

## ВИКОРИСТАННЯ СТЕГАНОГРАФІЇ В КІБЕРАТАКАХ

Стеганографія це спосіб передачі або зберігання інформації з урахуванням збереження в таємниці самого факту такої передачі. У даній роботі буде розглянуто використання стеганографії в зображенні. Тому варто також сказати, що стеганографія зображень – це приховування коду, можливо шкідливого, у звичайному зображенні.

Вперше поняття стеганографії було введено в 1499 році, але приховування інформації використовувалось ще до нашої ери. Наприклад в 240 році до нашої ери, китайський імператор Цин Шихуанді дуже любляв писати секретні листа [1]. Використовував він, для цього, густий рисовий відвар, який після висихання не залишав ніяких видимих слідів. Далі цей лист потрапляв в потрібні руки, і після змочування слабким спиртовим розчином йоду починали з'являтися написані раніше ієрогліфи.

Кібератака – це несанкціонована, шкідлива спроба людини або будь-якої нечесно налаштованої організації проникнути в інформаційну систему іншої людини або організації. Тобто кібератака – це масове зараження комп'ютерів вірусами. Як правило, зловмисники прагнуть отримати з цього вигоду. Яскравий приклад кібератаки стався у 2017 році, атака була націлена на Україну. Але через кілька годин вірус вирвався за її межі. Іменував він себе NotPetya. Потрапивши на один комп'ютер через оновлення M.E.Doc (українське програмне забезпечення для подання звітності до контролюючих органів), вірус отримував логін і пароль адміністратора і поширювався далі по локальній мережі. Можна сказати, що цей вірус покращив Україну в сфері кібербезпеки. Адже вже минуло більше трьох років, а нові, масштабні віруси більше не з'являлись. Але той факт, що з часів NotPetya в Україні не було жодної гучної атаки, не свідчить про те, що зловмисники припинили свою активність.

На сьогодні існує велика кількість різних алгоритмів і методів стеганографії. Основні з них це методи LSB та квантування; алгоритм Коха-Жао; метод, заснований на приховуванні даних в коефіцієнтах дискретного косинусного перетворення та метод приховування інформації в службових полях формату. Ці методи розглянуті у [2].

За останні 10 років стеганографія стала дуже часто використовуватися в різних шкідливих програмах і засобах кібершпіонажу. Нижче приведено список, який складається з десяти найбільш популярних вірусів, які в своїх неблагих цілях використовували стеганографію:

- 1) Duqu (2011);
- 2) KinS (2011);
- 3) Stegoloader (2012);
- 4) ZeusVM (2014);
- 5) Gatak (2015);
- 6) TeslaCrypt (2015);
- 7) NetTraveler (2016);
- 8) Cerber (2017);
- 9) Triton (Fibbit) (2017);
- 10) Microcin (SixLittleMonkeys) (2020).

Як ми бачимо віруси, які використовували стеганографію в поганих цілях, з'являлися майже щороку і це тільки популярні з них.

У даній роботі буде розказано про найперший вірус, який шифрував дані і приховував їх усередині графічних файлів "JPEG", які пізніше відправлялися на сервер управління. Даний вірус був спрямований на найбільші світові компанії. Його прозвали ім'ям Duqu. Про нього стало відомо 1 вересня 2011 року. Свого часу він торкнувся великої кількості країн (рисунк 1, [3]). Він містив дуже багато складних функцій, які могли бути розроблені тільки групою висококваліфікованих програмістів. Як вже було сказано раніше, ці функції включали стенографічні процеси, які шифрували вкрадені дані і вставляли їх в зображення перед тим, як відправити на сервери, контрольовані зловмисниками.



А – Франція, Нідерланди, Швейцарія, Україна; В – Індія; С – Іран; D – Іран;  
Е – Судан; F – В'єтнам

Рисунк 1 – Географічне поширення

Щоб не вдаватися в подробиці його змісту, а там дуже багато інформації, яка не пов'язана з цією роботою, перейдемо відразу до використання стеганографії у вірусі Duqu. В даному вірусі є файл Infostealer

[3]. Цей автономний виконуваний файл був завантажений вірусом Duqu. Його основні функції виконуються бібліотекою DLL, що міститься у виконуваному файлі. Крім того DLL зберігається у вигляді зашифрованих даних у файлі JPEG. JPG – це перші 8192 байт зображення Хаббла (рисунок 2, [3]).

Існування цього зображення змусило деяких припустити, що Duqu може бути загрозою «зірок», оголошеної іранськими офіційними особами в квітні 2011 року, але здається, що розробникам даного вірусного програмного забезпечення просто подобалася астрономія.

При виконанні файл витягував зашифровану DLL зі збереженого в ній JPEG, а потім виконував експорт DLL. DLL крав дані і зберігав їх у файлі з довільним номером в папці %Temp% користувача, додаючи до файлів журналу ~ DQ (наприклад, ~ DQ7.tmp).

Цей DLL міг вкрасти: списки запущених процесів; дані облікового запису; назву дисків; скріншоти; мережеву інформацію; натискання клавіш; назви відкритих вікон. Також він міг переглядати файли на всіх дисках, включаючи знімні. Детальніше про DLL розписано у [3].



Рисунок 2 – Зображення Хаббла

Як бачимо все це було зроблено за допомогою однієї маленької картинки про космос. Існує три головних причини використання стеганографії авторами шкідливого програмного забезпечення в своїх розробках [2]:

стеганографія дозволяє приховати сам факт завантаження/вивантаження даних, а не тільки самі дані; стеганографія 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.

Отже, після розгляду даної роботи можна зробити висновок, що використання стеганографії сьогодні дуже популярна ідея серед авторів шкідливого програмного забезпечення, тому потрібно обов'язково вміти з цим боротися.

Для цього існує безліч різних шляхів вирішення даної проблеми. Основне з них це постійне оновлення антивірусних програм. Хоч антивіруси і не врятовують від вразливості нульового дня, але подальший стабільний захист комп'ютера вони забезпечити зможуть. Більш докладне рішення даної проблеми буде розглянуто авторами пізніше.

### **СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ**

1. Стеганография. История тайнописи [Електронний ресурс]. – Режим доступу: <http://maxima-library.org/knigi/genre/b/451565?format=read>
2. Стеганография в современных кибератаках [Електронний ресурс]. – Режим доступу: <https://securelist.ru/steganography-in-contemporary-cyberattacks/79090/>
3. W32.Duqu. The precursor to the next Stuxnet. [Електронний ресурс]. – Режим доступу: [https://scadahacker.com/files/duqu/w32\\_duqu-the-next-precursor-to\\_the\\_next\\_stuxnet\\_v1.4.pdf](https://scadahacker.com/files/duqu/w32_duqu-the-next-precursor-to_the_next_stuxnet_v1.4.pdf)