О конфиденциальности корпоративных сетей. Часть 6

В статье приводятся данные о сборе производителями умных устройств, в том числе «подключенных» автомобилей и устройств Интернета вещей, информации о пользователях этих устройств. Обращается внимание на имеющиеся уязвимости и низкий уровень информационной безопасности умных устройств и их облачных хранилищ. Указывается на потенциальную опасность для сотрудников и руководителей различных организаций, вызванную возможным использованием такой информации спецслужбами иностранных государств или криминальными структурами.

Ключевые слова: Интернет вещей, умные устройства, сбор информации, информационная безопасность, слежка, манипуляции

Георгий Георгиевич Петросюк,
директор департамента информационных технологий
petrosyukgg@nrczh.ru

Иван Сергеевич Калачев,
начальник отдела департамента информационных технологий
kalachevis@nrczh.ru

ФГБУ «Национальный исследовательский центр «Институт имени Н. Е. Жуковского»

Андрей Юрьевич Юршев,
кандидат технических наук, ведущий эксперт направления «Защита АСУ ТП»
ГК «ИнфоВотч»
ay@infowatch.com

После прочтения всего написанного нами ранее[1] может сложиться впечатление, что за вашей организацией и лично вами ведется тотальная слежка. И как бы ни хотелось сейчас услышать обратное, подтверждаем: вы правы, ведется! Ведь кроме сбора информации о корпоративных сетях организаций и об их работниках, про который мы писали в предыдущих статьях, существуют еще и другие методы слежения и сбора данных. Постараемся осветить хотя бы часть из них, не утомляя читателей техническими подробностями, корректное отображение которых потребует другого формата и объема публикации.

Начнем с огромной и уже всеобъемлющей сферы умных гаджетов, например, таких как умные очки (HoloLens от Microsoft, Google Glass и др.), которые для использования должны быть подключены к «своим» облакам и могут скрытно следить за своим владельцем[2], или набирающие популярность умные колонки (как производимые ИТ-гигантами Google Home Max и Apple HomePod, Amazon Echo, Яндекс.Станция так и другими производителями – Xiaomi Mi AI Speaker, LG ThinQ, JBL Link и др.), постоянно подключенные к облачным сервисам (а также подключаемые и к системам умного дома),

En About the Privacy of Enterprise Networks. Part 6

G. G. Petrosiuk,
Director of IT Department
petrosyukgg@nrczh.ru

I. S. Kalachev,
Head of IT Operations and Helpdesk Department
kalachevis@nrczh.ru

The National Research Center Zhukovsky Institute

A. Y. Yurshev,
PhD (Eng.), Leading Expert of the Divison «Cyber Security of Industrial Automation»
InfoWatch
ay@infowatch.com

The article provides data on the collection by manufacturers of «smart» devices, including «connected» cars and «Internet of things» devices, information about users of these devices. Attention is drawn to the existing vulnerabilities and low level of information security of smart devices and their cloud storage. The potential danger for employees and managers of various organizations caused by the possible use of such information by special services of foreign states or criminal structures is indicated.

Keywords: Internet of things, smart devices, information gathering, information security, surveillance, manipulation

[1] *См. «Защита информации. Инсайд», №№ 3–6'2018, 3'2019.*
[2] *https://www.securitylab.ru/news/450767.php.*

всегда «слушающие» окружающее пространство, при этом использующие аккаунты пользователей только в «своих» облаках (они же зачастую совпадают с аккаунтами в смартфонах, которые уже знают о вас многое) с соответствующими последствиями – от несанкционированного включения из-за ошибок распознавания голосовых команд и пересылки разговоров сторонним «слушателям» до санкционированного прослушивания их производителем или его подрядчиками всех услышанных разговоров[3] или проникновения в корпоративные сети организаций[4].

Подобных умных гаджетов очень и очень много: даже детские игрушки, коляски и игрушки для «взрослых», и те активно следят за своими потребителями[5]. И практически все они привязываются к смартфонам своих владельцев и их учетным данным. Насколько «глубоко» хотят следить за пользователями производители этих гаджетов? А главное, ради чего? Чтобы «сделать свои устройства лучше»?

Теперь уже не приходится удивляться тому, что в сегодняшнем мире даже в кинотеатрах собирается информация о поле, возрасте и эмоциях зрителей при просмотре каждого фильма (рис. 1). Наверное, эта информация «крайне необходима» владельцу кинотеатра. Но зачем последнему содержать собственную инфраструктуру хранения данных – он тоже старается минимизировать свои издержки и зачастую хранит ее в облаках.

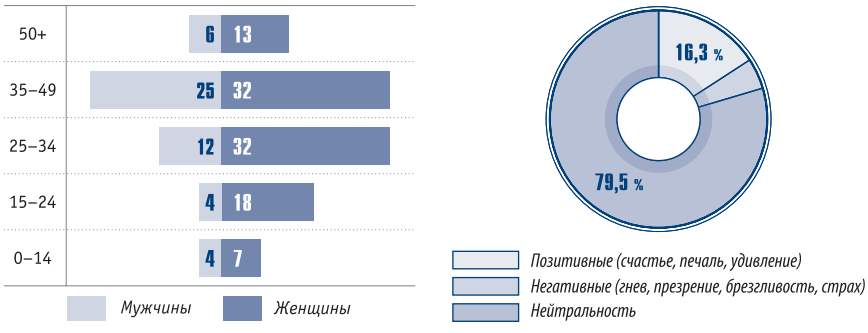
Некоторые крупные авиакомпании также подозреваются в слежке за своими пассажирами с помощью встроенных в бортовые видеосистемы кресел авиалайнеров видеокамер. А самолетами пользуются очень многие, в том числе бизнесмены, политики…

Ранее мы отмечали, что во многих магазинах и кафе установлены камеры видеонаблюдения, но мы хорошо знаем, что их использование уже давно вышло за стены организаций. Сегодня они расположены на входных дверях подъездов жилых домов и внутри них, в общественном транспорте, на улицах и много где еще. Часть из них подключена к системам распознавания лиц, походки или поведения, а в скором будущем человека можно будет опознать лишь по силуэту[6]. Причем многие системы видеонаблюдения принадлежат частным компаниям. Можно ли утверждать наверняка, в чьих интересах они собирают информацию (хранят ее они, как правило, опять же в облаках, причем, зачастую за границей Российской Федерации)?

Все большую популярность завоевывают появившиеся в последние несколько лет умные камеры, подключенные к системам искусственного интеллекта (которые всегда размещаются в своих облаках) и умным домам, оснащенные микрофоном и колонками, способные распознавать лица людей, отслеживать их перемещения, классифицировать объекты, реагировать на изменения обстановки, следить за микроклиматом и пр. Управляются они в большинстве случаев также из «своих» приложений для смартфонов, а устанавливаются не только в умных домах или в организациях, но и на автомобилях, и на «бытовых» квадрокоптерах. Все собранные с их помощью данные (видео, звук и телеметрия) также хранятся и обрабатываются в «зарубежных» облаках с доступом к ним, как минимум, сотрудников производителя. Ну и по недоброй традиции, производители «делятся» собранной информацией с киберпреступниками, так как, по информации SAM Seamless Network, подключенные к Интернету видеокамеры составляют почти половину всех скомпрометированных IoT-устройств.

Большое распространение в последнее время получили и системы распознавания голоса, которые используются как государственными организации, так и частными компаниями (те же самые умные колонки и не только). А современные нейросети позволяют не только распознать голос говорящего, но и учатся по голосу формировать его внешность[7] (рис. 2). И вот уже производитель умной колонки или владелец облака знает всех гостей вашей вечеринки! И не просто знает, а может и «портрет нарисовать».

Системы охранного видеонаблюдения вкупе со СКУД также достоверно идентифицируют пользователей, фиксируют график и траекторию их передвижения по предприятию и их поведение. Такие системы, как правило, имеют встроенную в оборудование функцию облачной аналитики и записи видеопотоков в облака. В большинстве своем это необходимо для обеспече-



а *б*

Рис. 1. ***Результат анализа просмотра фильма «Лёд» в одном из отечественных кинотеатров: а) половозрастная диаграмма, б) эмоции людей за сеанс***

[3] *http://d-russia.ru/podryadchiki-apple-regulyarno-proslushivayut-konfidentsialnuyu-informatsiyu-zapisej-siri-smi.html.*
[4] *https://xakep.ru/2018/05/25/amazon-alexa-spy-on-you/.*
[5] *https://habr.com/ru/post/408175/.*
[6] *http://tehnika.expert/novosti-texniki/teper-opoznat-cheloveka-mozhno-po-siluetu.html.*
[7] *https://habr.com/ru/news/t/454360/.*

ния безопасности и самих работников, и организаций в целом. Помимо прочего, эти системы не лишены своих уязвимостей, которые могут использоваться или используются для несанкционированного вмешательства[8].

Так что некоторые системы безопасности сами по себе совсем не безопасны, требуют защиты, или еще хуже – создают угрозы для защищаемого объекта и его обитателей. А ведь некоторые из них стоят на страже и частных/личных и государственных объектов различной степени важности. А информация о взломе систем безопасности таких объектов лежит в Интернете в открытом доступе и доступна как спецслужбам различных государств, так и криминальным или террористическим организациям.

И сами защищаемые объекты становятся все умнее благодаря так называемым системам умного дома (часть которых сразу же строятся в облаках Google, Amazon или др.), состоящих из огромного класса устройств. Они тоже содержат в себе как критические уязвимости, так и тайно встроенные системы слежения, как, например, скрытые микрофоны в устройствах домашней безопасности Google Nest Secure, управляемые через облачный сервис Google Assistant, и привязанные к учетной записи владельца «умного дома». Ох уж этот Google! Какая же «слежка» обходится без него! Он уже знает обо всем, что происходит в его умном доме с его владельцами и под его же охраной! А сколько еще других умных вещей различных производителей собирают и хранят данные в облаках Google!

Практически все эти гаджеты и системы потому и «умные», что им нужен постоянный доступ в сеть Интернет, к какому-либо облаку своего производителя, без чего они или перестают работать совсем, или создают проблемы своим владельцам. Управляются же они «своим»

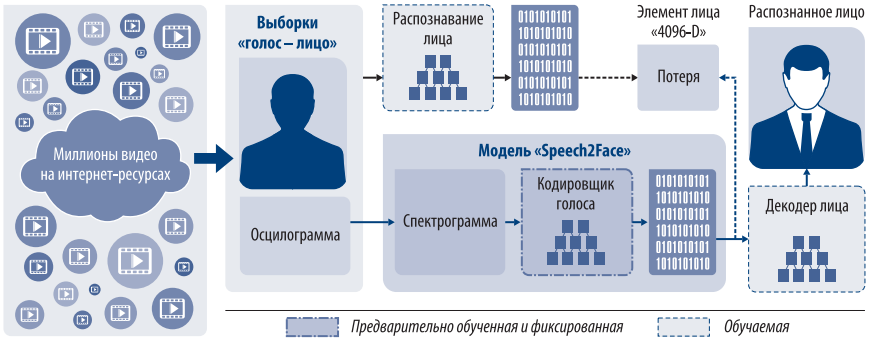


Рис. 2. ***Схема формирования портрета на основе голосовых данных***

приложением на смартфоне (о «безопасности» которых мы уже говорили). Плюс ко всему, в подавляющем большинстве случаев для их подключения используются домашние сети Wi-Fi, построенные на уязвимых роутерах, в том числе и лидеров рынка, таких как Cisco, Linksys и др.

При этом стоит отметить, что не только злоумышленники, но и сбой на сервере производителя или изменения в законодательстве, могут сделать умные дома, устройства и даже такие «умные» автомобили, как «Тесла», просто бесполезными «железками»[9].

А как обстоят дела с очень широко распространенными в наших домах устройствами – так называемыми смарт-телевизорами, обязательно подключаемыми к Интернету, в том числе с голосовым управлением (использующими, например, Google Assistant, Alexa и др.), коих в России, согласно исследованию Avast[10], более 46 % от всех умных устройств? Помимо уже известных функций записи и передачи звука со встроенных микрофонов, устанавливаемых в телевизорах и в пультах управления (в том числе и для слежения), встроенных за поверхность экрана и теперь уже неотключаемых видеокамер для записи и передачи видео и аутентификации по лицу или проведения видеозвонков, в некоторых моделях появились функции распознавания эмоций человека, проявляемых в ответ на определенные ТВ-сюжеты, и даже функции охранной системы. Ну и смарт-телевизоры аналогично умным колонкам постоянно передают информацию своим производителям, да и не только им[11].

Смарт-телевизор – это тот же компьютер, работающий под управлением своей ОС: Android TV (Google уже и в телевизорах!), Tizen от Samsung, webOS от LG и др. Однако в этот компьютер, в отличие от традиционного, пользователь не может установить средства информационной безопасности. Что дал производитель, тем и пользуемся. А встречающаяся в ряде моделей функция блокирования следящей активности вполне может оказаться бутафорской. При этом функционал смарт-телевизоров обновляется с каждой новой «прошивкой». Но знаем ли мы об этих изменениях, вносимых в новые версии «прошивок», разве производители телевизоров нам об этом сообщают? Да и многие ли из потребителей знают, что умные телевизоры обновляют свое программное обеспечение? А ведь установлены они не только в наших домах, но и в переговорных комнатах, кабинетах руководителей, приемных и иных помещениях наших организаций, и как правило, они тоже подключены к сети Интернет.

Сбором персональной информации о владельцах своих автомобилей занимаются и автопроизводители, например, Ford[12], причем не только по заявкам на кредит, но и удаленно собирая данные с мультимедийных

[8] *https://www.securitymedia.ru/news_one_5667.html.*
[9] *https://threatpost.ru/novyj-zlovred-delaet-iot-ustrojstva-bespoleznymi-kirpichami/21374/.*
[10] *https://www.securitylab.ru/news/498109.php.*
[11] *https://www.securitylab.ru/news/501197.php.*
[12] *https://www.securitylab.ru/news/496626.php.*

Таблица. ***Уязвимости в программном обеспечении автомобилей БМВ***

№ п.п.	Описание уязвимости	Тип доступа	Затрагиваемые компоненты	Справка
1	Вся подробная информация была удалена из соображений безопасности	Local (USB)	HU_NBT	CVE-2018-9322
2		Local (USB/OBD)	HU_NBT	
3		Remote	HU_NBT	Logic Issue
4		Remote	HU_NBT	Reserved
5		Local (USB)	HU_NBT	CVE-2018-9320
6		Local (USB)	HU_NBT	CVE-2018-9312
7		Remote (Bluetooch)	HU_NBT	CVE-2018-9313
8		Physical	HU_NBT	CVE-2018-9314
9		Physical	TCB	Reserved
10		Remote	TCB	Logic Issue
11		Remote	TCB	CVE-2018-9311
12		Remote	TCB	CVE-2018-9318
13		Indirect Physical	BDC/ZGW	Logic
14		Indirect Physical	BDC/ZGW	

систем и систем навигации посредством подключения автомобилей к Интернету, причем с целью увеличения своих доходов. В компании, правда, не конкретизируют, как именно они намерены монетизировать данные более 100 млн владельцев автомашин (данные по США) для повышения прибыли. По мнению же экспертов из компании Otonomo из Тель-Авива, к 2020 году солидная часть заработка автомобильных компаний будет формироваться именно за счет продажи таких данных третьим лицам.

Другие производители авто тоже не отстают от «моды»[13]. Поэтому все больше и больше автомобилей подключается к сети Интернет. Так, в 2017 году, по данным аналитического агентства Chetan Sharma Consulting, в США к сотовым сетям было подключено больше автомобилей, чем смартфонов. В частности, американский оператор связи AT&T подключал более миллиона автомобилей каждый квартал, а по оценкам, сделанным еще в 2018 году, более 98 % новых автомобилей будут оснащены модулем связи. По прогнозу генерального директора уже упоминавшейся компании Otonomo, в 2020 году на автодороги выедет уже четверть миллиарда сетевых автомобилей, и все они станут снабжать своих производителей телеметрической и иной информацией о себе и своих владельцах.

Но ведь автомобили продаются во всех странах мира, и данные владельцев «подключенных» автомобилей (в том числе личных и служебных автомобилей сотрудников и руководителей наших организаций) со всего мира будут стекаться к своим производителям (в США, Германию, Японию и т. д.) или в «заграничные» облака. Те же, в свою очередь, могут продавать их по своему усмотрению, например, страховым компаниям. Или «добровольно» передавать их специальным службам своей страны.

Помимо того, что утечки собранных таким образом данных могут реально создать угрозы водителям – от кражи их «ласточек» до несанкционированного вмешательства в процесс управления автомобилем, последние сегодня являют собой даже не один, а несколько (по некоторым данным – до 30–40) компьютеров на колесах, а их системы управления (фактически все произведенные за рубежом) составляют миллионы строк кода и, соответственно, содержат программные уязвимости (см. табл.), эксплуатировать которые могут и специальные службы, и криминальные или иные деструктивные элементы. А процесс компьютеризации автомобилей только набирает обороты.

И сколько аварий по вине некачественного программного обеспечения или внешнего вмешательства в управление автомобилем уже произошло? Наверное, мы об этом никогда не узнаем. Ведь после аварий и улик-то не остается! Да и кто анализирует, какие команды поступили на те или иные элементы управления автомобилем перед аварией? Где черный ящик «подключенного» автомобиля? А ведь еще с октября 2014 года в ЦРУ специально изучают различные системы контроля, разработанные для автотранспорта. Может быть, для проведения удаленных «спецопераций»?

Системы же защиты самих автомобилей настолько уязвимы, что позволяют открыть (и тайно установить любое, в том числе и подслушивающее устройство) или угнать автомобиль без каких-либо серьезных проблем для нарушителя[14]. Уже имеется и программное обеспечение для смартфонов для управления умными автомобилями или сигнализациями к ним. И оно тоже небезопасно. А есть еще автомобили каршеринга со своей телеметрией и со своими мобильными клиентами. И эти автомобили, и сами мобильные приложения к ним, тоже следят за водителями (рис. 3).

Даже электронные самокаты, и те уязвимы к внешнему несанкционированному воздействию, в них также присутствуют уязвимости, например, в смарт-самокате Lime, «самостоятельно(?)» блокирующем во время движения переднее колесо с травма-

[13] *https://auto.newsru.com/article/17jan2018/bigbrotherwatch/.*
[14] *https://autoreview.ru/articles/ugon-shou/klyuch-s-pravom-peredachi/.*

тическими последствиями для едущего человека[15].

Все эти умные гаджеты, устройства, автомобили, датчики и системы являются частью такого модного и стремительно распространяющегося Интернета вещей (IoT). По прогнозам Gartner, количество этих вещей в 2021 году превысит 46 млрд (включая и снабженные процессорами ARM Cortex R4 со всеми их возможностями, о которых мы писали в предыдущей статье).

Не забудем также особенно актуальные для корпоративных пользователей «следящие» и уязвимые аксессуары к мобильным устройствам (о них мы уже писали), принтеры или МФУ (передающие производителям данные о том, что печатают[16]), «умная» одежда и обувь (в том числе и опять от Google, см. например[17], модные аксессуары, фотоаппараты, смарт-протезы, оснащенные SIM-картой и отправляющие данные в Интернет, имплантанты, например кардиостимуляторы, содержащие уязвимости («спецоперации» уже можно выполнять «не выходя из дома»), иные медицинские устройства, охранные и пожарные сигнализации, замки, системы отопления (в том числе газового) и кондиционирования, пылесосы с микрофонами и инфракрасными камерами или уже встроенными системами охраны, холодильники, кофеварки, кухонные и микроволновые печи со встроенными видеокамерами, даже электрические розетки и лампы освещения (да-да, они тоже умные, и тоже могут представлять угрозу) и даже, извините, умные унитазы с Wi-Fi и приложениями для смартфонов.

И вновь констатируем, что практически все интернет-вещи управляются со смартфонов и, соответственно, привязаны к учетным записям их владельцев на серверах Google или Apple. А ведь есть еще и огромное число чисто IoT-устройств, устанавливаемых на наших промышленных предприятиях, объектах, в многоквартирных и частных домах.

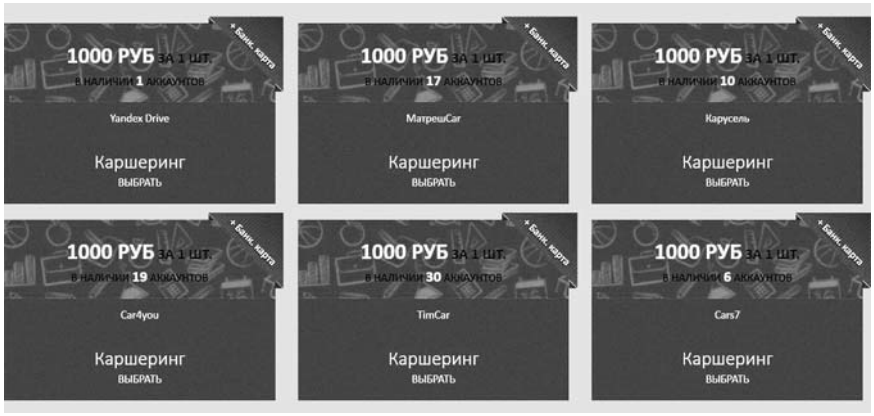


Рис. 3. ***Перечень аккаунтов каршеринга на продажу***

Получается, что следят за пользователями (работниками/руководителями наших организаций) и за самими организациями все устройства, хоть каким-то образом получившие «электронные мозги» и коммуникации. А подавляющее большинство этих устройств произведено иностранными компаниями.

Интернет вещей – это практически вся личная жизнь человека. И кто знает, какие из всего многообразия этих «вещей» помимо уязвимостей содержат специально оставленные тайные механизмы управления – так называемые бэкдоры, обеспечивающие умышленные утечки данных с этих устройств, к коим правоохранительные органы зарубежных стран имеют вполне законный доступ. Анализ этих данных может предоставить информацию о человеке, которая сделает его же жертвой шантажа или манипуляций. А знания об образе жизни и перемещениях могут пригодиться и криминальным структурам, в частности ворам, «очищающим» умные дома во время отпусков их хозяев[18].

Согласно исследованию Стэнфордского университета и компании Avast, в среднем 40 % домохозяйств по всему миру обладают хотя бы одним умным устройством, а всего в мире ***существует более 14 тыс. производителей IoT-устройств, и всего лишь 100 из них производят 94 % всех решений***. В России около 20 % домохозяйств содержит более пяти подключенных устройств. Самыми уязвимыми из них являются роутеры – 97 %, в основном по причине недостаточно сложных паролей и однофакторной аутентификации. Далее этот рейтинг выглядит так: телевизоры – 46 %, принтеры – 15 %, камеры видеонаблюдения – 11 %, медиаплееры – 9 %, планшеты – 8 %[19]. Что же касается умных домов, то в России более 44 % из них имеют одно или более умное устройство, уязвимое к кибератакам[20]. А из отчета Hewlett Packard выяснилось, что 70 % IoT-устройств имели уязвимости в безопасности учетных данных (логин и пароль), шифрование данных применялось слабо, наблюдались также проблемы с разрешением доступа. И дело даже не в том, что производители интернет-ве-

По данным компании Avast, в начале 2019 года на каждое IoT-устройство, доступное в сети Интернет, в день осуществлялось более 11,5 тысяч компьютерных атак.

[15] *https://www.securitylab.ru/news/498124.php.*
[16] *https://www.anti-malware.ru/news/2019-09-18-1447/30787/.*
[17] *https://dronreview.ru/umnaja-kurtka-google/.*
[18] *https://rg.ru/2017/01/17/kvartirnye-vory-stali-vybirat-zhertv-po-statusu-v-socsetiah.html.*
[19] *https://www.comnews.ru/content/120344/2019-06-21/milliony-iot-ustroystv-bezzashchitny/.*
[20] *https://www.securitylab.ru/news/498109.php.*

щей не спешат выпускать обновления, закрывающие уязвимости: IoT-устройства устаревают столь быстро, что создание обновлений к ним просто экономически нецелесообразно.

Взлом особенно критичен для корпоративных гаджетов, которые используют компании, в том числе для мониторинга работы сотрудников. Использование уязвимостей таких IoT-устройств – это широкие «ворота» в корпоративную сеть. В подтверждение своих слов приведем данные из отчета компании OpenDNS[21]:

- только 35 % компаний используют отдельную сеть Wi-Fi для потенциально небезопасных интернет-вещей;
- видеокамеры, медицинские гаджеты, фитнес-браслеты и другое оборудование передают данные за пределы периметра организации, и, соответственно, корпоративной сети;
- большинство телевизоров, интегрированных в IoT, не имеют сертификатов безопасности;
- устройства используют для хранения данных небезопасные облачные серверы.

Согласно информации AT&T, количество попыток просканировать устройства Интернета вещей и выявить уязвимости выросло в 30 раз за последние три года. Не работа ли это ЦРУ США? Ведь согласно упоминавшемуся в предыдущей статье отчету компании «Инфовотч», структура центра по кибербразведке ЦРУ включает в себя в том числе отдел интегрированных устройств (*Embedded Devices Branch*, EDB), разрабатывающий механизмы взлома Интернета вещей.

По данным Kaspersky Lab ICS CERT, с каждым годом растет количество кибератак, нацеленных на устройства Интернета вещей. За первую половину 2018 года его сотрудниками обнаружено втрое больше образцов вредоносного ПО, атакующего умные устройства, чем за весь 2017 год (кстати, тогда их было в 10 раз больше, чем годом ранее), при этом очень часто зараженные устройства применяются для DDoS-атак, добычи криптовалют и для проникновения в домашние сети или сети организаций, при этом по данным Positive Technologies, в I квартале 2019 года доля атак на IoT-устройства составила уже 2 % от общего количества атак.

Злоумышленники уже активно используют уязвимые IoT-устройства для целевых атак на организации и предприятия, например, в феврале 2019 года с использованием уязвимых роутеров[22] или с использованием взлома офисных принтеров и видеокодеров[23]. Но кроме роутеров, для атак могут также использоваться и устройства умного дома, смарт-ТВ, сетевые хранилища, охранные системы, промышленное оборудование IoT и даже упоминавшиеся ранее умные лампочки.

И некоторым читателям, наверное, уже и не удивительны заявления американской прессы, что спецслужбы США присутствуют в системах энергоснабжения России и активно их атакуют[24]. Но только ли энергосистему они атакуют? И только ли России? Атаки на промышленные объекты во всем мире носят уже перманентный характер, и атакам подвергаются не только организации, в том числе и гиганты индустрий, но и сектора экономики целых стран, например, Индии[25], или предприятия определенных отраслей в разных странах или целых регионах[26].

Удивительно, что даже святая святых, то что, казалось бы, должно быть абсолютно надежным, – современные системы вооружений – и те содержат программные уязвимости: ведь удалось же взломать модернизированный американский бронетранспортер Stryker Dragoon и истребитель F-15 Eagle[27].

Интересно, какую же роль в осуществлении подобных атак может играть (или играет) наличие у атакующих собранных данных о работниках/руководителях организаций и об их корпоративных сетях?

Мы уже фактически установили, что и мобильные устройства, и аксессуары к ним, и автомобили, и устройства Интернета вещей/промышленного интернета, используемые в том числе и в наших организациях и их персоналом, в большинстве своем находятся под неусыпным надзором (возможно, и управлением) их производителей, ну и, скорее всего, спецслужб США. Спецслужбы одной страны фактически контролируют почти всех пользователей умных устройств во всем мире?!

Но есть еще и «неизвестные» хакеры! Мы уже упоминали, что, по мнению WikiLeaks, архив «хакерского арсенала» ЦРУ попал в руки людей, не связанных с американскими властями. А бывает и наоборот. Например, разработчики одного из самых крупных ботнетов, состоящих из взломанных умных устройств, после ареста начали сотрудничать с ФБР[28]. Более того, до того разработчики трояна Mirai, на базе которого и работал ботнет, успели «поделиться» с хакерским сообществом своими разработками[29]. Так что в настоящее время данный инструмент в самых различных модификациях используется для совершения компьютерных атак как спецслужбами США, так и различными хакерскими группировками, в том числе атакуя и умные устройства с процессорами на архитектурах x86, ARM (про них мы ранее уже говорили), Sparc, MIPS, PowerPC, Motorola 6800 и даже ARC (широко используются для создания SOC-решений на одном чипе),

[21] *https://business-online.su/blog/internet-veshchey-problemy-bezopasnosti/.*
[22] *https://www.rbc.ru/technology_and_media/02/03/2019/5c7938b39a794723387f3e8e/.*
[23] *https://www.anti-malware.ru/news/2019-08-06-1447/30367/.*
[24] *https://tass.ru/mezhdunarodnaya-panorama/6554562/.*
[25] *https://topwar.ru/159083-indiju-ohvatili-ataki-hakerov.html.*
[26] *https://www.securitylab.ru/news/499472.php.*
[27] *https://www.securitylab.ru/news/497916.php и https://topwar.ru/161394-hakery-vzlomali-programmnyj-kod-f-15.html.*
[28] *https://xakep.ru/2018/09/20/no-jail-time-for-mirai-authors/.*
[29] *https://xakep.ru/2016/10/03/mirai-source-code/.*

которые применяются в миллиардах (!!!) стационарных и мобильных потребительских устройствах, IoT, в автомобилестроении, сетевом оборудовании и т. д.[30]

> Поверьте, сегодняшний мир гораздо более непредсказуем и опасен, чем тот, который описал Оруэлл.
>
> Эдвард Сноуден

Таким образом, общая картина с информационной безопасностью всего «умного» в целом, надеемся, понятна. Создается впечатление, что производители гаджетов, устройств, автомобилей, домов, промышленного IoT-оборудования абсолютно не заботятся об обеспечении их информационной безопасности, а качество их программного обеспечения оставляет желать лучшего. Можно ли требовать более ответственного отношения к своей продукции от производителя розеток, если, например, компания Boeing поручает написание программного кода для управления самолетом привлеченным, а не штатным сотрудникам[31] (что выяснилось в ходе расследования двух недавних катастроф с самолетами компании, повлекших сотни человеческих жертв). Безответственность в погоне за прибылью, безусловно, правит здесь бал, но стоит ли исключать возможность, что кого-то принуждают создавать продукцию с заранее встроенными каналами скрытого мониторинга и управления? А как иначе объяснить такой размах следящего и постоянно взламываемого «умного» разнообразия?

Напомним, что же еще объединяет все эти умные вещи? Большинство из них фактически ***не имеют встроенных средств информационной безопасности***. Реализованные же в отдельных изделиях ИБ-механизмы в подавляющем большинстве случаев не доступны для изменения владельцами. Также ***не предполагается установка в них каких-либо сторонних средств ИБ***. Период выпуска обновлений безопасности производителями их программного обеспечения для устранения выявленных уязвимостей, по некоторым оценкам, составляет ***от 6 месяцев до нескольких лет, а сам процесс доставки обновлений может быть скомпрометирован*** и приносить только новые уязвимости или «шпионский» функционал. И это при условии, что производитель вообще озаботился их выпуском и еще существует на рынке. При этом процесс установки таких обновлений, как правило, доступен только специалистам. Особенно опасна ситуация, связанная с владением устройствами с долгим периодом «жизни» (телевизорами, автомобилями, медицинскими устройствами, например, кардиостимуляторами). Так, по мнению старшего директора по ИБ сети больниц Ramsay Health Care Кристофера Нила, несмотря на уже существующие требования к обеспечению ИБ медицинского оборудования, оно еще на протяжении 15–20 лет будет представлять угрозу для жизни и здоровья пациентов, так как было изготовлено без учета этих требований.

Таким образом, как это ни прискорбно осознавать, владельцы умных устройств в настоящее время являются фактически заложниками производителей в вопросах обеспечения их же собственной безопасности .

Представим худший из возможных вариантов: все данные о наших гражданах, собранные в том числе и описанными нами в предыдущих статьях способами – приложениями и программным обеспечением их мобильных устройств и ПК, служебными и личными умными вещами, «подключенными» автомобилями и далее по списку стекаются, главным образом, в США и обрабатываются там в интересах иностранных компаний и спецслужб. На основе анализа собранных данных можно очень подробно узнать о всей жизни любого человека: где, кем и над чем он работает, сколько зарабатывает и где хранит сбережения, на чем, с кем и куда ездит, где живет (вплоть до плана и изображений интерьера жилища), с кем общается по служебным и личным делам, кто его родственники и где они проживают, чем питается и каково состояние его здоровья и многое-многое другое. Этакое ***полное электронное досье,*** *причем* ***с актуальными изменениями*** *фактически* ***в режиме реального времени***.

Все эти данные доступны специальным службам США (возможно и их партнерам) при поездке наших граждан за границу, вернее – уже на этапе подачи заявки на получение визы. Кроме того, даже высокоперсонифицированные данные о жителях целых стран (например, Эквадора[32]) могут по той или иной причине утечь в абсолютно неизвестном направлении. Да и какая, по большому счету, разница, данные были собраны или «утекли»? В конечном итоге они так и так попали совсем не в те руки, которым были доверены пострадавшими людьми. И стоит ли тогда удивляться различным неприятным сюрпризам, случающимся с нашими гражданами за границей?

Кто может поручиться, что нарисованная безрадостная картина – фантазия авторов, а не наша действительность? К сожалению, факты свидетельствуют, скорее, в пользу последнего.

Так, может быть, уже пора уделить этой теме самое пристальное внимание? При этом следует иметь в виду, что добиться перелома ситуации, то есть совместить необходимый обществу прогресс с обеспечением требуемого уровня безопасности граждан и государства, можно исключительно путем совершенствования федерального законодательства и разработки соответствующих обязательных к применению государственных стандартов. ■

[30] *https://xakep.ru/2018/01/18/okiru/.*
[31] *https://habr.com/ru/post/458224*
[32] *https://www.anti-malware.ru/news/2019-09-17-1447/30774/.*