КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.161171
УДК 004.056:519.856

Лахно Валерій Анатолійович
д.т.н., професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0000-0001-9695-4543
lva964@nubip.edu.ua

Волошин Семен Михайлович
к.т.н., доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0000-0002-4913-7003
voloshyn@nubip.edu.ua

Мамченко Сергій Миколайович
д.п.н., професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0009-0006-8743-5606
s.mamchenko@nubip.edu.ua

Матієвський Володимир Валерійович
старший викладач кафедри комп'ютерних систем, мереж та кібербезпеки Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0000-0002-1954-8493
mvv@nubip.edu.ua

Лахно Мирослав Валерійович
NET Full Stack Developer в e-Docs.UA, Київ, Україна
ORCID ID: 0000-0001-6979-6076
valss725@gmail.com

РЕАЛІЗАЦІЯ НА PYTHON МЕРЕЖІ БАЙЄСА ДЛЯ АНАЛІЗУ КІБЕРЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ DDOS-АТАКАМИ

Анотація. Дослідження кіберзлочинів, включно з DDoS-атаками, набуває дедалі більшого значення в контексті підвищеної уваги до кібернетичної безпеки, захисту інформації й інфраструктури організацій у сучасному світі, що залежать від цифрових технологій і комп'ютерних систем. У статті обґрунтовано, що використання байєсівських мережевих моделей (далі мережі Байєса — МБ) для аналізу кіберзлочинів (на прикладі розповсюджених DDoS-атак) дасть змогу врахувати безліч змінних та ймовірностей. Це робить схожі дослідження більш точними та надійними. На прикладі дослідження МБ у прикладному програмному пакеті GeNIe, продемонстровано процес використання апарату МБ для задачі розслідування кіберзлочину, пов'язаного з реалізацією з комп'ютера зловмисника DDoS-атакам. Описана МБ допомагає криміналістам у сфері розслідування подібних кіберзлочинів виявляти мотиви та зв'язки між учасниками атаки, що безумовно покращить ефективність розслідування. Демонстрація застосування м за допомогою пакета моделювання GeNIe, а також реалізація такої МБ у середовищі IDE PyCharm, підкреслює потенціал баєсівських мережевих моделей для підвищення якості розслідувань, зокрема пов'язаних із DDoS-атаками. Запропонований у статті опис програмної реалізації мовою Python такої МБ,

спрямований на підвищення ефективності подібного інструментарію, роблячи його більш практико-орієнтованим і надаючи нові можливості для аналізу кіберзлочинів, асоційованих з DDoS-атаками. Показано, що розвиток такого програмного рішення відкриває шлях до глибшого аналізу та розуміння подібних кіберзлочинів, що є важливим кроком у боротьбі з ними. Тому розвиток такого програмного забезпечення (ПЗ) є перспективним напрямом у галузі кібербезпеки, що підкреслює його актуальність і вагомість у сучасному цифровому світі.

Ключові слова: DDoS-атака; мережа Байєса; моделювання; розслідування злочинів; Python.

ВСТУП

З появою нових технологій і методів атак, таких як розподілені атаки через бот-мережі, необхідне постійне оновлення методів, інструментів для виявлення і розслідування DDoS атак. Як зазначається в [1], з кожним роком кількість DDoS атак збільшується, що вимагає розробки нових підходів до розслідування, для більш ефективної протидії подібним атакам [2]. DDoS атаки часто використовують анонімні проксі й інші методи приховування джерела атаки, що ускладнює їхнє виявлення та атрибуцію до конкретних зловмисників і, відповідно, ускладнює розслідування подібних комп'ютерних злочинів. Багато DDoS атак можуть призвести до серйозних матеріальних і репутаційних збитків для організацій, що підкреслює важливість розробки ефективних методів розслідування [3], [4]. Організація DDoS-атак є протизаконною і завдає шкоди інфраструктурі й економіці будь-якої країни. Крім того, DDoS-атаки можуть бути використані для витоку або знищення конфіденційної інформації, а їхнє розслідування допомагає виявити та покарати порушників безпеки даних. Зауважимо, що моделювання ймовірності того, коли вилучений комп'ютер було використано для DDoS-атаки, може допомогти в розслідуванні, надаючи докази й аналізуючи можливі сценарії злочину. Наприклад, наявність певних доказів, таких як знайдені DDoS-інструменти чи відповідність IP-адрес на комп'ютері та в логах атаки, може збільшити ймовірність того, що даний комп'ютер було використано для DDoS-атаки. Моделювання ймовірності допоможе судовим органам ухвалити обґрунтовані рішення на основі наявних доказів і мінімізувати помилки в розслідуванні.

Постановка проблеми. Розробка нових методів розслідування DDoS атак сприяє посиленню співпраці між правоохоронними органами та галузевими експертами з кібербезпеки, що дає змогу ефективніше боротися з кіберзлочинністю. При цьому створення доступних для експертів кібернетичних інструментів для атрибуції атак до конкретних зловмисників, дасть змогу притягати їх до відповідальності.

Аналіз останніх досліджень і публікацій. Як зазначено в роботах [4] – [6] DDoS атаки часто характеризуються невизначеністю, наприклад, у джерелі атаки або обсязі трафіку. Мережі Байєса (далі МБ) [7], [8] дають змогу враховувати цю невизначеність і адаптуватися до мінливих умов. На думку [9] МБ можуть інтегрувати експертні знання про характеристики DDoS атак, що підвищить якість моделі та допоможе виявляти нові загрози. Зауважимо, що МБ легко оновлюються з появою нових даних. Це дає змогу адаптувати модель до мінливих умов мережевої безпеки і вносити корективи на основі нової інформації про DDoS атаки. Результати, отримані за допомогою МБ, досить легко інтерпретувати, що дає змогу співробітникам правоохоронних органів краще розуміти суть аналізу та ухвалювати обґрунтовані рішення. Важливо, що МБ можуть навчатися на історичних даних про DDoS-атаки й автоматично оновлюватися з появою нової інформації, що робить їх ефективним інструментом для виявлення нових загроз.

Мережі Байєса добре підходять для моделювання невизначеності та ймовірнісних залежностей між різними змінними. У контексті розслідування DDoS атак, де дані можуть бути неповними або зашумленими, це дає змогу точніше оцінювати ймовірності різних сценаріїв атаки.

Порівнюючи з іншими математичними підходами, такими як графи атак [10], [11], нейронні мережі [12], [14], ланцюги Маркова [15], [16] тощо [17], [18], мережі Байєса мають певні переваги, що робить цей вибір більш привабливим для розслідування DDoS-атак.

Розробка спеціалізованого програмного забезпечення (далі ПЗ) з простим та інтуїтивно зрозумілим користувацьким інтерфейсом для взаємодії з МБ, що моделює ймовірність DDoS атаки, дасть змогу спростити роботу працівників правоохоронних органів, даючи їм змогу легко оновлювати дані та аналізувати результати без необхідності в глибоких знаннях математичної статистики.

Мета статті. Все вище зазначене й зумовило наш інтерес до досліджень у цьому напрямі. Мета дослідження — розробка спеціалізованого програмного забезпечення (ПЗ) для роботи з МБ, що моделює ймовірність проведення DDoS-атаки з певного комп'ютера, є важливим кроком у підвищенні ефективності роботи правоохоронних органів у сфері кібербезпеки.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Розслідування DDoS-атаки з погляду криміналістики включає в себе кілька основних етапів. Криміналісти спочатку повинні виявити факт DDoS-атаки. Атака може бути виявлена, наприклад, шляхом моніторингу мережевого трафіку, аналізу логів серверів і мережевого обладнання, а також через звіти про недоступність сервісів. Після виявлення атаки збираються всі доступні докази, наприклад, це можуть бути звіти про мережевий трафік, логи подій, записи автентифікації тощо. Отримані докази можуть бути проаналізовані для виявлення характеристик атаки, таких як джерело атаки, застосовані методи й інструменти, тривалість та інтенсивність атаки. Зауважимо, що також можливе вилучення комп'ютера потенційного злочинця, оскільки на ньому можуть зберігатися докази проведення DDoS-атаки.

Докази проведення DDoS-атаки, які можуть бути на комп'ютері організатора або учасника, можуть бути різноманітними та залежати від специфіки атаки та використаних інструментів. Деякі з можливих доказів включають:

- програмне забезпечення для проведення атаки. На комп'ютері може бути виявлено спеціалізоване ПЗ, що використовується для запуску DDoS-атаки. Це можуть бути інструменти типу LOIC (Low Orbit Ion Cannon), HOIC (High Orbit Ion Cannon) та інші;
- конфігураційні файли. Важливою частиною ПЗ для DDoS-атаки є конфігураційні файли, в яких зазначаються цілі атаки, методи і параметри атаки. Ці файли можуть бути знайдені на комп'ютері;
- логи та журнали. Під час проведення DDoS-атаки можуть генеруватися логи і журнали, в яких записуються дії атакуючого та результати атаки. Ці файли можуть містити інформацію про цілі атаки, час і тривалість атаки, а також про її інтенсивність;

- командні файли та скрипти. Для автоматизації та управління атакою можуть використовуватися командні файли та скрипти, які можуть бути виявлені на комп'ютері;
- дані про мережеву активність. Аналіз мережевої активності з комп'ютера може показати участь у DDoS-атаці, наприклад, надсилання великої кількості запитів на певні сервери чи використання аномальних мережевих протоколів;
- повідомлення або записи чатів. Якщо DDoS-атака була організована або координована через інтернет, на комп'ютері можуть бути знайдені повідомлення або записи чатів, які містять інформацію про атаку.

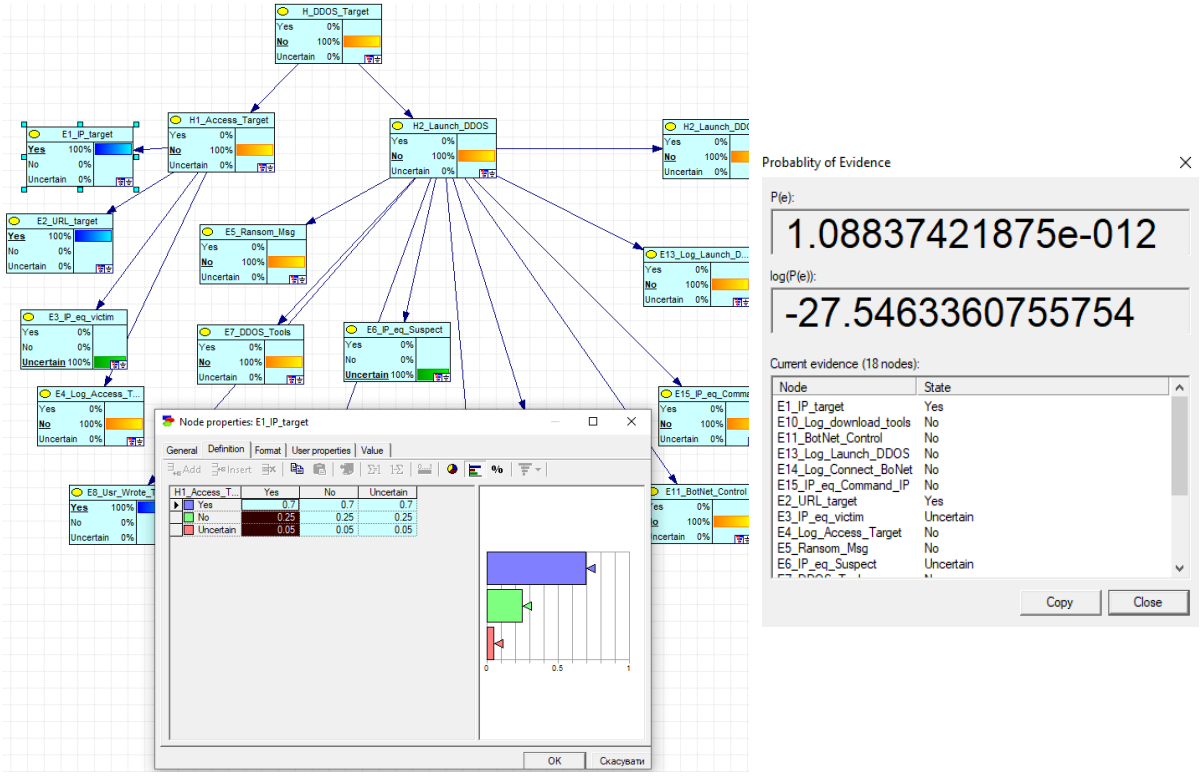
Наведені вище й інші докази можуть бути використані в розслідуванні для встановлення факту участі комп'ютера в DDoS-атаці, ідентифікації учасників та організаторів, а також для підтвердження інших обставин злочину.

МЕТОДИКА ДОСЛІДЖЕННЯ

На рис. 1 представлена МБ (побудована в GeNIe) моделює ймовірність того, що вилучений комп'ютер було використано для здійснення DDoS-атаки на цільовий комп'ютер. Початкова мережа була побудована на підставі результатів досліджень, представлених у роботі [9], проте модифікована з урахуванням подальшої реалізації на алгоритмічній мові Python для більш зручного використання, наприклад, співробітниками правоохоронних органів. МБ, наведена на рис. 1, складається з різних вершин, описаних нижче, які представляють гіпотези і докази, а також зв'язків між ними, що відображають ймовірнісні залежності.

GeNIe (Graphical Network Interface) — це програмний інструмент для моделювання байєсівських мереж (імовірнісних графів) і ухвалення рішень на їх основі. Крім базових функцій, таких як додавання вузлів і зв'язків, GeNIe надає розширені функції моделювання, наприклад, різні типи вузлів (дискретні, безперервні, тимчасові) і можливість додавання різних видів параметрів (CPD, utility nodes і т. д.). Важливо, що GeNIe надає інструменти для аналізу та прогнозування на основі побудованої моделі, такі як Variable Elimination для обчислення ймовірностей, а також інструменти для порівняння альтернативних моделей і прийняття рішень. Однак, незважаючи на потужні функції моделювання, GeNIe може виявитися недостатньо гнучким для деяких складних моделей або аналізу, що вимагає спеціалізованих методів, наприклад, складних кіберзлочинів.

ISSN 2663 - 4023



а) Реалізація МБ в середовищі GeNIe *б) Результати моделювання*

Рис. 1. Реалізація МБ розслідування злочинів, пов'язаних з організацією DDoS-атак у середовищі GeNIe

Нижче наведено основні вершини МБ, див. рис. 1.

$H\_DDOS\_T\arg et$ - вершина представляє собою головну гіпотезу, що вказує на те, чи був вилучений комп'ютер використаний у DDoS-атаці проти цільового комп'ютера. Вона має три можливі стани: «Так» (Yes), «Ні» (No) і «Невизначено» $(Uncertain)$. У процесі навчання МБ можна варіювати різними значеннями цих станів.

$H1\_Access\_T\arg et$ и $H2\_Launch\_DDOS$ — дві вершини, які є підгіпотезами. $H1\_Access\_T\arg et$ вказує на те, чи мав доступ вилучений комп'ютер до цільового комп'ютера, а $H2\_Launch\_DDOS$ — на те, чи було з вилученого комп'ютера запущено DDoS-атаку.

Умовні позначення E — вершини, які представляють собою різні вузли доказів, що впливають на підгіпотези і, отже, на головну гіпотезу. Наприклад, вершина $(E1\_IP\_t\arg et)$ відноситься до доказу, за яким IP-адресу цільового комп'ютера було знайдено на вилученому комп'ютері потенційного злочинця.

Стрілки в МБ зображують взаємозв'язки між змінними. Ступінь такого впливу вказується супроводжуючими числовими значеннями. Наприклад, наявність повідомлення про викуп $(E5\_Ransom\_Msg)$ зі 100% значенням, спрямоване на $(H1\_Access\_T\arg et)$, вказує про сильну кореляцію між цими подіями. Зазвичай DDoS-атаки використовують для порушення роботи онлайн-сервісів або вебсайтів, але іноді зловмисники можуть намагатися використовувати атаку як засіб для вимагання грошей. Прикладом такої ситуації може бути сценарій, за якого зловмисники запускають DDoS-атаку на сайт або онлайн-сервіс і потім надсилають повідомлення власникам або

адміністраторам системи з вимогою викупу для припинення атаки та відновлення нормальної роботи сервісу. Вони можуть погрожувати збільшенням інтенсивності атаки або тривалістю, якщо вимоги не будуть задоволені. Зауважимо, що здебільшого зловмисники, які запускають DDoS-атаки, ймовірно, не вдаватимуться до вимагання викупу, тому що такі вимоги можуть привернути увагу правоохоронних органів і збільшити ризик бути викритими. Замість цього, вони можуть використовувати атаку як спосіб тиску або помсти. Такі випадки не є частими, але вони можуть зустрічатися в мережі.

$E1-E4$ — докази (IP-адреса, URL, збіг IP-адреси/записів журналу) вказують на зв'язок між вилученим комп'ютером і цільовим комп'ютером, що потенційно свідчить про доступ $\left(H1\_Access\_T\arg et\right)$.

$E6$ — збіг IP-адрес. Коли під час розслідування DDoS-атаки виявляється, що IP-адреса комп'ютера, який було вилучено в рамках розслідування, збігається з IP-адресою зловмисника, зазначеною інтернет-провайдером на момент скоєння злочину, це може слугувати важливим доказом. При цьому слід врахувати, що IP-адреси можуть бути динамічними, тобто змінюватися з плином часу при кожному підключенні до мережі провайдера. Тому важливо мати підтвердження, що IP-адреса в момент атаки дійсно належала підозрюваному комп'ютеру. Також атакуючі можуть використовувати проксі-сервери або віртуальні приватні мережі (VPN) для приховування своєї реальної IP-адреси. У таких випадках IP-адреса вилученого комп'ютера може не збігатися з IP-адресою, вказаною провайдером. Крім того, комп'ютер може бути скомпрометований і використаний для DDoS-атаки без відома його власника. У цьому разі IP-адреса комп'ютера та адреса атакуючого збігатимуться, але це не буде доказом прямої участі власника комп'ютера в атаці.

Таким чином, важливо встановити, що саме власник комп'ютера мав доступ до нього в момент атаки, щоб виключити можливість використання комп'ютера кимось іншим. На підставі вищенаведеного, можна констатувати, що, хоча збіг IP-адрес може бути важливим елементом доказу, необхідно врахувати всі перераховані обставини, щоб зробити висновок про причетність власника комп'ютера до DDoS-атаки.

$E7-E15$ — докази у вигляді інструментів для реалізації DDoS. Наприклад, у ході розслідування DDoS-атаки був знищений комп'ютер, з якого припускають, що могли бути здійснені атаки. При аналізі вмісту цього комп'ютера виявлені спеціальні програми або скрипти, які можуть бути використані для запуску DDoS-атаки. Наприклад, DDoS-боти, тобто спеціальні програми-боти, призначені для участі в DDoS-атаках. Ці програми можуть мати функціонал для генерації та надсилання великої кількості запитів на цільовий сервер. До цієї категорії також можна віднести скрипти, які можуть автоматично генерувати й надсилати запити до цільового сервера з метою перевантаження його ресурсів. Під цю категорію потрапляють і інструменти для синхронізованих атак. Наприклад, на комп'ютері знайдено інструменти, що дають змогу координувати дії безлічі комп'ютерів для проведення синхронізованої DDoS-атаки. Можна додати до наведеного переліку відповідні логи або історію використання (тобто фактичні цифрові сліди — ЦС). В історії роботи або логах можуть бути виявлені записи про запуск інструментів, характерних для DDoS-атак, або записи про під'єднання до командних серверів, що використовуються для управління ботнетом. Таким чином, виявлення подібного інструментарію на комп'ютері може бути важливим доказом у розслідуванні DDoS-атаки, оскільки вказує на наявність засобів і можливості для здійснення атаки.

ISSN 2663 - 4023

Хоча спеціалізоване ПЗ для побудови МБ може бути корисним при моделюванні та навчанні цих мереж для розслідування DDoS-атак, існують значні переваги використання мов високого рівня, наприклад, Python, для реалізації подібного завдання. Так, Python дає змогу криміналістам прозоро відстежувати логіку роботи мережі Байєса і вносити необхідні зміни. У той час, як спеціалізоване ПЗ може бути «чорною скринькою», що ускладнює розуміння і контроль над моделями. Важливо, що додатковим аргументом, є і та обставина, що Python можна використовувати для парсингу та аналізу логів, що дасть змогу витягувати інформацію про підозрілу активність, пов’язану з DDoS-атакою, а також зібрати дані з різних джерел.

З огляду на вище сказане МБ, показана на рис. 1, була реалізована в середовищі програмування PyCharm (рис. 2).

Результат роботи в PyCharm МБ для розслідування злочинів, пов'язаних з організацією DDoS-атак представлено на рис. 3.

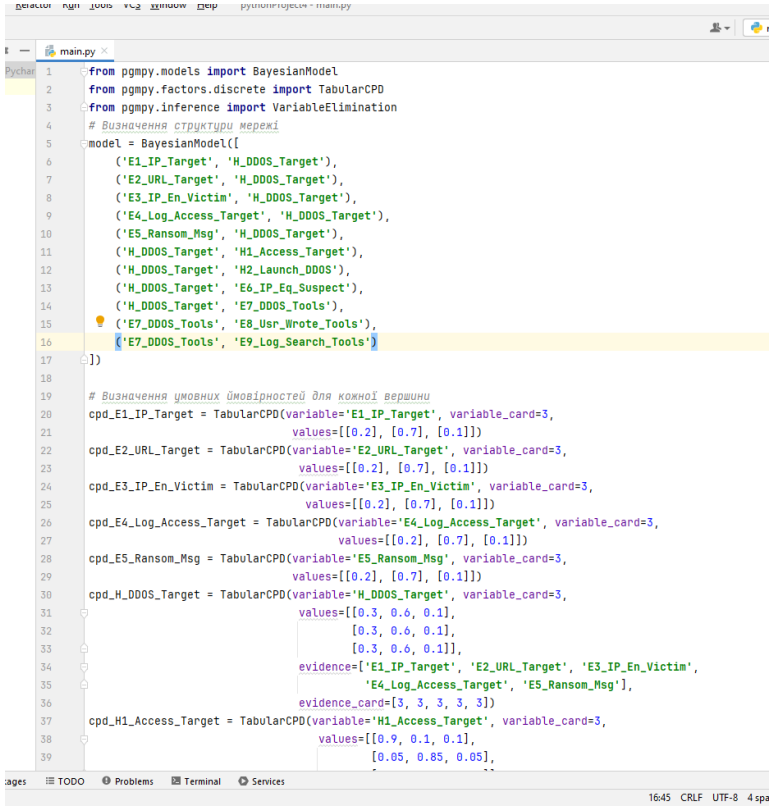


Рис. 2. Приклад реалізації в PyCharm МБ для розслідування злочинів, пов’язаних з організацією DDoS-атак

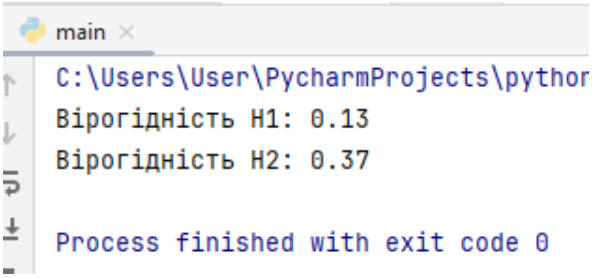


Рис. 3. Приклад висновків, згенерованих у результаті роботи в PyCharm МБ для розслідування злочинів, пов’язаних з організацією DDoS-атак

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Дослідження кіберзлочинів, таких як DDoS-атаки, стає дедалі актуальнішим у сучасному світі, де цифрова безпека відіграє ключову роль у захисті інформації та інфраструктури організацій.

Обґрунтовано, що використання байєсівських мережевих моделей (мереж Байєса — МБ) для аналізу кіберзлочинів дає змогу врахувати безліч змінних і ймовірностей, що робить дослідження більш точним і надійним. Продемонстровано, що використання МБ для розслідування кіберзлочинів дає змогу не лише визначити факт злочину, а й виявити можливі мотиви та зв'язки між учасниками злочинного угруповання, що значно покращує ефективність розслідування.

Показано на прикладі реалізації МБ за допомогою пакета моделювання GeNIe, також в IDE PyCharm, що байєсівські мережеві моделі можна ефективно використовувати для підвищення якості розслідувань кіберзлочинів, пов'язаних, наприклад, з реалізацією DDoS атак. Обґрунтовано перспективність розвитку представленого програмного забезпечення (ПЗ), призначеного для криміналістів, які ведуть розслідування DDoS атак. Розвиток подібного ПЗ відкриває нові можливості для глибшого аналізу та розуміння характеристик кіберзлочинів, пов'язаних з DDoS атаками, що є важливим кроком у боротьбі з ними. Розвиток подібного ПЗ, на наш погляд, є одним із ключових напрямків у сфері кібербезпеки, що підкреслює його актуальність і вагомість у сучасному світі цифрових технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Doshi, K., Yilmaz, Y., & Uludag, S. (2021). Timely detection and mitigation of stealthy DDoS attacks via IoT networks. *IEEE Transactions on Dependable and Secure Computing, 18(5),* 2164–2176.
2. Mittal, M., Kumar, K., & Behal, S. (2023). Deep learning approaches for detecting DDoS attacks: A systematic review. *Soft computing, 27(18),* 13039–13075.
3. Sarmento, A. G., Yeo, K. C., Azam, S., Karim, A., Al Mamun, A., & Shanmugam, B. (2021). Applying big data analytics in DDos forensics: challenges and opportunities. *Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability,* 235–252.
4. Traer, S., & Bednar, P. (2021). Motives behind ddos attacks. *Digital Transformation and Human Behavior: Innovation for People and Organisations,* 135–147.
5. Samiksha, S. (2021). *Investigating an association between DDoS and Phishing attacks (Master's thesis, University of Twente).*
6. Kopp, D., Dietzel, C., & Hohlfeld, O. (2021). DDoS never dies? An IXP perspective on DDoS amplification attacks. *International Conference on Passive and Active Network Measurement,* 284–301).
7. Reddy, K. G., & Thilagam, P. S. (2020). Naïve Bayes classifier to mitigate the DDoS attacks severity in ad-hoc networks. *International Journal of Communication Networks and Information Security, 12(2),* 221–226.
8. Singh, S., Kumari, K., Gupta, S., Dua, A., & Kumar, N. (2020). Detecting different attack instances of DDoS vulnerabilities on edge network of fog computing using gaussian naive bayesian classifier. *IEEE international conference on communications workshops (ICC Workshops),* 1–6.
9. Tse, H., Chow, K.-P., & Kwan, M. (2013). A Generic Bayesian Belief Model for Similar Cyber Crimes. *9th International Conference on Digital Forensics (DF),* 243–255. https://doi.org/10.1007/978-3-642-41148-9_17
10. Liu, X., Ren, J., He, H., Zhang, B., Song, C., & Wang, Y. (2021). A fast all-packets-based DDoS attack detection approach based on network graph and graph kernel. *Journal of Network and Computer Applications, 185, 103079.*
11. Ates, C., Özdel, S., & Anarim, E. (2020). Graph-based fuzzy approach against DDoS attacks. *Journal of Intelligent & Fuzzy Systems, 39(5),* 6315–6324.

12. Mustapha, A., Khatoun, R., Zeadally, S., Chbib, F., Fadlallah, A., Fahs, W., & El Attar, A. (2023). Detecting DDoS attacks using adversarial neural network. *Computers & Security, 127, 103117.*
13. Chartuni, A., & Márquez, J. (2021). Multi-classifier of DDoS attacks in computer networks built on neural networks. *Applied Sciences, 11(22), 10609.*
14. Yousuf, O., & Mir, R. N. (2022). DDoS attack detection in Internet of Things using recurrent neural network. *Computers and Electrical Engineering, 101, 108034.*
15. Chen, C. L., & Chen, J. M. (2021). Use of MARKOV Chain for Early Detecting DDoS Attacks. *International Journal of Network Security & Its Applications (IJNSA), 13(4).*
16. Balaji Bharatwaj, M., Aditya Reddy, M., Senthil Kumar, T., & Vajipayajula, S. (2022). Detection of DoS and DDoS attacks using hidden markov model. *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2021*, 979–992.
17. Balarezo, J. F., Wang, S., Chavez, K. G., Al-Hourani, A., & Kandeepan, S. (2022). A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. *Engineering Science and Technology, an International Journal, 31, 101065.*
18. Banitalebi Dehkordi, A., Soltanaghaei, M., & Boroujeni, F. Z. (2021). The DDoS attacks detection through machine learning and statistical methods in SDN. *The Journal of Supercomputing, 77(3),* 2383–2415.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

Valerii Lakhno
Doctor of Technical Sciences, Professor, Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
ORCID ID: 0000-0001-9695-4543
lva964@nubip.edu.ua

Semen Voloshyn
Ph. D, Associate Professor, Associate Professor at the Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
ORCID ID: 0000-0002-4913-7003
voloshyn@nubip.edu.ua

Sergii Mamchenko
Doctor of Technical Sciences, Professor, Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
ORCID ID: 0009-0006-8743-5606
s.mamchenko@nubip.edu.ua

Volodymyr Matiyevsky
Senior Lecturer at the Department of Computer Systems, Networks, and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
ORCID ID: 0000-0002-1954-8493
mvv@nubip.edu.ua

Myroslav Lakhno
NET Full Stack Developer in e-Docs.UA, Kiev, Ukraine
ORCID ID: 0000-0001-6979-6076
valss725@gmail.com

IMPLEMENTATION OF A BAYESIAN NETWORK IN PYTHON FOR ANALYSIS OF CYBERCRIMES ASSOCIATED WITH DDOS ATTACKS

Abstract. The research of cybercrimes, including DDoS attacks, is becoming increasingly important in the context of heightened attention to cybersecurity, protection of information and infrastructure of organizations in the modern world that rely on digital technologies and computer systems. The article argues that the use of Bayesian network models (hereinafter Bayesian networks — BN) for the analysis of cybercrimes (using distributed DDoS attacks as an example) will allow taking into account numerous variables and probabilities. This makes similar research more accurate and reliable. Using the example of BN research in the GeNIe applied software package, the process of using BN apparatus for the cybercrime investigation task related to the implementation of DDoS attacks from an attacker's computer is demonstrated. The described BN helps forensic experts in investigating such cybercrimes to identify motives and connections between attack participants, which undoubtedly improves the efficiency of investigations. The demonstration of BN application using the GeNIe modeling package, as well as the implementation of such BN in the PyCharm IDE environment, emphasizes the potential of Bayesian network models to enhance the quality of investigations, particularly those related to DDoS attacks. The description of the Python language software implementation of such BN proposed in the article aims to improve the efficiency of similar tools, making it more practical-oriented and providing new opportunities for the analysis of cybercrimes associated with DDoS attacks. It is shown that the development of such software opens the way for deeper analysis and understanding of such cybercrimes, which is an important step in

combating them. Therefore, the development of such software (SW) is a promising direction in the field of cybersecurity, emphasizing its relevance and significance in the modern digital world.

Keywords: DDoS attack; Bayesian network; modeling; crime investigation; Python.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Doshi, K., Yilmaz, Y., & Uludag, S. (2021). Timely detection and mitigation of stealthy DDoS attacks via IoT networks. *IEEE Transactions on Dependable and Secure Computing, 18(5),* 2164–2176.
2. Mittal, M., Kumar, K., & Behal, S. (2023). Deep learning approaches for detecting DDoS attacks: A systematic review. *Soft computing, 27(18),* 13039–13075.
3. Sarmento, A. G., Yeo, K. C., Azam, S., Karim, A., Al Mamun, A., & Shanmugam, B. (2021). Applying big data analytics in DDos forensics: challenges and opportunities. *Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability*, 235–252.
4. Traer, S., & Bednar, P. (2021). Motives behind ddos attacks. *Digital Transformation and Human Behavior: Innovation for People and Organisations*, 135–147.
5. Samiksha, S. (2021). *Investigating an association between DDoS and Phishing attacks (Master's thesis, University of Twente).*
6. Kopp, D., Dietzel, C., & Hohlfeld, O. (2021). DDoS never dies? An IXP perspective on DDoS amplification attacks. *International Conference on Passive and Active Network Measurement*, 284–301).
7. Reddy, K. G., & Thilagam, P. S. (2020). Naïve Bayes classifier to mitigate the DDoS attacks severity in ad-hoc networks. *International Journal of Communication Networks and Information Security, 12(2),* 221–226.
8. Singh, S., Kumari, K., Gupta, S., Dua, A., & Kumar, N. (2020). Detecting different attack instances of DDoS vulnerabilities on edge network of fog computing using gaussian naive bayesian classifier. *IEEE international conference on communications workshops (ICC Workshops),* 1–6.
9. Tse, H., Chow, K.-P., & Kwan, M. (2013). A Generic Bayesian Belief Model for Similar Cyber Crimes. *9th International Conference on Digital Forensics (DF),* 243–255. https://doi.org/10.1007/978-3-642-41148-9_17
10. Liu, X., Ren, J., He, H., Zhang, B., Song, C., & Wang, Y. (2021). A fast all-packets-based DDoS attack detection approach based on network graph and graph kernel. *Journal of Network and Computer Applications, 185, 103079.*
11. Ates, C., Özdel, S., & Anarim, E. (2020). Graph-based fuzzy approach against DDoS attacks. *Journal of Intelligent & Fuzzy Systems, 39(5),* 6315–6324.
12. Mustapha, A., Khatoun, R., Zeadally, S., Chbib, F., Fadlallah, A., Fahs, W., & El Attar, A. (2023). Detecting DDoS attacks using adversarial neural network. *Computers & Security, 127, 103117.*
13. Chartuni, A., & Márquez, J. (2021). Multi-classifier of DDoS attacks in computer networks built on neural networks. *Applied Sciences, 11(22), 10609.*
14. Yousuf, O., & Mir, R. N. (2022). DDoS attack detection in Internet of Things using recurrent neural network. *Computers and Electrical Engineering, 101, 108034.*
15. Chen, C. L., & Chen, J. M. (2021). Use of MARKOV Chain for Early Detecting DDoS Attacks. *International Journal of Network Security & Its Applications (IJNSA), 13(4).*
16. Balaji Bharatwaj, M., Aditya Reddy, M., Senthil Kumar, T., & Vajipayajula, S. (2022). Detection of DoS and DDoS attacks using hidden markov model. *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2021,* 979–992.
17. Balarezo, J. F., Wang, S., Chavez, K. G., Al-Hourani, A., & Kandeepan, S. (2022). A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. *Engineering Science and Technology, an International Journal, 31, 101065.*
18. Banitalebi Dehkordi, A., Soltanaghaei, M., & Boroujeni, F. Z. (2021). The DDoS attacks detection through machine learning and statistical methods in SDN. *The Journal of Supercomputing, 77(3),* 2383–2415.