

Re: OT (Sorta): DLL Registration under Restricted User Mode

Source:

<http://www.tech-archive.net/Archive/VB/microsoft.public.vb.general.discussion/2005-08/msg01133.html>

- *From:* "Bryan Dickerson" <txprphan@xxxxxxxxxxxxx>
 - *Date:* Thu, 11 Aug 2005 16:23:56 -0500
-

My point is to allow updates to in-house software while having users run in Restricted User mode—something I've got to try and accomplish per my network admin.

"Ralph" <nt_consulting64@xxxxxxxxx> wrote in message news:BN6dnaT-joYOK2bfRVn-vA@xxxxxxxxxxxxxxxxx

>

> "MikeD" <nobody@xxxxxxxxxxxx> wrote in message

> news:OKehrHrnFHA.1948@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

>>

>> "Bryan Dickerson" <txprphan@xxxxxxxxxxxxx> wrote in message

>> news:eQNsVuqnFHA.632@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

>>> This is sorta OT, but how can I get DLLs to Register in Restricted User

>>> mode?

>>

>>

>> To the best of my knowledge, you can't. A Restricted User does not have

>> write permissions for the parts of the Registry necessary for registering

>> ActiveX components (requires write permission for both HKEY_CLASSES_ROOT

> and

>> HKEY_LOCAL_MACHINE).

>>

>> With that said, from the Restricted User login, you could run

>> regsvr32.exe

>> (or any other program) in the context of a different login that has admin

>> rights. Here's a function to start a process under a different user

>> account:

>>

>> -----BEGIN CODE

>> Private Type PROCESS_INFORMATION

>> hProcess As Long

>> hThread As Long

>> dwProcessId As Long

>> dwThreadId As Long

>> End Type

>>

>> Private Type STARTUPINFO

Re: OT (Sorta): DLL Registration under Restricted User Mode

```
>> cb As Long
>> lpReserved As Long
>> lpDesktop As Long
>> lpTitle As Long
>> dwX As Long
>> dwY As Long
>> dwXSize As Long
>> dwYSize As Long
>> dwXCountChars As Long
>> dwYCountChars As Long
>> dwFillAttribute As Long
>> dwFlags As Long
>> wShowWindow As Integer
>> cbReserved2 As Integer
>> lpReserved2 As Byte
>> hStdInput As Long
>> hStdOutput As Long
>> hStdError As Long
>> End Type
>>
>> Private Declare Function CreateProcessWithLogonW Lib "Advapi32" (ByVal
>> lpUsername As Long, ByVal lpDomain As Long, ByVal lpPassword As Long,
>> ByVal
>> dwLogonFlags As Long, ByVal lpApplicationName As Long, ByVal
>> lpCommandLine
>> As Long, ByVal dwCreationFlags As Long, ByVal lpEnvironment As Long,
>> ByVal
>> lpCurrentDirectory As Long, lpStartupInfo As STARTUPINFO, lpProcessInfo
>> As
>> PROCESS_INFORMATION) As Long
>>
>> Private Declare Function CloseHandle Lib "kernel32" (ByVal hObject As
>> Long)
>> As Long
>>
>> Private Const INFINITE As Long = -1&
>> Private Const STATUS_WAIT_0 As Long = &H0
>> Private Const WAIT_OBJECT_0 As Long = STATUS_WAIT_0
>>
>> Private Const LOGON_WITH_PROFILE As Long = &H1&
>> Private Const LOGON_NETCREDENTIALS_ONLY As Long = &H2&
>> Private Const CREATE_DEFAULT_ERROR_MODE As Long = &H4000000
>> Private Const CREATE_NEW_CONSOLE As Long = &H10&
>> Private Const CREATE_NEW_PROCESS_GROUP As Long = &H200&
>> Private Const CREATE_SEPARATE_WOW_VDM As Long = &H800&
>> Private Const CREATE_SUSPENDED As Long = &H4&
>> Private Const CREATE_UNICODE_ENVIRONMENT As Long = &H400&
>> Private Const ABOVE_NORMAL_PRIORITY_CLASS As Long = &H8000&
>> Private Const BELOW_NORMAL_PRIORITY_CLASS As Long = &H4000&
>> Private Const HIGH_PRIORITY_CLASS As Long = &H80&
>> Private Const IDLE_PRIORITY_CLASS As Long = &H40&
```

Re: OT (Sorta): DLL Registration under Restricted User Mode

```
>> Private Const NORMAL_PRIORITY_CLASS As Long = &H20&
>> Private Const REALTIME_PRIORITY_CLASS As Long = &H100&
>>
>> Public Function RunAsUser(sLoginName As string, sPassword As String) As
>> Boolean
>>
>> Dim lpUsername As String
>> Dim lpDomain As String
>> Dim lpPassword As String
>> Dim lpApplicationName As String
>> Dim lpCommandLine As String
>> Dim lpCurrentDirectory As String
>> Dim StartInfo As STARTUPINFO
>> Dim ProcessInfo As PROCESS_INFORMATION
>>
>> lpUsername = sLoginName
>> lpDomain = "YourDomainName"
>> lpPassword = sPassword
>> lpApplicationName = <pathtofile>\program.exe"
>> lpCommandLine = vbNullString 'use the same as lpApplicationName
>> lpCurrentDirectory = vbNullString 'use standard directory
>>
>> If IsWin2K Then
>> StartInfo.cb = LenB(StartInfo) 'initialize structure
>> StartInfo.dwFlags = 0&
>>
>> CreateProcessWithLogonW StrPtr(lpUsername), StrPtr(lpDomain),
>> StrPtr(lpPassword), _
>> 0&, StrPtr(lpApplicationName), StrPtr(lpCommandLine), _
>> CREATE_DEFAULT_ERROR_MODE Or CREATE_NEW_CONSOLE Or
>> CREATE_NEW_PROCESS_GROUP, _
>> ByVal 0&, StrPtr(lpCurrentDirectory), StartInfo, ProcessInfo
>>
>> CloseHandle ProcessInfo.hThread 'close the handle to the main
> thread
>> since we don't use it
>> CloseHandle ProcessInfo.hProcess 'close the handle to the process
>> since we don't use it
>> 'note that closing the handles of the main thread and the process
> do
>> not terminate the process
>>
>> If ProcessInfo.hProcess > 0 Then
>> RunAsUser = True
>> End If
>> Else
>> If Shell(lpApplicationName) Then
>> RunAsUser = True
>> End If
>> End If
>> End Function
```

Re: OT (Sorta): DLL Registration under Restricted User Mode

>> -----END CODE
>>
>> Note that I made some on-the-fly changes from the actual function I use.
>> It's possible I missed something or screwed something up, but that's the
>> gist of it. If I missed any function, structure, or constant
> declarations,
>> let me know. You'll need to write your own IsWin2K function (mine
>> returns
>> True for Win2K and greater, so the above will work correctly with WinXP
> and
>> Windows Server 2003).
>>
>> --
>> Mike
>> Microsoft MVP Visual Basic
>>
>
> You also could just use "runas /user:<user> regsvr32 <dll>".
>
> As a sidenote, one of the first things one does after having gained access
> to a box is to go looking for executables that call
> CreateProcessWithLogonW() and I know kids that can rattle off its offset
> like their girlfriend's phone number. From there you back track - 90% of
> the
> time you find the password or location of the password hardcoded.
>
> If there is a reason to restrict a user then restrict them - don't say
> "now
> don't touch" then put the key under the flower pot. <g>
>
> -ralph
>
>

• *Follow-Ups:*

- ◆ **Re: OT (Sorta): DLL Registration under Restricted User Mode**
◇ From: Ralph

• *References:*

- ◆ **OT (Sorta): DLL Registration under Restricted User Mode**
◇ From: Bryan Dickerson
- ◆ **Re: OT (Sorta): DLL Registration under Restricted User Mode**
◇ From: MikeD
- ◆ **Re: OT (Sorta): DLL Registration under Restricted User Mode**
◇ From: Ralph

Re: OT (Sorta): DLL Registration under Restricted User Mode

- Prev by Date: [**Re: ANN: MZ-Tools 3.0 now provides setups**](#)
- Next by Date: [**Re: What kind of Program?**](#)
- Previous by thread: [**Re: OT \(Sorta\): DLL Registration under Restricted User Mode**](#)
- Next by thread: [**Re: OT \(Sorta\): DLL Registration under Restricted User Mode**](#)
- Index(es):
 - ◆ [**Date**](#)
 - ◆ [**Thread**](#)