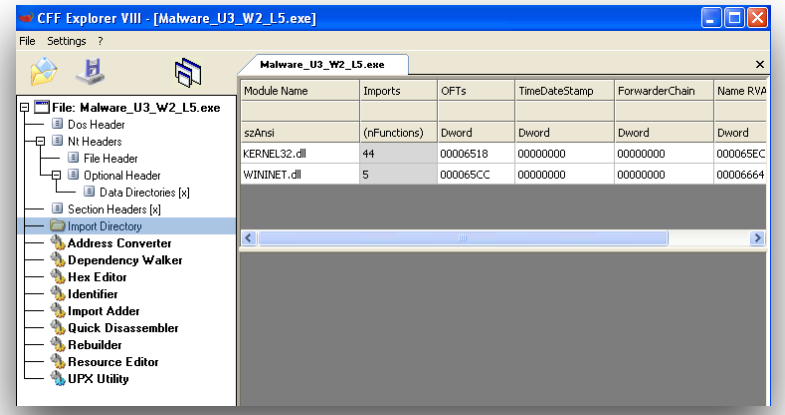
# 5. Analisi statica e dinamica: Un approccio pratico

Con riferimento al file Malware_U3_W2_L5 presente all'interno della macchina virtuale dedicata, rispondere ai quesiti.

**Quali librerie vengono importate dal file eseguibile?**

Utilizziamo il tool **CFF Explorer**




Le librerie importate all'interno del file sono due.

**KERNEL32.dll**

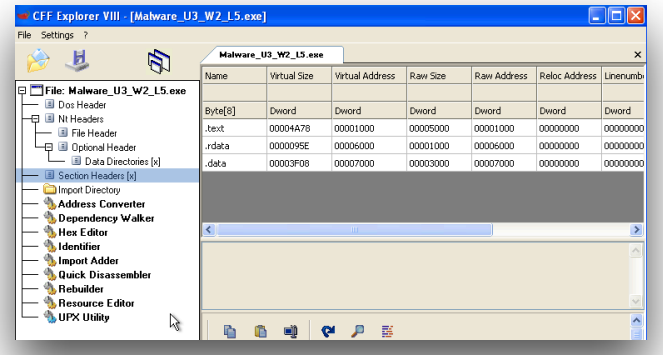
Libreria che contiene le funzioni principali per interagire col sistema operativo, come per esempio la manipolazione di file e la gestione della memoria.

**WININET.dll**

Libreria che contiene le funzioni per implementazione protocolli di rete come HTTP, FTP ed NTP.

**Quali sono le sezioni di cui si compone il file eseguibile del malware?**

Ci spostiamo in **Section Headers**



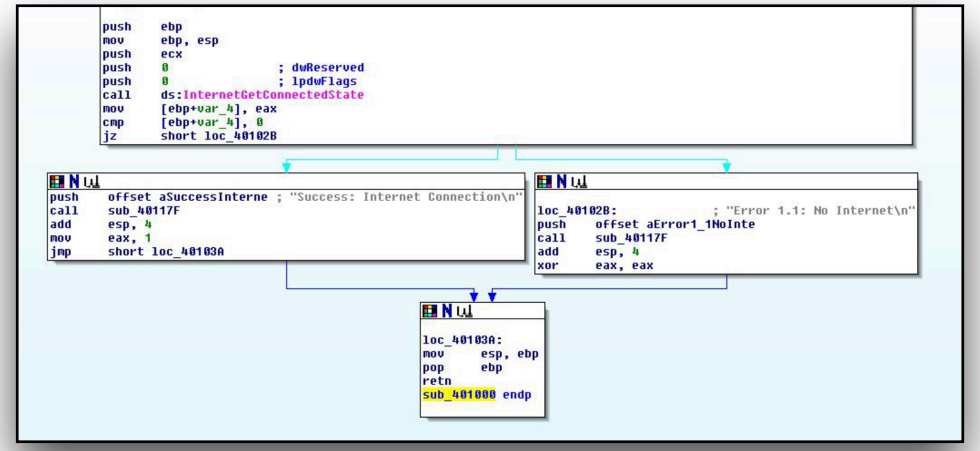

Le sezioni sono:

**.txt -** contiene le istruzioni che la CPU andrà ad eseguire una volta avviato il software.

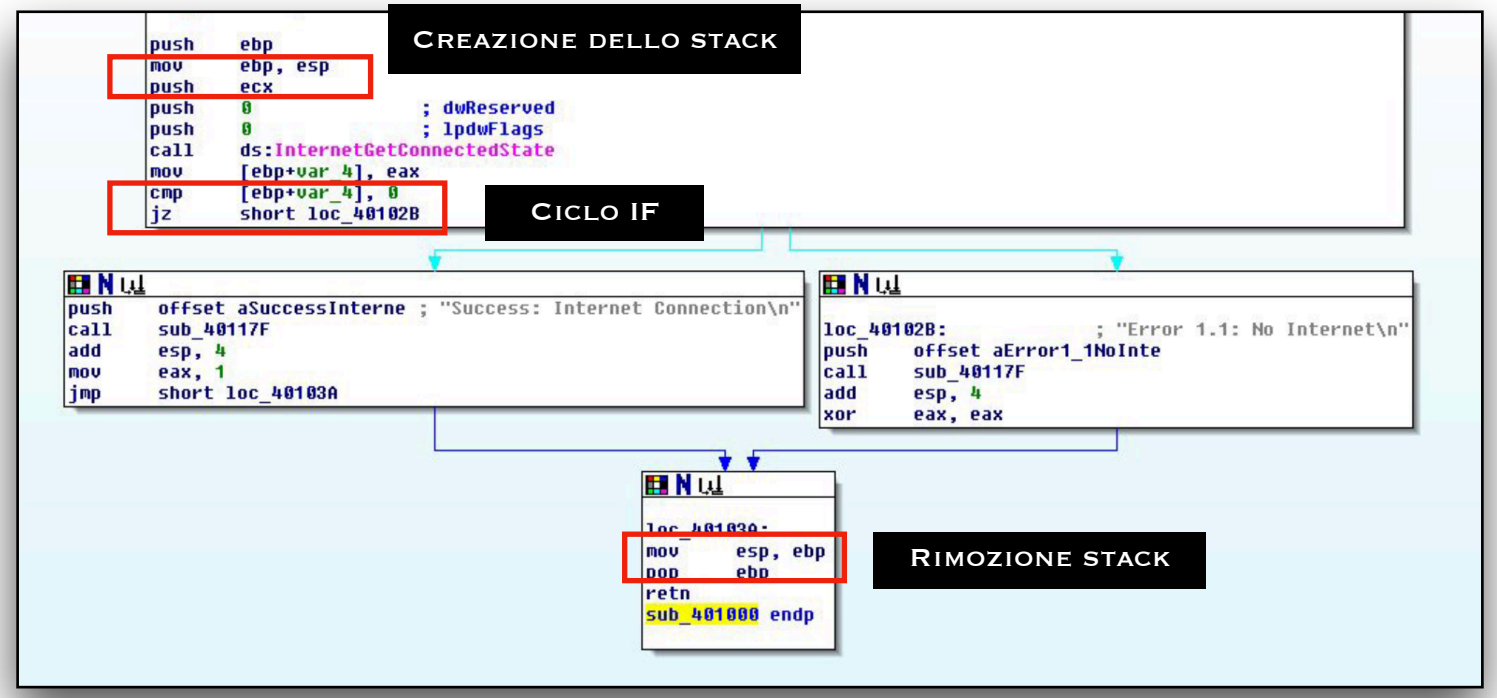
**.rdata -** contiene le informazioni delle librerie e le funzioni importate ed esportate dall'eseguibile.

**.data -** contiene i dati/variabili globali del programma eseguibile. In questo caso possiamo andare a vedere tramite CFF che contiene la seguente info.

**Con riferimento alla figura, risponde ai seguenti quesiti:**




**Identificare i costrutti noti (creazione dello stack, eventuali cicli, costrutti).**




**Ipotizzare il comportamento della funzionalità implementata.**

Questo frammento di codice in Assembly ci indica che attraverso la funzione **InternetGetConnectedState**, si determina se su una macchina è presente una connessione internet.
Attraverso il **costrutto IF**, avviene un controllo sulla funzione, che a seconda del parametro restituito (uguale a 0/diverso da zero) ci indica a schermo la presenza o meno di una connessione internet sulla macchina target.
Come possiamo vedere in figura, se c'è la presenza di una connessione internet, ci restituisce il messaggio '**Success: Internet Connection**', viceversa ci restituisce '**Error 1.1: No Internet**'.