
```
osboxes@osboxes:~$ ls
Desktop    Downloads        Music     Public  Templates  yara_rules
Documents  malware_samples  Pictures  snap    Videos     yara_rules.py
```

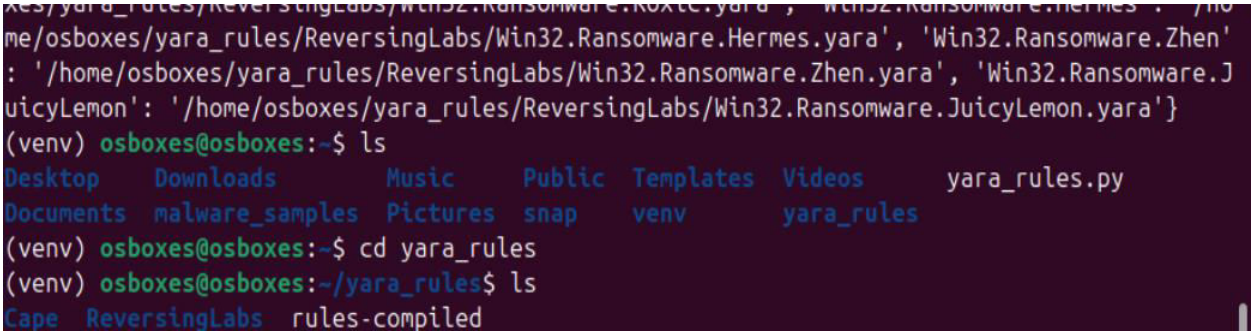
```
osboxes@osboxes:~$ sudo python3 -m venv venv
```

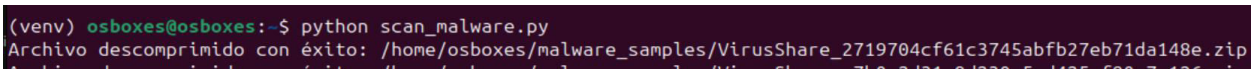
```
osboxes@osboxes:~$ sudo apt install python3.12-venv
```

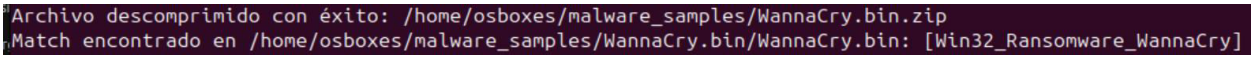
```
osboxes@osboxes:~$ python3 -m venv venv
osboxes@osboxes:~$ source venv/bin/activate
(venv) osboxes@osboxes:~$ pip install requests yara-python
```

```
(venv) osboxes@osboxes:~$ ls
Desktop    Downloads        Music     Public  Templates  Videos      yara_rules.py
Documents  malware_samples  Pictures  snap    venv       yara_rules
```

Para descargar las reglas Yara de los repositorios de GitHub de Cape y FeversingLabs utilice el programa yara_rules.pg



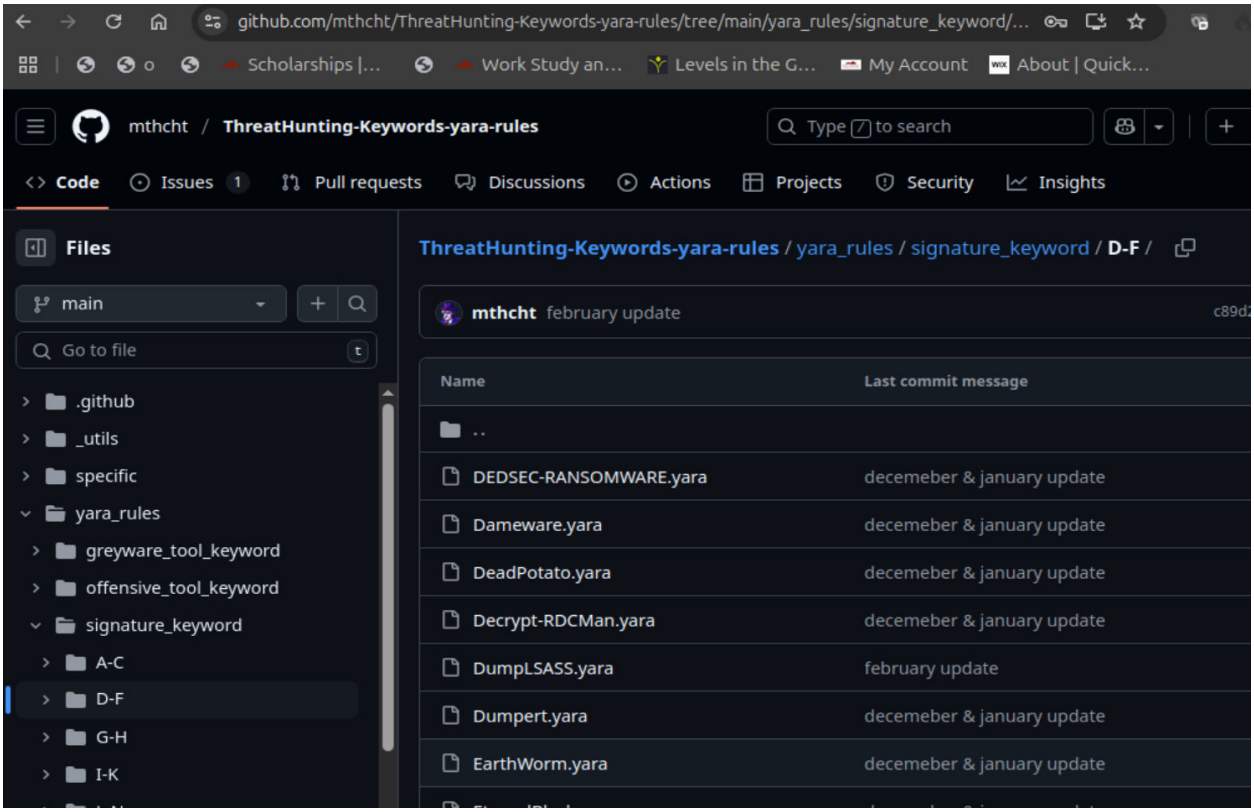




```
(venv) osboxes@osboxes:~/yara_rules/Cape$ ls
AgentTesla.yar          DoomedLoader.yar    LokiBot.yar         Rozena.yar
Amadey.yar              DoppelPaymer.yar    Lumma.yar           Ryuk.yar
Arkei.yar               Dreambot.yar        Magniber.yar        Scarab.yar
AsyncRAT.yar            DridexLoader.yar    MassLogger.yar      Sedreco.yar
Atlas.yar               DridexV4.yar        MegaCortex.yar      Seduploader.yar
AuroraStealer.yar       EmotetLoader.yar    Mole.yar            SmokeLoader.yar
Azer.yar                Emotet.yar          NanoLocker.yar      Socks5Systemz.yar
Azorult.yar             EternalRomance.yar  Nemty.yar           SparkRAT.yar
BadRabbit.yar           Fareit.yar          NetTraveler.yar     SquirrelWaffle.yar
Bazar.yar               Formbook.yar        Nighthawk.yar       Stealc.yar
BitPaymer.yar           Gandcrab.yar        NitrogenLoader.yar  TClient.yar
BlackDropper.yar        Gootkit.yar         Obfuscar.yar        TrickBot.yar
Blister.yar             Guloader.yar        Origin.yar          TSCookie.yar
BruteRatel.yar          Hancitor.yar        Oyster.yar          UrsnifV3.yar
BuerLoader.yar          Hermes.yar          Pafish.yar          Ursnif.yar
BumbleBee.yar           IcedIDLoader.yar    PetrWrap.yar        Varenyky.yar
Carbanak.yar            IcedID.yar          Petya.yar           Vidar.yar
CargoBayLoader.yar      Jaff.yar            PikaBot.yar         WanaCry.yar
Cerber.yar              KoiLoader.yar       QakBot.yar          XenoRAT.yar
CobaltStrikeBeacon.yar  Kovter.yar          Quickbind.yar       ZeroT.yar
CobaltStrikeStager.yar  Kpot.yar            Ramnit.yar          ZeusPanda.yar
Codoso.yar              Kronos.yar          RCSession.yar       Zloader.yar
Conti.yar               Latrodectus.yar     Remcos.yar
Cryptoshield.yar        Lockbit.yar         Rhadamanthys.yar
DarkGate.yar            Locky.yar           RokRat.yar
(venv) osboxes@osboxes:~/yara_rules/Cape$
```

```
(venv) osboxes@osboxes:~/yara_rules/Cape$ cat Jaff.yar
rule Jaff
{
    meta:
        author = "kevoreilly"
        description = "Jaff Payload"
        cape_type = "Jaff Payload"
    strings:
        $a1 = "CryptGenKey"
        $a2 = "353260540318613681395633061841341670181307185694827316660016508"
        $b1 = "jaff"
        $b2 = "2~1c0q4t7"
    condition:
        uint16(0) == 0x5A4D and (any of ($a*) ) and (1 of ($b*))
}
```

Descarge las reglas Yara del ***Github-ThreatHunting -signature_keyword*** como se muestra a continuación:



Puedes usar `git sparse-checkout` para clonar solo el subdirectorio que te interesa, en lugar de clonar todo el repositorio. Esto es más eficiente.

Instrucciones:

1. **Clonar el repositorio y realizar un `sparse-checkout`:**

bash Copy Edit

```
git init my-repo
cd my-repo
git remote add origin https://github.com/mthcht/ThreatHunting-Keywords-yara-rules.git
git config core.sparseCheckout true
echo "yara_rules/signature_keyword/*" >> .git/info/sparse-checkout
git pull origin main
```

2. Esto solo descargará los archivos dentro de `yara_rules/signature_keyword` (y sus subdirectorios), sin los otros directorios.
3. Luego, puedes copiar las reglas YARA de `signature_keyword` a tu carpeta de trabajo.

Descargue todas las reglas Yara del subdirectorio **signature_keyword** en el subdirectorio que aparece a continuación y ahora me queda colocarlas todas en un subdirectorio que llamare **signature_keyword** en el subdirectorio **yara_rules** original.

```
(venv) osboxes@osboxes:~/my-repo$ ls
yara_rules
(venv) osboxes@osboxes:~/my-repo$ cd yara_rules
(venv) osboxes@osboxes:~/my-repo/yara_rules$ ls
signature_keyword
(venv) osboxes@osboxes:~/my-repo/yara_rules$ cd signature_keyword
(venv) osboxes@osboxes:~/my-repo/yara_rules/signature_keyword$ ls
A-C  D-F  G-H  I-K  L-N  O-Q  R-T  U-W  X-Z
(venv) osboxes@osboxes:~/my-repo/yara_rules/signature_keyword$ cd A-C
(venv) osboxes@osboxes:~/my-repo/yara_rules/signature_keyword/A-C$ ls
 adfind.yara                  AmsiBypass.yara            Backstab.yara        BlockEtw.yara
 adPEAS.yara                 'Antivirus Signature.yara'  BadPotato.yara       bulletpassview.yara
 adrecon.yara                 antSword.yara              BadRentdrv2.yara    'Burntcigar KillAV.yara'
'advanced port scanner.yara'  AnyplaceControl.yara       Bat-Potato.yara      Carbanak.yara
 Adzok.yara                   arp.yara                   BeRoot.yara          cp.yara
'Ammyy Admin.yara'            AsyncRAT-C-Sharp.yara      BITSInject.yara      cryptomining.yara
 Amnesiac.yara                auditd.yara                Blank-Grabber.yara   cstealer.yara
(venv) osboxes@osboxes:~/my-repo/yara_rules/signature_keyword/A-C$
```

Si en la ejecución de las pruebas del programa necesito eliminar el contenido del subdirectorio malware_samples por alguna razón como que el programa repita los .exe cada vez que se ejecute el siguiente comando lo hace:

```
(venv) osboxes@osboxes:~$ rm -rf ~/malware_samples/*
(venv) osboxes@osboxes:~$ cd malware_samples
(venv) osboxes@osboxes:~/malware_samples$ ls
```

Copio el Malware/Ransomware .exe Windows, que está en /Home/Downloads/ al subdirectorio de malware_samples:

El siguiente screenshot muestra el bash para compilar las reglas yara manualmente de tres repositorios de GitHub: Cape, ReversingLabs y el subdirectorio signature_keyword de ThreatHunts. Pero antes tuve que cambiar los permisos porque no me dejaba crear el archivo **rules_compiled**.

```
(venv) osboxes@osboxes:~$ chmod u+w ~/yara_rules
```

```
(venv) osboxes@osboxes:~$ ls
bash_rm_malware  Documents  malware_samples  Pictures  scan_malware.py  Templates  Videos      yara_rules.py
Desktop          Downloads  Music            Public    snap             venv       yara_rules  yara_rules.py_1
```

```bash
yarac \
  ~/yara_rules/Cape/*.yar \
  ~/yara_rules/ReversingLabs/*.yara \
  ~/yara_rules/signature_keyword/*.yara \
  ~/yara_rules/rules-compiled
```

Ahí aparece el archivo rules_compiled.

```
(venv) osboxes@osboxes:~/yara_rules$ ls
Cape  Cape_1  Neo23x0  ReversingLabs  ReversingLabs_1  rules-compiled  signature_keyword
```

```
(venv) osboxes@osboxes:~$ cp ~/Downloads/*.zip ~/malware_samples/
(venv) osboxes@osboxes:~$ cd malware_samples
(venv) osboxes@osboxes:~/malware_samples$ ls
VirusShare_01ec08e3ef7d262891318dbc646db535.zip
VirusShare_0ebe19e549781865af5659e40132094c.zip
VirusShare_118094385cdbc55a1a8b478881109200.zip
VirusShare_14fe92196204effcebf383b6c229fa20.zip
VirusShare_17fac44461415765c8ec7cc6edfecefa.zip
VirusShare_1a27fceaa8cf30b45e58957195768a4e.zip
VirusShare_1bd18a8ce1a8dc4a40efb08bab9cb349.zip
VirusShare_207d4565d00f14a24a00e416681b70ef.zip
```

El programa Python siguiente descompacta de .zip a .exe:

```
(venv) osboxes@osboxes:~$ ls
Desktop    Downloads        Music     Public           snap       venv    yara_rules
Documents  malware_samples  Pictures  scan_malware.py  Templates  Videos  yara_rules.py
```

```
(venv) osboxes@osboxes:~$ ls
Desktop    Downloads        Music     Public           snap       venv    yara_rules
Documents  malware_samples  Pictures  scan_malware.py  Templates  Videos  yara_rules.py
(venv) osboxes@osboxes:~$ python scan_malware.py
```

```
Match encontrado en /home/osboxes/malware_samples/VirusShare_bdbd4fc61359702f2d19448f646a8b5e/de323a65795ab0f4935
4810b1609b7a6a48aae6bffc8561fb2c18b706e2d186: [SUSP_ELF_LNX_UPX_Compressed_File]
```

```
Match encontrado en /home/osboxes/malware_samples/VirusShare_2519c98f42652c037fa0cda2e6c1521d/666824d5b0f417241675
72a0a3e7842e5daf129a9825c57fe90177e236eb1c01: [SUSP_Imphash_Mar23_3]
```

```
Match encontrado en /home/osboxes/malware_samples/VirusShare_3cae48b354efc49cb552eb31b8dc5dc5/e70cbe73cf82874ef820
bd9d89163058dae6d237ad5ff4dcfae06352255c8136: [SUSP_ELF_LNX_UPX_Compressed_File]
```

```
Match encontrado en /home/osboxes/malware_samples/VirusShare_70af4fbaba8db3473f348bd0c87b0e64/59e285d12ad8a15e0516
3e1fdfd6044a89baf7bf198639dc86b9ff40747ecbfc: [SUSP_Imphash_Mar23_3]
Archivo descomprimido con éxito: /home/osboxes/malware_samples/VirusShare_d2c30edc9e6b8b0c23c48fcd2174151f.zip
Match encontrado en /home/osboxes/malware_samples/VirusShare_d2c30edc9e6b8b0c23c48fcd2174151f/e940adf69acf6525fd8f
05b54f289d0a85ff1c779086a8af9fcbb00c6a39f547: [SUSP_ELF_LNX_UPX_Compressed_File]
```

```
Match encontrado en /home/osboxes/malware_samples/VirusShare_2872ca7c0d549f058d4a1ca8316837c3/3a6ce58cbe810517f7b1
d1e1a9c7c509e695a35a3d7cbc749f1930ff9f197272: [SUSP_ELF_LNX_UPX_Compressed_File]
```

```
Match encontrado en /home/osboxes/malware_samples/VirusShare_d25424996ad8be44cde19921deefecc0/6e12275e6e97816d6406
7be52eeb832289cb98179a3444214a7ab6be84b91df1: [SUSP_ELF_LNX_UPX_Compressed_File]
Archivo descomprimido con éxito: /home/osboxes/malware_samples/VirusShare_ffc17dc3993e79642746e725f538dab8.zip
Match encontrado en /home/osboxes/malware_samples/VirusShare_ffc17dc3993e79642746e725f538dab8/85c57b6512b948330182
8f4a50d36e4c707454bd912ead9f287fa0cd2a3e8cbc: [SUSP_ELF_LNX_UPX_Compressed_File]
Archivo descomprimido con éxito: /home/osboxes/malware_samples/VirusShare_ccad735893a01f2e6ffd10d20eca5ce5.zip
```