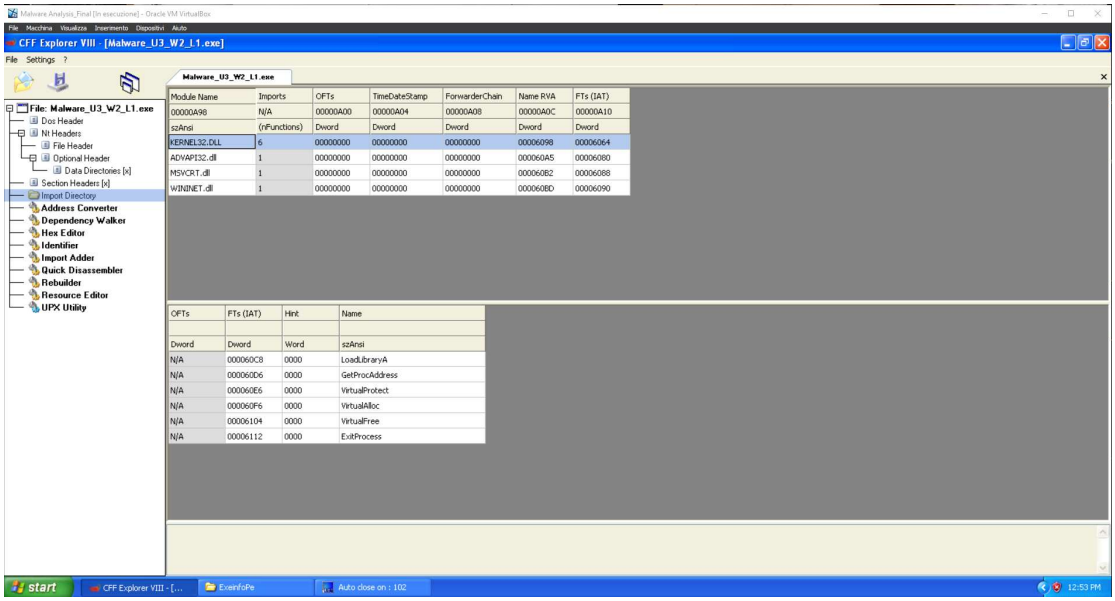
Pratica S10-L1 Malware analysis

Durante l'esercizio di oggi andremmo ad analizzare un malware presente sulla macchina virtuale che abbiamo installato.

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



Andando ad analizzare il malware con il programma CFF Explorer possiamo notare che vengono importate queste 4 librerie:

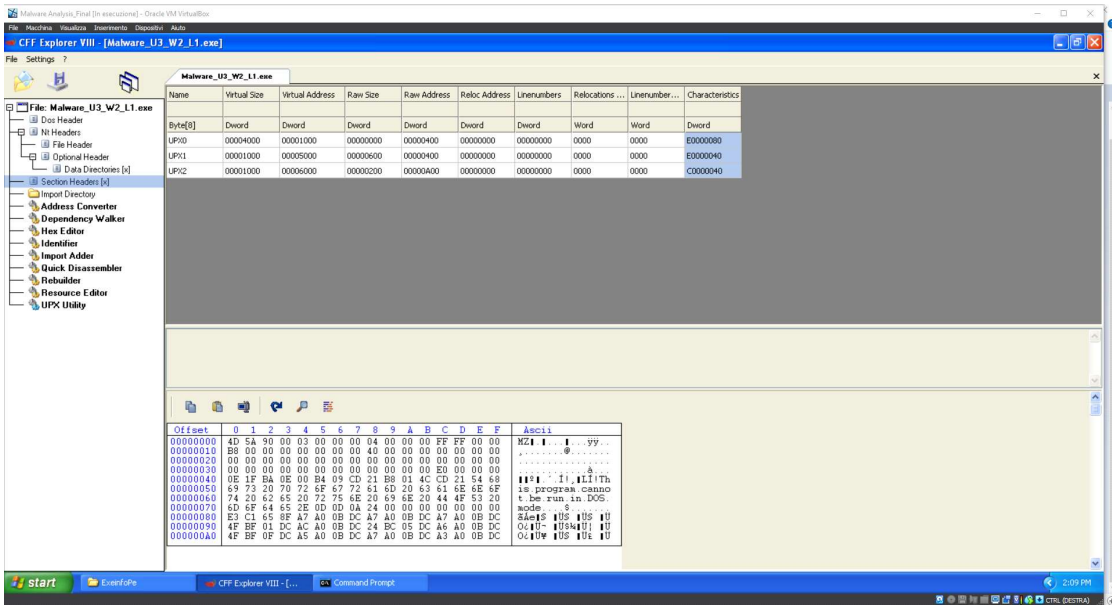
-KERNEL32.DLL : è una delle librerie di sistema principali in ambienti Microsoft Windows che ci permette ad esempio di manipolare file e gestire la memoria del sistema. E' è un processo di sistema necessario perché il PC funzioni correttamente.

-ADVAPI32.dll: è una libreria che fornisce una serie di funzioni di basso livello per l'interazione con il sistema operativo Windows.

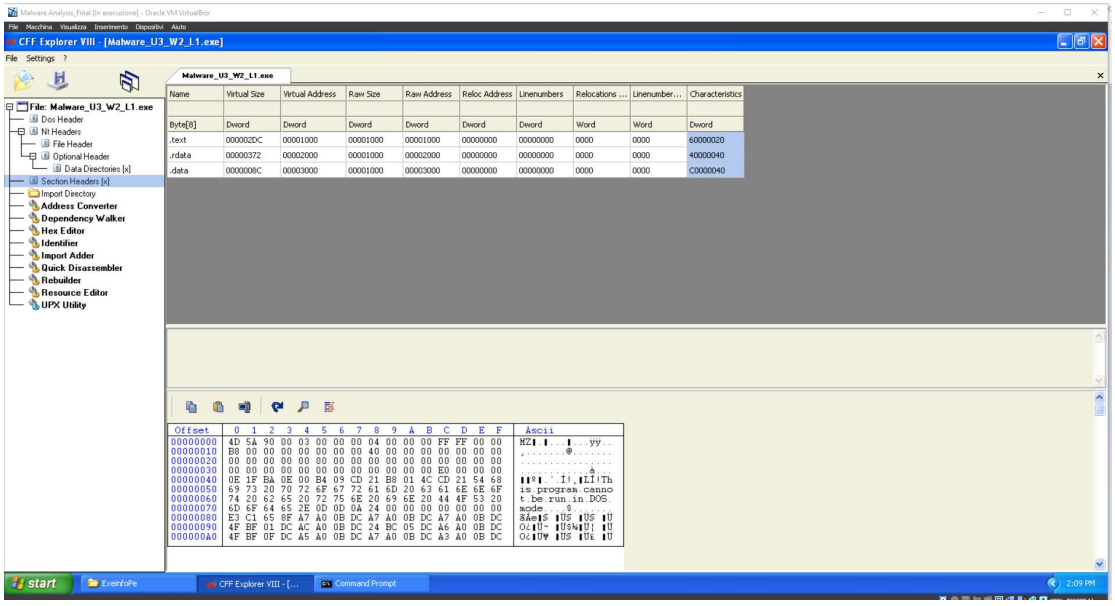
-MSVCRT.dll: questa libreria è parte dell'ambiente di runtime di Microsoft Visual C++ e fornisce funzionalità essenziali per le applicazioni sviluppate con il compilatore Microsoft Visual C++.

-WININET.dll: questa libreria fornisce un'interfaccia di programmazione delle applicazioni (API) che permette alle applicazioni Windows di interagire con i servizi Internet e di eseguire operazioni di rete.

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



Qui possiamo vedere che le sezioni sono state compresse e risultano come: UPX0, UPX1 e UPX2. Nell'ultima opzione possiamo in automatico spacchettare queste sezioni e vediamo in chiaro di cosa stiamo parlando.



Vediamo che abbiamo 3 sezioni: .text , .rdata e .data.

.text: la sezione «text» contiene le istruzioni che la CPU eseguirà una volta che il software sarà avviato.

.rdata: la sezione «rdata» include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer.

.data: la sezione «data» contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del

programma.

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

Andando a cercare informazioni sul malware attraverso CFF ho visto questa informazione

Facendo alcune ricerche su internet ho notato che questo malware è un trojan che potrebbe portare ad un attacco ddos, questo malware è abbastanza sofisticato perchè le sezioni erano state compresse con UPX così da renderle meno accessibili.