Metody kryptografii w analizie danych – Projekt

Steganografia w plikach ZIP

Ernest Roszak

12 marca 2023

1 Cel projektu

Celem projektu jest napisanie dwóch skryptów w języku Python. Pierwszy z nich będzie ukrywał dane w pliku w formacie ZIP, drugi – odczytywał je. Pliki nie powinny być wykrywane przez Windows Defendera jako szkodliwe, a samo archiwum nie powinno być odczytywane przez programy użyte do czytania plików ZIP jako zepsute (corrupted).

2 Format ZIP

Plik w formacie ZIP stanowią tzw. archiwum, w którym mogą być przechowywane inne pliki. Każdy plik przechowywany jest osobno, co umożliwia zastosowanie różnych metod kompresji dla każdego z plików. Dzięki temu można też dodawać i usuwać pliki z archiwum, modyfikując tylko jego fragmenty, bez modyfikacji plików sąsiednich.

Archiwum ZIP można podzielić na następujące dwie części:

- Sekcja file entries – pliki wraz z headerami, ułożone w losowej kolejności.
- Sekcja central directory, która zawiera nazwy plików przechowywanych w archiwum, ich metadane, jak również odpowiedni offset, oznaczający gdzie należy szukać tego konkretnego pliku.

Programy czytające pliki ZIP odczytują najpierw central directory, w celu wylistowania wszystkich plików. Jeśli więc jakiś plik zostanie dodany do archiwum, ale odpowiednia informacja nie zostanie dodana do central directory, programy służące do odczytywania archiwum nie wyświetlą go.

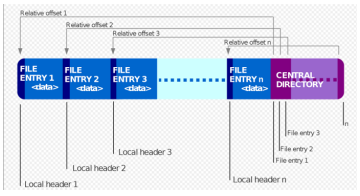
3 Pomysły

1. https://github.com/gromnitsky/zipography

   Dodanie pliku przed pierwszym headerem central directory i zmodyfikowanie wskaźnika znajdującego się w end of central directory, aby wskazywał na początek central directory

2. https://www.codeproject.com/Articles/13808/Steganography-16-Hiding-additional-files-in-a-ZIP

   Dodanie pliku w losowy miejscu, i usunięcie/nie wpisywanie informacji do central directory. Aby odczytać ukryty plik, przechodzimy po każdym lokalnym headerze w archiwum, aż nie znajdziemy takiego, którego specjalna zmienna ZipFileIndex została oznaczona jako -1.



Rysunek 1: $https://en.wikipedia.org/wiki/ZIP_(file_format)$