НОВОСТИ

Microsoft сообщила о масштабной кампании российских хакеров по взлому сетей Wi-Fi в отелях по всему миру

Настоящее Время

меньше минуты назад

Microsoft заявила о масштабной кибератаке со стороны Storm-2945 – подгруппы хакерской группировки Midnight Blizzard (Nobelium) – с целью манипулирования трафиком в сетях гостиничного сектора по всему миру.

Кампанию по взлому сетей Wi-Fi в отелях Microsoft назвала CaptiveCrunch. В ее рамках хакеры Storm-2945 использовали метод AitM [Adversary-in-the-Middle – тип атаки "человек посередине"] для перенаправления пользователей через контролируемую ими фишинговую инфраструктуру, а также распространения вредоносного программного обеспечения (ПО) под видом обновлений браузера или операционной системы в ответ на автоматические запросы о подключении, отправляемые браузерами пользователей.

По данным компании, было распространено несколько вариантов вредоносного ПО, в том числе полнофункциональные трояны удаленного доступа (RAT) для Windows, написанные на языке Golang. Они позволяют злоумышленникам собирать сведения о системе, файлы и данные о нажатиях клавиш; похищать учетные данные и токены сеанса, проводить аудио- и видеонаблюдение, мониторить съемные носители, а также предоставлять удаленный доступ к зараженным системам.

СМОТРИТЕ ТАКЖЕ:

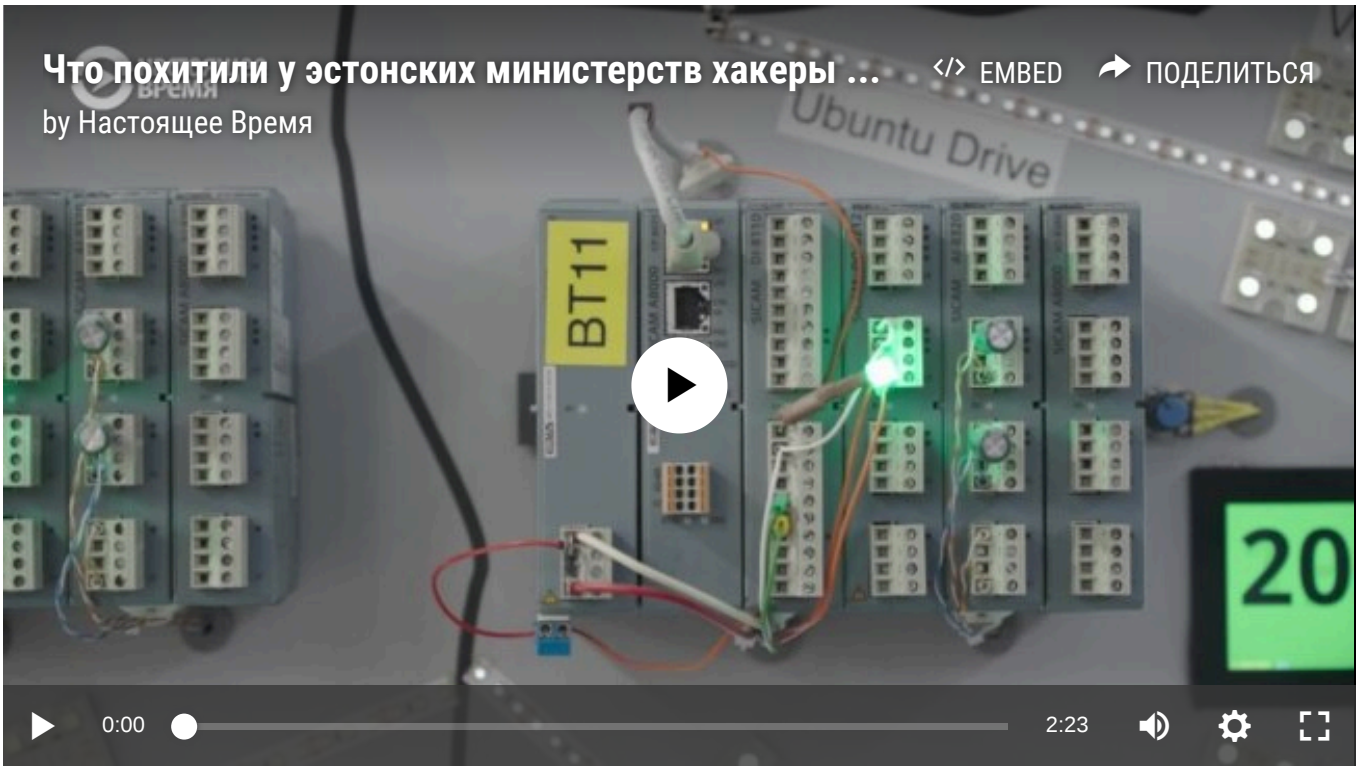
Спецслужбы ЕС, США и Украины раскрыли операцию российских хакеров по взлому Wi-Fi-роутеров по всему миру

Группа Storm-2945, как сообщается, проводит свои операции с февраля 2026 года, а наблюдение за ними Microsoft Threat Intelligence вела с мая этого года.

В Microsoft указывают, что Midnight Blizzard – российская хакерская группировка, которую в США и Великобритании относят к Службе внешней разведки России. Эта группировка, как отмечается, в основном нацелена на правительства, дипломатические представительства, НПО и поставщиков информационных технологий в США и Европе.

"Midnight Blizzard последовательна и настойчива в своих целях, и их задачи редко меняются. Их цель — сбор разведывательной информации посредством многолетней и целенаправленной шпионской деятельности в поддержку внешнеполитических интересов России", – заявили в компании.

Ранее спецслужбы Германии, США и Украины выяснили, что группировка российских хакеров APT28, также известная как Fancy Bear или Forest Blizzard, взломала несколько тысяч Wi-Fi-роутеров TP-Link по всему миру с целью получения информации, в том числе о критически важной инфраструктуре



СМОТРИТЕ ТАКЖЕ:

- Microsoft сообщила об атаке российских хакеров – они получили доступ к почте руководителей компании
- Суд в США арестовал 107 доменных имен, которые использовала связанная с ФСБ хакерская группа для кибератак на НКО, политиков и журналистов
- Великобритания обвинила ФСБ РФ в хакерских атаках и попытке вмешательства в политические процессы и ввела санкции против двух россиян
- Операция "Скайфрейм". Как иранская разведка зарабатывает в России на оружии, похищенном украинском зерне и детских мультфильмах
- Госдепартамент США объявил награду до 10 млн долларов за информацию о хакерах DarkSide
- США внесли в санкционный список 11 россиян, подозреваемых в киберпреступлениях против американских органов власти
- Суд арестовал на два месяца восьмерых задержанных по делу о хакерской группировке REvil
- В США россиянину предъявили обвинения в разработке программ для хакерской сети, ему грозит 60 лет тюрьмы
- Чем известна воинская часть 74455, где якобы служат офицеры – хакеры ГРУ
- Эксклюзив: ЕС введет санкции против российских хакеров – офицеров ГРУ, разыскиваемых за кибератаки против Эстонии
- Великобритания обвинила хакеров ГРУ во взломе около 10 тыс. камер на границе Украины и стран Европы для слежки за поставками западной помощи

МАТЕРИАЛ ИЗ РАЗДЕЛОВ: