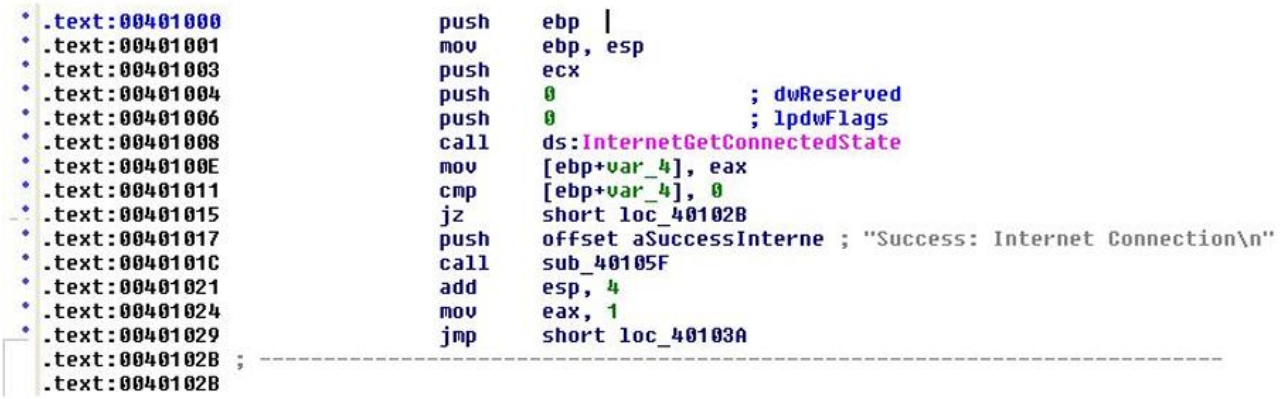
S10L4 – Analisi codice Assembly

Nell'esercizio di oggi esamineremo un frammento di codice **Assembly**, cercando di determinarne l'omologo codice C e la funzione. Il codice Assembly esaminato è illustrato nella seguente immagine.



- **.text:00401000 push ebp**
  .text:00401001 mov ebp, esp

  Segnala l'inizio di un nuovo stack.

- **.text:00401003 push ecx**

  Introduce una variabile ecx, a cui però non diamo un valore adesso.

- **.text:00401004 push 0 ; dwReserved**
  .text:00401006 push 0 ; lpdwFlags
  .text:00401008 call ds:InternetGetConnectedState

  Le prime due linee introducono variabili necessarie alla funzione richiamata alla terza linea. Questa funzione serve ad identificare la presenza o meno di una connessione internet: se l'output che verrà dopo salvato in eax è 0, la connessione è assente; se è 1 la connessione è presente.

- **.text:0040100E mov [ebp+var_4], eax**
  .text:00401011 cmp [ebp+var_4], 0
  .text:00401015 jz short loc_40102B

  Qui è presente un analogo di un ciclo if in C. Nella variabile eax viene incluso l'output della funzione precedente, questa viene poi paragonata con 0 settando quindi la ZF della variabile. Se le due corrispondono (la funzione restituiva 0, non era presente connessione) la ZF sarà indicata a 0 e il jz della linea successiva non effettuerà il salto; se la connessione era presente, la ZF sarà settata a 1 e quindi jz sarà risolta, effettuando il "salto" alla linea all'indirizzo di memoria indicato.

- **.text:00401017 push offset aSuccessInterne ; "Success: Internet Connection\n"**
  .text:0040101C call sub_40105

  Richiama nello stack una stringa, probabilmente come argomento per una funzione printf. Nella

seconda linea viene richiamata una subroutine, probabilmente una funzione di stampa per la stringa della linea precedente.

- **.text:00401021 add esp, 4**
  .text:00401024 inc eax, 1
  .text:00401029 jmp short loc_40103A

  La prima linea “sposta” l’indicatore dello stack. La seconda incrementa la variabile eax di uno per un motivo non chiaro, mentre l’ultima fa saltare ad una locazione specificata non però presente nel codice.

In conclusione, il codice preso in esame ha la funzione di controllare se la macchina ha accesso ad internet ed eventualmente di eseguire delle istruzioni predeterminate.