

Re: msconfig-startup

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-04/msg00822.html

- *From:* "David H. Lipman" <DLipman~nospam~@Verizon.Net>
 - *Date:* Sat, 29 Apr 2006 08:00:20 -0400
-

From: "Bodidleysquat" <Bodidleysquat@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

| I just ran a check of my msconfig-startup XP PRO to shut down unwanted
| programs and found several. I also found two programs with no letters for the
| name and command, just a series of squares and n with an accent mark above
| it. Under location they say SOFTWARE\Microsoft\WindowsNT\CurrentVersion...
| and I can't tell where this file is located. I don't think they're Microsoft
| programs. The first time I tried to shut them down, they came back after
| reboot as two more entries checked and running. I unchecked these and
| rebooted and the rogue program seems to have finally shut down. I'm posting
| this in the security forum, wondering if this is some kind of a spy program
| on my computer? Can anyone tell me the location and if I can delete this
| program?

If you are using any version of Sun Java that is prior to JRE Version 5.0,
then you are strongly urged to remove any/all versions that are prior to JRE
Version 5.0. There are vulnerabilities in them and they are actively being exploited.
It is possible that is how you got infected with malware.

Therefore, it is highly suggested that if there are any prior versions of Sun Java
to Version 5 on the PC that they be removed and Sun Java JRE Version 5.0 Update 6
be installed ASAP.

<http://www.java.com/en/download/manual.jsp>

For non-viral malware...

Please download, install and update the following software...

* Ad-aware SE v1.06

<http://www.lavasoft.de/>

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

<http://www.lavasoft.de/ms/index.htm>

* SpyBot Search and Destroy v1.4

Re: msconfig–startup

<http://security.kolla.de/>

<http://www.safer-networking.org/microsoft.en.html>

* SuperAntiSpyware

<http://www.superantispyware.com/superantispywarefreevspro.html>

After the software is updated, I suggest scanning the system in Safe Mode.

I also suggest downloading, installing and updating BHODemon for any Browser Helper Objects that may be on the PC.

* BHODemon

<http://www.majorgeeks.com/downloadget.php?id=3550&file=11&evp=245a87539eea8ed6904332b4b8b8442d>

For viral malware...

* Download MULTI_AV.EXE from the URL --

http://www.ik-cs.com/programs/virttools/Multi_AV.exe

To use this utility, perform the following...

Execute; Multi_AV.exe { Note: You must use the default folder C:\AV-CLS }

Choose; Unzip

Choose; Close

Execute; C:\AV-CLS\StartMenu.BAT

{ or Double-click on 'Start Menu' in C:\AV-CLS }

NOTE: You may have to disable your software FireWall or allow WGET.EXE to go through your FireWall to allow it to download the needed AV vendor related files.

C:\AV-CLS\StartMenu.BAT -- { or Double-click on 'Start Menu' in C:\AV-CLS }

This will bring up the initial menu of choices and should be executed in Normal Mode.

This way all the components can be downloaded from each AV vendor's web site.

The choices are; Sophos, Trend, McAfee, Kaspersky, Exit this menu and Reboot the PC.

You can choose to go to each menu item and just download the needed files or you can download the files and perform a scan in Normal Mode. Once you have downloaded the files needed for each scanner you want to use, you should reboot the PC into Safe Mode [F8 key during boot] and re-run the menu again and choose which scanner you want to run in Safe Mode. It is suggested to run the scanners in both Safe Mode and Normal Mode.

When the menu is displayed hitting 'H' or 'h' will bring up a more comprehensive PDF help file. <http://www.ik-cs.com/multi-av.htm>

Additional Instructions:

http://pcdid.com/Multi_AV.htm

* * * Please report back your results * * *

Re: msconfig–startup

Re: msconfig-startup

--

Dave

<http://www.claymania.com/removal-trojan-adware.html>

<http://www.ik-cs.com/got-a-virus.htm>

.