

Desafío: El Espía Oculto

A continuación, se presenta una imagen, la cual se ha recibido de forma sospechosa. Nuestra tarea es analizar la misma y descartar que contenga algún archivo malicioso o ver si tiene un mensaje oculto en su estructura, por lo que se van a utilizar distintas técnicas y herramientas para el análisis.

Imagen recibida:

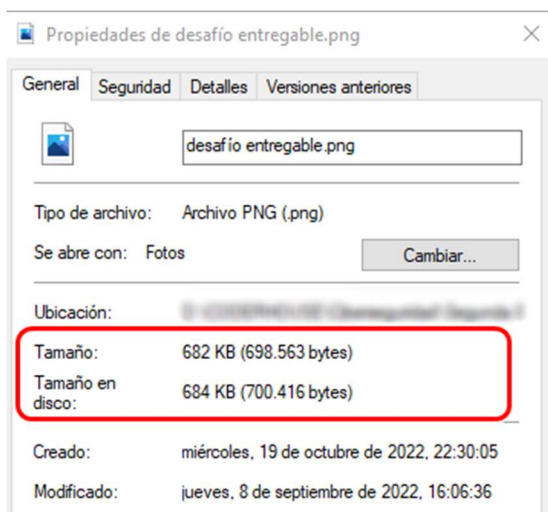


Nombre del archivo: desafío entregable.png

Lo primero que analizamos es el nombre y tipo de archivo, el cual tiene la extensión .PNG (*formato de **archivo** que se emplea de forma generalizada en los sitios*

web para mostrar imágenes digitales de alta calidad), indicativo de que es una imagen legítima.

Si realizamos una búsqueda visual y minuciosa en la imagen, podemos determinar que, a simple vista, no hay ningún mensaje evidente. De esta manera procedemos a buscar la información de la imagen (tamaño, detalle, propietario, etc.) dentro de las propiedades de la misma.



Visualizadas las propiedades, no encontramos ningún dato que nos parezca sospechoso. De esta manera, para realizar un análisis más profundo, nos abocamos al uso de la herramienta HxD Hex Editor para obtener los datos Hexadecimales de la imagen.

Tamaño del archivo: 47 4E 50 89 (cabecera) = 5.132.425 bytes

Tamaño en propiedades: 698.563 bytes

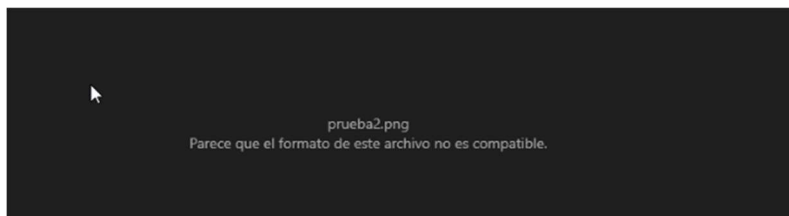
PNG: 50 4E 47

IHDR: 49 48 44 52

IEND: 49 45 4E 44

Teniendo en cuenta la cabecera PNG y tomando el IEND como último dato hexadecimal, se genera un archivo con extensión PNG, no pudiendo abrir el mismo.

Posiblemente esto se debe a que el archivo ya estaba en formato PNG y al extraer los datos hexadecimales se cambia el tamaño de la estructura, haciendo que el mismo quede inaccesible.



Luego se realizó otra prueba, copiando % (símbolo anterior a PNG) hasta IEND y se abre la imagen como la original pero no se detecta mensaje alguno.

De acuerdo al análisis Hexadecimal, se encontró una diferencia de tamaño por eso se buscaron posibles extensiones (.zip, .jpg, .txt, etc) dentro del archivo para descartar algún objeto incrustado, pero no se encontró ninguna.

Al no obtener buenos resultados hexadecimales (método manual), procedemos a utilizar otras herramientas.

Primero, utilizando la Herramienta Online:

<https://stylesuxx.github.io/steganography/>

Logramos decodificar la imagen obteniendo el siguiente mensaje:

CodeHouse Ciberseguridad

Steganography Online

Encode Decode

Decode image

To decode a hidden message from an image, just choose an image and hit the **Decode** button.

Neither the image nor the message that has been hidden will be at any moment transmitted over the web, all the magic happens within your browser.

Seleccionar archivo desafio entregable.png

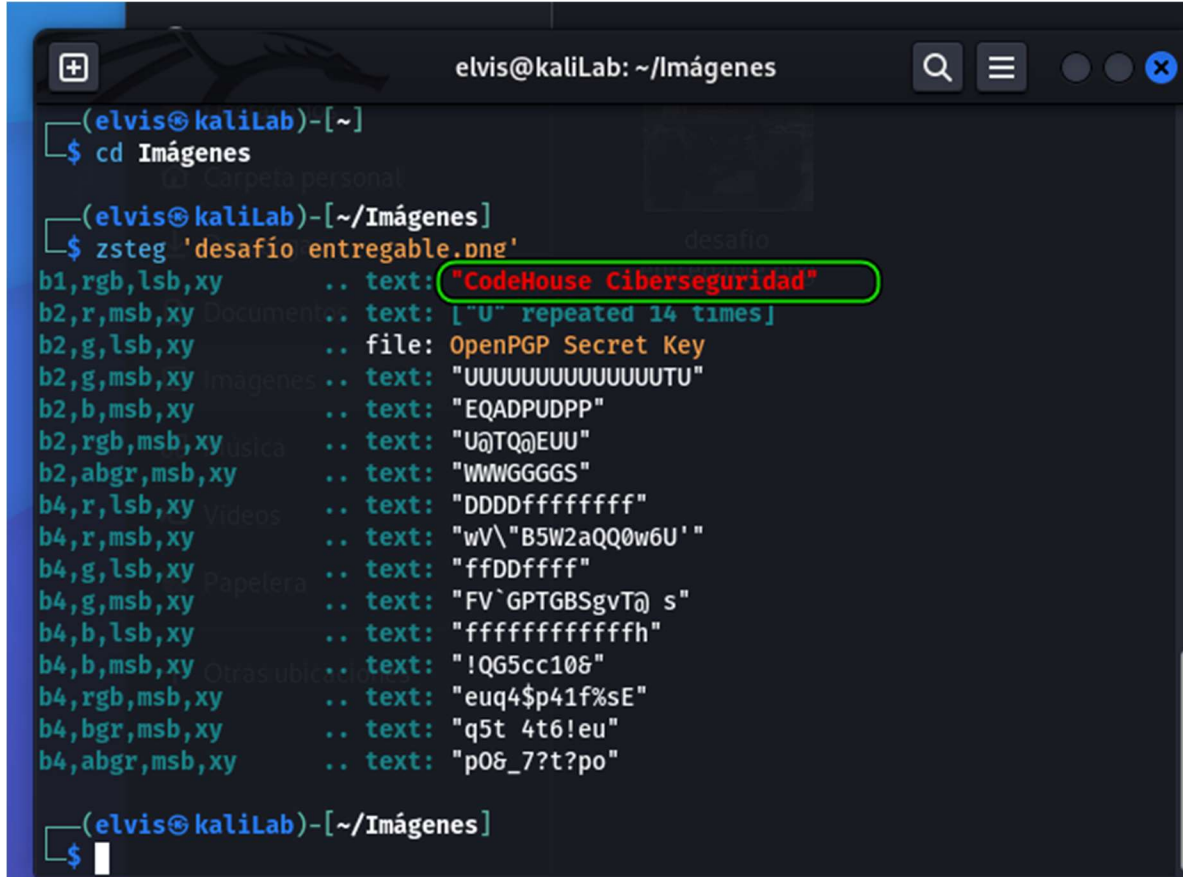
Decode

Hidden message

CodeHouse
Ciberseguridad

Segundo y para complementar la búsqueda, procedimos a utilizar una herramienta para Estenografía llamada ZSteg en Kali Linux.

En dicha herramienta se analizó el archivo, obteniendo el mismo resultado anterior con la herramienta web:

A terminal window titled 'elvis@kaliLab: ~/Imágenes' showing the execution of the 'zsteg' command on a file named 'desafío entregable.png'. The command is '\$ zsteg 'desafío entregable.png''. The output lists various steganographic parameters and their values. The first line of output, 'b1,rgb,lsb,xy .. text: "CodeHouse Ciberseguridad"', is highlighted with a green oval. The terminal background has a dark theme with a blue sidebar on the left showing a file explorer view with folders like 'Carpeta personal', 'Documentos', 'Imágenes', 'Música', 'Videos', 'Papetera', and 'Otras ubicaciones'.

```
(elvis@kaliLab)-[~]  
$ cd Imágenes  
  
(elvis@kaliLab)-[~/Imágenes]  
$ zsteg 'desafío entregable.png'  
b1,rgb,lsb,xy .. text: "CodeHouse Ciberseguridad"  
b2,r,msb,xy .. text: ["U" repeated 14 times]  
b2,g,lsb,xy .. file: OpenPGP Secret Key  
b2,g,msb,xy .. text: "UUUUUUUUUUUUUUUUUU"  
b2,b,msb,xy .. text: "EQADPUDPPP"  
b2,rgb,msb,xy .. text: "U@TQ@EUU"  
b2,abgr,msb,xy .. text: "WWWGGGGS"  
b4,r,lsb,xy .. text: "DDDDffffffff"  
b4,r,msb,xy .. text: "wV\"B5W2aQQ0w6U' "  
b4,g,lsb,xy .. text: "ffDDffff"  
b4,g,msb,xy .. text: "FV`GPTGBSgvT@ s"  
b4,b,lsb,xy .. text: "fffffffffffffh"  
b4,b,msb,xy .. text: "!QG5cc106"  
b4,rgb,msb,xy .. text: "euq4$p41f%sE"  
b4,bgr,msb,xy .. text: "q5t 4t6!eu"  
b4,abgr,msb,xy .. text: "p06_7?t?po"  
  
(elvis@kaliLab)-[~/Imágenes]  
$
```

Conclusión:

Luego de buscar por distintos medios y herramientas, e ir descartando los que no eran adecuados, podemos decir que se pueden encontrar datos ocultos dentro de lo que parece algo poco sospechoso o inofensivo como una imagen. Lo importante es tener en cuenta esto a futuro y así evitar que una red o un equipo particular se vea comprometido. Viendo el lado positivo, también se podría tener en cuenta para el envío de datos o mensajes ocultos para alguien que pueda realizar una decodificación y así poder acceder a esos datos.

Analista de Ciberseguridad: Galvalisi Elvis