

Re: hklm/software – virus?

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.registry/2005-06/msg00046.html>

- *From:* Paraleptropy <Paraleptropy>
 - *Date:* Wed, 22 Jun 2005 11:57:53 -0400
-

On 17 Jun 2005 06:18:30 -0700, "ddotsyl" <ddotsyl@xxxxxxxxxx> wrote:

>I'd appreciate any help I can get in simple terms! Yesterday, I was
>minding my own business when I was hit by a virus of some sort.
>Nortons alerted me of it but couldn't fix it, or stop it in time. As
>quick as it appeared on my screen, pop-ups started appearing 20 per
>second it seems. I downloaded another anti-virus system and I think I
>cleared it. Unfortunately, everything in my startup folder is now in
>the location HKLM/Software/Microsoft/Windows/CurrentVersion/Run.
>
>My question is how can I restore everything to normal without risking
>my system not running at all. Please help!
>
>Thanks
>Sylvia

Virus's are a real pain in the ass. I'm pretty familiar with what belongs in my windows and windows\system32 directories.

One thing to do is boot using an ERD disk. Get a directory listing in those two directories and sort them by date. Just by looking, I can usually tell what belongs and what does not belong. If you can't tell, you can always do a search for the file(s) in question.

Sort by date; the latest date of course. Remove files that don't belong. Make sure you unhide too because some will hide files. Go into your registry and rename your run key to RUN.BAK or something of the sorts.

Do this in both USER and MACHINE. Of course for user, you'll have to know the correct SID.

Rename your 'STARTUP' folders for both 'all users' and current logged on user. This is typically in, C:\documents and settings\<username>\start menu\programs\startup.

I know I'm being somewhat vague about this, but I know my stuff and am able to do this when needed without worrying about killing stuff. If

Re: hklm/software – virus?

you're not so familiar, you should get someone with more knowledge to help you.

check your explorer shell in the registry. Sometimes you may think you're running Explorer but you may be running something else that looks like explorer. Also, when explorer is run at startup, it could always be run with another executable attached to it. Don't forget to check this.

Hope that helps.

--Paraleptropy--

<http://www.neflyfishing.net>

0 Limit,Catch –n– Release

-----== Posted via Newsfeeds.Com – Unlimited–Uncensored–Secure Usenet News=====

<http://www.newsfeeds.com> The #1 Newsgroup Service in the World! 120,000+ Newsgroups

-----= East and West–Coast Server Farms – Total Privacy via Encryption =-----

.

• **References:**

◆ **[hklm/software – virus?](#)**

◇ *From: ddotsyl*

• Prev by Date: **[file association](#)**

• Next by Date: **[Re: key & value was missing from registry](#)**

• Previous by thread: **[Re: hklm/software – virus?](#)**

• Next by thread: **[file association](#)**

• Index(es):

◆ **[Date](#)**

◆ **[Thread](#)**