Проблемні питання, що виникають під час дослідження шкідливого програмного забезпечення

Євгеній Тарасенко

завідувач сектору, Сумський НДЕКЦ МВС України, м. Суми, Україна,
e-mail: t.expert.kte.sumy@gmail.com.

Розглянуто методи, які застосовують під час дослідження шкідливого програмного забезпечення, та проблемні питання, що виникають під час таких досліджень.

Ключові слова: *шкідливе програмне забезпечення (ШПЗ); вірус; аналіз; пісочниця.*

Challenges Emerging in the Course of Malware Analysis

Evgeniy Tarasenko

The paper presents methods employed in malware study and challenges emerging during such study.

Keywords: *malware; virus; analysis; sandbox.*

Нині комп'ютери, мобільні телефони, системи зберігання даних увійшли майже в усі сфери нашого життя. Уся важлива інформація про людину або компанію зберігається на носіях цифрової інформації. Тому останнім часом набирають актуальності кримінальні справи, пов'язані зі шкідливим програмним забезпеченням (далі — *ШПЗ*), націленим на викрадення інформації, її знищення або унеможливлення доступу до неї. Судові експертизи з питань ШПЗ відіграють одну з найважливіших ролей у таких справах, але подібні дослідження пов'язані з певними труднощами.

Термін «ШПЗ» доволі розпливчастий. Він означає, що таке програмне забезпечення несе шкоду користувачеві або системі, але немає чіткої межі, що саме може бути шкодою для системи. Наприклад, програми віддаленого доступу за відповідних налаштувань дають змогу підключатися до кінцевого пристрою без підтвердження цієї дії самим пристроєм. Підключення до пристрою без згоди користувача також є у функціоналі багатьох ШПЗ. Тому віднесення того чи того програмного забезпечення до категорії шкідливих — питання юридичне, відповідь на яке залежить від багатьох чинників. Експерт із правом проведення судової комп'ютерно-технічної експертизи не може на власний розсуд сказати, чи є надане на дослідження програмне забезпечення шкідливим. Відповідний висновок може бути даний лише з посиланням на результати роботи антивірусного програмного забезпечення, розробленого, щоб ідентифікувати ШПЗ. Тому при призначенні експертизи першим слід поставити запитання: «Чи визначається файл (назва файлу) антивірусним програмним забезпеченням як шкідливий?».

Дослідження функціональних можливостей ШПЗ пов'язане з труднощами, обумовленими як програмно-технічним забезпеченням, так і знаннями та досвідом самого експерта. Крім того, такі дослідження потребують значно більше часу, ніж інші види експертиз, адже вони потребують використання багатьох інструментів та аналізуваннями за допомогою різних методів. Щодо самого аналізування, то в ньому можна виокремити два основні типи: аналіз вихідного коду та динамічний аналіз.

Аналіз вихідного коду полягає в розборі файлів методом дизасемблювання. Для цього ми завантажуємо файл у дизасемблер і досліджуємо програмні інструкції, щоб зрозуміти, які функції в ньому закладено. Ці інструкції виконуються центральним процесором, і в такий спосіб ми можемо

дізнатися деталі поведінки програми. Головним недоліком даного методу є те, що вихідний код доволі часто буває обфускованим і його дуже складно, а інколи навіть неможливо прочитати. Обфускація, або заплутування коду,— це приведення вихідного коду програми до виду, що зберігає його функціональність, але ускладнює аналізування, розуміння алгоритмів роботи і модифікацію при декомпіляції. Крім того, такий метод вимагає спеціальних знань про програмування, дизасемблювання та конструкції програмного коду.

Динамічний аналіз, або аналіз поведінки,— це процес запуску файлу в ізольованому середовищі й відстеження його поведінки в системі. Щоб забезпечити безпечний запуск шкідливої програми, спершу підготовлюють середовище, яке дасть змогу вивчати її, не ризикуючи пошкодити систему або мережу. Для цього можна використовувати програми віртуалізації, наприклад «VirtualBox». Але найкраще проводити дослідження на спеціально виділеному комп'ютері, адже деякі ШПЗ мають функцію ідентифікації запуску у віртуальній операційній системі й можуть виявити не всі свої функції або навіть не запуститися. Для моніторингу дій у системі та мережевої активності слід установити додаткове програмне забезпечення, наприклад «Process Monitor», «Process Hacker», «Wireshark» або інші подібні програми. Значну кількість часу займає також аналіз зібраних журналів роботи, лог-файлів, змін у реєстрі операційної системи та інших даних, із яких необхідно вибрати потрібну інформацію та правильно її інтерпретувати.

Дослідження ШПЗ хоч і доволі новий напрям, якщо дивитися з позицій історичної перспективи, але існує достатньо довго, щоб з'явилися автоматизовані рішення для роботи з такими файлами. Хорошим рішенням буде використання спеціалізованого програмного забезпечення для аналізування ШПЗ, так званих «пісочниць» (*Sandbox*). Такі програми емулюють запуск ШПЗ у відповідно налаштованій системі, збирають дані про його дії, мережеву активність та зміни, які він вносить до системи під час своєї роботи. Крім того, завдяки таким рішення можна швидко встановити тип ШПЗ, його основні функціональні можливості. Після аналізування надається детальний звіт, у якому зазначені можливості програми та дії, які виконуються після її запуску. І хоч у таких звітах теж дуже багато даних, у них набагато легше зорієнтуватися, адже інформація структурована та подається в зручному для читання вигляді. Поміж рішень можна виділити програмне забезпечення (програмно-апаратний комплекс) «Joe Sandbox» від компанії Joe Security LLC. У ньому є можливість запуску файлів із метою простеження дій, моніторинг мережевої активності та інші функції для аналізування й розбирання шкідливих файлів. Існують також інші подібні рішення, але вони платні, і ціна в кожному випадку обговорюється із замовником.

Під час призначення експертиз, пов'язаних із ШПЗ, слід пам'ятати, що такі дослідження забирають багато часу і, залежно від складності програмного забезпечення, експерт не завжди в змозі виявити всі його приховані функції, особливо маючи в розпорядженні лише безкоштовні (вільні) інструменти з обмеженим функціоналом та можливостями. У будь-якому разі перед призначенням таких експертиз слід проконсультуватися з експертом, чи є в нього спеціальні знання та навички для виконання таких досліджень та як правильно поставити запитання.

Перелік джерел посилання

1. Monappa K. A. Learning Malware Analysis. 2018. 423 p.
2. Michael Sikorski and Andrew Honig. Practical Malware Analysis. 2012. 768 p.
3. Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (дата звернення: 06.09.2024).