

Esercizio S10L4

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
```

L'esercizio ci chiede di individuare eventuali costrutti all'interno del del codice in linguaggio assembly

```
.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
```

1) Creazione della memoria stack

2) Chiamata funzione

3) Ciclo if

1) Va a creare la memoria stack

2) E' una chiamata di una funzione InternetGetConnectedState. Vengono preparati alcuni argomenti nello stack prima di chiamare la funzione.

3) Viene memorizzato il risultato della funzione InternetGetConnectedState in una variabile locale (ebp+var_4) e successivamente viene confrontato con zero. Se il confronto precedente ha dato 0 (ZF=1), allora salta a loc_40102B, altrimenti prosegue con le istruzioni successive.