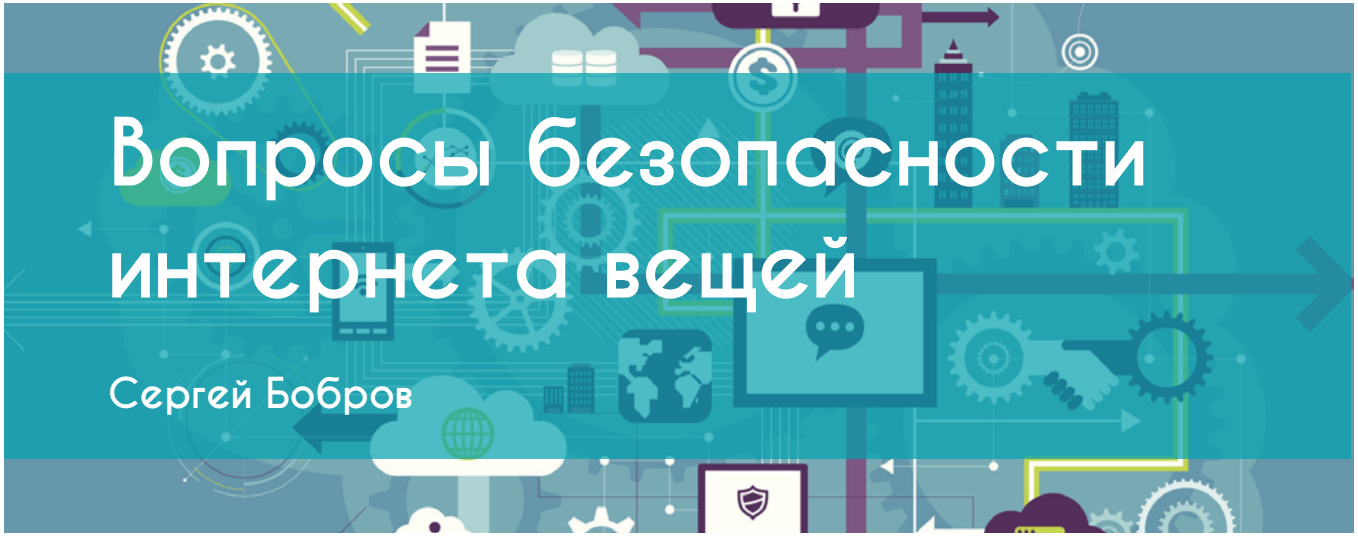


Вопросы безопасности интернета вещей

Сергей Бобров

Незаметно для большинства в нашем мире появилось новое семейство устройств, подключенных к Интернету и объединенных в группы. Пока это не цивилизация машин, и о «судном дне» речь еще не идет (хотя Илон Маск и пугает этим), но угроза от этого сообщества устройств исходить действительно может...

Совокупность таких устройств сейчас называют Internet of Things (IoT). Это в основном специализированные бытовые или промышленные устройства, которые для управления или обмена информацией были наделены новой возможностью – подключением к интернету или к серверу управления и контроля через интернет.

Это может быть бытовой прибор или система «умный дом», измерительный прибор или исполнительный модуль, домашний маршрутизатор или видеокамера, сельскохозяйственная машина или что угодно другое, но при этом у них есть особенность – сетевое подключение к интернету.

Для дальнейшего изложения важно то, что эти специализированные устройства с подключением к сети (проводным или беспроводным), обладают невысокой вычислительной мощностью, небольшим объемом памяти и ограниченным набором исполняемых команд.

Второй особенностью данных приборов является то, что пользователь, эксплуатирующий данное IoT-оборудование, не является ни в коей мере ИТ-специалистом, сетевым инженером или экспертом по безопасности и, соответственно, не может, да и не хочет правильно настроить устройство для безопасной и эффективной работы в сети. Поэтому оно должно быть или сразу эффективно предназначено или управляться производителем при его эксплуатации или станет потенциальным источников сетевых проблем.

Третьей особенностью является отсутствие сколько-нибудь серьезных функций безопасности, потому что любые ограничивающие настройки или функции могут создать проблемы при эксплуатации неподготовленными пользователями, а значит, в условиях жесткой конкуренции создать репутацию сложной, непонятной или неработающей техники, снизить привлекательность продукции и, как следствие, снизить продажи и доходы производителя.

В действительности представим ситуацию, что новый холодильник при включении задает много сложных вопросов и не просто о языке, временном поясе и пр., а просит домохозяйку указать настройки IP и DNS (если в сети нет DHCP-сервера или он некорректно отработал) или создать надежный пароль и, как «верх садизма», запомнить его. Думаю, что домохозяйка сразу же поделится в социальных сетях информацией о недружественности данного изделия и это, опосредовано, снизит рыночную долю производителя. Ограничения, накладываемые на сетевое взаимодействие устройства, могут привести к тому, что конфигурация сетевых настроек

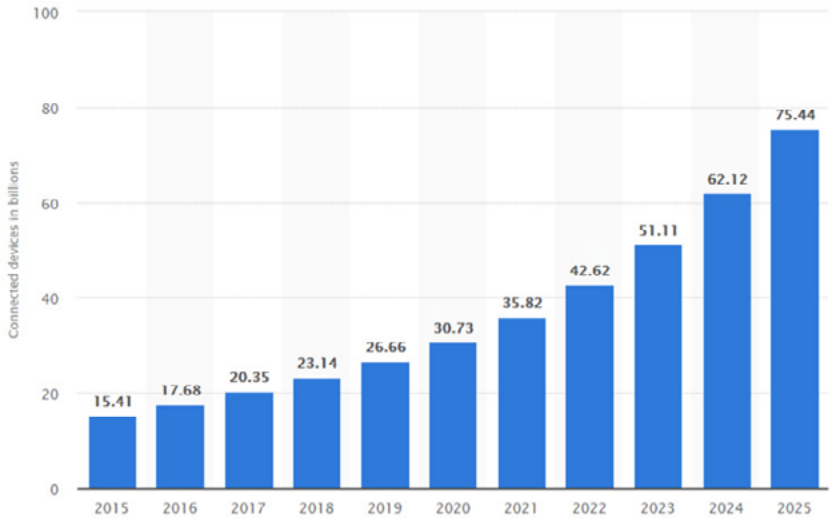
устройства и сетевого окружения не совпадут, и доступ к сети так и не будет установлен. В связи со всем этим производители стараются сделать количество ограничений и вопросов как можно меньшим, а сетевые настройки – как можно более открытыми.

Категория	2016	2017	2018	2020
Бытовые	3 963,0	5 244,3	7 036,3	12 863,0
Промышленные/корпоративные	2 418,7	3 136,4	4 160,3	7 552,4
Всего, млн. шт.	**6 381,8**	**8 380,6**	**11 196,6**	**20 415,4**

Источник: Gartner (January 2017)

Данные Gartner о количестве IoT-устройств

Понятно, что слабо или вообще не защищенное устройство, подключенное к сети, является лакомой добычей для разного рода злоумышленников. Это, может и не было бы проблемой, если бы количество этих устройств не исчислялось миллиардами и не становилось с каждым годом все больше. Например, выше приведены данные Gartner о количестве устройств IoT по категориям и прогноз на несколько лет вперед. Данные представлены в млн. устройств. Считается, что сейчас в мире более 8 млрд подключенных устройств, а к 2020 г. их будет более 20 млрд. Данные Statista еще более впечатляющие.



Данные Statista о количестве IoT-устройств

Но даже если принимать во внимание только данные Gartner, то уже сейчас количество подключенных устройств превышает количество людей на Земле (7,5 млрд чел), а к 2020 превысит почти в 3 раза. Поэтому мы не можем игнорировать вопросы безопасности миллиардов устройств, несмотря на то, что каждое из них весьма малопроизводительно.

По результатам анализа Corero Network Security, в 3-м квартале 2017 г. количество DDoS-атак выросло на 91% по сравнению с первым кварталом этого же года и составило в среднем 237 атак на организацию в месяц. Источниками достаточно большой части этих атак являются IoT-устройства, подчиненные злоумышленником и объединенные в сети, называемые ботнетами (botnet).

Так, в сентябре 2016 г. на сайт журналиста Брайана Кребса была совершена DDoS-атака с мощностью до 620 Гб/с. Затем атаке подвергся французский хостинг-провайдер OVH, который оказался под атакой 1 Тб/с. Как сообщил технический директор провайдера, источником атаки оказалось 152 тыс. «умных устройств», в основном уличные видеокамеры и видеорегистраторы.

Позже, в октябре 2016 г., была осуществлена DDoS-атака на крупнейшего в США провайдера DNS – компанию Dyn. Атака была осуществлена ботнетом, состоящим из сотен тысяч IoT-устройств. Мощность атаки достигла 1,2 Тб/с. Атака привела к недоступности или перебоям в работе около сотни крупнейших интернет-сервисов в течение нескольких часов по всему миру и вызвала такой резонанс, что даже получила персональное название по дате - 10/21, по аналогии с атакой на WTC – 9/11.

И таких примеров множество. Причем это не явление 2017 г. Такие атаки меньшего масштаба наблюдаются начиная с 2014 г.

Включение устройства в ботсеть происходит после заражения его вирусом, в случае IoT, обычно, имеют дело с вирусом семейства

Mirai (дано по имени бинарного файла) или подобным ему.

Данный вирус атакует Linux-устройства, использующие набор утилит Busybox. Вирус использует, так сказать, «социальную инженерию», а именно, пробует получить доступ к устройству через telnet, перебирая 50 вариантов имен/паролей, которые используются по умолчанию в IoT-устройствах крупнейших производителей (Ubiquiti, Raspberry, Ubuntu based, Dahua, Hikvision,...), например:

Самые распространенные имена	Самые распространенные пароли
ADMIN	ADMIN
ROOT	XC3511
ROOT	VIZXV
ROOT	JUANTECH
ROOT	DEFAULT
ADMIN	ADMIN1234
ROOT	PASSWORD
ROOT	ROOT
ROOT	XMHDIPC
ADMIN	SMCADMIN
ROOT	ADMIN
ADMIN	ROOT
DUP ROOT	123456
UBNT	12345
ACCESS	UBNT
DUP ADMIN	PASSWORD
TEST	1234
ORACLE	TEST
POSTGRES	QWERTY
PI	RASPBERRY

Как только доступ к устройству получен, вирус инсталлируется в систему, связывается с контроллером ботнета и сообщает о себе, далее стирает себя с носителя для уменьшения вероятности обнаружения, оставаясь в оперативной памяти, сканирует диапазон IP-адресов, проверяя на наличие уязвимых устройств, и отправляет эту информацию контроллеру ботнета. Как видно, вирус крайне прост, использует банальную методику перебор пароля “brute force”, но, как оказалось, и этого достаточно для организации ботнета на сотни тысяч IoT-устройств.

Сейчас новые заражения Mirai возникают все реже, но это не значит, что вирус побежден. Во-первых, существует множество мутаций и вариантов вируса (Hajime, LuaBot,...), а во-вторых, устройство, превращенное в члена ботнета, никак себя не проявляет и может быть использовано контроллером ботнета в следующих атаках, т.е. мы можем только предполагать, насколько вирус распространился и какое количество устройств он контролирует, но эксперимент осенью 2016 г. показал, что «незащищенное» устройство, выставленное в интернет, подверглось атаке уже через 40 мин, а за последующие 11 часов его пытались атаковать 300 раз.

Плюсом является то, что избавиться от вируса Mirai и предохраниться от последующего заражения довольно просто: отключить устройство от интернета, перезагрузить его, поменять имя/пароль на устойчивые к взлому, по возможности запретить подключение к устройству через интернет по telnet/ssh и прочим возможным способам управления и после этого подключить устройство к интернету опять. Хорошей рекомендацией будет также проверить наличие и установить обновления ПО.

Снижение активности Mirai происходит за счет того, что «кормовая база» вируса уменьшается: устройства, зараженные одним контроллером ботнета, не поддаются заражению другим, а после завершения атаки случается, что контроллер просто выключают и сеть остается в пассивном состоянии. Кроме того, количество «беззащитных» IoT-устройств уменьшается за счет выполнения рекомендаций ИТ-безопасности.

Этот пример приведен для демонстрации практически нулевого уровня ИТ-безопасности Io-устройств, так как даже такой простой вирус, который получает доступ путем банального перебора 50 паролей «по умолчанию», смог «пробиться» к сотням тысяч устройств и выполнять на них вредоносные действия.

Проблема еще и в том, что хозяева таких устройств не то, что не занимаются защитой, но даже не подозревают, что их устройство было атаковано, более того, зачастую, они даже не понимают, о чем речь, и в общем, по

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

Атака вируса BrickerBot.1

этому поводу не особенно переживают – проблемы же не у них.

Но, вообще-то, они так считают зря, потому что существует еще один класс вирусов – BrickerBot. Пока представлен двумя версия-ми – BrickerBot.1, BrickerBot.2.

Вирус был обнаружен и описан компанией Radware весной 2017 г. Результатом действия этих вирусов является PDoS (Permanent Denial of Service), а именно невозможность использования этого устройства, превращение его в «кирпич» (от англ. Brick – кирпич и происходит название вируса). Вирус атакует устройства IoT на базе Linux с набором Busybox. При атаке проверяется открытый TCP-порт 23 (telnet) и происходит подбор пароля, начиная с пары 'root'/'vizxv'. Как видно, в этом BrickerBot полностью похож на Mirai. Различия начинаются в действиях вируса после проникновения. BrickerBot оправдывает свое название – он пытается удалить все содержимое любого хранилища, внутреннего или непосредственно подключенного к устройству, нарушает связь с интернетом (net.ipv4.tcp_timestamps=0) и препятствует выполнению операций ядра (kernel.threads-max=1).

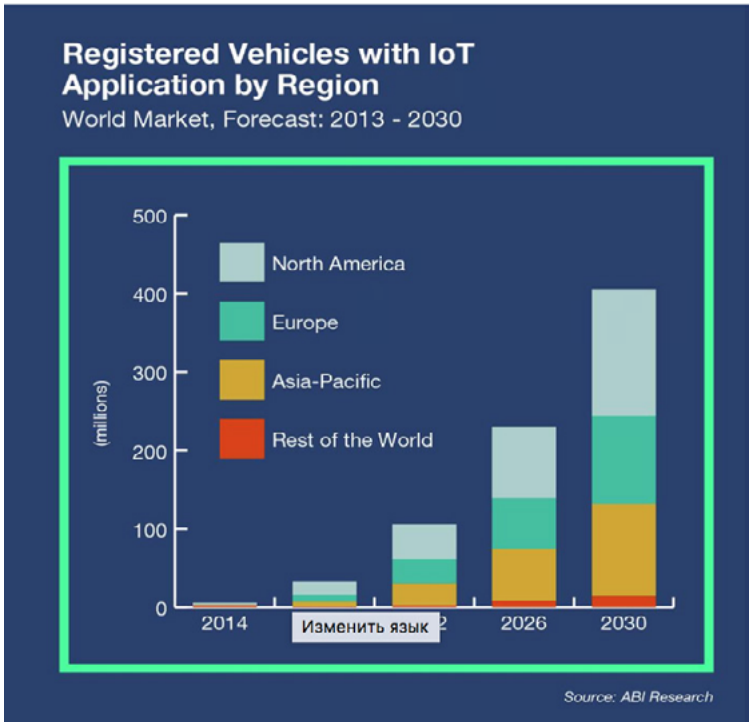
Таким образом, данный вирус, по сути, делает устройство недоступным, что приводит либо к замене устройства либо, в лучшем случае, к полному обнулению устройства и восстановлению прошивки. Отличие между BrickerBot.1 и BrickerBot.2 наблюдается в инициаторах заражения, способе действия после заражения и продолжительности атак. Если первый атаковал с определенного набора IP-адресов, то второй атаковал из сети TOR и соответственно отследить его инициаторов не так просто; кроме того, он не использует набор BusyBox, что делает его более универсальным. Считается, что BrickerBot.2 активен до сих пор.

Многие полагают, что BrickerBot был запущен для уменьшения «популяции» устройств, доступных для атаки типа Mirai, т.к. оба вируса используют одинаковые алгоритмы проникновения в устройство, и BrickerBot просто уничтожает устройство, которое доступно для заражения Mirai. Есть сообщения, что вирус вначале пытается помочь зараженному устройству, устранив уязвимости, ничего при этом не повреждая, но если это не получается, то происходят деструктивные действия, но эти сообщения пока невозможно ни подтвердить, ни опровергнуть. Но, несмотря на такие, возможно, благородные побуждения, BrickerBot несет реальную угрозу безопасности и жизни людей – представим «убитые» камеры видеонаблюдения или NVR на режимных объектах, неработоспособное медицинское оборудование у пациента или системы управления котлом зимой.

Конечно, перечень вирусов IoT-устройств не ограничивается Mirai, Hajime, LuaBot, BrickerBot.1 и BrickerBot.2. Они стали наиболее известными из-за общественного резонанса, вызванного крупными DDoS-атаками, и уничтожения устройств.

Дальнейшим трендом атак на IoT-устройства

является усложнение способа атаки и другие способы получения прибыли. Незащищенность IoT-устройств и наличие криптовалюты делает вымогательство при помощи взлома бытовых IoT-устройств наиболее «интересным» направлением. Уже проводились экспериментальные взломы домашних регуляторов температуры с их блокировкой и требованиями оплаты за разблокировку (действие аналогичные широко известному в нашей стране вирусу Petya), а с учетом того, что в среднем доме в благополучных странах находится около 12 устройств с подключением к интернету (в т.ч. маршрутизаторы, ТВ, холодильники, «умный дом», термостаты и пр.), то найти незащищенное устройство и, перехватив над ним управление, потребовать денег, не будет чем-то невозможным.



Прогноз по количеству автомобилей с подключением к IoT

Если мы уже заговорили о «перехвате управления», то нельзя не вспомнить об автомобилях, а точнее об «умных автомобилях».

По сообщениям ABI Research, по дорогам мира ездит около 20 млн авто, которые тем или другим способом подключены к интернету для диагностики, обновления дорожной информации и пр. Они могут стать объектом атаки, которая доставит реальные проблемы, по сравнению с которыми отключенный ТВ или холодильник будет выглядеть как мелкая неприятность. Так, в 2015 г. был продемонстрирован успешный перехват управления, блокировка дверей и отправка в кювет Jeep Cherokee с водителем. Атака была выполнена через информационно-развлекательную систему автомобиля, подключенную к интернету.

По мнению аналитиков, для решения проблемы безопасности IoT необходимо внедрять принципы, характерные для корпоративной системы ИТ-безопасности, которая для IoT рекомендует следующие первоочередные шаги:

- Изменить имя/пароль устройства на взломостойкое (требование к паролю – не менее 8 символов, содержать цифры, буквы верхнего регистра и специальные символы).
- Установить все обновления безопасности производителя.
- При приобретении устройства проверить репутацию производителя с точки зрения ИТ-безопасности и периодичность выхода обновлений безопасности.
- Отключить UPnP-протокол и доступ по telnet из интернета, если это возможно.
- Отключить все неиспользуемые протоколы и сетевые функции.
- Включать Wi-Fi в устройствах только после настройки аутентификации и шифрования.
- Анализировать аномалии трафика устройства.
- Контролировать известные сигнатуры атак для предотвращения заражения.
- Контролировать конфигурацию устройств и сигнализировать об ее изменении.

Есть четкое понимание того, как реализовывать это все в корпоративной среде. Но как же все это реализовать это для конечного пользователя, который подключен к интернету непредсказуемым образом, у которого все настройки безопасности стоят в лучшем случае «по умолчанию», а в худшем – отключены «чтобы не мешали»?

Кто может на себя взять решение этой задачи? Представляется, что тут возможен только комплексный подход, в котором пользователь не будет «играть первую скрипку» в силу естественного отсутствия компетенции.

Как видим, задача обеспечения безопасности IoT-устройств делится на две составляющие:

- настройки безопасности на самом устройстве;
- сетевая безопасность.

Внесение изменений в настройки и добавление функций безопасности – задача производителя, более того, это касается как новых устройств, на которых необходимо просто поменять настройки по умолчанию, так и существующих, но потенциально уязвимых. Производителю следует внести следующие изменения в устройстве:

- Установить требование по установке надежного пароля, как обязательный шаг при первом включении системы.
- Установить защиту от перебора пароля (таймаут перед очередной попыткой входа и блокировка эккаунта на время после трех неудачных попыток).
- Отключить по умолчанию все необязательные сетевые протоколы и telnet снаружи. Пользователь, который понимает, что он хочет, включит сам, остальным – не надо.
- Отключить Wi-Fi по умолчанию и включить его только после настройки безопасности не хуже WPA-PSK или, в самом худшем случае, WEP.

Решение по сетевой безопасности может быть задачей производителя IoT-устройств, как компании «кровно» заинтересованной в успехе продвижения своих устройств.

Если мы говорим, что производитель берет на себя все функции обеспечения безопасности, в том числе и ИТ-безопасность сетевого периметра устройства, то весь трафик устройства должен проходить через датацентр, в котором будет предусмотрена защита от сетевых атак и защита от вирусов. Для этого, после подключения к интернету, устройство устанавливает SSL-туннель на заранее установленный адрес кластера концентраторов в датацентре производителя (собственном или арендованном) и любой другой трафик наружу, кроме трафика VPN, запрещается.

Таким образом, на устройстве производитель может:

- обеспечивать защиту от заражения;
- обеспечивать защиту от сетевых атак;
- контролировать состояние и ошибки на устройстве для проактивной поддержки;
- контролировать актуальность ПО;
- контролировать изменения настроек.

Минусом данного решения является то, что весь трафик устройства идет не по оптимальному маршруту, т.е. вносится высокая задержка из-за того, что ему приходится проходить через глобальный или региональный ЦОД производителя.

Видится, что для производителя самым правильным путем будет обеспечение сетевой безопасности IoT-устройства, особенно для тех устройств, которые не используют подключение к интернету для передачи тяжелого контента (видео, аудио...). Это вызвано тем, что некоторые страны пошли на запрет определенных типов устройств из-за их небезопасности и уязвимости к взлому, который может привести к тяжелым последствиям. Например, в начале 2017 г. власти Германии запретили продажу куклы Cayla, т.к. ею использовался незащищенный канал в интернете, а осенью 2017 г. под запрет попали детские смартчасы в силу уязвимости для несанкционированного прослушивания и подмены информации о положении ребенка. Этот запрет, без сомнения, снизит объемы продаж производителя и обратит его внимание на повышение ИТ-безопасности устройств.

В случае невозможности или неготовности производителя к созданию своего ЦОДа с центром очистки трафика, эта функция может быть предложена оператором, в большинстве своем обладающим необходимыми ресурсами, которые он может адаптировать

под защиту IoT-трафика, тем более, что есть опасность, что трафик оператора может быть заблокирован из-за большого потока DDoS или других атак с его IP-адресов. Оператор/ISP может пропускать весь трафик через сетевую систему безопасности и взять на себя:

- выделение трафика IoT-устройств;
- проверку трафика IoT-устройств на вирусы и на аномалии трафика при помощи системы Advanced Mailware Protection;
- блокирование трафика к известным контроллерам ботнет.

Оператор также может предоставить услугу по управлению и контролю IoT-устройств абонентов на базе семейства протоколов TR-69, разместив в своей корпоративной сети управляющий сервер и передав его адрес в настройки абонентских устройств. Здесь, правда, возникает вопрос безопасности самого сервера, контроля доступа к нему и защиты от вредоносного ПО, но этот вопрос решается корпоративной ИТ-безопасностью весьма хорошо.

Для выполнения этих шагов:

- Производителю понадобится: встроить в IoT-устройства файерволы, TR-69 и VPN- клиенты, поменять настройки безопасности и усложнить первоначальную настройку устройств пользователем, построить ЦОД для обеспечения сетевой безопасности, установить управляющий сервер, расширить службу поддержки производителей группой по проблемам безопасности.
- Оператору может понадобиться: расширить свою подсистему malware protection.
- Пользователю понадобится: пройти более сложную процедуру настройки устройств и потратить немного больше на сетевую безопасность от производителя или ISP.

В конце концов, это себя окупит, потому что нельзя выходить на современное поле боя в «картонных латах и с деревянным мечом», надеясь, что тебя не зацепит. Как указывалось выше, зацепит, уже через 40 мин...

POST SCRITUM

А если опуститься на реальную землю и задать себе несколько вопросов:

Захочет ли производитель ради повышения ИТ-безопасности своих продуктов, что улучшает его имидж, но не приносит прямого дохода, понести новые затраты на построение ЦОДа и организацию системы сетевой безопасности, на разработку и внедрение протоколов и функций безопасности в устройство; внедрить описанные ужесточения и усложнения; получить в связи с этим море негатива по поводу «неработающего» устройства от не разобравшихся в нем пользователей?

Захочет ли оператор бесплатно выделять трафик IoT, анализировать его и нагружать свою дорогостоящую систему mailware protection и файерволы этим трафиком? Захочет ли пользователь при первом включении устройства проходить непривычную процедуру настройки безопасности вместо «включил и играй», приобретать устройство на несколько долларов дороже или оплачивать дополнительные услуги сетевой безопасности?

КАКИМ БУДЕТ ОТВЕТ НА ЭТИ ВОПРОСЫ И К ЧЕМУ ЭТО НАС ПРИВЕДЕТ?

Если ответом будет «нет», то снова и снова будут появляться люди, которые будут думать и действовать как создатель BrickerBot: «Как и многие другие, я был потрясен беспорядочными DDoS-атаками, которые устраивали IoT-ботнеты в 2016 году. Я думал, что такие крупные атаки вынудят индустрию наконец-то действовать сообща, но спустя несколько месяцев после этих рекордных атак стало очевидно, что, невзирая на все усилия, обычными методами проблему не удастся решить достаточно быстро».

А вот понравится ли нам их действия? Думаю, нет. Побудит ли исправить ситуацию? Посмотрим... C4IT

Автор статьи - начальник отдела разработки системных решений SeT Ukrane