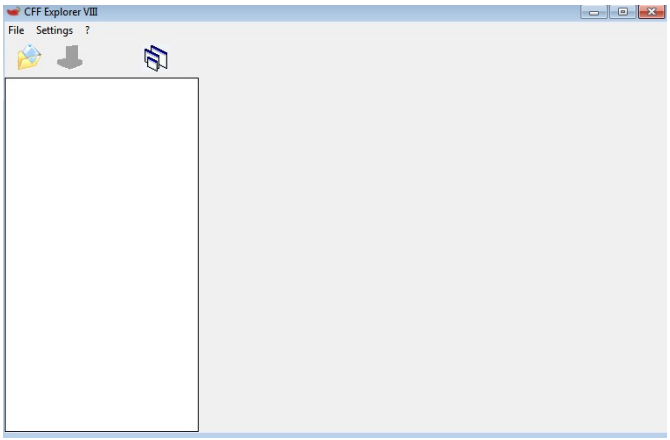
Adrian.Amarfii 09/01/2023
Report
Task
Traccia:

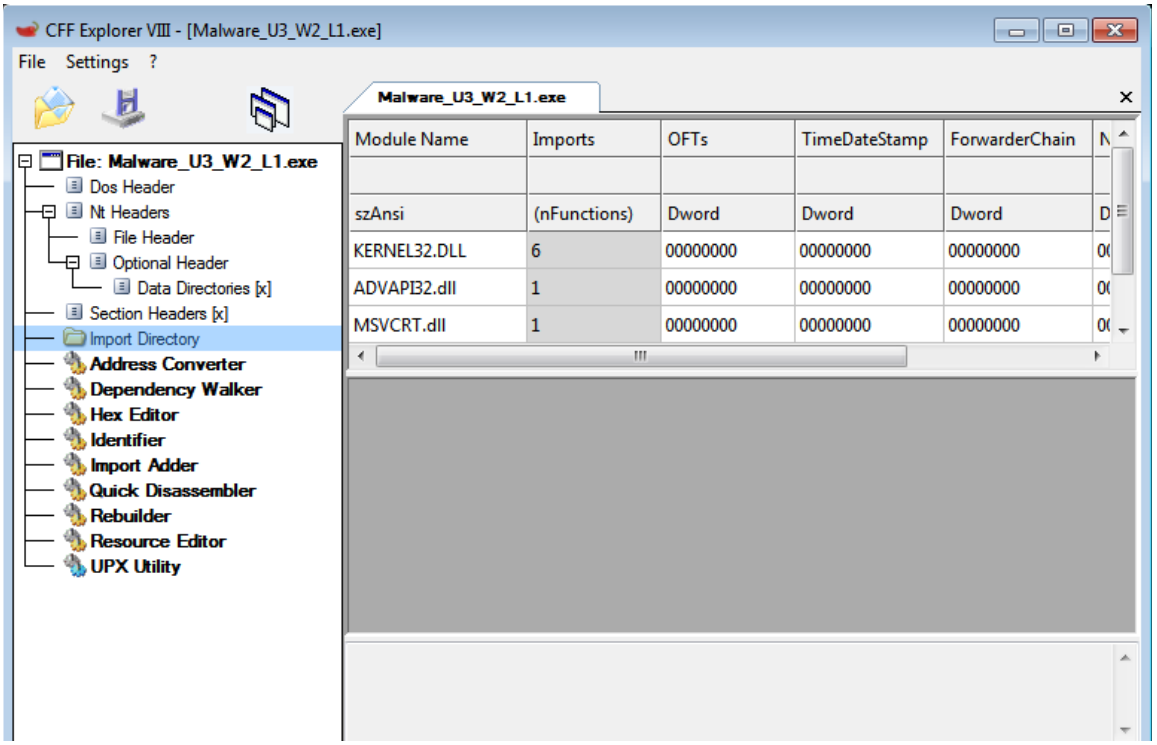
Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi statica basica.

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

Partiamo con l'apertura della macchina virtuale e trovare il file dopo di che andiamo subito a fare il primo punto della nostra task .Con l'aiuto di CFF EXPLORER vediamo che libreria usa questo file :

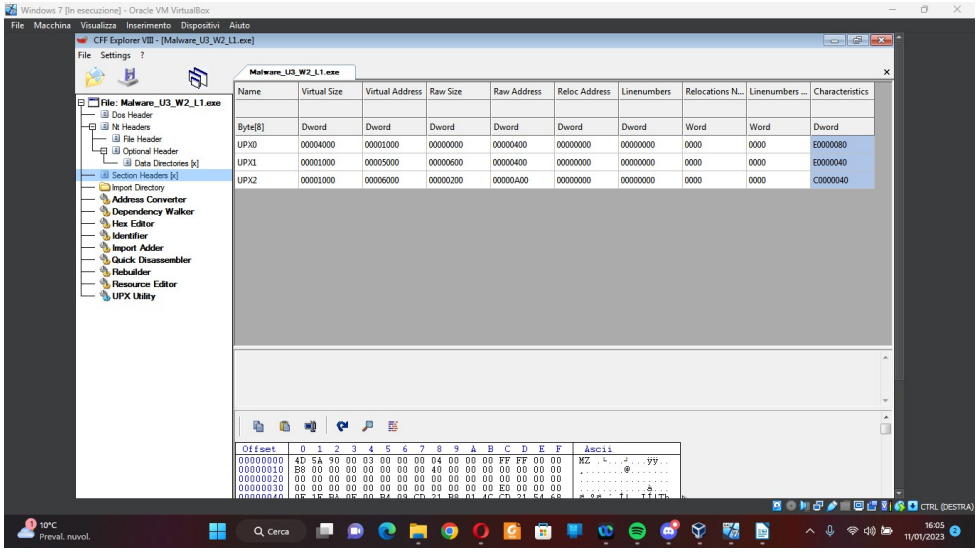




Come possiamo vedere abbiamo le seguente librerie :KERNEL32.DLL-ADVAPI32.DLL-MSVCRT.DLL

→ KERNEL.32 : contiene funzioni per interagire con il sistema operativo es.manipolazioe dei file la gestione della memoria
→ ADVAPI32.DLL: contiene funzioni per interagire con i servii ed i registri del sistema operativo MICROSOFT
→ MSVCRT.DLL: contiene funzioni per la manipolazione delle stringhe allocazione della memoria e chiamate per input e output in C.

Adesso andiamo a vedere le sezioni del file → andiamo su SECTION HEADERS



Come potete vedere abbiamo 3 sezioni :UPX0 UPX1 UPX2
UPX0,UPX1 molto simili vogliano dire =.data e .rdata→ ha accesso a qualsiasi data e variabili globali del programma eseguibile. .RDATA→ contiene informazioni sulle librerie importate
UPX2 → .text→contiene le instruzioni che la CPU eseguira una volta che il software sara aviato che nel nostro caso e unica che potra essere eseguita si come le altre sezioni che abbiamo si riferiscono ai dati .