УДК 621.396.96:623.62
DOI: https://doi.org/10.30837/IYF.IRTTPI.2024.497

МЕТОДИ ЛОКАЛІЗАЦІЇ КОРИСТУВАЧІВ СМАРТФОНІВ

Кашуба К. О.
Науковий керівник – к.т.н., доц. Ликов Ю.В.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ
м. Харків, Україна
e-mail: kateryna.kashuba@nure.ua

Modern developments in smartphone technology and wireless communications have provided unique opportunities for pinpointing the exact location of users. Localisation methods have become an integral part of the daily use of smartphones and other mobile devices. The most well-known methods for detecting the exact location of users are OSINT methods.

OSINT (Open Source Intelligence) – це сукупність методів та прийомів роботи з відкритими джерелами інформації. У цьому контексті найбільш очевидним способом визначення геолокації є аналіз загальнодоступної інформації, яку користувачі вводять у свої особисті онлайн-профілі. Це геомітки та чекіни в соціальних мережах, аналіз публічних записів, координати в метаданих завантажуваних фотографій, дослідження фото та відео контенту для виявлення розташування оператора тощо. До одного з найбільших постачальників публічної інформації можна віднести соціальні мережі. Майже кожен має обліковий запис в одній або кількох соціальних мережах. Існує кілька способів OSINT, які можна застосувати для виявлення розташування гаджетів.

Спосіб №1: Функція "Знайти мій телефон" на пристроях Android та iOS

І Apple, і Google дозволяють користувачам відстежувати та знаходити свої втрачені чи вкрадені пристрої. Для цього, необхідно мати увімкнену функцію «Знайти мій телефон» та активований обліковий запис Google/iCloud на пристрої. Відстеження доступне через веб-інтерфейс. Після того, як пристрій був втрачений або викрадений, потрібно увійти до свого облікового запису Google/iCloud за допомогою будь-якого пристрою і перейти на вкладку «Знайти мій телефон», розташовану за наступними адресами: Для iOS-пристроїв, Для Android-пристроїв.

Спосіб №2: Використання сервісів геологування

Ці сервіси дозволяють відстежувати розташування пристрою користувача під час переходу за гіперпосиланнями веб-сторінки. Працює це в такий спосіб. Спочатку сервіс геологування створює спеціальне гіперпосилання, що містить додаткові параметри передачі інформації про місцезнаходження користувача. І коли він переходить за згенерованим посиланням, браузер користувача надсилає дані про місцезнаходження (наприклад, координати GPS, LBS або інформацію про мережу Wi-Fi) на сервер, пов'язаний із

сервісом геологування. До популярних програм-геологерів входять в основному open source рішення (за винятком онлайн-сервісу IPlogger та програмного забезпечення Ngrok): Seeker, Trape, TrackUrl, Bigbro, R4ven, IPlogger, Ngrok.

Використання сервісів геологування має здійснюватися у межах законодавства. Це означає, що об'єкт стеження має дати дозвіл у браузері свого пристрою на передачу інформації геолокації. Якщо такий дозвіл отримано не було, його розташування буде визначено лише за IP-адресою.

В окремих випадках можна і за IP-адресою знайти розташування користувача. Але це буває вкрай рідко. У більшості випадків можна знайти лише дані про населений пункт, в якому користувач знаходиться.

IP (Internet Protocol) – це адреса пристрою в Мережі, яка визначає його місце розташування (деталізація обмежується країною і містом). Є дві версії протоколу IP: IPv4 (4 цифрові групи) і IPv6 (8 цифро-буквених груп). IP адреси можуть бути статичними (не змінюються) або динамічними (змінюються при кожному підключенні). VPN (Virtual Private Network) дозволяє змінювати IP-адресу, забезпечуючи шифрування трафіку та приховуючи локацію. Приховування розташування за IP-адресою допомагає зберегти приватність та захистити дані. Публічні IP-адреси унікальні і пов'язані з Інтернетом, приватні IP-адреси використовуються у межах конкретної мережі.

Спосіб №3: Спуфінг геолокації в Telegram

Цей спосіб передбачає зміну даних про місцезнаходження, щоб створити ілюзію, що ви знаходитесь в іншому місці. Справа в тому, що базовий функціонал Telegram надає функцію «Люди поряд», яка дозволяє знайти та взаємодіяти з іншими користувачами Telegram, які знаходяться поблизу. Ця функція ґрунтується на інформації про місцезнаходження, якою діляться самі користувачі месенджера та дає реальну можливість непомітно стежити за їх переміщеннями. API Telegram дозволяє це робити у радіусі від 500 метрів до 10 кілометрів. Тут можна скористатися одним із наступних open source рішень: Telegram Nearby Map, Telegram-Trilateration, Geogramint.

Головний недолік методу полягає в тому, що користувач, що відстежується, у будь-який момент може заборонити месенджеру доступ до геолокації в налаштуваннях смартфона. Не говорячи вже про те, що виявлення локації працює тільки щодо користувачів, які використовують Telegram на своїх пристроях. Також слід враховувати жорсткі обмеження месенджера. Сюди входить і обмеження кількості запитів 1 раз на 5 хвилин, і відключення радіусів пошуку 50 і 100 метрів.

Спосіб №4: Використання методів та прийомів ADINT

В основі способу ADINT (Advertising Intelligence) лежить ідея використання рекламних модулів, які часто містять коди відстеження або лічильники аналітики, щоб отримати інформацію про користувачів. ADINT дозволяє отримувати частковий портрет користувача (статтю, вік, місто проживання,

інтереси тощо) за рахунок аналізу даних, прив'язаних до його особистого рекламного ідентифікатора в різних системах. Для пошуку рекламних ідентифікаторів використовуються номер мобільного телефону, email та MAC-адреса. MAC-адреса – це унікальний ідентифікаційний номер обладнання, тоді як IP-адреса – це адреса, яка допомагає ідентифікувати мережеве з'єднання.

Ключовою особливістю ADINT є можливість відстеження переміщень користувача по всьому світу, використовуючи для цього геотаргетовану можливість реклами. Говорячи більш простою мовою, створюється реклама, яка буде показуватися на пристрої, що відстежується, в радіусі 500 метрів від його ймовірного місця знаходження. При його появі буде отримано повідомлення в особистому кабінеті рекламодавця. Для цього використовуються наступні сервіси: Яндекс. Аудиторії, Google Ads, Mytarget.

Цей спосіб, як і спуфінг в Telegram, передбачає не пряме відстеження пристрою користувача, а лише контроль над його можливою появою у певних локаціях (радіусом від 500 метрів до 10 кілометрів). При цьому ADINT не передбачає "стеження" за одним пристроєм. Рекламні майданчики допускають завантаження щонайменше 100 ідентифікаторів одночасно. Втім, виділити з них потрібний не так складно. Також за геотаргетинг у рамках ADINT доведеться платити.

В роботі розглянуто ще декілька інструменти геолокаційної розвідки OSINT.

Creepy – інструмент геолокаційної розвідки з відкритим вихідним кодом. Збирає інформацію про геолокацію через різні платформи (соціальні мережі та сервіси розміщення зображень). Представляє звіти на карті з фільтром пошуку за точним місцем та датою. Утиліта збирає геотеги з різних сервісів та виводить їх на Google-карту, показує ретвіти та статистику з пристроїв, з яких публікуються твіти.

SpiderFoot – відкритий інструмент розвідки, сумісний із Linux і Windows, написаний на Python. Має високу конфігураційну гнучкість та роботу на різних платформах. Інтегрується з командним рядком та простим графічним інтерфейсом. Автоматично запитує понад 100 джерел OSINT для отримання інформації про електронні листи, імена, IP-адреси та доменні імена.

У роботі розглянуто різні вразливості ПЗ смартфонів, методи і засоби, які дозволяють через ці вразливості отримати інформацію про розташування пристрою. Крім того, розглянуто питання забезпечення безпеки пристроїв використовуючи віртуальні приватні мережі (VPN).

Список використаних джерел:

1. Геолокація: Використання методів OSINT [Електронний ресурс] – URL: https://habr.com/ru/companies/tomhunter/articles/747162/ (дата звернення 03.03.2023).