Análisis de malware

Caso Práctico Ejercicio de reglas Yara

En primer lugar usaremos una máquina virtual de ubuntu en vmware donde haremos la compilación de las normas yara descargandonos los ficheros zip de github y tambien descargaremos los archivos malware que analizaremos.

Desde la máquina virtual nos descargamos los siguientes repositorios de github donde se encuentran reglas yara para poder realizar la compilacion:

https://github.com/reversinglabs/reversinglabs-yara-rules/tree/develop/yara

https://github.com/malpedia/signator-rules

https://github.com/Yara-Rules/rules

https://github.com/t4d/PhishingKit-Yara-Rules

https://github.com/advanced-threat-research/Yara-Rules

https://github.com/kevoreilly/CAPEv2

https://github.com/kevthehermit/PasteHunter

https://github.com/bartblaze/Yara-rules

https://github.com/SupportIntelligence/Icewater

https://github.com/mikesxrs/Open-Source-YARA-rules

https://github.com/m4nbat/yara_rules

https://github.com/evild3ad/yara-rules

https://github.com/ditekshen/detection

https://github.com/securitymagic/yara

https://github.com/filescanio/fsYara

Una vez descargados todos los archivos zip procedentes de github los descomprimimos y copiamos todas las reglas .yar y .yara en una misma carpeta. Usamos un script para compilar todas esas reglas y ejecutarlo con el comando yara -C contra los malware que hemos descargado.