

S10/L4

Stefano Di Prospero
NetRaiders

```
* .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:00401000 push ebp
* .text:00401001 mov ebp, esp In queste due prime righe si crea lo STACK

* .text:00401003 push ecx
* .text:00401004 push 0 ; dwReserved
* .text:00401006 push 0 ; lpdwFlags
* .text:00401008 call ds:InternetGetConnectedState Qui i parametri sono passati sullo stack tramite l'istruzione PUSH

* .text:0040100E mov [ebp+var_4], eax Copia il contenuto di eax nella variabile

* .text:00401011 cmp [ebp+var_4], 0
* .text:00401015 jz short loc_40102B Qui inizia un ciclo IF.

.text:0040102B ; ----- L'istruzione jump fa saltare su una locazione che indica la fine dell'IF

* .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

Corpo dell'IF. Ci mostra che è avvenuta una connessione internet con successo

Dalla chiamata della funzione [InternetGetConnectedState](#) vediamo che viene effettuato un controllo per certificare che ci sia una connessione attiva

* .text:00401000	push	ebp	Si spinge ebp che indica la base dello stack
* .text:00401001	mov	ebp, esp	Si copia il valore di esp(che punta alla cima dello stack) in ebp
* .text:00401003	push	ecx	Qui si fa il push di del registro ecx
* .text:00401004	push	0	; dwReserved Si fa il push di 0 nello stack e da commento viene indicato come Riservato per utilizzi futuri
* .text:00401006	push	0	; lpdwFlags Si fa il push di 0 nello stack e da commento che ne indica la sua funzionalità
* .text:00401008	call	ds:InternetGetConnectedState	Chiamata funzione
* .text:0040100E	mov	[ebp+var_4], eax	Copia del valore di eax nella variabile
* .text:00401011	cmp	[ebp+var_4], 0	qui avviene una sottrazione che risulta essere un paragone di controllo
* .text:00401015	jz	short loc_40102B	qui si fa un jump verso un'altra locazione
* .text:00401017	push	offset aSuccessInterne ; "Success: Internet Connection\n"	qui si fa il push di un printf
* .text:0040101C	call	sub_40105F	Questa è una chiamata ad una funzione che da ricerca risulta stampare il risultato di un controllo di connettività
* .text:00401021	add	esp, 4	qui si somma 4 a esp, ovvero viene fatto fare uno spostamento al puntatore esp di 4 byte
* .text:00401024	mov	eax, 1	copia il valore in eax
* .text:00401029	jmp	short loc_40103A	salto verso altra locazione