

Re: Blue screen crashes

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2007-12/msg01886.htm

- *From:* "Gerry" <gerry@xxxxxxxxxx>
 - *Date:* Fri, 21 Dec 2007 20:06:58 -0000
-

Dominic

I would try Start, Run, type "sfc /scannow" without quotes and hit Enter.

Description of Windows XP and Windows Server 2003 System File Checker (Sfc.exe)

<http://support.microsoft.com/default.aspx?scid=kb:en-us:310747>

You will need your CD.

Try Start, Run, type "sigverif.exe" without quotes and hit OK. What drivers are listed as unsigned? Disregard those which are not checked.

I am wondering whether you left behind a bit of logmein when you uninstalled?

--

Hope this helps.

Gerry

~~~~~

FCA

Stourport, England

Enquire, plan and execute

~~~~~

Dominiccoombe wrote:

Gerry,

the machine is about 1 1/2 years old.

it is custom built.

this is a desktop mostly used for browsing, ms office, and outlook

Re: Blue screen crashes

and ms money.

parts include

asus p5n32-sle se deluxe mobo
Kingston 2 * 1GB ram 5-5-5-15
WD SATA 3gb 250GB
xfx geforce 6800gt
Intel core duo E6600 cpu

Yes I did have some remote control software on the machine for a short time. it was logmein

my xp cd is xp pro from the microsoft action pack.

"Gerry" wrote:

Background information on Stop Error report:
<http://msdn2.microsoft.com/en-us/library/ms794023.aspx>

A kernel mode program generated an exception which the error handler didn't catch. These are nearly always hardware compatibility issues (which sometimes means a driver issue or a need for a BIOS upgrade).
<http://aumha.org/a/stop.htm>

Has there been any use of remote control software to maintain, update or service this computer. Is the laptop used for work as well as pleasure?

What is your Windows XP CD as it is described on the face of the CD?

What is your computer make and model? How old is it?

--

Hope this helps.

Gerry

~~~~~

FCA

Stourport, England

Enquire, plan and execute

~~~~~

Dominiccoombe wrote:

Re: Blue screen crashes

this is the latest dump analysis to go with the event viewer

Microsoft (R) Windows Debugger Version 6.8.0004.0 X86
Copyright (c) Microsoft Corporation. All rights reserved.

Loading Dump File

[C:\WINDOWS\Minidump\Mini122107-01.dmp]

Mini Kernel Dump File: Only registers and stack trace are available

Symbol search path is:

srv*c:\symbols*<http://msdl.microsoft.com/download/symbols>

Executable search path is: c:\windows\i386

Windows XP Kernel Version 2600 (Service Pack 2) MP (2 procs) Free

x86 compatible

Product: WinNt, suite: TerminalServer SingleUserTS

Built by: 2600.xpsp_sp2_gdr.070227-2254

Kernel base = 0x804d7000 PsLoadedModuleList = 0x805624a0

Debug session time: Fri Dec 21 02:36:31.843 2007 (GMT-5)

System Uptime: 0 days 7:58:40.554

Loading Kernel Symbols

.....
Loading User Symbols

Loading unloaded module list

.....

*

*

* Bugcheck Analysis

*

*

*

Use !analyze -v to get detailed debugging information.

BugCheck 1000008E, {c0000005, 80550320, a467aae8, 0}

Probably caused by : win32k.sys (win32k!HeavyFreePool+bb)

Followup: MachineOwner

Re: Blue screen crashes

0: kd> !analyze -v

```

*****
*
*
* Bugcheck Analysis
*
*
*****

```

KERNEL_MODE_EXCEPTION_NOT_HANDLED_M
(1000008e)

This is a very common bugcheck. Usually the exception address pinpoints the driver/function that caused the problem. Always note this address as well as the link date of the driver/image that contains this address.

Some common problems are exception code 0x80000003. This means a hard coded breakpoint or assertion was hit, but this system was booted /NODEBUG. This is not supposed to happen as developers should never have hardcoded breakpoints in retail code, but ...

If this happens, make sure a debugger gets connected, and the system is booted /DEBUG. This will let us see why this breakpoint is happening.

Arguments:

Arg1: c0000005, The exception code that was not handled
Arg2: 80550320, The address that the exception occurred at
Arg3: a467aae8, Trap Frame
Arg4: 00000000

Debugging Details:

EXCEPTION_CODE: (NTSTATUS) 0xc0000005 - The instruction at "0x%08lx" referenced memory at "0x%08lx". The memory could not be "%s".

FAULTING_IP:
nt!ExFreePoolWithTag+471

Re: Blue screen crashes

80550320 813e80000000 cmp dword ptr [esi],80h

TRAP_FRAME: a467aae8 -- (.trap 0xffffffa467aae8)

ErrCode = 00000000

eax=ffdf0004 ebx=89bb4b80 ecx=8055c600 edx=00000060

esi=00000024

edi=00000000 eip=80550320 esp=a467ab5c ebp=a467ab90

iopl=0

nv up ei pl nz na po nc cs=0008 ss=0010 ds=0023 es=0023

fs=0030

gs=0000 efl=00010202 nt!ExFreePoolWithTag+0x471:

80550320 813e80000000 cmp dword ptr [esi],80h

ds:0023:00000024=???????

Resetting default scope

CUSTOMER_CRASH_COUNT: 1

DEFAULT_BUCKET_ID: DRIVER_FAULT

BUGCHECK_STR: 0x8E

PROCESS_NAME: hpqste08.exe

LAST_CONTROL_TRANSFER: from bf802a9b to
80550320

STACK_TEXT:

a467ab90 bf802a9b e3b89b20 88f876c8 a467abb8
nt!ExFreePoolWithTag+0x471 a467aba0 bf80e88f e3b89b20
bf9ab0e8
e3b89b20 win32k!HeavyFreePool+0xbb a467abb8 bf838fac
e3b89b20
e3b89b20 a467abe0 win32k!HMFreeObject+0xa0 a467abc8
bf838f72
e3b89b20 e3a82430 bc513f0c
win32k!DestroyEmptyCursorObject+0x1b
a467abe0 bf84ac19 e3a82430 00000002 a467abfc
win32k!_DestroyCursor+0x105 a467abf0 bf84ac01
e3b89b20 a467ac14
bf8c09a6 win32k!DestroyUnlockedCursor+0xf a467abfc
bf8c09a6 bc5127e4
8905dde0 e3b3a820
win32k!HMDESTROYUnlockedObject+0x1c
a467ac14 bf8209f9 00000000 88d5fda8 00000000
win32k!DestroyProcessesObjects+0x70
a467ac3c bf819e30 00000001 a467ac64 bf819ef4
win32k!xxxDestroyThreadInfo+0x22c a467ac48 bf819ef4
88d5fda8
00000001 00000000 win32k!UserThreadCallout+0x4b
a467ac64 8056fc07
88d5fda8 00000001 88e3f968

Re: Blue screen crashes

win32k!W32pThreadCallout+0x3d a467acf0
8058c841 40010004 a467ad4c 804e74b8
nt!PspExitThread+0x3cc
a467acfc 804e74b8 88e3f968 a467ad48 a467ad3c
nt!PsExitSpecialApc+0x22 a467ad4c 804de263 00000001
00000000
a467ad64 nt!KiDeliverApc+0x1af a467ad4c 7df7bd1b
00000001 00000000
a467ad64 nt!Kei386EoiHelper+0x3a WARNING: Frame IP
not in any known
module. Following frames may be wrong. 0012fd34
00000000 00000000
00000000 00000000 0x7df7bd1b

STACK_COMMAND: kb

FOLLOWUP_IP:
win32k!HeavyFreePool+bb
bf802a9b 5d pop ebp

SYMBOL_STACK_INDEX: 1

SYMBOL_NAME: win32k!HeavyFreePool+bb

FOLLOWUP_NAME: MachineOwner

MODULE_NAME: win32k

IMAGE_NAME: win32k.sys

DEBUG_FLR_IMAGE_TIMESTAMP: 45f013f6

FAILURE_BUCKET_ID: 0x8E_win32k!HeavyFreePool+bb

BUCKET_ID: 0x8E_win32k!HeavyFreePool+bb

Followup: MachineOwner

"Dominiccoombe" wrote:

All,

I did verifier and chkdsk /r which ran for
about 2 hours on my 250gb
HDD

Re: Blue screen crashes

reinstalled the latest version of spysweeper.

Will see how it goes.

Dom

in meantime I will check out the malware

"Gerry" wrote:

Dominic

What Warning and Error Reports appear in Event Viewer since it's removal? Can you please post copies.

If you have had a malware infestation one holds the door open to let it's friends in.

Can you please post a copy of the latest Stop error report.

--

Hope this helps.

Gerry

~~~~

FCA

Stourport, England

Enquire, plan and execute

~~~~~

Dominiccoombe wrote:

Gerry,

SSFS0BB8.SYS

– does not
exist on the

Re: Blue screen crashes

machine
after the
uninstall
of webroot.

I will
follow your
spyware
suggestions
after I do
the verifier
and chkdsk
/r

Dominic

"Gerry"
wrote:

Dominic

Background
information
on
Stop
Error
message

<http://msdn2.microsoft.com/en-us/library/ms793989.aspx>

<http://aumha.org/a/stop.htm>

SSFS0BB8.SYS

-This
file
concerns
me
as
I
cannot
ascertain
what
it
is
but
it
has
often
cropped
up

Re: Blue screen crashes

in
HijackThis
files
where
the
user
is
seeking
to
remove
malware.

Can
you
locate
the
file
in
Windows
Explorer
and
examine
it's
properties
by
right
clicking
on
the
file.
Instructions
on
how
to
Show
hidden
files
are
in
the
next
paragraph.

Go
to
Start,
Control
Panel,
Folder
Options,
View,

Re: Blue screen crashes

Advanced
Settings
and
verify
that
the
box
before
"Show
hidden
files
and
folders"
is
checked
and
"Hide
protected
operating
system
files
"
is
unchecked.
You
may
need
to
scroll
down
to
see
the
second
item.
You
should
also
make
certain
that
the
box
before
"Hide
extensions
for
known
file
types"
is

Re: Blue screen crashes

not
checked.
Next
in
Windows
Explorer
make
sure
View,
Details
is
selected
and
then
select
View,
Choose
Details
and
check
before
Name,
Type,
Total
Size,
and
Free
Space.

What
are
your
anti-virus
and
anti-spyware
arrangements?

<http://www.elephantboycomputers.com/page2.html#Removin>

I
do
not
think
it
is
is
worth
pursuing
other
avenues
of

Re: Blue screen crashes

enquiry
until
the
situation
regarding
malware
is
clearer.

--

Hope
this
helps.

Gerry
~~~~  
FCA  
Stourport,  
England  
Enquire,  
plan  
and  
execute

~~~~~

Dominiccoombe
wrote:

Gerry,

The
last
line
of
the
minidump
says
"Probably
caused
by
:
SSFS0BB8.SYS
(
SSFS0BB8+2dd1
)"

Event
Viewer

Re: Blue screen crashes

Date
12/18/07
Event
Save
Dump
Time
5:05:31
event
id
1001