

LABORATORIO 4

Clasificación de Malware

Gerardo Méndez Alvarez 18239

Parte 1 - Análisis Estático

Obtención de llamadas a DDL y API e información de Sections

1 sample_qwrty_dk2

```
NO. OF API CALLS: 8  
NO. OF DLL CALLS: 5
```

2 sample_vg655_25th

```
NO. OF API CALLS: 114  
NO. OF DLL CALLS: 4
```

→ *¿Qué diferencias observa entre los ejemplos?*

Podemos observar que la principal diferencia se encuentra en la cantidad de llamadas a API que hay para cada archivo.

→ *¿Existe algún indicio sospechoso en la cantidad de DLLs y las APIs llamadas?*

Es sospechoso que existan tan pocas llamadas a APIs por parte del primer archivo.

Obtención de secciones del PE Header

```
*****sample_qwrty_dk2*****  
SECTION NAMES: ['UPX0', 'UPX1', '.rsrc']
```

```
*****sample_vg655_25th.exe*****  
SECTION NAMES: ['.text', '.rdata', '.data', '.rsrc']
```

→ *¿Qué significa que algunas secciones tengan como parte de su nombre “upx”?*

En el primer archivo, existen dos secciones con los nombres UPX. En este caso, esto significa que estas secciones fueron empaquetadas, y que la “verdadera” información del ejecutable no es visible al 100%.

APIs sospechosas

→ *¿En qué categoría sospechosas pueden clasificarse estos ejemplos en base a algunas de las llamadas a las APIs que realizan?*

Comportamiento	Categoría de Malware	Llamadas a API
1	Búsqueda de archivos para infectar	-
2	Copiar/Eliminar archivos	CloseHandle, CreateFile
3	Obtener información de archivos	GetShortPathName, GetTempPath, GetFullPathName, GetFileAttributes
4	Mover archivos	-
5	Leer/Escribir archivos	WriteFile, CreateFile
6	Cambio de atributos en archivos	SetFileAttributes

Podemos ver que la categoría que más llamadas a API tiene es la de Obtener información de archivos. Con esto podemos darnos una idea de qué es lo que estos archivos pretenden.

Obtención de Hash SHA 256

```
*****sample_vg655_25th.exe*****  
.text  
SHA 256 55cda830ff2543783350fb781ed2bf77e72aa123134d2513acfb944487773054  
.rdata  
SHA 256 a2acc94d242d28b6dd0a0859ec59ecc7f6b98d4ea09346b819d486b8827d2d79  
.data  
SHA 256 110357de37bd422f6c68b66035e4652b99767819353f4c398953249a930fa823  
.rsrc  
SHA 256 418c45aa8ad5b74ea7a820a4cf19b2fbc688502752d600a7800d3cbe1d058e44  
SECTION NAMES: ['.text', '.rdata', '.data', '.rsrc']
```

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

El nombre de esta DLL corresponde a: Advanced Windows 32 Base API. Provee acceso a funcionalidades avanzadas que vienen con el kernel. Además, es responsable del Windows registry, reiniciar y/o apagar el sistema, así como iniciar y detener servicios de Windows y el manejo de los usuarios en el sistema.

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

La función **CryptReleaseContext** devuelve el handle de un proveedor de servicios criptográficos (CSP) y el contenedor de llaves. Hay un contador de referencia que disminuye por 1 cada vez que se utiliza esta función, y que al llegar a 0 deja de aceptar llamadas a ese CSP, dado que el contexto fue liberado por completo.

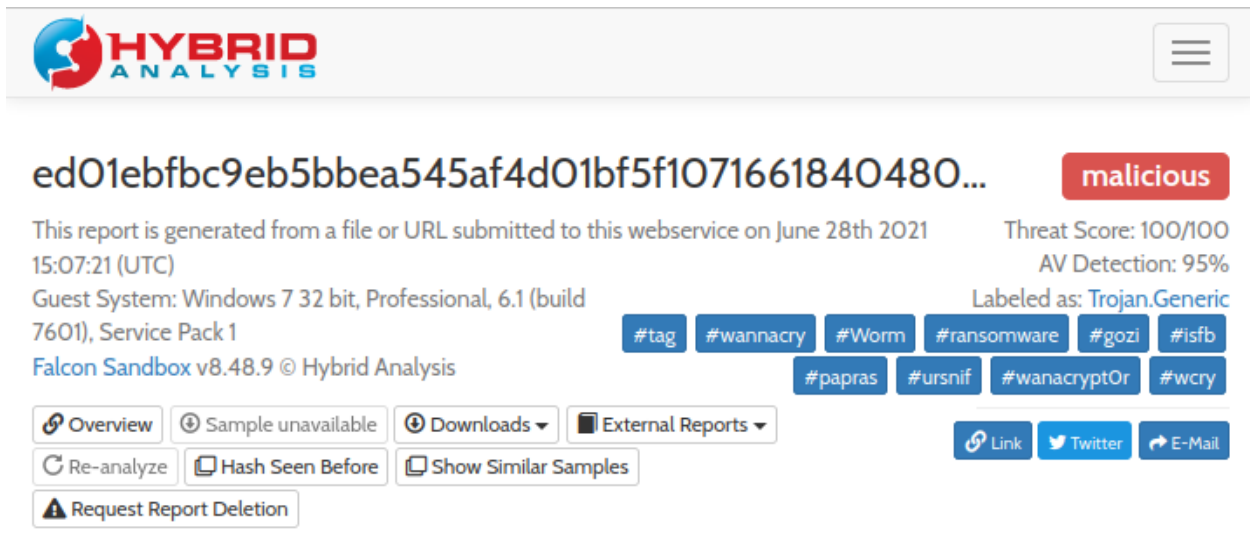
Con la información recopilada hasta el momento, indique para el archivo “sample_vg655_25th.exe” si es sospechoso o no, y cuál podría ser su propósito.

El archivo es sospechoso, ya que es raro que algún ejecutable utilice estas llamadas a las APIs y las DLL, más aún en conjunto. Por lo que hemos visto de comportamiento en algunos tipos de malware, puede tratarse de un virus que bloquee algunas funciones del sistema como parte del ataque.

Parte 2 - Análisis Dinámico

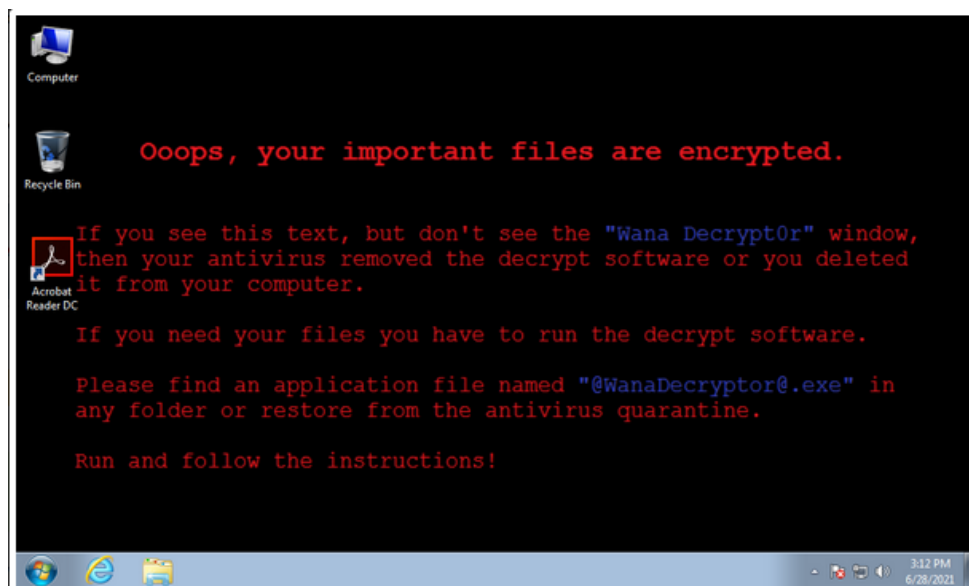
¿Se corresponde el HASH de la plataforma con el generado? ¿Cuál es el nombre del malware encontrado? ¿En qué consiste este malware?

Los hash no concuerdan con los generados anteriormente. El malware es de tipo Ransomware y el nombre de este método es WannaCry. Lo que hace es cifrar los archivos de la computadora, y para descifrarlos el usuario necesita enviar un pago a los atacantes. Los atacantes reciben un acceso remoto al equipo.



The screenshot shows the Hybrid Analysis web interface. At the top is the Hybrid Analysis logo. Below it, the file hash **ed01ebfbc9eb5bbea545af4d01bf5f1071661840480...** is displayed next to a red **malicious** label. The report details include: "This report is generated from a file or URL submitted to this webservice on June 28th 2021 15:07:21 (UTC)", "Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1", and "Falcon Sandbox v8.48.9 © Hybrid Analysis". The "Threat Score" is 100/100 and "AV Detection" is 95%. It is labeled as "Trojan.Generic". A series of blue tags are shown: #tag, #wannacry, #Worm, #ransomware, #gozi, #isfb, #papas, #ursnif, #wanacryptOr, and #wcry. At the bottom, there are several buttons: Overview, Sample unavailable, Downloads, External Reports, Re-analyze, Hash Seen Before, Show Similar Samples, Request Report Deletion, Link, Twitter, and E-Mail.

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?





Las capturas muestran, efectivamente, el bloqueo de acceso a cierta información personal del usuario, la cual puede ser accedida únicamente haciendo un pago en Bitcoin a los atacantes.