Malware Analysis

Analisi Statica Basica

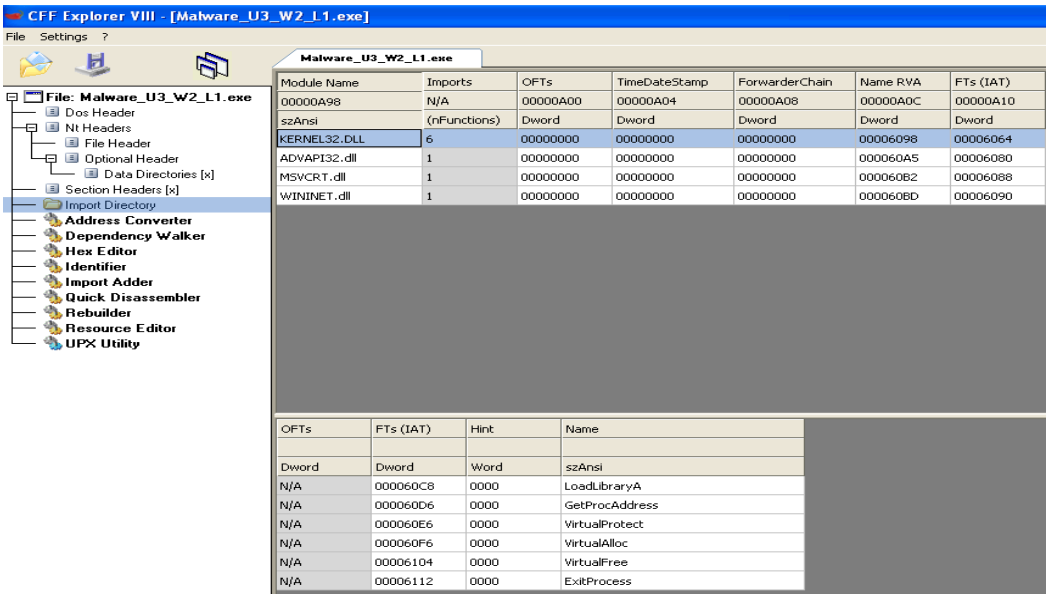
Traccia:

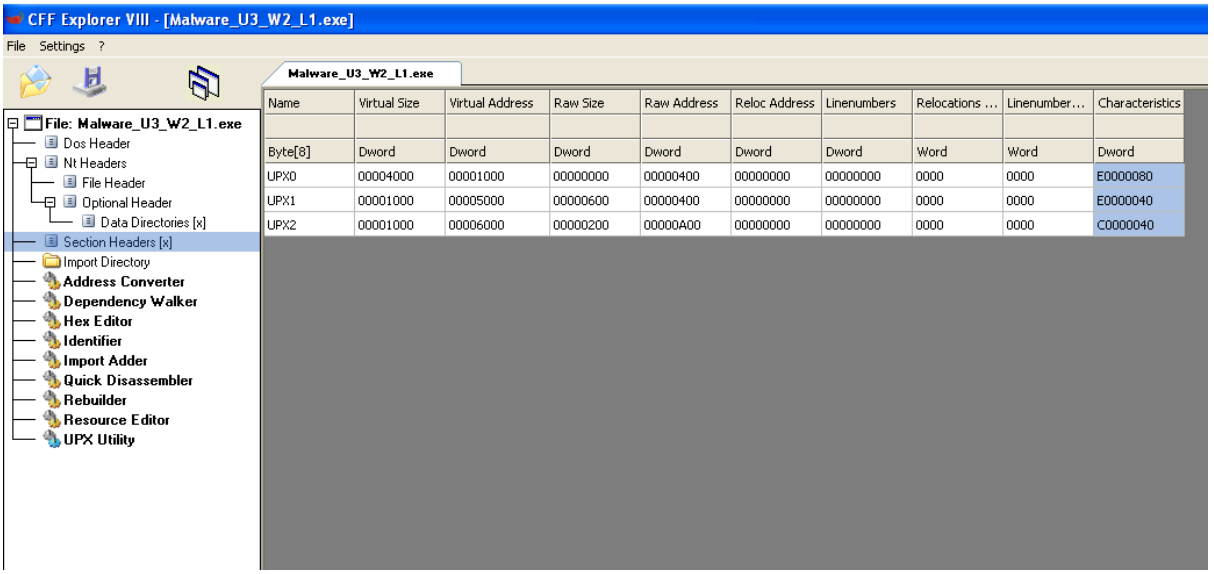
Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi statica basica.
Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- ☐ 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 librerie importate dal malware sono:

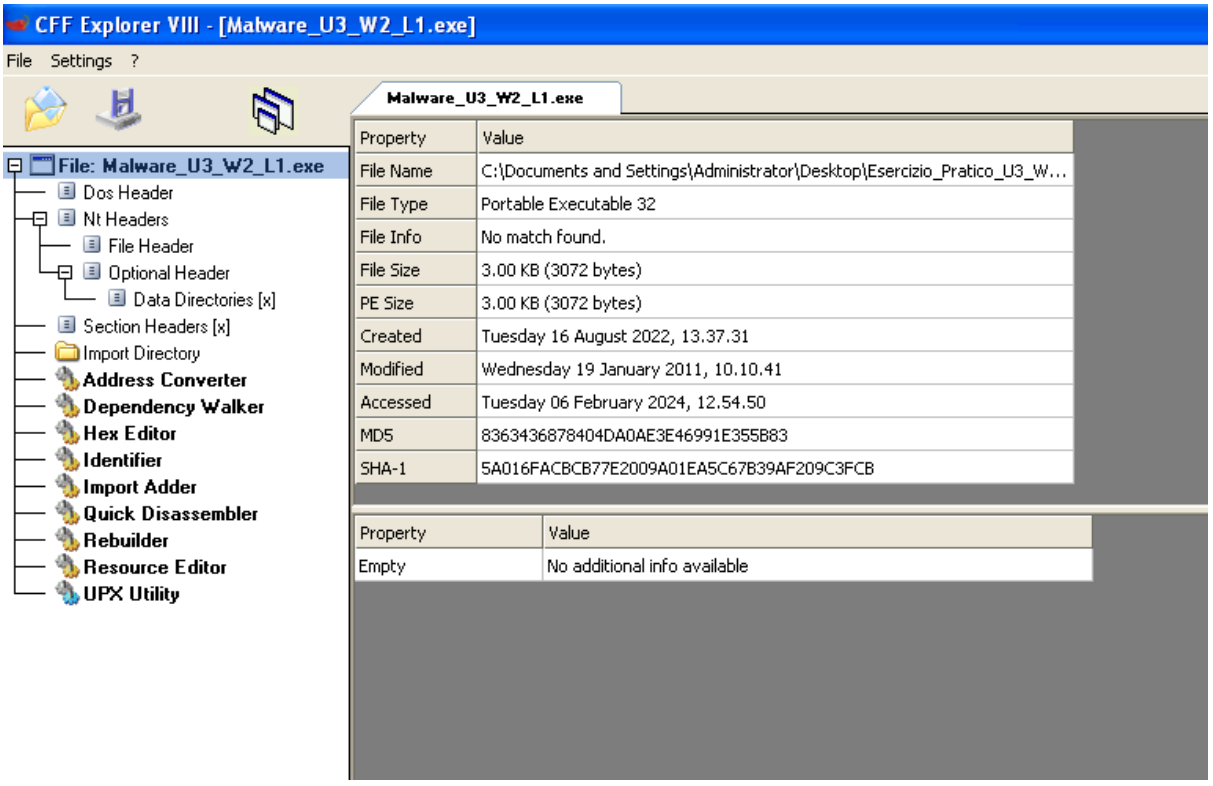
Kernel32.dll: che include le librerie per interagire con il sistema operativo
Advapi32.dll: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft
Msvcrt.dll: contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output in stile linguaggio C
Wininet.dll: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP





Dalla sezione Headers possiamo notare che sono presenti 3 componenti del malware, tuttavia non sono stato in grado di rilevare dati interessanti di analisi.

Infine possiamo andare a recuperare l'hash di identificazione del malware dalla pagine iniziale di CFF Explore e andare a cercare su internet se si tratta di un malware noto.



Questa è la scansione da Virus Total: