В сучасності багато людей користуються мережею інтернет і читають багато новин через соціальні мережі та мессенджери. Візьмемо наприклад популярні мессенджери Telegram, Viber, через нього поширюється новини, реклама, пропаганда.

Одним із явних інструментів зараз для протидії російської пропаганди використовується - канал «StopRussiaChannel | MRIYA», бот «StopRussia | MRIYA». Цей інструмент дозволяє викладати новини які продивляється велика аудиторія користувачів. Викладаючи новини сценаристи прописують правильні тексти, які будуть використовувати емоції людини підбурюючи їх до тісї думки, яка була задумана психологами цього каналу. З перших днів війни, команда розробників «МРІЯ» розуміючи важливість інформаційної підтримки наших військових, а також боротьби з кремлівським медіа-пропагандистам. Досвід у блокуванні ресурсів в діяльності щодо блокування каналів розповсюдження наркотичних засобів у Telegram вже існував. В Telegram існує багато можливостей для створення програмних засобів для інформування користувачів. Використовуючи ці можливості був розроблений Telegram BOT. Бот працює як база даних для користувачів які виявляють громадянську небайдужість і дає користувачам лінк за яким слід перейти та залишити репорт, також люди можуть залишати і посилання на канали, групи, ботів, користувачів які поширюють пропаганду. Також вже йде остання фаза тестування Viber BOT який не буде відрізнятися від Telegram боту, але в Viber не зовсім гарно створена взаємодія з автоматизацію процесів створення. Одним із найкращих способів просування груп - створення груп з великою кількістю користувачів адже люди схильні до перегляду новин від груп в яких багато користувачів.

Отже створення програмних інструментів є одним із важливих складових політичного управління, підготовки та ведення війни в наш час. Треба пам’ятати також про способи протидії методам інформаційної війни. Узагальнюючи все робимо висновок що, для створення програмних інструментів потрібно згуртована робота багатьох спеціалістів у різних сферах.

Каланча Андрій Андрійович
курсант 2 курсу факультету №4 Харківського національного університету внутрішніх справ
Світличний Віталій Анатолійович
доцент кафедри протидії кіберзлочинності факультету №4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

ПОРІВНЯННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОНКУРЕНТНОЇ РОЗВІДКИ ДЛЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ У ВОЄННИЙ ПЕРІОД

Із початку воєнного вторгнення росії в Україну, кіберполіція активно викриває осіб, що займаються шахрайством в глобальній мережі Інтернет. Досить часто шахраї здійснюють псевдоблагодійність, пропонують оренду житла, якого в реальному житті не існує, проводять фейкові пасажирські перевезення, або продають неіснуючу військову амуніцію; тобто, наживаються на

людському горі - війні. Найчастіше випадки обману можна зустріти під приводом перенаправлення через державний кордон чоловіків віку, придатного для несення служби, а також надання інформації щодо безвісти зниклих осіб [1].

Зважаючи на це, необхідно оперативно розшуковувати подібних осіб, щоб якомога скоріше припинити процес поширення їхньої діяльності та мінімізувати ризики введення в оману населення України. Тож *метою* роботи буде порівняння програмного забезпечення, що використовує дисципліну Open Source INTelligence (OSINT) для виявлення максимальної інформації щодо подібних кібершахраїв.

Отож, OSINT - це розвідувальна дисципліна, що включає пошук, вибір і збір розвідувальної інформації з загальнодоступних джерел, її аналіз та систематизація. Отримати подібні дані можна з відкритих джерел, так званої «поверхневої мережі», а також із метаданих; соціальних мереж, де люди часто бездумно діляться своєю персональною інформацією; номерів телефону; електронних скриньок; інформації про людей у відкритому доступі; картографуванні та геопросторових дослідженнях; зображеннях; аналізі мережі та пакетів даних, якими обмінюються користувачі мережі Інтернет [2].

Найпоширенішими інструментами у цій сфері є Maltego і SpiderFoot.

Maltego - це інструмент, створений для побудови та аналізу зв'язків між різними суб'єктами та об'єктами. її особливостями є: візуалізування отриманих даних, розвідка на основі відкритих джерел, комбінування для глибокого аналізу даних, отриманих із закритих та відкритих джерел, автоматичний аналіз відкритих джерел та автоматична побудова взаємозв'язків між виявленими об'єктами. Maltego дозволяє зібрати в цілісну картину усю інформацію, отриману з відкритих і закритих джерел, та візуалізувати агреговані дані. Maltego може бути використана для виявлення відносин та реальних зв'язків між: людьми, групами людей (соціальні мережі), компаніями, організаціями, веб-сайтами, інтернет-інфраструктурами (доменами, DNS-іменами, мережевими блоками, IP-адресами), документами та файлами.

Maltego - проста та швидка у встановленні й написана на Java, тож, як наслідок, бездоганно працює на Windows OS, MacOS та операційних системах на ядрі GNU/Linux. Maltego має графічний інтерфейс, який дозволяє бачити взаємозв'язки між об'єктами миттєво і точно, а це дає можливість простежити приховані зв'язки. Maltego унікальна тому, що вона використовує потужний і гнучкий фреймворк, який робить можливим налаштування під себе. Maltego може використовуватися на стадії збору інформації пов'язаної з безпекою [3].

Хорошим, якщо не найкращим, аналогом Maltego є інструмент для автоматизованої розвідки з відкритим вихідним кодом - SpiderFoot. Його мета - автоматизувати процес збору інформації про задану ціль. Є три основні сфери, де може бути корисний SpiderFoot: якщо користувач проводить тестування на проникнення, SpiderFoot автоматизує стадію збору інформації по цілі, дасть вам багатий набір даних, щоб допомогти визначити напрямки діяльності для тесту.

SpiderFoot також може бути використана для збору інформації про підозрілі чи шкідливі IP-адреси, які ви могли бачити у ваших лотах або отримали через канали розвідки погроз.

Основними перевагами SpiderFoot є більше 40 джерел, кількість яких лише продовжує зростати: серед них SHODAN, RIPE, Whois, PasteBin, Google, SANS та інші. Вбудована візуалізація, заснована на JavaScript, можливість експорту до GEXF/CSV для використання в інших інструментах, наприклад Gephi. Інтерфейс користувача заснований на веб. Простий у використанні, простий у навігації.

Оскільки це програмне забезпечення має повністю відкритий вихідний код, є можливість повністю кастомізувати цей інструмент під себе, зробивши свій форк на GitHub. Майже кожен модуль має налаштування, тому ви можете задати рівень нав'язливості та функціональності. Особливим плюсом є його висока модульність і можливість створення модулів на мові програмування Python, а також зв’язка із SQLite, що дозволяє зберегти усі дані у локальній базі SQLite. Одночасне сканування у власному потоці є також важливою перевагою, оскільки дозволяє виконати сканування безлічі цілей одночасно. Працює на операційних системах на ядрі GNU/Linux та Windows OS. На відміну від знаменитого конкурента Maltego, SpiderFoot повністю безкоштовний і набагато корисніший, оскільки здатний зібрати набагато більше інформації [4].

Основними відмінностями між цим програмним забезпеченням є:

1) Наявність відкритого програмного коду у SpiderFoot;

2) Можливість розгорнути SpiderFot на власній машині в якості сервера, та використовувати його на основі веб-технологій;

3) Модулі, що відрізняються ціною, оскільки варто пам’ятати, що у Maltego більшість модулів хоч і дуже ефективні, але мають велику ціну;

4) Використання відмінних мов програмування у програмному забезпеченні;

5) Різниця в налаштуванні під себе: SpiderFoot дозволяє глибше налаштування, оскільки має відкритий програмний код;

6) Можливість використання SQLite в роботі із SpiderFoot;

7) Maltego більш орієнтована на пошук інформації про людей, а SpiderFoot - загроз у системах безпеки;

8) Maltego інтегрується із intenzer Analyze, Polonious, Tisane, а SpiderFoot із censys, Hunter, OpenDNS, Pulsedive, RisklQ, SecurityTrails, VirusTotal;

У роботі розглянуто програмне забезпечення, призначене для збору інформації з відкритих джерел - Maltego і SpiderFoot, яке має ряд відмінностей але одну функцію. З ним кожен може долучитися до розшуку шахраїв у Інтернеті та досить швидко і ефективно знайти усю необхідну інформацію для кіберполіції, щоб пришвидшити процес затримання такого роду злочинців.

Список використаних джерел:

I.СтецьА. Кіберполіція розповіла про шахрайські схеми під час війни. ZAXID.NET.
URL: https://zaxid.net/kiberpolitsiya_rozpovila_pro_shahrayski_shemi_pid_chas_viyni_nl540381 (дата звернення: 08.10.2022).

2. Maltego - Инструменты Kali Linux. Инструменты Kali Linux - Список инструментов для тестирования на проникновение и их описание. URL: https://kali.tools/?p=127 (дата звернення: 08.10.2022).
3. SpiderFoot - Инструменты Kali Linux. Инструменты Kali Linux - Список инструментов для тестирования на проникновение и их описание. URL: https://kali.tools/?p=76 (дата звернення: 08.10.2022).
4. What Is Open Source Intelligence and How Is it Used?. Recorded Future: Securing Our World With Intelligence. URL: https://www. recordedfuture.com/open-source-intelligence-defmition (date of access: 08.10.2022).

Кісіль Ростислав Вікторович
курсант 1 курсу факультету №4 Харківського національного університету внутрішніх справ

Світличний Віталій Анатолійович
доцент кафедри протидії кіберзлочинності факультету №4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент, (науковий керівник)

ШАХРАЙСТВО В ІНТЕРНЕТІ ПІД ЧАС ВІЙНИ. ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ ТА ПОРЯДОК ДІЙ НА ВИПАДОК ВИЯВЛЕННЯ ЗЛОЧИНУ

Шахрайство в інтернеті буває різних видів, за час війни було виявлено багато випадків продажу не існуючих квитків на потяг, або про здачу в оренду квартир в безпечних місцях по передплаті, після якої псевдо орендатори перестають відповідати.

Попри цього було виявлено інші кіберзлочини, наприклад можливі сценарії:

Шахрайські сайти в інтернеті для допомоги українцям, які постраждали від війни, або збору коштів на ЗСУ. Фішингові сайти пропонують заповнити платіжну форму: номер картки, термін дії, тризначний код безпеки зі зворотного боку картки, код SMS від банку. Злочинці використовують отриману інформацію, щоб украсти гроші з рахунку.

Шахрай може зателефонувати від імені співробітника банку та повідомити, що ваша картка заблокована (або їй загрожує блокування). Щоб «розблокувати» її, шахрай обов'язково запитає конфіденційні реквізити.

Шахрай телефонує під виглядом співробітника Пенсійного фонду (чи іншої державної установи) та повідомляє про те, що на картку будуть перераховані гроші (надбавка до пенсії, додаткові нарахування, матеріальна допомога тощо). Або навпаки, що картку заблоковано та необхідно перевести ко-