

# Re: Malware in Windows XP

---

*Source:*

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2007-09/msg00203.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2007-09/msg00203.html)

---

- *From:* zhj23 <[zhj23@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:zhj23@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 26 Sep 2007 10:44:03 -0700
- 

Thanks for the info.

I have deleted the file. But still coming back on every reboot. Pls let me know how to remove it from "Windows StartUp"? Thanks.

It is really driving me crazy.

zhj23

"Malke" wrote:

zhj23 wrote:

Hello! Friends

I encounter this problem today. When I boot my PC, I keep on receiving this security warning from my anti-virus software: Malware Win32 Trojan\_gen exists in the following path:

C:\WINDOWS\system32\Drivers\mchInjDrv.sys

I tried to delete or "move to chest" (as recommended) it. But it keeps coming back when I reboot the PC. It is very irritating. How can I permanently remove it? Is it harmful?

A quick Google for "mchinjdrv.sys" tells me that:

"MchInjDrv.sys is a driver for injecting code to other processes. Publisher is legitimate: <http://madshi.net> But it is often used by malicious software. Kill the file mchInjDrv.sys and remove mchInjDrv.sys from Windows startup."

In addition to the doing the above, I suggest that you do:

Go through these general malware removal steps systematically –

Re: Malware in Windows XP

[http://www.elephantboycomputers.com/page2.html#Removing\\_Malware](http://www.elephantboycomputers.com/page2.html#Removing_Malware)

Include scanning with David Lipman's Multi\_AV and follow instructions to do all scans in Safe Mode.

<http://www.elephantboycomputers.com/page2.html#Multi-AV> – instructions  
[http://pcdid.com/Multi\\_AV.htm](http://pcdid.com/Multi_AV.htm) – download

You can also check to see if there are targeted removal steps for your malware here:

Bleeping Computer removal how-to's –

<http://www.bleepingcomputer.com/forums/forum55.html>

When all else fails, run HijackThis and post your log in one of the specialty forums listed at the first link above (not here, please).

Standard caveat: If the procedures look too complex – and there is no shame in admitting this isn't your cup of tea – take the machine to a professional computer repair shop (not your local version of BigComputerStore/GeekSquad). Please be aware that not all local shops are skilled at removing malware and even if they are, your computer may be so infested that Windows will need to be clean-installed. Have all your data backed up before you take the machine into a shop.

Malke

—

Elephant Boy Computers

[www.elephantboycomputers.com](http://www.elephantboycomputers.com)

"Don't Panic!"

MS-MVP Windows – Shell/User