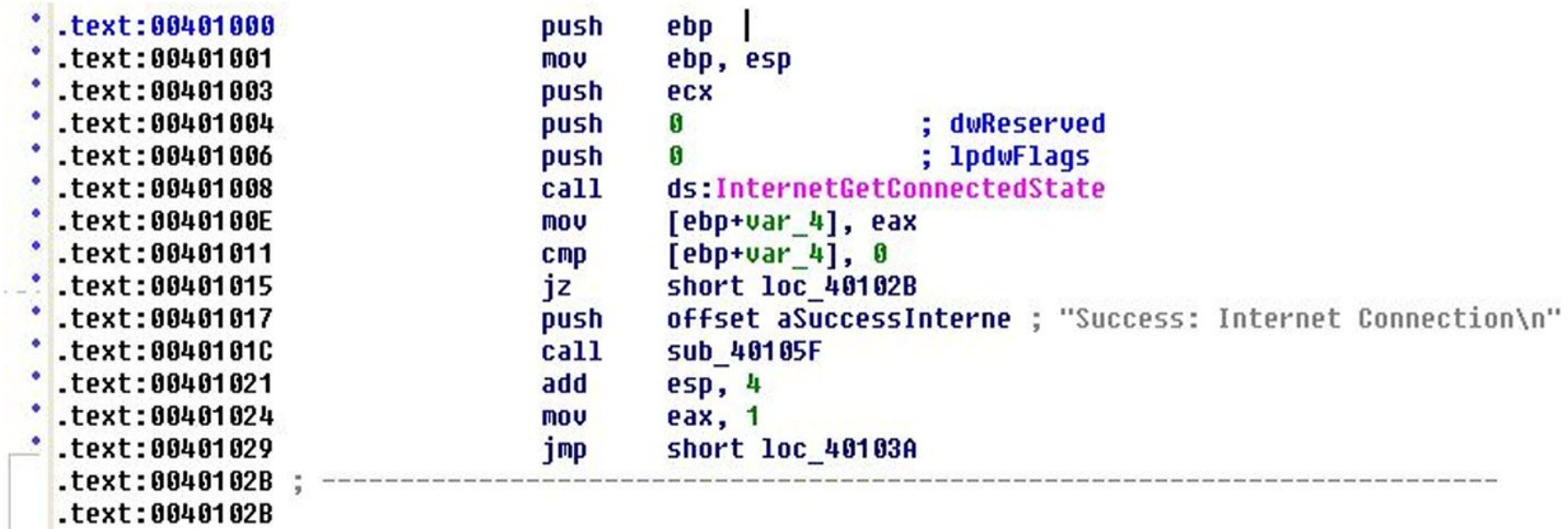
Traccia:

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
```

.text:00401000 push ebp: Salva il valore corrente del registro base EBP nello stack.

.text:00401001 mov ebp, esp: Imposta il registro base EBP per puntare alla cima dello stack corrente. Questo stabilisce un nuovo frame di stack.

.text:00401004 push 0 ;dwReserved

.text:00401006 push 0 ;lpdwFlags

Queste due righe indicano due variabili che sono impostate a **0** e sono parametri per la successiva funzione **.text:00401008 call ds:InternetGetConnectedState**. Viene quindi chiamata la funzione **InternetGetConnectedState** per verificare la connessione internet.

.text:0040100E mov [ebp+var_4], eax

cmp [ebp+var_4], 0

Il valore nel registro EAX viene copiato nella variabile **ebp+var_4** e viene fatta una comparazione (**cmp**) tra questo valore e **0.** Se il risultato di questo compare è 0 viene fatto un salto alla locazione **loc_40102B**.

push offset aSuccessInterne: Questa istruzione mette nello stack l'indirizzo di una stringa di connessione avvenuta e viene chiamata una funzione all' indirizzo di memoria **sub_40105F**

.text:00401021 add esp, 4: il puntatore dello stack ESP viene ripristinato al suo stato precedente. Questa istruzione aggiunge 4 a ESP.

inc eax, 1: aumenta di **1** il contenuto del registro **EAX**

.text:00401029 jmp short loc_40103A: esegue un jump all' indirizzo di memoria **loc_40103A**