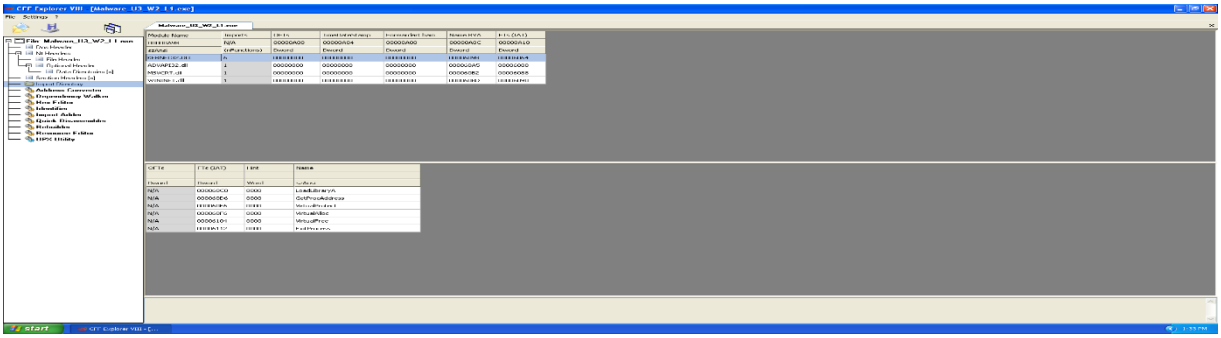
LIBRERIE E FUNZIONI IMPORTATE



Attraverso l'uso del tool CFF Explorer, abbiamo importato l'eseguibile per analizzare l'header del PE, e sotto IMPORT DIRECTORY possiamo notare quali sono le librerie che sono state importate dal malware, ovvero:

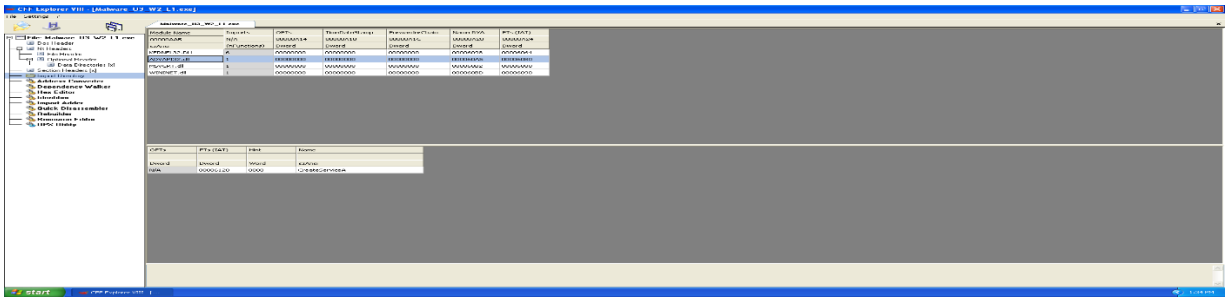
- **Kernel32.dll -** Contiene le funzioni per interagire con il S.O (es. manipolazione file, gestione della memoria etc). Andando nello specifico, vediamo sotto tale libreria, quali sono state le funzioni richiamate:
  - **a) Load Library**
  - **b) GetProcAddress**

    le prime due funzioni sopracitate vengono utilizzate per richiamare la libreria all'occorrenza cioè importate a tempo di esecuzione(runtime). In questo modo si possono nascondere le librerie importate, le funzioni, e anche le sezioni.

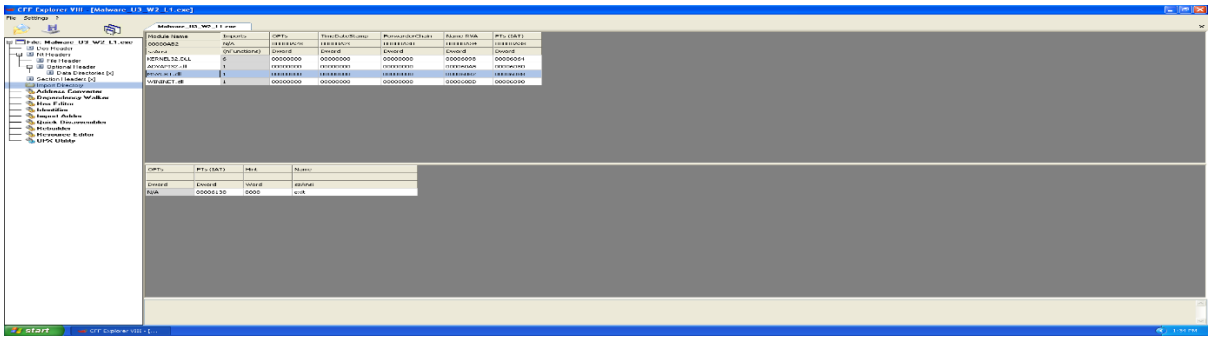
  - **c) Virtual Protect:** modifica la protezione di un'area di pagine di commit nello spazio indirizzi virtuali.

  - **d) Virtual Free:** modifica/riserva/commit dello stato di un'area di pagine nello spazio indirizzi virtuali.

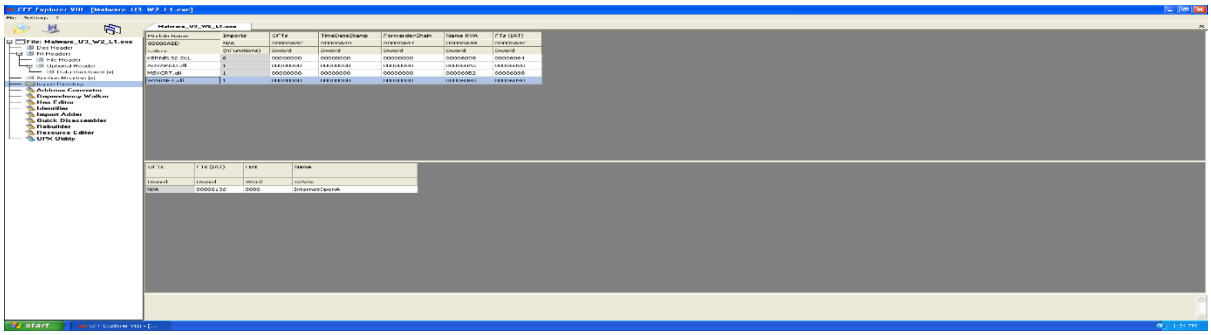
  - **e) Exit Process**



- **Advapi32.dll –** contiene funzioni per interagire con i servizi e i registri del S.O. Le funzioni richiamate sono:
  - **a) CreateServiceA:** Crea un oggetto servizio e lo aggiunge al DB di gestione controllo del servizio stesso.

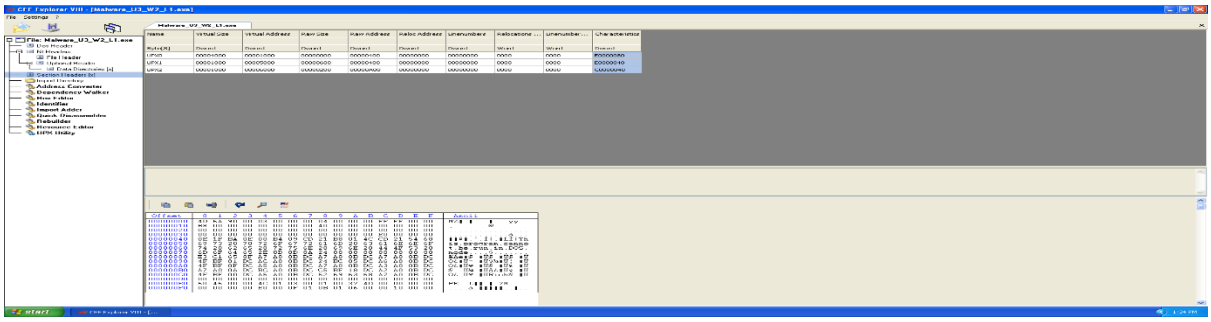


- **MSVCRT.dll –** contiene funzioni per la manipolazione delle stringhe e allocazione della memoria, chiamate I/O e altro. La funzione richiamata è **EXIT**



- **Wininet.dll –** contiene funzioni per l'implementazione di protocolli di rete per i servizi come http – ftp – ntp . In questo caso la funzione richiamata è **InternetOpenA (Inizializza l'uso di un applicazione delle funzioni di WinInet)**

SEZIONI CHE COMPONGONO IL MALWARE



Sempre tramite il tool CFF Explorer, sotto la voce SECTION HEADER, notiamo che l'eseguibile si compone di 3 sezioni che tuttavia sono state offuscate.

COMMENTI FINALI

Abbiamo recuperato qualche informazione riguardo al malware ma che tuttavia tramite l'analisi statica basica non sono sufficienti. Infatti il malware nasconde informazioni riguardo alle librerie importate come le sezioni che lo compongono, e lo vediamo dalle funzioni richiamate come LoadLibrary e GetProcAddress i quali importano le librerie runtime.