УГРОЗЫ ИНТЕРНЕТА ВЕЩЕЙ и возможные методы защиты

Д.Ярушевский, старший архитектор решений, "Лаборатория Касперского" / Dmitry.Yarushevsky@kaspersky.com

УДК 004.056.57; DOI: 10.22184/2070-8963.2019.78.1.62.65

Глобальная сеть, в которой основными участниками обмена данными являются не люди, а машины, таит в себе не только те же угрозы, что и "обычный" интернет, но и ряд новых. Для того чтобы мир IoT стал действительно безопасным, нужно сделать безопасными не отдельные устройства, а все экосистемы и их взаимодействие между собой в целом.

Подключенные вещи и их угрозы

Рождением Интернета вещей (IoT) принято считать период между 2008 и 2009 годами, когда количество подключенных к интернету устройств превысило население Земли. В 2010 году, по оценкам аналитиков компании Cisco IBSG, на одного человека приходилось в среднем 1,84 устройства, подключенного к интернету. К 2020 году, по их прогнозам, это число должно достигнуть 6,58 устройств на человека [1].

Сегодня нас окружают миллиарды "умных" (и, зачастую, не очень) устройств, подключенных к глобальной сети. Устройства эти абсолютно различны как по назначению (бытовые приборы и персональные гаджеты, комплексы сигнализаций и видеонаблюдения, медиаустройства, автомобильные системы управления, производственное оборудование и т.п.), так и по возможностям. Одни устройства умеют только собирать и передавать данные телеметрии, другие представляют собой полноценный компьютер с возможностью управлять физическими объектами (электрические реле, насосы, актуаторы, приводы, и т.д.).

В настоящее время Интернет вещей сложно назвать однородным – многообразие устройств и областей их применения создает множество экосистем, кажущихся более или менее изолированными друг от друга. Медицинские приборы "общаются" друг с другом и передают данные о здоровье владельца на серверы соответствующих учреждений. "Умная" дверь пропускает в дом только собаку с авторизированным чипом на ошейнике и отправляет уведомление о возвращении питомца владельцу на смартфон. Промышленные роботы на соседней фабрике выполняют заданную программу, "отчитываясь" о производственных показателях и технических подробностях работы управляющему центру и производителям оборудования (для предиктивного ремонта, например). На первый взгляд, эти экосистемы не связаны. Но это только на первый взгляд. Во-первых, Интернет вещей – это все-таки одна глобальная сеть, в которой потенциально возможен обмен данными между любыми узлами. Во-вторых, многие связи просто не очевидны. Например, телевизоры, собирающие данные о поведении и предпочтении своих владельцев, отправляют эту информацию на серверы производителя [2]. Производитель может продать эти данные третьей стороне – и вот уже "умный" магазин на первом этаже знает, что вы предпочитаете "пить коньяк по утрам", и спамит вас целенаправленной рекламой. Или же отлично защищенный от кибервзлома и угона автомобиль использует навигационное оборудование, регулярно отправляющее диагностические данные GPS (содержащие координаты последних перемещений) на слабозащищенные серверы разработчика навигационного ПО. Атаковав эти серверы, злоумышленник может получить данные

о ваших перемещениях, даже "не притрагиваясь" к автомобилю.

Таким образом, глобальная сеть, в которой основными участниками обмена данными являются не люди, а машины, таит в себе ровно те же угрозы, что и "обычный интернет", плюс ряд новых. Отличительной особенностью Интернета вещей является возможность взаимодействия с реальным, физическим миром. Сенсоры устройств измеряют свойства окружающего мира. На основе этих данных управляющая программа устройства в автоматическом режиме или же человек-оператор принимает решение о запуске того или иного управляющего воздействия. Например, включить веб-камеру, затемнить окна в доме, отключить полив газона, заглушить двигатель автомобиля, остановить кардиостимулятор, впрыснуть еще одну дозу инсулина, подать напряжение на двигатель электровоза... Обман сенсоров, манипуляция с поступающими в программу или демонстрируемыми оператору данными, воздействие непосредственно на исполнительные механизмы – успешные атаки на любые звенья этой цепочки могут привести к катастрофическим последствиям.

К сожалению, разработчики многих устройств не уделяют должного внимания обеспечению кибербезопасности. В качестве примера можно вспомнить недавнюю историю с производителем водителей сердечного ритма (кардиостимуляторов), довольно прохладно отреагировавших на демонстрацию уязвимостей, позволяющих злоумышленникам воздействовать на кардиостимуляторы, внедряя зловредный код в используемые докторами программаторы [3].

Некоторые угрозы связаны с тем, что используемые в IoT решения устаревают намного раньше, чем физическое оборудование, а исправлению уязвимостей и обновлениям уделяется недостаточно внимания. Иное программное обеспечение для IoT изначально написано со многими уязвимостями и элементами небезопасного кода. Например, в ходе одного из исследований [4] наши аналитики обнаружили множественные уязвимости, позволяющие захватить злоумышленнику контроль над контролерами автозаправочных станций. Среди обнаруженных уязвимостей были "зашитые" в коде учетные данные суперпользователя, небезопасные протоколы передачи данных, уязвимость к SQL-инъекциям и другие. В данном случае речь идет о промышленном коммерческом решении, широко использующемся в разных странах мира (США, Индия, Чили, Испания, Израиль и др.). С безопасностью "домашних" устройств Интернета вещей дела обстоят не лучше. В одной из распространенных моделей многофункциональных камер видеонаблюдения наши эксперты нашли ряд уязвимостей, позволяющих реализовать такие "интересные" атаки, как перенаправление или подмена изображения для конечного пользователя, и получить доступ через облако к любой из зарегистрированных камер этого производителя [5].

Но угрозы в мире Интернета вещей не ограничиваются уязвимостями и ошибками, допущенными при разработке. Так, одна из широко известных DDoS-атак на серверы DNS-провайдера DYN в 2016 году была осуществлена ботнетом, состоящим из сотни тысяч устройств Интернета вещей (видеоняни, роутеры, камеры и др.), зараженных червем Mirai. Ключевая особенность этого вредоноса в том, что для внедрения на устройства он использовал имя пользователя и пароль, заданные по умолчанию. То есть заражал устройства, пользователи которых не сменили заводские учетные данные. В текущий момент опасения экспертов вызывает более продвинутая версия вредоносного кода, способного эксплуатировать ряд известных уязвимостей в программном обеспечении IoT-устройств для заражения и закрепления в системе – IoT roop/Reaper [6]. IoT roop/Reaper уже успешно проявил себя в ходе атак в январе 2018-го на объекты финансового сектора с использованием зараженных роутеров известных производителей телевизоров, вебкамер и других устройств [7].

Несмотря на реальность угрозы, многие пользователи халатно относятся к элементарным правилам кибербезопасности. Так, по данным одного из исследований 2018 года, только 50% опрошенных россиян изменили пароли по умолчанию на роутере, 61% проверяют обновления раз в год или реже [8].

Как защитить IoT?

Из-за многообразия экосистем и устройств IoT, к сожалению, невозможно создать или применить одно универсальное средство, позволяющее сделать весь Интернет вещей безопасным. Безопасность – это процесс, и чтобы этот процесс был эффективным и непрерывным, требуются усилия и со стороны производителей устройств и программного обеспечения Интернета вещей, и со стороны пользователей, и со стороны разработчиков средств защиты. Для того чтобы мир IoT стал действительно безопасным, нужно сделать безопасными не отдельные устройства, а все экосистемы и их взаимодействие между собой в целом. Но любого слона "едят по кусочкам", и мы ведем работу сразу в нескольких направлениях.

Во-первых, "Лаборатория Касперского" ведет обширную работу с различными отечественными и международными регулирующими организациями по созданию, доработке и воплощению в жизнь стандартов кибербезопасности для Интернета вещей.

Решение Kaspersky IoT Secure Gateway

Во-вторых, мы помогаем разработчикам IoT-устройств вовремя выявить и устранить уязвимости в программном обеспечении. Наши исследователи анализируют и тестируют эти устройства так, как это делали бы злоумышленники, находят уязвимости и векторы атак, демонстрируют их разработчикам и предлагают рекомендации по их устранению.

В-третьих, мы помогаем пользователям понять, почему важно соблюдать хотя бы элементарные правила "кибергигиены" и что лично они могут сделать для того, чтобы обезопасить себя и своих близких от киберугроз. У нас есть ряд приложений, в том числе для защиты мобильных устройств и для анализа защищенности IoT-сети (Kaspersky IoT scanner) [9]. Наши коллеги публикуют популяризирующие информационные статьи, ведут каналы и блоги о кибербезопасности, пытаясь повысить общий уровень осведомленности пользователей.

Наконец, но не в последнюю очередь, мы разрабатываем комплекс решений по безопасности IoT. Одно из таких решений – Kaspersky IoT Secure Gateway [10]. В этом продукте используются методы, которые можно разбить на два направления. Первое – это обеспечение защиты ключевых точек IoT-сети, наиболее часто становящихся объектами атак: роутеров и шлюзов. Для этих целей мы разрабатываем решения, предназначенные для реализации принципов "корня доверия" (см. рисунок) и для усиления защиты устройства. Они позволят гибко сочетать (в зависимости от задач, характеристик рассматриваемого устройства и других факторов) наши технологии и продукты как для использования на создаваемых с нуля устройствах, так и для доработки существующих.

В рамках первого направления разработан ряд решений, начиная с Kaspersky OS (KOS) – операционной системы для встраиваемых устройств и устройств IoT. Она не основана ни на одной другой операционной системе, а создана с нуля. KOS позволяет создать на устройстве среду, в которой уязвимости и ошибки кода не будут представлять угрозы. В ее основе лежит микроядро, допускающее только определенный способ взаимодействий и исключающее несанкционированное взаимодействие компонент и приложений. Совместно с Kaspersky OS или с практически любой другой ОС (или прошивкой IoT-устройства) на базе Linux может использоваться Kaspersky Security System (KSS) – специальный механизм, выполняющий вычисление вердиктов безопасности в соответствии с заданными и настроенными политиками. Он позволяет изолировать приложения в контейнерах и определяет, каким образом компонентам ОС и приложениям можно взаимодействовать между собой и с окружающим миром.

В первое направление входит также Secure Boot – основанный на криптографии механизм безопасной загрузки устройства. Он позволит устройствам Интернета вещей проверять целостность и подлинность образа операционной системы (прошивки) перед загрузкой. Для этого образ прошивки шифруется и подписывается разработчиком с использованием ключей шифрования, открытая часть которых может храниться в аппаратной части IoT-устройства. К Secure Boot разработано дополнение – Secure Update, позволяющее проверить целостность и подлинность обновлений прошивки, скачиваемых на устройство из источника обновлений. Этот механизм должен не позволить

злоумышленникам установить модифицированную прошивку в обход или взломав систему обновлений IoT-устройства.

Сюда же мы относим Linux Application Control (LAC) – механизм, дающий возможность создавать и управлять белыми и черными списками бинарных файлов в операционных системах, основанных на Linux. LAC позволяет запретить запуск определенных приложений (black list) или разрешить запуск только разрешенных приложений (white list). LAC сможет взаимодействовать с глобальной базой знаний Kaspersky Security Network (KSN), вычисляя перед запуском бинарного файла его хэш-сумму и обращаясь к KSN для получения репутационной информации. Это должно обеспечить оперативную и эффективную защиту от угрозы распространения специализированных IoT-червей и майнеров, контролировать запускаемые процессы на устройствах промышленного Интернета вещей и т.д.

Второй комплекс технологий направлен на защиту остальных устройств IoT в сети и самой сети в целом. Среди них детектирование аномалий на базе машинного обучения, URL-фильтрация/родительский контроль. Фильтрация URL-запросов позволяет обеспечить защиту от фишинга, посещения зараженных веб-сайтов или от нежелательного контента. Классификация сайтов загружается из облака KSN и позволяет гибко настроить фильтр по множеству категорий. Для домашних роутеров мы планируем предложить технологию родительского контроля, позволяющую отслеживать активность ребенка в сети и защищать его от нежелательных контактов и контента.

Для обеспечения максимальной защиты IoT-устройств мы задействуем машинное обучение (machine leaning, ML). Этот механизм может применяться на сетевых устройствах (роутерах и шлюзах) или быть реализован в виде отдельного устройства, выполняющего мониторинг угроз в сети. Наша технология поможет определить зараженное вредоносным ПО устройство; выявить, что устройством начал управлять злоумышленник, или даже что, например, сработала встроенная производителем "закладка" и устройство начало передавать нетипичные данные в нетипичном направлении.

Первой задачей, решаемой механизмами, в основе которых лежит машинное обучение, – это обнаружение и классификация устройств в сети. Функции ML позволят обнаруживать, категоризировать и систематизировать все действующие в сети устройства. По определенным признакам устройство будет отнесено к соответствующему классу (например, IP-камера, медиаприставка, промышленный сенсор и т.д.). Следующим шагом для каждого найденного устройства будет создаваться или загружаться из облака KSN профиль, описывающий нормальное поведение устройства с этой версией прошивки в сети. Далее функция обнаружения аномалий будет следить за поведением устройств в сети и выявлять отклонения от нормы, а также заведомо вредоносное поведение. Это должно позволить обнаружить активность вирусов, участие в ботнетах и DDoS-атаках, эксплуатацию уязвимостей, модификации прошивки, просто несанкционированное подключение злоумышленников (даже при условии, что им стали известны учетные данные для подключения) и т.д. После анализа и принятия соответствующего решения возможно отключение подозрительного устройства от сети или его "перенос" в карантинную зону сети через команды к API сетевого оборудования.

Эти и другие технологии "Лаборатории Касперского" могут поставляться разработчикам IoT-решений в виде SDK или совместными усилиями встраиваться в прошивки уже существующих продуктов. Также мы совместно с партнерами работаем над созданием других решений, предназначенных для того, чтобы сделать мир IoT безопаснее.

ЛИТЕРАТУРА:

1. Evans Dave, Cisco IBSG. The Internet of Things. How the Next Evolution of Internet is changing everything. Электронный ресурс https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
2. Электронный ресурс https://www.kaspersky.ru/blog/smart-tv-sledit-za-toboj/2457/
3. Электронный ресурс https://www.wired.com/story/pacemaker-hack-malware-black-hat/
4. Электронный ресурс https://ics-cert.kaspersky.ru/reports/2018/02/13/gas-is-too-expensive-lets-make-it-cheap/
5. Электронный ресурс https://ics-cert.kaspersky.ru/reports/2018/03/12/somebodys-watching-when-cameras-are-more-than-just-smart/
6. Электронный ресурс https://krebsonsecurity.com/2017/10/reaper-calm-before-the-iot-security-storm/
7. Электронный ресурс https://www.recordedfuture.com/mirai-botnet-iot/
8. Электронный ресурс https://blog.avast.com/ru/issledovanie-avast-50-rossiyan-ne-menyayut-zavodskoj-parol-routerov
9. Электронный ресурс https://www.kaspersky.ru/blog/kaspersky-iot-scanner/18688/
10. Электронный ресурс https://os.kaspersky.ru/products/kaspersky-iot-secure-gateway/