УДК 004

МОДЕЛЬ-ГРАФ АТРИБУЦІЇ КІБЕРАТАК

К. Л. Сидоренко[1], О. М. Барановський[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

Робота присвячена основній проблемі атрибуції кібератак, що є на сьогодні, розкривається недостатність теперішніх моделей атрибуції, відсутність формалізації. Також наведено можливе рішення у вигляді орієнтованого графа, описано суть усіх складових моделі.

Ключові слова: атрибуція кібератак, розслідування, формалізація атрибуції

Вступ

Атрибуція кібератак – невелика, проте значна частина кібербезпеки, яка повинна знайти відповідь на запитання "Хто зловмисник?". Встановити атрибуцію досить складно, адже не існує єдиного алгоритму або автоматизованого рішення. До кожного інциденту необхідно розробляти окремий план аналізу інциденту. Формалізованого рішення щодо опису інциденту, роботи зі слідами залишеними зловмисниками на сьогодні не існує. Тема є актуальною, адже кожен день відбуваються атаки на організації приватного та державного рівня. А питання, як саме працювати з отриманими доказами, щоб якомога швидше прийти до правильного рішення, залишається невирішеним. Метою статі є огляд даної проблеми, також опис можливої моделі атрибуції, що обробляє докази як окремо, так і в контексті інших доказів.

1. Основна проблема атрибуції атаки як окремої частини комп'ютерної криміналістики

Сьогодні комп'ютерна криміналістика є молодою наукою, яка тільки розвивається. Теоретична база напрацьовується кожний день спеціалістами. Також, специфікою галузі є те, що вона потребує нові рішення кожен раз, як користувачі або зловмисники переходять на нові технології. Ця особливість також справедлива й до атрибуції кібератак. Ще не було вироблено міжнародних сертифікацій чи критеріїв щодо проведення атрибуції кібератак як окремого кроку розслідування.

2. Відомі сучасні практики

Існує посібник A Guide to Cyber Attribution (2018) від Кабінету Директора Національної Розвідки (Office of the Director of National Intelligence).[1] В ньому визначено ключові показники, що забезпечують атрибуцію (конспірація, інфраструктура, шкідливе програмне забезпечення, намір, інформація з зовнішніх джерел).

Повніше атрибуцію описує модель CAM (Cyber Attribution Model), що складається з двох основних частин: розслідування кібератак та профілювання акторів кіберзагрози. Атрибуція відбувається шляхом зіставлення цих частин. Основною метою розслідування кібератаки є відповідь на питання, хто є жертвою та чому, а також що саме сталося та як це було реалізовано. Відповідаючи на ці запитання, керуюся компонентами віктимологія, інфраструктура, можливості та мотивація. Метою профілювання кіберзлочинця є розробка профілів на основі минулих атак та пошук відповідного профілю висновкам з першої частини. Профілювання акторів кіберзагроз проводиться як постійно, так і спеціально під час розслідувань. У цьому випадку перша частина (знизу вгору) та друга частина (зверху вниз) працюють паралельно, щоб знайти відповідність між застосованими техніками, тактиками та процедурами можливими злочинцями [2].

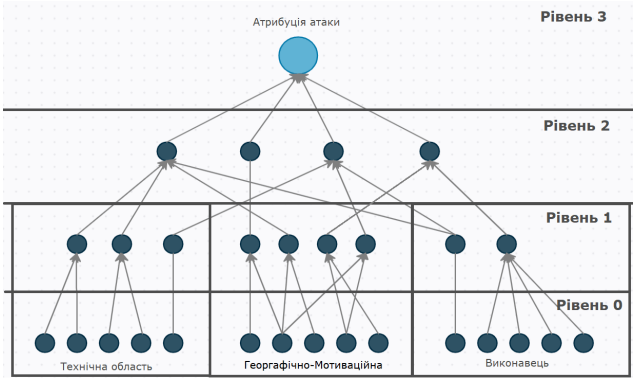

Рис. 1. Приклад Моделі-Графу Атрибуції кібератаки схематично.

3. Модель-Граф Атрибуції кібератак

Основні поняття:

«Доказ» – це будь-яка інформація або дані, що були знайдені та мають значення для розслідування.

«Область» – це окрема (одна з трьох) частина моделі, до якої можна віднести доказ на початковому етапі.

3.1. Рівень 0

Усі знайдені під час експертиз докази збираються та групуються за трьома областями: технічна, мотиваційно-географічна та виконавець.

До технічної належать усі докази, що стосуються стратегії атаки, використаного програмного забезпечення, технологій, інструментів тощо.

Географічно-мотиваційна – охоплює докази, які можна віднести до гуманітарних галузей, географічної (місце та час) складової атаки та визначає можливу мотивацію. Тобто, містить в собі відомості про жертву, її політичну або економічну позицію, місце знаходження та зону впливу, описуються юридичні аспекти, підраховуються втрати внаслідок атаки та збираються відомості щодо осіб, з якими у жертви є конфлікти інтересів.

Виконавець – це усі докази, які можуть навести на слід того, хто виконав атаку. Це можуть бути IP, підпис, який іноді люблять залишати зловмисники, щоб похизуватися, контакти або рахунки на які слід відправити гроші або дані, використані облікові записи, збіг імені користувача та всі інші докази, які приведуть до конкретної людини. Варіант, коли в певній області взагалі немає доказів також можливий.

3.2. Рівень 1

Об'єднання вершин нульового рівня, групування окремих доказів в межах певної області. Перша частина підбиття підсумків.

В технічній області може бути описана стратегія відповідно до семи кроків, описаними ATT&CK™, описаними у Finding Cyber Threats with ATT&CK™-Based Analytics (2017) [3]. Визначається набір інструментів, які були використані, описуються частини системи, що постраждали та підбиваються підсумки щодо складності проведеної атаки.

В області Виконавець: описується профіль того, хто виконав атаку, можливо, знайдені конкретні особистості, збіг імен, власних назв, особливих рядків тощо.

Географічно-мотиваційна: при об'єднанні кількох «слідів» – можна будувати гіпотези про те, хто зацікавлений в результатах атаки. Аналіз ситуації у сфері діяльності жертви, складення попереднього списку підозрюваних, обробка результатів часу проведення атаки на предмет збіг з часовими поясами, або проміжок часу довготривалої атаки, суть якої може бути приречена до певних заходів, свят та новин. Підбивання підсумків вже в загальному для області.

Якщо вершину з нульового рівня неможливо об'єднати з іншою, її слід перенести на перший рівень як окремий доказ.

3.3. Рівень 2

Об'єднання вершин з першого рівня вже на перетині областей. Так підсумки одиничних доказів розглядаються в контексті доказів з інших областей.

Виконавець-Технічна: в цьому перетині можна роздивитися аспект «почерку» коду зловмисної команди, характерні алгоритми або використання символів. Перевірка авторства програм або ж конкретні навички та стратегії. Перевірка IP адресу, їх місцеперебування.

Виконавець – Георгафічно-Мотиваційна: пошук зв'язків в профілі виконавця атаки. Спроба відповісти на питання, чи виконавець сам ініціював атаку, або ж довести існування замовника. Можливо, конкретний виконавець працював на одного з підозрюваних (з Георгафічно-Мотиваційної), або йому цілком можливо привласнити мотивацію. Пошук зв'язків, або навіть місця перебування виконавця відповідно до географічного аспекту.

Географічно-мотиваційна – Технічна: дозволяє порівнювати версії програм, мови написання, розкладку клавіатури та інші особливості. Можлива оцінка технічної (або ж ресурсної) потужності одного з можливих підозрюваних.

Окрім цього, можливо використовувати вершин Рівня 1 з усіх трьох областей або ж окремі одиничні докази з Рівня 0.

3.4. Рівень 3

Об'єднання усіх вершин Рівня 2 дає комплексну атрибуцію атаки, що враховує усі області. Підбиття підсумків. Окрім наведення вершин Моделі-Графу Атрибуції важливо виділити стратегії, які раніше не використовувалися або були характерними для вже відомих APT. Та врахувати їх при роботі на Рівні 3.

Висновки

У статті було наведено проблему формалізації процесу атрибуції атак. Розглянуто чинні рекомендації та моделі, було запропоновано власну Модель-Граф Атрибуції.

Її сильними сторонами є те, що спочатку докази аналізуються відповідно до області, що на початковому етапі підбиття підсумків захищає від можливої упередженості атрибуції. Також, з кожним рівнем обробка доказів стає все простішою: важливі докази беруться до уваги, в той час, як ті, що не несуть інформативності, відокремлюються, проте не відкидаються до кінця атрибуції, адже будь-який доказ може стати важливим у цьому процесі. На останньому рівні підсумки областей розглядаються в контексті одна одної.

Це допомагає знайти зв'язком між різними аспектами атаки та впевнитися у правильності окремих гіпотез.

Перелік використаних джерел

1. A Guide to Cyber Attribution. — Office of the Director of National Intelligence., 2018. — Access mode: `https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf`.
2. Skopik F, Pahi Timea. Under false flag: using technical artifacts for cyber attack attribution. — SpringerOpen, 2020. — Access mode: `https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00048-4#Sec21`.
3. Strom B. E., Battaglia J. A., Kemmerer M. S. Finding Cyber Threats with ATT&CK™-Based Analytics. — Mitre technical report, 2017.