

Presentation

S10-L1

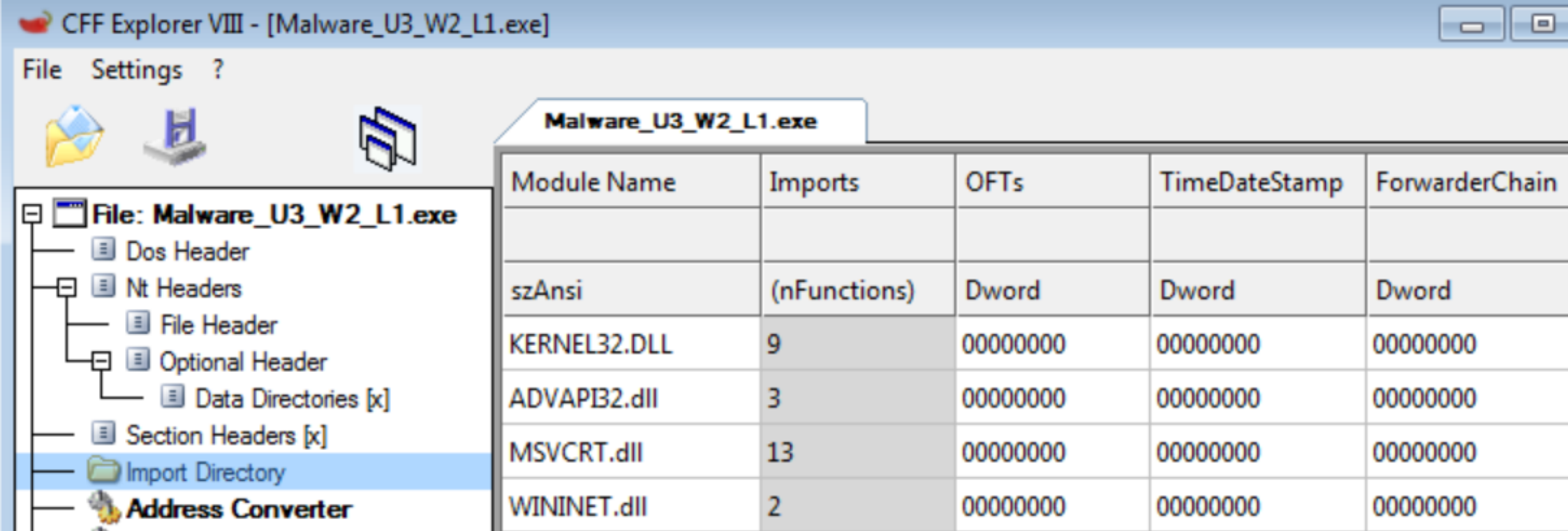
TRACCIA:

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



Grazie al software CFF explorer siamo in grado di analizzare il file .exe in questione, andiamo a vedere come controllare le librerie che vengono importate in questo software.

Le librerie vengono riprotate nella sezione “Import Directory”.



The screenshot shows the CFF Explorer VIII interface for the file Malware_U3_W2_L1.exe. The left pane displays the file's structure, with the 'Import Directory' selected. The right pane shows a table of imported modules.

Module Name	Imports	OFTs	TimeStamp	ForwarderChain
szAnsi	(nFunctions)	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000
ADVAPI32.dll	3	00000000	00000000	00000000
MSVCRT.dll	13	00000000	00000000	00000000
WININET.dll	2	00000000	00000000	00000000



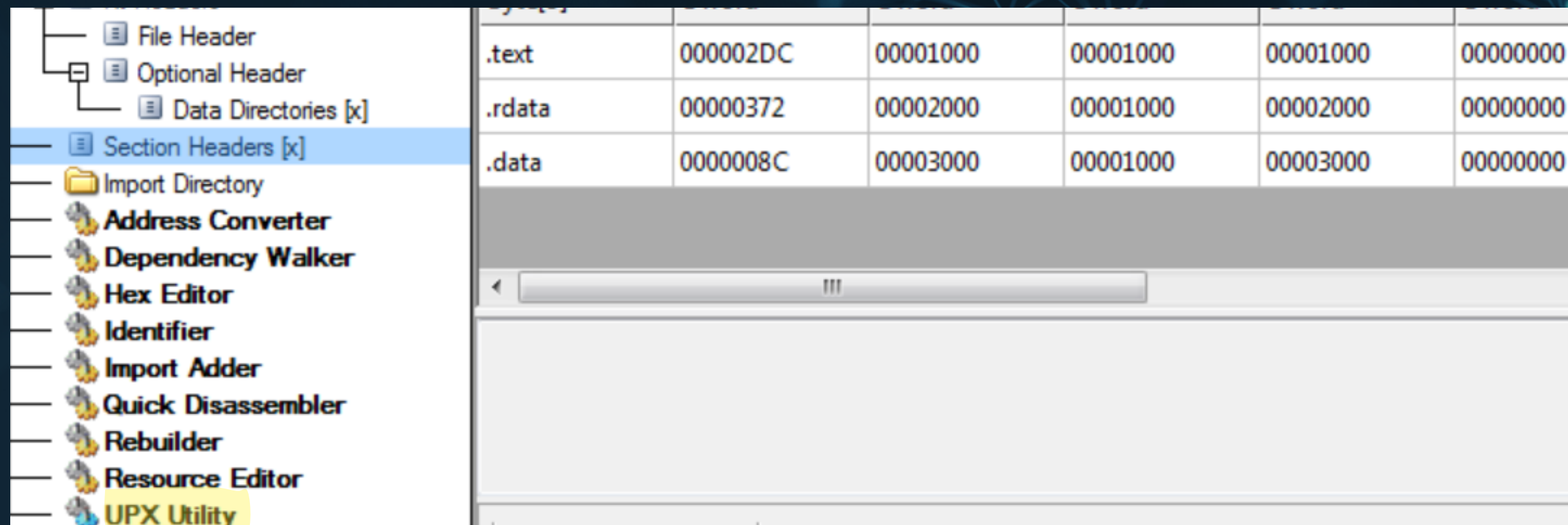
KERNEL32.DLL: Questa libreria fornisce diverse funzioni di base che sono essenziali per il corretto funzionamento di Windows. Tra le funzioni offerte vi sono la gestione della memoria, la gestione dei file e dei dispositivi di input/output, nonché la gestione degli errori e delle eccezioni.

ADVAPI32.DLL: Questa libreria fornisce funzioni per l'accesso al Registro di sistema, la gestione dei servizi di Windows, la crittografia dei dati e altre funzionalità avanzate di sicurezza e gestione del sistema.

MSVCRT.DLL: Questa libreria contiene le funzioni di runtime della libreria C di Microsoft Visual Studio. Essa fornisce supporto per diverse operazioni di input/output, gestione della memoria, operazioni matematiche e altre funzionalità di base.

WININET.DLL: Questa libreria fornisce un'interfaccia per accedere ai servizi Internet. Essa offre funzionalità per la gestione delle connessioni di rete, l'invio e la ricezione di richieste HTTP, nonché altre operazioni legate alla comunicazione su Internet.

Le sezioni di un malware si riferiscono alle diverse parti del codice malevolo che svolgono funzioni specifiche. Per analizzare queste sezioni a volte è necessario utilizzare la funzione "UPX Utiliy" messa a disposizione da "CFF Explorer" perché molte volte gli exe sono compressi o protetti da tecniche di "packing" che ne rendono difficile l'analisi diretta.



.data:

- **Questa sezione di un file eseguibile contiene principalmente dati inizializzati, come variabili globali o altre strutture dati che devono essere allocate e inizializzate prima che il programma venga eseguito.**

.text:

- **La sezione .text contiene il codice eseguibile, ovvero le istruzioni macchina che costituiscono il programma stesso. Questa sezione contiene il codice sorgente compilato che viene eseguito quando avvii il programma.**

.rdata:

- **Questa sezione contiene principalmente dati di sola lettura, come costanti o stringhe di testo che il programma utilizza durante l'esecuzione ma non modifica.**

Per sapere di più su questo file proviamo a inserirlo su virustotal, per avere un'idea più definita sul file in questione, come possiamo notare il file è stato etichettato come malware, nello specifico un Trojan, ovvero un file che potrebbe sembrare innocuo, ma in realtà potrebbe:

- rubare informazioni personali
- creare backdoor
- installare altri malware
- registrare le tue attività
- disabilitare firewall

