

Ciberseguridad: Análisis de malware (C|AM)

Diego Jhosué Cornejo Li

INDICE

1. ¿Que strings importantes encuentras en la muestra?	2
2. Listado completo de .dll llamados por la muestra.	3
3. Listado y explicación de las API que TÚ consideras más importantes para el análisis de la muestra.	4
4. Según tu análisis estático, que intuyes que realice el malware al ejecutarlo. Fundamenta tu respuesta	5

1. ¿Que strings importantes encuentras en la muestra?

```
WanaCrypt0r
Software\
.der
.pfx
.key
.crt
.csr
.p12
.pem
.odt
.ott
.sxw
.stw
.uot
.3ds
.max
.3dm
.ods
.ots
.sxc
.stc
.dif
.slk
.wb2
.odp
.otp
.sxd
.std
.uop
.odg
.otg
.sxm
.mml
.lay
.lay6
.asc
.sqlite3
.sqlitedb
.sql
.accdb
.mdb
.dbf
.odb
.frm
.myd
.myi
.ibd
.mdf
.ldf
.sln
.suo
.pot
.pptm
.pptx
.ppt
.xltn
.xltx
.xlc
.xlm
.xlt
.xlw
.xlsb
.xlsm
.xlsx
.xls
.dotx
.dotm
.dot
.docm
.docb
.docx
.doc
%s\%s
%s\Intel
%s\ProgramData
VS_VERSION_INFO
StringFileInfo
040904B0
CompanyName
Microsoft Corporation
FileDescription
DiskPart
FileVersion
6.1.7601.17514 (win7sp1_rtm.101119-1850)
InternalName
diskpart.exe
LegalCopyright
Microsoft Corporation. All rights reserved.
OriginalFilename
diskpart.exe
ProductName
Microsoft
Windows
Operating System
ProductVersion
6.1.7601.17514
VarFileInfo
Translation
```

Hay extensiones de varios tipos de archivos (.sql, xlsx, docx, doc, etc), además del “WannaCrypt0r” que ya indica que el archivo es un malware WannaCry

También contiene rutas como: Intel o ProgramData

Por otro lado también está el “diskpart.exe”, que según he investigado ayuda a administrar las unidades del equipo, pudiendo ser clave en la encriptación de los archivos por el ransomware

USER32.dll

The screenshot shows the VirusTotal interface for the file 'c:\users\cfc.user\desktop\sample\wannacry.exe'. The file is a 32-bit executable (PE32) with a size of 104,857 bytes. The 'Libraries' tab is selected, showing a list of imported DLLs: KERNEL32.dll, USER32.dll, ADVAPI32.dll, and MSVCRT.dll. The 'Imports' tab is also visible, showing a list of imported functions.

3. Listado y explicación de las API que TÚ consideras más importantes para el análisis de la muestra.

API marcadas como flag en pestudio:

imports (114)	flag (16)	type	ordinal	first-thunk (IAT)	first-thunk-original (INT)	library
WriteFile	x	implicit	-	0x0000D97E	0x0000D97E	KERNEL32.dll
SetFileAttributesW	x	implicit	-	0x0000D98A	0x0000D98A	KERNEL32.dll
CreateDirectoryW	x	implicit	-	0x0000D9E8	0x0000D9E8	KERNEL32.dll
CopyFileA	x	implicit	-	0x0000DAA6	0x0000DAA6	KERNEL32.dll
VirtualAlloc	x	implicit	-	0x0000DAC8	0x0000DAC8	KERNEL32.dll
VirtualProtect	x	implicit	-	0x0000DB36	0x0000DB36	KERNEL32.dll
CreateDirectoryA	x	implicit	-	0x0000DB96	0x0000DB96	KERNEL32.dll
CreateProcessA	x	implicit	-	0x0000DB32	0x0000DB32	KERNEL32.dll
CreateServiceA	x	implicit	-	0x0000DC2A	0x0000DC2A	ADVAPI32.dll
StartServiceA	x	implicit	-	0x0000DC52	0x0000DC52	ADVAPI32.dll
CryptReleaseContext	x	implicit	-	0x0000DC14	0x0000DC14	ADVAPI32.dll
RegCreateKeyW	x	implicit	-	0x0000DC04	0x0000DC04	ADVAPI32.dll
RegSetValueExA	x	implicit	-	0x0000DBF2	0x0000DBF2	ADVAPI32.dll
OpenSCManagerA	x	implicit	-	0x0000DC72	0x0000DC72	ADVAPI32.dll
rand	x	implicit	-	0x0000DCE6	0x0000DCE6	MSVCRT.dll
srand	x	implicit	-	0x0000DCEE	0x0000DCEE	MSVCRT.dll
GetFileAttributesW	-	implicit	-	0x0000DBFC	0x0000DBFC	KERNEL32.dll
GetFileSize	-	implicit	-	0x0000D912	0x0000D912	KERNEL32.dll
CreateFileA	-	implicit	-	0x0000D922	0x0000D922	KERNEL32.dll
InitializeCriticalSection	-	implicit	-	0x0000D930	0x0000D930	KERNEL32.dll
DeleteCriticalSection	-	implicit	-	0x0000D94C	0x0000D94C	KERNEL32.dll
ReadFile	-	implicit	-	0x0000D964	0x0000D964	KERNEL32.dll
GetFileSize	-	implicit	-	0x0000D970	0x0000D970	KERNEL32.dll
LeaveCriticalSection	-	implicit	-	0x0000D98A	0x0000D98A	KERNEL32.dll
EnterCriticalSection	-	implicit	-	0x0000D9A2	0x0000D9A2	KERNEL32.dll
SetCurrentDirectoryW	-	implicit	-	0x0000D9D0	0x0000D9D0	KERNEL32.dll
GetTempPathW	-	implicit	-	0x0000D9FC	0x0000D9FC	KERNEL32.dll

- Permite al programa gestionar los archivos del sistema:
 - WriteFile
 - SetFileAttributesW:
 - CopyFileA
 - CreateDirectoryA
 - SetCurrentDirectoryW
- Usado para la persistencia del malware:
 - CreateProcessA
 - CreateServiceA
 - StartServiceA
 - OpenSCManagerA
- Uso de apis para asignar parte de la memoria para el proceso de inyección del malware
 - VirtualAlloc
 - VirtualProtect
- Utiliza APIs criptograficas <https://malapi.io/winapi/CryptReleaseContext>
 - CryptReleaseContext
- Estas apis generan numeros pseudoaleatorios:
<https://learn.microsoft.com/en-us/cpp/c-runtime-library/reference/srand?view=msvc-170>
 - rand
 - srand

4. Según tu análisis estático, que intuyes que realice el malware al ejecutarlo. Fundamenta tu respuesta

Después de analizar la muestra, por los strings, dlls y apis se puede concluir que el malware es un ransomware.

Por su definición el ransomware es un software que cifra archivos y exige un pago para recuperarlos, usando apis de KERNEL32.dll para poder acceder a archivos del sistema para posteriormente cifrarlos con funciones criptográficas CryptReleaseContext y generación de números pseudoaleatorios (rand, srand) y mantener persistencia en el sistema creando servicios e iniciándolos con CreateService, StartService. Además de apoyarse de memoria para terminar su proceso de inyección de malware.

Este software encriptaría la mayoría de los archivos, por el análisis de strings se vió que hay varias extensiones de archivos comunes como .sql .docx .xlsl etc.

