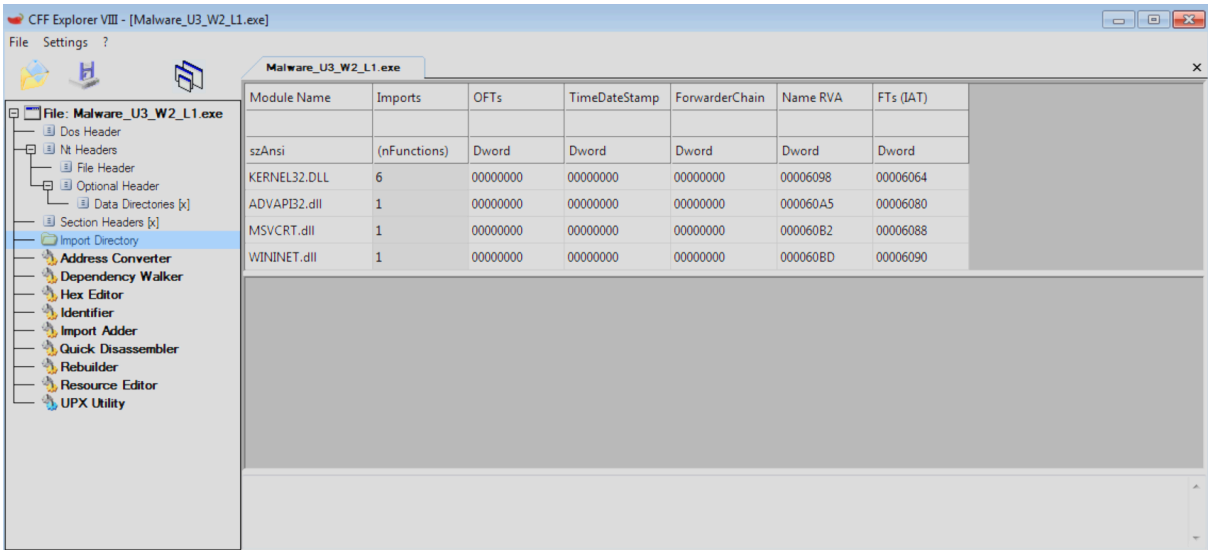
Lezione S10/L1
Rosario Giaimo

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

Svolgimento

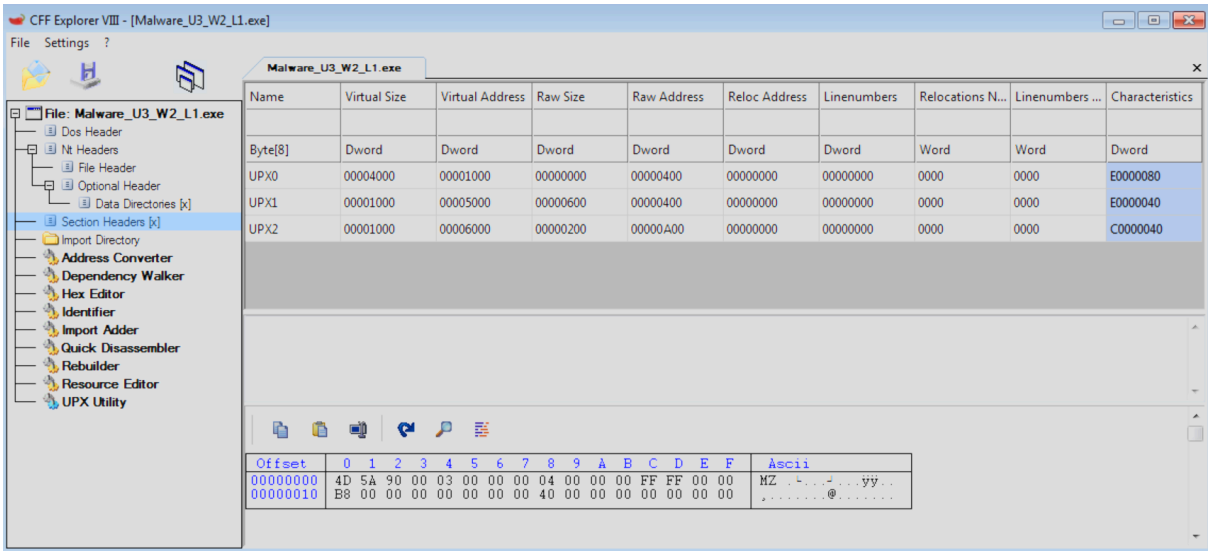
• Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse



KERNEL32.DLL: Questa DLL è una libreria fondamentale del sistema operativo Windows che fornisce funzioni di base come la gestione della memoria, la gestione dei processi e l'esecuzione del thread. È importata da quasi tutti i file eseguibili Windows.
ADVAPI32.dll: Questa DLL fornisce funzioni per l'autenticazione degli utenti, la gestione dei token di sicurezza e l'accesso al registro di sistema. È spesso

importata da file eseguibili che richiedono privilegi elevati o che devono accedere a risorse protette.
MSVCRT.dll: Questa DLL è la libreria runtime C standard per Windows. Fornisce funzioni di base per l'input/output, la gestione delle stringhe e la matematica. È importata da quasi tutti i file eseguibili Windows che utilizzano il linguaggio di programmazione C o C++.
WININET.dll: Questa DLL fornisce funzioni per l'accesso a Internet, come l'invio e la ricezione di richieste HTTP e il download di file. È importata da file eseguibili che devono connettersi a Internet.

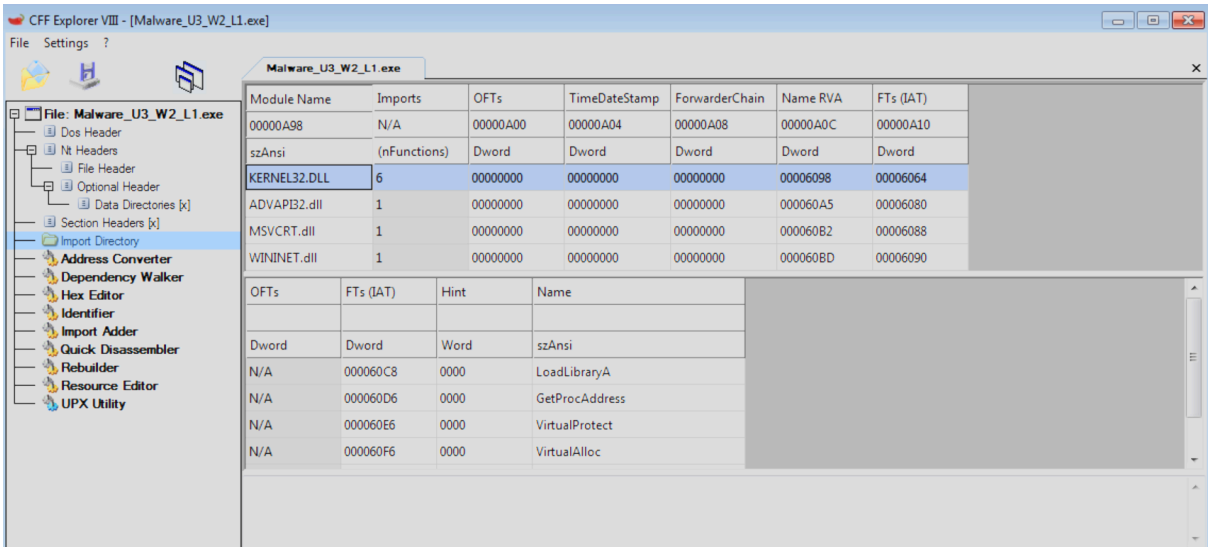
• Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa



UPX0, UPX1 e UPX2 non sono sezioni standard che si trovano nei file eseguibili. Invece, sono indicatori del fatto che il file è compresso con uno strumento di compressione chiamato UPX (Universal Packer for Executables).
UPX0, UPX1, UPX2: Questi sono nomi di sezioni creati dallo strumento di compressione UPX. Quando UPX comprime un eseguibile, sostituisce le sezioni originali (come .text, .data, .rsrc) con le sue sezioni chiamate UPX0, UPX1, UPX2 e così via. Queste sezioni contengono i dati compressi dalle sezioni originali.

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

Analizzando il file "Malware_U3_W2_L1.exe".



L'utilizzo delle funzioni "LoadLibrary" e "GetProcAddress" da parte del malware suggerisce che impiega il caricamento dinamico delle librerie. Ciò significa che il malware carica le librerie di cui ha bisogno solo in fase di esecuzione, rendendo più difficile identificare le sue dipendenze e il suo comportamento dannoso durante l'analisi statica. Questo file ha già suonato diversi campanelli d'allarme. Prima di tutto, il nome stesso "Malware" non è esattamente un voto di fiducia, poi ci sono le DLL che importa. Queste librerie sono come strumenti specializzati, e quelle che sta cercando di usare sono spesso utilizzate da programmi malintenzionati per intrufolarsi nel computer. Inoltre, il file è stato compresso con uno strumento chiamato UPX, che è come gettare un mantello dell'invisibilità sul suo codice per renderlo più difficile da decifrare. Di solito, i programmi legittimi non si preoccupano di nascondere il loro codice in questo modo. E per finire, non c'è nessuna informazione su chi ha creato questo file, il che è un altro segnale rosso.