Consegna S10-L1

Analisi Malware

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

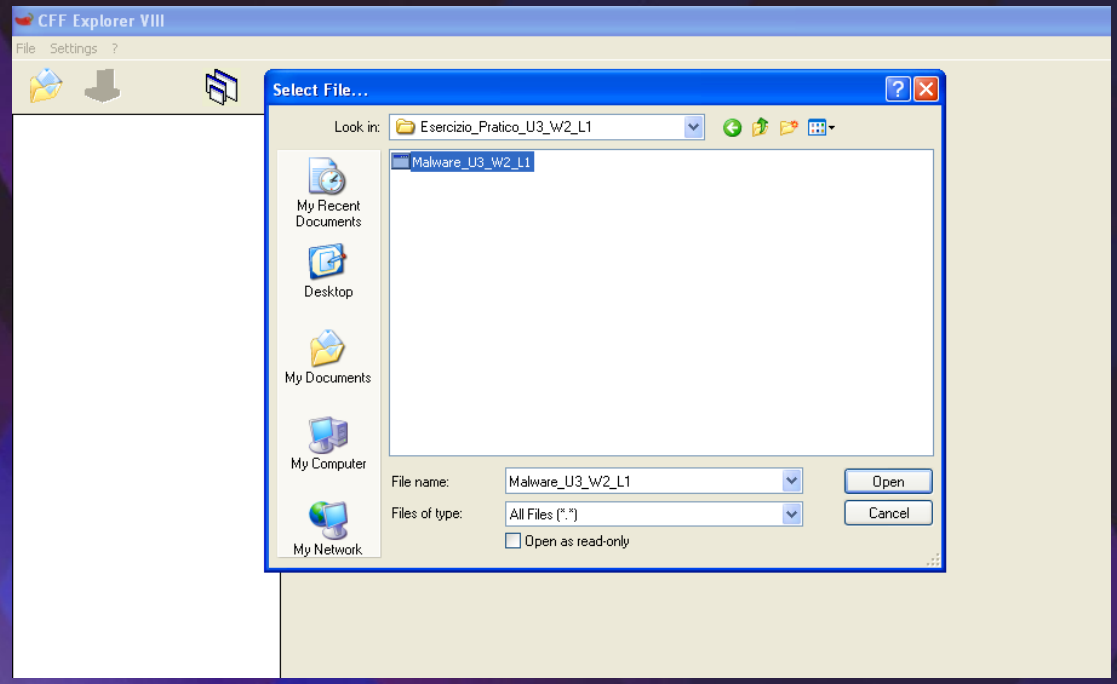
Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

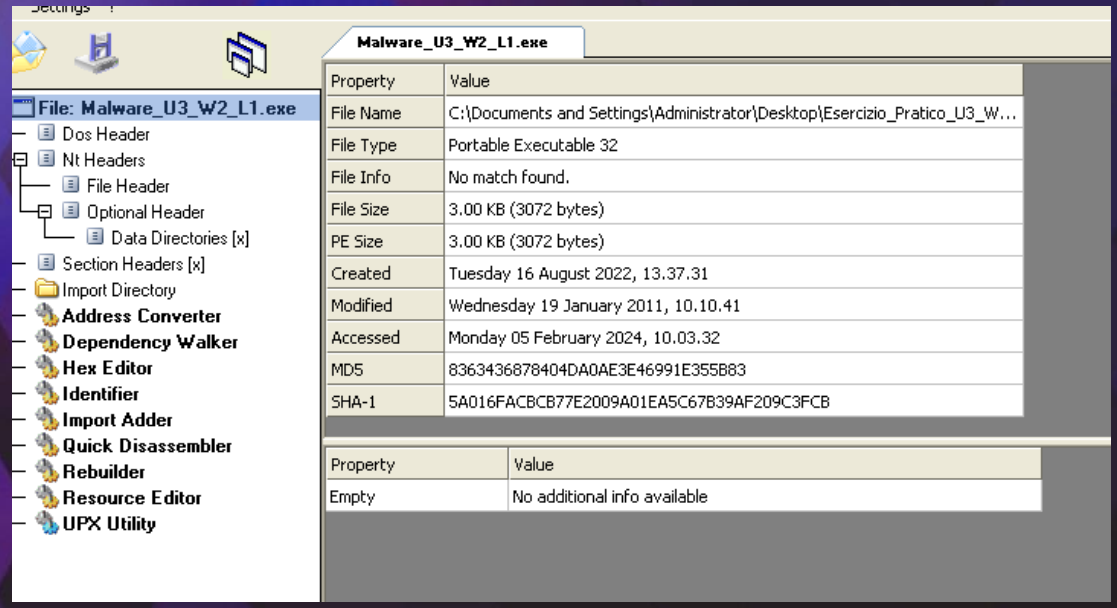
Installazione macchina virtuale

Per svolgere l'esercizio in sicurezza, dato che si ha a che fare con file dannosi, è stato necessario installare la macchina virtuale Malware Analysis su VirtualBox con rete disabilitata. Il sistema operativo della macchina è WindowsXP.

Utilizzo di CFF Explorer

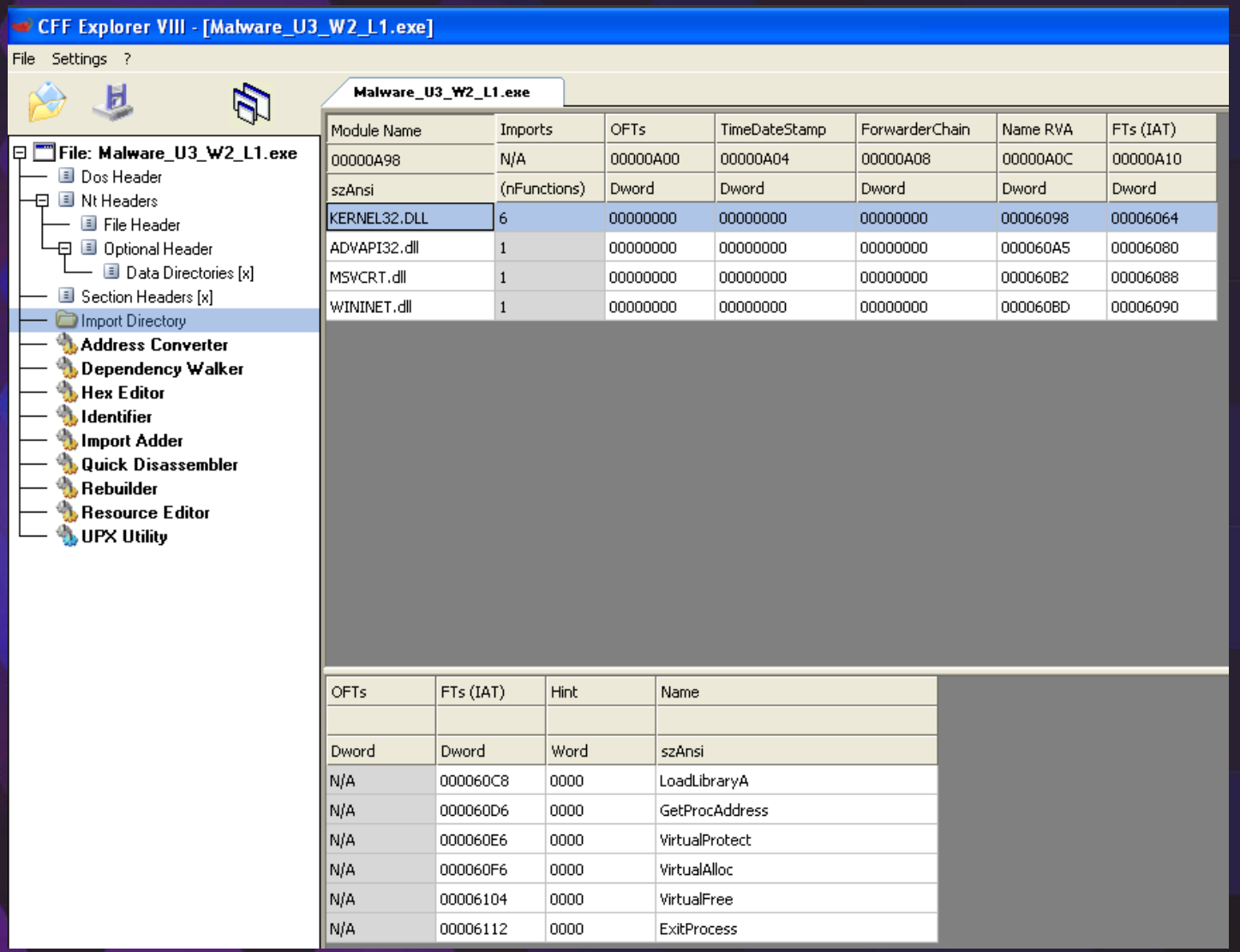
Dopo che CFF Explorer è stato avviato, è stato aperto il file richiesto dalla traccia. CFF Explorer è un tool preinstallato nella macchina che permette di controllare le funzioni importate ed esportate di un malware.





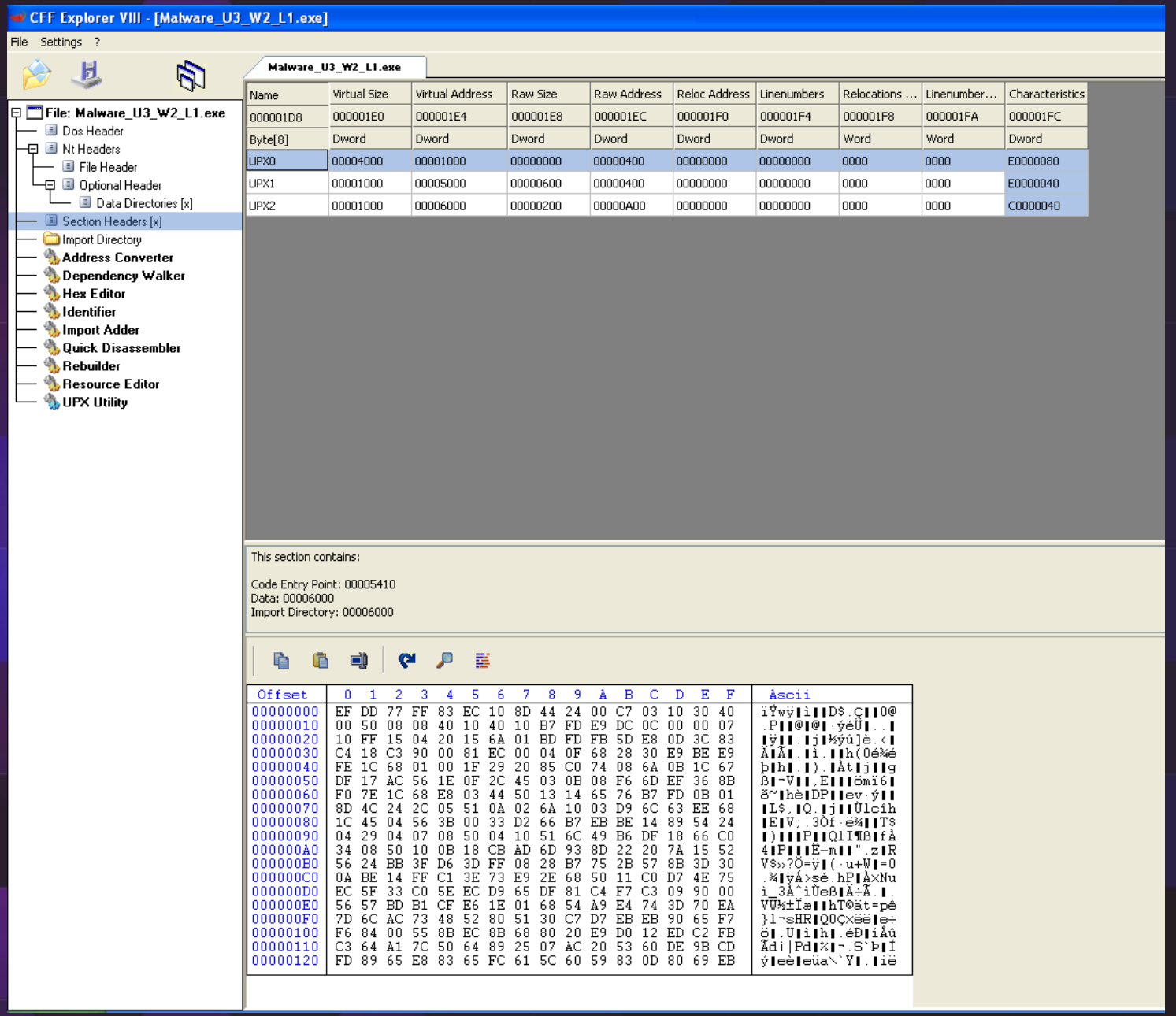
Analisi Import Directory

Selezionando la cartella Import Directory, è stato possibile accedere alla lista delle librerie importate dal malware. La tabella in basso analizza nel dettaglio la libreria al momento evidenziata. In questo caso la KERNEL 32.DLL che contiene le funzioni principali per interagire con il sistema operativo, ad esempio la manipolazione dei file e la gestione della memoria.



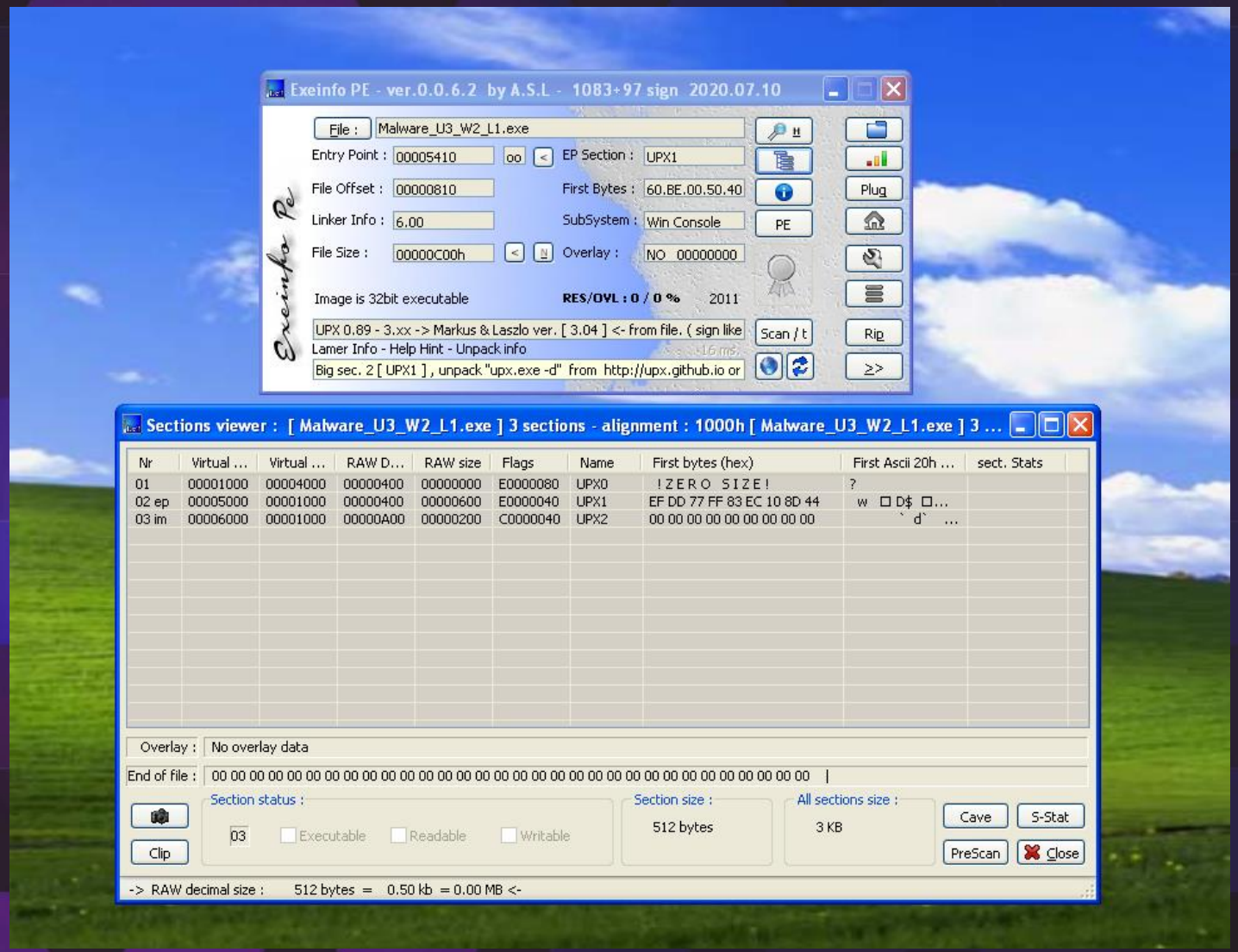
Analisi Section Headers

Nella sezione Section Headers è stato possibile controllare le informazioni circa le sezioni di cui si compone l'eseguibile. Il malware è diviso in tre parti, tutte compresse tramite lo strumento UPX.



Utilizzo ExeinfoPE

Per avere un secondo riscontro, è stato utilizzato anche il tollo ExeinfoPE. Una volta caricato il file dannoso sul programma, c'è stato un riscontro sulle informazioni riguardanti le sezioni del malware



Considerazioni

L’analisi statica non ha potuto fornirci molte informazioni sul malware. Alcuni malware, come quello in questione, utilizzano ad esempio il caricamento delle librerie durante l’esecuzione (runtime import) nascondendo di fatto all’analisi statica le funzioni e le librerie importate. Questi malware sono riconoscibili in quanto hanno generalmente poche entry nella sezione import, e tra esse figurano le funzioni «LoadLibrary e GetProcAddress» che vengono appunto utilizzate per caricare funzioni addizionali durante l’esecuzione.

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

Fine della presentazione

Amedeo Natalizi