Report di Analisi del Malware

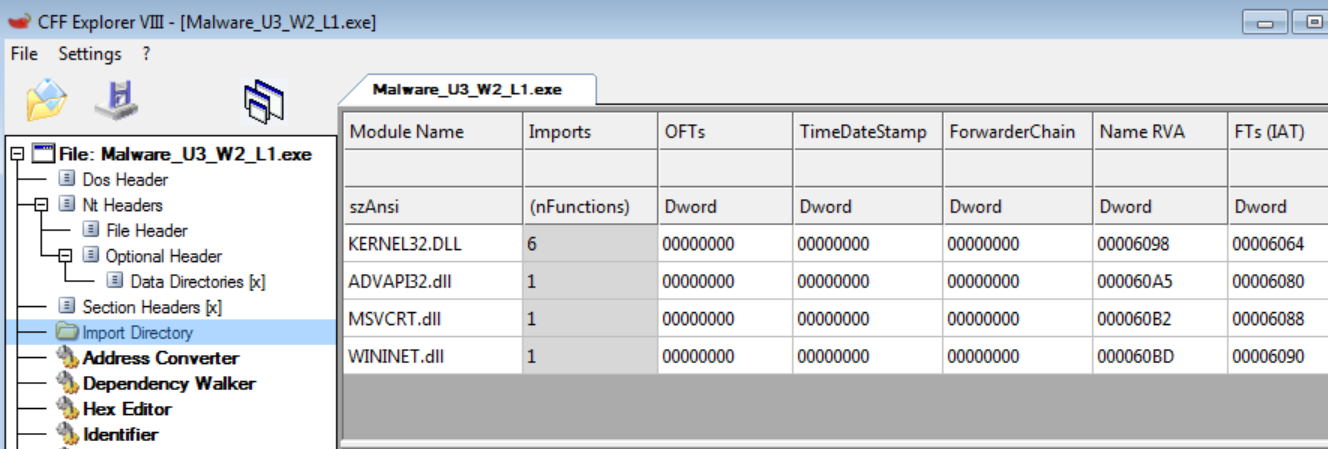
# Introduzione

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, rispondiamo 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.

# Import Librerie

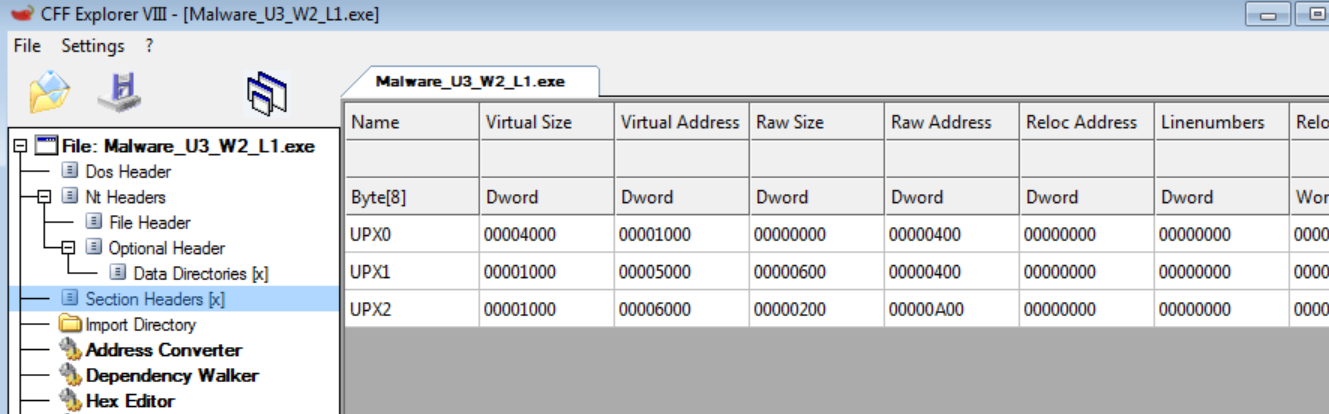
Utilizzando CFF Explorer, vediamo dalla sezione import directory che il malware U3\_W2\_L1 importa 4 librerie:

1. Kernel32.dll: include le funzioni core del sistema operativo  
2. Advapi32.dll: include le funzioni per interagire con registri e servizi Windows.  
3. MSVCRT.dll: libreria scritta in C per la manipolazione scritte o allocazione memoria.  
4. Wininet.dll: include le funzioni per implementare i servizi di rete come ftp, ntp, http.



# Sezioni del Malware

Dalla sezione «section header» vediamo che l’eseguibile ha 3 sezioni. Il malware abbia nascosto il vero nome delle sezioni e quindi non siamo in grado di capire che tipo di sezioni sono.



# Considerazioni Finali

Si tratta di un malware avanzato, non ci consente di recuperare molte informazioni sul suo comportamento con l'analisi statica basica.  
le funzioni importate troviamo «LoadLibrary» e «GetProcAddress», che ci fanno pensare ad un malware che importa le librerie a tempo di esecuzione

