными по умолчанию и ограниченной защитой брандмауэром.
- В рекомендациях содержатся подробные TTP и IOC, которые помогут сетевым защитникам идентифицировать угрозу и смягчить ее последствия.
- Рекомендация также включает информацию о том, как сопоставить вредоносную кибератиность с платформой MITRE ATT&CK framework.

- Организации, использующие Ubiquiti EdgeRouters, должны принять немедленные меры для защиты своих устройств от использования APT28.
- Рекомендуемые действия включают сброс оборудования к заводским настройкам, обновление до последней версии прошивки, изменение имен пользователей и паролей по умолчанию и внедрение стратегических правил брандмауэра.

C. Активность группы

Операции были нацелены на различные отрасли, включая аэрокосмическую и оборонную, образование, энергетику и коммунальные услуги, госсектор, гостиничный бизнес, нефть и газ, розничную торговлю, технологии и транспорт. Целевые страны включают Чешскую Республику, Италию, Литву, Иорданию, Черногорию, Польшу, Словакию, Турцию, Украину, Объединённые Арабские Эмираты и США

Потенциальные последствия воздействия включают:

- Утечка данных и кража конфиденциальной информации, интеллектуальной собственности или коммерческой тайны.
- Нарушение работы критически важных объектов инфраструктуры, таких как электросети, транспортные системы или производственные процессы.
- Компрометация правительственных сетей и систем, потенциально ведущая к шпионажу или угрозам национальной безопасности.
- Финансовые потери из-за сбоев в работе, кражи данных клиентов или ущерба репутации.
- Потенциальные риски для безопасности в случае взлома систем управления или сетей операционных технологий (OT).
- Потеря доверия клиентов и доверия к пострадавшим организациям.

D. OpenSSH-Троян Moobot

APT28 использовали учётные данные по умолчанию и троянизированные серверные процессы OpenSSH для доступа к Ubiquiti EdgeRouters, связанеые с Moobot, ботнетом на базе Mirai, который заражает устройства Интернета вещей (IoT) с использованием уязвимостей, которые можно использовать удалённо, таких как слабые пароли или пароли по умолчанию.

1) Троянские файлы OpenSSH-сервера

Троянские бинарные OpenSSH, загруженные с packinstall[.]kozow [.]com, заменили оригинальные бинарные файлы на EdgeRouters с целью удалённо обходить аутентификацию и получать несанкционированный доступ к скомпрометированным маршрутизаторам.

Ботнет Moobot известен своей способностью использовать уязвимости в устройствах Интернета вещей, особенно с ненадёжными паролями или паролями по умолчанию. Заменяя законные двоичные файлы сервера OpenSSH троянскими версиями, APT28 могут поддерживать постоянный доступ к скомпрометированным EdgeRouters и использовать их в различных вредоносных целях.

2) Ботнет на базе Mirai

Moobot – это ботнет на базе Mirai и является производным от Mirai, которая впервые появилась в 2016 году. Mirai был предназначен для сканирования и заражения IoT-устройств путём использования распространённых уязвимостей и учётных данных по умолчанию. Как только устройство заражено, оно становится частью ботнета и может использоваться для распределённых атак типа "отказ в обслуживании" (DDoS), credential stuffing и других вредоносных действий.

3) Воздействие на маршрутизаторы EdgeRouters

При наличии троянизированных процессов OpenSSH APT28 могут поддерживать постоянный доступ к скомпрометированным маршрутизаторы и использовать их в качестве платформы для вредоносных действий:

- Сбор учётных данных
- Сбор дайджестов NTLMv2
- Проксирование сетевого трафика
- Размещение целевых страниц для защиты от фишинга и пользовательских инструментов

E. Доступ с учётными данными через скрипты Python

APT28 размещали скрипты Python на скомпрометированных Ubiquiti EdgeRouters для сбора и проверки украденных учётных данных учётной записи веб-почты. Эти сценарии обычно хранятся вместе со связанными файлами журналов в домашнем каталоге скомпрометированного пользователя, например:

- /home/<compromised user>/srv/core.py
- /home/<compromised user>/srv/debug.txt

ФБР заявило о восстановлении подробных файлов журналов, содержащие информацию об активности APT28 на скомпрометированных EdgeRouters.

1) Пользовательские скрипты на Python

Размещённые крипты Python служат для сбора и проверки украденных данных учётной записи веб-почты. APT28 используют эти скрипты как часть своих операций сбора учётных данных, нацеленных на конкретных пользователей веб-почты.

Скрипты предназначены для автоматического устранения проблем с капчей на страницах входа в веб-почту, позволяя атакующим обойти эту меру безопасности и получить несанкционированный доступ к целевым учётным записям. Чтобы достичь этого, скрипты устанавливают соединения с API endpoint api[.]anti-captcha[.]com, который используется APT28 для решения проблем с капчей.

2) Yara-правила для обнаружения

Чтобы помочь найти скрипты сбора учётных данных на скомпрометированных EdgeRouters, ФБР разработало правило Yara. Yara – это инструмент, используемый для идентификации и классификации вредоносных программ на основе текстовых или двоичных шаблонов. Предоставленное ФБР правило Yara можно использовать для сканирования файловой системы EdgeRouters и обнаружения присутствия скриптов Python.

Помимо использования правила Yara, можно также запрашивать сетевой трафик на предмет подключений к api[.]anti-captcha[.]com endpoint. Обнаружение трафика, направленного к этому API, может помочь выявить скомпрометированные EdgeRouters и потенциальные действия по сбору учётных данных.

3) Смягчение последствий

При обнаружении наличия скриптов или подключений к api[.]anti-captcha[.]com endpoint сетевые необходимо предпринять немедленные действия для снижения риска и исследовать степень компрометации. Изоляция затронутых маршрутизаторов Edge от сети

- Выполнение тщательного анализа сценариев и файлов журналов для понимания объема операций по сбору учётных данных
- Сброс паролей для потенциально скомпрометированных учётных записей веб-почты

F. Эксплуатация CVE-2023-23397

APT28 использовали CVE-2023–23397, уязвимость с критическим повышением привилегий в Microsoft Outlook в Windows, для облегчения утечки учётных данных NTLMv2. Эта 0day-уязвимость позволяет передавать хэши Net-NTLMv2 в подконтрольную инфраструктуру.

1) Сбор учётных данных NTLMv2

Для использования CVE-2023–23397 и сбора учётных данных NTLMv2 использованы два общедоступных инструмента:

- **ntlmrelayx.py:** инструмент является частью Impacket suite, набора классов Python для работы с сетевыми протоколами. APT28 использовали ntlmrelayx.py для выполнения relay-атак NTLM [T1557] и облегчения утечки учётных данных NTLMv2.
- **Responder:** инструмент, предназначенный для сбора и передачи хэшей NTLMv2 путём настройки подконтрольного сервера аутентификации [T1556] для сбора учётных данных NTLMv2 от целевых учётных записей Outlook.

Безопасники могут выполнять поиск файлов журналов, а также наличия ntlmrelayx.py и Responder.db, Responder-Session.log для выявления потенциальной активности, связанной с эксплуатацией CVE-2023–23397.

2) Смягчение последствий

Чтобы снизить риск использования CVE-2023–23397 и утечки учётных данных NTLMv2 следует предпринять следующие шаги:

- **Применение исправления Microsoft:** Microsoft выпустила исправление для CVE-2023–23397.
- **Проверка на наличие скомпрометированных EdgeRouters:** необходимо использовать предоставленную информацию для проверки EdgeRouters на наличие ntlmrelayx.py, связанных с ними файлов журналов, провести идентификацию и изоляцию всех скомпрометированных маршрутизаторов для дальнейшего расследования.
- **Сброс скомпрометированных учётных данных:** при обнаружении утечки учётных данных NTLMv2 следует сбросить соответствующие учётные записи пользователей и применить дополнительные меры безопасности, такие как MFA.
- **Применение рекомендуемых мер по устранению неполадок:** меры по устранению включают сброс настроек оборудования к заводским настройкам, обновление до последней версии встроенного ПО и изменение имён пользователей и паролей по умолчанию.

G. Прокси-сервер и туннельная инфраструктура

APT28 использовали скомпрометированные Ubiquiti EdgeRouters для установления прокси-соединений и SSH-туннелей к подконтрольной инфраструктуре для поддержания постоянного доступа и контроля над скомпрометированными устройствами даже после смены пароля или других попыток взлома.

1) Reverse proxy-подключения

Были использованы правила iptables в EdgeRouters для установления подключений, например:

```
iptables -t nat -I PREROUTING -d <router IP address> -p tcp -m tcp --dport 4443 -j DNAT -to-destination <APT28 dedicated infrastructure>:10081
```

Это правило iptables перенаправляет входящий трафик через порт 4443 EdgeRouter в выделенную инфраструктуру на порту 10081.

2) Reverse SSH-туннели

Кроме того, APT28 загрузили контролируемые SSH-RSA-ключи на скомпрометированные EdgeRouters для создания SSH-туннелей. Эти туннели позволяют получать доступ к скомпрометированным устройствам даже после смены пароля или других попыток взлома.

Следующие каталоги необходимо просмотреть на предмет неизвестных ключей RSA:

- /root/.ssh/
- /home/<user>/.ssh/

Наличие неизвестных ключей RSA в этих каталогах может указывать на то, что их использовали для доступа к EdgeRouters в обход аутентификации по паролю.

Кроме того, безопасники могут проверить журналы сетевого трафика на EdgeRouters для идентификации аномальные сеансы SSH:

```
ssh –i <RSA key> -p <port> root@<router IP address> -R <router IP address>:<port>
```

Эта команда устанавливает SSH-туннель от EdgeRouter к инфраструктуре, позволяя поддерживать удалённый доступ и контроль над скомпрометированным устройством.

H. Вредоносная программа MASEPIE

В декабре 2023 года APT28 разработали MASEPIE, небольшой бэкдор на Python, способный выполнять произвольные команды на машинах-жертвах. Расследование ФБР показало, что скомпрометированные Ubiquiti EdgeRouters были использованы в качестве C2-инфраструктуры для бэкдоров MASEPIE.

1) Командно-контрольная инфраструктура

Хотя APT28 не развёртывает MASEPIE на самих EdgeRouters, скомпрометированные маршрутизаторы использовались в качестве инфраструктуры C2 для связи с бэкдорами MASEPIE и контроля над ними, установленными в системах, принадлежащих целевым лицам и организациям.

Данные, отправляемые на EdgeRouters, действующие как серверы C2, были зашифрованы с использованием случайно сгенерированного 16-символьного ключа AES, для затруднения обнаружения и анализа трафика.

2) Функциональность бэкдора MASEPIE

MASEPIE – это бэкдор на основе Python, который позволяет выполнять произвольные команды в заражённых системах. Этот бэкдор предоставляет возможности удалённого управления для выполнения действий:

- эксфильтрация данных
- распространение внутри скомпрометированной сети
- развёртывание дополнительных вредоносных программ или инструментов
- выполнение команд разведки и сбора разведданных

3) Смягчение последствий

Чтобы снизить риск появления бэкдоров MASEPIE и использования скомпрометированных EdgeRouters в качестве C2-инфраструктуры, следует предпринять следующие шаги:

- **Внедрение защиты конечных устройств:** развёртывание решений для защиты конечных устройств, способных обнаруживать и предотвращать выполнение MASEPIE и других вредоносных скриптов Python или бэкдоров.
- **Мониторинг сетевого трафика:** отслеживание сетевого трафика на предмет любых подозрительных зашифрованных сообщений или подключений к известной инфраструктуре, включая скомпрометированные EdgeRouters.
- **Анализ сетевых журналов:** просмотр сетевых журналов на предмет признаков зашифрованных сообщений или подключений к EdgeRouters, которые могут действовать как серверы C2.

I. TTPs MITRE ATT&CK

1) Разработка:

T1587 (разработка): создание пользовательских Py-скриптов для сбора учётных данных в т.ч веб-почты.

T1588 (возможности получения): доступ к EdgeRouters, скомпрометированным ботнетом Moobot, который устанавливает троянские программы OpenSSH.

2) Первоначальный доступ:

T1584 (скомпрометированная инфраструктура): доступ к EdgeRouters, ранее скомпрометированным троянцем OpenSSH.

T1566 (фишинг): межсайтовые скриптовые кампании и фишинговые кампании "браузер в браузере".

3) Выполнение:

T1203 (Использование для выполнения клиентом): использование уязвимости CVE-2023-23397.

4) Закрепление:

T1546 (выполнение, инициируемое событием): На скомпрометированных маршрутизаторах были размещены скрипты Bash и двоичные файлы ELF, предназначенные для бэкдора демонов OpenSSH и связанных с ними служб.

5) Доступ с учётными данными:

T1557 (Злоумышленник посередине): инструменты Impacket ntlmrelayx.py и Responder, на скомпрометированные маршрутизаторы для выполнения ретрансляционных атак NTLM.

T1556 (Изменение процесса аутентификации): серверы аутентификации-мошенники NTLMv2 для изменения процесса аутентификации с использованием и передачей украденных учётных данных.

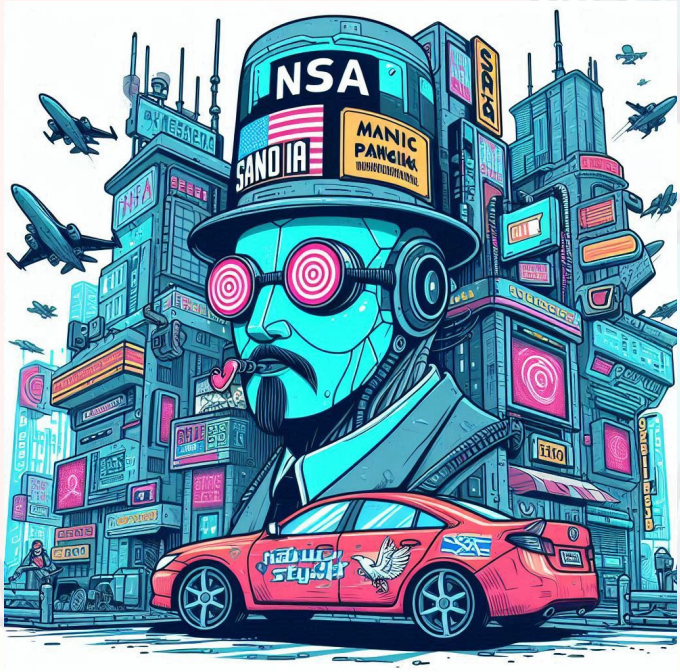
6) Сбор данных:

T1119 (автоматический сбор): APT28 использовал CVE-2023-23397 для автоматизации сбора хэшей NTLMv2.

7) Эксфильтрация данных:

T1020 (автоматизир2023–23397 сфильтрация): использование CVE-2023-23397 для автоматизации эксфильтрации данных в подконтрольную инфраструктуру.

АНБ В ИСТЕРИКЕ. SOHO



Аннотация – В документе представлен подробный анализ угроз, возникающих при использовании небезопасных маршрутизаторов для малого офиса / домашнего офиса (SOHO). Анализ охватывает различные аспекты, включая проблемы безопасности и эксплойты, воздействие на критическую инфраструктуру.

В документе предлагается качественная сводка текущего состояния безопасности маршрутизаторов SOHO, в которой подчёркиваются риски, создаваемые небезопасными устройствами, и шаги, которые можно предпринять для снижения этих рисков. Анализ полезен специалистам по безопасности, производителям и различным отраслям промышленности, обеспечивая всестороннее понимание угроз и руководящих принципов повышения безопасности маршрутизаторов SOHO.

A. Введение

Эксплуатация небезопасных маршрутизаторов SOHO злоумышленниками, особенно группами, спонсируемыми государством, представляет значительную угрозу для отдельных пользователей и критически важной инфраструктуры. Производителям настоятельно рекомендуется применять принципы security by-design, privacy-by-design и методы повышения прозрачности для снижения этих рисков, в то время как пользователям и безопасникам рекомендуется внедрять передовые методы обеспечения безопасности маршрутизаторов и сохранять бдительность в отношении потенциальных угроз.

B. Проблема небезопасных маршрутизаторов soho

Причины небезопасных маршрутизаторов SOHO многогранны, включая как технические уязвимости, так и ошибки производителей в методах безопасного проектирования и разработки, а также небрежность пользователей при обеспечении безопасности маршрутизаторов.

.

- **Распространённые уязвимости**: Значительное количество уязвимостей, общее число которых составляет 226, было выявлено в популярных брендах маршрутизаторов SOHO. Эти уязвимости различаются по степени серьёзности, но в совокупности представляют существенную угрозу.
- **Устаревшие компоненты**: Основные компоненты, такие как ядро Linux, и дополнительные службы, такие как VPN, в этих маршрутизаторах устарели. Это делает их восприимчивыми к известным эксплойтам уязвимостей, которые уже давно стали достоянием общественности.
- **Небезопасные настройки по умолчанию**: Многие маршрутизаторы поставляются с простыми паролями по умолчанию и отсутствием шифрования соединений, чем пользуются злоумышленники.
- **Отсутствие security-by-design**: Маршрутизаторам SOHO часто не хватает ряда функций безопасности, например возможностей автоматического обновления и отсутствия эксплуатируемых проблем, особенно в интерфейсах веб-управления.
- **Доступность интерфейсов управления**: Производители часто создают устройства с интерфейсами управления, с доступом через Интернет по умолчанию, часто без уведомления клиентов об этой небезопасной конфигурации.
- **Отсутствие прозрачности и подотчётности**: производители не обеспечивают прозрачность путём раскрытия уязвимостей продукта с помощью программы CVE и точной классификации этих уязвимостей с использованием CWE
- **Пренебрежение безопасностью в пользу удобства и функциональных возможностей**: Производители отдают предпочтение простоте использования и широкому спектру функций, а не безопасности, что приводит к созданию маршрутизаторов, которые "недостаточно безопасны" прямо из коробки, без учёта возможности эксплуатации.
- **Небрежность пользователей**: Многие пользователи, включая ИТ-специалистов, не соблюдают базовые правила безопасности, такие как смена паролей по умолчанию или обновление встроенного программного обеспечения, оставляя маршрутизаторы уязвимыми для атак.
- **Сложность идентификации уязвимых устройств**: Идентификация конкретных уязвимых устройств является сложной из-за юридических и технических проблем, усложняющих процесс их устранения.

C. Сектора / Отрасли

Эксплуатация небезопасных маршрутизаторов SOHO представляет серьёзную угрозу во многих секторах, что подчёркивает необходимость улучшения методов обеспечения безопасности.

1) Коммуникации

- **Утечки данных и перехват данных**: небезопасные маршрутизаторы могут привести к несанкционированному доступу к сетевому трафику, позволяя злоумышленникам перехватывать конфиденциальные сообщения.
- **Нарушение работы служб**: скомпрометированные маршрутизаторы могут использоваться для запуска распределённых атак типа "Отказ в обслуживании" (DDoS), нарушающих работу служб связи.

2) Транспорт и Логистика

Уязвимость инфраструктуры: транспортный сектор в значительной степени полагается на сетевые системы для выполнения операций. Скомпрометированные маршрутизаторы могут позволить злоумышленникам нарушить работу систем управления трафиком и логистических операций.

3) Водоснабжение

Операционные технологии (OT): небезопасные маршрутизаторы предоставляют злоумышленникам шлюз для атак на системы OT в секторе водоснабжения, что потенциально влияет на системы очистки и распределения воды.

4) Энергетика

Сетевая безопасность: Энергетический сектор, особенно предприятия электроэнергетики, подвержены риску целенаправленных атак через небезопасные маршрутизаторы. Злоумышленники могли получить доступ к системам управления, создавая угрозу стабильности электросети.

5) Другие отрасли

- **Здравоохранение**: Небезопасные маршрутизаторы могут скомпрометировать данные пациентов и нарушить работу медицинских служб, предоставляя злоумышленникам доступ к сетям здравоохранения.
- **Розничная торговля и гостиничный бизнес**: Эти сектора уязвимы для утечки данных, связанных с информацией о клиентах и финансовыми транзакциями, из-за небезопасных сетевых устройств.
- **Промышленность**: Промышленные системы управления могут быть взломаны через небезопасные маршрутизаторы, что влияет на производственные линии и производственные процессы.
- **Образование**: Школы и университеты подвержены риску утечки данных и сбоев в предоставлении образовательных услуг.
- **Государственный и общественный сектор**: небезопасные маршрутизаторы могут привести к несанкционированному доступу к правительственным сетям, подвергая риску конфиденциальную информацию и критически важные услуги

D. Основные выводы об использующих небезопасные маршрутизаторы SOHO

- **Эксплуатация группами, спонсируемыми государством**: Спонсируемая Китайской Народной Республикой (КНР) Volt Typhoon group активно компрометирует маршрутизаторы SOHO, используя проблемы ПО, который затем используются в качестве стартовых площадок для дальнейшей компрометации критически важных объектов инфраструктуры США.
- **Воздействие на критически важную инфраструктуру**: Взломанные маршрутизаторы SOHO представляют серьёзную угрозу, поскольку они могут использоваться для распространения внутри сетей и дальнейшего подрыва критически важных секторов инфраструктуры в США, включая связь, энергетику, транспорт и водоснабжение.
- **ZuoRAT Campaign**: Выявлена ZuoRAT кампания с использованием заражённых маршрутизаторов SOHO, где задействован троян, предоставляющий удалённый доступ и позволяющий сохранять незаметное присутствие в целевых сетях и для сбора конфиденциальную информацию.
- **Формирована ботнета**: скомпрометированные маршрутизаторы могут быть задействованы в ботнетах, крупных сетях заражённых устройств, используемых для запуска распределённых атак типа "отказ в обслуживании" (DDoS), кампаний рассылки спама и других вредоносных действий.
- **Атаки типа "MITM"**: использование уязвимости в маршрутизаторах для перехвата данных, проходящих по сети, и манипулирования ими, что приводит к утечке данных, краже личных данных и шпионажу.

1) TTPs

- **Вредоносное ПО KV Botnet**: Volt Typhoon внедрили вредоносное ПО KV Botnet в устаревшие маршрутизаторы Cisco и NETGEAR SOHO, которые больше не поддерживаются исправлениями безопасности или обновлениями ПО.
- **Сокрытие источника**: совершая действия через маршрутизаторы SOHO, возможно скрывать происхождение действий из КНР, что усложняет обнаружение и атрибуцию атак.
- **Нацеливание на электронные письма**: замечено, что Volt Typhoon нацеливались на электронные письма ключевых сетевых и ИТ-сотрудников, чтобы получить первоначальный доступ к сетям.
- **Использование мульти прокси-серверов**: для C2-инфраструктуры участники используют multi-hop прокси-серверы, обычно состоящие из VPS или маршрутизаторов SOHO.

- **Методы LOTL**: вместо того, чтобы полагаться на вредоносное ПО для выполнения после компрометации, Volt Typhoon использовали встроенные инструменты и процессы в системах, стратегию, известную как LOTL, для закрепления и расширения доступа к сетям жертв.

2) Воздействие и ответные меры

- **Нарушение работы критически важной инфраструктуры**: Эксплуатация маршрутизаторов представляет значительную угрозу, поскольку потенциально может нарушить работу основных служб, предоставляемых секторами критически важной инфраструктуры.
- **Федеральный ответ**: ФБР и Министерство юстиции провели операции по нарушению работы ботнета KV путем удаленного удаления вредоносного ПО с заражённых маршрутизаторов и принятия мер по разрыву их соединения с ботнетом.
- **Компромиссный ответ**: Volt Typhoon продемонстрировал сложность защиты от госкампаний кибершпионажа и решающую роль сотрудничества между правительством, частным сектором и международными партнёрами. Подчёркивалась необходимость комплексных стратегий кибербезопасности, которые включают защиту устройств, обмен информацией об угрозах и информирование общественности. Поскольку киберугрозы продолжают развиваться, необходимы и коллективные усилия по защите критически важной инфраструктуры и поддержанию целостности глобальных сетей.
- **Государственно-частное партнёрство**: Компромиссные меры в ответ на Volt Typhoon предполагали тесное сотрудничество между правительственными учреждениями, включая ФБР и CISA, и организациями частного сектора. Это партнёрство способствовало обмену информацией об угрозах, техническими индикаторами компрометации (IoC) и передовыми практиками по смягчению последствий.
- **Анализ прошивки и исправление**: Производители затронутых маршрутизаторов SOHO были предупреждены об уязвимостях, используемых участниками Volt Typhoon. Были предприняты усилия по анализу вредоносного ПО, пониманию методов эксплуатации и разработке исправлений для устранения уязвимостей.
- **Меры по смягчению последствий**: ФБР уведомляет владельцев или операторов маршрутизаторов SOHO, доступ к которым был получен во время операции «по демонтажу». Меры по смягчению последствий, санкционированные судом, носят временный характер, и перезапуск маршрутизатора без надлежащего смягчения последствий сделает устройство уязвимым для повторного заражения.

3) Общественный и потребительский спрос на безопасность

В современную цифровую эпоху безопасность сетевых устройств стала первостепенной заботой как для населения, так и для бизнеса. Такая повышенная осведомлённость обусловлена растущим числом громких кибератак и утечек данных, которые подчеркнули уязвимости, присущие подключённым устройствам. В результате растёт спрос со стороны потребителей и общественности на то, чтобы производители уделяли приоритетное внимание безопасности в своих продуктах.

a) Факторы, определяющие спрос

- **Повышение осведомлённости о киберугрозах**: Широкая общественность и предприятия становятся все более осведомлёнными о рисках, связанных с киберугрозами, включая потенциальные финансовые потери, нарушения конфиденциальности и сбои в работе сервисов.
- **Давление со стороны регулирующих органов**: Правительства и регулирующие органы по всему миру внедряют более строгие правила и стандарты кибербезопасности, вынуждая производителей улучшать функции безопасности своих продуктов.
- **Экономические последствия кибератак**: Экономические последствия кибератак, включая стоимость восстановления и влияние на репутацию бренда, сделали безопасность критически важным фактором для покупателей при выборе продуктов.
- **Взаимосвязанность устройств**: Распространение устройств Интернета вещей и взаимосвязанность цифровых экосистем усилили потенциальное воздействие взломанных устройств, сделав безопасность приоритетом для обеспечения целостности личных и корпоративных данных.

b) Ожидания клиентов

- **Встроенные функции безопасности**: теперь клиенты ожидают, что устройства будут поставляться с надёжными встроенными функциями безопасности, которые защищают от широкого спектра угроз, не требуя обширных технических знаний для настройки.
- **Регулярные обновления системы безопасности**: ожидается, что производители будут предоставлять регулярные и своевременные обновления системы безопасности для устранения новых уязвимостей по мере их обнаружения.
- **Прозрачность**: Клиенты требуют от производителей прозрачности в отношении безопасности их продуктов, включая чёткую информацию об известных уязвимостях и шагах, предпринимаемых для их устранения.
- **Простота использования**: Клиенты, требующие высокого уровня безопасности, также ожидают, что эти функции будут удобными для пользователя и не

повлияют на функциональность или производительность устройства.

4) *Ответственность производителей*

a) *Основные элементы Secure by Design*

- **Безопасность как основополагающее требование**: Безопасность следует рассматривать как основное требование, аналогичное функциональности, удобству использования и производительности на этапе всего жизненного цикла.
- **Минимизация поверхностей атаки**: Уменьшение количества потенциальных точек атаки внутри системы. Это предполагает ограничение функциональности и прав доступа системы только тем, что необходимо для ее функционирования, тем самым уменьшая возможности для эксплуатации.
- **Настройки безопасности по умолчанию**: Продукты должны поставляться с настройками безопасности по умолчанию, требующими от пользователей сознательного принятия решений по ослаблению безопасности. Это включает надёжные пароли по умолчанию, отключенные ненужные службы и включенное шифрование.
- **Принцип наименьших привилегий**: Обеспечение работы процессов, пользователей и систем с использованием минимального набора привилегий, необходимого для выполнения их задач. Это ограничивает потенциальный ущерб от эксплойта или взлома.
- **Безопасный отказ: проектирование** систем, обеспечивающих безопасный отказ в случае компрометации. Это означает, что когда система обнаруживает ошибку или нарушение, она по умолчанию переходит в состояние, которое минимизирует риск и подверженность.
- **Безопасность через прозрачность**: Поощрение открытости в отношении разработки и внедрения функций безопасности, обеспечение общественного контроля и экспертной оценки. Такая прозрачность помогает более эффективно выявлять и устранять уязвимости.
- **Privacy by Design**: интеграция Privacy by Design при разработке продукта, обеспечение защиты пользовательских данных и ответственного обращения с ними.
- **Оценка и управление рисками**: Проведение тщательной оценки рисков для понимания рисков безопасности, связанных с функциями и возможностями маршрутизатора, и управления ими.
- **Архитектура безопасности**: Разработка надёжной архитектуры безопасности, включающей аппаратные и программные компоненты, предназначенные для защиты от известных и возникающих угроз

b) *Реализация в маршрутизаторах SOHO*

- **Автоматические обновления**: Реализация механизмов автоматического обновления встроенного программного обеспечения для обеспечения того, чтобы на маршрутизаторах всегда работала последняя версия с самыми последними исправлениями безопасности. Это снижает зависимость от ручного обновления устройств.
- **Цифровая подпись**: Обеспечение цифровой подписи обновлений для проверки их подлинности и целостности. Это предотвращает установку вредоносных обновлений встроенного ПО, которые могут скомпрометировать маршрутизатор.
- **Безопасный веб-интерфейс управления**: Размещение веб-интерфейса управления на портах локальной сети и повышение его безопасности для обеспечения безопасного использования при доступе через Интернет. Это включает в себя внедрение надёжных механизмов аутентификации и шифрования.
- **Контроль доступа**: Ограничение доступа к веб-интерфейсу управления маршрутизатором со стороны локальной сети по умолчанию и предоставление опций для безопасного включения удалённого управления при необходимости.
- **Надёжные пароли по умолчанию**: Поставка маршрутизаторов с надёжными уникальными паролями по умолчанию для предотвращения несанкционированного доступа. Рекомендуется пользователям менять эти пароли во время первоначальной настройки.
- **Шифрование**: Использование шифрования для веб-интерфейса управления для защиты связи между маршрутизатором и пользователем.
- **Аутентификация**: Реализация механизмов надёжной аутентификации, включая возможность многофакторной аутентификации, для обеспечения доступа к интерфейсу управления маршрутизатором
- **Безопасные настройки по умолчанию**: маршрутизаторы по умолчанию поставляются с безопасными конфигурациями, такими как надёжные уникальные пароли, и отключены ненужные службы. Пользователей следует предостеречь от небезопасных конфигураций, если они решат переопределить значения по умолчанию.
- **Раскрытие уязвимостей и исправление**: Разработка четкой, ответственной политики раскрытия уязвимостей и своевременное предоставление исправлений. Это включает в себя участие в программе CVE по отслеживанию и раскрытию уязвимостей.

- **Поддержка по окончании срока службы**: Решающее значение имеет чёткое информирование о политике по окончании срока службы (EOL) для продуктов и предоставление поддержки и обновлений на протяжении всего жизненного цикла продукта. Для устройств, которые больше не поддерживаются, производителям следует предоставить рекомендации по безопасной утилизации или замене.

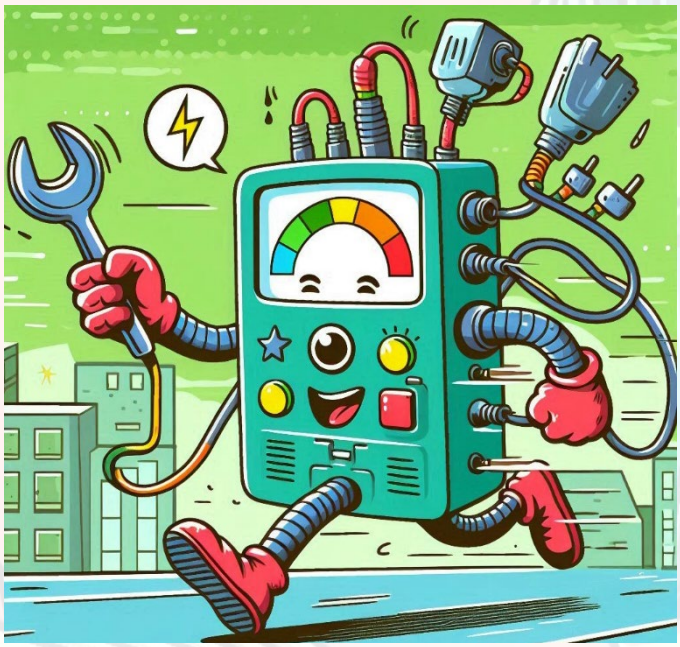
c) Последствия для производителей

- **Баланс между безопасностью и удобством использования**: Одной из проблем при реализации принципов Secure by Design является поддержание удобства использования. Меры безопасности не должны чрезмерно усложнять работу пользователя.
- **Финансовые издержки**: Разработка безопасных продуктов может повлечь за собой дополнительные расходы. Однако долгосрочные выгоды от снижения риска взломов и атак оправдывают эти инвестиции.
- **Непрерывное развитие**: Обеспечение безопасности — это не разовое мероприятие, оно требует постоянного внимания для адаптации к новым угрозам и уязвимостям.
- **Укрепление доверия**: Уделяя приоритетное внимание безопасности, производители получают возможность укреплять доверие клиентов, продукцию на конкурентном рынке.
- **Глобальная цепочка поставок**: Маршрутизаторы SOHO часто производятся как часть сложной глобальной цепочки поставок. Обеспечение безопасности по всей этой цепочке, от производителей компонентов до окончательной сборки, требует координации и соблюдения передовых методов обеспечения безопасности на каждом этапе.

E. Последствия атак на маршрутизаторы

- **Распространённые уязвимости**: Значительное количество уязвимостей, всего около 226 в совокупности представляют существенную угрозу безопасности.
- **Устаревшие компоненты**: Основные компоненты, такие как ядро Linux, и дополнительные службы, такие как VPN, устарели, что делает их уязвимыми для известных эксплойтов.
- **Пароли по умолчанию и незашифрованные соединения**: Многие маршрутизаторы поставляются с легко угадываемыми паролями по умолчанию и используют незашифрованные соединения, которыми могут легко воспользоваться злоумышленники.
- **Скомпрометированные устройства и данные**: После взлома маршрутизатора все устройства, защищенные его брандмауэром, становятся уязвимыми, позволяя злоумышленникам отслеживать, перенаправлять, блокировать или изменять данные.
- **Риск для критической инфраструктуры**: скомпрометированные маршрутизаторы SOHO могут использоваться для атаки на критическую инфраструктуру США, потенциально нарушая работу основных служб в секторах связи, энергетики, транспорта и водоснабжения.
- **Отказ в обслуживании и перехват трафика**: Уязвимости в протоколах могут приводить к атакам типа "отказ в обслуживании" против служб хоста и перехвату как внутреннего, так и внешнего трафика.
- **Перехват и кибератаки**: Злоумышленники могут перехватывать трафик и запускать дальнейшие сетевые атаки, затрудняя пользователям обнаружение взлома из-за минимальных пользовательских интерфейсов маршрутизатора.
- **Отсутствие методов обеспечения безопасности**: Исследования показывают, что многие пользователи, включая ИТ-специалистов, не соблюдают базовые методы обеспечения безопасности, такие как смена паролей по умолчанию или обновление встроенного программного обеспечения, что делает маршрутизаторы уязвимыми для атак.
- **Потенциал для широкомасштабной эксплуатации**: Само количество уязвимых устройств, исчисляемое миллионами, указывает на значительный потенциал для широкомасштабной эксплуатации злоумышленниками.
- **Юридические и технические проблемы**: Идентификация конкретных уязвимых устройств является сложной задачей из-за юридических и технических проблем, что усложняет процесс устранения этих уязвимостей.
- **Повышенная осведомлённость, но постоянные риски**: несмотря на растущую осведомлённость и усилия по повышению безопасности маршрутизаторов SOHO, многие известные недостатки остаются не устраненными, а продолжают обнаруживаться новые уязвимости

ОБНАРУЖЕНИЕ КИБЕРАТАК НА ИНТЕЛЛЕКТУАЛЬНЫЕ УСТРОЙСТВА С УЧЁТОМ ПОТРЕБЛЯЕМОЙ ЭНЕРГИИ



Аннотация – В научной статье "Detection of Energy Consumption Cyber Attacks on Smart Devices" подчёркивается растущая интеграция технологий Интернета вещей в умные дома и связанные с этим проблемы безопасности из-за нехватки ресурсов и ненадёжности сетей. Статья предлагает упрощённый метод обнаружения атак с использованием энергопотребления путём анализа принятых пакетов с учётом протоколов TCP, UDP и MQTT и оперативного оповещения при обнаружении аномального поведения, эффективно идентифицируя с помощью измерений скорости приёма пакетов.

A. Введение

В научной статье "Detection of Energy Consumption Cyber Attacks on Smart Devices" подчёркивается влияние интеграции технологии Интернета вещей в умные дома и связанные с этим проблемы безопасности.

- **Энергоэффективность**: подчёркивается важность энергоэффективности в системах Интернета вещей, особенно в средах "умного дома" для комфорта, уюта и безопасности.
- **Уязвимости**: уязвимость устройств Интернета вещей к кибератакам и физическим атакам из-за ограниченности их ресурсов подчёркивает необходимость защиты этих устройств для обеспечения их эффективного использования в реальных сценариях.
- **Предлагаемая система обнаружения**: Авторы предлагают систему обнаружения, основанную на анализе энергопотребления интеллектуальных устройств. Цель этой платформы – классифицировать состояние атак отслеживаемых устройств путём изучения структуры их энергопотребления.
- **Двухэтапный подход**: Методология предполагает двухэтапный подход. На первом этапе используется короткий промежуток времени для грубого обнаружения атаки, в то время как второй этап включает в себя более детальный анализ.
- **Облегчённый алгоритм**: представлен облегчённый алгоритм, который адаптирован к ограниченным ресурсам устройств Интернета вещей и учитывает три различных протокола: TCP, UDP и MQTT.
- **Анализ скорости приёма пакетов**: Метод обнаружения основан на анализе скорости приёма пакетов интеллектуальными устройствами для выявления аномального поведения, указывающего на атаки с использованием энергопотребления.

B. Преимущества и недостатки

Преимущества и недостатки дают сбалансированное представление о возможностях и ограничениях предлагаемой системы обнаружения, подчёркивая её потенциал для повышения безопасности "умного дома".

1) Преимущества

- **Облегчённый алгоритм обнаружения**: Предлагаемый алгоритм разработан таким образом, чтобы быть облегчённым, что делает его подходящим для устройств Интернета вещей с ограниченными ресурсами. Это гарантирует, что механизм обнаружения не будет чрезмерно нагружать устройства, которые он призван защищать.
- **Универсальность протокола**: Алгоритм учитывает множество протоколов связи (TCP, UDP, MQTT), что повышает его применимость к различным типам интеллектуальных устройств и конфигурациям сетей.
- **Двухэтапное обнаружение подход**: использование двухэтапного обнаружения подход позволяет повысить точность определения потребления энергии ударов при минимальном количестве ложных срабатываний. Этот метод позволяет как быстро провести первоначальное обнаружение, так и детальный анализ.
- **Оповещения в режиме реального времени**: Платформа оперативно оповещает администраторов об обнаружении атаки, обеспечивая быстрое реагирование и смягчение потенциальных угроз.
- **Эффективное обнаружение аномалий**: измеряя скорость приёма пакетов и анализируя структуру энергопотребления, алгоритм эффективно выявляет отклонения от нормального поведения, которые указывают на кибератаки.

2) Недостатки

- **Ограниченные сценарии атак**: Экспериментальная установка ориентирована только на определённые типы атак, что ограничивает возможность обобщения результатов на другие потенциальные векторы атак, не охваченные в исследовании.
- **Проблемы с масштабируемостью**: хотя алгоритм разработан таким образом, чтобы быть лёгким, его масштабируемость в более крупных и сложных

средах "умного дома" с большим количеством устройств и различными условиями сети может потребовать дальнейшей проверки.

- **Зависимость от исходных данных**: Эффективность механизма обнаружения зависит от точных базовых измерений скорости приёма пакетов и энергопотребления. Любые изменения в нормальных условиях эксплуатации устройств могут повлиять на исходные данные, потенциально приводя к ложноположительным или отрицательным результатам.
- **Ограничения ресурсов**: несмотря на легковесность, алгоритм по-прежнему требует вычислительных ресурсов, что может стать проблемой для устройств с крайне ограниченными ресурсами. Постоянный мониторинг и анализ также могут повлиять на срок службы батареи и производительность этих устройств.

C. Предлагаемый алгоритм

В работе подчёркивается роль алгоритмов машинного обучения (ML) в системах обнаружения вторжений (IDS) и проблемы, связанные с их развёртыванием на устройствах Интернета вещей с ограниченными ресурсами.

1) Пакетные измерения

- **Скорость приёма пакетов (PRR)**: обсуждается использование скорости приёма пакетов (PRR) в качестве ключевого показателя для обнаружения атак с энергопотреблением. PRR определяется как отношение успешно принятых пакетов к общему количеству пакетов, отправленных по сети.
- **Учёт протокола**: Алгоритм учитывает различные протоколы связи, включая TCP, UDP и MQTT, для измерения PRR. Каждый протокол обладает уникальными характеристиками, влияющими на передачу и приём пакетов.
- **Обнаружение аномального поведения**: Отслеживая PRR, алгоритм может выявлять отклонения от нормального поведения, которые могут указывать на наличие атаки. Значительное снижение PRR может быть признаком продолжающейся атаки на потребление энергии.

2) Измерения энергии

- **Анализ энергопотребления**: основное внимание уделяется анализу моделей энергопотребления интеллектуальных устройств для обнаружения аномалий. Алгоритм измеряет энергию, потребляемую устройствами, с течением времени и сравнивает её с ожидаемыми уровнями потребления.
- **Краткосрочные и долгосрочные измерения**: Предлагаемый метод использует двухэтапный подход с короткими и долгосрочными интервалами. В первом случае используется для первоначального, приблизительного обнаружения потенциальных атак, в то время как во втором – обеспечивается более подробный анализ для подтверждения наличия атаки.
- **Обнаружение конкретных атак**: Измерения энергопотребления помогают идентифицировать конкретные типы атак, такие как атаки типа "Отказ в обслуживании" (DoS) или распределённые атаки типа "Отказ в обслуживании" (DDoS), путём обнаружения необычных скачков или падений энергопотребления.

D. Эксперименты

Эксперименты проводились в моделируемой среде "умного дома" с различными устройствами Интернета вещей, и для оценки предлагаемой системы обнаружения были смоделированы различные типы атак с энергопотреблением. Результаты показывают, что алгоритм дерева решений (DT), развёрнутый на устройстве, обеспечивает лучшую производительность с точки зрения времени вывода и энергопотребления по сравнению с другими моделями ML.

1) Экспериментальная установка

- **Испытательный стенд для умного дома**: Эксперименты проводились в моделируемой среде "умного дома", состоящей из различных устройств Интернета вещей, таких как интеллектуальные светильники, камеры видеонаблюдения и интеллектуальные колонки, взаимодействующие по различным протоколам (TCP, UDP, MQTT).
- **Сценарии атак**: Авторы смоделировали различные типы атак с энергопотреблением, такие как атаки типа "Отказ в обслуживании" (DoS), распределённый отказ в обслуживании (DDoS) и DDoS-атаки на основе энергопотребления (EC-DDoS), чтобы оценить эффективность предлагаемой системы обнаружения.
- **Базовые измерения**: Базовые скорости приёма пакетов (PRR) и уровни энергопотребления были установлены для интеллектуальных устройств в нормальных условиях эксплуатации, чтобы служить ориентиром для обнаружения аномалий.
- **Показатели производительности**: определение показателей производительности: точность обнаружения, частота ложноположительных срабатываний и вычислительные издержки, для оценки эффективности алгоритма.

2) Результаты и анализ

- **Анализ скорости приёма пакетов**: анализируется изменения скорости приёма пакетов (PRR), наблюдаемые во время моделируемых атак, демонстрируя способность алгоритма обнаруживать отклонения от нормального поведения.
- **Анализ энергопотребления**: анализ моделей энергопотребления интеллектуальных устройств подчёркивает способность алгоритма выявлять аномальное энергопотребление, указывающее на атаки.
- **Оценка двухэтапного подхода**: оценка эффективности предлагаемого подхода в рамках использования короткого промежутка времени для первоначального грубого обнаружения и более

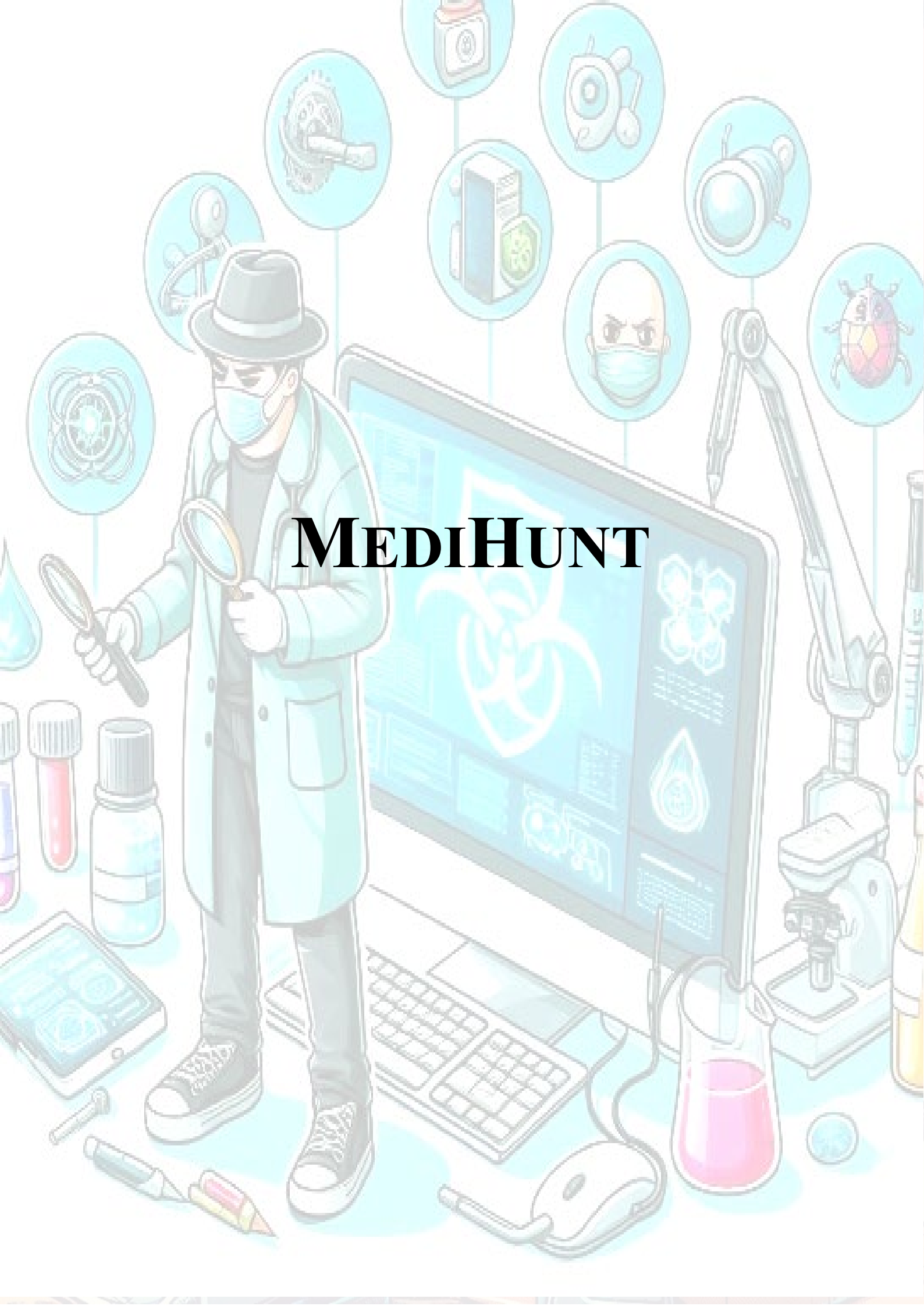
длительного промежутка времени для детального анализа, с точки зрения повышения точности обнаружения и уменьшения количества ложных срабатываний.

- **Наблюдения, относящиеся к конкретному протоколу**: Результаты могут включать наблюдения, относящиеся к различным протоколам связи (TCP, UDP, MQTT), использованным в экспериментах, и обсуждение их влияния на скорость приёма пакетов и структуру энергопотребления во время атак.
- **Оценка производительности**: оценка производительности алгоритма на основе определённых показателей, таких как точность обнаружения, частота ложноположительных срабатываний и вычислительные издержки, сравнивая её с существующими методами или базовыми показателями.

E. Заключение

В нем подчёркивается эффективность предлагаемой облегчённой системы обнаружения при выявлении кибератак на интеллектуальные устройства, связанных с потреблением энергии, подчёркивается её высокая точность обнаружения и низкий уровень ложноположительных результатов.

- **Краткое изложение выводов**: подчёркивается успешное использование скорости приёма пакетов (PRR) и моделей энергопотребления для обнаружения аномалий.
- **Производительность алгоритма**: подчёркивается высокая точность обнаружения и низкая частота ложных срабатываний, достигаемые двухэтапным подходом к обнаружению.
- **Масштабируемость и эффективность**: обсуждаются масштабируемость и эффективность фреймворка в реальных средах "умного дома", отмечается его пригодность для устройств Интернета вещей с ограниченными ресурсами.
- **Направления будущих исследований**: предлагаются направления будущих исследований:
  - Расширение фреймворка для охвата широкого спектра типов атак и умных устройств.
  - Усовершенствование алгоритма для повышения скорости обнаружения и снижения вычислительных затрат.
  - Интеграция дополнительных источников данных: сетевой трафик и журналы поведения устройств, для расширения возможностей обнаружения.
  - Использование передовых методов машинного обучения для дальнейшего повышения точности и надёжности системы обнаружения.
- **Сравнение с существующими методами**: сравнивается подход с существующими методами обнаружения аномалий, подчёркивая преимущества своего лёгкого двухэтапного метода с точки зрения точности, эффективности и пригодности для устройств с ограниченными ресурсами.
- **Практическое применение**: рассматриваются потенциальные практические применения платформы обнаружения, включая её внедрение в коммерческие системы "умного дома" и интеграцию с существующими решениями безопасности для обеспечения комплексной защиты от кибератак.



MEDIHUNT

Аннотация – В статье "MediHunt: A Network Forensics Framework for Medical IoT Devices" представлена разработка MediHunt, автоматической платформы сетевой криминалистики, предназначенной для обнаружения атак сетевого трафика на основе потоков в сетях MQTT, которые обычно используются в средах интеллектуальных больниц. MediHunt может обнаруживать различные атаки уровня TCP/IP и уровня приложений в сетях MQTT, используя модели машинного обучения. Платформа направлена на расширение возможностей криминалистического анализа в средах MIoT, обеспечивая эффективное отслеживание вредоносных действий и смягчение их последствий.

A. Введение

В документе "MediHunt: A Network Forensics Framework for Medical IoT Devices" рассматривается необходимость надёжной сетевой криминалистики в медицинских средах Интернета вещей (MIoT), особенно с упором на сети MQTT. Эти сети обычно используются в интеллектуальных больничных средах благодаря их облегчённому протоколу связи. Освещаются проблемы обеспечения безопасности устройств MIoT, которые часто ограничены в ресурсах и обладают ограниченной вычислительной мощностью. В качестве серьёзной проблемы упоминается отсутствие общедоступных потоковых наборов данных, специфичных для MQTT, для обучения систем обнаружения атак.

В документе представлен MediHunt как решение для автоматизированной сетевой криминалистики, предназначенное для обнаружения атак на основе сетевого трафика в сетях MQTT в режиме реального времени. Его цель – предоставить комплексное решение для сбора данных, анализа, обнаружения атак, представления и сохранения доказательств. Он разработан для обнаружения различных уровней TCP / IP и атак прикладного уровня в сетях MQTT и использует модели машинного обучения для расширения возможностей обнаружения и подходит для развёртывания на устройствах MIoT с ограниченными ресурсами.

B. Преимущества и недостатки предлагаемого решения

1) Преимущества

- **Обнаружение атак в режиме реального времени**: MediHunt предназначен для обнаружения атак на основе сетевого трафика в режиме реального времени для уменьшения потенциального ущерба и обеспечения безопасности сред MIoT.
- **Комплексные возможности криминалистики**: Платформа предоставляет комплексное решение для сбора данных, анализа, обнаружения атак, представления и сохранения доказательств. Это делает его надёжным инструментом сетевой криминалистики в средах MIoT.
- **Интеграция с машинным обучением**: Используя модели машинного обучения, MediHunt расширяет свои возможности обнаружения. Использование пользовательского набора данных, который включает данные о потоках как для атак уровня TCP/IP, так и для атак прикладного уровня, позволяет более точно и эффективно обнаруживать широкий спектр кибератак.
- **Высокая производительность**: решение показало высокую производительность, получив баллы F1 и точность обнаружения, превышающую 0,99 и указывает на то, что она обладает высокой надёжностью при обнаружении атак на сети MQTT.
- **Эффективность использования ресурсов**: несмотря на свои широкие возможности, MediHunt разработан с учётом экономии ресурсов, что делает его подходящим для развёртывания на устройствах MIoT с ограниченными ресурсами (raspberry Pi).

2) Недостатки

- **Ограничения набора данных**: хотя MediHunt использует пользовательский набор данных для обучения своих моделей машинного обучения, создание и обслуживание таких наборов данных может быть сложной задачей. Набор данных необходимо регулярно обновлять, чтобы охватывать новые и зарождающиеся сценарии атак.
- **Ограничения ресурсов**: хотя MediHunt разработан с учётом экономии ресурсов, ограничения, присущие устройствам MIoT, такие как ограниченная вычислительная мощность и память, все ещё могут создавать проблемы. Обеспечить бесперебойную работу фреймворка на этих устройствах без ущерба для их основных функций может быть непросто.
- **Сложность реализации**: Внедрение и поддержка платформы сетевой криминалистики на основе машинного обучения может быть сложной задачей. Это требует опыта в области кибербезопасности и машинного обучения, который может быть доступен не во всех медицинских учреждениях.
- **Зависимость от моделей машинного обучения**: Эффективность MediHunt в значительной степени зависит от точности и надёжности его моделей машинного обучения. Эти модели необходимо обучать на высококачественных данных и

регулярно обновлять, чтобы они оставались эффективными против новых типов атак.

- **Проблемы с масштабируемостью**: хотя платформа подходит для небольших развёртываний на устройствах типа Raspberry Pi, ее масштабирование до более крупных и сложных сред MIoT может вызвать дополнительные проблемы. Обеспечение стабильной производительности и надёжности в более крупной сети устройств может быть затруднено

C. MediHunt в сравнении с другими решениями

MediHunt выделяется среди фреймворков сетевой криминалистики, особенно в контексте медицинских сред Интернета вещей (MIoT), благодаря своей специализированной направленности, производительности и точности. При сравнении MediHunt с другими сетевыми криминалистическими фреймворками подчёркивается его уникальность и эффективность:

- **Специализированный фокус на MIoT**: В отличие от многих общих фреймворков сетевой криминалистики, MediHunt разработан специально для домена MIoT. Такая специализация позволяет ИТ-отделу решать уникальные задачи и требования, предъявляемые к медицинским устройствам Интернета вещей, таким как ограниченность ресурсов и необходимость обнаружения атак в режиме реального времени.
- **Обнаружение атак в режиме реального времени**: способность MediHunt обнаруживать атаки в режиме реального времени является значительным преимуществом. Эта функция имеет решающее значение для сред MIoT, где своевременное обнаружение может предотвратить потенциальный вред пациентам и медицинским операциям. Хотя обнаружение в режиме реального времени является целью многих фреймворков, MediHunt's адаптирована к ограниченному характеру устройств MIoT, обеспечивая минимальное влияние на производительность устройства.
- **Производительность и точность**: MediHunt демонстрирует исключительную производительность и точность при обнаружении сетевых атак. Благодаря баллам F1 и точности обнаружения, превышающей 0,99, он превосходит многие существующие платформы по своей способности точно выявлять вредоносные действия без высокого уровня ложных срабатываний. Такой уровень точности особенно важен в медицинских учреждениях, где ложные срабатывания могут иметь серьёзные последствия.
- **Эффективность использования ресурсов**: несмотря на свои широкие возможности, MediHunt разработан с учётом экономии ресурсов, что делает его подходящим для развёртывания на устройствах MIoT с ограниченными ресурсами. Это контрастирует с некоторыми другими фреймворками, которые могут требовать более значительных вычислительных ресурсов, что делает их менее жизнеспособными для развёртывания в сценариях MIoT.
- **Интеграция с машинным обучением**: MediHunt использует модели машинного обучения для расширения возможностей обнаружения атак. В то время как другие фреймворки также используют машинное обучение, подход MediHunt специально разработан для типов атак, распространенных в сетях MIoT, с использованием пользовательского набора данных, который включает данные потока как для атак уровня TCP / IP, так и для атак прикладного уровня.
- **Набор данных и обучение модели**: Пользовательский набор данных для обучения моделей машинного обучения - ещё один аспект, в котором выделяется MediHunt. Многие фреймворки сталкиваются с нехваткой всеобъемлющих наборов данных для обучения, особенно в контексте MIoT. MediHunt устраняет этот пробел, используя набор данных, охватывающий широкий спектр сценариев атак, имеющих отношение к средам MIoT

D. Предыдущие исследования

1) Обзор существующих систем криминалистики

Освещаются сильные стороны и ограничения существующих фреймворков. Например, традиционные системы цифровой криминалистики хорошо зарекомендовали себя и широко использовались в различных контекстах, но они часто оказываются несостоятельными при применении к уникальным и сложным средам систем интернета вещей. Обсуждаемые фреймворки включают те, которые ориентированы на криминалистику устройств, сетевую криминалистику экспертизу и облачную криминалистику, каждая из которых имеет свой собственный набор методологий и инструментов, предназначенных для решения конкретных задач криминалистики.

2) Проблемы криминалистики MIoT

Подчёркиваются уникальные проблемы, с которыми сталкивается криминалистика в области медицинского интернета вещей (MIoT). Одной из основных проблем является ограниченность ресурсов устройств MIoT, которые часто имеют ограниченную вычислительную мощность, память и возможности хранения данных. Это затрудняет внедрение традиционных инструментов и методов криминалистики. Кроме того, существует значительная нехватка полных наборов данных для обучения моделей машинного обучения, которые имеют решающее значение для эффективного обнаружения атак и криминалистического анализа. Неоднородность устройств MIoT с их различными операционными системами, протоколами связи и форматами данных усложняет процесс криминалистики.

3) Сравнение с традиционной криминалистикой

Проводится сравнение между традиционной цифровой криминалистикой и криминалистикой Интернета вещей. Традиционная цифровая криминалистика обычно имеет дело с чётко определёнными и однородными средами,

такими как персональные компьютеры и серверы, где могут быть эффективно применены стандартные инструменты и методы. Напротив, криминалистике Интернета вещей приходится иметь дело с крайне неоднородной средой и ограниченными ресурсами. Обычные инструменты криминалистики часто неадекватны для систем Интернета вещей, которые требуют специализированных подходов для работы с разнообразным и динамичным характером устройств и сетей Интернета вещей.

4) Использование машинного обучения

Обсуждается применение методов машинного обучения (ML) в сетевой криминалистике, в частности, для обнаружения и анализа аномалий сетевого трафика. Машинное обучение обладает значительным потенциалом для повышения точности и эффективности forensics-исследований за счёт выявления закономерностей и аномалий в сетевом трафике, которые могут указывать на вредоносную активность. Эффективность моделей ML в зависит от доступности высококачественных наборов данных, охватывающих широкий спектр сценариев атак, особенно адаптированных к характеристикам систем Интернета вещей на основе MQTT.

5) Существующие наборы данных

Представлен обзор существующих наборов данных, используемых для обучения моделей машинного обучения в сетевой криминалистике. Эти наборы данных имеют решающее значение для разработки и валидации ML-моделей, но они часто имеют ограничения с точки зрения разнообразия и всесторонности. Многие существующие наборы данных неадекватно отражают разнообразие сценариев атак в системах Интернета вещей на основе MQTT, что ограничивает эффективность обученных моделей. В этом разделе подчёркивается важность разработки более полных и репрезентативных наборов данных для повышения эффективности криминалистических инструментов, основанных на ML.

6) Степень разработанности темы

Выявляются пробелы в текущей литературе (степень научно-практической разработанности темы) по криминалистике MIoT. Одним из ключевых пробелов является потребность в возможностях обнаружения атак в режиме реального времени, которые необходимы для оперативного выявления и смягчения угроз в средах MioT и усовершенствованных методах сохранения forensics-доказательств, гарантирующих, что они останутся нетронутыми и допустимыми в ходе forensics-исследования. Устранение этих пробелов имеет решающее значение для развития области цифровой MIoT-криминалистики и повышения безопасности и надёжности медицинских систем Интернета вещей.

E. Предлагаемая система сетевой криминалистики

- **Разработка фреймворка**: MediHunt разработан для решения конкретных задач сетевой криминалистики в средах MIoT с особым упором на протокол MQTT. Он направлен на обнаружение атак в режиме реального времени и сохранение необходимых журналов для последующего анализа.
- **Обнаружение атак в режиме реального времени**: Способность обнаруживать кибератаки по мере их возникновения имеет решающее значение для уменьшения потенциального ущерба и немедленного начала forensics-исследования.
- **Механизм хранения журналов**: Учитывая ограниченность памяти устройств MIoT, MediHunt включает эффективный механизм хранения журналов, что гарантирует доступность журналов, относящихся к обнаруженным атакам, для анализа без перегрузки ёмкости хранилища.
- **Интеграция с машинным обучением**: MediHunt использует методы ML для расширения возможностей обнаружения атак. Он использует пользовательский набор данных, который включает данные потока как для атак уровня TCP / IP, так и для атак прикладного уровня, устраняя нехватку наборов данных для систем интернета вещей на основе MQTT.
- **Набор данных и обучение модели**: Пользовательский набор данных, используемый в MediHunt, охватывает широкий спектр сценариев атак, позволяя обучать модели ML распознавать различные типы кибератак. Шесть различных моделей ML были обучены и оценены на предмет их эффективности при обнаружении атак в режиме реального времени.
- **Показатели производительности**: Эффективность MediHunt количественно измеряется с использованием баллов F1 и точности обнаружения, и достигнутая высокая производительность превышает 0,99, что указывает на её надёжность при обнаружении атак в сетях MQTT.
- **Комплексный криминалистический анализ**: помимо обнаружения атак, MediHunt облегчает процесс комплексного анализа. Он поддерживает сбор, анализ, представление и сохранение цифровых доказательств в соответствии с принципами сетевой криминалистики.
- **Эффективность использования ресурсов**: MediHunt разработан с учётом экономии ресурсов, что делает его подходящим для развёртывания на устройствах MIoT с ограниченными ресурсами.

F. Обучение ML-модели

1) Сбор данных о сетевом трафике MQTT

- **Типы собираемых данных**: Собираемые данные включают как обычный трафик, так и трафик атаки. Это гарантирует, что набор данных является всеобъемлющим и может быть использован для эффективного обучения моделей машинного обучения.
- **Данные на основе потоков**: сбор данных на основе потоков включает информацию о потоках связи между устройствами. Этот тип данных имеет решающее значение для обнаружения аномалий и атак в сетевом трафике.
- **Сценарии атак**: сценарии произвольных атак моделируются для генерации атакующего трафика

и включают атаки TCP / IP и прикладного уровня, специфичные для MQTT.

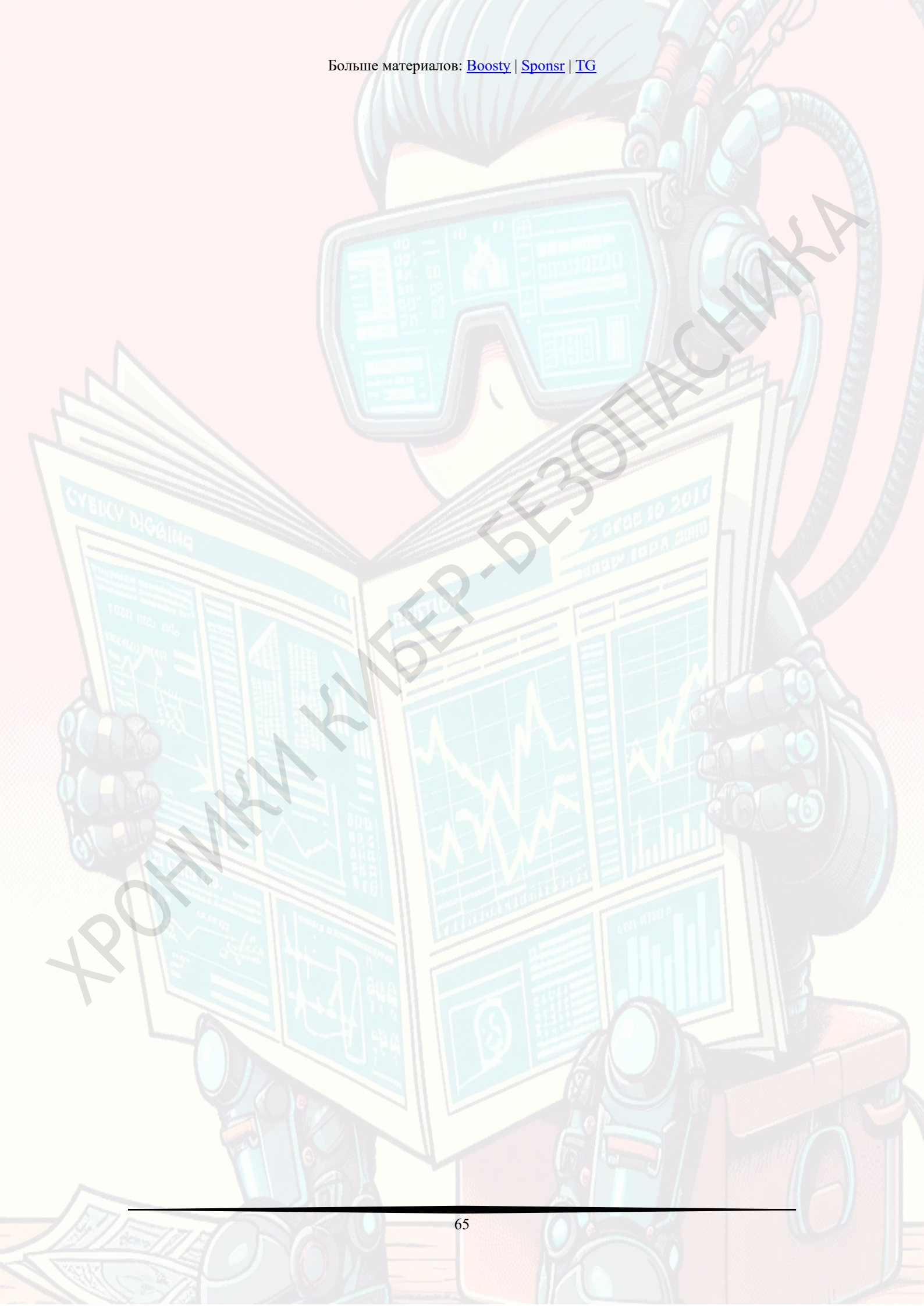
- **Генерация набора данных**: Собранные данные обрабатываются для создания набора данных, который может быть использован для обучения моделей машинного обучения. Этот набор данных включает помеченные экземпляры как обычного трафика, так и трафика атаки.

2) Обучение модели ML и анализ эффективности

- **Модели машинного обучения**: оцениваются шесть различных моделей, включая деревья принятия решений, случайные леса, машины опорных векторов и нейронные сети.
- **Процесс обучения**: Процесс обучения включает использование сгенерированного набора данных для обучения моделей машинного обучения. Модели обучены распознавать закономерности в данных, которые указывают на нормальный трафик или трафик атаки.
- **Показатели производительности**: Производительность обученных моделей оценивается с использованием таких показателей, как оценка F1 и точность обнаружения, которые обеспечивают количественный показатель эффективности моделей при обнаружении атак.
- **Высокая производительность**: достигаются баллы F1, а точность обнаружения превышает 0.99, что подтверждает эффективность обнаружения атак в режиме реального времени.
- **Обнаружение в режиме реального времени**: t обученные модели интегрированы в платформу MediHunt для обеспечения обнаружения атак в режиме реального времени. Это позволяет незамедлительно реагировать и смягчать потенциальные угрозы.

G. Оценка на Raspberry Pi

- **Реализация на Raspberry Pi**: проанализирована производительность алгоритмов машинного обучения (ML) на моделях Raspberry Pi 3B для реализации платформы сетевой криминалистики MediHunt на устройствах MIoT с ресурсами.
- **Сопоставимое время вывода и обучения**: Оценка показала, что время вывода и обучения алгоритмов ML были сопоставимы на устройствах Raspberry Pi. В частности, время вывода на облачной платформе составляло около 2 мс, в то время как на Raspberry Pi оно составляло 0,17 мс.
- **Легковесная обнаружения вторжений**: MediHunt описывается как облегчённое решение для обнаружения вторжений, разворачиваемое на ограниченных ресурсами устройствах (Raspberry Pi).
- **Обнаружение атак в режиме реального времени**: подчёркивается способность платформы обнаруживать атаки в режиме реального времени, обеспечивая немедленное реагирование и смягчение потенциальных угроз.
- **Эффективное использование ресурсов**: несмотря на широкие возможности для сетевой криминалистики, платформа MediHunt разработана с учётом экономии ресурсов, что делает её подходящей для развёртывания на устройствах MIoT с ограниченными ресурсами, таких как Raspberry Pi.



Рубрика: Исследование

FUXNET

Аннотация – в документе представлен анализ Fuxnet, приписываемого хакерской группе Blackjack, которое, как сообщается, нацелено на инфраструктуру отдельных стран. Анализ включает в себя различные аспекты вредоносного ПО, включая его технические характеристики, влияние на системы, механизмы защиты, методы распространения, цели и мотивы, стоящие за его внедрением. Изучив эти аспекты, цель документа-обеспечить подробный обзор Fuxnet по возможности и её значение для кибербезопасности.

Документ предлагает качественное описание Fuxnet, основанное на информации, которой публично доступной от экспертов по кибербезопасности. Этот анализ полезен для специалистов в области ИБ, ИТ-специалистов и заинтересованных сторон в различных отраслях, поскольку он не только проливает свет на технические тонкости сложной киберугрозы, но и подчёркивает важность надёжных мер кибербезопасности для защиты критически важной инфраструктуры от возникающих угроз. Документ способствует более широкому пониманию тактики ведения кибервойны и повышает готовность организаций к защите от подобных атак в будущем.

A. Введение

Хакерская группа Blackjack, предположительно связанная с украинскими спецслужбами, взяла на себя ответственность за кибератаку, которая якобы поставила под угрозу возможности обнаружения чрезвычайных ситуаций и реагирования на них в прилегающих районах РФ. Эта группа была связана с предыдущими кибератаками, направленными против интернет-провайдеров и военной инфраструктуры. Их последнее заявление касается нападения на компанию, отвечающую за строительство и мониторинг инфраструктуры подземных вод, канализации и коммуникаций.

Группа распространила подробную информацию об атаке на веб-сайте ruexfil[.]com, включая использование Fuxnet, включая скриншоты систем мониторинга, серверов и баз данных, которые, по их утверждению, были удалены и выведены из строя, а также дампы паролей.

Основные выводы из анализа Fuxnet, в т.ч. из материалов Team82 и Claroty:

- **Неподтверждённые заявления**: Team82 и Claroty не смогли подтвердить заявления относительно влияния кибератаки на возможности правительства по реагированию на чрезвычайные ситуации или степени ущерба, причинённого Fuxnet.
- **Несоответствие в сообщениях о воздействии**: первоначальное утверждение о 2659 сенсорных шлюзов не совпали с информацией об атаке 1700. А проведённый Team82 анализ показывает, что только немногим более 500 были фактически затронуты Fuxnet. На это последовали заявление Blackjack об выведено из строя 87000 датчиков также было разъяснено, заявив, что они отключили датчики, «уничтожив шлюзы путём фаззинга», а не физическое уничтожение датчиков.
- **Фаззинг M-Bus**: метод был направлен на отключение датчиков, но точное количество датчиков оказалось невозможно установить ввиду их недоступности извне.
- **Отсутствие прямых доказательств**: отсутствуют прямые доказательства, подтверждающие масштабы ущерба или влияние на возможности обнаружения чрезвычайных ситуаций и реагирования на них в т.ч. о Москоллектор.
- **Разъяснение от Blackjack**: после публикации первоначального анализа Team82 Blackjack обратилась с просьбой предоставить разъяснения, в частности, оспорив утверждение о том, что было затронуто только около 500 сенсорных шлюзов и обнародованные файлы JSON были лишь примером полного объёма их деятельности.

B. Отрасли и последствия

1) Возможные отрасли:

- **Коммунальные службы**: Основной целью Fuxnet был сектор коммунальных услуг, в частности сенсорные шлюзы, управляющие системами водоснабжения и канализации. Это может иметь последствия для предоставления этих основных услуг и мониторинга за ними.
- **Службы экстренной помощи**: Группа утверждала, о получении доступ к службе экстренной помощи 112, что могло повлиять на способность эффективно реагировать на чрезвычайные ситуации.
- **Транспорт**: Группа также утверждала, что вывела из строя датчики и контроллеры в критически важных объектах инфраструктуры, включая аэропорты и метро, что могло нарушить транспортное обслуживание и безопасность.
- **Энергетика**: В качестве ещё одной цели были упомянуты газопроводы, что указывает на потенциальный риск для систем распределения энергии и мониторинга.

2) Возможные последствия:

- **Нарушение работы служб**: Разрушение или неисправность сенсорных шлюзов может привести к нарушению работы систем мониторинга и управления коммунальными службами, что потенциально может привести к перебоям в обслуживании.
- **Нарушение безопасности**: В транспортном и энергетическом секторах потеря функциональности датчиков может представлять угрозу безопасности, поскольку эти датчики часто имеют решающее значение для обнаружения опасных условий.
- **Экономический эффект**: Потенциальные простои и затраты на ремонт, связанные с заменой или перепрошивкой повреждённых шлюзов датчиков, могут иметь значительные экономические последствия для затронутых отраслей.
- **Задержки с реагированием на чрезвычайные ситуации**: может привести к задержкам в реагировании на чрезвычайные ситуации, что повлияет на общественную безопасность.
- **Утечка данных**: возможная компрометация сетевые системы потенциально может привести к утечке данных и утечке конфиденциальной информации.
- **Потеря общественного доверия**: может привести к потере общественного доверия к сервисам и организациям, ответственным за их безопасность.

C. Moscollector-атака

Недавно группа обнародовала свою деятельность и украденную информацию на веб-сайте ruexfil, подробно описав масштабы и последствия своего кибератаки. Выход из строя этой системы потенциально может привести к нарушению возможностей реагирования на чрезвычайные ситуации, что скажется на безопасности населения.

1) Установка датчиков и контроллеров критически важной инфраструктуры

Группа утверждает о взломе датчиков и контроллеров в критически важных секторах инфраструктуры, включая аэропорты, метро и газопроводы. Это действие, если оно было реальным, могло привести к отключению основных систем мониторинга и контроля, что привело бы к значительным сбоям в работе общественных служб и обеспечении безопасности.

2) Сбой в работе сетевого устройства

Группа утверждает, что они отключили сетевые устройства, такие как маршрутизаторы и брандмауэры. Это оказало бы каскадное воздействие на целостность сети, потенциально изолировав различные сегменты и затруднив коммуникацию в инфраструктуре.

3) Удаление серверов и баз данных

Злоумышленники утверждают, что удалили серверы, рабочие станции и базы данных, уничтожив около 30 ТБ данных, включая диски резервных копий. Такого рода уничтожение данных может привести к потере исторических данных, нарушению текущих операций и усложнению усилий по восстановлению.

4) Аннулирование доступа в офисное здание

Все карточки-ключи от офисного здания, как сообщается, признаны недействительными. Это действие может помешать сотрудникам получить доступ к своему рабочему месту, что ещё больше затруднит любые попытки оценить ущерб или запустить протоколы восстановления.

5) Сброс пароля

Также было заявлено о сбросе паролей из нескольких внутренних служб, что могло быть повлечь несанкционированный доступ к различным системам и данным, усугубляя последствия взлома и потенциально приводя к дальнейшей эксплуатации.

D. Набор юного атакующего

Основное внимание было уделено коммуникационным шлюзам, которые служат критическими узлами для передачи данных от датчиков к глобальным системам мониторинга. Эти датчики являются неотъемлемой частью различных систем мониторинга окружающей среды, в том числе используемых в пожарной сигнализации, газовом мониторинге и системах управления освещением.

Датчики предназначены для сбора физических данных, таких как температура, и передачи этой информации по последовательному соединению или шине, в частности по шине RS485/Meter-Bus, на шлюз. Эти шлюзы действуют как узлы передачи, позволяя передавать телеметрические данные через Интернет в централизованную систему мониторинга, которая обеспечивает операторам видимость и контроль над системами.

Стандарт связи RS485, как упоминалось в деталях атаки, является широко распространённым протоколом для промышленных систем управления благодаря своей надёжности и возможностям связи на большие расстояния. Это позволяет нескольким устройствам взаимодействовать по единой системе шин, что важно для централизованного мониторинга различных датчиков и контроллеров.

Шина M-Bus — это протокол связи, используемый для сбора и передачи данных о потреблении, обычно для коммунальных услуг, таких как электричество, газ, вода или тепло. В сочетании с RS485 он образует надёжную сеть, позволяющую промышленным датчикам передавать информацию в центральные системы.

Компрометируя шлюзы, можно потенциально нарушить передачу телеметрии и управление датчиками, что приведёт к потере оперативной видимости и потенциально вызовет хаос в системах, которые полагаются на эти данные.

1) Утечка информации

Информация из файлов JSON была подтверждена двумя видеороликами на YouTube, демонстрирующими развёртывание Fuxnet. Устройства, перечисленные в видеороликах, соответствовали шлюзам из файла JSON, подтверждая, что шлюзы TMSB / MPSB были основными целями Fuxnet.

Данные включали типы и названия устройств, IP-адреса, порты связи и данные о местоположении. В файле JSON были перечислены следующие типы устройств:

- MPSB (шлюз датчиков): 424 устройства
- TMSB (сенсорный шлюз+модем): 93 устройства
- IBZ (3g-маршрутизатор): 93 устройства
- Windows 10 (рабочая станция): 9 устройств
- Windows 7 (рабочая станция): 1 устройство
- Windows XP (рабочая станция): 1 устройство

Этот список указывает на то, что атака была сосредоточена на сенсорных шлюзах, а не на самих конечных датчиках. Шлюзы служат узлами связи для потенциально многочисленных датчиков, подключённых по последовательной шине, такой как RS485/Meter-Bus.

Утечка данных, включая скриншоты и экспорт в формате JSON, выявила два конкретных типа шлюзов, скомпрометированных во время атаки:

- **Шлюз MPSB**: Этот шлюз разработан для обмена информацией с внешними устройствами через несколько интерфейсов. Он поддерживает Ethernet и протоколы последовательной связи, включая CAN, RS-232 и RS-485. Шлюз MPSB является важнейшим компонентом для интеграции различных входных данных датчиков в единую систему мониторинга.
- **Шлюз TMSB**: Аналогичный по функциям MPSB, шлюз TMSB включает встроенный модем 3G / 4G, который позволяет передавать данные непосредственно через Интернет в удалённую систему без необходимости в дополнительном маршрутизирующем оборудовании.

Кибератака была нацелена на критически важную часть экосистемы датчиков: устройств оркестраторов / шлюзов, в частности шлюзы MPSB и TMSB. Эти устройства необходимы для считывания показаний основных датчиков ввода-вывода и управления ими, а также для передачи данных в глобальную систему мониторинга для централизованного надзора.

В ходе атаки использовались каналы связи между датчиками и глобальной системой мониторинга:

- **Для шлюза MPSB**: **Датчик —--- MBus/RS485 → MPSB + IoT роутер —---Интернет→ Система мониторинга.** данные датчика передаются через MBus/ RS485 на шлюз MPSB, который затем передает данные через маршрутизатор Интернета вещей в Интернет и, наконец, в систему мониторинга.
- **Для шлюза TMSB**: **Датчик —---- MBus/RS485 → TMSB (3g/4g модем) ----Интернет → Система мониторинга.** данные датчика передаются через MBus/ RS485 непосредственно на шлюз TMSB, который использует встроенный модем для передачи данных через Интернет в систему мониторинга.

2) Ошибки в системе безопасности и методология атак

Значительный недостаток в системе безопасности: использованием учётных данных по умолчанию (имя пользователя: sbk, пароль: temppwd) для доступа к шлюзам через SSH. Эта уязвимость позволила злоумышленникам легко скомпрометировать устройства.

Злоумышленники также опубликовали скриншоты из пользовательского интерфейса управления датчиками, демонстрирующие топологию сети.

Помимо модуля TMSB со встроенными возможностями 3/4G, злоумышленники упомянули использование роутеров iRZ RL22w. Эти маршрутизаторы, использующие OpenWRT использовались в качестве интернет-шлюзов для подключения датчиков к Интернету через 3G.

Сообщается, что злоумышленники использовали SSH для подключения к этим устройствам Интернета вещей и туннелирования к внутренним устройствам, вероятно, после получения паролей root. Поисковые запросы Shodan и Censys показали, что тысячи маршрутизаторов iRZ доступны в Интернете, при этом около 4100 устройств напрямую предоставляют свои услуги и около 500 подключены к Telnet.

3) Программное обеспечение для управления датчиками и ввода их в эксплуатацию:

ПО подключается к устройствам с использованием проприетарного протокола, который работает через порт TCP 4321. Интерфейс позволяет получать доступ к настройкам датчиков и изменять их, включая конфигурации ввода / вывода, узлы и показания. Эта возможность необходима для надлежащей настройки и обслуживания сенсорных сетей, гарантируя их эффективную и точную работу в назначенных условиях.

Особенности программного обеспечения:

- **Подключение устройства**: используется проприетарный протокол поверх TCP/4321 для установления безопасного соединения с датчиками.
- **Возможности настройки**: параметры датчиков, включая корректировку их рабочих параметров и управление данными, которые они собирают.
- **Пользовательский интерфейс**: интерфейс предоставляет средства взаимодействия с подключёнными датчиками

4) Техническое воздействие

Система мониторинга датчиков является важным компонентом инфраструктуры, предназначенной для. Эта система предназначена для объединения и отображения телеметрии и отчётов о состоянии, поступающих от сети датчиков, позволяя системным операторам получать оповещения в режиме реального времени, регистрировать данные и удалённо управлять датчиками.

Согласно заявлениям, группа успешно взломала эту систему мониторинга и получили доступ к полному списку управляемых датчиков и смогли географически сопоставить эти датчики на карте. Это раскрыло конфиденциальные оперативные данные, позволило

манипулировать выходными данными датчиков для нарушения их работы:

- **Функции геолокации**: Система мониторинга имеет геолокационные метки, которые помогают визуализировать физическое расположение датчиков по всей сети. Эта функция особенно полезна при крупномасштабных операциях, когда датчики разбросаны по обширным площадям.
- **Мониторинг конкретного объекта**: скриншоты из системы показывают, что она способна фокусироваться на конкретных объектах, таких как больницы, что указывает на её использование в критически важных инфраструктурных объектах, где точный мониторинг необходим для обеспечения безопасности и работоспособности.

E. Анализ Fuxnet

Логические процессы, выявленные в поведении Fuxnet, включают несколько шагов, направленных на нанесение необратимого ущерба целевым устройствам.

- Fuxnet была специально разработана для атаки на сенсорные шлюзы и их выведения из строя, а не на конечные датчики.
- Действия вредоносного ПО включали блокировку устройств, «уничтожение» файловых систем, чипов NAND и томов UBI, а также флуд в каналах связи.
- Атаке, вероятно, способствовало использование учётных данных по умолчанию и уязвимостей в протоколах удалённого доступа.
- Несмотря на заявления о компрометации 87 000 устройств, фактическое воздействие, по-видимому, ограничено сенсорными шлюзами, а конечные датчики, вероятно, остались нетронутыми.

1) Сценарий развёртывания

Злоумышленники составили полный список IP-адресов сенсорных шлюзов, на которые они намеревались напасть, наряду с подробными описаниями физического местоположения каждого датчика. Затем вредоносная программа была распространена среди каждой цели, вероятно, с использованием протоколов удалённого доступа, таких как SSH или проприетарный протокол SBK sensor protocol, через TCP-порт 4321.

2) Блокировка устройств и «уничтожение» файловой системы

После запуска на целевом устройстве Fuxnet инициировала процесс его блокировки. Повторное монтирование файловой системы с доступом на запись приводилось к удалению критически важных файлов и каталогов. Fuxnet также отключал службы удалённого доступа, включая SSH, HTTP, telnet и SNMP, эффективно предотвращая любые попытки удалённого восстановления. Кроме того, Fuxnet удалила таблицу маршрутизации устройства, что привело к нарушению его коммуникационных возможностей.

3) «Уничтожение» чипов NAND

Вывод из строя достигался путём выполнения операции изменения битов на участках чипа SSD NAND, многократно записывая и перезаписывая память до полного отказа чипа, так как память NAND имеет ограниченное количество циклов записи.

4) Разрушающий томов UBI

Чтобы предотвратить перезагрузку датчика, Fuxnet переписывает том UBI используя интерфейс IOCTL UBI_IOCVOLUP, чтобы заставить ядро ожидать, что будет записано большее количество байт, чем фактически отправлено было на запись, в результате чего устройство зависало на неопределённый срок. Затем вредоносная программа перезаписала том UBI ненужными данными, дестабилизируя файловую систему.

5) Отказ в обслуживании при мониторинге

Последним шагом в процессе работы вредоносного ПО было нарушение связи между шлюзами датчиков и самими датчиками. Fuxnet замусорила каналы RS485 / Meter-Bus случайными данными, перегружая шину и датчики, что предотвратило передачу и приём данных датчиками и шлюзами, сделав процесс сбора данных бесполезным.

6) Стратегия фаззинга M-Bus

Стратегия включала постоянную отправку данных M-Bus по последовательному каналу RS485 с целью перегрузки и потенциального повреждения датчиков, подключённых к этой сети.

- **Случайный фаззинг**: формирование случайных байт и отправку их по M-Bus с добавлением простого CRC, чтобы гарантировать, что данные не будут проигнорированы. Цель состояла в том, чтобы охватить весь диапазон возможных полезных нагрузок M-Bus, действительных или нет, в надежде вызвать неисправности датчиков или уязвимости.
- **Структурированный фаззинг**: формирование допустимых данных с изменением определённых полей в протоколе. Более точно придерживаясь структуры M-Bus, была увеличена вероятность того, что датчик сочтёт пакет действительным и полностью проанализирует его, тем самым увеличив шансы срабатывания уязвимости.