Trustwave® SpiderLabs®

Esteganografía, ¿Qué es y con qué se come?

Workshop

M.Sc. Jesús Olguín
Security Researcher

Junio 22, 2018

Agenda

- ¿Qué es esteganografía?
- Método esteganográfico básico
- Categorías de métodos esteganográficos
- ¿Cuál es el riesgo?
- Características de las técnicas esteganográficas
- Método LSB
- Programación del método LSB

¿Qué es esteganografía?

¿Qué es esteganografía?

La esteganografía es el antiguo arte de ocultar mensajes dentro de un archivo portador, de tal manera que solo el transmisor y el receptor del mensaje sepan sobre la existencia de dicha información.

- στεγανος : *steganos* : Cubierto, escondido, protegido
- γραφος : *graphos* : Dibujo o escrito

¿Qué es esteganografía?

a) b)

Fig. 1. a) An image without any modification. b) An image after embedding a list of names, emails and cellphone numbers.

El mensaje se debe ocultar de tal forma que no sea perceptible ninguna alteración a simple sentido humano.

Si alguien que no forma parte de la cadena del mensaje (emisor y receptor) es capaz de detectar alguna anomalía en el archivo portador, se considera que el método ha fallado.

¿Qué es esteganografía?

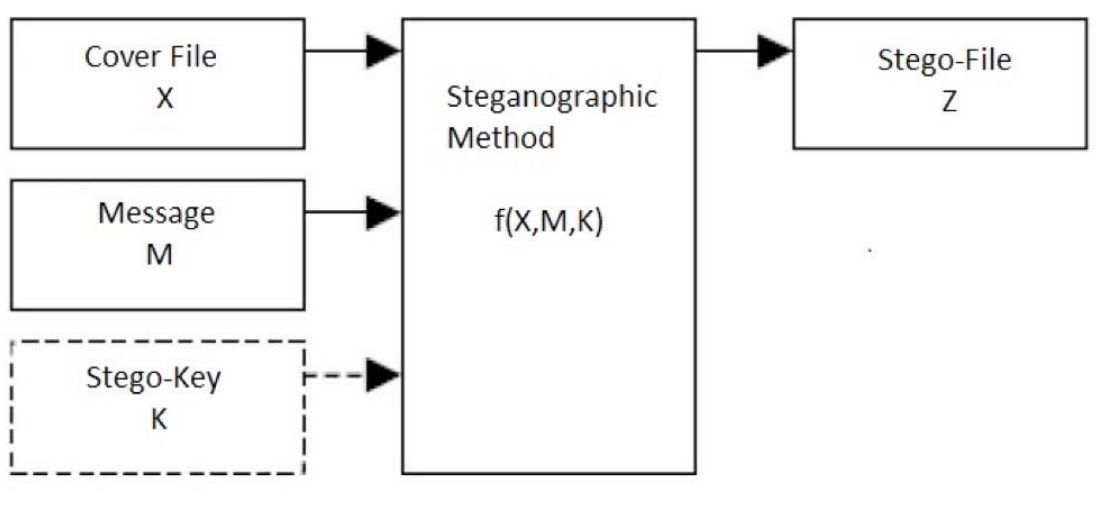
La esteganografía y la criptografía son primos en el área de seguridad informática. Sin embargo, las técnicas que emplean son distintas.

- En criptografía, la estructura original del archivo es modificada para crear algo que no tenga sentido por si mismo.
- En esteganografía, el mensaje se oculta dentro de un archivo que DEBE tener un sentido por si mismo.

Ambos tienen como objetivo principal proteger el mensaje/archivo que se pretende enviar.

Método esteganográfico básico

Método esteganográfico básico



- **Cover File (Archivo portador), 'X'** : Este es el archivo que se utilizará para ocultar el mensaje.
- **Message (Mensaje), 'M'** : Información secreta que se ocultará en 'X'.
- **Stego-Key (Llave esteganográfica), 'K'** : Algunos métodos esteganográficos requieren de una llave para poder ocultar/recuperar 'M' de 'X'.
- **Steganographic Method (Método esteganográfico), 'f(X,M,K)':** Existe una gran variedad de métodos.
- **Stego-File (Archivo resultante), 'Z'** : El archivo que contiene el mensaje oculto.

Método esteganográfico básico

Para recuperar el mensaje solo debemos aplicar el proceso inverso utilizando la misma llave esteganográfica (en caso de ser necesaria) que utilizamos para ocultar el mensaje.

Una vez que recuperamos el mensaje oculto, el contenido del archivo portador no es relevante por lo que no debemos preocuparnos por recuperar la información perdida de dicho archivo.

Categorías de métodos esteganográficos

Categorías de métodos esteganográficos

Existen distintas maneras de categorizar los métodos esteganográficos. Dos de las formas mas comunes es por:

- Tipo de llave
- Dominio en el que trabajan

Categorías de métodos esteganográficos

Tipo de llaves:

- Sin llave
  - Son los métodos que no requieren de ninguna llave. Son los más sencillos de implementar, pero los mas inseguros.
- Secreta
  - Tanto el emisor como el receptor comparten la misma llave para esconder y recuperar el mensaje.
- Pública
  - Se utilizan 2 llaves distintas, una para esconder el mensaje y otra para recuperarlo.

Categorías de métodos esteganográficos

Dominio en el que trabajan:

- Espaciales
  - Aquellos que trabajan sobre los valores directos del archivo portador.
- Frecuenciales
  - Aquellos que requieren de una transformación en los valores del archivo portador, como una transformación de Fourier o Wavelet, para trabajar sobre ellos.

¿Cuál es el riesgo?

¿Cuál es el riesgo?

El uso de esteganografía puede llegar a ser muy grave debido a que es un modo muy sencillo en el que se puede extraer información sensible de las organizaciones, como contratos o información de contactos, sin que exista una detección oportuna.

En internet se pueden obtener diversos programas para ocultar archivos dentro de imágenes o audios sin ningún costo, por lo que se puede considerar como una amenaza latente y de fácil implementación.

Características de las técnicas esteganográficas

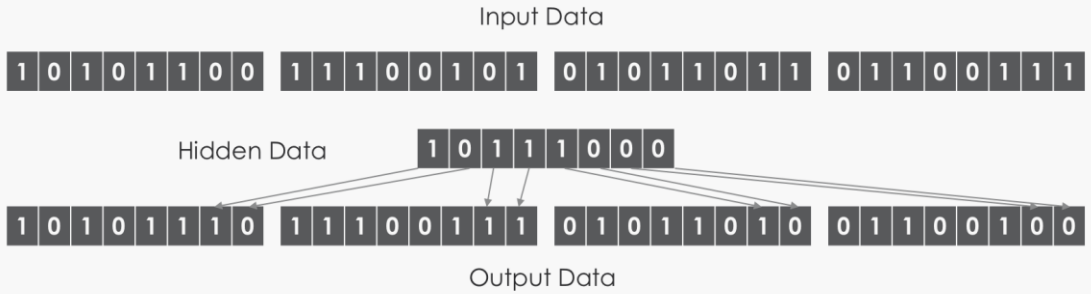
Características de las técnicas esteganográficas

a) Imagen Natural b) Stego-Imagen

- Capacidad de ocultamiento
- Transparencia perceptual
- Robustez
- Resistencia a la manipulación

Método LSB

Método LSB



El método esteganográfico del Bit Menos Significativo (LSB, por sus siglas en inglés) es uno de los más comunes y más famosos en la literatura. En este método se modifican, como su nombre lo indica, los bits menos significativos del cuerpo del archivo.

Existen dos métodos de LSB: LSB Replacement (LSB-R) y LSB Matching (LSB-M).

Método LSB

En LSB-R, todo lo que se hace es cambiar un bit menos significativo del cuerpo del archivo por uno del mensaje que se desea ocultar hasta terminar con el mensaje. Es muy sencillo detectar si este algoritmo ha sido utilizado debido a la nula complejidad del método.

En LSB-M, se utilizan algunas operaciones matemáticas para esparcir el mensaje por todo el cuerpo del archivo mediante el uso de una llave. No se hace una simple sustitución de bits, se debe acordar si se sumará o restará un valor predefinido a los bytes.

Programación del método LSB

¿Preguntas rápidas?

Para preguntas más detalladas:
jolguin@trustwave.com

Smart security on demand