РЕЦЕНЗІЯ

на статтю

«Виявлення слідів використання програмного забезпечення типу "Stealer"»

Автори:

судові експерти Одеського науково-дослідного інституту судових експертиз Міністерства юстиції України

Старенький Іван Володимирович та Донченко Олександра Ігорівна

В статті, що представлена на рецензію автори висвітлюють завдання досліджень, сферу застосування, проблематику особливостей дослідження та можливості і принципи їх проведення.

Тематика статі, що представлена на рецензію є актуальною з наступних міркувань:

- проведення криміналістичних досліджень програмних продуктів, що відносяться, або позиціонуються як шкідливе програмне забезпечення має важливе значення для правоохоронних органів, так як злочини з використанням програмного забезпечення типу «Stealer», активно використовуються злочинцями, а виконуючі файли такого програмного забезпечення є безпосереднім знаряддям злочину;
- проведення дослідження складових потенційного шкідливого програмного забезпечення дає можливість у підтвердженні або спростуванні факту належності об'єкту дослідження до категорії шкідливого програмного забезпечення, а у випадку з дослідженням програмних продуктів типу «Stealer», дозволяю встановити С2-сервер, з яким встановлює з'єднання виконуючий файл, а також додаткову інформацію про файли-звіти, щодо роботи «Stealer»-програми в середовищі інфікованої робочої станції.

Слід зазначити, щоб провести дослідження таких виконуючих файлів, їх потрібно спочатку знайти серед інформаційного вмісту в пам'яті накопичувача інформації. Саме це питання розглядається авторами в даній статті, і тому дана проблема є актуальною в нашому сьогоденні.

В статті детально розглянуто використання програмного модулю «Timeline», що відноситься до програмного забезпечення «Autopsy - Digital Forensics» з метою відтворення та відстеження подій та процесів, що відбувалися на накопичувачі інформації, для виявлення моменту ініціалізації виконуючого файлу програмного забезпечення типу «Stealer», що в свою чергу надасть можливість встановити початкову точку початку роботи даного програмного продукту.

Стаття спрямована на стимулювання проведення судових комп'ютерно-технічних експертиз з використанням програмного забезпечення «Autopsy - Digital Forensics» в більш широкому його спектрі можливостей, а не тільки для вилучення історії браузерів та файлів, що відносяться до певної категорії. Це дасть змогу не лише покращити роботу експертів у майбутньому, а й належним чином використати технічні засоби та методи при проведенні криміналістичних досліджень.

Дана стаття несе рекомендаційний характер та має суттєве практичне значення. Матеріал поданий у статті послідовно, оформлений згідно вимог до збірника. Стаття рекомендується до друку у випуску 68 міжвідомчого науково-методичного збірника «Криміналістика і судова експертиза».

Завідувачка кафедри
Інформаційні системи
Національного університету
«Одеська політехніка»
доктор технічних наук, професор Арсірій Олена Олександрівна

Особистий підпис Арсірій О.О
засвідчую
Ст. інспектор

ВІДДІЛ КАДРІВ