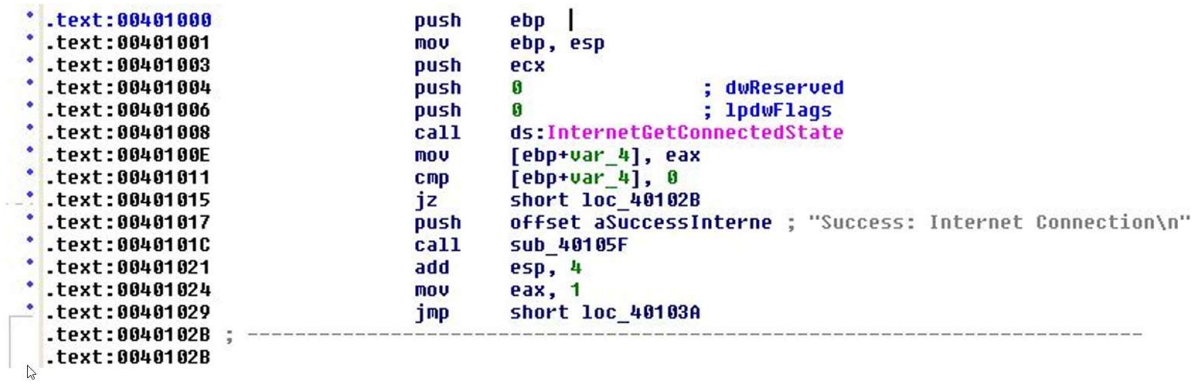
Traccia:

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
```

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.

Analisi del codice:

1. Preparazione per la chiamata alla funzione:

   - Viene creato lo stack per la funzione.
   - I parametri della funzione, dwReserved e lpdwFlags, vengono inseriti nello stack.

2. Verifica della connessione a internet:

   - Viene chiamata una funzione per verificare se la macchina ha accesso a internet.
   - Il valore di eax viene assegnato alla locazione di memoria puntata da ebp più un offset definito in precedenza.

3. Controllo del valore nella memoria:

   - Il valore contenuto nell'area di memoria viene confrontato con 0.
   - I flag ZF e CF vengono impostati in base al risultato del confronto.

4. Salto condizionato:

   - Se ZF è alto (il valore è uguale a 0), si verifica un salto condizionato (jz).
   - Vengono saltate tutte le istruzioni successive.

5. Elaborazione in caso di mancata connessione:

    - Se ZF è basso (il valore non è uguale a 0), il salto non viene effettuato.
    - L'indirizzo (offset) dell'etichetta aSuccessInterne viene calcolato e inserito nello stack.
    - L'etichetta aSuccessInterne viene probabilmente stampata.

6. Conclusione:

    - Il valore di ebp viene spostato.
    - eax viene valorizzato con 1.
    - Un salto incondizionato (jmp) viene eseguito.