Universidad del Valle de Guatemala
Facultad de Ingeniería
Departamento de Ciencias de la Computación
CC3094 Security Data Science
Catedrático: Jorge Yass
Ciclo 1 de 2023

HDT #2
Malware detection

Diego Arredondo 19422

Guatemala, 09 de marzo de 2023

1. Utilice la herramienta pefile para examinar el PE header y obtenga las DLL y las APIs que cada uno de los ejecutables utiliza. ¿Qué diferencias observa entre los ejemplos? ¿Existe algún indicio sospechoso en la cantidad de DLLs y las APIs llamadas?

File: sample_qwrty_dk2

```
DLL:
b'KERNEL32.DLL'
APIs:
b'LoadLibraryA'
b'ExitProcess'
b'GetProcAddress'
b'VirtualProtect'

DLL:
b'MSVCRT.dll'
APIs:
b'atol'

DLL:
b'SHELL32.dll'
APIs:
b'SHChangeNotify'

DLL:
b'USER32.dll'
APIs:
b'LoadStringA'

DLL:
b'WS2_32.dll'
APIs:
b'closesocket'
```

File: sample_vg655_25th.exe

Existe una diferencia notable en cuanto a las llamadas al API de cada uno de los archivos, el archivo sample_qwrty_dk2 hace muchas menos llamadas al API que el archivo sample_vg655_25th.exe, pero esto aun no es un indicio que alguno de los dos puede ser malicioso, pero si es sospechosa tanta llamada al API.

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.

File: sample_qwrty_dk2

```
Sections:
Name:  b'UPX0\x00\x00\x00\x00' Virtual Address:  0x1000 Misc_VirtualSize:  0x5000 SizeOfRawData:  0
Name:  b'UPX1\x00\x00\x00\x00' Virtual Address:  0x6000 Misc_VirtualSize:  0x1000 SizeOfRawData:  4096
Name:  b'.rsrc\x00\x00\x00' Virtual Address:  0x7000 Misc_VirtualSize:  0x1000 SizeOfRawData:  512
```

File: sample_vg655_25th.exe

```
Sections:
Name:  b'.text\x00\x00\x00' Virtual Address:  0x1000 Misc_VirtualSize:  0x69b0 SizeOfRawData:  28672
Name:  b'.rdata\x00\x00' Virtual Address:  0x8000 Misc_VirtualSize:  0x5f70 SizeOfRawData:  24576
Name:  b'.data\x00\x00\x00' Virtual Address:  0xe000 Misc_VirtualSize:  0x1958 SizeOfRawData:  8192
Name:  b'.rsrc\x00\x00\x00' Virtual Address:  0x10000 Misc_VirtualSize:  0x349fa0 SizeOfRawData:  3448832
```

UPX son las siglas de Ultimate Packer for Executables, el cual es un empaquetador simple, esto significa que las llamadas del archivo sample_qwrty_dk2 están empaquetadas. El UPX también se usa para empaquetar malware, aunque no es muy recomendado por los autores de malware. Este paquete puede "ocultar" ciertas llamadas al API, para que no se note que es un malware como tal.

File: sample_qwrty_dk2 unpacked

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.

File: sample_qwrty_dk2

API	Categoría
CloseHandle	Copy/Delete Files
GetShortPathName	Get File Information
WriteFile	Read/Write Files

File: sample_vg655_25th.exe

API	Categoría
CreateFileA	Read/Write Files
CloseHandler	Copy/Delete Files
WriteFile	Read/Write Files
CopyFileA	Read/Write Files
SetFilesAttributes	Change File Attributes
GetTempPathW	Get File Information
GetFullPathNameA	Get File Information
GetFileAttributesA	Get File Information
GetFileSizeEx	Get File Information
GetFileAttributesW	Get File Information
GetFileSize	Get File Information

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

```
SHA256:
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
```

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

El propósito de este DLL es dar servicios y dar acceso a los componentes de Windows, este DLL es un Advanced Windows 32 Base API y se considera un archivo de Win32 DLL. Como se puede observar para el archivo sample_vg655_25th.exe, hace varias llamadas al API a servicios de este DLL.

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

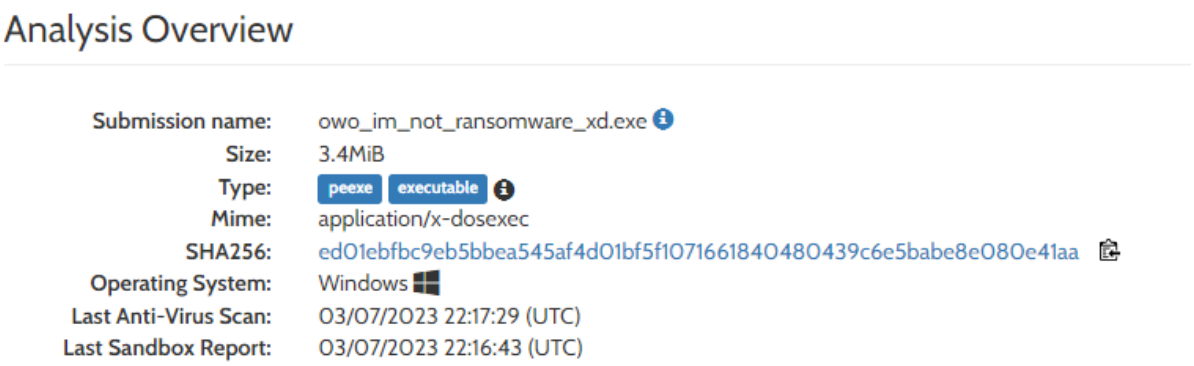
Este API es el identificador de un proveedor de servicios criptográficos (CSP) y un contenedor de claves. Y Su propósito es liberar algún identificador de un CSP y las llaves que este contenga.

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.

Efectivamente, puede decirse que este archivo es sospechoso por que este usa el CryptReleaseContext, con el cual puede capturar datos del usuario y más sospechoso por todas las APIS sospechosas que presenta este archivo.

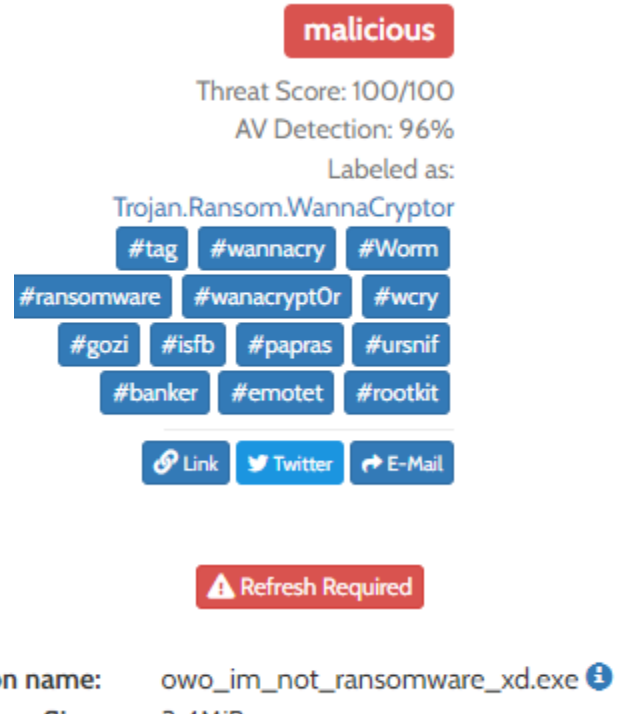
Parte 2 – análisis dinámico

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?



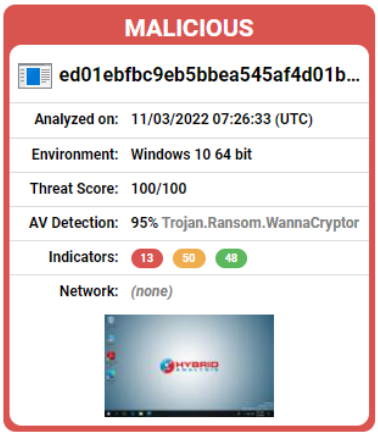

```
SHA256:
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
```

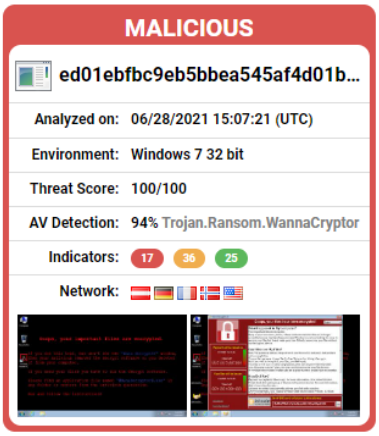
Sí, el Hash corresponde con el generado.

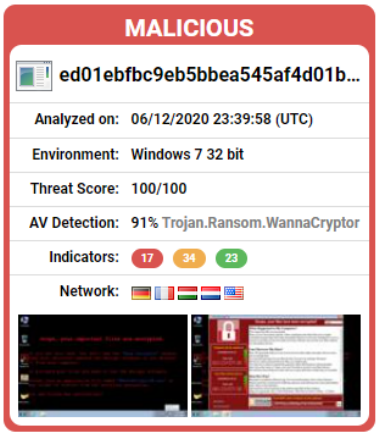


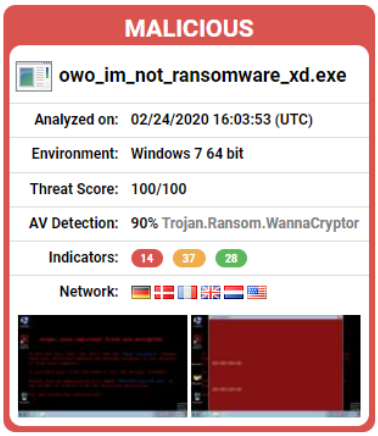
El archivo esta Categorizado como un Trojan.Ransom.WannaCryptor y el nombre del malware es owo_im_not_ransomware_xd.exe.

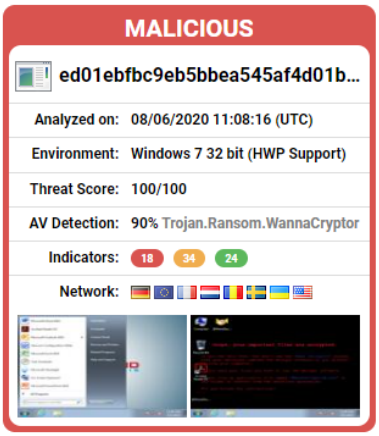
9. Muestre las capturas de pantalla sobre los mensajes que este malware presenta a usuario. ¿Se corresponden las sospechas con el análisis realizado en el punto 7?

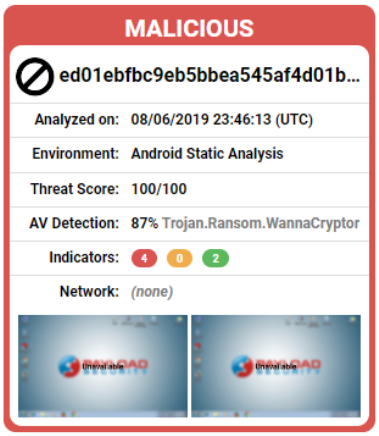


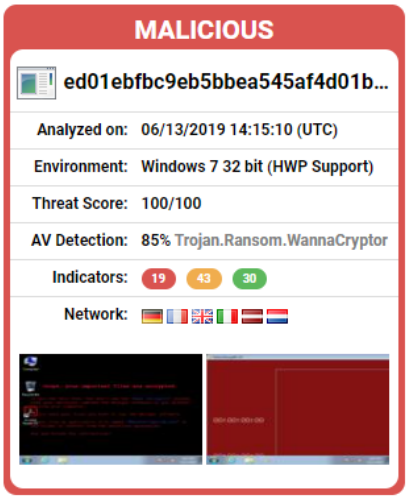


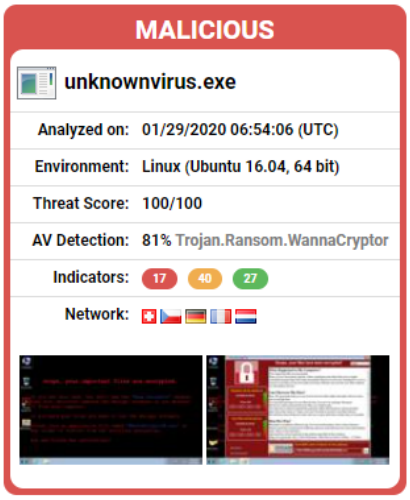












Y efectivamente, como se pueden ver en todas la imágenes del análisis dinámico, las sospechas del Inciso 7 fueron correctas.