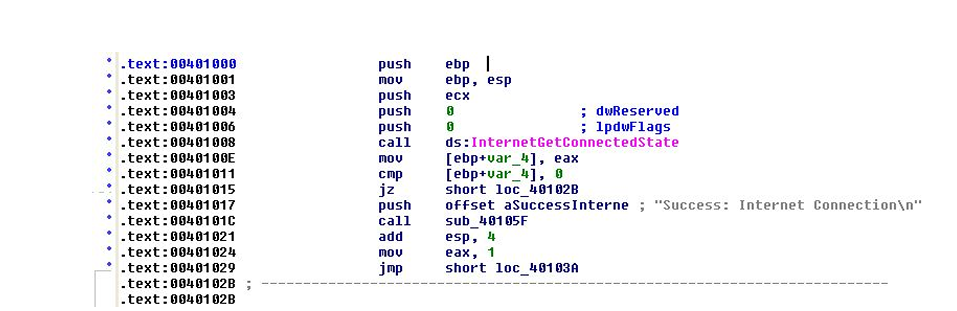
Esercizio 4 Settimana 10

L’esercizio di oggi prevede di identificare i costrutti presenti nel seguente estratto di un codice malware.



Possiamo facilmente capire che il linguaggio usato è l’assembly.

Analizzando il codice possiamo capire che, una volta convertito in linguaggio C ci sono diversi costrutti.

Il primo è quello che crea lo stack (nelle prime 2 righe);

Il costrutto successivo è quello che richiama la funzione, che parte dal comando “push ecx” fino al “call ds:”;

è un IF in quanto l’IF viene rappresentato in assembly con i due passaggi “cmp” e “jump (jz)”. Questo perché l’istruzione cmp prevede una comparazione tra le due variabili. Andrà a sottrarre la prima alla seconda e, nel caso le due risultassero diverse, effettuerà il jump alla locazione stabilita e riprenderà ad eseguire il codice da quel punto. In caso invece il risultato della sottrazione delle due variabili risultasse uguale a 0, allora vorrà dire che le due variabili sono uguali e quindi non verrà effettuato il jump ma il codice proseguirà dal comando “push”.

Come secondo punto dell’esercizio, dovevamo capire cosa faceva questa parte di programma, che sembra fare un controllo sulla connessione Internet e stampare un messaggio di successo se la connessione è attiva.