УДК 528.71
DOI 10.33764/2618-981X-2025-6-65-69

А. С. Зонов[1]✉, А. В. Шабурова[1]

Сканер прошивок оптических роутеров: подходы к обнаружению программных закладок

[1]Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: alex301919@yandex.ru

Аннотация. Оптические роутеры (PON) занимают ключевое место в современных сетях, обеспечивая высокоскоростной доступ в интернет. Однако их прошивки часто содержат уязвимости или преднамеренно внедренные программные закладки, такие как бэкдоры, что создает риски для корпоративных и домашних сетей. В статье представлен метод разработки сканера прошивок, способного автоматизировать процесс выявления вредоносных внедрений. Инструмент реализован на языке Python3 и сочетает методы сравнения хэшей, статического анализа и эмуляции среды. Тестирование продемонстрировало эффективность сканера в обнаружении модифицированных прошивок, включая интеграцию reverse-shell и подозрительных ссылок на системные файлы. Результаты работы подчеркивают необходимость внедрения подобных решений для обеспечения безопасности IoT-устройств в условиях роста киберугроз.

Ключевые слова: PON, безопасность сети, аудит, маршрутизатор, статических анализ

A. S. Zonov[1]✉, A. V. Shaburova[1]

Firmware scanner for optical routers: approaches to detecting software implants

[1]Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: alex301919@yandex.ru

Abstract. Optical routers (PON) occupy a key place in modern networks, providing high-speed internet access. However, their firmware often contains vulnerabilities or deliberately embedded software implants, such as backdoors, which creates risks for corporate and home networks. The article presents a method for developing a firmware scanner capable of automating the detection of malicious implants. The tool is implemented in Python3 and combines hash comparison, static analysis, and environment emulation. Testing demonstrated the scanner's effectiveness in detecting modified firmware, including reverse-shell integration and suspicious references to system files. The results emphasize the necessity of implementing such solutions to ensure the security of IoT devices amid growing cyber threats.

Keywords: PON, network security, audit, router, static analysis

Введение

Оптические роутеры (PON) стали неотъемлемой частью современных сетей, обеспечивая высокоскоростной доступ в интернет для миллионов пользователей — от домашних хозяйств до крупных корпораций [1]. По данным Mordor Intelligence доля PON-устройств в структуре глобальных сетей активно возрастает,что связано с их высокой пропускной способностью и низкой задержкой [2]. Однако

массовое распространение этих устройств привело к повышенному интересу со стороны злоумышленников. Согласно актуальной статистике Positive Technologies на конец 2024 года большинство атак было направлено на серверы и сетевое оборудование, куда и входят атаки на оптические роутеры [3,4].

Особую опасность представляет цепочка поставок [5]. Производители и сторонние разработчики часто внедряют в прошивки скрытые функциональные элементы, такие как бэкдоры [6], для удаленного управления устройствами. Например, в некоторых роутеров TP-Link были обнаружены уязвимости, позволяющие реализовать удаленное выполнение команд [7]. Подобные случаи демонстрируют, что даже легальное оборудование может содержать преднамеренные закладки, что ставит под угрозу конфиденциальность данных и устойчивость сетей [8,9].

Разработанный сканер прошивок решает эти проблемы за счет комбинации методов проверки целостности и статического анализа. Инструмент позволяет обнаруживать сигнатуры бэкдоров и подозрительные системные вызовы, предупреждать пользователей о рисках исплоьзования уязвимых версий.

Методы и методики

Разработанный сканер прошивок базируется на комплексном подходе, объединяющем проверку целостности, статический анализ. Проверка целостности осуществляется через сравнение хэша SHA-256 анализируемой прошивки со значениями полученными с сайта производителя, что позволяет выявить несанкционированные изменения [10]. Статический анализ использует YARA-правила для поиска сигнатур бэкдоров, таких как подозрительные строки (например, /etc/passwd) или системные вызовы (execve, system) [11,12].

В качестве демонстрации работы сканера будет загружен бэкдор в прошивку оптического роутера, при этом внедрение бэкдора в прошивку включает несколько этапов. На первом этапе злоумышленник генерирует вредоносную нагрузку, например, reverse-shell, с использованием инструментов типа msfvenom (рис. 1) [13,14].

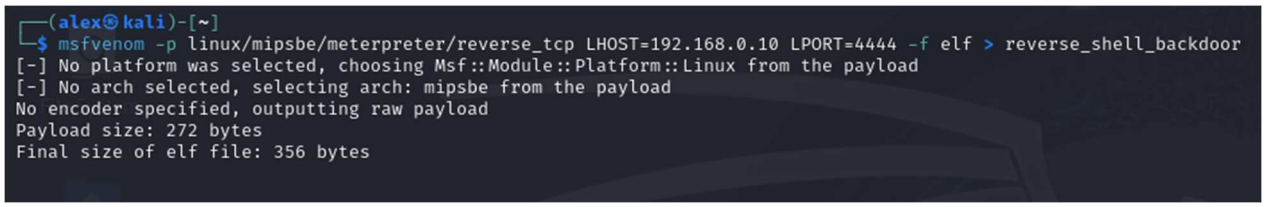

Рис. 1. Создание полезной нагрузки

Для архитектуры MIPS, характерной для PON-роутеров, создается ELF-файл, который затем интегрируется в прошивку через фреймворки типа Router Post-Exploitation Framework, либо вручную [15,16,17]. Данный инструмент требует указания целевой прошивки и пути к вредоносному файлу. После модифи-

кации прошивка перепаковывается и распространяется через неофициальные источники или подмену легальных обновлений.

Результаты

Сканирование оригинальной прошивки, полученной с сайта производителя, продемонстрировало, что прошивка, действительно получена с сайта производителя, так как прошла проверку сравнения по хэш-сумме. После распаковки файловой системы сканер вычислил хэш SHA-256 прошивки и сравнил его со значением из базы данных [18]. Совпадение хэша подтвердило отсутствие модификаций, о чем свидетельствовало сообщение: «Проверено! Прошивка не модифицирована и соответствует официальной» (рис. 2). Это указывает на то, что прошивка сохранила целостность и не содержит несанкционированных изменений.

```
diplom@diplom:~/Desktop/diplom_final$ python3 main.py -h
usage: main.py [-h] [--url URL] [--firmware FIRMWARE] [--download_folder DOWNLOAD_FOLDER] [--hash_file HASH_FILE] [--update]

Анализатор прошивок и сканер обновлений

options:
  -h, --help            show this help message and exit
  --url URL             Ссылка для сбора файлов с прошивками
  --firmware FIRMWARE   Путь к файлу с прошивкой для анализа
  --download_folder DOWNLOAD_FOLDER
                        Папка для загрузки файлов
  --hash_file HASH_FILE
                        Файл с хэш-суммами прошивок
  --update              Обновление базы прошивок и хэшей
diplom@diplom:~/Desktop/diplom_final$ python3 main.py --firmware original_firmware.fw.bin

[+] Проверка пройдена: прошивка соответствует официальной версии 'ntu-52w-3.0.3-build1511.fw.bin'
diplom@diplom:~/Desktop/diplom_final$
```

Рис. 2. Проверка оригинальной прошивки

При анализе модифицированной прошивки сканер выявил несколько критических аномалий [19]. В процессе статического анализа были обнаружены файл reverse_shell_backdoor с помощью YARA правил по сигнатуре, соотвествующей полезной нагрузке msfvenom, внедрённый в прошивку [20]. Сканер отметил эти компоненты как потенциально опасные и выдал предупреждение: «Проверка не пройдена! Будьте осторожны при использовании данной прошивки» (рис. 3).

```
diplom@diplom:~/Desktop/diplom_final$ python3 main.py --firmware 123.bin

[!] Хэш не найден в базе. Запуск анализа...
[+] Прошивка распакована
[+] Загружено YARA правил для анализа: 3

[!] КРИТИЧЕСКИЕ НАХОДКИ:

🔴 YARA Rule: Backdoor
   File: [description="Detect ELF reverse shell backdoor from signature",author="Alexandr Zonov",date="2024-12-12",hash=""] /tmp/fw_analysis/_123.bin.extracted/iso
-root/IMAGE_PA/_SQUASHFS.extracted/squashfs-root/bin/reverse_shell_backdoor
   Metadata: N/A

🔴 YARA Rule: Custom_Backdoor
   File: [description="Detects msfvenom MIPS reverse shell",author="Alexandr Zonov"] /tmp/fw_analysis/_123.bin.extracted/iso-root/IMAGE_PA/_SQUASHFS.extracted/squa
shfs-root/bin/reverse_shell_backdoor
   Metadata: N/A

🚨 Подозрительные системные файлы:
   /tmp/fw_analysis/_123.bin.extracted/iso-root/IMAGE_PA/_SQUASHFS.extracted/squashfs-root/.lstripped

[+] Очистка завершена

[!] Внимание! Прошивка не прошла проверку подлинности
```

Рис. 3. Результат сканирования модифицированной прошивки

Заключение

Исследование и устранение уязвимостей в сетевых устройствах, особенно в PON-роутерах, играют ключевую роль в обеспечении информационной безопасности современных сетей. Эти устройства, являясь основой высокоскоростных оптоволоконных инфраструктур, требуют специализированных подходов к анализу и защите из-за их широкой распространенности и уязвимости к целенаправленным атакам. Разработанный сканер прошивок, сочетающий методы проверки целостности и статического анализа, демонстрирует высокую эффективность в обнаружении бэкдоров, подозрительных системных вызовов и модификаций, что подтверждено тестированием на модифицированной прошивке, созданной в качестве примера для демонстрации работы сканера.

Инструмент позволяет не только выявлять известные угрозы, такие как reverse-shell, но и минимизировать риски, связанные с цепочкой поставок и отсутствием своевременных обновлений.

Перспективы работы включают расширение базы хэшей прошивок, создание и добавление новых YARA правил, а также анализ модицированных прошивок с целью определения новых вариаций полезных нагрузок, используемых злоумышленниками. Реализация этих шагов станет значимым вкладом в глобальную защиту сетевой инфраструктуры, обеспечивая устойчивость к кибератакам в условиях цифровизации и роста числа IoT-устройств.

Таким образом, предложенное решение не только повышает уровень безопасности PON-роутеров, но и формирует основу для стандартизации подходов к анализу прошивок, что способствует укреплению доверия к критически важным компонентам сетевой экосистемы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Зингеренко Ю. А. Пассивные оптические сети xPON. – Текст: непосредственный / Ю. А. Зингеренко. – СПб.: Университет ИТМО, 2020. – 115 с.
2. Анализ размера и доли рынка пассивных оптических сетей – тенденции роста и прогнозы [Электронный ресурс]. URL: https://www.mordorintelligence.com/ru/industry-reports/passive-optical-network-pon-equipment-market
3. Зловред в роутере: скрытая угроза [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/router-malware/33319/
4. Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda
5. Заметные атаки на цепочки поставок в 2024 году [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/supply-chain-attacks-in-2024/39004/
6. Нефёдова М. В маршрутизаторах FiberHome Networks обнаружено более 20 бэкдоров [Электронный ресурс] // Журнал «Хакер». – URL: https://xakep.ru/2021/01/18/fiberhome-networks-backdoors/
7. TP-Link Router Remote Code Execution Vulnerability [Электронный ресурс]. URL: https://www.hkcert.org/security-bulletin/tp-link-router-remote-code-execution-vulnerability
8. Шубин В. В. Информационная безопасность волоконно-оптических систем. - Текст: непосредственный / В. В. Шубин – Саров, ФГУП «РФЯЦ-ВНИИЭФ», 2015. – 257 с.

9. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – Текст: непосредственный / R. Anderson – Wiley, 2008. – 1232 с.

10. US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF) [Электронный ресурс]. URL: https://datatracker.ietf.org/doc/rfc6234/

11. Монаппа К. А. Анализ вредоносных программ. – Текст: непосредственный / К. А. Монаппа. – Москва: ДМК Пресс, 2019. – 452 с.

12. Обзор правил YARA: изучение инструмента исследования вредоносного ПО [Электронный ресурс]. URL: https://habr.com/ru/companies/varonis/articles/584618/

13. Kennedy D. Metasploit: The Penetration Tester's Guide. – Текст: непосредственный / D. Kennedy – San Francisco, 2011. – 328 с.

14. Что такое Netcat? Bind Shell и Reverse Shell в действии [Электронный ресурс]. URL: https://habr.com/ru/articles/657613/

15. Харрис Д. М. Цифровая схемотехника и архитектура компьютера. – Текст: непосредственный / Д. М. Харрис, С. Л. Харрис. – СПб, 2016. – 672 с.

16. Что такое ELF и как он работает в Linux? [Электронны ресурс]. URL: https://habr.com/ru/companies/timeweb/articles/784534/

17. RouterSploit Framework [Электронный ресурс]. URL: https://github.com/threat9/routersploit

18. Хеш-функция, что это такое? [Электронный ресурс]. URL: https://habr.com/ru/articles/534596/

19. Обнаружение аномального поведения программ для дальнейшего использования при решении задачи защиты от вредоносного ПО [Электронный ресурс]. URL: https://www.okbsapr.ru/library/links/obnaruzhenie-anomalnogo-povedeniya-programm-dlya-dalneyshego-ispolzovaniya-pri-reshenii-zadachi-zashch/

20. Исследование file signature header [Электронный ресурс]. URL: https://scilead.ru/article/6926-issledovanie-file-signature-header