УДК 004.056.4

Г. А. Дмитрук
Н. В. Копайгородська
В. В. Карпінець

ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ ЗАСОБІВ У КІБЕРАТАКАХ ТА ШПИГУНСЬКОМУ ПЗ

Вінницький національний технічний університет

Анотація

Проаналізовано динаміку використання стеганографічних методів під час розробки шкідливого ПЗ та засобів кібератак. В ході аналізу були виявленні причини частого використання стеганографічних методів в кібератаках, а також їх ефективність для зловмисників. Було досліджено низку методів знаходження заповених стегоконейнерів, та визначено ефективність використання кожого з них в тій чи іншій ситуації..

Ключові слова: повідомлення, ключ, стегоканал, стегосистема, контейнер (стегоконтейнер).

Abstract

The dynamics of the use of steganographic methods during the development of malware and cyberattacks is analyzed. The analysis identified the reasons for the frequent use of steganographic methods in cyberattacks, as well as their effectiveness for attackers. A number of ways to counter such attacks have been proposed.

Keywords: message, key, stegochannel, stegosystem, container (stegocontainer).

В даний час комп'ютерна стеганографія продовжує розвиватись: формується теоретична база, ведеться розробка нових, більш стійких методів вмонтовування повідомлень. Серед основних причин зростання зацікавленості стеганографією можна виділити прийняті в ряді країн обмеження на використання сильної криптографії, а також проблему захисту авторських прав на художні твори в цифрових глобальних мережах [1].

Комп'ютерна стеганографія широко використовується при обміні секретними повідомленнями, написанні вірусних програм, у захисті авторських прав, для приховування даних від копіювання і т.д. Останнім часом вона набула популяності в використанні саме розробниками шкідливого ПЗ, а також зловмисниками з кібератак [2].

За недавній час використання стеганографії здійснювалося в наступних шкідливих програмах і засобах кібершпіонажу: Microcin (AKA six little monkeys), NetTraveler, Zberp. Enfal (its new loader called Zero.T), Shamoon, KinS, ZeusVM. Triton (Fibbit) [3].

Проаналізувавши ці дані, можна виокремити три основні причини активного використання стеганографії авторами шкідливого ПЗ:

- це дозволяє їм приховати сам факт завантаження / вивантаження даних, а не тільки самі дані;
- допомагає обійти DPI-системи, що актуально в корпоративних мережах;
- використання стеганографії може дозволити обійти перевірку в AntiAPT-продуктах, оскільки останні не можуть обробляти всі графічні файли (їх занадто багато в корпоративних мережах, а алгоритми аналізу досить дорогі) [4].

Існує декілька статистичних методів аналізу даних на вміст у них прихованої стеганографічними методами різного роду інформації. Розглянемо декілька з них.

Гістограмний метод статистичного аналізу також відомий як «хі-квадрат» -метод. Весь растр аналізується, для кожного кольору вважається кількість точок такого кольору в растрі (для простоти тут говоримо про зображення, що має одну колірну площину). Метод виходить з припущення, що кількість точок двох сусідніх кольорів («сусідні» кольору - кольору, які відрізняються тільки найменш значущим бітом) різниться суттєво для нормального, звичайного зображення (порожнього контейнера) І кількість пікселів таких кольорів є приблизно однаковим для заповненого контейнера. Таким чином, для зон, у яких розраховане значення хі-квадрат менше порогового, можна прийняти вихідну гіпотезу «розподіл частот сусідніх квітів - однакове, отже, це заповнений стегоконтейнер».

Дійсно, якщо подивитися на зображення для візуальної атаки, нескладно помітити, що ці області містять запроваджене повідомлення [5]. Таким чином, для впроваджених повідомлень з високою ентропією метод працює.

Ще один метод називається RS-метод, де RS означає «регулярний-сингулярних». Всі зображення розділяється на безліч груп пікселів, далі для кожної групи застосовується спеціальна фліппінг-

процедура. На підставі значення функції-дескримінанта до і після застосування фліппінга всі групи діляться на регулярні, сингулярні і невикористовувані [6]. Алгоритм грунтується на припущенні, що кількість регулярних і сингулярних груп пікселів в оригінальному зображенні і в зображенні після застосування фліппінга має бути приблизно рівним. Якщо кількість таких груп істотно змінюється в процесі застосування фліппінга, це означає, що досліджуване зображення є заповненим контейнером [7].

Результи тестів на правильність роботи вище зазначених методів показали, що на зображеннях з низькою ентропією атака типу «хі-квадрат» не може бути застосована - результати або незадовільні, або не цілком точні, зате RS-атака відпрацювала відмінно: в обох випадках було визначено наявність прихованого повідомлення [8]. Але що ж робити якщо автоматичні методи аналізу показали відсутність впровадженого повідомлення, а ми все ще підозрюємо це? Можна використовувати конкретні процедури для отримання корисного навантаження, розроблені для конкретних сімейств шкідливого ПЗ.

Отже, все більше і більше розробників шкідливого ПЗ починає використовувати стеганографію, в тому числі - для приховування комунікації з командним центром і для завантаження модулів. Це дає результат, адже процедури аналізу контейнерів імовірнісні і дорогі. Саме більшість захисних рішень не можуть собі дозволити обробляти всі об'єкти, які потенційно можуть бути заповненими контейнерами.

Однак рішення є, вони засновані на комбінуванні різних способів аналізу, високошвидкісних предетектах, дослідженні метаданих потенційно заповненого контейнера тощо. Було досліджено низку методів знаходження заповених стегоконейнерів, та визначено ефективність використання кожого з них в тій чи їншій ситуації..

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Хорошко В.О. Комп’ютерна стеганографія: [навчальний посібник] / В. О. Хорошко, Ю. Є. Яремчук, В. В. Карпінець. –Вінниця : ВНТУ, 2017. –155 с.
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.
3. Карпінець В. В. Аналіз впливу цифрових водяних знаків на якість векторних зображень / В. В. Карпінець, Ю. Є. Яремчук // Сучасний захист інформації. — 2011. — № 1. — С. 72—82.
4. В.О.Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є.Яремчук. Основи комп’ютерної стеганографії. – Вінниця ВДТУ, 2003.
5. Корольов В. Ю. Планування дослідження методів стеганографії та стегоаналізу / В. Ю. Корольов, В. В. Поліновський, В.А. Герасименко М. Л. Горінштейн // Вісник Хмельницького національного університету, № 4, 2011 – 187-196 с.
6. Корльов В. Ю. RS-стегоаналіз. Принципи роботи, недоліки та концепція метода його обходу / В. Ю. Корольов, В. В. Поліновський, В.А. Герасименко // Вісник Вінницького політехнічного інституту – 2010 - №6 – 66-71 с.
7. Грибунин В.Г, Оков И.Н., Туринцев И.В. Цифровая стеганография. - М.: СОЛОН-Пресс, 2012.
8. Азарова А.О. Методичні вказівки до проведення практичних занять та до виконання самостійної індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 –«Менеджмент» та 6.170103 –«Управління інформаційною безпекою» / Азарова А.О., Карпінець В.В. –Вінниця: ВНТУ, 2013. –44 с.

Дмитрук Ганна Анатоліївна — студентка групи УБ-19м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: anytka2227@ukr.net.

Копайгородська Наталія Василівна — студентка групи УБ-19м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail:natali4ka16@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** — кандидат технічних наук, доцент, завідувач кафедри менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця

Dmitruk Hanna A. — student, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnytsia, email : anytka2227@ukr.net

Kopaihorodska Nataliia V. — student, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnytsia

Supervisor: **Karpinets Vasyl V**.—Ph. D., assistant professor, Head of the Department of Management and Security of Information Systems, Vinnitsa National Technical University, Vinnytsia.