

Forum:[Hack Forums](#)

Thread: [Replacing system DLL file](#)

Kisame? - July 10, 2017, 8:47 am

Hello,

To get my hidden RDP to work, I need to replace a file in the C:/Windows/Windows32 folder. It is about a DLL file about the system. Replacing that one with the one I found online should allow parallel sessions.

However, it seems that I cannot replace it. I have admin permission for my program but still it doesn't let me. Is there any way to do this?

Thanks in advance.

Ninja - July 10, 2017, 9:13 am

Maybe this is of help:

<http://www.tech-recipes.com/rx/7168/how-to-overwrite-system-files-in-windows-7/>

Kisame? - July 10, 2017, 10:40 am

Seems nice and gave it a shot. However, even after successfully taking ownership it does not work. :/

Ninja - July 10, 2017, 10:44 am

(Jul 10, 2017 10:40 AM)Kisame? Wrote: [\[CITE\]](#) Seems nice and gave it a shot. However, even after successfully taking ownership it does not work. :/

Is the command line you are starting in C# (the one from your program, not the one used to gain ownership) elevated with Administrator privileges? Maybe that matters.

Also, is the DLL in use when you try replacing it, by any chance?

Kisame? - July 10, 2017, 11:13 am

(Jul 10, 2017 10:44 AM)Ninja Wrote: [\[CITE\]](#) Is the command line you are starting in C# (the one from your program, not the one used to gain ownership) elevated with Administrator privileges? Maybe that matters.

Also, is the DLL in use when you try replacing it, by any chance?

Considering it's a system DLL, it being in use would be possible.

If you want to take ownership you need admin rights, and since I succeeded that part I have not forgotten admin. But I still cannot replace the file.

How to stop the file from being in use, seeing as it is a system DLL?

We're talking about Termsrv.dll here.

Pongik - July 10, 2017, 11:43 am

You have to take ownership of the folder (you can do the file individually but just do it for the whole folder) from the Trustedinstaller. You will need to get administrator rights for this though so make sure you can.

You have to first change the manifest file of your project to this:

```
Code <requestedExecutionLevel level="requireAdministrator" uiAccess="false" />
```

Then, proceed by typing the following code to gain ownership of System32:

```
Code string Command1 = "takeown /f C:\Windows\System32 /r /d y";  
string Command2 = "icacls C:\Windows\System32 /grant Administrators:F /t";  
System.Diagnostics.Process.Start("cmd.exe", Command1);  
System.Diagnostics.Process.Start("cmd.exe", Command2);
```

This code will give all administrator accounts full rights to delete files in System32, with the exception of one file that is required by the system to run. You can choose to make command prompt run hidden, this is just a small example. After this, you can edit, replace, delete the file you want there. This is if you want to do it through code, if not just take the commands in the code and write them in command prompt by yourself.