УДК 004.056:003.27

ВИКОРИСТАННЯ СТЕГАНОГРАФІЇ ДЛЯ ЗБЕРЕЖЕННЯ ТА ПЕРЕДАЧІ ІНФОРМАЦІЇ

Капуста Р.Д., Горяінова К.О.
Науковий керівник – ст. викл. Волотка В.С.
Харківський національний університет радіоелектроніки,
кафедра ІКІ ім. В.В. Поповського, м. Харків, Україна
тел. +38(095) 30-771-72, e-mail: roman.kapusta@nure.ua
тел. +38(097) 95-610-28, e-mail: karyna.horiainova@nure.ua

This work is dedicated to the study of the method of increasing the security of data storage and transmission by using a tool for steganographic file modification. The rapid development of information storage and transmission technologies entails a certain list of challenges related to the security of users' personal data. However, a potential thief can also use steganography to hide and transfer harmful software code, leading to undesirable consequences.

Ще давно людство використовувало різноманітні шифри для захисту інформації та недопущення розкриття даних у разі потрапляння інформації у інші руки. Сьогодні шифрування та кодування інформації стало звичайною справою без якої неможлива передача інформації у будь-який спосіб по мережі інтернет. Проте окрім класичних зашифрованих даних, які мають досить явний вигляд, використовується також і приховані повідомлення, що досягаються завдяки стеганографії.

Сучасна стеганографія відрізняється своїм різноманіттям інструментів та можливостей, одним з яких є приховування текстової інформації у вигляді зображення. Розглянемо використання програмного продукту "Outguess", який можливо використовувати на базі Linux-подібних операційних систем у нашому випадку це Kali Linux.

Функціонал даного програмного продукту дозволяє вставляти приховану інформацію в надлишкові біти джерел даних, а також природа джерела даних не має значення для роботи. Програма покладається на специфічні для даних обробники, які витягують надлишкові біти і записують їх назад після модифікації та підтримуються формати JPEG, PPM і PNM.

Для прикладу, створюємо простий скрипт, який дозоляє робити знімки екрану користувача без його відома та зберігати їх у відповідній папці. Назвемо цей файл «vir.py». Наступним кроком завантажуємо зображення під назвою «File1.jpg» та розміщуємо його у одній папці разом зі шкідливим програмним кодом. Використовуючи програмний продукт "Outguess" проводимо злиття файлів для отримання кінцевого зображення, яке містить у собі файл скрипту. Результат виконання перетворення файлів та відповідні результати приведено на рис. 1.

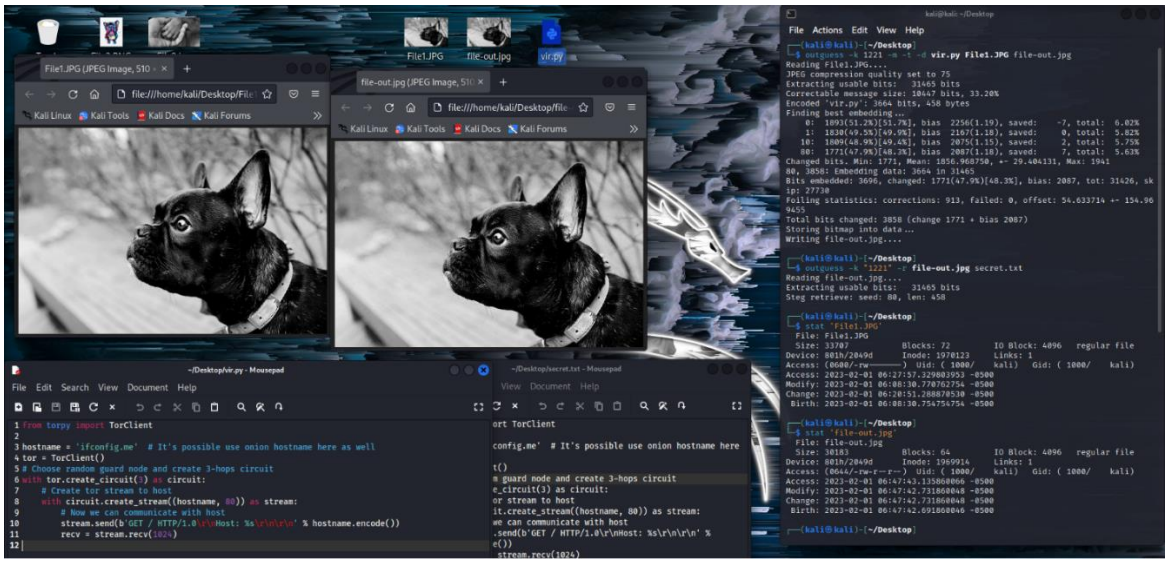

Рисунок 1 – Виконання перетворення

Розглянемо послідовність дій в консолі. Для початку встановимо ключ «пароль», в нашому випадку це “1221” та дані «vir.py» помістимо в зображення «File1.jpg». Ключ встановлюється для того, щоб в подальшому вилучити інформація с файлу без ключа було неможливо. Далі витягнемо повідомлення з даних в файл «secret.txt» за допомогою ключа. Відтепер можемо розглянути дані які були зашифровані.

Слід звернути увагу на те, що розмір зображення змінився. Спочатку 33707 байтів, а після внесення та шифровки даних 30183 байтів, а також кількість блоків – спочатку 72, а потім 64. Тобто оригінал виходить більше, ніж з тими даними, які були усередині.

Спираючись на отримані результати ми можемо дійти висновків, що стеганографія може бути використана зловмисником для передачі шкідливого програмного скриту у зображені, яке зовнішньо майже нічим не буде відрізнятися від оригіналу. Найкращій метод збереження власних даних від подібних пасток шахраїв - ігнорування підозрілих файлів від невідомих відправників, а також перевірка версій зміни файлів.

Ваша пильність та обачність – запорука безпеки персональних даних!

Список використаних джерел:

1. Martin, K. (2020, 27 січня). Що таке стеганографія та чим вона відрізняється від криптографії? instagalleryapp.com. https://instagalleryapp.com/informacijna-bezpeka/shho-take-steganografija-ta-chim-vona/.

2. Semilof, M., & Clark, C. (2021, 6 липня). What is Steganography? - Definition from SearchSecurity. Security. https://www.techtarget.com/searchsecurity/definition/steganography