PROGETTO S10L5

TRACCIA

Con riferimento al file Malware_U3_W2_L5 presente all'interno della cartella «Esercizio_Pratico_U3_W2_L5 » sul desktop della macchina virtuale dedicata per l'analisi dei malware, rispondere ai seguenti quesiti:

1. Quali librerievengono importate dal file eseguibile?

2. Quali sono le sezioni di cui si compone il file eseguibile del malware? Con riferimento alla figura in slide 3, risponde ai seguenti quesiti:

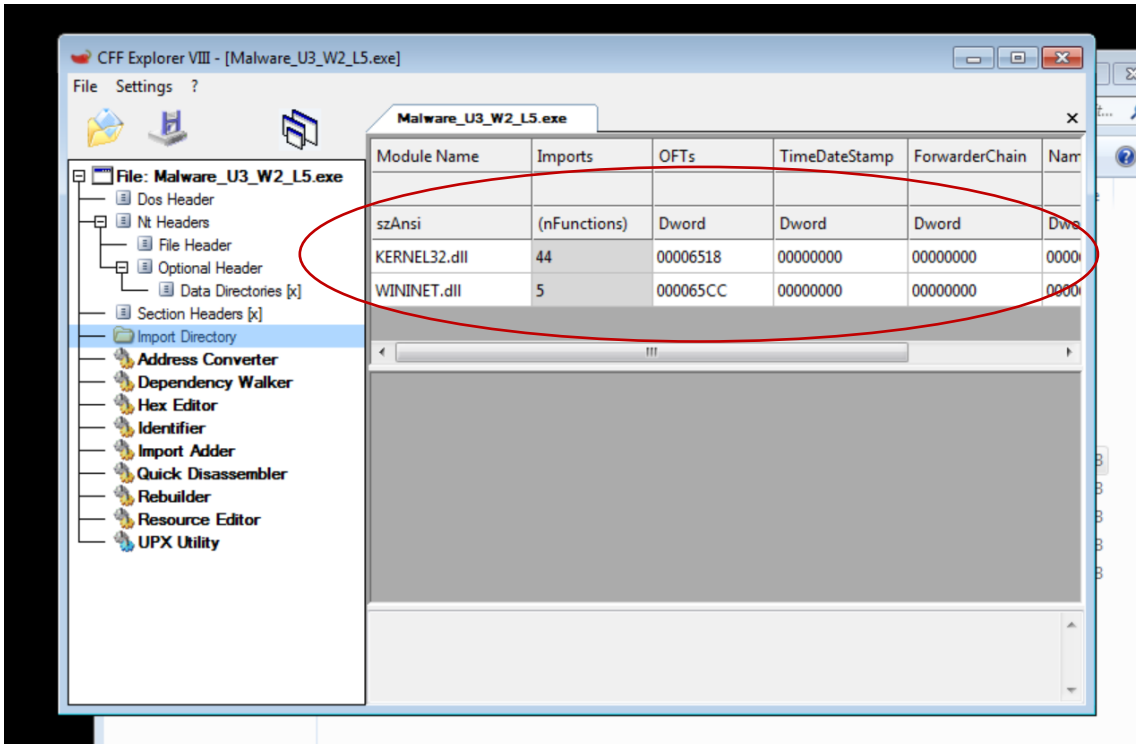
3. Identificare i costrutti noti (creazione dello stack, eventuali cicli, altri costrutti)

4. Ipotizzare il comportamento della funzionalità implementata 5. BONUS fare tabella con significato delle singole righe di codice assembly

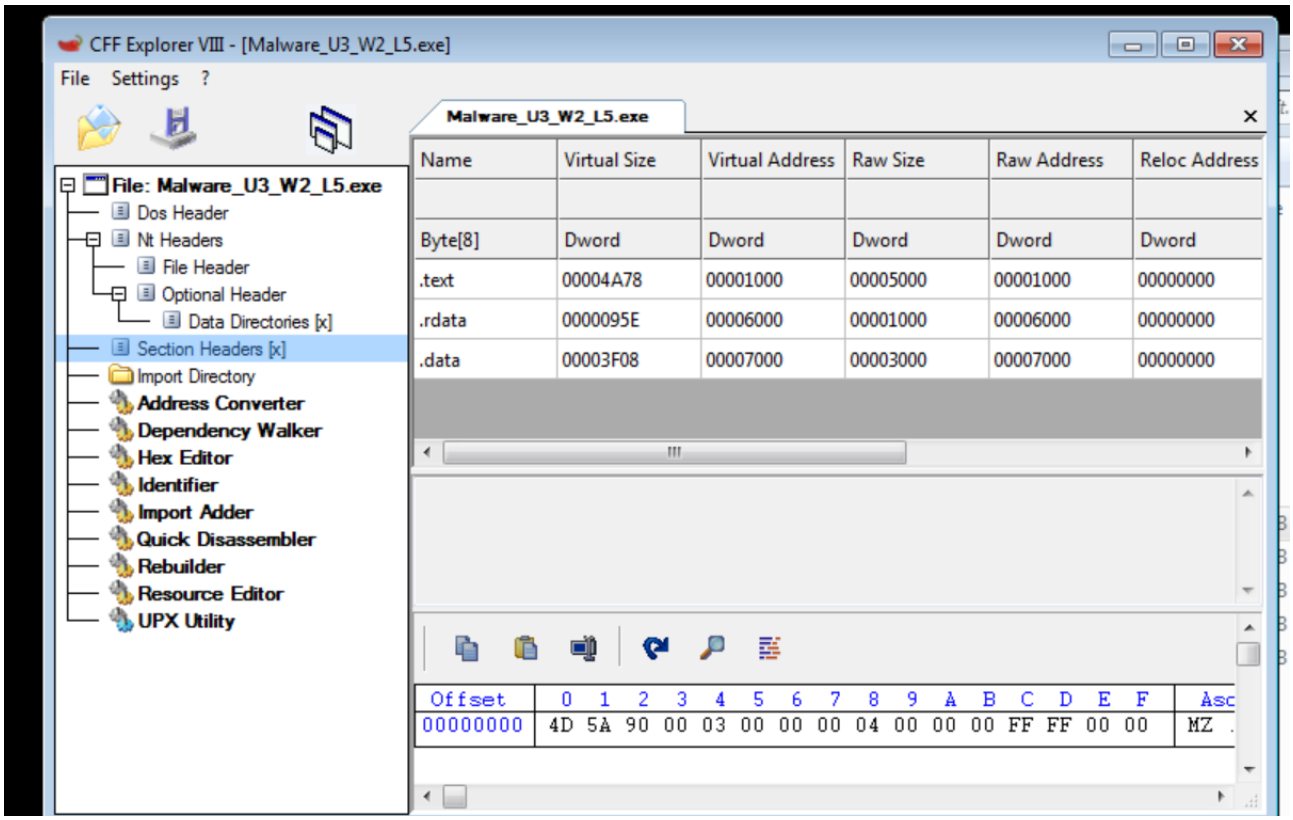
RISPOSTE

1. Utilizzando CFF Explorer, scegliendo «Import directory» dal pannello principale a sinistra. Le librerie importate dal file eseguibile sono:

- Kernel32.dll
- WININET.dll



2. Possiamo controllare le sezioni di cui si compone il file utilizzando ancora CFF Explorer, spostandoci nella sezione «section headers».

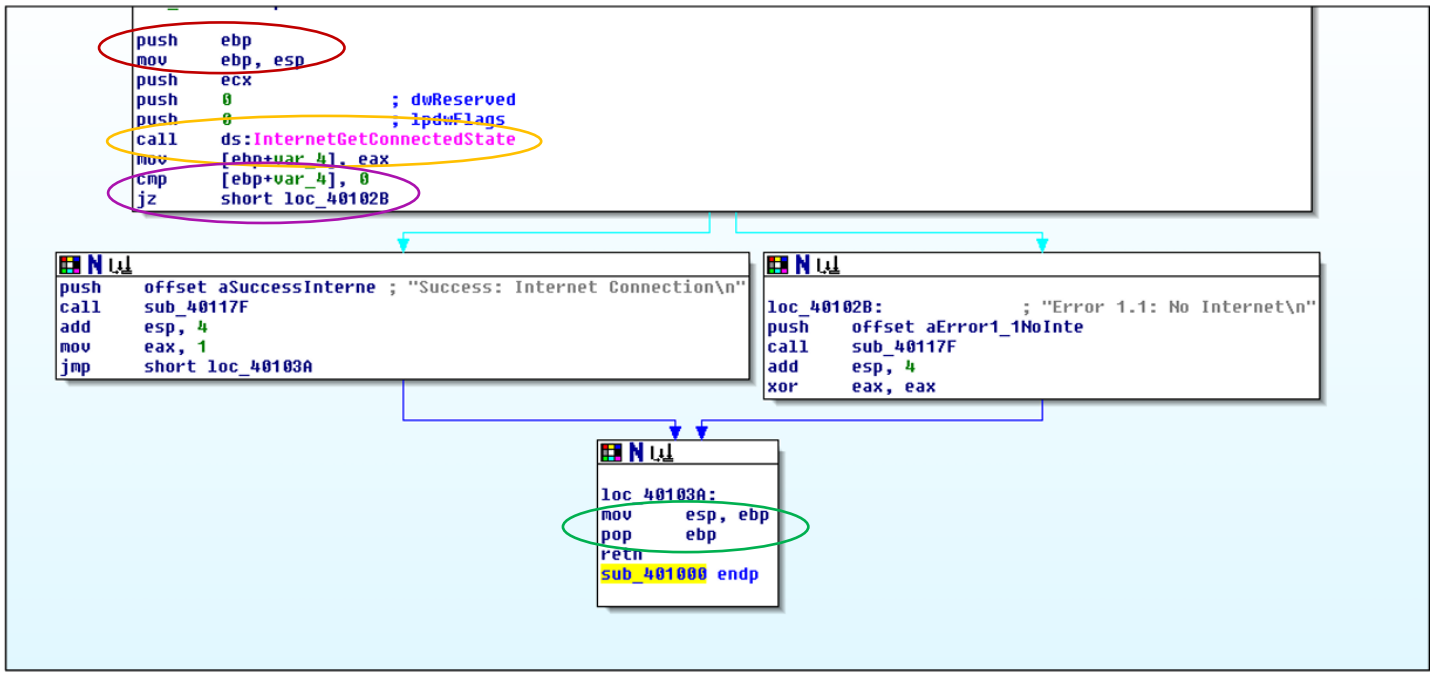


Le sezioni presenti sono:

- **.test**
- **.rdata**
- **.data**

3.

Figura 1



- Creazione dello stack
- Chiamata della funzione
- Costrutto condizionale «IF»
- Rimozione dello stack

4. Questa funzionalità ha lo scopo di controllare se sulla macchina è presente la connessione ad internet. Il costrutto IF «controlla» se il valore restituito dalla funzione getinternetconnectstate è uguale a 0. Se è uguale a 0, la funzione scrive a schermo «no internet» e completa l'esecuzione, mentre se il valore di ritorno della funzione getinternetconnectstate è diverso da 0, la funzione scrive a schermo «Success: Internet Connection».