УДК 004.855.5

МЕТОДЫ ЗАЩИТЫ «УМНЫХ» ПРИБОРОВ НА ПРИМЕРЕ ТЕЛЕВИЗОРА SAMSUNG

© 2019 И. Е. Пустыльник, Ю. П. Преображенский

Воронежский институт высоких технологий (г. Воронеж, Россия)

В настоящее время, количество «умных» приборов, используемых в быту, быстро растет. Вместе с этим растет и количество захватов подобных приборов хакерами с целью использования их в DDos и Spam атаках на другие сети и отдельные компьютеры. В статье рассматриваются способы данных атак (наиболее распространенным является обновление программного обеспечения умного прибора, осуществляемое с помощью подмены DNS адресации) и методы защиты от них путем усиления защиты роутеров и чистки кэша DNS.

Ключевые слова: отравление DNS, несанкционированное обновление, чистка кэша DNS

Интернет вещей стремительно развивается как в количественном (прогнозируется, что на руках у пользователей будет до 50 млрд. различных устройств), так и в качественном (разрабатываются различные виды «умных» устройств от программируемых лампочек до сложнейших систем контроля за производственными процессами). В этой статье рассматривается вид «умных» устройств, которые появились на заре интернета вещей, а именно, приборы, используемые в быту: холодильники, телевизоры, и т. д. [1]

Данные приборы помимо своей основной «начинки», помогающей им выполнять основную работу, как-то создание холодной среды, показ телепередач или уборку пыли, снаряжаются программным обеспечением, дающим возможность контролировать данные приборы удаленно, через интернет. Подобные устройства чаще всего оснащаются небольшим компьютером (сравнимым по силе и размеру) с оснащением бытового смартфона. Они имеют встроенную операционную систему, обычно на основе Linux и ряд функциональных возможностей, позволяющим управлять устройствами, на которых они установлены.

Руководствуясь данными, приведенными на сайте Статиста, можно понять, на сегодняшний день в мире используется более 3 млрд. бытовых устройств, имеющих «умную» начинку. Из них примерно 2,15 млрд. составляют бытовые смартфоны и 280 млн. бытовые планшеты, которые используются практически повсеместно в интерактивном режиме и поддаются прямому визуальному контролю.

Из остальных устройств наиболее распространены телевизоры (160 млн.). На остальные домашние устройства, как-то холодильники, терморегуляторы и иные приборы, приходится примерно 60 млн. устройств. Главная проблема данных устройств – невозможность контролировать их операции постоянно и интерактивно. Можно сказать также, что такие устройства могут подвергаться хакерскому захвату, который может быть обнаружен далеко не сразу.

В отличие от ряда индустриальных приборов с «умной» начинкой, разработки для «умных» бытовых приборов обычно опираются на открытые технологии и алгоритмы. Рассматривая три телевизора, наиболее распространённых брендов (LG, Sharp, Samsung), можно заметить, что все они используют операционные системы, ранее использовавшиеся в других устройствах. Samsung использует OS Tizen, которая ранее создавалась для смартфонов и планшетов. LG использует Web OS, которая выросла из Palm OS, операционной системы используемой в наладонниках. Sharp[IP1] имеет в наличии телевизоры, использующие разные устройства, использующие Tizen, Android TV и Roku TV системы. Все эти системы хорошо известны пользователям, а значит и хакерам, осуществляющим попытки взлома подобных устройств.

Останавливаясь на телевизорах, как типичных образцах бытовых «умных» приборов, можно отметить, что все они подключаются к сети по одинаковой схеме, представленной на рисунке 1.

Пустыльник И. Е. – Воронежский институт высоких технологий, студент.

Преображенский Юрий Петрович – Воронежский институт высоких технологий, к. т. н., профессор, petrovich@vivt.ru.

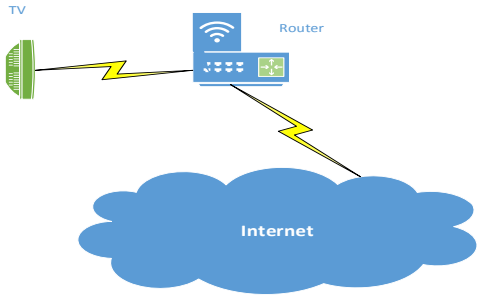

Рисунок 1. Подключение «умного» телевизора.

Практически все телевизоры сегодня подключаются к интернету, используя беспроводной метод Wi-Fi. Стандартный домашний роутер разрешает подключение по стандарту N или AC на частотах 2.4 или 5 гигагерц. Подключение к роутеру подразумевает, что телевизор получает локальный адрес и доступ ко всем возможностям интернета, включая сетевые протоколы SMTP, POP, DNS, и другие. Это также означает, что устройство становится видимым из сети и может быть атаковано хакерами.

В процессе написания данной статьи использовалась информация, доступная на роутере ASUS RT-N66R. Хотя роутеры слегка отличаются друг от друга подачей информации о клиентах, содержание информации остается примерно одним и тем же. На рисунке 2 видно, что роутер получает информацию о типе подключенного устройства.

WN3000RP	192.168.2.24	Static	84:1B:5E:45:FA:9A	2.4 G	300	300	00:10:25
Samsung	192.168.2.34	DHCP	28:39:5E:4E:EB:D5	2.4 G	78	104	00:01:09
DESKTOP-BG9ASHL	192.168.2.70	DHCP	2C:FD:A1:E0:4C:62		-	-	-
android-f012592311ebac30	192.168.2.107	DHCP	94:A1:A2:56:8D:B1	2.4 G	5.5	2	42:59:52

Рисунок 2. Отображение трафика от устройств, подключенных к роутеру.

Вторая линия четко показывает, что к роутеру подключено устройство Samsung, в нашем случае – это телевизор. Таким образом, доступ к информации от роутера позволяет спланировать атаку данное устройство. Насколько бы данная информация не являлась тривиальной, но первой линией защиты умных устройств является защита роутера, к которому они подключаются. Ни для одного специалиста, работающего с подобными системами, не является секретом то, что обычно все роутеры приходят с завода с именем пользователя и паролем admin. Замена имени пользователя представляет собой определенные сложности, но вот замена пароля должна производиться моментально после подключения роутера к локальной сети.

Как видно на рисунке 2, устройство Samsung использует беспроводную связь Wi-Fi на частоте 2.4Ггц. Этот канак связи часто настроен на заводе как незащищенный. Для защиты данного канала используются стандарты нередко WPA и WPA2. Сразу после подключения роутера к сети необходимо установить пароль (кодовое слово), которое пользователь будет обязан вводить при входе в сеть. Случайный наблюдатель или хакер могут войти в сеть через беспроводной канал и захватить роутер.

Проведение вышеописанных процедур может уменьшить возможность проникновения хакера в домашний интернет с «умным» телевизором, но оно ни в коем случае не может считаться эффективным способом защиты против атак на устройства интернета вещей. Исследования домашнего интернета показывают, что проникновение в систему, даже защищенную надлежащим образом вполне возможно. Далее в этой статье говорится о методах защиты против более-менее изощренного хакера, который может пройти или взломать элементарную защиту, представляемую домашним роутером, стоящим на входе в домашний интернет.

Любой пользователь, имеющий доступ к адресу «умного» телевизора, в данном случае 192.168.2.34 может с помощью программы NMAP сканировать устройство по данному адресу на наличие открытых портов. Любой из этих портов может стать целью различных DDOS атак. Рисунок 3 показывает наличие подобных портов у телевизора Samsung.

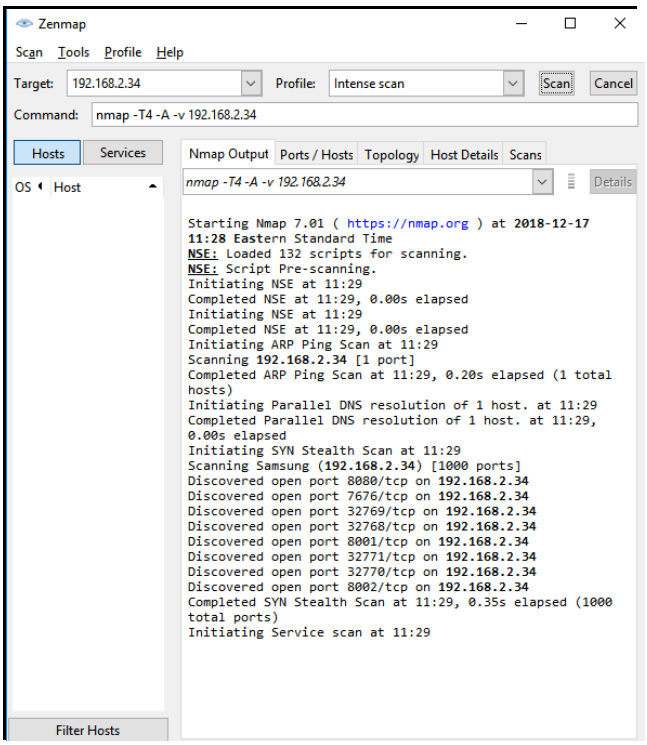

Рисунок 3. Открытые порты телевизора Samsung.

Любой домашний роутер имеет несложный Firewall, который может регулировать входящий и выходящий сетевой трафик на отдельных портах. Сверившись с документацией на данное устройство, необходимо закрыть все порты, которые не используются телевизором для работы. Если это возможно, то рекомендуется открывать данные порты для необходимых отладочных действий (когда требуется) и немедленно закрывать их после окончания данных действий. Многие подобные порты оставляются производителем для возможной удаленной отладки или починки системы. Такие порты являются идеальными точками входа в систему через «заднюю дверь» (backdoor).

Один из открытых портов, обнаруженный с помощью NMAP является входом в локальный REST Service сервер, который предоставляет информацию о телевизоре, которая очень похожа на ту, которую предоставляют устройства по протоколу Plug-n-Play. Можно создать запрос в любой операционной системе с помощью утилиты cURL и получить полную информацию о телевизоре, используя URL на порту 8001: http://192.168.2.34:8001/api/v2.

Информация на Рисунке 4, конечно же, не является полной. Однако, принимая во внимание, что роутер дает информацию только о фирме изготовителе и локальном адресе, такой объем информации может быть весьма полезен, т. к. дает подробные сведения об операционной системе, виде устройства и т. д. Обладающий информацией о слабостях различных устройств хакер может рассчитать какой именно алгоритм взлома может быть наиболее полезен при работе с определенным устройством, с характеристиками, подобными изображенным на рисунке 4.

Одним из наиболее распространенных видов атаки на умные устройства является захват данного устройства с целью использования его в любых других целях. Известен случай, когда «умный» холодильник марки Samsung был захвачен хакером и использован для пересылки е-мэйл сообщений (спам). Очевидно, что штатная операционная система Tizen и программное обеспечение, устанавливаемое на приборы фирмы Samsung, не в состоянии выполнять операции массовой рассылки почты. Для того, чтобы заставить «умный» прибор выполнять подобные операции, хакер должен изменить программное обеспечение.

Рассматривая порты, определенные NMAP мы не наблюдаем входов для программ типа sch, telnet или ftp, которые бы позволили скопировать и запустить программы на устройстве удаленно. Инженеры фирмы Samsung, очевидно, предусмотрели подобные ситуации и защитили устройство от них. Здесь рассмотрена несколько иная

ситуация, позволяющая хакеру заставить устройство выполнять команды, не предусмотренные в штатном программном обеспечении.

Рисунок 4. Информация об «умном» телевизоре Samsung.

Любое устройство фирмы Samsung требует постоянного обновления программного обеспечения с целью устранения ошибок и проблем безопасности. Обновление происходит по запросу на серверы домена Samsung.com. Информация об адресе данного домена хранится в DNS сервере, который обычно в домашней сети расположен на домашнем роутере. Хотя сам сервер достаточно безобиден и работает с внешними DNS серверами Интернет-провайдера, он хранит внутри роутера обновляемый DNS-кэш. В этом кэше хранятся наиболее часто запрашиваемые пары имя-адрес. Хакер может изменить адрес домена Samsung.com в кэше и перенаправить запросы на изменение программного обеспечения на сервер, где хранится версия программ, измененная хакером. Ранее в этой статье говорилось, что большинство операционных систем используемых в интернете вещей (точнее в «умных» телевизорах) являются или были созданы с кодом свободного доступа, который можно легко заменить на требуемый хакеру. Поэтому каждое обновление программного обеспечения может таить в себе потенциальную опасность «заражения» прибора.

Как бороться с подобным захватом и «заражением» кэша? Самый простой и действенный способ – это периодическая чистка кэша на роутере, которая может производиться с помощью утилит, существующих на роутерах и персональных компьютерах. Далее говорится о системе практической чистки DNS-кэша.

1. Большинство роутеров не имеет входа через telnet, который необходим для подобных операций. Во избежание проблем с безопасностью самого роутера производители держат закрытым порт 23. Некоторые роутеры, подобно рассматриваемому в этой статье имеют опции для открывания порта 23.

Рисунок 5. Управление опцией Telnet.

2. После того, как возможность входа в роутер через telnet обеспечена, можно осуществить ее. Обычно роутеры имеют только одну пару имя-пароль, которую можно использовать. Т. к. пользователь получает полный контроль над роутером, эту опцию надо отменять после того, как работа по очистке кэша закончена. Войти можно с помощью команды, показанной на рисунке 6, которую можно выполнить из любого окна cmd, terminal или shell.

```
C:\Users\Igor Pustylnick>telnet 192.168.2.1 -l admin
```

Рисунок 6 Вход в роутер из утилиты cmd.

3. После входа в роутер можно выполнить необходимые команды из shell-окна самого роутера. Команда, представленная на рисунке 7, позволяет полностью очистить DNS кэш.

```
RT-N66R login: admin
Password:
admin@RT-N66R:/tmp/home/root# killall -1 dnsmasq
admin@RT-N66R:/tmp/home/root#
```

Рисунок 7. Очистка КЭШа.

Если «умный» прибор еще не заражен, то периодическая чистка DNS кэша может быть очень действенным способом защиты от заражения роутера. Если же это уже произошло, то имеет смысл просматривать входящий и выходящий сетевой трафик с данного устройства. Большинство домашних роутеров имеют такую опцию, которой может воспользоваться практически любой пользователь. На рисунке 8 показан экран утилиты роутера ASUS, который следит за трафиком в сети.

Internet	Icon	Clients Name	Client IP address		Clients MAC Address	Interface	Tx Rate (Mbps)	Rx Rate (Mbps)	Access time
		WN3000RP	192.168.2.23	DHCP	84:1B:5E:45:FA:9A	2.4 G	300	300	00:33:30
		Samsung	192.168.2.34	DHCP	28:39:5E:4E:EB:D5	2.4 G	117		00:33:27
		DESKTOP-BG9ASHL	192.168.2.70	DHCP	2C:FD:A1:E0:4C:62		-	-	
		android	192.168.2.128	DHCP	96:A1:A2:56:8D:B1	2.4 G	300	243	00:32:42
		HUAWEI_P20-25a20c263de369	192.168.2.165	DHCP	7C:76:68:BA:E7:09	2.4 G	144.4		00:33:08

Рисунок 8. Трафик в домашней сети, замеряемый роутером ASUS.

Очевидно, что «умные» приборы имеют достаточно большой легитимный трафик во время общения с интернетом. «Умный» телевизор может служить входом в интернет или точкой просмотра программ из сетевых приложений типа Netflix или YouTube. Домашний пользователь должен быть более-менее знаком с легитимными переменами в сетевом трафике чтобы распознать аномалии.

Что делать если «умный» телевизор выглядит зараженным и производит большой объем несанкционированного или просто необъяснимого трафика. В случае, если такое отклонение становится системным, имеет смысл вернуть телевизор к фабричному стан-

дарту. При этом все изменения, вызванные хакерскими атаками, будут уничтожены.

Существует множество различных видов атак на «умные» приборы типа телевизоров или холодильников. Как видно из данной статьи, большинство из них можно остановить средствами, имеющимися в распоряжении любого пользователя, а именно защитой домашней сети, роутера и самих приборов. Естественно, существуют другие атаки, которые требую большего внимания или серьезного подхода к защите входов в локальную сеть и ее элементов. Однако, в среднестатистическом случае метод, описанный в данной статье, может оказаться достаточно эффективным.

ЛИТЕРАТУРА

1. Гринберг, Э. «Hacker Lexicon: What Is DNS Hijacking?,» WIRED, 09 04 2017. [В Интернете]. Available: https://www.wired.com/story/what-is-dns-hijacking/. [Дата обращения: 19 12 2018].

2. Кадир, М. «What is DNS hijacking and How It Works?» Pure VPN, 1 4 2018. [В Интернете]. Available: https://www.purevpn.com/blog/dns-hijacking/. [Дата обращения: 19 12 2018].

3. Перта, В., Марбера, Б, Тайсон, Г., Хаддади, Х. и Мэй, А., «A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients,» в Proceedings on Privacy Enhancing Technologies, 2015.

4. Хофман, К. «What is DNS Cache Poisoning?,» 08 03 2017. [В Интернете]. Available: https://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/. [Дата обращения: 19 12 2018].

5. SuperHosting.BG, «https://blog.superhosting.bg/en/dns-cache-how-the-dns-works.html,» Superhosting.BG, New York, 2017. [Дата обращения: 31 03 2019 г.]

6. Статиста**,** Unit sales of smart devices worldwide by category worldwide from 2013 to 2020 (in millions). *Statista. The statistics Portal.* [В Интернете] 2019 г. https://www.statista.com/statistics/671053/smart-devices-unit-sales-worldwide/. [Дата обращения: 31 03 2019 г.]

METHODS OF PROTECTING SMART APPLIANCES BASED ON THE EXAMPLE OF SAMSUNG TV SET

© 2019 I. E. Pustylnick

Voronesh Institute of High Technologies (Voronezh, Russia)

At present the number of smart appliances, used in the households is growing very rapidly. At the same time there is a following growth of capturing of such devices by hackers with the intention to use them in DDos and Spam related attacks on the other networks and standalone computers. The paper reviews the methods of such attacks (of which the most widespread is the renewal of the software of the smart device, which is conducted via the altering of DNS addressing) as well as the methods of protection from such attacks via strengthening the security of the routers and wiping of the DNS cache.

Keywords: DNS poisoning, non-sanctioned software renewal, wiping DNS cache.