M6 D4

ESERCIZIO

```
.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
```

ESTRATTO DEL CODICE DI UN MALWARE

Hint:
La funzione **internetgetconnectedstate** prende in input 3 parametri e permette di controllare se una macchina ha accesso ad Internet.

- **CREAZIONE STACK:**
  - 00401000: push ebp - Crea il valore ebp, creando lo stack
  - 00401001: mov ebp, esp - Sposta il valore esp su ebp
- **CHIAMATA DI FUNZIONE:**
  - 00401003: push ecx - Crea il valore ecx sullo stack
  - 00401004: push 0 - Crea il valore 0 sullo stack come secondo parametro (var 004)
  - 00401006: push 0 - Crea il valore 0 sullo stack come primo parametro (var 006)
  - 00401008: call ds:InternetGetConnectedState - Chiama la funzione "InternetGetConnectedState"
  - 0040106E: mov [ebp+var_4], eax - Sposta il valore di eax nella variabile ebp+var_4 salvata nello stack

- **ISTRUZIONE DI CONTROLLO (IF):**
    - 00401011: cmp [ebp+var_4], 0 - Confronta il valore di ebp+var_4 con 0
    - 00401015: jz short loc_406102B - Salta all'indirizzo loc_406102B se i due valori sono uguali
    - 00401017: push offset aSuccessInterne - Inserisce la stringa "Success: Internet Connection\n" nello stack
    - 0040101C: call sub_40105F - Chiama alla funzione su indirizzo "sub_40105F" (non presente nel codice)
    - 00401021: add esp, 4 - Aggiunge 4 all'indirizzo di memoria esp
    - 00401024: mov eax, 1 - Sposta il valore 1 nel registro eax
    - 00401029: jmp short loc_461083A - Salta all'indirizzo loc_461083A
- **FINE CODICE:**
    - 0040102B

Dal codice analizzato si vede la chiamata alla funzione internetgetconnectedstate e il seguente controllo del valore di ritorno tramite “IF”. Se il valore di ritorno sarà differente da 0, verrà stampata a schermo la stringa “Success: Internet Connection”.