УДК 004.056.53:004.89

ПОБУДОВА ДЕРЕВА РІШЕНЬ ДЛЯ ПРОЦЕДУРИ КІБЕРРОЗВІДКИ

Д. В. Медвецький[1,a], О. В. Козленко[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У цій роботі досліджується предметна область процедури кіберрозвідки для розуміння її технік та інструментів в залежності від типу і методології. Проводиться огляд математичної концепції моделі дерева рішень. Результат цієї роботи допоможе більш структуровано підходити до збору і аналізу даних під час процедури розвідки у кіберпросторі.

Ключові слова: кіберрозвідка, дерево, джерело, алгоритм, підхід, метод

Вступ

Стрімкий розвиток інформаційних технологій постійно супроводжує потреба у захисті інформаційних систем будь-якого призначення, оскільки росте як і кількість цих систем, так і вдосконалюються навички зловмисників у кіберпросторі. Усі ці аспекти впливають на кількість загроз у кіберпросторі, на їх складність і витонченість. Тому виникає необхідність шукати структуровані підходи до збору та аналізу даних про ті чи інші кіберінциденти, задля ефективного запобігання загроз або зменшення їх впливу. У цьому нам і допоможе процедура кіберрозвідки.

1. Постановка задачі

Метою дослідження є побудова дерева рішення для процесу кіберрозвідки задля більш ефективного і структурованого збору та аналізу даних.

2. Поняття кіберрозвідки

2.1. Особливості кіберрозвідки

Термін кіберрозвідка (англ. cyber threat intelligence) можна визначити як збір і аналіз інформації, добутої з електронних обчислювальних машин, інформаційно-телекомунікаційних систем або будь-якого іншого середовища обробки даних [1]. Вона є невід'ємною частиною кібербезпеки і дедалі частіше стає ефективним методом захисту не тільки від поточних загроз, а й від запобігання їх у майбутньому. На відміну від традиційних засобів захисту, таких як антивіруси, фаєрволи, системи IPS/IDS чи системи SIEM, кіберрозвідка має важливу особливість – здатність команди захисту до прогнозування.

Ось ще декілька особливостей [2, 3]:

- замість очікування кібератаки, є можливість її запобігти і не дозволити зловмиснику завдати шкоди;
- можна створити більш індивідуальні і ефективні стратегії захисту, шляхом вивчення суб'єктів загроз спрямованих на певну галузь чи регіон;
- допомога керівникам при ухваленні стратегічних рішень, щодо захисту організації.

Слід зауважити, що сама по собі процедура не є одноразовою дією, а являє собою трудомісткий процес, який можна представити у вигляді кроків:

1. визначення методів і мети;
2. збір даних;
3. обробка даних;
4. аналіз результатів;
5. розповсюдження результатів.

2.2. Класифікація процедур кіберрозвідки

Процес кіберрозвідки умовно можна розділити на типи і методи, які, у свою чергу теж поділяються: типи – в залежності від рівня деталізації і сфери застосування отриманих даних, а методи – безпосередньо за описом способів отримання цієї інформації. Спочатку про типи [4, 5]:

- Тактична розвідка – зосереджена саме на поточних загрозах. Основний фокус йде на забезпечення безпеки системи шляхом надання конкретних технічних даних про загрози;
- Оперативна розвідка – фокусується на дослідженні діяльності APT-груп для кращого розуміння зловмисника;
- Стратегічна розвідка – більш широкий погляд на процедуру розвідки.

Оскільки зловмисники ніколи не діють в умовах «вакууму», потрібно також брати до уваги геополітичні ризики, економічні фактори тощо.

Перейдемо до методів. Зазвичай вони позначаються як «INT» (від англ. Intelligence) і, оскільки чіткої стандартизації немає, розглянемо декілька основних методів [6]:

- Human Intelligence (HUMINT);
- Imagery Intelligence (IMINT);
- Signals Intelligence (SIGINT);

[a] meddvv23@gmail.com

- Open-Source Intelligence (OSINT);
- Measurement and Signature Intelligence (MASINT).

3. Концепція дерева рішень

Дерево рішень [7] – це графічна модель, яка представляє собою деяку послідовність рішень і виступає у ролі засобу для розв'язання первісної проблеми. Інакше кажучи, це граф, вершини якого відповідають ключовим станам, а дуги – різним подіям, що можуть відбутися в ситуації, яка обумовлюється вершиною. Саме через невизначеності, що виникають у процесі кіберрозвідки, можна використати модель дерева рішень для процедури кіберрозвідки, оскільки це надасть уяву про вплив випадкових факторів на результат, при виборі конкретних дій чи інструментів.

4. Побудова дерева

Проаналізувавши предметну область, можна виокремити деякі типи вузлів, а саме:

- корінь;
- техніка;
- сабтехніка;
- процедура;
- інструмент.

За допомогою експертної оцінки, вузлам надано ваги, які відображені в таблиці 1.

Таблиця 1: Типи вузлів та їх ваги

Node	Type	Weight
Active Scanning	RecTechnique	4.5
Scanning IP Blocks	RecSubTechnique	4.2
Nmap	tool	4.8
Routersploit	tool	3.8
Vulnerability Scanning	RecSubTechnique	4.5
Nessus	tool	4.8
OpenVAS	tool	4.3
Wordlist Scanning	RecSubTechnique	3.5
Subdomain Enumeration	procedure	3.7
GoBuster	tool	3.6
Gather Victim Host Informationr	RecTechnique	3.8
Hardware	RecSubTechnique	3.2
Software	RecSubTechnique	4.1
Phishing	procedure	5.0
Firmware	RecSubTechnique	2.8
Client Configurations	RecSubTechnique	3.5
Gather Victim Identity Information	RecTechnique	4.3
Credentials	RecSubTechnique	4.7
Email Addresses	RecSubTechnique	3.7
OpenSourceResearch	procedure	4.0
Hunter.io	tool	4.1
Employee Names	RecSubTechnique	3.5

Таблиця 1: Типи вузлів та їх ваги (Продовження)

Node	Type	Weight
Gather Victim Network Information	RecTechnique	4.0
Domain Properties	RecSubTechnique	3.7
Whois	tool	4.5
SecurityTrails	tool	4.0
DNS	RecSubTechnique	4.3
Network Trust Dependencies	RecSubTechnique	3.5
Network Topology	RecSubTechnique	4.1
IP Addresses	RecSubTechnique	3.9
Network Security Appliances	RecSubTechnique	3.8
Gather Victim Org Information	RecTechnique	3.7
Determine Physical Locations	RecSubTechnique	2.9
Business Relationships	RecSubTechnique	3.5
Identify Business Tempo	RecSubTechnique	2.9
Identify Roles	RecSubTechnique	4.0
SocialEngineering	procedure	4.6
Phishing for Information	RecTechnique	4.6
Spearphishing Service	RecSubTechnique	4.4
Spearphishing Attachment	RecSubTechnique	4.3
Spam	procedure	3.2
Spearphishing Link	RecSubTechnique	4.5
EvilProxy	tool	4.3
Evilginx2	tool	4.6
Spearphishing Voice	RecSubTechnique	4.0
SIMswapping	procedure	3.5
BlackCat	tool	4.1
Search Closed Sources	RecTechnique	3.5
Threat Intel Vendors	RecSubTechnique	3.7
Subdomain Enumeration	procedure	3.7
sublist3r	tool	3.6
Purchase Technical Data	RecSubTechnique	4.0
DarkWebResearch	procedure	3.9
Search Open Technical Databases	RecTechnique	3.5
DNS Passive DNS	RecSubTechnique	4.0
DNSDumpster	tool	4.1
SecurityTrails	tool	4.2
WHOIS	RecSubTechnique	3.8

Для побудови дерева і візуалізації результатів використовувалася графічна база даних Cayley [8] у поєднанні з GizmoAPI [9]. За допомогою запитів на мові gizmo, було побудовано дерево, де відображено зв'язки між вузлами (Рисунок 1).

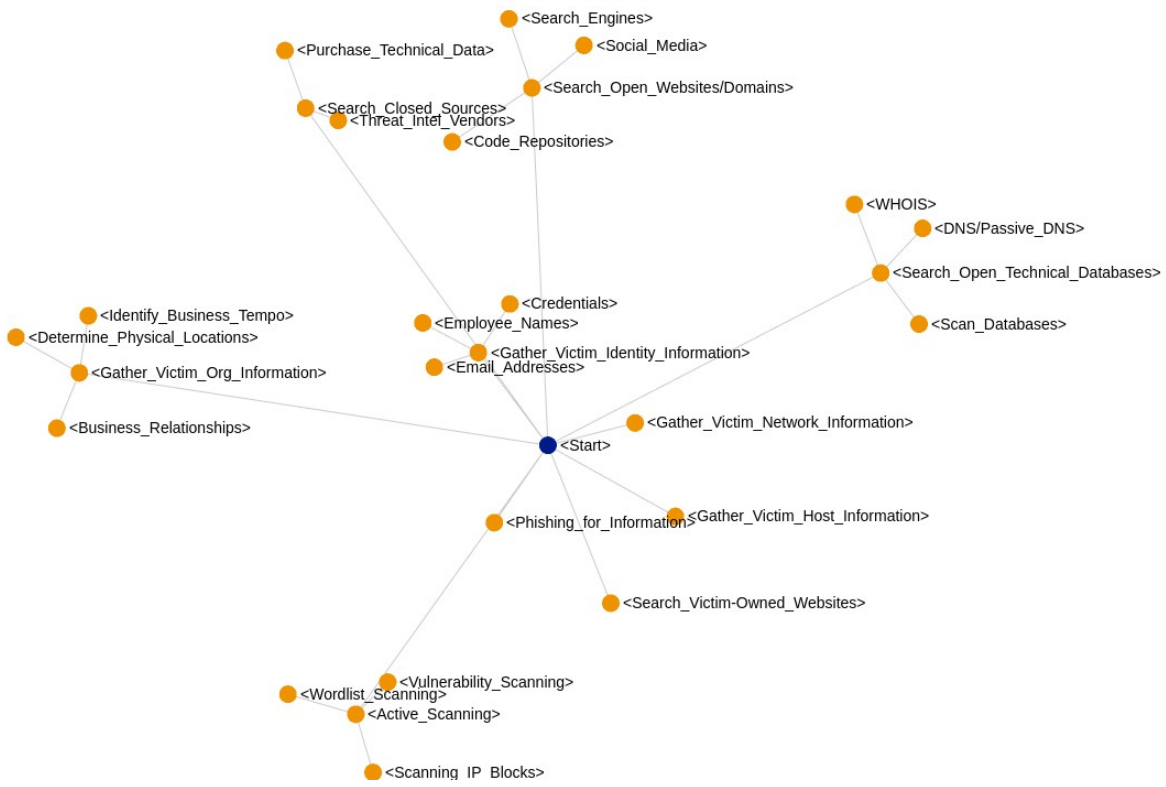

Рис. 1. Дерево зв'язків для процедури у кіберрозвідці

Висновки

У цій статті було запропоновано підхід до побудови дерева рішень у сфері кіберрозвідки, де кожному елементу дерева (техніці, сабтехніці, інструменту або процедурі), за допомогою експертних оцінок, призначається вага. Для моделювання структури дерева було використано графову базу даних Cayley, що дозволяє зберігати та візуалізувати відношення між об'єктами та здійснювати запити до них за допомогою мови Gizmo. Розроблений підхід дозволяє не лише будувати гнучкі моделі процесу збору розвідданих, але й визначати, чи є зібраної інформації достатньо для завершення розвідки на поточному рівні. Запропонована система вагування дозволяє враховувати контекст використання інструментів, що підвищує точність прийняття рішень.

Перелік використаних джерел

1. *Kyva V.*, *Sudnikov Y.*, *Voitko O.* Методи розвідки кіберпростору // Сучасні інформаційні технології у сфері безпеки та оборони. — 2018. — Груд. — Т. 33. — С. 45—52. — DOI: 10.33099/2311-7249/2018-33-3-45-52.
2. *Distribution I. I.* Розвідка кіберзагроз. — URL: https://iitd.ua/rozvidka-kiberzagroz/.
3. *Xcitium.* What is Cyber Threat Intelligence? — URL: https://www.xcitium.com/knowledge-base/cyber-threat-intelligence/.
4. *GmbH M. T.* Understanding the Different Types of Intelligence Collection Disciplines. — URL: https://www.maltego.com/blog/understanding-the-different-types-of-intelligence-collection-disciplines/.
5. *CrowdStrike Holdings I.* Cyber Threat Intelligence Explained. — URL: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/.
6. *Kootneeti T.* A Comprehensive Overview of Intelligence Gathering Methods: HUMINT, SIGINT, IMINT, and OSINT. — URL: https://thekootneeti.in/2022/08/03/a-comprehensive-overview-of-intelligence-gathering-methods-humint-sigint-imint-and-osint/.
7. *Кушлик-Дивульська О. І.*, *Кушлик Б. Р.* Основи теорії прийняття рішень : Навчальний посібник. — Київ : НТУУ «КПІ», 2014. — С. 94. — URL: https://ela.kpi.ua/handle/123456789/6917.
8. *cayleygraph.* Cayley: An open-source graph database. — 2019. — URL: https://github.com/cayleygraph/cayley ; GitHub repository, Apache-2.0 license.
9. *Cayley Documentation.* Gizmo API. — 2020. — URL: https://cayley.gitbook.io/cayley/query-languages/gizmoapi.