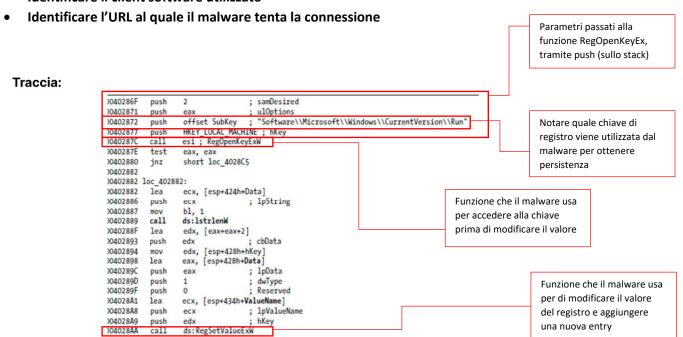
WINDOWS MALWARE

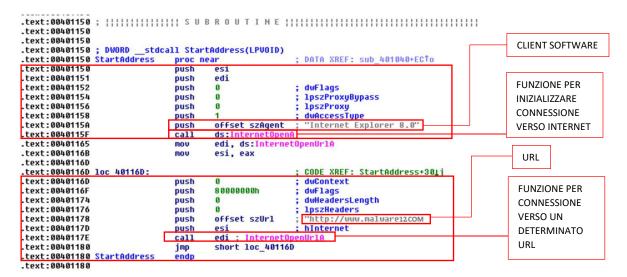
Con rifermento alle tracce presenti

- Descrivere come il malware ottiene persistenza
- Identificare il client software utilizzato



Spesso i Malware utilizzano le funzioni per modificare i valori delle chiavi di registro. Nel codice possiamo notare come apre una chiave di registro, per aggiungere un valore, in modo tale da ottenere persistenza. I Malware aggiungono se stessi alle entry dei programmi che devono essere eseguiti all'avvio del pc. In modo da essere automatici e permanenti senza azioni da parte dell'utente.

Traccia:



BONUS - ISRTRUZIONE "lea"

Questa istruzione copia l'effettivo valore esadecimale a 16 bit di una etichetta, passata come operando sorgente, nel registro di destinazione.

Il registro coinvolto per ricevere l'**offset*** del puntatore associato all'etichetta può essere uno qualunque dei registri a 16 bit.

Lea edx [eax+eax+2] - valore esadecimale [aex+eax+2] / registro di destinazione edx

"http://www.giobe2000.it/Tutorial/Schede/07-IstruzioniCpu/LEA.asp"

^{*}L'offset di un'istruzione può essere usato per spostare il codice di una quantità specifica di byte e, come operatore del compilatore, può indicare che si sta facendo riferimento all'indirizzo di un valore e non al valore stesso. Offset è la prima istruzione che leggerà in fase di compilazione