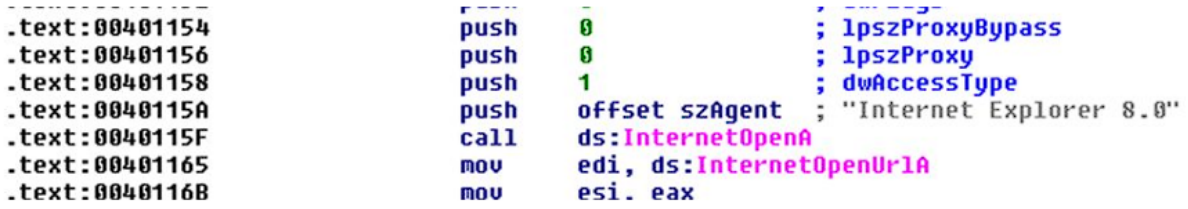
1. Soluzione – Persistenza Il malware ottiene la persistenza inserendo un nuovo valore all'interno della chiave di registro Software\\Microsoft\\Windows\\CurrentVersion\\Run, che include tutti i programmi che sono avviati all'avvio del sistema operativo. Le funzioni utilizzate sono: RegOpenKey, che permette di aprire la chiave selezionata. I parametri sono passati sullo stack tramite le istruzioni «push» che precedono la chiamata di funzione RegSetValueEx, che permette al malware di inserire un nuovo valore all'interno della chiave di registro appena aperta
2. Soluzione – Client utilizzato per la connessione ad Internet Il client utilizzato dal malware per connettersi ad internet è Internet Explorer, più precisamente la versione 8.



3. Soluzione – URL di destinazione Il malware cerca di connettersi all'URL www.malware12.com. La chiamata di funzione che consente al malware la connessione verso un URL è «Internet OpenURL». L'URL è passato come parametro di questa funzione sullo stack, tramite l'istruzione push.