Проєктування та розробка програмного застосунку деанонімізації користувачів у одноранговому протоколі BitTorrent в рамках OSINT-розвідки

Підготував:
Студент групи БК-812м
Д.І. ОРЛОВСЬКИЙ

Керівник:
к.т.н, доцент кафедри ІБтаН
Г.В. НЕЛАСА

АНОТАЦІЯ

- **Об’єкт дослідження** – деанонімізація користувачів у одноранговому протоколі BitTorrent.
- **Предмет дослідження** – одноранговий протокол BitTorrent.
- **Мета роботи** – створити аналітичну систему на основі протоколу BitTorrent, за допомогою якого можна буде проаналізувати завантаження торентів з окремої IP-адреси та провести їх класифікацію по типу. У результаті ми отримали працюючий прототип аналітичної системи, яка може бути використана правоохоронними органами з метою пошуку підозрілої/незаконної активності, прототип власноруч зробленого шпигунського BitTorrent-клієнту. Система реалізована із використанням мови програмування JavaScript, бази даних PostgreSQL та Redis, брокеру повідомлень BullMQ, бібліотеки штучного інтелекту TensorFlow, системи контейнеризації Docker та клієнт сього сайту, написаного із використанням фреймворку NextJS (React).

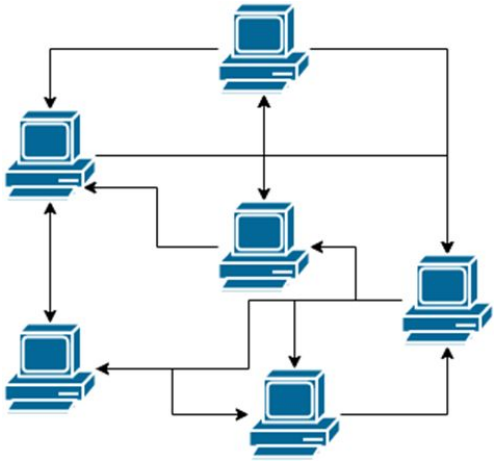
ЗАДАЧА РОБОТИ

1. Ознайомлення з принципами роботи однорангових мереж та протоколу *BitTorrent*
   a. Вивчення функціонування і особливостей протоколу *BitTorrent*.
   b. Аналіз структури та принципів однорангових мереж.
2. Аналіз існуючих методів деанонімізації користувачів
   a. Вивчення методів ідентифікації користувачів в *P2P*-мережах.
   b. Розгляд юридичної практики деанонімізації у правоохоронних органах.
3. Спроектувати програмний застосунок з деанонімізації
4. Створення підробленого *BitTorrent*-клієнту
5. Створення сервера аналітичної системи завантажень в мережі *BitTorrent*
   a. Розробка серверної частини для обробки даних та збору статистики завантажень.
6. Розробка серверу класифікації контенту за допомогою бібліотеки штучного інтелекту *TensorFlow*
   a. Використання технологій штучного інтелекту для класифікації та аналізу даних завантажень.
7. Розробка клієнтського програмного застосунку для моніторингу трафіку у мережі *BitTorrent*
   a. Створення програмного забезпечення для відстежування та аналізу трафіку в *BitTorrent* мережах.

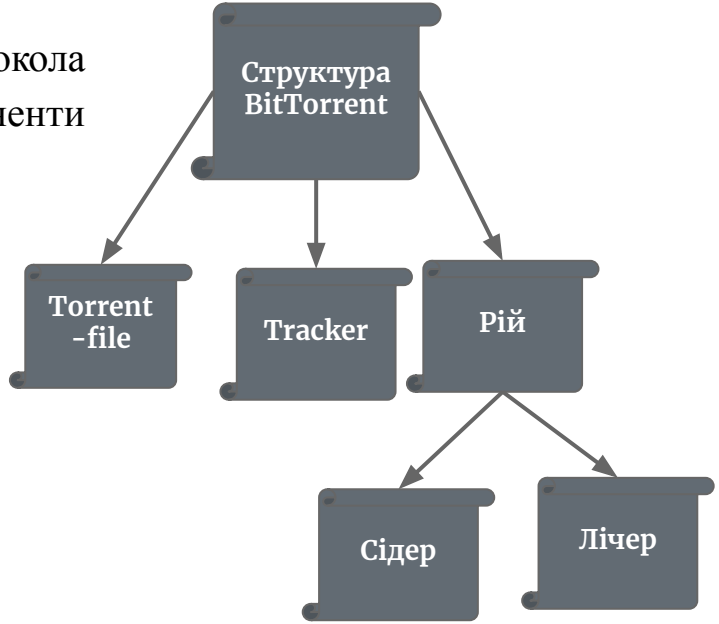
ПРИНЦИП РОБОТИ ОДНОРАНГОВИХ МЕРЕЖ ТА ПРОТОКОЛУ BITTORRENT

Поняття однорангових мереж:

- Клієнт як сервер
- Сервер як клієнт



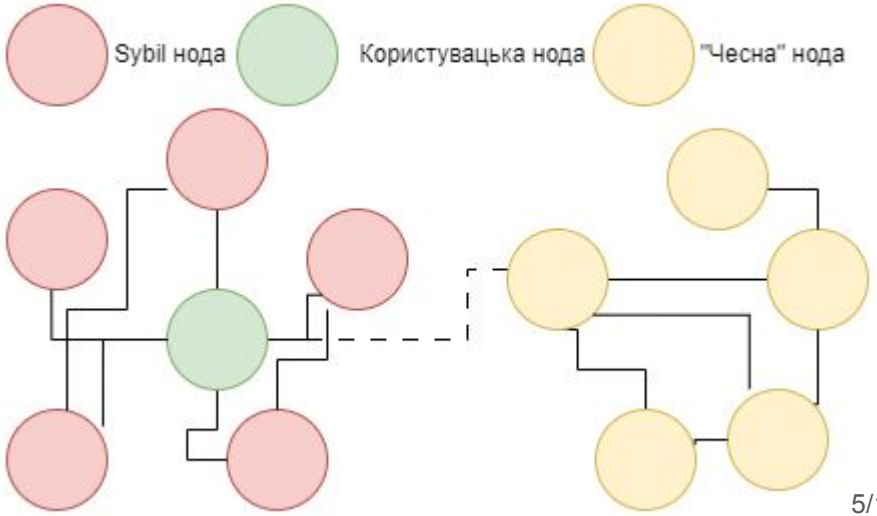
Яка структура протокола BitTorrent? Які компоненти мережі є основними?



МЕТОДИ ДЕАНОНІМІЗАЦІЇ В ОДНОРАНГОВИХ МЕРЕЖАХ

Man in the middle

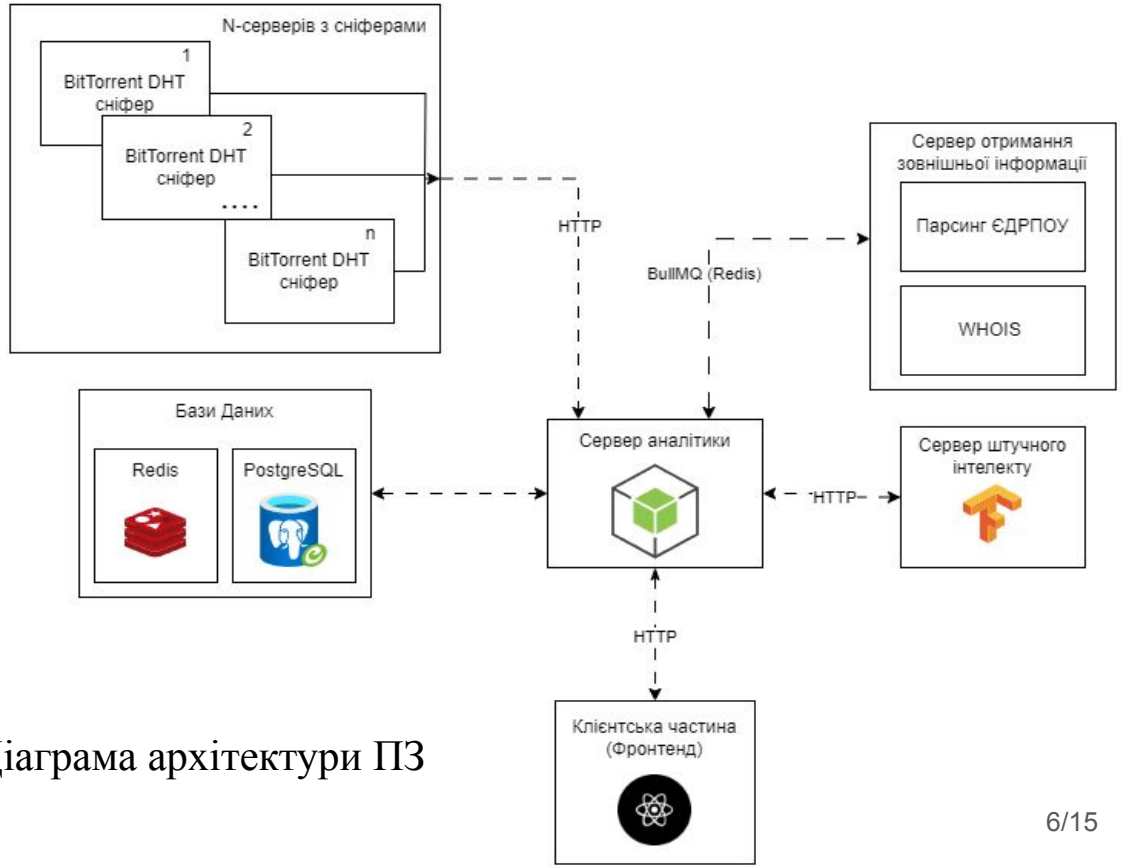
Атака Сивіли



ПРОЄКТУВАННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАСТОСУНКУ З ДЕАНОНІМІЗАЦІЇ

Цільова аудиторія розробки:

Кіберполіція



Діаграма архітектури ПЗ

ЮРИДИЧНІ АСПЕКТИ КОРИСТУВАННЯ МЕРЕЖЕЮ BITTORRENT

Юридичний аспект використання мереж BitTorrent в Україні:

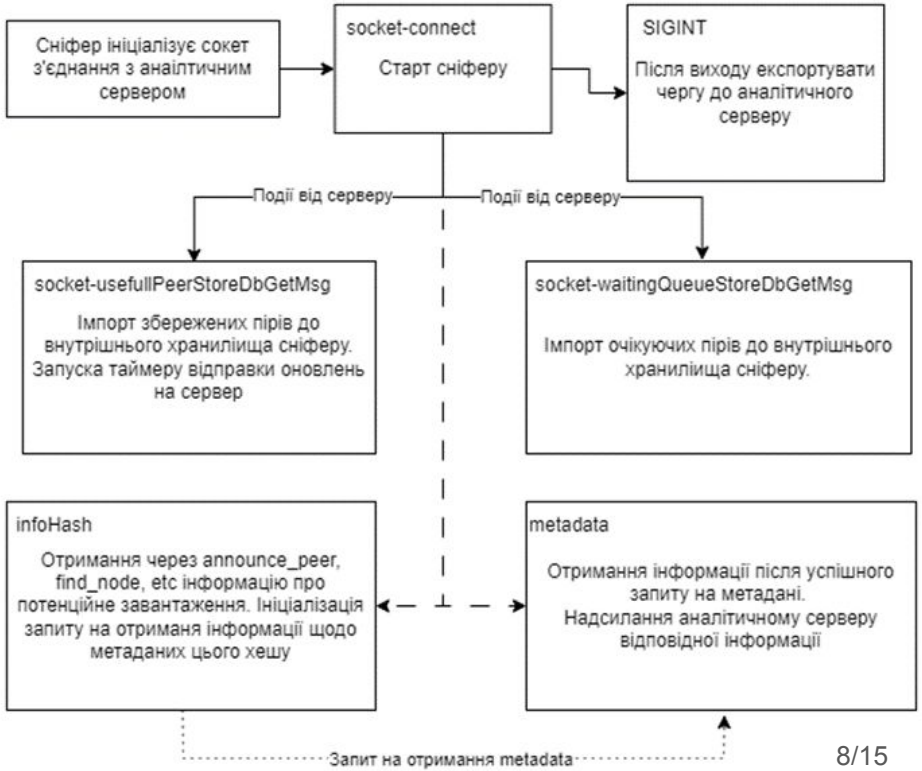
- Регулють використання P2P-мереж:
  - ЗУ “Про авторське право і суміжні права”
  - ЗУ “Про основні засади розвитку”
- Велика частина завантажень - “піратський контент”
- В Україні є кримінальна відповідальність за розповсюдження нелегального контенту
- В Україні є цивільна відповідальність за порушення авторських прав. Провайдери інтернет послуг та розробники ПО повинні забезпечувати захист інформації та дотримання авторських прав

Юридичний аспект деанонімізації мереж BitTorrent в Україні:

- IP адреса може бути прикладом “персональних даних” а може і не бути;
- Згідно судової практики України та ЄС, якщо адреса анонімізована (знеособлена від прив’язки до конкретної особи) то вона не є персональними даними;
- В Україні правоохоронні органи деанонімізують користувачів у рамках досудових розслідувань. Приклад:
  - Кримінальні провадження - 12018040150000125
  - Кримінальні провадження - 12022244000000060

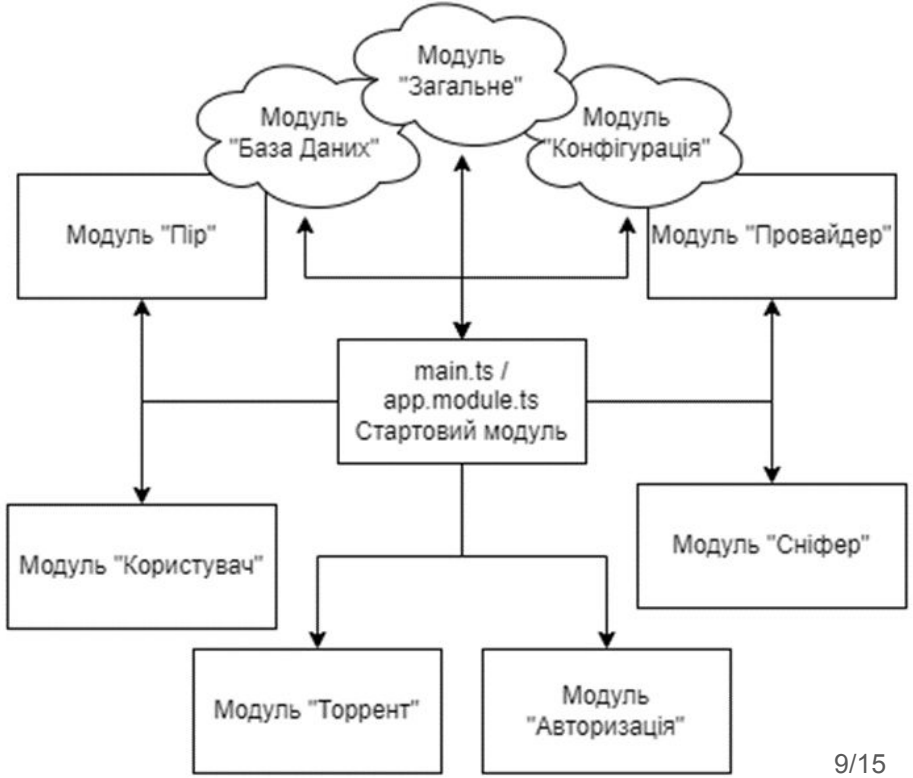
РОЗРОБКА ПІДРОБЛЕНОГО BITTORRENT-КЛІЄНТУ

- Що таке Bencode? Як працює K-RPC?
- Які існують основні переліки DHT-запитів?
- bittorrent-dht - як реалізація на Node JS
- Класс DHTSniffer, як базовий клас сніферу
- Метод ініціалізації та під’єднання до серверу (схема)



РОЗРОБКА АНАЛІТИЧНОГО СЕРВЕРА ДЕАНОНІМІЗАЦІЇ У P2P МЕРЕЖАХ

- “Користувач” / “Авторизація” - збереження сутності користувача та назначення ролі (адміністратор, користувач)
- “Пір” - збереження інформації про IP-адресу
  - З’єднання до сервера зовнішньої інформації (ЄДРПО, WHOIS)
- “Провайдер” - збереження інформації про провайдера отриманого від модуля “Пір”
- “Торрент” - збереження інформації про отриманий торрент-infohash
- “Сніфер” - збереження усіх зареєстрованих сніферів у системі



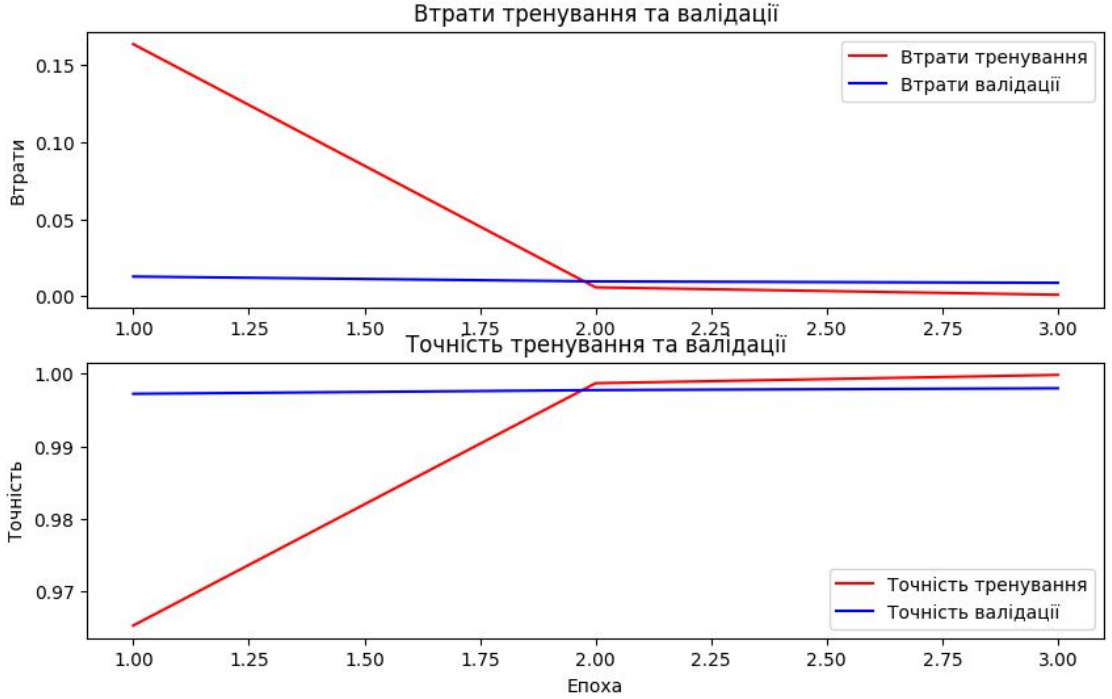
РОЗРОБКА ШТУЧНОГО ІНТЕЛЕКТУ КЛАСИФІКАЦІЇ BITTORRENT: Опис та розробка

Вихідні дані:

- Python
- Tensorflow

Результат:

- Похибка - 0.0086;
- Точність - 0.9979.



РОЗРОБКА ШТУЧНОГО ІНТЕЛЕКТУ КЛАСИФІКАЦІЇ BITTORRENT: Результат

Вісь:

- X - (0 – це Application, 1 – Game, 2 – Movie, 3 – Music, 4 – XXX)
- Y -

```
examples = [
    'fist dsg Repack By', //Game
    'Oppenheimer mkv HDRip', //Movie
    'photoshop iso', //Application
    'queen - show must go on (1975) mp3', //Music
    'assassins creed black flag', //Game
    'OnlyTarts - Eva Elfie - Eva Goes Cheating (18.08.2023) rq.mp4',
//XXX
    'Fding.Afternoon.RePack.by.Chovka', //Game
    ]
```

	0	1	2	3	4
0	0.000242:	0.997953...	0.000092...	0.001642...	0.000069...
1	0.064249...	0.019876...	0.820362...	0.042546...	0.052964...
2	0.965878...	0.014324...	0.003711...	0.000934...	0.015151...
3	9.16e-8	0.002943...	0.000104...	0.996818...	0.000133...
4	0.007652...	0.907288...	0.003647...	0.072493...	0.008918...
5	0.000003...	1.2e-9	3.2e-9	0.000002...	0.999994...
6	0.000077...	0.998613...	0.000030...	0.001248...	0.000029...

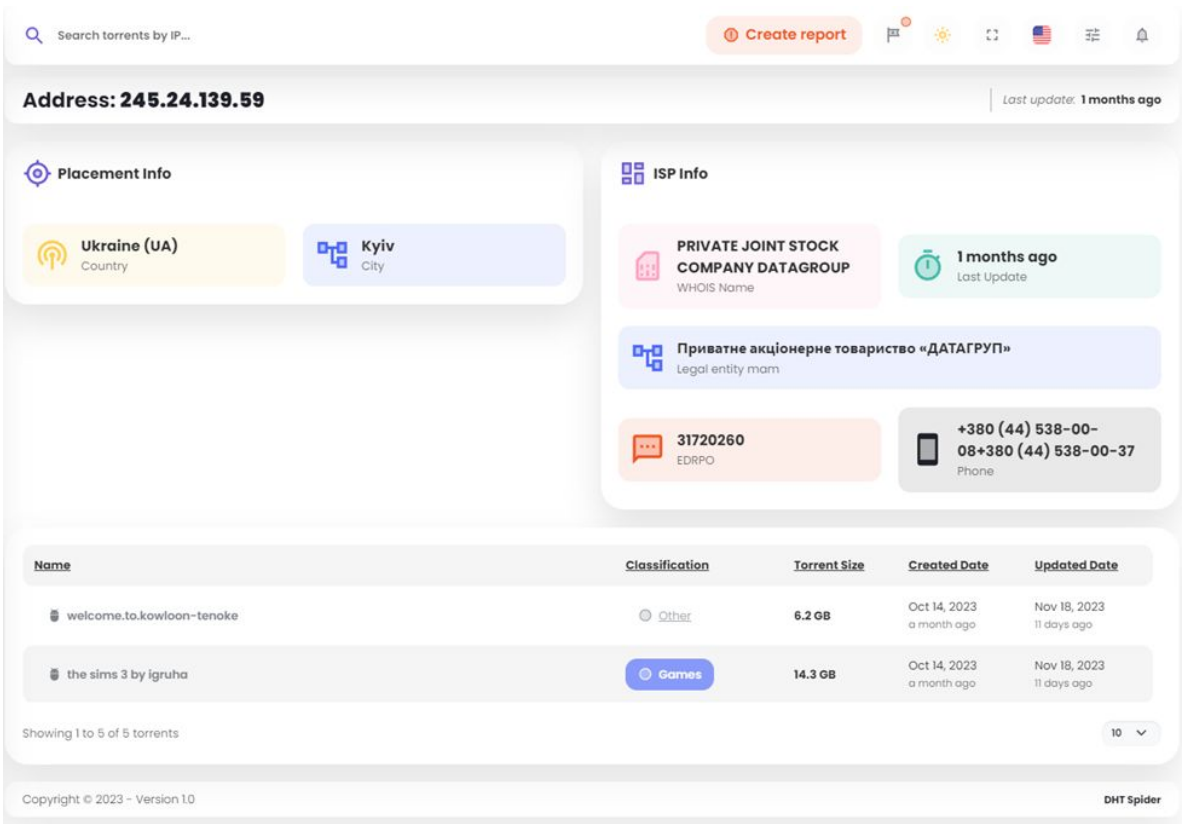
РОЗРОБКА ВІЗУАЛЬНОГО ІНТЕРФЕЙСУ АНАЛІТИЧНОЇ СИСТЕМИ: Основа

React

NextJS

Redux

TypeScript

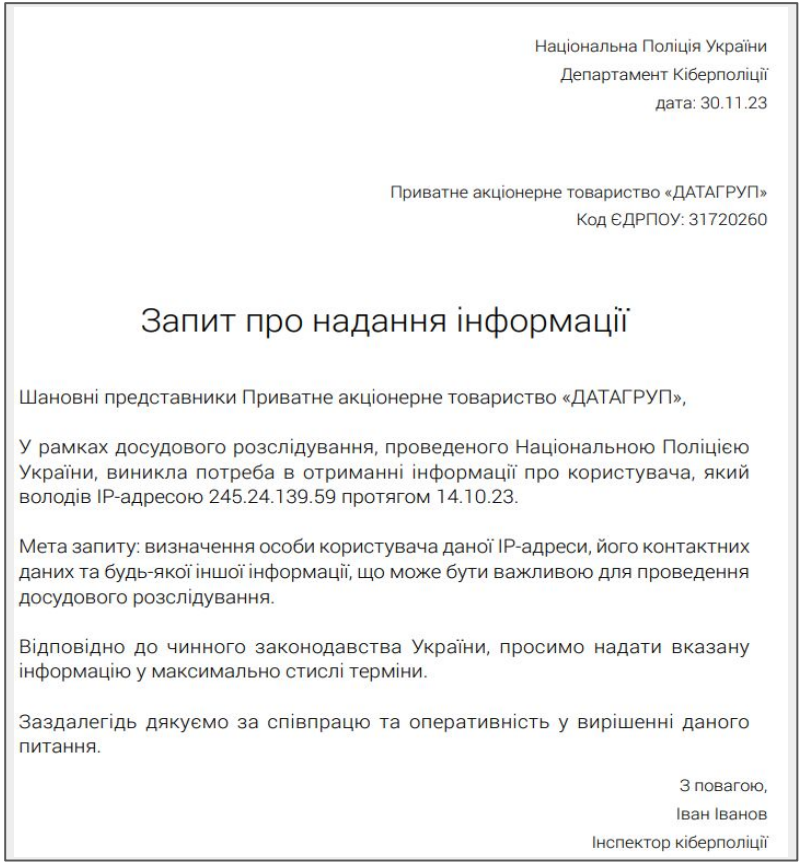


РОЗРОБКА ВІЗУАЛЬНОГО ІНТЕРФЕЙСУ АНАЛІТИЧНОЇ СИСТЕМИ: Звіт

Інспектор має можливість переглянути відповідний звіт за бажаною IP адресою після натиску на кнопку Create report

За натиском на цю кнопку відкривається модалка, після якої надається можливість завантажити звіт за допомогою кнопки Download now!

Після цього користувач отримає необхідний PDF-файл.



Національна Поліція України
Департамент Кіберполіції
дата: 30.11.23

Приватне акціонерне товариство «ДАТАГРУП»
Код ЄДРПОУ: 31720260

Запит про надання інформації

Шановні представники Приватне акціонерне товариство «ДАТАГРУП»,

У рамках досудового розслідування, проведеного Національною Поліцією України, виникла потреба в отриманні інформації про користувача, який володів IP-адресою 245.24.139.59 протягом 14.10.23.

Мета запиту: визначення особи користувача даної IP-адреси, його контактних даних та будь-якої іншої інформації, що може бути важливою для проведення досудового розслідування.

Відповідно до чинного законодавства України, просимо надати вказану інформацію у максимально стислі терміни.

Заздалегідь дякуємо за співпрацю та оперативність у вирішенні даного питання.

З повагою,
Іван Іванов
Інспектор кіберполіції

ВИСНОВКИ

Під час виконання цієї роботи було охоплено ряд ключових аспектів, пов’язаних із проєктуванням та розробкою програмного застосунку для деанонімізації користувачів в однорангових мережах, зокрема використовуючи протокол BitTorrent. Вивчений юридичний аспект користуванян та деанонімізації. Проведено проєктування відповідного ПЗ. Нами було розроблено декілько застосунків, кожен з яких має відповідну мету:

- **підроблений клієнт** - збирання інформації про завантаження користувачів у мережі BitTorrent;
- **аналітичний сервер** - агрегація усієї інформації, координація процесів збору;
    - **сервер отримання зовнішньої інформації** - WHOIS, ЄДРПОУ;
- **сервер штучного інтелекту** - сервер для класифікації торрентів за типом;
- **візуальна частина** - адміністративна панель для представника правоохоронних органів з можливістю генерації звіту;

Таким чином, автором продемонстровані вразливості анонімності користувача у мережі BitTorrent та розроблене ПЗ яке може бути використане правоохоронними органами з метою деанонімізації користувачів.

Дякую за увагу!