

WARNING Long Reply – Re: java virtual machine

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-06/27145.html>

From: Jim Byrd (jrbyrd_at_spamlessadelphia.net)

Date: 06/27/04

Date: Sun, 27 Jun 2004 00:22:38 -0700

Hi Karen – Sounds like you did it right. My guess at what may be going on here is that there's some Java application that's entered as a startup task packaged as an executable Jar file which has become corrupted. This could also be due to malware, however, or an artifact from the (incomplete)uninstall of the screensaver.

First, see if you can boot up in Safe mode without the error. HOW TO Restart in Safe Mode

<<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001052409420406>>

Read carefully the directions for XP.

If so, Uncheck /Safeboot and restart normally. You'll now need to find out which startup program is doing the damage, however I would recommend that you first eliminate the possibility of malware. Do the following and don't omit any steps.

If you go to this page at Jim Eshelman's site, here:

<http://aumha.org/a/noads.htm> and wait a little bit (be patient), an analysis of a number of possible parasites on your machine will be made to help you identify and remove them. NOTE: You will need to disable Ad Blocking in Zone Alarm 3.x, if present or any other Ad Blocking software which interferes with Java Scripting for this scan to work. You should get a message between the two lines of **** giving the results of the scan

Start with CWebShredder then AdAware and SpyBot below, in that order). Do the following:

Before you try to remove spyware using any of the programs below, download a copy of LSPFIX from any of the following sites:

<http://www.cexx.org/lspfix.htm>

<http://www.spychecker.com/program/winsockxpfix.html> (if your OS is Win2k or XP)

The process of removing certain malware may kill your internet connection. If this should occur, this program, LSPFIX, will enable you to regain your connection.

All of the following removal tools should be run from Safe mode when possible.

Download, UPDATE before running, and run:

<http://209.133.47.200/~merijn/files/CWShredder.exe> to remove the parasite.

Be sure to close all instances of IE and OE. You may also get it here if that link is blocked: <http://www.zerosrealm.com/downloads/CWShredder.zip>

BE SURE that you get v.158 or later!

You will need to show Hidden files first and then at the end clear the malware garbage from your System Restore backups after you've cleaned up. It's best to perform CWShredder (and most other malware fixers too) from Safe mode and then reboot. AFTER cleaning things up, then you can disable and then re-enable System Restore. See ***** below.

The following links give instructions on how to do these various functions:

HOW TO Restart in Safe Mode

<<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001052409420406>>

HOW TO Enable Hidden Files

<<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2002092715262339>>

HOW TO Disable/Flush System Restore (do this at the end AFTER cleaning or use the suggested procedure for XP at the *****'s)

<<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001111912274039>>

(WinXP)

<<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001012513122239>>

(WinME)

Then download and run:

http://www.kellys-korner-xp.com/regs_edits/iegentabs.reg to restore your tabs and remove any restrictions that the parasite has put in place.

Now download and run:

http://www.kellys-korner-xp.com/regs_edits/RestoreSearch2.REG to restore your search functions if they've been affected (as they probably will have been).

Be sure that you also download and install hotfix Q816093, here:

<http://support.microsoft.com/?kbid=816093>

which blocks the exploit upon which this parasite family depends.

.

Get Ad-Aware 6.0, Build 181 or later, here:

<http://www.javasoftusa.com/support/download/>. UPDATE and run this regularly to get rid of most "spyware/hijackware" on your machine. If it has to fix

things, be sure to re-boot and rerun AdAware again and repeat this cycle until you get a clean scan. The reason is that it may have to remove things which are currently "in use" before it can then clean up others.

Another excellent program for this purpose is SpyBot Search and Destroy available here: <http://security.kolla.de/> SpyBot Support Forum here: <http://www.net-integration.net/cgi-bin/forums/ikonboard.cgi>. I recommend using both normally. After UPDATING and fixing things with SpyBot S&D, be sure to re-boot and rerun SpyBot again and repeat this cycle until you get a clean "no red" scan. The reason is that SpyBot sometimes has to remove things which are currently "in use" before it can then clean up others.

Note that sometimes you need to make a judgement call about what these programs report as spyware. See here, for example: <http://www.imilly.com/alex.htm>

Both of these programs should normally be UPDATED and run after doing any other fix such as CWS shredder and, as a minimum, normally at least once a week.

ONLY IF you've successfully eliminated the malware, you can now make a new, clean Restore Point and delete any previously saved (possibly infected) ones. The following suggested approach is courtesy of Gary Woodruff: For XP you can run a Disk Cleanup cycle and then look in the More Options tab. The System Restore option removes all but the latest Restore Point. If there hasn't been one made since the system was cleaned you should manually create one before dumping the old possibly infected ones.

Once you get this cleaned up, you might want to consider installing the SpywareBlaster and SpywareGuard here to help prevent this kind of thing from happening in the future:

<http://www.javacoolsoftware.com/spywareblaster.html> (Prevents malware Active X installs) (BTW, SpyWare Blaster is not memory resident ... no CPU or memory load – but keep it UPDATED) The latest version as of this writing will prevent installation or prevent the malware from running if it is already installed, and it provides information and fixit-links for a variety of parasites.

<http://www.javacoolsoftware.com/spywareguard.html> (Monitors for attempts to install malware) Keep it UPDATED. Both Very Highly Recommended

Finally, go to Windows Update and ensure that ALL Critical updates are installed.

Now that you've probably eliminated malware as a cause, you need to try and isolate the "bad" program. Open the Configuration Utility again (Start|Run then enter msconfig) go to the Startup tab and click on Disable All. Now re-boot. If you're OK, then repeat this process except each time add a few

microsoft.public.windowsxp.general: WARNING Long Reply – Re: java virtual machine

programs back (don't do the Disable All again) until things fail, then isolate to the particular one of those you last added by now adding the in one-at-a-time. You get the idea.

Let us know what happens, please.

--

Please respond in the same thread.
Regards, Jim Byrd, MS-MVP

--

Please respond in the same thread.
Regards, Jim Byrd, MS-MVP

In news:21cc601c45b7e\$45ee7980\$a501280a@phx.gbl,
anonymous@discussions.microsoft.com <anonymous@discussions.microsoft.com>
typed:

> No this still did not work. Let me make sure I did it
> correctly--When I have Norton shutoff will the yellow
> shield have a red circle and line through it?? I had
> assumed that that means not activated so I proceeded with
> the steps you suggested. Still gettig the error message
> on start up

>> -----Original Message-----

>> Hi Karen - Try re-installing that Sereene screensaver and then
un-installing

>> it again. However, this time for both the install and the uninstall, be
>> sure that as many programs as possible are turned off, especially any
>> anti-virus and VERY ESPECIALLY any Norton/Symantec software such as NIS
or

>> NAV. Post back with your results, please. If that doesn't work, we can
>> look at something else.

>>

>> --

>> Please respond in the same thread.

>> Regards, Jim Byrd, MS-MVP

>>

>>

>>

>> In news:21e1b01c45b17\$bb04dcd0\$a001280a@phx.gbl,
>> anonymous@discussions.microsoft.com <anonymous@discussions.microsoft.com>
>> typed:

>>> I just downloaded from MS from one of your links and the
>>> installation was successful-rebooted and then still got
>>> the message box -COULD NOT FIND MAIN CLASS. PROGRAM WILL
>>> EXIT.

>>

>> <snip>

>>

>>>>> "Karen Page" <anonymous@discussions.microsoft.com> wrote in message

>>>>> news:20b2101c459ed\$756d6000\$a301280a@phx.gbl...

>>>>> After removing a screen saver program(Serene Screen) I
>>>>> now have a message that Java Virtual Machine is not able
>>>>> to function How can I go about fixing Thought I could
>>>>> reload an update

>>>>>

>>>>> kp

>>>>>

>>>>>

>>>>> .

>>>>

>>>> .

>>

microsoft.public.windowsxp.general: WARNING Long Reply – Re: java virtual machine

>> .