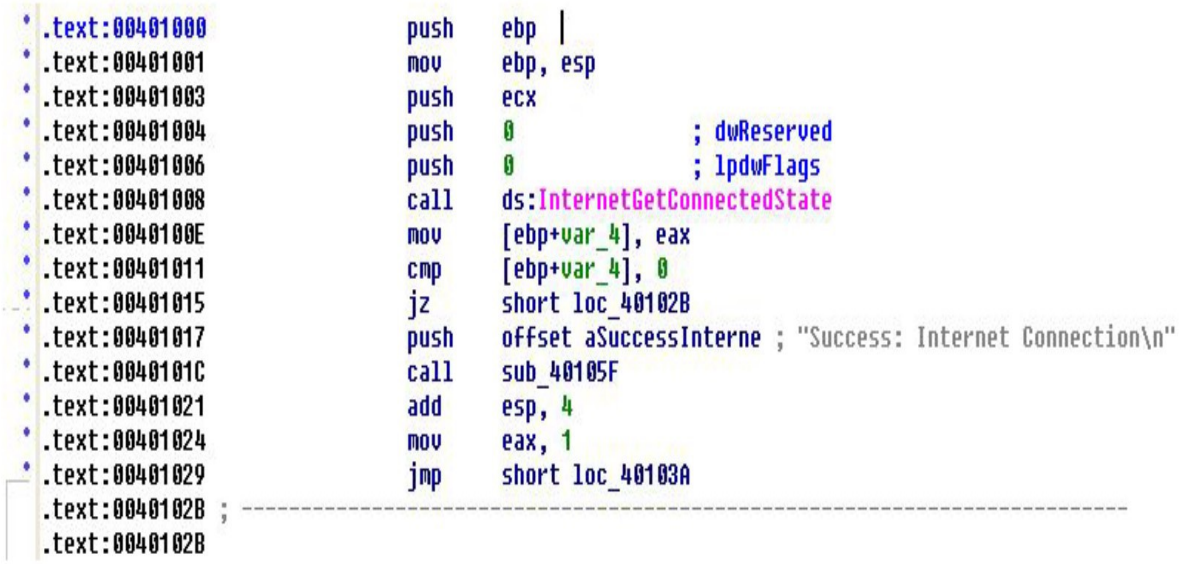
ESERCIZIO U3W2 Giorno 4

Traccia:

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



```
.text:00401000                push    ebp
.text:00401001                mov     ebp, esp
.text:00401003                push    ecx
.text:00401004                push    0               ; dwReserved
.text:00401006                push    0               ; lpdwFlags
.text:00401008                call    ds:InternetGetConnectedState
.text:0040100E                mov     [ebp+var_4], eax
.text:00401011                cmp     [ebp+var_4], 0
.text:00401015                jz      short loc_40102B
.text:00401017                push    offset aSuccessInterne ; "Success: Internet Connection\n"
.text:0040101C                call    sub_40105F
.text:00401021                add     esp, 4
.text:00401024                mov     eax, 1
.text:00401029                jmp     short loc_40103A
.text:0040102B ; ---------------------------------------------------------------------------
.text:0040102B
```

Nell'esercizio odierno andiamo a convertire il nostro codice assemblyx86 in un linguaggio di alto livello ovvero in C.La traduzione fatta evidenzierà una variabile per eseguire una determinata funzione che ancora non sappiamo.

CODICE CONVERTITO IN C TRAMITE www.codeconvert.ai :

```
 #include <stdio.h>

int main() {
    int var_4;
    int ecx = 0;

    if  var_4 = ecx
        printf("Success: Internet connected\n");

   else var_4 /= ecx
       printf("Error: Internet not connected\n");



    return;
}
```

il codice in questione ,analizzando il corpo della funzione in C ,potrebbe essere un codice per una creazione di una backdoor dove grazie ad un booleano se il risultato è true ovvero uguale a 0 permette una connessione ad internet ,mentre se risulta false ovvero diverso da 0 rifiuterà di connettersi.