Мобильные приложения могут отслеживать ваше местоположение и продавать данные о нем третьим лицам. Что с этим можно сделать?

https://te.legra.ph/Mobilnye-prilozheniya-mogut-otslezhivat-vashe-mestopolozhenie-i-prodavat-dannye-o-nem-tretim-licam-CHto-s-ehtim-mozhno-sdelat-11-13

Какие мобильные приложения следят за вами

В марте, когда пандемия еще только начиналась, в твиттере компании Tectonix появилась красивая визуализация того, как люди, отдыхавшие на одном из пляжей во Флориде, впоследствии разъехались по всей территории США. Она основывалась на данных, предоставленных некой компанией X-Mode. Увидев эту визуализацию, директор Костин Райю (Costin Raiu) задумался: откуда в X-Mode взяли эти данные?

Как выяснилось, эта организация разрабатывает SDK (компонент, который разработчики могут легко встроить в свои приложения) и готова ежемесячно платить использующим ее разработчикам ту или иную сумму в зависимости от количества пользователей приложения. Этот компонент, в свою очередь, собирает информацию о местоположении и некоторые другие данные (в частности, показания датчиков движения смартфона) и отправляет их на серверы X-Mode. Впоследствии компания продает эти данные всем желающим.

В X-Mode утверждают, что, во-первых, данные продаются в обезличенном виде, а во-вторых, что SDK почти не влияет на время работы смартфона от одной зарядки и тратит от 1 до 3% заряда, так что пользователи даже не заметят его и не испытают каких-либо неудобств. В компании также считают, что заниматься подобным сбором сведений «вполне законно» и что их SDK полностью соответствует Общему регламенту по защите данных (GDPR).

Сколько существует подобных приложений для отслеживания

Райю задался вопросом, а не отслеживают ли и *его* смартфон аналогичным образом? Он пришел к выводу, что самый простой способ это выяснить — определить адреса командных серверов, которые использует SDK, и затем начать анализировать исходящий трафик с устройства. Если какое-то приложение на смартфоне связывается хотя бы с одним из таких узлов, значит, слежка действительно ведется. Соответственно, для начала Райю нужно было узнать адреса этих серверов. Проведенное расследование легло в основу его выступления на конференции SAS@Home.

Потратив некоторое время на реверс-инжиниринг, расшифровку данных и прочие процедуры, Райю определил адреса командных серверов и написал программу, которая сообщает, если какое-либо приложение пытается к ним обратиться. По сути, он выяснил, что если в приложении есть определенная строка программного кода, то оно использует «следящий» SDK.

Райю обнаружил более 240 приложений со встроенной SDK. Суммарно число их установок перевалило за 500 миллионов. Если предположить, что каждый пользователь загрузил такое приложение единожды, то можно примерно оценить, что у каждого 16-го жителя планеты на устройстве есть приложение, следящее за его перемещениями. Выражаясь иначе, вероятность того, что *лично у вас* на смартфоне есть одно из этих приложений — 1/16.

Более того, X-Mode — лишь одна из десятков компаний в данной отрасли. Есть другие, и у них уже свои SDK.

Ничто не мешает разработчикам использовать сразу несколько подобных SDK. Например, когда Райю изучал одно из приложений, в которое автор встроил X-Mode SDK, он обнаружил еще пять подобных компонентов других компаний, которые тоже собирали данные о местоположении. Очевидно, что разработчик пытался выжать из приложения максимум прибыли.

Что самое интересное, вышеупомянутое приложение было платным! Так что даже если вы раскошелились на приложение, к сожалению, это еще не значит, что разработчики не попытаются заработать *еще больше*, продавая ваши данные.

Что можно сделать для борьбы со слежкой

Проблема с подобными SDK для отслеживания в том, что при загрузке и установке приложения вы просто не знаете, содержит оно такие компоненты или нет. Приложение может на вполне законных основаниях запрашивать разрешение на доступ к информации о местоположении, ведь без него многие функции не будут корректно работать. Но вместе с тем оно сможет продавать эти данные, и пользователю будет непросто понять, делает оно это или нет.

Чтобы помочь технически подкованным пользователям снизить вероятность слежки, Райю составил список серверов, которыми пользуются SDK для отслеживания. Он доступен на личной странице эксперта на GitHub. Компьютер RaspberryPi с установленными программами Pi-hole и WireGuard поможет проанализировать трафик в вашей домашней сети и выявить приложения, которые пытаются связаться с командными серверами любопытных SDK.

Однако для большинства пользователей это очень сложный путь. К счастью, есть более простые способы снизить риск слежки со стороны таких приложений и служб — ограничить права, которые они имеют на вашем устройстве.

- Проверьте, каким приложениям разрешено использовать информацию о местоположении. Мы уже рассказывали, как это сделать на Android 8 (в более поздних версиях ОС настройки могут немного отличаться, но общий принцип тот же). А вот как

можно остановить сбор информации о местоположении в iOS. Если вы считаете, что приложению не нужен доступ к вашему местоположению, смело его отзывайте.

- Используйте частичное разрешение на доступ к информации о местоположении — например, с помощью опции «только во время использования приложения». Это помешает приложениям следить за вами в фоновом режиме.
- Удаляйте приложения, которыми больше не пользуетесь. Если вы не открывали приложение месяц или дольше, то, скорее всего, оно вам и не нужно. Держать его «на всякий пожарный», бессмысленно — если в будущем оно понадобится, можно без проблем установить его заново. А пока смело его удаляйте.
- Учтите, что компоненты для отслеживания местоположения — это еще не самое страшное, что может скрываться в приложениях, даже легитимных и загруженных из официальных магазинов. Некоторые приложения изначально создаются вредоносными, а какие-то становятся таковыми после продажи или обновления. Поэтому мы рекомендуем установить на смартфон надежную защиту. Например, Kaspersky Internet Security для Android убережет от всех видов мобильных угроз.