

Forum:[Hack Forums](#)

Thread: [How to have admin rights ?](#)

R3Cix - October 11, 2018, 12:08 pm

Hello everyone,

I don't know how to have admin rights without asking to users ?
I want to put my app in the startup folder (In oder to execute it when windows is load)

Thank you

PS: English is not my first language (I think you saw it)

vacsucczcrapyeah - October 11, 2018, 3:18 pm

(Oct 11, 2018 12:08 PM)R3Cix Wrote: [\[CITE\]](#) Hello everyone,

I don't know how to have admin rights without asking to users ?
I want to put my app in the startup folder (In oder to execute it when windows is load)

Thank you

PS: English is not my first language (I think you saw it)
on win7 there is an unpatched UAC exploit

vaiperboy - October 13, 2018, 7:27 am

(Oct 11, 2018 12:08 PM)R3Cix Wrote: [\[CITE\]](#) Hello everyone,

I don't know how to have admin rights without asking to users ?
I want to put my app in the startup folder (In oder to execute it when windows is load)

Thank you

PS: English is not my first language (I think you saw it)it's easier than said, you're basically asking for a exploit in windows systems which you won't find on the internet for free (if it even exists on win10), but since that "startup" folder only exists on win7 (as far as i know) there would sure be some exploits you can find, then.

NYANxCAT - October 13, 2018, 9:11 am

(Oct 11, 2018 12:08 PM)R3Cix Wrote: [\[CITE\]](#) Hello everyone,

I don't know how to have admin rights without asking to users ?
I want to put my app in the startup folder (In oder to execute it when windows is load)

Thank you

PS: English is not my first language (I think you saw it)
Or you can ask for UAC just once, and after PC restart your application will startup as admin ...
forever

SaefkoTeam - October 13, 2018, 9:51 am

there is two way you set in config file before compiling, or request it at run time

ASMR - October 13, 2018, 12:16 pm

[The UACME project on github](#) has plenty of ways to bypass UAC and is updated with new ways pretty frequently as they are found and published. Tho its in C and the precompiled files are heavily sigged by antiviruses so you cant just use the executable of it without problems, but rather you need to either need to pick the required stuff and compile some C yourself, or translate it to C# yourself.

There is also this [SharpSploit post-exploitation project](#) that features a UAC bypass and bunch of other handy tools. The mimikatz library and other stuff in it might be sigged too, so i recommend taking snippets from it into your project instead of adding the whole library.

And last but not least, is the good old way of just asking for the UAC. after that its easy to always make your executable run elevated in the future. Many users suffer from "dialog box fatigue" and are assumed to just click the "Yes, run this" almost automatically. And the few who actually even bother to read what the UAC notification is about can be easily fooled by just disguising your process temporarily as some updater or similar.

SIM-3124535 - October 15, 2018, 10:21 am

If by "startup folder" you mean shell:startup, then there's no admin rights required.

However if you want to use registry for startup, you can use

Code HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunIt doesn't require admin rights to write to it, so it should be more than enough.

There's also a subkey located in HKEY_LOCAL_MACHINE under the same path, which isn't any different, except you need admin rights to remove/write to it. However it will not make your file run as administrator.

If you want your file to be executed as administrator on startup, you should probably use the Windows Task Scheduler.