DOI https://doi.org/10.36059/978-966-397-300-5-70

АНАЛІЗ ГРАФІВ ПІД ЧАС РОЗВІДКИ КІБЕРІНЦИДЕНТУ

Шевченко Д.
здобувача вищої освіти першого (бакалаврського) рівня
2-го курсу спеціальності 262 – Правоохоронна діяльність
Міжнародний гуманітарний університет
Науковий керівник: ***Слатвінська В. М.***
експерт комп'ютерно-технічних експертиз,
викладач кафедри кримінального права, процесу та криміналістики
Міжнародний гуманітарний університет
м. Одеса, Україна

Дані, які необхідно опрацювати в рамках комплексних розслідувань (журнали автоматизованих систем і засобів захисту, вивантаження бізнес-систем, транзакції, артефакти операційних систем, результати OSINT-аналізу, пояснення співробітників за фактом інциденту), – це, звісно, не Big Data, але інформація, яка також потребує спеціальних інструментів для фільтрації релевантних до розслідування даних, їх опрацювання та формування цілісної картини.

На думку Жилін А. В.: «Інцидент кібербезпеки (кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів» [1, с. 19].

Аналіз графів – ефективний інструмент для виявлення кібератак. Графи дозволяють візуалізувати зв'язки між елементами системи та інфраструктурами, що може допомогти виявити підозрілі зв'язки. Аналіз графів також дозволяє виявляти зміни в мережі, такі як зміна розташування файлів чи збільшення трафіку. Результати аналізу графів можуть допомогти в ідентифікації загроз та встановленні шаблонів атак, які можуть бути використані в майбутньому. Для успішного аналізу графів необхідно мати доступ до великої кількості даних про мережу, таких як логи подій, дані про взаємодію користувачів, інформація про мережеву топологію тощо. Автоматизовані засоби аналізу графів дозволяють значно зменшити час,

потрібний для аналізу великих обсягів даних та виявлення підозрілих зв'язків. На основі результатів аналізу графів можна розробляти стратегії відповіді на кібератаки, в тому числі розробляти профілактичні заходи та визначати пріоритетні напрямки захисту мережі.

Графи дозволяють зображати зв'язки між різними елементами мережі та її інфраструктурами, що дозволяє зрозуміти, як працює мережа та виявити підозрілі зв'язки. Графи також дозволяють відстежувати зміни в мережі, такі як зміна трафіку чи зміна розташування файлів, що може свідчити про кібератаку. Застосування аналізу графів під час розвідки кіберінцидентів дозволяє здійснювати глибокий аналіз мережі та її взаємодій, що допомагає виявити загрози та захиститися від них. Графи можуть бути використані для виявлення нових загроз, включаючи атаки, які не були відомі раніше. Використання графів в розвідці кіберінцидентів може допомогти визначити найбільш вразливі місця в мережі та встановити заходи захисту. Автоматизовані засоби аналізу графів дозволяють збільшити швидкість виявлення та реагування на кіберінциденти.

Основна мета графової моделі – не доставити естетичну насолоду, а дати цілісну картину, відсіявши нерелевантну інформацію. Крім того, граф масштабований і, якщо будуть ще фішингові розсилки, може бути доповнений новими елементами.

Спосіб відображення інформації про інцидент відіграє найважливішу роль у сприйнятті і, як наслідок, розумінні та встановленні причин і обставин інциденту – в основних завданнях розслідування. У низці випадків найефективніший для сприйняття спосіб відображення – подання інформації у вигляді графа. Такий спосіб використовувався і в докомп'ютерну епоху, але після поширення комп'ютерів набув нових переваг, оскільки усував обмеження, пов'язані з кількістю відображуваної інформації, швидкістю побудови і складністю приховування від сторонніх очей. Крім того, в електронному вигляді простіше застосовувати математику на графах. Використання графів є типовим під час розслідувань, пов'язаних із соціальними мережами або банківськими транзакціями, та інших розслідувань, у рамках яких вивчаються зв'язки однорідних елементів.

З вищевказаного випливає, що використання графів дозволяє розуміти мережу та її взаємодії більш глибоко, що допомагає виявити загрози та підвищити рівень захисту мережі.

Література:

1. Жилін А. В. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.