

# **Informe Módulo 8**

## **Practica – Reglas YARA**

Fecha: 31 de Mayo de 2024

Autor: **Azael Ramírez Pérez**

Mail: **keepcoder\_test@gmail.com (ficticio)**

Empresa: **KeepCoder.inc (ficticio)**

# Contenido

Ámbito y alcance.....	3
Estructura del proyecto.....	4
Lista de repositorios descargados de GitHub.....	6
Muestras de Malware analizadas.....	9
Pruebas con el programa de Python.....	12

## **Ámbito y alcance**

Se desarrollo un pequeño programa el cual utiliza una lista de repositorios de GitHub los cuales contienen reglas YARA, la funcionalidad básica es que podamos concentrar la mayoría de reglas posibles para después hacer un solo archivo compilado, de esta manera podamos detectar archivos que en su interior contienen malware.

## Estructura del proyecto

El proyecto está estructurado con 3 clases escritas en Python, adicionalmente cuenta algunos directorios y subdirectorios, a continuación, se hará la descripción de los elementos que componen el proyecto.

Clases de Python:

- **Constants.py:** clase que contiene la definición de rutas que se utilizaran dentro del proyecto. Por mencionar algunas rutas se usan para almacenar los archivos de los repositorios se descarguen de GitHub, así como para guardar el archivo compilado de reglas YARA, también contine la lista de los distintos repositorios a descargar de la red.
- **main.py:** clase principal de Python, esta misma inicia todo el flujo del proceso y contiene distintas funciones las cuales hacen la descarga de los archivos .zip, así como la descompresión de estos mismos, hacen también la búsqueda de archivos **.yar** ó **.yara** para posteriormente concentrar todas estas reglas en un directorio (CONCENTRADO).
- **compile\_yara\_rules.py:** esta clase compila todas las reglas YARA que han sido descargadas en el directorio **CONCENTRADO** de los distintos repositorios de la red, el archivo resultante de la compilación se guarda en el directorio **COMPILACION**.

Directorios utilizados en el proyecto:

**COMPILACION:** directorio que aloja el archivo compilado **rules\_compiled** el cual contiene en su interior todas las reglas YARA que han sido descargadas de los diferentes repositorios de GitHub.

**CONCENTRADO:** directorio que contiene todos los archivos con las reglas .yar o .yara.

**MUESTRAS\_MALWARE:** Este directorio aloja todas las muestras de malware que deseemos analizar a través de las reglas YARA.

En la siguiente imagen se muestra la estructura antes mencionada:

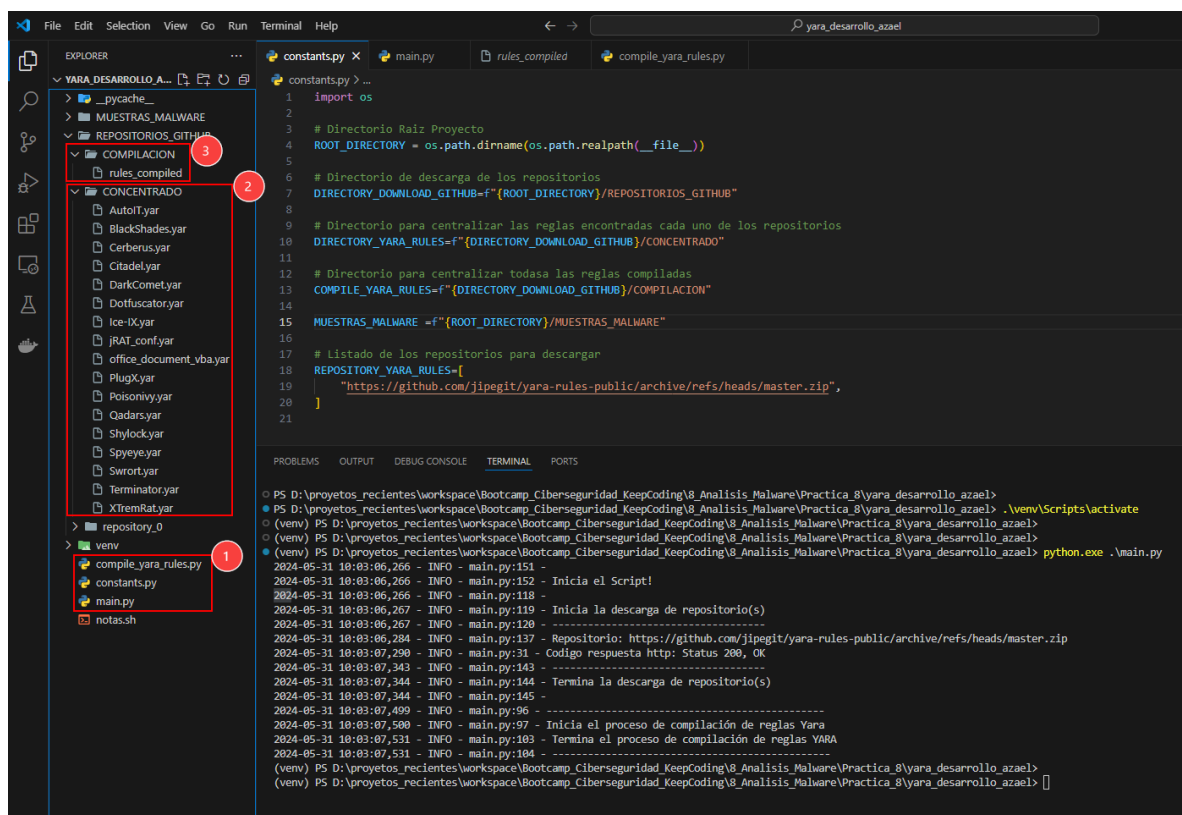


Imagen 1. Estructura del proyecto

## Lista de repositorios descargados de GitHub

A continuación, se muestra la lista de repositorios que se utilizaron para realizar las pruebas con programa de Python.

- [github.com/anyrun/YARA/archive/refs/heads/main.zip](https://github.com/anyrun/YARA/archive/refs/heads/main.zip)

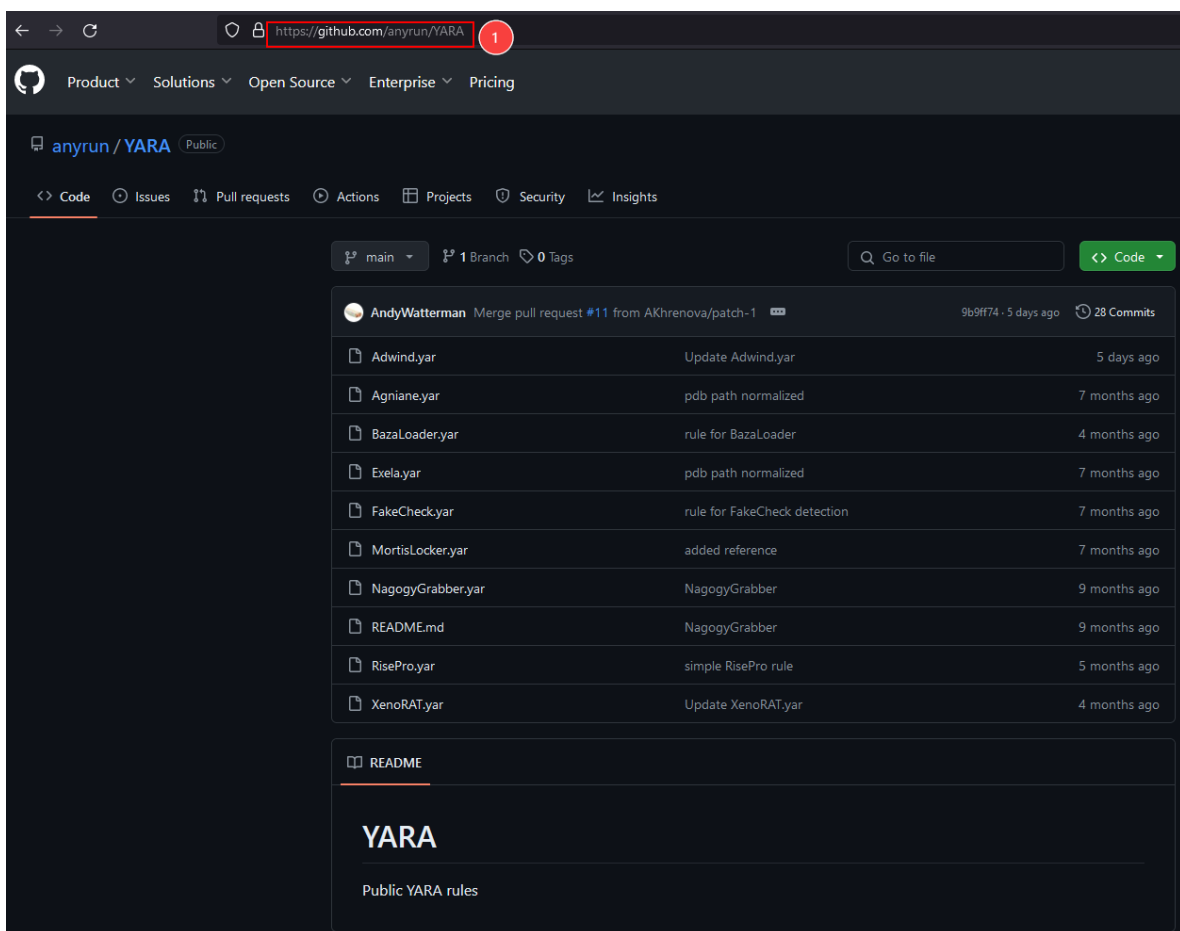


Imagen 2. Repositorio de GitHub que contiene reglas Yara

- [github.com/jipegit/yara-rules-public/archive/refs/heads/master.zip](https://github.com/jipegit/yara-rules-public/archive/refs/heads/master.zip)

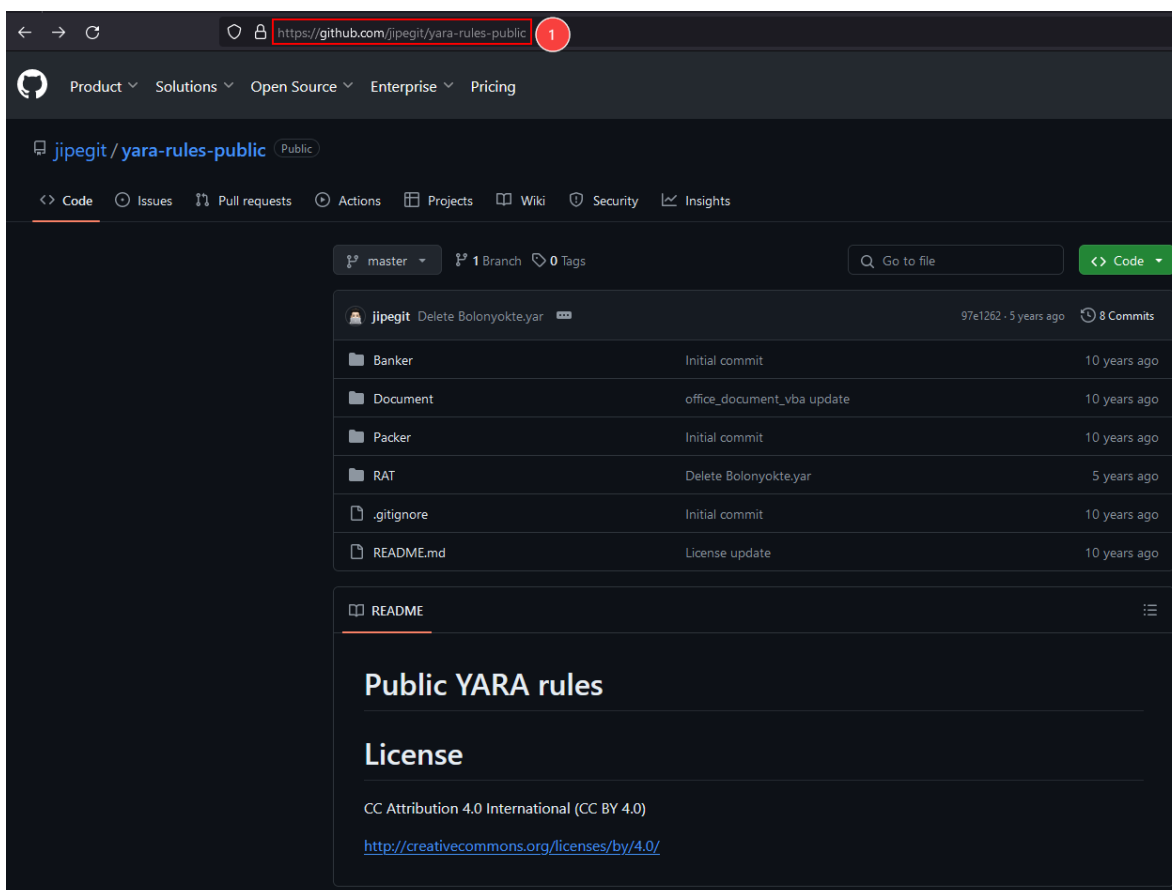


Imagen 3. Repositorio de GitHub que contiene reglas Yara

- [github.com/rapid7/Rapid7-Labs](https://github.com/rapid7/Rapid7-Labs)

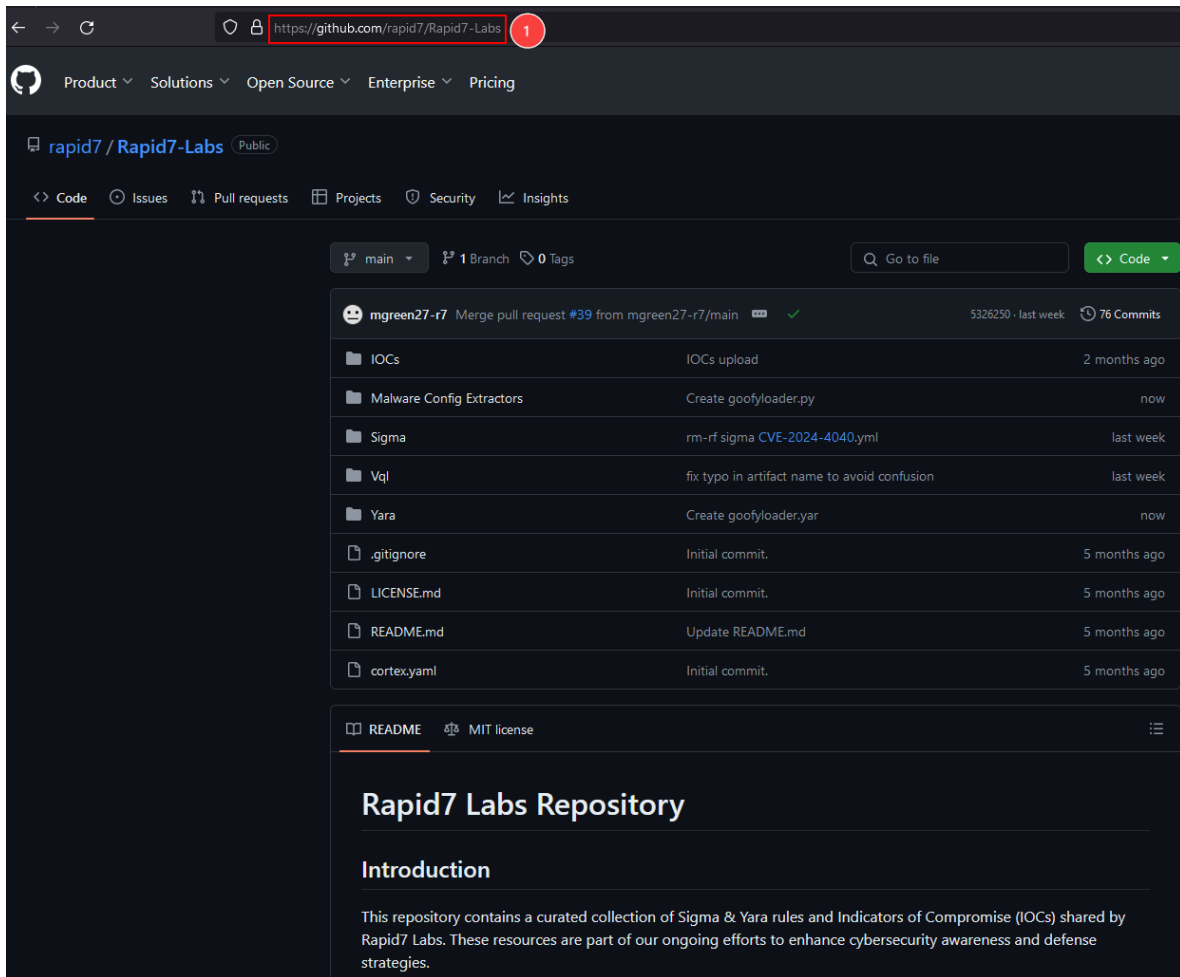


Imagen 4. Repositorio de GitHub que contiene reglas Yara



## Muestras de Malware Analizadas

A continuación, se listan las muestras de Malware que se analizaron usando el programa de Python y las reglas YARA.

### Archivo 1 - Archivo Excel

#### URL de la muestra:

<https://bazaar.abuse.ch/sample/b9575221797dae0ee2baa74764e906e4ad2988b0bcc6ecd782060584c4c8c2ee/>

**SHA256:** 9575221797dae0ee2baa74764e906e4ad2988b0bcc6ecd782060584c4c8c2ee

The screenshot shows the MalwareBazaar Database interface. At the top, there's a navigation bar with links like Browse, Upload, Hunting, API, Export, Statistics, FAQ, About, and Login. The main heading is "MalwareBazaar Database". Below it, a disclaimer states: "You are currently viewing the MalwareBazaar entry for SHA256 b9575221797dae0ee2baa74764e906e4ad2988b0bcc6ecd782060584c4c8c2ee. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious."

The "Database Entry" section features three colored boxes: a grey one labeled "Threat unknown", a blue one labeled "Vendor detections: 7", and a red one labeled "Maldoc score: 14".

Below these are tabs for "Intelligence 7", "IOCs", "YARA 10", "File information", "Comments", and an "Actions" dropdown. The "Intelligence" tab is active, showing a table with the following data:

SHA256 hash:	b9575221797dae0ee2baa74764e906e4ad2988b0bcc6ecd782060584c4c8c2ee
SHA3-384 hash:	636add2bde227d0ebfd44fbc29017d4631f5b034feb8ed762e851e3ed05f79fd25a9e0dcdbce7106db94eba1d17081e1
SHA1 hash:	272cebdd8a63e7963034fe41a369b00980b83a7b
MD5 hash:	9acd26176423fd95bae030ae9f154548
humanhash:	echo-sweet-yellow-charlie
File name:	AS-2023-CS.xlsm
Download:	<a href="#">download sample</a>
File size:	2'655'659 bytes
First seen:	2024-05-31 13:11:38 UTC
Last seen:	Never
File type:	xlsm
MIME type:	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet

Imagen 5. Muestra de Malware (Excel) descargada de la red

## Archivo 2 - Archivo Imagen

### URL de la muestra:

<https://bazaar.abuse.ch/sample/35a9558eeb948ab7b945acf5b3f712da7d349422c2be490c018f55d686deaf59>

**SHA256:** 35a9558eeb948ab7b945acf5b3f712da7d349422c2be490c018f55d686deaf59

**MALWARE** bazaar  
by ABUSE

Browse Upload Hunting API Export Statistics FAQ About Login

## MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 35a9558eeb948ab7b945acf5b3f712da7d349422c2be490c018f55d686deaf59**. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

### Database Entry

AgentTesla

Vendor detections: 7

Intelligence 7	IOCs	YARA 7	File information	Comments	Actions
<b>SHA256 hash:</b>	1	35a9558eeb948ab7b945acf5b3f712da7d349422c2be490c018f55d686deaf59			
<b>SHA3-384 hash:</b>	a21263c2baf91204b6f4fca920bec509c6c00a16910c1692513af85a5c2e539436d6557f4dddfde39e15bbf5ff8c2247				
<b>SHA1 hash:</b>	8dfafe32e713f89eb0b3118133d50b94414f9167				
<b>MD5 hash:</b>	0f94c8fea558e9bc37132736aa995dde				
<b>humanhash:</b>	angel-cold-single-oklahoma				
<b>File name:</b>	nZam%F3wienie Z23.img				
<b>Download:</b>	download sample				
<b>Signature</b>	AgentTesla Alert				
<b>File size:</b>	260'096 bytes				
<b>First seen:</b>	2024-05-31 15:31:04 UTC				
<b>Last seen:</b>	Never				
<b>File type:</b>	2	img			
<b>MIME type:</b>	application/x-iso9660-image				
<b>ssdeep</b>	6144:C8K118D8K4EsutOdyvLf+a8SzeNxUeOs:3w18D8K/nOdyvaiSFOs				

Imagen 6. Muestra de Malware (imagen) descargada de la red

## Archivo 3 - Archivo WannaCry Ransomware

URL de la muestra:

<https://bazaar.abuse.ch/sample/72406ec12b191d2fa211cf1899e62c9257379d5bdd1d850c66cc546685f3d8ea>

**SHA256:** 72406ec12b191d2fa211cf1899e62c9257379d5bdd1d850c66cc546685f3d8ea

**MALWARE** bazaar  
by ABUSE

Q Browse Upload Hunting API Export Statistics FAQ About Login

## MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 72406ec12b191d2fa211cf1899e62c9257379d5bdd1d850c66cc546685f3d8ea**. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

### Database Entry

WannaCry

Vendor detections: 17

Intelligence 17	IOCs	YARA 6	File information	Comments	Actions
<b>SHA256 hash:</b>	72406ec12b191d2fa211cf1899e62c9257379d5bdd1d850c66cc546685f3d8ea 1				
<b>SHA3-384 hash:</b>	7e121f7494ffc55d64099ad5d4f1ac8be6b584968c412d4379d5a7270a743ec196792348b5734eff138c51b0b4f343f7				
<b>SHA1 hash:</b>	fcc5ba39aa2ef5b48e62270bb0a8880856b677d4				
<b>MD5 hash:</b>	ecf4ccc75a4d40f2b70f3e05b4f0695c				
<b>humanhash:</b>	nitrogen-orange-violet-tennis				
<b>File name:</b>	72406ec12b191d2fa211cf1899e62c9257379d5bdd1d850c66cc546685f3d8ea				
<b>Download:</b>	<a href="#">download sample</a>				
<b>Signature</b>	WannaCry Alert				
<b>File size:</b>	2'281'472 bytes				
<b>First seen:</b>	2022-10-10 04:28:02 UTC				
<b>Last seen:</b>	Never				
<b>File type:</b>	exe 2				
<b>MIME type:</b>	application/x-dosexec				
<b>imphash</b>	9ecce117164e0b870a53dd187cdd7174 (74 x WannaCry, 1 x Worm.Virut)				

Imagen 7. Muestra de Malware (WannaCry) descargada de la red

## Pruebas con el programa de Python

Ejecución de **main.py**.

Se realiza la ejecución de la primera clase de Python (main.py) para la descarga de las reglas YARA de los repositorios de GitHub.

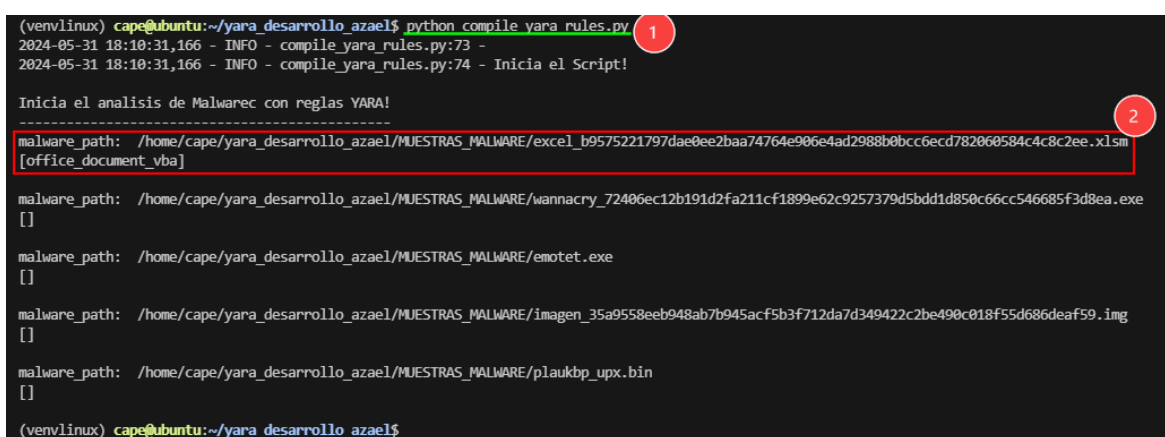
```
(venvlinux) cape@ubuntu:~/yara_desarrollo_azael$ python main.py
2024-05-31 18:10:27,032 - INFO - main.py:151 -
2024-05-31 18:10:27,032 - INFO - main.py:152 - Inicia el Script!
2024-05-31 18:10:27,032 - INFO - main.py:118 -
2024-05-31 18:10:27,032 - INFO - main.py:119 - Inicia la descarga de repositorio(s)
2024-05-31 18:10:27,032 - INFO - main.py:120 - -----
2024-05-31 18:10:27,069 - INFO - main.py:137 - Repositorio: https://github.com/anyrun/YARA/archive/refs/heads/main.zip
2024-05-31 18:10:27,666 - INFO - main.py:31 - Código respuesta http: Status 200, OK
2024-05-31 18:10:27,669 - INFO - main.py:137 - Repositorio: https://github.com/jipegit/yara-rules-public/archive/refs/heads/master.zip
2024-05-31 18:10:28,253 - INFO - main.py:31 - Código respuesta http: Status 200, OK
2024-05-31 18:10:28,257 - INFO - main.py:137 - Repositorio: https://github.com/rapid7/Rapid7-Labs/archive/refs/heads/main.zip
2024-05-31 18:10:28,939 - INFO - main.py:31 - Código respuesta http: Status 200, OK
2024-05-31 18:10:28,944 - INFO - main.py:143 - -----
2024-05-31 18:10:28,945 - INFO - main.py:144 - Termina la descarga de repositorio(s)
2024-05-31 18:10:28,945 - INFO - main.py:145 -
(venvlinux) cape@ubuntu:~/yara_desarrollo_azael$
```

Imagen 8. Ejecución de la primera clase Python, concentrado de reglas YARA

Ejecución de `compile_yara_rules.py`.

Se realiza la ejecución de la clase de Python que nos ayudara a compilar todas las reglas YARA en un solo archivo, después se realizara el análisis de 3 las muestras de Malware que se han mencionado anteriormente.

En la imagen siguiente se muestra que las reglas YARA han detectado como malicioso el archivo de Excel.



```
(venvlinux) cape@ubuntu:~/yara_desarrollo_azael$ python compile_yara_rules.py
2024-05-31 18:10:31,166 - INFO - compile_yara_rules.py:73 -
2024-05-31 18:10:31,166 - INFO - compile_yara_rules.py:74 - Inicia el Script!

Inicia el analisis de Malwarec con reglas YARA!
-----
malware_path: /home/cape/yara_desarrollo_azael/MUESTRAS_MALWARE/excel_b9575221797dae0ee2baa74764e906e4ad2988b0bcc6ecd782060584c4c8c2ee.xlsx
[office_document_vba]

malware_path: /home/cape/yara_desarrollo_azael/MUESTRAS_MALWARE/wannacry_72406ec12b191d2fa211cf1899e62c9257379d5bdd1d850c66cc546685f3d8ea.exe
[]

malware_path: /home/cape/yara_desarrollo_azael/MUESTRAS_MALWARE/emotet.exe
[]

malware_path: /home/cape/yara_desarrollo_azael/MUESTRAS_MALWARE/imagen_35a9558eeb948ab7b945acf5b3f712da7d349422c2be490c018f55d686deaf59.img
[]

malware_path: /home/cape/yara_desarrollo_azael/MUESTRAS_MALWARE/plaukbp_upx.bin
[]

(venvlinux) cape@ubuntu:~/yara_desarrollo_azael$
```

Imagen 9. Ejecución de la segunda clase Python, análisis de malware con reglas YARA