

Re: virus problem

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-03/1624.html

From: Malke (noreply_at_invalid.com)

Date: 03/19/05

Date: Sat, 19 Mar 2005 12:27:00 -0800

craig wrote:

- > *Having problem with a virus than seems to run on startup and is*
- > *contained i think in system restore? Usually i am ok getting rid of*
- > *any viruses but this*
- > *one has got me stumped. I have removed the registry entry and all*
- > *folders*
- > *but every time i restart it comes back. Cmd line is C:\127021.exe. I*
- > *don't know much about DOS and when i type this ono the c prompt access*
- > *is denied.*
- > *Ad-Aware picks this up seems to fix it but always back after restart.*
- > *I run sophos anti-virus but IDE files have not been updated for some*
- > *time as no*
- > *longer in contact with person who installed. Every hour os so sophos*
- > *prompts me to this virus but cannot delete it.*
- >
- > *Can anyone advise how to remove this or direct me to instructions on*
- > *how to locate and delete.*
- >
- > *Any response will be appreciated...*

I'm not sure what you mean by saying your Sophos av files haven't been updated "as no longer in contact with person who installed". Having outdated virus definitions is almost worse than having no av installed at all. If you are unable to update Sophos, uninstall it and get a full-featured av immediately. If the virus is running on startup, it is **not** contained only in System Restore points. The virus files in the System Restore points aren't active; something else on your hard drive is.

Delete all Temporary and Temporary Internet Files. Then scan in Safe Mode with TrendMicro's Sysclean:

TrendMicro's Sysclean is an extensive antivirus tool which has the advantage of not needing to be installed. It requires two parts – the scanning engine and the virus pattern files.

1. Create a new folder on your Desktop or the C: drive named something useful like "Sysclean".
2. Go here and download the two parts of the program to that folder:

<http://www.trendmicro.com/download/dcs.asp> – Sysclean

<http://www.trendmicro.com/download/pattern.asp> – virus pattern files

The pattern files will be zipped – extract them with your unzipper (like WinZip) or if you have XP, you can just open the folder. You need to put the extracted files in the Sysclean folder you made.

3. Restart your computer in Safe Mode. Get into Safe Mode by repeatedly tapping the F8 key as the computer is starting up to get to the proper menu.
4. Go to the Sysclean folder you made and double-click on sysclean.com. Start the scan. After the scan is finished, look at the log. You may need to make a note of where any viruses were found if they were not able to be removed so you can manually delete them.

After you've scanned with Sysclean, get and install the full-featured av (uninstall Sophos first), update it, and do a thorough scan in Safe Mode. After you've done your virus scanning, remove non-viral malware with Ad-aware and Spybot Search & Destroy. Make sure you update those programs before you run them, and do your scans in Safe Mode.

After you know your computer is 100% clean, you can make a new System Restore point and then delete all the previous ones by using Disk Cleanup's More Options feature.

Malke

--

MS MVP - Windows Shell/User
www.elephantboycomputers.com
In Memoriam - MVP Alex Nichol
The world is diminished without him.