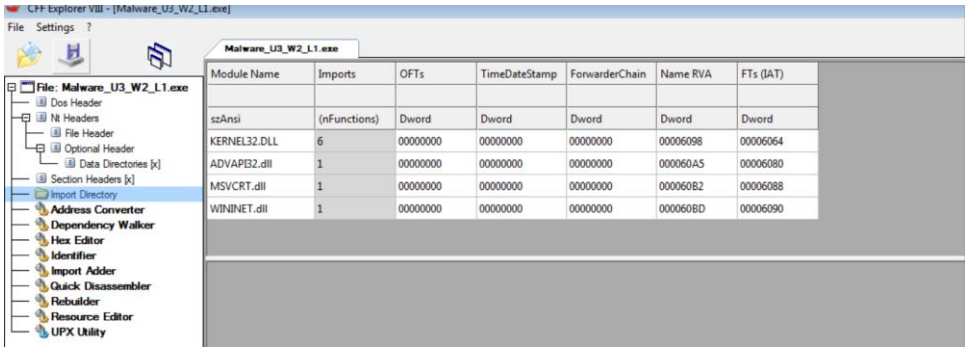
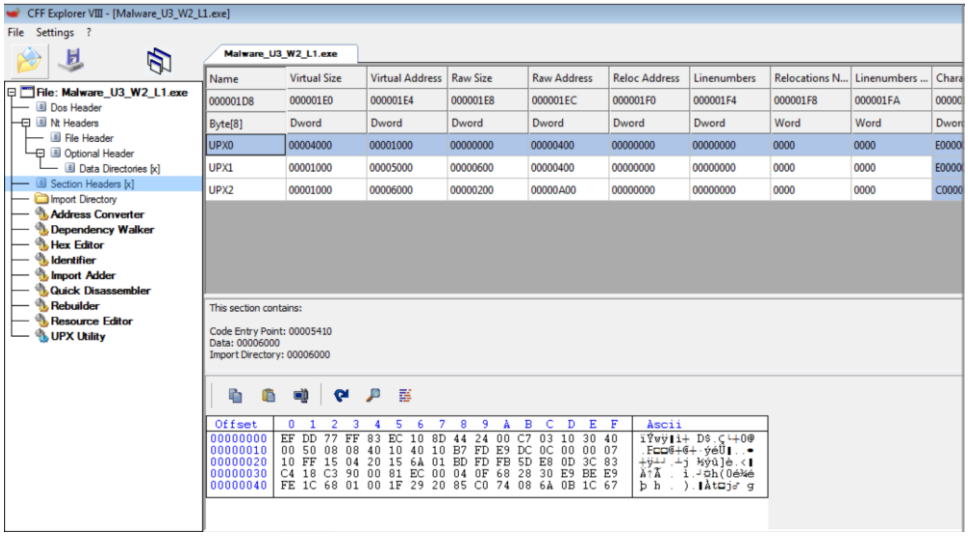
S10L1

IMPORT LIBRERIE



Kernel32.dll: Contiene le funzioni fondamentali del sistema operativo.
Advapi32.dll: Fornisce le funzioni per interagire con registri e servizi di Windows.
MSVCRT.dll: È una libreria scritta in linguaggio C utilizzata per la manipolazione e l'allocazione della memoria.
Wininet.dll: Fornisce le funzioni necessarie per l'implementazione di servizi di rete come FTP, NTP e HTTP.

SEZIONI



Dall'analisi con CFF Explorer, possiamo osservare che l'eseguibile è suddiviso in 3 sezioni. Tuttavia, sembra che il malware abbia occultato i veri nomi delle sezioni, rendendo difficile determinarne il tipo o la funzione.

CONSIDERAZIONI FINALI

Questo malware presenta una sofisticata protezione che limita le informazioni ottenibili tramite un'analisi statica di base. È evidente dalla presenza di funzioni importate come "LoadLibrary" e "GetProcAddress", suggerendo che il malware carichi dinamicamente le librerie durante l'esecuzione.