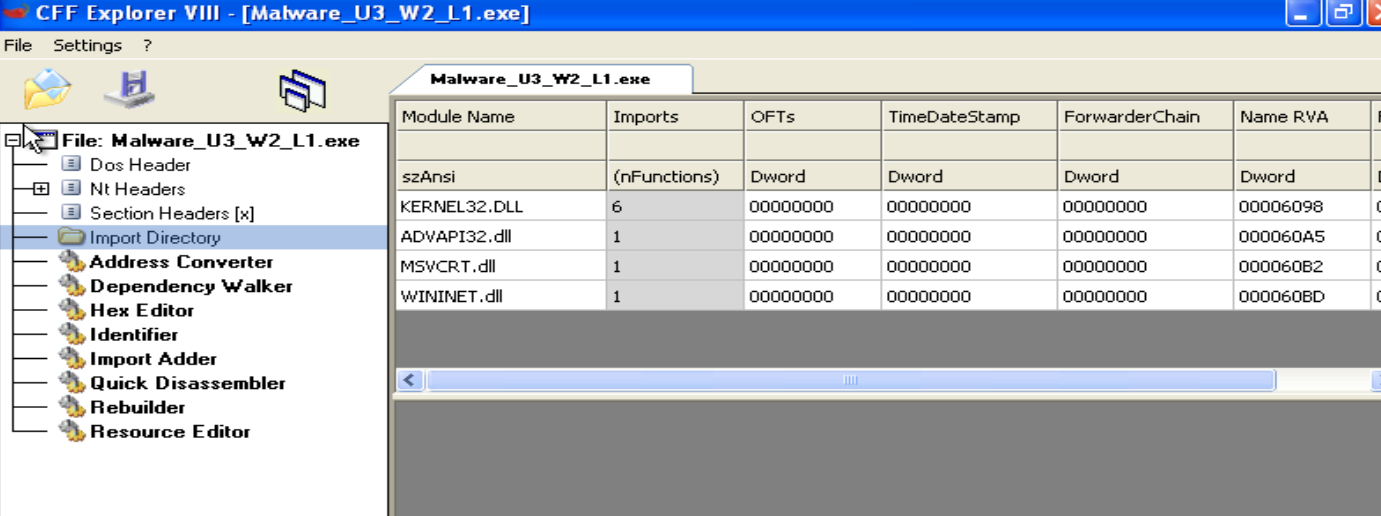
Analisi Statica Basica

L'analisi statica di un malware è un processo che coinvolge l'esame del codice sorgente o dell'eseguibile del malware senza eseguirlo effettivamente. Questo tipo di analisi è utile per ottenere informazioni sul comportamento previsto del malware e comprendere come interagisce con il sistema.

Nella pratica bisognerà analizzare il malware ‘Esercizio\_Pratica\_U3\_W2\_L1’ indicando le librerie importate dal malware fornendo una descrizione e indicare le sezioni di cui si compone fornendo anche qui una descrizione.



Dopo aver dato in pasto il malware al tool CFF Explorer si ha una panoramica dettagliata del programma malevolo.

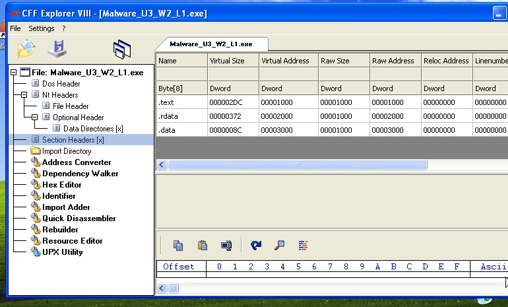
Come si può notare questo codice malevolo importerà queste directory che verranno importate alla esecuzione del codice malevolo.

-Kernel32.dll: Contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.

-Advap132.dll: Contiene le funzioni per interagire con i servizi ed i registri del sistema operativo

-Msvcrt.dll: Contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.

-Wininet.dll: Contiene le funzioni per l’implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.



Ora esaminiamo le sezioni degli header che ci fornisce altre informazioni importanti come, ad esempio, le sezioni di cui si compone il software.

Prima di tutto abbiamo tradotto le tre sezioni che erano ‘nascoste’ in formato UPX utilizzando l’utility che ci fornisce CFF.

Una volta tradotto in chiare queste informazioni possiamo notare da quali header è composto il software.

* .text: Contiene le righe di codice 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 e le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Considerazioni

Da questa analisi con il tool CFF e il sito web Virustotal possiamo dire che questo Malware sia un ‘Trojan downloader’ significa che è progettato per infiltrarsi nel sistema di un utente in modo apparentemente legittimo o attraverso la mimetizzazione di un file o un programma attendibile.

Una volta che il trojan è attivo sul sistema, il suo obiettivo principale è scaricare e installare ulteriori componenti dannosi sul computer dell’utente.