S10/L1

L’esercizio di oggi prevede di analizzare un malware con il tool CFF explorer.
Si tratta di un’analisi statica basica, ovvero consiste nell’esaminare un file eseguibile senza vedere le istruzioni che lo compongono.

Traccia:
Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul Desktop della vostra macchina virtuale dedicata all’analisi dei malware, rispondere ai seguenti quesiti:
• Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse.
• Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa.
• Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte.

Il primo punto ci chiede di indicare le librerie importate dal malware.
Apriamo nella cartella Esercizio_Pratico_U3_W2_L1 il file del malware con CFF explorer.

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

Le librerie sono le seguenti:

Kernel32.dll: contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.

Advapi32.dll: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo

MSVCRT.dll: contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.

Wininet.dll: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Le sezioni del malware sono contenute in "Section headers" e sono indicate in rosso nell'immagine.

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
000001D8	000001E0	000001E4	000001E8	000001EC	000001F0	000001F4	000001F8	000001FA	000001FC
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Le sezioni del malware sono criptate e non si riesce a capire cosa ci sia all'interno.