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
                                                                   ; dwReserved
; lpdwFlags
 .text:00401004
                                       push
 .text:00401006
                                       push
 .text:00401008
                                       call
                                                ds:InternetGetConnectedState
                                                [ebp+var_4], eax
[ebp+var_4], 0
short loc_40102B
 .text:0040100E
                                       mov
 .text:00401011
                                       cmp
 .text:00401015
                                       jz
                                                offset aSuccessInterne ; "Success: Internet Connection\n"
 .text:00401017
                                       push
                                                sub_40105F
esp, 4
eax, 1
short loc_40103A
 .text:0040101C
                                       call
 .text:00401021
                                       add
 .text:00401024
                                       MOV
 .text:00401029
                                      imp
 .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. Creazione Stack

```
.text:00401000
                                  push
                                           ebp |
 .text:00401001
                                  mov
                                           ebp, esp
 .text:00401003
                                  push
* .text:00401004
                                  push
                                           0
                                                              dwReserved
text:00401006
                                  push
                                                            ; lpdwFlags
 .text:00401008
                                  call
                                           ds:InternetGetConnectedState
                                           [ebp+var_4], eax
[ebp+var_4], 0
.text:0040100E
                                  mov
 .text:00401011
                                  cmp
 .text:00401015
                                           short loc_40102B
                                  jz
 .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
```



2. Tramite push passaggio parametri allo Stack

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

3. Creazione Ciclo IF

```
.text:00401000
                                  push
                                           ebp
.text:00401001
                                  mov
                                           ebp, esp
.text:00401003
                                  push
                                           ecx
.text:00401004
                                  push
                                           0
                                                               dwReserved
.text:00401006
                                  push
                                                             ; lpdwFlags
.text:00401008
                                           ds:InternetGetConnectedState
                                  call
.text:0040100E
                                           [ebp+var 4], eax
                                  mov
                                           [ebp+var_4], 0
short loc 40102B
.text:00401011
                                  CMP
.text:00401015
                                  jz
.text:00401017
                                  push
                                           offset aSuccessInterne ; "Success: Internet Connection\n'
.text:0040101C
                                  call
                                           sub_40105F
                                           esp, 4
eax, 1
short loc_40103A
.text:00401021
                                  add
.text:00401024
                                  mov
.text:00401029
                                  jmp
.text:0040102B
.text:0040102B
```

Si ipotizza che il malware con la chiamata della funzione "InternetConnectState" controlla il valore di ritorno con un if e se il valore è diverso da 0, vuol dire che c'è la presenza di una connessione Internet.