

microsoft.public.security.virus: RE: how to fix the problem when screen is blank! (sassser worm??)

RE: how to fix the problem when screen is blank! (sassser worm??)

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-05/1788.html>

From: Venkat Srinivasan.R (venkatsr_at_online.microsoft.com)

Date: 05/12/04

Date: Wed, 12 May 2004 16:59:30 GMT

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

Try to get into SAFE mode .

1. Shutdown ur machine
2. Power it ON
3. To go into safe mode keep tapping the F8 function key on the top row of ur key board
4. Select the plain "SAFE MODE" option
5. Then try removing the sassser virus steps

SASSER REMOVAL STEPS :

Here is some hints on Sasser virus.

Just sent an email to Virus Auto Help [virushlp@microsoft.com] . So when ever u send a mail to this email address a self explained mail like the one below will be sent to u.

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

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

RE: how to fix the problem when screen is blank! (sassser worm??)

microsoft.public.security.virus: RE: how to fix the problem when screen is blank! (sassser worm??)

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.

a) Unplug their internet cable(s). (Preferred method)

Enable your Internet Connection Firewall (ICF).

If you are using Windows XP:

Click the Start button and then click Control Panel. Double-click "Networking and Internet Connections" and then click Network Connections. Right-click the current Internet or Network connection and then click Properties.

On the Advanced tab, click select the option to "Protect my computer or network."

Plug your internet cable if you have removed it previously

Install Microsoft Security Patch MS04-011

Connect to the Internet and install the patch from Microsoft to remove the vulnerability. You must disable your antivirus software before installing the patch.

To install the patch, visit the following Web site:

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

Reboot the machine after the patch is installed.

Run the Sasser Removal Tool.

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

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/>

RE: how to fix the problem when screen is blank! (sassser worm??)

microsoft.public.security.virus: RE: how to fix the problem when screen is blank! (sassser worm??)

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 or e-mail viruscsc@microsoft.com.

Regards,

Venkat.

ARE YOU PROTECTED AGAINST SASSER?

Follow the links below to find out more

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

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

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

Get Secure: <http://www.microsoft.com/security>

Stay up to date: <http://www.windowsupdate.com>