

LABORATORIO #4

Ricardo Valenzuela 18762 – Sara Zavala 18893

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?

```

./LAB04/MALWIR2
> sudo python3 sa.py
[sudo] password for sarita:

Seccion
b'UPX0\x00\x00\x00' 0x1000 0x5000 0

Seccion
b'UPX1\x00\x00\x00\x00' 0x6000 0x1000 4096

Seccion
b'.rsrc\x00\x00\x00' 0x7000 0x1000 512
Llamadas DLL:
b'KERNEL32.DLL'
Llamadas a funciones:
b'LoadLibraryA'
b'ExitProcess'
b'GetProcAddress'
b'VirtualProtect'
Llamadas DLL:
b'MSVCRT.dll'
Llamadas a funciones:
b'atoi'
Llamadas DLL:
b'SHELL32.dll'
Llamadas a funciones:
b'SHChangeNotify'
Llamadas DLL:
b'USER32.dll'
Llamadas a funciones:
b'LoadStringA'
Llamadas DLL:
b'WS2_32.dll'
Llamadas a funciones:
b'closesocket'

```

```

./LAB04/MALWIR2
b'GetProcAddress'
b'VirtualProtect'
Llamadas DLL:
b'MSVCRT.dll'
Llamadas a funciones:
b'atoi'
Llamadas DLL:
b'SHELL32.dll'
Llamadas a funciones:
b'SHChangeNotify'
Llamadas DLL:
b'USER32.dll'
Llamadas a funciones:
b'LoadStringA'
Llamadas DLL:
b'WS2_32.dll'
Llamadas a funciones:
b'closesocket'

Header
[IMAGE_FILE_HEADER]
0xE4 0x0 Machine: 0x14C
0xE6 0x2 NumberOfSections: 0x3
0xE8 0x4 TimeDateStamp: 0x4A0C5108 [Thu May 14 17:12:40 2009 UTC]
0xEC 0x8 PointerToSymbolTable: 0x0
0xF0 0xC NumberOfSymbols: 0x0
0xF4 0x10 SizeOfOptionalHeader: 0xE0
0xF6 0x12 Characteristics: 0x10F

Hash
ce22997469ed4607411c0a87f410ba5ae2d566cdaeb516d7a757d51f87e8b060

Seccion
b'.text\x00\x00\x00' 0x1000 0x69b0 28672

```

```

Header
[IMAGE_FILE_HEADER]
0xE4 0x0 Machine: 0x14C
0xE6 0x2 NumberOfSections: 0x3
0xE8 0x4 TimeDateStamp: 0x4A0C5108 [Thu May 14 17:12:40, 2009 UTC]
0xEC 0x8 PointerToSymbolTable: 0x0
0xF0 0xC NumberOfSymbols: 0x0
0xF4 0x10 SizeOfOptionalHeader: 0xE0
0xF6 0x12 Characteristics: 0x10F

Hash
ce22997469ed4607411c0a87f410ba5ae2d566cdaeb516d7a757d51f87e0b060

Section
b'.text\x00\x00\x00' 0x1000 0x69b0 28672

Section
b'.rdata\x00\x00' 0x8000 0x5f70 24576

Section
b'.data\x00\x00\x00' 0xe000 0x1958 8192

Section
b'.rsrc\x00\x00\x00' 0x10000 0x349fa0 3448832
Llamadas DLL:
b'KERNEL32.dll'
Llamadas a funciones:
b'GetFileAttributesW'
b'GetFileSizeEx'
b'CreateFileA'
b'InitializeCriticalSection'
b'DeleteCriticalSection'
b'ReadFile'

```

```

b'.data\x00\x00\x00' 0xe000 0x1958 8192

Section
b'.rsrc\x00\x00\x00' 0x10000 0x349fa0 3448832
Llamadas 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'
b'GetFullPathNameA'
b'CopyFileA'
b'GetModuleFileNameA'
b'VirtualAlloc'
b'VirtualFree'

```

```

b'GetStartupInfoA'
b'SetFilePointer'
b'SetFileTime'
b'GetComputerNameW'
b'GetCurrentDirectoryA'
b'SetCurrentDirectoryA'
b'GlobalAlloc'
b'LoadLibraryA'
b'GetProcAddress'
b'GlobalFree'
b'CreateProcessA'
b'CloseHandle'
b'WaitForSingleObject'
b'TerminateProcess'
b'GetExitCodeProcess'
b'FindResourceA'
Llamadas DLL:
b'USER32.dll'
Llamadas a funciones:
b'wsprintfA'
Llamadas DLL:
b'ADVAPI32.dll'
Llamadas a funciones:
b'CreateServiceA'
b'OpenServiceA'
b'StartServiceA'
b'CloseServiceHandle'
b'CryptReleaseContext'
b'RegCreateKeyW'
b'RegSetValueExA'
b'RegQueryValueExA'
b'RegCloseKey'
b'OpenSCManagerA'
Llamadas DLL:

```

```

b'RegQueryValueExA'
b'RegCloseKey'
b'OpenSCManagerA'
Llamadas DLL:
b'MSVCRT.dll'
Llamadas a funciones:
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'773@YAPAX@Z'
b'memcmp'
b'_except_handler3'
b'_local_unwind2'
b'wcsrchr'
b'swprintf'
b'772@YAPAXI@Z'
b'memcpy'
b'strcmp'
b'strchr'
b'__p__argv'
b'__p__argc'
b'_stricmp'
b'free'

```

```

b'calloc'
b'strcat'
b'_mbsstr'
b'??iotype_info@UAE@XZ'
b'_exit'
b'_XcptFilter'
b'_exit'
b'_acmdln'
b'__getmainargs'
b'_initterm'
b'_setusermatherr'
b'_adjust_fdiv'
b'__p__commode'
b'__p__fmode'
b'__set_app_type'
b'__controlfp'

Header
[IMAGE_FILE_HEADER]
0xFC 0x0 Machine: 0x14C
0xFE 0x2 NumberOfSections: 0x4
0x100 0x4 TimeDateStamp: 0x4CE78F41 [Sat Nov 20 09:05:05 2010 UTC]
0x104 0x8 PointerToSymbolTable: 0x0
0x108 0xC NumberOfSymbols: 0x0
0x10C 0x10 SizeOfOptionalHeader: 0xE0
0x10E 0x12 Characteristics: 0x10F

Hash
6caeca67b7c6a82989f4e7cefb5312a13e59151ae84f3ba6964c70e799729bac

```

- Podemos observar que tenemos distintos tipos de llamadas, por ejemplo, se llama a User32, el cual es encargado de las acciones que el usuario realiza, también se llama a WS2_32 lo cual nos permite observar las conexiones con las que se cuentan.
- La diferencia primordial entre los archivos previamente manejados es que el archivo sample_qwrty_dk2 tiene secciones que están empaquetadas en extensión UPX, mientras que el archivo sample_vg655_25th.exe tiene secciones empaquetadas en extensión .txt.
- Entre otras diferencias, la lista de llamadas del segundo archivo (sample_vg655_25th.exe) tiene una cantidad mas grande de llamadas en comparación al primer archivo.

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.

```
Header
[IMAGE_FILE_HEADER]
0xFC      0x0    Machine:                0x14C
0xFE      0x2    NumberOfSections:          0x4
0x100     0x4    TimeDateStamp:             0x4CE78F41 [Sat Nov 20 09:05:05 2010 UTC]
0x104     0x8    PointerToSymbolTable:      0x0
0x108     0xC    NumberOfSymbols:           0x0
0x10C     0x10   SizeOfOptionalHeader:      0xE0
0x10E     0x12   Characteristics:          0x10F
```

```
Header
[IMAGE_FILE_HEADER]
0xE4      0x0    Machine:                0x14C
0xE6      0x2    NumberOfSections:          0x4
0xE8      0x4    TimeDateStamp:             0x4A0C5108 [Thu May 14 17:12:40 2009 UTC]
0xEC      0x8    PointerToSymbolTable:      0x0
0xF0      0xC    NumberOfSymbols:           0x0
0xF4      0x10   SizeOfOptionalHeader:      0xE0
0xF6      0x12   Characteristics:          0x10F
```

```
> upx-ucl -d sample_qwrty_dk2 sample_vg655_25th.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2018
UPX 3.95      Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

  File size      Ratio      Format      Name
  -----
    8192 <-      5632      68.75%     win32/pe     sample_qwrty_dk2
upx-ucl: sample_vg655_25th.exe: NotPackedException: not packed by UPX

Unpacked 1 file.
```

- a. UPX → Secciones comprimidas inversamente, esto permite que el archivo no sea tomado por el sistema como sospechoso
- b. UPX es un empaquetador ejecutable gratuito, portátil, extensible y de alto rendimiento para varios formatos ejecutables.
- c. UPX logra una excelente relación de compresión y ofrece una descompresión muy rápida. Sus ejecutables no sufren sobrecarga de memoria ni otros inconvenientes para la mayoría de los formatos admitidos, debido a la descompresión en el lugar.

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

Comportamiento	Malware	API Calls
1	Buscar archivos a infectar	FindClose
2	Copiar archivos eliminados	CloseHandle
3	Obtener información de archivo	GetModuleFileName GetPathName
4	Mover Archivos	MoveFileEx
5	Leer/Escribir Archivos	ReadFile, WriteFile
6	Cambiar atributos de archivos	SetFileApis

Y las que el libro propone son las siguientes:

TABLE 1
MAIN MALICIOUS BEHAVIOUR GROUPS OF API CALL FEATURES

Behaviour	Malware Category	API Function Calls
Behaviour 1	Search Files to Infect	FindClose, FindFirstFile, FindFirstFileEx, FindFirstFileName, TransactedW, FindFirstFileNameW, FindFirstFileTransacted, FindFirstStream, TransactedW, FindFirstStreamW, FindNextFile, FindNextFileNameW, FindNextStreamW, SearchPath.
Behaviour 2	Copy/Delete Files	CloseHandle, CopyFile, CopyFileEx, CopyFileTransacted, CreateFile, CreateFileTransacted, CreateHardLink, CreateHardLink, Transacted, CreateSymbolicLink, CreateSymbolic, LinkTransacted, DeleteFile, DeleteFileTransacted.
Behaviour 3	Get File Information	GetBinaryType, GetCompressed, FileSize, GetCompressedFile, SizeTransacted, GetFileAttributes, GetFileAttributesEx, GetFileAttributes, Transacted, GetFileBandwidth, Reservation, GetFileInformation, ByHandle, GetFileInformation, ByHandleEx, GetFileSize, GetFileSizeEx, GetFileType, GetFinalPathName, ByHandle, GetFullPathName, GetFullPathName, Transacted, GetLongPathName, GetLongPathName, Transacted, GetShortPathName, GetTempFileName, GetTempPath.
Behaviour 4	Move Files	MoveFile, MoveFileEx, MoveFileTransacted, MoveFileWithProgress.
Behaviour 5	Read/Write Files	OpenFile, OpenFileByid, ReOpenFile, ReplaceFile, WriteFile, CreateFile, CloseHandle.
Behaviour 6	Change File Attributes	SetFileApisToANSI, SetFileApisToOEM, SetFileAttributes, SetFileAttributesTransacted, SetFileBandwidthReservation, SetFileInformationByHandle, SetFileShortName, SetFileValidData

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

```
Header
[IMAGE_FILE_HEADER]
0xFC 0x0 Machine: 0x14C
0xFE 0x2 NumberOfSections: 0x4
0x100 0x4 TimeDateStamp: 0x4CE78F41 [Sat Nov 20 09:05:05 2010 UTC]
0x104 0x8 PointerToSymbolTable: 0x0
0x108 0xC NumberOfSymbols: 0x0
0x10C 0x10 SizeOfOptionalHeader: 0xE0
0x10E 0x12 Characteristics: 0x10F

Hash
6caeca67b7c6a82989f4e7cefb5312a13e59151ae84f3ba6964c70e799729bac
```

5. Para el archivo “sample_vg655_25th.exe”, ¿cuál es el propósito de la DLL ADVAPI32.dll?
 - a. ADVAPI32 → biblioteca que se con ayuda de numeras APIs ayuda al funcionamiento diario del sistema. Tiene como objetivo manejar la administración de tareas, registro y manipulación de servicios.
 - b. ADVAPI32.dll → Proceso indispensable para el funcionamiento del sistema. Permite que las tareas pendientes se realicen correctamente sin pasar por una cola de espera larga.
 - c. Existen programas que se disfrazan de este proceso, esto ocurre principalmente cuando no lo podemos encontrar en la carpeta System32
6. Para el archivo “sample_vg655_25th.exe”, ¿cuál es el propósito de la API CryptReleaseContext?
 - a. CryptReleaseContext → Da a conocer el identificador de un proveedor de servicios criptográficos
 - b. Este también almacena claves
 - c. El recuento de referencias a esta función se reduce uno, cada vez que se manda a llamar
 - d. El recuento se vuelve inútil para toda función cuando este llega a ser igual a cero
 - e. Al terminar de utilizar CSP, el identificador se libera y este se vuelve invalido para futuros usos.
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.
 - a. Si es sospechoso. Esto se debe a que tiene bastantes privilegios, como lo son lee y escribir dentro del sistema. Posiblemente el propósito sea mover archivos importantes, o también tomar control y reescribir fólder de alto valor. De esta manera podría infectar todo el sistema.

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?

Como podemos ver en la screen anterior, según el análisis, los hashes no corresponden.

Nombre de Malware → WannaCry

WannaCry es un ejemplo de ransomware de cifrado, un tipo de software malicioso (malware) que los cibercriminales utilizan a fin de extorsionar a un usuario para que pague. El ransomware ataca cifrando archivos valiosos para que no puedas acceder a ellos, o bien bloqueando tu acceso al ordenador para que no puedas utilizarlo.

El ransomware que utiliza cifrado se llama ransomware de cifrado. El tipo que bloquea tu acceso al ordenador se llama ransomware de bloqueo. Al igual que otros tipos de ransomware de cifrado, WannaCry secuestra tus datos con la promesa de devolverlos si pagas un rescate. WannaCry tiene como objetivo los ordenadores que utilizan Microsoft Windows como sistema operativo. Cifra los datos y exige el pago de un rescate en la criptomoneda bitcoin por su devolución.

Analysis Environments

Name sample_vg655_25th.exe
Size 3.4MiB
Type **peexe** **executable** ⓘ
MIME application/x-dosexec
SHA256 ed01ebfbc9eb5b...abe8e080e41aa 📄

Available:

- ☐ Windows 7 32 bit
- ☐ Windows 7 32 bit (HWP Support) ⓘ
- ☐ Windows 7 64 bit
- ☒ Linux (Ubuntu 16.04, 64 bit)
- ☐ Android Static Analysis ⓘ
- ☐ Quick Scan ⓘ

Analysis Overview

Request Report Deletion

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: 03/24/2022 15:35:06 (UTC)
Last Sandbox Report: 06/28/2021 15:07:21 (UTC)

malicious

Threat Score: 100/100

AV Detection: 95%

Labeled as: Trojan.Generic

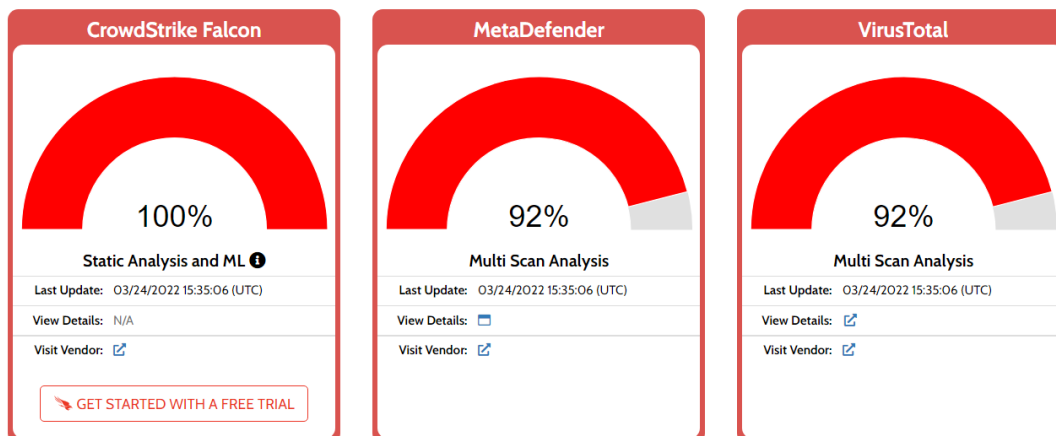
#tag #wannacry #Worm
#ransomware #wannacrypt0r #wcry
#gozi #isfb #papas #ursnif
Link Twitter E-Mail

Anti-Virus Results

Refresh

Anti-Virus Results

Refresh







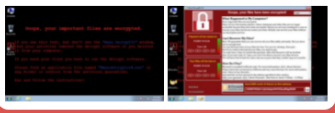

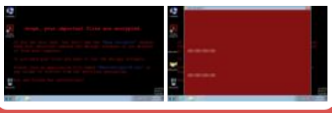





Related Hashes

Related files


Name	Sha256	Verdict
wanna707a9f323556179571bc832e34fa592066b1d5f2cac4a7426fe163597e3e618a.bin	59a3230782c6d74bcb8ff8bd4101db211f0f9ace82aa2af054915e4133b21cb2	malicious ⓘ
Ransomware.WannaCry.zip	707a9f323556179571bc832e34fa592066b1d5f2cac4a7426fe163597e3e618a	malicious
Ransomewaare.exe.zip	7c42f6f0696c1b6954c3aea6136c8e25b2f179922a143984254f00561d53e784	malicious
Ransomware.WannaCry.zip	61a5eed5d3cf4cf0924bac118acf3deffd2ab3a8fc67024f3c35fcc2061e6511	malicious
Ransomware.WannaCry.zip.zip	c1aeafa14591bbc30cf385e69e13e71438e0c963b3b0de72ede00c7131194478	malicious
Ransomware.WannaCry.zip.zip	3eadbb62d7b951ebb98effa2e7f617e14bf8b47b0cf20fc43bec272475913d44	malicious

Falcon Sandbox Reports

MALICIOUS		MALICIOUS		MALICIOUS	
	ed01ebfbc9eb5bbea545af4d01...		ed01ebfbc9eb5bbea545af4d01...		owo_im_not_ransomware_xd...
Analyzed on: 06/28/2021 15:07:21 (UTC)		Analyzed on: 06/12/2020 23:39:58 (UTC)		Analyzed on: 02/24/2020 16:03:53 (UTC)	
Environment: Windows 7 32 bit		Environment: Windows 7 32 bit		Environment: Windows 7 64 bit	
Threat Score: 100/100		Threat Score: 100/100		Threat Score: 100/100	
AV Detection: 94% Trojan.Ransom.WannaCryptor		AV Detection: 91% Trojan.Ransom.WannaCryptor		AV Detection: 90% Trojan.Ransom.WannaCryptor	
Indicators: 17 36 25		Indicators: 17 34 23		Indicators: 14 37 28	
Network: 		Network: 		Network: 	
					

MALICIOUS		MALICIOUS		MALICIOUS	
	ed01ebfbc9eb5bbea545af4d01...		ed01ebfbc9eb5bbea545af4d01...		ed01ebfbc9eb5bbea545af4d01...
Analyzed on: 08/06/2020 11:08:16 (UTC)		Analyzed on: 08/06/2019 23:46:13 (UTC)		Analyzed on: 06/13/2019 14:15:10 (UTC)	
Environment: Windows 7 32 bit (HWP Support)		Environment: Android Static Analysis		Environment: Windows 7 32 bit (HWP Support)	
Threat Score: 100/100		Threat Score: 100/100		Threat Score: 100/100	
AV Detection: 90% Trojan.Ransom.WannaCryptor		AV Detection: 87% Trojan.Ransom.WannaCryptor		AV Detection: 85% Trojan.Ransom.WannaCryptor	
Indicators: 17 36 25		Indicators: 17 34 23		Indicators: 14 37 28	

Incident Response

 Risk Assessment

Remote Access	Reads terminal service related keys (often RDP related)
Ransomware	Deletes volume snapshots (often used by ransomware) Detected indicator that file is ransomware
Spyware	Contains ability to open the clipboard Deletes volume snapshots (often used by ransomware)
Persistence	Disables startup repair Grants permissions using icaccls (DACL modification) 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
Evasive	Marks file for deletion Possibly checks for the presence of an Antivirus engine
Network Behavior	Contacts 48 hosts. View all details

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 corresponden a las sospechas del punto 7, porque como se estableció, se bloquean los archivos importantes por medio del CRC, y se despliega en pantalla el mensaje del secuestro de datos y demás.



```

Oops, your important files are encrypted.

you see this text, but don't see the "Wana Decrypt0r" window,
in your antivirus removed the decrypt software or you deleted
it from your computer.

you need your files you have to run the decrypt software.

please find an application file named "@WanaDecryptor@.exe" in
your folder or restore from the antivirus quarantine.

and follow the instructions!

```