Report

Windows Malware

Riferendoci al seguente malware andremo a:

- Descrivere come il malware ottiene la persistenza, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite;
- Identificare il client software utilizzato dal malware per la connessione ad Internet;
- Identificare l'URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzione che permette al malware di connettersi all'URL.

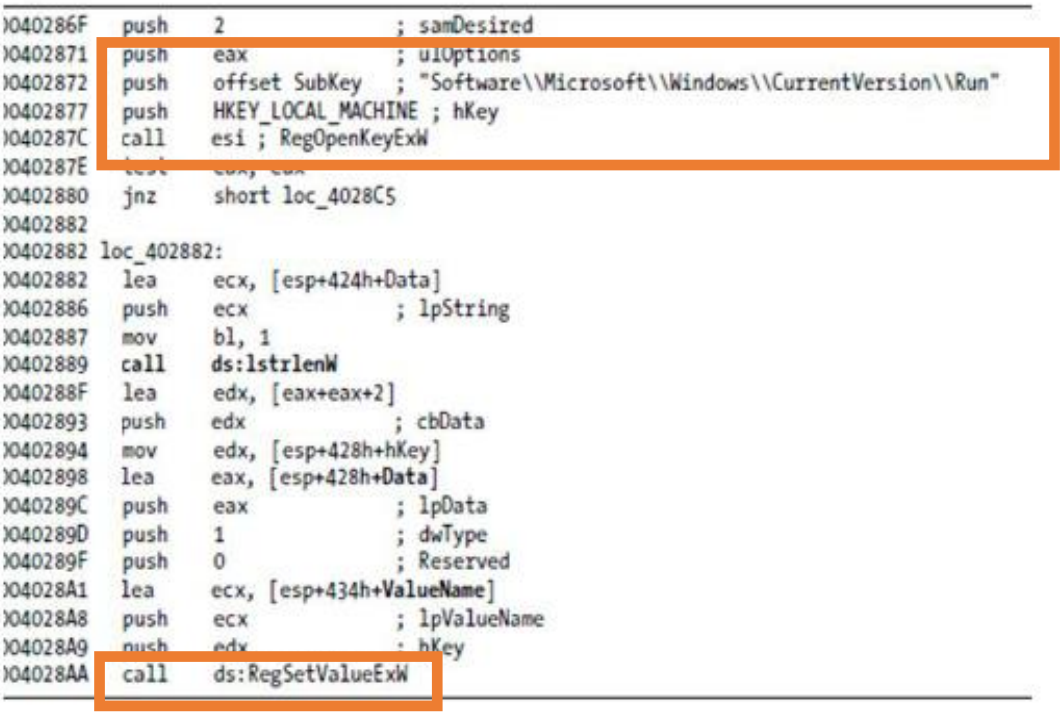
1. Persistenza del malware

Con il termine "persistenza" viene indicata l'esecuzione automatica del malware all'avvio del PC, senza dover effettuare la richiesta all'utente o all'amministratore di sistema. Attraverso questo meccanismo

Le funzioni evidenziate all'interno di questo malware sono:

- **RegOpenKeyEx:** questa funzione permette di aprire una chiave di registro al fine di modificarla. Essa accetta come parametri, tra gli altri, la chiave da aprire.
- **RegSetValueEx**: questa funzione permette invece di aggiungere un nuovo valore all'interno del registro e di settare i rispettivi dati. Accetta come parametri la chiave, la sottochiave e il dato da inserire.

Nel seguente caso, il malware accede al registro per poi poterlo modificare.



2. Client server e connessione all'URL

Nella seconda parte del codice, attraverso il primo blocco di codice evidenziato, riusciamo a rintracciare il browser utilizzato dal malware per connettersi, ovvero "Internet Explorer 8.0".

Nel secondo blocco di codice invece individuiamo la connessione al dominio http://www.malware12.com.