ПРОБЛЕМАТИКА ВИКОРИСТАННЯ ВІДКРИТИХ ДЖЕРЕЛ ДАНИХ У РОЗСЛІДУВАНІ КІБЕРЗЛОЧИНІВ У МЕРЕЖАХ СТАНДАРТУ IEEE 802.11

Банах Роман Ігорович
аспірант кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Україна

Науковий керівник: Піскозуб Андріян Збігнєвич
ORCID ID: 0000-0002-3582-2835
канд. техн. наук, доцент, доцент кафедри захисту інформації
Національний університет «Львівська політехніка», Україна

Розвідка на основі відкритих джерел (OSINT) — це підхід до збору, аналізу та використання публічно доступної інформації з різноманітних джерел. Цей метод стає все більш популярним та стрімко розвивається, особливо у зв'язку з поширенням інтернету та інформаційних технологій.

Одним з ключових чинників, що сприяють розвитку OSINT, є зростання обсягу публічної інформації в онлайн-середовищі. Інтернет став величезним резервуаром даних, де кожен може знайти інформацію з різних джерел: соціальних медіа, новинних сайтів, відеоплатформ, блогів тощо. Таке розмаїття джерел дозволяє збирати інформацію з різних кутків та перевіряти її достовірність за допомогою перехресних перевірок.

OSINT може допомогти у пошуку людей за допомогою ресурсів, таких як WiGLE [1] або WiFiDB [2], через аналіз інформації про бездротові мережі Wi-Fi. WiGLE і WiFiDB – це бази даних (БД), які містять інформацію про розташування та характеристики бездротових мереж Wi-Fi по всьому світу.

Одним із способів використання цих ресурсів для пошуку людей є аналіз бездротових мереж, до яких підключаються пристрої конкретної людини. Коли пристрій підключається до мережі Wi-Fi, він відправляє ідентифікатор мережі (SSID) та інші дані. WiGLE та WiFiDB зберігають ці дані, які можуть бути використані для визначення приблизного місцезнаходження пристрою.

У роботі [3] представлено методику збору інформації про зловмисників, які намагались чи здійснили атаку на мережі стандарту IEEE 802.11 (Wi-Fi), такою інформацією може бути пошуковий пакет (Dot11ProbeRequest). Після виявлення даного пакету із пристрою зловмисника пропонується здійснити пошук у відкритих джерелах даних, наприклад ресурсі WiGLE, який є публічним і дозволяє завантажувати дані будь-кому.

Наприклад, якщо зловмисник постійно користується бездротовими мережами у певних місцях, можливо, що його можна виявити або зрозуміти її звички переміщення шляхом аналізу даних з публічних БД. Це може бути корисно для різних цілей, включаючи пошукові або дослідження поведінки.

Основною проблемою публічних БД з пошуку точок доступу є те, що доступ до завантаження даних у них може отримати будь-хто. Кожен пристрій, який збирає інформацію про Wi-Fi точки доступу має унікальні характеристики. Окрім того характеристики антен можуть бути різні і якщо один пристрій зможе ідентифікувати точку доступу на відстані 10 метрів, то інший, із потужнішою антеною ідентифікує її за 100 метрів. Також проблемою є те, що дані, які завантажуються користувачами не

проходять жодної перевірки і вважаються завідома правильними. Це може призвести до того, що в реальному місці локації такої точки доступу може не існувати.

Якщо говорити про БД WiFiDB, то в порівнянні з WiGLE, даних в ній не так багато (рис. 1—2). Як видно з рис. 2, то покриття на карті значно щільніше аніж на рис.1. З початку 2023 року БД WiGLE не відображає інформацію на карті по всій території України, але цю інформацію можна отримати якщо зробити запит до прикладного програмного інтерфейсу (application programming interface, API) ресурсу. Якщо запросити таку інформацію про певну точку доступу, то можна отримати дані про неї протягом великих проміжків часу. До прикладу, якщо дані про неї сканувались протягом години часу кожну секунду і відправлялись до сервісу WiGLE, то таких записів у базі даних буде 3600.

Рис. 1. **Покриття бази даних WiFiDB**

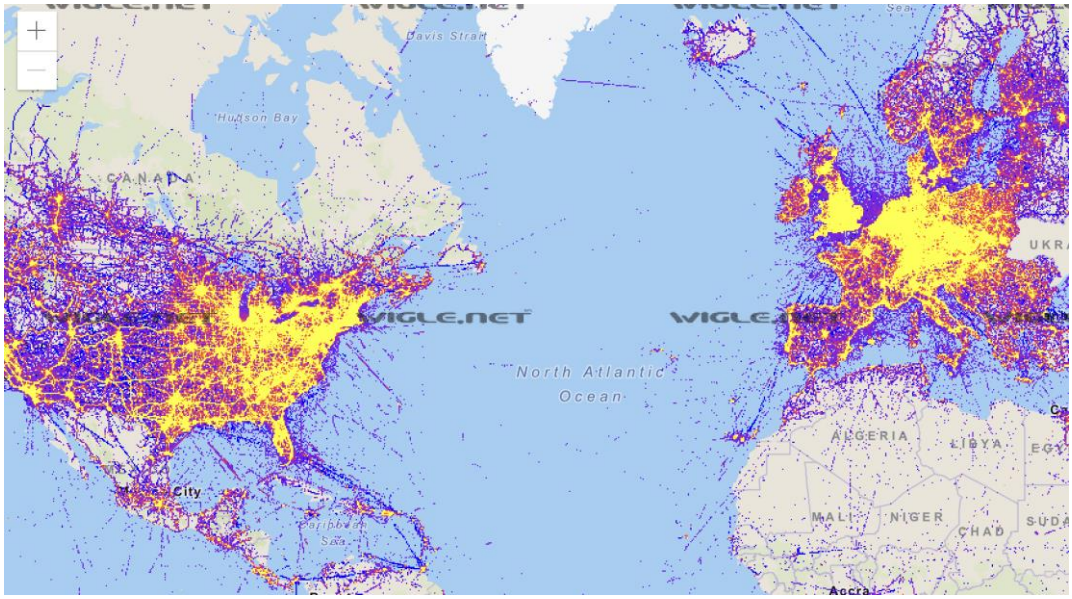

Рис. 2. **Покриття бази даних WiGLE**

При аналізі даних, коли дослідник знає інформацію лише про ідентифікатор імені (SSID) точки доступу, а БД повертає занадто велику кількість не агрегованих даних, дуже важко здійснити пошук можливого перебування зловмисника.

Висновки. Хоч відкриті джерела даних і можуть значно допомогти дослідникам у галузі кібербезпеки у розслідуванні злочинів проти комп'ютерних мереж стандарту IEEE 802.11. Та на сьогодні існує доволі велика проблема із відрізненням легітимних даних від зіпсованих даних у публічних БД. Причиною цієї проблеми є відсутність стандартизації обладнання, відсутність валідації та верифікації інформації, яка надходить до БД, відсутність агрегації даних та збір даних на основі часових рядів.

Все вище описане вище є проблемою для дослідників кіберзлочинів у мережах стандарту IEEE 802.11. Виправити ситуацію може підхід на основі агрегування даних, стандартизації обладнання для збору даних про точки доступу Wi-Fi, верифікація користувачів, які завантажують дані та валідація даних які завантажуються.

Список використаних джерел:

1. Wigle.net, All the networks. Found by Everyone [Електронний ресурс]. – Режим доступу: https://wiggle.net – Заголовок з екрану.
2. Vistumbler WifiDB [Електронний ресурс]. – Режим доступу: https://wifidb.net/ – Заголовок з екрану.
3. R. Banakh and A. Piskozub, "Attackers' Wi-Fi Devices Metadata Interception for their Location Identification," 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), Lviv, Ukraine, 2018, pp. 112-116, doi: 10.1109/IDAACS-SWS.2018.8525538.