WINDOWS MALWARE

1) **Persistenza Malware**

   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, tramite le funzioni utilizzate:
   RegOpenKey, che permette di aprire la chiave selezionata.
   RegSetValueEx, che permette al malware di inserire un nuovo valore all'interno della chiave di registro appena aperta.

2) **Client utilizzato per la connessione internet**
   Il client utilizzato per connettersi ad internet è **"Internet Explorer 8.0"**

3) **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 **«InternetOpenUrlA".**