УДК 004.492
DOI 10.33764/2618-981X-2022-6-192-196

Исследование прошивок PON-роутеров на предмет программных закладок

Д. Е. Пешков[1], А. В. Шабурова[1]*

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: peshkowdima@yandex.ru

Аннотация. Сетевые маршрутизаторы — это неотъёмная часть любой корпоративной и домашней сети. Количество устройств в сети организации может исчисляться десятками и не всегда удается следить за актуальностью версий или их безопасностью. Этим зачастую и пользуются злоумышленники и недобросовестные производители. И чтобы не предотвращать последствия атаки хакеров, нужно своевременно осуществлять деятельность для обеспечения информационной безопасности. И начать нужно с сетевых устройств и с их многообразия. У каждого такого устройства есть прошивка, которую специалисты могут проверить и обнаружить в ней как уязвимости, так и спланированно заложенные программные закладки, например бекдоры, шеллы или же ботнеты. Для упрощения и ускорения этой работы можно использовать сканер прошивок.

Ключевые слова: сеть, сетевая безопасность, маршрутизатор, PON, прошивка, бекдор

Research of firmware of PON routers for software bookmarks

D. E. Peshkow[1], A. V. Shabrova[1]*

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: peshkowdima@yandex.ru

Abstract. Network routers are an integral part of any corporate and home network. The number of devices in an organization's network can number in the dozens and it is not always possible to monitor the relevance of versions or their security. This is often used by malefactors and unscrupulous manufacturers. And in order not to prevent the consequences of a hacker attack, it is necessary to carry out activities in a timely manner to ensure information security. And you need to start with network devices and their diversity. Each such device has a firmware that specialists can check and detect both vulnerabilities and planned software bookmarks, such as backdoors, in it. To simplify and speed up this work, you can use a firmware scanner.

Keywords: network, network security, router, PON, firmware, backdoor

Введение

Нарушение целостности данных и программного обеспечения всегда было большой угрозой для информационной инфраструктуры [1]. Достаточно вспомнить только хакерскую атаку шифровальщика PETYA, который по мнению кибер-полиции начался через механизм обновления бухгалтерского программного обеспечения. А ведь данный шифровальщик появился в 2016 – 2017 году, тогда была зафиксирована наиболее активная его работа.

Однако целью хакерских атак может стать не только крупный вендор программного обеспечения, у которого явно имеются всевозможное средства защиты, но и рядовой пользователь интернета, который редко задумывается о своей сетевой безопасности [2].

Целью статьи является исследование программного обеспечения, с помощью которого в прошивку роутеров и других сетевых устройств может быть внедрена вредоносная полезная нагрузка.

Методика исследования

Для достижения поставленных целей будет изучены практики защиты от данного рода уязвимостей в OWASP Top 10, в который в 2021 году добавили уязвимость [3] «нарушение целостности данных и программного обеспечения». Далее для демонстрации и эмуляции прошивки сетевого устройства будет использован скрипт, который позволяет внедрять вредоносную полезную нагрузку. В результате будет получена прошивка роутера с программной закладкой.

Сканирование прошивок роутеров на предмет программных закладок

О нарушение целостности данных так же задумались в OWASP. Open Web Application Security Project – это открытый проект обеспечения безопасности веб-приложений [4]. Сообщество OWASP включает в себя корпорации, образовательные организации и частных лиц со всего мира. Раз в несколько лет OWASP выпускает документ OWASP Top 10 — это отчет, в котором перечислены основные проблемы, связанные с безопасностью веб-приложений. Он регулярно обновляется, чтобы постоянно отображать 10 наиболее серьезных рисков, с которыми сталкиваются организации. OWASP рекомендует всем компаниям учитывать выводы документа при построении корпоративных процессов, чтобы минимизировать и смягчить актуальные риски безопасности [5]. И в 2021 году в этот топ попала такая уязвимость как «Нарушение целостности данных и программного обеспечения», что может свидетельствовать о действительной распространённости и критичности этой уязвимости, и что данная уязвимость используется хакерами для атак на информационные системы бизнеса, государства и рядового пользователя.

Наибольшая угроза всех хакерских атак – это их массовость, когда атакуется не конкретная цель, а сотни тысяч пользователей, которые ежедневно пользуются интернетом [6]. Но что же объединяет такое огромное количество пользователей, чтобы сделать атаку универсальной для всех них? Это их роутер – устройство, которое позволяет им всем выходить в сеть интернет.

Роутеры бывают разные, но в данной статье мы остановимся конкретно на PON-роутерах, как наиболее современных и удобный устройствах по части скорости.

Основная проблема всех роутеров – это их прошивка, а точнее ее не обновление [7]. Зачастую прошивки роутера не обновляются ни пользователями этих роутеров, ни их разработчиками. В лучшем случае вы можете сами скачать новую прошивку с сайта разработчика, но так поступают единицы. И даже найденные критичные уязвимости в прошивках не всегда получают своевременное об-

новление. А наличие все возможных программных закладок или бэкдоров не проверяется [8].

Для компрометации прошивки роутера злоумышленнику не нужны особые знания в написании кода, достаточно воспользоваться нужным программам решением [9].

Для внедрения вредоносной полезной нагрузки можно воспользоваться скриптом Router Post-Exploitation Framework, который был скачен с хранилища открытого кода github. Данный фреймворк достаточно просто использовать необходима только версия прошивки и сама вредоносная программная нагрузка, которая будет внедрена в прошивку (Рис. 6). В качестве прошивки для тестирования выла выбрана прошивка достаточно распространённого роутера Dlink DIR-601 (Рис. 7).

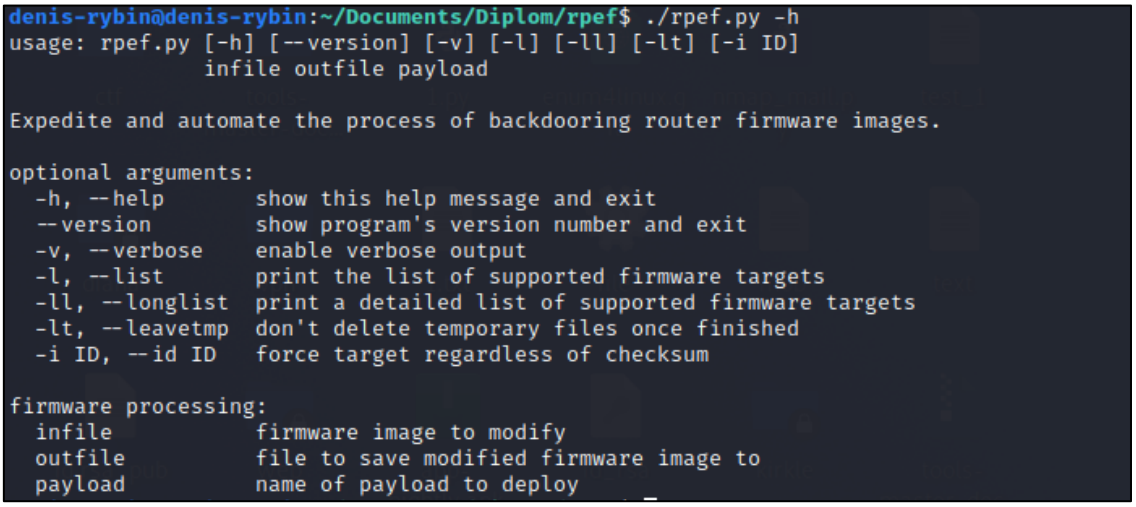

Рис. 6. Интерфейс скрипта rpef.py

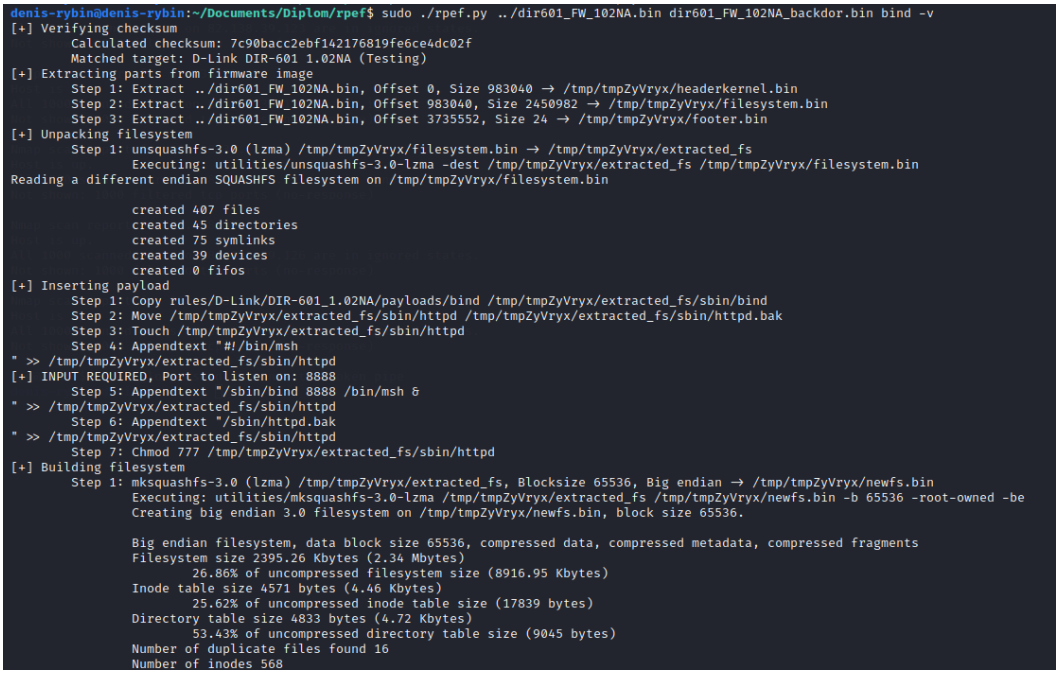

Рис. 7. Внедрение бэкдора в прошивку роутера

Этими действиями будет эмулирована прошивка с программными закладными устройствами, которая может присутствовать в каком-либо маршрутизаторе в сети дома или организации [10].

Для обнаружения такого рода специалисту закладок необходимо воспользоваться сканером исходного кода прошивок. Однако выполнить стандартными средствами это не представляется возможным. Также доступных программных решений не было найдено. Из чего следует что данная уязвимость может повлечь серьезные риски для безопасности сети.

Заключение

Отсутствие простой и быстрой реализации сканера прошивок для обнаружения закладных программных устройств создает угрозы для сетей личного, рабочего и общественного использования.

В ходе работы было исследовано программное обеспечение для внедрения программных закладок в прошивки сетевых устройств.

В работе планируется исправить это упущение и разработать простую и быструю программу сканирования и детектирования программах закладок и бэкдоров в коде прошивок PON-роутеров.

В ходе реализации программного продукта будут соблюдены следующие принципы:

- скорость работы;
- простота запуска;
- работа с большим количеством прошивок;
- работа на всех операционных системах.

Для осуществления всех поставленных целей будет разработана программа на языке программирования python3.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кизилов Е. А. Моделирование коммутаторов ethernet в промышленных сетях / Е. А. Кизилов, Н. Н. Коннов, В. Б. Механов // Новые информационные технологии и системы: сб. статей. – Пенза, 2014. – С. 326-329.

2. Казарин О. В. Безопасность программного обеспечения компьютерных систем. Москва, МГУЛ, 2003. – 212 с.

3. Кириллов А.С. Метод обнаружения и кластеризации вредоносного программного обеспечения с использованием признаков декларируемого и фактического функционала: автореф. дис. на соиск. учен. степ. канд. тех. наук (05.13.19) / Кириллов Алексей Сергеевич; ФГАОУВО Южный федеральный университет. – Таганрог, 2022. – 24 с.

4. Милославская, Н.Г. Визуализация процессов управления информационной безопасностью / Наталья Геннадьевна Милославская // Научная визуализация. - 2017. - Том 9, № 5. - С. 117-136. (дата обращений 23.03.2022).

5. ГОСТ Р «Защита информации. Мониторинг информационной безопасности. Общие положения». Проект [Электронный ресурс]: Веб-сайт / ФСТЭК России. - Режим доступа: https://fstec.ru/tk-362/standarty-tk362/303-proekty/1896-proekt-natsionalnogo-standarta-gost-r-4 (дата обращения: 17.04.2022).

6. Воронина А.А., Скрипина И.И. Предупреждение инцидентов нарушения информационной безопасности данных // Научный результат. Информационные технологии. – Т.6, №3, 2021 (дата обращения: 04.05.2022).

7. Вьющенко О.О., Маслова М.А. Об обеспечении безопасности в сфере интернета вещей // Научный результат. Информационные технологии. – Т.6, №3, 2021 (дата обращения: 29.04.2022).

8. Ревенков П.В., Бердюгин А.А. Кибербезопасность в условиях интернета вещей и электронного банкинга // Национальные проекты: приоритеты и безопасность. – Т.11, стр. 158-169, 2016 (дата обращения: 22.04.2022)

9. Вишняков Я.Д., Харченко С.А. Управление обеспечением безопасности предприятий: экономические подходы // Менеджмент в России и за рубежом. - №5, 2019 (дата обращения: 02.05.2022).

10. Гибилинда Р. В. Разработка автоматизированных методов анализа воздействий на файлы в задаче расследования инцидентов информационной безопасности: автореферат диссертации на соискание ученой степени кандидата технических наук / Гибилинда Роман Владимирович; учебно-научный центр «Информационная безопасность» Института радиоэлектроники и информационных технологий - РтФ ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина», Екатеринбург - 2021. – 21 с. – Библиогр.: с. 16–29. – Текст: автореф.дис (дата обращения: 12.05.2022).