

CONSEGNA S10/L4

Malware Analysis

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
```

Creazione dello stack:

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

Chiama 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:00401011      cmp     [ebp+var_4], 0
.text:00401015      jz      short loc_40102B
```