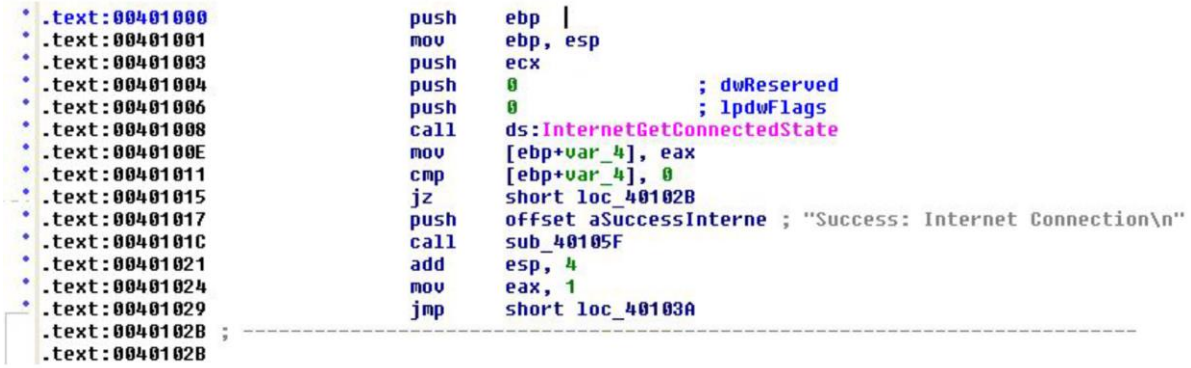
Traccia:

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 EBP
- Spostamento del valore ESP sullo stack EBP
- Crea il valore ECX sullo stack
- Crea il valore 0 sullo stack (secondo parametro)
- Crea il valore 0 sullo stack (primo parametro)
- Chiamata alla funzione InternetGetConnectedState
- Sposta il valore della variabile EAX alla variabile EBP+Var_4
- Confronta il valore di EBP + Var_4 con 0
- Se i due valori sono uguali, salta all'indirizzo loc_406102B
- Pusha la stringa "Success: Internet Connection" nello stack
- Chiamata alla funzione su indirizzo sub_40105F
- Aggiunge il valore 4 alla alla memoria ESP
- Sposta il valore 1 in EAX
- Salta alla locazione di codice loc_461083°
- Fine del codice