Об угрозах безопасности, возникающих при использовании Smart-технологии
Гатиятуллин Т. Р.

Гатиятуллин Тимур Радикович / Gatijatullin Timur Radikovich – студент 4 курса,
Институт управления и безопасности предпринимательства,
Башкирский государственный университет, г. Уфа

Аннотация: *данная статья призвана показать, насколько не безопасны современные Smart-технологии и рассказать об основных угрозах в них.*
Ключевые слова: *информационная безопасность, защита информации, взлом, интернет вещи, гаджеты, Smart TV.*

Резкое увеличение популярности подключенных к интернету бытовых устройств открывает большой потенциал не только для пользователей, но и для правонарушителей. Согласно анализу, проведенному работниками отдела безопасности компании Hewlett-Packard, множество устройств интернета вещей имеют грубые уязвимости, ставящие под угрозу безопасность своих хозяев [1]. Например, взлом смарт-холодильника позволил хакерам украсть пользовательский пароль аккаунта Google [2]. Также, эксперты HP выяснили, что 70% техники, подключенной к интернету, применяют незашифрованные сетевые сервисы.

Проблема безопасности «интернет вещей» – одна из основных на сегодня. «Умная» техника - наиболее уязвимая технология с точки зрения интернет угроз. Угроза появляется, когда люди покупают технику и подключают ее к сети интернет, не изменяя заводских настроек и паролей, что становится причиной того, что злоумышленники могут удаленно управлять их техникой. Следует заметить, что желающих купить смарт-холодильник или чайник немного, поэтому проблема не такая массовая. Большинство людей покупает смарт-телевизоры, что делает проблему широко распространённой.

В ноябре специалист Symantec, Candid Wueest, продемонстрировал, как легко может быть инфицирован смарт-телевизор, и как сложно потом его вылечить. Он установил на телевизор под управлением Android OS вирус-вымогатель, который каждые несколько секунд выводил на экран телевизора сообщение с требованием выслать некоторую сумму денег, и таким образом сделал невозможным просмотр телепередач. Эксперт утверждает, что большинство вирусов-вымогателей работают на телевизорах с Android OS [3]. Помимо вирусов, смарт-телевизоры подвержены другим видам угроз. Хакеры могут взломать телевизор для выполнения операций по скликиванию рекламы, получению криптовалюты, кражи личных данных пользователей или включения телевизора в ботнет. Помимо большого количества уязвимостей в «умных» телевизорах, позволяющих злоумышленникам взламывать их, существует другая проблема.

Покупая «умные» телевизоры, мы не думаем о каких-то скрытых алгоритмах присутствующих в электронике, нам интересно опробовать новые технологические возможности. Но со временем мы всё чаще начинаем обращать внимание на присутствие молчаливого наблюдателя, который скрупулёзно накапливает всю информацию о нас, он анализирует и выдает рекламу, которая нам должна быть интересна, выводит список каналов по нашим предпочтениям. Это кажется удобным функционалом, но не более того, однако выбирая эти функции, мы соглашается с тем фактом, что вся информация о нас может быть передана третьим лицам. Именно об этом говорится в пользовательском соглашении, которое прилагается к комплекту поставки «умного» телевизора Samsung. Помимо речевой информации, смарт-телевизор собирает массу других сведений о своем владельце, в том числе, историю поиска в сети и посещенные вебсайты — «… для улучшения качества рекомендаций, предлагаемых в службе Smart TV». Отключить такой сбор сведений, либо очень сложно, либо невозможно, но отключив, мы получаем урезанный функционал. И поэтому остается только надеяться, что информация, собираемая компаниями-производителями, действительно нужна исключительно для улучшения качества обслуживания или оптимизации потоков рекламы [4].

Низкий уровень безопасности «умных» вещей обусловлен плохой развитостью технологии в целом: понятие «интернет вещей» появилось 25 лет назад, но сама технология пришла в нашу жизнь несколько лет назад и находится в зачаточном состоянии [1].

Подводя итог, можно сделать вывод, что Smart-технологии становятся все менее безопасными. Тем, кто хочет приобрести «умные» гаджеты, нужно помнить, что за удобство придется платить, в том числе и рисками.

Литература

1. Юнна Коцар. Интернет вещей небезопасен [Электронный ресурс]: Газета.ru. URL: http://www.gazeta.ru/tech/2014/07/30_a_6152017.shtml (дата обращения: 08.01.2016).
2. Ауслендер Дмитрий. Хакеры взломали смарт-холодильник Samsung [Электронный ресурс]: Hi-News. URL: http://hi-news.ru/technology/xakery-vzlomali-smart-xolodilnik-samsung.html (дата обращения: 09.01.2016).
3. Catalin Cimpanu. Ransomware on Your TV, Get Ready, It's Coming [Электронный ресурс]: Softpedia. URL: http://news.softpedia.com/news/ransomware-on-your-tv-get-ready-it-s-coming-496685.shtml (дата обращения: 07.01.2016).
4. Умные вещи – обратная сторона медали [Электронный ресурс]: Geektimes. URL: http://geektimes.ru/company/icover/blog/268600 (дата обращения: 07.01.2016).