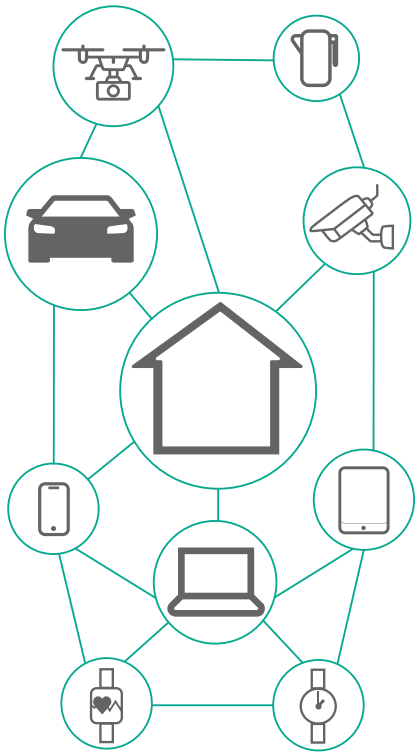
Kaspersky®
IoT Security

Безопасность как приоритет развития интернета вещей

Промышленный интернет вещей (IIoT) может быть основой городской экосистемы или индустриального объекта. Получение злоумышленниками доступа к системам управления транспортным потоком, освещением, водоснабжением и канализацией, экстренного оповещения, контроля состояния воздуха, пожаробезопасности, автоматизированной доставки может привести не только к многомиллионным финансовым убыткам, но и причинить вред окружающей среде, жизни и здоровью людей.



В современном мире нас окружают миллиарды устройств интернета вещей. Промышленные роботы и холодильники, самостоятельно заказывающие продукты, автомобили с автопилотом и «умный дом», определяющий способы экономии электричества, – сегодня это уже реальность.

Традиционно безопасность пользовательских решений ассоциируется с защитой персональных данных. Но сегодня, в эпоху интернета вещей, безопасность необходима для защиты личного пространства, права на конфиденциальность и частную жизнь, а иногда – самой жизни и здоровья обычных граждан. Удалённое подключение злоумышленников к камерам наблюдения, захват управления «умным домом», отключение или выведение из строя автопилота автомобиля, кража личности и персональных данных, нарушение работы носимого медицинского оборудования (например, кардиостимуляторов) – вот далеко не полный список угроз, с которыми уже сейчас сталкиваются или могут столкнуться пользователи интернета вещей.

В то же время интернет вещей и связанные с ним технологии уже стали неотъемлемой частью современного общества. Более того, интернет вещей предоставляет колоссальные возможности для разработки и производства устройств, включая аппаратные компоненты и программное обеспечение, развития телекоммуникационных услуг и рынка интеграции. Отсутствие доверия конечных пользователей к возможностям интернета вещей может заблокировать или серьезно замедлить их реализацию. Поэтому комплексная безопасность решений интернета вещей является основным и общим приоритетом всех заинтересованных в его развитии сторон.

Что угрожает интернету вещей

В конце 2016 года была осуществлена успешная атака на домашние роутеры одного из европейских телеком-провайдеров. Виновником инцидента была специально разработанная злоумышленниками версия червя Mirai. Он превращал скомпрометированные устройства в армию ботов, которые впоследствии участвовали в очень крупных DDoS-атаках[1] (например, в атаке на DNS-провайдера Dyn, которая привела к нарушениям в работе сервисов Twitter, Amazon, Spotify, Github, CNN, Netflix, и Visa в 2016 году). Год спустя получил распространение более продвинутый червь IoTroop/Reaper. В начале 2018 года международный ботнет из зараженных, (предположительно IoTroop/Reaper,) роутеров MikroTik, Ubiquity, Cisco, ZyXEL, TP-Link, веб-камер, смарт-телевизоров и других устройств интернета вещей атаковал несколько компаний финансового сектора. В атаке участвовало более 13 000 зараженных устройств из 139 стран мира[2,3]. По оценке аналитиков, IoTroop/Reaper способен заразить более миллиона устройств[4].

Анализируя инциденты, связанные с атаками Mirai и IoTroop/Reaper, мы пришли к выводу, что пользователи даже не подозревали, что их домашние устройства были скомпрометированы и стали частью огромной ботсети.

Производители конечных устройств интернета вещей и телекоммуникационного оборудования часто игнорируют основные принципы кибербезопасности: аппаратное обеспечение не контролирует целостность прошивки, устройства поставляются с предустановленными паролями, включая пароли администратора, не говоря уже о слабых настройках сетевой безопасности или использовании старых и уязвимых версий программного обеспечения.

1 https://securelist.com/ddos-attacks-in-q4-2016/77412/
2 https://www.recordedfuture.com/mirai-botnet-iot/
3 https://www.securityweek.com/financial-services-ddos-attacks-tied-reaper-botnet
4 https://research.checkpoint.com/iotroop-botnet-full-investigation/

Стоит отметить, что пользователи часто не знают о сетевой активности ряда домашних устройств, подключённых к сети, таких как телевизоры, видеоняни, стиральные машины и т.д., и ошибочно полагают, что они подключены только к серверам провайдера конечной услуги – например, телевизор имеет доступ только к ресурсам провайдера цифрового телевидения или потокового видео. Однако, на самом деле устройство зачастую подключается ещё к десятку серверов для передачи и приёма телеметрии, обработки голосовых команд, получения обновлений и т.д.

Сложность инфраструктуры интернета вещей предоставляет злоумышленникам массу возможностей для реализации различных атак. В массе сетевых запросов легко скрыть передаваемые атакующими данные; а среди большого числа функций, реализуемых устройством или сервисом, непременно найдутся уязвимые.

При этом ПО устройств не всегда обновляется, и они годами работают без обновлений, оставаясь уязвимыми для действий злоумышленников. Успешная атака на такие устройства – лишь вопрос времени.

Получается, что основным источником угроз для интернета вещей является он сам – его инфраструктурная и технологическая сложность в совокупности с высокими темпами его развития.

Кто отвечает за защиту интернета вещей

Для обеспечения безопасности интернета вещей необходимы совместные усилия нескольких сторон:

- производителей конечных устройств;
- производителей телекоммуникационных устройств;
- поставщиков базового оборудования для устройств интернета вещей и телекоммуникационных устройств;
- провайдеров услуг телекоммуникации;
- провайдеров прикладных услуг в области интернета вещей;
- системных интеграторов, работающих в сфере интернета вещей и подключённых устройств.

В основе доверия лежат гарантии того, что поставщик – производитель решения или его части, либо интегратор – прикладывает усилия к тому, чтобы на уровне своей ответственности и в меру своих возможностей избежать некорректного поведения устройств и предотвратить атаки на инфраструктуру интернета вещей. Такой поставщик обладает надежной репутацией, которая, в конечном счете, позволяет ему сохранить и закрепить за собой соответствующую часть рынка решений и интеграционных услуг в сфере интернета вещей.

Все перечисленные стороны в силу своих бизнес-потребностей заинтересованы в безопасной и предсказуемой работе конечных устройств. Чем больше каждый из них заботится о доверии потребителей к качеству своих решений и услуг, тем надёжнее и безопаснее становятся реализуемые конечные устройства.

Kaspersky OS

В основе KasperskyOS лежит надёжное микроядро, которое допускает только определённый способ взаимодействий. Будучи компактным, оно может использоваться на различных платформах. Архитектура приложений основана на компонентной модели, благодаря чему разработка решения становится проще и удобнее. KasperskyOS была задумана и создана как безопасная. Она остается безопасной в течение всего своего жизненного цикла.

KSS for Linux:

- предоставляет средства для внедрения политик безопасности, наиболее подходящих для соответствующей области применения;
- заключает приложения в контейнеры Linux;
- обеспечивает каналы взаимодействия между этими контейнерами;
- управляет контейнерами, защищает каналы взаимодействия и обеспечивает выполнение преднастроенных политик безопасности;
- предоставляет набор готовых компонентов, таких как безопасное удалённое управление системой, аудит/логирование, безопасное хранилище;
- может быть расширен до индивидуально настроенных политик безопасности;
- предоставляет средства для безопасного обновления компонентов ядра Linux (криптографических библиотек, сертификатов, ключей и других данных, относящихся к безопасности).

Secure Boot (Безопасная загрузка)

Secure Boot может использовать защищенное хранилище ключей, реализуемое с поддержкой аппаратного обеспечения, чтобы определить, не был ли повреждён или подменён образ прошивки.

Secure Boot стартует на устройстве до загрузки ОС и начинает проверку цифровой подписи образа прошивки. Если подпись верна (т.е. выдана доверенным источником, а прошивка не изменена), Secure Boot переходит к расшифровке образа прошивки. Если расшифровка прошла успешно (т.е. образ был зашифрован с использованием доверенной пары ключей), то образ прошивки будет загружен. Если же хотя бы один из шагов не выполняется, Secure Boot попытается загрузить предыдущий образ прошивки либо переключиться на режим обслуживания. Таким образом, если прошивка была подменена, изменена, заражена или повреждена, то она не сможет загрузиться, так как не будет иметь подписи и/или не будет зашифрована с помощью соответствующих авторизованных ключей.

Secure Update (Безопасное обновление)

Безопасное обновление работает следующим образом:

1. С консоли управления поступает команда на скачивание файлов прошивки
2. Загрузчик получает образ обновления
3. Загрузчик сохраняет образ во временное хранилище обновлений и запечатывает его
4. Данные из хранилища передаются на проверку специальному контроллеру
5. Этот контроллер выполняет проверку образа и авторизует его в случае успеха.
6. Авторизованный образ поступает в апдейтер

Доверенный интернет вещей

Доверие на уровне устройств

В основе обеспечения гарантий безопасной работы устройств интернета вещей лежит принцип цепочки доверия (chain of trust). Начальная точка доверия выбирается в зависимости от требуемого уровня гарантий, и в случаях, когда необходимы гарантии самого высокого порядка, устанавливается на уровне аппаратной части. Технологии и решения «Лаборатории Касперского» позволяют построить защищённое устройство, реализуя корень доверия (root of trust) на любом уровне.

Доверие на уровне инфраструктуры

Используя интеллектуальный облачный автоматизированный сервис «Лаборатории Касперского» Kaspersky Security Network (KSN) для анализа деперсонализированных данных, мы можем не только обнаруживать инциденты и аномалии в инфраструктуре заказчика, но и, при его желании, предотвращать их. Интеллектуальные сервисы обеспечивают мгновенную реакцию и защиту от новейших угроз по всему миру. Дополнительным преимуществом является возможность объединения всех продуктов «Лаборатории Касперского» в единую систему контроля и управления, что позволяет значительно снизить затраты на поддержку и аппаратные ресурсы и усилить защиту устройств с использованием продуктов «Лаборатории Касперского» для защиты конечных устройств, защиты от передовых угроз и целевых атак, защиты промышленных инфраструктур, управления угрозами безопасности и др. Это дает возможность обеспечить безопасность и бесперебойную работу инфраструктуры заказчика и свести к минимуму вероятность успешных кибератак.

Технологии «Лаборатории Касперского» для защиты устройств интернета вещей

Kaspersky OS
KasperskyOS – это безопасная операционная система для встроенных подключённых устройств с особыми требованиями к информационной безопасности. KasperskyOS создает среду, в которой уязвимости и ошибки кода больше не представляют угрозы.

Kaspersky Security System
Kaspersky Security System (KSS) – это движок, выполняющий вычисление вердиктов политик безопасности. Он может использоваться совместно с KasperskyOS (также может встраиваться в прошивки на базе Linux) в качестве системы, осуществляющей выполнение вердиктов KSS.

Secure Boot (Безопасная загрузка)
Secure Boot позволяет устройствам интернета вещей посредством криптографических методов подтверждать целостность и подлинность образа прошивки до его загрузки.

Secure Update (Безопасное обновление)
Secure Update обеспечивает проверку целостности и подлинности обновлений прошивки с помощью криптографических методов. Технология Secure Update работает вместе с Secure Boot и позволяет обновлять прошивку только с использованием корректно подписанных и зашифрованных образов, полученных из доверенных источников.

Веб-фильтрация
Веб-фильтрация от «Лаборатории Касперского» – это технология, которая обеспечивает защиту от фишинга, заражённых веб-сайтов и нежелательного контента.

Веб-фильтрация классифицирует сайты по ряду категорий, что позволяет:
- защитить пользователей и сеть, блокируя фишинг и вредоносные веб-сайты;
- контролировать просмотр веб-страниц и сократить объём корпоративного трафика;
- повысить продуктивность сотрудников, ограничив их доступ к не связанным с работой веб-сайтам, таким как социальные сети и сайты онлайн-игр;
- использовать функционал родительского контроля, блокируя доступ детей к нежелательному контенту.

Родительский контроль
Родительский контроль даёт возможность отслеживать активность ребёнка в сети, защитить его от нежелательных контактов, блокировать доступ к нежелательному контенту и играм, управлять скачиванием приложений, контролировать общение в социальных сетях и предотвращать нежелательный сторонний доступ к его личным данным.

Machine Learning-based protection
Функционал ML, например, может определить, когда устройство заражено зловредом либо управляется злоумышленником, пытается отправлять необычные данные или обычные данные в необычном направлении. Также технологии позволяют определить вредоносную активность и скрытую передачу данных в обычном трафике.

Технологии защиты на базе ML используют не только системные ресурсы устройства, но и облако Kaspersky Security Network для быстрого обучения и оперативного принятия решений на основе данных, полученных от других устройств и сервисов, использующих продукты «Лаборатории Касперского».

Функционал ML позволяет работать как с «сырым» трафиком, так и на основе извлечённых из него значений, характеризующих физическое поведение устройства.

Безопасный аудит (Secure Audit)
Secure audit – это функция KasperskyOS, которая распознаёт, записывает и сохраняет журнал аудита, предоставляя гарантии того, что записи журнала не будут подменены. Безопасный аудит может использовать технологию блокчейн для распределенного и безопасного управления журналом.

Контроль приложений (Linux Application Control)
Перед исполнением нового бинарного файла Linux Application Control высчитывает его хэш-сумму и обращается к Kaspersky Security Network для получения репутационного уровня доверия и рекомендаций по безопасности для этого приложения. В тех случаях, когда хэш-сумма приложения совпадает с хэш-суммой заражённого кода в базе данных KSN, Контроль приложений блокирует запуск этого приложения на устройстве. Данная технология позволяет избежать заражения устройств интернета вещей такими зловредами, как Mirai и Bashlite и может использоваться на устройствах под управлением ОС на базе Linux.

Веб-фильтрация / Родительский контроль (Web-filter/Parental control)
В зависимости от предназначения устройства, в его прошивку могут быть добавлены технологии веб-фильтрации (для организаций и индустриальных устройств) или родительского контроля (для пользовательских устройств).

Защита на базе машинного обучения (Machine Learning-based protection)
Чтобы обеспечить надёжную защиту пользовательских сетей, мы разработали защитный механизм на базе машинного обучения (Machine Learning – ML), который может применяться в сетевых устройствах (гейтвеях или роутерах). ML используется для идентификации и классификации всех устройств в сети путем активного и пассивного анализа их поведения, составления профиля каждого устройства и детектирования аномальной или непредусмотренной активности.

Обнаружение активов на базе ML (ML asset discovery)
Технология обнаружения активов с использованием ML позволяет автоматически обнаруживать, категоризировать и систематизировать все активы в защищённой сети. Используя специальную технологию распознавания по идентификационным меткам (fingerprints), наше решение идентифицирует тип устройства, название производителя, модель и даже версию прошивки, анализируя при этом лишь определенные элементы (метаданные) произведённого устройством сетевого трафика.

Анализ поведения устройств на базе ML (ML device behavior analysis)
Когда активы в сети обнаружены и категоризированы, для них создаются особые профили. Профиль описывает нормальное поведение устройства с данной прошивкой в данной пользовательской сети.

Детектирование аномалий на базе ML (ML Anomaly Detection)
Использование технологий на базе ML для обнаружения активов и создания профилей устройств позволяет выявить любую аномалию в устройствах интернета вещей, в том числе индустриального. Технология детектирования аномалий на базе ML регистрирует активность зловредов и ботнетов, участие устройств в DDoS-атаках, эксплуатацию прошивки, майнинг, хакерский перехват управления устройствами и т.д.

Заключение

Технологии «Лаборатории Касперского» позволяют построить безопасный интернет вещей. При этом неважно, создаются устройства и программные прошивки с нуля или требуется встраивание средств защиты в уже существующие программные компоненты. Наши решения могут быть кастомизированы под программную и аппаратную платформу заказчика. С помощью технологий «Лаборатории Касперского» провайдеры связи и производители устройств интернета вещей, в том числе индустриального, могут создавать защищённые решения, полностью отвечающие нуждам бизнеса и требованиям безопасности в условиях современного ландшафта угроз.

www.kaspersky.ru

Продукты на базе KasperskyOS®: os.kaspersky.ru/products/
АО «Лаборатория Касперского»: www.kaspersky.ru
Аналитика и отчеты о киберугрозах от экспертов «Лаборатории Касперского»: www.securelist.ru

#kasperskyos
#truecybersecurity