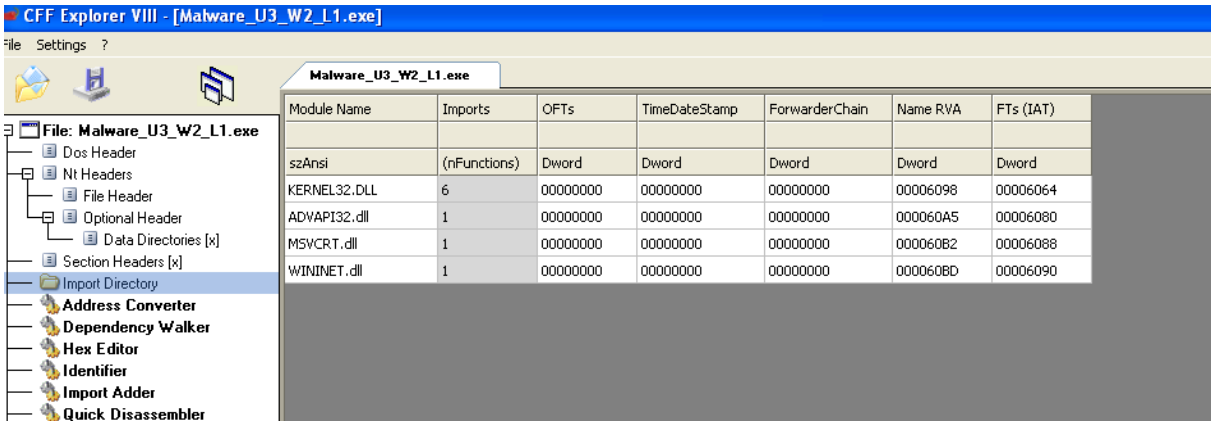
ANALISI STATICA BASICA

Ho aperto CFF EXPLORER VIII, selezionando la tab IMPORT DIRECTORY per vedere le librerie importate nel malware



:

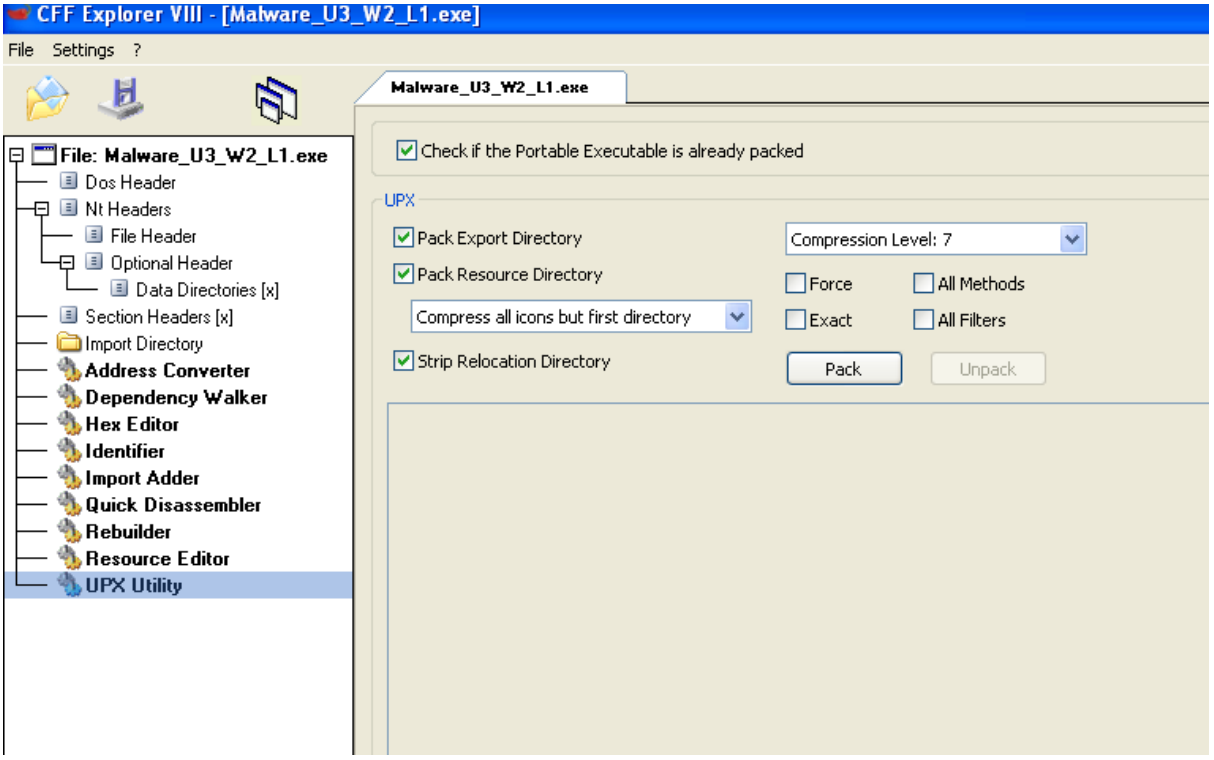
• KERNEL32.DLL: libreria usata per le funzioni principali per interagire con il sistema operativo. Un malware potrebbe sfruttare tale libreria per manipolare i file e per accedere la gestione della memoria

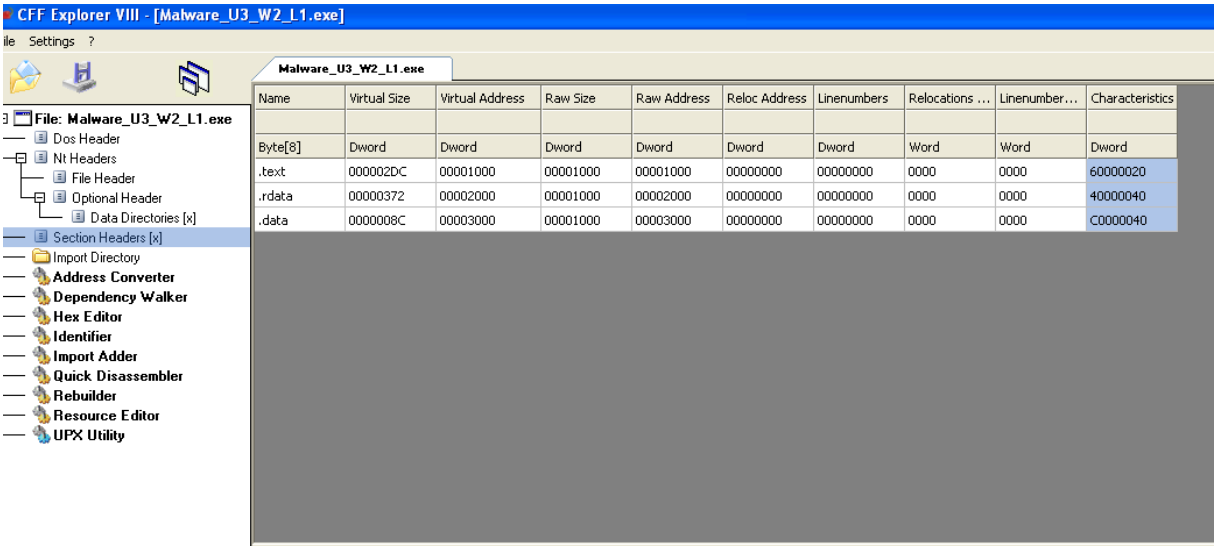
• ADVAPI32.dll: libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft, tramite la quale un malware potrebbe creare nuovi account utente, accedere al registro di sistema e crittografare o decrittografare dati sensibili;

• MSVCRT.dll: libreria che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C. Tramite questa libreria un malware potrebbe sfruttare delle vulnerabilità presenti o per eseguire codice malevolo;

• WININET.dll: libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come http, FTP, NTP. Un malware potrebbe sfruttare tale libreria per comunicare con server remoti, scaricare e caricare file, inviare dati sensibili...

In seguito ho selezionato la tab SECTION HEADERS, dove ho identificato le sezioni UPX0, UPX1 e UPX2 da estrarre.
A questo punto ci spostiamo sulla sezione UPX Utility e procedo all'estrazione con "unpack" ora le sezioni sono visibili.





• .text: Questa sezione contiene le istruzioni, ovvero le righe di codice che la CPUeseguirà quando il software viene avviato. È la sezione principale di un file eseguibile, poiché contiene il codice effettivo che viene eseguito per far funzionare il programma. Tutte le altre sezioni contengono dati o informazioni di supporto per questa sezione.

• .rdata: Questa sezione contiene informazioni sulle librerie e le funzioni importate ed esportate dall'eseguibile. Qui vengono memorizzate le informazioni sui moduli esterni che l'eseguibile utilizza, come librerie di sistema o librerie condivise, e le funzioni che vengono importate o esportate per l'utilizzo all'interno del programma.

• .data: Questa sezione contiene dati e variabili globali del programma eseguibile. Le variabili definite in questa sezione sono accessibili da qualsiasi parte del programma, poiché sono globalmente dichiarate.

Dai risultati delle analisi, possiamo trarre alcune conclusioni:

Tramite l'analisi statica basica possiamo confermare che il file è malevolo e possiamo fornireinformazioni generiche sulle sue funzionalità. Possiamo vederne le dimensioni e le librerie annesse ma possiamo solo ipotizzare cosa fa effettivamente non avendo un esecuzione del malware.