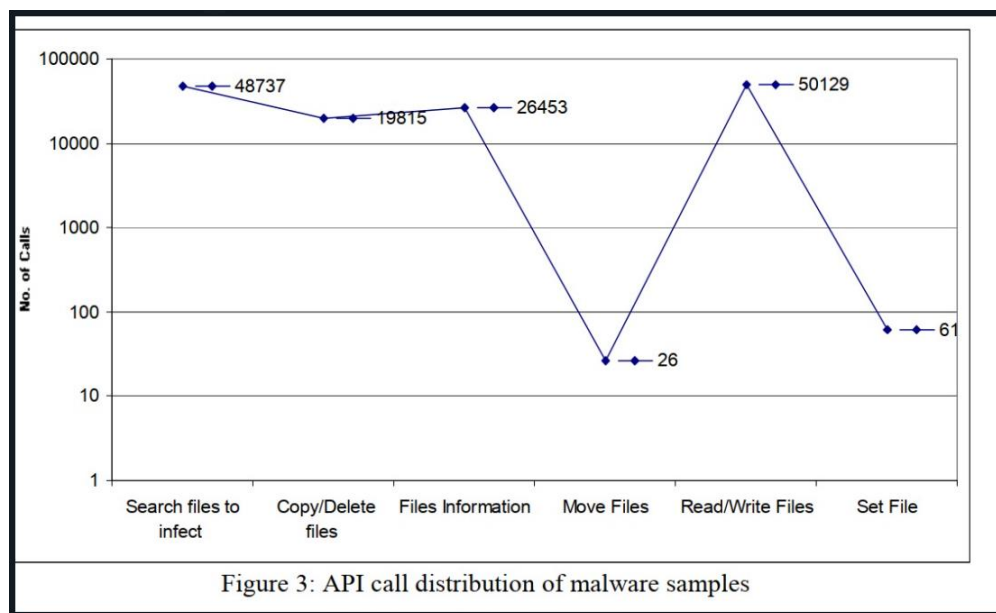


Hoja de Trabajo 2 – Security Data Science

1. Entre los ejemplos el ejecutable contine muchas más llamadas al API, que se enfocan más en llamadas al kernel. Mientras que el primero tiene un DLL que hace una llamada para poder escribir directamente sobre el disco duro. Si es sospechoso que el ejecutable este haciendo muchas llamadas al kernel y el otro este escribiendo directamente en el disco duro.
2. UPX es una manera de comprimir archivos y las personas que escriben malware lo utilizan para que los antivirus no los detecten tan fácil.
3. Este se puede clasificar en:
 - a. Search Files to Infect
 - b. Copy/Delete Files
 - c. Read/Write Files



4.

```
(kali@kali)-[~/Desktop/hdt2]
$ sha256sum sample_vg655_25th.exe
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa sample_vg655_25th.exe
```

5. Esta librería provee acceso avanzado que es parte del kernel. Este es responsable de reiniciar o apagar la máquina.
6. El CryptReleaseContext es el que maneja los servicios de criptografía y la llave con la que se trabaja.

7. Con estas pruebas, este archivo es sospechoso y lo que puede hacer es que encripte la maquina y saque al usuario de la maquina al momento de ejecutarse.
- 8.

Free Automated Malware

[Kali Linux](#)
[Kali Tools](#)
[Kali Docs](#)
[Kali Forums](#)
[Kali NetHunter](#)
[Exploit-DB](#)
[Google Hacking DB](#)
[OffSec](#)

[HYBRID ANALYSIS](#)
[Sandbox](#)
[Quick Scans](#)
[File Collections](#)
[Resources](#)
[Request Info](#)

[IP, Domain, Hash...](#)

Analysis Overview

Submission name:

owo_jm_not_ransomware_xd.exe

Size:

3.4MiB

Type:

peexe executable

Mime:

application/x-dosexec

SHA256:

ed01ebfbc9eb5bba545af4d01bf5f071661840480439c6e5babe8e080e41aa

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

#wannacrypt0r

#perc

#p00p

#sub

#p0p0s

#p0p0l

#b00k0r

#ern0t0t

#p0p0l

Link

Twitter

Twitter

E-Mail

Analysis Overview

Anti-Virus Scanner Results

Related Hashes

Falcon Sandbox Reports (31)

Incident Response

Community (55)

Back to top

Anti-Virus Results

Refresh Required

CrowdStrike Falcon

MetaDefender

VirusTotal

100%

92%

95%

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

Related files

Name	Sha256	Verdict
Ransomware.WannaCry.zip	707a9f323556179571bc832e34fa592066b1d5f2cac4a7426fe163597e3e618a	malicious
RansomeWARE.exe.zip	7c42f6f0696c1b6954c3aea6136c8e25b2f179922a143984254f00561ed53e784	malicious
Ransomware.WannaCry.zip	61a5eed5d3cf4cf0924bac18ac3dfeff2ab3a8fc67024f3c35fcc2061e6511	malicious
Ransomware.WannaCry.zip	c1aeafa14591bbc30cf3685e69e13e71438e0c963b3b0de72ede00c7131194478	malicious
Ransomware.WannaCry.zip	3eaddb62d7b951ebb98effa2e7f61e14bf8b47b0cf20fc43bec272475913d44	malicious

Samples that dropped this file

Name	Sha256	Verdict
Server.exe	5c17f43e95f71d09ae9d3a12e5c586eb257d0bf49ce6551709468c4617a0bf8f	malicious
file	1e06140672b73dfe337dfde7bc9dead5612bdfb4a8069be5de78fe68da6c75c4	malicious
file	73aa2e53b8290b3c2827187b2c1c36167ae968aec846674a5e2cb72e55f32b7e	malicious
WannaCry.exe	91afb972e14584b4c1e23802e2b26813f57b802689f61a540fda162cecd7493	malicious
wannacry.exe	8d30a543523066e4bb1788104f6b8ae402b0331d76a6543285e51fc0faf6a56	malicious

Como se puede observar el Hash generado es el mismo al que se generó. El nombre del file es un owo_im_not_ransomware_xd.exe. El propósito del

malware es entrar como un troyano y luego obtener las llaves del sistema y borrar grandes volúmenes de información.

9. Queda claro que las sospechas del punto 7 fueron confirmadas con el analizador.