

# Análisis de Malware

La primera parte consiste en el análisis de dos ejecutables de Windows proporcionados. Se proporciona una carpeta con el nombre MALWR2.zip en CANVAS, la cual posee la contraseña *infected*. Se sugiere utilizar una VM con Linux para trabajar. Se debe descargar el archivo y descomprimirlo en la ubicación deseada. Luego se debe descomprimirlo y NO se debe manipular manualmente ningún archivo, de hacerlo se corre el riesgo de ejecutarlo e infectarse.

NOTA: se proporcionan ejemplos reales de malware, para efectos de aplicar los conocimientos académicos de análisis estático y dinámico de malware, y es responsabilidad del alumno(a) cualquier uso adicional que no sea el indicado en este laboratorio. Luego de finalizar el laboratorio se deben eliminar todos los ejemplares.

## 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. ¿Qué diferencias observa entre los ejemplos? ¿Existe algún indicio sospechoso en la cantidad de DLLs y las APIs llamadas?
  - a Al observar el archivo se encontré los siguientes DLLs
    - i Kernel32.dll
    - ii User32.dll
    - iii ADVAPI32.dll
    - iv MSVCRT.dll
  - 1 Todos contenían llamadas raras, tales como GetComputerName, GetCurrentDirectory, copy memory, entre otras, dando a entender que el primer paso del virus es comprender donde esta para así lograr moverse por otros directorios.
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 Que tenga el termino UPX significa que las secciones se encuentran empaquetadas.
  - b Al desempaquetar se obtiene las siguientes secciones:

```
Sections:
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
```

c Con las siguientes llamadas a sistema

```
b'KERNEL32.dll'
0x40802c b'GetFileAttributesW'
0x408030 b'GetFileSizeEx'
0x408034 b'CreateFileA'
0x408038 b'InitializeCriticalSection'
0x40803c b'DeleteCriticalSection'
0x408040 b'ReadFile'
0x408044 b'GetFileSize'
0x408048 b'WriteFile'
0x40804c b'LeaveCriticalSection'
0x408050 b'EnterCriticalSection'
0x408054 b'SetFileAttributesW'
0x408058 b'SetCurrentDirectoryW'
0x40805c b'CreateDirectoryW'
0x408060 b'GetTempPathW'
0x408064 b'GetWindowsDirectoryW'
0x408068 b'GetFileAttributesA'
0x40806c b'SizeofResource'
0x408070 b'LockResource'
0x408074 b'LoadResource'
0x408078 b'MultiByteToWideChar'
0x40807c b'Sleep'
0x408080 b'OpenMutexA'
0x408084 b'GetFullPathNameA'
0x408088 b'CopyFileA'
0x40808c b'GetModuleFileNameA'
```

- d
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.

API Maliciosa	Categoria
GetFileAttributes	Get file information
GetFileSize	Get file information
CreateFile	Copy/Delete Files
SetFileAttributes	Change file attributes
CreateFile	Read/Write files
GetFileAttributes	Get File information

4. Para el archivo “sample\_vg655\_25th.exe” obtenga el HASH en base al algoritmo SHA256.

SHA256 ES :

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

- a
5. Para el archivo “sample\_vg655\_25th.exe”, ¿cuál es el propósito de la DLL ADVAPI32.dll?
- a Su propósito es administrar los APIS del sistema, incluyendo a las llamadas de seguridad y registro., sin embargo, esta api en el programa esta programada para que realice lo siguiente:




```
ADVAPI32.dll.CreateServiceA Hint[100]
ADVAPI32.dll.OpenServiceA Hint[431]
ADVAPI32.dll.StartServiceA Hint[585]
ADVAPI32.dll.CloseServiceHandle Hint[62]
ADVAPI32.dll.CryptReleaseContext Hint[160]
ADVAPI32.dll.RegCreateKeyW Hint[467]
ADVAPI32.dll.RegSetValueExA Hint[516]
ADVAPI32.dll.RegQueryValueExA Hint[503]
ADVAPI32.dll.RegCloseKey Hint[459]
ADVAPI32.dll.OpenSCManagerA Hint[429]
```

6. Para el archivo “sample\_vg655\_25th.exe”, ¿cuál es el propósito de la API CryptReleaseContext?
- a Esta función permite bloquear las siguientes llamadas o bloques de contenido.
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.

En base a lo investigado este virus puede ser considerado un ransomware de cifrado, debido que lo primero que hace es crear un servicio, lo abre, lo inicializa y de ahí lograr bloquear un segmento, impidiendo al usuario acceder a dicho contenido bloqueado.

## Parte 2 – 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? ¿Cuál es el propósito de este malware?
- a Si el hash obtenido es el mismo obtenido por el código

Submission name:	owo_im_not_ransomware_xd.exe 
Size:	3.4MiB
Type:	<span>peexe</span> <span>executable</span> 
Mime:	application/x-dosexec
SHA256:	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Operating System:	Windows 
Last Anti-Virus Scan:	03/07/2023 22:17:29 (UTC)
Last Sandbox Report:	03/10/2023 00:22:48 (UTC)

i

- b El nombre de este virus es RansomwareWannaCry
- c Y básicamente es un ransomware que busca bloquear ciertas secciones de la PC
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 cumplió con lo dicho en el inciso 7, el cual solo buscan encriptar datos como otro ransomware.