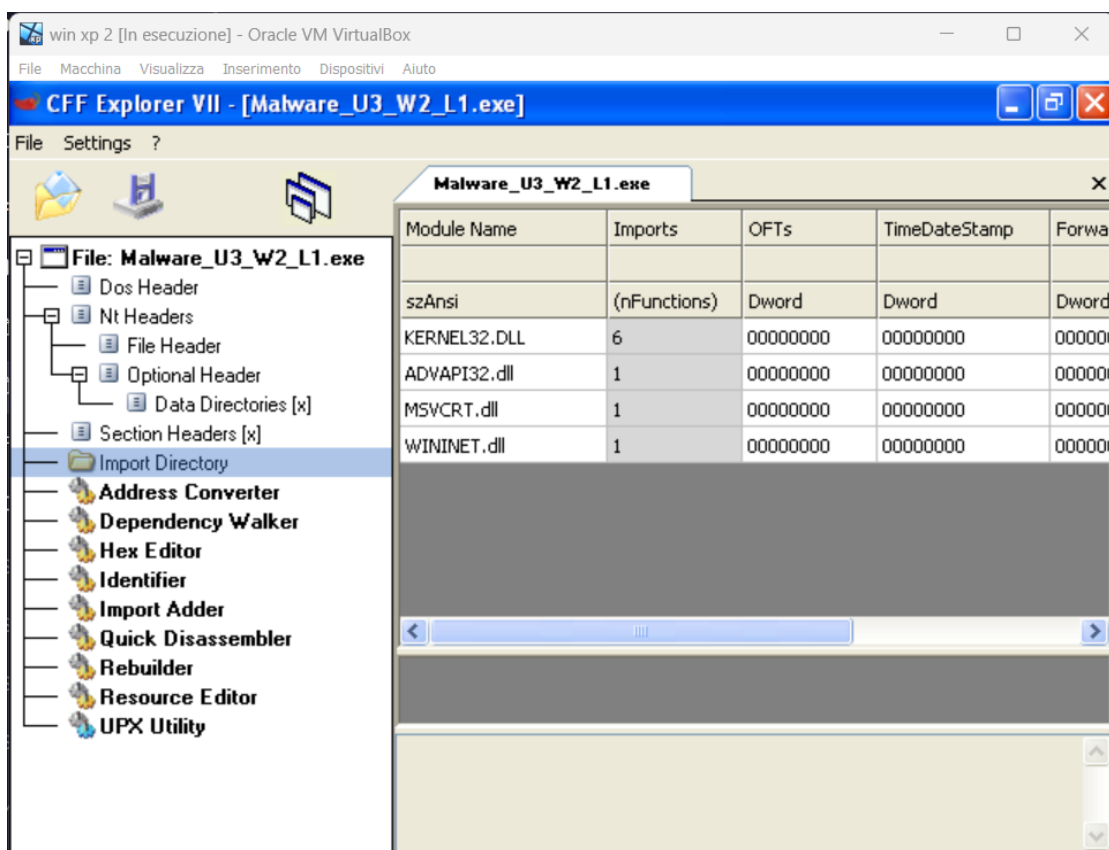


Esercizio Epicode 27.11.2023

Malware analysis statica base

Analizzare il file eseguibile Malware_U3_W2_L1:

- 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



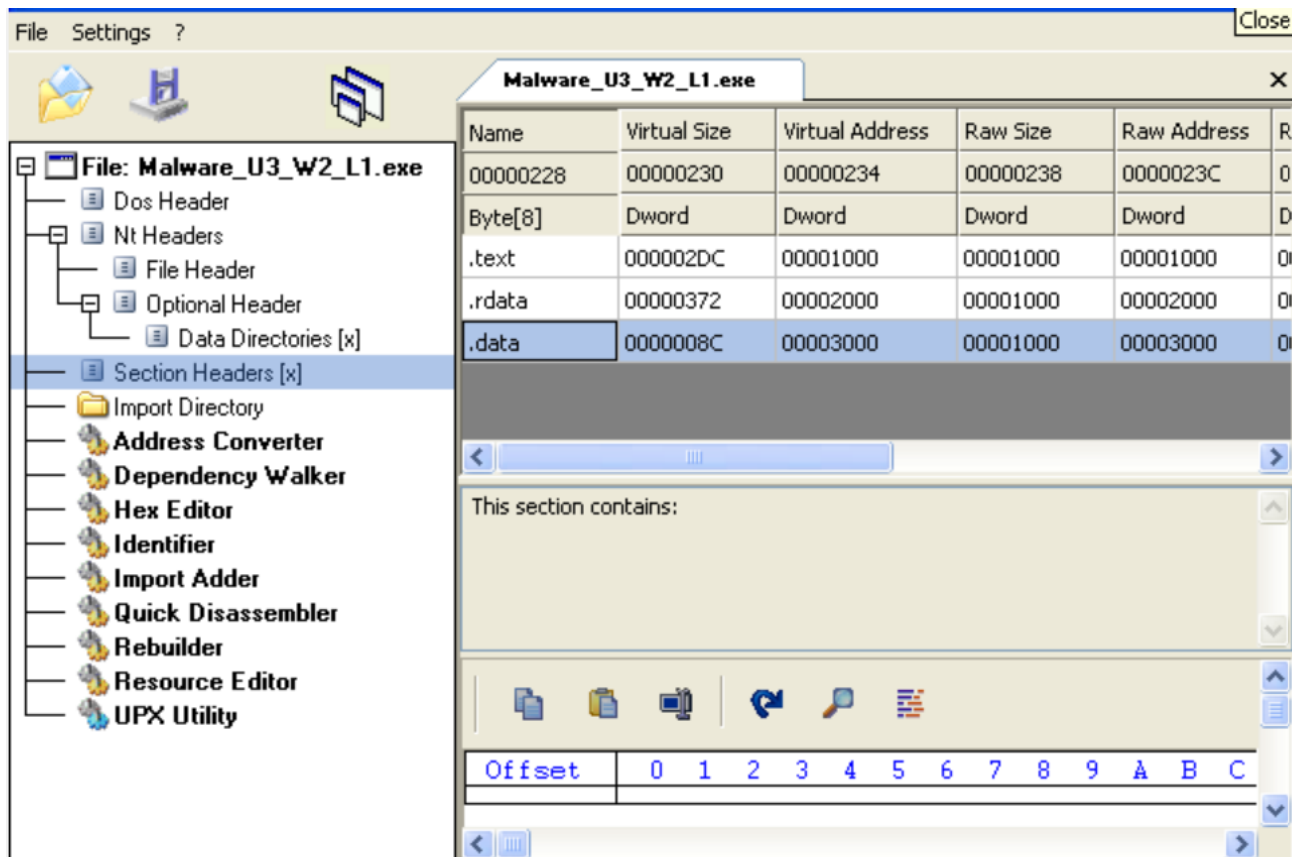
Le info riprese tramite cff explore ci riportano le seguenti librerie

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

Advapi32.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



Dopo aver decompresso le sezioni tramite UPX Utility ho trovato:

.text: contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.

.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: contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Una variabile si dice globale quando non è definita all'interno di un contesto di una funzione, ma bensì è globalmente dichiarata ed è di conseguenza accessibile da qualsiasi funzione all'interno dell'eseguibile.

Infine effettuando un ultimo check con Total Virus, tramite il codice hash MD5 procurato da cff explorer, l'eseguibile risulta essere un Malware Trojan Downloader.