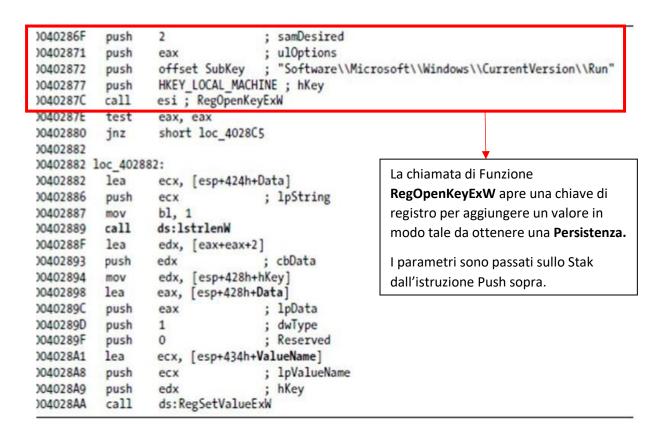
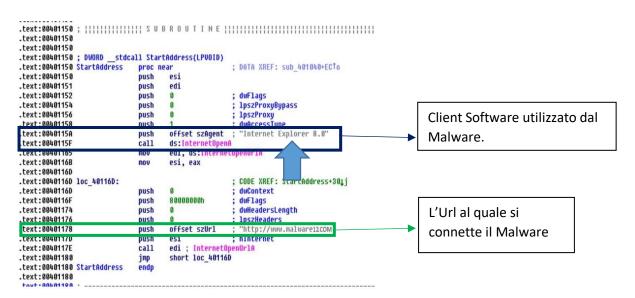
Obiettivo: Con riferimento all'estratto di codice di un Malware reale, dato nell'immagine seguente. Trovare come il Malware ottiene la persistenza, identificare il Client software utilizzato dal Malware, identificare l'URL al quale il Malware tenta di di connettersi e infie spiegare il funzionamento dell'istruzione Assembly "lea".





L'istruzione **lea** carica in un registro l'indirizzo effettivo di una certa variabile, consente di fare operazioni in linea che con **mov** non puoi fare. Lo scopo di lea è farti risparmiare istruzioni rispetto all'uso di mov quando lavori con gli offset, perché puoi fare operazioni in linea, anche molto complesse