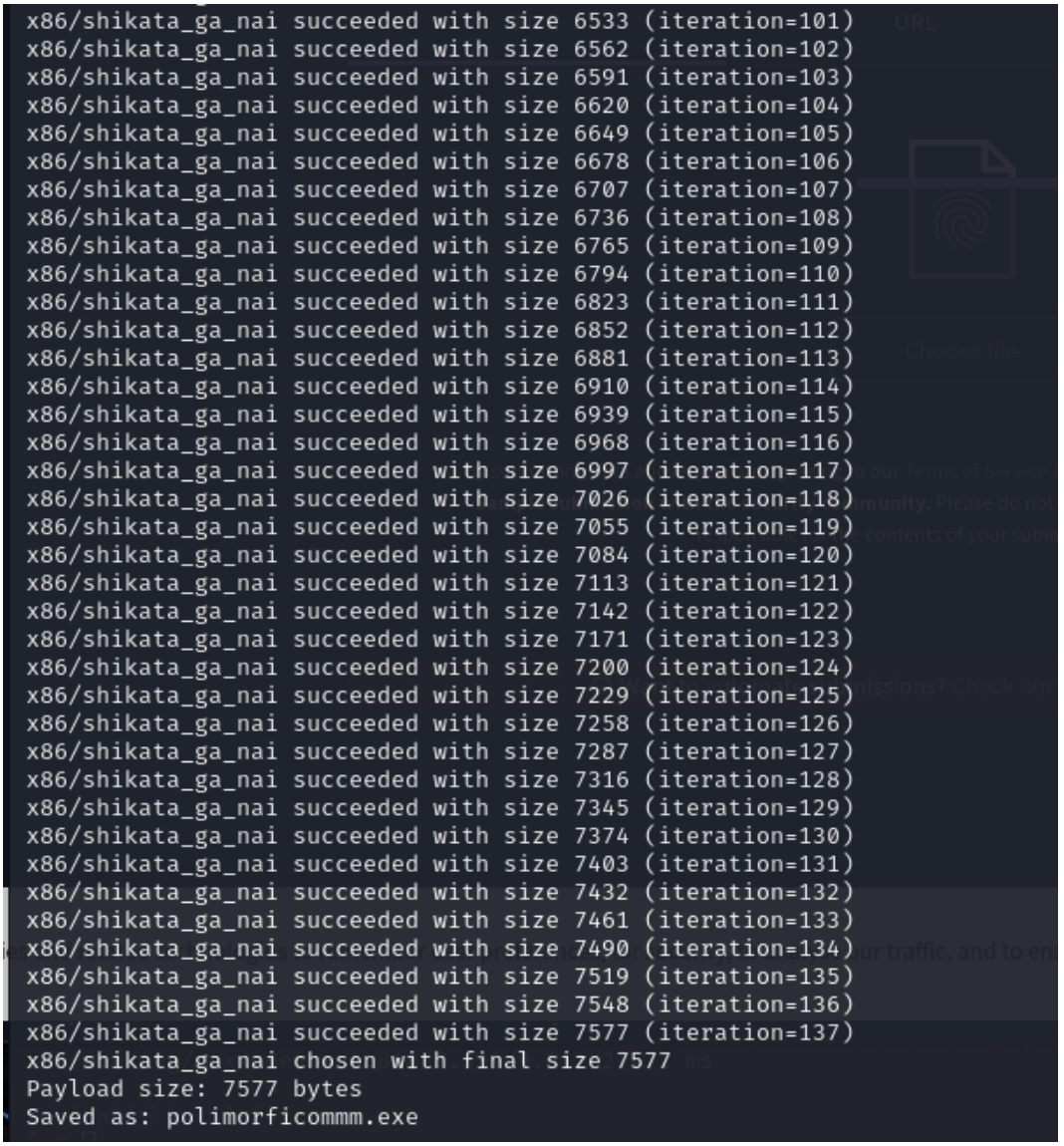
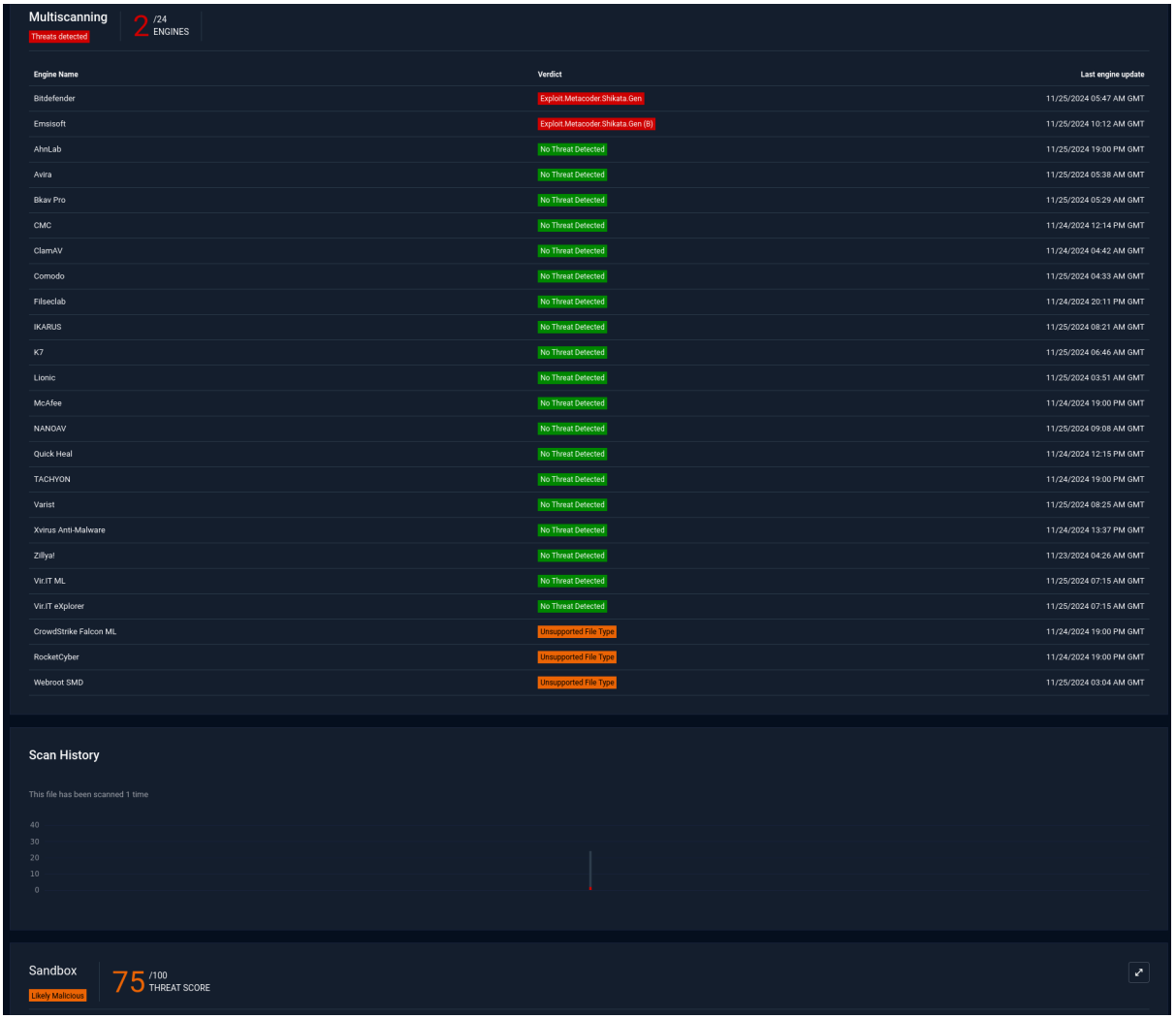
Esercizio S9L1 - msfvenom e VirusTotal

In questo esercizio, ho utilizzato msfvenom per creare un payload di tipo meterpreter con un reverse TCP, utilizzando più tecniche di offuscamento. Lo scopo era generare un payload che fosse in grado di sfuggire ai sistemi di rilevamento antivirus. La configurazione originale prevedeva l'uso dell'encoder shikata_ga_nai e countdown. Successivamente, ho verificato l'efficacia del payload su una piattaforma di analisi dei file, come MetaDefender, per valutarne la rilevabilità.

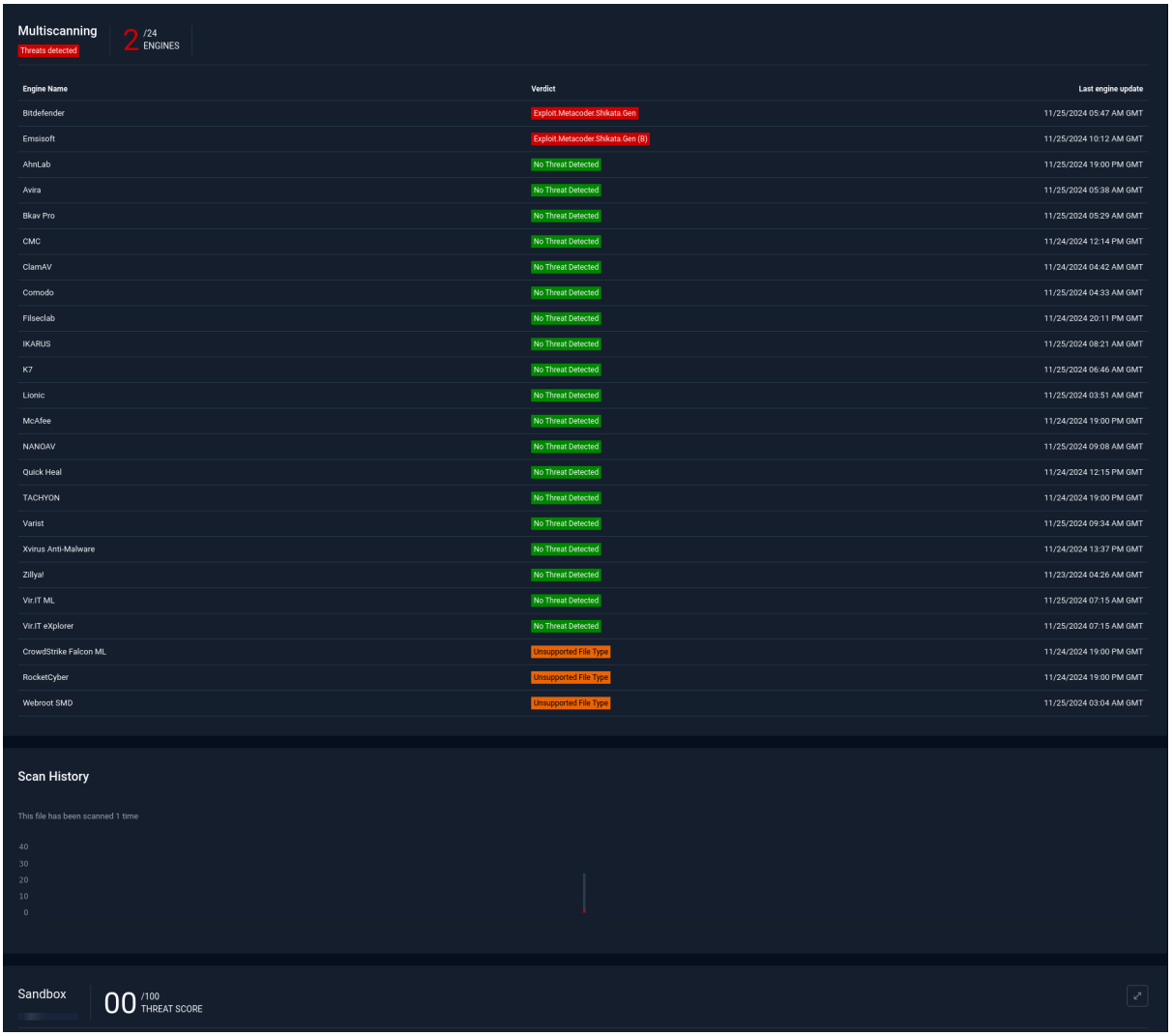


Lo screenshot mostra il comando eseguito per generare il payload con msfvenom. Il comando utilizza una combinazione di encoder per creare un file .exe chiamato polimorficomm.exe, con l'intento di rendere il file meno rilevabile. Il risultato finale è stato un payload pronto per essere testato su MetaDefender.

Il payload iniziale, dopo essere stato caricato su MetaDefender, ha ricevuto un punteggio di 75/100. Questo risultato suggerisce che il payload è stato rilevato da alcune delle soluzioni antivirus analizzate dalla piattaforma, ma non da tutte.



Successivamente, ho rifatto il payload utilizzando una combinazione di encoder aggiuntivi come xor_dynamic e più iterazioni di shikata_ga_nai. Questo nuovo payload, denominato polimorficomm2.exe, è stato caricato su MetaDefender, che ha restituito un punteggio di 0/100. Ciò indica che il nuovo file è stato completamente invisibile ai rilevatori antivirus presenti nella piattaforma, suggerendo un miglioramento significativo nell'offuscamento.



Il risultato finale dimostra come l'uso di tecniche multiple di offuscamento, combinando diversi encoder e aumentando le iterazioni, possa migliorare notevolmente la capacità di sfuggire ai sistemi di rilevamento antivirus. Sebbene non esista una soluzione definitiva per evitare completamente il rilevamento, l'uso di metodi avanzati, come quelli mostrati, riduce significativamente le probabilità di identificazione.