

## Re: Mysterious Rundll32.exe, Administrator privileges

**Source:**

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2004-12/1817.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-12/1817.html)

---

**From:** shafty (*shafty.1i01md\_at\_mail.mcse.ms*)

**Date:** 12/28/04

Date: Tue, 28 Dec 2004 10:57:23 -0600

This is a very tough job if not done right. Follow these instructions. These are available only for general education. This means proceed at your own risk. I am not responsible for any damage you may cause.

VX2 does the following to your system:

- 1) can create the file c:\windows\system32\guard.tmp
- 2) also creates random .dll files in c:\windows\system32  
–fortunately they are the same file size and will have today's date so they're easy to spot
- 3) upon shutdown, rebooting will generate new random .dll files  
–it uses only 1 random .dll file at a time, it will create an extra one that will become the new .dll file to be used by RunDll32.exe on the next boot. When you reboot, another .dll file is created for when you reboot again. See how sneaky it is.
- 4) Look in processes and you will see RunDll32.exe running  
–hit ctrl + alt + delete and click processes to look for it  
–You can end the RunDll32.exe process but it will come back, over and over
- 5) attaches itself to the winlogon process used by windows  
–therefore can run in safe mode as well, doh!
- 6) Pops up spyware windows occasionally from the RunDll32.exe process

Software you will need. Do a search online for these:

- 1) VX2Finder.exe
- 2) Hijackthis
- 3) Process Viewer (<http://downloads.subratam.org/pv.zip>)
- 4) Killbox.exe
- 5) Ad-Aware SE
- 6) Spybot
- 7) CWSredder

Here is the trick to removing this nasty spyware.

- 1) run the runme.bat file in the Process Viewer folder  
–should be located on the Tech Bench Tools cd in sftw fixes\spyware.

microsoft.public.windowsxp.security\_admin: Re: Mysterious Rundll32.exe, Administrator privileges

–use option 5, a log file should be created in notepad. Next use option

3. You should have two logfiles opened.

–look through these log files for any entries that do not have the words

"xp" out to the far right. exclude

COMRes.dll,OLEAUT32.dll,CLBCATQ.dl,

or any others that tell you exactly who the publisher is.

2) Now that you have the proper files pinpointed, run killbox.exe

–should be located on the Tech Bench Tools cd in sftw fixes\spyware.

Copy/paste the location of the file into the text input box. Select

the option to delete on reboot. Hit yes when prompted if ok to delete,

but hit no when asked to reboot. Repeat this for all other suspected files.

3) navigate to c:\windows and delete the file named wininit.ini if it exists.

–This is commonly used by spyware to rename itself upon windows restarting. Windows also u