

Re: HijackThis Log Help

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-12/msg00644.html>

- *From:* Richard K <RichardK@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 4 Dec 2007 18:33:01 -0800
-

Thanks for the help Michael. I need to get more well-versed in how to fight these things when they come up. I would appreciate it if I can get some help on this one since the user is in a crunch. Do you have an email address I can send the log?

-Richard

"Michael Jenkin [SBS-MVP]" wrote:

Hello Richard,

I spend alot of time reading hijackthis logs and removing malware. feel free to flick the log along.

It is possibly better suited to another newsgroup so if we get heavily into this, we can arrange offlist contact.

With these infections I normally use hijackthis to remove items from autorunning on boot, process explorer to kill them if they are in memory, I clear all temporary files in the users profile and also C:\windows\temp, I clear internet explorer cache and then look for very new weirdly named files in the C:\windows and C:\windows\system32 folder and rename them so they can't run (But this should only be done by someone who knows what they are doing). Quite often running "smitrem" will remove most of these infections.

I have a list of my favirote removal tools here

<http://www.mickyj.com/tools.htm>

Also some instructions here

<http://www.mickyj.com/helpme.htm>

you might also consider spybot.

<http://www.mickyj.com/spybotsetup.htm>

Re: HijackThis Log Help

Thanks

Richard K wrote:

OK, I'm running an SBS 2003 Prem setup with 10 xp pro clients. I have one client that was just added and they were WAY behind in updating service packs and security fixes but they were running the TM CSM 3.6 (server and clients).

The appears to be some type of spyware/malware/virus that is on this one xp client that I cannot get rid of even after updating the client with security packs and running TM scans. My next step is to create a HijackThis log file but I need help interpreting the results to know what to change. Where do I go?

As for this client issue.... there is a pop-up telling them they are infected with the netsky virus and to download this software, and flashing "X" appears in the system tray, new shortcuts are put on the desktop to the same software. I googled for anything and someone mentioned a voipwet.dll file that I just renamed, rebooted and the problem goes away but I suspect there is more there I want to clean up.

Thanks for any help.

-Richard K

—
Michael J. Jenkin MVP – SBS, MCP, Small Business Specialist, Senior
Systems Engineer
Visit <http://www.mickyj.com>