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
```

1.

```
.text:00401000                push    ebp
.text:00401001                mov     ebp, esp
```

Le prime due istruzioni creano uno stack di grandezza 0, dove i valori della cima (ESP) e della base (EBP) dello stack sono uguali (mov ebp, esp).

2.

```
.text:00401003                push    ecx
.text:00401004                push    0               ; dwReserved
.text:00401006                push    0               ; lpdwFlags
.text:00401008                call    ds:InternetGetConnectedState
```

Successivamente tre istruzioni push passano i tre parametri richiesti alla funzione che viene chiamata successivamente con l'instruzione call: **InternetGetConnectedState**, che recupera lo stato di connessione del sistema locale.

Rif: https://learn.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-internetgetconnectedstate

3.

Successivamente abbiamo un blocco che implementa la funzione **If**:

Nella prima istruzione la variabile [ebp+var_4] viene inizializzata con il valore del registro eax con il comando mov.

L'istruzione **cmp [ebp+var_4], 0** con un'operazione di sottrazione, verifica il valore della variabile:

se [ebp+var_4] = 0, lo Zero Flag viene settato a 1 e il Carry Flag a 0

se [ebp+var_4] > 0, lo Zero Flag viene settato a 0 e il Carry Flag a 0

se [ebp+var_4] < 0, lo Zero Flag viene settato a 0 e il Carry Flag a 1

L'istruzione **jz short loc_40102B** esegue il salto condizionale, passando all'indirizzo specificato se lo Zero Flag = 1.

Il salto viene effettuato, quindi, se [ebp+var_4] = 0.

4.

Le istruzioni dopo il jz vengono eseguite se [ebp+var_4] <> 0.