

**** READ THIS BEFORE POSTING – answers to frequently asked questions 2004.05.07**

Source:

<http://www.tech-archive.net/Archive/Scripting/microsoft.public.scripting.virus.discussion/2004-05/0128.html>

From: Karl Levinson [x y] mvp (levinson_k_at_despammed.com)

Date: 05/07/04

Date: Fri, 7 May 2004 07:39:47 -0400

Before you post a question to a Microsoft.public.*.security newsgroup, note that your question may already be answered below:

Answers to Top Frequently Asked Questions:

<http://securityadmin.info>

I'm getting an LSASS error message, and/or I have the Sasser virus.

1) Run anti-virus that is configured to download the latest updates every week or even every day. www.grisoft.com is free anti-virus.

2) You also need to install all the patches for your system software from <http://windowsupdate.microsoft.com>, starting with the MS04-011 patch. Microsoft generally releases security patches on the second Tuesday of more or less every month. [The MS04-011 patch is also available here: <http://www.microsoft.com/technet/security/bulletin/ms04-011.msp> ... though you still want to visit the Windows Update site to get all patches.]

3) Once you're infected, you may need to download and run a free Sasser virus removal tool such as the Stinger tool from www.McAfee.com or the free tool from <http://www.microsoft.com/security/incident/sasser.asp>

4) You're not running a firewall, or your firewall isn't protecting you. Running a firewall would have protected you from this. Free firewall software is available from www.kerio.com, www.zonealarm.com and/or www.sygate.com

5) You need to do ALL of these things, or you won't have much success. You should also make sure you get the latest Microsoft patches monthly and anti-virus updates at least weekly.

My question is not mentioned below. How do I get an answer immediately, with no waiting?

<http://securityadmin.info/faq.htm#moreinfo>

See also: http://www.google.com/groups?as ugoup=microsoft.public.*

See also: http://www.google.com/advanced_group_search

See also: <http://www.google.com>

I want to post a problem or question to the newsgroup. What info do I need

to post in order to get a correct answer quickly?

<http://securityadmin.info/faq.htm#netiquette>

I just heard about a new Microsoft security patch update. Where can I get the patch?

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

<http://www.microsoft.com/technet/security/current.asp>

I just installed a Microsoft security patch update, and now my computer is having problems.

<http://securityadmin.info/faq.htm#patchbroke>

I received an email from Microsoft / Microsoft Support / Microsoft Internet Security Center claiming to be a security patch [or comprehensive Internet Explorer update]. Is this a virus?

<http://securityadmin.info/faq.htm#microsoftemail>

ALSO NOTE: www.grisoft.com is free antivirus, USE IT.

I received a virus email from a Microsoft email address. Who do I report this to?

<http://securityadmin.info/faq.htm#microsoftemail>

I have the RPC Blaster worm "virus," what do I do?

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

ALSO NOTE: www.grisoft.com is free antivirus, USE IT.

My computer is giving RPC Remote Procedure Call messages.

There is a TFTP message or file on my computer.

My computer keeps locking up, and/or rebooting, or telling me that it will reboot in 1 minute.

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

ALSO NOTE: www.grisoft.com is free antivirus, USE IT.

Where can I download the Blaster worm / RPC DCOM patch?

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

<http://www.microsoft.com/technet/security/current.asp>

I'm having a problem caused by the JDBGMGR.EXE Teddy Bear "virus" hoax, or I want to replace this file.

<http://securityadmin.info/faq.htm#jdbgmgr>

I forgot my Windows logon password and can't log in. How do I reset it?

<http://securityadmin.info/faq.htm#password>

I have a problem or a question with a virus or with antivirus.

<http://securityadmin.info/faq.htm#virus>

NOTE: www.grisoft.com is free antivirus, USE IT.

Why is Outlook Express blocking my attachments as "unsafe"?

<http://securityadmin.info/faq.htm#attachments>

How do I stop getting pop-up messages? Or adware? Or spyware?

<http://securityadmin.info/faq.htm#pop-ups>

How do I block people from viewing adult or objectionable content on a computer?

<http://securityadmin.info/faq.htm#contentfilter>

How do I block spam emails?

<http://securityadmin.info/faq.htm#spam>

There is a Content Advisor password blocking me from certain web sites.

<http://securityadmin.info/faq.htm#contentadvisor>

How do I delete an FTP folder that a hacker put on my computer and I cannot delete?

<http://securityadmin.info/faq.htm#ftpfolder>

Have I been hacked? What do I do if I've been hacked?

<http://securityadmin.info/faq.htm#hacked>

How do I re-secure a computer that has been hacked?

<http://securityadmin.info/faq.htm#re-secure>

How do I test or improve the security on my computer to avoid being hacked?

<http://securityadmin.info/faq.htm#harden>

How do I investigate a suspicious IP address that may be trying to hack me?

<http://securityadmin.info/faq.htm#trace>

How do I report a hacker?

<http://securityadmin.info/faq.htm#reporthacker>

How do I use a port scanner or vulnerability scanner to test my security?

<http://securityadmin.info/faq.htm#portscanner>

How do I encrypt my files and/or hard drive?

<http://securityadmin.info/faq.htm#encryption>

How do I get a firewall? IDS?

<http://securityadmin.info/faq.htm#firewall>

I want to use the IPSec filtering or IP filtering feature of Windows to block certain ports and have a problem or question.

<http://securityadmin.info/faq.htm#ipsec>

I have a problem or question with the XP ICF firewall.

<http://securityadmin.info/faq.htm#icf>

I have a problem or question with the IIS URLScan tool.

<http://securityadmin.info/faq.htm#urlscan>

How do I change the banner on my computer or server to hide what software version I'm using?

<http://securityadmin.info/faq.htm#banner>

How do I enable Windows Auditing to tell who logged into Windows or who accessed a file?

<http://securityadmin.info/faq.htm#auditing>

How do I inspect and disable programs that start up when Windows starts?

<http://securityadmin.info/faq.htm#startup>

How do I use RUNAS or let someone use RUNAS to run commands as administrator without having to type the password?

<http://securityadmin.info/faq.htm#runas>

How do I let non-administrator users run Defrag or change their IP address?

<http://securityadmin.info/faq.htm#runas>

My question is not mentioned above. How do I get an answer immediately, with no waiting?

<http://securityadmin.info/faq.htm#moreinfo>

See also: http://www.google.com/groups?as_ugroup=microsoft.public.*

See also: http://www.google.com/advanced_group_search

See also: <http://www.google.com>

I want to post a problem or question to the newsgroup. What info do I need to post in order to get a correct answer quickly?

<http://securityadmin.info/faq.htm#netiquette>

Note that this is NOT a full list of all the questions answered in the FAQ.

Chances are, your question has probably already been answered. The complete FAQ is at:

<http://securityadmin.info/faq.htm#contents>

I hope this is helpful. Feedback, suggestions and criticism regarding the FAQ are welcome and may be emailed to me.

kind regards,

Karl Levinson, CISSP, MCSE, MVP

email: levinson_k@despammed.com