застосуванні альтернативних форм розв'язання кримінально-правових конфліктів, а також різних способів прискорення та спрощення досудового розслідування та судового розгляду (укладання угоди про визнання винуватості та примирення сторін, застосування медіації, спрощене провадження щодо кримінальних проступків, провадження в суді присяжних та ін.) тощо.

Література:

1. Кримінальний процес України: у питаннях і відповідях : навч. посіб. / авт. кол. ; за заг. ред. д-ра юрид. наук, доц. Т. Г. Фоміної. Харків : ХНУВС, 2021. 300 с.

2. Кримінальний процес : підручник / за заг. ред. О. В. Капліної, О. Г. Шило. Харків: Право, 2019. 584 с.

3. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 15.08.2024 р.).

АЛГОРИТМ ДОСЛІДЖЕННЯ ПОТЕНЦІЙНОГО ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID

Старенький Іван,
судовий експерт лабораторії досліджень об'єктів інформаційних технологій, телекомунікаційних систем (обладнання) та засобів Одеського науково-дослідного інституту судових експертиз Міністерства юстиції України

Донченко Олександра,
старший судовий експерт лабораторії досліджень об'єктів інформаційних технологій, телекомунікаційних систем (обладнання) та засобів Одеського науково-дослідного інституту судових експертиз Міністерства юстиції України

Шкідливе програмне забезпечення (ШПЗ) для мобільних операційних систем (ОС), зокрема Android, займає значну частку серед усіх типів ШПЗ, а ОС Android є найбільш поширеною мобільною платформою у світі, тому вона стає основною мішенню для зловмисників, після електронно-обчислювальних машин, які працюють на ОС Windows.

Відповідно до різних звітів з кібербезпеки, доля ШПЗ для Android складає близько 70–90% від усіх виявлених мобільних загроз, що робить його найбільш уразливою платформою серед мобільних ОС.

Таким чином, актуальним є розгляд питання алгоритму дослідження потенційного ШПЗ (ПШПЗ) для ОС Android, стосовно якого може бути назначено проведення експертизи за експертною спеціальністю 10.9 «Дослідження комп'ютерної техніки та програмних продуктів», враховуючи те, що порядок дослідження ШПЗ для ОС Android в [1] не розглянуто.

Для ОС Android виконуючими файлами, які є інсталяційними пакетами будь-якого ПЗ для даної ОС, є файли з розширенням »*.apk» (apk від «Android Package»).

Дослідження будь-якого ПШПЗ розділяється на два етапи – статичний та динамічний аналіз. Під час статичного аналізу проводиться дослідження ПШПЗ в «стані покою», тоді як динамічне дослідження передбачає аналіз поведінки ШПЗ під час виконання в контрольованому середовищі. Цей підхід дозволяє виявити, які дії виконує шкідливий код, як він впливає на систему, які мережеві з'єднання встановлює і які дані передає або отримує.

В першу чергу при статичному аналізі ПШПЗ, у випадку якщо це, наприклад, виконуючий файл або архів, необхідно визначити його контрольну суму за алгоритмом SHA1 [2], та за отриманим значенням провести пошук щодо даного файлу серед різноманітних сервісів з власними базами даних ШПЗ та інформації щодо нього, наприклад, «VirusTotal» [3] »AnyRun» [4].

Наступним кроком у статичному аналізі apk-файлу є проведення процесу декомпіляції останнього, з метою отримання його вихідних файлів, які разом з їхнім інформаційним вмістом, стануть подальшими об'єктами дослідження. Інструментом для декомпіляції apk-файлів є ПЗ «Apktool» [5].

В переважній більшості випадків, будь-який apk-файл в своєму декомпільованому вмісті буде мати наступні файли «strings.xml», «AndroidManifest.xml» з інформаційного вмісту яких можна встановити назву ПЗ, встановленого в середовищі ОС Android та встановити перелік прав доступу необхідних даному ПЗ – відповідно.

Серед декомпільованого вмісту apk-файлу також можна встановити зовнішній вигляд ярлика ПЗ, яке буде встановлене в середовищі ОС Android.

Основною метою статичного аналізу декомпільованого apk-файлу є аналіз інформаційного вмісту файлів з розширенням «*.smali».

Smali-файли використовуються в контексті розробки та reverse engineering (зворотнього програмування) застосунків для ОС Android.

Вони містять вихідний код на подібній до мови Assembler, яка є частиною Dalvik байт-коду, що використовується в Android-застосунках. Таким чином, дослідивши інформаційний вміст певної кількості smali-файлів, можна сформувати відповідні висновки.

Також за допомогою ПЗ «Ghidr» [5] можна провести процес декомпіляції файлу та встановити перелік всіх текстових рядків, що може бути корисним, за умови якщо хід дослідження вимагає від експерта пошуку за певними ключовими словами або словосполученнями.

Далі, розглянемо основні етапи динамічного аналізу, які можна розділити наступним чином:

1. Підготовка дослідницького середовища

– використання емуляторів або фізичних пристроїв. Для аналізу можна використовувати емулятори ОС Android (наприклад, «NoxPlayer» [6] або «BlueStacks» [7] та ін.) або фізичні пристрої з root-доступом, аби мати більше контролю над системою;

– ізоляція середовища. Необхідною умовою є налаштування ізольованого середовища для безпечного аналізу ПШПЗ, що запобігає втратам даних або зараженню інших пристроїв;

– інструменти для моніторингу. Встановлення певного переліку ПЗ для моніторингу дій ПШПЗ, таких як логери системних подій, мережеві аналізатори та інші застосунки (наприклад, «Logcat» [8], «Reqable API Testing & Capture» [9] та Wireshark [10] та ін.).

2. Запуск потенційно шкідливого застосунку

– інсталяція потенційно шкідливого APK-файлу. Встановлення застосунку на тестовому об'єкті чи емуляторі, з подальшим запуском встановленого ПЗ для ініціалізації його потенційних шкідливих дій;

– моніторинг поведінки. Одночасно з виконанням застосунку відстежується його поведінка, в тому числі створення нових процесів, використання системних ресурсів, мережева активність тощо.

3. Аналіз мережевої активності

– відстеження мережевих з'єднань. Аналіз мережевих запитів від встановленого застосунку, зокрема підключення до віддалених C2-серверів в мережі Інтернет, з яких до інфікованого пристрою можуть надходити команди щодо завантаження додаткових даних або виконання зловмисних команд;

– аналіз мережевого трафіку. Використання мережевих аналізаторів, таких як «Wireshark», для аналізу переданого і отриманого трафіку.

4. Спостереження за системними змінами

– аналіз змін у файловій системі. Виявлення будь-яких змін, внесених застосунком у файлову систему (ФС), зокрема створення нових файлів, модифікації або видалення існуючих файлів;

– моніторинг системних журналів (логів). Аналіз системних журналів для виявлення ознак підозрілої активності, таких як виклики нестандартних системних команд, спроби отримання доступу до привілейованих даних або функцій.

5. Аналіз використання ресурсів пристрою

– використання оперативної пам'яті. Вивчення того, як ПШПЗ використовує оперативну пам'ять тестового об'єкту або виділену для емулятора, включаючи виділення пам'яті для зберігання даних або виконання певних операцій;

– аналіз споживання енергії. Оцінка впливу встановленого застосунку на витрати енергії пристрою, що може бути свідченням виконання «важких» ресурсомістких завдань у фоновому режимі.

6. Завершення аналізу та складання відповідних висновків

– відновлення середовища. Після завершення динамічного аналізу, відновлення системи або емулятора до первинного стану з метою проведення подальших досліджень у майбутньому;

– документування результатів. Детальний опис всіх дій ШПЗ, виявлених під час динамічного аналізу, включаючи мережеві адреси (IP-адреси або URL-адреси), зміни у файловій системі, реєстрі та особливості поведінки;

– формування висновків. Висновки щодо мети та шкідливих можливостей застосунку, встановленого в середовищі ОС Android з APK-файлу, а також щодо потенційних загроз для користувачів та рекомендації щодо захисту.

Етап, який передбачає аналіз мережевої активності, в розрізі експертного дослідження за спеціальністю 10.9, може вимагати залучення експерта за напрямом експертної спеціальності 10.17 «Дослідження телекомунікаційних систем (обладнання) та засобів».

Таким чином, на основі описаного вище алгоритму проведення статичного та динамічного аналізів ПШПЗ можна провести вичерпне дослідження цільового APK-файлу та зробити відповідні висновки в розрізі поставлених замовником питань.

Література:

1. Методика судових комп'ютерно-технічних експертиз з дослідження шкідливого програмного забезпечення / М.О. Можаєв та ін. Харків : Національний науковий центр «Інститут судових експертиз ім. Засл. проф. Бокаріуса», Київський НДІСЕ Міністерства юстиції України, Одеський НДІСЕ Міністерства юстиції України, 2022. 100 с.

2. SHA1. *Вікіпедія: вільна енциклопедія*. веб-сайт. URL: https://ru.wikipedia.org/wiki/SHA-1 (дата звернення 15.08.2024).

3. VirusTotal. веб-сайт. URL: https://www.virustotal.com/gui/home/upload (дата звернення 15.08.2024).

4. AnyRun. веб-сайт. URL: https://any.run/ (дата звернення 15.08.2024).
5. Ghidra. веб-сайт. URL: https://ghidra-sre.org/ (дата звернення 15.08.2024).
6. NoxPlayer. *Вікіпедія: вільна енциклопедія*. веб-сайт. URL: https://ru.wikipedia.org/wiki/NoxPlayer (дата звернення 15.08.2024).
7. BlueStacks. веб-сайт. URL: https://www.bluestacks.com/ (дата звернення 15.08.2024).
8. Logcat. веб-сайт. URL: https://play.google.com/store/apps/details?id=com.tananaev.logcat&hl=ru&pli=1 (дата звернення 15.08.2024).
9. Reqable API Testing & Capture. веб-сайт. URL: https://play.google.com/store/apps/details?id=com.reqable.android&hl=ru (дата звернення 15.08.2024).
10. Wireshark. веб-сайт. URL: https://www.wireshark.org/ (дата звернення 15.08.2024).

ДЕЯКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ РЕЄСТРАЦІЇ ГЕНОМНОЇ ІНФОРМАЦІЇ ЛЮДИНИ НА СТАДІЇ ДОСУДОВОГО РОЗСЛІДУВАННЯ

Степанюк Руслан,
доктор юридичних наук, професор,
професор кафедри оперативно-розшукової діяльності та розкриття злочинів Харківського національного університету внутрішніх справ

Іонова Вікторія,
завідувач відділу біологічних досліджень та обліку
Харківського науково-дослідного експертно-криміналістичного центру
Міністерства внутрішніх справ України

Запровадження Закону України «Про державну реєстрацію геномної інформації людини» стало важливою віхою у визначенні перспектив розвитку національної бази даних ДНК і галузі криміналістичного ДНК-аналізу в цілому. У цьому законі визначено правові засади поводження із генетичними даними людини під час їх державної реєстрації, яка здійснюється насамперед у цілях розкриття та розслідування кримінальних правопорушень. У зв'язку з цим перед органами досудового розслідування не тільки виникли нові перспективи, зумовлені розширеними можливостями використання інструментів ДНК-аналізу для встановлення обставин, які мають