Practica

Reglas Yara

De

Daniel Shved

# OBJETIVOS:

* Desarrollar un script en .py que descarga .yar y .yara de repositorios de github para compilarlo, y lanzarlo contra diferentes malware. Se meterá en zip independientes los repositorios usados y los malware probados.

# Herramientas usadas para el ejercicio de reglas yara

* IDLE THONY
* GITHUB

# reglas yara

El funcionamiento del script se divide en tres partes. La primera es la declaración de las rutas de carpetas y archivos para descomprimirlos copiarlos moverlas borrarlos.

La segunda parte establece los directorios locales que se tiene que recorrer para compilar.

La tercera parte son llamadas a funciones que siguen el siguiente orden;

* Descarga librería de reglas yara de github
* Descifra la ruta especificad del .zip
* Crea un directorio local asignado en la primera parte del script
* Copia los ficheros descifrados a dicho directorio.
* Borra la carpeta local descifrada
* Borra la carpeta local cifrada.

Los repositorios github usados son los siguientes:

https://github.com/SupportIntelligence/Icewater

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

https://github.com/droberson/yararules

https://github.com/StrangerealIntel/Orion

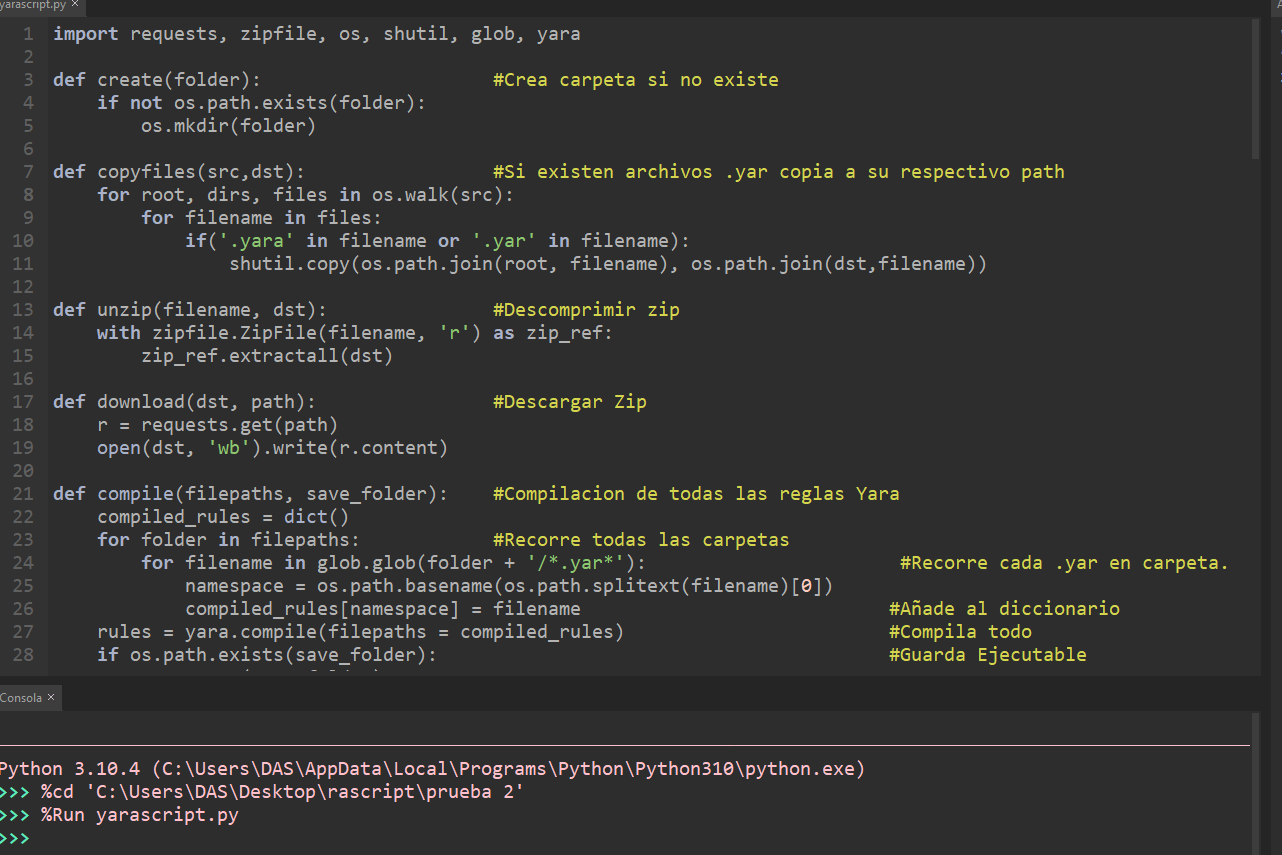
https://github.com/bartblaze/Yara-rules

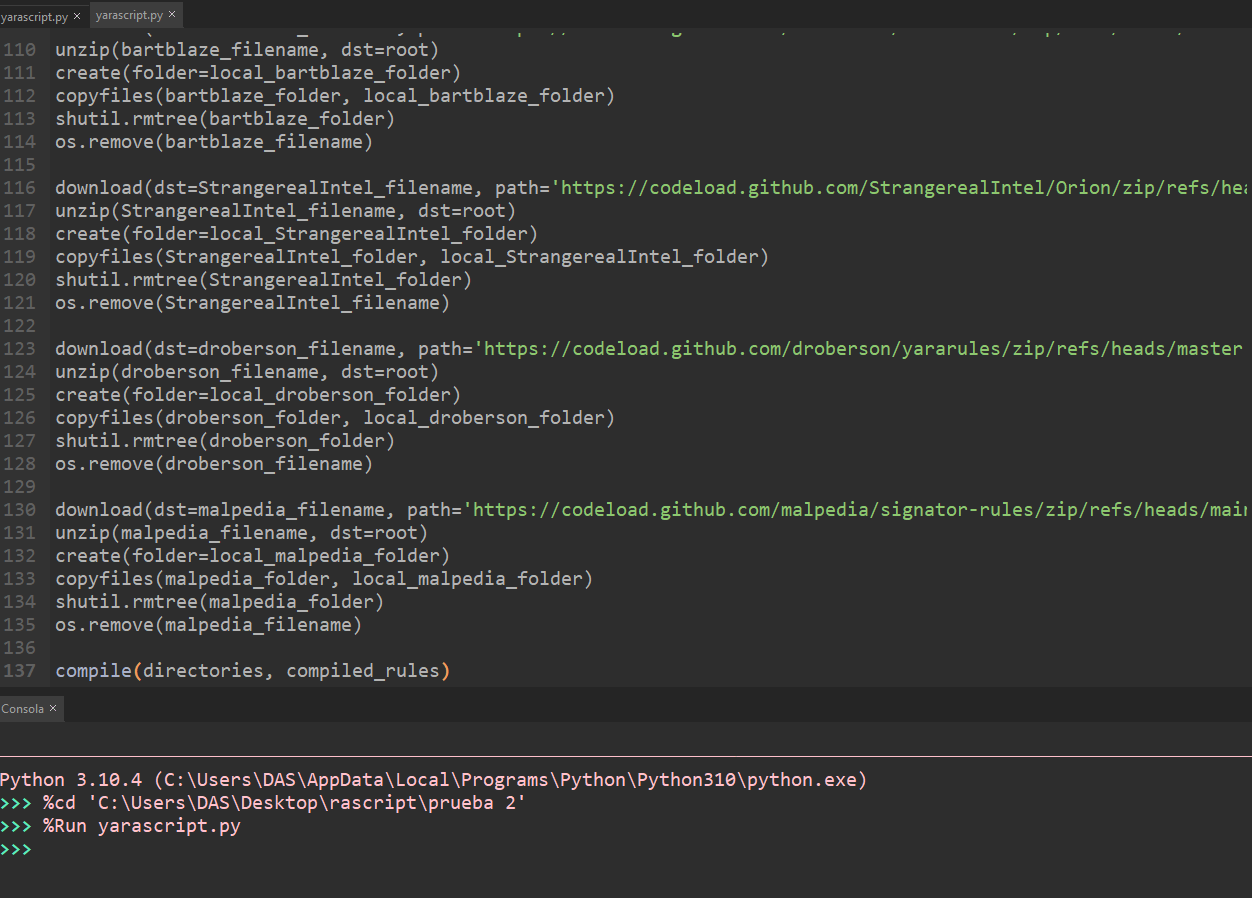
https://github.com/advanced-threat-research/Yara-Rules

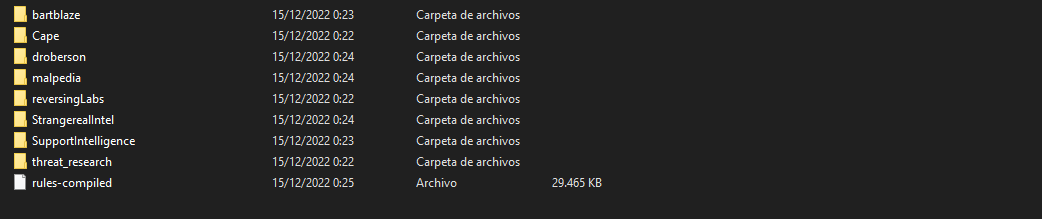
https://github.com/reversinglabs/reversinglabs-yara-rules

https://github.com/kevoreilly/CAPEv2

Prueba de uso:



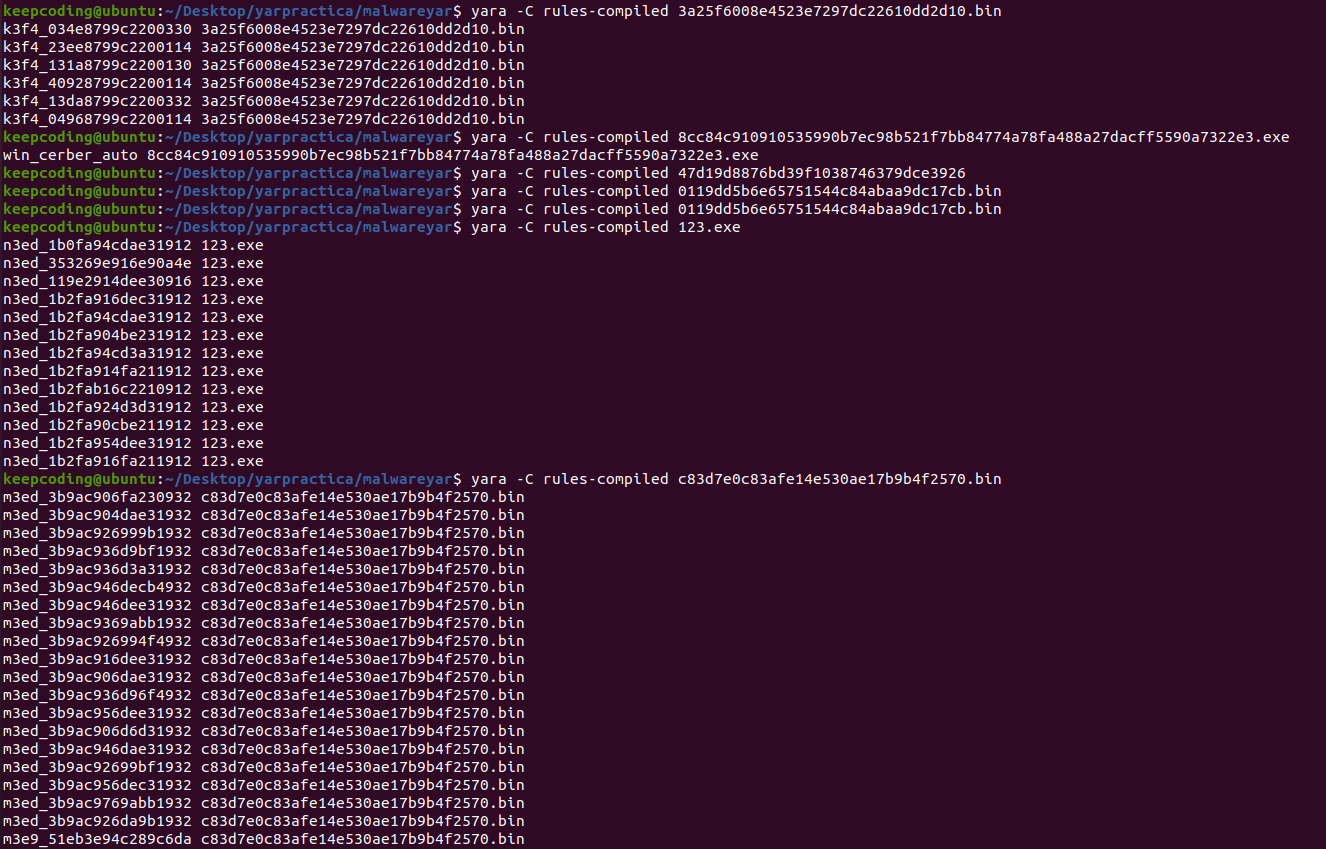




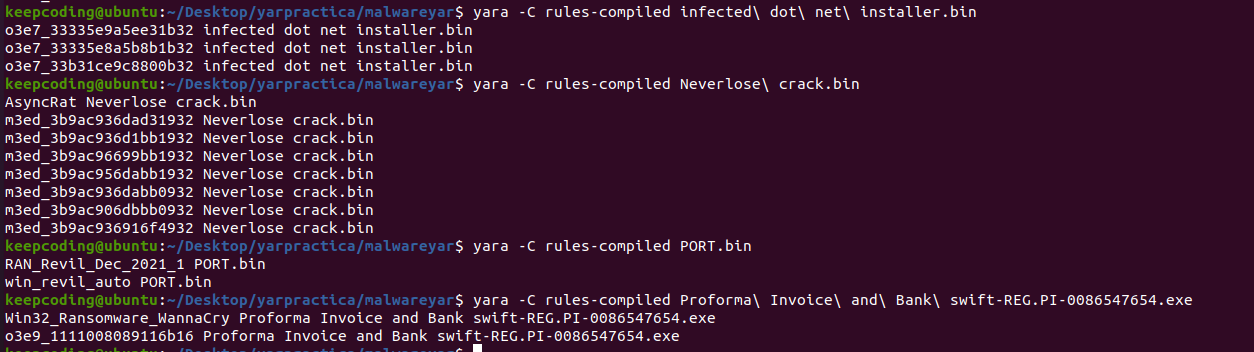
Probamos las reglas compiladas contra 14 malwares descargados de any.run. Escogi a dedo 3 ransomware, 3 spyware, 3 gusanos 3 de una practica de clase y dos aleatorios.



El resultado es que reconoció todos excepto dos(85% de deteccion):







Entre los que no reconoció esta un trojan ransomware darkside y un rat/backdoor dcrat. Respectivos hashes:

* MD5:47d19d8876bd39f1038746379dce3926
* SHA256:a82aec54cad176b368967fa8e41e41a8129ffafe6ab627312e111e63605b8478
* MD5: 0119dd5b6e65751544c84abaa9dc17cb
* SHA256:25952379e5996ee2563716778ad1f597de228c1bd2d918005152a8ba9299c28d