

microsoft.public.windowsxp.general: WinXP SE: SvcHost (SYSTEM) process takes most of CPU

WinXP SE: SvcHost (SYSTEM) process takes most of CPU

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2005-02/1251.html>

From: Arvi Laanemets (*garbage_at_hot.ee*)

Date: 01/27/05

Date: Thu, 27 Jan 2005 09:31:43 +0200

Hi

Yesterday evening I was asked to control a computer (WinXP HE, SP1, ADSL modem, WinXP firewall), because it was too slow. I checked it with 3 different antivirus (AntiVir, Housecall PC-Cillin on-line, AVG) and removed 25-30 infected files, mostly trojans. I checked the computer with Ad-Aware SE and Spybot too ~70 objects were found and removed. All temporary folders were emptied. I checked with regedit all Run keys in HKLM & HKCU and removed all abundant (2 spyware records) from there. Comfile, exefile etc. keys in HKCR looked OK.

After that, when restarted, all was OK in task manager's TaskList - until ADSL connection started. Then one of svchost (SYSTEM) processes started to take more and more CPU. It was 4%-10% at start, then 10%-30%, etc. until 50%-95% after some time. A little after the CPU usage stabilized, there was a sudden change - CPU dropped to ~20%, and then rised again to ~90% - then dropped again, etc. The length of cycle was less than a minute.

At same time as svchost, was active taskmgr which used ~4% CPU.

I tried to investigate, what really was using this much CPU (from command window: tasklist /svc), but tasklist.exe was missing from computer at all. Then I checked with regedit, what was started from various svchost's (HKLM\Software\Microsoft\Windows NT\CurrentVersion\SvcHost) , and I deleted all entries which somehow had to do with remote access to computer and were not essential to OS working. Nothing was changed!

Maybe some fresh ideas available here!

Thanks in advance!

--

When sending mail, use address arvil<at>tarkon.ee
Arvi Laanemets