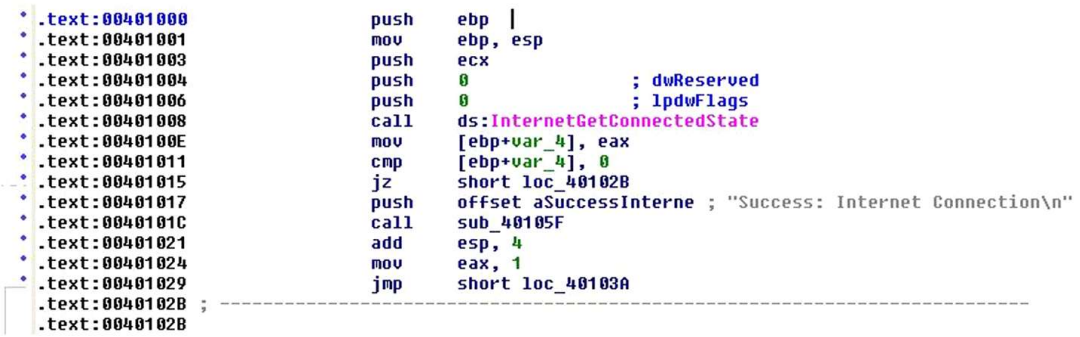
Pratica S10/L4 - Costrutti C - Assembly X8

L'esercizio di oggi consiste nell'identificare i costrutti del malware sotto in figura.



Come prima cosa possiamo notare la creazione dello stack nelle prime 2 righe

Come seconda cosa vediamo come i parametri vengano passati allo stack tramite push e il call prende in input i 3 parametri per controllare se la macchina ha accesso ad internet.

E sotto inizia un ciclo IF-ELSE

Probabilmente questa parte di codice del malware controlla se c'è la connessione ad internet e se esse c'è stampa un messaggio di connessione avvenuta.