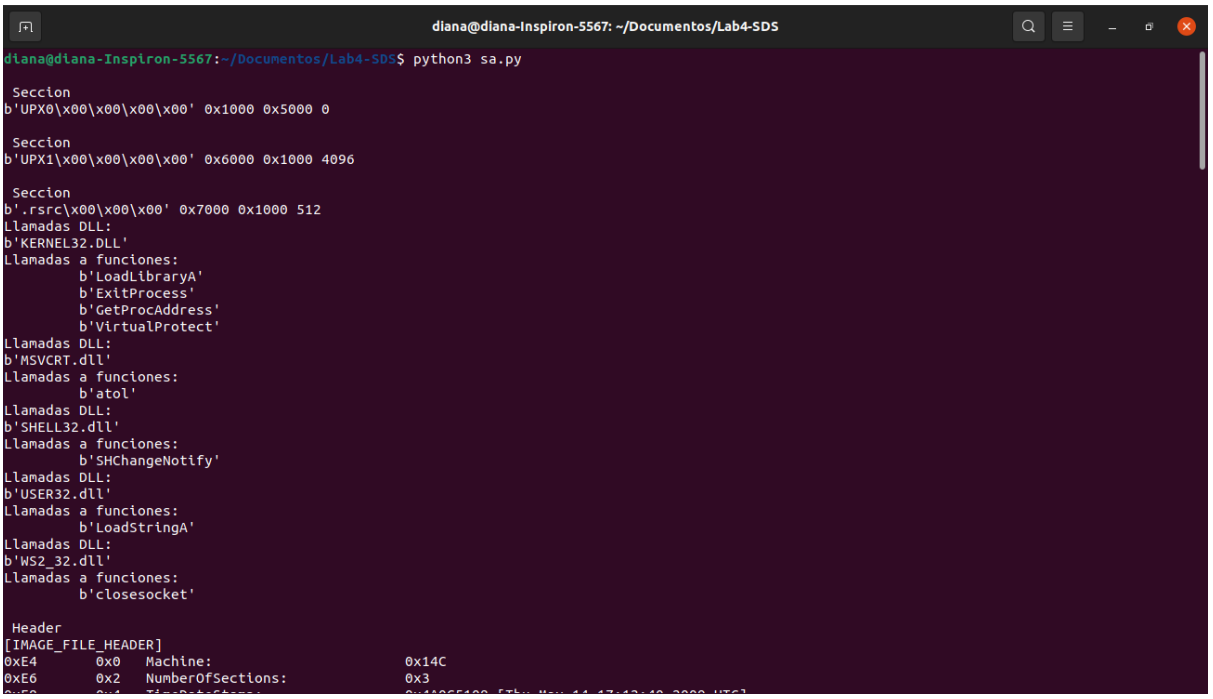
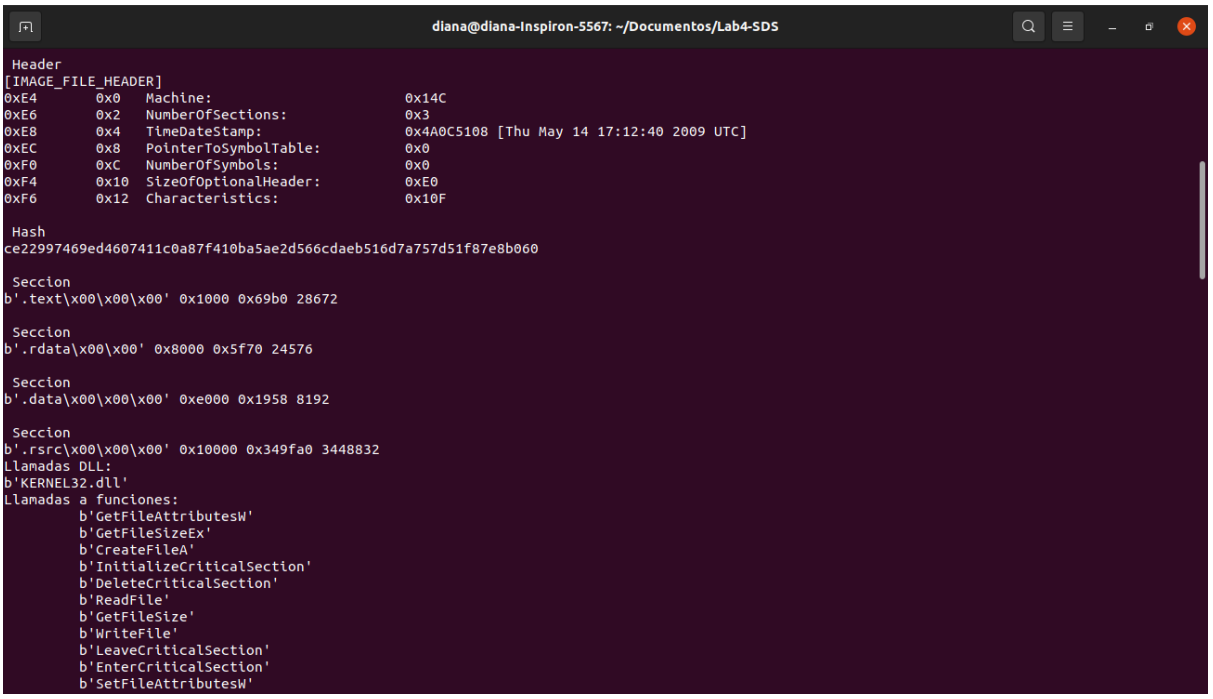
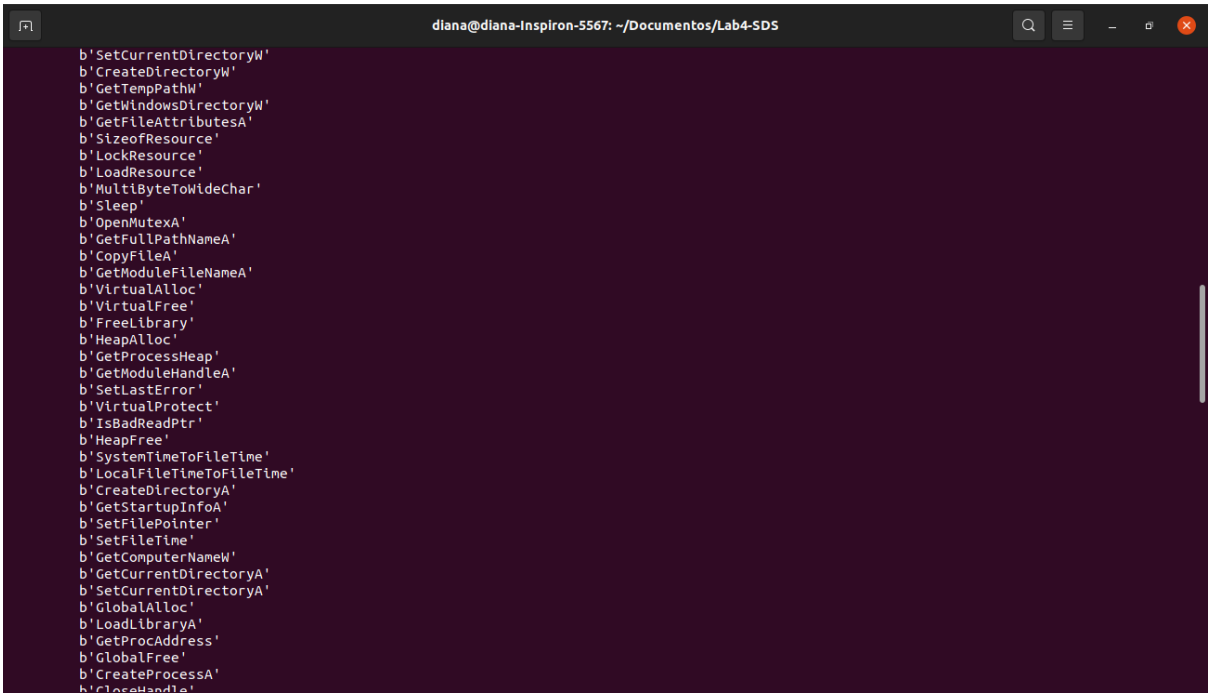
**Parte 1 - Análisis de un malware**

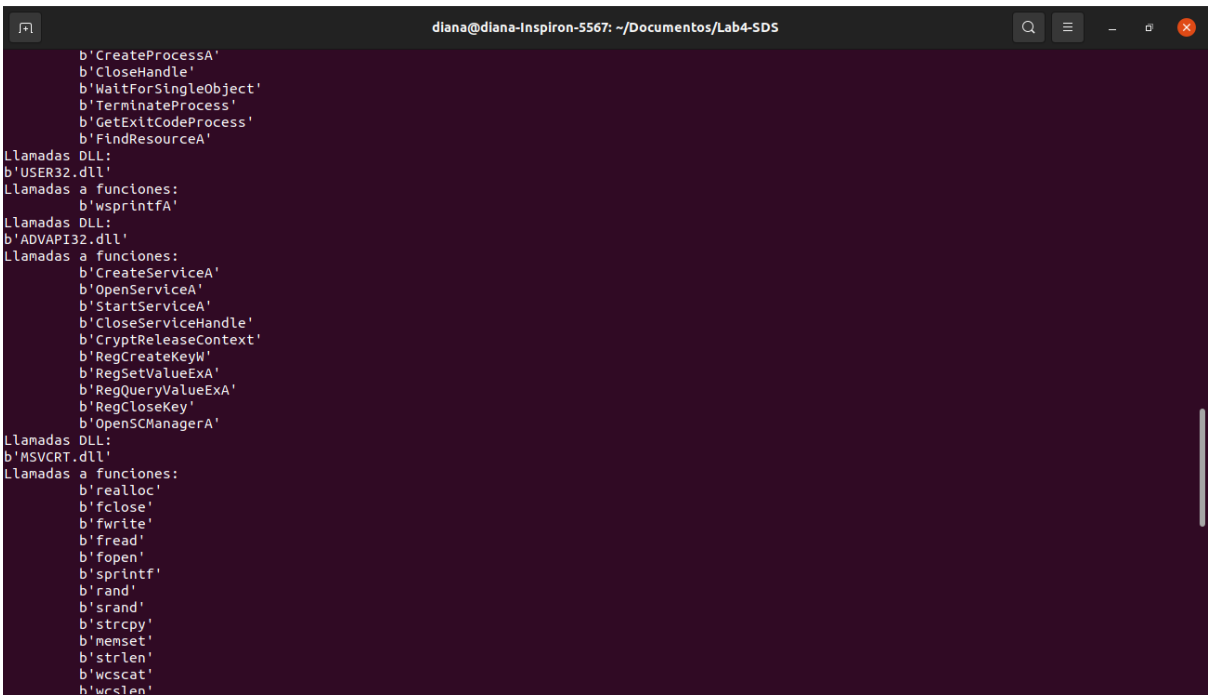
- **Análisis estático**
  - **Utilice la herramienta pefile para examinar el PE header y obtenga las DLL y las APIs que los ejecutables llaman. ¿Qué diferencias observa entre los ejemplos? ¿Existe algún indicio sospechoso en la cantidad de DLLs y las APIs llamadas?**

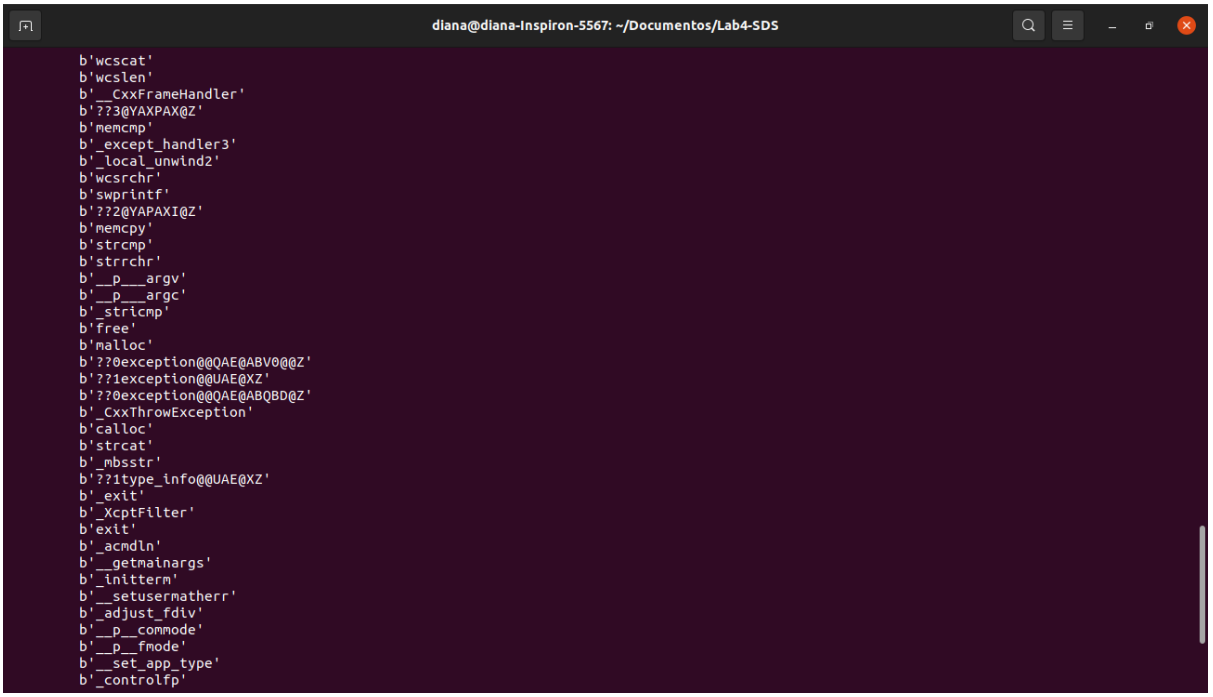
El archivo sample_qwrty_dk2 tiene unas secciones que son extensión UPX, mientras que sample_vg655_25th.exe tiene secciones con extensión .text, .rdata, .data, .rsrc
Asimismo el archivo sample_vg655_25th.exe tiene más llamadas a DLLs y APIs que el archivo sample_qwrty_dk2

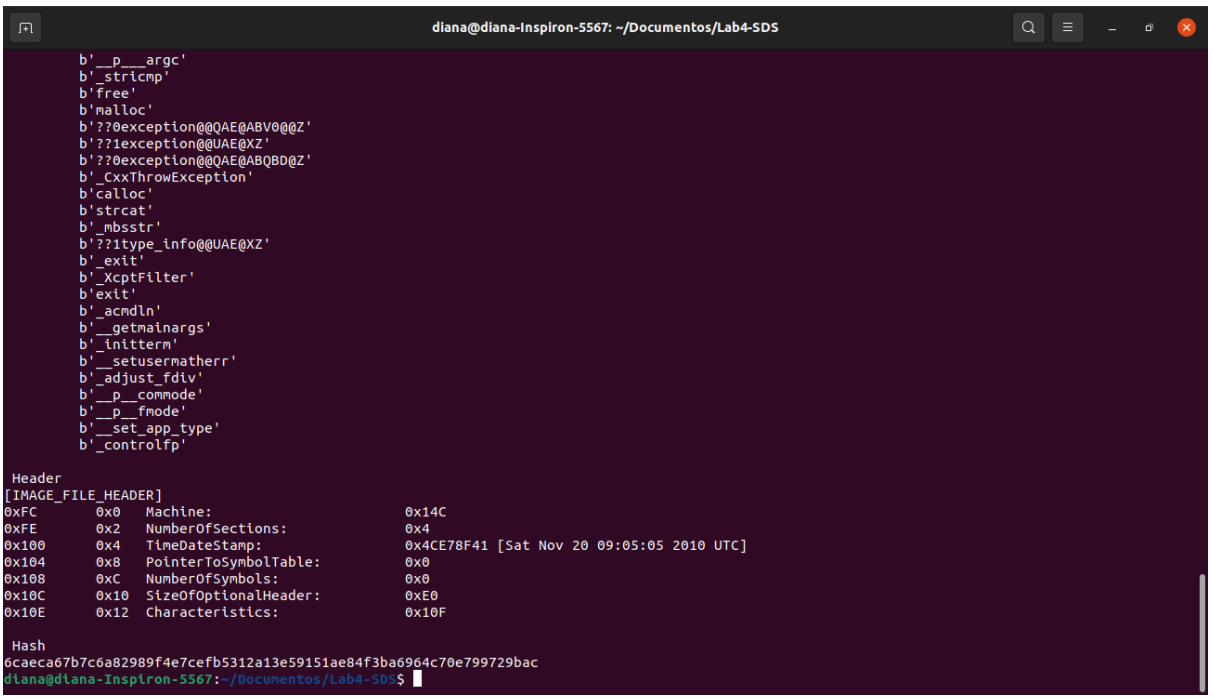



diana@diana-Inspiron-5567: ~/Documentos/Lab4-SDS
b'SetCurrentDirectoryW'
b'CreateDirectoryW'
b'GetTempPathW'
b'GetWindowsDirectoryW'
b'GetFileAttributesA'
b'SizeofResource'
b'LockResource'
b'LoadResource'
b'MultiByteToWideChar'
b'Sleep'
b'OpenMutexA'
b'GetFullPathNameA'
b'CopyFileA'
b'GetModuleFileNameA'
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'

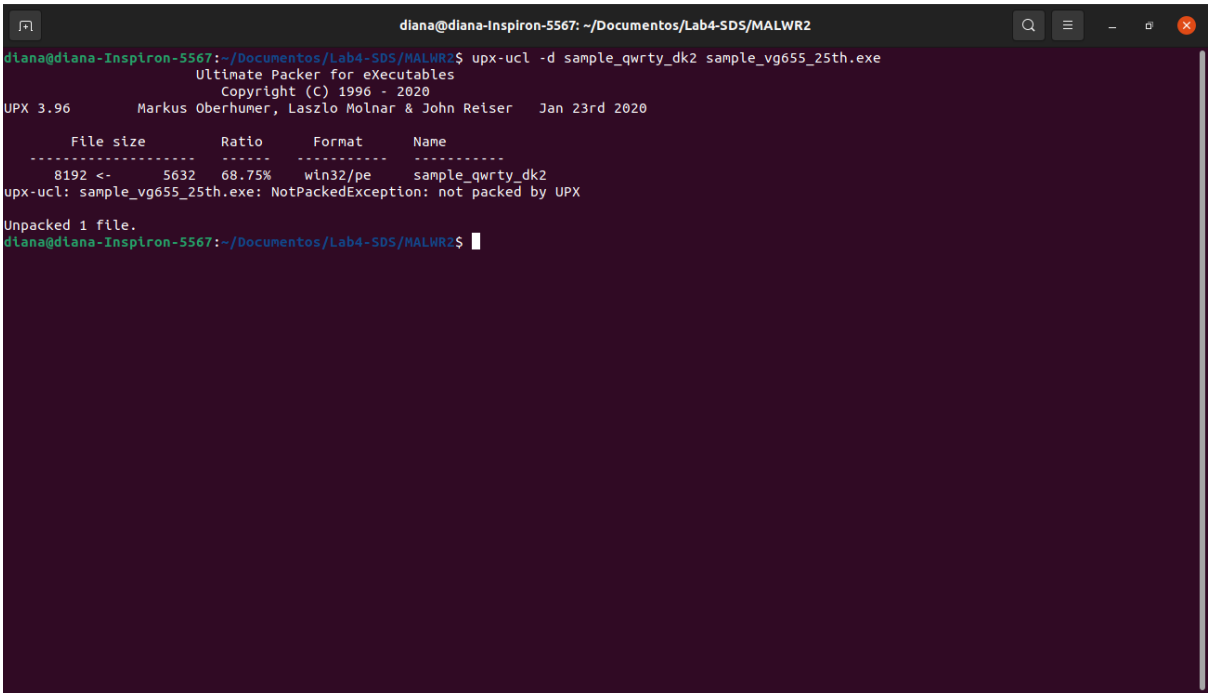

diana@diana-Inspiron-5567: ~/Documentos/Lab4-SDS
b'CreateProcessA'
b'CloseHandle'
b'WaitForSingleObject'
b'TerminateProcess'
b'GetExitCodeProcess'
b'FindResourceA'
Llamadas DLL:
b'USER32.dll'
Llamadas a funciones:
b'wsprintfA'
Llamadas DLL:
b'ADVAPI32.dll'
Llamadas a funciones:
b'CreateServiceA'
b'OpenServiceA'
b'StartServiceA'
b'CloseServiceHandle'
b'CryptReleaseContext'
b'RegCreateKeyW'
b'RegSetValueExA'
b'RegQueryValueExA'
b'RegCloseKey'
b'OpenSCManagerA'
Llamadas DLL:
b'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'

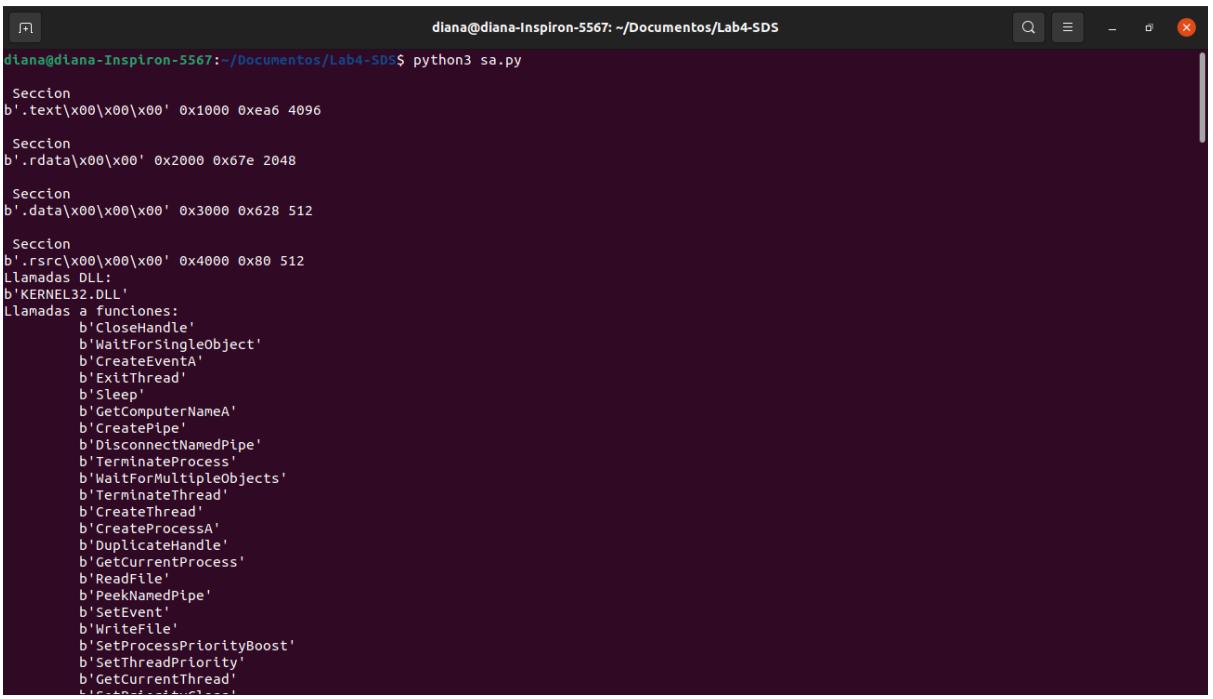


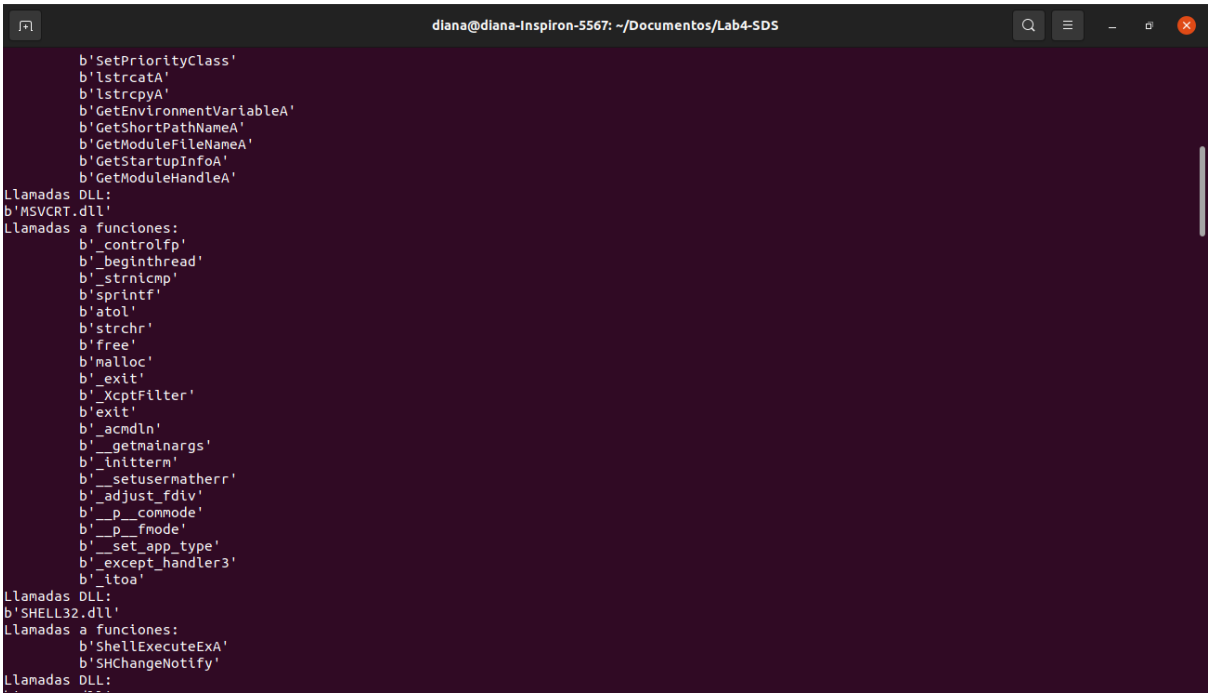



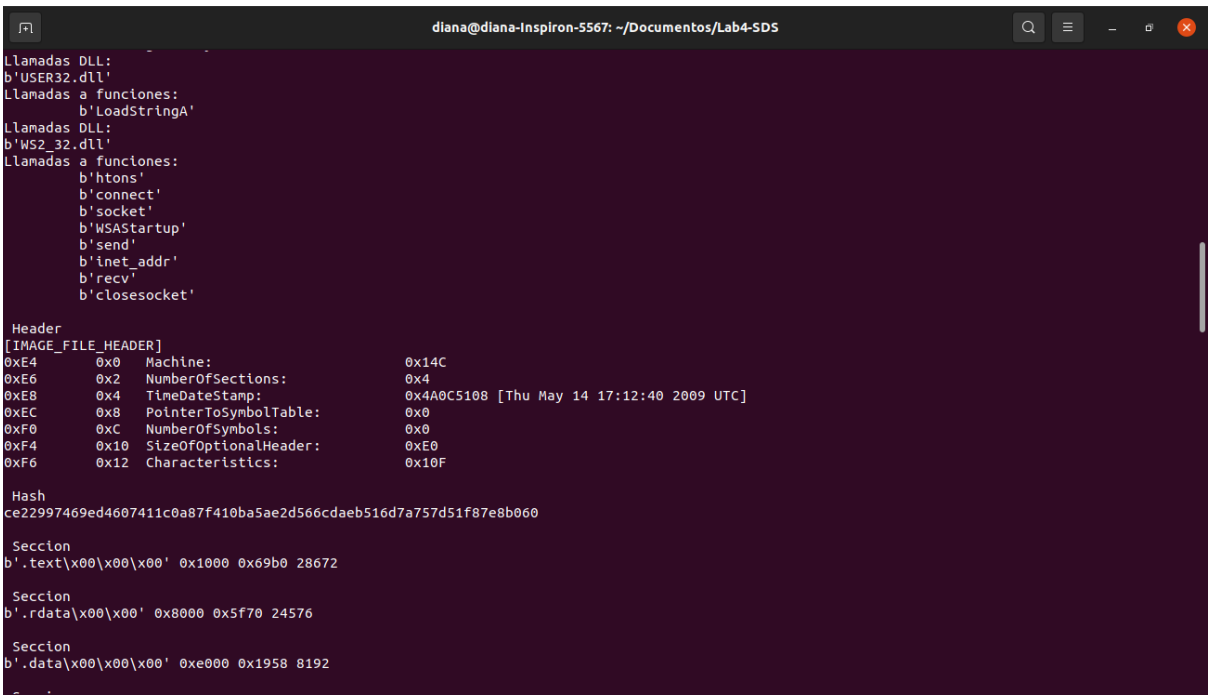

- **Obtenga la información de las secciones del PE Header. ¿Qué significa que algunas secciones tengan como parte de su nombre “upx”? Realice el procedimiento de desempaquetado para obtener las llamadas completas de las APIs.**

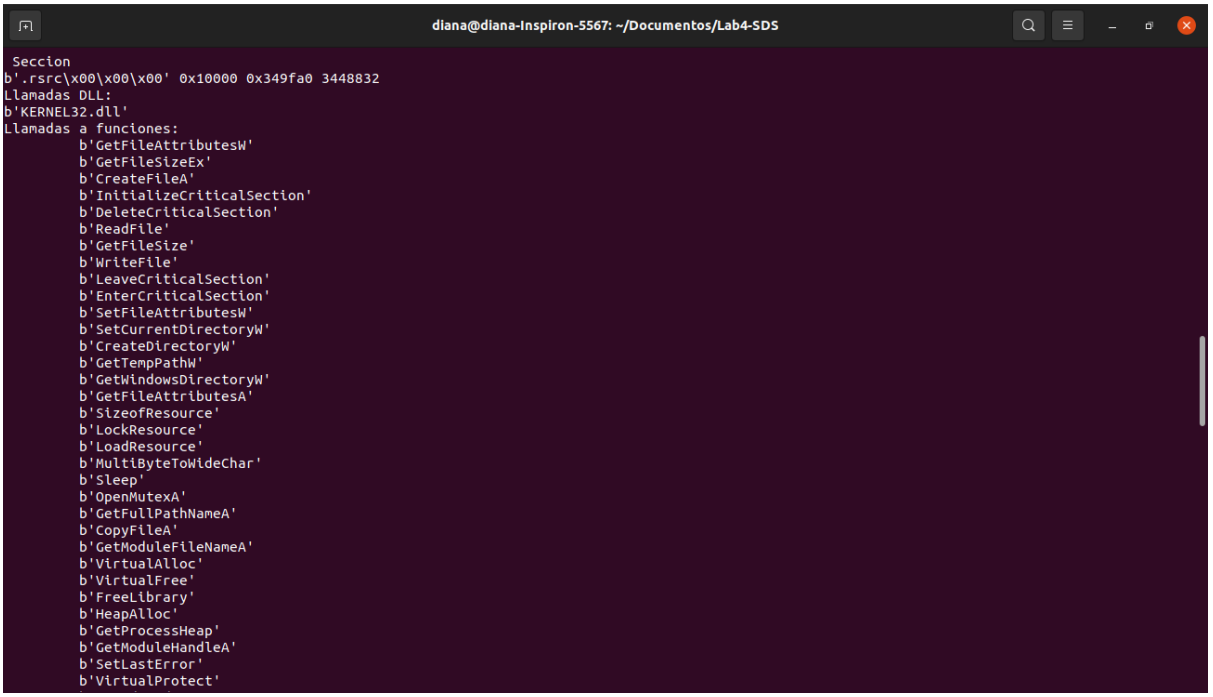
Ultimate Packer for eXecutables (UPX) es una herramienta de compresión de archivos ejecutables, sin embargo, algunos virus y programas maliciosos utilizan UPX para ocultar su comportamiento.

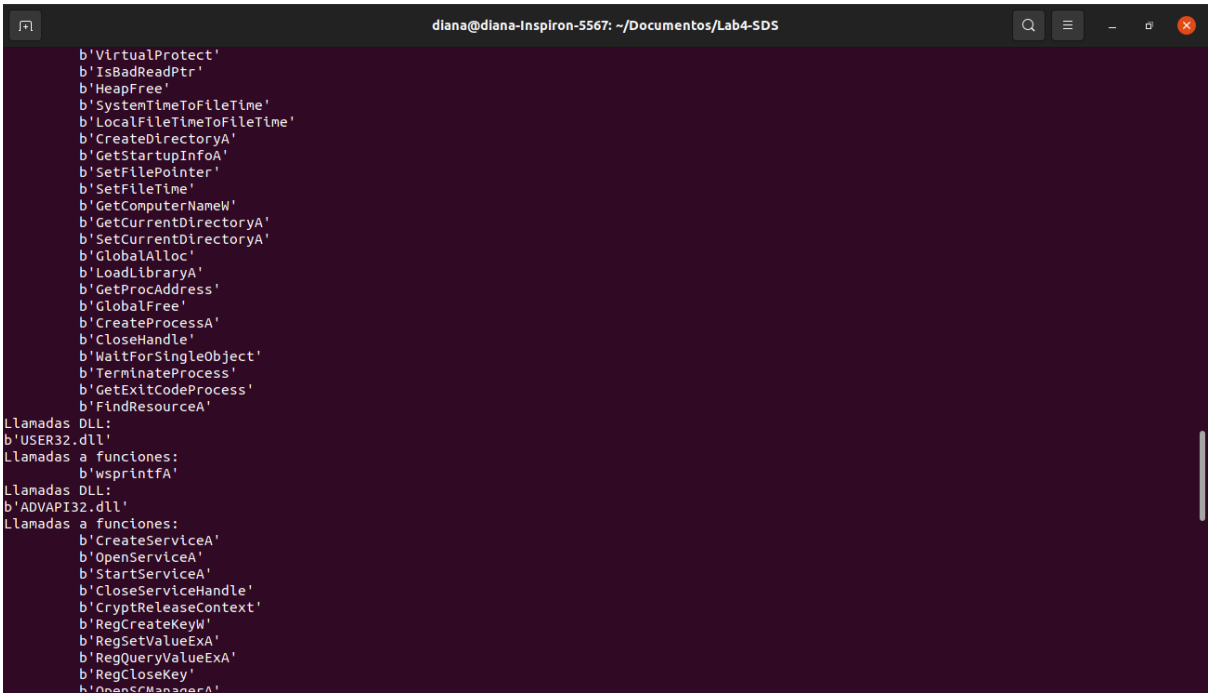

diana@diana-Inspiron-5567: ~/Documentos/Lab4-SDS/MALWR2
diana@diana-Inspiron-5567:~/Documentos/Lab4-SDS/MALWR2$ upx-ucl -d sample_qwrty_dk2 sample_vg655_25th.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX 3.96 Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020
File size Ratio 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.
diana@diana-Inspiron-5567:~/Documentos/Lab4-SDS/MALWR2$

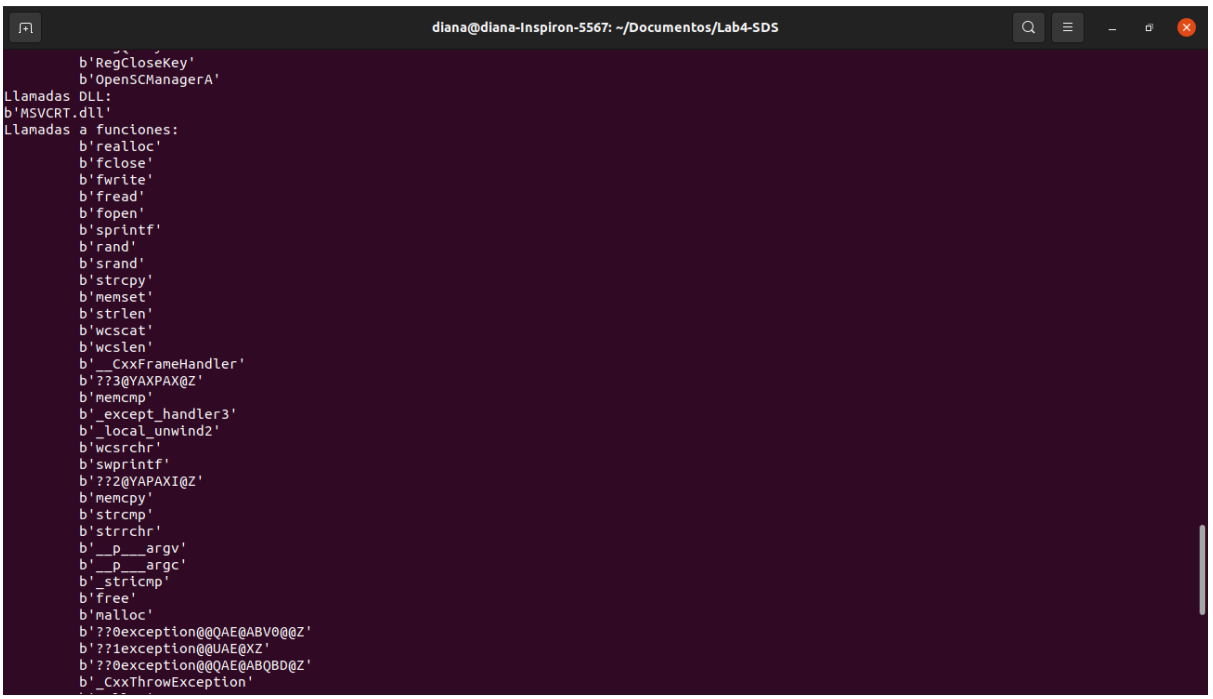

diana@diana-Inspiron-5567: ~/Documentos/Lab4-SDS
diana@diana-Inspiron-5567:~/Documentos/Lab4-SDS$ python3 sa.py
Seccion
b'.text\x00\x00\x00' 0x1000 0xea6 4096
Seccion
b'.rdata\x00\x00' 0x2000 0x67e 2048
Seccion
b'.data\x00\x00\x00' 0x3000 0x628 512
Seccion
b'.rsrc\x00\x00\x00' 0x4000 0x80 512
Llamadas DLL:
b'KERNEL32.DLL'
Llamadas a funciones:
b'CloseHandle'
b'WaitForSingleObject'
b'CreateEventA'
b'ExitThread'
b'Sleep'
b'GetComputerNameA'
b'CreatePipe'
b'DisconnectNamedPipe'
b'TerminateProcess'
b'WaitForMultipleObjects'
b'TerminateThread'
b'CreateThread'
b'CreateProcessA'
b'DuplicateHandle'
b'GetCurrentProcess'
b'ReadFile'
b'PeekNamedPipe'
b'SetEvent'
b'WriteFile'
b'SetProcessPriorityBoost'
b'SetThreadPriority'
b'GetCurrentThread'


diana@diana-Inspiron-5567: ~/Documentos/Lab4-SDS
b'SetPriorityClass'
b'lstrcatA'
b'lstrcpyA'
b'GetEnvironmentVariableA'
b'GetShortPathNameA'
b'GetModuleFileNameA'
b'GetStartupInfoA'
b'GetModuleHandleA'
Llamadas DLL:
b'MSVCRT.dll'
Llamadas a funciones:
b'_controlfp'
b'_beginthread'
b'_strnicmp'
b'sprintf'
b'atol'
b'strchr'
b'free'
b'malloc'
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'_except_handler3'
b'_itoa'
Llamadas DLL:
b'SHELL32.dll'
Llamadas a funciones:
b'ShellExecuteExA'
b'SHChangeNotify'
Llamadas DLL:


diana@diana-Inspiron-5567: ~/Documentos/Lab4-SDS
Llamadas DLL:
b'USER32.dll'
Llamadas a funciones:
b'LoadStringA'
Llamadas DLL:
b'WS2_32.dll'
Llamadas a funciones:
b'htons'
b'connect'
b'socket'
b'WSAStartup'
b'send'
b'inet_addr'
b'recv'
b'closesocket'
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
Hash
ce22997469ed4607411c0a87f410ba5ae2d566cdaeb516d7a757d51f87e8b060
Seccion
b'.text\x00\x00\x00' 0x1000 0x69b0 28672
Seccion
b'.rdata\x00\x00' 0x8000 0x5f70 24576
Seccion
b'.data\x00\x00\x00' 0xe000 0x1958 8192


diana@diana-Inspiron-5567: ~/Documentos/Lab4-SDS
Seccion
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'FreeLibrary'
b'HeapAlloc'
b'GetProcessHeap'
b'GetModuleHandleA'
b'SetLastError'
b'VirtualProtect'



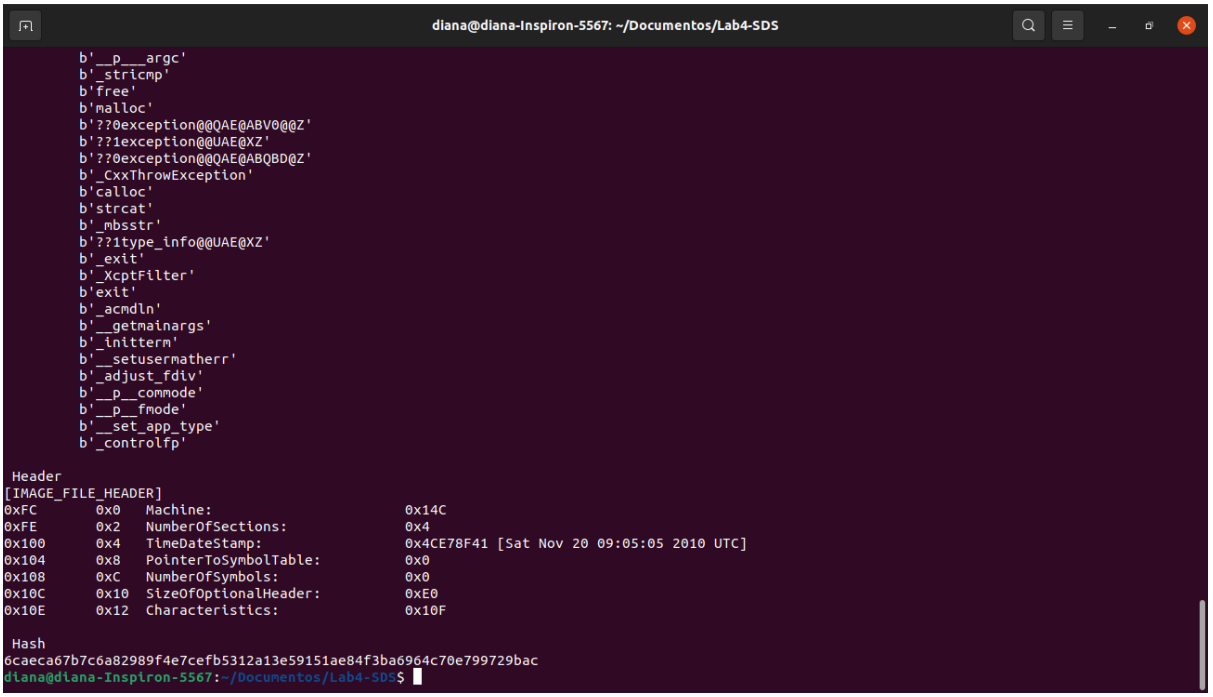

- **Según el paper “Towards Understanding Malware Behaviour by the Extraction of API Calls”, ¿en qué categoría sospechosas pueden clasificarse estos ejemplos en base a algunas de las llamadas a las APIs que realizan? Muestre una tabla con las APIs sospechosas y la categoría de malware que el paper propone.**

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 |

El primero podría ser un malware de categoría Copy/Delete Files y el segundo de categoría Get File Information, basándonos en la tabla del paper y las llamadas a APIs obtenidas.

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




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

advapi32.dll es una parte de una biblioteca avanzada de los servicios del API que utiliza APIs numerosos incluyendo muchas llamadas de seguridad y registro.

advapi32.dll es un proceso del sistema necesario para que la computadora funcione correctamente. Lo que hace es permitir que los puntos de referencia fuercen las tareas pendientes para ser ejecutadas sin una larga espera y de forma sencilla.

Algunos programas maliciosos se disfrazan de advapi32.dll, especialmente cuando no se encuentran en la carpeta C:\Windows\System32.

- **Para el archivo "sample_vg655_25th.exe", ¿cuál es el propósito de la API CryptReleaseContext?**

Mostrar el identificador de un proveedor de servicios criptográficos (CSP) y un contenedor de claves. Con cada llamada a la función el recuento de referencias en el CSP se reduce en uno y al tomar el valor de cero, el contexto se libera por completo y para evitar que este sea utilizado por otra función del software. Este archivo llama CryptReleaseContext después de usar el CSP para que al finalizar el identificador CSP liberado ya no sea válido y se protejan los contenedores de claves y pares de claves.

- **Con la información recopilada hasta el momento, indique para el archivo "sample_vg655_25th.exe" si es sospechoso o no, y cuál podría ser su propósito.**

Si es sospechoso porque hace llamadas al sistema que no cualquier archivo hace y cuyas intenciones posiblemente sean tomar el control del sistema para infectarlo con algún tipo de malware.

- **Análisis dinámico**
  - **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 qué consiste este malware?**

**Submission name:**
owo_im_not_ransomware_xd.exe

**Size:**
3.4MiB

**Type:**
peexe (/search?query=filetype:peexe&block_redirect=1) executable (/search?query=filetype:executable&block_redirect=1)

**Mime:**
application/x-dosexec

**SHA256:**
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa (/search?query=context:ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa&block_redirect=1)

**Operating System:**
Windows

**Last Anti-Virus Scan:**
03/11/2022 22:00:31 (UTC)

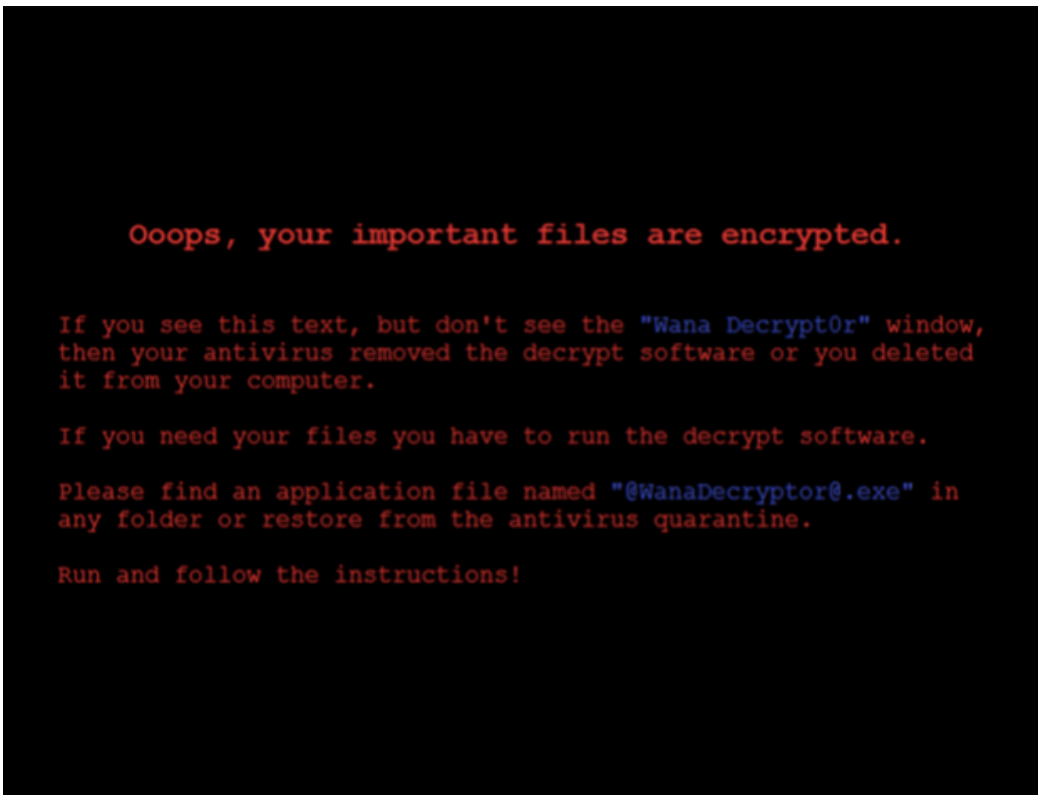
**Last Sandbox Report:**
06/28/2021 15:07:21 (UTC)

malicious

Threat Score: 100/100
AV Detection: 95%
Labeled as: Trojan.Generic (/search?query=vxfamily%3A"Trojan.Generic")

El nombre del ransomware es WannaCry y consiste en un software que bloquea los archivos del usuario para luego exigir un pago (AKA rescate) a cambio de recuperar (descifrar) los archivos. El Hash no coincide con el generado en el análisis estático.

- **Muestre las capturas de pantalla sobre los mensajes que este malware presenta al usuario. ¿Se corresponden las sospechas con el análisis realizado en el punto 7?**


Ooops, your important files are encrypted.
If you see this text, but don't see the "Wana DecryptOr" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.
If you need your files you have to run the decrypt software.
Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.
Run and follow the instructions!