S10L1

Consegna:

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:

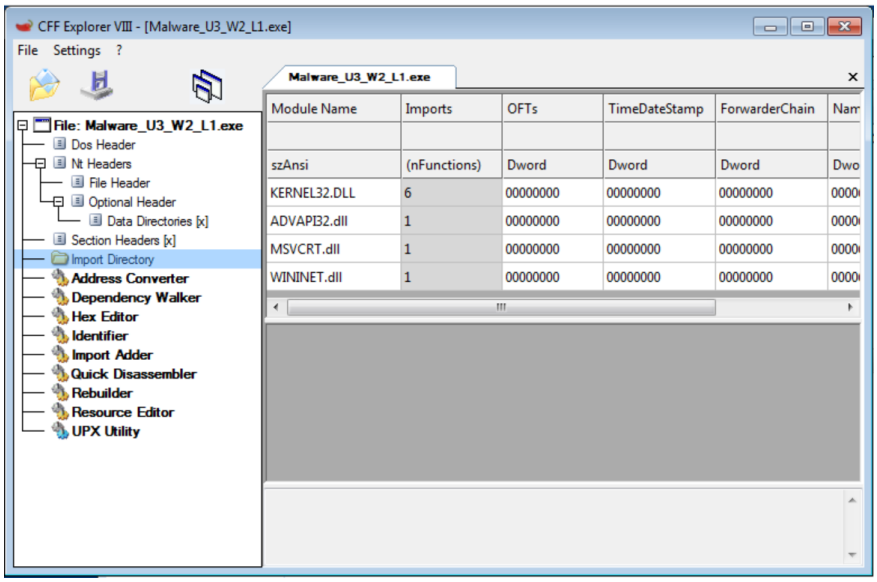
• Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse

• 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

Esecuzione:

Per poter controllare le librerie utilizzate da un malware si deve utilizzare un tool apposito, in questo caso è stato utilizzato "CFF Explorer" che consente di poter controllare anche le funzioni contenute nelle librerie.



Le librerie utilizzate dal malware sono:

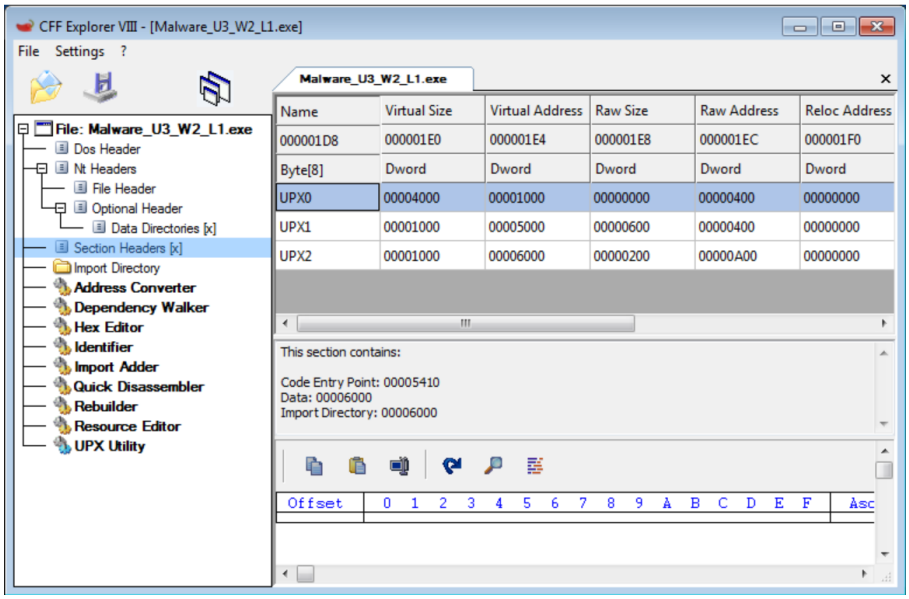
KERNEL32.DLL: è la libreria che contiene delle funzioni che si occupano dell'interazione con il sistema operativo su cui è stato fatto partire il malware

ADVAPI32.dll: è la libreria che contiene le funzioni relative all'interagire con i registri del sistema operativo su cui è stato fatti girare il malware

MSVCRT.dll: è la libreria che contiene le funzioni che si occupano della manipolazione delle stringhe di codice

WININET.dll: è la libreria che contiene le funzioni che si occupano di implementare ulteriori protocolli di rete

CFF Explorer consente anche di controllare le funzioni di un malware; tuttavia, quelle utilizzate dal programma analizzato sono state cifrate e non è possibile quali sezioni nello specifico sono state utilizzate, ma possiamo capire che ce ne sono almeno 3.



Per quanto riguarda le considerazioni finali si può constatare che è un malware decisamente troppo complesso per essere analizzato da una analisi statica basica, di conseguenza non è possibile essere sicuri sulle supposizioni.