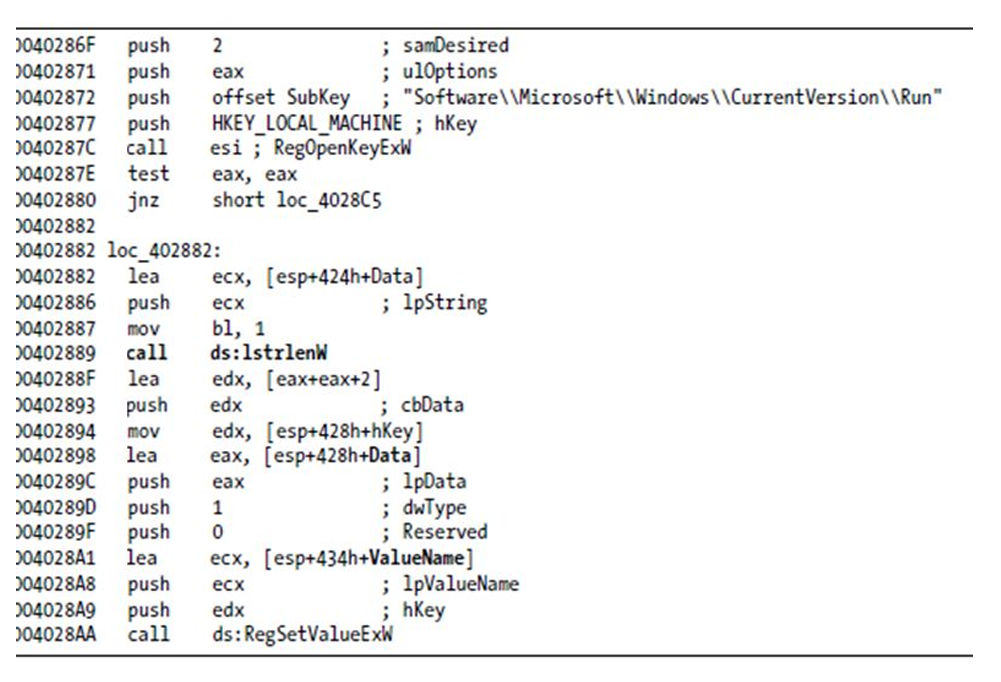
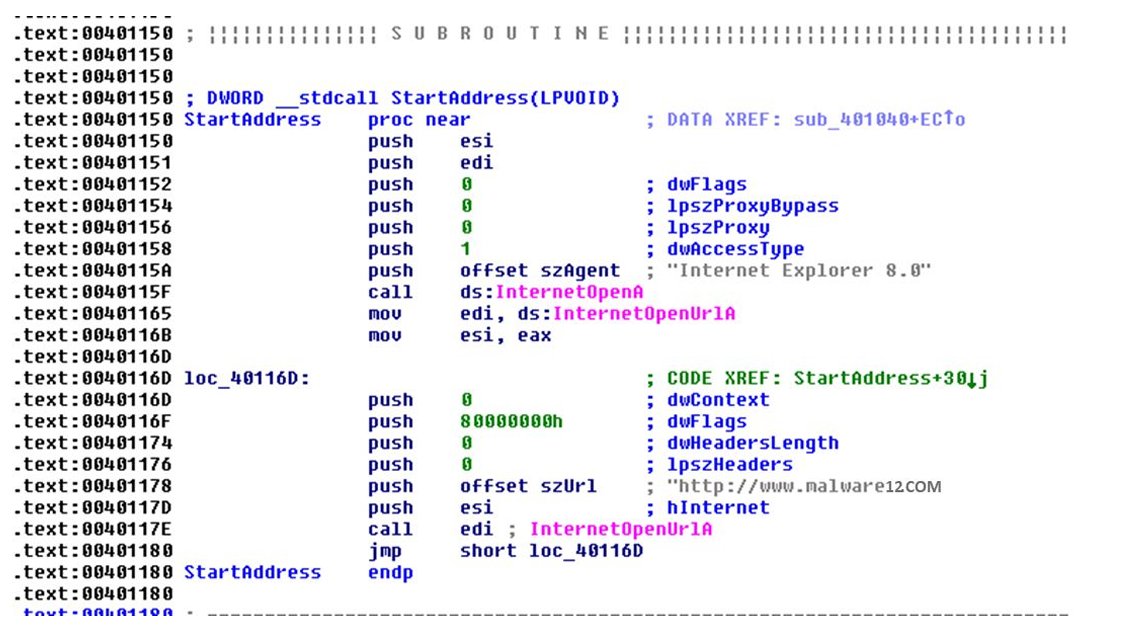
**INTRO E CONCETTI DI WINDOWS AVANZATI**

**TRACCIA**

Con riferimento agli estratti di un malware reale presenti nelle prossime slide, rispondere alle seguenti domande:   
1) Descrivere come il malware ottiene la persistenza, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite.  
2) Identificare il client software utilizzato dal malware per la connessione ad Internet.  
3) Identificare l’URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzione che permette al malware di connettersi ad un URL.  
4) Significato e funzionamento del comando assembly “LEA”.  
  
**ESERCIZIO**

  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
LEA (Load Effective Address): Questa istruzione calcola l'indirizzo di memoria dell'operando sorgente e carica tale indirizzo nell'operando destinazione.  
In pratica viene utilizzato per ottenere l'indirizzo di memoria di una variabile o di una posizione specifica e memorizzarlo in un registro.  
Ciò può essere utile per eseguire calcoli sugli indirizzi di memoria, ad esempio per l'indicizzazione di array o l'accesso a membri di una struttura.

**PERSISTENZA DEL MALWARE**

Il malware cerca di ottenere la persistenza nel sistema manipolando la chiave del registro di sistema.  
  
Il malware apre la chiave del registro di sistema "Software\Microsoft\Windows\CurrentVersion\Run" con privilegi appropriati (samDesired), cercando così di inserire sé stesso tra i programmi in esecuzione all'avvio del sistema.



**URL DI CONNESSIONE DEL MALWARE**

Il malware tenta di connettersi all'URL "http://www.malware12com/" utilizzando InternetOpenUrlA. Questo indica una possibile attività di download o comunicazione con un server remoto.

**CLIENT SOFTWARE PER LA CONNESSIONE A INTERNET**

Il malware utilizza la libreria wininet.dll per effettuare una connessione a Internet.

Successivamente apre una connessione a Internet utilizzando InternetOpenA e specifica "Internet Explorer 8.0" come browser.