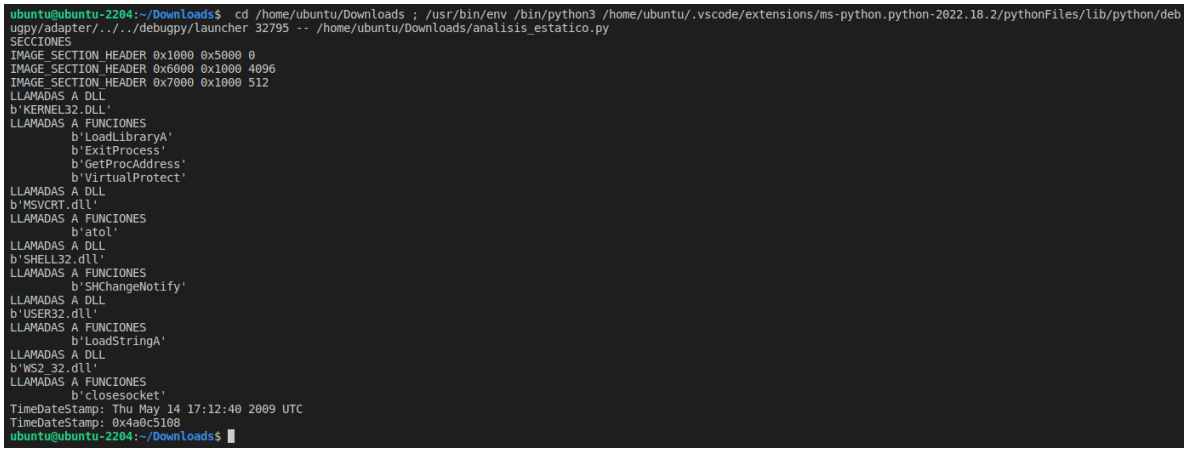
Javier Hernández 19202

Hoja de trabajo – Análisis de Malware

Parte 1 – análisis estático 1.

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?

   Ejecutable: sample_qwrty_dk2



```
ubuntu@ubuntu-2204:~/Downloads$  cd /home/ubuntu/Downloads ; /usr/bin/env /bin/python3 /home/ubuntu/.vscode/extensions/ms-python.python-2022.18.2/pythonFiles/lib/python/debu
gpy/adapter/../../debugpy/launcher 32795 -- /home/ubuntu/Downloads/analisis_estatico.py
SECCIONES
IMAGE_SECTION_HEADER 0x1000 0x5000 0
IMAGE_SECTION_HEADER 0x6000 0x1000 4096
IMAGE_SECTION_HEADER 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
ubuntu@ubuntu-2204:~/Downloads$
```

   Ejecutable: sample_vg655_25th.exe

```
ubuntu@ubuntu-2204:~/Downloads$  cd /home/ubuntu/Downloads ; /usr/bin/env /bin/python3 /home/ubuntu/.vscode/extensions/ms-python.python-2022.18.2/pythonFiles/lib/python/debu
gpy/adapter/../../debugpy/launcher 38699 -- /home/ubuntu/Downloads/analisis_estatico.py
SECCIONES
IMAGE_SECTION_HEADER 0x1000 0x69b0 28672
IMAGE_SECTION_HEADER 0x8000 0x5f70 24576
IMAGE_SECTION_HEADER 0xe000 0x1958 8192
IMAGE_SECTION_HEADER 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'
```

   La primera diferencia es que el primero tiene más llamadas a DLLs, 5, y la segunda solo son 4. Segundo, es que la segunda hace más llamadas a funciones en cada DLL, y pasa lo mismo con las APIs. Y sí hay sospechas con las cantidades porque son muchas llamadas de diferencia y algunas tienen nombres bastantes sospechosos.

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.

   Significa que esas secciones han sido comprimidas, puede que se hayan comprimido con UPX o cualquier otra herramienta.

```
ubuntu@ubuntu-2204:~/Downloads$ upx-ucl -d MALWR/sample_qwrty_dk2
                       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

Unpacked 1 file.
```

3. 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.

API	CATEGORÍA
CloseHandle	Copy/Delete Files
WriteFile	Read/Write Files
GetFileAttributesW	Get File Information
CreateFileA	Read/Write Files
GetFileSize	Get File Information
SetFileAttributesW	Change File Attributes
GetFileAttributesW	Get File Information
GetFullPathNameA	Get File Information
…	…

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

```
ubuntu@ubuntu-2204:~/Downloads$ sha256sum ./MALWR/sample_vg655_25th.exe
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa  ./MALWR/sample_vg655_25th.exe
ubuntu@ubuntu-2204:~/Downloads$
```

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

   Su propósito es la autorización y autenticación de usuarios, administración de cuentas y gestionar permisos y derechos. Por lo tanto, no debe ser eliminada para evitar daños al sistema.

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

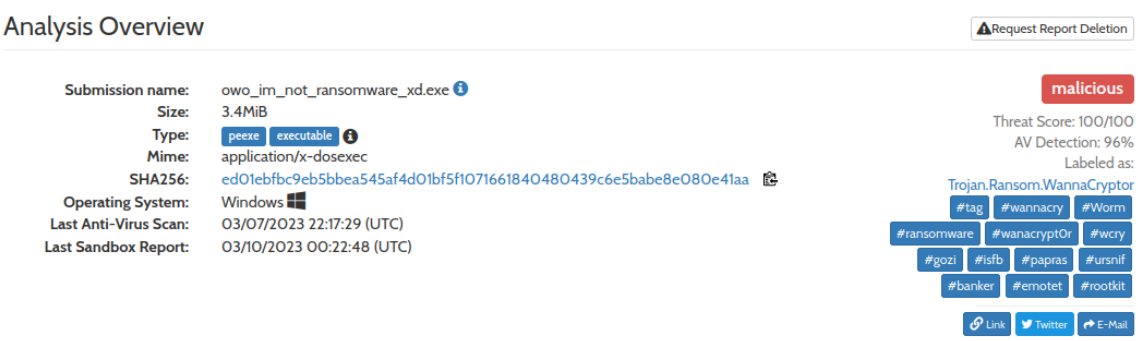
   Su propósito es liberar recursos relacionados al contexto, es decir que eso estuvo o está encriptado. Por eso se usa para liberar o desencriptar. Es importante tener en cuenta que no liberar correctamente el contexto de criptografía puede tener consecuencias graves, incluyendo posibles vulnerabilidades de seguridad en el sistema.

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.

   El archivo sí es sospechoso por la información obtenida. Ahora podemos asumir que su propósito es manipular archivos encriptados y obtenerlos, ya sea una copia o transferirlos a otro lugar. También gestiona nuestra cuenta de usuario obteniendo información, puede ser credenciales y cosas por el estilo. Es como un ransomware.

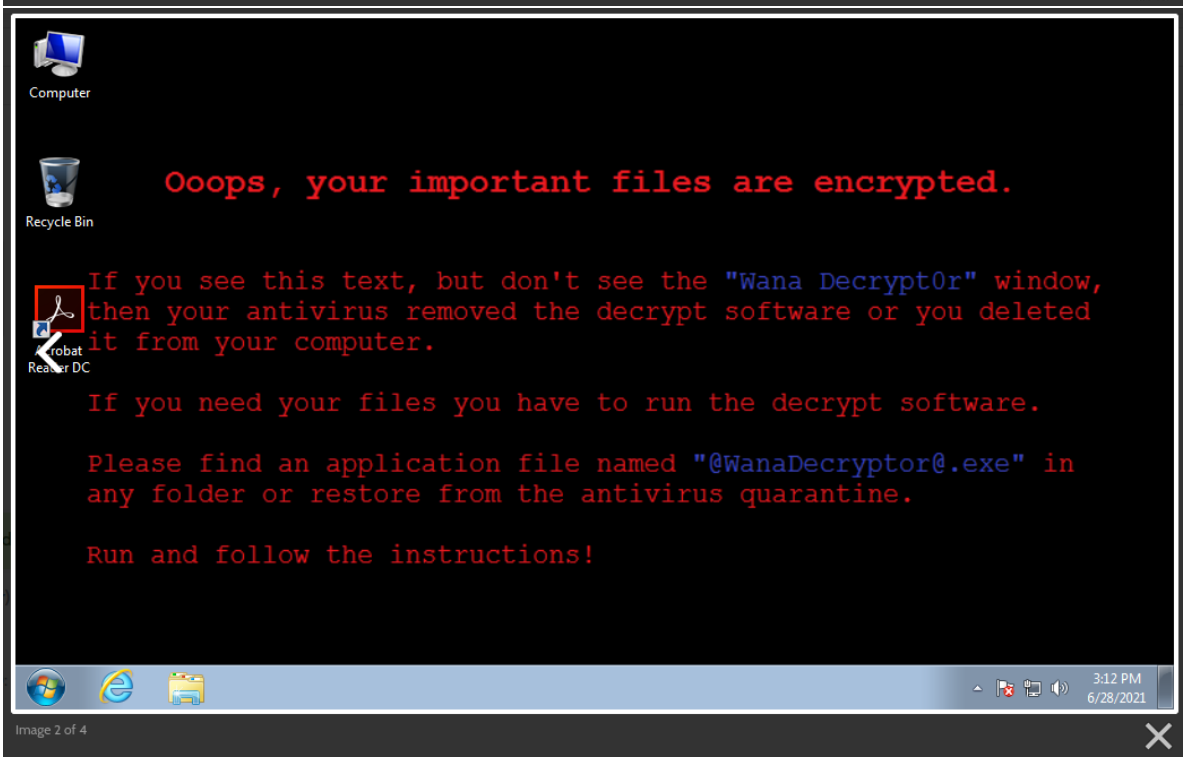
Parte 2 – análisis dinámico

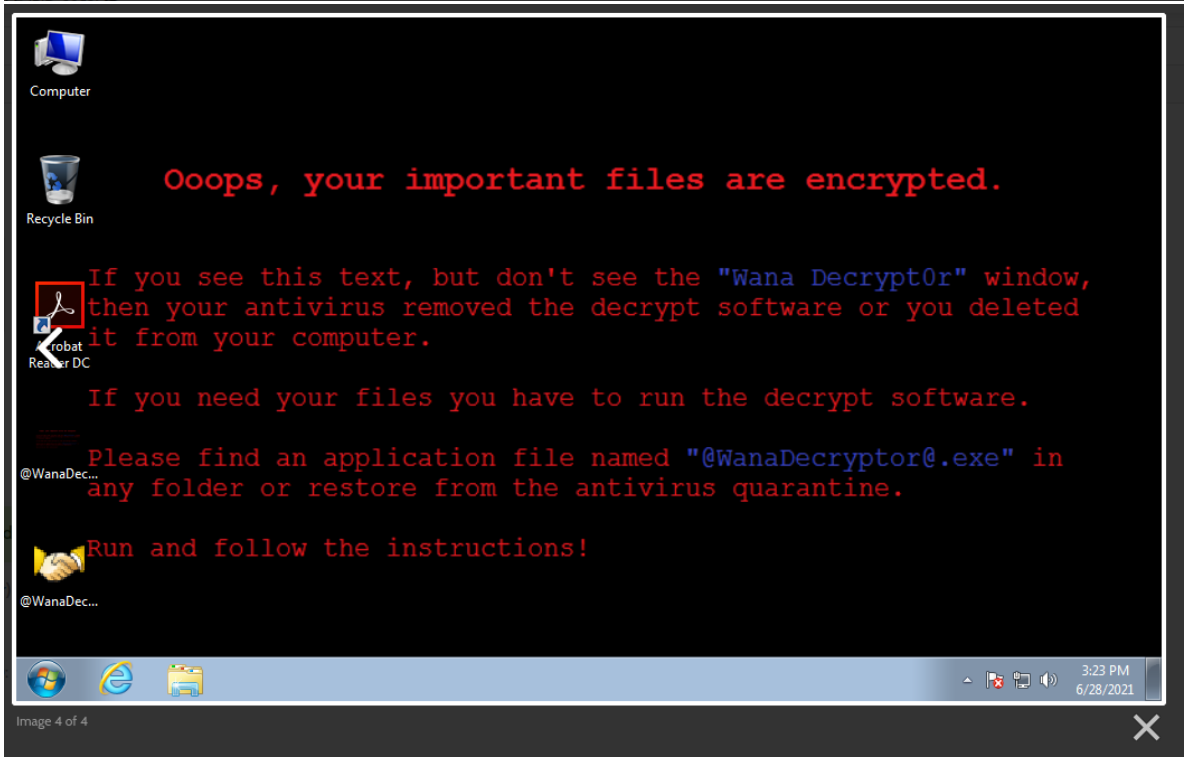
8. Utilice la plataforma de análisis dinámico https://www.hybrid-analysis.com y cargue el archivo “sample_vg655_25th.exe”. ¿Se corresponde el HASH de la plataforma con el generado? ¿Cuál es el nombre del malware encontrado? ¿Cuál es el propósito de este malware?



El HASH de la plataforma sí corresponde al generado.
Nombre del malware: owo_im_not_ransomware_xd.exe
Labeled as: Trojan.Ransom.WannaCryptor
Propósito: Ransomware.

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?





Sí corresponden las sospechas del punto 7.