Universidad de Talca
Facultad de Ingeniería
Departamento de Ciencias de la Computación

Seguridad Informática

Tarea 2

Erik Regla
eregla09@alumnos.utalca.cl

3 de mayo de 2020

1. Enunciado

Deberá entregar un informe sobre la técnica denominada Esteganografía, donde deberá definir que es e identificar en cual o cuales de las fases de un ataque informático se utiliza. Además deberá entregar un ejemplo concreto de su utilización.

2. Desarrollo

2.1. Definición de esteganografía

La esteganografía se define como el encapsulado de información utilizando otro medio como portador. Uno de los ejemplos más simples es el de la utilización de tinta invisible reactiva a UV (popular en los años 90). La diferencia en la coloración del papel de la tinta invisible es casi inperceptible para el ojo humano, sin embargo, al ser expuesto el papel a una fuente de radiación UV, esta brilla con tonos fosforecentes dejando visible el mensaje oculto en el medio (figura 1).

2.2. Utilización en un ataque informático

Esteganografía como técnica puede ser utilizada para ocultar información en archivos que admitan el concepto de "perdida de compresión"[1]. Si bien esta puede ser utilizada sobre archivos que no admitan pérdida, si detección es mucho mas simple. Casos como este son las muestras de puntos que dejan las impresoras laser, las cuales permiten identificar que impresora imprimió un documento y su firma de tiempo. Estas no son perceptibles por un ojo humano, pero si son fácilmente identificables por una máquina (figura 2).

Ejemplos de este tipo de archivos son archivos de imágenes en formato jpg, audio en formato ogg o mp3. Esta técnica no está limitada solo al uso de estos formatos, pero son los más simples de encontrar.

[1] https://en.wikipedia.org/wiki/Lossy_compression

Figura 1: Ejemplo de uso de tinta invisible

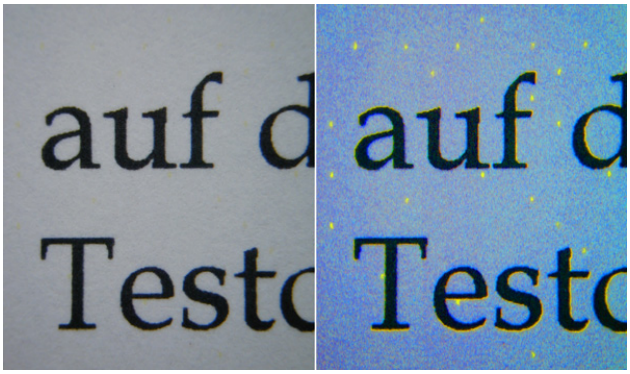

Figura 2: Puntos amarillos de las impresoras

Durante la etapa de reconocimiento puede ser utilizado para obtener información por medio de la propagación de medios y firmas (por ejemplo, trazar los usuarios que tuvieron contacto con un contenido), ocultar información de identidades u otra necesaria para esta. Durante la etapa de adquisición de acceso puede ser utilizada para transportar datos o cargas a un equipo destino para su posterior ejecución, de ahí en adelante su uso permite la mantención de acceso. Debido a esto, se puede decir que esta técnica primariamente considera tres de las cinco fases de un ataque, sin embargo, transitivamente puede extenderse a ocultar rastros (ya que por lo general el proceso de estenografía es ejecutado de manera ortogonal) y a la etapa de exploración debido a las mismas características del escaneo por su uso en pentesting físico.[2]

2.3. Ejemplo de utilización

Uno de los ejemplos más simples de visualizar es el ocultar cargas ejecutables dentro de un archivo de uso común, como por ejemplo una imagen digital[3].

```
#!/bin/bash
## instalar herramientas
sudo apt-get install steghide

## obtener imagen portadora
wget -O carrier.jpg https://avatars2.githubusercontent.com/u/3944601\?s\=400\&u\=15c877e746043bd5136706f0f51ce6bc0d69353c\&v\=4

## guardar texto
echo "haha._Esto_podria_ser_un_ejecutable." > payload.txt

## embed contenido en archivo
steghide embed -p le_passwd  -cf carrier.jpg -ef payload.txt -sf new_carrier.jpg

## compare
cmp carrier.jpg new_carrier.jpg
xxd carrier.jpg > carrier.hex
xxd new_carrier.jpg > new_carrier.hex
diff carrier.hex new_carrier.hex #check that it's important to preserve the header

## delete originals
rm carrier.jpg payload.txt

## retrieve file
steghide extract -p le_passwd  -sf new_carrier.jpg -xf payload_retrieved.txt

## haha
cat payload_retrieved.txt
```

[2]https://publications.computer.org/computer-magazine/2018/11/15/how-steganography-works/
[3]https://securelist.com/steganography-in-contemporary-cyberattacks/79276/