покращення ситуації у зв'язку з активізацією роботи з наповнення електронного реєстру геномної інформації після впровадження профільного законодавства.

Третя проблема зумовлена організаційними складнощами та окремими прогалинами і помилками у практичній діяльності щодо призначення слідчими та прокурорами судової молекулярно-генетичної експертизи з метою ідентифікації загиблих. Наприклад, слідчі не завжди виважено підходять до підготовки постанови про призначення такої експертизи та додаткових матеріалів, які надають експертам. Тут вкрай важливо зазначати точні відомості щодо ступеня родинного зв'язку безвісти зниклої особи та родича, який надав свої біологічні зразки. Адже існують істотні відмінності між завданнями автоматизованого пошуку близькородинних зв'язків (батьки, діти) та далекородинних (брати, сестри, дядьки, тітки, бабусі, дідусі та ін.).

Також іноді трапляється несвоєчасне спрямування відібраних зразків на експертне дослідження. Здебільшого такі випадки є наслідком бюрократичної тяганини через зміну підслідності, коли, наприклад, матеріали кримінального провадження передають від слідчих поліції до слідчих органів безпеки. Процедура передавання матеріалів може тривати певний час, але, на нашу думку, в обставинах, які зараз переживає суспільство (зокрема родичі загиблих та безвісти зниклих осіб), такі зволікання є неприпустимими. В умовах воєнного стану ускладнено роботу з родичами безвісти зниклих осіб. Наразі у кожному відомстві (Національній поліції і Службі безпеки України, прокуратурі та Експертній службі МВС) визначено відповідальних за роботу з пошуку та ідентифікації осіб, але поки що відсутня чітка злагоджена взаємодія між різними суб'єктами цієї діяльності.

До того ж варто звернути увагу на необхідність чіткого дотримання судово-медичними експертами методичних вимог до відбирання біологічного матеріалу трупів. Досвід роботи експертів-генетиків Харківського НДЕКЦ МВС із біологічним матеріалом осіб, тіла яких виявлено у масових похованнях у м. Ізюм, дає змогу визначити пріоритетні зразки, із яких із великою долею вірогідності можливо швидко отримати якісний ДНК-профіль для ідентифікації. Але є випадки, коли експерти, які відбирають посмертні зразки, ігнорують ці рекомендації, що значно збільшує строки і вартість ідентифікації особи.

Проблемні питання під час виконання експертиз, пов'язаних зі шкідливим програмним забезпеченням

Євгеній Тарасенко,
Сумський НДЕКЦ, 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; вірус; аналіз; пісочниця.

Problematic issues when performing examinations related to malware

Evgeniy Tarasenko

This paper examines the methods used during the research of malicious software and the problematic issues that arise during such research.

Keywords: malware; virus; analysis; sandbox.

У наш час 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 актуальні кримінальні справи, пов'язані зі шкідливим програмним забезпеченням (далі — *ШПЗ*), націленим на викрадення цінної 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 «шкідливе програмне забезпечення» доволі розпливчастий. Він означає, що таке програмне забезпечення завдає шкоди користувачеві або системі, але немає чіткої межі, що саме може бути шкодою для системи, а що ні. Наприклад, програми віддаленого доступу при відповідних налаштуваннях дають змогу підключатися до кінцевого пристрою без підтвердження самим пристроєм. Підключення до пристрою без згоди користувача також є у функціоналі багатьох ШПЗ. Тому належність того чи того програмного забезпечення до категорії шкідливих — це юридичне

питання, 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 зроблено лише з посиланням на результати роботи антивірусного програмного забезпечення, розробленого для того, щоб ідентифікувати ШПЗ. Тому, призначаючи експертизу, першим слід поставити питання: «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 вимагають використання багатьох інструментів та аналіз за допомогою різних методів. Щодо самого аналізу, то можна визначити два його основних типи: аналіз вихідного коду та динамічний аналіз.

Аналіз вихідного коду полягає в розборі файлів методом дизасемблювання. Для цього ми завантажуємо файл в дизасемблер і досліджуємо програмні інструкції, щоб зрозуміти, які функції в ньому закладені. Ці інструкції виконуються центральним процесором, тому в такий спосіб ми можемо дізнатися деталі поведінки програми. Головним недоліком даного методу є те, що вихідний код 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 аналіз, розуміння алгоритмів роботи й модифікацію при декомпіляції. Крім того, такий метод вимагає спеціальних знань із програмування, дизасемблерування та конструкції програмного коду.

Динамічний аналіз, або аналіз поведінки, — це процес запуску файлу в ізольованому середовищі й відстеження його поведінки в системі. Щоб зробити безпечним запуск шкідливої програми, спершу готують середовище, яке дасть змогу вивчати її, не ризикуючи пошкодити систему або мережу. Для цього можна використовувати програми віртуалізації, наприклад *VirtualBox*. Але краще за все проводити дослідження на спеціально виділеному комп'ютері, адже деякі ШПЗ мають функцію ідентифікації запуску у віртуальній операційній системі та 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. Значний час 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 історичної перспективи, але існує достатньо довго, щоб з'явилися автоматизовані рішення для роботи з такими файлами. Хорошим рішенням буде використання спеціалізованого програмного забезпечення для аналізу ШПЗ, так звані «пісочниці» (*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 рішенням можна швидко встановити тип ШПЗ, його основні функціональні можливості. Після аналізу надається детальний звіт, у якому розібрані 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. Серед таких рішень можна виділити програмне забезпечення (програмно-апаратний комплекс) *Joe Sandbox* від компанії *Joe Security LLC*, у якому є можливість запуску файлів із метою простеження дій, моніторинг мережевої активності та інші функції для аналізу й розбору шкідливих файлів. Існують також інші подібні рішення, але вони платні, й ціна в кожному випадку обговорюється із замовником.

Призначаючи експертизи, пов'язані із ШПЗ, слід пам'ятати, що такі дослідження забирають багато часу, і в залежності 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 на предмет того, 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. Sikorski M., Honig A. 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/stru#Stru (дата звернення: 01.03.2023).