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

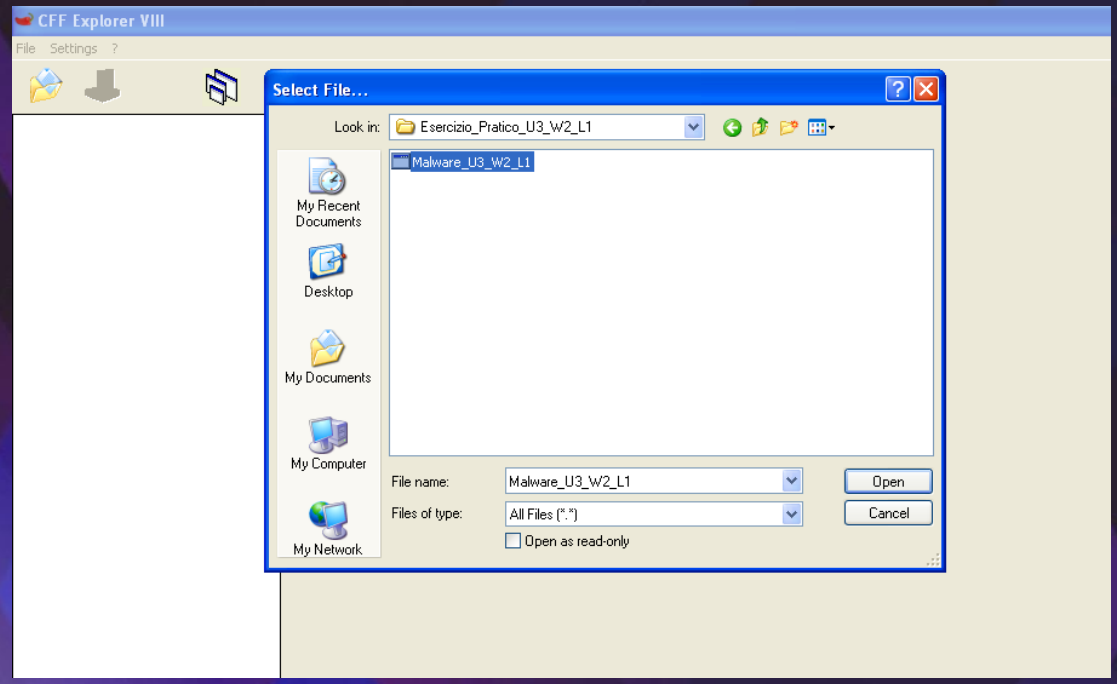
Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

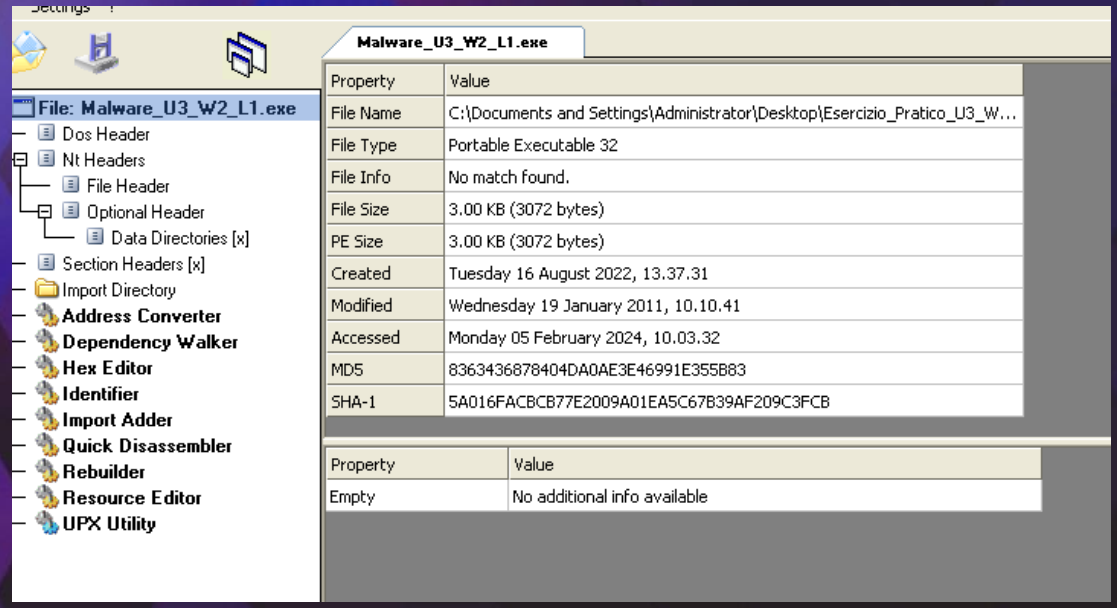
Installazione macchina virtuale

Per garantire un ambiente sicuro durante l'esecuzione dell'esercizio, è stato adottato l'approccio di utilizzare una macchina virtuale dedicata alla Malware Analysis su VirtualBox, con la connettività di rete disabilitata. La piattaforma operativa scelta per questa macchina virtuale è Windows XP.

Utilizzo di CFF Explorer

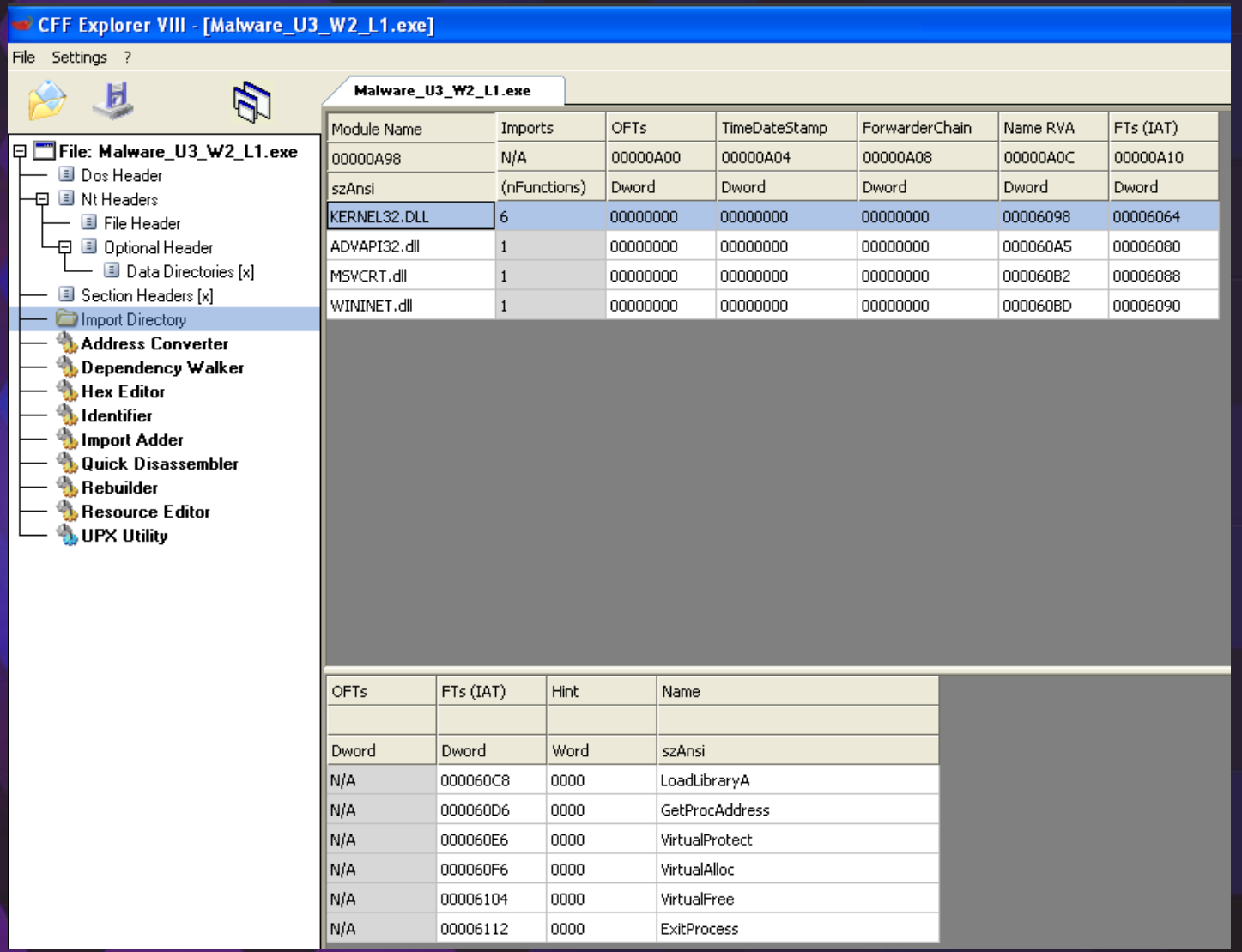
Dopo l'avvio di CFF Explorer, è stato aperto il file indicato nella traccia. CFF Explorer, un'applicazione già presente nella configurazione della macchina, offre la possibilità di analizzare le funzioni importate ed esportate di un malware.





Analisi Import Directory

Selezionando la directory di importazione nella cartella, è stato agevole esaminare l'elenco delle librerie importate dal malware. La tabella sottostante fornisce un'analisi dettagliata della libreria attualmente evidenziata, come nel caso della KERNEL32.DLL, la quale racchiude le funzioni fondamentali per interagire con il sistema operativo, come la manipolazione dei file e la gestione della memoria.

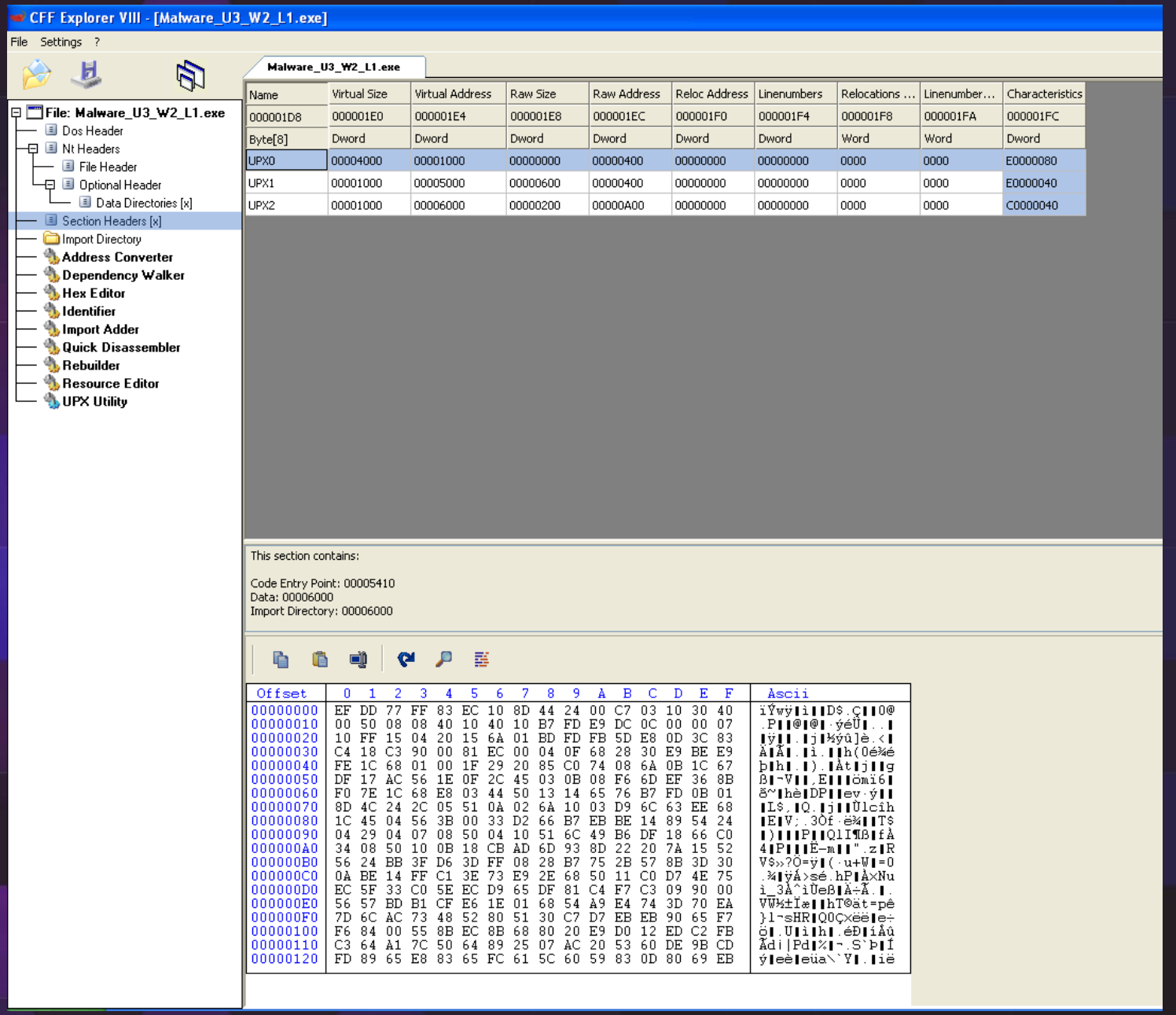


Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080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

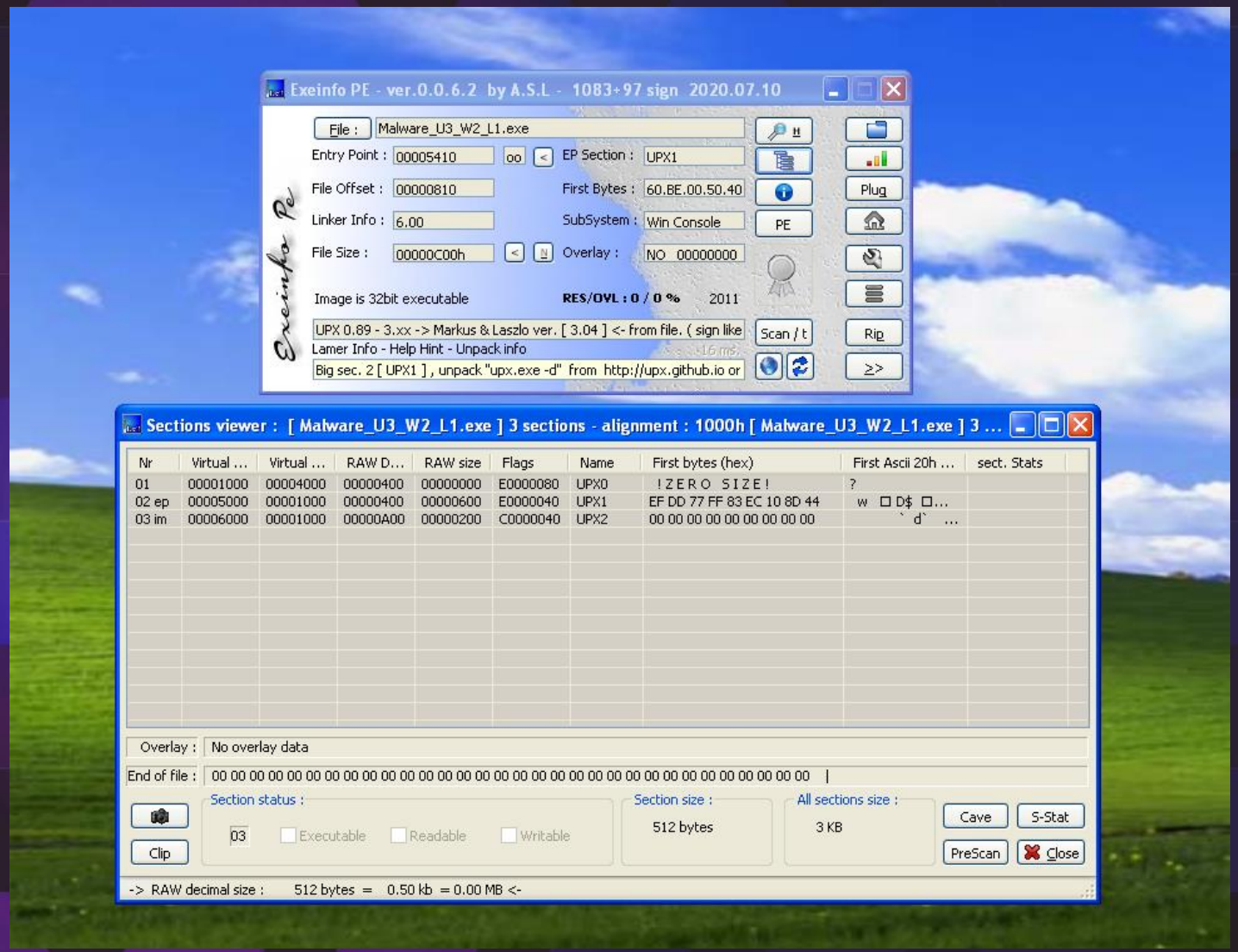
Analisi Section Headers

Nella sezione Section Headers, è stato possibile esaminare le informazioni relative alle sezioni costituenti dell'eseguibile. Il malware è suddiviso in tre parti, tutte compresse mediante l'utilizzo dello strumento UPX.



Utilizzo ExeinfoPE

Per ottenere una conferma aggiuntiva, è stato impiegato il tool ExeinfoPE. Caricando il file dannoso nel programma, sono state fornite ulteriori informazioni sulle sezioni del malware.



Considerazioni

L'analisi statica ha fornito poche informazioni sul malware in questione. Alcuni tipi di malware, come quello esaminato, adottano strategie come il caricamento dinamico delle librerie durante l'esecuzione (runtime import), rendendo di fatto nascoste all'analisi statica le funzioni e le librerie importate. Questi malware si distinguono spesso per la presenza limitata di voci nella sezione di importazione, tra cui spiccano le funzioni "LoadLibrary" e "GetProcAddress", utilizzate per caricare dinamicamente funzioni aggiuntive 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