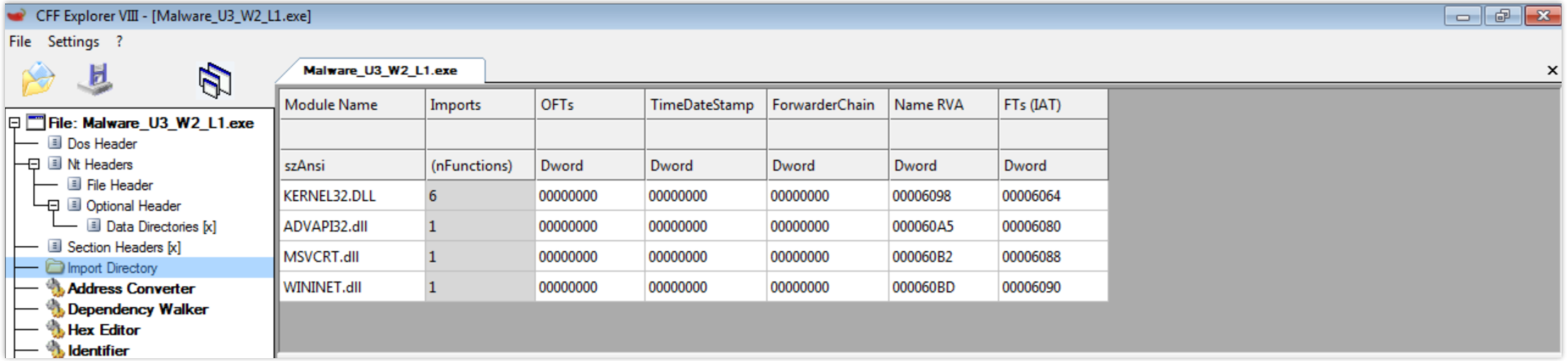
Esercizio S10/L1

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

PER VISUALIZZARE LE LIBRERIE IMPORTATE DAL MALWARE CI PORTIAMO AVANTI NELLA SEZIONE IMPORT DIRECTORY, OSSERVIAMO CHE IL MALWARE IMPORTA 4 LIBRERIE: KERNEL32.DLL,ADVAPI32.DLL,MSVCRT.DLL, WININET.DLL



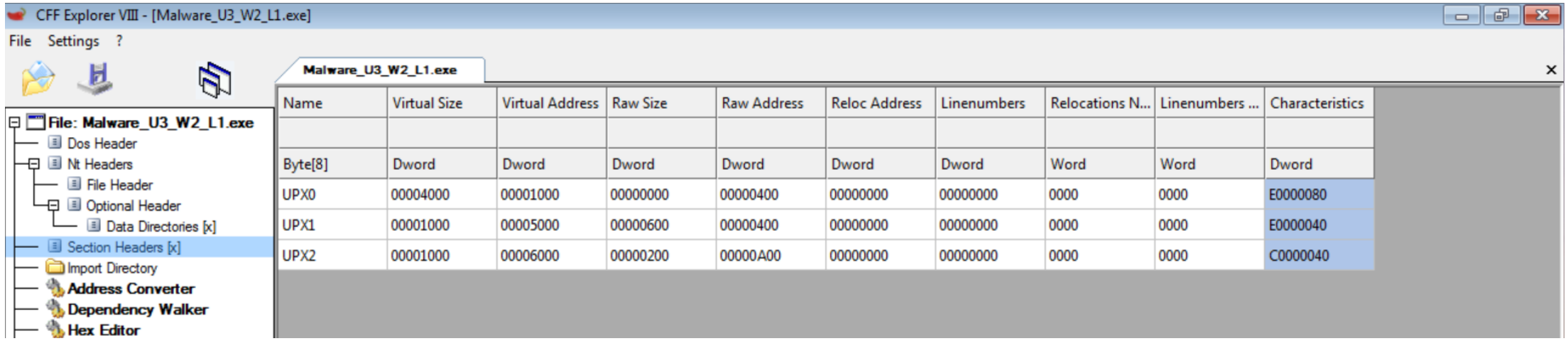
LIBRERIE MALWARE
COSA FANNO QUESTE LIBRERIE?

LIBRERIE MALWARE

- Kernel32.dll: è un modulo kernel di windows, è una libreria di collegamento a 32 bit utilizzata nel sistemi operativi windows. Viene caricato in memoria protetta all'avvio in modo da non essere danneggiato da altri processi del sistema. Svolge operazioni di input/output, gestione memoria.
- Advapi32.dll: libreria di servizi API avanzati, assegna l'accesso a funzionalità fornite al kernel. E' responsabile di cose come il riavvio del sistema, l'arresto, il registro di windows, gestione dell'account utente.
- Msvcrt.dll: è importantissimo per il sistema operativo di windows, contiene funzionalità e risorse utilizzate da programmi per eseguire attività come allocazione della memoria, input output, gestione di eccezioni.
- Wininet.dll: svolge un ruolo importante per le connessioni internet. E' responsabile della gestioni dei protocolli http, ftp, https,, la gestione dei cookie e della memoria cache.

Sezione del Malware

Per la visualizzazione della varie sezioni di cui è strutturato il malware, ci trasferiamo nella sezione "section headers(x), notiamo che il malware ha 3 diverse sezioni.



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

Notiamo che il malware ha "nascosto" il nome delle sezioni dando nomi come: UPX0, UPX1, UPX2,
Non permettendo di risalire al vero nome delle sezioni e non è possibile quindi analizzare approfonditamente le sezioni.

CONSIDERAZIONI FINALI

Dalle analisi appena effettuate, possiamo dire che il malware è in grado di nascondere le sezioni, è un malware avanzato che sfrutta le librerie e rende difficile l'analisi dettagliata sfruttando tecniche di analisi basica statica.