ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ВИКРИТТЯ КРИМІНАЛЬНИХ ЕЛЕМЕНТІВ НА ОСНОВІ АНАЛІЗУ АКТИВНОСТІ ІНТЕРНЕТ-СПІЛЬНОТ»

Виконав студент 6 курсу, групи БСЗМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Брянцев Є. О.
(прізвище та ініціали)
Керівник Савченко В.А.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 202__ року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Брянцнцеву Єгору Олеговичу
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія викриття кримінальних елементів на основі аналізу активності інтернет спільнот»
керівник магістерської роботи Савченко Віталій Анатолійович, д.т.н., професор
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «16» лютого 2022 року № 22.

2. Строк подання студентом магістерської роботи 25.05.2022 р.

3. Вихідні дані до магістерської роботи
теоретичні основи інтернет розвідки;
технології та програмні комплекси інтернет розвідки;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми інтернет розвідки.
2. Огляд технологій інтернет розвідки.
3. Перелік графічного матеріалу

1. Тема магістерської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3. Результати аналізу проблеми інтернет розвідки.
4. Результати дослідження технологій інтернет розвідки.
5. Деанонімізація кримінального елементу на прикладі.
6. Структура пророблennої роботи.
7. Опис можливостей розвідки.
8. Рекомендації щодо проведення інтернет розвідки.
10. Висновки за результатами роботи.

6. Дата видачі завдання 16.02.2022 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
Визначення актуальності проблеми інтернет розвідки.	25.10.2022 р	
Аналіз наукової та технічної літератури з питань теми магістерської роботи.	06.11.2022 р	
Аналіз методів та засобів інтернет розвідки.	13.11.2022 р	
Дослідження технологій та програмних продуктів інтернет розвідки.	20.11.2022 р.	
Деанонімізація кримінального елементу на прикладі.	04.12.2022 р.	
Оформлення результатів дослідження. Проходження перевірки на плагіат	15.12.2022 р.	
Підготовка доповіді до захисту.		

Студент Брянцев Є.О.
(підпис) прізвище та ініціали

Керівник магістерської роботи Савченко В.А.
(підпис) прізвище та ініціали

ЗМІСТ

ВСТУП..... 9
РОЗДІЛ 1. АНАЛІЗ СУТНОСТІ ІНТЕРНЕТ РОЗВІДКИ…… 13
1.1. Термінологія та різновиди інтернет спротиву…….. 13
1.2. Види хакерських атак…… 17
1.3. Основні елементи здобуття інформації……... 20
Висновки до розділу 1..... 25
РОЗДІЛ 2. ДОСЛІДЖЕННЯ МЕТОДІВ ПОШУКУ ІНФОРМАЦІЇ…… 26
2.1. Постановка проблеми..... 26
2.2. Розбір інструментів та опрацювання інформації……... 29
2.3. Теорія збору даних…… 32
Висновки до розділу 2..... 35
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТЕХНІК ЗДОБУТТЯ ІНФОРМАЦІЇ ДЛЯ БІЛЬШ ГЛИБОКОГО
АНАЛІЗУ……. 36
3.1. Інтеграція в середовище..... 36
3.2. Збір даних……... 40
3.3. Хактивісти. Деанонімізація…….. 43
Висновки до розділу 3..... 60
ВИСНОВКИ..... 61
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 63
ДОДАТОК А..... 67

РЕФЕРАТ

Текстова частина магістерської роботи: 67 сторінок, 32 зображення, 36 джерел.

Об'єкт дослідження – технологія викриття кримінальних елементів на основі аналізу активності інтернет-спільнот.

Предмет дослідження – дослідження методології пошуку інформації про контакт, людину або певну особу та сопоставлення фактів для створення досьє.

Методи дослідження – було досліджено методології пошуку інформації за допомогою відкритих данних та баз даних.

Мета роботи – Проведення аналізу певних фокусів та факторів для встановлення особистості особ в мережі інтернет.

В роботі проведено аналіз проблеми забезпечення кібербезпеки в інформаційному просторі та визначено мета та завдання викриттям кінцевих точок соціальної структури кримінальної системи. Проаналізовано
існуючі технології викриття інформації в інтернет просторі кінцевих точок соціальної структури кримінальної системи

Досліджено методи та засоби управління захистом кінцевих точок на прикладі викриття хакерського гурту, який наносив інтелектуальну шкоду безпеці України. Визначено призначення, основні функції та склад команди. Визначено призначення, основні функції та принципи роботи рішень та цілей команди. На основі досліджень проведених в роботі розроблено варіант топології системи викриття кінцевих точок соціальної структури кримінальної системи та рекомендації щодо пошуку інформації.

Галузь використання – кібербезпека в інформаційному просторі.

Ступінь новизни одержаних результатів – у ході дослідження було виявлено, що обрану тему не освітлював ніхто до сьогодні, отже ступінь новизни можна оцінювати як оригінальний.

Ключові слова: КІБЕРБЕЗПЕКА, OSINT (Open Source Intelligence), ВІДКРИТІ ДАННІ, НЕСАНКЦІАНОВАНИЙ ДОСТУП, ШТУЧНИЙ ІНТЕЛЕКТ, ДЕАНОНІМІЗАЦІЯ, ЮНІТ, APT (Advanced Persistent Threats)

ABSTRACT

Text part of the master's thesis: 67 pages, 32 figures, 36 sources.

The object of the research is the technology of identifying criminal elements based on the analysis of the activity of the Internet community.

The subject of the study is the study of the methodology of searching for information about a contact, a person or a certain person and compiling facts to create a dossier.

Research methods - the methodology of information search using open data and databases was investigated.

The purpose of the work is to conduct an analysis of certain focuses and factors for establishing a person's identity on the Internet.

The paper analyzes the problems of ensuring cyber security in the information space and defines the purpose and task of exposing the endpoints of the social structure of the criminal system. Analyzed

existing technologies of information disclosure in the space of the Internet are the endpoints of the social structure of the criminal system

The methods and means of managing the protection of endpoints were studied on the example of the exposure of a hacker group that caused intellectual damage to the security of Ukraine. The purpose, main functions and composition of the team are determined. The purpose, main functions and working principles of solutions and the entire team are determined. On the basis of the research carried out in the work, a version of the topology of the system of exposing the endpoint of the social structure of the criminal system and recommendations for information search have been developed.

The field of use is cyber security in the information space.

The degree of novelty of the obtained results - during the research it was found that the selected topic has not been studied by anyone until today, and the degree of novelty can be estimated as original.

Keywords: CYBERSECURITY, OSINT (Open Source Intelligence), OPEN DATA, UNAUTHORIZED ACCESS, ARTIFICIAL INTELLIGENCE, DEANONIZATION, UNIT, APT (Advanced Persistent Threats)

ВСТУП

Сучасний спосіб життя суспільства важко уявити без використання продуктів інформаційних технологій. Кількість користувачів інтернету у світі незабаром досягне позначки половини населення Землі. Інформаційні ресурси впливають головні сфери нашого життя, зокрема і процеси комунікації. Існує думка, що інформація стає головною міжнародною валютою. Але, на жаль, мережеві технології досить вразливі до цілеспрямованих атак. Причому такі атаки можуть здійснюватись віддалено, у тому числі і з-за меж національних кордонів. Деякі сучасні форми бізнесу повністю базуються на мережевих технологіях (електронна торгівля, IP-телефонія, мережевий провайдинг тощо) і тому вони вразливі.

Розуміння того, як здійснюються кібератаки, та зіставлення стратегії захисту підприємства з їх життєвим циклом показують, як можна виявляти, зупиняти та зривати ці атаки, відновлюватися після них та де мають бути посилені операції із забезпечення безпеки. Термін Cyber Kill-Chain спочатку був запропонований корпорацією Lockheed Martin як частина їхньої моделі Intelligence Driven Defense1 для ідентифікації та запобігання процесам кібер-вторгнення. Ця модель визначає, що повинні зробити хакери для того, щоб досягти своїх цілей, атакуючи мережу, виймаючи дані та підтримуючи присутність в організації. Завдяки цій моделі ми знаємо, що блокування хакерів на будь-якому етапі розриває весь ланцюжок атаки.

Першим та основним є етап зовнішньої розвідки. Цей етап можна визначити як фаза вибору мети, виявлення особливостей організації, специфічних вимог у цій галузі, вибір технологій, вивчення активності компанії шляхом використання методів OSINT.

Розвідка на основі відкритих джерел (англ. Open source intelligence, OSINT) – один із методів ведення технічної розвідки за допомогою моніторингу інформації з публічних джерел, її збирання, аналізу та застосування для вирішення певних розвідувальних завдань.

У термінології OSINT існують два важливі визначення:

Відкрите джерело – особа чи група, яка надає інформацію без вимоги збереження її конфіденційності – інформація чи ставлення незахищені від публічного розкриття. Відкрите джерело інформації може бути загальнодоступним, але не вся публічно доступна інформація є відкритим джерелом. Відкриті джерела відносяться до середовища загальнодоступної інформації і не мають обмеження у доступі для фізичних осіб.

Загальнодоступна інформація – дані, факти, інструкції чи інші матеріали, опубліковані чи розміщені для широкого використання; доступні для громадськості; законно побачені чи почуті випадковими спостерігачами; чи представлені на відкритих зустрічах для громадськості.

Приклади відкритих джерел для OSINT:

• засоби масової інформації;

• публічні звіти та заяви уряду;

• Інтернет (соціальні мережі, чати, форуми та ін.)

Соціальні мережі як суспільне явище з'явилися досить давно, але популярність здобули після 1995 року. Початком розквіту цих сервісів прийнято вважати 2003-2004 (були запущені LinkedIn, MySpace, Facebook). Соціальні мережі здебільшого – онлайн-сервіси, що мають на увазі

відображення соціальних взаємин в інтернеті. В результаті таких соціальних взаємодій генерується величезний потік даних, що представляє інтерес для дослідницьких центрів та різних компаній. На даний момент соціальні мережі є одними із найбільших джерел даних в інтернеті.

Соціальні мережі містять величезну кількість інформації, витяг, аналіз та графічне уявлення якої становить інтерес у цій роботі. Як конкретне джерело даних було обрано вітчизняну соціальну мережу ВКонтакте.

У цій роботі робиться припущення про те, що за інформацією, яку користувач породжує та публікує, є можливість досить точно встановити такі дані як: місце проживання або рідне місто, університет, школу та особисті інтереси користувача. Маються на увазі профілі з максимально закритими налаштуваннями приватності. Все, що ми можемо аналізувати у такому разі – список друзів. Не всі друзі користувача знають або вважають важливими налаштування конфіденційності, більша їх частина не обмежує інформацію, яку вони публікують. Тому актуальним є завдання автоматичного збирання, аналізу та візуалізації подібної інформації.

Мета роботи полягає у розробці моделі аналізу інформації на основі технології OSINT, що отримується із соціальних мереж, а також її візуалізації на основі теорії графів та семантичних мереж.

Наукові завдання:

1. Вивчення та аналіз технології Open Source Intelligence для збирання інформації з відкритих джерел; вивчення графових моделей для візуалізації такої інформації.

2. Розробка механізму збору та аналізу інформації із загальнодоступних джерел на основі API ВКонтакте.

3. Вибір суб'єкта оцінювання за необхідними та заздалегідь заданими характеристиками (наприклад, стать, вік тощо).

4. Тематичне моделювання та аналіз активності користувача для оцінки міжособистісних комунікацій.

5. Аналіз виявлення групи (кластерів) друзів користувача з однаковими атрибутами.

6. Виявлення інтересів користувача за допомогою механізмів обробки текстів та ШІ аналізу даних.

7. Побудова графа друзів та кластерів, отриманих на кроці 3.

8. Візуалізація даних на площині.

У першому розділі даної роботи розглянуто поняття аналізу соціальних мереж, соціального графа та вивчено алгоритми їх візуалізації. Також розглянуті алгоритми аналізу текстів природною мовою.

У другому розділі розроблено макет вилучення та аналізу даних із загальнодоступних джерел із позначенням загальновідомого інструментарію для здобуттю та аналізу інформації.

У третьому розділі описана процедура взаємодії із середовищем з використанням позначених у попередніх розділах інструментах та техніках, збір інформації, аналіз дійсного масиву даних, деанонімізація певних осіб та формування звітності.

РОЗДІЛ 1.
АНАЛІЗ СУТНОСТІ ІНТЕРНЕТ РОЗВІДКИ

1.1 Термінологія та різновиди інтернет спротиву

Ціль деанонімізація юніту. Розвідка — це збирання відомостей про супротивника чи конкурента для забезпечення своєї безпеки та отримання переваг у галузі збройних сил, воєнних дій, політики чи економіки.

Open Source Intelligence, більш відома як OSINT, — це технологія, яка стосується загальнодоступних і відкритих джерел інформації (на відміну від таємних або таємних джерел), які використовуються у зв’язку з розвідкою. OSINT – це інформація, яка надходить із публічних та відкритих джерел. Велику кількість оперативної та передбачуваної розвідувальної інформації отримано з відкритих і несекретних джерел. Це означає, що зібрана інформація доступна не лише громадськості для споживання, але й усій розвідувальній спільноті.

Найпоширеніші OSINT-ресурси:

- Пошук метаданих;
- Пошукові системи;
- Соц.медіа;
- Інтернет-спільноти;
- Адреси електронної пошти;
- Імена користувачів;
- Пошукові системи людей;

- Номери телефонів;
- Онлайн карти;
- Пошук коду;
- Документи;
- Зображення;
- Відео;
- Доменні імена;
- IP-адреси;
- Державні та ділові документи;
- Віртуальні валюти;
- Розширені інструменти Linux;
- Геопросторові дослідження;
- Порушення та витік даних.

Рис. 1.1. Ресурси OSINT

Технічно кажуть, що кожен, хто знає, як використовувати ці інструменти та методи для доступу до інформації, використовував цей процес. Однак через технологічні зміни ці методи є мінливими, більшість із них не можуть бути використані будь-ким із знаннями.

Всі ці заходи можуть бути направлені на окремих людей чи їх груп. Певним чином угруповування хакерів або хактивістів іноді назвивають APT (Advanced Persistent Threats) в залежності від обставин та шкоди, яку вони несуть. Це супротивник(и) з сучасним рівнем спеціалізованих знань і значними ресурсами, які дозволяють йому створювати можливості для досягнення цілей за допомогою різних векторів атаки. Сама ж атака APT складна, довготривала та зловмисна, яка, здається, грає в довгу гру, шпигуючи за цільовою інфраструктурою протягом місяців або років, перш ніж успішно зламати мережу.

Рис. 1.2. Життєвий цикл APT

APT-атаки дуже небезпечні. Атаки груп APT є більш витонченими та складними, ніж звичайний злом. Групи APT складаються з висококваліфікованих, здатних і невловимих членів із глибоким технічним досвідом. Мотивація, що стоїть за хакерськими групами, часто фінансова або політична, тоді як мотивація, що стоїть за групами APT, здебільшого стратегічна. Загалом групи APT спонсоруються національною державою або державою, мають набагато кращі та вдосконалені пристрої та вже забезпечені фінансовим забезпеченням.

Атака APT може мати різні цілі. А саме крадіжка коштів або персональних даних; маніпулювання бізнес-процесами, послаблення конкуренції, шантаж і вимагання; крадіжка інтелектуальної власності; спроби зробити політичну заяву або зірвати роботу міської інфраструктури.

OSINT має вирішальне значення для моніторингу загроз:

- Використання OSINT дає нам більш повне уявлення про групи APT.
- Групи APT мають обмежені ресурси та час. Вони можуть повторно використовувати деякі спеціальні інструменти чи інфраструктуру знову і знову.
- Зовнішня розвідка буде корисною.
- OSINT може допомогти нам зіставити свідчення про актора.

Інструменти APT. Інструменти, якими користуються групи APT, більшу частину часу доступні в Інтернеті. Аналіз таких інструментів дає нам чітке уявлення про те, яку зброю використовують угруповання APT і яку стратегію слід розробити, щоб запобігти цим нападам.

Неможливо точно оцінити, скільки коштує APT-атака. Однією з причин є труднощі оцінки унікального програмного забезпечення, яке використовують

злочинні групи. У більшості випадків цим групам APT навіть не потрібно використовувати дорогі інструменти для злому. Наприклад;

Рис. 1.3. Експлойт для продажу в темній мережі

1.2 Види хакерських атак

Фішинг — ефективний спосіб проникнення у внутрішню мережу компанії, який використовують 90 відсотків груп APT. Інструменти для створення шкідливих вкладень, без урахування вартості експлойтів для вразливостей нульового дня, коштують близько 2000 доларів.

Після проникнення у внутрішню мережу половина груп APT використовує законні засоби адміністрування та комерційне програмне забезпечення для тестування на проникнення вартістю від 8 000 до 40 000 доларів США.

Інший варіант APT атак відбувається за допомогою технології DDoS Атак. Цей найнижча ланка в хакерській аудиторії і найдешевша по реалізації до слабких систем, коли проти добрезахищенного ресурсу затрати можуть сягати і 100 000

доларів. Але все ж навіть бюджетна атака в вмілих руках не меньш дієва, ніж соціальна інженерія, тощо.

DDoS Атака (denial-of-service attack), Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

Аналізатори протоколів (sniffers) або Аналізатор трафіку. Також досить поширений вид атаки, заснований на роботі мережевої карти в режимі promiscuous mode, а також monitor mode для мереж Wi-Fi. В такому режимі всі пакети, отримані мережевою картою, пересилаються на обробку спеціальному додатку, званому сніффером. В результаті зловмисник може отримати велику кількість службової інформації: хто, звідки і куди передавав пакети, через які адреси ці пакети проходили. Найбільшою небезпекою такої атаки є отримання самої інформації, наприклад логінів і паролів співробітників, які можна використовувати для незаконного проникнення в систему під виглядом звичайного співробітника компанії.

Mailbombing. Вважається найстарішим методом атак, хоча суть його проста і примітивна: велика кількість поштових повідомлень роблять неможливими роботу з поштовими скриньками, а іноді і з цілими поштовими серверами. Для цієї мети було розроблено безліч програм, і навіть недосвідчений користувач може зробити атаку, вказавши всього лише e-mail жертви, текст повідомлення, і кількість необхідних повідомлень. Такі програми дозволяють ховати реальний IP-адрес відправника, використовуючи для розсилки анонімний поштовий сервер. Цій атаці складно запобігти, так як навіть поштові фільтри провайдерів не можуть визначити реального відправника спаму. Провайдер

може обмежити кількість листів від одного відправника, але адреса відправника і тема часто генеруються випадковим чином.

Атака «людина посередині» (Man-in-the-Middle). Вид атаки, коли зловмисник перехоплює канал зв'язку між двома системами, і отримує доступ до всієї інформації, що передається. При отриманні доступу на такому рівні зловмисник може модифікувати інформацію потрібним йому чином, щоб досягти своєї цілі. Мета такої атаки — незаконне отримання, крадіжка або фальсифікування переданої інформації, або ж отримання доступу до ресурсів мережі. Такі атаки вкрай складно відстежити, оскільки зазвичай зловмисник знаходиться всередині організації.

У реаліях повномасштабного вторнення Росії в Україну місця зіткнення не обмежується водою, повітрям чи суходолом. В час виликого розвитку технологій відкривається новий фронт в кіберпросторі.
На мою думку, Україна має одну най з сильніших сил захисту в інтернеті у світі. Діапозон активності розпливається від звичайної кібергігієни рядового солдата, до відбивання в реальному часі силових атак, та блокування можливості проводити противником нову в том самому місті.

За тлумаченням термін Кібервійна – це комп'ютерне протистояння у просторі Інтернету.
Основні напрямки кібервійни спрямовані передусім на дестабілізацію комп'ютерних систем і доступу до інтернету державних установ, фінансових та ділових центрів і створення безладу та хаосу в житті країн, які покладаються на інтернет у повсякденному житті. Міждержавні стосунки і політичне протистояння часто знаходить продовження в інтернеті у вигляді кібервійни: вандалізмі,пропаганді, шпигунстві, та безпосередніх атаках на комп'ютерні системи та сервери.

Український професор міжнародного права О. О. Мережко визначає кібервійну так: «кібервійна» — використання Інтернету й пов'язаних з ним технологічних і інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній та інформаційній безпеці та суверенітету іншої держави.

1.3 Основні елементи здобуття інформації

Посилаючись до пункту 1.1 Де я писав про найпоширеніші OSINT-ресурси розберемось із алгорітмом дій для виявлення корисної інформації із можливого сегменту масива даних.

Яка початкова інформація для пошуку в нас є – від цього і залежатиме напрям пошуку та вибір інструментів для нього. Загальний OSINT Framework вміщує наступне:

- Username (Ім’я користувача\Нік\Логін);
- Email Address (Емайл Адрес);
- Domain Name (Домейн);
- IP Address (IP Адрес);
- Images / Videos / Docs (Картинки\Відео\Документи);
- Social Networks (Соціальні мережі);
- Instant Messaging (Переписки);
- People Search Engines (Пошукові системи людей);
- Dating (Сховища\Масиви даних);
- Telephone Numbers (Телефонні номери);
- Public Records (Публічні записи);

- Business Records (Корпоративні записи);
- Geolocation Tools / Maps (Гєо-локація та Мапи);
- Search Engines (Пошукові засоби);
- Forums / Blogs / IRC (Форуми, блоги або любий інший сервіс протоколу IRC);
- Archives (Архіви);
- Language Translation (Мовні перекладання);
- Metadata (Метаданні);
- Mobile Emulation (Емуляція мобільного телефону);
- Dark Web ;
- Digital Currency (Цифрова валюта\Транзакції);
- Classifieds (Оголошення);
- Encoding / Decoding (Кодування\Декодування);
- Malicious File Analysis (Аналіз шкідливих файлів);
- Exploits & Advisories (Експлойти та рекомендації);
- Threat Intelligence (Розвідка загроз);
- OpSec (Операційна безпека);
- Documentation (Документація).

Тут і далі так само потрібно діяти від інформації, яку ми маємо, або змогли отримати. Пошук здійснюється як мануально (руками), так і за допомогою штучного інтелекту, або вже готових збірок інструментів для кошуку. Але пошук цим не обмежується, і є більш глубокі координати для заглиблювання в пошуку. Маючи, наприклад IP Адрес ми можемо отримати для себе дуже корисну інформацію:

- Geolocation (Гєо-локація);
- Host / Port Discovery (Хост\Порт);
- IPv4;

- IPv6;
- BGP (Протокол динамической маршрутизации);
- Reputation (Репутація);
- Blacklists (Чорні списки);
- Neighbor Domains (Сусідні домени);
- Protected by Cloud Services (Захист облачних сервісів);
- Wireles Network Into (Безпроводні мережі);
- Network Analysis Tools (Мережеві інструменти аналізу);
- IP Loggers.

І кожну з них потрібно розбирати окремо. Добивати пошуки можна за допомогою програм та сервісів таких як: Shodan, Mr. Looquer, Scans.io, ZoomEye, Nmap (T), Internet Census 2012, Internet Census Search, urtscan.io, Scan less.

Конкретно при знанні безпровідних мереж (або доступу до них) можна торкатись питання WiGLE (відображення бездротової мережі) та OpenCellid (бази даних веж стільникового зв'язку). Також взяти до уваги інструменти:

- Wireshark;
- NetworkMiner;
- Packet Total;
- NetworkTotal.

Якщо питання пошуку торкається якогось бізнесу або компанії, дуже у нагоді буде використання відкритої інформації такої як: річні звіти, загальна інформація та новини, бізнес-записи профілю компанії, профілі та резюме працівників. Для останнього буде у нагоді: RecruitEm, Linkedln, Market Visual, Jobster, XING, Indeed, IntelTechniques Resume Search, CVGadget, LeadFerret.com

Ми торкнулись питання Дарк вебу, але мабуть треба трошки розповісти, що це таке.

Dark web — це вміст загальної мережі інтернет, який існує в даркнетах: накладаються мережі, які використовують Інтернет, але для доступу потрібне спеціальне програмне забезпечення, конфігурації або авторизація. Через темну мережу приватні комп'ютерні мережі можуть спілкуватися та вести бізнес анонімно, не розголошуючи ідентифікаційної інформації, такої як місцезнаходження користувача. Темна мережа утворює невелику частину глибокої мережі, частини Інтернету, яка не індексується пошуковими системами, хоча іноді термін глибока мережа помилково використовується для позначення саме темної мережі. – Це пояснення з Вікіпедії.

Інструметарій для Dark web:

- General Info;
- Clients;
- TOR Search;
- TOR Directories;
- TOR2WEB;
- Discovery (Дослідження).

В дослідженні нам допоможуть (OnionScan, Tor Scan, Onioff, Hunchly Hidden Services Report, docker-onion-nmap)

Простими словами, щоб зайти в дарк веб достатньо мати браузер TOR, та перелік доменів необхідний сайтів зі складним написанням із пошуку по загальному інтернету. Так, як нас в даному випадку можуть зацікавити саме форуми то на цьому тут і зупинимось.

Ще є одна цікава гілка, про яку я хочу додати інформації – це Threat Intelligence або Розвідка Загроз. Вона більше торкається соціального (або людського) фактору, та при доречному користуванні та реалізації – буде дуже у нагоді для розвідки загалом, і для мого дослідження у третьому розділі також.

- Phishing;
- IOC Tools;
- TTPs;
- IBM X-Force Exchange;
- Malware Information Sharing Platform;
- Malware Patrol;
- Project Honey Pot;
- Cymon Open Threat Intelligence;
- Mlsec Project / combine;
- hostintel - keithjjones Github;
- 1 massive-octo-spice - csirtgadgets Github;
- Bot Scout;
- Blueliv Threat Exchange (R);
- APTnotes;
- HoneyDB;
- Pulsedive.

Просто запом’ятаємо про цей пункт, і у третьому розділі повернемось до цього. Єдине ще зазначу – корисні ресурси для фішингу:

- https://openphish.com/feed.txt;
- PhishTank;
- PhishStats.

Висновки до розділу 1

Пошук в інтернеті – дуже великий шар можливостей, а також складний світ реалізації необхідних потреб. Більшість часу необхідно витратити не на сам пошук, а на зачепку, де її взагалі може не бути. Терпіння і винахідливість – товарищи в OSINT. Координати пошуку дуже великі, тому знання і розуміння термінології дуже спрощуватиме роботу в пошуку на методичній основі.

Наперед сам же OSINT потрібен для того, щоб знайти інформацію о місці, заході чи людині (компанії людей) щоб вміти протидіяти загрозливим чинникам, які вони можуть нести.

РОЗДІЛ 2.
ДОСЛІДЖЕННЯ МЕТОДІВ ПОШУКУ ІНФОРМАЦІЇ

2.1 Постановка проблеми

Стрімкий розвиток комп'ютерних мереж та Інтернету породило за собою безліч різних способів атак на них, відповідно питання про методи виявлення аномалій у мережі як ніколи актуальне. Безпека комп'ютерної мережі насамперед залежить від своєчасного та точного виявлення вторгнення та різноманітних атак.

Більшість підходів до виявлення вторгнень у комп'ютерну мережу базуються з урахуванням набору правил, які входять у експертну систему. Системи на основі правил не мають достатньої гнучкості, що є їх істотним недоліком. Експертні системи вимагають частого оновлення, інакше послаблюються можливості системи захисту, а користувачі вводяться в оману щодо захищеності мережі. Подібні системи не здатні виявляти сценарії атак протягом тривалих періодів часу.

Але ми знаємо, що кожен день ці атаки відбуваються і іноді вони можуть заважати звичайному життю пересічної людини. В більшості випадків за різними взломами можуть стояти одні і ті самі люди, самоорганізовані в групи, тощо.

Одна з найпоширеніших проблем для веб-інфраструктури України – це DDoS Атаки, хоч вони не мають грандіозного впливу на хід історії, все ж багато хто прибігає саме до цієї методології так як це найдоступніше із світу кібер атак. В дійсності для того, щоб провести звичайну DoS Атаку, вистачить 10 хвилин, щоб знайти в інтернеті інструкцію так повторити кожен крок.

Із-за популярізації підримуючих поглядів що до війни, в Росії став дуже популярний рух хактивізму. В тривалий термін після початку в п’ять місяців залишились на плаву не багато, однак із за цього вони стрімко набирали аудиторію впродовж останнього часу, і сили від цього їх зросли.

Окрім всіх угрупувань, таких як: Killnet, Заря, інші – я обрав цілью “Народная CyberАрмия”, так як саме вони чи випадково, чи навмисно зачепнули нашу інфраструктуру.

Хто це? Це спілка хактивістів, яких об’єднує жага насильства:

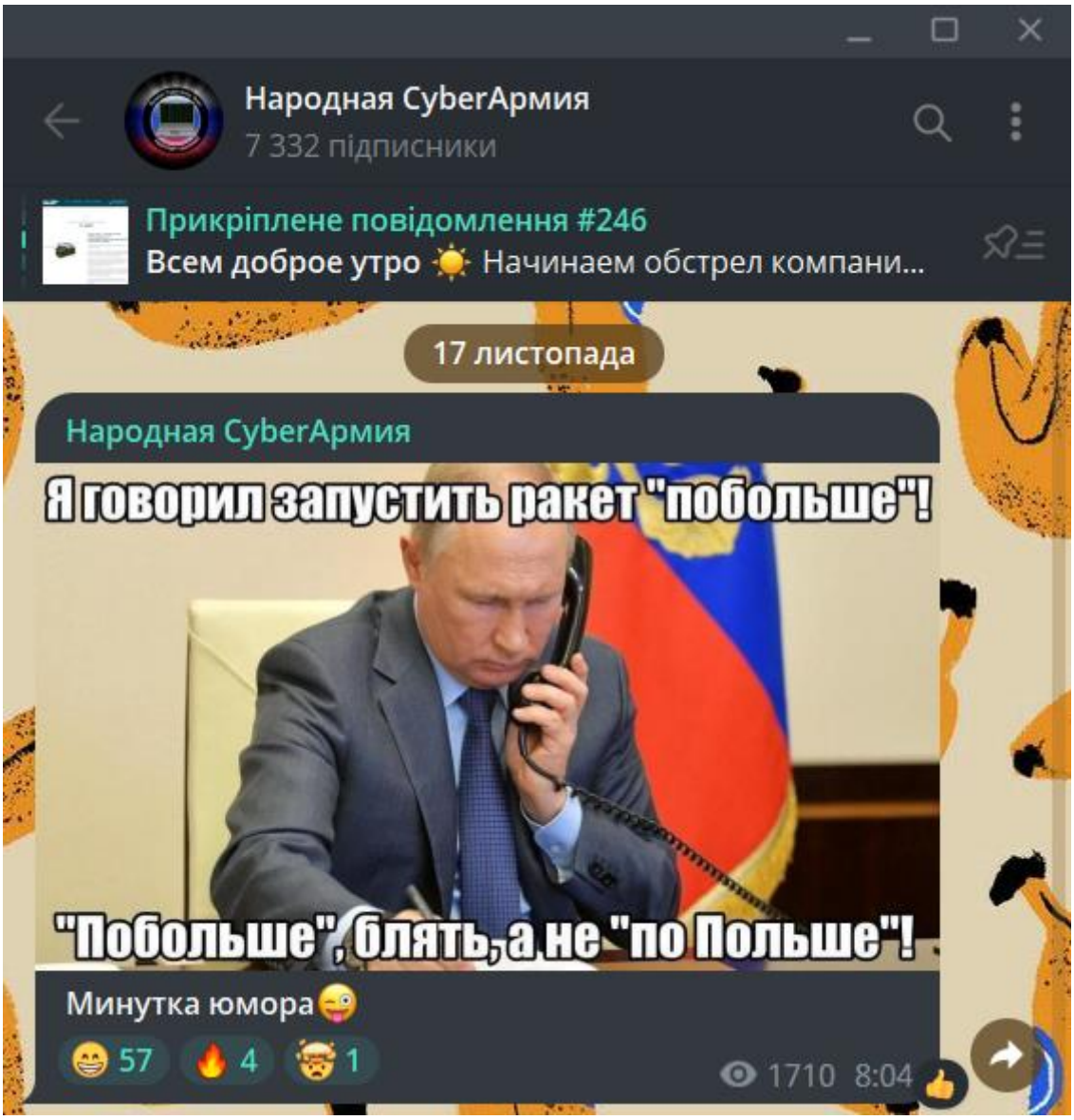


Рис. 2.1. Витримка з каналу “Народної CyberАрмії”

Що вони роблять? Вони проводять DDoS-Атаки та шукають вразливості на сайтах, для того, щоб поміняти головну сторінку та залишити своє повідомлення.

До чого це приводить? Деякі веб-сервіси можуть не відповідати тривалий час. Як звичайний громодянин не може зареєструватись на сайті лікарні, зробити замовлення в інтернет-магазині, в решті решт знайти відповідь на форумі. Для компаній та бізнесів це приводить в необхідності купляти більші пакети захисту Кдауд-сервісів, які спеціалізуються на захисті від DDoS-Атак. Залежно від рівню компанії, ціна за такі послуги може бути не виправданно велика, але і за час простою таким чином компанія втрачає гроші. А якщо все ж таки мати захист, то зловмисник може посилювати свою проможну здатність атаки, тим самим роблячи підприємцю великий чек, який потрібно витратити на клауд-сервіси.

А як це взагалі працює? Тобто що я маю наувазі під цим запитанням. Безкоштовно це все не відбувається, звідки ці хактивісти беруть гроші для поліпшення своїх технік, набирання профільної аудиторії та інше. Так само як вони перейшли від маленьких рейдів “у вечорі” до 24\7. Єдина реклама, яка фігурувала в них в пабліку – Державна. Я маю сміливість припустити, що і фінансуються вони державою.

Але за кожним хактивістом стоїть його минуле, коли він ше не знав терміну “Кібергігієна”.

2.2 Розбір інструментів та опрацювання інформації

Основна інформація, яка поступає для пошуку особи через інтернет – це:

- Фотографія;
- Ім’я або Прізвище;
- Номер телефону.

Це найпростіші ключові дані для пошуку. Так відбувається, коли людина вже є в полі зору служби безпеки, тощо. Інші категорії я розпишу пізніше.

За можливістю почати пошук саме із цієї інформації, потрібно обирати інструменти такі як: пошук по обличчю та відкриті\оприлюднені бази даних.

Пошук за обличчям: Це можна робити ручками, якщо є відома інформація про життя людини, її місто народження або дату народження. Для цього добре підійдуть соціальні мережі (Вконтакте, Одноклассники, Фейсбук, Майл.ру, Інстаграм, Тік-ток)

Рис. 2.2. Штучний інтелект пошуку облич

Але також є штучний інтелект, який аналізує людське обличчя та знаходить схожі в інтернеті (pimeyes.com, nec.com, tineye.com).

Бази данних для пошуку по імені, призвищу та номеру телефону можна знайти де завгодно. Починаючи від OpenDataBot, українського реєстру, до DarkWeb на форумах де хтось може виставити конкретну базу на спільний доступ або на продаж.

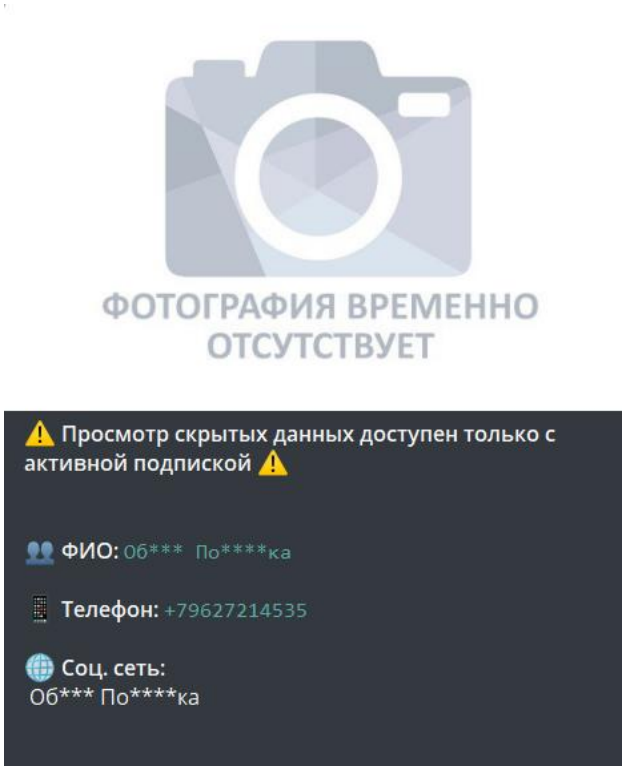


Рис. 2.3. Штучний інтелект пошуку облич

Велика кількість ботів в телеграмі, які налаштовані на бази різних систем та корпорацій, які одного часу просто прогледіли вразливість в своїй архітектурі. Це, загалом, стається із-за “браку” фінансування на інтернет-заходи, та необізнонасті керівництва. Можу припустити, що це саме аудиторія РФ таким може похизуватись, тому у цьому мені пощастило.

Для роботи в напрямку розвідки, для створення хронологій, дерев взаємодій, ієрархій – дуже зручний застосунок Maltego. В ньому купа різних функцій і фішок для пошуку та здобуття інформації. За останні роки він став дуже потужним, але є декілька “Але”:

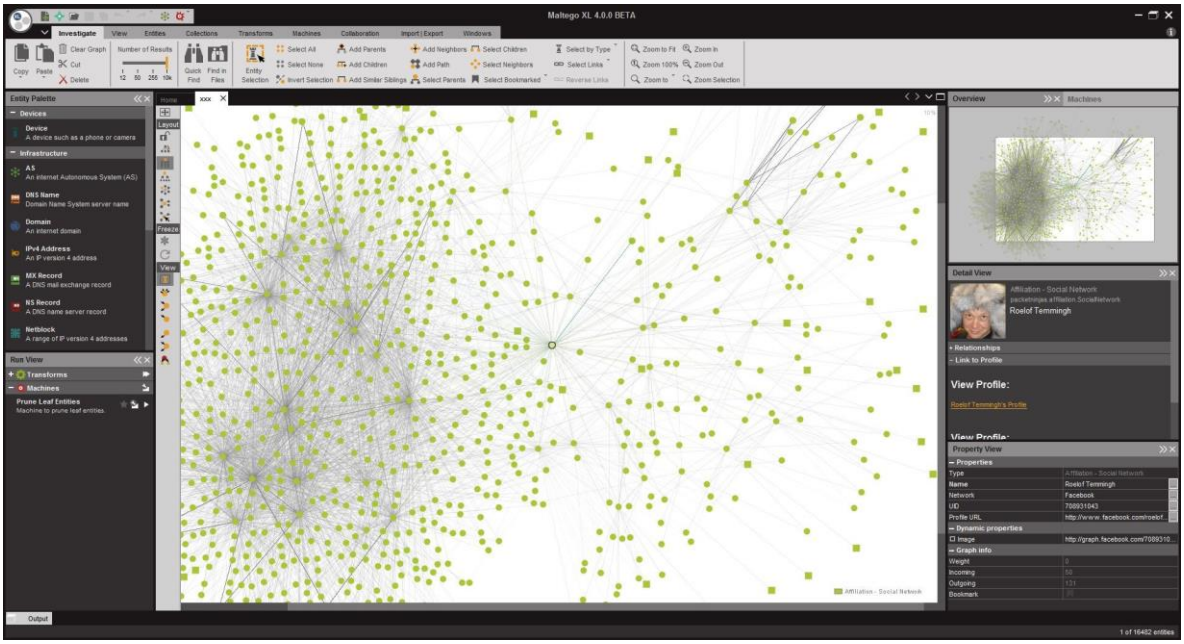
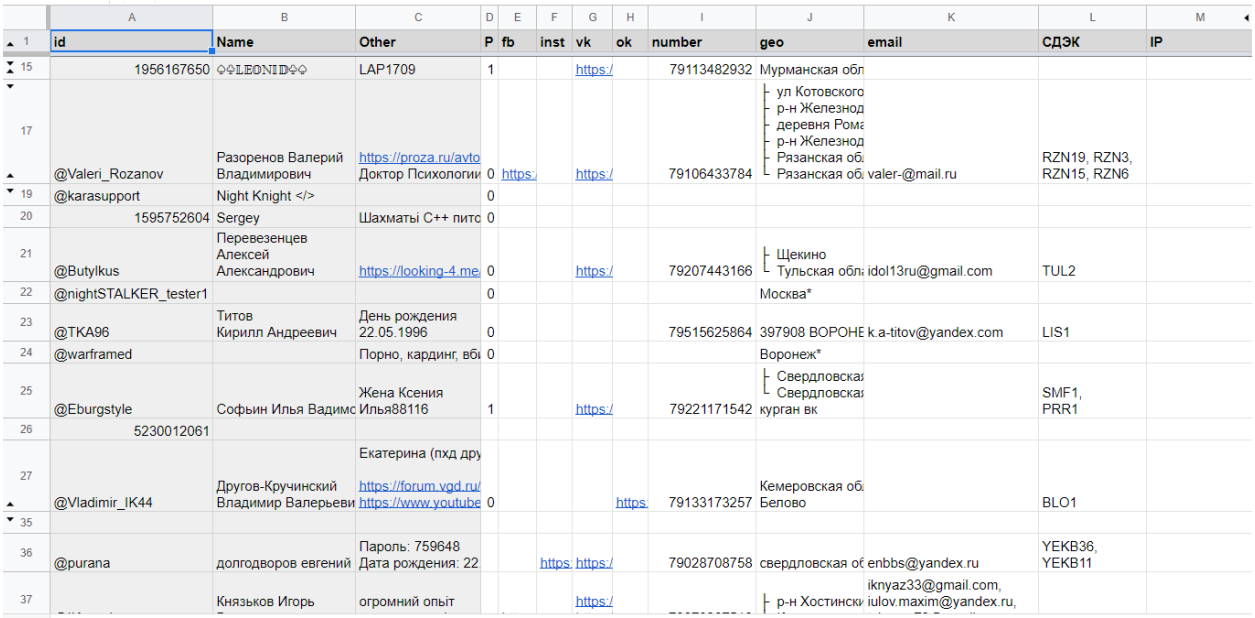


Рис. 2.4. Робоча зона Maltego

Вона платна, її функціонал в безкоштовінй версії достатньо урізаний. Вона більше направлена на західну культуру, а з російським “контєнгєнтом” вона працює не ідеально. Та і зручна вона лише коли дуже багато зв’язків. Тому беру на себе особисту сміливість робити все в Google-Doc, а всі хронології тримати в голові.

Є спойлер, який вигляд воно матиме замість інтерфейсу Maltego:



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	id	Name	Other	P	fb	inst	vk	ok	number	geo	email	СДЭК	IP
15	1956167650	♤♤LEONID♤♤	LAP1709	1			https:/		79113482932	Мурманская обл			
17	@Valeri_Rozanov	Разоренов Валерий Владимирович	https://proza.ru/avto Доктор Психологии	0	https:		https:/		79106433784	├ ул Котовского ├ р-н Железнод ├ деревня Рома ├ р-н Железнод ├ Рязанская об └ Рязанская об	valer-@mail.ru	RZN19, RZN3, RZN15, RZN6	
19	@karasupport	Night Knight </>		0									
20	1595752604	Sergey	Шахматы C++ пито	0									
21	@Butylkus	Перевезенцев Алексей Александрович	https://looking-4.me	0			https:/		79207443166	├ Щекино └ Тульская обл	idol13ru@gmail.com	TUL2	
22	@nightSTALKER_tester1			0						Москва*			
23	@TKA96	Титов Кирилл Андреевич	День рождения 22.05.1996	0					79515625864	397908 ВОРОНЕ	k.a-titov@yandex.com	LIS1	
24	@warframed		Порно, кардинг, вб	0						Воронеж*			
25	@Eburgstyle	Софьин Илья Вадимс	Жена Ксения Илья88116	1			https:/		79221171542	├ Свердловска └ Свердловска курган вк		SMF1, PRR1	
26	5230012061												
27	@Vladimir_IK44	Другов-Кручинский Владимир Валерьеви	Екатерина (пхд дру https://forum.vgd.ru/ https://www.youtube	0				https:	79133173257	Кемеровская об Белово		BLO1	
35													
36	@purana	долгодворов евгений	Пароль: 759648 Дата рождения: 22			https	https:/		79028708758	свердловская об	enbbs@yandex.ru	YEKB36, YEKB11	
37		Князьков Игорь	огромный опыт				https:/			├ р-н Хостински	iknyaz33@gmail.com, iulov.maxim@yandex.ru,		

Рис. 2.4. Робоча зона Google Spreadsheets

2.3 Теорія збору даних

І так, методологія дій. В основі і в ідеалі виглядає таким чином:

1. Я лажу і дивлюсь всі коментарі по сепаратистьских каналах по типу “Вставай Домбас”, “Херсон – русский город”, “Партизаньі Днепропетровска”, і так далі.
2. Беру перший же цікавий мені коментар першого цікавого мені профілю.

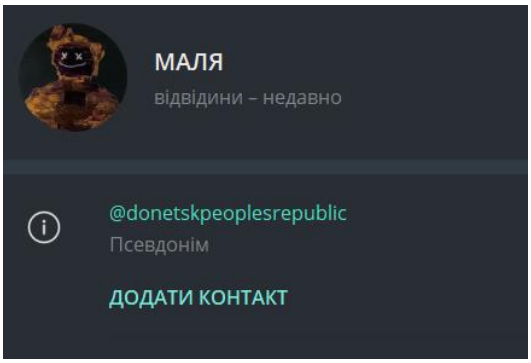


Рис. 2.5. Телеграм профіль умовного сепаратиста

*Зараз фотографія профілю дещо відрізняється. Коли я знайшов його, на аватарці був молодий парубок в військовій формі, з шевроном “ДНР” та закритим обличчям.

3. Дивлюсь по своїх все перевірених базах активність телеграм аккаунту в надії знайти шось цікаве:

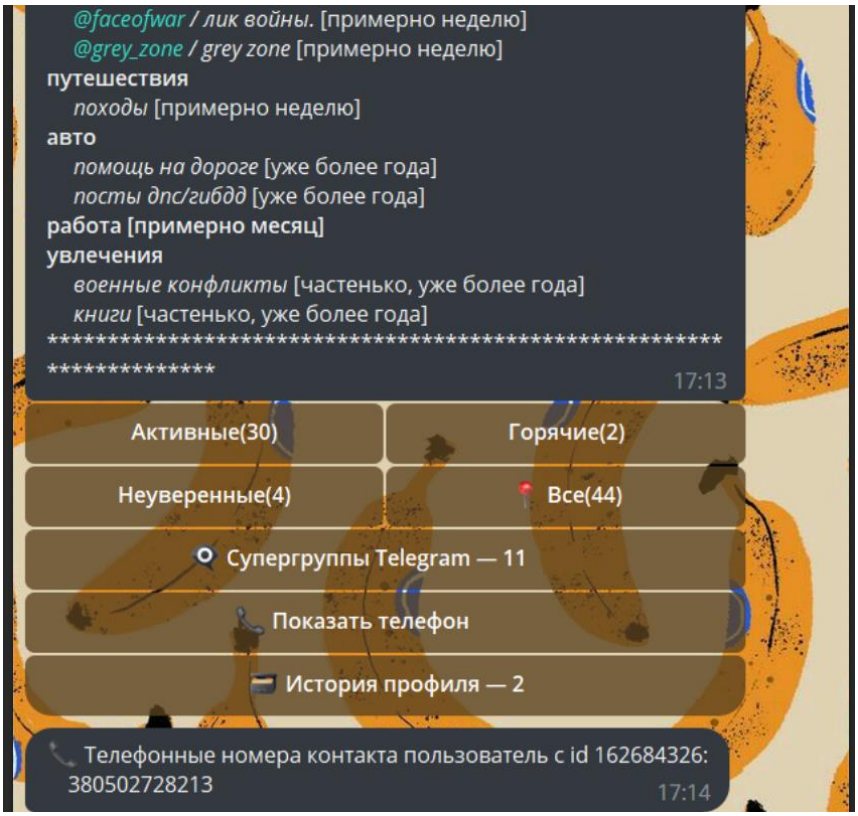


Рис. 2.6. Аналіз телеграм профілю

4. Знаходжу.

В ітозі я маю український номер телефону: 380502728213. Як так склалось? За замовчуванням в телеграмі (або так було раніше) стоїть демонстрація вашого номеру телефону у світ. Тобто люба людина може зайти на ваш профіль і його побачити. Цей унікум продовжував спілкування в чатах та каналах із відкритим номером телефону тривалий час, від чого і потрапив випадково до бази даних.

Але має бути інший крок.

5. Тепер шукаю, кому належить номер телефону:

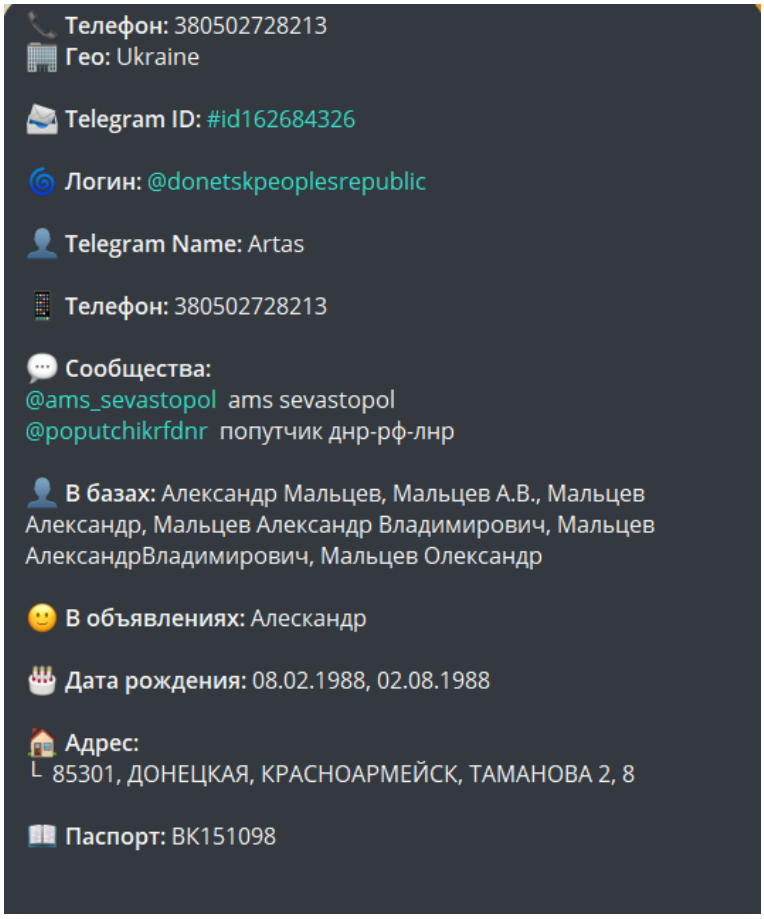


Рис. 2.7. Аналіз власника номера телефону

*Зрозуміло, робота в базах означає якісь програми для цього. Я вже відійшов від кроносів і це мій власний вибір працювати через телеграм, бо телеграм доступний і з телефону.

Все. Загалом це вся інформація, що мені потрібна для передачі її куди варто. Якщо мені потрібно знайти обличчя людини, я копіюю її ім’я, і іду в Вконтакте або Одноклассники.ру і в 9 з 10 випадків швидко знаходжу людину. Далі вже частка відсотку, що людина немає профілю.

Але так просто буває не завжди. Іноді ні номеру телефона, ні імені я не знаю разом з базою даних, і доводиться шукати і читати всі повідомлення людини залишені в відкритих чатах або каналах для отримання хоч якоїсь зачепки. Якщо абсолютно нічого немає, доводиться якось викручуватись. Наприклад, як один з напрямків, що я розписував вище – Фішинг.

Я слідкую за людиною, і пробую наладити з нею контакт. Якщо вона знаходиться в Україні, мені достатньо IP Адреса. Тому в такому випадку відправляю IP-Logger прикритий якимось дійсним посиланням.

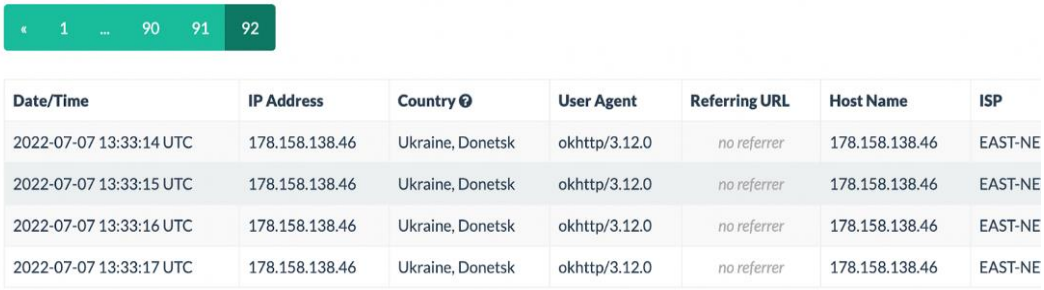


Рис. 2.8. Статистика IP Logger

Висновки до розділу 2

Світ не ідеальний, як і люди в ньому. Нажаль, навіть звичайна бабушка може виявитись шпигункою кремля. Однак в епоху цифровізації майже весь світ дублюється або продовжується в інтернеті, а це вже привід навчитись користуватись інструментами та навичками пошуку інформації.

РОЗДІЛ 3.
РЕАЛІЗАЦІЯ ТЕХНІК ЗДОБУТТЯ ІНФОРМАЦІЇ ДЛЯ БІЛЬШ ГЛИБОКОГО АНАЛІЗУ

3.1 Інтеграція в середовище

Випадково я побачив новину на телеграм каналі російських хактивістів про пошук дизайнера для створення логотипу, і вирішив почати діяти, бо краще нагоди годі і шукати. Так і потрапив в їх закритий спільний чат. Я представився тим, кого вони шукали, і ожливо із-за цього вони були менш обачливими і перешли за посиланням на “резюме” так званого дизайнера.

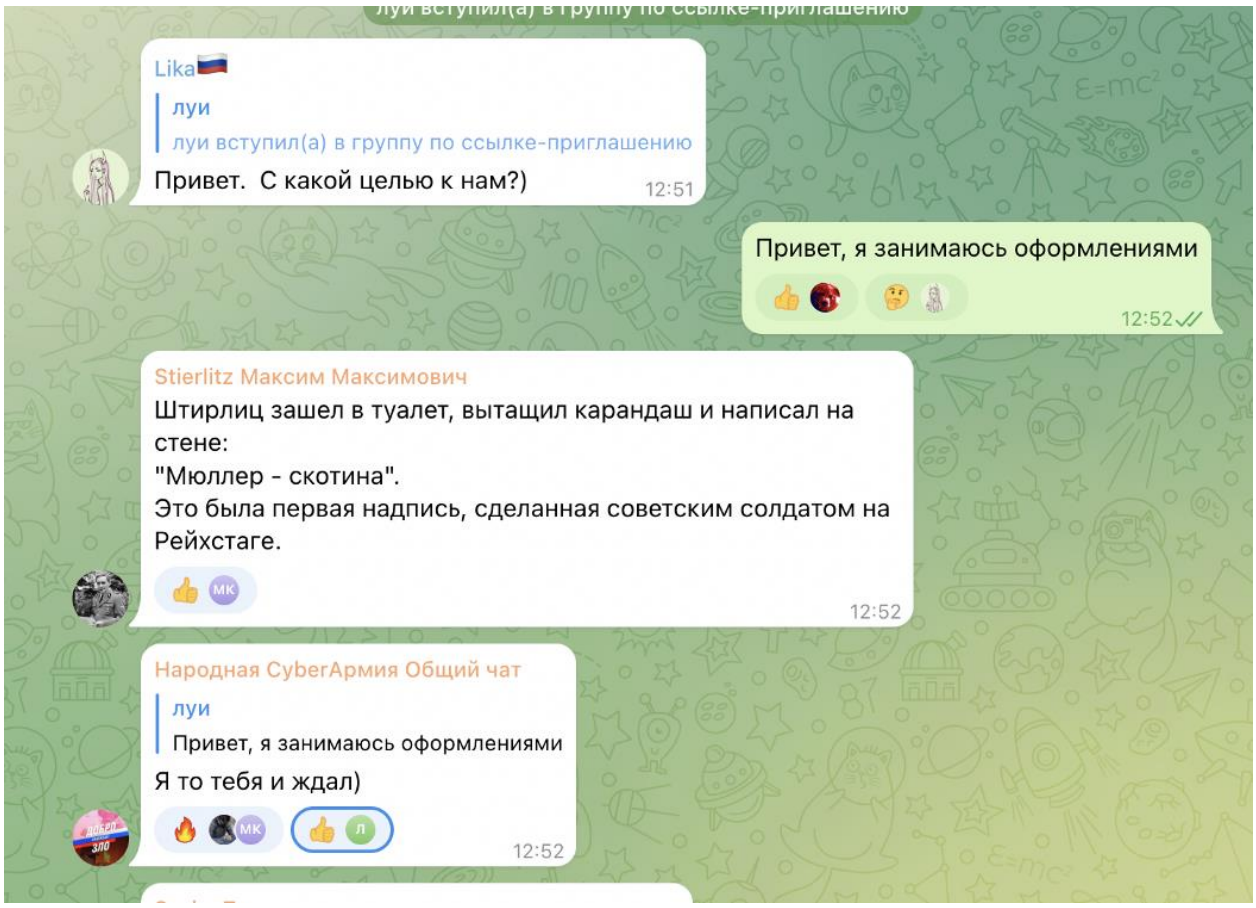


Рис. 3.1. Чат “Народной CyberАрмии”

Рис. 3.2. Чат “Народной CyberАрмии”

2022-07-07 12:00:07 UTC	94.233.102.19	Russia, Kamyshin	Mozilla/5.0 (iPhone; CPU iPhone OS 14_7_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1	no referrer	dsl-94-233-102-19.vlz.ru	Rostelecom	More Info
2022-07-07 12:00:51 UTC	95.105.125.226	Russia, Orenburg	Mozilla/5.0 (X11; Linux x86_64; rv:101.0) Gecko/20100101 Firefox/101.0	no referrer	95.105.125.226.dynamic.o56.ru	JSC Ufanet	More Info
2022-07-07 12:01:41 UTC	188.244.191.130	Russia, Yakutsk	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36	no referrer	188.244.191.130	Limited Liability Company TTK-Svyaz	More Info
2022-07-07 12:02:17 UTC	79.142.66.229	Netherlands, Schiphol-Rijk	Mozilla/5.0 (Linux; Android 12; SAMSUNG SM-G998B) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/17.0 Chrome/96.0.4664.104 Mobile Safari/537.36	no referrer	79-142-66-229.equinoxservers.nl.switchlayer.com	AltusHost B.V.	More Info

Рис. 3.3. Частина зафіксованих переходів по ссилці

Не менш дивним виявилося, що у посиланні був айпілогер, який засвітив місце перебування власника кліку на резюме.

Ними виявилися координаторка дудосів, технічний інженер, який вчить громаду створювати атаки, і просто Євген Капітанець, але про всіх трохи згодом (Звідки я знаю, що саме вони? Це я відслідкував у розмові в чаті).

За кілька годин прикриття все ж стало шатким, але гра у шпигунів була продовжена. Як же так? Здається, було б дивно спрямовувати DDoS-атаку на звичайне посилання, але все ж це сталося. І навіть якщо брати за основу дійсний намір, відповідь залишається за рамками. Таким чином, ми отримали IP-адреси учасників Народної CyberАрмії, ймовірно core-team.

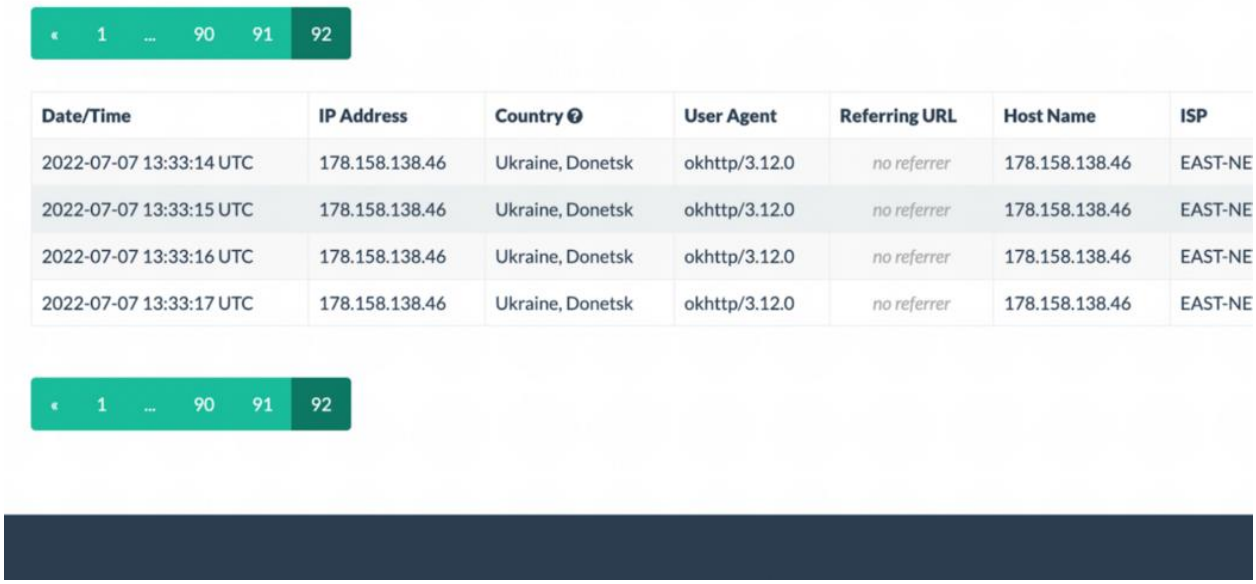


Рис. 3.4. Частина зафіксованих переходів по ссилці

Ось що сталося із статистикою переходів. Таким чином були зібрані всі адреса, з яких вони ведуть атаки на веб-інфраструктуру України. Але всяке буває, підемо далі. Десь через півгодини з інсайдером був продовжений контакт від імені “командуючого”:

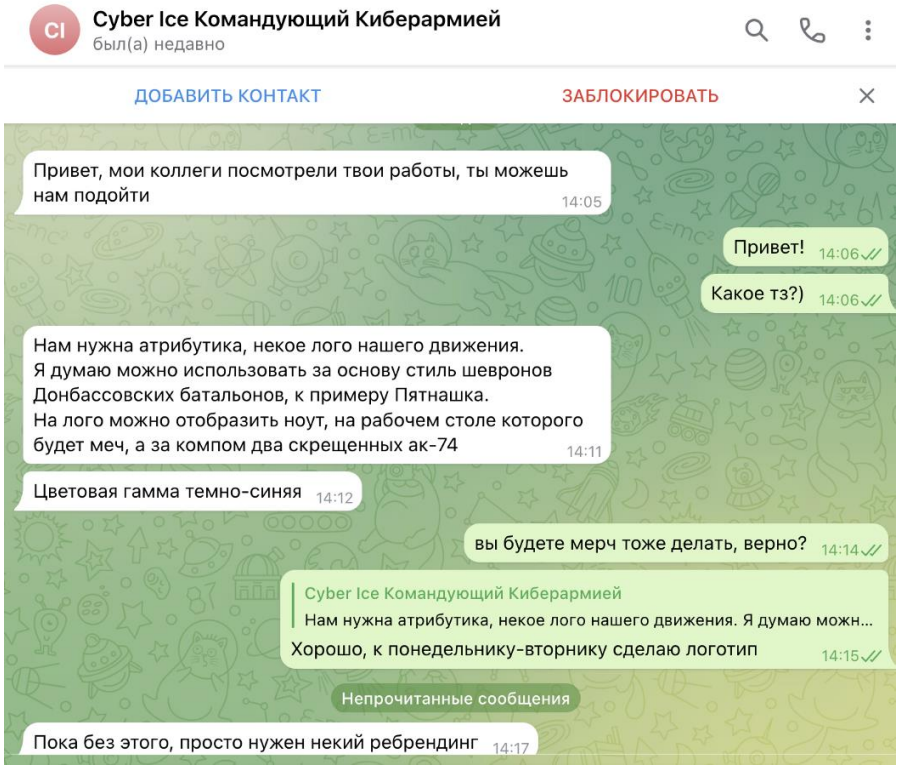


Рис. 3.5. Діалог з представником команди угрупування

Рис. 3.6. Діалог з представником команди угрупування

Також одним із червоних маркерів про “гру в шпіонів” свідчить невдала спроба зустрічного ір-логування (зверху і знизу різні посилання. І нащо переходити, коли є прев’ю?). І що ж, це була п’ятниця, тому сміливо пообіцяли знов зв’язатись у понеділок, на цьому розійшлись.

3.2 Збір даних

Але робота тільки починалась, тому що треба було з’ясувати, що там всередині спілки хактивістів відбувається… А нічого цікавого. Жарти про Україну, пусті бесіди, еротика, обговорення, хто що з’їв та скільки випив. А потім статистика із Call of Duty. Виглядає, як їх домашнє кубло, де вони немов давні друзі.

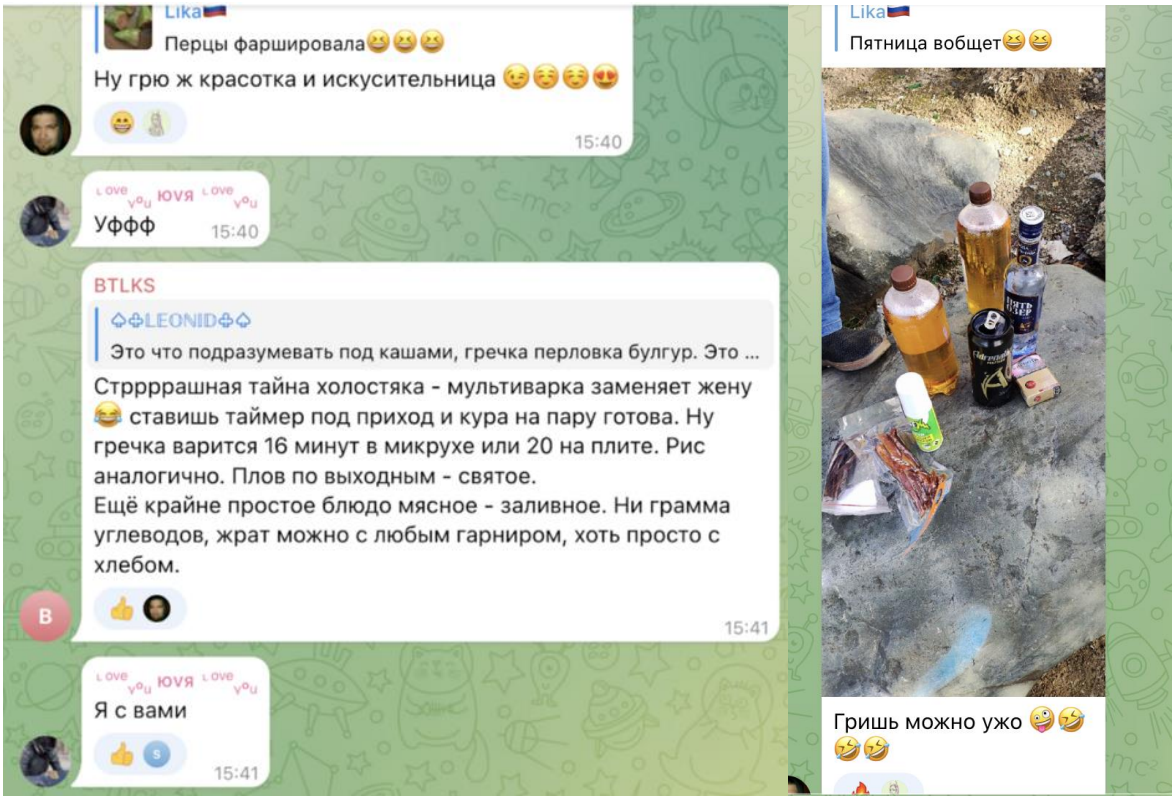


Рис. 3.7. Витримки із чату

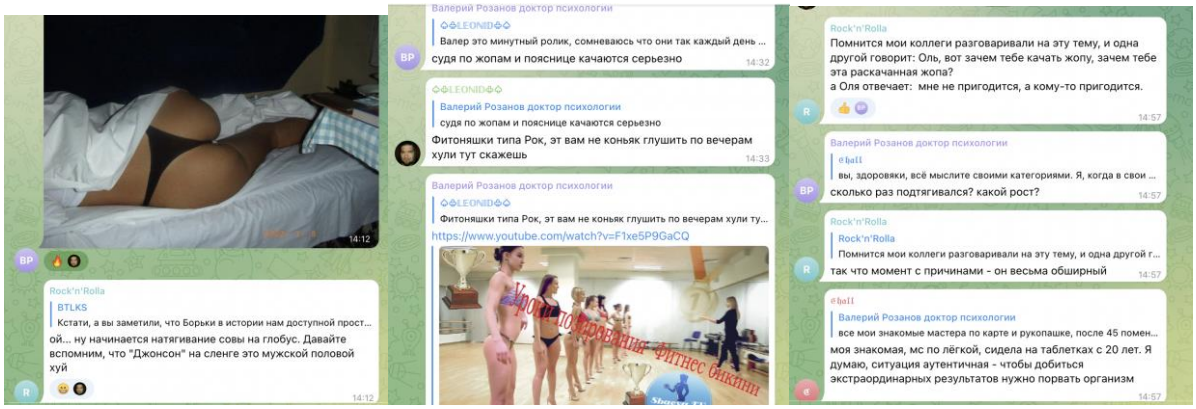


Рис. 3.8. Витримки із чату

Рис. 3.9. Витримки із чату

А ось вже останній скріншот більше цікавий для нас. Вони не забувають продемонструвати свої тайм зони у скрінах, а також іноді називають одне одного справжніми іменами:

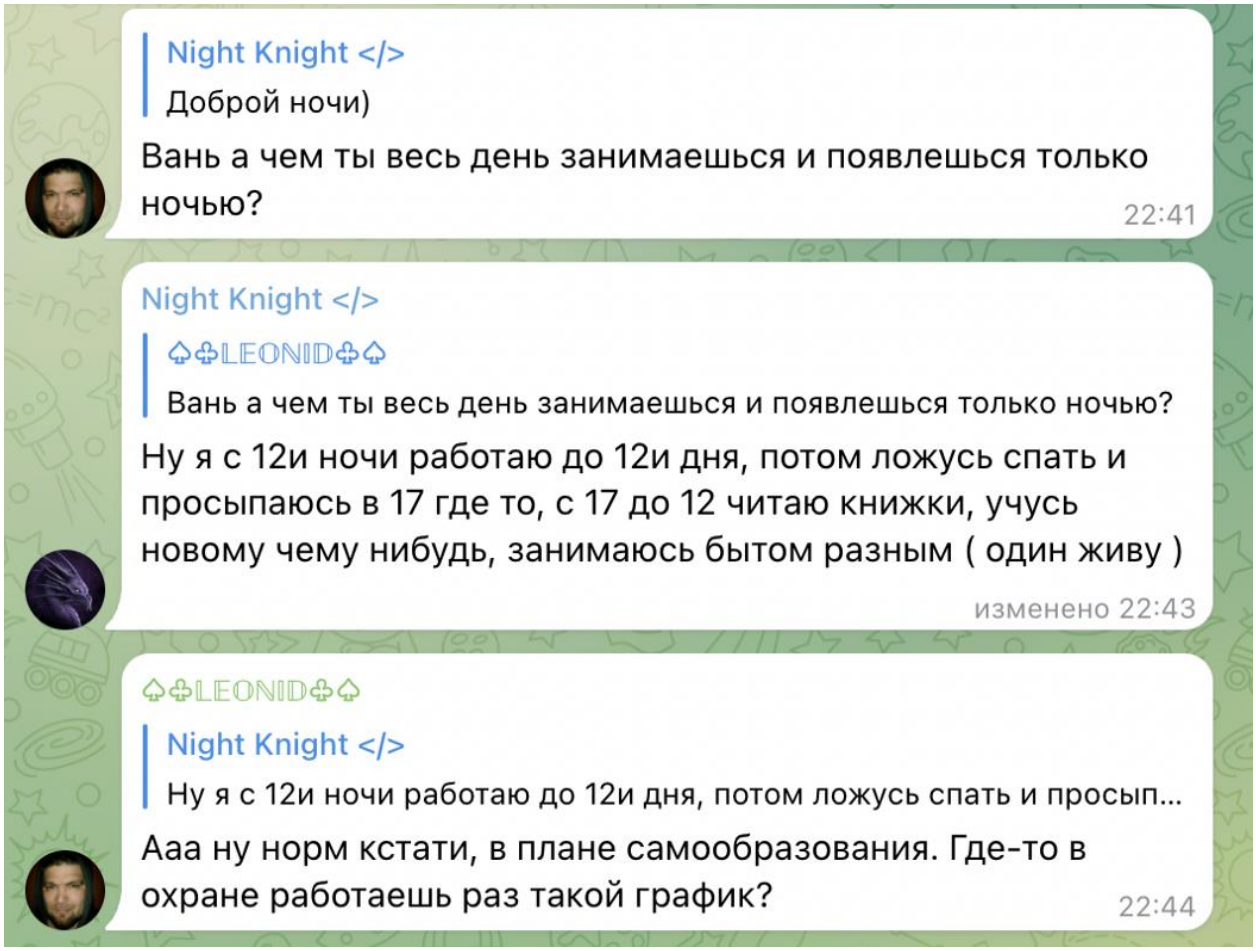


Рис. 3.10. Витримки із чату

Дійсно, де ще може працювати російский хактивіст, як не в охороні чи на заводі. Втомлюються очі читати тонни інформації про їх життя та слідкувати за їх пустими діалогами, але ми це зробили. Отже, з усього активного ком’юніті в чаті є приблизно 50 осіб, і з частиною їх пропонуємо познайомитись:

3.3 Хактивісти. Деанонімізація

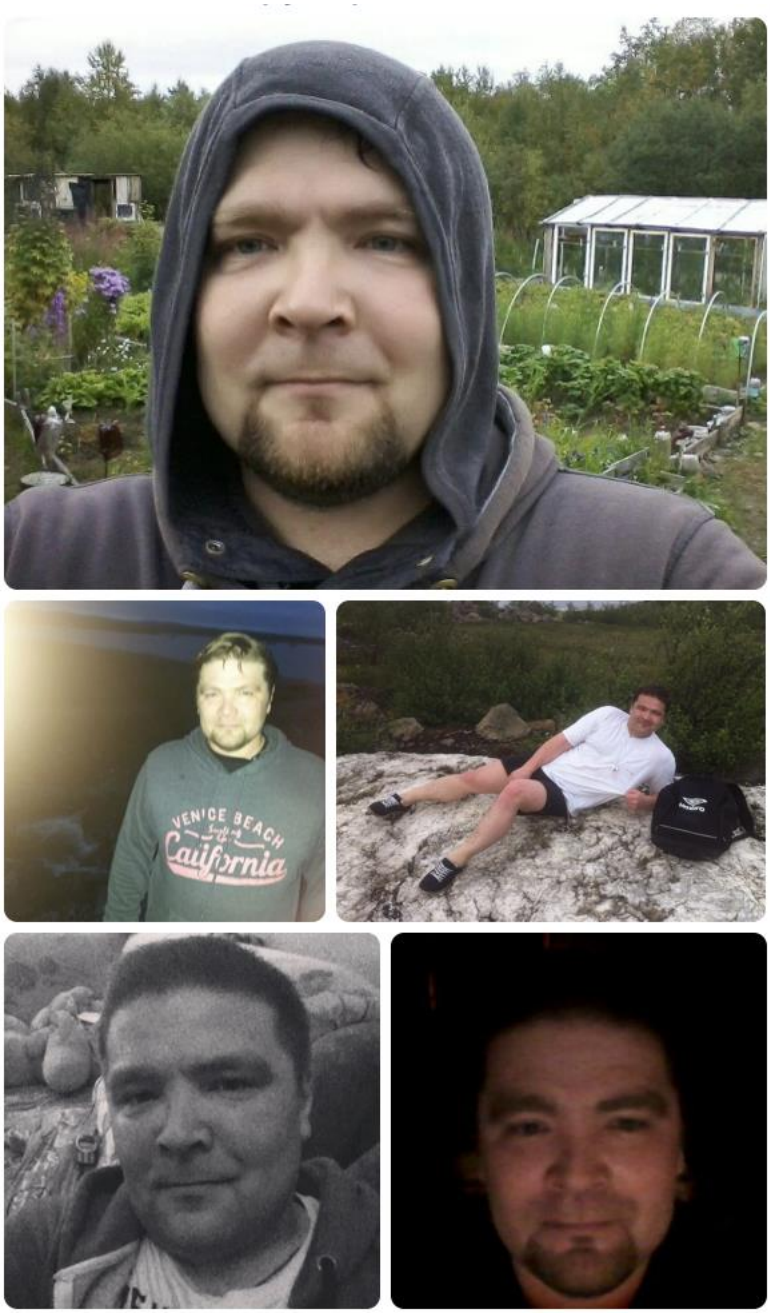


Рис. 3.11. Хактивіст Леонід

Це Леонід. Впізнали ми його по фотографіям із веб архівів ВК, які він видалив разом із сторінкою. Ім’я користувача у Телеграм він не має, але є ID: 1956167650.

Він живе поряд з Фінляндією, у Мурманській області. В нього є донька, він полюбляє випити після роботи та пограти у Call of Duty онлайн.
Також виявилось, що він колись залишив в телеграмі свій номер телефону публічним, тому ось: +79113482932.

Рис. 3.12. Хактивіст Валерий Разорєнов

Наступний захисник росії у кіберпросторі у Телегам є @Valeri_Rozanov. Разорєнов Валерій Володимирович, позиціонує себе як доктор психології. Дуже захоплюється езотерикою, про що свідчить його Фейсбук та ВК:

https://www.facebook.com/Valerij.Razorenov, https://vk.com/razomir. Цей діяч дуже медійна особа. Всіх наставляє і заохочує читати його книжки про щось псевдонаукове. Їх, а також його новели можна подивитись тут: https://proza.ru/avtor/razomir, можливо, рецензію захочете написати. Сторінки зареєстровані на номер телефону: +79106433784, також є позначки з авіто та злитих баз про його кубло: Рязанская область, Рязань р-н Железнодорожный Островского 26, та відділення пошт, які він відвідує: RZN19, RZN3, RZN15, RZN6. Про їх місцезнаходження завжди можна дізнатися на офіційному сайті: https://www.cdek.ru/ru/offices/list/ryazan. Також його електронна пошта: valer-@mail.ru, може знадобитися.

Рис. 3.13. Хактивіст Перевезенцев Алексей

На наступному фото можна побачити особу під ніком @Butylkus в Телеграм, який зареєстрований на номер +79207443166, як і ця сторінка в ВК: https://vk.com/id287340393. Збережений у контактах як Перевезенцев Алексей Александрович з Тульської області, Щекінский район, Совєтск, вулиця Площа Совєтов. Він у нас відеоблогер на ютубі і дзені, де грає у ігри та показує уроки з електроніки.

До номеру телефону закріплена адреса. Також якщо хочете замовити рекламу на його ютубі, ось його емейл idol13ru@gmail.com і адреса поштомату, де забирає пакунки TUL2.

Рис. 3.13. Хактивіст Другов-Кручинський Володимир

Одним із російських кібер активістів є житель м. Білово Кемеровської області Володимир Валерійович Другов-Кручинський з ніком @Vladimir_IK44 в Телеграм. Цікаве співпадіння, що напис “ІК-44” в ніку можна розшифрувати як “Исправительная колония 44”, яка також знаходиться в Білово.

Має дружину Катерину, є активним учасником геологічного форуму ВГД, цікавиться історією, подіями Першої світовою війни і географією Росії, що можна побачити на його сторінці з форуму https://forum.vgd.ru/index.php?m=feed&a=list_warn4&u=189310.

Також йогономер телефону теж не був загублений: +79133173257

Володимир активно коментує пости в спільноті міста Білово зі свого акаунту в Однокласниках https://ok.ru/profile/333785976647.
Його поштове відділення — “BLO1”.

У вільний час Володимир веде свій ютуб-канал, який станом на 12.07.2022 налічує цілих 2 підписники: https://www.youtube.com/channel/UCJ-4yZ5fh0_jUrwQ3nA1dyw/featured

З наявних відео можна побачити, що він полюбляє відпочинок на березі Чорного моря в Любимовці, яка знаходиться в анексованому Росією Криму.

Рис. 3.14. Хактивіст Долгодворов Євгеній

Це Євгеній Борисович Долгодворов під прізвиском deb. В Телеграм відомий як @purana. Народився він 22.09.1975 року. Займається вільним велокатом, професійною фотографією і постійно публікує фото з природою на своїй сторінці в Інстаграм: https://www.instagram.com/puranoia, яка має більше 12 тис підписників. Іноді там можна зустріти дивні псевдополітичні дописи на кшталт цього:

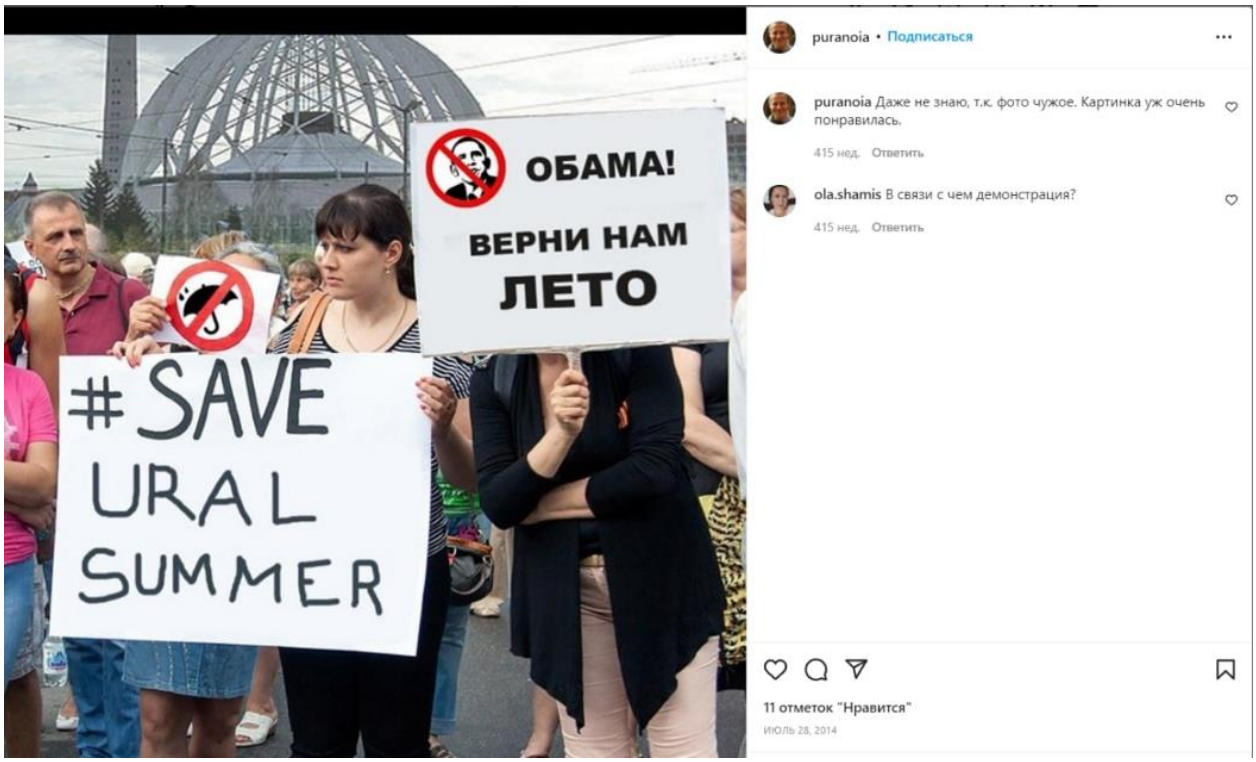


Рис. 3.15. Пост з Інстаграму Долгодвороа Євгенія

Проживає Євгеній за адресою: Свердловская обл, г Екатеринбург, р-н Октябрьский, ул. Курганская 3 кв. 81, про що ми дізналися із злитих баз даних. Також ми знайшли його закриту сторінку в ВК: https://vk.com/id102300738 і його номер телефону: +79028708758. Його електронна пошта: enbbs@yandex.ru, поштові відділення: “”YEKB36, YEKB11". У злитих базах даних знайшли його пароль: 759648.

Рис. 3.16. Хактивіст Рябиченко Никита

Складніше стало з наступною персоною. Всі соціальні медіа видалені або закриті, і ледве зміг виудити з веб архіву його фотографію, яка давно стояла в його вконтактє і то дуже малого розміру. І так на фото Рябиченко Никита Сергійович, який іменується в Телеграм як @Ben_Aflick. Його номер телефону: +79887485886

Народився 3 грудня 1993 року. Місце реєстрації: Ставропольский край, Кочубеевский муниципальный округ, с. Кочубеевское. Сторінка в ВК: https://vk.com/id135516618 зі статусом “Fallaces sunt rerum species”, що перекладається як: “Зовнішній вигляд оманливий”, певне відсилаючи на його кібер боротьбу з українцями.

А от з іншим індивідом вийшло набагато цікавіше. Підписаний в Телеграм як Ігор Князьков і має нік @IKnyazkov. Там же має статус: “Солнечный привет из Сочи, увлечен страстью к программированию. 61 год”. Аккаунт в Телеграм зареєстрований на номер телефону: +79673287510. На номер зареєстрована сторінка в ВК: https://vk.com/id571113163. Але ми знайшли дуже дуже схожу сторінку в ВК: https://vk.com/id412562094 на ім’я Вадима Кирсанова і датою народження 25 червня 1985 г за адресою: Находка Приморського краю.

Але у минулому його на сторінці знали як Артема, про це свідчить і коментарі, і архіви, у яких також написано, що він із Виборгу, Лєнинградской області.

Незважаючи на це, фото з профілю в телеграмі й в ВК зображають одну й ту ж персону.

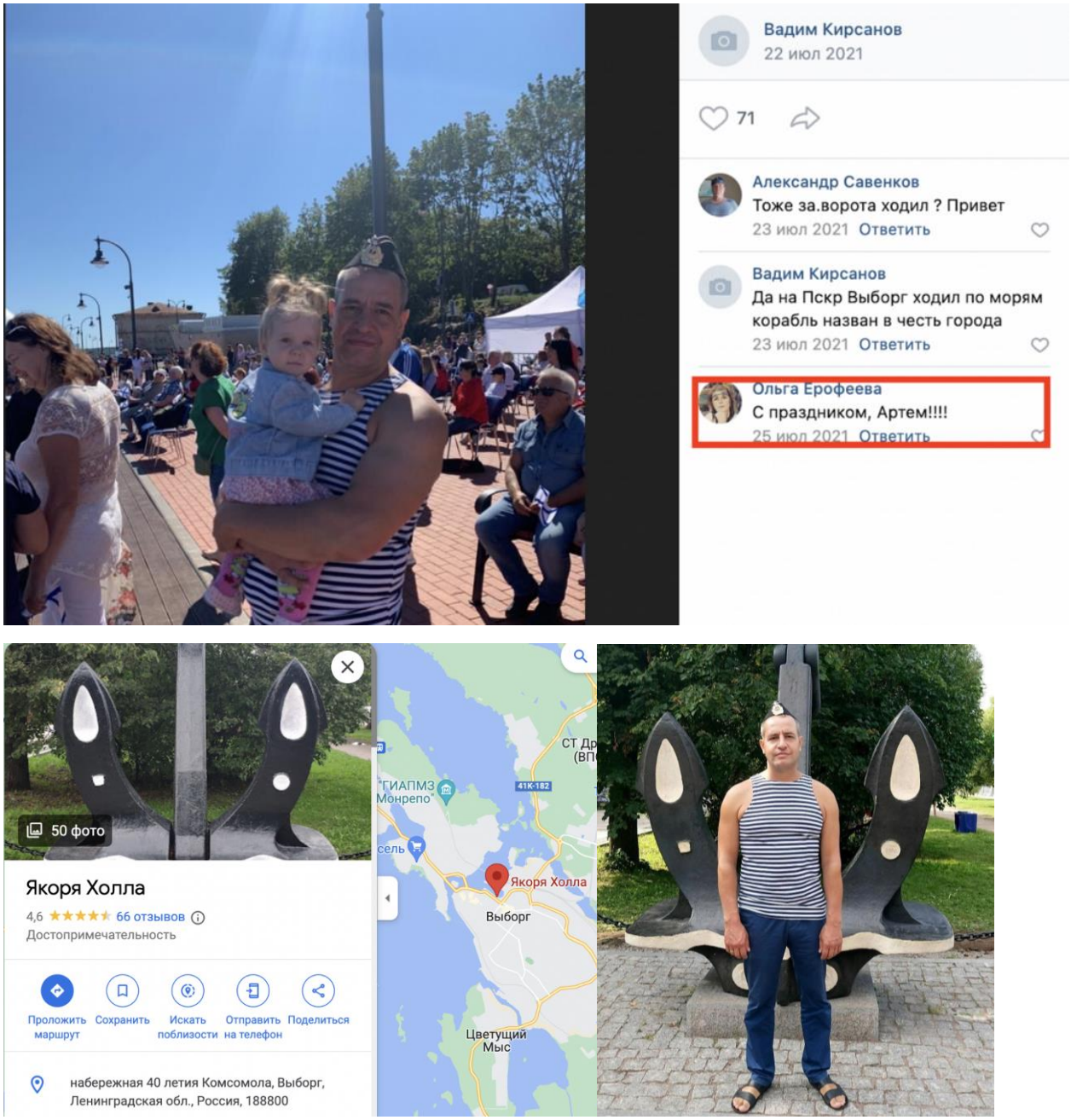


Рис. 3.17 Артем чи Ігор поряд з якорем у Виборзі

Це свідчить про те, що акаунт переробили на фейковий. Але ми змогли довідатись інформацію про власника номеру телефону. Його адреса: Краснодарский край, Сочи, микрорайон Приморье, ул. Есауленко, 4/6 р-н Хостинский; його поштові скриньки: iknyaz33@gmail.com,

iulov.maxim@yandex.ru, tvknyaz70@gmail.com. Його акаунт в Фейсбук є пустим: https://www.facebook.com/profile.php?id=100013405442154. А ось в Однокласниках https://ok.ru/profile/578099673486/photos, де нароблено купа копій, має фото, і це свідчить про те, що все ця особистість була позичена. Але, згідно фотографій, можна зробити висновок, що справжній Ігор Князьков служив у флоті, як і наша ціль, і можна припустити, що вони служили разом. А прізвище Кірсанов, яке фігурує в обох, можливо, шифр, прізвище шанованої ними людини, яка, наприклад, зараз може продавати кораблі.

Рис. 3.18 Витримка з ОК.ру

І нарешті ми дійшли до відповідальних осіб. Ієрархія групи доволі проста: Є модератори, які слідкують за чатом, вони ж фільтрують учасників та приймають на розгляд майбутні цілі. Команда розробників і спеціалістів різного плану. Усі підподпорядковані “головному”, якого іноді тегають у чаті з приводу технічних питань. Він і з’язався з підставним акаунтом, пам’ятаєте?

Рис. 3.19 Хактивіст Зарніцька Єкатерина

Модераторка @lika_in_wonderland — вона ж Катюша Александровна Зарницкая. 11 вересня 1983 року народження із Мічурінська. І ось телефон, на який зареєстровано акаунт у Телеграм: +79037816316. На ций же номер зареєстрована вже заморожена сторінка ВК: https://vk.com/id94480556 та закрита сторінка Фейсбук: https://www.facebook.com/ekaterinalika.zarnitskaya/. Також за пошуком імені, вказаного у попередньому посиланні, можна знайти ютуб з фотографією і ще одну сторінку в ВК. Такий же userID дає підставу рахувати, що ця сторінка теж її: https://vk.com/likainwonderland.

У злитих базах даних є пароль Катюши, дуже нагадуючий чиюсь дату народження: 22061994, можливо впізнаю пізніше – записую.

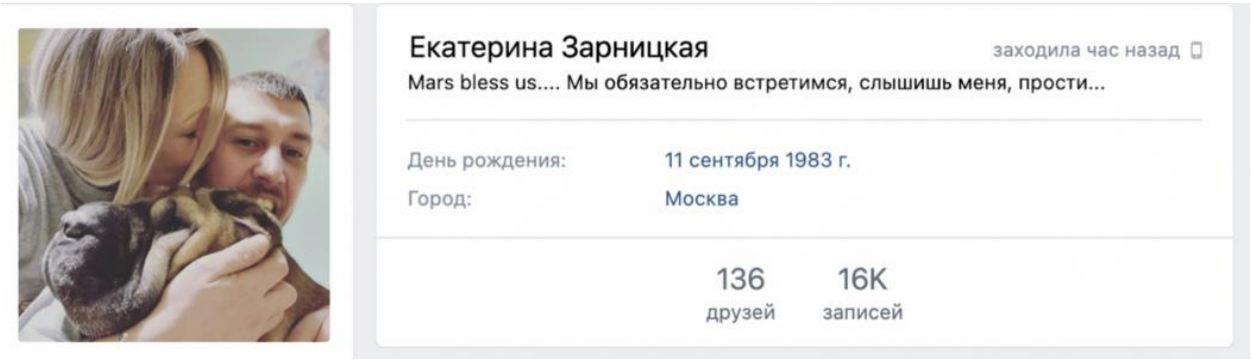


Рис. 3.19 Витримка з ВК.ру

Судячи із сумного статусу роблю припущення, що вона когось вже не дочекається. Ось її електронні пошти: cerguo@mail.ru, likacid@gmail.com, postoronnim_v83@mail.ru;

А ось адреса із коментарем із служби доставки: г. Москва, ул. улица Полины Осипенко, д. 14к1, кв. 216, (Комментарий: Комментарий к доставке: подъезд 4 домофон 216 этаж 8)

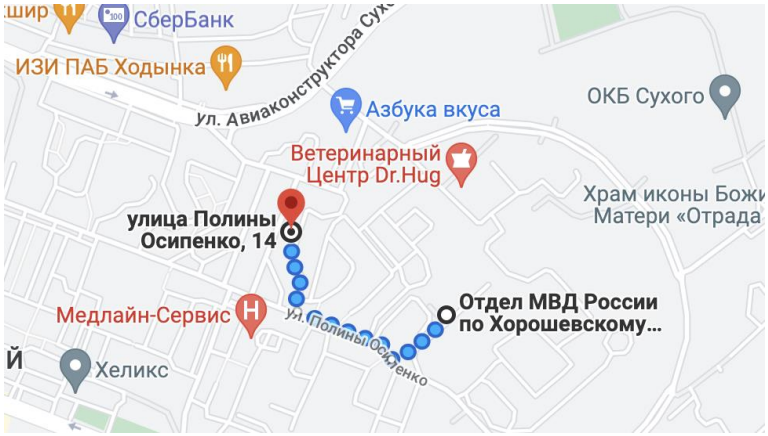


Рис. 3.20 Мапа з адресою будинка

“Возле Ликиного дома как всегда ментов куча , все в парадной форме))) , ну каждому свистков раздал , обещали её мелодией “ С добрым утром Госпожа “ встретить)))” — підмітив один із хлопців у чаті. І ось співпадіння, за

адресою в 5 хвилинах поліцейський відділок. Можливо, все на те вказує, що саме там зараз Ліка і перебуває.

Рис. 3.20 Хактивіст Дегтяренко Денис

@DvoZ060 — він же Дегтяренко Денис Олегович, 9 октября 1989 року народження, живе у Орську, як не дивно. Точніше Оренбургская область, Орск, микрорайон Новый город, пр-т Ленина, 130 (або 134. на авіто вказував обидва будинки), працює у РЖД.

З відкритих інтернет-джерел дізналися, що Денис займається фрілансом з 2011 року на посаді веб-майстра. Одружений на Юлії Чабанюк (нар. 09.05.1992 р.). Має як мінімум дві сестри: Віру Данилову (Саприкіну), Юлію Дегтяренко. З 2010 по 2011 рр. служив у збройних силах рф у в/ч №63935,

Брянск-18; в/ч 42685, Брянск-18. Мав бізнес “Детям-игрушки.рф”, який, схоже, прогорів. Наразі працює в РЖД.

На його номер телефону: +79325417211 окрім Телеграм зареєстрований акаунт у ВК: https://vk.com/id24726978. denisvsd@mail.ru електронна пошта по-класиці і поштове відділення: “ORS2, ORS4, ORS5”. До речі, у цього юніта ми знаємо і ip-адрес: 95.105.125.226. Саме він робить відео з туторіалами про DDoS-атаки, це стало відомо із чату.

Рис. 3.21 Хактивіст Панченко Юрий

@hand_0f_fate — Панченко Юрий Александрович. Номер телефону +79147176504, https://vk.com/id14277584 і ВК зареєстрованний на цей номер. Цікаво, що у цього номеру телефону також значиться (чи значився) власник і з ще купою номерів: ООО “Пск, Барботкин Михаил Валерьевич +79147093383, +79084481272, +79147176504, +79243373967, +79243200721.

Проживає в Приморському краї, м. Находка. Навчався в МТИ (МосТех) (бывш. МТИ «ВТУ»). Його поштове відділення: “NXD2, VLK14”.

Продає автозапчастини, про що можна довідатися у: https://zav-gar.com/contacts/.

Згідно аналізу відкритих даних його телеграм-акаунта, Юра є людиною різноплановою: він цікавиться блокчейном, а саме: криптовалютою, nft-токенами, майнингом (також більше року цікавиться відеокартами й asic-майнерами, що може означати те, що він сам є майнером). Він цікавиться військовими конфліктами (близько півроку), IT індустрією і політикою. З нелегальної тематики можна відмітити, що він більше року цікавиться підробкою і продажем документів, наркотиками (причому регулярно, судячи зі статистики), і, звичайно, DDoS-атаками, якими почав цікавитися приблизно в лютому місяці. Також відомо, що Юра слідкує за трейдингом. Як і більшість росіян, він підписаний на багато пропагандистських пабліків, які висвітлюють російських солдат як “асвабадітєлєй”, з-поміж яких: kadyrov_95, война с фейками, russiamyvmeste, тощо.

Наступний: Капитанец Евгений Валентинович, у Телегам немає логіну, тому тримайте його ID: 17473649.

Чим займається у групі, не ясно, але має права адміна і часто кидає новини з проросійських пабліків в перемішку з мемами у чат.

Номер телефону: +79142256723; доречі його ip: 188.244.191.130

Поштові скриньки: geektator.com@miltor.ru, akarisaki@gmail.com, harleyquinn@mail.ru

Рис. 3.21 Хактивіст Капитанец Евгений

Зі злитих баз даних відома адреса проживання Євгена: Якутск пер. Вилюйский, 6, Якутск ул. Губина, 3, 1 этаж, NA N/a ROSSIYA, YAKUTSK, KIROVA 21 B, 677027, Саха /Якутия/ респ., г. Якутск, ул. Орджоникидзе, д. 21 оф. 3.

Про Євгена також відомо, що він народився 20.03.1987 року. Активно займається підприємницькою діяльністю, а саме:

- Мав у власності інтернет-магазин geektator.com, останній снапшот в якому був у 2019-му році. Ось його сторінка в Інстаграм:

https://www.instagram.com/geektator_ltd/ І у ВК: https://vk.com/geektator. Наразі бізнес знаходиться в стадії ліквідації.

- Володіє 100% ООО “ИМПОРТ ВКУСА”, яке нині діюче й знаходиться за адресою: 677000, респ Саха /Якутия/, город Якутск, улица Лермонтова, дом 23 КОРПУС 2, КВАРТИРА 30. Займається оптовою торгівлею харчових продуктів. Їх прибуток у 2018 р. склав 2 млн рублів.
- був генеральним директором ООО “ПРОДВИЖЕНИЕ”, яка була пов’язана з виробництвом, прокатом та показом фільмів; ліквідована в 2015 році

Згідно аналізу відкритих даних його телеграм-акаунта, Євген цікавиться мобільними додатками, соціальними мережами, маркетплейсами, блокчейном (ethereum eth, ico, смарт-контрактами, платформами на блокчейні), IT-сферою, військовими конфліктами (причому регулярно, більше року) та політикою (найбільш приділяється увага: геополітиці, націоналізму, правим та нетолерантності).

На жаль, про ID2006328911 на ім’я “ᴸᵒᵛᵉ$_{γou}$ юvя ᴸᵒᵛᵉ$_{γou}$” відомо або нічого, або недостатньо. У особи новий телеграм акаунт, який використовується і поза діяльністю групи.

А Юля насамперед дуже комунікабельна дівчина, яка хоч і зберігає кібергігієну, але все ж любить поділитись своїм життям. Таким чином, із спілкування у чаті було встановлено, що вона проходить курси хімеотерапії у Краснодарському краю, по фаху є клінічним психологом. Також постила відео із морем і пляжем в Анапі.

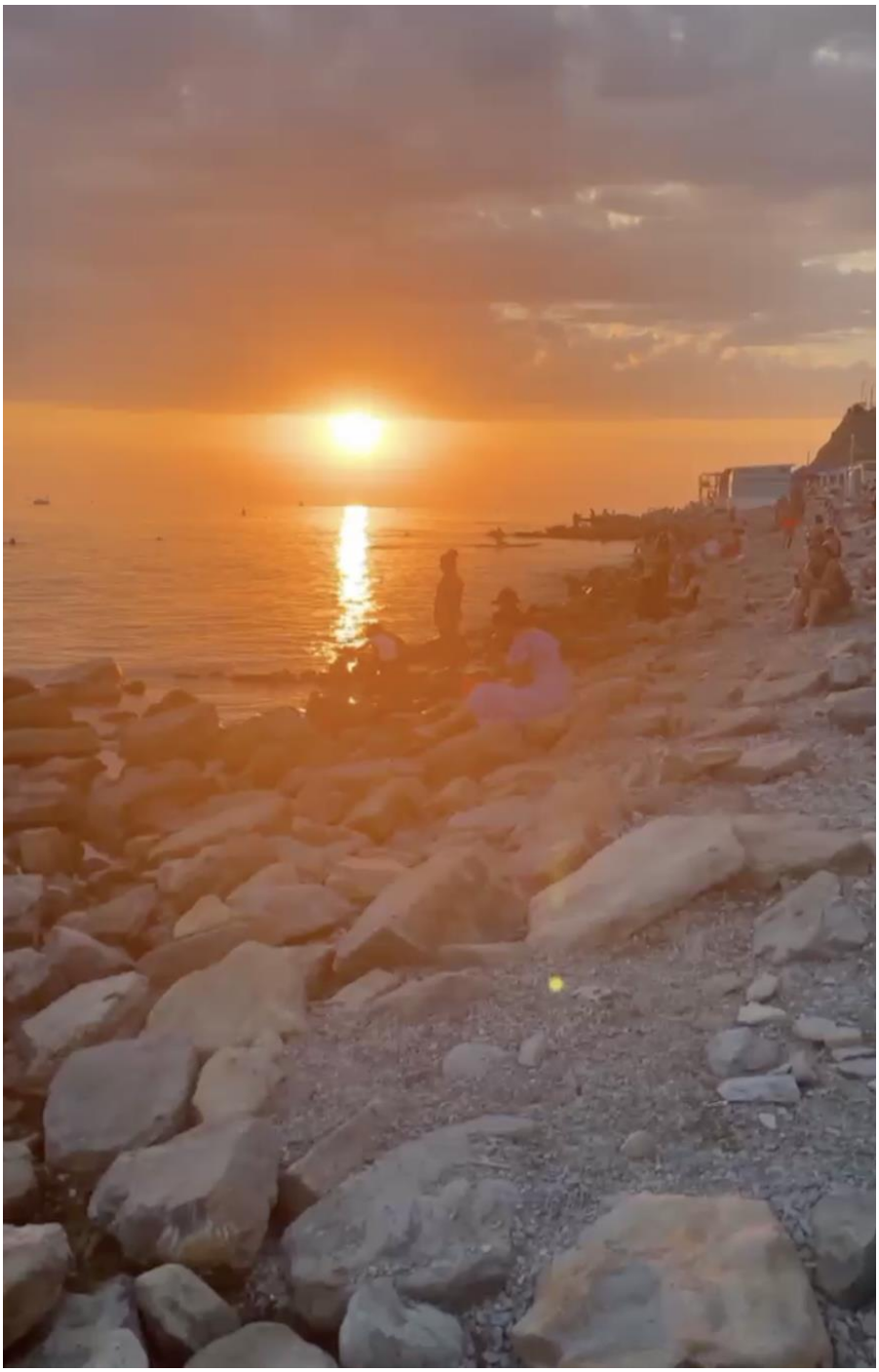


Рис. 3.22 Фрагмент із відео

Як і у інших, у Юлі було виявлено цікаве прагнення до 3д принтерів. І Леонід із початку статті, і Ліка із команди були частиною спілки публічної групи з питань по 3д принтерам у Телеграм. Підписана на різні пабліки з тематикою кібербезпеки, починаючи від взломів, закінчуючи розвідкою по

відкритих даних. Слідкує за Beregini (Телеграм групи заблокували, але тут можна побачити історію https://t.me/s/hackberegini?before=34) , жінки хакери із України, як вони кажуть, мають домен сайту .ru та допомагають окупантам. Ось і вся інформація, на жаль.

Висновки до розділу 3

Дуже несподівано виявляється, що середній вік активних персонажів перебігає за 30+. Можна було б подумати, що це могли бути ІПсО, реальні дядьки та тьоті, які працюють на державу, але ні, це дилетанти, які у повсякденному житті займаються у більшості навіть не в ІТ. Більшість або повністю, або частково не чули про кібергігієну і ще більше не здогадуються, що є веб архіви, які зберігають інформацію, яка залишається, навіть якщо хтось змінив ім’я чи видалив всі фото. Но то на наще щастя.

ВИСНОВКИ

1. В даній роботі було розглянуті методи пошуку інформації:

- Штучні нейронні мережі
- Мануальна робота (пошук без автоматизації)
- Використання баз данних (во благо)

З усіх методів ми обрали штучні нейронні мережі, як найшвидшу для пошуку інформації, та пройшли кожен крок від початку, до деанонімізації людини.

2. У даній роботі описано задачу виявлення виявлення особ, які приймають участь у збройному конфлікті Росії проти України у кіберпросторі.

Для проекту було обрана низка опрелюдниних баз даних, через їх актуальність в рамках пошуку особ на території України та РФ.

Під час аналізу та пошуку інформації була виявлена та ідентифікована група людей, що стоїть за терроризмом веб-інфраструктури України.

Для розрахунку та пошуку інформації використовувались як автоматизовані рішення, так і мануальні. Пошук через соціальні мережі, ідентифікація місць через Google Maps, та інше.

В результаті відбулясь деанонімізація частини спілки хактивістів.

3. У результаті дослідження було розкрито декілька персон, їх імена, призвища, номера телефонів, адреси реєстрації, загальні місця перебування, фотографії, тощо. Наприкінці було проаналізовано результати запропонованого рішення.

Ціль роботи передбачала не тільки аналіз інформації, але і спроба протидії реальному тероризму зі сторони РФ на веб-інфраструктуру України.

В результаті дослідження була опрелюдненна стаття, для демонстрації особистої інформації людей в публічний простір.

Після цього була проведена робота аналізу наслідків. Номери телефонів були деактивовані та змінені, соціальні мережі буди видалені або закриті. Актив чату команди після нетривалого оговорення цієї теми перейняв інформаційну тишу.

Нажаль, ця тиша не змогла триватись довго. Так, співзасновники цього проєкту були напугані, більшість хактивістів покинули спілку (або змінили профілі взаємодії), але терор продовжується і надалі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Vinayak gupta, Brijesh kumar singh, parmesh war lal bhanwariya “An Introduction to security issues in wireless sensor networks” Journal of environment al science, computer science and engineering and technology (JECET); November 2013;vol.2 No.4,pp.1276-1285.

2. Al-Sakib Khan Pathan, Hyung-Woo Lee ,Choong Seon Hong “Security in wireless sensor networks: issues and challenges”. The International conference on advanced computing and technologies (ICACT); 2006; february 20-22; pp.1043-1048.

3. Бельфер Р.А. Угрозы информационной безопасности в беспроводных самоорганизующихся сетях // Вестник МГТУ им. Н.Э. Баумана. — Сер. Приборостроение. Спец. вып. «Технические средства и системы защиты информации». 2011. С. 116–124.

4. Shaohe lv,xiaodong wang, xin zhav, xingming zhou, “Dtecting the Sybil attack cooperatively in wireless sensor network”. computational intelligence and security,2008CIS ‘08' International conference vol.1; 13-17 dec 2008;pp.442- 446.

5. Cheng-Lung Yang, Wernhuar Tarng, Kuen-Rong Hsieh, Mingteh Chen “A security mechanism for clustered wireless sensor network based on elliptic curve cryptography”. Intelligent internet systems IEEE dec 2010.

6. Md. Safiqul Islam, Rasib Hayat Khan, Dewan Muhammad Bar ry. A hierarchical intrusion detection system in wireless sensor networks // int. j. of computer science and network security. 2010. Vol. 10. No 8.

7. Пахомова В. М. Можливості розвитку комп’ютерних мереж в автоматизованих системах транспорту. *Дніпропетровськ: ДІІТ*, 2015. – 203 с.

8. Пахомова В. М., Коннов М. С. Дослідження двох підходів до виявлення мережевих атак з використанням нейромережної технології. *Наука*

та транспортний прогрес. Вісник Дніпропетровського національного університету транспорту , 2020. №3(87). – 81-93 с.

9. Пахомова В. М. Дослідження інформаційно-телекомунікаційної системи з використанням штучного інтелекту. *Вид-во ПФ «Стандарт - Сервіс»*. Дніпро. 2018. – 220 с.

10. Анил К. Введение в искусственные нейронные сети. *Мічіганський університет*, США: Мічіганський університет, 1996. – 20 с.

11. Бочков М.В. Реализация методов обнаружения программных атак и противодействия программному подавлению в компьютерных сетях на основе нейронных сетей и генетических алгоритмов оптимизации. *Сб. докл. VI Межд. конф. по мягким вычислениям и измерениям SCM'2003*. СПб.: СПГЭТУ, 2003. т.1. С. 376-378.

12. Гришин А.В. Нейросетевые техонологии в задачах обнаружения компьютерных атак. *Информационные технологии и вычислительные системы*. 2011. – С. 53-64.

13. Штовба, С.Д. Проектирование нечетких систем средствами MatLAB *Горячая линия* – Телеком, 2007. – 288 с.

14. Ярушкина, Н.Г. Основы теории нечетких и гибридных систем. *Финансы и статистика*, 2004. – 320 с.

15. Heady R., Luger G., Maccabe A. and Servilla M. The Architecture of a Network Level Intrusion Detection System. *Computer Science Department*, University of New Mexico, Tech. Rep. TR-90. 1990. 21 p. URL: https://www.osti.gov/servlets/purl/425295 (дата звернення: 02.09.2020)

16. Anderson J. P. Computer Security Threat Monitoring and Surveillance. James P Anderson Co, Fort Washington, Pennsylvania, Tech. Rep., 1980. 56 p. URL: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf (дата звернення: 03.09.2020)

17. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey. *ACM Computing Surveys*. 2009. Vol. 41, no. 3. P. 15–38.

18. Ghorbani A., Lu W., Tavallaee M. Network Intrusion Detection and Prevention: Concepts and Techniques. New York: Springer-verlag, 2009. 216 p.

19. Ning P., Jajodia S. Intrusion Detection Techniques. HBidgoli (Ed.), The Internet Encyclopedia, 2003. URL: https://doi.org/10.1002/047148296X.tie097 (дата звернення: 06.09.2020)

20. Daniel B., Julia C., Sushil J, Ningning W. ADAM: a test bed for exploring the use of data mining in intrusion detection. *ACM SIGMOD Record.* 2001. Vol. 30, no. 4, pp. 15–24.

21. Широчин В. П., Мухін В. Є., Кулик А. В. Питання проектування засобів захисту інформації в комп'ютерних системах та мережах. Київ; «СТОРІН+». 2000. - 111 с.

22. Ганієв С. К., Карімов М. М. «Питання оптимального сегментування топології локальних комп'ютерних мереж».-Ташкент, Проблеми інформатики та енергетики, 2001, № 2.-С.20-25.

23. В. Г. Оліфер, Н. А. Оліфер. Комп'ютерні мережі. Принципи, технології, протоколи 4 видання - Пітер-2010. 944с.

24. Платонов В. В. Програмно-апаратні засоби захисту інформації: підручник для студ. Установ вис. Освіта/ - М: Видавничий центр «Академія», 2014.

25. Люгер, Дж.О. Штучний інтелект: стратегії та методи вирішення складних проблем / Дж.О. Люгер. – М.: Діалектика, 2016. – 864 с.

26. Нільсон, Н. Принципи штучного інтелекту/Н. Нільсон. – М.: Радіо та зв'язок, 2015. – 373 с.

27. Рассел, С. Штучний інтелект: сучасний підхід/С. Рассел, П. Норвіг. – М.: Вільямс, 2016. – 578 с.

28. Слейгл, Дж. Штучний інтелект / Дж. Слейгл. – М.: Світ, 2016. – 320 с.

29. Тей, А. Логічний підхід до штучного інтелекту / А. Тей, П. Грибомон, та ін. – М.: Світ, 2015. – 432 с.

30. Як компанія SeoPult стала беззаперечним лідером ринку оптимізації сайтів // Секрет Фірми, 2014. - 120 с.

31. Каллан Робертс. Основні концепції нейронних мереж // Каллан Робертс - М.: Видавничий дім "Вільямс", 2013. - 287 с.

32. Колесніков А.В. Гібридні інтелектуальні системи. Технологія розробки/О.В. Колесніков - СПб.: Вид-во СПбДТУ, 2011. - 111 с.

33. Лохін В.М. Інтелектуальні системи управління: поняття, визначення, принципи побудови/В.М. Лохін, В.М. Захаров// Мехатроніка. - 2013. - №2. - 27-35 с.

34. Галушкіна А.І. Нейрокомп'ютери та їх застосування. / За загальною ред. А.І. Галушкіна, Я.З. Ципкіна. - М.: ІПРЖР, 2011. - 145 с.

35. Пупков, К.А. Інтелектуальні системи/К.А. Пупков, В.Г. Коньков - М.: Вид-во МДТУ ім. н.е. Баумана, 2013. - 148 с.

36. Романов, В.П. Інтелектуальні інформаційні системи економіки: Навчальний посібник / В.П. Романов; за ред. д.е.н., проф. Н.П. Тихомирова. - М.: Іспит, 2013. - 96 с.

37. Рудська Є. Н., Десятніченко Л. В. Штучний інтелект для бізнесу: трансформація ефективних запитів у реальні продажі // Молодий учений. - 2015. - №8. - 121-131 с.

38. Анісімов С.Ю. Алгоритми штучного інтелекту. -

39. [Електронний ресурс]. URL: http://faqs.org.ru/progr/common/ai.html

ДОДАТОК А
ЛІСТИНГ ПРОГРАМИ