

Re: shutting down

Source:

<http://www.tech-archive.net/Archive/Scripting/microsoft.public.scripting.virus.discussion/2004-05/0119.html>

From: Bill Sanderson (*Bill_Sanderson_at_msn.com.plugh.org*)

Date: 05/06/04

Date: Thu, 6 May 2004 17:38:50 -0400

<anonymous@discussions.microsoft.com> wrote in message
news:957e01c4337a\$29610f70\$a301280a@phx.gbl...

>

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

>>I'm running Xp, i have the sasser anti virus tool, but

> how

>>do I stop the pc rebooting?

>>.

>>Hi I think I have the same problem did you find a

> solution??? Please help!!!

>

> Natasha x

Natasha—there is a saying here "famous last words" However, on the chance that, in fact, your problem is related to the one that began this thread, here's the definitive Microsoft article about how to fix this:

NEW WORM: SASSER

If the recovery procedures in this bulletin do not resolve your issue, please contact Microsoft at 1-866-PCSafety (1-866-727-2338).

Microsoft has learned about a worm identified as "W32.Sasser.worm" that is currently circulating on the Internet. The worm exploits the Local Security Authority Subsystem Service (LSASS) vulnerability which was fixed in Microsoft Security Update MS04-011 on April 13, 2004.

Microsoft encourages customers to protect themselves against this worm by immediately installing Microsoft Security Bulletin MS04-011 from the following Web site:

www.microsoft.com/technet/security/bulletin/ms04-011.msp

PRODUCTS AFFECTED

- . Windows XP Home
- . Windows XP Professional
- . Windows XP 64 Bit Edition
- . Windows 2000 Professional
- . Windows 2000 Server Edition

IMPACT OF ATTACK

Remote Execution of Code

TECHNICAL DETAILS

For additional details on this worm from antivirus software vendors participating in the Microsoft Virus Information Alliance (VIA), please visit the following Web sites:

. F-secure: <http://www.f-secure.com/v-descs/sasser.shtml>

. Global Hauri:

http://www.globalhauri.com/html/notice/notice_read.html?uid=447

. Network Associates: http://vil.nai.com/vil/content/v_125007.htm

. Norman: http://www.norman.com/Virus/Virus_descriptions/14919/en-us

. Panda: http://www.pandasoftware.com/virus_info/threats.aspx

. Sophos: <http://www.sophos.com/virusinfo/analyses/w32sasser.html>

. Symantec:

<http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>

. Trend Micro:

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SASSER.A

For more information about Microsoft's Virus Information Alliance, please visit the following Web site:

. <http://www.microsoft.com/technet/security/topics/virus/via.msp>

For more information about Microsoft's Virus Information Alliance please visit the following Web Site:

. <http://www.microsoft.com/technet/security/topics/virus/via.msp>

Please contact your Antivirus Vendor for additional details about this virus.

PREVENTION

1. Install the latest Microsoft Security Bulletin MS04-011 from the following Web site:

<http://www.microsoft.com/technet/security/bulletin/ms04-011.msp>

2. Users who have enabled the Windows XP Firewall are protected from the vector this worm attacks — the TCP Port 139. Most third party firewalls also block this attack vector by default.

RECOVERY

If your computer has been infected with this virus, please contact your preferred antivirus vendor or Microsoft Product Support Services for assistance with removing it.

Follow the below steps to try and resolve the issue:

If you are connected to a network within your company, refer to the Anti-Virus software vendor for support on the Sasser or AgoBot viruses.

If your machine is rebooting, sluggish or your Internet connection is slow

1. Terminate the following processes in Task Manager.

Access your Task Manager one of the following ways:

1. Right click the Taskbar and select Task Manager.

2. On the keyboard, press CTRL + ALT + DEL and then select Task Manager.
3. Click on processes tab.
4. Highlight process to terminate and press End Process.
 1. any process ending with _up.exe
 2. any process starting with avserv
 3. hkey.exe
 4. msiwin84.exe
 5. wmiprvsw.exe

****Note: There is a legitimate system process called 'wmiprvse.exe' that does NOT need to be terminated.

2. Remove your computer from the Internet by:
 - a) Unplug their internet cable(s). (Preferred method)
 - b) Disable their internet connection.

Note: This is a required step. If you do not disconnect your internet connection, it may result in crash.

Enable your Internet Connection Firewall (ICF).

If you are using Windows XP:

1. Click the Start button and then click Control Panel. Double-click "Networking and Internet Connections" and then click Network Connections.
2. Right-click the current Internet or Network connection and then click Properties.
3. On the Advanced tab, click select the option to "Protect my computer or network."

If you are using Windows 2000:

Enable Advanced TCP/IP filtering on all interfaces to block un-solicited incoming network packets.

1. Click the Start button, click Run and type: cmd.exe
2. Click Enter and then type the following command:

```
echo dcpromo >%systemroot%\debug\dcpromo.log
```

3. Then type the following command:

```
attrib +R %systemroot%\debug\dcpromo.log
```

Install Microsoft Security Patch MS04-011

1. Connect to the Internet and install the patch from Microsoft to remove the vulnerability. You must disable your antivirus software before installing the patch.
2. To install the patch, visit the following Web site:
<http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx>
3. Reboot the machine after the patch is installed.

Run the Sasser Removal Tool.

To access the tool, visit one of the following Web sites:

[.http://www.microsoft.com/security/incident/sasser.asp](http://www.microsoft.com/security/incident/sasser.asp)

.
<http://www.microsoft.com/downloads/details.aspx?amp;displaylang=en&familyid=76C6DE7E-1B6B-4FC3-90D4-9>
. Via KB article 841720 located at
<http://support.microsoft.com/default.aspx?scid=kb;EN-US;841720>.

Check your machine for infection from a variant of the Agobot worm.

The Agobot worm can infect your machine using the same method as the Sasser worm.

1. Contact your antivirus vendor or run the update on your antivirus signatures to ensure you have the latest version.
2. Run a full antivirus scan on your machine.

Note If you do not have an antivirus product installed, you can perform a free antivirus scan from HouseCall TrendMicro. For more information, visit the following Web site:

<http://housecall.trendmicro.com/>

3. Finally, go to Windows Update to ensure you have all other necessary Critical Updates installed on your machine. Microsoft recommends doing this on a regular basis to ensure your machine is kept up to date.

For more information about Windows Update, visit the following Web site:

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

If these steps do not resolve the issue please call 1-866-PCSAFETY or (866) 727-2338.

During a virus situation you may experience longer than normal hold times or a busy signal.

--

Regards,

Jerry Bryant - MCSE, MCDBA

Microsoft IT Communities

Get Secure! www.microsoft.com/security

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