4. Malware analysis: Assembly pt. 2 e tecniche di ingegneria inversa

La figura seguente mostra un estratto del codice di un malware. Identificare i costrutti noti visti durante la lezione teorica.

```
.text:00401000
.text:00401001
.text:00401003
.text:00401004
                                                             ebp, esp
                                                             push
.text:00401006
.text:00401008
                                                 push
call
                                                             [ebp+var_4], eax
[ebp+var_4], 0
short loc_40102B
 .text:0040100E
                                                 mov
.text:00401011
.text:00401015
                                                 cmp
jz
                                                             offset aSuccessInterne; "Success: Internet Connection\n" sub_40105F
                                                 push
call
add
 .text:88481817
.text:0040101C
.text:00401021
                                                              esp, 4
eax. 1
 .text:00401024
.text:00401029
.text:0040102B
.text:0040102B
```

Creazione stack

```
.text:00401000
                                       push
text:00401001
                                        mnu
                                                 ebp, esp
.text:00401003
                                        push
                                                  ecx
                                       push
.text:00401004
                                                 B
                                                                        dwReserved
                                                 0 ; lpdwFlags
ds:InternetGetConnectedState
.text:00401006
                                       push
.text:00401008
.text:0040100E
                                       call
                                                 [ebp+var_4], eax
[ebp+var_4], 0
short loc_40102B
                                       mov
.text:00401011
                                        cmp
.text:00401015
                                                 offset aSuccessInterne ; "Success: Internet Connection\n"
sub_40105F
.text:00401017
                                       push
.text:0040101C
                                        call
.text:00401021
                                                  esp, 4
                                                 eax, 1
short loc_40103A
.text:00401024
                                       mov
                                        jmp
.text:0040102B
.text:0040102B
```

```
* .text:00401000
                                    push
                                                                     Tramite push i parametri sono passati allo stack
 .text:00401001
                                              ebp, esp
                                    MOV
 .text:00401003
 .text:00401004
                                    push
                                                                  dwReserved
 .text:00401006
                                                                ; lpdwFlags
                                    push
 .text:00401008
                                     call
                                             [ebp+var_4], eax
[ebp+var_4], 0
short loc_40102B
offset aSuccessInterne; "Success: Internet Connection\n"
 .text:0040100F
                                    mov
 .text:00401011
                                    cmp
 .text:00401015
                                    push
 .text:00401017
 .text:0040101C
                                    call
                                              sub_40105F
 .text:00401021
                                    add
                                              esp, 4
eax, 1
 .text:00401024
                                     mov
 .text:00401029
                                              short loc_40103A
 .text:0040102B
 .text:0040102B
```

```
.text:00401000
                                     push
 .text:00401001
                                      mov
                                               ebp, esp
  .text:00401003
                                     push
                                               ecx
                                                                  ; dwReserved
  .text:00401004
                                     push
 .text:00401006
                                                                  ; lpdwFlags
                                     push
 .text:00401008
                                               ds:InternetGetConnectedState
                                      call
                                               [ebp+var 4], eax
[ebp+var_4], 0
short loc_40102B
 .text:0040100E
.text:00401011
                                      mov
                                                                               Ciclo IF
                                     cmp
 .text:00401015
                                     push
                                               offset aSuccessInterne ; "Success: Internet Connection\n"
 .text:00401017
 .text:0040101C
                                               sub_40105F
                                     call
  .text:00401021
                                      add
                                               esp, 4
                                               eax, 1
short loc_40103A
 .text:00401024
                                      mnu
 .text:00401029
                                     jmp
  .text:0040102B
 .text:0040102B
```

Funzionamento

Il malware con la chiamata della funzione InternetGetConnectedState controlla il valore di ritorno con un if e se il valore di ritorno è diverso da 0, vuol dire che c'è la presenza di una connessione ad internet.