# Laboratorio 4

## Parte 1

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?**

| Archivo | Cantidad de DLL's | Cantidad de Llamadas |
|---|---|---|
| sample_vg655_25th.exe | 4 | 114 |
| sample_qwrty_dk2 | 5 | 8 |

Se puede notar que, a pesar de tener menos DLL's, el archivo sample_vg655_25th.exe tiene una cantidad mucho más grande que el otro archivo, esto definitivamente es sospechoso.

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.**

UPX comúnmente se utiliza para reducir el tamaño de los ejecutables, sin embargo, es posible utilizarlo en malwares para esconder información del ejecutable y así no ser identificado.

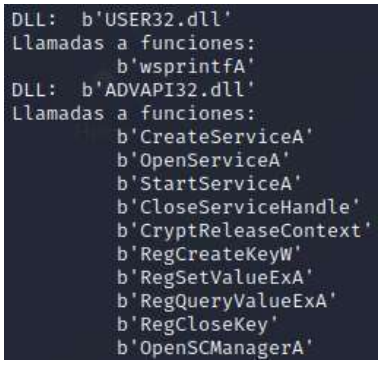
**Secciones:**

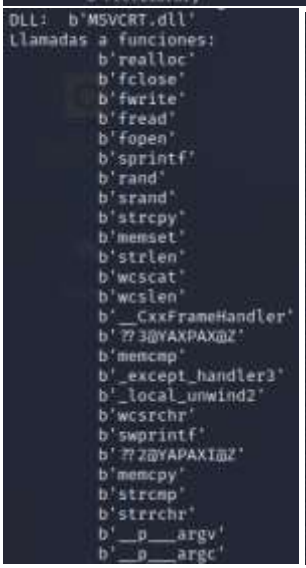
```
Secciones para el archivo sample_vg655_25th.exe:
IMAGE_SECTION_HEADER 0×1000 0×69b0 28672
IMAGE_SECTION_HEADER 0×8000 0×5f70 24576
IMAGE_SECTION_HEADER 0×e000 0×1958 8192
IMAGE_SECTION_HEADER 0×10000 0×349fa0 3448832


Secciones para el archivo sample_qwrty_dk2:
IMAGE_SECTION_HEADER 0×1000 0×5000 0
IMAGE_SECTION_HEADER 0×6000 0×1000 4096
IMAGE_SECTION_HEADER 0×7000 0×1000 512
```

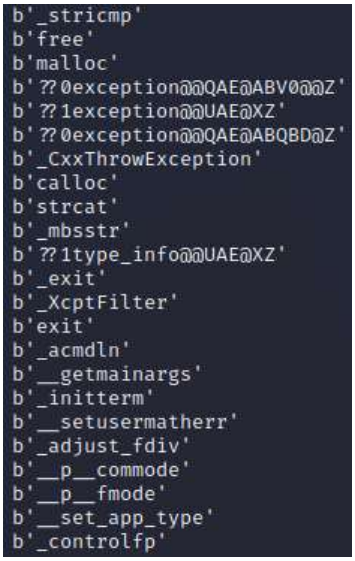
**Llamadas completas:**

sample_vg655_25th.exe:

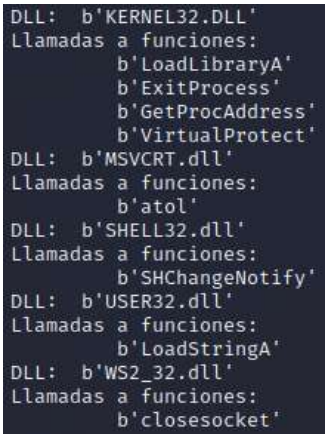





sample_qwrty_dk2:



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.**

Para el archivo sample_vg655_25th.exe se encuentran las siguientes APIs sospechosas:

| API | Categoría |
|---|---|
| b'GetFileAttributesW' | 3 |
| b'GetFileSizeEx' | 3 |
| b'CreateFileA' | 5 |
| b'ReadFile' | 5 |
| b'GetFileSize' | 3 |
| b'WriteFile' | 5 |
| b'SetFileAttributesW' | 6 |
| b'GetTempPathW' | 3 |
| b'GetWindowsDirectoryW' | 3 |
| b'GetFileAttributesA' | 3 |
| b'SizeofResource' | 3 |
| b'GetFullPathNameA' | 3 |
| b'CopyFileA' | 2 |
| b'GetModuleFileNameA' | 3 |
| b'GetProcessHeap' | 3 |
| b'GetModuleHandleA' | 3 |
| b'SetLastError' | 6 |
| b'GetStartupInfoA' | 3 |
| b'SetFilePointer' | 6 |
| b'SetFileTime' | 6 |
| b'GetComputerNameW' | 3 |
| b'GetCurrentDirectoryA' | 3 |
| b'SetCurrentDirectoryA' | 6 |
| b'GetProcAddress' | 3 |
| b'CloseHandle' | 5 |
| b'FindResourceA' | 1 |

Para el archivo sample_qwrty_dk2 se encuentran las siguientes APIs sospechosas:

| API | Categoría |
|---|---|
| b'GetProcAddress' | 3 |

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

```
Hash SHA256 para el archivo sample_vg655_25th.exe:
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
```

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

   Proporciona acceso a las funcionalidades avanzadas del kernel. Es responsable de cosas como el registro de Windows, reiniciar y apagar el sistema, iniciar/detener y crear servicios de Windows y administrar cuentas de usuario.

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

   La función CryptReleaseContext libera el identificador de un proveedor de servicios criptográficos (CSP) y un contenedor 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 es sospechoso. Es posible que su propósito sea detener servicios de Windows hasta dejar inusable el sistema. También es posible que encripte archivos del equipo para que el usuario ya no pueda acceder a ellos.

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 qué consiste este malware?**


El hash obtenido si coincide.
El nombre del malware es owo_im_not_ramsomware_xd.exe
Este malware consiste en encriptar los archivos del equipo para que no puedan ser utilizados y pide compensación económica a través de bitcoin para poder desencriptar los archivos.

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?**



Si se confirma que el archivo es malicioso y se utiliza para encriptar archivos del usuario.