Intro e concetti di windows

andiamo ad analizzare un malware e ricerchiamo parte di codice all'interno.
Per prima cosa analizziamo dove il malware prende persistenza.

```
0040286F   push    2                   ; samDesired
00402871   push    eax                 ; ulOptions
00402872   push    offset SubKey       ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
00402877   push    HKEY_LOCAL_MACHINE ; hKey
0040287C   call    esi ; RegOpenKeyExW
```

Qui possiamo vedere il malware aprire la chiave del registro di sistema.

```
004028A1   lea     ecx, [esp+434h+ValueName]
004028A8   push    ecx                 ; lpValueName
004028A9   push    edx                 ; hKey
004028AA   call    ds:RegSetValueExW
```

E qui possiamo osservare il malware scrivere la chiave di registro, cosi da insidiarsi nel sistema.

```
.text:0040115A                  push    offset szAgent  ; "Internet Explorer 8.0"
```

Il browser internet utilizzato è internet explorer 8.0.

```
.text:00401178                  push    offset szUrl    ; "http://www.malware12COM
```

E qui possiamo individuare il sito su cui si collega: malware12.com.

Bonus

L'istruzione “lea” (load effective address) in assembly serve per caricare l'effettivo indirizzo di memoria, che può essere qualsiasi registro di uso generale.
Questo ci da la capacità di eseguire addizioni con due o tre operandi e la possibilitò di memorizzare il risultato in qualsiasi registro