Кто взломает вашу кофеварку: безопасен ли интернет вещей?

«У PewDiePie проблемы, и ему нужна ваша помощь, чтобы победить T-Series!» — такой свежераспечатанный плакат обнаружили в 2018 году владельцы более 50 000 принтеров по всему миру[1]. Объединяли эти устройства, от простейших бытовых до «навороченных» офисных, три особенности: все были умными, все управлялись удалённо с помощью интернета вещей — IoT, но все стали жертвой хакерской атаки фаната известного видеоблогера. Забавно? Увы, нет: сегодня число подобных гаджетов — от кофеварок до станков с ЧПУ — только в России составляет около 40 млн, в мире достигает 24 млрд, а вопрос кибербезопасности для их хозяев перестал быть чем-то малореальным. Стоит ли всерьёз опасаться собственного котла, холодильника или микроволновки? Спросим специалистов.

Безопасна ли крупная умная бытовая техника: что, если злоумышленники заставят котёл взорваться, а стиральную машину — устроить потоп?

Действительно, сегодня современная техника позволяет полностью «переложить» заботы, например о поддержании комфорта в доме, на электронику. А управлять ею и мониторить состояние устройств — непосредственно со смартфона из любой точки мира, где есть интернет. Теоретически такое действительно даёт возможность злоумышленнику завладеть контролем над бытовым девайсом, однако критичным (а тем более опасным) это не станет.

[1] https://www.bbc.com/news/technology-46552339.

«ECORADIOSYSTEM Visio — интегрированное в заводской комплектации устройство регулирования отопления, позволяющее управлять котлом удалённо, — ***объясняет Роман Гладких, технический директор компании FRISQUET, ведущего французского производителя премиальных газовых котлов.*** *— Связь с теплогенератором осуществляется по выделенному радиоканалу с использованием зашифрованного протокола FRISQUET Visio, перехватить его удалённо физически невозможно. То есть, чтобы попытаться такое предпринять, нужно находиться рядом. Чтобы добраться до управления, следует либо завладеть смартфоном или планшетом, с которого это можно сделать, либо попробовать взломать доступ в облачный сервис, через который реализуется весь процесс, что крайне сложно и в целом бессмысленно. Но даже в таком случае превратить котёл в "бомбу" не выйдет: автоматика безопасности теплогенератора не подчиняется указаниям и действует автономно. В случае угрозы она просто отключит агрегат».*

Примерно так же происходит и с другой потенциально опасной бытовой техникой: системы, влияющие на безопасность устройства, невозможно «заставить» отключиться удалённо. Как правило, это простые и надёжные решения, которые реагируют на угрозу блокировкой.

Чем угрожает «захват» бытовой техники хакерами?

С высокой долей вероятности вы даже этого не заметите — обычно хакеры занимаются умными вещами совсем не для того, чтобы испортить утренний кофе или даже получить интимные фото (хотя и это случается). Чаще всего атака направлена на завладение долей вычислительных мощностей устройства с целью взлома паролей, рассылки спама или майнинга криптовалюты. А едва ли не самым популярным использованием IoT в последнее время стала организация массовых DDoS-атак на компании и банки с помощью вредоносных программ — ботнетов.

Статистика IBM свидетельствует, что меньше чем за год, с октября 2019 по июнь 2020-го, количество атак через IoT в четыре раза превысило сумму нападений за предшествующие два года и продолжает расти, причём угроза интернациональна. Свежие (по итогам II квартала 2021-го) данные указывают, что, хотя большинство заражённых устройств (31,8 %) находится в Китае, Россия занимает четвёртое место после США (12,5 %), чуть уступив Германии (5,8 против немецких 5,9 %).

*«Примечательно, — **говорит Яна Юракова, аналитик по информационной безопасности российской ИТ-компании Positive Technologies**, — что во всех случаях киберпреступники доставляли вредоносное ПО, эксплуатируя уязвимости в маршрутизаторах, системах контроля доступа, хранения данных и других IoT-устройствах»*.

Массированные атаки имеют вполне конкретные цели: помочь кражам по-настоящему больших объёмов денег и баз персональных данных, совершению диверсий на производствах и прочим организованным преступлениям. Собственно, поэтому уровень хакерских нападений на устройства IoT только за месяцы пандемии вырос на 700 % (по данным компании Zscaler).

Можно ли себя обезопасить, не жертвуя удобством?

В целом относительно спокойно можно спать владельцам мелкой умной бытовой техники, поскольку хакеры предпочитают взламывать ТВ-приставки (29 %), телевизоры (20 %) и часы (15 %). Однако расслабляться не стоит: за последний год увеличились атаки на холодильники, автомобили, карты памяти со встроенным Wi-Fi. Поэтому, как и в случае с компьютерами и телефонами, необходимо соблюдать цифровую гигиену.

*«По большей части все взломы идут через социальную инженерию, — **подчёркивает Николай Груздев, инженер по электронике, специалист по компьютерной безопасности.** — Потому что проблема безопасности чаще всего заключается в "прокладке между креслом и компьютером". Чтобы не стать жертвой злоумышленников, нужно следовать инструкциям умных вещей, где обязательно есть вменяемые рекомендации для повышения уровня их защиты, сразу менять заводские пароли и регулярно повторять это действие, следить за обновлениями программного обеспечения и вовремя их устанавливать, потому что серьёзные компании постоянно совершенствуют ПО, закрывая возможные уязвимости. Безусловно, не стоит переходить по подозрительным ссылкам, скачивать сторонние приложения и передавать данные, даже если кажется, что письмо или сообщение пришло от производителя»*.

Минимум, что можно сделать для того, чтобы обезопасить себя от вторжения через умную технику, по мнению специалиста, выглядит примерно так:

✔ проверить (желательно с помощью сведущего человека, знакомого с вопросами кибербезопасности) все IoT-устройства на предмет сторонней вычислительной нагрузки. Если она обнаружена, срочно принять меры по устранению проблемы;

✔ выяснить, какие настройки актуальны. Если они остались заводскими, немедленно изменить, настроив на максимальную конфиденциальность;

✔ заменить все пароли на надёжные. И делать это следует раз в несколько месяцев. Учтите, что для каждого устройства нужен свой уникальный пароль;

✔ проводить такой аудит регулярно.

Мы не можем остановить диджитализацию нашей жизни — умных вещей с каждым годом будет становиться всё больше. А вместе с ними и новых рисков, которые будут касаться каждого из нас. Поэтому единственный способ избежать серьёзных потерь и даже угроз для жизни и здоровья — максимально полно использовать весь доступный арсенал средств кибербезопасности и не забывать о личной кибергигиене.