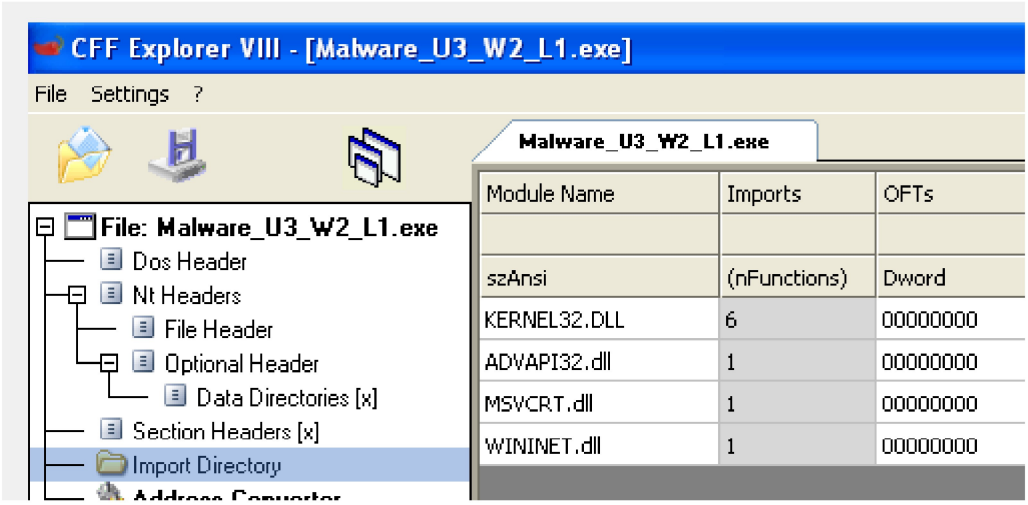
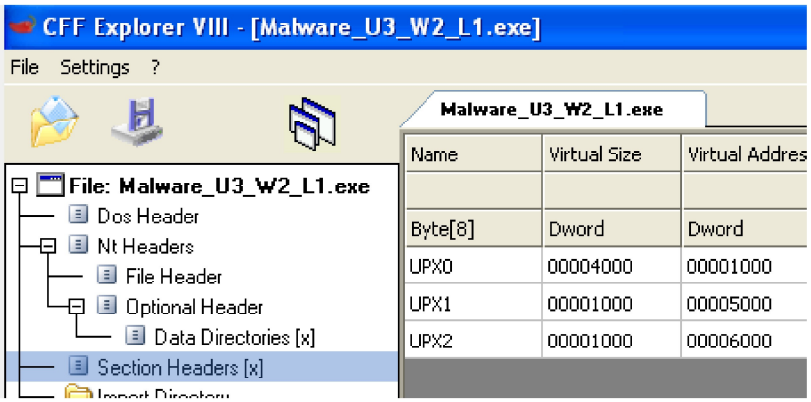
Librerie importate dal Malware

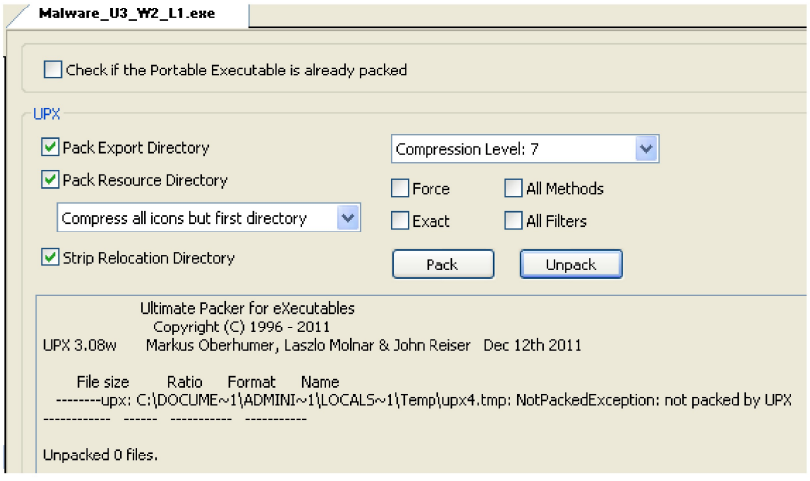


Possiamo notare come il malware analizzato importi 6 funzioni di kernel32.dll, quindi possiamo immaginare che manipoli i file e le cartelle, poi vediuamo la advapi32, quindi interagisce con i registri di windows, poi la msvcrt che sappiamo serve per chiamate i/o e allocazione memoria, in ultimo la wininet, quindi sappiamo che probabilmente fa richieste su internet o invia dati.

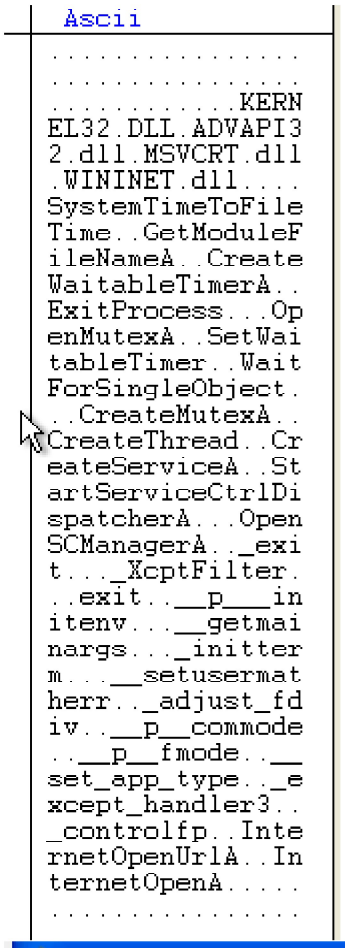
Analisi sezioni



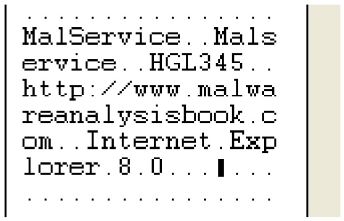
Sono funzioni di compressione, proviamo quindi a usare l'utility interna di CFF per decomprimere

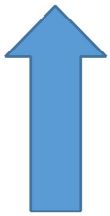


In questo modo possiamo vedere in chiaro alcune stringhe nel Hex editor

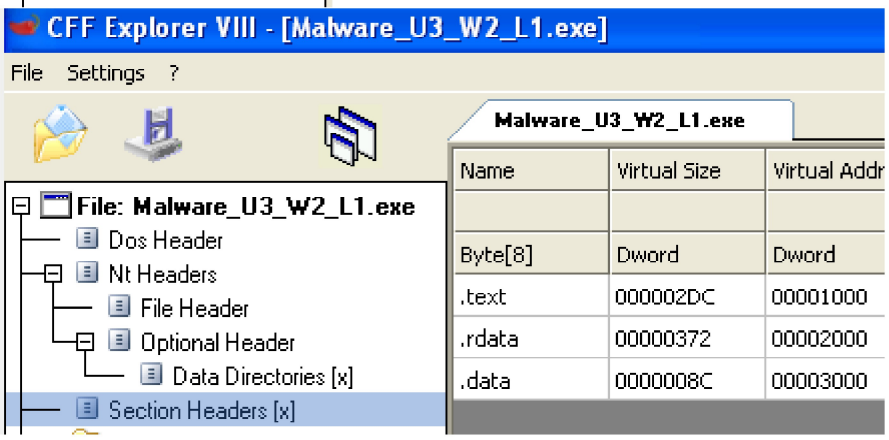


Qui possiamo notare invece una serie di stringhe, probabilmente i nomi delle funzioni richiamate





Qui per esempio vediamo un link in chiaro



Inoltre possiamo notare che ora i nomi delle funzioni sono cambiati

Considerazioni

Con una ricerca su google troviamo un github che spiega il funzionamento di questo malware

https://github.com/SafeEval/practical-malware-analysis/blob/master/exercises/lab-07-1.md

5) Purpose of the program?

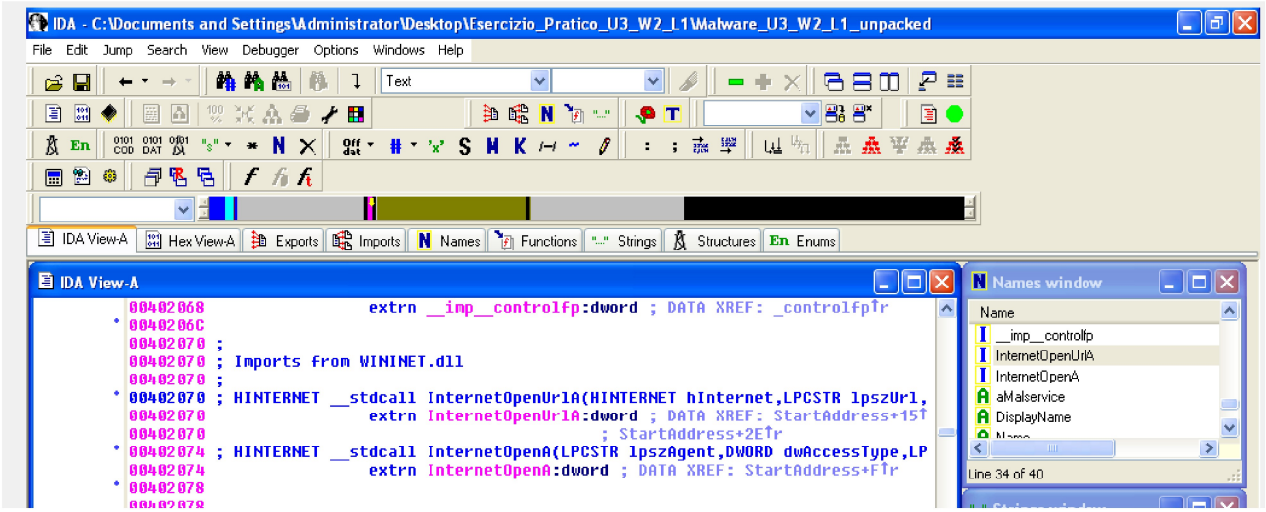
Installs a DDoS service with 20 threads attacks `http://www.malwareanalysisbook.com` in the year 2100.

Connects to `http://www.malwareanalysisbook.com` in infinite loop. Leaves a mutex open to let other instances know it's running.

Program starts a service dispatcher, allowing `malservice` to execute in this process. Calls ServiceMain.

Questo è quello che fa il malware.

Grazie a IDA possiamo vedere meglio le funzioni



Per esempio internet url open conferma quello che avevamo trovato prima.