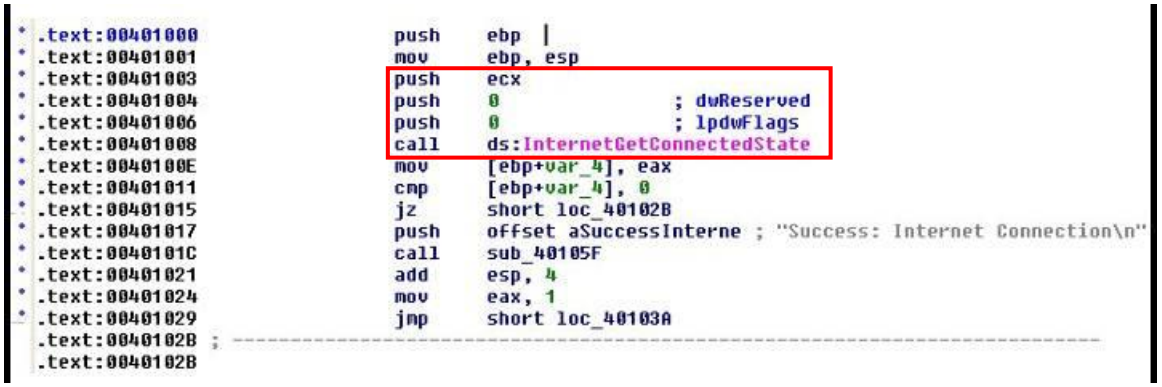
Esercizio 4 Settimana 10

Assembly parte 2

Dato l'estratto di codice di un Malware, la traccia ci chiede di identificare i costrutti noti.

Il primo costrutto che possiamo notare è dato dalle prime due righe di codice che va a creare uno stack per le variabili locali. Possiamo anche notare la presenza dei due puntatori EBP (Extended Base Pointer) ed ESP (Extended Stack Pointer) che puntano rispettivamente alla base ed alla cima dello stack, una parte della memoria che viene utilizzata per gestire variabili locali e parametri delle funzioni durante l'esecuzione di un programma.



Il secondo costrutto evidenziato è una chiamata della funzione 'InternetGetConnectedState' tramite le istruzioni 'push' che passano i parametri allo stack.

Il terzo costrutto è un ciclo if, con una istruzione cmp viene effettuata una sottrazione tra il parametro contenuto nel registro ebp+4_var e 0 la quale modifica la ZF (zero flag). L'istruzione call poi andrà a chiamare la funzione printf.