

RE: System Shutdown Message

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.applications/2004-06/0091.html>

From: BryanB (*anonymous_at_discussions.microsoft.com*)

Date: 06/07/04

Date: Mon, 7 Jun 2004 07:23:47 -0700

Yes the system is showing that it is clean. I have followed all microsoft recommendations and fixes for sasser and still having this issue. I have tried everyhting from the latest McAfee virusscan and stinger. Microsft's scanner and everything shows clean. Even checked the registry in the run section per McAfee instructions and that even comes up clean. Please help kids are running out of time for school.

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

>Hi,

>

>This is an indication on the sasser worm. Please follow the instructions in
>the following link.

>

>Windows 2000 Users: What to Do If Your Computer Has Been Infected by Sasser

>http://www.microsoft.com/security/incident/sasser_print2000.msp

>

>I am attaching the contents of the page for your reference at the end. Also

>please find the related Knowledge Base articles.

>

>1) What You Should Know About the Sasser Worm and Its Variants

><http://www.microsoft.com/security/incident/sasser.asp>

>

>2) A tool is available to remove the Sasser worm variants

><http://support.microsoft.com/default.aspx?scid=kb:en-us;841720>

>

>3) Security Update for Windows 2000 (KB835732)

>

><http://www.microsoft.com/downloads/details.aspx?FamilyId=0692C27E-F63A-414C->

>B3EB-D2342FBB6C00&displaylang=en

>

>Additional Information and Recommendations:

>Protect your PC in 3 Steps:

><http://www.microsoft.com/security/protect/>

>

>

>

>

>Windows 2000 Users: What to Do If Your Computer Has Been
Infected by Sasser

>Published: May 4, 2004

>

>Print this page now to get instructions for yourself (if
your computer

>keeps shutting down), or to help a friend.

>

>If you are using Microsoft® Windows 2000 Service Pack 2
(SP2), Windows 2000

>SP3, or Windows 2000 SP4 and your computer has been
infected by the Sasser

>worm, you can take these steps to update your software,
remove the worm,

>and help protect against future infections.

>

>Step 1: Disconnect from the Internet

>To avoid further problems, disconnect from the Internet:

>

>. Broadband connection users: Locate the cable that runs
from your external

>DSL or cable modem and unplug that cable either from the
modem or from the

>telephone jack.

>

>. Dial-up connection users: Locate the cable that runs
from the modem

>inside your computer to your telephone jack and unplug
that cable either

>from the telephone jack or from your computer.

>

>Top of page

>

>Step 2: Mitigate the Vulnerability

>You can temporarily remove the vulnerability that allows
the worm to infect

>your computer by creating a log file.

>

>Create the log file

>

- >1. *On the taskbar at the bottom of your screen, click Start, and then*
- >*click Run.*
- >
- >2. *Type: cmd and then click OK.*
- >
- >3. *At the command prompt, type: echo dcpromo*
- >>*%systemroot%\debug\dcpromo.log and then press ENTER.*
- >
- >
- >*Make the log file read-only*
- >
- >1. *At the command prompt, type: attrib +R %systemroot%\debug\dcpromo.log*
- >*and then press ENTER.*
- >
- >*Top of page*
- >
- >*Step 3: Improve System Performance*
- >
- >*If your computer is acting sluggish or if the Internet connection is slow,*
- >*the worm may be flooding your local network connection.*
- >*This may make it*
- >*impossible for you to download and install the required software update. To*
- >*improve system performance:*
- >
- >1. *Press CTRL+ALT+DELETE, and then click Task Manager.*
- >
- >2. *For each of the following tasks that may be listed, click the task to*
- >*select it, and then click the End Task button to end it.*
- >
- >. *Any task ending with _up.exe (for example, 12345_up.exe).*
- >
- >. *Any task starting with avserve (for example, avserve.exe).*
- >
- >. *Any task starting with avserve2 (for example, avserve2.exe).*
- >
- >. *Any task starting with skynetave (for example, skynetave.exe).*
- >
- >. *hkey.exe*
- >
- >. *msiwin84.exe*
- >
- >. *wmiprvsw.exe*

>Note Do not end the wmiprvse.exe task; it is a legitimate system task.

>

>Top of page

>

>Step 4: Enable a Firewall

>

>A firewall is a piece of software or hardware that creates a protective barrier between your computer and the Internet. Microsoft does not manufacture stand-alone software firewalls. The following resources provide more information about some firewall options.

>

>Hardware Firewalls

>

>Hardware firewalls are a good choice for versions of the Windows operating system prior to Windows XP. Some home-networking hardware, such as wireless access points and broadband routers, comes with built-in hardware firewalls. These help protect most home networks.

>

>Software Firewalls

>

>Microsoft strongly recommends that all users obtain and install a firewall before connecting to the Internet. However, we realize that some users may find downloading software to be their only option. If you choose to reconnect to the Internet to obtain a software firewall, here are some options:

>

>. BlackICE PC Protection-Save 25% (<http://blackice.iss.net/microsoft.php>)

>

>. Computer Associates-12-month free trial (<http://www.my-etrust.com/microsoft/>)

>

>. F-secure-6-months free trial (<http://www.f-secure.com/protectyourpc/>)

>

>. McAfee Security-save up to 35% (<http://us.mcafee.com/root/campaign.asp?cid=8437>)

>

>. Panda Software-90-day free trial (<http://www.pandasoftware.com/microsoft/>)

- >
- >. *Symantec/Norton–90–day free trial*
- >(http://www.symantecstore.com/dr/v2/ec_dynamic.main?sp=1&pn=46&sid=27674)
- >
- >. *Tiny Software: Tiny Personal Firewall*
- >(<http://www.tinysoftware.com>)
- >
- >. *ZoneAlarm–save \$20*
- >
- >(<http://download.zonelabs.com/bin/promotions/microsoftsecurity/>)
- >
- >*Top of page*
- >
- >*Step 5: Reconnect to the Internet*
- >
- >*Plug the cable (referred to in Step 1) back into your computer, telephone jack, or modem.*
- >
- >*Top of page*
- >
- >*Step 6: Install the Required Update*
- >
- >*To help protect your computer against this worm in the future, you must*
- >*download and install security update 835732, which was released with*
- >*Microsoft Security Bulletin MS04–011. To download security update 835732,*
- >*go to <http://go.microsoft.com/?LinkID=526386>*
- >
- >*Top of page*
- >
- >*Step 7: Check For and Remove Sasser*
- >
- >*After you have installed the update and restarted your computer, go to the*
- >*Web page "What You Should Know About the Sasser Worm and Its Variants" at*
- ><http://www.microsoft.com/security/incident/sasser.msp>.
- >*Use the Sasser Worm*
- >*Removal Tool to search your hard disk for and remove Sasser.A, Sasser.B,*
- >*Sasser.C, Sasser.D, Sasser.E, and Sasser.F.*
- >
- >*Top of page*
- >
- >*About Firewalls*
- >

microsoft.public.win2000.applications: RE: System Shutdown Message

>To learn more about software firewalls made by other
companies, hardware
>firewalls, and network routers, and for information about
selecting a
>firewall for your computer, see "Why You Should Use a
Computer Firewall" at
><http://www.microsoft.com/security/articles/firewall.asp>.
If you have a
>different configuration, a small network, or want to
learn more about
>firewalls, read "Frequently Asked Questions About
Internet Firewalls" at
><http://www.microsoft.com/security/protect/firewall.asp>.

>-----
>
>
>Hope the issue is resolved.

>
>Thank you,

>
>Rashmi

>
>This posting is provided "AS IS" with no warranties, and
confers no rights.

>| Content-Class: urn:content-classes:message
>| From: "BryanB" <anonymous@discussions.microsoft.com>
>| Sender: "BryanB" <anonymous@discussions.microsoft.com>
>| Subject: System Shutdown Message
>| Date: Sat, 5 Jun 2004 07:18:34 -0700
>| Lines: 10
>| Message-ID: <18b4301c44b07\$fca0afe0\$a001280a@phx.gbl>
>| MIME-Version: 1.0
>| Content-Type: text/plain;
>| charset="iso-8859-1"
>| Content-Transfer-Encoding: 7bit
>| X-Newsreader: Microsoft CDO for Windows 2000
>| X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4910.0300
>| Thread-Index: AcRLB/ygZXJhVxtyQ4+cduRcbnbArQ==
>| Newsgroups: microsoft.public.win2000.applications
>| Path: cpmsftngxa10.phx.gbl
>| Xref: cpmsftngxa10.phx.gbl
microsoft.public.win2000.applications:16766
>| NNTP-Posting-Host: tk2msftngxa08.phx.gbl 10.40.1.160
>| X-Tomcat-NG: microsoft.public.win2000.applications
>|
>| Win2000 pro srvp4 o/s. When on the internet via msn9
dial

RE: System Shutdown Message

>/ up I am getting a "system shutdown message in system
>/ process c:\winnt\system32\lsass.exe unexpected status
code
>/ 128" when the timer runs out the system reboots.
Sometimes
>/ I can be on the internet for 5 minutes to 15 minutes
>/ before this occurs. I have ran a complete mcafee
>/ virusscan with all the latest dats and scan engine and
no
>/ viruses are being detected. Any ideas what may be
causing
>/ this problem? In dire need of support kids have online
>/ classes to finish.
>/
>
>.
>