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:

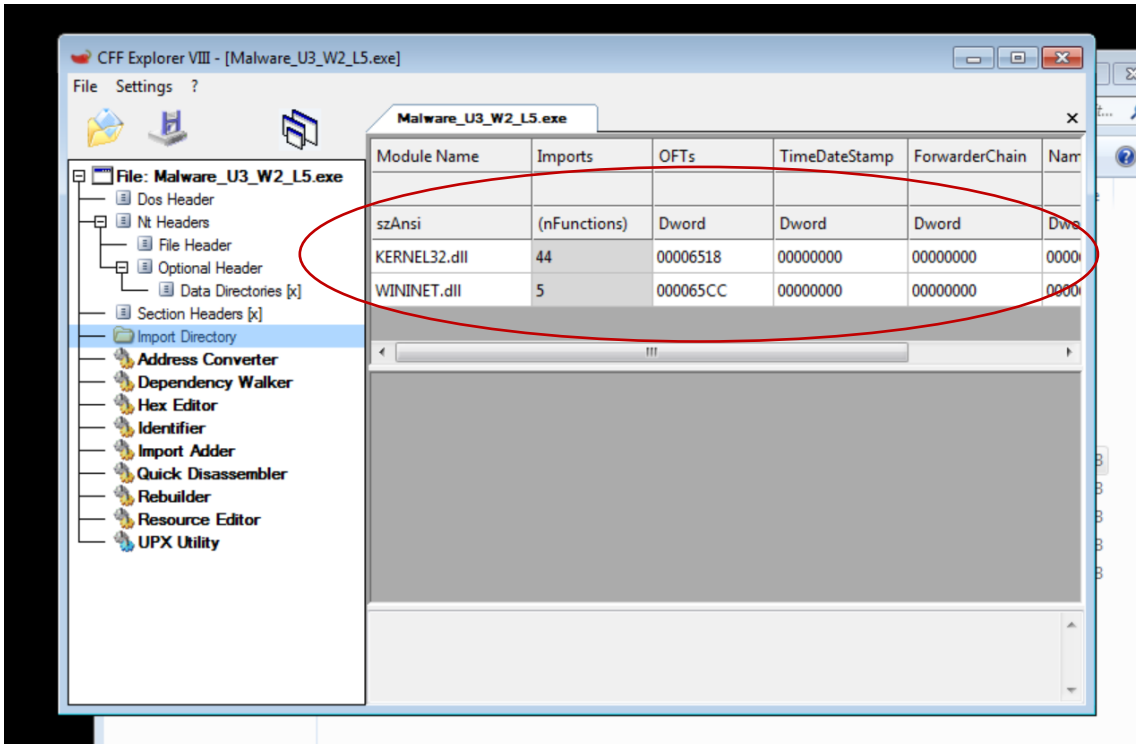
3. Identificare i costrutti noti (creazione dello stack, eventuali cicli, altri costrutti)

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

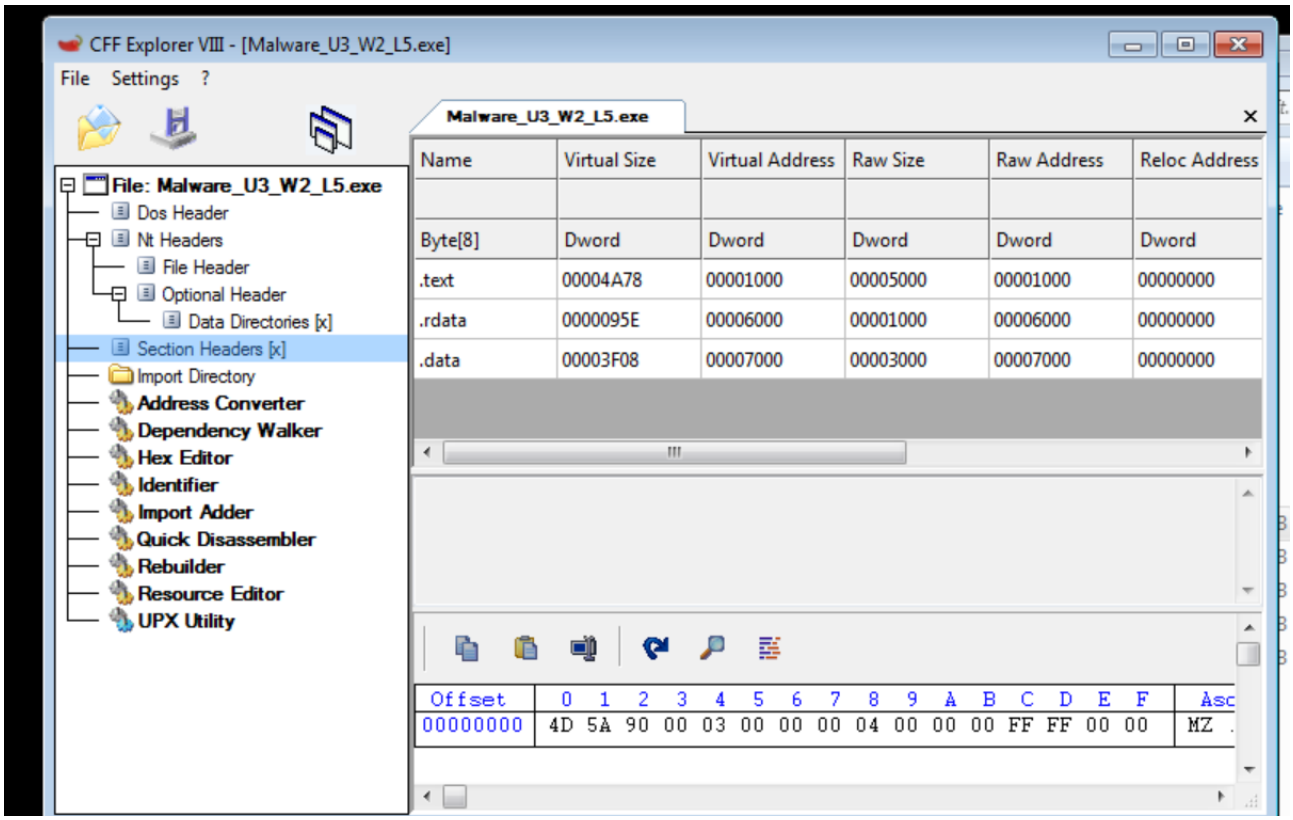
RISPOSTE

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**

.test:

La sezione .test, o .text, è una parte del codice di un programma che contiene le istruzioni eseguibili. Questa sezione contiene il codice macchina che viene eseguito dal processore. Quando si compila un programma, il compilatore traduce il codice sorgente in istruzioni in linguaggio macchina e lo colloca nella sezione .test del file eseguibile. Questo è il codice vero e proprio del programma, che viene caricato in memoria quando il programma viene avviato e viene eseguito dall'unità centrale di elaborazione (CPU).

.rdata:

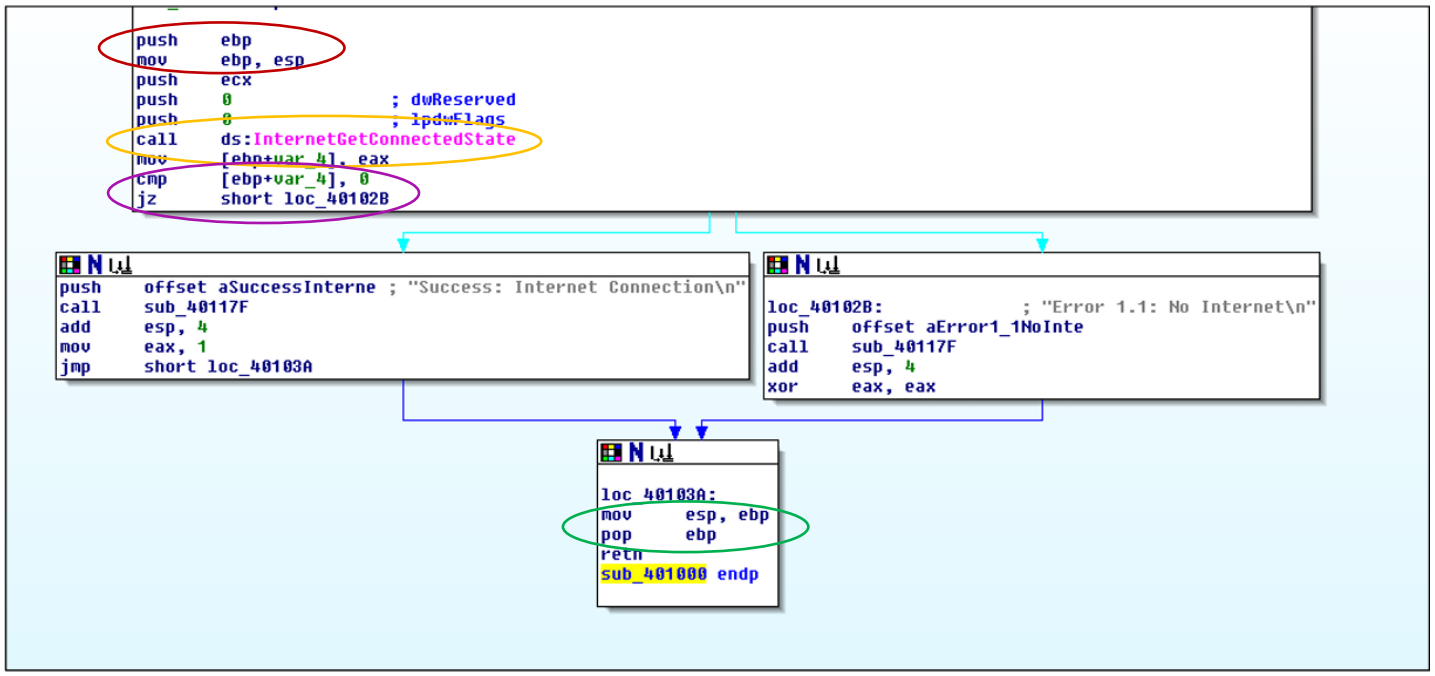
La sezione .rdata, o sezione dati di sola lettura, contiene dati costanti che sono accessibili in sola lettura durante l'esecuzione del programma. Questa sezione è utilizzata per memorizzare dati che non cambiano durante l'esecuzione del programma. Ad esempio, potrebbe contenere stringhe di testo costanti, tabelle di dati predefinite o altre costanti che il programma deve utilizzare. I dati nella sezione .rdata possono essere letti dal programma, ma non possono essere modificati. Questa sezione è particolarmente utile per garantire che i dati costanti siano immutabili e per ottimizzare l'accesso ai dati durante l'esecuzione del programma.

data:

La sezione .data contiene dati inizializzati che possono essere letti e scritti durante l'esecuzione del programma. Questa sezione è utilizzata per memorizzare variabili globali e dati che devono essere modificati durante l'esecuzione del programma. Quando il programma viene avviato, lo spazio necessario per la sezione .data viene allocato e i dati inizializzati vengono copiati in questa sezione. Durante l'esecuzione del programma, il programma può leggere e scrivere questi dati secondo necessità. La sezione .data è utile per memorizzare informazioni dinamiche che devono essere conservate tra diverse chiamate di funzioni o durante l'esecuzione del programma.

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».