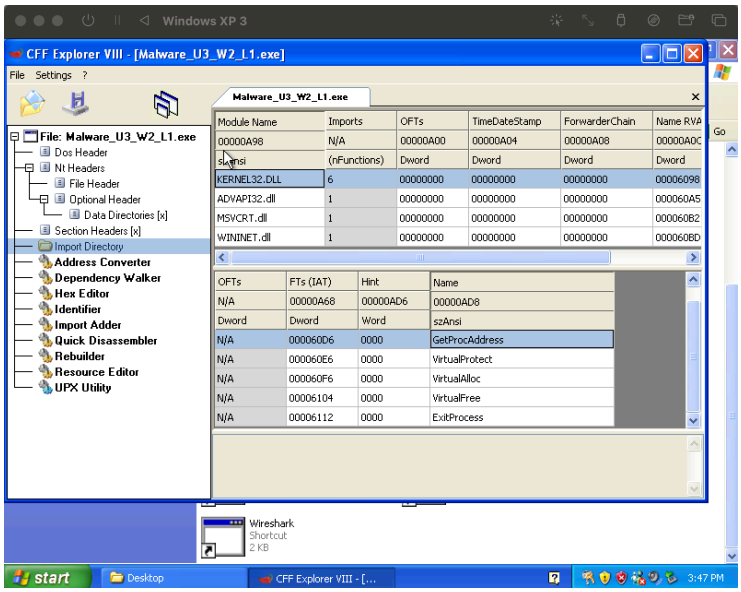
1. Malware analysis: Analisi statica basica

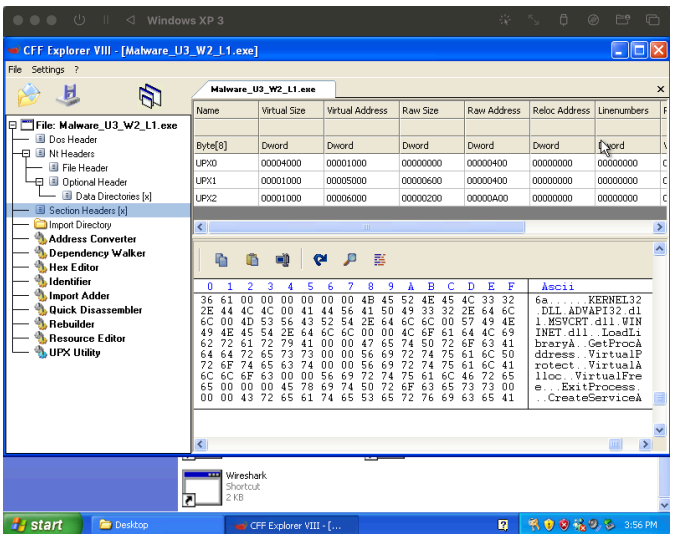
Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1»:

- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse.

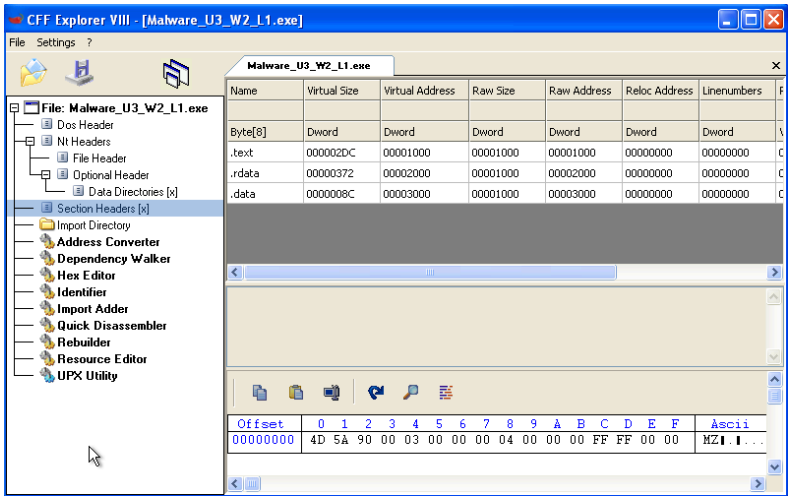


KERNEL32.DLL
Libreria che contiene le funzioni principali per interagire col sistema operativo, come per esempio la manipolazione di file e la gestione della memoria.
ADVAPI32.DLL
Libreria che contiene le funzioni per interagire con i registri e i servizi del sistema operativo Microsoft.
MSVCRT.DLL
Libreria che contiene le funzioni per la manipolazione di stringhe, allocazioni memoria ed altro.
WININET.DLL
Libreria che contiene le funzioni per implementazione protocolli di rete come HTTP, FTP ed NTP.

- Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa.



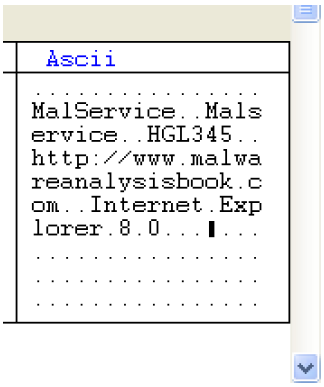
Andiamo a spacchettare le sezioni e troviamo:



.txt contiene le istruzioni per la cpu andrà ad eseguire una volta avviato il software.

.rdata contiene le informazioni delle librerie e le funzioni importate ed esportate dall'eseguibile.

.data contiene i dati/variabili globali del programma eseguibile. In questo caso possiamo andare a vedere tramite CFF che contiene la seguente info.



- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte.

Il malware è stato progettato per essere altamente sofisticato e difficile da individuare.
Il malware crea un attacco DDoS mandando molteplici richieste HTTP.