




# Esercizio 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
```

Opzionale: Provate ad ipotizzare che funzionalità è implementata nel codice assembly.



Analizzando con attenzione il codice proposto facciamo le seguenti osservazioni. Oltre che essere relativamente breve non sembra contenere molte funzioni di comparazione e salto, le quali sono indicative di costrutti più complessi come switch, cicli for e cicli while, invece noto una singola coppia di istruzioni `cmp + jz` agli indirizzi 00401011 e 00401015 che plausibilmente fanno riferimento ad una condizione di controllo attribuibile ad un unico costrutto `if`.

```
.text:00401011      cmp     [ebp+var_4], 0
.text:00401015      jz      short loc_40102B
.text:00401017      push    offset aSuccessInterne
```

Se dovessi ipotizzare quale sia il funzionamento del codice presentato direi che rappresenti una funzione che determina se sia stabilita una connessione ad internet oppure una funzione che prova a stabilire una connessione ad internet.

Questa spiegazione è supportata dal richiamo di una funzione chiamata `InternetGetConnectedState` all'indirizzo 00401008 e dal codice all'indirizzo 00401017.

```
.text:00401008      call    ds:InternetGetConnectedState
.text:00401017      push    offset aSuccessInterne ; "Success: Internet Connection\n"
```