Cristina Bautista 161260
Abril Palencia 18198

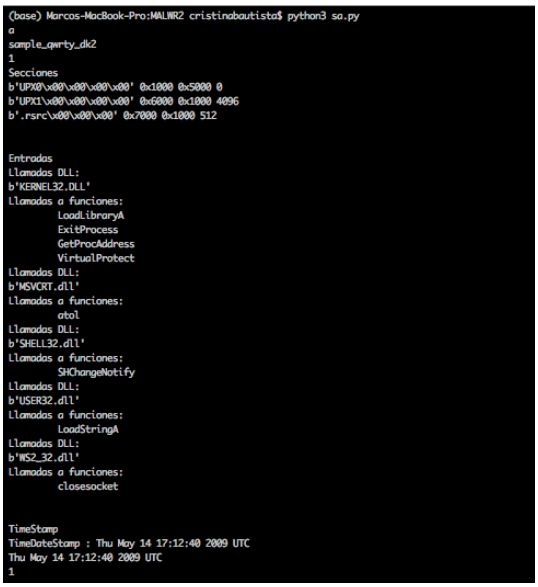
Laboratorio 4

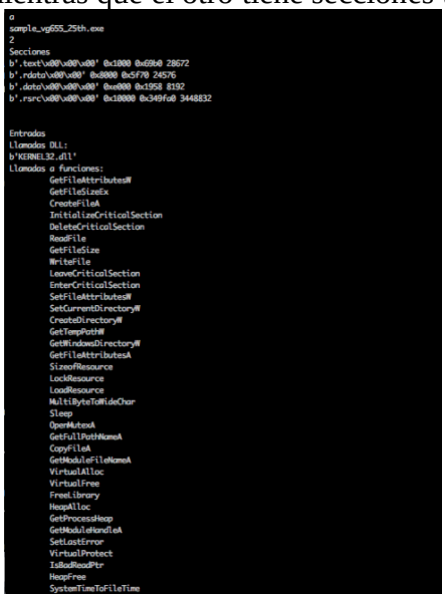
Análisis estático

1. Utilice la herramienta pefile para examinar el PE header y obtenga las DLL y las APIs que los ejecutables llaman. ¿Qué diferencias observa entre los ejemplos? ¿Existe algún indicio sospechoso en la cantidad de DLLs y las APIs llamadas?
   a. Primer ejemplo
   b. KERNEL32.DLL
   c. MSVCRT.dll
   d. SHELL32.dll
   e. USER32.dll
   f. WS2_32.dll
   g. Segundo ejemplo
   h. KERNEL32.dll
   i. USER32.dll
   j. ADVAPI32.dll
   k. MSVCRT.dll

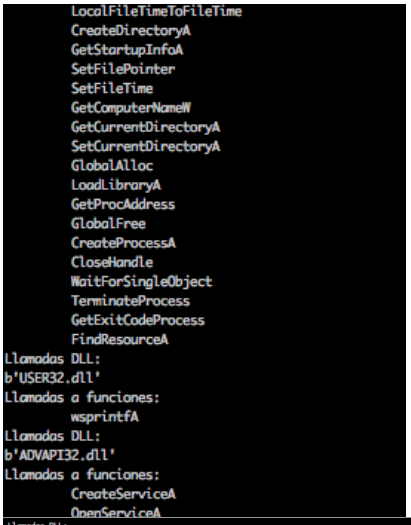
   Tienen en común las siguientes llamadas “kernel32.dll, msvcrt.dll, user32.dll”. El primero permite acceder a funciones del sistema, como iniciar, detener, entre otras. El segundo hace llamadas a las redes, lo que significan que pueden acceder al internet. El último tiene la capacidad de hacer llamadas por el sistema operativo y sus aplicaciones, como botones, acciones del sistema, entre otros.

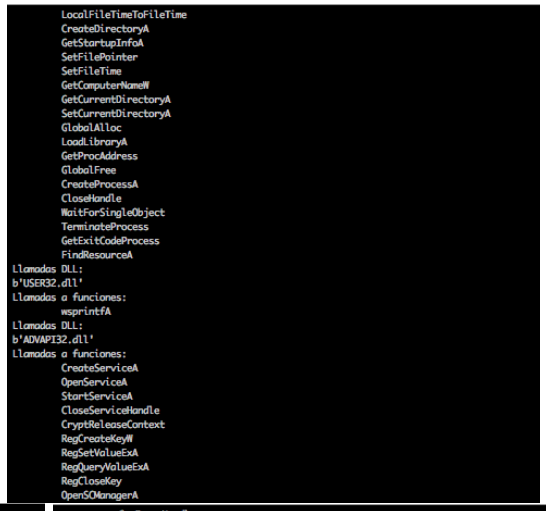
   El primero tiene secciones UPX mientras que el otro tiene secciones txt





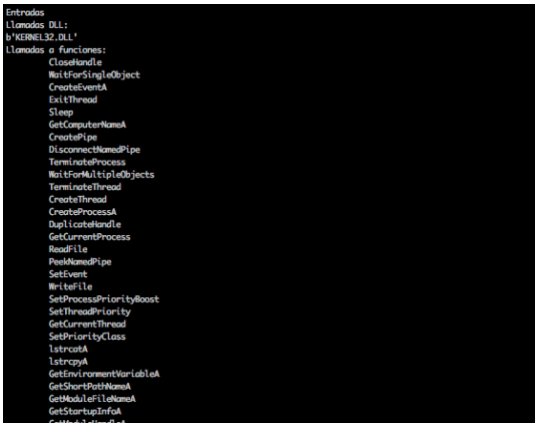
Cristina Bautista 161260
Abril Palencia 18198





2. Obtenga la información de las secciones del PE Header. ¿Qué significa que algunas secciones tengan como parte de su nombre “upx”? Realice el procedimiento de desempaquetado para obtener las llamadas completas de las APIs.
    a. (Ver imágenes anteriores para ver los headers)
    b. Cuando tiene UPX significa que están comprimidas.
    c. El primer archivo tuvo un cambio significativo en la cantidad de funciones.

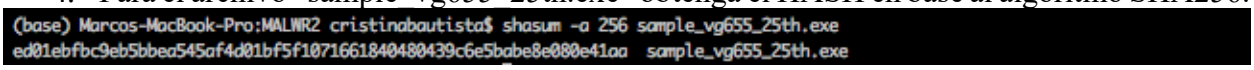
Cristina Bautista 161260
Abril Palencia 18198



3. Según el paper "Towards Understanding Malware Behaviour by the Extraction of API Calls", ¿en que categoría sospechosas pueden clasificarse estos ejemplos en base a algunas de las llamadas a las APIs que realizan? Muestre una tabla con las APIs sospechosas y la categoría de malware que el paper propone.

Behaviour	Malware Category	API function calls
1	Buscar archivos para infectar	
2	Copiar/Eliminar archivos	CloseHandle,
3	Conseguir información de archivos	GetFileSize, GetFileSizeEx,
4	Mover archivos	
5	Leer/Escribir archivos	WriteFile, CloseHandle
6	Cambiar atributos de archivos	

4. Para el archivo "sample_vg655_25th.exe" obtenga el HASH en base al algoritmo SHA256.



ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

5. Para el archivo "sample_vg655_25th.exe", ¿cuál es el propósito de la DLL ADVAPI32.dll?

Es una guía que almacena información e instrucciones para archivos ejecutables. Asignan memoria, para el archivo, hace llamadas de seguridad y de registro.

6. Para el archivo "sample_vg655_25th.exe", ¿cuál es el propósito de la API CryptReleaseContext?

Libera la función del servicio criptográfico del proveedor (CSP) y el contenedor de llaves. No elimina contenedores de llaves.

7. Con la información recopilada hasta el momento, indique para el archivo "sample_vg655_25th.exe" si es sospechoso o no, y cual podría ser su propósito.

Si se sospechoso, puede hacer llamadas de seguridad y de registro en la memoria, puede hacer llamadas a accesos de internet. Puede que mueva archivos, los bloquee con encriptación.

Cristina Bautista 161260
Abril Palencia 18198

Análisis dinámico

8. Utilice la plataforma de análisis dinámico https://www.hybrid-analysis.com y cargue el archivo “sample_vg655_25th.exe”. ¿Se corresponde el HASH de la plataforma con el generado? ¿Cuál es el nombre del malware encontrado? ¿En que consiste este malware?

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa, si corresponde al mismo HASH del inciso 4. El nombre del malware es Wanna Cry, es un ransomware, que consiste en bloquear archivos importantes y pedir dinero o recursos a cambio de la clave para desbloquearlos o solo la acción de desbloquearlos

9. Muestre las capturas de pantalla sobre los mensajes que este malware presenta a usuario. ¿Se corresponden las sospechas con el análisis realizado en el punto 7?

Definitivamente corresponde a las sospechas del punto 7, incluso corresponde con las sospechas de lo que podría pasar si se infecta la computadora.