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?

```
┌──(kali㉿kali)-[~/Desktop/HT2]
└─$ python peheader.py
Ejecutable: ./MALWR/sample_qwrty_dk2
SECCIONES
b'UPX0\x00\x00\x00\x00' 0x1000 0x5000 0
b'UPX1\x00\x00\x00\x00' 0x6000 0x1000 4096
b'.rsrc\x00\x00\x00' 0x7000 0x1000 512
LLAMADAS A DLL
b'KERNEL32.DLL'
LLAMADAS A FUNCIONES
        b'LoadLibraryA'
        b'ExitProcess'
        b'GetProcAddress'
        b'VirtualProtect'
LLAMADAS A DLL
b'MSVCRT.dll'
LLAMADAS A FUNCIONES
        b'atol'
LLAMADAS A DLL
b'SHELL32.dll'
LLAMADAS A FUNCIONES
        b'SHChangeNotify'
LLAMADAS A DLL
b'USER32.dll'
LLAMADAS A FUNCIONES
        b'LoadStringA'
LLAMADAS A DLL
b'WS2_32.dll'
LLAMADAS A FUNCIONES
        b'closesocket'
TimeDateStamp : Thu May 14 17:12:40 2009 UTC
TimeDateStamp: 0x4a0c5108
```

Figura 1: Resultados del análisis para el ejecutable sample_qwrty_dk2

```
└─$ python peheader.py
Ejecutable: ./MALWR/sample_vg655_25th.exe
SECCIONES
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
LLAMADAS A 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'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'LoadLibraryA'
        b'GetProcAddress'
        b'GlobalFree'
        b'CreateProcessA'
        b'CloseHandle'
        b'WaitForSingleObject'
        b'TerminateProcess'
        b'GetExitCodeProcess'
        b'FindResourceA'
LLAMADAS A DLL
b'USER32.dll'
LLAMADAS A FUNCIONES
        b'wsprintfA'
LLAMADAS A 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 A 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'wcscat'
        b'wcslen'
        b'__CxxFrameHandler'
        b'??3@YAXPAX@Z'
        b'memcmp'
        b'_except_handler3'
        b'_local_unwind2'
        b'wcsrchr'
        b'swprintf'
        b'??2@YAPAXI@Z'
```

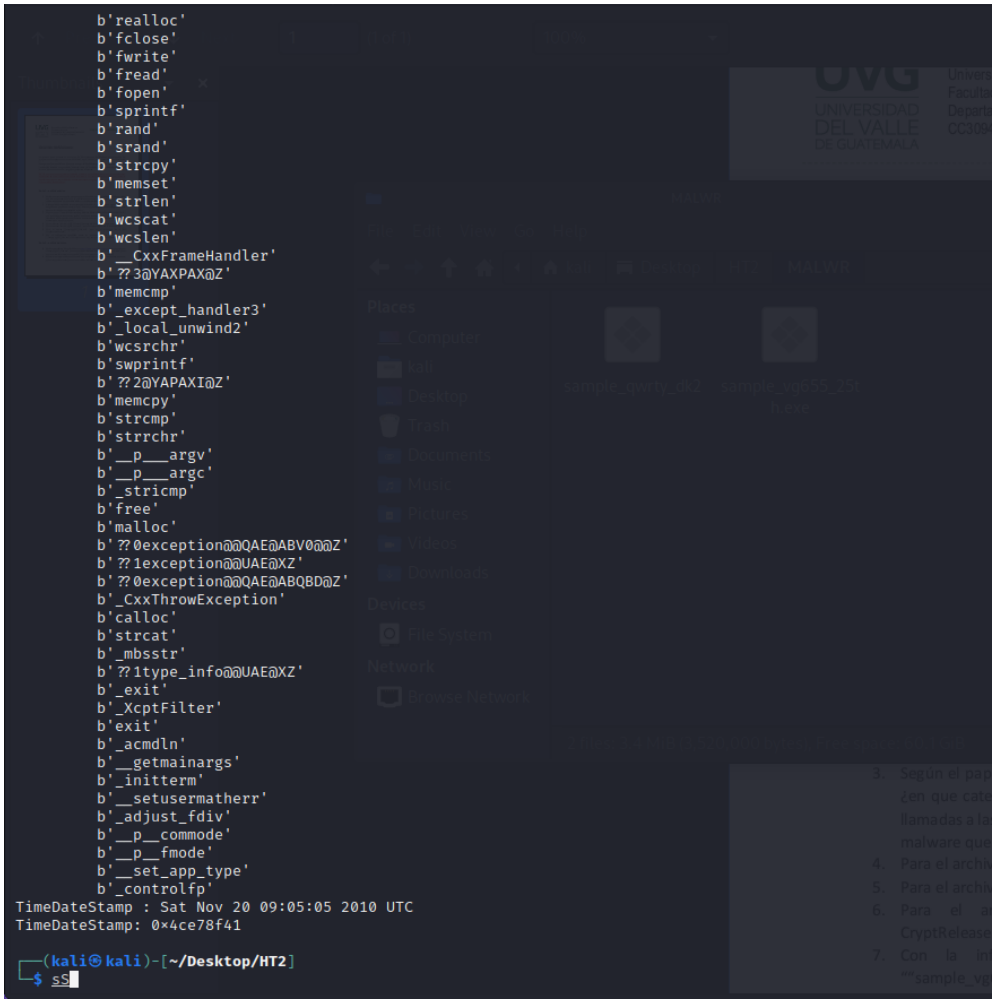


Figura 2: Resultados del análisis para el ejecutable sample_vg655_25th

Como se puede observar en las figuras anteriores, al realizar el análisis para los dos ejecutables, el ejecutable sample_vg655_25th es el que tiene más llamadas a funciones que el ejecutable sample_qwrty_dk2. Además de esto, las llamadas que hace sample_vg655_25th son un poco sospechosas, ya que hace llamadas para poder: Crear, leer, escribir y modificar archivos, modificar de la misma forma los servicios del equipo, etc.

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.

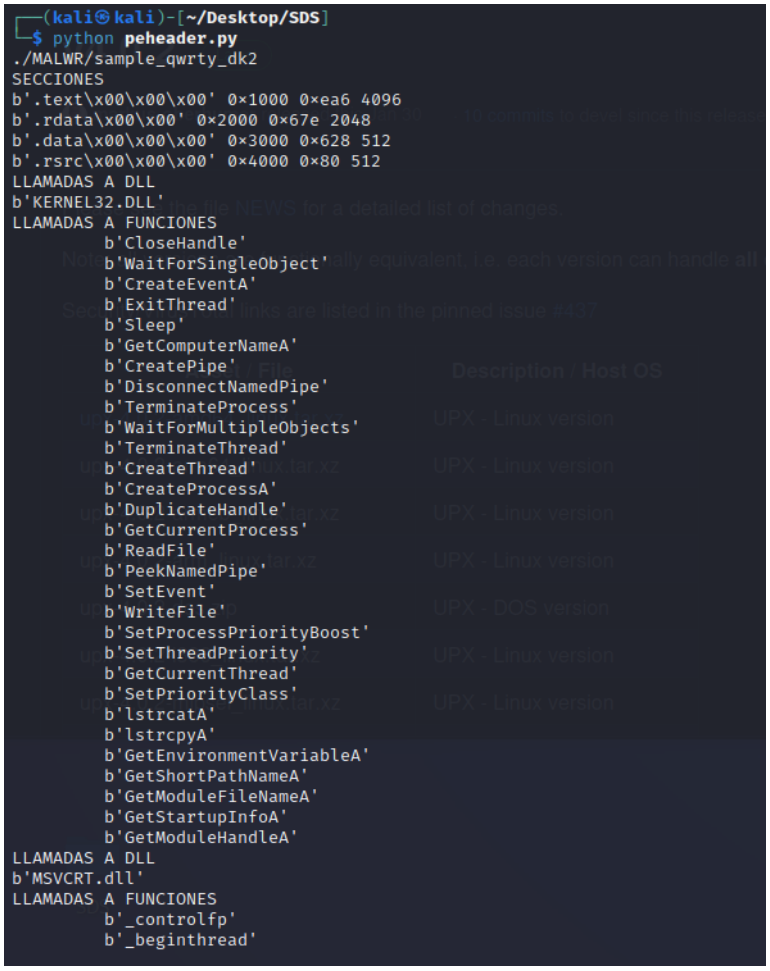


Figura 3: Funciones que llama la DLL ADVAPI32.dll

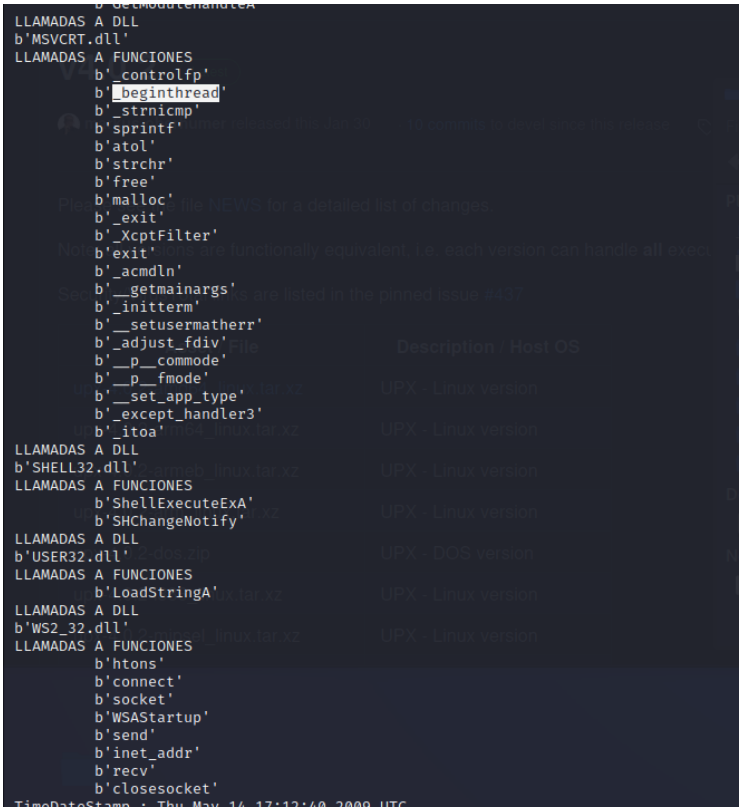


Figura 4: Funciones que llama la DLL ADVAPI32.dll

Como se puede observar en las figuras anteriores, el archivo sample_qwrty_dk2 posee secciones que tienen la palabra UPX en ellas, estas hacen referencia a Ultimate packer for executables, los cuales son secciones

que se encuentran empaquetadas. Al realizar el desempaque de estas, se puede observar que ahora, el archivo hace más llamadas a API´s del sistema, los cuales se parecen mucho al ejecutable sample_vg655_25th.

3. 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.

Behaviour	Malware Category	Api Functions Calls
Behaviour 1	Search file to infect	
Behaviour 2	Copy/Delete files	CloseHandle
Behaviour 3	Get File Information	GetFilseSizeEx, GetFileSize
Behaviour 4	Move Files	
Behaviour 5	Read/Write files	WriteFile, CloseHandle
Behaviour 6	Change File Attributes	Aunque no aparezcan exactamente las mismas llamadas que en la tabla, sí hace llamadas para cambiar atributos de los archivos. Ejemplo SetFileAttributesW

Tabla 1: Categorización de las llamadas API´s del archivo sample_vg655_25th

Behaviour	Malware Category	Api Functions Calls
Behaviour 1	Search file to infect	
Behaviour 2	Copy/Delete files	CloseHandle
Behaviour 3	Get File Information	
Behaviour 4	Move Files	
Behaviour 5	Read/Write files	CloseHandle, WriteFile
Behaviour 6	Change File Attributes	

Tabla 2: Categorización de las llamadas API´s del archivo sample_qwrty_dk2

4. Para el archivo "sample_vg655_25th.exe" obtenga el HASH en base al algoritmo SHA256.
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
MALWR/sample_vg655_25th.exe
5. Para el archivo "sample_vg655_25th.exe", ¿cuál es el propósito de la DLL ADVAPI32.dll?

```
LLAMADAS A 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'
```

Figura 5: Funciones que llama la DLL ADVAPI32.dll

Como se puede observar en la figura anterior, esta dll se encarga de llamar servicios que son los requeridos para crear/iniciar/terminar/cerrar algún servicio en la computadora. Además, esta puede llamar servicios que se podrían utilizar para encriptar datos.

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

   Esta API tiene el propósito de liberar todos los manejos que hay en el sistema relacionados con la encriptación de datos (Microsoft, 10/2021).

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.

   Luego de analizar todas las API´s que utiliza este archivo, se puede decir que este ejecutable es sospechoso de malware, debido a que tiene llamadas a funciones que se encargan de modificar archivos (modificaciones que no se encargan solamente del contenido del archivo, sino que también de modificaciones de los atributos) y tiene llamadas a funciones que están relacionados con la encriptación de datos. Es por esto que el propósito de esto podría ser la encriptación de los datos del sistema.

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?

Related files

Name	Sha256	Verdict
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

Samples that dropped this file

Name	Sha256	Verdict
Server.exe	5c17f43e95f71d09ae9d3a12e5c586eb257d0bf49ce6551709468c4617a0bf8f	malicious
file	1e06140672b73dfe337dfde7bc9dead5612bdbf4a8069be5de78fe68da6c75c4	malicious
file	73aa2e53b8290b32c827187b2c1c36167ae968aec846674a5e2cb72e55f32b7e	malicious
WannaCry.exe	91afb972e14584bc1e23802e2b26813f57b802689fe61a540fdaf162cecd7493	malicious
wannacry.exe	8d30a5435253066e4bb1788104f6b8ae402b0331d76a6543285e51fc0faf6a56	malicious

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	⌄
Writes data to 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	⌄

Risk Assessment

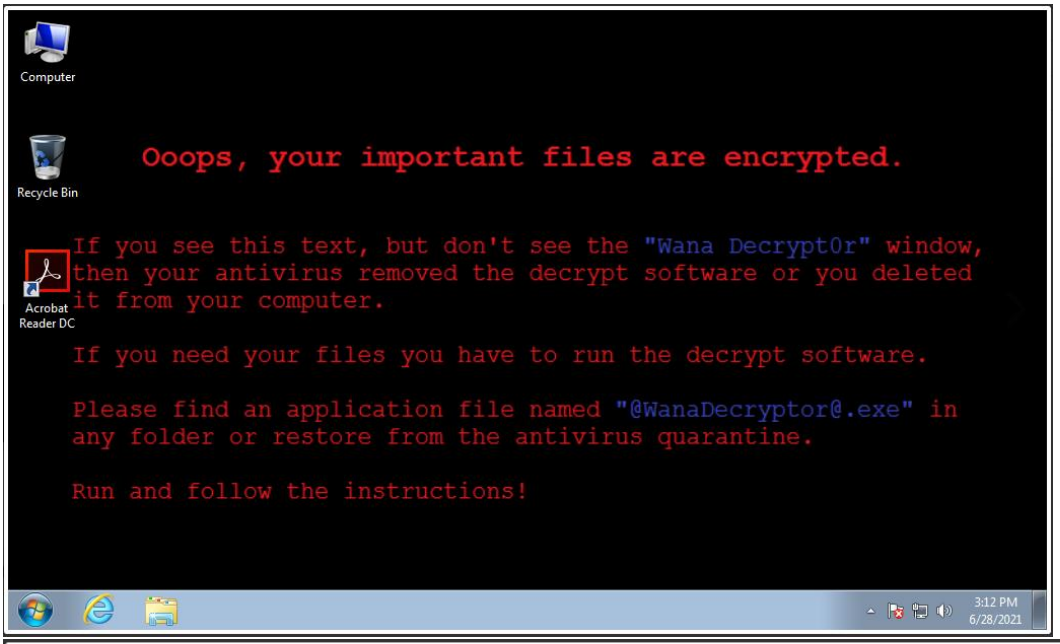
Remote Access	Reads terminal service related keys (often RDP related)
Spyware	Accesses potentially sensitive information from local browsers Contains ability to open the clipboard Deletes volume snapshots (often used by ransomware) Hooks API calls
Persistence	Disables startup repair Grants permissions 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

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1106	Native API	• Execution	Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Learn more		• 2 confidential indicators	• Contains ability to dynamically load libraries • Contains ability to retrieve the NetBIOS name of the local computer (API string) • Calls an API typically used to create a process • Contains ability to retrieve the name of the user associated with the current thread (API string)
T1569.002	Service Execution	• Execution	Adversaries may abuse the Windows service control manager to execute malicious commands or payloads. Learn more		• Contains ability to open/control a service	
T1059.005	Visual Basic	• Execution	Adversaries may abuse Visual Basic (VB) for execution. Learn more		• 1 confidential indicators	• Launches a VBS file
T1059	Command and Scripting Interpreter	• Execution	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. Learn more			• Drops or executes a batch file
T1203	Exploitation for Client Execution	• Execution	Adversaries may exploit software vulnerabilities in client applications to execute code. Learn more		• Contains ability to download file/payload	
T1059.003	Windows Command Shell	• Execution	Adversaries may abuse the Windows command shell for execution. Learn more			• Runs shell commands

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1134	Access Token Manipulation	• Privilege Escalation • Defense Evasion	Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Learn more		• 1 confidential indicators	
T1134.001	Token Impersonation/Theft	• Privilege Escalation • Defense Evasion	Adversaries may duplicate then impersonate another user's token to escalate privileges and bypass access controls. Learn more		• 1 confidential indicators	• Contains ability to obtains specified information about the security of a file or directory (API string) • Imports system security related APIs
T1055.012	Process Hollowing	• Privilege Escalation • Defense Evasion	Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Learn more	• Allocates virtual memory in a remote process • Creates a process in suspended mode (likely for process injection)		
T1055	Process Injection	• Privilege Escalation • Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more	• Writes data to a remote process		

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1497	Virtualization/Sandbox Evasion	• Defense Evasion • Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments. Learn more		• 1 confidential indicators	• The input sample possibly contains the RDTSCP instruction • Contains ability to delay the execution of current thread
T1070.004	File Deletion	• Defense Evasion	Adversaries may delete files left behind by the actions of their intrusion activity. Learn more		• Opens file with deletion access rights	
T1027.002	Software Packing	• Defense Evasion	Adversaries may perform software packing or virtual machine software protection to conceal their code. Learn more		• PE file has unusual entropy sections • 1 confidential indicators	• Matched Compiler/Packer signature
T1222.001	Windows File and Directory Permissions Modification	• Defense Evasion	Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files. Learn more	• Modifies the access control lists of files	• 1 confidential indicators	
T1134	Access Token Manipulation	• Privilege Escalation • Defense Evasion	Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Learn more		• 1 confidential indicators	
T1134.001	Token Impersonation/Theft	• Privilege Escalation • Defense Evasion	Adversaries may duplicate then impersonate another user's token to escalate privileges and bypass access controls. Learn more		• 1 confidential indicators	• Contains ability to obtains specified information about the security of a file or directory (API string) • Imports system security related APIs

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?



Al ver las capturas de pantalla, se puede concluir que, efectivamente, el malware se encarga de encriptar los datos que hay en el sistema y para desencriptarlos, pide un rescate de 300$ en bitcoins.

Referencias

- Microsoft (10/2021). CryptReleaseContext function (wincrypt.h). https://learn.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-cryptreleasecontext