

Hoja de Trabajo – Análisis de Malware

(Análisis Dinámico)

8. Como se puede observar, el sha256 es el mismo que se obtuvo en el análisis estático realizado. La pagina reporta que se trata de un ransomware.

Analysis Environments

Name

sample_vg655_25th.exe

Size

3.4MiB

Type

peexe

executable

MIME

application/x-dosexec

SHA256

ed01ebfbc9eb5b...abe8e080e41aa

Available:

☐

Windows 7 32 bit

☐

Windows 7 32 bit (HWP Support)

☐

Windows 7 64 bit

☒

Windows 10 64 bit

☐

Linux (Ubuntu 16.04, 64 bit)

☐

Linux (Ubuntu 20.04, 64 bit)

☐

Android Static Analysis

☐

Quick Scan

There are 11 files in the processing queue.
Currently, the average processing time per sample is 9 minutes and 46 seconds seconds.

<< Back

Runtime Options

Generate Public Report

Size:

3.4MiB

Type:

peexe

executable

Mime:

application/x-dosexec

SHA256:

ed01ebfbc9eb5b5bea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

9. Según las imágenes que se pueden observar, el malware efectivamente se trata de un ransomware, el cual encripta los archivos y pide un rescate para desencriptarlos. En el análisis realizado en el inciso 7, se llega a la conclusión que podría tratarse de un ransomware por lo que las sospechas fueron correctas.

