Malware analysis

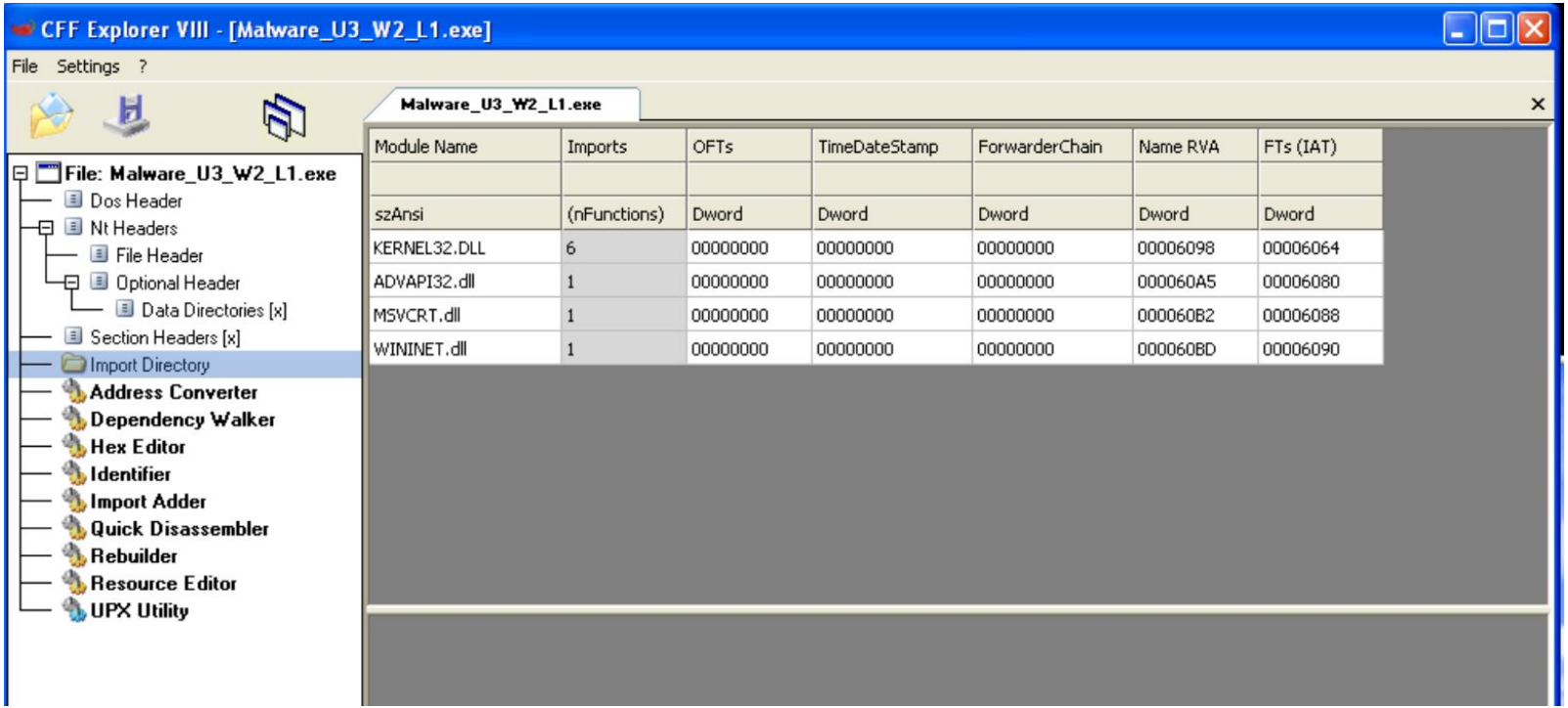
Analisi statica basica

Esercizio_Pratico_U3_W2_L1

L’esercizio di oggi consiste nell'analisi del malware che troviamo preinstallato sulla macchina.

Abbiamo utilizzato CFF Explorer per individuare le varie librerie utilizzate, nella sezione ‘Import Directory’. Nella sezione ‘section Headers’, invece, troviamo la sezione da cui è composto.

Librerie presenti



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

Librerie presenti nel malware

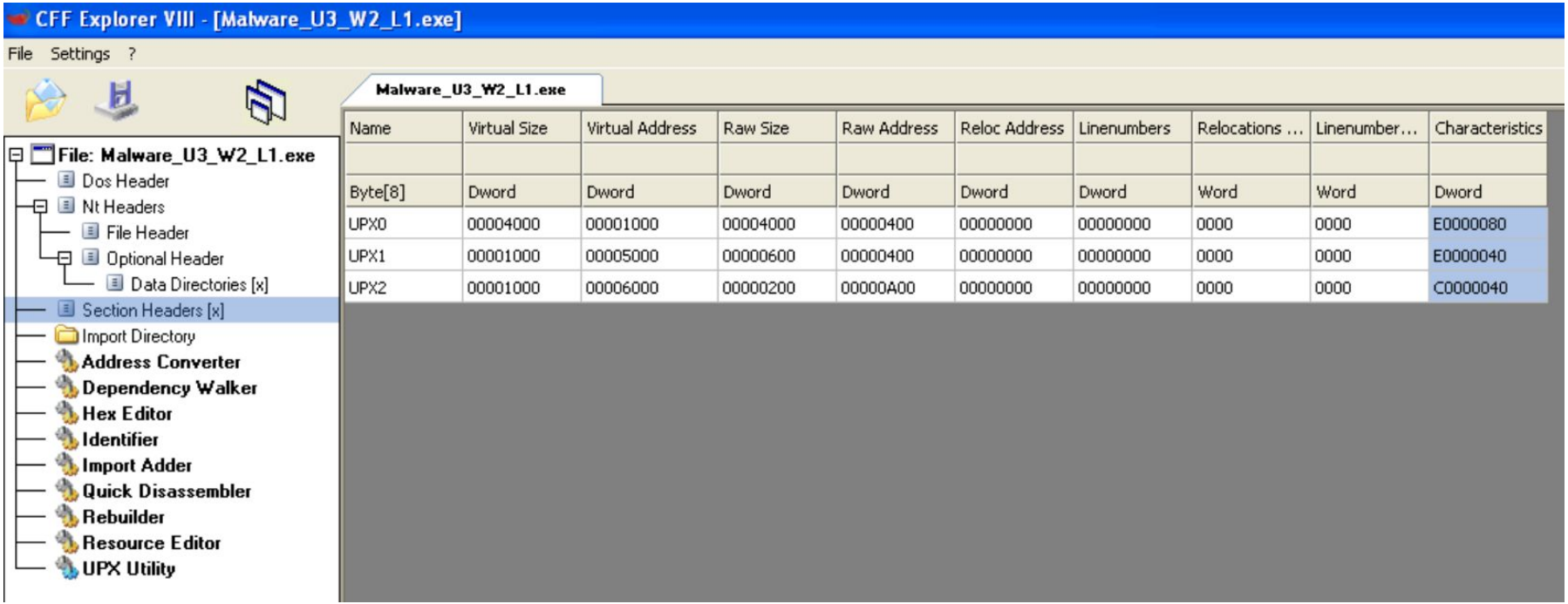
Kernel32.dll: libreria contenente funzioni principali per interagire con il OS (es. gestione memoria);

Advapi32.dll: libreria contenente funzioni per interagire con i servizi ed i registri dell os

MSVCRT.dll: libreria contenente funzioni per la manipolazione di stringhe, allocazione memoria;

Wininet.dll: libreria contenente funzioni per l'implementazione di alcuni protocolli come HTTP, FTP, NTP.

Sezioni che compongono il malware



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00004000	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

Sezioni

Le sezioni più comuni di un file sono: .text, .rdata, .data, .rsrc. mentre qui troviamo i file UPX0, UPX1 e UPX2, questi ultimi devono essere spacchettati con un codice.

UPX è un packer open-source , forse il più conosciuto.