

Re: Windows Task Manager

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.perform_maintain/2004-10/2333.html

From: Chuck (*none_at_example.net*)

Date: 10/19/04

Date: 19 Oct 2004 18:26:16 -0500

On Tue, 19 Oct 2004 15:19:02 -0700, "Darin" <Darin@discussions.microsoft.com> wrote:

>What minimum applications should be running in the task manager? I have
>msys.exe that runs all the time and takes up 70% of the cpu usage. Another
>file, cvhost.exe seems to us quite alot also. Any thoughts on what apps can
>be killed here and possibly permentantly unavailable?

Darin,

The best way to identify what tasks should be running would be for you to run HijackThis, and get expert advice (see below). But first do some preliminary cleanup!

The "msys.exe" may be RapidBlaster, a noxious parasite.
<<http://www.sysinfo.org/startuplist.php?filter=msys.exe>>

Is "cvhost.exe" actually "scvhost.exe"?
<<http://www.sysinfo.org/startuplist.php?filter=cvhost.exe>>

Start by downloading each of the following free tools:

AdAware <<http://www.lavasoftusa.com/>>

CWShredder <<http://www.majorgeeks.com/download4086.html>>

HijackThis <<http://www.majorgeeks.com/download.php?det=3155>>

LSP-Fix and WinsockXPFix <<http://www.cexx.org/lspfix.htm>>

RapidBlaster Killer

<<http://www.wilderssecurity.net/specialinfo/rapidblaster.html>>

Spybot S&D <<http://www.safer-networking.org/index.php?page=download>>

Stinger <<http://us.mcafee.com/virusInfo/default.asp?id=stinger>>

Create a separate folder for HijackThis, such as C:\HijackThis – copy the downloaded file there. AdAware, CWShredder, and Spybot S&D have install routines – run them. The other downloaded programs can be copied into, and run from, any convenient folder.

First, run Stinger. Have it remove any problems found.

Next, close all Internet Explorer and Outlook windows, and run CWShredder. Have it fix all problems found.

Run RapidBlaster Killer.

Next, run AdAware. First update it ("Check for updates now"), configure for full scan (<<http://forum.aumha.org/viewtopic.php?t=5877>>), then scan. When scanning finishes, remove all Critical Objects found.

Next, run Spybot S&D. First update it ("Search for updates"), then run a scan ("Check for problems"). Trust Spybot, and delete everything ("Fix Problems") that is displayed in Red.

Then, run HijackThis ("Scan"). Do NOT make any changes immediately. Save the HJT Log.

<<http://forums.spywareinfo.com/index.php?showtopic=227>>

<<http://www1.spywareinfo.com/articles/hijacked/prevent.php>>

Finally, have your HJT log interpreted by experts at one or more of the following security forums (and please post a link to your forum posts, here):

Aumha: <<http://forum.aumha.org/index.php>>

Net-Integration: <<http://forums.net-integration.net/>>

Spyware Info: <<http://forums.spywareinfo.com/>>

Spyware Warrior: <<http://spywarewarrior.com/index.php>>

Tom Coyote: <<http://forums.tomcoyote.org/>>

If removal of any spyware affects your ability to access the internet (some spyware builds itself into the network software, and its removal may damage your network), run LSP-Fix and / or WinsockXPFix.

Finally, improve your chances for the future.

Harden your browser. There are various websites which will check for vulnerabilities, here are three which I use.

<http://www.jasons-toolbox.com/BrowserSecurity/>

<http://bcheck.scanit.be/bcheck/>

https://testzone.secunia.com/browser_checker/

Block Internet Explorer ActiveX scripting from hostile websites (Restricted Zone).

<<https://netfiles.uiuc.edu/ehowes/www/main.htm>> (IE-SpyAd)

Block known dangerous scripts from installing.

<<http://www.javacoolsoftware.com/spywareblaster.html>>

Block known spyware from installing.

<<http://www.javacoolsoftware.com/spywareguard.html>>

Make sure that the spyware detection / protection products that you use are reliable:

http://www.spywarewarrior.com/rogue_anti-spyware.htm

microsoft.public.windowsxp.perform_maintain: Re: Windows Task Manager

Harden your operating system. Check at least monthly for security updates.

<http://windowsupdate.microsoft.com/>

Block possibly dangerous websites with a Hosts file. Three Hosts file sources I use:

http://www.accs-net.com/hosts/get_hosts.html

<http://www.mvps.org/winhelp2002/hosts.htm>

(The third is included, and updated, with Spybot (see above)).

Maintain your Hosts file (merge / eliminate duplicate entries) with:

eDexter <http://www.accs-net.com/hosts/get_hosts.html>

Hostess <<http://accs-net.com/hostess/>>

Secure your operating system, and applications. Don't use, or leave activated, any accounts with names or passwords with trivial (guessable) values. Don't use an account with administrative authority, except when you're intentionally doing administrative tasks.

Use common sense. Yours. Don't install software based upon advice from unknown sources. Don't install free software, without researching it carefully. Don't open email unless you know who it's from, and how and why it was sent.

Educate yourself. Know what the risks are. Stay informed. Read Usenet, and various web pages that discuss security problems. Check the logs from the security products that you use regularly, look for things that don't belong, and take action when necessary.

How did I get infected in the first place?

<http://forums.net-integration.net/index.php?showtopic=3051>

Essential tips for infection prevention

<http://forums.spywareinfo.com/index.php?showtopic=24339>

Cheers,

Chuck

Paranoia comes from experience – and is not necessarily a bad thing.