

Fernando José Garavito Ovando 18071

Análisis de Malware

La primera parte consiste en el análisis de dos ejecutables de Windows proporcionados. Se proporciona una carpeta con el nombre MALWR2.zip en CANVAS, la cual posee la contraseña *infected*

Se sugiere utilizar una VM con Linux para trabajar. Se debe descargar el archivo y descomprimirlo en la ubicación deseada. Luego se debe descomprimirlo y NO se debe manipular manualmente ningún archivo, de hacerlo se corre el riesgo de ejecutarlo e infectarse.

NOTA: se proporcionan ejemplos reales de malware, para efectos de aplicar los conocimientos académicos de análisis estático y dinámico de malware, y es responsabilidad del alumno(a) cualquier uso adicional que no sea el indicado en este laboratorio. Luego de finalizar el laboratorio se deben eliminar todos los ejemplares.

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?

El archivo que se otorgó como sample_qwrty_dk2 puede hacer muchas llamadas tanto al shell como al kernel. Pienso que tienen diferencia en cuanto al upx. Además de la cantidad de llamadas que se utilizan.

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.

Bueno el UPX como tal va a reducir el tamaño de los archivos. Básicamente estaríamos comprimiendo. Reducir el tiempo de carga de la red, el espacio del disco duro y sus diferentes costos de distribución.

3. Según el paper “Towards Understanding Malware Behaviour by the Extraction of API Calls”, ¿en que 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.

Towards Understanding Malware Behaviour by the Extraction of API calls

Mamoun Alazab
Internet Commerce Security
Laboratory (ICSL)
University of Ballarat
m.alazab@ballarat.edu.au

Sitalakshmi Venkataraman
Internet Commerce Security
Laboratory (ICSL)
University of Ballarat
s.venkataraman@ballarat.edu.au

Paul Watters
Internet Commerce Security
Laboratory (ICSL)
University of Ballarat
p.watters@ballarat.edu.au

Abstract— One of the recent trends adopted by malware authors is to use packers or software tools that instigate code obfuscation in order to evade detection by antivirus scanners. With evasion techniques such as polymorphism and metamorphism malware is able to fool current detection techniques. Thus, security researchers and the anti-virus industry are facing a herculean task in extracting payloads hidden within packed executables. It is a common practice to use manual unpacking or static unpacking using some software tools and analyse the application programming interface (API) calls for malware detection. However, extracting these features from the unpacked executables for reverse obfuscation is labour intensive and requires deep knowledge of low-level programming that includes kernel and assembly language. This paper presents an automated method of extracting API call features and analysing them in order to understand their use for malicious purpose. While some research has been conducted in arriving at file birthmarks using API call features and the like, there is a scarcity of work that relates to features in malcodes. To address this gap, we attempt to automatically analyse and classify the behavior of API function calls based on the malicious intent hidden within any packed program. This paper uses four-step methodology for developing a fully automated system to arrive at six main categories of suspicious behavior of API call features.

engines use signatures or 'byte sequences' to detect known malware. These signatures are generated by human experts by disassembling the file and selecting pieces of unique code. Signature-based detection is very effective for known malware, but the noteworthy weakness is the incapability to detect anonymous malware and hence is not effective against "zero day attack" (unknown malware) [6]. Code obfuscation has created another challenge for digital forensic examiners, namely the detection rate of new and unknown malware that is currently only being detected between 70 to 80% [7] [8] [9] and identifying benign code as malicious (false alarm rate or false positive) is quite high [7]. Signature based detection suffers from two hindrances, first, high false positive [7] (identifying benign files as malware) and second, high false negative (fail to detect malware) [8]. Therefore, in this research we focus on anomaly based detection using feature extraction such as application programming interface (API) calls and code obfuscation features. The obfuscation features include behaviours based on the content of malware such as source address, destination address, ASCII, UNICODE, and other contents that are relevant for the analysis [3] [5].

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

```
] import hashlib
```

```
] salida = hashlib.sha256(b"sample_qwrty_dk2").hexdigest()
print(salida)
```

```
7026ae73db9abc61dc85969de8aa105ed075aa797266e2e909d9b84fbfd82802
```

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

Este sería parte de una biblioteca de los servicios del API. Se tiene que controlar la administración de tareas, manipulación y los registros. Tomando en cuenta los puntos de referencia.

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

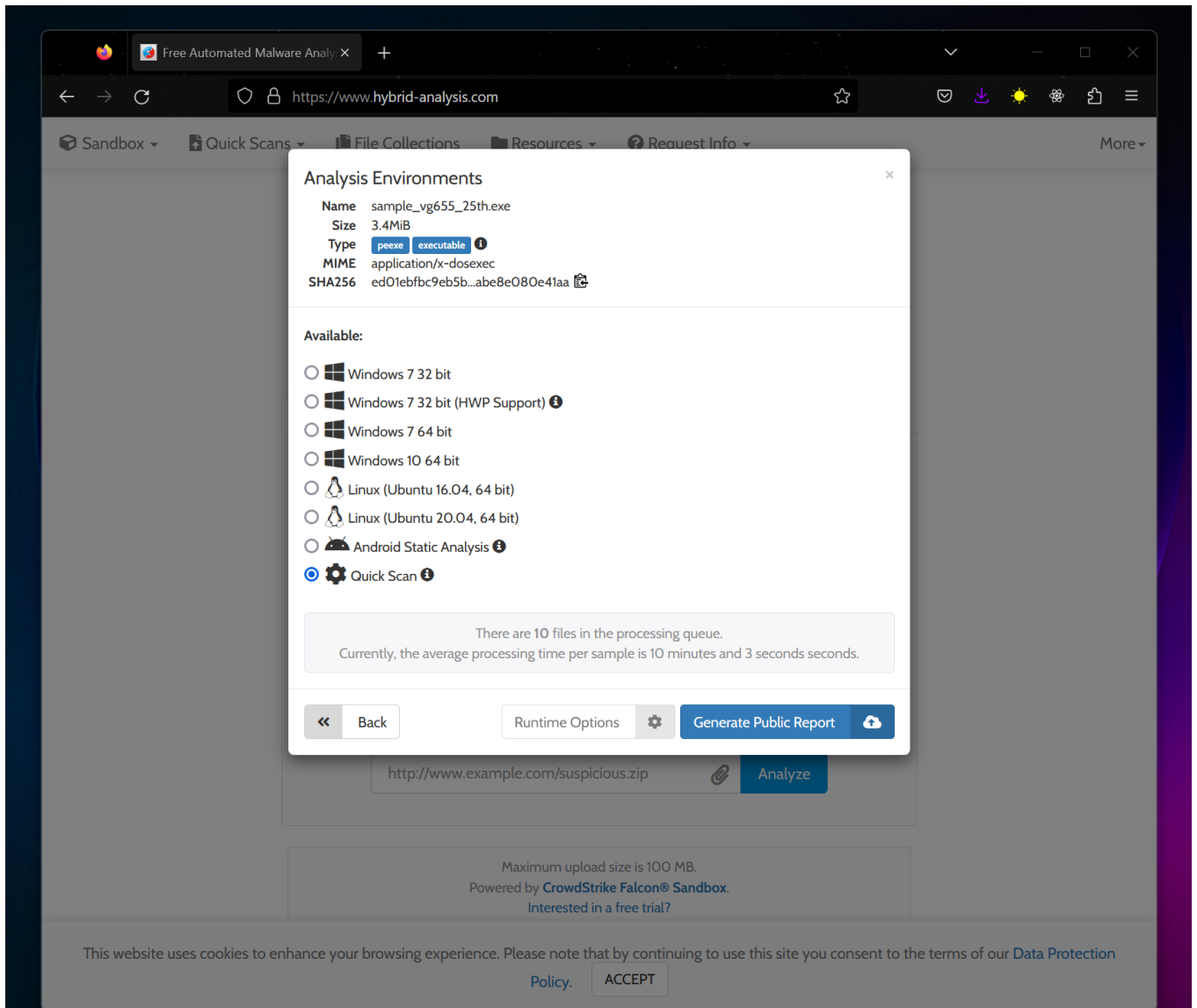
Nos muestra el identificador al proveedor de servicios de criptografía y las claves. Como también se debería llamar al conteo y reducirse 1 y que si el contador está en 0 no hace nada.

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.

Si sería sospechoso porque no necesariamente tendría APIS que sean muy comunes.

Parte 2 – 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? ¿Cuál es el propósito de este malware?



- 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?

Free Automated Malware Analysis

https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f10

HYBRID ANALYSIS

Request Info

IP, Domain, Hash...

Anti-Virus Results

Refresh Required

CrowdStrike Falcon

100%

Static Analysis and ML

Last Update: 03/07/2023 22:17:29

View Details: N/A

Visit Vendor: [Visit Vendor](#)

GET STARTED WITH A FREE TRIAL

MetaDefender

92%

Multi Scan Analysis

Last Update: 03/07/2023 22:17:29

View Details: [View Details](#)

Visit Vendor: [Visit Vendor](#)

VirusTotal

N/A

Multi Scan Analysis

Last Update: 03/07/2023 22:17:29

View Details: N/A

Visit Vendor: [Visit Vendor](#)

Analysis Overview

Anti-Virus Scanner Results

Related Hashes

Falcon Sandbox Reports (37)

Community (55)

Back to top

Related Hashes

Related files

Name	Sha256	Verdict
Ransomware.WannaCry.zip	707a9f323556179571bc832e34fa592066bd5f2cac4a7426fe163	malicious

This website uses cookies to enhance your browsing experience. Please note that by continuing to use this site you consent to the terms of our [Data Protection Policy](#). [ACCEPT](#)

Free Automated Malware Analysis

https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f10

HYBRID ANALYSIS

Request Info

IP, Domain, Hash...

File Collections

Name	Files number	Verdict
Unknown Files Collection	2	malicious
Unknown Files Collection	1	malicious
Unknown Files Collection	16	malicious
TEST	2	malicious
Unknown Files Collection	32	malicious
Unknown Files Collection	27	malicious
Discord fake update and WannaCry	2	malicious
Unknown Files	30	malicious
Unknown Files Collection	15	malicious
Unknown Files Collection	57	malicious

Falcon Sandbox Reports

There are 37 reports, although only 24 have loaded screenshots. You can still see all of the screenshots while going to the report page.

MALICIOUS

MALICIOUS

MALICIOUS

Analysis Overview

Anti-Virus Scanner Results

Related Hashes


Falcon Sandbox Reports (37)

Incident Response

Community (55)

Back to top

This website uses cookies to enhance your browsing experience. Please note that by continuing to use this site you consent to the terms of our [Data Protection Policy](#). [ACCEPT](#)


Free Automated Malware Analysis

<https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f10>
Request Info

There are 37 reports, although only 24 have loaded screenshots. You can still see all of the screenshots while going to the report page.

Analysis Overview

Anti-Virus Scanner Results

Related Hashes


Falcon Sandbox Reports (37)

Incident Response

Community (55)

Back to top

MALICIOUS

 ed01ebfbc9eb5b...

Analyzed on: 11/03/2022 ...


Environment: Windows 10 ...

Threat Score: 100/100


AV Detection: 95% Trojan.R...

Indicators: 13 50

Network: (none)



MALICIOUS

 ed01ebfbc9eb5b...


Analyzed on: 06/28/2021 ...


Environment: Windows 7 3...

Threat Score: 100/100


AV Detection: 94% Trojan.R...

Indicators: 17 36

Network: 



MALICIOUS

 ed01ebfbc9eb5b...


Analyzed on: 06/12/2020 ...


Environment: Windows 7 3...

Threat Score: 100/100


AV Detection: 91% Trojan.R...

Indicators: 17 34

Network: 



MALICIOUS

 owo_im_not_ran...


Analyzed on: 02/24/2020 ...

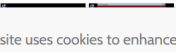
Environment: Windows 7 6...

Threat Score: 100/100


AV Detection: 90% Trojan.R...

Indicators: 14 37

Network: 



MALICIOUS

 ed01ebfbc9eb5b...


Analyzed on: 08/06/2020 ...

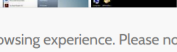
Environment: Windows 7 3...

Threat Score: 100/100


AV Detection: 90% Trojan.R...

Indicators: 18 34

Network: 



MALICIOUS

 ed01ebfbc9eb5b...

Analyzed on: 08/06/2019 ...

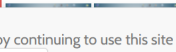
Environment: Android Stati...

Threat Score: 100/100

AV Detection: 87% Trojan.R...

Indicators: 4 0

Network: (none)



This website uses cookies to enhance your browsing experience. Please note that by continuing to use this site you consent to the terms of our [Data Protection Policy](#).

ACCEPT