Невидимая паутина подключений плотно опутывает каждый смартфон, подрывая приватность владельца.

Современные мобильные приложения активно взаимодействуют с различными интернет-сервисами, даже когда телефон находится в режиме ожидания. Недавнее исследование, проведённое изданием Cybernews — это информационное издание, которое занимается освещением проблем информационной безопасности. Они публикуют новости, статьи, аналитику и исследования, касающиеся различных аспектов кибербезопасности, включая уязвимости в ПО, кибератаки и защиту данных. Cybernews также предоставляют информацию о технологиях защиты и направлениях развития индустрии кибербезопасности." data-html="true" data-original-title="Cybernews" >Cybernews, демонстрирует, что даже одно установленное на смартфоне приложение может подключаться к десяткам доменов.

Так, если установить на iPhone приложение Instagram* или X** (Twitter), устройство подключится к 10 доменам на каждое приложение, а в случае с Reddit, даже без входа в учётную запись, количество доменов для подключения и вовсе перевалит за 30.

Эти цифры существенно увеличиваются при активном использовании устройств и установке десятков различных приложений. А если растянуть наблюдение хотя бы на неделю, то можно с удивлением для себя обнаружить, что ваш любимый смартфон подключался без вашего ведома к сотням различных доменов.

Домен представляет собой адрес веб-сайта, который используется для доступа к различным сервисам, например, «facebook.com» или «google.com». Система доменных имён (DNS (Domain Name System) — это система, используемая для преобразования доменных имен в IP-адреса. В основном, она служит своеобразной телефонной книгой Интернета.

 Когда вы вводите URL-адрес в браузере, например, «www[.]example[.]com», DNS определяет соответствующий этому домену IP-адрес, чтобы браузер мог подключиться к нужному веб-серверу и отобразить запрашиваемую страницу.

 Эта система позволяет людям использовать запоминающиеся доменные имена вместо сложных числовых IP-адресов при поиске ресурсов в Интернете." data-html="true" data-original-title="DNS" >DNS) переводит эти адреса в IP-адреса, понятные устройствам.

Количество фактических подключений к доменам может значительно превышать число DNS-запросов. Так, эксперт по кибербезопасности Даниэль Трахтемберг из компании ReasonLabs пояснил, что один DNS-запрос может соответствовать множеству

фактических API (Application Programming Interface) — это набор готовых функций и процедур, которые позволяют разработчикам создавать программное обеспечение, взаимодействующее с другими приложениями или сервисами. API определяет, как различные компоненты программного обеспечения должны взаимодействовать друг с другом, обеспечивая при этом безопасность и стабильность работы системы. API часто используется в веб-разработке для создания сайтов и приложений, которые используют данные и функциональность других сервисов." data-html="true" data-original-title="API" >API-вызовов, поскольку устройства кэшируют результаты запросов и используют их до истечения срока действия записи.

На практике это означает, что устройства могут совершать тысячи подключений к серверам в течение часа. Например, приложения для отслеживания маршрутов могут обращаться к серверам каждую секунду для обновления данных о местоположении.

Результаты прошлых экспериментов Cybernews показали, что iPhone в среднем совершает 3308 DNS-запросов в день, в то время как Android-смартфоны — 2323 запросов. Кроме того, некоторые из запросов могут направляться, например, в Россию или Китай, даже если устройство физически находится на территории условной Литвы.

Частота и количество подключений не всегда говорят о содержании передаваемых данных. Данные могут включать как телеметрию устройства, так и личную информацию пользователя, которая затем используется для поведенческого анализа и рекламы. Иногда эти данные могут продаваться третьим сторонам.

Apple в своём инструменте App Privacy Report подчёркивает, что домены, с которыми контактируют множество приложений, могут собирать данные о пользователях для создания профилей и использования их в рекламных целях.

Эксперт по VPN Джеймс Миллин-Эшмор из Independent Advisor рекомендует регулярно проверять настройки конфиденциальности используемых сервисов. Большинство платформ предоставляют пользователям возможность контролировать, кто видит их публикации и личную информацию, а также, кто — может получать доступ к этим данным.

Тем не менее, полагаться исключительно на настройки конфиденциальности недостаточно. Для минимизации нежелательного трафика следует использовать блокировщики рекламы, DNS-фильтры, VPN и ограничивать количество установленных приложений. Пользователи iPhone, в свою очередь, могут также воспользоваться режимом «Lockdown Mode», который позволит многократно снизить любые риски.

* Компания Meta и её продукты признаны экстремистскими, их деятельность запрещена на территории РФ. ** Социальная сеть запрещена на территории Российской Федерации.