УДК 004.492
DOI 10.33764/2618-981X-2023-6-203-208

Д. Е. Пешков[1], А. В. Шабурова[1]*

Исследование программного обеспечения pon-роутера на предмет уязвимостей и программных закладок

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

Аннотация. Одной из важных задач в обеспечении информационной безопасности корпоративной и домашней сети является обеспечение безопасности и целостности данных в сети. Развитие сетевой инфраструктуры неизбежно связано с возникновением рисков информационной безопасности, связанных с сетевым оборудованием. Одной из сложнейших задач администрирования крупных корпоративных сетей является отслеживание и контроль версий сетевого оборудования для установки актуальных обновлений, если они имеются. Кибергруппировки все активнее используют атаки на цепочки поставки. Подделывая данные программного обеспечения или внедряя в него программные закладки, злоумышленники доводят до конечного пользователя уязвимое устройств. Пользователь же ничего не подозревает, получая устройства или обновления из легитимных источников. Поэтому необходимо выполнять сканирование программного обеспечения роутеров на предмет программных закладок.

Ключевые слова: целостность данных, программное обеспечение, атаки на цепочки поставки, программные закладки

D. E. Peshkov[1], A. V. Shaburova[1]*

Investigation of the Software of the Pon-Router for Vulnerabilities and Software Backdoors

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

Abstract. One of the important tasks in ensuring the information security of corporate and home networks is to ensure the security and integrity of data in the network. The development of network infrastructure is inevitably associated with the emergence of information security risks associated with network equipment. One of the most difficult tasks of the administration of large corporate networks is tracking and version control of network equipment to install up-to-date updates, if any. Cyber groups are increasingly using attacks on supply chains. By faking software data or introducing software bookmarks into it, attackers bring vulnerable devices to the end user. The user does not suspect anything, receiving devices or updates from legitimate sources.

Key words: data integrity, software, supply chain attacks, software backdoor

Введение

Распространение сетевых устройств в домашних и корпоративных сетях повлекло за собой повышения интереса злоумышленников к данному виду устройств и атак на них [1, 2]. И если пользователи зачастую выбирают устройство по красивой коробке, не проверяя присутствуют ли в нем какого-либо рода

уязвимости, то бизнес может просто не уследить за всем имевшимся оборудование в виду расширения мощностей. Вендоры же данного оборудования зачастую не стравляться с новыми вызовами, которые ставят перед ними злоумышленники. Устройства на момент выхода уже имеют встроенные уязвимости, которые злоумышленникам лишь нужно обнаружить. А если говорить не о новых устройствах, то данные уязвимости имеют и публичные рабочие эксплойты.

Данную проблему могло бы решить регулярное обновление программного обеспечения или микропрограммы устройств, но зачастую в жизненном цикле таких устройств такие события случаться лишь изредка. Этим и пользуются злоумышленники.

К данным проблемам последние несколько лет добавляться и новые. В последние несколько лет злоумышленники выполняют атаки на цепочку поставок [3]. Данный вид атаки нацелен на разработчиков программного обеспечения и поставщиков. Их основная цель – это получить доступ к исходным кодам, процессам сборки или механизмам обновления путем заражения допустимых приложений для распространения вредоносных программ [4]. Тем самым устройство поступает владельцу от легитимного источника, но с измененным исходным кодом.

В рамках статьи будет исследовано стандартное программное обеспечение роутера с внедренной программной закладкой [5].

Целью статьи является выявление возможных уязвимостей в программном обеспечении, и попытка обнаружить программную закладку в стандартном сетевом оборудовании [6].

Методика исследования

Для достижения поставленной цели необходимо произвести анализ программного обеспечения роутера и выявить все возможные уязвимости, в том числе программные закладки. Для данной задачи будет использован «The Firmware Analysis and Comparison Tool». Данный инструмент с открытым исходным кодом предназначен для автоматизации большей части процесса анализа встроенного программного обеспечения. Он распаковывает внутренние файлы программного обеспечения и выполняет анализ файлов.

После установки всех зависимостей, которые имеются у данного инструмента, и запуска «The Firmware Analysis and Comparison Tool» представляет собой веб-приложение с возможностью загрузки программного обеспечения. Помимо загрузки также иметься список всех выполненных загрузок и продвинутый поиск по загруженным файлам.

В качестве уязвимого программного обеспечения был выбран роутер D-Link DIR-620. Версия программного обеспечения DIR-620-1.3.0.bin была изменена для внедрения в нее программной закладки [7].

В качестве программной закладки был сгенерирован исполняемый файл линукс, который инициализирует подключение к удаленному ip-адресу. Программное обеспечение роутера было декомпилировано для внедрения в него программной закладки, после чего снова собрано.

Результаты

Основным способом выявления уязвимостей программного обеспечения является статический анализ. В данном способе все файлы программного обеспечения анализируются по очереди, и на основе найденной информации делается вывод о наличии той или иной уязвимости. Имея сигнатуры уязвимого кода, можно с достаточно большой точностью выявлять уязвимости в коде программного обеспечения.

Для данной работы по выявлению уязвимостей и программных закладок будет выбрана прошивка роутера D-LINK DIR-620 [8]. В данной прошивке присутствуют множественные уязвимости. Данная прошивка свободно распространяется и ее можно получить с сайта производителя.

Для внедрения программной закладки необходимо извлечь исходный код программного обеспечения и внедрить в него код программной закладки (рис. 1).

```
ubuntu@ubuntu:~/Diplom/firmware-mod-kit$ ./extract-firmware.sh ../DIR_620_1.3.0.bin
Firmware Mod Kit (extract) 0.99, (c)2011-2013 Craig Heffner, Jeremy Collake

Scanning firmware...

Scan Time:     2023-05-04 11:32:11
Target File:   /home/ubuntu/Diplom/DIR_620_1.3.0.bin
MD5 Checksum:  43fd5794b1aa97968a42bdccfb050be1
Signatures:    344

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header CRC: 0x47252455, created: 2011-12-07 13:33:45, image size: 90
oint: 0x8027F000, data CRC: 0x79AC8763, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "DIR_620"
64            0x40            LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 2727584 bytes
983040        0xF0000         Squashfs filesystem, little endian, non-standard signature, version 3.1, size: 3564733 bytes, 883 inodes,
3:33:41

Extracting 983040 bytes of uimage header image at offset 0
Extracting squashfs file system at offset 983040
4587520
4587520
0
Extracting squashfs files...
Firmware extraction successful!
Firmware parts can be found in '/home/ubuntu/Diplom/firmware-mod-kit/fmk/*'
```

Рис. 1. Извлечение исходного кода программного обеспечения

Также для генерации программной закладки необходимо знать тип архитектуры программного обеспечения (рис. 2).

```
ubuntu@ubuntu:~/Diplom/firmware-mod-kit/fmk/rootfs$ file bin/busybox
bin/busybox: setuid ELF 32-bit LSB executable, MIPS, MIPS32 rel2 version 1 (SYSV), statically linked, stripped
```

Рис. 2. Тип архитектуры устройства

Из этого становиться известно, что программная закладка должна работать с архитектурой MIPS. Для генерации программной закладки был использован msfvenom (рис. 3). С помощью msfvenom был создан исполняемый файла backdoor в каталоге роутера rootfs/usr/bin/.

После перемещения данного эксплойта в код прошивки и установки автозапуска прошивка может быть обратно скомпилирована (рис. 4).

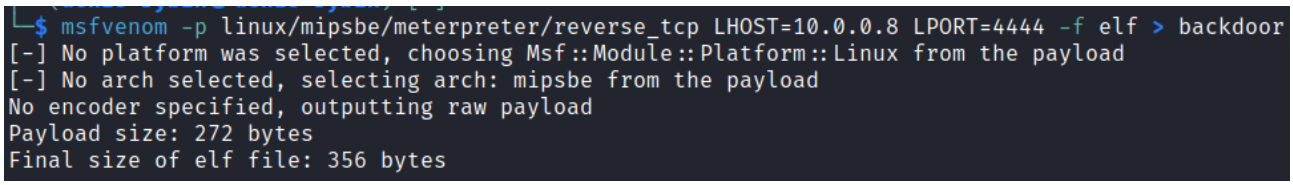

Рис. 3. Генерация программной закладки

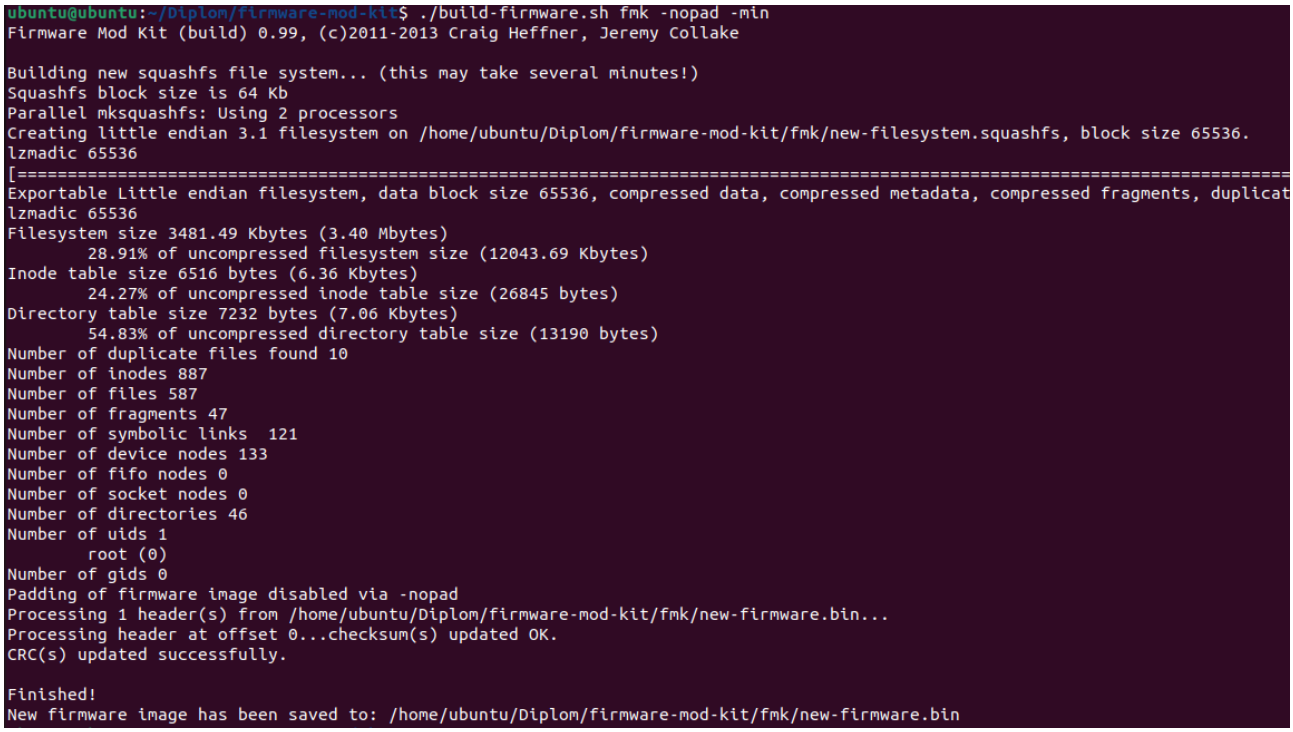

Рис. 4. Сборка прошивки с установленной программной закладкой

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

После подготовки уязвимого программного обеспечения можно переходить к этапу сканирования. Полученная прошивка была загружена и просканирована инструментом «The Firmware Analysis and Comparison Tool». В результате работы является отчет по разным модулям работы инструмента (рис. 5).

Однако несмотря на то, что найденные уязвимости являются критическими, программная закладка не была обнаружена инструментом. Таким образом данный инструмент должен быть существенно модернизирован и дополнен модулем поиска программных закладок.

BusyBox 1.19.2 (CRITICAL)	router router - dir 620 test 2 backdoor (router) | /903533_unknown.bin | /13693.squashfs | /bin/busybox Size: 472.65 KiB , Type: application/x-executable
Dnsmasq 2.55 (CRITICAL)	router router - dir 620 test 2 backdoor (router) | /903533_unknown.bin | /13693.squashfs | /usr/sbin/dnsmasq Size: 183.15 KiB , Type: application/x-executable
GNU Zebra 0.95a	router router - dir 620 test 2 backdoor (router) | /903533_unknown.bin | /13693.squashfs | /usr/sbin/ripd Size: 392.68 KiB , Type: application/x-executable
Linux Kernel 2.6.21 (CRITICAL)	router router - dir 620 test 2 backdoor (router) | /uboot.lzma | //uboot.lzma~ Size: 2.60 MiB , Type: application/octet-stream
Point-to-Point Protocol daemon (CRITICAL)	router router - dir 620 test 2 backdoor (router) | /903533_unknown.bin | /13693.squashfs | /sbin/pppd Size: 615.08 KiB , Type: application/x-executable
portable SDK for UPnP 1.3.1 (CRITICAL)	router router - dir 620 test 2 backdoor (router) | /903533_unknown.bin | /13693.squashfs | /lib/libupnp.so Size: 245.93 KiB , Type: application/x-sharedlib
Pure-FTPd 1.0.34	router router - dir 620 test 2 backdoor (router) | /903533_unknown.bin | /13693.squashfs | /usr/sbin/pure-ftpd Size: 99.40 KiB , Type: application/x-executable

Рис. 5. Обнаруженные уязвимости

Заключение

Таким образом можно сделать вывод, что с поиском известных уязвимостей программные продукты справляться достаточно хорошо, однако для более сложных атак они еще не готовы.

Данную проблему можно решить ручным или поведенческим анализом прошивки, но тогда пострадает скорость и автоматизация процесса [9]. Также данные два способа занимают достаточно много времени и специалиста.

В данный момент ведется разработка инструмента по автоматизированному сканированию программного обеспечения роутера, который позволит в автоматическом режиме обнаруживать программные закладки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Яскевич В.И. Секьюрити. Организационные основы безопасности фирмы: учеб. пособие / В.И. Яскевич. М.: Ось-89, 2012. – 230 с.

2. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М.: Книжный мир, 2012. – 352 с.

3. Милославская Н.Г. Визуализация процессов управления информационной // Научная визуализация. – 2017. – Том 9, № 5. – С. 117–136.

4. ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения = Information protection. Information security monitoring. General provi-

sions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 июля 2021 г. N 656-ст : введен впервые : дата введения 2022-04-01 / подготовлен Федеральной службой по техническому и экспортному контролю (ФСТЭК России), обществом с ограниченной ответственностью "Центр безопасности информации" (ООО "ЦБИ"). Москва : Стандартинформ, 2021 – 10 с.

5. Федоров С.Е. Компьютерное моделирование и исследование систем автоматического управления: учебно-методическое пособие / Федоров С.Е. – Москва : Русайнс, 2020. – 92 с.

6. Мельников В.П. Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 2-е изд., стер. – М. : Academia, 2014. – 330 с.

7. Ржавский К.В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: учеб. пособие. – Волгоград: Изд-во ВолГУ, 2002. – 122 с.

8. Жарова А.К. Правовая классификация угроз и рисков в информационной сфере / А.К. Жарова // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2016. – № 7-8 (97-98). – С. 130-138.

9. Астахова Л.В. Кадровые проблемы построения системы управления информационной безопасностью на предприятии / Л.В. Астахова, Л.О. Овчинникова // Вестник УрФО. Безопасность в информационной сфере. – 2016. – № 3 (21). – С. 38-46.