Esercizio S10-L2

L’obiettivo dell’esercizio era eseguire una analisi dinamica basica su un malware.

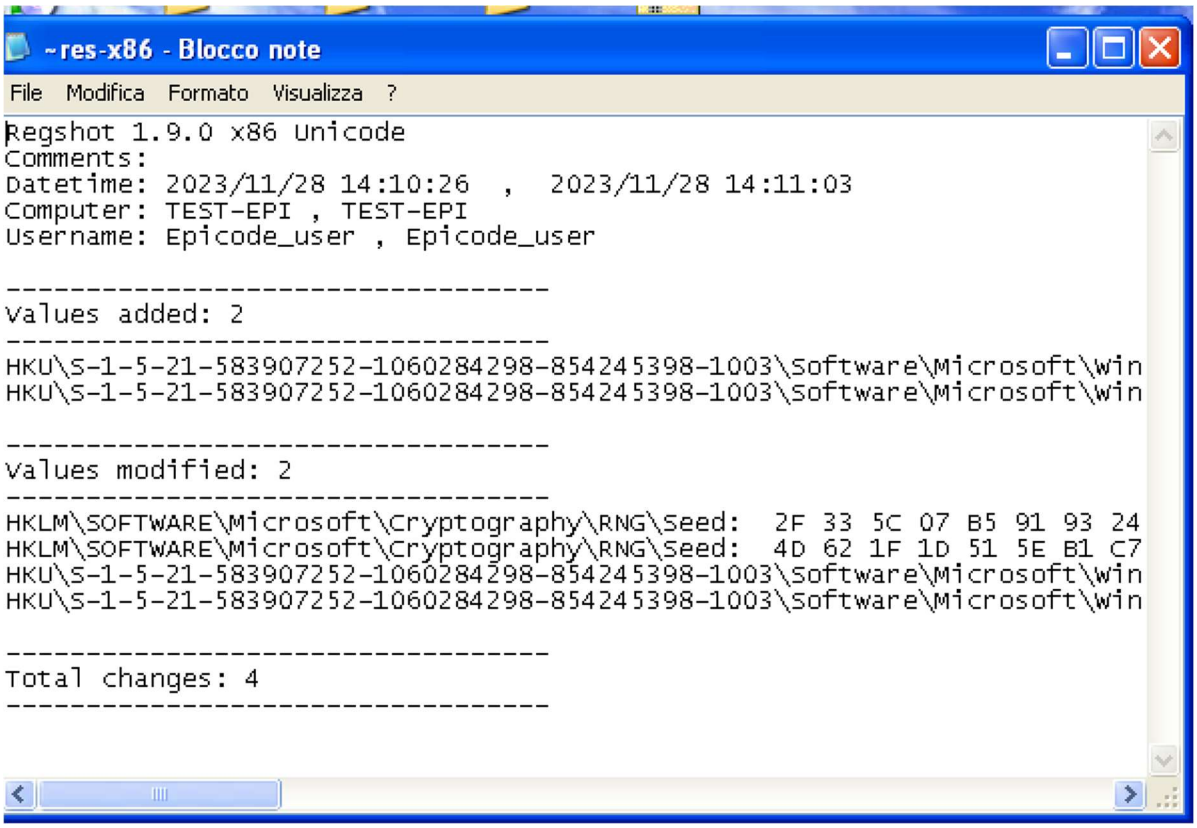
Il procedimento utilizzato è stato aprire procmon (cosi da non avere dei dati “falsati” aprendo regshot successivamente) e poi regshot, eseguendo il primo shot.

Aperti entrambi i programmi si può andare ad avviare il malware.

Dopo averlo avviato e lasciato runnare per un po' si esegue il secondo shot con reghsot.

Su procmon adesso, si può andare ad indagare sui processi del malware. Io li ho trovati impostando un filtro corrispondente a “nome processo, contenente, “Malware””.

Time...	Process Name	PID	Operation	Path	Result	Detail
15.10....	Malware_U3_...	1332	Process Start		SUCCESS	Parent PID: 1416, ...
15.10....	Malware_U3_...	1332	Thread Create		SUCCESS	Thread ID: 788
15.10....	Malware_U3_...	1332	Load Image	C:\Documents and Settings\Epicode_u...	SUCCESS	Image Base: 0x400...
15.10....	Malware_U3_...	1332	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
15.10....	Malware_U3_...	1332	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
15.10....	Malware_U3_...	1332	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b...
15.10....	Malware_U3_...	1332	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77b...
15.10....	Malware_U3_...	1332	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77f...
15.10....	Malware_U3_...	1332	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77d...
15.10....	Malware_U3_...	1332	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f...
15.10....	Malware_U3_...	1332	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 700, Comman...
15.10....	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe					Thread ID: 788, Us...
15.10....	Malware_U3_...	1332	Process Exit		SUCCESS	Exit Status: 0, User...



Su procmon è possibile osservare nel path le librerie usate dal malware, incontrate già nella lezione sull’analisi statica basica.

Inoltre, è possibile capire che il malware è un keylogger dato che verrà creato un file di testo nella cartella del malware nel quale verrà scritto tutto ciò che l'utente digita dopo l'esecuzione del malware.