Под колпаком у роутера

Екатерина Лаштун

Сетевые мошенники с каждым годом придумывают все более изощренные способы обмана пользователей, а число кибератак на абонентские устройства с целью дальнейшего управления различными девайсами, подключенными к домашней сети, неуклонно растет. Злоумышленники зачастую выбирают роутер как «входную дверь» в каждый дом.

Количество кибератак злоумышленников на абонентские устройства растет с каждым годом. Так, в ноябре 2016 года немецкая телекоммуникационная компания Deutsche Telekom, крупнейшая в Европе и третья по величине в мире, подверглась атакам неизвестных хакеров. «Проблема заключалась в уязвимом оборудовании, которое оператор предоставил своим клиентам. Роутеры почти 900 тыс. пользователей несколько дней работали некорректно: связь либо постоянно прерывалась, либо вовсе отсутствовала», — рассказал «Теле-Спутнику» директор по управлению сетью АО «ЭР-Телеком Холдинг» (торговая марка «Дом.ru») Кирилл Пищальников. Он сообщил, что в США одним из последних крупных инцидентов стала DDoS-атака на инфраструктуру DNS-провайдера Dyn, источником которой являлся ботнет Mirai, а для нападения было задействовано около 100 тыс. инфицированных IoT-устройств. Атака осуществлялась посредством пакетов TCP и UDP, через 53-й порт. В результате атаки возникли проблемы с доступом ко многим веб-сайтам и социальным сервисам, в частности Twitter, Etsy, Github, Soundcloud, Spotify, Heroku. «Взломанные роутеры NanoStation 2 и AirOS использовались в ботнете Dyreza в качестве первых слоев прокси», — добавляет генеральный директор ООО «Доктор Веб» **Борис Шаров.**

Узкое горлышко

«Современные ТВ-приставки представляют собой достаточно развитую компьютерную систему. А при наличии выхода в Интернет любое устройство, даже ТВ-приставку, можно использовать в качестве точки проникновения. И такие случаи взлома абонентских устройств — не редкость», — продолжил руководитель группы развития телевизионных платформ «АКАДО Телеком» Сергей Васюк. Таким образом, домашние интернет-роутеры и IPTV-приставки являются тем самым «узким горлышком» — технологически слабым местом, с помощью которого киберпреступники могут несанкционированно управлять пользовательскими устройствами и снимать с них различные данные (например, с компьютера или смартфона, подключенных к домашней сети). Сетевой мошенник, взламывая домашний маршрутизатор, получит через него доступ ко всем подключенным девайсам.

Технически это происходит следующим образом. Домашние Wi-Fi-сети защищены паролем, поэтому просто подключиться к ним нельзя. Однако существуют специальные программы для взлома роутеров. «Сделать это можно во время подключения к беспроводной сети, когда к роутеру приходит запрос на разрешение и абонент вводит пароль, а также во время

работы, когда роутер продолжает обмениваться данными, посылая пакеты информации, среди которой указывается и пароль сети. Эти пакеты данных можно перехватить и расшифровать, а в дальнейшем узнать пароль сети и взломать ее», — объясняет Кирилл Пищальников из «ЭР-Телеком Холдинг». Часть программ, по его словам, работает по принципу перебора паролей. В этих случаях очень важно заменить заводской пароль на более сложный и выбрать устойчивый способ шифрования Wi-Fi-сети. В некоторые роутеры встроена блокировка перебора паролей, что дополнительно защищает пользователя от взлома. В октябре 2017 года была обнаружена и опубликована серьезная уязвимость механизмов защиты Wi-Fi, позволяющая легко получать несанкционированный доступ к сети. «Мы рекомендуем всем пользователям установить последние обновления прошивки роутеров и включить механизм двухфакторной аутентификации», — подчеркивает топ-менеджер «ЭР-Телеком Холдинг». Также несанкционированный доступ к роутеру, по его мнению, возможен через внешний IP-адрес роутера или IPTV-приставки. Если оператор устанавливает собственное оборудование, то техник сервиса обязан произвести корректную настройку конфигурации межсетевого экрана (firewall) и заблокировать наиболее уязвимые параметры и ресурсы своей сети. При обнаружении новых уязвимостей оператор должен дистанционно обновлять прошивку пользовательских оконечных устройств. IPTV-приставка, как и Wi-Fi-роутер, имеет собственный IP-адрес и может быть доступна в сети. Поэтому для домашней сети эксперты рекомендуют использовать локальные (частные) IP-адреса, которые не доступны из сети Интернет. IPTV-приставки имеют собственное программное обеспечение, обновлять которое также должен оператор.

«В нашей практике наиболее часто встречающееся явление — стандартный, одинаковый для всех пароль доступа к консоли управления, который пользователь чаще всего не утруждается поменять. К сожалению, мы практически не сталкивались с тем, чтобы произво-

дители задумывались над правильными стандартными настройками своих роутеров», — подчеркивает глава компании «Доктор Веб» Борис Шаров.

По словам директора департамента исследований угроз компании Avast (зарубежный разработчик решений для домашних и корпоративных пользователей в области информационной безопасности) Михала Салата (Michal Salat), злоумышленники часто выбирают роутер как «входную дверь» в каждый дом. Также, по его мнению, дело обстоит с видеорекордером, который обычно используется для записи видео с камер наблюдения. «Видеорекордеры также могут подключаться к Интернету и отличаются аналогичными проблемами безопасности, что и роутеры, — слабые пароли, пароли, используемые по умолчанию, и обход аутентификации», — отмечает Михал Салат.

По данным исследования компании Avast, в России 23,7% всех устройств Интернета вещей (IoT) уязвимы для кибератак, что создает риск для людей, их личных данных и безопасности. Среди таких устройств можно отметить веб-камеры и видеоняни — два устройства из пяти обладают рядом уязвимостей, которые могут использоваться злоумышленниками для слежки за пользователями и их детьми. Более того, 26,9% принтеров также небезопасны. Однако наиболее подвержены риску именно роутеры — согласно данным Avast, в России 69,2% этих устройств уязвимы. «На сегодняшний день наиболее частый и простой способ, которым пользуются злоумышленники при взломе IoT-устройств, — это подбор стандартных (заводских) паролей, которые изначально установлены на якобы защищенные устройства», — соглашается с экспертами Михал Салат. Он добавляет, что также существуют атаки CSRF (Cross Site Request Forgery), которые немного сложнее и атакуют маршрутизатор буквально «изнутри». Таким образом, если пользователь заходит на зараженный или вредоносный веб-сайт, то в браузере может быть запущен JavaScript, который попытается изменить в роутере DNS-настройки, используя либо стандартные учетные данные, либо данные, хранящиеся в файле cookie (в случае если пользователь в недавнем прошлом подключался к роутеру), либо уязвимости устройства для обхода аутентификации. Затем злоумышленник может перенаправить трафик на принадлежащий ему сервер и выполнить MitM-атаку (Man in the Middle attack), не обращаясь к SSL-серверу.

Кирилл Пищальниковов отмечает, что защита Wi-Fi-роутера начинается с установки надежного пароля, состоящего более чем из 10 чередующихся символов, и выбора устойчивого способа шифрования. Для этого нужно выбрать протокол шифрования WPA2-AES как более надежный. «Более старый протокол WEP намного легче взломать, и в нем много уязвимостей», — считает **Кирилл Пищальников.** По его мнению, протокол WPA надежнее потому, что для взлома нужно использовать только опре-

деленные пакеты данных. Также эксперт считает, что пользователю необходимо отказаться от функции WPS, которая запоминает подключающиеся устройства и позволяет даже посторонним девайсам автоматически подключаться к известной сети. Кроме того, должен быть включен и корректно настроен межсетевой экран (firewall), защищены интерфейсы управления и удаленного доступа к оборудованию. Для защиты прошивки IPTV-приставки также должен быть включен и корректно настроен межсетевой экран и заблокирована возможность несанкционированного обновления прошивки. Что касается теоретической возможности подмены контента в OTT-сетях, по мнению Кирилла Пищальникова, производители систем условного доступа, такие как Conax, Nagra и Verimatrix, управляют доступом к контенту и ключами шифрования OTT-сервисов. Оказывая техническую поддержку, они имеют только удаленный доступ к серверам CAS/DRM и могут изменить конфигурацию по ошибке. При ее изменении произойдет сбой в шифровании сигнала, и контент у клиентов оператора перестанет воспроизводиться. «Подменить один контент в OTT-сервисах другим возможно только на серверах подготовки и доставки контента пользователю, к этим серверам доступ есть только у доверенных сотрудников оператора», — сообщил Кирилл Пищальников.

«В OTT для защиты используется не CAS, а DRM (Digital Rights Management). CAS применяется для защиты вещательных сервисов — DVB2», — уточнил Сергей Васюк. По его словам, если допустить теоретическую возможность того, что администратор CAS захочет произвести замену контента, то ему надо будет этот контент где-то получить. Но так как и CAS, и DRM находятся в закрытых сетях оператора, сделать это невозможно. Поэтому технически осуществить замену контента в OTT-сервисах нельзя.

Единым фронтом

«Предотвращение кибератак на пользовательские устройства — это комплекс защитных и профилактических мер, которые должны предпринять как производители оборудования и операторы, так и абоненты. Поскольку наличие даже одного уязвимого звена может привести к сбою всей системы», — считает Сергей Васюк из «АКАДО Телеком». «Действительно, в одиночку задачу по обеспечению информационной безопасности устройств не решить, должны прикладывать усилия все стороны», — соглашается системный администратор ЗАО «Элекард Девайсез» Роман Чухно. Производители, по его мнению, должны защищать от проникновения в прошивки и вовремя устранять уязвимости во встроенном программном обеспечении. Провайдерам услуг следует мониторить обстановку в области безопасности и вовремя информировать абонентов об угрозах, а в случае обслуживания маршрутизаторов и приставок на стороне абонента самим позаботиться о предотвращении инцидентов. Пользователи тоже не должны оставаться в стороне — им нужно принимать меры по обеспечению безопасности (применять надежные пароли, не использовать заводские пароли на устройствах, поддерживать встроенное ПОактуальной версии).

По мнению эксперта из компании Avast, производители могут включить в перечень стандартных услуг настройку оборудования и политик безопасности, заставив конечных пользователей изменить пароль по умолчанию своего устройства. То же самое могут сделать и интернет-провайдеры, поскольку они часто предоставляют пользователям роутеры с уже предустановленной учетной записью, которые распределяются между всеми соединенными устройствами в сети провайдера, прежде всего для упрощения дистанционного управления. Однако этим могут воспользоваться злоумышленники, что угрожает безопасности пользователей.

«Единственная мера, которую мы считаем эффективной, — это заставить производителей устройств нести ответственность за их безопасность. В ряде стран сейчас хотят ввести сертификацию этих устройств, чтобы на рынок попадали только те изделия, которые гарантированно отвечают требованиям, определенным государством», — резюмирует гендиректор «Доктор Веб» Борис Шаров. ■