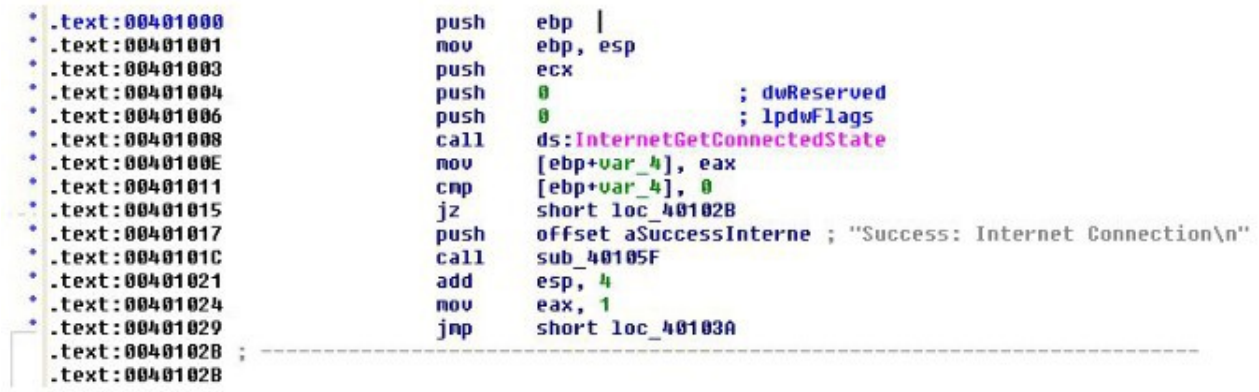
Assembly parte 2



1)La prima istruzione punta la registro ebp.
2)con il comando mov copio il valore di esp in ebp
3) con i tre comandi push da in input i valori alla funzione seguente che chiama la funzione di controllo di connessione ad internet.
4) Inizializza la variabile con il valore di eax e la compara con il valore 0
5) jz (jump zero) questa istruzione andrà a saltare alla short location solo nel caso lo zero flag è uguale a 1.
6) aggiunge 4 al registro esp
7) assegna ad eax il valore 1.

La funzionalità del malware quindi è quella di controllare se c'è connessione ad internet e se esiste andrà a eseguira una determinata funzione.