Guatemala, 09 de marzo de 2023

Hoja de Trabajo 2 - Análisis de Malware

Josue Sagastume 18173

Parte 1 - Análisis estático

1. Utilice la herramienta pefile para examinar el PE header y obtenga las DLL y las APIs que cada uno de los ejecutables utilizan.

```
SECCIONES
        b'UPX0\x00\x00\x00\x00' 0x1000 0x5000 0
        b'UPX1\x00\x00\x00\x00' 0x6000 0x1000 4096
        b'.rsrc\x00\x00\x00' 0x7000 0x1000 512
LLAMADAS A DLL
        b'KERNEL32.DLL'
                LLAMADAS A FUNCIONES
                        b'LoadLibraryA'
                        b'ExitProcess'
                        b'GetProcAddress'
                        b'VirtualProtect'
LLAMADAS A DLL
        b'MSVCRT.dll'
                LLAMADAS A FUNCIONES
                        b'atol'
LLAMADAS A DLL
        b'SHELL32.dll'
                LLAMADAS A FUNCIONES
                        b'SHChangeNotify'
LLAMADAS A DLL
        b'USER32.dll'
                LLAMADAS A FUNCIONES
                        b'LoadStringA'
LLAMADAS A DLL
        b'WS2_32.dll'
                LLAMADAS A FUNCIONES
                        b'closesocket'
TimeDateStamp: Thu May 14 17:12:40 2009 UTC
TimeDateStamp: 0x4a0c5108
```

Imagen 1. DLL y APIs del archivo “sample_qwrty_dk2.exe”.

```
SECCIONES
        b'.text\x00\x00\x00' 0x1000 0x69b0 28672
        b'.rdata\x00\x00' 0x8000 0x5f70 24576
        b'.data\x00\x00\x00' 0xe000 0x1958 8192
        b'.rsrc\x00\x00\x00' 0x10000 0x349fa0 3448832
LLAMADAS A DLL
        b'KERNEL32.dll'
                LLAMADAS A FUNCIONES
                        b'GetFileAttributesW'
                        b'GetFileSizeEx'
                        b'CreateFileA'
                        b'InitializeCriticalSection'
                        b'DeleteCriticalSection'
                        b'ReadFile'
                        b'GetFileSize'
                        b'WriteFile'
                        b'LeaveCriticalSection'
                        b'EnterCriticalSection'
                        b'SetFileAttributesW'
                        b'SetCurrentDirectoryW'
                        b'CreateDirectoryW'
                        b'GetTempPathW'
                        b'GetWindowsDirectoryW'
                        b'GetFileAttributesA'
                        b'SizeofResource'
                        b'LockResource'
                        b'LoadResource'
                        b'MultiByteToWideChar'
                        b'Sleep'
                        b'OpenMutexA'
```

Imagen 2. Algunas DLL y APIs del archivo “sample_vg655_25th.exe”.

¿Qué diferencias observa entre los ejemplos?

La principal diferencia entre ambos archivos es la cantidad de secciones, DLLs y llamadas a APIs, pues el segundo cuenta con muchas más respecto al primero.

¿Existe algún indicio sospechoso en la cantidad de DLLs y las APIs llamadas?
No, basándome en el nombre de las funciones, a primera vista no parece haber nada sospechoso o peligroso.

2. Obtenga la información de las secciones del PE Header. ¿Qué significa que algunas secciones tengan como parte de su nombre "upx"?
   Esto significa que este archivo ha sido empaquetado bajo upx, esta también es la razón por la cual se puede notar una gran diferencia entre la cantidad APIs de ambos archivos.

3. Según el paper "Towards Understanding Malware Behaviour by the Extraction of API Calls", ¿en qué 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.

Archivo	APIs	Categoría de Malware
sample_qwrty_dk2.exe	-CloseHandle	Copy/Delete Files
sample_vg655_25th.exe	-GetFileAttributesW -GetFileSizeEx -GetFileSize -GetTempPathW -GetFileAttributesA -GetFullPathNameA	Get File Information
sample_vg655_25th.exe	-CreateFile -CopyFileA -CloseHandle	Copy/Delete Files
sample_vg655_25th.exe	-WriteFile	Read/Write Files
sample_vg655_25th.exe	-SetFileAttributesW	Change File Attributes

Tabla 1. Categorías en las que podrían clasificarse los archivos según sus APIs.

4. Para el archivo "sample_vg655_25th.exe" obtenga el HASH en base al algoritmo SHA256.
   Hash generado con la librería hashlib de python:
   ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

5. Para el archivo "sample_vg655_25th.exe", ¿cuál es el propósito de la DLL ADVAPI32.dll?
   Esta DLL le da acceso a funcionalidades avanzadas que vienen junto con el kernel.

6. Para el archivo "sample_vg655_25th.exe" ¿cuál es el propósito de la API CryptReleaseContext?
   Esta función libera al manejador de un proveedor de servicios criptográficos y un contenedor de claves. En cada llamada a esta API, el recuento de referencias del CSP se reduce en uno.

Cuento el recuento de referencias llega a cero, el contexto se libera por completo y ya no puede ser utilizado por ninguna función de la aplicación.

7. Con la información recopilada hasta el momento, indique para el archivo "sample_vg655_25th.exe" si es sospechoso o no, y cuál podría ser su propósito.
   Dada la información anterior, este archivo sí parece ser sospechoso y su propósito podría ser obtener la información de archivos y encriptarlo, para que el dueño de dichos archivos ya no pueda acceder a la información que contienen.

Parte 2 - Análisis dinámico

8. Utilice la plataforma de análisis dinámico y cargue el archivo "sample_vg655_25th.exe". ¿Se corresponde el HASH de la plataforma con el generado?
   HASH: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
   Sí, son el mismo HASH.

   ¿Cuál es el nombre del malware encontrado?
   Trojan.Ransom.WannaCryptor.

   ¿Cuál es el propósito de este malware?
   Este identifica el ransomware WannaCry, que encripta el dispositivo afectado y pide el pago de un rescate para restablecer su uso normal.

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

Imagen 3. Mensaje mostrado que el malware Trojan.Ransom.WannaCryptor presenta a los usuarios.

Esto confirma las sospechas del punto 7, pues este malware hace un tipo de extorsión, en el que encripta los archivos del usuario atacado y luego le pide dinero para que le devuelva sus archivos.