

Re: possible virus? and how get rid of it...

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2005-06/msg07367.html>

- *From:* "Steve N." <me@xxxxxxxx>
 - *Date:* Wed, 15 Jun 2005 00:58:54 GMT
-

David H. Lipman wrote:

From: "Naturegal74" <Naturegal74@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

```
| I have Windows XP.
|
| I use the internet rarely, and it's usually to Yahoo email, and I never open
| documents from people I don't know.
|
| I have Norton and it's up-to-date.
|
| I logged onto the internet, and after a few minutes, I got this message that
| my computer will shut down in 1 minute. It had something like
| system/32/lsass.exe in the message. And then it shut down after 1 minute. It
| does this over and over.
|
| I have had this happen before, and I've immediately gone to Microsoft.com to
| download any security downloads they had to try and fix it. Plus I've run
| Norton. I've always been able to get rid of whatever was in there without an
| issue.
|
| This time, I did the same exact thing. I downloaded the Malicious Threat
| download that is on Microsoft.com plus ran Norton. Nothing came up from
| either scan. But the computer keeps shutting down with that same message.
|
| A window did pop up that suggested a free scan to check the computer
| registry, but then after it scans, it wants you to be $40 to fix the problem.
| And then another window said to download a patch for $20. I wasn't sure if
| these were legit or not. I do not have Service Pack II, so should I download
| that? Would that help? I don't know if the computer will stay on long enough
| for me to do it, but I can try...
|
| Any thoughts or advice?
```

Although it "sounds" like the Sasser worm, I have seen information of occurrences which caused a Lsass NT Shutdown situation that mirrors a Lsass Exploit such as Sasser.

You indicated thaty Norton and the MS Malicious software scanners found nothing.

Re: possible virus? and how get rid of it...

What you don't indicate is if you are at SP2 level.

When you get the shutdown message, go to: Start --> Run
enter; shutdown -a

This will halt the shutdown and give you a chance to Download the McAfee worm removal tool
Stinger: <http://vil.nai.com/vil/stinger/>

Please read the following URL:
http://www.microsoft.com/security/incident/sasser_printxp.mspx

Please install and/or verify that the patch that fixes the
Lsass vulnerability that the
Sasser and other infectors exploit has indeed been installed
-- KB835732
<http://www.microsoft.com/downloads/details.aspx?FamilyId=3549EA9E-DA3F-43B>

Start killing off SVCHOST processes and see what happens.

The problem is determining what is causing which interdependant system
service to crash. Worms? The OP indicates that has been fairly well
eliminated.

Steve

.