



28/03/2024

# Costrutti C - Assembly x86

Prepared by:  
Manuel Buonanno

Organized by:



# Indice

1) Traccia.....	3
2) Spiegazione e costrutti.....	4
2.1) spiegazione e costrutti.....	5
3) Esecuzione.....	6

# 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
```

Provate ad ipotizzare che funzionalità è implementata nel codice assembly.


Hint: La funzione `<<internetgetconnectedstate>>` permette di controllare se una macchina ha accesso ad Internet.

Consegna:

1. Identificare i costrutti noti (es. while, for, if, switch, creazione/distruzione stack, ecc.)
2. Ipotizzare la funzionalità – esecuzione ad alto livello
3. BONUS: studiare e spiegare ogni singola riga di codice

## 1.3. Spiegazione e costrutti

- **push ebp**  
creazione dello stack inserendo il valore del registro ebp.
- **mov ebp, esp**  
sposta il valore del registro esp nel registro ebp dello stack.
- **push ecx**  
inserisci nello stack il valore del registro ecx.
- **push 0**  
inserisci un contatore settato a 0 nello stack.
- **push 0**  
inserisci un flag settato a 0 nello stack.
- **call ds:InternetGetConnectedState**  
controlla se la macchina ha accesso ad internet.
- **move [ebp+var\_4], eax**  
assegna alla variabile ebp+var\_4 il valore contenuto del registro eax (registro che di default é un accumulatore).
- **cmp [ebp+var\_4], 0**  
compara il valore presente nell'indirizzo di memoria ebp+var\_4 con il valore 0. Se sono uguali lo ZF verrà impostato a 1, altrimenti a 0. Se diverso da 0 allora c'è una connessione attiva.

- **jz short loc\_40102B**  
salta alla locazione di memoria 40102B usando un if.  
(descrizione alla riga precedente).
  - **push offset aSuccessInterne**  
connessione andata a buon fine.
  - **call sub\_40105F**  
esegue una chiamata alla funzione specificata.
  - **add esp, 4**  
somma 4 al valore contenuto nel registro esp.
  - **mov eax, 1**  
inserisci il valore 1 nel registro eax.
  - **jmp short loc\_40103A**  
salto incondizionato alla locazione di memoria 40103A.
- 

## 2. Esecuzione

```
state = internetgetconnectedstate (par1,0,0);
```

```
If (state !=0) printf ("Active connection");
```

```
Else return 0;
```

