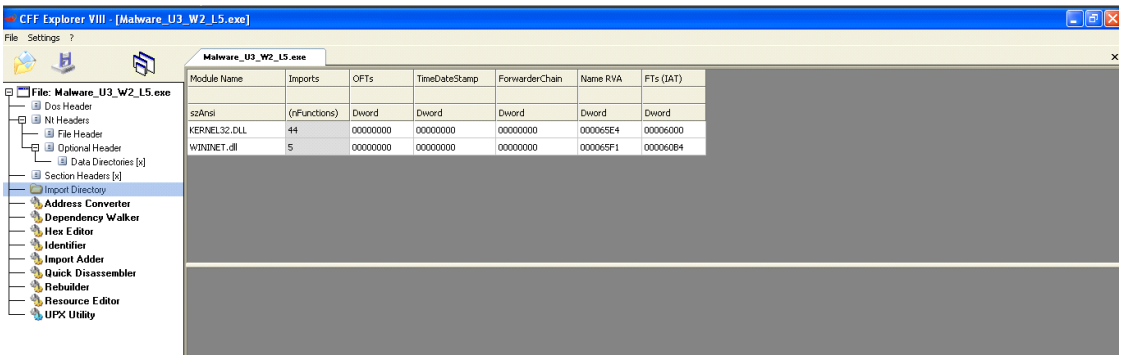
Progetto
31/03/2023

Facendo riferimento al file **Malware_U3_W2_L5** presente all'interno della cartella **Esercizio_Pratico_U3_W2_L5** sul desktop della macchina virtuale dedicata per l'analisi dei malware ho, con l'utilizzo di CFF Explorer (strumento di analisi dei file che consente di esaminare i contenuti di un file eseguibile), esaminato le librerie importate dal file eseguibile e le sezioni di cui si compone il file eseguibile del malware.

Librerie importate dal file eseguibile

Dopo aver aperto il file eseguibile sopra citato su CFF Explorer, ho scelto 'import directory' dal pannello principale a sinistra ed ho così ottenuto:

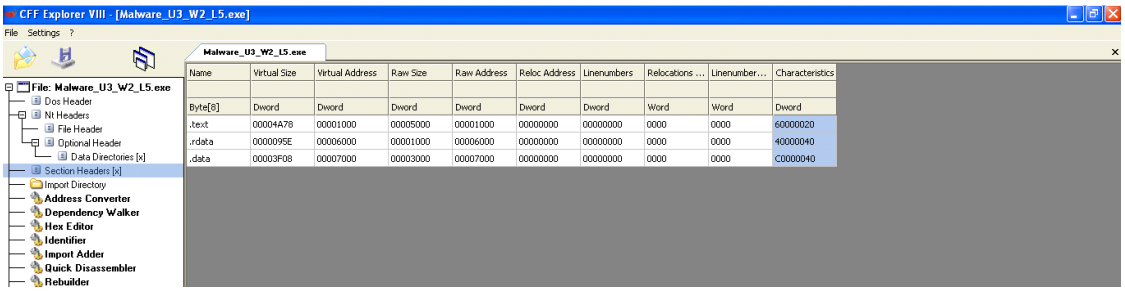


Le librerie importate dal file eseguibile sono:

- Kernel32.dll: libreria comune che contiene le funzioni principali per interagire con il sistema operativo, ad esempio, manipolazione dei file e gestione della memoria;
- WININET.dll: libreria che contiene le istruzioni per l'implementazione di alcuni protocolli di rete come HHTP ed FTP.

Sezioni del file eseguibile

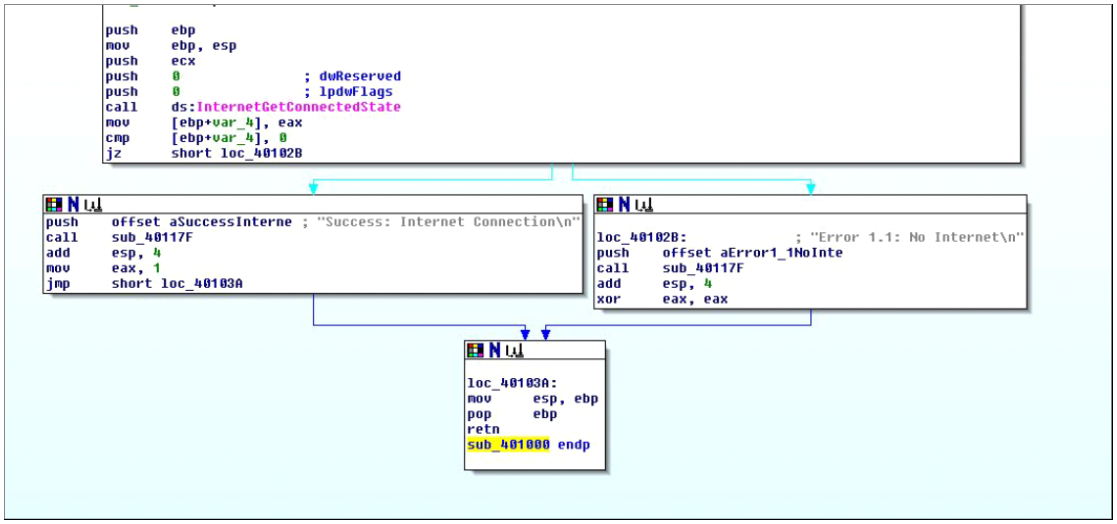
Per verificare le sezioni di cui si compone il file, sempre utilizzando CFF Explorer, mi sono spostato su 'section headers' ottenendo così:



Le sezioni di cui si compone il file eseguibile sono:

- .text: contiene le istruzioni che la CPU eseguirà una volta che il software sarà avviato;
- .rdata: include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile;
- .data: contiene tipicamente i dati/le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Costrutti noti



- Le istruzioni "push ebp" e "mov ebp, esp" creano un nuovo stack;
- Le istruzioni "push ecx" , "push 0" e "push 0" preparano gli argomenti per la chiamata alla funzione "InternetGetConnectedState";
- La chiamata alla funzione "InternetGetConnectedState" viene effettuata tramite "call ds: InternetGetConnectedState";
- Il valore restituito dalla chiamata alla funzione viene memorizzato nella variabile locale "[ebp+var_4]";
- La funzione esegue un controllo sul valore della variabile "[ebp+var_u]" utilizzando le istruzioni "cmp" e "jz". Se il valore è uguale a 0la funzione passa al blocco di codice contrassegnato come "loc_40102B", altrimenti passa al blocco di codice contrassegnato come "loc_40103A";
- Nel blocco di codice "loc_40102B" viene chiamata la funzione "sub_40117F" con un messaggio di errore "Error 1.1: No Internet\n";
- Nel blocco di codice "loc_40103A" viene impostato il valore di ritorno della funzione a 1 se la connessione ad internet è stata stabilita con successo, altrimenti viene impostato a 0;
- L'istruzione "mov esp, ebp" ripristina il registro dello stack pointer;

- L'istruzione "pop ebp" ripristina il registro base dello stack;
- L'istruzione "retn" restituisce il valore di ritorno alla funzione chiamante.

Ipotizzare il comportamento della funzionalità implementata

La funzionalità è quella di controllare se la connessione ad Internet è disponibile o meno e di restituire un valore che indica se il controllo è stato eseguito correttamente o meno. Solo se la connessione non è disponibile verrà stampato un messaggio di errore.