

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА**

**Навчально-науковий інститут
«Інститут інформаційних технологій в економіці»**

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА	«Системний аналіз»
СПЕЦІАЛЬНІСТЬ 124	«Системний аналіз»
СПЕЦІАЛІЗАЦІЯ (пакет)	

Форма навчання: денна

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему **«Використання OSINT інструментів для розвідки на основі відкритих джерел»**

здобувача Кравцова Дмитра В'ячеславовича _____

Науковий керівник: к.т.н., доц. Пархоменко І.І.

**Робота допущена до захисту перед екзаменаційною комісією
з атестації здобувачів вищої освіти (ЕК)**

Завідувач кафедри: д-р. ф.-м. н, проф. Джалладова І.А.

Київ 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

Навчально-науковий інститут
«Інститут інформаційних технологій в економіці»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Системний аналіз»

СПЕЦІАЛЬНІСТЬ 124

«Системний аналіз»

СПЕЦІАЛІЗАЦІЯ (пакет)

ПОГОДЖЕНО

Керівник проектної групи (гарант)
освітньо-професійної програми

ЗАТВЕРДЖУЮ

Завідувач кафедри

Джалладова І.А.

(підпис)

20__р.

(підпис)

20__р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти Кравцову Дмитру В'ячеславовичу
(прізвище, ім'я, по батькові)

денної форми навчання
денної, заочної, дистанційної

на підготовку кваліфікаційної магістерської роботи на тему

«Використання OSINT інструментів для розвідки на основі відкритих джерел»

Тему затверджено наказом ректора Університету від "____" _____ 20__р.

№

Кваліфікаційна магістерська робота виконується на матеріалах
ННЛ «Полігон Кібербезпеки»

План кваліфікаційної магістерської роботи

Розділ 1	Теоретико-методичні основи застосування OSINT інструментів	
Розділ 2	Дослідження результативності використання інструментів OSINT для розвідки на основі відкритих джерел	
Розділ 3	Шляхи удосконалення використання OSINT інструментів	
Об'єкт дослідження:	процес збору та аналізу інформації з відкритих джерел за допомогою OSINT інструментів	
Предмет дослідження:	конкретні OSINT інструменти та методики їх використання для розвідки на основі відкритих джерел.	
Мета кваліфікаційної магістерської роботи:	систематизація теоретико-методичних основ використання OSINT інструментів та розроблення науково-практичних рекомендацій щодо розвідки на основі відкритих джерел.	

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1

Провести теоретичний аналіз історичних фактів та тенденцій розвитку OSINT. Дослідити наявні методи використання OSINT технологій. Проаналізувати міжнародний досвід використання методологій розвідки на основі відкритих джерел. А також виокремити юридичні аспекти використання OSINT

У розділі 2

Проаналізувати основні OSINT інструменти та з'ясувати їхні можливості. Розробити стратегію дослідження в контексті розвідки на основі відкритих джерел. Дослідити використання методів розвідки, як превентивний метод.

У розділі 3

Провести практичний аналіз використання OSINT інструментів на певних прикладах. Дослідити можливість використання OSINT інструментів для ефективного управління інформаційними ризиками.

**Завдання підготував
науковий керівник**

(підпис)

(прізвище, ініціали)

«_____» _____ 20__ р.

**Завдання одержав
здобувач**

(підпис)

(прізвище, ініціали)

«_____» _____ 20__ р.

Реферат

Кваліфікаційна магістерська робота містить 70 сторінок, 1 таблицю, 34 рисунки, перелік джерел посилення з 50 найменувань.

«Використання OSINT інструментів для розвідки на основі відкритих джерел»

Об'єктом дослідження це процес збору та аналізу інформації з відкритих джерел за допомогою OSINT інструментів.

Предметом дослідження це конкретні OSINT інструменти та методики їх використання для розвідки на основі відкритих джерел.

Мета кваліфікаційної магістерської роботи – систематизація теоретико-методичних основ використання OSINT інструментів та розроблення науково-практичних рекомендацій щодо розвідки на основі відкритих джерел.

Відповідно до поставленої мети були визначені такі *завдання*:

- Провести теоретичний аналіз історичних фактів та тенденцій розвитку OSINT.
- Дослідження наявних методів використання OSINT технологій.
- Проаналізувати міжнародний досвід використання методологій розвідки на основі відкритих джерел.
- Виокремити юридичні аспекти використання OSINT
- Аналіз основних OSINT інструменти та з'ясування їхніх можливостей.
- Розробка стратегії дослідження в контексті розвідки на основі відкритих джерел.
- Дослідити використання методів розвідки, як превентивний метод.
- Провести практичний аналіз використання OSINT інструментів на певних прикладах.
- Дослідження можливостей використання OSINT інструментів для ефективного управління інформаційними ризиками.

Практичне значення отриманих результатів. Практичним результатом нашої роботи є реалізація використання інструментів OSINT для розвідки на основі відкритих джерел.

У роботі описується значення методів використання інструментів OSINT як ефективного процесу отримання та збору інформації у різних цільових областях з дотриманням норм законодавства.

Рік виконання кваліфікаційної магістерської роботи 2024. Рік захисту роботи 2024.

Ключові слова: OSINT, розвідка, відкриті джерела, бізнес-розвідка, інструмент, OSINT аналіз, збір даних, інформація, дані

В і д г у к
про кваліфікаційну магістерську роботу здобувача
навчально-наукового інституту
«Інститут інформаційних технологій в економіці»
освітньо-професійної програми « Системний аналіз»
Кравцова Дмитра В'ячеславовича
на тему Використання OSINT інструментів для розвідки
на основі відкритих джерел

1. Актуальність теми: Актуальність дослідження визначається широким застосуванням цифрових технологій в сучасному світі. Відкриті джерела інформації стають все більш важливими у контексті кібербезпеки, оскільки вони дозволяють збирати, аналізувати та використовувати дані для різноманітних цілей, включаючи розвідку та протидію загрозам. Однак, незважаючи на це, багато аспектів використання OSINT інструментів залишаються недостатньо дослідженими. Ця робота пропонує дослідити використання OSINT інструментів для розвідки на основі відкритих джерел, що допоможе покращити розуміння цієї важливої області та розробити ефективні стратегії та методи для її використання.

2. Позитивні риси кваліфікаційної роботи: було присвячено достатньо уваги та зусиль на аналіз існуючих методів OSINT інструментів, враховуючи динамічне кіберсередовище. Це дозволило провести огляд різноманітних підходів та вибрати найбільш ефективні методи для використання.

3. Наявність самостійних розробок автора: В роботі представлено теоретичні аспекти проблематики використання OSINT інструментів, розроблено стратегію дослідження в контексті розвідки на основі відкритих джерел та проведено практичний аналіз використання OSINT інструментів.

4. Цінність теоретичних висновків та практичних рекомендацій: Цінність даної роботи полягає в узагальненні інформації, пов'язаної з використанням OSINT інструментів в сучасному кіберсередовищі. Робота спрямована на оптимізацію та підвищення ефективності використання цих інструментів для збору, аналізу та використання даних з відкритих джерел.

5. Наявність недоліків: для подальшого розвитку роботи необхідно більше уваги приділити практичним аспектам використання OSINT інструментів.

6. : Загальна оцінка кваліфікаційної магістерської роботи та її допущення до захисту перед ЕК:

Критерії оцінювання	<i>Шкала, балів</i>	Оцінка, балів
1. Логіко-структурний рівень	<i>0 – 6 – 8 – 10</i>	8
2. Рівень пошукової глибини	<i>0 – 6 – 8 – 10</i>	9
3. Науково-теоретичний рівень (розділ 1)	<i>0 – 6 – 8 – 10</i>	9
4. Аналітико-методичний рівень (розділ 2)	<i>0 – 6 – 8 – 10</i>	9
5. Конструктивний рівень (розділ 3)	<i>0 – 6 – 8 – 10</i>	8
6. Рівень наукової етики	<i>0 – 6 – 8 – 10</i>	9
7. Організаційний рівень	<i>0 – 6 – 8 – 10</i>	8
Загальна оцінка	<i>0 – 70</i>	60

Науковий керівник _____ **к.т.н., доцент** **Пархоменко І.І.**

(підпис)

(науковий ступінь, учене звання)

(прізвище, ініціали)

доцент кафедри системного аналізу та кібербезпеки

(посада)

“24” травня 2024 р.

Рецензія

на кваліфікаційну магістерську роботу
здобувача вищої освіти

Кравцова Дмитра В'ячеславовича

Тема

Використання OSINT інструментів для розвідки на основі відкритих джерел

Актуальність теми кваліфікаційної роботи і доцільність її розроблення пояснюється широким застосуванням цифрових технологій в сучасному світі. Відкриті джерела інформації (OSINT) стають все більш важливими у контексті кібербезпеки, оскільки вони дозволяють збирати, аналізувати та використовувати дані для різноманітних цілей, включаючи розвідку та протидію загрозам.

Якість проведеного дослідження: результати демонструють високу якість та глибину дослідження. В роботі було враховано широкий спектр наукових джерел, що свідчить про ґрунтовну підготовку та добре обґрунтовану підбірку літературних джерел. Було враховано актуальні методи та технології, пов'язані з OSINT інструментами, та детально проаналізовано їх використання для збору, аналізу та використання даних з відкритих джерел.

Позитивні риси кваліфікаційної роботи: комплексний аналіз OSINT інструментів, надані практичні рекомендації щодо використання OSINT інструментів для розвідки на основі відкритих джерел

Зауваження: В даній роботі автор міг би приділити більше уваги оптимізації використання OSINT інструментів, що допомогло б зробити процес розвідки більш ефективним.

Практична значимість висновків і рекомендацій: аналіз роботи свідчить про глибоке бачення автора проблеми захисту інформації, це дозволяє зробити висновок про те, що кваліфікаційна магістерська робота «Використання OSINT інструментів для розвідки на основі відкритих джерел» відповідає всім вимогам, що висуваються до кваліфікаційних робіт та заслуговує на оцінку добре.

к.т.н., доцент, доцент кафедри
кібербезпеки та захисту інформації
факультету
інформаційних технологій
КНУ ім. Т. Шевченка

Браїловський Микола Миколайович

Підпис засвідчую

(посада, підпис)

Місце печатки організації, де працює рецензент

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1	5
ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ЗАСТОСУВАННЯ OSINT ІНСТРУМЕНТІВ.....	5
1.1 Історія та розвиток OSINT	5
1.2 Дослідження наявних методів OSINT	7
1.3 Аналіз застосування методологій розвідки з відкритих джерел в міжнародному контексті.....	9
1.4 Юридичні аспекти щодо використання методів розвідки з відкритих джерел	11
РОЗДІЛ 2	16
ДОСЛІДЖЕННЯ РЕЗУЛЬТАТИВНОСТІ ВИКОРИСТАННЯ ІНСТРУМЕНТІВ OSINT ДЛЯ РОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ	16
2.1 Основні OSINT інструменти та їх можливості	16
2.2 Розробка стратегії дослідження в контексті розвідки з відкритих джерел ..	32
2.3 Використання методів розвідки з відкритих джерел як профілактичний інструмент	33
РОЗДІЛ 3	36
ШЛЯХИ УДОСКОНАЛЕННЯ ВИКОРИСТАННЯ OSINT ІНСТРУМЕНТІВ.....	36
3.1 Практичне значення використання OSINT інструментів	36
3.1.1 Принцип роботи пошукової системи Shodan	37
3.1.2 Використання методології аналізу рівня помилок	44
3.1.3 OSINT аналіз електронного листа	54
3.1.4 OSINT аналіз за адресою криптогаманця.....	56
3.2 Інтеграція OSINT інструментів для ефективного управління інформаційними ризиками	58
ВИСНОВКИ.....	65
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	66

ВСТУП

Десятиліття тому навіть найпотужніші спецслужби світу не могли робити те, що сьогодні можна зробити за допомогою простого підключення до Інтернету.

Для збору інформації їм доводилося покладатися на екстремальну шпигунську тактику, таку як прослуховування телефонних розмов, перехоплення пошти та соціальна інженерія.

Однак сучасні технології, такі як супутникові знімки з високою роздільною здатністю, доступ до темної павутини і оновлення соціальних мереж, були для цих агентств лише мрією.

Нова форма розвідки з відкритих джерел, відома як OSINT, полегшила роботу слідчих. OSINT передбачає збір, обробку і передачу інформації з відкритих джерел цільовому одержувачу для вирішення конкретних розвідувальних завдань.

Це важлива дисципліна, яка забезпечує осіб, що приймають рішення, повною інформацією, не вдаючись до таємних методів.

Мета і завдання дослідження. Метою цієї роботи є дослідження можливостей використання OSINT інструментів для розвідки на основі відкритих джерел. Для досягнення цієї мети необхідно виконати наступні завдання:

- Провести теоретичний аналіз історичних фактів та тенденцій розвитку OSINT.
- Дослідження наявних методів використання OSINT технологій.
- Проаналізувати міжнародний досвід використання методологій розвідки на основі відкритих джерел.
- Виокремити юридичні аспекти використання OSINT
- Аналіз основних OSINT інструменти та з'ясування їхніх можливостей.
- Розробка стратегії дослідження в контексті розвідки на основі відкритих джерел.

- Дослідити використання методів розвідки, як превентивний метод.
- Провести практичний аналіз використання OSINT інструментів на певних прикладах.
- Дослідження можливостей використання OSINT інструментів для ефективного управління інформаційними ризиками.

Об’єкт дослідження – це процес збору та аналізу інформації з відкритих джерел за допомогою OSINT інструментів.

Предмет дослідження – це конкретні OSINT інструменти та методики їх використання для розвідки на основі відкритих джерел.

Головним теоретичним результатом є вивчення питання застосування методів OSINT для розвідки на основі відкритих джерел.

Практичним результатом нашої роботи є реалізація використання інструментів OSINT для розвідки на основі відкритих джерел.

У роботі описується значення методів використання інструментів OSINT як ефективного процесу отримання та збору інформації у різних цільових областях з дотриманням норм законодавства.

Інструменти, що надаються в наукових дослідженнях, можуть використовуватися для ефективного управління інформаційними ризиками.

Робота складається з трьох розділів, висновків та списку використаних джерел.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ЗАСТОСУВАННЯ OSINT ІНСТРУМЕНТІВ

1.1 Історія та розвиток OSINT

У 21 столітті ми стикаємося з інтенсивним прогресом в області інформаційних технологій. На сьогоднішній день 95% інформації майже завжди можна знайти в інтернеті. Таким чином, роль і значення інформації зростає кожного дня. Перш за все, необхідно визначити дефініцію "OSINT" та історію появи цього терміну. Open Source Intelligence (OSINT) – це набір засобів та методологій для збору та використання даних з публічних джерел, що сприяють прийняттю обґрунтованих рішень в області безпеки.

Розвідка в узагальненому визначенні OSINT також може розумітися не як "розвіддані", а як "аналітичні документи" та "аналітична інформація", отримані в результаті процесів аналізу та синтезу законно отриманої первинної інформації [1].

OSINT (Open Source Intelligence) слід відрізняти від OSIF (Open Source Intelligence InFormation), OSIF - це дані та інформація, що циркулюють у вільно доступних медіа-каналах, а OSINT - це спеціалізована інформація, зібрана та структурована певним чином для відповіді на конкретне питання [2]. Різниця полягає в тому, що проблемним завданням агентів є отримання необхідної інформації з джерел, які часто неохоче діляться своїми даними, тоді як проблемне завдання розвідки з відкритих джерел вимагає надійних джерел загальнодоступної інформації. Важливою частиною OSINT є вміння визначати, які джерела є надійними та які дані можна вважати достовірними. Це включає в себе критичний аналіз джерел інформації, перевірку фактів та кореляцію даних з різних джерел.

OSINT використовується в різних сферах, включаючи правоохоронні органи, розвідку, бізнес-аналітику, журналістику та наукові дослідження. Вона

допомагає до збору та аналізу великих обсягів даних, що можуть бути важливими для розуміння тенденцій, виявлення загроз та вирішення проблем.

Важливим завданням є також дослідження історії виникнення та розвитку OSINT. Хоча достеменно невідомо, коли з'явилася ця технологія і які були її передумови, науковці виділяють кілька стадій. Зокрема

1) Кінець 1941 року - у США було створено Адміністрацію з нагляду за іноземним мовленням, яка займалася розслідуванням радіопрограм. В результаті співробітники цього бюро виявили зв'язок між ціною на апельсини в Парижі та успішним підливом залізничного мосту;

2) У 2005-2009 роках у США було створено центр, що аналізував розвідувальні матеріали з відкритих джерел. Це відбувалося на тлі збільшення обсягів інформації, що публікується в Інтернеті;

3) 2009-2016 рр. - швидкий розвиток Інтернету, а також суттєве зростання його ролі та впливу на життя людини;

4) 2017 - теперішній час - поступове впровадження концепції OSINT не тільки у сфері національної оборони, а й в інших сферах людської діяльності.

Велике значення в розвідувальній практиці має JISR (Joint Intelligence, Surveillance, Reconnaissance). Це синхронізація та включення оперативних і розвідувальних спроможностей і заходів з метою надання своєчасної та необхідної інформації для прийняття певного рішення. “Циклічний процес JISR” - це уніфікована розвідувальна і оперативна функція, яка вимагає обширної координації та достатньої кількості зв'язків між спільнотами на багатьох рівнях. Якщо звернути на JISR НАТО, то їхні дії можна визначити як інтеграцію сил, засобів, політики, процедур і систем розвідки, спостереження і рекогносцировки (СРР) Альянсу і країн-членів з метою надання розвідувальної підтримки особам, командирам і лідерам, що мають приймати рішення, від політико-стратегічного рівня до тактичного. Така схема процесу гарантує, що наявні розвідувальні можливості інтегровані в загальну концепцію операції. Розвідка є лише частиною операції, і командир визначає загальні оперативні пріоритети, а також позиціонування і

діяльність розвідки на підтримку операції: постановка завдань, збір, обробка, використання і поширення розвідувальної інформації, скорочено TCPED.

Додатково, важливо враховувати, що JISR не обмежується лише військовими операціями. Цей підхід може бути також використаний в цивільних сферах, таких як правоохоронні органи, корпоративна безпека та кібербезпека. Використання JISR в цих контекстах може допомогти виявити потенційні загрози, виявити злочини та забезпечити безпеку інформації. Крім того, важливо пам'ятати, що успіх використання JISR залежить від якості збору, аналізу та поширення інформації, а також від ефективності координації між різними стейкхолдерами.

1.2 Дослідження наявних методів OSINT

Дослідження на основі розвідки з відкритих джерел не є новим видом діяльності для великих світових держав, а її використання має бути предметом актуальних досліджень в умовах стрімкого розвитку інформаційних технологій.

Ця концепція охоплює вибір інформації, реєстрацію, облік, аналіз та синтез первинних даних, зберігання та розповсюдження інформації, інформаційну безпеку та публікацію результатів досліджень. Після процесу аналізу та синтезу, первинна інформація з відкритих джерел перетворюється на цінну інформацію і може стати конфіденційною, за умови, що вона не входить до категорії інформації, яка не може бути класифікована як державна таємниця [1].

Інформацію з відкритих джерел та загальнодоступну інформацію можна отримати з таких джерел:

- Форуми, блоги, соціальні мережі, веб-сайти для обміну відео, такі як YouTube.com, Вікіпедія, записи Whois зареєстрованих доменів, метадані, цифрові файли, веб-ресурси даркнету, дані геолокації, IP-адреси, контактні дані, пошукові системи та інші ресурси, доступні в Інтернеті.

- Дипломатичні місії;

- Релігійні організації;
- Національні спецслужби;
- Академічні дисципліни - тези, дисертації, дослідження тощо;
- Архіви (бібліотеки) та дослідницькі центри;
- "Сіра література" - наукові звіти, економічні звіти, маркетингові дослідження тощо. Останні часто трактуються як публікації, які не є широкодоступними і тому їх важко отримати [3].

У деяких випадках розвідувальні дані, отримані з загальнодоступних джерел, не тільки не відрізняються від секретної інформації, але й перевищують її за цінністю. Цінність розвідувальних даних має наступні характеристики [4]

- Швидкість - якщо в географічному регіоні виникає криза, а можливості розвідки в цьому регіоні є низькими, фахівці розвідки та особи, відповідальні за формування політики національної безпеки, швидше за все, шукатимуть інформацію на телебаченні та в інтернеті.

- Кількість - блогерів, журналістів, аналітиків, науковців та інших експертів у певній галузі набагато більше, ніж професіоналів розвідки. Два-три професійні розвідники з налагодженою розвідувальною мережею часто мають значну перевагу над 100 журналістами з точки зору доступу до секретної інформації. Однак професійно зібрана інформація, зібрана експертами з відкритих джерел, як правило, є більш достовірною, ніж звіти розвідки.

- Якість - в розвідувальній роботі нерідко звіти ґрунтуються на газетних статтях або сфабрикованій (недостовірній) інформації. Слід зазначити, що інформація з відкритих джерел менш заплямована брехнею, ніж подібні звіти.

- Ясність - у випадку з відкритою інформацією, надійність відкритих джерел може бути ясною або невизначеною. Ступінь надійності інформації, отриманої конфіденційно, в багатьох випадках є незрозумілою.

- Простота використання - секрети, приховані за грифом "секретно" і захищені спеціальними програмами доступу, часто важко донести до осіб, які приймають рішення, або навіть до інших співробітників розвідки. Розвідувальну інформацію може отримати будь-яка уповноважена особа.

- Вартість - розвідувальні супутники, розробка, запуск і обслуговування яких коштує цілий статок (мільярди доларів США), фотографують дахи заводів з виробництва зброї і корпуси підводних човнів. Зарубіжні журнали, передплата на які коштує близько 100 доларів США, мають можливість публікувати фотографії, зроблені фотографами. Іноземний журнал, передплата на який коштує близько 100 доларів США, може публікувати фотографії, зроблені в заводському цеху або відсіку підводного човна. Аналізуючи потенціал, роль і цінність інформації, науковці часто приходять до певних хибних уявлень. Наприклад, переважає думка, що інформація з відкритих, загальнодоступних джерел не має більшої цінності, ніж інформація з медіа-джерел. Насправді ж, інформація може надходити з різних джерел, а їх поєднання має багато нюансів [4].

1.3 Аналіз застосування методологій розвідки з відкритих джерел в міжнародному контексті

У 1947 році аналітик ЦРУ Кен Шерман зазначив, що держава отримує майже 80% інформації з відкритих джерел, а пізніше (генерал-лейтенант, керівник управління військової розвідки США) Семюель Вілсон стверджував, що 90% розвідувальної інформації є результатом пошуку з відкритих джерел і лише 10% надходить з результатів роботи агентів.[2, с. 62].

США часто використовують інформацію, що була здобута за допомогою інструментів OSINT. Ця інформація допомагає у плануванні військових операцій, організації та проведенні бойових дій, а також для убереження від терористичних актів та запровадження превентивних заходів для їх уникнення[2, 3]. На думку аналітиків американської розвідки, найбільші проблеми з сучасними методами OSINT - це непідтверджені джерела, провокаційні джерела і дезінформація. Щоб отримати найбільш актуальну і якісну інформацію, необхідно обробити великий обсяг інформації з різних джерел і узагальнити її відповідно до цілей і завдань

дослідження. Сполучені Штати мають розгалужену мережу штаб-квартир і офісів, які проводять розвідку OSINT і надають інформацію більш ніж 7000 споживачам розвідувальної інформації. Це результат дій, координованих виключно законодавчими та адміністративними органами уряду, спрямованих на реалізацію цілеспрямованої політики національної безпеки. Аналогічні структури доступні на кожному рівні [4].

Ізраїль також використовує OSINT в першу чергу для аналізу військових можливостей своїх супротивників. У структурі військової розвідки існує незалежний спеціальний підрозділ з аналізу відкритих джерел розвідданих під назвою "Хатсаф", який збирає розвіддані виключно для військових цілей.

У Великій Британії первинний збір розвідувальної інформації за допомогою OSINT здійснюють цивільні журналісти з моніторингової служби BBC, які потім передають її офіцерам розвідки для використання в конкретних напрямках розслідування. З огляду на міжнародний досвід використання OSINT, зрозуміло, що для отримання якісної та актуальної інформації необхідна велика кількість джерел розвідданих. Обробка інформації є необхідною, про що свідчить той факт, що інформацію не завжди вдається отримати вчасно. Для того, щоб цей метод працював належним чином і ефективно, недостатньо просто знайти інформацію, її необхідно обробити, проаналізувати і перевірити, щоб підтвердити факти, події та явища, що досліджуються, оскільки занадто багато інформації генерується з метою дезінформації. Показник ефективності відкритих джерел підтверджує необхідність та актуальність залучення досвіду США та європейських країн для вирішення оперативних, тактичних та стратегічних завдань правоохоронних органів.

1.4 Юридичні аспекти щодо використання методів розвідки з відкритих джерел

Збір та аналіз інформації з відкритих джерел як сфера діяльності має відбуватися в правовому полі держави. Основою для цього є конституційна гарантія права шукати, збирати, передавати та використовувати інформацію в усіх демократичних країнах. Закони різних великих держав світу сприяли використанню інформаційних систем з відкритим вихідним кодом. Наприклад, у 1996 році в США був прийнятий Закон про свободу інформації, який задекларував обов'язок приватних федеральних агентств надавати громадянам вільний та безперешкодний доступ до інформації. Закон накладає обмеження лише на матеріали, пов'язані з національною обороною, фінансові та особисті документи, а також документи правоохоронних органів. Однак зазначимо, що в деяких країнах законодавці фактично заборонили розвідку з відкритих джерел, наклавши обмеження на таку діяльність. В Україні “кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір” (Конституція України, Розділ 2, ст. 34). В Україні правове регулювання в інформаційній сфері базується на певних засадах, а саме:

- 1) свобода законно займатись пошуком, одержанням, передачею, виробництвом та поширенням інформації;
- 2) обмеження на доступ до інформації можуть встановлюватися виключно законодавством держави;
- 3) інформація про діяльність держорганів та органів місцевого самоврядування повинна бути відкритою, а доступ до неї - вільним, за винятком випадків, що передбачені законодавством держави;
- 4) інформація класифікується за категорією доступу на відкриту (доступну для загального користування) та інформацію з обмеженим доступом.

Також, такої дефінації як “OSINT” в законах України не існує, хоча діяльність зі пошуку, збереження, обробки та поширення інформації

урегульовано переліком законодавчих і нормативних актів:

- Закон України “Про інформацію” від 02.10.92 р. № 2657-XII (зі змінами від 13.01.11 р.), ст. 5–7[5];
- ЗУ “Про друковані засоби масової інформації в Україні” від 16.11.92 р. № 2782-XII, ст. 6, 25 [6];
- ЗУ “Про охоронну діяльність” від 22.03.12 р. № 4616-VI, ст. 9, 13, 19 [7];
- ЗУ “Про захист персональних даних” № 2297-VI від 01.06.10 р.[8];
- Цивільний кодекс України (ст. 505), Кримінальний кодекс України (ст. 231, 232), Кодекс України про адміністративні правопорушення (ст. 163, ст. 163).

Слід звернути увагу, що використання методів OSINT в рамках забезпечення безпеки компанії в деяких випадках може розцінюватися як оперативно-розшукова діяльність, здійснювати яку, згідно із ЗУ “Про оперативно-розшукову діяльність” № 2135-XII від 18.02.1992 р. [9] вправі тільки суб’єкти, що вказані в окремих статтях окреслених Законом України. У встановленому указі Президента України “Про стратегію кібербезпеки України” від 15.03.16 р. №96/2016 визначаються ключові завдання для силових структур, а також передбачено “формування системи оперативного виявлення, протидії та нейтралізації кіберзагроз, зокрема, за допомогою волонтерських організацій”[10]. Немає сумнівів, що все це має відношення до використання інструментів конкурентної розвідки в цій області. Згідно з діючим ККУ (Кримінальним Кодексом України), передбачено кримінальну відповідальність за нелегальне збирання або використання інформації, яка є комерційною таємницею, а також за її розголошення. Проте така інформація перевищує межі розвідки на основі відкритих джерел.

Нечітке та широке визначення правових норм робить процеси збору, обробки та зберігання інформації про конкурентів майже непокараними, тобто законними, з одного боку, і складними для доступу громадян, з іншого. В українській практиці доступ до значної частини інформації, яка є вільно

доступною в інших демократичних країнах, наприклад, про земельні ділянки, нерухомість (як власну, так і заставну) та банківські рахунки, є практично закритим. Значну частину цієї інформації можна отримати, лише звернувшись до експертів. Особливо гостро стоїть проблема криміналізації деяких державних установ, які вже використовують у своїй діяльності розвідувальні дані з відкритих джерел. Сьогодні багато підрозділів як державних, так і приватних служб безпеки використовують бази даних, що містять інформацію про фізичних осіб (тобто персональні дані). Ці інформаційні бази даних використовуються в проактивних цілях, наприклад, для перевірки інформації про співробітників, конкурентів і партнерів. Ці бази даних і надалі використовуватимуться компаніями та приватними особами, але їм доведеться піти в підпілля, порушуючи закон. Технічно можливість використання та ведення таких баз даних забезпечується низкою баз даних типу "Кронос".

Технічно можливість використання та ведення таких баз даних забезпечується низкою систем типу "Кронос" (легально продаються оболонки). За допомогою таких інструментів будь-який зацікавлений користувач Інтернету може отримати доступ до низки баз даних, що працюють під цими оболонками [9]. Фундаментальною цінністю людства сьогодні, поряд з правом на життя і свободу вираження поглядів, стає недоторканність приватного життя. Інформація про людей - персональні дані - все частіше стає цінним товаром, за який люди готові платити великі гроші. Такий обсяг інформації в руках недоброзичливців може стати потужною зброєю. Банки, держустанови та великі корпорації часто не забезпечують достатній захист баз даних з персональною інформацією, які вони мають, що призводить до витоку великої кількості конфіденційної інформації на ринок. Тому важливо приділити особливу увагу захисту персональних даних. Враховуючи поточну ситуацію, головними європейськими регулятивами в сфері захисту персональних даних є Конвенція РЄ "Про захист осіб у зв'язку з автоматичною обробкою персональних даних" від 28 січня 1981 року (ETS

№108) та “Пакет захисту даних” Європейського Парламенту та Ради від 27 червня 2016 року [11]. Ці документи обов’язкові для всіх країн-членів Європейського Союзу і служать основою для законодавства в цій сфері, включаючи Україну. Країни ЄС мають гармонізувати своє законодавство з цими правовими стандартами. Конституція України забезпечує право на приватність (Стаття 32 КУ) Додатково, Конституція України передбачає захист інших аспектів приватності (стаття 30 Конституції України про недоторканність житла, стаття 31 КУ про таємницю листування, стаття 32 КУ про заборону дій щодо конфіденційної інформації про особу без її згоди, а також стаття 28 КУ щодо заборони піддавати особу без її згоди певним дослідженням). Конвенція Ради Європи від 28 січня 1981 року про захист осіб у зв’язку з автоматичною обробкою персональних даних (ратифікована Україною 06.07.2010 р.) визначає принципи передачі персональних даних через національні кордони, які підлягають автоматичній обробці або зібрані з цією метою.

Законодавство України вимагає інформування про обробку персональних даних. Перед тим, як почати обробку персональних даних, власник або відповідальна особа (оператор) має обов’язок інформувати уповноважений орган з питань захисту прав суб’єктів персональних даних про свої наміри щодо обробки персональних даних. Крім того, інформація про власника або відповідальну особу (оператора) вноситься до спеціалізованого реєстру операторів. Дані, що зберігаються в реєстрі операторів, є відкритими для загального перегляду.

Закон "Про захист персональних даних" поширюється на більшість громадян, які беруть участь в обробці даних. Закон також є загальним і застосовується до всіх, оскільки кожна людина є суб’єктом персональних даних. Персональні дані часто використовуються в соціальних мережах, особливо в службах електронної пошти.

Сучасні інтернет-компанії збирають і обробляють різні типи персональних даних, включаючи дані працівників, підрядників і користувачів послуг. Люди, які публікують інформацію про себе в соціальних мережах і службах знайомств,

свідомо роблять цю інформацію доступною для всіх користувачів цих ресурсів; юридично це трактується як "загальнодоступна", тобто не вимагає особливої конфіденційності, але соціальні мережі можуть використовуватися для приховування інформації про користувачів від певних осіб. Вони також містять інформацію, яка доступна лише групі користувачів ("друзів"). У цьому випадку інтернет-джерела повинні забезпечувати спеціальні гарантії.

Органи влади, які збирають інформацію з відкритих джерел, обробляють персональні дані, які є загальнодоступними в Інтернеті, тобто доступними для всіх. Така обробка не вимагає згоди суб'єкта даних.

Однак відповідальність за доведення того, що оброблювані персональні дані є загальнодоступними, лежить на контролері або розпоряднику. Це означає, що вони повинні або надати докази того, що дані були отримані з загальнодоступного джерела, або зберігати ці документи за згодою суб'єкта даних. Крім того, документи повинні підтверджувати, що джерело персональних даних є загальнодоступним. Водночас залишається відкритим питання, чи підтверджує джерело інформації (веб-сайт) письмову згоду власника на обробку.

РОЗДІЛ 2

ДОСЛІДЖЕННЯ РЕЗУЛЬТАТИВНОСТІ ВИКОРИСТАННЯ ІНСТРУМЕНТІВ OSINT ДЛЯ РОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ

2.1 Основні OSINT інструменти та їх можливості

OSINT-розвідка зазвичай здійснюється за допомогою трьох основних типів збору інформації: пасивного, напівпасивного та активного. Вибір найбільш ефективного типу значною мірою залежить від сценарію, за яким здійснюється процес збору інформації, і типу даних, що цікавлять суб'єкта збору розвідданих.

Під пасивним збором інформації розуміють найпоширеніший тип збору та обробки даних. Цей вид збору інформації, як правило, здійснюється лише за допомогою використання наявних ресурсів.

У процесі реалізації напівпасивного збору даних, з технічної точки зору, цей тип збору інформації надсилає обмежений трафік на цільовий сервер з метою отримання найзагальнішої інформації про цільовий сервер. Цей трафік має бути схожим на звичайний інтернет-трафік і не повинен привертати увагу громадськості до розвідувальної діяльності відповідних органів.

Активний збір розвідувальної інформації передбачає безпосередню взаємодію з системою, з якої розвідувальні органи збирають інформацію. Оскільки особа або організація, яка зберігає інформацію, використовує сучасні методи, такі як сканування вразливостей (наприклад, неліцензійної Windows), сканування додатків веб-серверів, доступ до відкритих портів тощо, для збору технічних даних про цільову IT-інфраструктуру, проти інформатора проводяться контррозвідувальні операції. Такий трафік підозрюється або інтерпретується як зловмисна поведінка і залишає сліди в системах виявлення вторгнень (IDS) і

системах запобігання вторгненням (IPS). Атаки соціальної інженерії трактуються як форма активного збору розвідувальних даних [5].

Реалізація такої розвідки вимагає використання відповідних інструментів з доступом до відкритих джерел інформації. Одними з найпоширеніших інструментів, що використовуються для збору розвідувальних даних з відкритих джерел та стеків програмного забезпечення, є Recon-ng, URL Scan, SpiderFoot, Maltego та FOCA.

Recon-ng - це фреймворк веб-розвідки з відкритим вихідним кодом, написаний на мові Python, що пропонує високу розширюваність. Ми використовуємо Recon-ng для збору розвідувальної інформації про домени, компанії, приватних осіб тощо, отримуючи доступ до численних API та відкритих джерел даних.

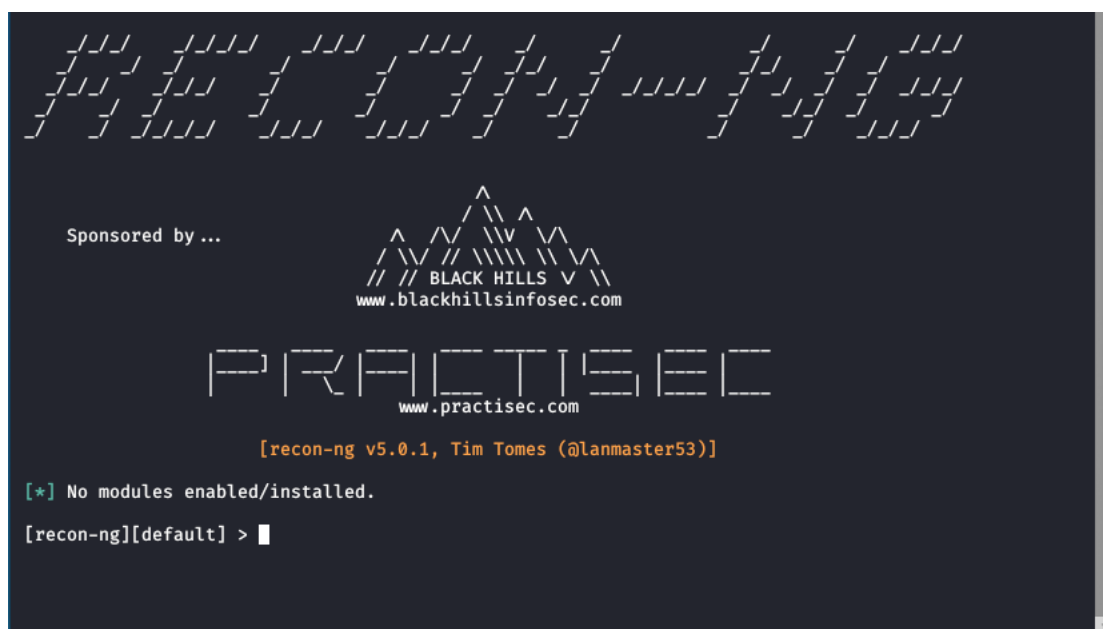


Рисунок 2.1 – Програма Recon-ng [19]

Програма Recon-ng має ряд переваг, а саме:

- Вільний і відкритий вихідний код;
- Простота встановлення та використання;
- Виняткова кастомізація за допомогою модулів;
- Широке охоплення API та джерел даних;

- Цінний для збору розвідданих про загрози.

Не дивлячись на переваги програми Recon-ng, є і перелік важливих недоліків:

- Працює виключно через інтерфейс командного рядка;
- Крута крива навчання на початковому етапі;
- Складні робочі процеси вимагають написання сценаріїв;
- Вразливий до проблем залежності та сумісності.

Recon-ng дає можливість навіть молодшим аналітикам автоматизувати збір даних з різних відкритих джерел та API в Інтернеті. Його інтерактивний інтерпретатор спрощує конфігурацію модулів та виконання команд. Оснащений численними вбудованими функціями, фреймворк виконує такі поширені розвідувальні завдання, як вирішення доменів, виявлення субдоменів і пошук записів WHOIS.

Однак справжня універсальність Recon-ng полягає в підтримці користувацьких модулів, розроблених користувачами. Аналітики можуть створювати модулі, пристосовані до конкретних вимог збору даних, інтегруючи власні канали даних. Це дає змогу використовувати Recon-ng для виконання цільових завдань, таких як збір розвідувальної інформації про суб'єктів загроз, скомпрометовані облікові дані, вразливі системи тощо. Він виводить результати в базу даних, що дозволяє зручно фільтрувати, аналізувати та співставляти їх.

Завдяки своїй адаптивній, розширюваній та автоматизованій природі Recon-ng слугує фундаментальним інструментом у нашій повсякденній діяльності з розвідки безпеки. Він допомагає виявляти приховані загрози та сприяє покращенню процесів прийняття рішень в рамках наших операцій.

Тепер звернемо увагу на ще один OSINT інструмент, а саме Maltego. Maltego - це запатентований інструмент для проведення розслідувань, що спеціалізується на графічному аналізі зв'язків, спрямований на збір і взаємозв'язок загальнодоступної інформації, розпорошеної по всьому Інтернету. У своїй роботі

ми використовуємо можливості візуалізації Maltego для проведення імпровізованих досліджень і поглиблених розслідувань загроз.

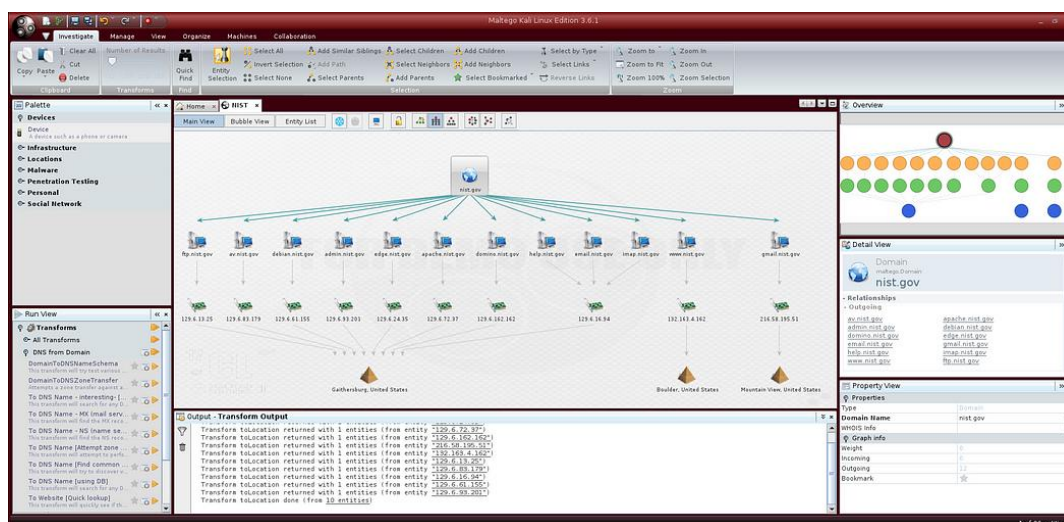


Рисунок 2.2 – Програма Maltego [20]

Аналізуючи роботу даного OSINT інструменту ми виокремили наступні переваги:

- Надійний візуальний аналіз зв'язків;
- Інтеграція з цінними онлайн-джерелами даних;
- Корисні функції управління справами;
- Доступність у настільній та хмарній версіях.

Варто зазначити, що даний інструмент має і свої недоліки, до яких можна віднести:

- Дороге ліцензування;
- Обмеження використання в хмарній пропозиції;
- Потенційні обмеження масштабованості;
- Крута крива навчання.

Maltego працює, поглинаючи початкові точки даних, такі як фрази, імена, веб-сайти, домени тощо, перетворюючи їх на графічну мережеву карту, яка ілюструє зв'язки та асоціації між відповідними об'єктами. Таке графічне представлення спрощує розуміння складних взаємозв'язків реального світу, забезпечуючи більш інтуїтивний підхід у порівнянні з переглядом таблиць даних. Завдяки візуальному інтерфейсу аналітики швидко збирають розвідувальну

інформацію про загрози. Наприклад, починаючи з підозрілої IP-адреси, аналітик може переглянути власників, пов'язані хости, технології, що використовуються, географічні кореляції та пов'язані з ними порушення, виявляючи приховані загрози. Інструменти управління справами полегшують спільне розслідування інцидентів. Maltego легко інтегрується з іншими інструментами безпеки, забезпечуючи безперебійний робочий процес. Десктопний клієнт підходить для невеликих локальних команд, а хмарна версія - для глобально розподілених команд.

Хоча цінова структура може створювати проблеми з масштабуванням для невеликих команд, відмінний графічний аналіз зв'язків і зручний інтерфейс Maltego роблять його безцінним доповненням до набору інструментів OSINT для SOC. Він допомагає в проактивному пошуку загроз і прискорює розслідування інцидентів.

Наступний OSINT інструмент, що підлягає аналізу – це URL Scan. URL Scan виявився безцінним безкоштовним онлайн-сервісом, який відіграє ключову роль у нашому SOC, ретельно перевіряючи та скануючи веб-сайти на наявність потенційних загроз. Цей сервіс безпечно відображає надіслані сторінки та витягує відповідну інформацію про безпеку.

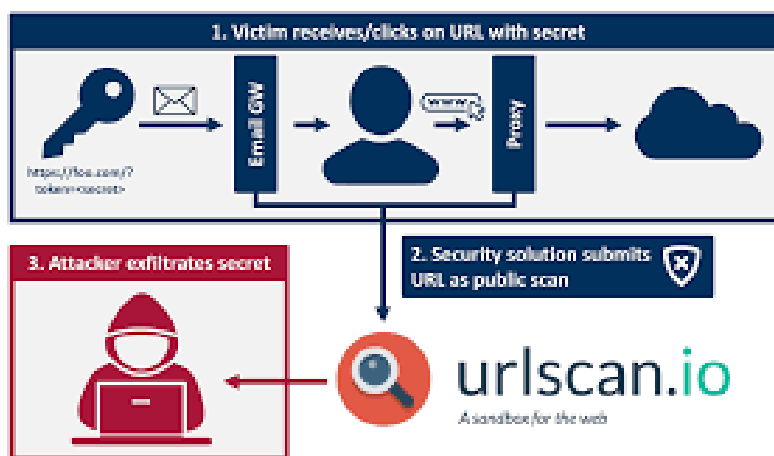


Рисунок 2.3 – Програма URL Scan [21]

Серед ключових переваг використання даного інструменту є:

- Безкоштовний онлайн-сервіс;
- Швидкий аналіз вмісту сторінок;
- Можливість інтеграції з різними інструментами;
- Простий і зручний інтерфейс;

- Надання цінних даних з експертизи веб-сайтів.

Але й присутні певні мінуси, а саме:

- Обмежені можливості для налаштування;
- Може не помічати динамічно завантажений вміст;
- Обмежена історія сканування;
- Потребує ручного аналізу.

URL Scan приймає URL-адресу веб-сайту і відображає сторінку в безпечному середовищі, що дозволяє нашим аналітикам спостерігати за завантаженням контенту, не наражаючи наші активи безпосередньо на потенційні загрози. Цей сервіс витягує цінні метадані, включаючи встановлені файли cookie, завантажені ресурси, перенаправлення, виконані скрипти тощо. Така інформація дає уявлення про дії, які намагаються виконати веб-сайти під час відвідування. URL Scan також виявляє певні відомі загрози і вразливості, аналізуючи відбитки сервісів і загальні шаблони. URL Scan значно допомагає у швидкій початковій розвідці підозрілих веб-сайтів, доменів і сторінок, які зустрічаються під час полювання на загрози. Аналітики можуть легко обмінюватися звітами, збагаченими додатковим контекстом і криміналістичними знімками, що полегшує співпрацю з іншими командами. Незважаючи на обмеження в автоматизації, налаштуванні та збереженні даних у порівнянні з іншими пропозиціями, доступність, простота використання та надання цінної інформації про безпеку веб-сайтів роблять URL Scan незамінним доповненням до наших можливостей веб-орієнтованої розвідки з відкритим кодом.

Наступний інструмент, що ми обрали для аналізу – це SpiderFoot. SpiderFoot - це інструмент автоматизації розвідки з відкритим вихідним кодом, що об'єднує понад 200 модулів, призначених для зіставлення розвідувальної інформації з різних відкритих джерел даних. В рамках наших операцій ми використовуємо SpiderFoot для розвідки доменів, мережевих блоків, електронних листів, імен та іншого.

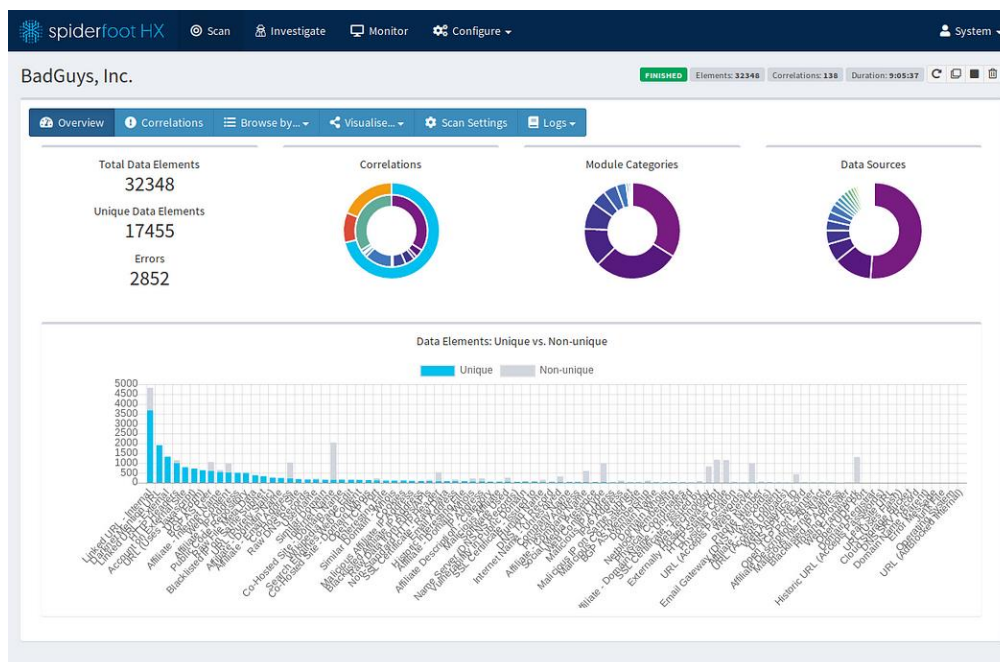


Рисунок 2.4 – Програма SpiderFoot [22]

Ключовими перевагами даного інструменту є:

- Вільний і відкритий вихідний код;
- Високоавтоматизований процес збору даних;
- Цінний для полювання на загрози;
- Інтеграція з різноманітними та корисними джерелами даних;
- Наявність хмарного хостингу.

Із суттєвих недоліків можна виокремити наступні:

- Застарілий користувацький інтерфейс;
- Крута крива навчання;
- Складні потоки даних;
- Обмежена масштабованість.

SpiderFoot працює, використовуючи початкові дані, такі як IP-адреси, домени, електронні адреси тощо, і автоматично запитує безліч відкритих джерел даних, таких як пошукові системи, Pastebin, записи WHOIS, супутникові карти тощо, щоб нанести на карту пов'язані з ними об'єкти. Цей процес виявляє пов'язану інфраструктуру, технології, документи, витоки тощо з мінімальним ручним втручанням.

Аналітики можуть вибирати з попередньо створених модулів і каналів, що охоплюють загрози, мережі та місцезнаходження, серед іншого. Результати зберігаються локально в базі даних для спрощеної фільтрації та аналізу. Веб-інтерфейс користувача дозволяє керувати скануванням і переглядати результати. Для великих команд SpiderFoot пропонує хмарний варіант із загальним доступом. Незважаючи на застарілий користувацький інтерфейс і складні робочі процеси, особливо складні для новачків, широкий спектр джерел даних, можливості автоматизації і тактичні інтеграції роблять SpiderFoot універсальним доповненням до арсеналу сучасних SOC для збору зовнішніх розвідувальних даних. Він виявляється корисним як для ініціатив з полювання на загрози, так і для прискорення процедур реагування на інциденти.

Наступний інструмент, який ми розглянули – FOCA. FOCA (Fingerprinting Organizations) - це OSINT-інструмент з відкритим вихідним кодом, призначений для виявлення цифрового сліду організації шляхом вилучення метаданих і прихованої інформації з публічних документів і файлів. В рамках наших операцій ми використовуємо FOCA для збору розвідувальної інформації з таких форматів документів, як PDF і DOCX, під час слідчих процедур.

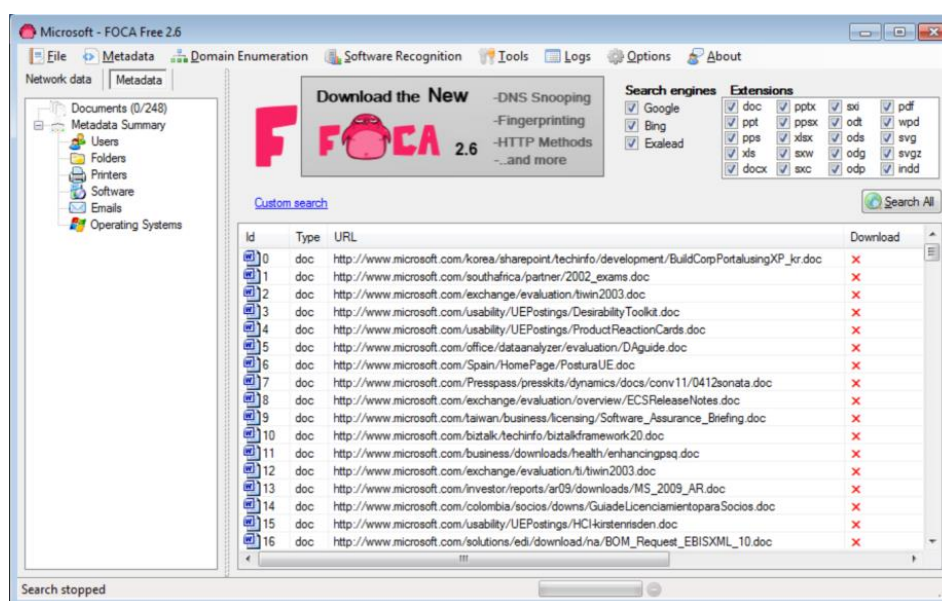


Рисунок 2.5 – Програма FOCA [23]

Із переваг можна виокремити наступні:

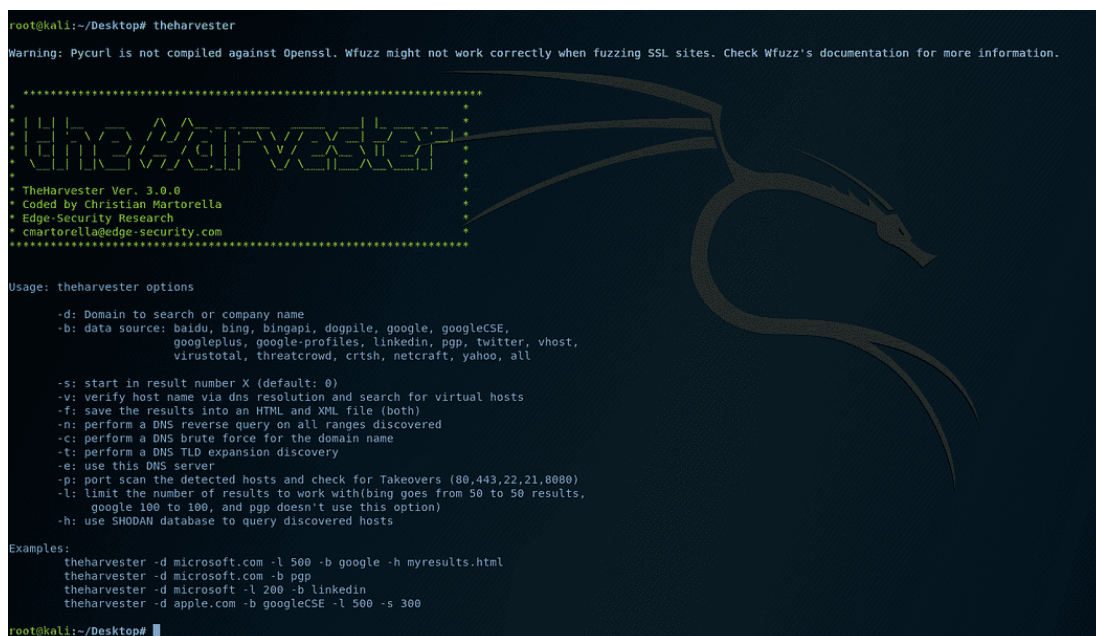
- Автоматизоване вилучення даних з документів;
- Робота з різними типами файлів;
- Корисно для слідчих цілей;
- Безкоштовний інструмент з відкритим вихідним кодом.

В програмі FOCA присутні суттєві недоліки, а саме:

- Офіційно сумісний лише з Windows;
- Застарілий інтерфейс командного рядка;
- Обмежені можливості інтеграції;
- Інформація представлена в розрізненому вигляді.

FOCA дозволяє завантажувати потенційно конфіденційні документи, такі як фінансові звіти, презентації та електронні таблиці, отримані під час розвідки організації. Він систематично витягує метадані, інформацію про авторство, хеші, URL-адреси, електронні листи та інші вбудовані дані у файлах. Ця можливість дозволяє аналітикам ефективно витягувати розвідувальну інформацію з документів без трудомісткого ручного перегляду, виявляючи ідентифікаційні дані, пов'язані з ними суб'єкти, шаблони використання тощо. FOCA має можливість рекурсивно сканувати документи і веб-сайти, будуючи "організаційну піраміду", яка візуалізує структурні взаємозв'язки. Зібрана інформація відображається на різних вкладках веб-інтерфейсу, зводячи до мінімуму необхідність ручного аналізу для з'єднання точок. Незважаючи на недоліки інтерфейсу командного рядка (CLI) та інтерфейсу користувача (UI), автоматизоване вилучення даних з документів за допомогою FOCA надає неоціненну підтримку інструментарію OSINT SOC. Це корисно для розслідувань внутрішніх загроз і доповнює збір даних про інциденти.

Ще одним із відомих OSINT інструментів можна назвати theHarvester. theHarvester - це практичний інструмент розвідки з відкритим вихідним кодом, призначений для збору електронних адрес, імен, субдоменів, IP-адрес, URL-адрес та іншого з численних відкритих джерел. В рамках нашої діяльності ми використовуємо theHarvester для автоматизації попередньої зовнішньої розвідки.



```

root@kali:~/Desktop# theharvester
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

*****
  theHarvester
*****
* TheHarvester Ver. 3.0.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

Usage: theharvester options

-d: Domain to search or company name
-b: data source: baidu, Bing, BingAPI, dogpile, google, googleCSE,
    googleplus, google-profiles, linkedin, pgp, twitter, vhost,
    virustotal, threatcrowd, crtsh, netcraft, yahoo, all
-s: start in result number X (default: 0)
-v: verify host name via dns resolution and search for virtual hosts
-f: save the results into an HTML and XML file (both)
-n: perform a DNS reverse query on all ranges discovered
-c: perform a DNS brute force for the domain name
-t: perform a DNS TLD expansion discovery
-e: use this DNS server
-p: port scan the detected hosts and check for Takeovers (80,443,22,21,8080)
-l: limit the number of results to work with(bing goes from 50 to 50 results,
    google 100 to 100, and pgp doesn't use this option)
-h: use SHODAN database to query discovered hosts

Examples:
theharvester -d microsoft.com -l 500 -b google -h myresults.html
theharvester -d microsoft.com -b pgp
theharvester -d microsoft -l 200 -b linkedin
theharvester -d apple.com -b googleCSE -l 500 -s 300

```

Рисунок 2.6 – Програма theHarvester [24]

Аналізуючи роботу даного OSINT інструменту ми виокремили наступні переваги:

- Простий і зручний інтерфейс;
- Послідовні та надійні результати;
- Сумісність з платформами Linux та Windows;
- Широке охоплення відкритих джерел.

Не дивлячись на переваги програми theHarvester, є і перелік важливих недоліків:

- Спочатку переважно консольний інтерфейс;
- Потребує додаткового аналізу результатів;
- Складна конфігурація джерел даних;
- Обмежені можливості кастомізації.

theHarvester прискорює початкову розвідку, дозволяючи аналітикам вказувати домени, компанії або ключові слова для автоматичного сканування в пошукових системах, записах DNS, базах даних WHOIS, сховищах PGP, на дошках оголошень про роботу та інших джерелах. Це полегшує пошук пов'язаних адрес електронної пошти, хостів, імен співробітників і попередньої розвідки.

Цей процес дає змогу отримати швидкий і широкий огляд присутності організації в Інтернеті, перш ніж заглиблюватися в більш спеціалізовані інструменти. Уся зібрана інформація збирається в локальний HTML-звіт, що дає змогу для подальшого уточнення та дослідження. Незважаючи на те, що Harvester вимагає початкових навичок роботи з інтерфейсом командного рядка і не має вбудованих функцій візуалізації, простота використання, надійність і широкий доступ до відкритих джерел роблять його важливим початковим елементом багатьох робочих процесів зі збору OSINT-інформації в SOC. Такий підхід дозволяє цілеспрямовано застосовувати більш цінні спеціальні інструменти до розвідувальних зачіпок, підтверджених за допомогою автоматизованого початкового сканування Harvester.

Наступний інструмент, що ми проаналізували – це Google Dorks. Google Dorks дає змогу ретельно видобувати приховану інформацію, використовуючи широкі можливості пошуку Google. Ці спеціалізовані пошукові запити, створені за допомогою просунутих операторів, розкривають приховану організаційну інформацію.

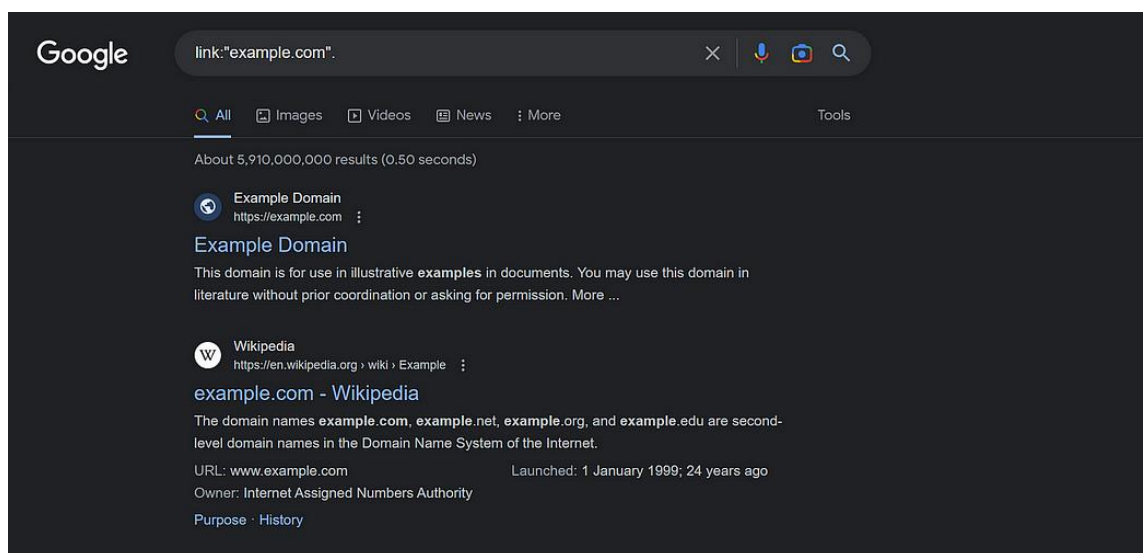


Рисунок 2.7 – Програма Google Dorks [25]

Аналізуючи роботу даного OSINT інструменту ми виокремили наступні переваги:

- Використовує безкоштовну загальнодоступну пошукову платформу;

- Відкриває безцінну інформацію;
- Цінний для початкової розвідки;
- Широке охоплення джерел даних.

Але й присутні певні мінуси, а саме:

- Обмеження у використанні, накладені Google;
- Ризик хибнопозитивних результатів;
- Крута крива навчання для користувачів;
- Для точності потрібна ручна перевірка.

Google Dorks творчо використовує величезні індексовані дані Google за допомогою розумного пошукового синтаксису та спеціальних налаштувань. Ця методика дозволяє аналітикам всебічно сканувати поверхню Інтернету, виявляючи вразливі документи, облікові дані, конфіденційні процеси та багато іншого завдяки вмілому використанню Dorks. Наприклад, спеціальні пошукові запити можуть виявити вразливі системи через ненавмисне оприлюднення порталів для входу в систему, файлів резервних копій, інструкцій до серверів тощо. Дорк-пошуки в Google також можуть виявити внутрішні загрози через відкриті облікові дані співробітників і дані в кешах, сховищах коду та ненавмисні завантаження. Незважаючи на те, що кожен окремий випадок здається нешкідливим, сплетіння інформації, отриманої в результаті стратегічного пошуку Google Dorking по людям, доменам, локаціям і технологіям, розкриває приховані взаємозв'язки і підвищує рівень розвідки загроз. Це, однак, вимагає вмілого складання пошукових запитів з урахуванням обмежень у використанні. Завдяки безпрецедентному доступу до глобально індексованих даних, стратегічне використання Google Dorks слугує основою для багатьох досліджень SOC OSINT, допомагаючи проактивно виявляти приховані загрози і прискорюючи розслідування інцидентів за допомогою дослідження вразливостей.

Останній інструмент, що ми проаналізували – це OSINT Framework.

OSINT-розслідування можуть бути трудомісткими і складними, особливо для новачків, які не знайомі з різними інструментами і ресурсами, доступними для OSINT-розслідувань. Саме тут на допомогу приходить OSINT Framework -

комплексний ресурс, який надає колекцію інструментів і ресурсів для OSINT-розслідувань в одному місці.

OSINT Framework - це веб-сайт, який надає централізований список інструментів і ресурсів для проведення OSINT-розслідувань. Веб-сайт створений, щоб допомогти слідчим, дослідникам і фахівцям з кібербезпеки швидко знайти потрібні інструменти та ресурси для своїх розслідувань.

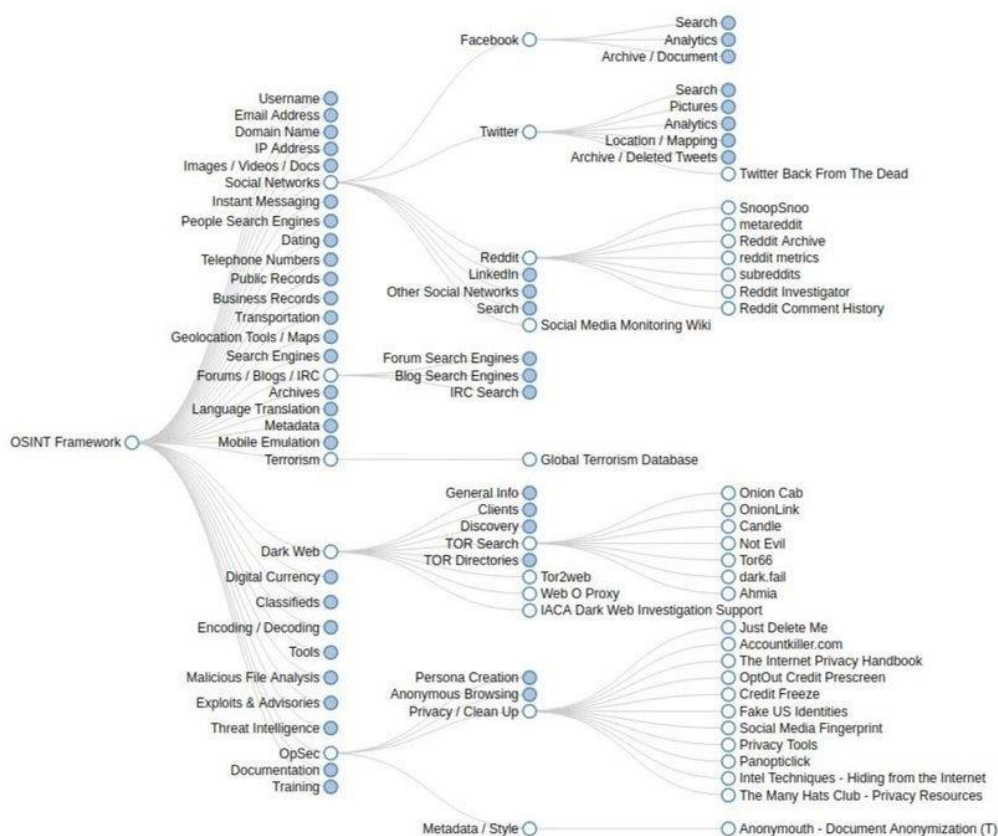


Рисунок 2.8 – Веб-сайт OSINT Framework [26]

Сайт OSINT Framework розділений на кілька категорій, зокрема:

- Пошукові системи;
- Соціальні мережі;
- Пошук людей;
- Пошук за телефонними номерами;
- Пошук за доменом;
- Пошук електронної пошти;

- Пошук компанії;
- Різне.

Кожна категорія містить перелік OSINT-інструментів та ресурсів, які можуть бути використані для відповідного розслідування. Використовувати OSINT Framework просто і зрозуміло. Для початку відвідайте веб-сайт за адресою osintframework.com.

На головній сторінці ви побачите список категорій, які відповідають різним типам OSINT-розслідувань. Натисніть на будь-яку категорію, щоб побачити список інструментів і ресурсів, доступних для цієї категорії. Наприклад, якщо ви натиснете на категорію "Соціальні мережі", ви побачите список платформ соціальних мереж та інструментів, які можна використовувати для розслідування в соціальних мережах. Після того, як ви визначили інструменти та ресурси, які хочете використовувати для свого розслідування, натисніть на посилання, щоб перейти на відповідний інструмент або ресурс. Більшість інструментів і ресурсів, перелічених на OSINT Framework, є безкоштовними для використання, але деякі з них можуть вимагати підписки або оплати.

OSINT Framework є цінним ресурсом для всіх, хто проводить OSINT-розслідування. Ось деякі з переваг використання OSINT Framework:

Комплексність: OSINT Framework надає вичерпний перелік інструментів і ресурсів для OSINT, які регулярно оновлюються, що робить його універсальним інструментом для проведення OSINT-розслідувань.

Зручний для користувача: Веб-сайт має просту навігацію, що дозволяє легко знайти потрібні інструменти та ресурси для вашого розслідування.

Економічно ефективний: Більшість інструментів і ресурсів, перелічених на OSINT Framework, є безкоштовними для використання, що може бути корисним для розслідувачів з обмеженим бюджетом.

Спільнота: OSINT Framework також надає посилання на онлайн-спільноту OSINT-практиків, де ви можете зв'язатися з іншими дослідниками, обмінятися знаннями та досвідом, а також отримати підтримку у проведенні розслідувань.

Із мінусів можна назвати:

- Потенційне перевантаження інформацією;
- Різна якість окремих інструментів;
- Потребує ручної перевірки;
- Залежність від зовнішніх посилань.

З урахуванням всіх проведених досліджень необхідним стає узагальнення результатів щодо переваг та недоліків OSINT інструментів. (табл. 2.1)

Таблиця 2.1 – Узагальнена характеристика OSINT інструментів

Назва OSINT інструменту	Переваги інструменту	Недоліки інструменту
Recon-ng	• Вільний і відкритий вихідний код; • Простота встановлення та використання; • Виняткова кастомізація за допомогою модулів; • Широке охоплення API та джерел даних; • Цінний для збору розвідданих про загрози.	• Працює виключно через інтерфейс командного рядка; • Крута крива навчання на початковому етапі; • Складні робочі процеси вимагають написання сценаріїв; • Вразливий до проблем залежності та сумісності.
Maltego	• Надійний візуальний аналіз зв'язків; • Інтеграція з цінними онлайн-джерелами даних; • Корисні функції управління справами; • Доступність у настільній та хмарній версіях.	• Дороге ліцензування; • Обмеження використання в хмарній пропозиції; • Потенційні обмеження масштабованості; • Крута крива навчання.
URL Scan	• Безкоштовний онлайн-сервіс; • Швидкий аналіз вмісту сторінок; • Можливість інтеграції з різними інструментами; • Простий і зручний інтерфейс; • Надання цінних даних з експертизи веб-сайтів.	• Обмежені можливості для налаштування; • Може не помічати динамічно завантажений вміст; • Обмежена історія сканування; • Потребує ручного аналізу.

Продовження таблиці 2.1

1	2	3
SpiderFoot	• Вільний і відкритий вихідний код; • Високоавтоматизований процес збору даних; • Цінний для полювання на загрози;	• Застарілий користувацький інтерфейс; • Крута крива навчання; • Складні потоки даних; • Обмежена масштабованість.

	• Інтеграція з різноманітними та корисними джерелами даних; • Наявність хмарного хостингу.	
FOCA	• Автоматизоване вилучення даних з документів; • Робота з різними типами файлів; • Корисно для слідчих цілей; • Безкоштовний інструмент з відкритим вихідним кодом.	• Офіційно сумісний лише з Windows; • Застарілий інтерфейс командного рядка; • Обмежені можливості інтеграції; • Інформація представлена в розрізненому вигляді.
theHarvester	• Простий і зручний інтерфейс; • Послідовні та надійні результати; • Сумісність з платформами Linux та Windows; • Широке охоплення відкритих джерел.	• Спочатку переважно консольний інтерфейс; • Потребує додаткового аналізу результатів; • Складна конфігурація джерел даних; • Обмежені можливості кастомізації.
Google Dorks	• Використовує безкоштовну загальнодоступну пошукову платформу; • Відкриває безцінну інформацію; • Цінний для початкової розвідки; • Широке охоплення джерел даних	• Обмеження у використанні, накладені Google; • Ризик хибнопозитивних результатів; • Крута крива навчання для користувачів; • Для точності потрібна ручна перевірка.
OSINT Framework	• Комплексність; • Зручний для користувача; • Економічно ефективний; • Спільнота.	• Потенційне перевантаження інформацією; • Різна якість окремих інструментів; • Потребує ручної перевірки; • Залежність від зовнішніх посилань. •

Джерело: розроблено автором на базі [19-26]

2.2 Розробка стратегії дослідження в контексті розвідки з відкритих джерел

Розробка плану досліджень OSINT є критично важливою, оскільки необхідно мати чітке розуміння плану дій для знаходження всієї корисної інформації. План розвідки в соціальних медіа OSINT може включати такі етапи:

- Встановлення цілі. Перш за все, потрібно чітко визначити мету дослідження. Це може бути збір інформації про певну особу, компанію, організацію або виявлення конкретної активності або зв'язку.
- Вибір соціальних мереж. Вирішіть, яку соціальну мережу варто дослідити як частину вашого дослідження. Facebook, Instagram, Twitter, LinkedIn, YouTube та інші, в залежності від контексту, можливо, варто розглянути можливість використання власної платформи, такої як GitHub, для перевірки взаємодії з розробниками.
- Збір відкритої інформації. Почніть зі збору відкритої інформації на вибраній соціальній мережі. Огляньте особистий або корпоративний профіль і перегляньте публічні публікації, фотографії та взаємодію з іншими користувачами. Зверніть увагу на деталі профілю, включаючи місце роботи, освіту, інтереси та контакти.
- Дослідження діяльності об'єкта. Вивчіть активність об'єктів розвідки в соціальних мережах. Уважно вивчіть дописи, коментарі, лайки та реакцію на дописи інших користувачів. Це допоможе виявити, думки, інтереси або потенційно небезпечну поведінку.
- Дослідження зв'язків. Розвідка аналізує зв'язок між об'єктом та іншими особами. Перегляньте список друзів, підписників, підписників та спільних груп. Це може дати уявлення про соціальні мережі людини, її вплив та зв'язки з іншими.
- Використання OSINT інструментів. Використовуйте спеціальні інструменти виявлення OSINT, такі як SpiderFoot, Maltego, FOCA, щоб знайти

додаткову інформацію про те, що ви хочете виявити, або виконати розширений пошук за допомогою спеціальних ключових слів та пошукових запитів.

- Підведення підсумків. Після отримання потрібних даних, треба їх проаналізувати та спробувати виявити закономірності, шаблони, виявити ризики та можливості. Запишіть результати та створіть звіт.

Дотримання законів також важливо. Слід пам'ятати, що при проведенні розвідки з використанням OSINT технологій необхідно дотримуватися закону і правил конфіденційності. Не використовуйте отриману інформацію для незаконних або шкідливих дій. Наслідки можуть бути дуже серйозними, тому це слід враховувати при складанні алгоритму розвідки і під час його реалізації.

Це загальна схема, використання OSINT у розвідці. Оскільки кожен випадок може мати свої особливості та вимоги, схема може змінюватися залежно від контексту та вимог розвідки

2.3 Використання методів розвідки з відкритих джерел як профілактичний інструмент

Експертам з безпеки методи OSINT можуть допомогти швидко знайти загальнодоступну інформацію про внутрішню діяльність або зовнішні дані фізичної чи юридичної особи, а також компанії або юридичної особи. Це може включати дані про співробітників, корпоративну структуру, фінансову інформацію та інше. Часто конфіденційна інформація міститься в метаданих, випадково опублікованих фізичними або юридичними особами [27]. До таких даних відносяться:

- Незахищені з'єднання та порти пристроїв
- Неоновлене програмне забезпечення;
- Назва пристрою, версія програмного забезпечення, мережа та IP-адреса;
- витік даних, таких як власний код на GitHub.

Ці дані можуть бути використані для виявлення потенційних вразливостей та загроз безпеки. Багато точок входу в корпоративну мережу визначають багато векторів атаки, доступних для зловмисника. Точки входу можна формально класифікувати наступним чином:

- інформаційні системи, розташовані по периметру і мають доступ до Інтернету (наприклад, сервери, робочі станції, панелі управління спеціалізованим обладнанням)

- Мобільні пристрої, що використовуються співробітниками як всередині периметра, так і за його межами

- Облікові записи хмарних сервісів (у тому числі ті, що використовуються в особистих цілях).

Кінцева точка зазвичай вимагає від зловмисника взаємодії з жертвою (наприклад, спілкування з метою фішингової атаки), що підвищує ризик виявлення. Тому в деяких випадках пріоритетними є точки входу в периметр, які можуть бути використані [28].

Периметр мережі - це концепція, яка поступово зникає з розвитком технологій і поширенням хмарних технологій. Принесіть свій власний пристрій

Концепція BYOD, яка дозволяє співробітникам компанії використовувати свої особисті пристрої для бізнес-процесів, розмиває кордони, так само як і поява хмарних середовищ. Контролювати потік даних між корпоративною мережею та зовнішнім світом стало дуже складно. Це полегшує зловмисникам життя з більш різноманітними варіантами атак.

Слід також зазначити, що соціальні мережі та веб-сайти виступають джерелом інформації, особливо щодо співробітників компанії. Постачальники та партнери компанії часто надають відкритий доступ до певних деталей ІТ-середовища компанії, які краще тримати в таємниці. Крім того, існує низка неіндексованих файлів і веб-сайтів, відомих як "невидимі мережі" [29].

"Невидима мережа", або "Deer Web", включає в себе веб-сторінки, які не індексуються стандартними пошуковими системами. Це може включати бази даних, приватні соціальні мережі, інтранети та інші ресурси. Невидима або

прихована мережа, технічно все ще є загальнодоступною, але вимагає спеціальних знань та інструментів для доступу.

Тому методи OSINT можна використовувати для впровадження превентивних заходів у відповідь на кіберінциденти. Наприклад, проактивна розвідка про компанію, отримана з відкритих джерел, може запобігти витoku інформації або зірвати повномасштабну кібератаку на організацію. Іншими словами, подивившись на свою компанію очима хакера, ви можете дізнатися, яка інформація знаходиться у відкритому доступі. Крім того, використання OSINT-методів є процедурою забезпечення фінансової безпеки компанії, а тому витрати на неї мінімальні. Однак результати розвідки з відкритих джерел про організацію та її співробітників можуть допомогти захистити бюджет компанії та інформацію про зустрічі, що в іншому випадку може призвести до значних фінансових втрат.

Методи та інструменти OSINT дозволяють отримувати та аналізувати інформацію, а використання OSINT як превентивного заходу може запобігти повномасштабній атаці на організацію чи компанію.

РОЗДІЛ 3

ШЛЯХИ УДОСКОНАЛЕННЯ ВИКОРИСТАННЯ OSINT ІНСТРУМЕНТІВ

3.1 Практичне значення використання OSINT інструментів

Немає сумнівів, OSINT - це технологія, яка визначає сучасність і майбутнє. Особа, яка володіє знаннями її інструментів та принципів роботи, завжди матиме перевагу в питаннях, що стосуються конкуренції, індивідуальної, корпоративної та національної безпеки. Це надає можливість адаптуватися до швидко змінюваних умов інформаційного середовища, розуміти тенденції та передбачати можливі загрози [30].

В Україні спроби використання OSINT у військових операціях робляться з 2014 року, але його застосування в державному управлінні та політиці національних інтересів все ще перебуває на стадії наукових досліджень [31].

Використання OSINT - це складний процес, який вимагає уважності до деталей. Першим кроком є визначення події, її тривалості та дій, що відбулися під час неї. Розуміння цих ключових факторів дозволяє аналізувати ситуацію та вибирати відповідні інструменти та методи для розслідування. Незважаючи на те, що не існує універсального шаблону для кожного випадку, є певні аспекти, на які можна орієнтуватися під час розслідування. Наприклад, у випадку кіберінциденту або масштабної кібератаки завжди буде доступна інформація про подію. Збір первинної інформації про інцидент є початковим етапом для подальшого розслідування і використання OSINT.

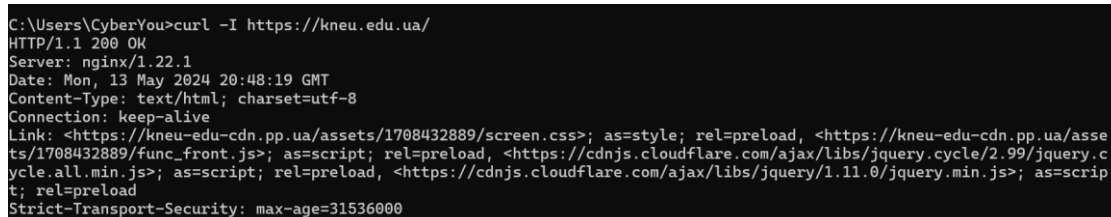
Крім того, важливо зазначити, що OSINT не обмежується лише відкритими джерелами в Інтернеті. Він також може включати в себе аналіз фізичних документів, громадських записів, патентів, академічних досліджень та інших джерел інформації. Отже, важливо мати гнучкий підхід до використання OSINT і бути готовим адаптуватися до різних сценаріїв та викликів.

3.1.1 Принцип роботи пошукової системи Shodan

Принцип роботи Shodan заключається в тому, що він шукає і збирає банери, які описують службу, що використовується на пристрої. Банер для Shodan це основна одиниця інформації [32].

Один із прикладів банера - це банер веб-сервера, тобто заголовок. Щоб побачити заголовок веб-сервера можна, наприклад, ввести команду:

`curl -I https://kneu.edu.ua/`



```
C:\Users\CyberYou>curl -I https://kneu.edu.ua/
HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Mon, 13 May 2024 20:48:19 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Link: <https://kneu-edu-cdn.pp.ua/assets/1708432889/screen.css>; as=style; rel=preload, <https://kneu-edu-cdn.pp.ua/assets/1708432889/func_front.js>; as=script; rel=preload, <https://cdnjs.cloudflare.com/ajax/libs/jquery.cycle/2.99/jquery.cycle.all.min.js>; as=script; rel=preload, <https://cdnjs.cloudflare.com/ajax/libs/jquery/1.11.0/jquery.min.js>; as=script; rel=preload
Strict-Transport-Security: max-age=31536000
```

Рисунок 3.1 – Результат команди `curl -I https://kneu.edu.ua/`

Аналізуючи результат ми бачимо, що використовується протокол HTTP. І код статусу 200.

За кодами статусів можна зрозуміти як реагує сервер на запит:

- 200 - усе добре, запит успішний;
- 300 - перенаправлення на іншу сторінку;
- 400 - проблема із запитом;
- 500 - проблема із сервером.

Після цього йде безпосередньо сам заголовок у якому міститься різноманітна технічна інформація. З цього можна зробити висновок, що в абсолютно будь-якому протоколі є банер. А в абсолютно будь-якому банері є технічна інформація, яка відрізняється залежно від протоколу. Саме ці дані і збирає Shodan. А з огляду на те, що, дуже часто, в банері міститься досить багато даних, що описують сам пристрій, це може бути дуже корисно. Крім цього Shodan також збирає метадані пристрою. Наприклад геолокацію, операційну систему тощо.

Для початку роботи в Shodan треба зареєструватися. Це відкриє доступ до функцій, а саме стане доступно більше результатів пошуку, фільтри і можемо отримати свій API ключ. А тому переходимо безпосередньо до пошуку.

Найпростіший варіант пошуку - це ввести назву або виробника потрібного нам пристрою. Наприклад, якщо ми введемо tp-link, то праворуч побачимо знайдені пристрої та їхні банери, а зліва деякі статистичні дані, за якими також можна відфільтрувати пристрої. Також потрібно пам'ятати, що це не Google, а тому запит для пошуку обробляється як точний вираз, без жодних варіацій.

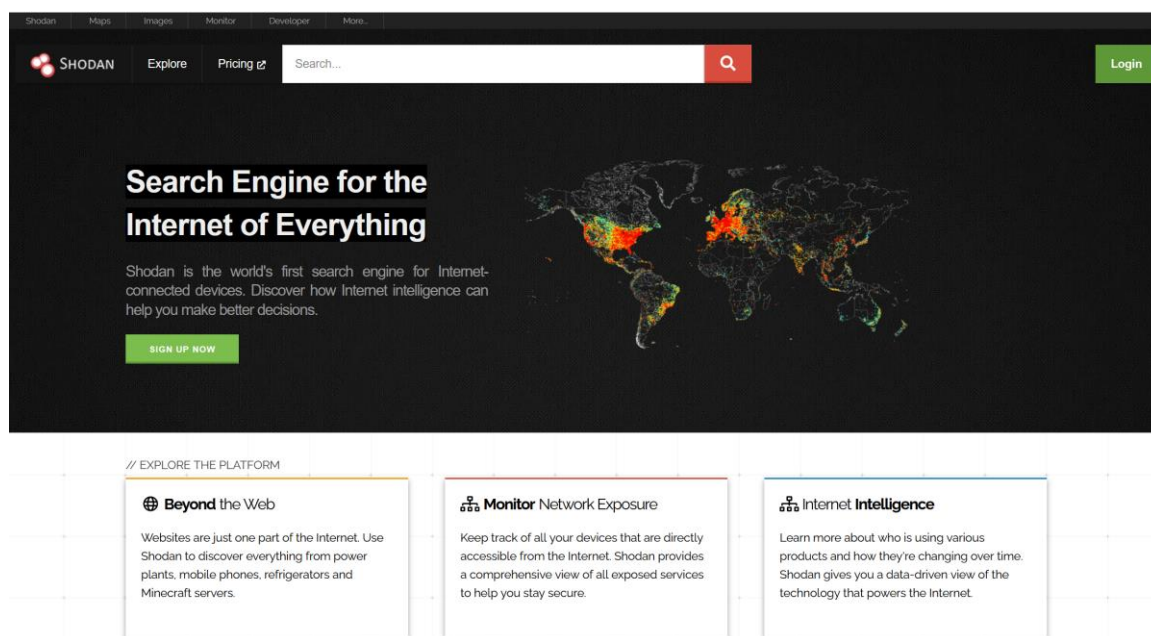


Рисунок 3.2 – головна сторінка Shodan

Фільтри – це просто конкретизація запиту. Вони працюють як уточнення запиту. Тут потрібно враховувати, що щоб максимально ефективно використовувати Shodan, потрібно дуже добре розуміти: по-перше, що ти хочеш знайти, а по-друге, як працює потрібний тобі пристрій: яке програмне забезпечення використовує, які в нього бувають версії, який протокол, та іншу технічну інформацію залежно від пристрою. Найімовірніше, те, що ти хочеш знайти, вже хтось колись шукав, а отже, він міг поділитися своєю методикою пошуку і дець опублікувати запит, який дав результат. Для цього Shodan збирає найбільш популярні запити: <https://www.shodan.io/explore/popular?page=1>

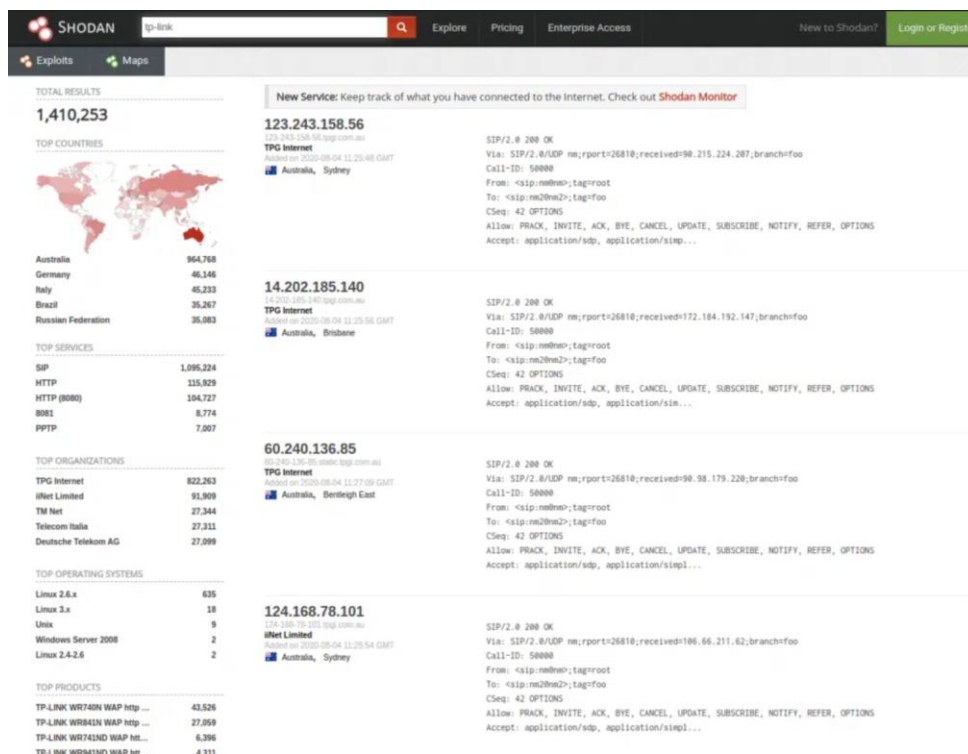


Рисунок 3.3 – Запит tp-link в Shodan

Тепер більш детально про самі фільтри. Як можна побачити запит `tp-link` дав нам майже півтора мільйона результатів. Це забагато. Що б скоротити кількість результатів, для початку ми можемо відфільтрувати їх за країною. Для цього використовується фільтр `country` і, після двокрапки, без пробілів вказуємо код країни. Наприклад: `tp-link country:UA` покаже результати в Україні. За таким самим принципом працюють і інші фільтри. Тобто логіка їх використання така: спочатку вказуємо сам запит, а потім пишемо фільтр і через двокрапку, без пробілу, значення для фільтра. Якщо значення складається з декількох слів, то його потрібно взяти в лапки.

Існує ряд найпопулярніших фільтрів Shodan, а саме:

- `country:` - покаже дані тільки за обраною країною, наприклад `country:RU`
- `city:` - покаже дані тільки за обраним містом, наприклад `city:Moscow`
- `os:` - знайти певну операційну систему, наприклад `os:linux`
- `geo:` - пошук за геопозицією, потрібно вказати координати, наприклад `geo:"45.0746,39.0587"`
- `port:` - покаже результати тільки за обраним портом, наприклад `port:22`

- **hostname:** - шукатиме тільки в певній доменній зоні, наприклад **hostname:.ua**
- **net:** - пошук у заданому мережевому діапазоні, наприклад **net:190.73.40.50/24**
- **product:** - пошук за назвою програми, що віддає банер, наприклад **product:openssh**

Також потрібно знати, що якщо ми хочемо прибрати з видачі результати за якимось фільтром, то перед фільтром потрібно поставити знак мінус, наприклад, якщо написати **country:UA -city:Kiev**, то нам покаже всі результати пошуку в Україні, без результатів по Києву. За таким же принципом це працює і з іншими фільтрами. Щоб було зрозуміліше, як усе це працює, варто розглянути реальні приклади пошуку. Для прикладу знайдемо вебкамери у Варшаві, які використовують порт 8080:

webcam country:PL city:Warsaw port:8080

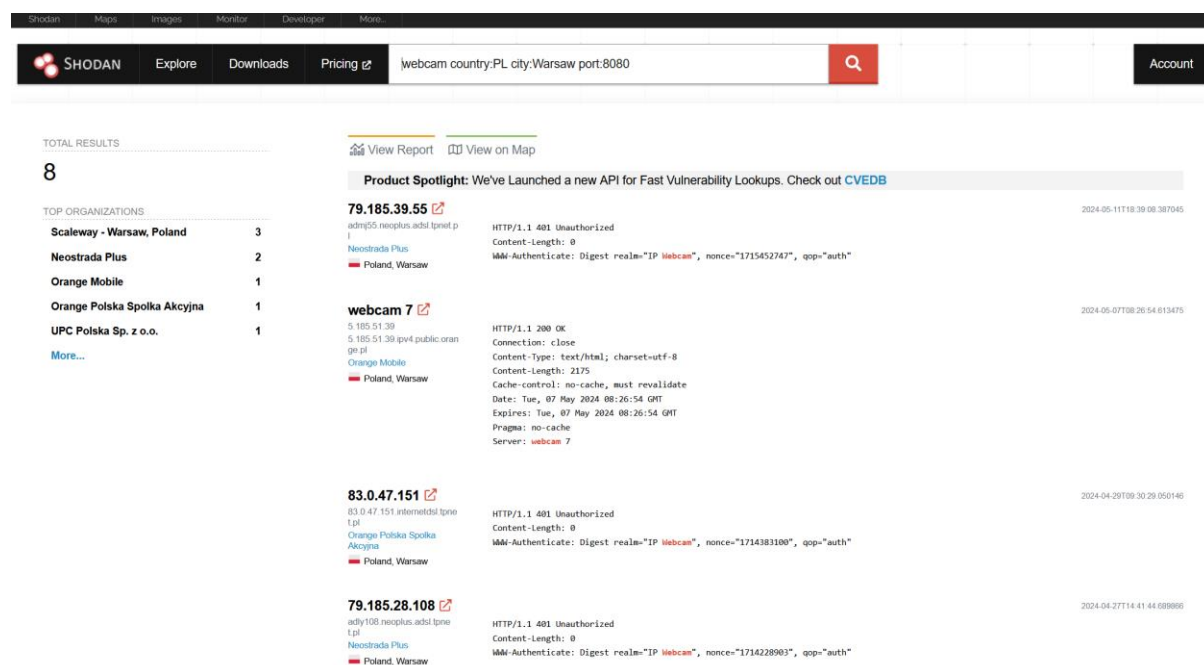


Рисунок 3.4 – Результати пошуку **webcam country:PL city:Warsaw port:8080**

Тепер знайдемо сервера **nginx**, під управлінням операційної системи **Linux**, з відкритим портом **5000**

nginx os:linux port:5000

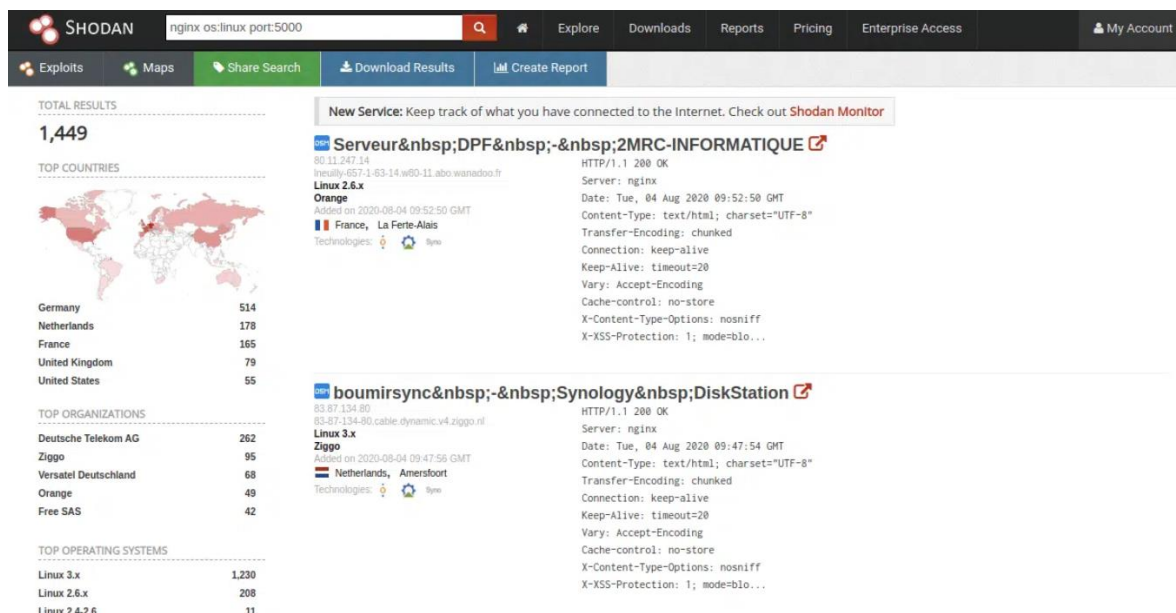


Рисунок 3.5 – Результати пошуку nginx os:linux port:5000

Як можна побачити, таких серверів не мало. Отримані результати ми можемо додатково відфільтрувати за параметрами, які ми бачимо в таблиці зліва. А якщо виберемо якийсь конкретний результат, то побачимо розгорнуту інформацію про нього. Зокрема IP-адресу, геопозицію, країну, які порти відкрито, які служби ці порти використовують та банери цих служб.

Працювати з Shodan можна не тільки через сайт, а й прямо з терміналу. Причому в деяких ситуаціях так навіть зручніше і швидше. Для початку потрібно встановити бібліотеку Python для Shodan. Потім додати свій API-ключ, щоб його отримати, потрібно зареєструватися на сайті та перейти в розділ My Account.

Команди для встановлення Shodan CLI

```
sudo apt install python3-shodan
```

```
shodan init API
```

```
shodan
```

Вводимо команду Shodan і бачимо довідку з використання.

```

C:\Users\user>shodan
Usage: shodan [OPTIONS] COMMAND [ARGS]...

Options:
  -h, --help  Show this message and exit.

Commands:
  alert      Manage the network alerts for your account
  convert    Convert the given input data file into a different format.
  count      Returns the number of results for a search
  data       Bulk data access to Shodan
  domain     View all available information for a domain
  download   Download search results and save them in a compressed JSON...
  honeyscore Check whether the IP is a honeypot or not.
  host       View all available information for an IP address
  info       Shows general information about your account
  init       Initialize the Shodan command-line
  myip       Print your external IP address
  org        Manage your organization's access to Shodan
  parse      Extract information out of compressed JSON files.
  radar      Real-Time Map of some results as Shodan finds them.
  scan       Scan an IP/ netblock using Shodan.
  search     Search the Shodan database
  stats      Provide summary information about a search query
  stream     Stream data in real-time.
  trends     Search Shodan historical database
  version    Print version of this tool.

```

Рисунок 3.6 – Результат команди shodan

Використання: shodan [OPTIONS] COMMAND [ARGS]...

Опції:

-h, --help Показати це повідомлення і вийти.

Команди:

alert Керування мережевими сповіщеннями для вашого облікового запису

convert Перетворити вказаний файл вхідних даних в інший формат

count Повертає кількість результатів пошуку.

data Масовий доступ до Shodan

domain Перегляд усієї доступної інформації для домену

download Завантажити результати пошуку та зберегти їх у форматі JSON

honeyscore Перевірити, чи є IP-адреса приманкою чи ні.

host Перегляд усієї доступної інформації за IP-адресою

info Показати загальну інформацію про ваш обліковий запис

init Ініціалізувати командний рядок Shodan

myip Показати зовнішню IP-адресу

org Керування доступом вашої організації до Shodan

parse Витягти інформацію з файлів JSON.

radar Карта деяких результатів у реальному часі, коли їх знаходить Shodan.

scan Сканування IP/netblock за допомогою Shodan.

search Пошук у базі даних Shodan

stats Показати зведену інформацію про пошуковий запит

stream Потокове передавання даних у реальному часі.

version Версія для друку цього інструмента.

Це загальна довідка по Shodan. Також за кожною командою є додаткові фільтри та параметри, які можна вказати. Наприклад, щоб побачити фільтри для команди search:

shodan search -h

```
C:\Users\user>shodan search -h
Usage: shodan search [OPTIONS] <search query>

Search the Shodan database

Options:
  --color / --no-color      List of properties to show in the search results.
  --fields TEXT              The number of search results that should be returned
                             Maximum: 1000
  --limit INTEGER           The separator between the properties of the search
                             results.
  --separator TEXT          Show this message and exit.
  -h, --help
```

Рисунок 3.7 – Результат команди shodan search -h

Почати роботу з Shodan CLI можна з команди count, вона покаже скільки всього результатів за запитом, який нас цікавить. Наприклад, переглянемо, скільки в Україні серверів nginx з відкритим портом 443:

shodan count nginx port:443 country:UA

```
C:\Users\user>shodan count nginx port:443 country:UA
35580
```

Рисунок 3.8 – Результат команди shodan count nginx port:443 country:UA

Бачимо з відповіді, що таких серверів 35580 штук і аналізувати таку кількість сенсу немає. Запит треба уточнювати. Ця команда дає нам змогу швидко оцінити можливу кількість результатів пошуку. Наступна команда яку доведеться

застосовувати це download. Вона дає змогу зробити пошук за нашим запитом і завантажити результати у файл JSON, в якому кожен новий рядок це новий банер. За замовчуванням завантажує першу тисячу результатів. Якщо потрібна інша кількість, то використовується параметр -limit.

shodan download nginx port:5555 country:UA

```
C:\Users\user>shodan download nginx port:5555 country:UA
Search query:                port:5555 country:UA
Total number of results:     3436
Query credits left:          0
Output file:                 nginx.json.gz
[-----] 0%
Notice: fewer results were saved than requested
Saved 0 results into file nginx.json.gz
```

Рисунок 3.9 – Результат команди shodan download nginx port:5555 country:UA

Ще одна цікава особливість Shodan у тому, що він збирає вразливості та експлойти. Їхній пошук трохи відрізняється, нам потрібно вказати платформу, під яку ми хочемо знайти вразливість, і вид вразливості. Наприклад:

platform:windows type:exploit

SHODAN | Exploits | platform:windows type:exploit | Logout

TOTAL RESULTS
987

PLATFORM	Count
Windows	987
Linux	65
Java	36
OSX	24
Unix	20

AUTHOR

juan vazquez	207
MC <mc@metasploit.com>	206
jduck	118
sinn3r	111
<sinn3r@metasploit.com>	111
hdm <hdm@metasploit.com>	72

MS09-002 Microsoft Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruption
dean <dean@zeroday-solutions.com>
Windows
... This module exploits an error related to the CFunctionPointer function when attempting to access uninitialized memory. A remote attacker could exploit this vulnerability to corrupt memory and execute arbitrary code on the system with the privileges of the victim. ...

HP OpenView NNM 7.53, 7.51 OVAS.EXE Pre-Authentication Stack Buffer Overflow
hameddi <hameddi@metasploit.com>, mts
Windows
...
Exploitation is tricky due to character restrictions. It was necessary to utilize a egg hunter shellcode which was alphanumeric encoded by mts in the original exploit.
If you plan on using exploit this for a remote shell, you will likely want to migrate to a different process as soon as possible. Any connections get reset after a short period of time. This is probably some timeout handling code that causes this. ...

HP OpenView Network Node Manager ov.dll _OVBuildPath Buffer Overflow
Anyway <AnyWayAnyWay@gmail.com>, juan vazquez <juan.vazquez@metasploit.com>, sinn3r <sinn3r@metasploit.com>
Windows
This module exploits a stack buffer overflow in HP OpenView Network Node Manager 7.53 prior to NNM.01213 without the SSR100649 hotfix. By specifying a long 'textFile' argument when calling the 'webappon.exe' CGI program, an attacker can cause a stack-based buffer overflow a ...

Рисунок 3.10 – Результат пошуку platform:windows type:exploit

3.1.2 Використання методології аналізу рівня помилок

Одним із проблемних аспектів експертизи цифрових зображень є пояснення технічних питань, які важко зрозуміти неспеціалістам. Навіть якщо докази фальсифікації абсолютно очевидні, суто технічні документи незрозумілі широкому загалу. Існує ймовірність того, що розлогі тексти зі складними описами не будуть сприйняті. У гіршому випадку, це викликає образливе негативне ставлення.

Найбільш прийнятним і зрозумілим методом, який також надає багато відправних точок для нефахівців, є виявлення простих композицій зображень, які можна знайти за допомогою функції зворотного пошуку зображень за допомогою основних постачальників пошукових систем. Бачити, де саме і в який спосіб було здійснено маніпуляцію, є загальновизнаним і найбільш переконливим доказом [26].

Для розвідувальної роботи із залученням громадськості візуалізація є одним із найефективніших засобів, але не обов'язково найкращим. Візуальний метод, який знайшов своє місце в криміналістиці цифрових зображень, називається аналізом рівня помилок (Error Level Analysis). Однак існує ризик неправильного застосування. Використання методології ELA завжди повинно розглядатися дуже ретельно. Аналіз рівня помилок ґрунтується на характеристиках форматів зображень, які базуються на стисненні зображень з втратами. Цей метод може виділити області зображення, які мають різний ступінь стиснення. Особливо добре цей метод підходить для формату JPEG (одного з найпопулярніших форматів зображень в Інтернеті) [27].

Для кращого розуміння необхідно знати, як створюються зображення у форматі JPEG. JPEG використовує стиснення зображення з втратами. Кожен процес перекодування (нове збереження), що виконується над зображенням, призводить до подальшої втрати якості. Алгоритм JPEG базується на сітці 8x8 пікселів. Таким чином, кожна квадратна сітка 8x8 обробляється і стискається окремо. Якщо зображення не змінено, то всі ці квадрати 8x8 матимуть однаковий потенційний рівень помилок. Якщо зображення у форматі jpeg зберігається знову, то кожен квадрат повинен бути безперервно зменшений до приблизно однакового рівня. У процесі ELA оригінальне зображення, яке досліджується, буде збережено з певним рівнем якості JPEG (наприклад, 75%). Повторне збереження призводить

до відомого ступеня стиснення, який поширюється на все зображення. Новозбережене зображення використовується для порівняння з оригінальним зображенням. Людське око навряд чи помітить зміни. Тому ELA-зображення візуалізує, зокрема, лише різницю між двома зображеннями. Таким чином, отримане ELA-зображення показує різний ступінь стиснення потенціалів.

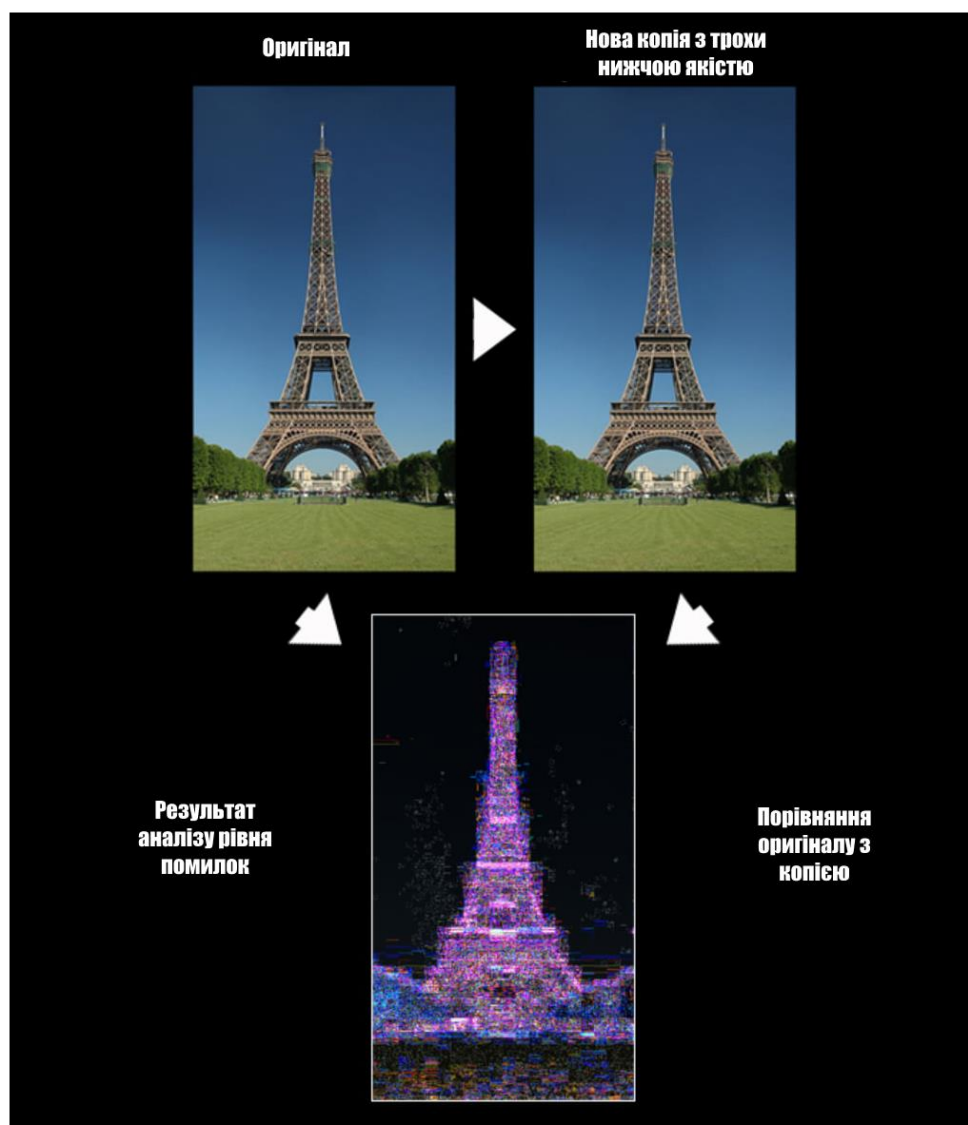


Рисунок 3.11 – Різниця ступеню стиснення потенціалів

В основі методу виявлення підроблених JPG зображень лежить ідея, що якщо зображення було відредаговано, то кожен квадрат 8×8 , на який вплинули зміни, містить більший потенціал помилки, ніж решта зображення [28].

Навіть без маніпуляцій із зображенням, ELA-перегляд покаже різні ділянки на оригінальних зображеннях, які виходять на передній план. Ці природні характеристики необхідно знати, якщо ви хочете мати можливість довести маніпуляції за допомогою цього підходу. Вигляд ELA підкреслює різні потенціали стиснення, що виникають на зображенні. Області з однорідним кольором, такі як безхмарне блакитне небо або яскраво-біла стіна, показують темні результати ELA порівняно з сильно контрастними ділянками країв, які виглядають набагато яскравіше.

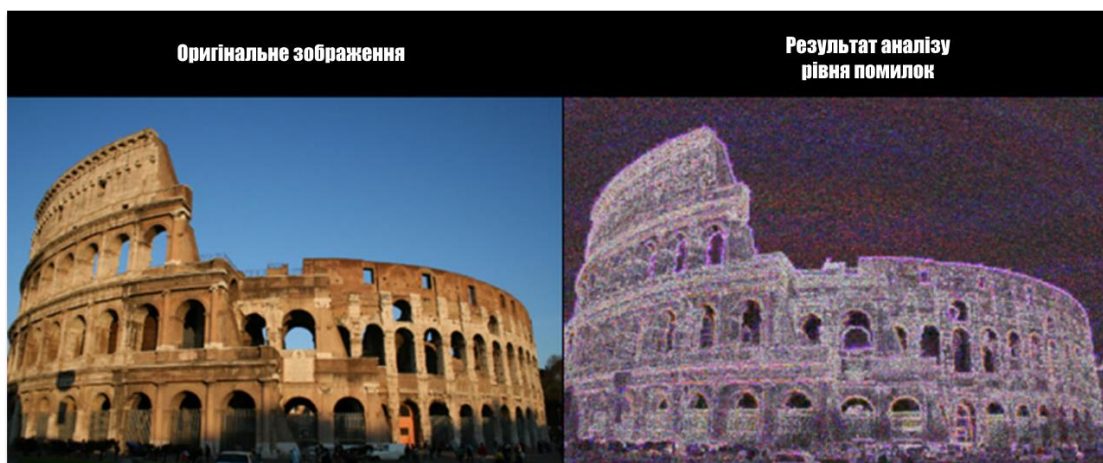


Рисунок 3.12 – Порівняння оригіналу з результатом ELA

Однорідні області зображення, такі як небо на прикладі фотографії Колізею, можуть бути ефективно стиснуті. Завдяки цьому потенціал стиснення є низьким при повторному циклі стиснення відповідно в новому збереженні і призводить до більш темного кольору на зображенні ELA. На противагу цьому, нерегулярні патерни з тонкими контурами та складними градієнтами кольору і яскравості матимуть лише кілька надлишкових зображень, які не можуть бути так добре зменшені. Повторне збереження зображення у форматі JPG видаляє високочастотні частини зображення і зменшує різницю між сильно контрастними краями, текстурями і поверхнями. Зображення у форматі JPG, збережене з найнижчим рівнем якості, відображається відповідно набагато темніше, ніж з вищим рівнем якості.



Рисунок 3.13 – Порівняння оригіналу нижчої якості з результатом ELA

JPEG-файл, який створює власну таблицю Хаффмана на основі статистичного аналізу відповідного вмісту зображення, називається прогресивним JPEG. Зображення, згенеровані цифровими камерами, однак, не оптимізуються таким чином. Оригінальні знімки з цифрових камер завжди повинні мати високий ступінь змін після нового збереження і, таким чином, мати відносно світлі ділянки в результатах ELA. Дуже темний результат ELA на прикладі зображення (із зображенням Колізею), яке було збережено в нижчому рівні якості, є чіткою ознакою того, що це зображення жодним чином не є оригінальним файлом JPEG, який було завантажено безпосередньо з камери.

Наступна серія прикладів ілюструє, як може виглядати унікальний доказ несанкціонованого доступу за допомогою методу ELA. Навіть не маючи оригінального зображення (рис. 3.14), ELA може показати, де щось було змінено на зображенні (рис. 3.15).



Рисунок 3.16 – У верхній частині по центру було вставлено поперечну назву DVD-диска з вигаданою обкладинкою "Рембо 5000".

Результат ELA шаблону зображення, що піддавався маніпуляціям. Обкладинка DVD-диска з іншим рівнем стиснення чітко виділяється з набору сусідніх обкладинок. Немає жодних природних причин, чому ця обкладинка DVD виглядає такою темною. Існують й інші схожі обкладинки, що демонструють рівномірний яскравий шум зображення. Маніпуляція із зображенням у цьому випадку цілком очевидна.

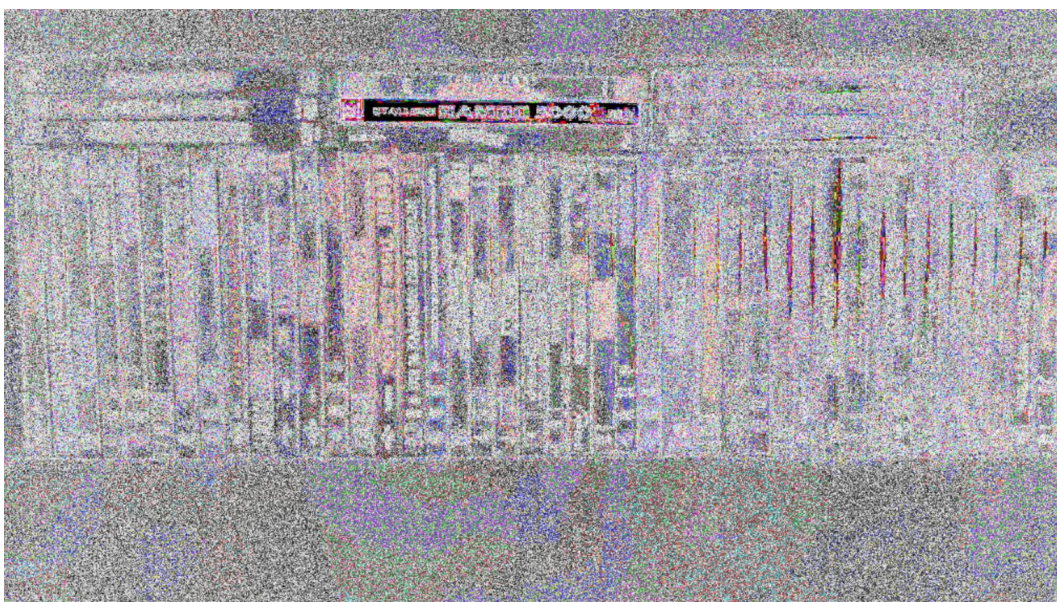


Рисунок 3.17 – Результат ELA

Зображення у форматі JPG, які зберігаються з найнижчим рівнем якості (або максимальним стисненням), виглядають дуже темними у вікні результатів ELA . Якщо ми додамо скопійовані елементи з шаблону зображення, який існував у вищому рівні якості, то це буде чітко видно на зображенні ELA у вигляді набагато яскравіших ділянок. Ці скопійовані елементи мають значно вищий потенціал стиснення на відміну від решти зображення.



Рисунок 3.18 – Оригінальне зображення

Ця версія зображення є повторно збереженою копією DVD-прикладу, але з нижчим рівнем якості.

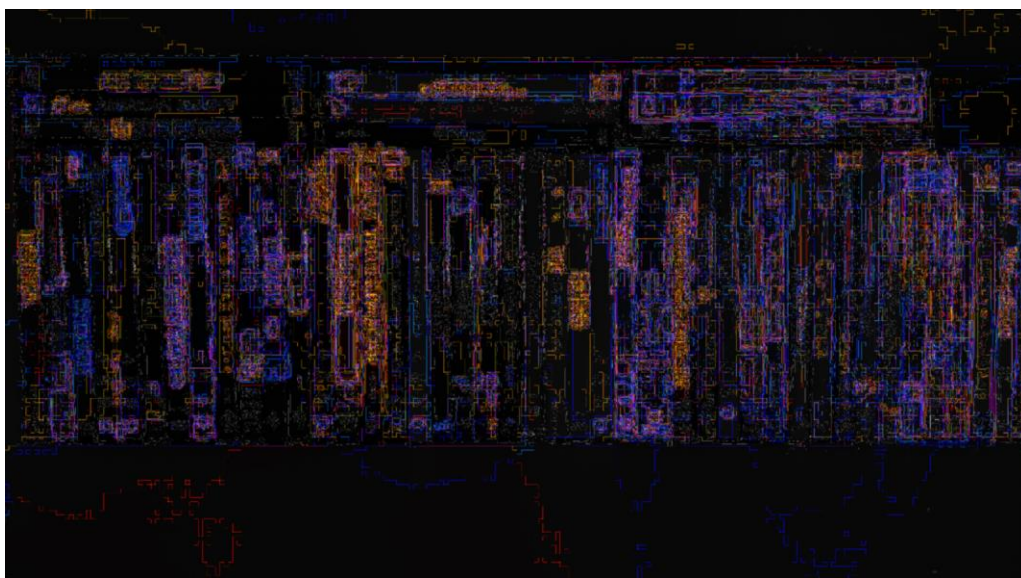


Рисунок 3.19 – Похідний результат ELA від вихідного зображення

Представлений тут графік ELA набагато темніший порівняно з результатами ELA з першого прикладу.



Рисунок 3.20 – Вихідне зображення зі скопійованими елементами у лівій частині

На цьому зображенні дві скопійовані обкладинки DVD були розміщені поверх існуючих обкладинок у правій частині. Скопійовані елементи походять з іншого шаблону, який зберігався у вищій якості.

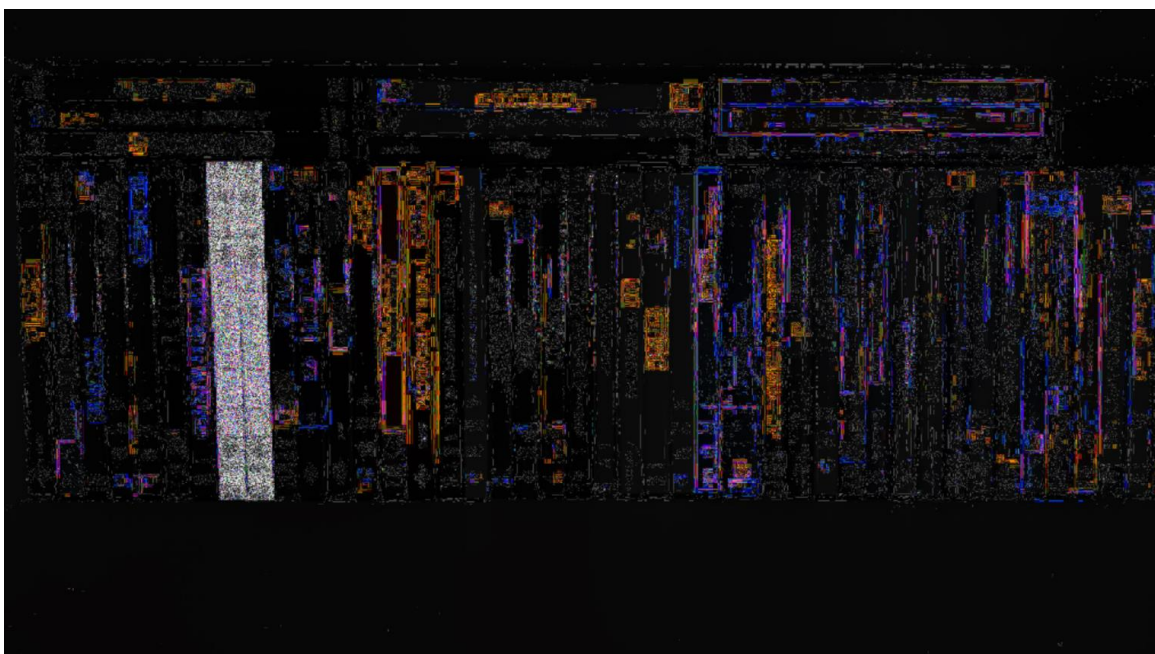


Рисунок 3.21 – Результат ELA маніпульованого зображення.

Маніпульований DVD-диск значно виділяється іншим рівнем стиснення порівняно з іншими сусідніми дисками.

Аналіз рівня помилок може за певних умов чітко вказати, чи були здійснені маніпуляції із зображенням і де саме. Однак, така визначеність досягається лише в деяких випадках. У більшості професійних криміналістичних аналізів зображень метод ELA використовується лише як один із можливих інструментів для отримання перших підказок, які потім можна вибірково перевірити за допомогою інших методів. За винятком тих випадків, коли ELA може дати однозначний результат, він не може бути використаний як доказ в інших випадках. Або можна навести чіткі докази фальсифікації, або утриматися від зобов'язуючої заяви через брак придатних для використання даних.

3.1.3 OSINT аналіз електронного листа

Яскравим прикладом використання OSINT інструментів може бути отримання електронного листа з вкладенням, в якому міститься архів, що містить шкідливе програмне забезпечення. Після відкриття і збирає даний файл та передає його на сторонній сервер. Такі випадки сьогодні не рідкість. Відправниками таких листів є або новачки, які тільки експериментують і тестують подібні інструменти, або люди, які намагаються здійснити хакерську атаку на організацію та отримати її дані.

Відправною точкою для розслідування такого типу інцидентів має бути адреса електронної пошти відправника та його IP-адреса; використовуючи методологію OSINT, можна перевірити, чи є адреса електронної пошти в базі даних спаму, а також визначити можливого власника адреси електронної пошти. Наприклад, за допомогою інструментів, описаних раніше в цій статті, можна перевірити, чи зареєстрована електронна адреса відправника на веб-ресурсі або чи використовувалася вона для реєстрації в соціальній мережі.

Якщо завантажити лист на комп'ютер і відкрити його в текстовому редакторі, можна побачити IP-адресу відправника і сервіс, з якого було надіслано лист. На рисунку 3.22 показано приклад відкритого листа.

```

1 X-Source: ABBF2xw7ZKxJfNDG5D9Wx6H2G1stfTfBYFC12F8vD5y1OTfM0S0nVYAcj03a2QhA3J2
2 X-Received: by 2021a1710b13a771: with SMTP id x37m3773204qjb.89.163577203555;
3 Mon, 01 Nov 2021 06:07:15 -0700 (PDT)
4
5 ARC-Seal: i=1; a=rsa-sha256; t=1635772035; o=google;
6 d=google.com; s=sma-20160816;
7 b=1w/10L1y0D3K4wqIspU1L18p3G5C5y11MqQdPC3Yx/WEKX3aFgYhuE8F806
8 c18X0u778EocCqT8TE/uyQm/f64fca2B019hnp872vyyv9B8F64g9Yma
9 c03vKae21Fz187caBAd0mTuf/0Pp121y0m/SaM000q3780c1Y4p9e1vz
10 v76d4FazJ5f6b18k1FLOFT8Fq48FTq2a5D0X0uXW0b117C1VY2qy7/03y/06
11 12b7F3an92/VxIDtH1MTI008071qH0U0L0m46112v1CT749J7CJL20132R8
12 Yd8w=
13
14 ARC-Message-Signature: i=1; a=rsa-sha256; o=relaxed/relaxed; d=google.com; s=sma-20160816;
15 b=1w/10L1y0D3K4wqIspU1L18p3G5C5y11MqQdPC3Yx/WEKX3aFgYhuE8F806
16 c18X0u778EocCqT8TE/uyQm/f64fca2B019hnp872vyyv9B8F64g9Yma
17 c03vKae21Fz187caBAd0mTuf/0Pp121y0m/SaM000q3780c1Y4p9e1vz
18 v76d4FazJ5f6b18k1FLOFT8Fq48FTq2a5D0X0uXW0b117C1VY2qy7/03y/06
19 12b7F3an92/VxIDtH1MTI008071qH0U0L0m46112v1CT749J7CJL20132R8
20 Yd8w=
21
22 ARC-Authentication-Results: i=1; mx.google.com;
23 dkimpass header.a@email.crunchease.com header.sma-20160816 header.b="TLKX/ig0";
24 spfpass (google.com) domain of mspvri=18939ekvve5@bounces-280172-59@gmailtechnolo.com designates 192.174.84.252 as permitted sender; smtp.mailfrom=mspvri=18939ekvve5@bounces-280172-59@gmailtechnolo.com;
25 dmarpass (p=QUADRTIME sp=QUADRTIME gl=NONE) header.from=crunchease.com
26 Return-Path: mspvri=18939ekvve5@bounces-280172-59@gmailtechnolo.com
27 Received: from mta-84-252.sparkpostmail.com (mta-84-252.sparkpostmail.com [192.174.84.252])
28 by mx.google.com with ESMTPS id 110v21104632ip.45-2021.11.01.06.07.16
29 for <maxxer6@gmail.com>
30 (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
31 Mon, 01 Nov 2021 06:07:15 -0700 (PDT)
32
33 Received-SPF: pass (google.com) domain of mspvri=18939ekvve5@bounces-280172-59@gmailtechnolo.com designates 192.174.84.252 as permitted sender; client-ip=192.174.84.252;
34 Authentication-Results: mx.google.com;
35 dkimpass header.a@email.crunchease.com header.sma-20160816 header.b="TLKX/ig0";
36 spfpass (google.com) domain of mspvri=18939ekvve5@bounces-280172-59@gmailtechnolo.com designates 192.174.84.252 as permitted sender; smtp.mailfrom=mspvri=18939ekvve5@bounces-280172-59@gmailtechnolo.com;
37 dmarpass (p=QUADRTIME sp=QUADRTIME gl=NONE) header.from=crunchease.com
38 X-SPFBL: 865yC0/n3M6131215197/0C182BQCTQ176u0=eyD1Wkbn8FwG0u
39 c03vKae21Fz187caBAd0mTuf/0Pp121y0m/SaM000q3780c1Y4p9e1vz
40 c1w18WVc0FzV9p2C161Ym8ec22028U2ZHTe4502k8w011v1YV4s59ZKX
41 f8w011y0D3K4wqIspU1L18p3G5C5y11MqQdPC3Yx/WEKX3aFgYhuE8F806
42 Yd8w=
43 DKIM-Signature: v=1; a=rsa-sha256; o=relaxed/relaxed;
44 d=email.crunchease.com; s=sma-20160816; t=1635772035;
45 b=1w/10L1y0D3K4wqIspU1L18p3G5C5y11MqQdPC3Yx/WEKX3aFgYhuE8F806
46 c18X0u778EocCqT8TE/uyQm/f64fca2B019hnp872vyyv9B8F64g9Yma
47 c03vKae21Fz187caBAd0mTuf/0Pp121y0m/SaM000q3780c1Y4p9e1vz
48 v76d4FazJ5f6b18k1FLOFT8Fq48FTq2a5D0X0uXW0b117C1VY2qy7/03y/06
49 12b7F3an92/VxIDtH1MTI008071qH0U0L0m46112v1CT749J7CJL20132R8
50 Yd8w=
51
52 To: maxxer6@gmail.com
53 Message-ID: <047-10526-D46EF716@ch.mta1west.co.gov.sparkpost>
54 Date: Mon, 01 Nov 2021 13:06:15 +0000
55 Content-Type: multipart/alternative; boundary="-----gmD04FIDMA48u10oI2Dqmm_02/47-10526-D46EF716"
56 MIME-Version: 1.0
57 Reply-To: newletter@crunchease.com
58 Subject: India's unicorn herd grows as VC investment outpaces China, $2B round leads biggest funding deals of the week, and more - November 1, 2021
59 X-Campaign-ID: 3117443
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

```

Рисунок 3.22 – Приклад відкритого листа.

Для відкриття листа було використано програму Notepad++. IP-адресу відправника можна побачити в рядку 27 файлу листа, показаного на рисунку 3.1: 192.174.84.252. За допомогою інструменту "whois" або веб-ресурсу "https://whoer.net/ru/checkwhois"

Ви можете знайти інформацію про хостинг-провайдерів, які надають послуги за цією IP-адресою. На рисунку 3.23 показано, що інформація про відправника фізично зберігається на сервері SparkPost.

Сервер розміщений за наступною адресою.

IP-адрес: 192.174.84.252

Местоположение:



США (US), N/A

Регион:

Огайо (5165418)

Город:

Дублин

Индекс:

43017

Хост:

mta-84-252.sparkpostmail.com →
192.174.84.252

IP-диапазон:

192.174.80.0 - 192.174.95.255

Провайдер:

Sparkpost

Организация:

Sparkpost

Черный список:

Нет

TOR:

Нет

Часовой пояс:

America/New_York

Локальное:

Sat Nov 27 2021 10:03:45 GMT-0500 (EST)

Рисунок 3.23 – Результат викорситання SparkPost [38]

Таким чином, використовуючи лише методи та інструменти OSINT, вони змогли з'ясувати, за допомогою якого сервісу були надіслані повідомлення та де зберігається інформація про відправника. Зібрана інформація, безумовно, прискорить розслідування і, в разі звернення до правоохоронних органів, дозволить їм оперативно розбиратися з подібними випадками.

Таким чином, незважаючи на те, що до повідомлення був прикріплений файл, без аналізу цього файлу ми змогли отримати багато інформації, яка може лягти в основу нашого розслідування. Звичайно, без детального аналізу файлу і того, як ним маніпулювали, не вдасться скласти повну картину кіберінциденту.

Існує також багато інших випадків кіберінцидентів, коли використання методів OSINT є бажаним. Приклади таких інцидентів розглянуті нижче.

3.1.4 OSINT аналіз за адресою криптогаманця

При розслідуванні кіберінцидентів, пов'язаних з криптогаманцями, можна встановити особу власника гаманця; інструменти OSINT можна використовувати для аналізу інформації про криптогаманці. Крім того, технологія блокчейн дозволяє будь-кому побачити статус гаманця та здійснені з ним транзакції, якщо він знає адресу гаманця. OSINT-технологія дозволяє більш комплексно підійти до пошуку такої інформації [39]. Дані про власників криптогаманців не є винятком. Одним з OSINT-інструментів, що використовується для отримання інформації, є Maltego, описаний раніше і показаний на рисунках 3.24 та 3.25.

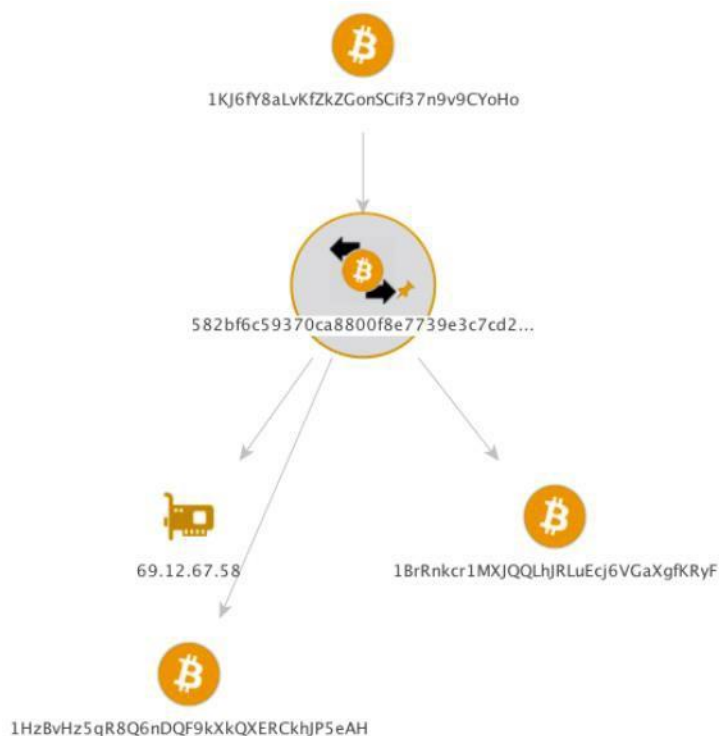


Рисунок 3.24 – Приклад використання інструменту Maltego

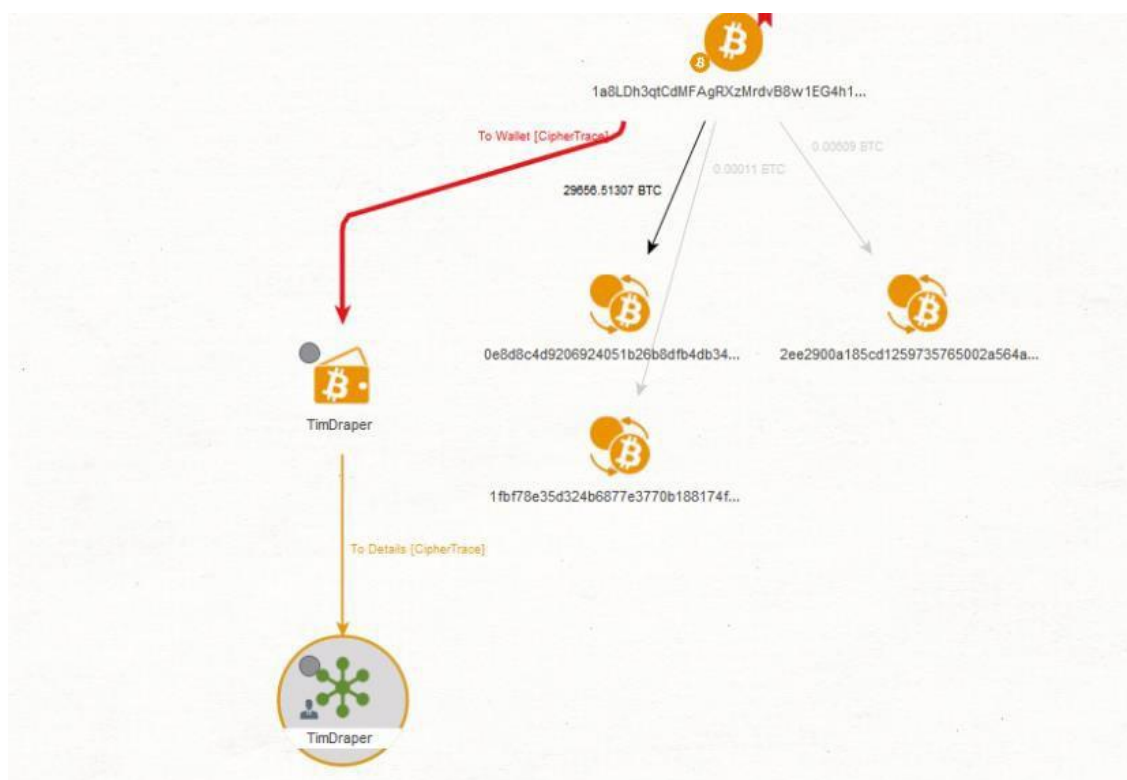


Рисунок 3.25 – Приклад використання інструменту Maltego

Також можна шукати гаманці в пошукових системах, таких як Google, Bing і Boardreader. Часто такі гаманці вказані в реквізитах форумів в Інтернеті. Навіть так звані “хакерські форуми” дозволяють пошуковим системам індексувати такі сторінки. Це відкриває можливості для збору інформації про потенційні цілі атаки або для виявлення можливих слабких місць в системах безпеки.

Існує також багато веб-ресурсів для пошуку криптогаманців. Найвідоміші з них - “blockchain.com/explorer”, “blockchair.com/”, “etherchain.org” та “etherscan.io”. Ці ресурси надають детальну інформацію про транзакції та баланси гаманців, що може бути корисним для аналізу фінансових потоків та виявлення підозрілих дій.

Технологія OSINT, завдяки своїй універсальності та нешаблонному підходу до отримання інформації, дозволяє підійти до проблеми з різних боків. Вона може бути використана в поєднанні з іншими методами та техніками дослідження, що може надати повну та об’єктивну інформацію про справу.

3.2 Інтеграція OSINT інструментів для ефективного управління інформаційними ризиками

Інформаційна безпека залежить від того, наскільки добре система може реагувати на виклики та загрози. У той же час аналіз умов зовнішньої і внутрішньої безпеки стає все більш важливим. Розгляд взаємозалежності та взаємозв'язку цих основних компонентів безпеки створює передумови для успішного захисту інтересів.

OSINT - одна з областей розвідки. Це включає пошук, відбір та збір даних із відкритих джерел, а також їх аналіз. У розвідувальному співтоваристві термін "відкритий" відноситься до ресурсу, який є загальнодоступним (на відміну від секретних і обмежених ресурсів) і не відноситься до поняття відкритого вихідного коду або публічної розвідки.

Збір інформації в OSINT сильно відрізняється від інших методів збору інформації. Основна проблема використання методів розвідки-це Витяг інформації з джерела, яке завжди існувало. Основним завданням OSINT є пошук значущих та надійних джерел інформації з широкого спектру інформації в кіберпросторі.

Хороший спосіб знайти інформацію з відкритого джерела інформації показаний на рисунку 3.26.



Рисунок 3.26 – Алгоритм пошуку інформації з відкритих джерел

Суть його полягає в наступному: отримання необхідної інформації про проблему. Створення якомога більшої кількості питань, групування питань за характеристиками, встановлення взаємозв'язку між групою та окремими темами, пошук інформації по кожній темі, об'єктивність, новизна, надійність тощо. Для цього необхідно проаналізувати джерела. Вибирайте найкращі джерела, упорядковуйте та упорядковуйте інформацію. Донедавна ринок пропонував ряд програмних продуктів для автоматизації етапів життєвого циклу інформаційних систем управління ризиками. Всі вони відрізняються, мають різні форми подання, використовують різні методології управління ризиками, оцінки безпеки інформаційних систем, ієрархії та класифікації ресурсів. Він базується на різних джерелах, включаючи бази даних про загрози та вразливості. У зв'язку з цим впровадження єдиного автоматизованого інструменту є найбільш перспективним для впровадження системного підходу до управління інформаційними ризиками.

Для створення єдиної автоматизованої системи управління в першу чергу необхідно визначити основні напрямки автоматизації процесів управління інформаційною безпекою на всіх етапах циклу управління: планування, впровадження, валідація, вдосконалення стандартів серії ДСТУ[40].

Процес планування має включати такі етапи:

1. Встановлення списку інформаційних ресурсів підприємства. Автоматизовані інструменти можуть сприяти зберіганню даних про джерела інформації та їх зміни, а також полегшити процес збору даних.
2. Оцінка важливості інформації. В цьому контексті автоматизовані інструменти можуть зберігати лише дані опитувань.
3. Оцінка безпеки інформаційних ресурсів. Інтеграція бази даних про вразливості з вбудованою базою даних загроз може оптимізувати цей процес та забезпечити його цілісність. Також можлива інтеграція з різними сканерами вразливостей.
4. Визначення інформаційних ризиків. Вбудоване алгоритмічне рішення розраховує інформаційний ризик на основі введених даних. Результати представляються у вигляді звіту.
5. Вибір стратегії управління ризиками та визначення способів зменшення ризику. За допомогою автоматизованих технологій можна гнучко і зручно моделювати різні варіанти застосування захисту, оцінювати ефективність планованих заходів і вибирати найкращу стратегію захисту [41].

Додатково, важливо враховувати, що процес планування також повинен включати перегляд та оновлення плану. Це означає, що після виконання кожного кроку плану, необхідно переглянути результати, оцінити ефективність виконання та внести необхідні корективи. Це допоможе забезпечити, що план залишається актуальним і відповідає поточним потребам та обставинам.

Впровадження процедур IMS для підвищення безпеки включає їх впровадження в організаційні процеси. У цьому випадку автоматизований інструмент може збирати інформацію, підтримувати зв'язок між фахівцями і діяти як планувальник завдань.

На цьому етапі основним завданням автоматизованого інструменту є реєстрація документів:

- Нормативні документи (інструкції, положення, інструкції);
- запис, що підтверджує виконання існуючих процедур в організації;

Це означає, що всі документи про вимірювання зберігаються в центральному сховищі і при необхідності своєчасно подаються зацікавленим сторонам (наприклад, внутрішнім або зовнішнім аудиторам). Щоб переконатися, що процес ЦРТ працює належним чином і ефективно, або якщо є невідповідності, наприклад, щоб визначити, які поліпшення необхідні на цьому етапі, автоматизовані інструменти можуть виконувати наступні ролі:

Статистика та аналіз подій. Аналіз інцидентів є основним критерієм ефективності та адекватності інформаційної безпеки в організації, а також ефективності загальних показників. Заходи щодо поліпшення заходів з відновлення визначаються на основі інформації про інцидент [42]. Автоматизовані інструменти структурно зберігають інформацію про всі ІР-події, збирають статистику за різними параметрами і відображають об'єкти подій. Збір показників для оцінки ефективності ІС. Результат та частота інцидентів, пов'язаних з інформаційною безпекою, є найбільш очевидними показниками для оцінки їх ефективності. З іншого боку, автоматизовані інструменти можуть виявити вразливості, ефективність застосованих заходів, список ІР-адрес тощо.

На підставі отриманих і проаналізованих показників ефективності визначаються подальші дії і складається план їх реалізації. Зазвичай коригуючими діями є зміни в процедурах, документації, нових засобах захисту, тобто зміни в самій організації. Автоматизовані інструменти допомагають переглядати результати, зберігати дані та відстежувати зміни в безпеці джерел інформації.

В кінці завершального етапу весь прогрес повертається до етапу планування і періодично повторюється протягом усього життєвого циклу системи управління інтелектуальною власністю [43].

Назва компанії або продукту може з'являтися в Інтернеті 1 мільйон разів на день. Організації можуть використовувати більш активний підхід до управління

ризиками бренду, впроваджуючи найкращі практики OSINT для оцінки глобальної репутації бренду.

Захист заходів та майданчиків: шкідлива поведінка та дії можуть не тільки завдати фізичної шкоди відвідувачам, але й завдати шкоди іміджу бренду в довгостроковій перспективі. За допомогою технології OSINT ви можете брати участь в розвідувальній роботі для підвищення безпеки заходів і майданчиків до, під час і після заходу. Він забезпечує безпечний досвід для клієнтів та зацікавлених сторін, виявляючи потенційні загрози, надаючи інформацію про окремих осіб та групи інтересів, а також відстежуючи інші типи загроз, такі як кібератаки та небезпечні прогнози [44].

Тенденція ринку: маркетингові групи хочуть знати, що говорять про інтернет-бренди, особливо тому, що майже всі кампанії базуються на розумінні цільового ринку. Метод OSINT дозволяє цим командам розуміти сприйняття клієнтів та ключових зацікавлених сторін шляхом послідовного моніторингу ресурсів PAI для виявлення відповідних розмов та розуміння їх наслідків [45]. Це допомагає маркетинговим командам адаптувати свої стратегії та підходи до потреб та очікувань своєї аудиторії, що в свою чергу підвищує ефективність їх кампаній.

Зв'язки з громадськістю: щоб зрозуміти тенденції на ринку, менеджер зі зв'язків з громадськістю повинен знати, що говориться про його компанію і хто це говорить. Він повинен планувати потенційні сценарії застосування методу OSINT, визначати відповідні розмови на різних мовах, повинен швидко слідувати методу OSINT, щоб отримати огляд на 360°. Це допоможе менеджеру зі зв'язків з громадськістю випередити будь-які можливі проблеми та відповідати на них відповідним чином. Це допоможе вам випередити ситуацію зі зв'язками з громадськістю, щоб прийняти правильне рішення і зробити наступний крок.

Кіберзагрози поширені у всіх галузях. Команда з кібербезпеки пропонує ще один спосіб запобігання загрозам всередині та за межами брандмауера за допомогою методу OSINT. Це включає в себе моніторинг відкритих джерел на предмет потенційних загроз, а також використання OSINT для виявлення слабких

місць в системах безпеки. Це може допомогти організаціям краще захистити свої системи та дані від кібератак.

Виявлення внутрішніх загроз: не секрет, що інсайдери компанії становлять потенційну загрозу безпеці бізнесу. Реалізація методу OSINT надає співробітникам Служби безпеки інструменти, необхідні для попередження їх про потенційно підозрілу поведінку. Рішення OSINT також забезпечує постійну пильність і постійний моніторинг, необхідні для виявлення цих загроз [47].

ІТ-компанії, які покладаються на патенти та торгові марки для захисту, повинні знати про можливі витoki IP-адрес в Інтернеті, особливо в глобальній електронній комерції. Метод OSINT дає компаніям глибоке розуміння можливої крадіжки IP-адрес. Перевірка раі дозволить виявити місцезнаходження крадіжки, джерело контрафактних товарів і дозволить компаніям зробити необхідні кроки для зниження втрат, пов'язаних з крадіжкою інтелектуальної власності.

Боротьба з підробкою: підроблена продукція не тільки впливає на вартість бренду та прибуток, але й деякі продукти можуть негативно впливати на здоров'я населення. неділя Дек. Технологія OSINT допомагає компаніям впроваджувати моніторинг шахрайства за допомогою інструментів для постійного міжмовного моніторингу незаконних веб-сайтів та ринків, точного визначення місцезнаходження виробників, відстеження грошових слідів тощо [48].

Деякі типи загроз виходять за рамки внутрішніх процесів і поширюються на глобальні операції. Безпека та здоров'я ключових працівників можуть піддаватися ризику залежно від типу загрози. Використання методу OSINT допомагає компаніям випереджати потенційні операційні ризики та пом'якшувати їх наслідки.

Безперервність бізнесу: на безперервність бізнесу можуть вплинути різні природні та техногенні катастрофи. Ці катастрофи можуть легко спонукати компанії до дій, не вживаючи належних заходів.

Ви можете використовувати інформацію з глобальних джерел, яким може довіряти ваша команда, для підвищення обізнаності та прозорості ситуації.

Безпека критичної інфраструктури: оскільки критична інфраструктура підтримує компанії та країни, важливо зрозуміти можливі перешкоди. Метод OSINT

забезпечує систему раннього попередження для прогнозування та зменшення ризиків, які можуть вплинути на Вашу інфраструктуру.

Захист керівників і співробітників: забезпечення безпеки всіх співробітників є головним пріоритетом для бізнесу. Метод OSINT покращує наше розуміння потенційних загроз, виявляє ознаки раннього попередження про ризик і дозволяє нам вживати відповідних запобіжних заходів [50].

ВИСНОВКИ

У цій дипломній роботі було проведено детальний аналіз методів та інструментів OSINT. Основна мета роботи полягала в дослідженні та висвітленні застосування методів OSINT в контексті кібербезпеки.

Використання технологій OSINT у різних країнах світу дозволило нам оцінити їх ефективність та практичну цінність в різних сферах діяльності. Було проведено аналіз роботи міжнародних органів, які спеціалізуються на розвідці з відкритих джерел. Додатково було розглянуто питання застосування технологій OSINT в Україні, а також правові аспекти використання методів розвідки з відкритих джерел.

У процесі виконання роботи було проведено класифікацію основних типів інструментів розвідки з відкритих джерел та досліджено способи їх використання. Було змодельовано декілька сценаріїв, які демонструють практичне застосування технологій OSINT та їх потенціал.

Ця робота сприяє розумінню значущості та потенціалу методів OSINT в контексті кібербезпеки, а також підкреслює необхідність подальшого дослідження та розвитку цієї області. Зокрема, важливо зосередитись на розробці нових методів та технологій, які б дозволили ефективніше використовувати відкриті джерела інформації для підвищення рівня кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Землянікіна, М. П. (2021). Історія становлення та сучасний стан технології пошуку інформації OSINT. Scientific works of National Aviation University. Series: Law Journal “Air and Space Law”
2. Мартинюк, С. О. (2021). Характеристика принципів функціонування OSINT у сфері національної безпеки
3. Кожушко О. О. Розвідка відкритих джерел інформації (osint) у розвідувальній практиці США.
4. Ржевська Н.Ф., Кожушко О.О. Розвідка Відкритих Джерел (OPEN SOURCE INTELLIGENCE)
5. Про інформацію: Закон України від 02.10.92 р. № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
6. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.92 р. № 2782-XII. URL: <https://zakon.rada.gov.ua/laws/show/2782-12#Text>
7. Про охоронну діяльність: Закон України від 22.03.12 р. № 4616-VI. URL: <https://zakon.rada.gov.ua/laws/show/4616-17#Text>
8. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
9. Ланде Д.В. Правові питання конкурентної розвідки
10. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”: Указ Президента України від 15.03.16 р. № 96/2016. URL: <https://www.president.gov.ua/documents/4472021-40013>
11. Розробка системи управління кіберінцидентами в мережах LTE URL: <https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/13036/18086>
12. Abatabaei, Fahimeh, and Douglas Wells. "OSINT in the Context of Cyber-

Security." *Open Source Intelligence Investigation: From Strategy to Implementation* (2017): 213-231.

13. Benes, Libor. "OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm." *Journal of Strategic Security* 6.3 (2013): 22-37.

14. Ivanjko, Tomislav, and Tomislav Dokman. "Open Source Intelligence (OSINT): issues and trends." *7th International Conference The Future of Information Sciences, INFUTURE2019*. FF press, 2019.

15. Питання європейської та євроатлантичної інтеграції: Указ Президента України від 20.04.19р. №155/2019. URL: <https://zakon.rada.gov.ua/laws/show/155/2019#Text>

16. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.16р. №242/2016. URL: <https://zakon.rada.gov.ua/laws/show/242/2016>

17. Про оперативно-розшукову діяльність: Закон України від 18.02.92 р. № 2135-XII URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text>

18. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.16 р. № 96/2016. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>

19. Інструмент RECON-NG. URL: <https://github.com/lanmaster53/recon-ng>

20. Інструмент Maltego. URL: <https://www.maltego.com/>

21. Інструмент URLSCAN. URL: <https://urlscan.io/>

22. Інструмент GIFTHUB. URL: <https://github.com/smicallef/spiderfoot>

23. Інструмент FOCA. URL: <https://github.com/foca-js/foca>

24. Інструмент theHarvester. URL: <https://github.com/laramies/theHarvester>

25. Інструмент Google Dorks. URL <https://x-ray.contact/blog/useful-google-dorks-for-open-source-intelligence-investigations/>
26. Інструмент Osint Framework . URL <https://osintframework.com/>
27. Горбач М. М. Використання технології OSINT для збору, узагальнення та аналізу інформації на основі різних соціальних мереж: кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / М. М. Горбач. – Тернопіль : ТНТУ, 2023. – 60 с.
28. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor1:2014, IDT).
29. Перелік категорій кіберінцидентів URL: <https://cert.gov.ua/recommendation/16904>
30. OSINT Jenkinson, A. J. Book Chapter Digital Blood on Their Hands Vol. 1, 2023, pp.45 -52
31. Сучасні інформаційні технології у сфері безпеки та оборони №1
32. Complete Guide to Shodan URL: <https://ia800705.us.archive.org/17/items/shodan-book-extras/shodan/shodan.pdf>
33. Error Level Analysis URL: <https://fotoforensics.com/tutorial-ela.php>
34. Best practices for digital forensic evidence. National Institute of Justice. URL: <https://nij.ojp.gov/topics/articles/best-practices-digital-forensic-evidence>
35. Віщун В. В., Омелянчук А. В. Технологія виявлення загроз інформаційній безпеці шляхом аналізу інформації з відкритих джерел //Сучасні інформаційні технології у сфері безпеки та оборони. – 2012. – №. 3. – С. 5-7.
36. Open Source Intelligence (OSINT): Issues for Congress, December 5,2007. // www.fas.org/sgp/crs/intel/RL34270.pdf
37. Албул С.В. До питання концептуалізації напрямів вдосконалення інформаційно-аналітичного забезпечення негласної роботи суб'єктів оперативно-розшукової діяльності в Україні. Правові та організаційно-тактичні засади оперативно-розшукової діяльності Національної поліції України: Матеріали Всеукраїнської науково- практичної інтернет-конференції (м. Одеса,

30 жовтня 2020р.). Одеса: ОДУВС, 2020. С. 9–12.

38. Інструмент Sparkpost: веб-сайт. URL <https://sparkpost.com/>
39. Інструмент Maltego: веб-сайт. URL <https://www.maltego.com/solutions/cyber-threat-intelligence/>
40. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT).
41. Заєць П.М., Іванова О.С. Визначення підходів щодо впровадження засобів і систем автоматизації процесів управління інформаційною безпекою організації // https://academy.ssu.gov.ua/uploads/p_57_35588992.pdf
42. Яремик Христина Ярославівна, Яремик Мирослав Іванович Організація інформаційно-аналітичного забезпечення фінансово-економічної безпеки
43. Book chapter Chapter 6: OSINT Tools and Techniques Hacking Web Intelligence 2015 Sudhanshu Chauhan Nutan Kumar Panda
44. Research article A framework for threat intelligence extraction and fusion Computers & Security September 2023 Yongyan Guo Zhengyu Liu Jiayong Liu
45. Кузьо О. О., Крилов В. К., Мацюк Н. Л. Використання технології osint для формування портрету користувача //Матеріали XI Міжнародної науково-практичної конференції молодих учених та студентів „Актуальні задачі сучасних технологій “. – 2022. – С. 140-140.
46. Минько О. В. и др. Використання технологій OSINT для отримання розвідувальної інформації //Системи управління, навігації та зв'язку. – 2016. – №. 4. – С. 81-84.
47. Запорожченко М. М. Місце osint в життєвому циклі кібератаки //телекомунікаційні та інформаційні технології. – 2023. – №. 1. – С. 53-60.
48. Додонов О. Г. и др. Підхід до прогнозування дієвості державного управління з використанням технологій OSINT. – 2019.
49. Кожевников О. А., Кожевников О. А. Особенности комплексного

використання спеціальних знань та технологій osint 3-36 Застосування інформаційних технологій у діяльності. – 2020. – С. 52.

50. Єсіна М. В., Азаров М. О. Дослідження та аналіз інструментів і методів, що використовує механізм osint //The 7 th International scientific and practical conference “Modern research in world science”(October 2-4, 2022) SPC “Sci-conf. com. ua”, Lviv, Ukraine. 2022. 1320 p. – 2022. – С. 251.

Короткий звіт подібності



Ім'я користувача: Комп'ютерної математики та інформаційної безпеки...	ID перевірки: 1016276676
Дата перевірки: 23.05.2024 15:42:46 EEST	Тип перевірки: Doc vs Internet + Library
Дата звіту: 23.05.2024 15:45:51 EEST	ID користувача: 100005746

Назва документа: Диплом Кравцов

Кількість сторінок: 64 Кількість слів: 11241 Кількість символів: 89407 Розмір файлу: 25.17 MB ID файлу: 1016068115

6.81%
Схожість

Найбільша схожість: 3.36% з джерелом з Бібліотеки (ID файлу: 1015325217)

3.99% Джерела з Інтернету 182 Сторінка 66

4.96% Джерела з Бібліотеки 252 Сторінка 67

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 2