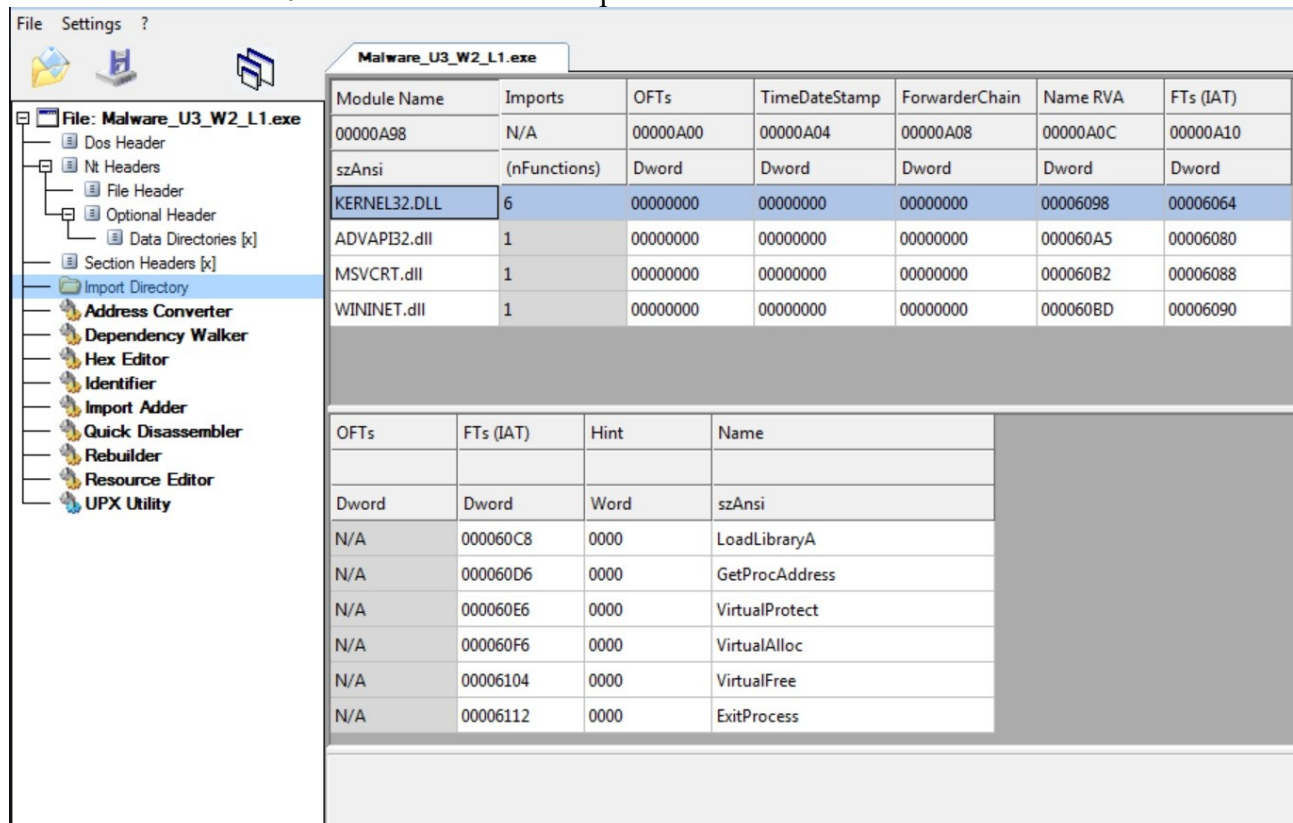


Esercizio settimana 10 lezione 1 Daniele D'Esposito

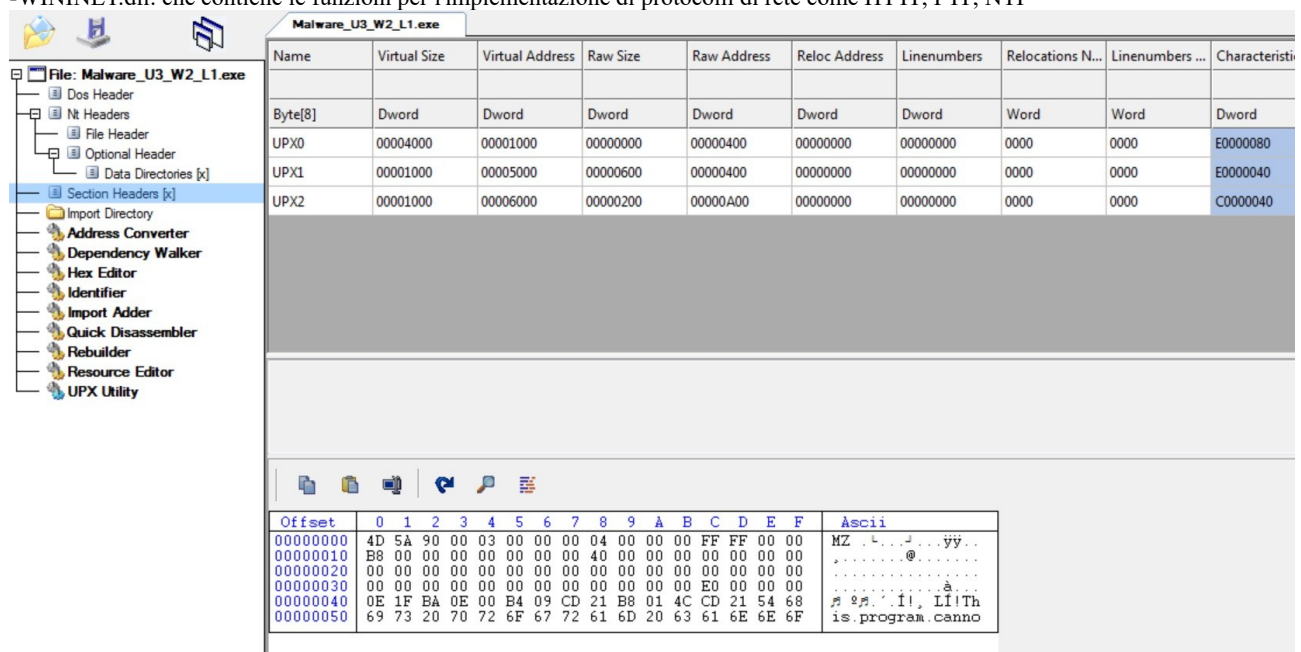


Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	000060C8	0000	LoadLibraryA
N/A	000060D6	0000	GetProcAddress
N/A	000060E6	0000	VirtualProtect
N/A	000060F6	0000	VirtualAlloc
N/A	00006104	0000	VirtualFree
N/A	00006112	0000	ExitProcess

inserendo l'applicazione da analizzare su CFF Explorer VIII si possono vedere nella cartella import directory tutte le librerie utilizzate dal programma, in questo caso sono:

- KERNEL32.DLL: che contiene le funzioni principali per interagire col sistema operativo
- ADVAPI32.dll: che contiene le funzioni per interagire con i registri
- MSVCRT.dll: che contiene le funzioni per la manipolazione di stringhe e altro
- WININET.dll: che contiene le funzioni per l'implementazione di protocolli di rete come HTTP, FTP, NTP



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristi
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

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ yy .
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00 @
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	E0	00	00	00 A
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	is . program . canno
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	

Andando su section headers, si vede che le sezioni sono 3 ma dai nomi non si capisce che funzione hanno. Tra le funzioni della libreria KERNEL32 vi sono LoadLibraryA e GetProcAddress che servono a richiamare librerie durante l'esecuzione del programma e non in anticipo come si fa di solito.

CONSIDERAZIONI FINALI

E' un malware avanzato che nasconde le sue funzioni quindi non e' possibile trarre conclusioni solo da un'analisi statica basica