ESERCIZIO 4 SETTIMANA 10

Identificare i costrutti del seguente estratto di codice di un malware:

```
push    ebp
mov     ebp, esp
push    ecx
push    0               ; dwReserved
push    0               ; lpdwFlags
call    ds:InternetGetConnectedState
mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0
jz      short loc_40102B
push    offset aSuccessInterne ; "Success: Internet Connection\n"
call    sub_40105F
add     esp, 4
mov     eax, 1
jmp     short loc_40103A
```

In questo codice possiamo identificare i costrutti **if** e **for** grazie alle istruzioni **cmp** e **jz**.

```
cmp     [ebp+var_4], 0
jz      short loc_40102B
```

Viene controllato se il valore salvato in **'[epb+var_4]**' è uguale a 0, che corrisponde alla connessione internet riuscita che, se vera fa un salto (**jz**) a **loc_40102B.**

La parte **loc_40102B** viene eseguita solo se la condizione viene soddisfatta.

Questo codice in Assembly sembrerebbe controllare lo stato della connessione internet. Se connesso stampa un messaggio di successo. Dopo che è stato creato un nuovo frame di stack viene chiamata la funzione **InternetGetConnectedState.** Il valore che verrà restituito dalla funzione sarà controllato e, se la connessione è attiva stampa un messaggio di conferma, se non è attiva invece salta a una parte di codice.