

## Assembly parte 2

```
* .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 a$uccessInterne ; "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) La prima istruzione punta la registro ebp.
- 2) con il comando mov copio il valore di esp in ebp
- 3) con i tre comandi push da in input i valori alla funzione seguente che chiama la funzione di controllo di connessione ad internet.
- 4) Inizializza la variabile con il valore di eax e la compara con il valore 0
- 5) jz ( jump zero) questa istruzione andrà a saltare alla short location solo nel caso lo zero flag è uguale a 1.
- 6) aggiunge 4 al registro esp
- 7) assegna ad eax il valore 1.

La funzionalità del malware quindi è quella di controllare se c'è connessione ad internet e se esiste andrà a eseguire una determinata funzione.