Феміда на швидкості 150 км/год: чому в Україні статус нардепа став «ліцензією на вбивство»

Магічне зникнення підстав для санкцій проти резидента ФСБ Юрія Іванющенка

РПЦ як секта депортацій: свідчення Владислава Гаврилова про викрадення

Бойтесь лампочек. Как хакеры ломают «умный» дом

КІБЕРЗЛОЧИННІСТЬ | ВС, 2021-06-13 08:37

Версия для печати

Киберпреступники могут получить доступ к вашим электронным устройствам, и это очень опасно.

«**Умный дом**» был яркой идеей. Это словно из научной фантастики. Все приборы в доме - батареи, лампочки, дверные звонки, посудомоечные машины, пылесосы и дверные замки - объединены в сеть и «общаются» между собой. Нажимаешь кнопку - и все приборы, которые надо, работают или наоборот - переходят в режим экономии энергии. Экономно, высокотехнологично, современно ...

> На эту тему: **Что такое современный «умный дом»: безопасность и комфорт на новых технологиях**

И опасно. Ведь «**интернет вещей**» - это также интернет, а значит любая вещь, которая к нему подключена, уязвима к хакерским атакам. И если вы думаете, что ваша **умная швабра** (это еще **не самое худшее** из «умного», что бывает на рынке) никому не нужна, то ошибаетесь - хакерам нужны, по меньшей мере, ваши данные.

Рынок умных домов растет: в 2019 году его **оценили** в 32,3 миллиарда долларов, и эта цифра **возрастет** до 93,4 млрд до 2027 года. В то же время **все больше** предметов, о которые мы раньше никогда не подумали, что они могут быть подключены к интернету, «умнеют». Зеркало на стене превращается в экран, газонокосилка косит газон сама, коврик для йоги регулирует давление на тело человека, холодильник сигнализирует, когда заканчивается молоко, а лампочка тускнеет или становится ярче по голосовой команде; есть даже **умный вазон**.

Растет и опасность. Если эти штуки используют беспроводной доступ к интернету, их можно сломать и взять под контроль. В некоторых случаях такой взлом угрожает жизни и здоровью людей. Хакеры могут заставить приборы подглядывать за вами, подслушивать вас или собирать данные о вас.

Хакер под псевдонимом LimitedResults сломал лампочку LIFX - компании, производящей освещение для умных домов. Он **рассказал**, как менее чем за час получил доступ к логину и паролю беспроводной сети владельца дома. Для этого ему пришлось буквально разломать подержанную «умную» лампочку и выковырять микросхему. Подсоединив чип к другому через USB-порт, хакер добрался до памяти лампочки и обнаружил, что пароль и логин к беспроводной сети дома, где она стояла, записан простым текстом. Производители никак не защитили лампочку - каждый мог контролировать ее и записывать данные в ее память.

В 2017 году **сломали** «умные» игрушки компании Spiral Toys. Более двух миллионов записей голосов детей и личная информация 800 000 пользователей, в том числе адреса электронной почты и пароли, оказались в открытом доступе в сети.

НОВИНИ

20:00 **Погода в Україні на 8 травня: місцями короткочасні дощі та грози**

19:09 **Павло Казарін: Пастка безстроковості**

18:04 **Олег Чеславський: ЦПК і розкрадання стратегічних активів**

17:10 **Геннадій Левітас: Піхота - рід військ, який зникає**

16:04 **Касьянов: Вони крадуть 4 млн доларів на добу**

15:10 **Батьки очільника столичної прокуратури Сергія Ходаківського та судді Соборного суду Дніпра Максима Ходаківського у 2020 році придбали квартиру в Москві**

14:59 **ВАКС засудив заступника голови Рівненської облради за хабар до 9 років позбавлення волі**

13:01 **2500 гектарів лісу палає на Чернігівщині через російські обстріли**

12:19 **Підозрювана у хабарництві: ВРП звільнила львівську суддю Ірину Малех**

11:50 **УПЦ МП має повернути державі споруди Богоявленського монастиря у Кременці - суд**

ПІДПИСКА НА КАНАЛ

За две недели до взлома немецкие законодатели **предупредили** родителей, что «умная» кукла Spiral Toys под названием My Friend Cayla опасна. Федеральное агентство по сети **заявило**, что изъяло куклы Cayla с рынка Германии, и призвало родителей уничтожить «шпиона». С тех пор куклы, которые имеют микрофоны и ставят детям вопрос о них и их родителях, в Германии запрещены как «скрытые ишпионские устройства».

В 2019 году американец Арджун Суд **сообщил**, что камеры наблюдения и термостат в его «умном» доме сломали. Когда он вошел в комнату семимесячного ребенка, то услышал голос, который общался с малышом. Его жена заметила, что термостат настроен на температуру 32.2°C. Когда мужчина отнес ребенка в гостиную, «умная» камера включилась и кто-то начал ругаться.

«Когда я понял, что происходит, наступила паника и растерянность, и у меня остыла кровь, - сказал Суд. - Мы не знаем, как долго кто-то был в нашем аккаунте и сколько частных разговоров он прослушал». Устройства «умного дома» Суда изготовила компания Nest, которой владеет Google. Компания заявила, что ее системы не сломали, а пароль к устройствам Суда якобы был украден через другие сайты.

В 2015 году группе исследователей **удалось** установить полный контроль над **паркетным внедорожником**. Они подключили машину к сети, воспользовавшись уязвимостью программы во время ее обновления, и угнали джип. Они **могли** полностью контролировать машину - ускорять, тормозить, изменять направление движения.

«Я ехал со скоростью 113 километров в час окраиной Сент-Луиса, когда хакерская программа захватила авто. Я не касался панели управления, но джип начал выпускать холодный воздух с максимальной мощностью. Затем радиоприемник переключился на местную хип-хоп волну и выкрутил громкость на полную. Я нажал кнопку выключения на панели управления, но ничего не произошло. Затем начали работать стеклоочистители и жидкость разлилась по лобовому стеклу», - **описал** свой опыт участия в этом эксперименте журналист Wired Энди Гринберг.

> На эту тему: **Константин Корсун: «Существующая система кибербезопасности - живой труп»**

Это был уже не первый такой эксперимент. В 2013 году исследователи Чарли Миллер и Крис Валасек **выключили** тормоза, посигналили, отключили ремень безопасности и дистанционно побыли за рулем двух машин. Это был «допотопный» взлом: компьютер ученых был подключен к встроенному диагностическому порту автомобилей. И даже раньше - в 2011 году - американские исследователи **продемонстрировали**, как можно по беспроводной сети выключить тормоза и замки на автомобиле. Правда, деталей они не раскрывали. Производители автомобилей даже после этих успешных взломов настаивали, что в реальной жизни взять авто под контроль невозможно - оно надежно защищено. Однако технологии развиваются, машины становятся все более компьютеризированными, поэтому их уязвимость для хакеров растет.

Дома, которые поджаривают своих владельцев, и машины, которые не слушаются руля, - это значительно опаснее лампочки.

По **словам** доктора Захида Анвара из американского университета Фонбонн, уязвимые «умные» устройства - это «уличные» автоматы со встроенным компьютером, например, поливалки или механизмы для закрывания гаражных дверей. Они часто совсем не поддерживают протоколы безопасности. Сильно уязвимы устройства, которыми управляют с помощью программы на компьютере или смартфоне, - камеры безопасности, «умные» выключатели и лампочки, дверные замки, термостаты и т. д. Сравнительно менее уязвима обычная бытовая техника - холодильники, печки, стиральные машинки. Но и их ломают.

Прежде чем купить «умное» устройство, подключаемое к сети, следует убедиться, что оно качественное. Ищите отзывы, попробуйте выяснить, ломали ли уже изделия этой компании и что она сделала, чтобы их обезопасить. Посмотрите, что пишет производитель о безопасности на своем сайте, позволяет ли он обновлять устройства и обеспечены ли они автоматической корректировкой ошибок.

Очень важно изменить пароль и логин, установленные на устройстве по умолчанию. По **подсчетам** Positive Technologies, 15% владельцев «умных» устройств оставляют заводской пароль, который хакерам даже не придется подбирать, - он указан в инструкции. Хакеры, которые создают сети ботов, используют этот стандартный пароль, чтобы добавлять компьютеры к сети. Это, кстати, аргумент для людей, которые считают, что хакеры никогда не заинтересуются их компьютерами и устройствами. Чтобы пострадать от хакерских атак, не обязательно быть важной персоной; иногда злоумышленникам нужны не вы и ваши секреты, а мощности вашего компьютера, которым будут руководить дистанционно, а вы об этом даже не будете подозревать.

Защититься может помочь безопасная беспроводная сеть. Приобретите роутер надежного бренда и измените логин и пароль, установленные на умолчанию. Назовите сеть так, чтобы она не выдавала ваших персональных данных. Возможно, стоит воспользоваться возможностью скрыть сеть, чтобы она не просматривалась для всех - тогда ее не так легко сломать.

> На эту тему: **Будущее наших персональных данных**

Многие роутеры позволяют создавать несколько вайфай-сетей. Создайте отдельную для «умных» устройств. Если хакеры ее взломают, это даст им доступ к вашему холодильнику или роботу-пылесосу, но не к ноутбуку и телефону. И наоборот - люди, которые имеют пароль к вашей рабочей сети, без доступа к «умным» устройствам.

Когда едете из города, выключайте технику, которая не будет работать. Это не только сэкономит энергию, но и сделает устройства неуязвимыми для хакеров (ломать выключенные аппараты они еще не научились). Оставьте работать холодильник,

камеру наблюдения, но выключите пылесос и печь.

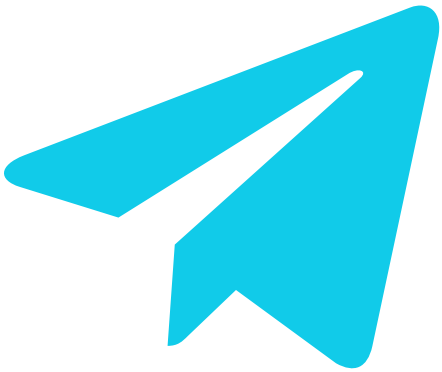
Если вы решили продать, выбросить или подарить какойе-то из ваших «умных» устройств, удалите из него все данные. Как это сделать, написано в инструкции. Иначе человек, к которому попадет устройство, сможет автоматически получить доступ ко всей вашей сети.

—

София Ходева, опубликовано в издании DETECTOR.media

На эту тему:

- **Увы, это не паранойя: за нами следят**
- **После Сноудена: как разоблачения предателя ЦРУ изменили мир**
- **Битвы Великой технологической: как в современном мире сражаются за мировое господство**
- **Китайский вызов. Поднебесная и Интернет. Часть 1**
- **Китайский вызов. Поднебесная и Интернет. Часть 2: Огненная стена**
- **Терабайты — «нефть» будущего. Метод анализа больших данных меняет социальную реальность**
- **США подозревают власти Китая в краже персональных данных свыше 500 млн человек - NYT**
- **Тиаго Форте: Будущее будет странным**



Читайте «Аргумент» в **Facebook** и **Twitter**

Если вы заметили ошибку, выделите ее мышкой и нажмите ***Ctrl+Enter.***

Коментарі

НОВИНИ ПАРТНЕРІВ

РЕКЛАМА

ВІДЕО

Воїни «Альфи» СБУ — ТОП-1 серед підрозділів Сил оборони за результатами бойової роботи у квітні

Про що не можна було жартувати в СРСР

HEAVY SHOT, VAMPIRE, NEMESIS: як «Баба Яга» б'є ок*пантів

Контакт: ***uargumentum@gmail.com***