Pratica S10/L4

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

Provate ad ipotizzare che funzionalità è implementata nel codice assembly.

Hint:
La funzione internetgetconnectedstate prende in input 3 parametri e permette di controllare se una macchina ha accesso ad Internet.

Consegna:

1. Identificare i costrutti noti (es. while, for, if, switch, ecc.)

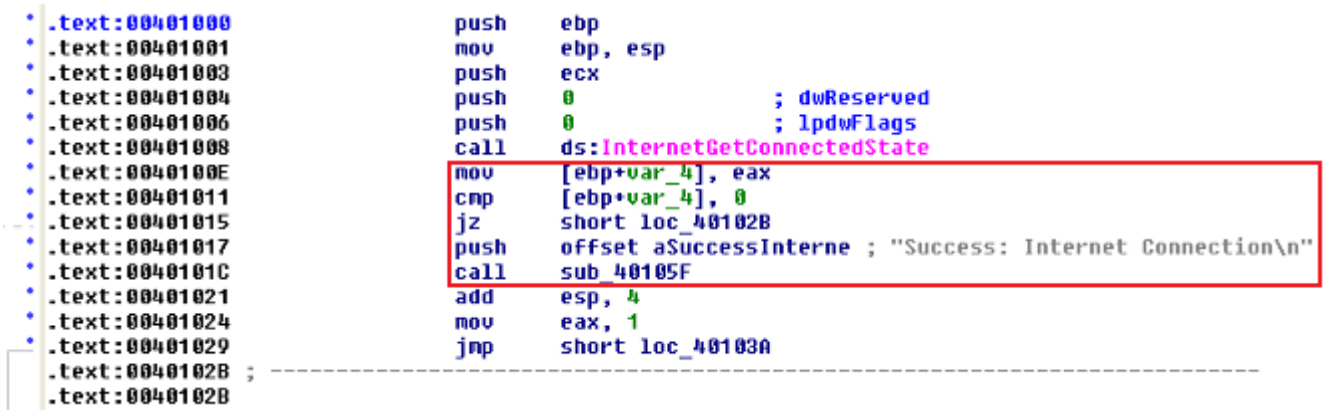
Creazione dello STACK

```
.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
```

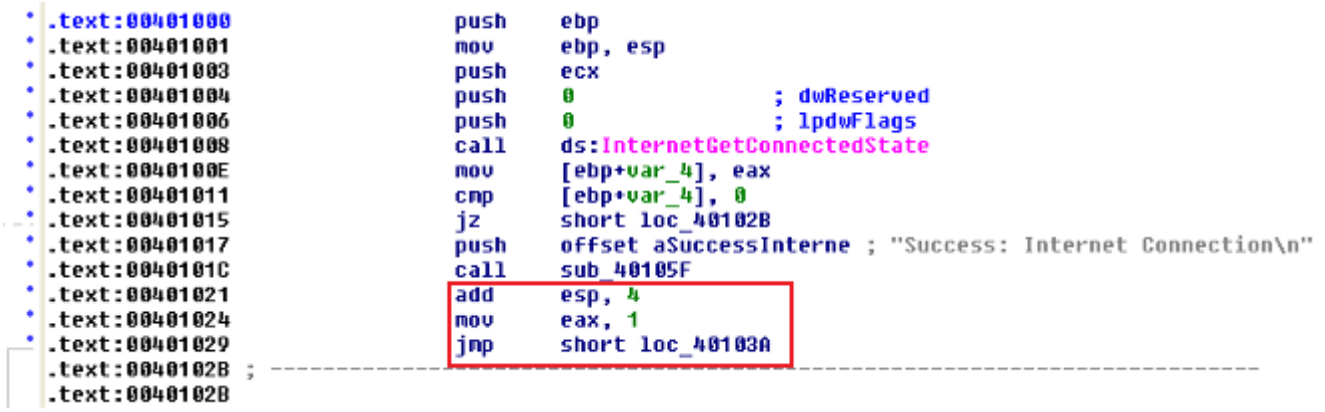
Parametri della funzione InternetFGetConnectedState

```
.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
```

Ciclo IF



ELSE



2. Ipotizzare la funzionalità –esecuzione ad alto livello

Int = a ;[ebp+var_4]
If a = 0
Printf(“Success: Internet Connection\n”);
break;
else
return 0;

3. BONUS: studiare e spiegare ogni singola riga di codice

00401000 push ebp	Crea un stack alla base
00401001 mov ebp, esp	Crea uno spazio in cima allo stack e lascia spazio alle altre funzioni
00401003 push ecx	Crea una variabile c
00401004 push 0 ;dwReserved	Crea una variabile 0 assegnando la parola Reserved
00401006 push 0 ;lpdwFlags	Crea una variabile 0 assegnando la parola Flags
00401008 call ds:InternetGetConnectedState	Chiama la funzione InternetGetConnectedState
0040100E mov [ebp+var_4], eax	Addiziona la variabile a alla variabile b
00401011 cmp [ebp+var_4], 0	Compara la variabile b con 0
00401015 jz short loc_40102B	Salto Condizionato dal paragone tra la variabile [ebp-var_4] e 0
00401017 push offset aSucceccInterne ; “Success: Internet Connection\n”	Visualizza che la connessione internet ha avuto successo
0040101C call sub_40105F	Stampa la stringa
00401021 add esp, 4	Addiziona 4 byte allo Stack Point
00401024 mov eax, 1	Aggiunge alla variabile eax il valore di 1
00401029 jmp short loc_40103A	Salta all’indirizzo di memoria 40103A
0040102B ; ----------	
0040102B	