

ДОСЛІДЖЕННЯ ЕВРИСТИЧНОГО АНАЛІЗУ АНТИВІРУСІВ ТА МЕТОДИ ЇХ ПОКРАЩЕННЯ

Комп'ютерні віруси та шкідливе програмне забезпечення почали з'являтися ще у минулому столітті, але проблема антивірусної боротьби є актуальною й на сьогоднішній день. Згідно статистики державної служби спеціального зв'язку та захисту інформації України за перше півріччя 2023 року у середньому за місяць виникало до 128 інцидентів, найпопулярнішими типами з яких є фішинг та розповсюдження шкідливих програм [1]. Саме тому варто дослідити як працюють модулі евристики антивірусів та розглянути методи покращення його роботи.

Евристичний аналіз на основі типових програмних інструкцій робить висновок чи відбувається шкідлива дія. Зазвичай, він використовується для визначення гібридів і нових версій раніше відомих вірусів.

Для даного дослідження було використано:

- IDA Freeware через зручний hex-view-редактор та вбудованими розширеннями взаємодії з ним [2];
- CFF Explorer VII для аналізу структури файлу [3];
- програма з фрагментом коду, який імітує шпигунську діяльність [4].

У ході дослідження «шпигунської програми» було припущено, якщо у структурі файлу було знайдено фрагмент коду, який відповідає за перехват клавіатури та передачу даних через Інтернет-з'єднання, то це може бути шкідлива програма. На жаль, це не є ефективним підходом до виявлення вірусної активності чи виявлення шкідливої дії, адже більшість застосунків буде вважатися шкідливими, бо мають аналогічну логіку роботи. Як наслідок, буде велика кількість хибних спрацювань і користувачі вимкнуть або видалять дане антивірусне програмне забезпечення. У разі додавання до фаєрволу білих та чорних списків з діапазону IP-адрес кількість хибних спрацювань зменшиться, але не суттєво саме через проблему підтримування їх актуальності [5]. Саме тому це дослідження показує, що не можливо зберегти цілісність даних, використовуючи тільки один підхід. Інформаційна безпека є складним міждисциплінарним завданням, яке вимагає комплексного підходу та використання різноманітних інструментів та методів.

Проаналізувавши дане дослідження, пропонуються методи для покращення виявлення вірусів:

- використання фаєрволу – у разі під’єднання до Інтернету, виконати перевірку IP-адрес за чорними та білими списками, окремо перевірити чорні та білі списки розробників ПЗ та діапазон адрес, на які були підозри щодо джерел шкідливих програм;

- використання антивірусу – перевірка частин коду програми на співпадіння сигнатур у відомих антивірусних базах даних за допомогою емпіричного аналізу для виявлення раніше створених вірусів чи їх штамів. У разі, якщо є підозра у вірусній активності або у знайденні шкідливого програмного забезпечення, то застосувати додаткові методи перевірки;

- використання віртуалізації робочого оточення для аналізу поведінки роботи програми;

- виконання запуску виконуваного коду у відокремленому просторі (Sanbox) для аналізу поведінки програми, застосовуючи метод аналізу контрольних сум.

Можна зазначити, що ідеальних методів для попередження вірусної атаки не існує. Ця тема може бути актуальною тривалий час. Звичайний користувач може знизити вірогідність зараження свого робочого середовища дотримуючись звичайних правил кібергігієни [6]. Натомість програмістам рекомендується у розроблюваному антивірусному програмному забезпеченні використовувати наявні проактивні засоби захисту та не зупинятися щодо методів до їх поліпшення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Російські кібероперації. Аналітика за перше півріччя 2023 року [Електронний ресурс]. – Режим доступу : <https://cip.gov.ua/services/cm/api/attachment/download?id=60201>

2. IDA Freeware [Electronic recourse]. – Access mode : <https://hex-rays.com/ida-free/>

3. CFF Explorer VII [Electronic recourse]. – Access mode : https://ntcore.com/?page_id=388

4. Шпигунська програма [Електронний ресурс]. – Режим доступу : <https://github.com/bb33bb/SpywareVirus>

5. Why We Don't Whitelist IP Addresses [Electronic recourse]. – Access mode : <https://www.firesideagency.ca/other/why-we-dont-whitelist-ip-addresses/>

6. Кіберполіція попереджає про масовану атаку «вірусу» на державні установи та приватні компанії [Електронний ресурс]. – Режим доступу : <https://cyberpolice.gov.ua/news/kiberpolicziya-poperedzhaye-pro-masovanu-ataku-virusu-na-derzhavni-ustanovy-ta-pryvatni-kompaniyi-768/> (дата звертання: 07.04.2024).