COSTRUTTI C –ASSEMBLY X86

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
```

OPZIONALE: PROVATE AD IPOTIZZARE CHE FUNZIONALITÀ È IMPLEMENTATA NEL CODICE ASSEMBLY.
HINT: LA FUNZIONE INTERNETGETCONNECTEDSTATE PRENDE IN INPUT 3 PARAMETRI E PERMETTE DI CONTROLLARE SE UNA MACCHINA HA ACCESSO AD INTERNET.

1. `push`: Questo comando viene utilizzato per inserire un valore nello stack.

2. `mov`: Questo comando viene utilizzato per copiare un valore da una posizione a un'altra.

3. `lea`: Questo comando (Load Effective Address) viene utilizzato per calcolare un indirizzo e metterlo in un registro.

4. `call`: Questo comando viene utilizzato per chiamare una funzione.

5. `cmp`: Questo comando viene utilizzato per confrontare due valori.

6. `jz`: Questo comando (Jump if Zero) viene utilizzato per saltare a un'altra parte del codice se il risultato dell'ultimo confronto o calcolo era zero.

7. `add`: Questo comando viene utilizzato per sommare due valori.

8. `nop`: Questo comando (No Operation) non fa nulla. Viene spesso utilizzato per il padding.

9. `jmp`: Questo comando (Jump) viene utilizzato per saltare a un'altra parte del codice.

Il codice sta utilizzando la funzione `InternetGetConnectedState` per controllare se una macchina ha accesso a Internet. Se la macchina è connessa a Internet, il codice stampa "Success: Internet Connection". Questo potrebbe essere utilizzato, ad esempio, da un malware per verificare la connettività Internet prima di eseguire ulteriori azioni dannose.