



S10/L4

Maurizio Marcantoni

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.

Provate ad ipotizzare che funzionalità è implementata nel codice assembly.

```
.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
```

Svolgimento

Creazione dello stack

```
* .text:00401000      push    ebp
* .text:00401001      mov     ebp, esp
```

Chiamata di funzione . I parametri sono passati sullo stack tramite le istruzioni push

```
* .text:00401003      push    ecx
* .text:00401004      push    0                ; dwReserved
* .text:00401006      push    0                ; lpdwFlags
* .text:00401008      call   ds:InternetGetConnectedState
```

Ciclo if

```
* .text:0040100E      mov     [ebp+var_4], eax
* .text:00401011      cmp     [ebp+var_4], 0
```

La funzionalità implementata all'interno del malware è piuttosto semplice da identificare. Il malware chiama la funzione `internetgetconnectedstate` e ne controlla con un «if» il valore di ritorno. Se il valore di ritorno (return) della funzione è diverso da 0, allora vuol dire che c'è una connessione attiva.

Pseudocodice C:

```
state = internetgetconnectedstate (parl,0,0);
If (state !=0) printf ("Active connection");
Else return 0;
```