УДК 004.056.53
DOI: 10.31673/2409-7292.2024.030007

Король О. Г., Лаптєва Т. О.

МЕТОД ВИКОРИСТАННЯ КІБЕРРОЗВІДКИ ДЛЯ ВИЯВЛЕННЯ ІНДИКАТОРІВ КОМПРОМЕТАЦІЇ НА БАЗІ МАТРИЦІ MITRE ATT&CK

В сучасних умовах існує необхідність створення системи обробки інформації та ухвалення рішень щодо можливих атак в інформаційній сфері. Особливо корисною є інформація про наміри порушників, про підготовку до атаки. Тобто необхідною та достатньою умовою для побудови успішної системи захисту є повнота інформації про кіберзагрозу. З цією метою використовується індикатори компрометації (IOC), які безпосередньо пов’язані з поняттям Threat Intelligence. Індикатори компрометації можуть бути використані для пошуку, ідентифікації та класифікації загроз в рамках процесу розвідки загроз. Це дозволяє вже на початковому етапі підготовки до атаки реагувати на потенційні загрози та приймати відповідні заходи безпеки для захисту інформації. Предметом дослідження є актуальне наукове завдання по виявленню індикаторів компрометації на базі матриці MITRE ATT&CK. Доведено необхідність кіберрозвідки для пошуку індикаторів компрометації та припинення можливих атак на інформаційну систему. Проаналізовано модель класифікації індикаторів компрометації «The Pyramid of Pain», що складається з шести рівнів та демонструє взаємозв'язок між типами індикаторів, що використовуються для виявлення діяльності зловмисника. Розглянуто MITRE ATT&CK Matrix , яка є загальнодоступною базою знань про тактики та техніки зловмисників протягом реалізації кібератаки. Структура ATT&CK є потужним інструментом для покращення кіберзахисту та розвідки загроз. Дослідження довели, що без фахівців люба система виявлення індикаторів компрометації не працюватиме достатньо адекватно, не можна заздалегідь передбачити всі дрібниці та винятки. Тому тільки комплексний підхід може надати захист від кібератак.

Ключові слова: захист інформації, індикатори компрометації, кіберрозвідка, піраміда Боля, матриця, порушник, класифікація.

Вступ

В сучасних умовах, умовах війни з росією, окрім прямого зіткнення військ набирає обертів кібервійна. Для успішного кібернападу необхідна інформація, а для отримання інформації необхідна кіберрозвідка або Threat Intelligence. Немає сумніву, що превентивне отримання інформації про кіберзагрози це вже шлях до її подолання, але нажаль саме по собі це інфраструктуру не убезпечить. Потреба «розвідувальних даних» – це наслідок розвитку галузі інформаційної безпеки, зміни її рівня зрілості в позитивний бік.

Необхідно створити систему яка допоможе обробити отриману інформацію та прийняти міри захисту від можливої атаки. Особлива корисна інформація про наміри порушників, про підготовку до атаки. Тобто необхідною та достатньою умовою для побудови успішної системи захисту є повнота інформації про кіберзагрозу. З цією метою використовується індикатори компрометації (IOC), які безпосередньо пов’язані з поняттям Threat Intelligence. Індикатори компрометації можуть бути використані для пошуку, ідентифікації та класифікації загроз в рамках процесу розвідки загроз. Це дозволяє вже на початковому етапі підготовки до атаки реагувати на потенційні загрози та приймати відповідні заходи безпеки для захисту інформації. Тому розробка науково-методичного апарату виявлення індикаторів компрометації за допомогою Cyber Threat Intelligence є актуальним завданням.

Аналіз літературних джерел та формулювання проблеми

Cyber Threat Intelligence (кіберрозвідка) – це пошук інформації про потенційних зловмисників, зокрема про серйозні кіберзлочинні групи, які називаються APT-угрупованнями (Advanced Persistent Threat -ускладнена стійка загроза, або цільова кібератака). Ці APT-угруповання являють собою стійке кіберзлочиннє формування, в якому чітко розподілені функції зловмисників: є організатори, є програмісти, є фахівці в галузі соціальної інженерії, та своя технічна підтримка. Виявлення таких угруповань здійснюється за допомогою виявлення індикаторів компрометації.

Методам та методикам використання кіберрозвідки для виявлення кіберзлочинних груп та індикаторів компрометації присвячено велика кількість публікацій. Так у роботі [1] обґрунтовано актуальність та необхідність проведення розвідувальних заходів у

кібернетичному просторі противника. Визначено етапи, складові та методи кібернетичної розвідки. Але шляхи пошуку індикаторів компрометації не вказані.

У роботах [2, 3] наведено перелік критичних даних, які необхідно добути у ході проведення кіберрозвідки. Досліджено засоби розвідки кібернетичного простору, зроблені порівняльні характеристики засобів кіберрозвідки та визначено критерії щодо їх побудови. Використання засобів кіберрозвідки з метою пошуку індикаторів компрометації не наводяться.

У роботах [4, 5] визначаються основні переваги та недоліки активного та пасивного методу добування розвідувальних даних та запропоновано комплексний підхід використання переваг кожного методу, що дасть можливість підвищити ефективність проведення кіберрозвідки у інформаційних мережах. Але детального методичного апарату пошуку індикаторів компрометації не наведено, наведений матеріал обмежено загальними принципами кіберрозвідки.

У роботі [6] проведено аналіз індикаторів кібератак та інструменти їх отримання. Здійснено порівняння стандартів опису індикаторів компрометації та платформ їх обробки. Але загального методу виявлення індикаторів компрометації за допомогою кіберрозвідки ненаведене.

У роботах [7, 8] розроблено методику Threat Intelligence в задачах оперативного виявлення та блокування кіберзагроз державним інформаційним ресурсам. Ця методика дає можливість покращити продуктивність роботи аналітиків кібербезпеки та підвищити захищеність ресурсів та інформаційних систем, але розповсюдження методики на усі інформаційні ресурси не було зроблено. Методика має вузький напрямок.

Проте, більшість наукових досліджень мають обмежений характер і спрямовані на вдосконалення нормативно-правового регулювання інформаційного простору, призначені для вирішення окремих часткових завдань захисту інформації, не враховують особливості сучасних кіберзагроз.

Таким чином, на підставі проведеного аналізу, результатів вивчення наукових публікацій за темою досліджень, патентів, монографій та практичних розробок встановлено, що на сучасному етапі розвитку прогресивних інформаційних технологій остаточно не вирішено питання виявлення кіберзагроз, тому актуальним є завдання виявлення індикаторів компрометації за допомогою кіберрозвідки.

Мета роботи та цілі дослідження

Метою роботи є виявлення індикаторів компрометації на базі матриці MITRE ATT&CK за допомогою кіберрозвідки.

Для вирішення поставленої мети розглянуто такі завдання:

проаналізувати застосування кіберрозвідки для виявлення індикаторів компрометації;

дослідити взаємозв'язок між типами індикаторів, що використовуються для виявлення діяльності порушника;

запропонувати виявлення індикаторів компрометації за допомогою матриці MITRE ATT&CK.

Метод використання кіберрозвідки для виявлення індикаторів компрометації на базі матриці MITRE ATT&CK

Первинні дані Threat Intelligence можна отримувати з різних джерел. Це можуть бути безкоштовні підписки, інформація від партнерів, група технічного розслідування компанії та ін.

З проведеного аналізу свідчить, що існує чотири основні етапи роботи з інформацією, отриманою в рамках процесу Threat Intelligence (рис. 1):

отримання інформації, первинна обробка;

детектування індикаторів компрометації;

ретроспективна перевірка;

сповіщення відповідних установ про загрозу.

Рис.1. Схематичний процес виявлення індикаторів компрометації

Одним з головних завданнь Threat Intelligence є виявлення індикаторів компрометації.

Indicator of Compromise (індикатори компрометації) - це ознаки або показники, які вказують на можливість або наявність вторгнення, компрометації або несанкціонованої діяльності в комп'ютерній системі або мережі.

Для забезпечення систематичного підходу до обробки інформації, рекомендується розподілити індикатори, отримані з Threat Intelligence, на дві широкі категорії - індикатори, пов'язані з хостами, тобто конкретними комп'ютерами або серверами, і індикатори, пов'язані з мережею, тобто мережевими з'єднаннями і трафіком. Виявлення мережевих індикаторів може, ще не свідчити про однозначну компрометацію системи, і навпаки детектування хостових індикаторів, як правило, достовірно сигналізує про зловмисну активність.

Найпопулярнішим рішенням класифікації індикаторів компрометації є «піраміда Болю», введена David Bianco у 2013 році, що зображена на рис. 2. Вона демонструє взаємозв'язок між типами індикаторів, що використовуються для виявлення діяльності зловмисника, та тим, як багато складнощів йому створює блокування певного рівня.

Дана структура, що використовується для вимірювання потенційної користі даних про загрози, оцінює користь даної інформації, враховуючи складнощі, пов'язані з отриманням цієї інформації та ухиленням від виявлення на різних рівнях (з точки зору порушника). Чим вище рівень в піраміді, тим більше часу та зусиль необхідно витратити на виправлення тактик і технік, які використовуються для атак на інфраструктуру.

Хеш-значення – це числове значення фіксованої довжини, яке унікально ідентифікує дані.

IP-адреса використовується для ідентифікації будь-якого пристрою, підключеного до мережі. З точки зору захисту, знання IP-адрес зловмисника, може бути використано для блокування, видалення або заборона вхідних запитів з IP-адрес на вашому периметрі або зовнішньому брандмауері.

Доменні імена можна розглядати як відповідність IP-адреси та рядку тексту.

Мережевим артефактом може бути назва агента (браузера) користувача, інформація про C2-сервер або певні URI, за якими слідують запити HTTP POST. Артефакти хоста – це сліди або спостережувані елементи, які зловмисники залишають у системі, наприклад значення реєстру, підозрілі виконання процесів, моделі атак або файли, видалені зловмисними програмами, або будь-що, що стосується поточної загрози.

Інструменти – це коли зловмисники використовують утиліти для створення шкідливих макродокументів (maldocs) для спроб фішингу, бекдори, які можна використовувати для встановлення з'єднання з C2-серверами (інфраструктурою для командування та контролю), будь-які власні .exe та .dll- файли, корисні навантаження або кейлогери. Антивірусні

© Король, О. Г., & Лаптєва, Т. О. (2024). Метод використання кіберрозвідки для виявлення індикаторів компрометації на базі матриці MITRE ATT&CK. Сучасний захист інформації, 3(59), 69–74. https://doi.org/10.31673/2409-7292.2024.030007.

сигнатури, правила виявлення та правила YARA можуть стати чудовою зброєю для боротьби з зловмисниками на цьому етапі.

Рис. 2. Візуалізація піраміди Болю [10].

TTPs (Tactics, Techniques & Procedures) – це система яка включає в себе всю матрицю MITRE ATT&CK [4, 11].

У цьому дослідженні зупинимося на верхньому рівні піраміди, а саме на TTPs. Системі яка включає в себе всю матрицю MITRE ATT&CK. Матриця MITRE ATT&CK визначає всі кроки, вжиті зловмисником для досягнення своєї мети.

Задля проведення якісного дослідження необхідно обирати для себе оптимальну модель згідно з якою можна передбачити подальші потенційні дії зловмисника. Після проведеного аналізу ми обрали модель Cyber Kill Chain. Саме Kill Chain допоможе розглянути життєвий цикл ATT&CK від MITRE.

MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) – це загально доступна база знань про тактики, техніки і інформацію про зловмисників протягом реалізації атаки [3, 10].

Американська некомерційна компанія MITRE представила матрицю (рис. 3), яка описує та класифікує поведінку зловмисників на основі реальних спостережень. Ця матриця являє собою структурований список відомих типів поведінки зловмисників, які об'єднані в тактики і техніки і згруповані в декількох матрицях. Оскільки цей список досить повно відображає різну поведінку зловмисників при компрометуванні мереж, він корисний для розвідки загроз, оцінки різних захисних заходів, вивчення фактів і т.д.

Ця матриця досить повно відображає різну поведінку зловмисників при компрометуванні мереж, він корисний для кіберрозвідки, оцінки різних захисних заходів, вивчення дії зловмисників і т. д.

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Connection Proxy
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	PowerShell	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Component Firmware	Exploitation of Vulnerability	DLL Injection	Input Capture	Network Service Scanning	Remote Desktop Protocol	Process Hollowing	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Obfuscation
Component Object Model Hijacking	Legitimate Credentials	DLL Search Order Hijacking	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Regsvcs/Regasm	Email Collection	Exfiltration Over Other Network Medium	Fallback Channels
DLL Search Order Hijacking	Local Port Monitor	DLL Side-Loading	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Regsvr32	Input Capture	Exfiltration Over Physical Medium	Multi-Stage Channels

Рис. 3. Матриця класифікації поведінки зловмисників на основі реальних спостережень (візуалізація компанії MITRE).

Висновки

У статті розглянуто поняття індикаторів компрометації та Threat Intelligence. Наведено декілька переваг індикаторів компрометації таких як раннє виявлення загроз або покращене реагування на інциденти. Наведено перелік джерел, які можна використовувати для збору індикаторів компрометації. Доведено, що розвідка загроз є важливим етапом в процесі забезпечення кібербезпеки, оскільки дозволяє заздалегідь виявити можливі шляхи атак та вжити заходів для їх запобігання. Проаналізовано модель класифікації індикаторів компрометації “The Pyramid of Pain”, що складається з шести рівнів та демонструє взаємозв'язок між типами індикаторів, що використовуються для виявлення діяльності зловмисника. Розглянуто MITRE ATT&CK Matrix – це загальнодоступна база знань про тактики та техніки зловмисників протягом реалізації кібератаки. Структура ATT&CK є потужним інструментом для покращення кіберзахисту та розвідки загроз.

Розуміння та використання MITRE ATT&CK Matrix є важливим інструментом для захисника мережі, оскільки ця матриця дає повну картину можливих атак та етапів їх виконання. Знання про індикатори компрометації допомагає виявити потенційні загрози та недоліки у системах забезпечення безпеки, тоді як розвідка загроз надає можливість передбачити можливі атаки та вжити відповідних заходів для запобігання їм. Завдяки цим підходам, організації можуть покращити свою реакцію на потенційні кіберзагрози, зменшити ризик інцидентів та зберегти свою інформацію, системи та активи в безпеці.

Але без фахівців система не працюватиме достатньо адекватно, не можна заздалегідь передбачити всі дрібниці та винятки. Група моніторингу може прибрати з фінального звіту активність пісочниці, перевірку адміністраторів на успішне блокування шкідливого ресурсу, але додати активність про неуспішне зовнішнє сканування, показуючи замовнику, що його інфраструктуру перевіряють зловмисники. Машина таких рішень не ухвалить. Тому тільки комплексний підхід може надати захист від кібератак.

Таким чином, ефективне використання індикаторів компрометації та розвідки загроз є ключовим компонентом у побудові стратегії кіберзахисту сучасної організації. Використання

© Король, О. Г., & Лаптєва, Т. О. (2024). Метод використання кіберрозвідки для виявлення індикаторів компрометації на базі матриці MITRE ATT&CK. Сучасний захист інформації, 3(59), 69–74. https://doi.org/10.31673/2409-7292.2024.030007.

інструментів, таких як MITRE ATT&CK, у поєднанні з аналізом індикаторів компрометації, дозволяє організаціям не лише швидше виявляти загрози, але й краще розуміти методи та техніки зловмисників. Однак повністю автоматизовані рішення не завжди можуть покрити всі аспекти безпеки — важливим елементом залишається людський фактор. Саме кваліфіковані фахівці здатні оперативно реагувати на нетипові загрози, робити детальний аналіз даних та адаптувати засоби захисту відповідно до нових викликів. Тому інтеграція технологій та людської експертизи є найкращим підходом для створення надійної системи кібербезпеки.

Перелік посилань

1. Кива, В. Ю., Судніков, Є. О., Войтко, О. В. Методи розвідки кіберпростору. Сучасні інформаційні технології у сфері безпеки та оборони. 2018. 33(3) стр.45-52 DOI:10.33099/2311-7249/2018-33-3-45-52

2. Особливості забезпечення національної безпеки у високотехнологічному суспільстві [Електронний ресурс]. Режим доступу до ресурсу : http://www.kbuapa.kharkov.ua.

3. Закон України Про основні засади забезпечення кібербезпеки України. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403 https://zakon.rada.gov.ua/laws/show/2163-19#Text

4. Жилін Артем, Ніколаєнко Богдан, Бакалинський Олександр. Підвищення захищеності державних інформаційних ресурсів за рахунок застосування платформи threat intelligence. Захист інформації.2021. Том 23, №3. Стр136-146 DOI: 10.18372/2410-7840.23.16401

5. MITRE ATT&CK. 2021. [Електронний ресурс] – https://attack.mitre.org/

6. What is a Threat Intelligence Platform (TIP)? 2018. [Електронний ресурс] – https://www.anomali.com/resources/what-is-a-tip

7. Постанова КМУ “Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури” від 19 червня 2019 р. № 518. [Електрон-ний ресурс] – https://zakon.rada.gov.ua/laws /show/518-2019-% D 0%BF#Text.

8. Yevseiev, S., Laptiev, O., Korol, O., Pohasii, S., Milevskyi, S., Khmelevsky,R. Analysis of information security threat assessment of the objects of information activity. International independent scientific journal. Poland. Vol. 1, №34, 2021, pp.33 – 39. ISSN 3547-2340

9. Лаптєв, О. А., Бучик, С. С., Савченко, В. А., Наконечний, В .С., Михальчук, І. І, Шестак, Я. В., Виявлення та блокування повільних ddos-атак за допомогою прогнозування поведінки користувача. Наукоємні технології. Інформаційні технології, кібербезпека. Том 55 № 3 .2022. С.184-192. DOI: 10.18372/2310-5461.55.16908

10. Serhii Yevseiev, Khazail Rzayev, Oleksandr Laptiev, Ruslan Hasanov, Oleksandr Milov, Bahar Asgarova, Jale Camalova, Serhii Pohasii. Development of a hardware cryptosystem based on a random number generator with two types of entropy sources. Eastern-European journal of enterprise technologies. Vol. 5 №9 (119), 2022 P. 6–16. ISSN (print) 1729 - 3774. ISSN (on-line) 1729-4061. https://doi.org/ 10.15587/1729-4061.2022.265774 Scopus.

11. Олександр Лаптєв, Віталій Савченко, Віталій Пономаренко, Сергій. Копитко, Іван Пархоменко. Удосконалення методу підвищення завадостійкості систем виявлення сигналів засобів негласного здобуття інформації. Захист інформації. Том 24 № 3 (2022): Захист інформації. С.128-136. https://jrnl.nau.edu.ua/index.php/ZI/issue/view/906

Надійшла 28.07.2024