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

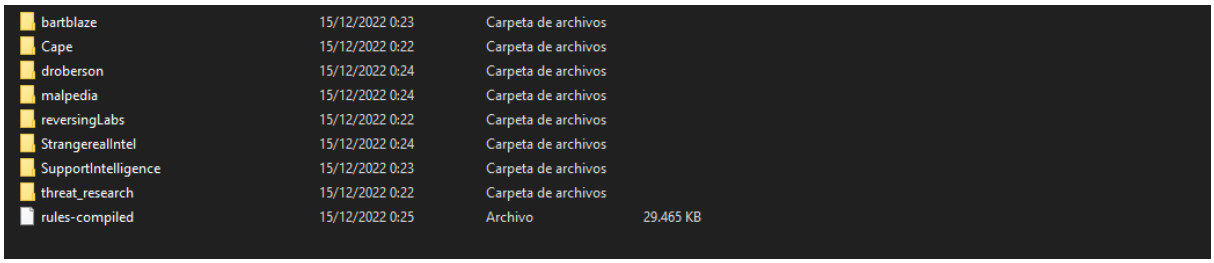
Prueba de uso:

```python
import requests, zipfile, os, shutil, glob, yara

def create(folder):                     #Crea carpeta si no existe
    if not os.path.exists(folder):
        os.mkdir(folder)

def copyfiles(src,dst):                 #Si existen archivos .yar copia a su respectivo path
    for root, dirs, files in os.walk(src):
        for filename in files:
            if('.yara' in filename or '.yar' in filename):
                shutil.copy(os.path.join(root, filename), os.path.join(dst,filename))

def unzip(filename, dst):               #Descomprimir zip
    with zipfile.ZipFile(filename, 'r') as zip_ref:
        zip_ref.extractall(dst)

def download(dst, path):                #Descargar Zip
    r = requests.get(path)
    open(dst, 'wb').write(r.content)

def compile(filepaths, save_folder):    #Compilacion de todas las reglas Yara
    compiled_rules = dict()
    for folder in filepaths:            #Recorre todas las carpetas
        for filename in glob.glob(folder + '/*.yar*'):                    #Recorre cada .yar en carpeta.
            namespace = os.path.basename(os.path.splitext(filename)[0])
            compiled_rules[namespace] = filename                          #Añade al diccionario
    rules = yara.compile(filepaths = compiled_rules)                      #Compila todo
    if os.path.exists(save_folder):                                       #Guarda Ejecutable
```

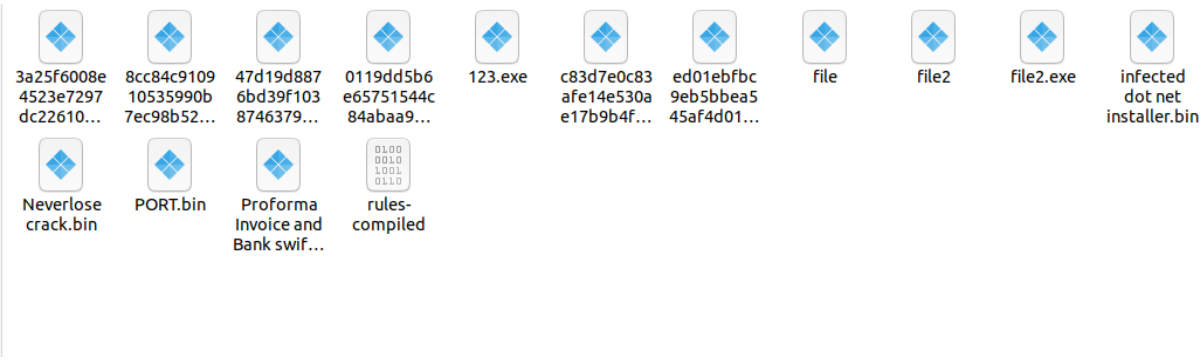
```
Consola ×

Python 3.10.4 (C:\Users\DAS\AppData\Local\Programs\Python\Python310\python.exe)
>>> %cd 'C:\Users\DAS\Desktop\rascript\prueba 2'
>>> %Run yarascript.py
>>>
```

```python
unzip(bartblaze_filename, dst=root)
create(folder=local_bartblaze_folder)
copyfiles(bartblaze_folder, local_bartblaze_folder)
shutil.rmtree(bartblaze_folder)
os.remove(bartblaze_filename)

download(dst=StrangerealIntel_filename, path='https://codeload.github.com/StrangerealIntel/Orion/zip/refs/he
unzip(StrangerealIntel_filename, dst=root)
create(folder=local_StrangerealIntel_folder)
copyfiles(StrangerealIntel_folder, local_StrangerealIntel_folder)
shutil.rmtree(StrangerealIntel_folder)
os.remove(StrangerealIntel_filename)

download(dst=droberson_filename, path='https://codeload.github.com/droberson/yararules/zip/refs/heads/master
unzip(droberson_filename, dst=root)
create(folder=local_droberson_folder)
copyfiles(droberson_folder, local_droberson_folder)
shutil.rmtree(droberson_folder)
os.remove(droberson_filename)

download(dst=malpedia_filename, path='https://codeload.github.com/malpedia/signator-rules/zip/refs/heads/mai
unzip(malpedia_filename, dst=root)
create(folder=local_malpedia_folder)
copyfiles(malpedia_folder, local_malpedia_folder)
shutil.rmtree(malpedia_folder)
os.remove(malpedia_filename)

compile(directories, compiled_rules)
```

```
Consola ×

Python 3.10.4 (C:\Users\DAS\AppData\Local\Programs\Python\Python310\python.exe)
>>> %cd 'C:\Users\DAS\Desktop\rascript\prueba 2'
>>> %Run yarascript.py
>>>
```



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):

```
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled 3a25f6008e4523e7297dc22610dd2d10.bin
k3f4_034e8799c2200330 3a25f6008e4523e7297dc22610dd2d10.bin
k3f4_23ee8799c2200114 3a25f6008e4523e7297dc22610dd2d10.bin
k3f4_131a8799c2200130 3a25f6008e4523e7297dc22610dd2d10.bin
k3f4_40928799c2200114 3a25f6008e4523e7297dc22610dd2d10.bin
k3f4_13da8799c2200332 3a25f6008e4523e7297dc22610dd2d10.bin
k3f4_04968799c2200114 3a25f6008e4523e7297dc22610dd2d10.bin
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled 8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacff5590a7322e3.exe
win_cerber_auto 8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacff5590a7322e3.exe
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled 47d19d8876bd39f1038746379dce3926
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled 0119dd5b6e65751544c84abaa9dc17cb.bin
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled 0119dd5b6e65751544c84abaa9dc17cb.bin
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled 123.exe
n3ed_1b0fa94cdae31912 123.exe
n3ed_353269e916e90a4e 123.exe
n3ed_119e2914dee30916 123.exe
n3ed_1b2fa916dec31912 123.exe
n3ed_1b2fa94cdae31912 123.exe
n3ed_1b2fa904be231912 123.exe
n3ed_1b2fa94cd3a31912 123.exe
n3ed_1b2fa914fa211912 123.exe
n3ed_1b2fab16c2210912 123.exe
n3ed_1b2fa924d3d31912 123.exe
n3ed_1b2fa90cbe211912 123.exe
n3ed_1b2fa954dee31912 123.exe
n3ed_1b2fa916fa211912 123.exe
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac906fa230932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac904dae31932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac926999b1932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac936d9bf1932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac936d3a31932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac946decb4932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac946dee31932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac9369abb1932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac926994f4932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac916dee31932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac906dae31932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac936d96f4932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac956dee31932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac906d6d31932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac946dae31932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac92699bf1932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac956dec31932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac9769abb1932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3ed_3b9ac926da9b1932 c83d7e0c83afe14e530ae17b9b4f2570.bin
m3e9_51eb3e94c289c6da c83d7e0c83afe14e530ae17b9b4f2570.bin
```

```
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.bin
Win32_Ransomware_WannaCry ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.bin
o3e9_1111008089116b16 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.bin
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled file
k26bb_193e6de357b2f316 file
k26bb_193e65e15db2f316 file
m26bb_13624ec344000916 file
m26bb_13a6bec144000916 file
k26bb_193e65e35db2f316 file
k26bb_193e6de353b2f316 file
k26bb_193e65e355b2f316 file
m26bb_13a9a715c1a6f116 file
k26bb_193e61e355b2f316 file
k26bb_193e69e355b2f316 file
k26bb_193e71e35db2f316 file
m26bb_13615ec144000916 file
k26bb_193e61e35db2f316 file
o3e7_33b31ce9c8800b32 file
k26bb_093659e3dec34b16 file
k26bb_193e6de155b2f316 file
m26bb_13696a65969bf116 file
m26bb_13a3260f913b7116 file
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled file2
o26bb_632da928d3a30912 file2
k26bb_193e6de357b2f316 file2
k26bb_193e65e15db2f316 file2
m26bb_13624ec344000916 file2
m26bb_13a6bec144000916 file2
k26bb_193e65e35db2f316 file2
k26bb_193e6de353b2f316 file2
k26bb_193e65e355b2f316 file2
m26bb_13a9a715c1a6f116 file2
o26bb_630da120dfa30912 file2
k26bb_193e61e355b2f316 file2
k26bb_193e69e355b2f316 file2
k26bb_193e71e35db2f316 file2
k3e9_193e79e3dec34916 file2
m26bb_13615ec144000916 file2
k26bb_193e61e35db2f316 file2
o3e7_33b31ce9c8800b32 file2
k26bb_093659e3dec34b16 file2
k26bb_193e6de155b2f316 file2
m26bb_13696a65969bf116 file2
m26bb_13a3260f913b7116 file2
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled file2.exe
m3ed_3b9ac906fa230932 file2.exe
m3ed_3b9ac904dae31932 file2.exe
```

```
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled infected\ dot\ net\ installer.bin
o3e7_33335e9a5ee31b32 infected dot net installer.bin
o3e7_33335e8a5b8b1b32 infected dot net installer.bin
o3e7_33b31ce9c8800b32 infected dot net installer.bin
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled Neverlose\ crack.bin
AsyncRat Neverlose crack.bin
m3ed_3b9ac936dad31932 Neverlose crack.bin
m3ed_3b9ac936d1bb1932 Neverlose crack.bin
m3ed_3b9ac96699bb1932 Neverlose crack.bin
m3ed_3b9ac956dabb1932 Neverlose crack.bin
m3ed_3b9ac936dabb0932 Neverlose crack.bin
m3ed_3b9ac906dbbb0932 Neverlose crack.bin
m3ed_3b9ac936916f4932 Neverlose crack.bin
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled PORT.bin
RAN_Revil_Dec_2021_1 PORT.bin
win_revil_auto PORT.bin
keepcoding@ubuntu:~/Desktop/yarpractica/malwareyar$ yara -C rules-compiled Proforma\ Invoice\ and\ Bank\ swift-REG.PI-0086547654.exe
Win32_Ransomware_WannaCry Proforma Invoice and Bank swift-REG.PI-0086547654.exe
o3e9_1111008089116b16 Proforma Invoice and Bank swift-REG.PI-0086547654.exe
```

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