Недавнее исследование раскрыло слежку беспрецедентного масштаба.

Исследователи из Университета Мэриленда выявили серьёзные проблемы безопасности и конфиденциальности в системах геолокации Apple Inc. – американская корпорация, которая занимается производством персональных и планшетных компьютеров, телефонов, аудиоплееров и программного обеспечения. Наиболее известные продукты компании это линейка персональных компьютеров Macintosh, мобильные телефоны iPhone, планшетные компьютеры iPad, операционная система Mac OS X, медиаплеер для проигрывания и систематизации аудио и видеофайлов iTunes, набор мультимедийного программного обеспечения iLife, набор приложений iWork, web-браузер Safari и мобильная операционная система Apple iOS.

 Международное исследовательское агентство Millward Brown признало торговую марку Apple самым дорогим брендом в мае 2011 года. В начале августа 2011 года Apple стала самой дорогой компанией по рыночной капитализации, которая составляла $338,8 млрд 10 августа." data-html="true" data-original-title="Apple" >Apple и Starlink — это проект компании SpaceX, основанной Илоном Маском, направленный на создание глобальной сети спутникового интернета. Основная цель Starlink — обеспечить доступ к высокоскоростному интернету в отдалённых районах по всему миру, где традиционные средства связи недоступны или неэффективны.

 Система Starlink включает в себя сеть тысяч спутников, которые непрерывно летят вокруг Земли на низких орбитах. Эти спутники связываются с небольшими терминалами на поверхности Земли, которые клиенты могут устанавливать у себя дома или в офисе.

 Преимущества Starlink включают в себя высокую скорость интернета, низкие задержки и возможность подключения в отдалённых регионах, где проводная инфраструктура отсутствует. Этот проект может также иметь значительное значение для связи в кризисных ситуациях и для обеспечения интернетом научных исследований в далёких уголках планеты." data-html="true" data-original-title="Starlink" >Starlink. В ходе исследования стало ясно, что данные, которые компании собирают и публично делятся, могут использоваться для отслеживания местоположения миллиардов устройств по всему миру.

Apple собирает данные о точном местоположении всех Wi-Fi точек доступа, видимых её устройствами. Это позволяет устройствам компании предоставлять пользователям информацию о местоположении без постоянного обращения к GPS. Аналогичные системы работают и у Google. Оба гиганта фиксируют идентификаторы Wi-Fi точек доступа, такие как MAC-адреса (BSSID).

В отличие от Google, Apple возвращает геолокацию до 400 близлежащих BSSID, что позволяет устройствам определять своё местоположение на основе известных точек

доступа. Этот объем данных позволил исследователям из Мэриленда отслеживать перемещение отдельных устройств в любой точке мира. Они запросили данные о более чем миллиарде случайно сгенерированных BSSID и получили информацию о 488 миллионах точек доступа.

Так, исследователи использовали полученные данные для мониторинга перемещений спутников Starlink. Каждое устройство Starlink оснащено собственной Wi-Fi точкой доступа, которая автоматически индексируется ближайшими устройствами Apple с включёнными службами геолокации.

В ответ на результаты исследования, компания Starlink выпустила обновления программного обеспечения, которые рандомизируют BSSID устройств, что затрудняет их отслеживание. Исследователи отметили, что в последние месяцы количество устройств Starlink, местоположение которых можно было бы определять с помощью системы Apple, действительно снизилось.

Apple также отреагировала на исследование, внеся изменения в свою политику конфиденциальности. В марте 2024 года компания позволила пользователям исключать свои Wi-Fi точки доступа из системы, добавив суффикс «_nomap» к имени сети.

Исследователи подчеркнули, что отсутствие возможности отказаться от сбора данных ранее представляло серьёзную угрозу для конфиденциальности. По их словам, Apple должна внедрить дополнительные меры для ограничения злоупотреблений своим API, например, ограничение скорости запросов.

Обнаруженные уязвимости представляют серьёзную проблему для пользователей по всему миру. Исследование показывает необходимость дополнительных мер безопасности и конфиденциальности в системах геолокации, чтобы защитить пользователей от потенциальных угроз и злоупотреблений.