ESERCIZIO

L'esercizio di oggi consiste nel aprire il file sul desktop di windows xp malware analysis e rispondere ai seguenti quesiti

1. Le librerie importate dal malware con descrizione
2. Indicare le sezioni del malware con descrizione
3. Aggiungere una considerazione finale

1. IMPORT LIBRERIE

Utilizzando CFF Explorer, vediamo dalla sezione import directory che il malware U3_W2_L1 importa 4 librerie:
Kernel32.dll, che include le funzioni core del sistema operativo
Advapi32.dll, che include le funzione per interagire con registri e servizi Windows
MSVCRT.dll, libreria scritta in C per la manipolazione scritte o allocazione memoria
Wininet.dll, include le funzione per implementare i servizi di rete come ftp, ntp, http

szAnsi	(nFunctions)	Dword	Dword	Dword	Dw
KERNEL32.DLL	6	00000000	00000000	00000000	000
ADVAPI32.dll	1	00000000	00000000	00000000	000
MSVCRT.dll	1	00000000	00000000	00000000	000
WININET.dll	1	00000000	00000000	00000000	000

2. SELEZIONE DEL MALWARE:
   Da CFF Explorer, dalla sezione «section header» vediamo che l'eseguibile si compone di 3 sezioni. Purtroppo sembra che il malware abbia nascosto il vero nome delle sezioni e quindi non siamo in grado di capire che tipo di sezioni sono.

Byte[8]	Dword	Dword	Dword	Dword
UPX0	00004000	00001000	00000000	00000400
UPX1	00001000	00005000	00000600	00000400
UPX2	00001000	00006000	00000200	00000A00

3. CONSIDERAZIONE FINALE:
   Si tratta di un malware avanzato che non ci consente di recuperare molte informazioni sul suo comportamento con l'analisi statica basica. Ciò è supportato dal fatto che tra le funzioni importate troviamo «LoadLibrary e GetProcAddress», che ci fanno pensare ad un malware che importa le librerie a tempo di esecuzione (runtime) nascondendo di fatto le informazioni circa le librerie importate a monte.