

Re: UPHClean log question

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2005-01/5197.html

From: Jon Erlandson (*jerlands_at_NOSPAM.sbcglobal.net*)

Date: 01/13/05

Date: Thu, 13 Jan 2005 11:35:47 -0600

A quick check to see which ports the computer is listening on is to run "netstat -an | more" from the command prompt. Suspect ports are 555, 666, 777, 6667 or anything greater than 32767. Also, search your computer for the svchost file and see that it doesn't reside outside %windir%\System32 folder (specifically not in %windir%\System32\Wins folder.) You might also carefully look over all running processes by running HijackThis <http://www.tomcoyote.org/hjt/>.

"WinGuy" <no_spam@nomail.bot> wrote in message
news:LWvFd.1444\$8Z1.1369@newssvr14.news.prodigy.com...

> I've started using UPHClean available for Windows 2000 and XP from

>

> <http://www.microsoft.com/downloads/details.aspx?familyid=1b286e6d-8912-4e18-b570-42470e2f3582&displaylan>

> after recently noticing greatly increased (fully and up to date updated
> retail XP-Pro) shutdown time and lots of Event Viewer complaints centering
> around the svchost.exe file (which also is generating security logs from
> Windows Firewall saying that the application svchost.exe has been blocked
> from listening on some varying ports). Does anyone know if this log
> extract from UPHClean might indicating a specific problem that should be
> addressed? I use AVG, AdawareSE, Spybot, SpywareBlaster, Microsoft
> AntiSpyware beta, and Sygate Personal Firewall. All scans for malware are
> coming up negative. No bangs of any kind are showing up in Event Viewer.
> Comments and thoughts appreciated! The following UPHClean log seems a
> little ominous to me.

> -----

> The following handles have been closed because they were preventing the
> profile from unloading successfully:

> svchost.exe (656)

> HKCU (0x374)

> 0x77e3b4b7 ADVAPI32!<no symbol>

> 0x77e072b1 ADVAPI32!IsTextUnicode+0x9cb4

> 0x77dd6b20 ADVAPI32!RegOpenKeyExW+0xa8

> 0x77dd773e ADVAPI32!RegOpenKeyW+0x2f

> 0x77ddb2dc ADVAPI32!SaferComputeTokenFromLevel+0x587

> 0x77ddb296 ADVAPI32!SaferComputeTokenFromLevel+0x541

> 0x77dd9e9e ADVAPI32!IdentifyCodeAuthzLevelW+0xd9

> 0x7c819653 kernel32!BasepCheckWinSaferRestrictions+0x17e

- > 0x7c818d2c kernel32!GetNlsSectionName+0x10cb
- > 0x77df7838 ADVAPI32!CreateProcessAsUserW+0xc3
- > 0x76ab3e6d rpcss!<no symbol>
- > 0x76aae117 rpcss!<no symbol>
- > 0x77e79dc9 RPCRT4!CheckVerificationTrailer+0x75
- > 0x77ef321a RPCRT4!NdrStubCall2+0x215
- > 0x77ef36ee RPCRT4!NdrServerCall2+0x19
- > 0x77e7988c RPCRT4!NdrGetTypeFlags+0x1c9
- > 0x77e797f1 RPCRT4!NdrGetTypeFlags+0x12e
- > 0x77e7971d RPCRT4!NdrGetTypeFlags+0x5a
- > 0x77e7bd0d RPCRT4!NdrConformantArrayFree+0x42e
- > 0x77e7bb6a RPCRT4!NdrConformantArrayFree+0x28b
- > 0x77e76784 RPCRT4!I_RpcBCacheFree+0x14c
- > 0x77e76c22 RPCRT4!I_RpcBCacheFree+0x5ea
- > 0x77e76a3b RPCRT4!I_RpcBCacheFree+0x403
- > 0x77e76c0a RPCRT4!I_RpcBCacheFree+0x5d2
- > 0x7c80b50b kernel32!GetModuleFileNameA+0x1b4
- >