

microsoft.public.security: Re: Downloaded program installed second "Explorer"

Re: Downloaded program installed second "Explorer"

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2002-05/0851.html>

From: David Dickinson [MVP] (eis@no-spam.softhome.net)

Date: 05/31/02

From: "David Dickinson [MVP]" <eis@no-spam.softhome.net>

Date: Thu, 30 May 2002 22:06:57 -0600

Wimpyjoe wrote:

> *Hi! One of my sons allowed a program to download and
> install a new "explorer" that loads when I start the
> computer – I now have 2 explorers running at once. The
> new one keeps accessing the Internet and showing Casino
> sites – a new window opens like every 15 seconds and
> overwhelms the computer. Can someone help? I can not
> find the offensive file on the machine.*

It would help if we knew what operating system you are using and had a more exact description of what is appearing on the screen (like actual window titles). Also, this question might be more appropriate in a newsgroup that has your operating system as a topic.

However, if you think you understand these steps you can try them, otherwise call a professional for help:

1. Unplug the cable that connects your computer to the internet and start your computer in Safe Mode.
2. If you are using Windows 95, 98, or ME, click Start, Run, and type "msconfig" into the Run dialog box. On the Startup tab, remove the checkmarks next to everything except your antivirus software, the system tray, and your modem driver if you have a winmodem that loads its driver at startup.
3. If you are using Windows 2000 or XP and don't know what the Registry Editor or the Services MMC snap-in is for, call a consultant. Otherwise, disable unneeded services, move everything in Start\Programs\Startup to a new folder at Start\Programs\Disable Startup Items. Then use regedit to export these registry keys to files on your hard drive:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

and for each user under HKEY_USERS except .DEFAULT,

Re: Downloaded program installed second "Explorer"

microsoft.public.security: Re: Downloaded program installed second "Explorer"

..\Software\Microsoft\Windows\CurrentVersion\Run

Then, in each of those keys, delete everything. The use Notepad to edit C:\WINNT\win.ini and put a semicolon in front of the LOAD= and RUN= lines.

5. Right-click Internet Explorer, select Properties, and click both the "Delete Files" and "Delete Cookies" buttons (if there is one). In the Home Page section, click the "Use Blank" button. Also click the "Clear History" button. Then under the Security tab, click on each of the zones and click the "Default Level" button.

6. Restart the computer normally. If the same symptoms appear, call a professional technician.

7. Buy some decent antivirus software such as Norton Antivirus or McAfee VirusScan (and there are others). Install it and connect to the internet to get the latest updates for it. Use it to run a full scan of your computer.

8. While you are connected to the internet, go to <http://www.lsfileserv.com/>. Read about Ad-aware (anti-spyware software) and download it along with Refupdate and Reghance. Disconnect from the internet. Install the software according to the instructions. Run Refupdate and configure its Preferences to store the referencfile in Ad-aware's program folder, usually "C:\Program Files\Lavasoft Ad-aware" (if you used the default installation options). Then run Refupdate to get the latest updates. Then run Ad-aware, configure it so that it knows where Reghance is (usually "C:\Program Files\Lavasoft RegHance"), and then tell it to scan everything.

9. Make copies of the registry key files you (might have) exported in step 4 and delete anything suspicions from the copies. Then right-click them to Merge them into the registry. Then use Notepad to edit win.ini again, remove the semi-colons from the ;RUN= and ;LOAD= lines, and restart the computer.

10. Restart your computer.

11. Use your up-to-date antivirus software and Ad-aware to perform an additional full scan of your computer for each.

12. If you are still having problems, get professional help.

Please note that these steps are not guaranteed to clean your computer and solve the problem, but they'll give you a fighting chance.

Finally, keep your antivirus and anti-spyware software up to date, get critical updates from Windows Update or from Microsoft TechNet Security regularly, and scan your computer regularly. And buy and use personal firewall software such as ZoneAlarm Pro (there are other good ones, but I think ZoneAlarm Pro is best for people who don't know what TCP/IP is all about). And remember: if you own the computer then it's not your kid's

Re: Downloaded program installed second "Explorer"

microsoft.public.security: Re: Downloaded program installed second "Explorer"

fault that this happened.

It's yours. Up-to-date top-of-the-line antivirus software probably would have prevented this problem.

--

David Dickinson, MVP (Security)
EveningStar Information Services
Las Cruces, NM USA
Summary of Microsoft Security Bulletins
<http://www.zianet.com/bwd/securitybulletins.asp>