

Re: SASSER?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-03/0255.html>

From: David H. Lipman (*DLipman~nospam~_at_Verizon.Net*)

Date: 03/09/05

Date: Wed, 9 Mar 2005 15:25:56 -0500

From: "PHILLIP2393" <PHILLIP2393@discussions.microsoft.com>

| I have windows 2000 professional on my computer at home. Let me breakdown
| the events from the las few days, because before then the computer was
| working fine:

| 3 days ago:

| I get a WINLOGON.EXE error but computer boots up. Most of my desktop was
| wiped clean, and the only reason I was able to recover some of the files I
| saved under my user profile is because it created a backup user folder. I
| tried restarting and I got the error: stop:c000021 (Bad Image checksum) Image
| CRYPT.dll is possibly corrupt. Gave up after trying to restart several times
| with out success.

| 2 days ago:

| First time I try starting up I get error: C:WINNT\system32\lsass.exe
| terminated unexpectedly with status code 128, and my computer restarted
| before it was completely started up. Then it would get to the windows screen
| and restart and it kept doing that, so I gave up for the day.

| 1 day ago:

| I got the following error codes on separate occasions: First: WINDOWS 2000
| could not start because the following file is missing or
| corrupt:\WINNT\SYSTEM32\CONFIG\SYSTEM, and the computer would keep
| restarting. Second: WINDOWS 2000 could not start because the following file
| is missing or corrupt:\WINNT\SYSTEM\vgaem.fon, and the computer would keep
| restarting.

|
| I have important files on my C drive that I am afraid I have lost. This is
| my father-in-laws computer and he has no idea where disk is. I have try
| starting up in Safe mode and evry other mode when you press F8 but nothing
| works. Sorry for the novel but I wanted to give a good desription. Any help
| is appreciated.

Does not sound like a Sasser problem at all. Could be a user profile problem or a DLL
corruption problem butm no indications of the Sasser Internet worm. Could even be a hard
disk corruption since that FON font error is a sign of such.

Dump the contents of the IE Temporary Internet Folder cache (TIF)

microsoft.public.security.virus: Re: SASSER?

start --> settings --> control panel --> internet options --> delete files

Open a Command Prompt.

In the Command Prompt type the following...

CHKDSK C: /F

If it replies..

"Chkdsk cannot run because the volume is in use by another process.

Would you like to schedule this volume to be checked the next time the system restarts?

(Y/N)"

Choose – Y

type; EXIT

Reboot the PC.

A full Check Disk will want to be performed, allow it.

When it reboots, perform a defragmentation of the hard disk.

You can get to the Defragmenting program easily by executing; dfrg.msc

Start --> run -->

type; dfrg.msc

--

Dave