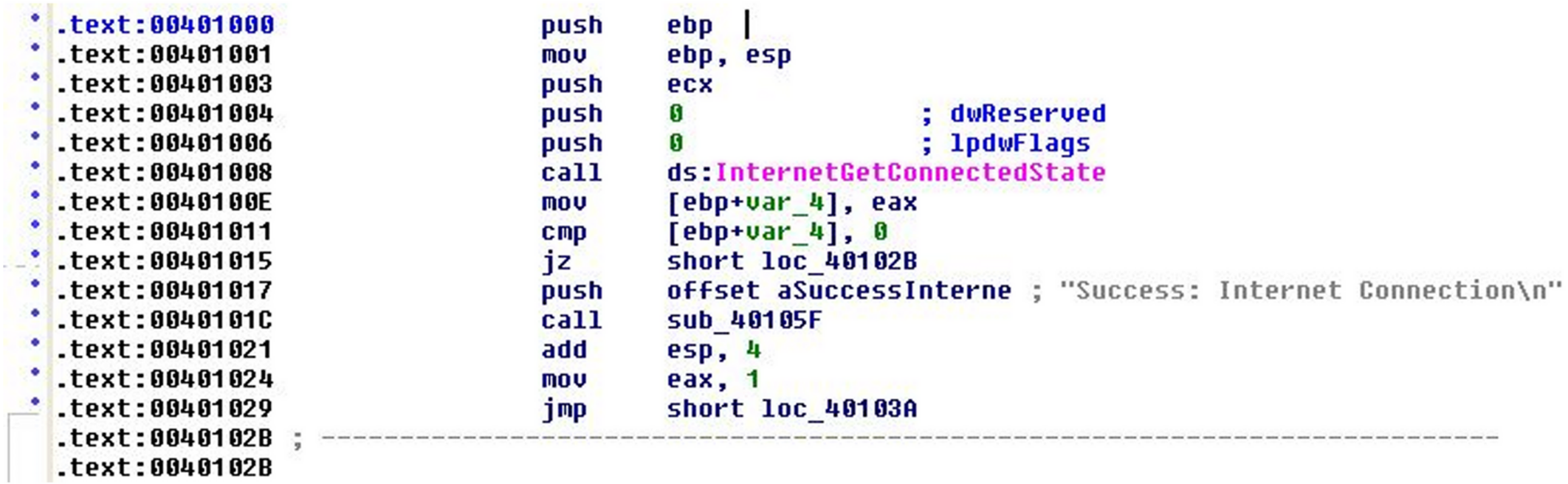
CONSEGNA
S10/L4

di Giuseppe Lupoi

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
```

Opzionale: 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.

Svolgimento

Svolgerò l’esercitazione riferendomi all’immagine della traccia precedente.
Ci viene chiesto di identificare i possibili costrutti presenti nel codice secondo le lezioni fatte fin’ora.

Leggendo attentamente il codice possiamo individuare un ciclo “if” grazie all’istruzione “jz” che rappresenta appunto una condizione in codice C.
L’istruzione “jz” permette di saltare da un risultato 0 o 1 in base al flag impostato nella riga prima da “cmp”, in questo caso ci confermerà o smentirà la connessione a internet della macchina interessata con un messaggio a schermo.

Possiamo quindi ipotizzare che questo codice controlli la connessione a internet di una macchina in quanto se la connessione è attiva va a “sub_40105F” e stampa il messaggio:
“Success: Internet Connection \n”
In caso contrario salta il passaggio e va direttamente a “loc_40103A”.