Пресс-релиз

Эксперты Avast: 44% «умных» домов в России подвержены риску атак киберпреступников

Проверка 1 119 791 российских домашних сетей выявила новые уязвимости «умных» домов, актуальные для всех стран мира

- В 44,07% «умных» домов есть хотя бы одно уязвимое устройство, которое ставит под угрозу безопасность всей сети.
- 96,66% домашних маршрутизаторов уязвимы.

Конференция MOBILE WORLD CONGRESS, Барселона, Испания, 25 февраля 2019 г. — Специалисты компании Avast (LSE:AVAST), мирового лидера в области решений по цифровой безопасности, рассказали, что почти половина «умных» домов уязвимы к кибератакам. В отчете Avast Smart Home Report 2019 представлены данные анализа 16 миллионов сетей «умных» домов. Согласно этим данным, в 20,11% домов в России имеется более пяти подключенных устройств. В 44,07% таких «умных» домов есть хотя бы одно уязвимое устройство. Эти цифры свидетельствуют о серьезном риске, который технология «интернет вещей» представляет для домовладельцев. Всего лишь одно незащищенное устройство может поставить под угрозу работу всей домашней сети.

«Люди, которые покупают телевизор с функцией «Smart TV», чтобы смотреть любимый сериал по подписке Netflix, или подключают детский видеомонитор к сети Интернет, часто не знают, как обеспечить безопасность этих цифровых приборов, — отмечает **Ондржей Влчек** (Ondrej Vlcek), президент подразделения потребительских решений компании Avast. — Чтобы подключиться к сети дома, хакеру достаточно найти одно незащищенное устройство. После этого он получит доступ к остальным устройствам, а также к персональным данным, которые на них хранятся или передаются с их помощью, включая видеотрансляции в режиме реального времени и голосовые сообщения. Простые меры безопасности — использование сложных уникальных паролей и двухфакторной аутентификации для защиты устройств, своевременная установка исправлений и обновление встроенного ПО — позволят значительно повысить надежность цифрового дома».

Слишком простые пароли и устаревшие программы

Как выяснили эксперты, источник уязвимости большинства домашних устройств в (68,9% в России) — недостаточно сложные пароли и использование однофакторной аутентификации. На 33,6% устройствах в России не были установлены последние исправления безопасности.

Специалисты Avast также проверили 11 миллионов маршрутизаторов по всему миру. Выяснилось, что более половины устройств (59,7%) имеют упомянутые уязвимости в реквизитах доступа и ПО. В России этот показатель составил 96,66%. Устаревшие программы часто являются самым слабым звеном в системе безопасности. Через них киберпреступники легко получают доступ к другим подключенным приборам.

Самые уязвимые устройства

Исследователи Avast назвали пять популярных устройств, которые наименее защищены от атак хакеров:

1. Принтер — 32,9%.
2. Сетевое устройство (точка подключения, способная принимать и отправлять данные, выступая в качестве узла связи) — 28,9%.
3. Камера видеонаблюдения — 20,8%.
4. Сетевое хранилище данных (NAS) — 7,8%.
5. Медиаплеер (ТВ-приставка, Chromecast, TiVo) — 5.3%.

В России самые уязвимые устройства:

1. Телевизор — 46.4%.
2. Принтер — 15.4%.
3. Камера видеонаблюдения — 11.2%.
4. Медиаплеер — 8.9%.
5. Планшет — 8.3%.

Принтеры оказались самыми многочисленными уязвимыми устройствами во всем мире. В каждой из стран, в которых проводилось исследование, они занимали одну из трех

верхних строчек этого антирейтинга, а в США, Канаде, Австралии, Сингапуре, Южной Корее и Японии вышли на первое место. Медиаплееры (ТВ-приставки, Chromecast, TiVo), которые также вошли в пятерку плохо защищенных «лидеров», являются третьим по популярности видом устройств IoT в любом «умном» доме. Первые два — это телевизоры и принтеры.

Полная версия отчета доступна по ссылке:
https://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf

***Методология**
Представленные в документе данные получены по результатам сканирований, выполненных пользователями Avast на ПК с помощью решения Avast WiFi Inspector в сентябре 2018 года. Всего исследование охватило 16 миллионов домашних сетей во всех странах мира. Сканирование затронуло 56 миллионов устройств. Главное внимание в отчете уделяется новым подключенным приборам, данные по ПК и смартфонам остались за рамками исследования.

О платформе Avast Smart Life
Платформа безопасности IoT-устройств Avast Smart Life на базе ИИ анализирует отклонения в сетевом трафике «умного» дома и уведомляет пользователя об аномальном поведении устройств — например, если их холодильник начал отправлять множество электронных писем без видимых причин. В настоящее время компания Avast разрабатывает версию сервиса Smart Life для мобильных устройств, которая будет предоставляться пользователям через партнеров-операторов связи, а также потребительское решение на базе Smart Life с простой установкой и настройкой.

Avast (LSE: AVST) — мировой лидер в области решений цифровой безопасности. Компания предлагает продукты под брендами Avast и AVG, которые обеспечивают более 400 миллионов интернет-пользователей качественной защитой от всех типов интернет-угроз и опасностей растущего Интернета вещей. Сеть обнаружения угроз Avast является одной из самых совершенных в мире и использует технологии машинного обучения и искусственного интеллекта для обнаружения и предотвращения угроз в режиме реального времени. Продукты Avast для мобильных устройств, ПК и Mac удостоены сертификатов VB100, AV-Comparatives, AV-Test, OPSWAT, West Coast Labs и др. Посетите сайт: www.avast.com.