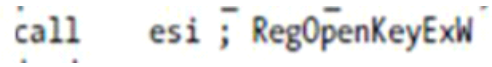
-PERSISTENZA

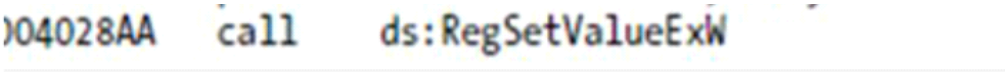
Il malware viene eseguito all' avvio del sistema operativo perchè aggiunge una voce alla chiave di registro:"Software\\Microsoft\\Windows\\CurrentVersion\\Run"

Per mezzo delle funzioni:

-RegOpenKey: è una funzione dell' API di Windows che permette di aprire la chiave che abbiamo selezionato. I valori dei parametri vengono inseriti nello stack con l' uso dell'istruzione push prima di effettuare la chiamata della funzione.



-RegSetValueEx: è una funzione utilizzata per impostare il valore di un' entrata di registro.Il malware può aggiungere un nuovo valore alla chiave che è stata aperta



-CLIENT SOFTWARE

Il client utilizzato è: "Internet Explorer 8.0"

-URL

Il malware utilizza la funzione "InternetOpenUrl" per connettersi all' url www.malware12.com. L' URL viene passato come parametro tramite push nello stack