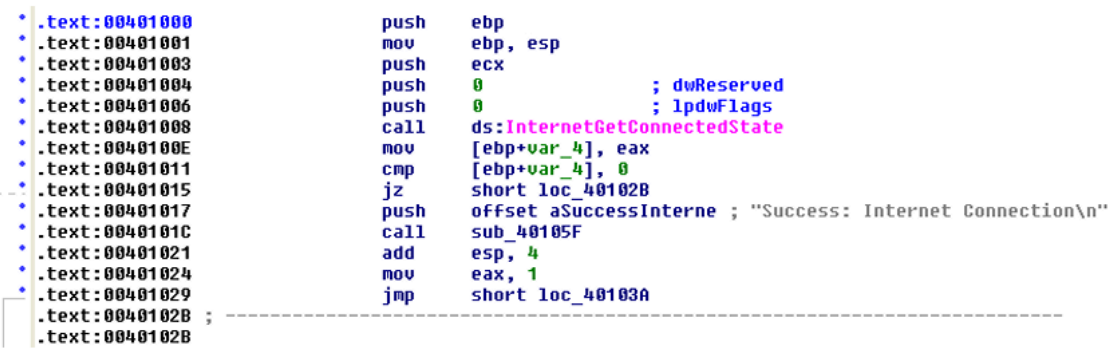
S10L4

1. Identificare i costrutti noti (es. while, for, if, switch, ecc.)

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'unico costrutto noto presente in questo codice assembly è il seguente:

cmp [ebp+var_4], 0 **confronta la variabile con 0**
jz short loc_40102B **in caso la condizione è vera(ovvero che la variabile è uguale a 0),il flusso salta alla locazione loc_40102B(If).**

2.Ipotizzare la funzionalità –esecuzione ad alto livello

il codice controlla lo stato della connessione Internet utilizzando la funzione di sistema ***internetgetconnectdstate*** e gestisce il flusso del programma di conseguenza, eseguendo azioni specifiche a seconda dello stato della connessione.

BONUS: studiare e spiegare ogni singola riga di codice

1. push ebp: Questa istruzione inserisce il valore di ebp nello stack.
2. mov ebp, esp: Questa istruzione inserisce il valore dello stack pointer (esp) nel base pointer (ebp).
3. push ecx:Mette il valore corrente del registro ecx nello stack.
4. push 0:Mette il valore zero nello stack,utilizzato per la funzione internetgetconnectdstate.
5. push 0:Mette un altro valore zero nello stack,per la funzione internetgetconnectdstate.
6. call ds:internetgetconnectdstate:Questa istruzione chiama la funzione di sistema internetgetconnectdstate.
7. mov [ebp+var_4], eax: Salva il risultato contenuto in eax dentro la variabile locale [ebp+var_4].
8. cmp [ebp+var_4], 0: Confronta il valore salvato nella variabile locale con zero.
9. jz short loc_40102B: Se la condizione è vera, il flusso salta a loc_40102B.
10. push offset asuccessinterne: Mette l'indirizzo dell'etichetta asuccessinterne nello stack.
11. call sub_40104F: Chiama una subroutine.
12. add esp, 4:aggiunge 4 ad esp.
13. mov eax, 1: Carica 1 nel registro eax.
14. jmp short loc_40103A: Salta a loc_40103A