Costrutti C - Assembly x86

Cyber Security &
Ethical Hacking

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
```

```
.text:00401000 push ebp

.text:00401001 mov ebp, esp

.text:00401003 push ecx
```

Queste istruzioni iniziano una funzione, salvando il valore corrente del registro di base (ebp) nello stack e impostando ebp come l'indirizzo corrente dello stack.

```
.text:00401004 push 0 ; dwReserved

.text:00401006 push 0 ; lpdwFlags

.text:00401008 call

ds:InternetGetConnectedState
```

Queste istruzioni chiamano la funzione InternetGetConnectedState per verificare lo stato della connessione internet. I parametri dwReserved e lpdwFlags sono entrambi impostati a 0 prima della chiamata.

```
.text:0040100E mov [ebp+var_4], eax


.text:00401011 cmp [ebp+var_4], 0

.text:00401015 jz short loc_40102B
```

Il risultato della chiamata a InternetGetConnectedState viene memorizzato in una variabile locale ([ebp+var_4]).

Viene effettuato un confronto tra il risultato e zero. Se il risultato è zero (jz = jump if zero), viene eseguito un salto corto (short) a loc_40102B.

```
.text:00401017 push offset asuccessInterne ;
"Succes Internet Connection\n"
.text:0040101C call sub_40105F
.text:00401021 add esp, 4
.text:00401024 mov eax, 1
.text:00401029 jmp short loc_40103A
```

Se il risultato è diverso da zero, vengono eseguite queste istruzioni. Viene chiamata una subroutine sub_40105F con un messaggio come parametro, e successivamente viene restituito il valore 1.

In breve, sembra che questo codice assembly verifichi lo stato della connessione internet utilizzando la funzione InternetGetConnectedState. Se la connessione è attiva, viene stampato un messaggio e la funzione restituisce 1; altrimenti, il flusso di controllo potrebbe passare ad altro codice (che potrebbe gestire il caso in cui la connessione internet non è attiva).