

Hoja de Trabajo 2

Andrea Amaya 19357

Parte 1.

a. DLL y APIs

sample_qwrty_dk2

```
(kali㉿kali)-[~/Desktop/MALWR]
$ python parte1.py
[*] Listing imported DLLs ...
    KERNEL32.DLL
    MSVCRT.dll
    SHELL32.dll
    USER32.dll
    WS2_32.dll

(kali㉿kali)-[~/Desktop/MALWR]
$ python apis.py
[*] Listing APIs ...
    b'LoadLibraryA'
    b'ExitProcess'
    b'GetProcAddress'
    b'VirtualProtect'
    b'atol'
    b'SHChangeNotify'
    b'LoadStringA'
    b'closesocket'
```

sample_vg655_25th.exe

```
(kali㉿kali)-[~/Desktop/MALWR]
$ python parte1.py
[*] Listing imported DLLs ...
    KERNEL32.dll
    USER32.dll
    ADVAPI32.dll
    MSVCRT.dll
```

```
(kali㉿kali)-[~/Desktop/MALWR]
$ python apis.py
[*] Listing APIs ...
    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'
    b'GetFullPathNameA'
    b'CopyFileA'
    b'GetModuleFileNameA'
    b'VirtualAlloc'
    b'VirtualFree'
    b'FreeLibrary'
    b'HeapAlloc'
    b'GetProcessHeap'
    b'GetModuleHandleA'
    b'SetLastError'
    b'VirtualProtect'
    b'IsBadReadPtr'
    b'HeapFree'
    b'SystemTimeToFileTime'
    b'LocalFileTimeToFileTime'
    b'CreateDirectoryA'
    b'GetStartupInfoA'
    b'SetFilePointer'
    b'SetFileTime'
    b'GetComputerNameW'
    b'GetCurrentDirectoryA'
    b'SetCurrentDirectoryA'
    b'GlobalAlloc'
    b'realloc'
    b'fclose'
    b'fwrite'
    b'fread'
    b'fopen'
    b'sprintf'
    b'rand'
    b'srand'
    b'strcpy'
    b'memset'
    b'strlen'
    b'wscat'
    b'wcslen'
    b'__CxxFrameHandler'
    b'??3?YAPAX@Z'
    b'memcmp'
    b'__except_handler3'
    b'__local_unwind2'
    b'wcsrchr'
    b'wcsrchr'
    b'swprintf'
    b'??2?YAPAXI@Z'
    b'memcpy'
    b'strcmp'
    b'strchr'
    b'__p_argv'
    b'__p_argc'
    b'stricmp'
    b'free'
    b'malloc'
    b'??0exception@@QAE@ABV0@@Z'
    b'??1exception@@QAE@Z'
    b'??0exception@@QAE@ABQBD@@Z'
    b'__CxxThrowException'
    b'calloc'
    b'strcat'
    b'__mbstr'
    b'??1type_info@@QAE@KZ'
    b'_exit'
    b'__xcpFilter'
    b'_acmdln'
    b'__getmainargs'
    b'__initterm'
    b'__setusermatherr'
    b'_adjust_fdiv'
    b'__p_commode'
    b'__p_fmode'
    b'__set_app_type'
    b'__controlfp'
```

¿Qué diferencias observa entre los ejemplos? ¿Existe algún indicio sospechoso en la cantidad de DLLs y las APIs llamadas? Al comparar los DLL entre ambos archivos, el único sospechoso es el WS2_32.dll el cual es un archivo ejecutable en el disco duro del ordenador. Ahora al comprar las llamadas API, el .exe contiene muchas más que el otro archivo. Y, al revisar el listado, en el .exe se encuentran nombres sospechosos como “??1type_info@@UAE@XZ” u otros que no son legibles para un humano. Al revisar los nombres de las llamadas, el primer archivo también cuenta con algunos nombres dudosos como “LoadStringA” el cual probablemente intente modificar alguno de los archivos de inicio del Windows al tener el dll WS2_32.

b. ¿Qué significa que algunas secciones tengan como parte de su nombre “upx”?

Upx es un compresor de archivos, lo cual hace que se salten los pasos de seguridad (antivirus) al estar comprimidos y no el archivo completo.

c. 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.

Nombre	Categoría
ReadFile, WriteFile, CreateDirectory	Read/Write Files
DeleteCriticalSection	Copy/Delete Files
GetFileAttributesW, GetFileSize	Search files to infect

d. Para el archivo “sample_vg655_25th.exe” obtenga el HASH en base al algoritmo SHA256.

```
(kali@kali)~[~/Desktop/MALWR]
$ sha256sum sample_vg655_25th.exe
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa sample_vg
```

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

ADVAPI32 hace referencia a los archivos esenciales del sistema operativo. Además, incluye APIs de llamadas de seguridad y registros. Cuando Advapi32.dll se corrompe o falta, empieza a provocar que el sistema informático se des controle.

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

Es la función encargada de liberar identificadores de proveedores de servicios criptográficos (CSP) y un contenedor de claves. Luego de esta función, el CSP y los objetos hash existentes ya no son válidos.

- g. 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.

Sí es sospechoso, el posible propósito es que encripte la información del usuario de forma aleatoria hasta terminar todos los archivos y que ya no se pueda acceder a la máquina. Esto se debe a que los hash son invalidados al volver a llamar la función.

Parte 2.

- a. ¿Se corresponde el HASH de la plataforma con el generado? ¿Cuál es el nombre del malware encontrado? ¿Cuál es el propósito de este malware?

Sí corresponde el hash de la plataforma con el generado. El nombre del malware es `owo_im_not_ransomware_xd.exe`. El propósito del malware es obtener las llaves del sistema y eliminar grandes volúmenes de datos.

Analysis Overview

Submission name:	owo_im_not_ransomware_xd.exe ⓘ
Size:	3.4MiB
Type:	peexe executable ⓘ
Mime:	application/x-dosexec
SHA256:	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa ⓘ
Operating System:	Windows ⚑
Last Anti-Virus Scan:	02/15/2023 11:04:30 (UTC)
Last Sandbox Report:	12/19/2022 08:54:11 (UTC)

Related Hashes

Related files		
Name	Sha256	Verdict
Ransomware.WannaCry.zip	707a9f323556179571bc832e34fa592066b1d5f2cac4a7426fe163597e3e618a	malicious
Ransomevaare exe.zip	7c42f6f0696c1b6954c3aea6136c8e25b2f179922a143984254f00561d53e784	malicious
Ransomware.WannaCry.zip	61a5eed5d3cf4cf0924bac118acf3deffd2ab3a8fc67024f3c35fcc2061e6511	malicious
Ransomware.WannaCry.zip.zip	c1aeafa14591bbc30cf385e69e13e71438e0c963b3b0de72ede00c7131194478	malicious
Ransomware.WannaCry.zip.zip	3eadbb62d7b951ebb98effa2e7f617e14bf8b47b0cf20fc43bec272475913d44	malicious

**b. 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?**

Según los mensajes obtenidos, el malware intenta cambiar archivos, inyección de procesos, cambia archivos de seguridad y genera una gran cantidad de procesos. Corresponde en ciertas partes, porque sí menciona que logra deshabilitar la reparación del dispositivo por medio del startup y que puede acceder a toda la información incluso por navegador web.

Malicious Indicators		13
Anti-Detection/Stealthiness		
Attempts to change the attributes of the files		▼
Creates a process in suspended mode (likely for process injection)		▼
External Systems		
Sample detected by CrowdStrike Static Analysis and ML with relatively high confidence		▼
Sample was identified as malicious by a large number of Antivirus engines		▼
Sample was identified as malicious by a trusted Antivirus engine		▼
General		
The analysis extracted a file that was identified as malicious		▼
The analysis spawned a process that was identified as malicious		▼
Installation/Persistence		
Allocates virtual memory in a remote process		▼
Pattern Matching		
YARA signature match		▼
Spyware/Information Retrieval		
Contains ability to capture the screen		▼
System Security		
Modifies the access control lists of files		▼
Unusual Characteristics		
Spawns a lot of processes		▼
Suspicious Indicators		50
Anti-Detection/Stealthiness		
Contains ability to open/control a service		▼
Queries process information		▼
Anti-Reverse Engineering		
PE file has unusual entropy sections		▼

An application crash occurred	▼
Calls an API typically used to copy file from one location to another	▼
Calls an API typically used to create a directory	▼
Calls an API typically used to create a process	▼
Contains ability to delay the execution of current thread	▼
Contains ability to dynamically load libraries	▼
Contains registry location strings	▼
Creates mutants	▼
Drops or executes a batch file	▼
Found API related strings	▼
Launches a VBS file	▼
Logged script engine calls	▼
Overview of unique CLSIDs touched in registry	▼
PE file contains executable sections	▼
PE file contains writable sections	▼

👁 Risk Assessment	
Remote Access	Reads terminal service related keys (often RDP related)
Spyware	Accesses potentially sensitive information from local browsers Contains ability to open the clipboard Deletes volume snapshots (often used by ransomware) Hooks API calls
Persistence	Disables startup repair Grants permissions using icacls (DACL modification) Installs hooks/patches the running process Spawns a lot of processes Tries to suppress failures during boot (often used to hide system changes) Writes data to a remote process
Fingerprint	Queries kernel debugger information Queries process information Reads system information using Windows Management Instrumentation Commandline (WMIC) Reads the active computer name Reads the cryptographic machine GUID Reads the windows installation language
Evasive	Contains ability to detect virtual environment (API) Input file contains API references not part of its Import Address Table (IAT) Marks file for deletion Possibly checks for the presence of an Antivirus engine
Ransomware	Deletes volume snapshots (often used by ransomware) Detected indicator that file is ransomware
Network Behavior	Contacts 48 hosts. 🔍 View all details