ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕХНОЛОГИИ УЯЗВИМОСТИ IoT

© И. У. Хашумов, М. Р. Хаджиев, Х. Х. Мальцагов
ГГНТУ им. акад. М. Д. Миллионщикова, Грозный, Россия

В данной статье рассматривается проблема информационной безопасности IoT и уязвимость в различных областях использования интернета вещей. В настоящее время мы можем найти статьи о том, как находят уязвимости, например, в такой технике, как автомобиль, холодильник или системах домашней сигнализации. Все эти вещи могут быть объединены одним термином IoT (Интернет вещей), и на сегодняшний день данная тема и данная технология является одной из самых популярных. Само название Интернет вещей (IoT) вызывает в воображении две противоречивые мысли: с одной стороны, это доступность и удобство управления любой техникой, с другой стороны, это опасность со стороны злоумышленников и хакеров, опасение за то, что, если все подключено к интернету, любой хакер может подключиться и навредить, изобретая множество способов проникновения в вашу жизнь с помощью ваших же гаджетов. В статье исследуются потенциальные риски и способы их снижения, необходимые учесть, прежде чем эксплуатировать устройства с поддержкой IoT.

Ключевые слова: IoT, умный дом, информационная безопасность, уязвимости.

Исследователи уже много лет анализируют устройства IoT, но проблемы с кибербезопасностью в мире IoT все еще сохраняются, что ставит пользователей под значительный риск. При анализе IoT были обнаружены возможные векторы атаки, влияющие как на устройство, так и на сеть в целом, к которой они подключены. Например, интеллектуальный концентратор, предназначенный для управления датчиками и устройствами, установленными дома. Он может использоваться для различных целей, таких как управление электропитанием и водой, видеонаблюдение и даже системы безопасности.

«Гаджетов Интернета вещей не бывает слишком много» – это распространенное мнение людей при покупке очередного устройства IoT с расширенными функциональными возможностями.

Эта крошечная коробка получает информацию со всех подключенных к нему устройств, и если что-то происходит или идет не так, он немедленно уведомляет своего пользователя по телефону, SMS или электронной почте в соответствии с его предпочтениями. Интересно

также и то, что концентратор можно подключить к местным службам экстренной помощи, к которым будут отправляться соответствующие оповещения. Итак, что, если кто-то сможет «взломать» систему этого умного дома и получить контроль над домашними контроллерами? Это может не только превратить в кошмар жизнь пользователя, но и нарушить функционирование экстренных служб. При проверке этой гипотезы «Лабораторией Касперского» на выставке Mobile World Congress 2018 были обнаружены логические уязвимости, предоставляющие киберпреступникам несколько возможностей для атак [1].

Правда в том, что мы не совсем понимаем всю степень риска.

Мы можем с уверенностью предположить, что для каждого гаджета «умного дома» определенные злоумышленники заняты поиском своей «ахиллесовой пяты» в безопасности.

Давайте рассмотрим возможные сценарии, чтобы увидеть, насколько плохими они могут быть.

В прошлом атаки со стороны ботнета Mirai не только выводили из строя умные устрой-

ства, но и парализовали некоторые сегменты сети Интернет.

Согласно недавнему отчету Касперского, Mirai явился в свое время наиболее опасной угрозой, поскольку он один несет ответственность за 21 процент всех IoT-атак.

27 октября 2016 года произошла одна из крупнейших DDoS-атак в новейшей истории против Netflix, GitHub, Reddit, Twitter, Airbnb, Amazon, а также крупнейшего провайдера DNS, точнее говоря, после атаки в пятницу 21 октября на управляемую DynDNS-инфраструктуру, который затронул многих пользователей в нисходящем направлении. Хотя личность и мотивы хакеров все еще неясны, эксперты по безопасности говорят, что это могла быть попытка вымогательства или просто рекламная акция. Фирма Flashpoint, специализирующаяся на кибербезопасности, проследила широко распространенное отключение IoT-устройств, зараженных ботнетом, которые затем использовались для запуска массивной DDoS-атаки. Заражение IoT было выполнено с помощью вредоносной программы Mirai.

Причина того, что такая атака стала возможна, заключается в том, что после покупки IoT устройств в целях предполагаемого удобства или по незнанию пользователи не меняют заданные по стандарту разработчиком пароли, которые соответствуют друг другу, и знание одного пароля позволяет ботнету получить доступ к огромному числу устройств [3].

Однако даже смена пароля не дает абсолютной защиты IoT устройств в вашем доме, так как большинство пользователей использует широко распространенные пароли, такие как: qwerty, 12345 и т.д., что практически не отличается от оставления пароля по умолчанию, так как взлом такого пароля занимает лишь несколько секунд.

Однако даже подбор качественного пароля не дает гарантии безопасности, ведь возникает проблема попыток входа в систему и отсутствия шифрования в приложениях IoT для смартфонов.

Источники уязвимостей Internet-of-Things

В первую очередь источник уязвимости IoT – это сами пользователи, легкость покупки и использования устройств «Интернета вещей» при-

водит к тому, что они воспринимаются людьми как обычные бытовые приборы, не углубляясь в инструкцию, не понимают, что необходимо что-то менять в настройках по умолчанию.

Обманчивая простота устройств Интернета вещей.

Для удобства и простоты использования умных устройств производители не добавляют более одного пароля, а для меньшего потребления электроэнергии не используют технологии и способы шифрования.

Проблемы присутствуют не только в бытовых устройствах IoT, но и в промышленных – IIoT, Industrial Internet of Things.

В январе было обнаружено семь серьезных уязвимостей в Things Pro Suite, шлюзе IIoT и диспетчере устройств, разработанном Мохаммеда.

Задача ThingsProSuite – сбор данных с технологических сетевых устройств. Используя ошибки в прошивке, хакеры могут получить административный доступ к шлюзу и выполнить любые команды на нем.

Стоит отметить, что вы можете обнаружить уязвимые устройства Мохаммеда и получить контроль без глубоких технических знаний.

Стремясь сделать использование IoT максимально прозрачным, разработчики автоматизируют установку обновлений прошивки устройства.

С одной стороны, это позволяет своевременно устранять выявленные недостатки и уязвимости. С другой стороны, простота процедуры позволяет заменить исходный файл прошивки вредоносным ПО.

После такой установки обновления есть возможность выхода устройства из строя или его переход под чужой контроль.

Вредоносная программа BrickerBot, эпидемия которой была зарегистрирована в 2017 году, взломала устройства IoT с помощью словарной атаки и запустила несколько команд Linux, после чего интеллектуальное устройство превратилось в бесполезный кирпич.

Компрометируя устройства IoT и IIoT, киберпреступники преследуют весьма конкретные цели, связанные с коммерческим использованием захваченных ресурсов.

Популярными вариантами являются создание бот-сетей для анонимной рассылки спа-

ма и распространение вредоносных программ, а также промышленный шпионаж.

В 2016 году было выявлено массовое использование роутеров для «DNS-угона» – атака с подменой DNS.

Программы DNSChanger и Switcher заменили адреса DNS-серверов в настройках маршрутизаторов на адреса злоумышленников для отображения рекламы и распространения вредоносных программ на устройствах, подключенных к маршрутизаторам.

Лечение клиентского компьютера в таких случаях не помогает, поскольку источник проблем находится в роутере.

Спам-атака

Большая часть IoT-устройств работает под управлением ОС Linux, богатый функционал которой позволяет устанавливать дополнительные компоненты. Установка прокси-сервера SOCKS позволяет использовать устройство в качестве анонимайзера, чтобы, оставаясь ненайденным, устраивать массовые рассылки спама и взламывать корпоративные сети.

DDoS-атаки

Наиболее распространенный способ использования взломанных устройств IoT – это организация бот-сетей для проведения распределенных атак типа «отказ в обслуживании» (DDoS). Несколько факторов облегчают эту задачу.

Все устройства IoT / PoT подключены к Интернет-каналу, часто с избыточной для него пропускной способностью.

Протокол CoAP, который используется для взаимодействия с различными «умными» устройствами, идеально подходит для организации DDoS: он использует протокол UDP без установления соединения и включает в себя отправку пакета данных в ответ на запрос.

Согласно исследованию TrendMicro, используя возможность передачи блоков, предоставляемую протоколом CoAP, можно сформировать такой запрос, чтобы ответ устройства был в 32 раза больше, чем самого запроса, обеспечивая 32-кратный коэффициент усиления. Таким образом, для организации атаки с пропускной способностью 32 Мбит/с злоумышленнику необходим только канал с пропускной способностью 1 Мбит/с.

Эта особенность протокола CoAP ставит его в один ряд с протоколами DNS и SSDP, коэффициенты усиления которых составляют от 28х до 98х и от 30х до 64х соответственно. Они также часто используются для DDoS-атак. По данным TrendMicro, Россия находится на третьем месте в мире по количеству уязвимых серверов CoAP.

Риски и уязвимости Интернета вещей

Умные устройства присутствуют во всех сферах человеческой деятельности, окружают нас дома и на работе. В этих условиях риску подвергаются практически все: от частных лиц до промышленных гигантов.

Взяв под контроль кардиостимулятор, преступники могут шантажировать родственников пациента, или, организовав бот-сеть из умных лампочек, могут заглушить все сети Wi-Fi в городе [2].

Google Chromecast – взлом IoT для начинающих

Chromecast – это устройство или недорогой USB-накопитель, способный передавать потоковое видео с любого гаджета на телевизор или другой экран. Динамика работы данного устройства: пользователь производит процедуру подключения к HDMI телевизора. Далее Chromecast подключается в домашнюю сеть Wi-Fi для произведения предварительной настройки. После установления соединения с гаджетом WLAN деактивируется, и происходит установление соединения с домашней сетью WLAN пользователя.

Таким образом, информация, которая высвечивается на экране, может транслироваться злоумышленником. Алгоритм действия: злоумышленник заменяет «прошивку» с мощеннического устройства на основе микрокомпьютера RaspberryPi. Устройство Chromecast включает собственный модуль Wi-Fi, Google Chromecast автоматически подключается к устройству злоумышленника, чтобы контент мог быть перехвачен хакером.

В данном случае необходимо выключить телевизор, отключить Wi-Fi и дожидаться, пока хакер прекратит атаку.

Главным ограничением атаки является то, что злоумышленник должен находиться в зоне действия сети Wi-Fi, к которой подключен це-

левой Chromecast. Однако в нашем собственном эксперименте мы обнаружили, что это не обязательно ограничение, если есть дешевая направленная антенна Wi-Fi и программное обеспечение на базе ОС KaliLinux. Chromecast можно «прокручивать» на гораздо большее расстояние, чем обычный диапазон сигналов для домашних сетей Wi-Fi. Это означает, что, если хакер атакует по первому сценарию – находясь в поле зрения невооруженного глаза, есть риск быть замеченным сердитым владельцем Chromecast, что затруднительно при атаке посредством направленной антенны [4].

Эта «находка» не может рассматриваться как новое открытие в области безопасности. Это только расширяет ранее известные и еще не решенные проблемы безопасности.

Риск: контент на экране жертвы передается от источника злоумышленника.

Смягчение: используйте эту опцию в отдаленных районах вашего дома, поскольку это снижает риск направленных антенн.

Статус: не зафиксирован.

Исследование уязвимости IP-камер.

В 2013 и 2015 годах был случай, когда хакеры взламывали радионяню и разговаривали с детьми через её динамики.

Производитель исследуемой IP-камеры позиционировал её в качестве радионяни. Вы кладете камеру в детскую, устанавливаете приложение на свой смартфон, подключаете камеру к приложению и Wi-Fi, и все готово: вы можете наблюдать за ребенком в любое время и в любом месте.

После изучения этих устройств стало известно, что они используют два приложения для связи с камерой, у обоих из которых были проблемы с безопасностью. Позже поставщик обнаружил, что одно из этих приложений устарело, но все еще использовалось рядом владельцев камер. Было также обнаружено, что это устаревшее приложение содержит жестко закодированные данные для учетной записи Gmail:

```
public static final String EMAIL_FROM =
«*****@gmail.com»;
```

```
public static final String EMAIL_
PASSWORD = «*****»;
```

```
public static final String EMAIL_SMTP_
```

```
HOST = «smtp. gmail. com»;
```

```
public static final String EMAIL_
USERNAME = «*****@gmail. com».
```

Позже продавец сообщил, что учетная запись использовалась для сбора отчетов о технических проблемах от пользователей камеры.

Проблема в том, что отчеты были отправлены с их собственных учетных записей электронной почты на эту предварительно установленную учетную запись. Злоумышленникам даже не нужно было покупать камеру. Все, что им нужно было сделать, это загрузить и перепроектировать одно из приложений, чтобы получить доступ к технической учетной записи электронной почты и собрать адреса электронной почты всех пользователей камеры, у которых возникли технические проблемы. Является ли серьезной проблемой то, что ваша электронная почта может быть раскрыта третьим лицам из-за использования этой уязвимости? Однако возможно, что эта уязвимость не является привлекательной целью для массового сбора личной информации, в первую очередь из-за ее относительно небольшой базы жертв. Технические проблемы редки, и приложение было старым и не актуальным уже к моменту исследования [5, 6].

Следующий риск: полный контроль над камерой со стороны злоумышленника.

Еще одна интересная проблема была обнаружена в следующей версии приложения.

Приложение связывается с камерой через облачный сервис, а соединение между приложением и облачным сервисом шифруется с использованием протокола https.

В таких обстоятельствах нетрудно представить реальный вариант использования приложения, в котором участвует сторонний разработчик.

Уязвимость исправлена. Третья проблема, обнаруженная при исследовании камеры, управляемой смартфоном, заключалась не в приложении, а в самой камере – заводской пароль root для SSH в прошивке. Это легко выяснить, так как приложение камеры работает в ОС Linux, и с паролем root использовать режим разработчика может любой, кто имеет доступ к устройству и знает пароль. С прошивкой камеры можно делать все: ме-

нять, удалять. Злоумышленнику нужно только последовательно загрузить и затем извлечь прошивку с веб-сайта производителя (для получения URL-адреса, с которого загружается прошивка, злоумышленник должен находиться в той же сети, что и атакованное устройство), распаковать его и выполнить следующие инструкции [7,8].

Второе предположение –разработчики просто забыли, что они оставили пароль в прошивке. Как показали наши исследования, часть устройства, где были обнаружены пароли SSH – чипсет – обычно предоставляется третьей стороной. По умолчанию сторонний поставщик услуг оставляет пароль SSH в камере, чтобы поставщик конечного продукта

(радионяня) мог настраивать набор микросхем и связывать его с другим оборудованием и программным обеспечением. Таким образом, конечный производитель делает это, а затем просто забывает удалить пароль. Уязвимость уже исправлена.

Выводы: Производители делают все возможное, чтобы заботиться о кибербезопасности устройств, которые они производят, что хорошо. Тем не менее, любое подключенное управляемое приложением устройство, которое называется устройством IoT, почти наверняка будет иметь хотя бы одну проблему безопасности. Однако вероятность того, что они будут критическими, или неисправимыми, не так высока.

ЛИТЕРАТУРА

1. Муравицкий А. А., Дащенко В. А., Сако Р. В. // Взлом IoT: как взломать умный дом снова 2018. [Электронный ресурс] // ResearchGate. URL: <https://securelist.com/iot-hack-how-to-break-a-smart-homeagain/84092/> (в свободном доступе).
2. Кондрашин М. А. // Уязвимости IoT: как злоумышленники могут взломать ваши устройства? 2019. [Электронный ресурс] // Research Gate. URL: <https://rb.ru/opinion/uyazvimosti-iot> (в свободном доступе).
3. Mirai Botnet против Дун – атака, обрушившая половину американского интернета 2016. [Электронный ресурс] // Research Gate. URL: <https://www.globaldots.com/blog/mirai-botnet-vs-dyn-attack-brought-half-us-internet> (в свободном доступе).
4. Анюшен В. А., Крылов В. И. Выживание в мире с поддержкой IoT. Как использовать смарт-устройства и оставаться в безопасности от хакеров 2015. // [Электронный ресурс] // Research Gate. URL: <https://securelist.com/surviving-in-an-iot-enabled-world/72595/> (в свободном доступе).
5. Кычкин А. В., Артемов С. А., Белоногов А. В. Распределенная система энергомониторинга реального времени на основе IoT // Датчики и системы. 2017.
6. Финогеев А. А., Финогеев А. Г., Нефедова И. С. Технология конвергентной обработки данных в защищенной сети системы мониторинга // Фундаментальные исследования. 2015.
7. Kelly D. T., Suryadevara N. K., Mukhopadhyay S. C. Towards the implementation of IoT for environmental condition monitoring in homes, IEEE Sensors Journal // Vol. 13, 2013.
8. Osuwa A. A., Ekhorgbon E. B., Fat L. T. Application of artificial intelligence in Internet of Things. In 2017 9th international conference on computational intelligence and communication networks (CICN), IEEE // New York 2017.

FORMATION SECURITY TECHNOLOGY AND VULNERABILITY OF IOT

© I. U. Khashumov, M. R. Khadzhiev, Kh. Kh. Maltzagov

GSTOU named after acad. M. D. Millionshchikov, Grozny, Russia

This article addresses the issue of IoT information security and vulnerability in various areas of the use of the Internet of things. Currently, we can find articles on how to find vulnerabilities, for example, in such techniques as a car, a refrigerator or home alarm systems. All these things that can be united by one term IoT (Internet of things), and today this topic and this technology is one of the most popular. The very name of the Internet of Things (IoT) conjures up two conflicting thoughts on the one hand, it is the accessibility and convenience of controlling any technology on the other hand, it is a danger from intruders and hackers, the fear that everything is connected to the Internet, any hacker can connect and harm by inventing millions of ways to enter your life with your gadgets. The article examines the potential risks, and the likelihood of their reduction, before using devices with IoT support.

Keywords: IoT, information security, smart home, vulnerabilities.

REFERENCES

1. *Muravitsky, A. A., Dashchenko, V. A. and Sako, R. V.* (2018) [Vzлом IoT: kak vzlomat' umnyi dom snova [Hacking IoT: how to hack a smart home... again], available at: <https://securelist.com/iot-hack-how-to-break-a-smart-home-again/84092/>
2. *Kondrashin, M. A.* (2019) IoT Vulnerabilities: How Can Attackers Hack Your Devices? [Uyazvimosti IoT: kak zloumyshlenniki mogut vzlomat' vashi ustroystva?], available at: <https://rb.ru/opinion/uyazvimosti-iot/>
3. Mirai Botnet against Dyn – an attack that brought down half of the American Internet in 2016, available at: <https://www.globaldots.com/blog/mirai-botnet-vs-dyn-attack-brought-half-us-internet>
4. *Alyushin, V. A. and Krylov, V. I.* (2015) Vyzhivanie v mire s podderzhkoi IoT. Kak ispol'zovat' smart-ustroystva i ostavat'sya v bezopasnosti ot khakerov [Surviving the world with IoT support. How to use smart devices and stay safe from hackers], available at: <https://securelist.com/surviving-in-an-iot-enabled-world/72595>
5. *Kychkin A. V., Artemov S. A., Belonogov A. V.* IoT-based distributed real-time energy management system // Sensors and Systems. 2017.
6. *Finogeev A. A., Finogeev A. G., Nefedova I. S.* The technology of convergent data processing in a secure senti monitoring system // Fundamental Research. 2015.
7. *Kelly D. T., Suryadevara N. K., Mukhopadhyay S. C.* Towards the implementation of IoT for environmental condition monitoring in homes, IEEE Sensors Journal // Vol. 13, 2013.
8. *Osuwa A. A., Ekhoragbon E. B., Fat L. T.* Application of artificial intelligence in Internet of Things. In 2017 9th international conference on computational intelligence and communication networks (CICN), IEEE // New York 2017.