ESERCITAZIONE

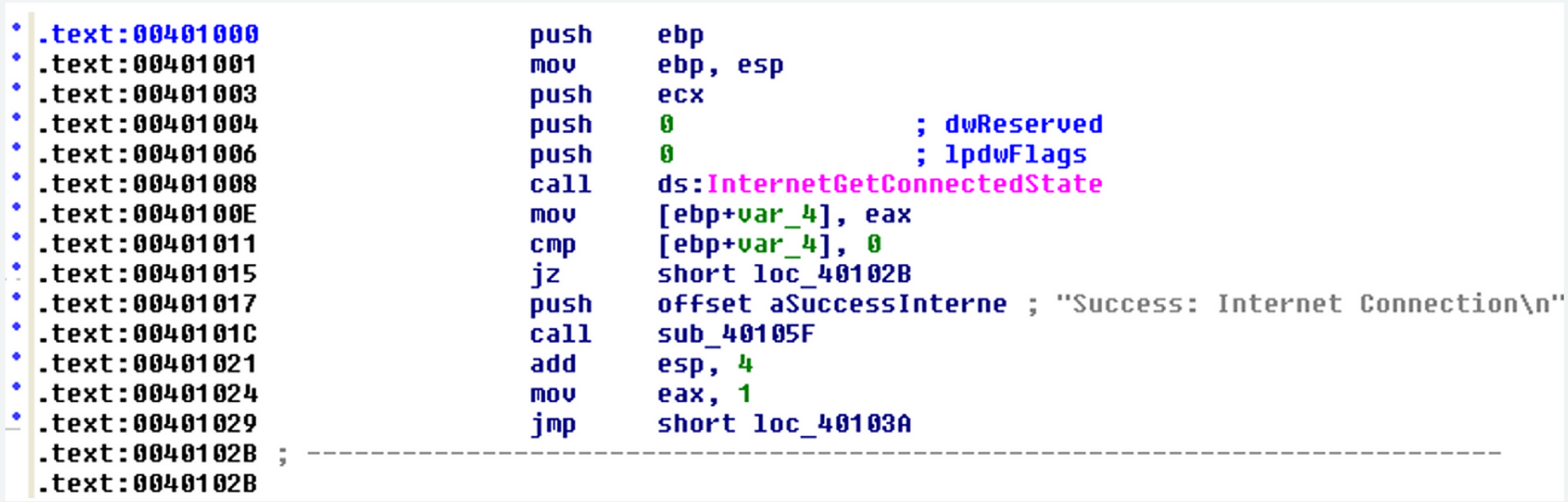
S10 - L4

NET. REBELS.

MICHELANGELO BORROMEO

TRACCIA

La figura seguente mostra un estratto del codice di un malware. Identificare i costrutti noti Esercizio Linguaggio Assembly vis ti 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
```

ASSEMBLY

```
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
```

CREAZIONE STACK

```
push    ebp
mov     ebp, esp
```

push EBP

Inserisce EBP nello stack

mov EBP,ESP

Copia il valore di ESP all'interno di EBP

CREAZIONE PARAMETRI E CHIAMATA FUNZIONE

```
push    0                   ; dwReserved
push    0                   ; lpdwFlags
call    ds:InternetGetConnectedState
```

push 0 ; dwReserved

Inserisce il valore 0 nello stack con commento ; **dwReserved**

push 0 ; lpdwFlags

Inserisce 0 nello stack con commento ; **lpdwFlags**

call ds: InternetGetConnectedState

Chiama la funzione con i parametri: **dwReserved - lpdwFlags**

CLICLO ' IF '

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

cmp [EBP+var_4], 0

Effettua una comparazione tra 0 e il valore di [EBP+var_4]

jz short loc_40102B.

Se il risultato del confronto è zero, salta all'etichetta loc_40102B

ASSEMBLY

```
push    offset aSuccessInterne ; "Success: Internet Connection\n"
call    sub_40117F
add     esp, 4
mov     eax, 1
jmp     short loc_40103A
```

CREAZIONE PARAMETRI E CHIAMATA FUNZIONE

```
push    offset aSuccessInterne
"Success: Internet Connection\n"
```

push offset aSuccesInterne

Inserisce l’offset all’interno della stringa

```
call    sub_40117F
```

call sub_40117F

Richiama la funzione sub_40117F

```
jmp     short loc_40103A
```

jmp short loc_40103A.

Se il risultato del confronto è zero, salta all'etichetta loc_40102A