

## Re: NT AUTHORITY SYSTEM

**Source:**

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2005-01/8427.html>

---

**From:** Bruce Chambers ([bruce\\_a\\_chambers\\_at\\_hotmail.com](mailto:bruce_a_chambers_at_hotmail.com))

**Date:** 01/11/05

Date: Mon, 10 Jan 2005 19:06:34 -0700

Pinto1uk wrote:

- > *Hi, my friends computer has got major porblems. The computer gets to the log*
- > *in screen, but after selecting a user, the computer gives my friend a message*
- > *that the computer has been shut down my NT AUTHORITY SYSTEM and will be*
- > *restarted (countdown in seconds). My friend also noticed the following peices*
- > *of information on the same page:*
- >
- > *NT AUTHORITY SYSTEM*
- > *1073741819*
- > *C:/WINDOWS/SYSTEM32/SERVICES.EXE*
- >
- > *No porgrams have been installed recently. Has the computer got a virus?*
- > *(running NORTON).*
- >
- > *What can i do to resolve this problem.*
- >
- > *regards and thanks in advance.*

Your friend has apparently contracted the latest worm, W32.Sasser.Worm, specifically designed to attack people who do not update their computers promptly and who do not practice "safe hex." In other words, like Blaster, this worm was developed and distributed after a patch for the vulnerability was announced and made publicly available. Further, and also like Blaster, this worm could not affect any computer whose user had taken the basic precaution of using a properly configured firewall.

To stay on-line long enough to get the necessary updates, patches, and removal tools, click Start > Run, and enter "shutdown -a" when the next Shutdown countdown begins. This will abort the shut down. Also, make sure you've enabled a firewall before starting, to preclude any more intrusions while getting the updates/patches/tools.

What You should Know about the Sasser Worm and its Variants

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

microsoft.public.windowsxp.general: Re: NT AUTHORITY SYSTEM

Microsoft Security Bulletin MS04-011

<http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>

W32.Sasser.Worm

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

A tool is available to remove the Sasser worm variants

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

W32.Sasser.Worm Removal Tool

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

McAfee AVert Stinger Virus Removal Tool

<http://vil.nai.com/vil/stinger/>

--

Bruce Chambers

Help us help you:

<http://dts-l.org/goodpost.htm>

<http://www.catb.org/~esr/fags/smart-questions.html>

You can have peace. Or you can have freedom. Don't ever count on having both at once. - RAH