



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

Hoja de trabajo 2

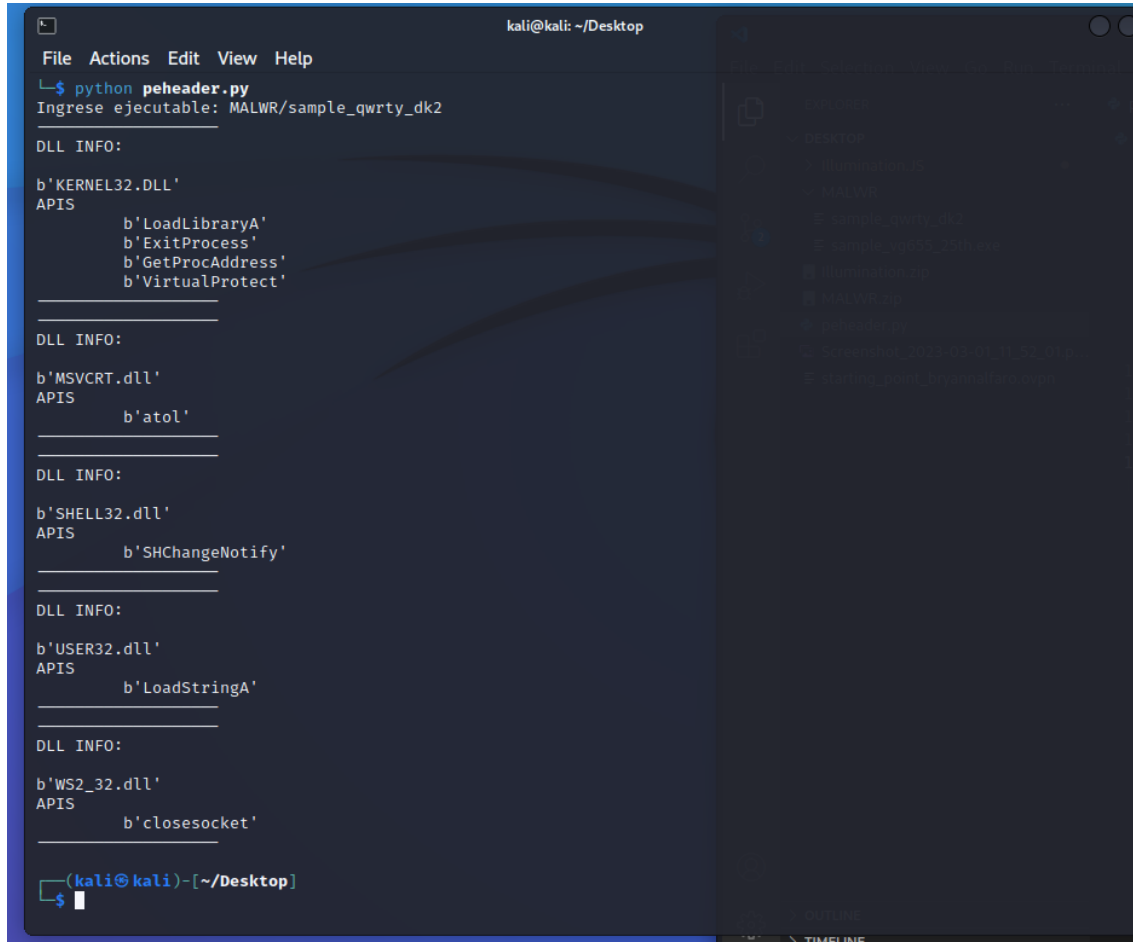
Bryann Alfaro 19372

Guatemala, 7 de marzo de 2023

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?

Ejecutable: sample_qwrty_dk2



```
kali@kali: ~/Desktop
File Actions Edit View Help
└─$ python peheader.py
Ingrese ejecutable: MALWR/sample_qwrty_dk2

DLL INFO:
b'KERNEL32.DLL'
APIS
    b'LoadLibraryA'
    b'ExitProcess'
    b'GetProcAddress'
    b'VirtualProtect'

DLL INFO:
b'MSVCRT.dll'
APIS
    b'atol'

DLL INFO:
b'SHELL32.dll'
APIS
    b'SHChangeNotify'

DLL INFO:
b'USER32.dll'
APIS
    b'LoadStringA'

DLL INFO:
b'WS2_32.dll'
APIS
    b'closesocket'

(kali@kali)-[~/Desktop]
└─$
```

Ejecutable: sample_vg655_25th.exe



kali@kali: ~/Desktop

File Actions Edit View Help

(kali@kali)-[~/Desktop]

\$ python peheader.py

Ingrese ejecutable: MALWR/sample_vg655_25th.exe

DLL INFO:

b'KERNEL32.dll'

APIS

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'

```

DLL INFO:

b'USER32.dll'
APIS
    b'wsprintfA'

DLL INFO:

b'ADVAPI32.dll'
APIS
    b'CreateServiceA'
    b'OpenServiceA'
    b'StartServiceA'
    b'CloseServiceHandle'
    b'CryptReleaseContext'
    b'RegCreateKeyW'
    b'RegSetValueExA'
    b'RegQueryValueExA'
    b'RegCloseKey'
    b'OpenSOManagerA'

DLL INFO:

b'MSVCRT.dll'
APIS
    b'realloc'
    b'fclose'
    b'fwrite'
    b'fread'
    b'fopen'
    b'sprintf'
    b'rand'
    b'srand'
    b'strcpy'
    b'memset'
    b'strlen'
    b'wscat'
    b'wcslen'
    b'__CxxFrameHandler'
    b'??3@VAXPAK@Z'
    b'memcmp'
    b'_except_handler3'
    b'_local_unwind2'
    b'wcsrchr'
    b'wprintf'
    b'??2@VAPAXI@Z'
    b'memcpy'
    b'strcmp'
    b'strchr'
    b'__p__argv'
    b'__p__argc'
    b'_stricmp'
    b'free'
    b'malloc'
    b'??0exception@@QAE@ABV0@@Z'
    b'??1exception@@QAE@XZ'
    b'??0exception@@QAE@ABQ80@Z'
    b'_CxxThrowException'
    b'calloc'
    b'strcat'
    b'_mbstr'
    b'??1type_info@@QAE@XZ'
    b'_exit'
    b'_XcptFilter'
    b'_exit'
    b'_acndln'
    b'__getmainargs'
    b'_initterm'
    b'_setusermatherr'
    b'_adjust_fdiv'
    b'__p__comode'
    b'__p__fmode'
    b'__set_app_type'
    b'_controlfp'

```

Discusión: Se observa diferencia notable en la cantidad de llamadas a APIs, en el ejemplar **sample_qwrty_dk2** se notan menos llamadas a APIs, caso contrario de **sample_vg655_25th.exe** en donde se realizan varias llamadas a APIs.

- 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.

```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ python peheader.py
Ingrese ejecutable: MALWR/sample_qwrty_dk2
b'UPX0\x00\x00\x00' 0x1000 0x5000 0
b'UPX1\x00\x00\x00\x00' 0x6000 0x1000 4096
b'.rsrc\x00\x00\x00' 0x7000 0x1000 512

(kali@kali)-[~/Desktop]
$ python peheader.py
Ingrese ejecutable: MALWR/sample_vg655_25th.exe
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

(kali@kali)-[~/Desktop]
$
```

Que algunas secciones tengan como parte de su nombre “upx” en primer lugar significa que el archivo se encuentra empaquetado, por lo que incluso se podrían estar ocultando ciertas llamadas a APIs , lo que explicaría la poca cantidad de llamadas en el inciso anterior en el caso del ejemplar **sample_qwrty_dk2**. Por último, upx nos indica que esta herramienta fue utilizada para el empaquetamiento por lo que puede usarse para desempaquetar el ejecutable.

```
UPX COMES WITH ABSOLUTELY NO WARRANTY; FOR DETAILS VISIT https://upx.github.io

(kali@kali)-[~/Desktop]
$ upx -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

MALWR/sample_qwrty_dk2
File size      Ratio      Format      Name
-----
8192 ←      5632      68.75%      win32/pe      sample_qwrty_dk2

Unpacked 1 file.

(kali@kali)-[~/Desktop]
$
```

```
(kali@kali)-[~/Desktop]
$ python peheader.py
Ingrese ejecutable: MALWR/sample_qwrty_dk2
```

DLL INFO:

```
b'KERNEL32.DLL'
APIS
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'
b'SetPriorityClass'
b'lstrcatA'
b'lstrcpyA'
b'GetEnvironmentVariableA'
b'GetShortPathNameA'
b'GetModuleFileNameA'
b'GetStartupInfoA'
b'GetModuleHandleA'
```

DLL INFO:

```
b'MSVCRT.dll'
APIS
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'
```

```

DLL INFO:
b'SHELL32.dll'
APIS
    b'ShellExecuteExA'
    b'SHChangeNotify'

DLL INFO:
b'USER32.dll'
APIS
    b'LoadStringA'

DLL INFO:
b'WS2_32.dll'
APIS
    b'htons'
    b'connect'
    b'socket'
    b'WSAStartup'
    b'send'
    b'ineta_addr'
    b'recv'
    b'closesocket'

b'.text\x00\x00\x00' 0x1000 0xea6 4096
b'.rdata\x00\x00' 0x2000 0x67e 2048
b'.data\x00\x00\x00' 0x3000 0x628 512
b'.rsrc\x00\x00\x00' 0x4000 0x80 512

(kali@kali)~/Desktop
$

```

Al desempaquetar se puede observar claramente que existían más llamadas a APIs que no estaban siendo mostradas anteriormente en el ejemplar **sample_qwrty_dk2**.

- 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.

Ejecutable: **sample_qwrty_dk2**

Llamada a API	Categoría
CloseHandle	Copy/Delete Files, Read/Write Files
WriteFile	Read/Write Files
GetShortPathNameA	Get File Information

Ejecutable: **sample_vg655_25th.exe**

Llamada API	Categoría
-------------	-----------

GetFileAttributesW	Get File Information
GetFileSizeEx	Get File Information
CreateFileA	Read/Write Files
GetFileSize	Get File Information
WriteFile	Read/Write Files
SetFileAttributesW	Change File Attributes
GetTempPathW	Get File Information
GetFileAttributesA	Get File Information
GetFullPathNameA	Get File Information
CopyFileA	Copy/Delete Files
CloseHandle	Copy/Delete Files Read/Write Files

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

```
(kali@kali)-[~/Desktop]
$ python hash.py
Enter the input file name: MALWR/sample_vg655_25th.exe
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

(kali@kali)-[~/Desktop]
$
```

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

advapi32.dll forma parte de la biblioteca avanzada de los servicios de Windows. Provee el acceso a los componentes básicos avanzados de Windows como lo es el administrador de servicios y el registro. Esto se puede comprobar al observar las funciones que se llaman como CreateService u OpenService, lo cual indica que hace manipulación de servicios. (Reddy, 2019) (ProcessLibrary, s.f)


```

DLL INFO:
b'USER32.dll'
APIS
    b'wsprintfA'

DLL INFO:
b'ADVAPI32.dll'
APIS
    b'CreateServiceA'
    b'OpenServiceA'
    b'StartServiceA'
    b'CloseServiceHandle'
    b'CryptReleaseContext'
    b'RegCreateKeyW'
    b'RegSetValueExA'
    b'RegQueryValueExA'
    b'RegCloseKey'
    b'OpenSManagerA'

DLL INFO:
b'MSVCRT.dll'
APIS
    b'realloc'
    b'fclose'
    b'fwrite'
    b'fread'

```

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

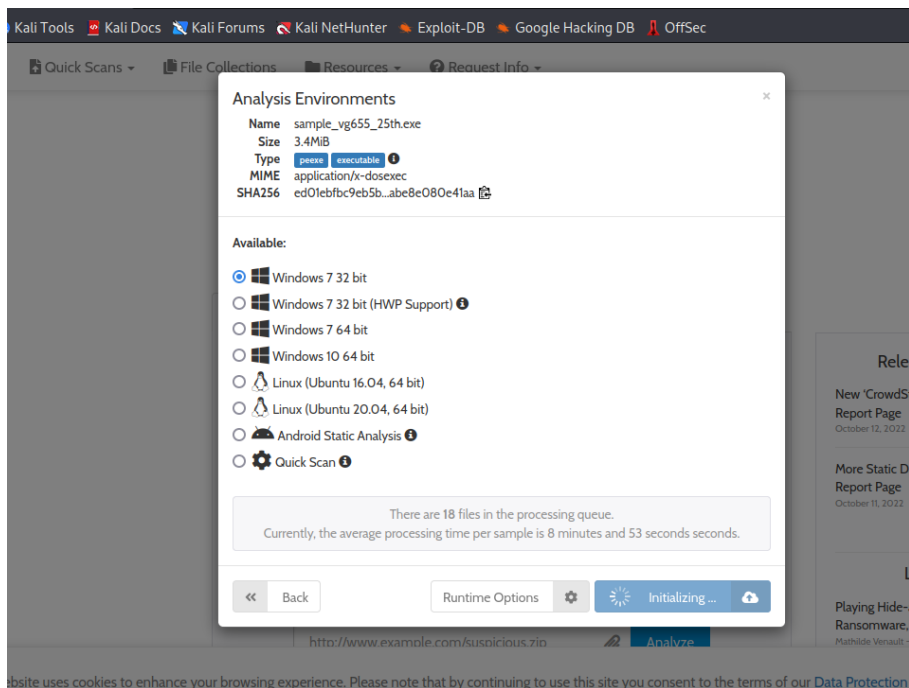
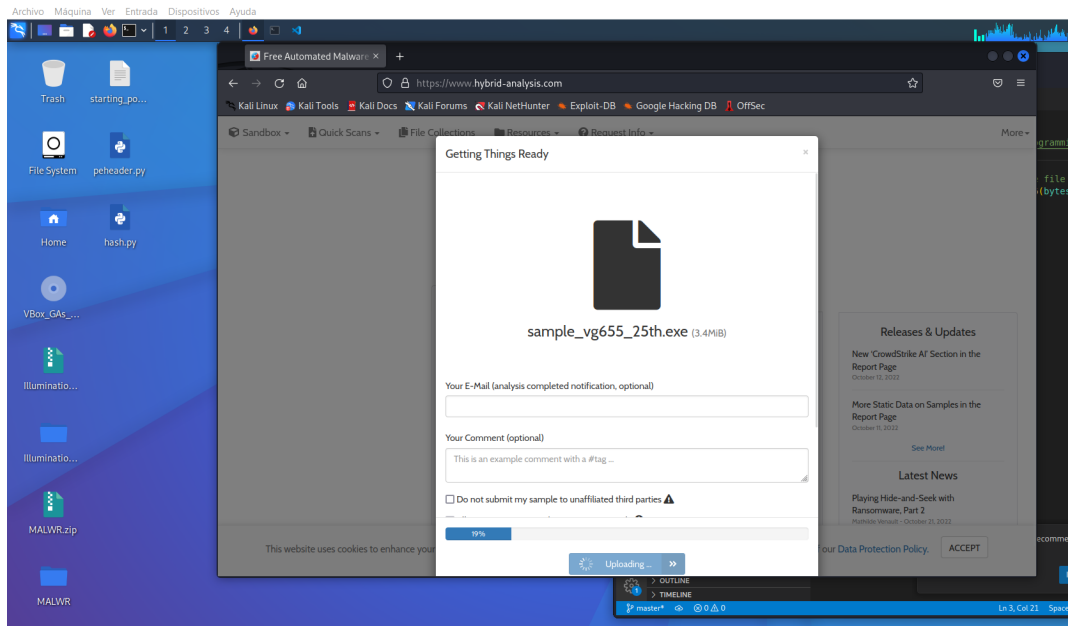
La API CryptReleaseContext se utiliza para poder liberar el identificador de un CSP (Cryptographic Service Provider) y un contenedor de llaves. Esto podría indicar que está realizando algún tipo de encriptación de datos. (Microsoft, 2021)

7. 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

Con la información recopilada, este archivo es sospechoso y su propósito podría ser el de capturar datos y encriptarlos tipo ransomware, debido al uso de la API CryptReleaseContext y la tabla de propósitos en donde se observa manipulación de archivos.

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?



Analysis Overview

Submission name: owo_im_not_ransomware_xd.exe ⓘ
Size: 3.4MiB
Type: peexe executable ⓘ
Mime: application/x-dosexec
SHA256: ed01ebfbc9eb5b545af4d01bf5f1071661840480439c6e5babe8e080e41aa ⓘ
Operating System: Windows
Last Anti-Virus Scan: 02/15/2023 11:04:30 (UTC)
Last Sandbox Report: 12/19/2022 08:54:11 (UTC)

⚠ Request Report Deletion

malicious

Threat Score: 100/100

AV Detection: 96%

Labeled as:

Trojan.Ransom.WannaCryptor

#tag #wannacry #Worm

#ransomware #wannacryptOr #wcry

#gozi #isfb #paprass #ursnif

#banker #emotet #rootkit

🔗 Link 🐦 Twitter ✉ E-Mail

Analysis

Anti-Vir

Related

Falcon S

Incident

Comm

Back to 1

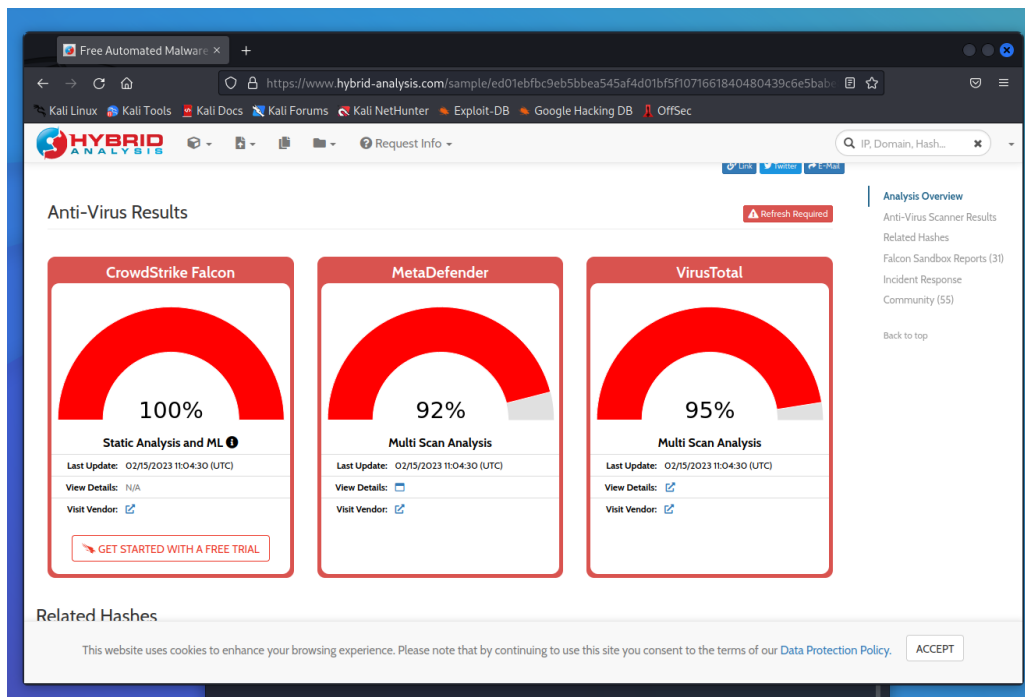
Anti-Virus Results

⚠ Refresh Required

CrowdStrike Falcon

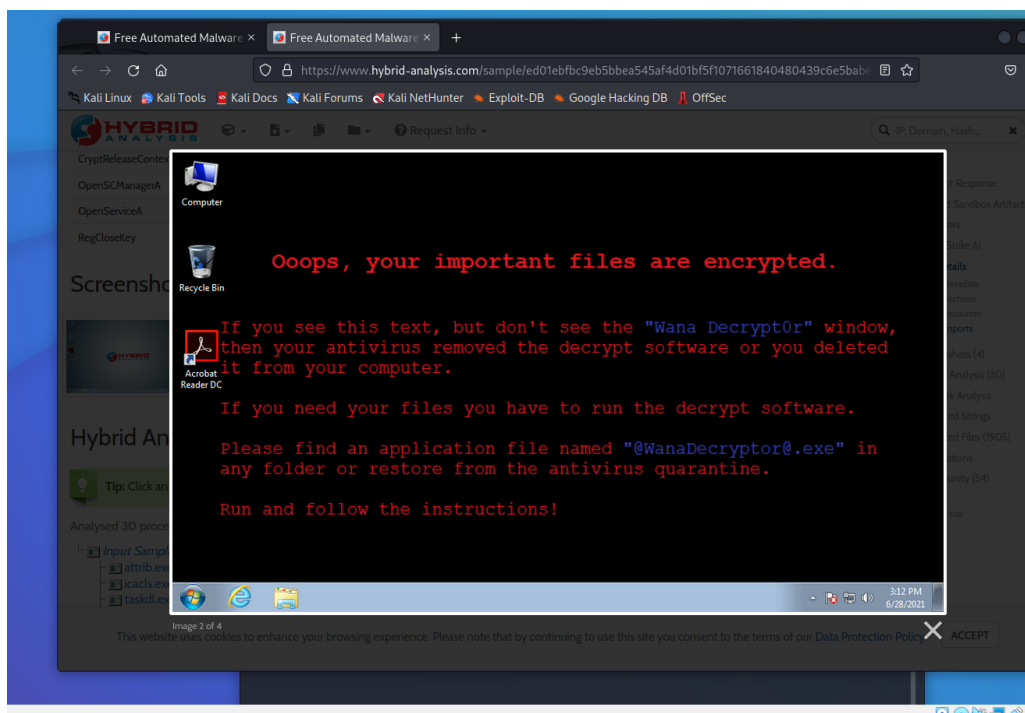
MetaDefender

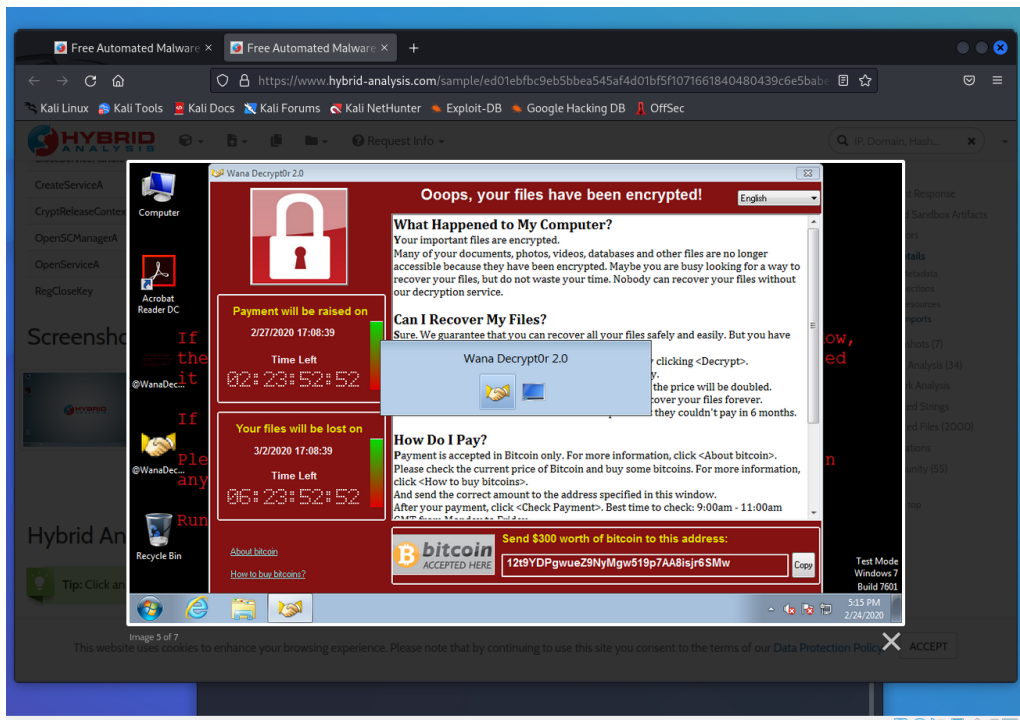
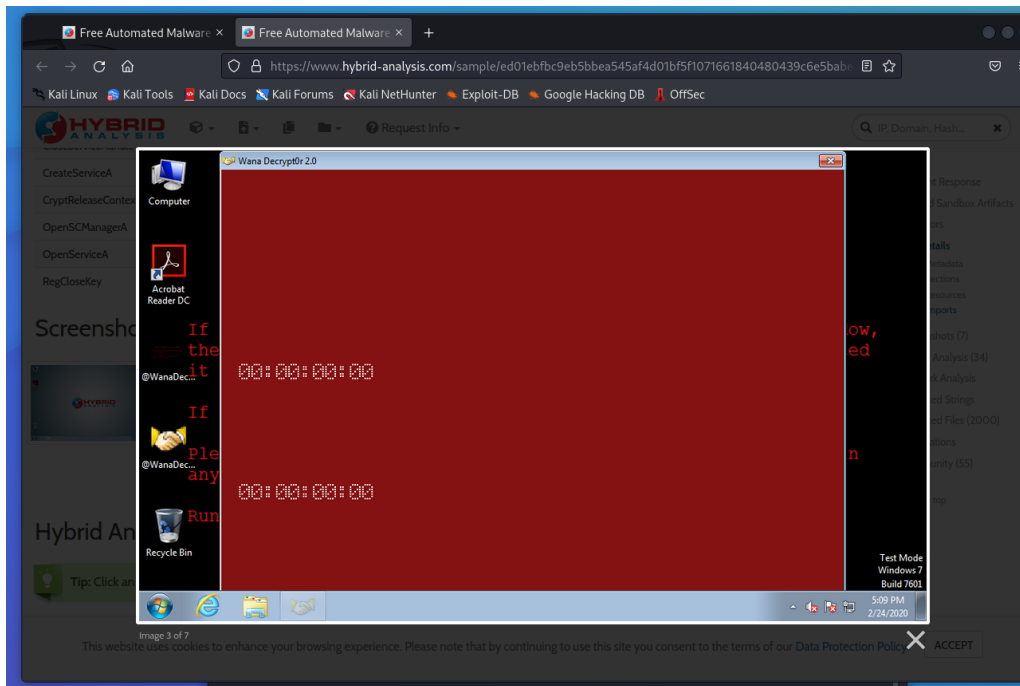
VirusTotal



El hash sí corresponde con el obtenido anteriormente. El archivo fue etiquetado como Trojan.Ransom.WannaCryptor y el submission name es: owo_im_not_ransomware_xd.exe. El propósito de este malware (Ransomware WannaCry) es cifrar archivos que puedan ser considerados “valiosos” y se pide una recompensa con tal de recuperar los mismos. (Kaspersky, s.f)

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?







Las sospechas sí corresponden a lo analizado en el inciso 7, ya que efectivamente era un ransomware del tipo WannaCry, el cual encripta datos.

Literatura citada:

ProcessLibrary. (s.f). advapi32.dll. Extraído de:
<https://www.processlibrary.com/es/directory/files/advapi32/22015/>

Reddy, K. (2019). Basic Static analysis of malware and common DLL. Extraído de:
<https://medium.com/mrx-007/basic-static-analysis-of-malware-and-common-dll-ef9455d49968>

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

Kaspersky. (s.f). ¿Qué es el ransomware WannaCry?. Extraído de:
<https://www.kaspersky.es/resource-center/threats/ransomware-wannacry>