УДК 004.056(477)

Орест-Остап РОМАНЮК

Західноукраїнський національний університет

ІНСТРУМЕНТИ ТА МЕТОДИ МОНІТОРИНГУ ВІДКРИТИХ ДЖЕРЕЛ

Вступ. Розвиток інформаційних технологій і поширення цифрових комунікацій вимагають ефективного моніторингу інформації з відкритих джерел. Вивчення інструментів та методів аналізу опублікованих даних стає все більш важливим у різних сферах, від кібербезпеки до журналістських розслідувань.

Мета: проаналізувати сучасні інструменти та методологічні підходи до моніторингу відкритих джерел, визначити їхню ефективність та особливості практичного застосування в різних галузях.

1. Основні інструменти та методи моніторингу відкритих джерел для виявлення загроз на темному вебу

Дослідження темного вебу та його потенційних загроз становить складну технічну задачу, яка вимагає глибоких знань у сфері кібербезпеки та розвідувальних технологій. Специфіка моніторингу передбачає використання спеціалізованого програмного забезпечення, яке дозволяє здійснювати анонімний доступ та аналіз захищених інформаційних середовищ. Мережа Tor, що є основною інфраструктурою темного вебу, створює додаткові технічні бар'єри для традиційних методів розвідки та моніторингу. Складність полягає в необхідності подолання multiplex-шифрування, яке унеможливлює миттєву ідентифікацію джерел та учасників комунікацій [1].

На рисунку 1 зображено схему взаємодії основних інструментів моніторингу темного вебу. Схема відображає послідовність і взаємозв'язки між компонентами, що забезпечують процес збору, аналізу та обробки інформації з прихованих мереж.

Рисунок 1 - Схема взаємодії інструментів моніторингу темного вебу

Ключовими інструментами для моніторингу темного вебу виступають спеціалізовані краулери та агрегатори інформації, розроблені з урахуванням специфіки анонімних мереж. Серед найбільш ефективних рішень можна виділити програмні комплекси Maltego, Memex, та SpiderFoot, які дозволяють здійснювати комплексний збір та кореляцію розрізнених інформаційних слідів. Технічна архітектура цих інструментів передбачає використання складних алгоритмів машинного навчання для автоматичної класифікації потенційно небезпечного контенту. Принципово важливим є застосування техніки fingerprinting - унікальної ідентифікації інформаційних об'єктів без розкриття первинного джерела [2].

Методологія розвідки темного вебу включає декілька послідовних етапів технічної розвідки. Первинний збір даних здійснюється через спеціалізовані браузери з підтримкою анонімізації, такі як Tor Browser або Tails. Наступним кроком виступає технічна кореляція зібраних інформаційних слідів з використанням штучного інтелекту, здатного розпізнавати приховані патерни

комунікацій. Машинне навчання дозволяє класифікувати потенційні загрози за рівнем ризику, враховуючи контекст, лінгвістичні особливості та мережеву поведінку учасників [3].

На рисунку 2 зображено архітектуру розподіленої системи моніторингу, що складається з таких ключових компонентів:

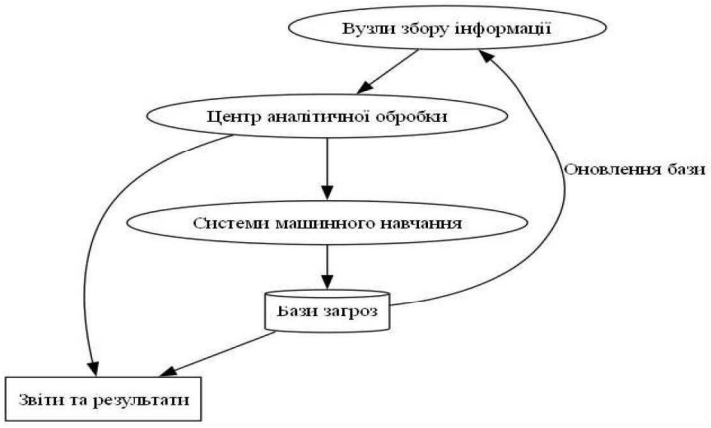

Рисунок 2 - Архітектура розподіленої системи моніторингу

Технічні обмеження традиційних інструментів розвідки спонукають дослідників до розроблення гібридних підходів, що поєднують технології комп'ютерної лінгвістики, нейронних мереж та статистичного аналізу. Принципово новим напрямком є використання квантових алгоритмів для декодування складних криптографічних послідовностей темного вебу, що дозволяє здійснювати більш глибокий аналіз латентних комунікативних каналів. Важливим елементом моніторингу темного вебу є верифікація отриманих даних, що передбачає використання методів перевірки достовірності інформації. Це може включати аналіз метаданих, перевірку джерел та вивчення контексту, в якому інформація була отримана. Застосування технологій блокчейн для фіксації даних про транзакції та комунікації може суттєво підвищити рівень довіри до зібраної інформації. Водночас, важливо враховувати етичні аспекти моніторингу, оскільки анонімність користувачів темного вебу може бути порушена, що викликає питання про конфіденційність та права людини [4].

Окрім того, для виявлення загроз на темному вебу використовуються методи соціальної інженерії, які дозволяють дослідникам отримувати інформацію шляхом взаємодії з учасниками анонімних мереж]. Це може включати створення фальшивих профілів або участь у закритих форумах, де обговорюються незаконні дії. Такі методи вимагають високого рівня обережності та знань про специфіку комунікацій у темному вебі, оскільки будь-яка помилка може призвести до викриття особи дослідника.

На рисунку 3 зображено графік залежності типів загроз, який демонструє взаємозв'язки між основними видами незаконної діяльності, що здійснюється у темному вебі. Важливим є також використання аналітичних платформ, які дозволяють візуалізувати дані та виявляти зв'язки між різними об'єктами. Це може включати графічні інтерфейси, які демонструють мережі взаємодії між учасниками, а також інструменти для аналізу тексту, що дозволяють виявляти ключові слова та фрази, пов'язані з загрозами. Візуалізація даних допомагає не лише виявляти загрози, але й формувати стратегії реагування на них.

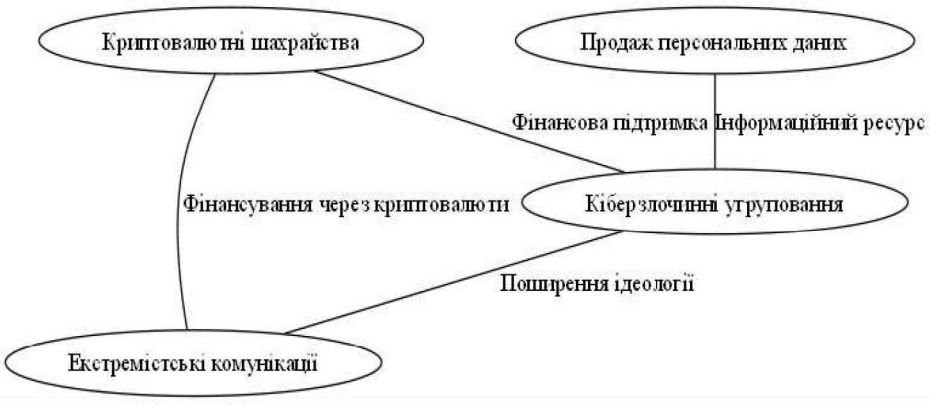

Рисунок 3 - Графік залежності типів загроз

Висновок. Вивчення інструментів і методів моніторингу темного Інтернету показує надзвичайну складність і багатогранність процесу виявлення потенційних загроз в анонімному мережевому середовищі. Технологічний ландшафт сучасної кібербезпеки вимагає постійного вдосконалення підходів до розвідки та аналізу потоків інформації, що циркулюють за межами традиційного інтернет-простору. Еволюція інструментів моніторингу безпосередньо пов'язана з розвитком штучного інтелекту, машинного навчання та квантових обчислювальних технологій. Практичне застосування розглянутих технологій показує, що ефективність моніторингу темного інтернету залежить від комплексного підходу, який поєднує в собі технічні інструменти, алгоритми машинного аналізу і глибоке розуміння деталей середовища анонімного спілкування. Важливою особливістю сучасних розвідувальних технологій є здатність не тільки фіксувати інформаційні сліди, а й прогнозувати потенційний напрямок розвитку загроз. Технічні обмеження, пов'язані з багаторівневим шифруванням та анонімізацією комунікацій, спонукають дослідників постійно вдосконалювати свій методологічний підхід. Інтегруючи різні інструменти, від спеціалізованих сканерів до нейронних мереж, ви можете сформувати більш повне уявлення про обробку інформації в темній мережі. У той же час етичні та юридичні аспекти такого стеження вимагають особливої уваги і дотримання балансу між необхідністю забезпечення безпеки і повагою конфіденційності користувачів.

Перелік використаних джерел.

1. Tiwari, Shiva Verma, Ravi Jaiswal, Janvi Rai, Bipin Kumar. (2020). Open Source Intelligence Initiating Efficient Investigation and Reliable Web Searching. 151-163. 10.1007/978-981-15-6634-9_15.

2. What is Cyber Threat Intelligence? [Електронний ресурс].- Режим доступу: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/?srsltid=AfmBOopOlO5IslR2vDLs_tGLzNMfb2wag82U2IMhQfajoZbRPgbTy6pP

3. Brenner, S. W. (2013). Cybercrime: Criminal Threats from Cyberspace. Routledge. [Електронний ресурс].- Режим доступу: https://ecommons.udayton.edu/cgi/viewcontent.cgi?article=1023context=law_fac_pub

4. Mäntymäki, M., Riemer, K. (2016). Enterprise social networking: A knowledge management perspective. International Journal of Information Management, 36(6, Part A), 1042–1052.