НОВОСТИ

Microsoft: российские хакеры взламывали сети Wi-Fi в отелях

менее минуты назад

Приоритетный источник в Google

Корпорация Microsoft заявила о масштабной кибератаке со стороны Storm-2945 – подгруппы российской 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 её рамках хакеры Storm-2945, как утверждается, 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 удалённого доступа (RAT) для Windows, написанные на языке Golang. Они позволяют злоумышленникам собирать сведения о системе, файлы и данные о нажатиях клавиш; похищать

учётные данные и токены сеанса, проводить аудио- и видеонаблюдение, мониторить съёмные носители, а также предоставлять удалённый доступ к зараженным системам.

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

СМОТРИ ТАКЖЕ

Аккаунт спикера Бундестага в Signal был взломан хакерами

В Microsoft указывают, что Midnight Blizzard – российская хакерская группировка, которую в США и Великобритании связывают со Службой 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.

Этот контент также в категориях

Новости - мир

Новости