

Re: svchost.exe

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-02/1819.html

From: Roger Abell [MVP] (mvpNOSPAM@asu.edu)

Date: 02/17/03

From: "Roger Abell [MVP]" <mvpNOSPAM@asu.edu>

Date: Mon, 17 Feb 2003 03:24:03 -0700

"Justin" <nitsuj@wwnet.net> wrote in message news:016a01c2d663\$343ec330\$a001280a@phx.gbl...

> *I have an instance of svchost.exe running that constantly*
> *causes page faults. This program is not in the System32*
> *directory, but in the winnt\system\drivers\etc directory.*
> *It is 224 KB and cannot be shutdown normally. Is this*
> *file just corrupted or should I even have it? If it is a*
> *normal file, is there anyway to get a clean copy without*
> *reinstalling? thanks for your time.*

svchost.exe normally lives in system32

The one you have alive and stored elsewhere is very possibly some form of malware – since the system will not be looking for it there to launch you are left to figure what is launching it and what it holds.

You can try listing out this info on Pro with
tasklist /svc

--

Roger Abell

MS MVP (Security, Windows), MCDBA, MCSE both
Associate Expert - Windows XP ExpertZone

<http://www.microsoft.com/windowsxp/expertzone>