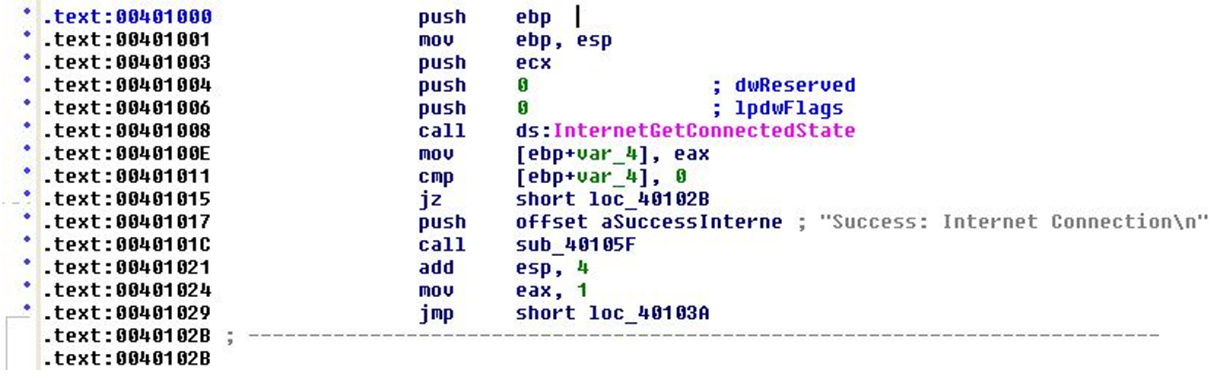
Costrutti C - Assembly X86

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



Il blocco di codice con le istruzioni cmp, jz, push, call, add, mov, e jmp forma un costrutto condizionale tipico di un'istruzione **if** nell'assembly.

L'istruzione cmp [ebp+var_4], 0 confronta il valore salvato in [ebp+var_4] con zero.

L'istruzione jz short loc_40102B effettua un salto condizionale alla posizione di memoria loc_40102B se il risultato della comparazione è zero, indicando che la condizione è soddisfatta.

Nel caso in cui la condizione sia soddisfatta, il blocco di codice successivo, che inizia con push offset aSuccessInterne, viene eseguito. Questo blocco gestisce il caso in cui la connessione Internet è attiva.

Dopo l'esecuzione del blocco condizionale, l'istruzione jmp short loc_40103A effettua un salto incondizionato a loc_40103A.

Questo codice in assembly sta facendo una verifica. Guarda se c'è una connessione Internet attiva. Se c'è, stampa un messaggio "Success: Internet Connection". Se non c'è connessione, salta ad un'altra parte del programma senza fare nulla di specifico per il caso in cui la connessione è assente.