Дмитро ЛАНДЕ,
завідувач кафедри інформаційної безпеки
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»,
керівник наукового центру Державної наукової установи
«Інститут інформації, безпеки і права
Національної академії правових наук України»,
доктор технічних наук, професор
Ігор СУБАЧ,
завідувач кафедри Інституту спеціального зв'язку
та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»,
доктор технічних наук, старший науковий співробітник

РОЗВІДКА У ВІДКРИТИХ ДЖЕРЕЛАХ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Важливим інструментом забезпечення інформаційної та кібернетичної безпеки на цей час є розвідка у відкритих джерелах (Open Source Intelligence, OSINT), за допомогою якої забезпечується добування інформації з Інтернет, соціальних мереж, публічних баз даних, новинних статей, які доступні для загального використання [1]. На цей час для більш ефективного використання OSINT все частіше використовуються так інструменти, як інтелектуальний аналіз даних, технології штучного інтелекту, машинне навчання.

Користувачі, що відвідують відкриті інформаційні ресурси Інтернету, вносять неявні експертні оцінки. Виявлення та екстрагування цих прихованих знань є важливою складовою інформаційної та кібернетичної безпеки. Цей процес зазвичай виконується з використанням методології та стеку технологій OSINT, які забезпечують узагальнення отриманих знань та їх аналітичну обробку. Використання OSINT може допомогти виявляти загрози та потенційних злочинців, сприяти виявленню вад в безпеці в системах та програмах, забезпечувати контроль за розповсюдженням небажаних матеріалів та інформації.

Мета роботи – представлення кейсів застосування OSINT як інструмента забезпечення інформаційної та кібернетичної безпеки.

Розслідування кіберінцидентів

Методика, що описується у першому кейсі, базується на аналізі змістовної складової інтернет-простору і дозволяє визначати об'єкти кібербезпеки та їх зв'язки. Застосування цієї методики допомагає вирішувати різноманітні завдання, включаючи цільовий збір та обробку інформації, виділення потрібних сутностей, встановлення зв'язків між ними та створення мережі об'єктів. Також за допомогою цієї методики можна проводити кластерний аналіз мережі об'єктів, визначати центри кластерів та виконувати інші подібні завдання. Ця методика розслідування кібернетичних інцидентів, що вже відбулися передбачає виконання наступних кроків [2]: 1) Встановлення часового проміжку, під час якого відбувся кібернетичний інцидент. 2) Збір найбільш можливого обсягу посилань на повідомлення з Інтернету, що стосується вказаного кіберінциденту. 3) Отримання повних текстів всіх повідомлень, що відповідають зібраним посиланням. 4) Групування отриманих повідомлень за часом їхньої публікації в мережі Інтернет та побудувати часову послідовність динаміки публікацій. 5) Дослідження часового ряду, виявлення аномалій, періодичності тощо, порівняння з відомими шаблонами кібернетичних інцидентів. 6) Виділення з текстів концепти – іменовані сутності. Відображення на географічній карті топонімів, що відповідають вибраному кібернетичному інциденту. 7) Формування мережі цих сутностей та знаходження групи найбільш зв'язаних. 8) Формування дайджесту з повідомлень, що відображають найважливіші аспекти визначеного кіберінциденту.

Як приклад розслідування за цією методикою можна навести розслідування кібератаки Colonial Pipeline (7 травня 2021 року), яка за оцінками преси була найуспішнішою кібератакою на нафтову інфраструктуру США. У відповідності із представленою методикою було зібрано декілька тисяч документів за визначений проміжок часу, побудовано динаміку їх публікацій (рис. 1, див. на с. 47), для виявлення аномалій і подібності фрагментів досліджуваного часового ряду у різних масштабах

використовувався вейвлет-аналіз. Після цього були сформовані мережі сутностей, для відображення яких був використаний спеціальний програмний модуль, результат роботи якого – набір даних у форматі CSV, що відповідає матриці суміжності. Відображення і кластеризація здійснювалось за допомогою системи аналізу графів Gephi [3]. У програмі Gephi відкривається створений CSV-файл. На основі зібраних даних було сформовано дайджест – список релевантних документів, що відображають різні найбільш важливі різні аспекти визначеного кіберінциденту.

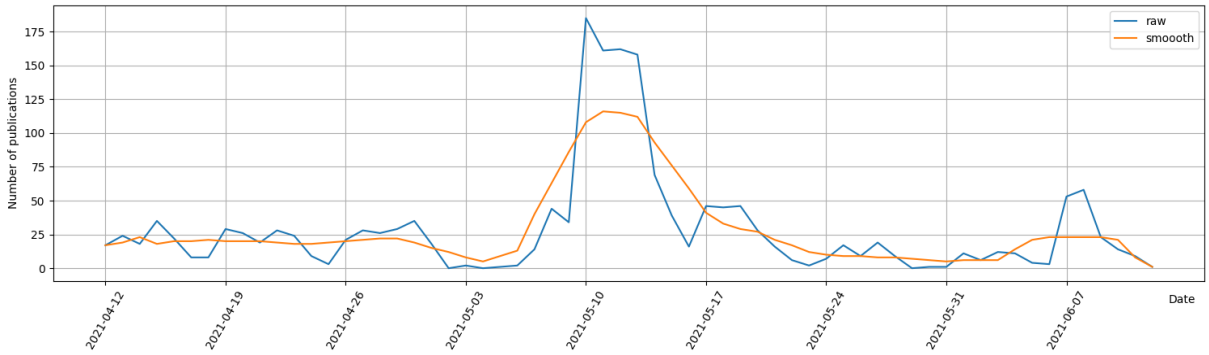

Рисунок 1 – Вихідний та згладжений ряди

Після цього були сформовані мережі сутностей, відображення і кластеризація якої здійснювалось за допомогою системи аналізу графів Gephi. На основі зібраних даних було сформовано дайджест – список документів, що відображають найбільш важливі різні аспекти кіберінциденту.

Виявлення злочинних кібернетичних угрупувань

Другий кейс присвячено проблемі екстрагування понять із текстів документів із мережевих джерел, а саме злочинних російських і білоруських хакерських угрупувань, що є учасниками сучасної кібервійни, а також відповідного шкідливого програмного забезпечення. Для вирішення цієї проблеми пропонується методика, сутність якої полягає у виконанні таких технологічних операцій, як: 1) добування інформації; 2) екстрагування понять – об’єктів кібербезпеки; 3) фільтрація понять із залученням експертів або засобів штучного інтелекту; 4) формування мережі об’єктів кібербезпеки; 5) аналіз (у тому числі кластеризація) і

візуалізація цієї мережі; 6) візуалізація динаміки появи понять у часі.

Проводився аналіз активності російських/білоруських хакерських угрупувань впродовж 2022 і початку 2023 року. Для цього на 1-му етапі формується тематичний інформаційний масив, для чого мають використовуватись наявні інформаційно-пошукові системи, як загальнодоступні, так і корпоративні системи контент-моніторингу, наприклад систем контент-моніторингу Cyber Aggregator, Attack Index і InfoStream, які дозволяють збирати інформацію із веб-сайтів і 12 соціальних мереж. Для отримання інформаційного масиву публікацій щодо кібербезпеки необхідно визначити необхідний період опрацювати тематичний запит, наприклад такий:

хакер|(вредоносн-программн)|(шкідл-програмн)|(кибер-атак)|кібератак|(кібер-атак)|кібератак

Після цього застосовувалась методологія визначення іменованих сутностей в області кібербезпеки [4], а на останньому етапі здійснюється кластерний аналіз відібраної мережі та знаходження об’єктів – центрів кластерів (рис. 2).

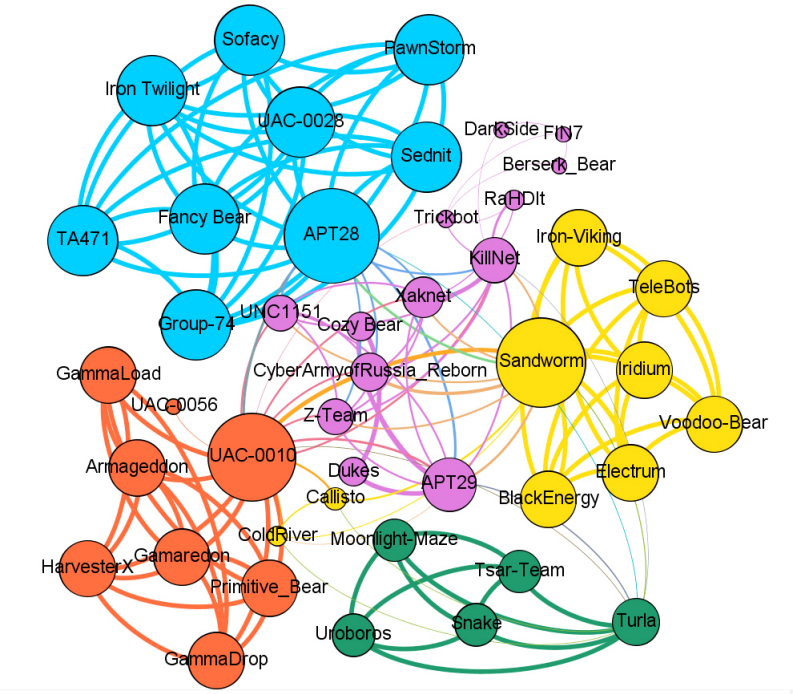

Рисунок 2 – Мережа основних хакерських угрупувань із росії/білорусії

Результати контент-моніторингу інтернет-ресурсів і подальшої кластеризації вказують на переважну приналежність розглянутих хакерських угрупувань до спецслужб рф і білорусії, а саме ФСБ рф; ГУ ГШ ЗС рф (ГРУ); СЗР рф; Міністерство оборони рб; інші проросійські угрупування.

Наведені в доповіді методики враховують приховані знання, внесені експертним мережевим середовищем. Разом з цим, публікація детальної інформації з полів кібервійни у відкритих джерелах, безумовно, може бути застосована і ворогом, тому, вочевидь, вимагає деяких обмежень, які мають законодавчо регулюватись у сучасних умовах.

Література:

1. ATP 2-22.9. Army Techniques Publication No. 2-22.9 (FMI 2-22.9). Open-Source Intelligence. Headquarters Department of the Army Washington, DC. 2012, 10 July.

2. D. Lande, O. Puchkov, I. Subach, M. Boliukh, D. Nahornyi OSINT investigation to detect and prevent cyber attacks and cyber security incidents // Information Technology and Security. 2021. Vol. 9(2). P. 209–218. DOI: doi.org/10.20535/2411-1031.2021.9.2.249921 (дата звернення: 04.03.2023).

3. Cherven K. Mastering Gephi Network Visualization. – Packt Publishing. 2015. 378 p. ISBN 78-1-78398-734-4.

4. Ланде Д. В., Пучков О. О., Субач І. Ю. Методика виявлення об’єктів кібербезпеки на базі технології OSINT. *Інформаційні технології і безпека* : матеріали XXII Міжн. наук.-практ. конф. ІТБ-2022. Київ : Інжиніринг. С. 9–13. URL: http://dwl.kiev.ua/art/itb2022-1/2022itb1.pdf (дата звернення: 05.03.2023).

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ
КОМІТЕТ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПИТАНЬ
НАЦІОНАЛЬНОЇ БЕЗПЕКИ, ОБОРОНИ ТА РОЗВІДКИ
АПАРАТ ВЕРХОВНОЇ РАДИ УКРАЇНИ
ДЕРЖАВНА НАУКОВА УСТАНОВА
«ІНСТИТУТ ІНФОРМАЦІЇ, БЕЗПЕКИ І ПРАВА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ»
ІНСТИТУТ ДОСЛІДЖЕННЯ КІБЕРВІЙНИ

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ РОЗВИТКУ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Збірник матеріалів
науково-практичного семінару

(Київ, 23 березня 2023 року)

Київ
2023

УДК 004.056:351.746.1
О-64

***Рекомендовано до друку*:**
Вченою радою Державної наукової установи «Інститут інформації, безпеки і права» Національної академії правових наук України (протокол № 4 від 11 квітня 2023 року);
засіданням Науково-організаційного центру Національної академії Служби безпеки України (протокол № 7 від 05 квітня 2023 року)

О-64 **Організаційно-правові** засади розвитку системи забезпечення кібербезпеки України : збірник матер. наук.-практ. семінару (Київ, 23 березня 2023 р.) / упорядн.: Ю. Найдьон, В. Пилипчук, Н. Ткачук, М. Теплюк, Т. Давидова, Л. Заславська. – Київ : НА СБУ, 2023. – 144 с.

До збірника увійшли матеріали, в яких висвітлюються актуальні проблеми щодо формування та реалізації державної політики у сфері забезпечення кібербезпеки України; становлення національної системи кібербезпеки та пріоритетів її розвитку; правового регулювання організації та діяльності суб'єктів забезпечення кібербезпеки та юридичної відповідальності у сфері кібербезпеки.

Рекомендовано для фахівців, експертів сфери забезпечення інформаційної і кібербезпеки, здобувачів вищої освіти, аспірантів, наукових і науково-педагогічних працівників, а також всіх, хто цікавиться тематикою науково-практичного семінару.

УДК 004.056:351.746.1

ЗМІСТ