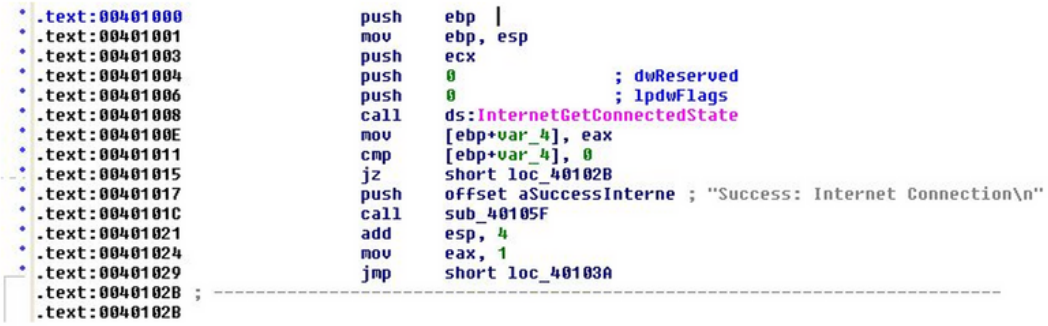
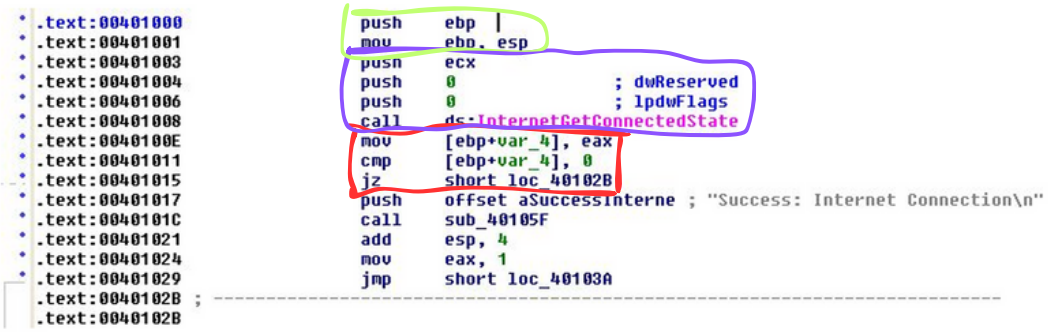
Esercizio S10L4

Traccia:

La figura seguente mostra un estratto del codice di un malware. Identificare i costrutti noti visti durante la lezione teorica.



L'esercizio ci chiede di individuare eventuali costrutti all'interno del del codice in linguaggio assembly



1) Creazione della memoria stack

2) Chiamata funzione

3) Ciclo if

1) Va a creare la memoria stack

2) E' una chiamata di una funzione InternetGetConnectedState. Vengono preparati alcuni argomenti nello stack prima di chiamare la funzione.

3) Viene memorizzato il risultato della funzione InternetGetConnectedState in una variabile locale (ebp+var_4) e successivamente viene confrontato con zero.Se il confronto precedente ha dato 0 (ZF=1), allora salta a loc_40102B, altrimenti prosegue con le istruzioni successive.