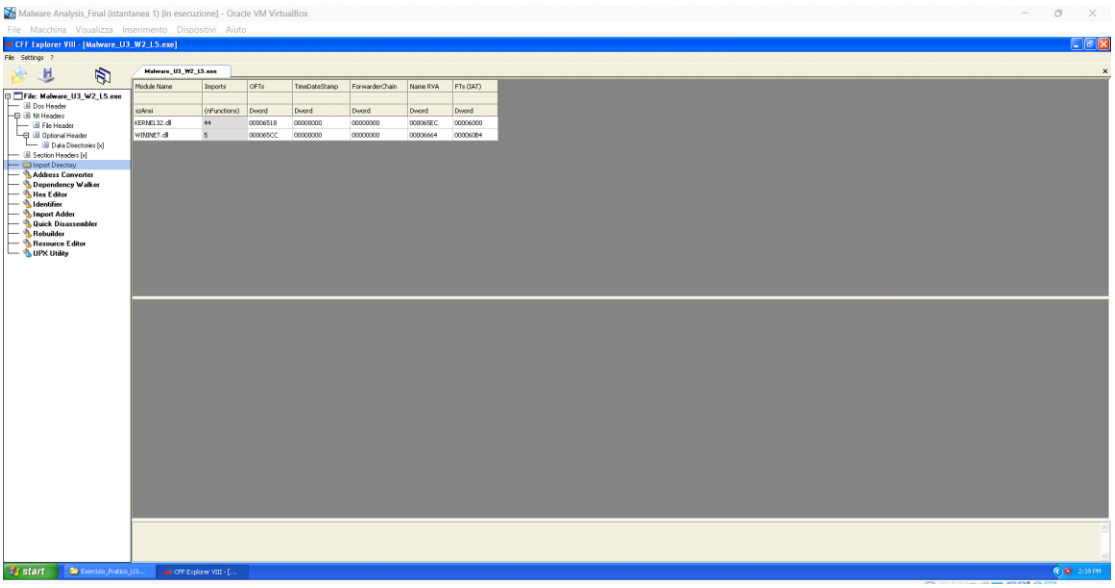
Con riferimento al file Malware_U3_W2_L5 presente all'interno della cartella "Esercizio_Pratico_U3_W2_L5" sul desktop della nostra macchina virtuale dedicata per l' analisi dei malware,si può utilizzare il tool CFF Explorer per controllare le librerie importate dal file eseguibile e le sezioni di cui si compone.

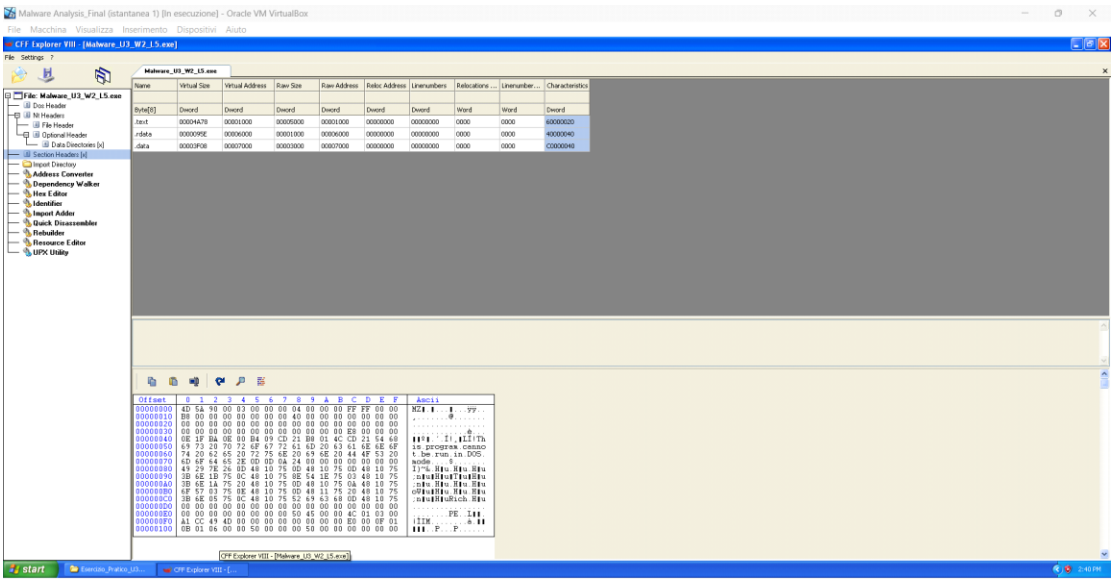
Utilizzando il tool,nella sezione "import directory" del pannello principale possiamo vedere le librerie importate



-Kernell32.dll: Libreria che contiene le funzioni principali per interagire con il sistema operativo

-Wininet.dll: Libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP,FTP,NTP

Possiamo poi controllare le sezioni di cui si compone il file spostandoci nella sezione "section headers"

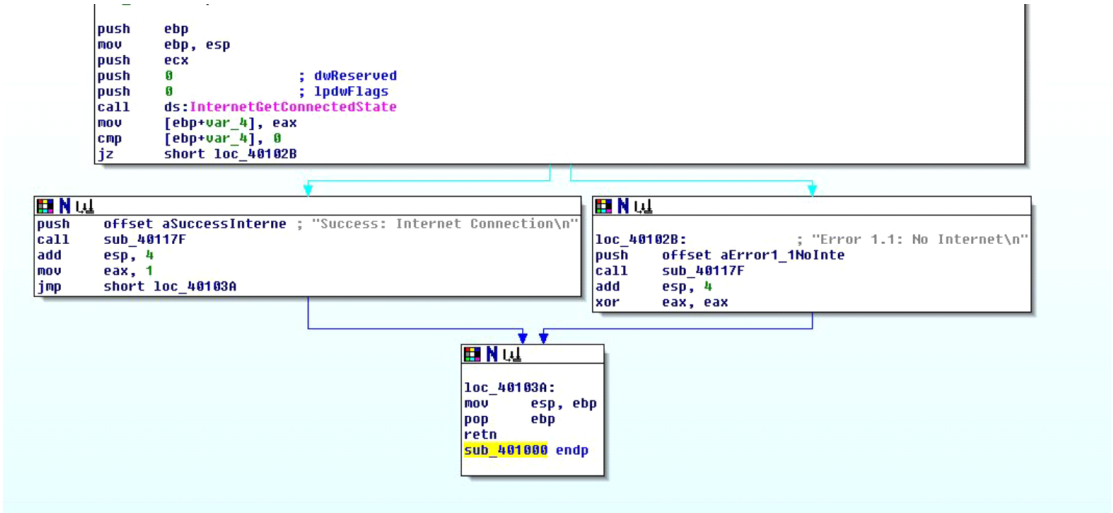


Qui troviamo:

.Test : questa sezione contiene le istruzioni che la CPU eseguirà una volta che il software sarà avviato.

.rdata : questa sezione include le informazioni circa le librerie e le funzioni importate ed esportate dall' eseguibile

.data : contiene tipicamente i dati/le variabili globali del programma eseguibile



Tra i costrutti noti,troviamo:

-La creazione dello stack(porzione di memoria dedicata per il salvataggio delle variabili locali di una data funzione) tramite le istruzioni push ebp e mov ebp,esp nella prime righe del codice

-Costrutto condizionale "IF" dato dalle istruzioni "cmp" e "jz"

-Il blocco di istruzioni finale ripristina il registro dello stack pointer attraverso l istruzione "mov esp, edp". L istruzione "pop edp" ripristina il registro base dello stack.

Possiamo dire che il comportamento della funzione sembra sia di controllare se la connessione a internet è disponibile o meno,restituendo un valore che indica se il controllo è stato eseguito con successo o meno. Se la connessione non è disponibile viene stampato un messaggio di errore