

Re: Windows SBS 2003 blue desktop!!

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-03/msg01332.html>

- *From:* Jose Alves <JoseAlves@xx>
 - *Date:* Mon, 10 Mar 2008 14:54:29 -0700
-

Hi Pedro.

Thanks, i will do that.

later i tell ahow it works.

"Pedro CR" wrote:

Hi

In case you actually want to get the system up and running (without formatting) here are a couple of hints:

- From your description I understand that EVERYTHING in the server is working. The only thing that does not work is the graphical interface after logging in.
- The graphical interface is provided by a process called "explorer.exe". Recent viruses usually attach themselves to explorer.exe as a loaded DLL/extension. This makes them a lot harder to remove. What happened to you is that the removal process probably deleted some file/DLL that was attaching itself to explorer.exe and now explorer.exe cannot start correctly.

This is relatively simple to solve assuming you know what you are doing:

- 1- On another computer Download Autoruns from SysInternals/Technet: <http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx>, extract and save it on a device (CDRom or USB drive)
- 2- Place the media on the server (usb drv/cd) and log on
- 3- Press Ctrl+Alt+Del and open Task Manager.
- 4- On Task manager choose File->Run and open the autoruns.exe file on the cd/usb drv.
- 5- Now that you are running Autoruns on the server, inside the autoruns window, open the "Explorer" tab. At this point I would recomend you choose File->Save and save a copy of the current configuration just in case.
- 6- Next look at the entries listed. Un-check all the entries that may look

Re: Windows SBS 2003 blue desktop!!

suspicious. Don't uncheck items from "Microsoft Corporation" or any other well known corporations/hardware vendors like "Symantec", "Adobe", "ATI", etc. at this point.

Simply UN-check the items that may look suspicious or that the "Image Path" is marked as Not found.

7- Document all the changes and reboot the server.

Check to see if you can now log on normally.

If things are WORSE than they were go back and undo your changes one by one.

If they are the same and you still can't log on normally, move on to more aggressive cleaning:

8- Restart at step 1 and do all steps up to step 5. On the "Explorer" tab check to see if there is any item that has reappeared, after you have unchecked it. This will mean that there is still one entry reactivating the virus. Disable all the suspect processes again.

If all is OK on the "Explorer" tab, move to step 9.

9- Look in the "Logon" and "Winlogon" tabs for suspect entries and uncheck them.

10- Look in the "Everything" tab and uncheck any other suspect entries.

Reboot and retry the logon.

If you still can't log on then the virus may still be present. Search the Internet for the entries that you unchecked (considered suspect). You will probably find additional information about those that may help you manually remove the virus.

In the future, ALWAYS use AntiVirus and AntiSpyware software from a reputed company like Symantec, Trend, etc.

Free AVs like AVG free SPYBOT resident are VERY INSUFFICIENT. Also install gateway filtering at the exchange server (ie Symantec Mail Security For Microsoft Exchange).

Pedro.

PS:

Also a good troubleshooting hint is checking to see if you can normally log on when booting in SAFE MODE:

If you can log on in safe mode then the solution is above.

If you can't log on in safe mode you may be missing important files. Open the command prompt and try running "sfc / scannow".

"Jose Alves" <JoseAlves@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> escreveu na mensagem

Re: Windows SBS 2003 blue desktop!!

news:35353AEC-A70F-4989-8C84-26C2A89438F8@xxxxxxxxxxxxxxxxxxxx

Hi.

I have a windows sbs 2003 that was infected with some different virus (trj/agent.hfm, downloader.rlv, w32.perlogva)

Before and after virus removal (scan "c:\\" of server over the network with updated panda clientshiled installed in a windows xp) i have one BIG problem, that it's after doing "ctl-alt-del" and logon as administrator the desktop does not show. It only show a screen with blue background. If i do "ctrl-alt-del" i can select the task manager or end session (the normal options).

The network it's ok and client machines communicate with server with no problems .

With task manager i have executed the "mmc" command and access to "active directory users and computers" snap-in. I've create a new user with administrator rights, but when i logon with this new user i have the same problem.

Please help.

Thanks in advance,
Jose Alves