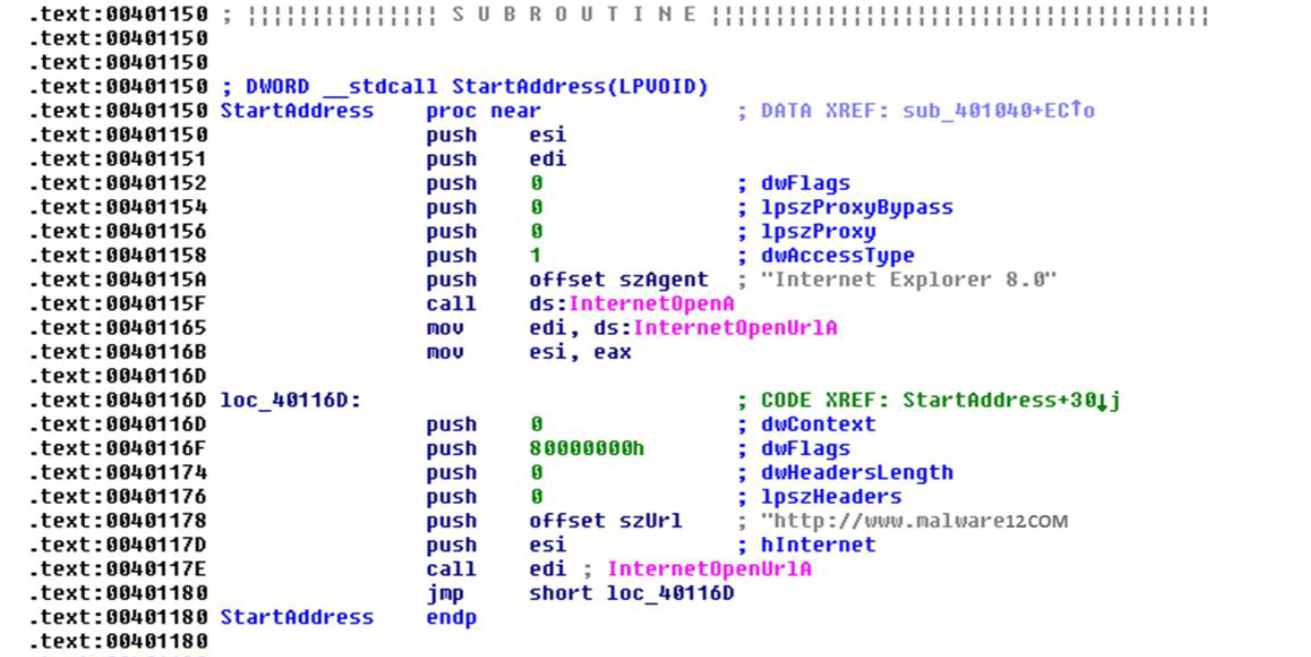
Analisi statica avanzata

L’esercizio di oggi ci chiedeva analizzare il codice del malware e trovare:

* Come il malware ottiene la persistenza.
* Il client software usato dal malware per connettersi ad internet.
* L’URL al quale il malware tenta di connettersi.

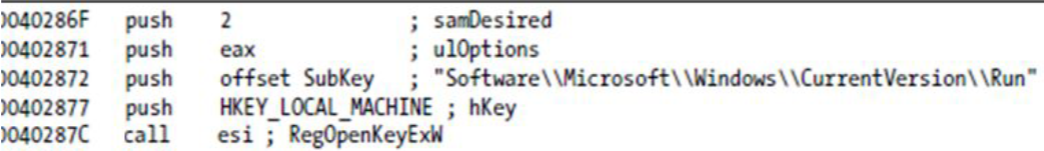
Codice malware



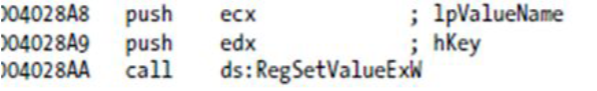


Persistenza del malware

Qui notiamo la funzione **RegOpenKeyEx** ed i suoi parametri passati tramite il comando push, con questa funzione il malware accede alla chiave di registro prima di modificarne il valore.



Anche per la funzione **RegSetValueEx** i parametri vengono passati sullo stack tramite il comando push. La funzione viene utilizzata per modificare il valore del registro, ed aggiungere una nuova entry per ottenere la persistenza all’avvio del sistema operativo.



Networking in Windows

Qui vediamo il tipo di browser usato dal malware e la sua funzione chiamante.



Identificazione URL malware

Questo è l’URL al quale il malware tenta di connettersi e la sua funzione chiamante.

