S10-L4

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
```

Evidenziamo i 4 costrutti

Le prime due istruzioni evidenziate (push e mov) servono per la creazione dello stack.

Le altre istruzioni cerchiate (le push e la call) serve per richiamare la funzione, sono stesso i push a passare sullo stack i parametri.

Le altre due evidenziate sono il costrutto IF, avente come else il jump.

Le ultime due istruzioni cerchiate (push e call ancora) servono per richiamare la funzione.

Ipotesi funzionalità
Il codice assembly sembra controllare se c'è una connessione Internet attiva utilizzando la funzione InternetGetConnectedState. Se la connessione è presente, il programma stampa un messaggio di successo "Success: Internet Connection". Dopo di che, chiama un'altra funzione sub_40105F, che probabilmente esegue ulteriori operazioni se la connessione è attiva.