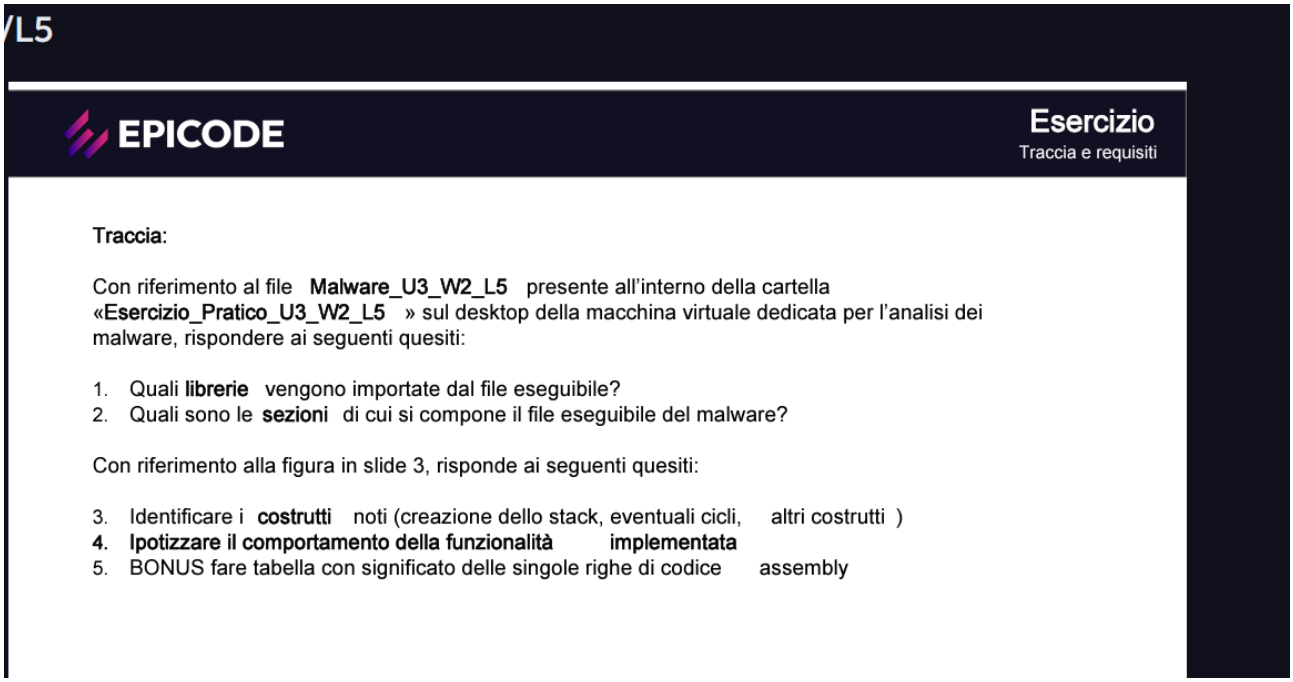


Per poter rispondere ai quesiti riportati nella traccia dobbiamo usare il tool di “CFF Explorer”

Breve

CFF Explorer, è particolarmente utile per analizzare e modificare file PE, che sono il formato standard dei file eseguibili utilizzati nei sistemi operativi Windows. Ecco alcune delle sue principali caratteristiche:

1. Ispezione dei File PE: CFF Explorer consente di esaminare la struttura dei file PE, compresi gli header, le sezioni, le importazioni, le esportazioni, le risorse e altro ancora.

2. Modifica dei File: È possibile modificare vari aspetti di un file PE, come gli header, inclusi il cambio dei timestamp, le informazioni sulla versione del file e l'aggiunta o la rimozione di sezioni.

3. Visualizzazione dei Direttori dei Dati: Fornisce una visualizzazione dettagliata dei direttori dei dati all'interno di un file PE, come il direttorio di esportazione, il direttorio di importazione, il direttorio delle risorse e altro ancora.

4. Editor Esadecimale: CFF Explorer include un editor esadecimale, che consente agli utenti di visualizzare e modificare la rappresentazione esadecimale del file.

5. Dependency Walker: Ha una funzione di dependency walker che aiuta a identificare le dipendenze delle librerie di collegamento dinamico (DLL) di un file PE.

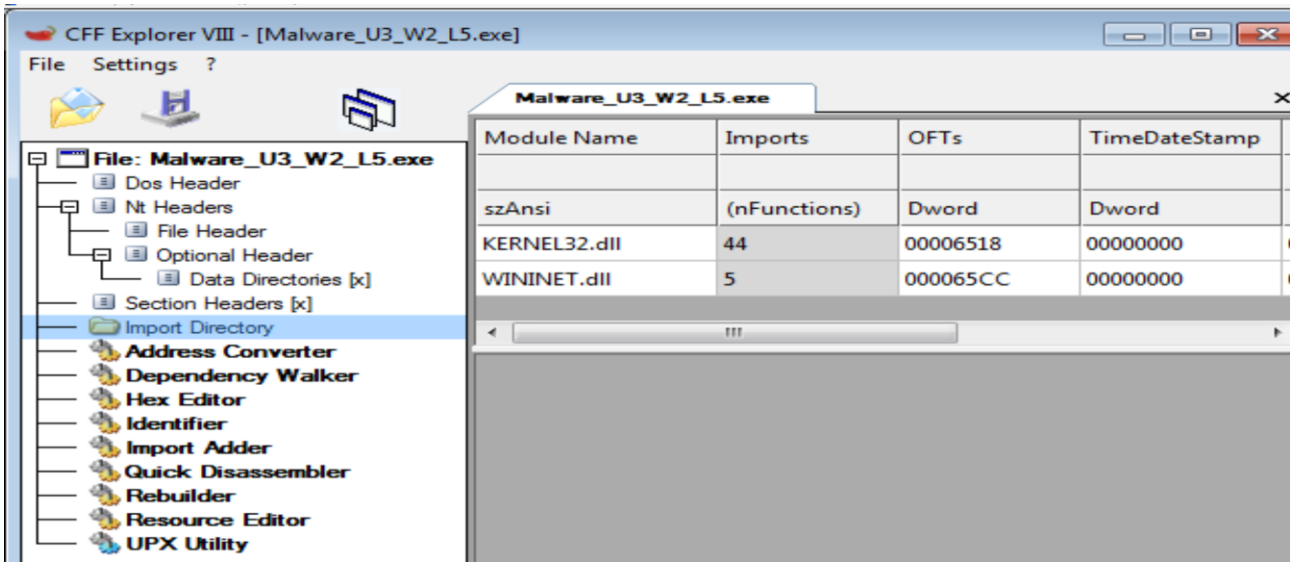
6. Visualizzatore/Editor di Risorse: È possibile visualizzare e modificare le risorse incorporate all'interno di un file PE, come icone, stringhe, bitmap e finestre di dialogo.

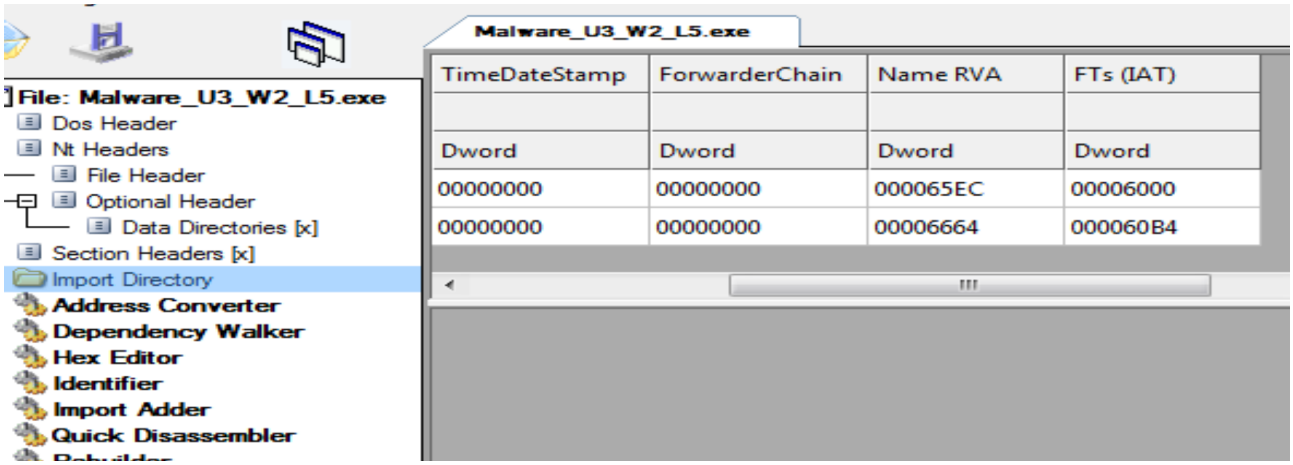
7. Ricostruzione dei File PE: CFF Explorer consente agli utenti di ricostruire i file PE, rendendolo utile per il patching e la modifica degli eseguibili esistenti.

Esercizio

Le Librerie che vengono importate dal file eseguibile sono due e sono:
Kernel32.dll

WININET.dll



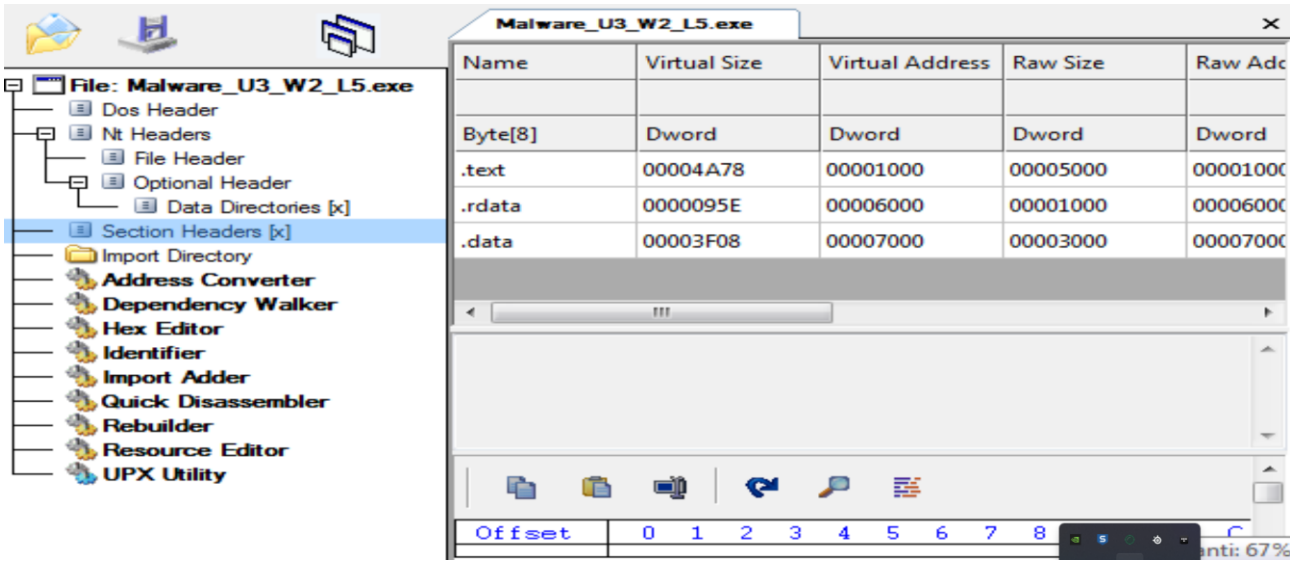


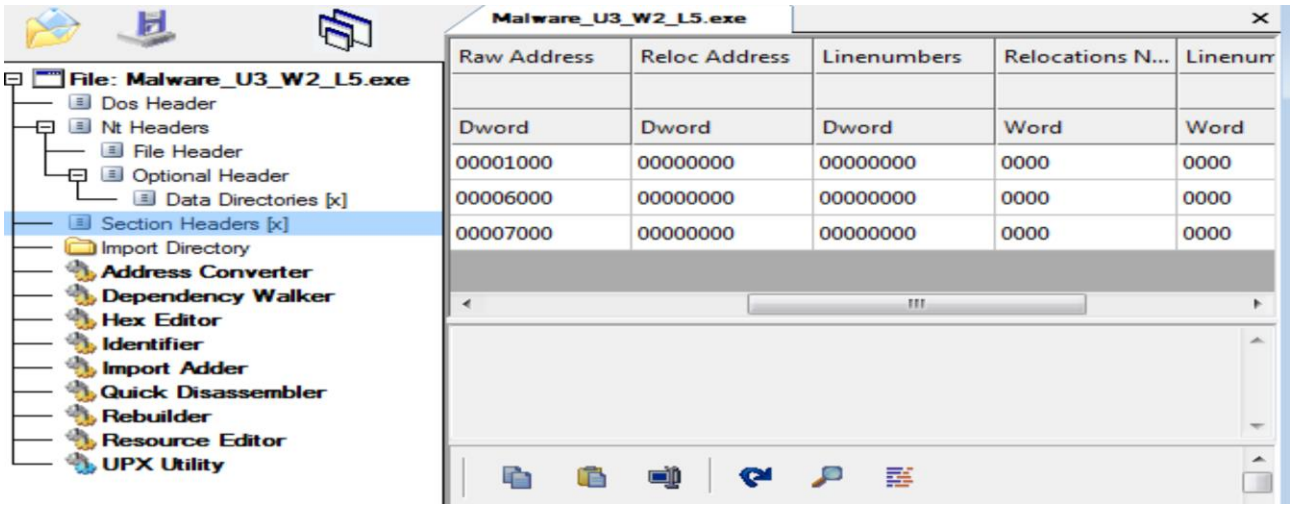
Per trovare le sezioni del file eseguibile presenti ;basta recarsi nella sezione “section Headers”:
le sezioni presenti in questo caso sono 3 e sono:

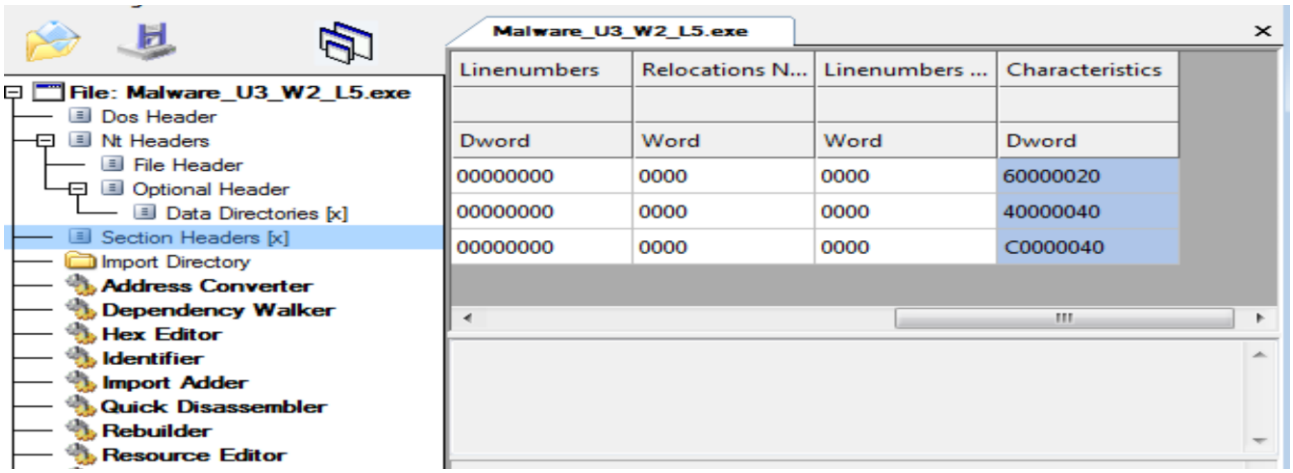
.test

.rdata

.data







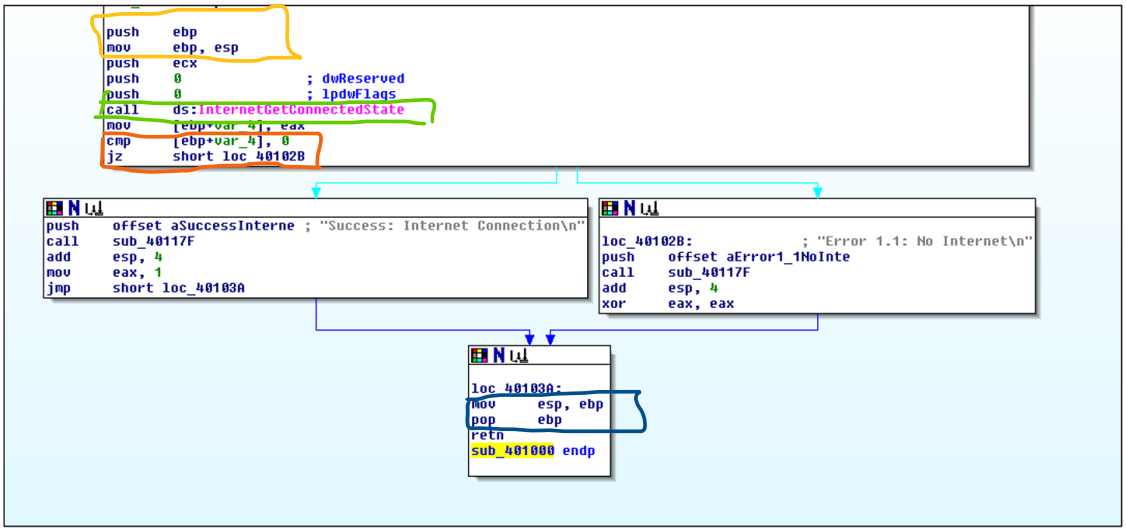
Costrutti noti rappresentati in figura:

1 costrutti che provocano la creazione dello stack (evidenziati in giallo)

2 costrutto condizionale (evidenziato in arancione)

3 costrutti che provocano la rimozione dello stack (evidenziati in blu scuro)

Figura 1



3

Evidenziata di verde nella figura sopra si può una chiamata alla funzione “getinternetconnectstate” che ha lo scopo di effettuare un check della connessione e quindi vedere se la macchina è connessa o meno a internet.

Il costrutto if verifica se il parametro della funzione “getinternetconnectstate” ad esso collegato sia o meno uguale a 0.

Se è uguale a 0 , compare la scritta “no internet” (grazie alla funzione)e si completa l’esecuzione.

Se è il valore della funzione “getinternetconnectstate” diverso da 0, allora a schermo compare la scritta «Success: Internet Connection» e poi viene concluso il compito della funzione.