

УДК 004.056

Піківець Г.М.¹, Корольков Р.Ю.²

¹ студ. гр. БКз-813м НУ «Запорізька політехніка»

² доц. кафедри інформаційної безпеки та наноелектроніки, НУ «Запорізька політехніка»

ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ АНАЛІТИКІВ ПІД ЧАС OSINT- РОЗСЛІДУВАНЬ

У сучасному світі, де відкриті джерела інформації (OSINT) стали важливим інструментом для розслідувань, питання анонімності аналітиків

набуває критичного значення [1]. Збір і аналіз даних з відкритих джерел охоплюють різноманітні платформи — від соціальних мереж до баз даних, доступних у відкритому доступі. Це створює додаткові ризики для аналітиків, які можуть стикатися з кіберзагрозами, ризиком розкриття особистих даних або тиском з боку тих, хто може бути об'єктом досліджень. Можна виділити наступні ризики. Перший — юридично-правовий. Слід розуміти, що не всі інструменти, які використовуються для розслідувань, є легальними: деякі програми можуть порушувати закони про конфіденційність або доступ до особистої інформації. Перед застосуванням будь-якого інструменту варто перевірити, чи відповідає його використання чинному законодавству. Другий ризик — фізичний. Розслідування, що стосуються впливових осіб, можуть бути небезпечними, оскільки такі особи можуть вдаватися до погроз або навіть застосовувати фізичне насильство [2]. З огляду на це, важливо діяти з максимальною обережністю та забезпечувати свою анонімність. Третій ризик — цифровий, який можна поділити на такі ризики як деанонімізація та зараження пристроїв шкідливим програмним забезпеченням. Використання персональної електронної пошти, телефонного номера, справжньої IP-адреси або банківської картки для розслідувань є недоцільним, оскільки це може значно спростити ідентифікацію аналітика з OSINT-розвідки. Програми з шкідливим програмним забезпеченням, або "віруси", можуть потрапити на пристрій, якщо завантажити файл з ненадійного джерела, перейти за підозрілим посиланням або встановити неліцензійне програмне забезпечення. У результаті стороння особа може отримати віддалений доступ до пристрою аналітика з OSINT-розвідки без його відома. Крім того, пристрій може бути уражений вірусом-шифрувальником, який зашифрує всі файли, що унеможливить їх відновлення. Тому важливо бути обережним із підозрілими файлами та посиланнями для мінімізації ризику зараження [3].

Для забезпечення анонімності під час OSINT-розслідувань важливо застосовувати комплекс стратегій, які допоможуть захистити особисту інформацію аналітика та мінімізувати ризики ідентифікації [4].

Перш за все, перед початком роботи треба підготувати окремі облікові записи під псевдонімами в соціальних мережах та на інших платформах [5], які використовуються для збору даних та телефонні номери та налаштувати робоче середовище на пристрої таким чином, щоб зберігати анонімність та захищати персональні дані.

Також, щоб мінімізувати ризик випадкового розкриття особистих даних, аналітики повинні працювати в ізольованому робочому середовищі. Це дозволяє відділити потенційно небезпечні завдання від основної операційної системи, зменшуючи ризик інфікування шкідливим програмним забезпеченням або випадкового витоку даних. Завдяки цьому підходу

аналітик може працювати з неперевіреними файлами, підозрілими сайтами та іншими небезпечними джерелами інформації, не піддаючи ризику основний комп'ютер.

Програмне забезпечення для віртуалізації надає широкі можливості налаштувань для створення окремих, ізольованих середовищ. VirtualBox, як програмний продукт з відкритим вихідним кодом, є одним із найпопулярніших варіантів, що дає змогу використовувати декілька операційних систем паралельно на одному пристрої. Його відкритий код забезпечує прозорість і дозволяє спільноті здійснювати аудит безпеки програми. VMware Workstation Pro, у свою чергу, є надійним та продуктивним рішенням, яке пропонує високий рівень підтримки та інтеграції, а також різноманітні функції для захисту конфіденційності й анонімності.

Крім того, при роботі в ізольованому середовищі аналітик має змогу створювати та відновлювати "знімки" (snapshots) системи, що забезпечує можливість швидкого повернення до попереднього стану в разі компрометації віртуальної машини або появи непередбачених проблем. Це значно підвищує ефективність роботи і знижує ризики втрати важливих даних або розкриття особистої інформації.

Другим кроком є використання певних браузерів, які можна використовувати для різних задач, та віртуальних приватних мереж (VPN). Браузер від компанії Google Chrome відомий своєю зручністю, швидкістю та стабільністю, регулярно отримує оновлення та має велику кількість розширень, крім того може створювати окремі профілі щоб розділити персональне використання та робоче візуально. Дуже добре реалізовано питання безпеки, кожна вкладка, плагін або розширення працюють у своєму власному ізольованому середовищі – це, так звана, технологія пісочниці. Головним недоліком Google Chrome є питання конфіденційності компанія збирає забагато даних про своїх користувачів через що важче забезпечити анонімність в роботі. Firefox від компанії mozilla у свою чергу приділяє більше уваги питанню конфіденційності та приватності на відміну від Chrome, за замовченням блокує рекламні трекери та має відкритий код, є технологія пісочниці однак вона не настільки добре реалізована як у Google Chrome. Браузер Tor є одним із найпопулярніших браузерів для анонімного доступу до інтернету. Він маршрутизує трафік через кілька серверів (вузлів), що дозволяє приховати IP-адресу та геолокацію користувача, дозволяє обходити цензуру, а також має вбудований захист від стеження. Його недоліком є зниження швидкості підключення через багаторівневий процес маршрутизації та варто пам'ятати що він орієнтований на анонімність а не на безпеку.

VPN є ефективним інструментом для захисту приватності та безпеки в інтернеті. Він приховує справжню IP-адресу користувача, що ускладнює визначення його геолокації, а також шифрує дані, забезпечуючи безпечне з'єднання навіть при використанні публічних Wi-Fi мереж. Крім того, VPN надає доступ до контенту, заблокованого у певних регіонах.

Варто зазначити, що VPN-розширення в браузері захищає тільки трафік, який проходить через цей браузер, тоді як окремих VPN-додаток забезпечує шифрування всього інтернет-трафіку на пристрої користувача. При виборі VPN-сервісу доцільно звертати увагу на такі важливі аспекти, як політика No logs (відсутність реєстрації активності користувача), використання надійного алгоритму шифрування (наприклад, AES-256), підтримка сучасних безпечних протоколів (таких як OpenVPN, IKEv2, WireGuard), а також наявність функції Kill Switch, яка забезпечує автоматичне відключення від інтернету у разі втрати VPN-з'єднання.

Для забезпечення безпеки під час OSINT-розслідувань важливо використовувати надійне шифрування для захисту даних, що зберігаються чи передаються. Існує три основні способи зберігання даних: на комп'ютері, у хмарних сервісах та на зовнішніх накопичувачах. Для зберігання на комп'ютері необхідно захистити пристрій як від віддалених загроз (ліцензійне ПЗ, антивіруси, регулярне оновлення системи), так і від фізичних (пароль на вхід, шифрування диска, збереження ключа шифрування). Вбудовані механізми шифрування, такі як BitLocker на Windows, FileVault на macOS та LUKS на Linux, часто потребують активації.

Для збереження даних резервні копії можна зберігати окремо — у хмарі чи на зовнішніх носіях (USB, HDD, SSD). Хмарні сервіси (Google Диск, Dropbox, OneDrive, iCloud) забезпечують певний безкоштовний обсяг сховища, але вимагають надійних паролів та двофакторної автентифікації. Для зовнішніх накопичувачів також рекомендоване шифрування з паролем.

Таким чином, в умовах сучасних ризиків, анонімність є запорукою безпеки аналітиків під час OSINT-розслідувань, дозволяючи працювати незалежно та ефективно. Забезпечення конфіденційності стає комплексним процесом, який включає застосування віртуалізованих середовищ, спеціалізованих браузерів та VPN-засобів, шифрування даних, а також дотримання етичних стандартів та обізнаність у галузі інформаційної безпеки [6]. Надійна організація процесів зберігання й захисту даних, зокрема резервне копіювання та шифрування зовнішніх носіїв, значно знижує ризик компрометації або витоку конфіденційної інформації, захищаючи аналітиків від кіберзагроз та мінімізуючи небезпеку ідентифікації. Реалізація цих заходів сприяє безпечній і ефективній роботі аналітиків, відповідаючи на виклики сучасного інформаційного простору та зміцнюючи захист особистих даних у процесі розслідувань.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. González-Manzano, L. A Primer on Open Source Intelligence (OSINT) Leveraging Existing Tools. Primer Congreso del Espacio y Ciberespacio EMAVI 2020 – Мадрид: Мадридський університет Карлоса III, 2020 – 8с. URL: <https://e-archivo.uc3m.es/bitstreams/c382872a-f774-4880-8be8-02a4d6406c77/download> (дата звернення: 01.11.2024)
2. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень : підручник - Одеса : Видавництво «Юридика», 2024. - 180с. URL: <https://dspace.onua.edu.ua/bitstreams/106c5467-2afb-4055-a0fb-3a500102db9c/download> (дата звернення: 01.11.2024)
3. ESET. URL: Дослідження на основі відкритих джерел або OSINT: де використовується та в чому небезпека – 2021. URL: <http://surl.li/mvddej> (дата звернення: 04.11.2024)
4. OSINT Industries Team. Scrubbing Up On OSINT Cyber Hygiene (Best Practices) – 2024. URL: <https://www.osint.industries/post/scrubbing-up-on-osint-cyber-hygiene-best-practices> (дата звернення: 04.11.2024)
5. Narasimhan, P. K., Bhosale, C., Pervez, M. H., Naqvi, N. Z., Ecevit, M. I., Schwarz, K., & Creutzburg, R. Open-Source Intelligence (OSINT) Investigation in Facebook - IS&T International Symposium on Electronic Imaging 2023, Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Application, 2023. URL: <https://library.imaging.org/admin/apis/public/api/ist/website/downloadArticle/ei/35/3/МОВМУ-357> (дата звернення: 04.11.2024)
6. Гузій І. 21 правило цифрової безпеки: Європейський Простір – 2018. URL: <https://euprostitir.org.ua/practices/133410> (дата звернення: 04.11.2024)