

Re: Multiple SVC.HOST plus virus

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-04/0268.html>

From: *Vanguard* (no-email_at_post-reply-in-newsgroup.invalid)

Date: 04/04/04

Date: Sat, 3 Apr 2004 17:09:57 -0600

"JD Watkins" said in news:1355901c419ce\$501b72b0\$a001280a@phx.gbl:

- > *I am a real novice so I apologize if this is a dumb*
- > *question, but why would there be 5 listings of*
- > *SVCHOST.exe in my running processes? I have run a /SVC*
- > *to see what was attached to each. I just don't know what*
- > *is legitimate and what isn't. I have been receiving*
- > *notices that my machine is sending out virus infected*
- > *emails, but my virus definitions are uptodate and say "no*
- > *viruses". something is going on I just don't know what.*
- > *The Baseline security scan says I have critical patches*
- > *missing, but when I go to critical updates page to*
- > *download it says I have everything installed. HELP!!*
- > *I will attach the log in case there is anyone more*
- > *experienced than me who might help.*
- > *Thank you in advance:*
- >
- > *icrosoft Windows XP [Version 5.1.2600]*
- > *(C) Copyright 1985-2001 Microsoft Corp.*
- >
- > *C:\Documents and Settings\June>Tasklist /SVC*
- >
- > *Image Name PID Services*
- > =====
- > =====
- > *System Idle Process 0 N/A*
- > *System 4 N/A*
- > *SMSS.EXE 500 N/A*
- > *CSRSS.EXE 556 N/A*
- > *WINLOGON.EXE 580 N/A*
- > *SERVICES.EXE 624 Eventlog, PlugPlay*
- > *LSASS.EXE 636 PolicyAgent,*
- > *ProtectedStorage, SamSs*
- > *SVCHOST.EXE 828 RpcSs*
- > *SVCHOST.EXE 880 AudioSrv, Browser,*
- > *CryptSvc, Dhcp, dmserver,*
- > *ERSvc, EventSystem,*
- >

- > *FastUserSwitchingCompatibility, helpsvc,*
- > *lanmanserver,*
- > *lanmanworkstation, Netman,*
- > *Nla, RasMan, Schedule,*
- > *seclogon, SENS,*
- > *SharedAccess,*
- > *ShellHWDetection, TapiSrv,*
- > *TermService, Themes,*
- > *TrkWks, uploadmgr,*
- > *w32time, winmgmt,*
- > *WmdmPmSp, wuauserv, WZCSVC*
- > *SVCHOST.EXE 968 Dnscache*
- > *SVCHOST.EXE 988 LmHosts, RemoteRegistry,*
- > *SSDPSRV, WebClient*
- > *explorer.exe 1272 N/A*
- > *SPOOLSV.EXE 1344 Spooler*
- > *mcagent.exe 1452 N/A*
- > *mcvsshld.exe 1468 N/A*
- > *PPMemCheck.exe 1476 N/A*
- > *point32.exe 1492 N/A*
- > *PPControl.exe 1528 N/A*
- > *McVSEscn.exe 1604 N/A*
- > *MpfTray.exe 1608 N/A*
- > *hpztsb03.exe 1636 N/A*
- > *DSentry.exe 1684 N/A*
- > *DadApp.exe 1692 N/A*
- > *CookiePatrol.exe 1712 N/A*
- > *avgcc32.exe 1724 N/A*
- > *Directcd.exe 1740 N/A*
- > *Taumon.exe 1756 N/A*
- > *CTFMON.EXE 1772 N/A*
- > *dadtray.exe 1828 N/A*
- > *MpfAgent.exe 1988 N/A*
- > *ALG.EXE 208 ALG*
- > *avgserv.exe 156 AvgServ*
- > *CISVC.EXE 248 CiSvc*
- > *mcvsrte.exe 312 MCVSRte*
- > *mdm.exe 372 MDM*
- > *MpfService.exe 364 MpfService*
- > *nvsvc32.exe 676 NVSvc*
- > *SVCHOST.EXE 916 stisvc*
- > *OUTLOOK.EXE 1144 N/A*
- > *McShield.exe 2092 McShield*
- > *WINWORD.EXE 2624 N/A*
- > *IEXPLORE.EXE 4092 N/A*
- > *CIDAEMON.EXE 2496 N/A*
- > *CIDAEMON.EXE 1132 N/A*
- > *MSIEXEC.EXE 2840 MSIServer*
- > *CMD.EXE 1916 N/A*
- > *TASKLIST.EXE 2412 N/A*
- > *WMIPRVSE.EXE 1956 N/A*

microsoft.public.security: Re: Multiple SVC.HOST plus virus

>

> *C:\Documents and Settings\June*>

Check what NT services you have enabled for Automatic load on Windows startup. Svchost.exe is the process under which one, or more services will run.

A Description of Svchost.exe in Windows XP

<http://support.microsoft.com/?kbid=314056>

--

Post replies to newsgroup. Share with others. E-mail not accepted.
