

УДК 004.45

Лізунов С. І.¹, Філобок Є.В.², Верещака М.П.²

¹ канд. техн. наук, доц НУ «Запорізька політехніка»

² асп. НУ «Запорізька політехніка»

МЕТОДИ ТА ІНСТРУМЕНТИ ЦИФРОВОЇ КРИМІНАЛІСТИКИ В РОЗСЛІДУВАННІ СУЧАСНИХ КІБЕРІНЦИДЕНТІВ

У сучасному світі, де інформаційні технології стрімко розвиваються і проникають у всі сфери життя, кількість і складність кіберінцидентів

постійно зростає. Для того щоб ефективно розслідувати такі інциденти, необхідно використовувати спеціальні методи та інструменти цифрової криміналістики, які дозволяють збирати, аналізувати та документувати цифрові докази.

Загальний принцип роботи цифрової криміналістики полягає у систематичному підході до збору та аналізу цифрових доказів з дотриманням юридичних процедур. Фахівці з цифрової криміналістики отримують дані з різних джерел, аналізують їх на відповідність критичним вимогам розслідування і формують доказову базу для подальшого використання в юридичних процесах. Ці методи дозволяють відновити хронологію подій, ідентифікувати зловмисників та визначити механізми атаки.

Розглянемо більш детально різні типи сучасних кіберзагроз та відповідні методи їх розслідування.

Програми-вимагачі (Ransomware)

Програми-вимагачі шифрують дані жертви та вимагають викуп за їх розшифрування. Сучасні варіанти ransomware, такі як Ryuk, Conti та DarkSide, використовують подвійне вимагання – окрім шифрування даних, зловмисники викрадають конфіденційну інформацію та погрожують її оприлюдненням [1].

Методи розслідування атак ransomware включають:

- аналіз зразків шкідливого ПЗ для визначення типу ransomware та можливих вразливостей;

- дослідження журналів подій для встановлення вектору проникнення; аналіз мережевого трафіку для виявлення комунікацій з командними серверами;

- відстеження транзакцій криптовалют та електронних гаманців для ідентифікації зловмисників.

Атаки на веб-додатки

Атаки на веб-додатки, такі як SQL-ін'єкції, Cross-Site Scripting та Cross-Site Request Forgery, залишаються поширеними методами компрометації систем. За даними OWASP, ін'єкційні атаки та неправильна автентифікація є найпоширенішими вразливостями веб-додатків [2].

Методи розслідування атак включають:

- аналіз журналів веб-серверів та додатків;

- дослідження HTTP-запитів та відповідей;

- аналіз коду веб-додатків на наявність вразливостей;

- відтворення атаки у тестовому середовищі.

Інструменти, такі як OWASP ZAP та Burp Suite, дозволяють аналізувати веб-трафік та виявляти вразливості. Спеціалізовані системи моніторингу, зокрема ModSecurity та NAXSI, забезпечують детальне логування спроб атак на веб-додатки.

Методи розслідування мережевих атак

Розслідування мережевих атак вимагає глибокого аналізу трафіку та журналів подій мережевих пристроїв. При виявленні підозрілої активності фахівці з цифрової криміналістики проводять ретельний аналіз PCAP-файлів (Packet Capture), які містять записи трафіку. Цей аналіз дозволяє відновити послідовність дій зловмисника, виявити використані вразливості та визначити скомпрометовані системи [3].

Важливим аспектом розслідування є аналіз DNS-запитів, який може виявити спроби зв'язку з командними серверами або використання технік DNS-тунелювання для прихованої передачі даних. Також досліджуються аномалії в мережевому трафіку, такі як незвичайні обсяги даних, нетипові протоколи або з'єднання з підозрілими IP-адресами та доменами.

Методи аналізу шкідливого програмного забезпечення

Аналіз шкідливого програмного забезпечення є фундаментальним елементом цифрової криміналістики. Цей процес поєднує статичний аналіз (дослідження коду без його виконання) та динамічний аналіз (спостереження за поведінкою шкідливого ПЗ у контрольованому середовищі). Статичний аналіз дозволяє виявити сигнатури, функціональність та потенційні вразливості, тоді як динамічний аналіз демонструє реальну поведінку шкідливого ПЗ, включаючи мережеві комунікації, модифікації файлової системи та реєстру.

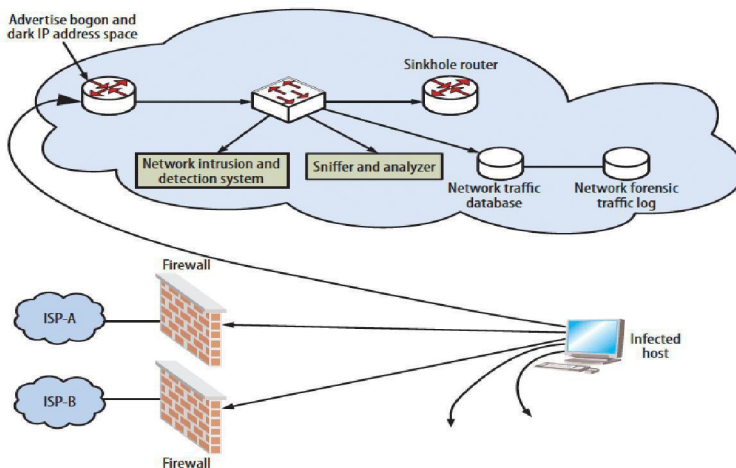


Рисунок 1 – Методологія розслідування мережевих атак

Сучасні методи аналізу шкідливого ПЗ також включають реверс-інжиніринг – процес дослідження бінарного коду для розуміння його

функціональності та механізмів роботи. Це дозволяє виявити приховані функції, механізми ухилення від виявлення та командні сервери, що використовуються для керування зараженими системами.

Аналіз методів мобільної криміналістики

Мобільна криміналістика є одним з найбільш динамічних напрямків цифрової криміналістики, що постійно адаптується до нових технологій та механізмів захисту мобільних пристроїв. Процес розслідування інцидентів, пов'язаних з мобільними пристроями, включає кілька ключових етапів.

Першим кроком є ізоляція пристрою від мережі для запобігання віддаленому стиранню даних або модифікації доказів. Це досягається шляхом активації режиму "польоту" або використання спеціальних екранованих контейнерів, які блокують всі радіосигнали.

Наступним етапом є вилучення даних, яке може здійснюватися різними методами залежно від типу пристрою, рівня захисту та доступних інструментів. Логічне вилучення використовує API операційної системи для доступу до даних, що зберігаються на пристрої. Фізичне вилучення передбачає пряме копіювання вмісту пам'яті пристрою, що дозволяє отримати доступ до видалених даних та обійти деякі механізми захисту.

Основною програмою в цій методиці використовують Cellebrite UFED (Universal Forensic Extraction Device), яка є стандартом в галузі мобільної криміналістики. UFED підтримує вилучення даних з понад 31000 моделей мобільних пристроїв, включаючи смартфони, планшети та GPS-навігатори. Процес роботи з UFED починається з підключення мобільного пристрою до системи через спеціальний кабель або адаптер. Після встановлення з'єднання фахівець обирає тип вилучення (логічне, файлова система або фізичне) та запускає процес [4].

UFED автоматично визначає модель пристрою та пропонує оптимальні методи вилучення даних. Для пристроїв Android система може використовувати ADB (Android Debug Bridge) для логічного вилучення або експлуатувати відомі вразливості для отримання root-доступу та проведення фізичного вилучення. Для пристроїв iOS UFED може створювати резервні копії iTunes, використовувати jailbreak або експлуатувати вразливості bootloader для доступу до зашифрованих даних.

Після вилучення даних UFED проводить їх декодування та аналіз, відновлюючи видалені повідомлення, фотографії, контакти та історію дзвінків. Система також аналізує геолокаційні дані, історію використання додатків та інформацію з соціальних мереж. Результати аналізу представляються у зручному для дослідження форматі з можливістю створення детальних звітів, що включають часові мітки, хеш-суми та інші метадані, необхідні для забезпечення допустимості доказів у суді.

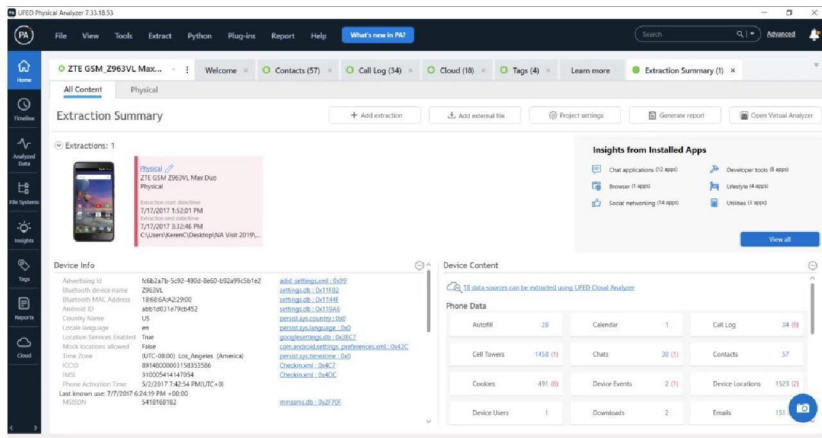


Рисунок 2 – Інтерфейс UFED системи

Важливою функцією UFED є можливість аналізу зв'язків між різними типами даних, що дозволяє відновити хронологію подій та виявити приховані зв'язки. Наприклад, система може пов'язати телефонні дзвінки з повідомленнями, геолокаційними даними та фотографіями, створюючи комплексну картину активності користувача пристрою.

З розвитком технологій та появою нових типів кіберзагроз, методи цифрової криміналістики постійно еволюціонують. Інтеграція штучного інтелекту, розвиток хмарної криміналістики та вдосконалення інструментів аналізу шкідливого програмного забезпечення відкривають нові можливості для ефективного розслідування складних кіберінцидентів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Identity crisis: Why ransomware groups rebrand — and disappear [Електронний ресурс]. — Режим доступу: <https://www.cybersecuritydive.com/news/ransomware-ryuk-conti-revil-2021/608845/>
2. Безпека веб-додатків: найкращі практики та вразливості [Електронний ресурс]. — Режим доступу: <https://itproger.com/ua/news/bezopasnost-veb-prilozheniy-luchshie-praktiki-i-uyazvimosti>
3. Network Forensics: An Analysis of Techniques, Tools, and Trends [Електронний ресурс]. — Режим доступу: <https://www.computer.org/csdl/magazine/co/2012/12/mco2012120036/13rUxBa5qc>

4. How To Use UFED Physical Analyzer 7.33 [Электронный ресурс]. – Режим доступа: <https://www.forensicfocus.com/articles/how-to-use-ufed-physical-analyzer-7-3-3/>