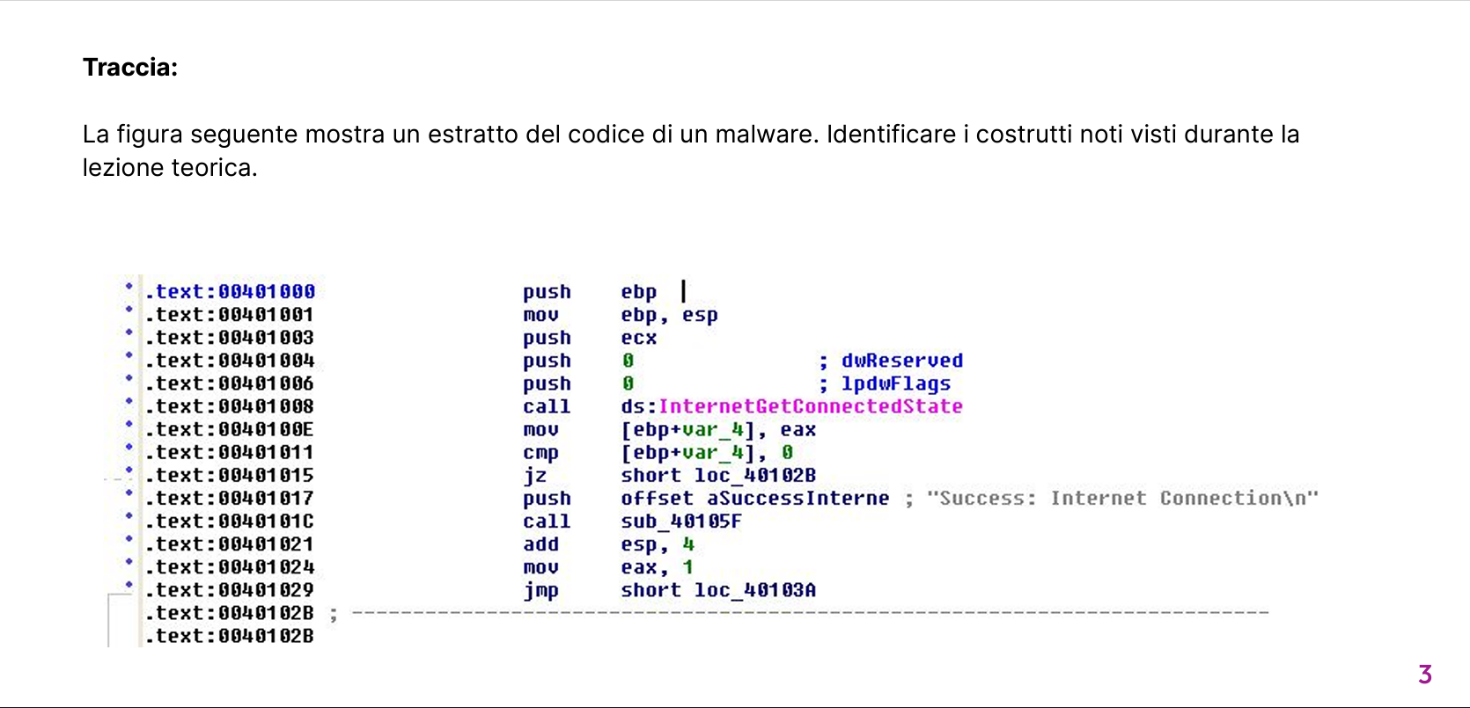
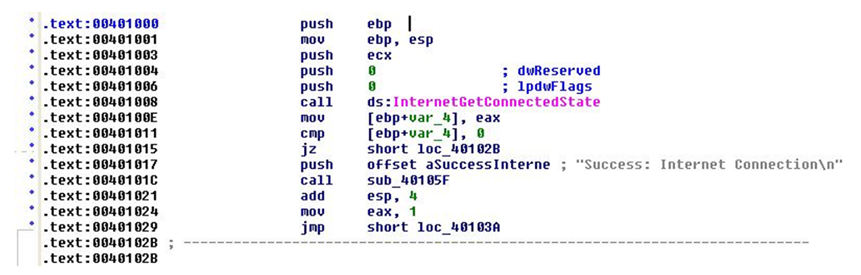
**Costrutti C - Assembly X86**

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

  
  
  
  
  
  
  
  
  
  
  
  
**Esercizio**  
  
  
  
  
  
  
  
  
  
1) Creazione dello Stack personalizzato  
Il registro "ESP" creare lo stack e viene definito. L'EBP per definire la fine.   
  
2) Passaggio parametri allo Stack  
Il registro ECX e i parametri dwReserved e lpdwFlags vengono passati nello Stack.  
  
3) Costrutto If Else  
  
Il costrutto If Else consente di eseguire un'azione se una condizione è soddisfatta e un'altra azione se la condizione non è soddisfatta.  
  
Se il valore della variabile [ebp+var\_4] è uguale a zero, il processore esegue l'istruzione jz short loc 40102B. Questa istruzione salta alla cella di memoria 40102B se il valore della variabile [ebp+var\_4] è uguale a zero.  
Se il valore della variabile [ebp+var\_4] è diverso da zero, il processore esegue le istruzioni successive alla cella di memoria 401015.   
  
Nel caso fosse diverso da zero, verrà salvata la stringa “Success: Internet Connection” nello Stack e stampata.

1.

2.

3.

