

## Re: Stop 0x50 occurring after Exch SP1 and e-mail bomb

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-08/3763.html>

---

**From:** mrceolla (mrceolla\_at\_terracom.net)

**Date:** 08/11/04

Date: 11 Aug 2004 09:00:59 -0700

rayfong@online.microsoft.com (Ray Fong [MSFT]) wrote in message news:<t87NO5xfEHA.3356@cpmsftngxa06.phx.gbl>...

> Run "!analyze -v" in WinDbg, then post back the results.

>

> If you have POP3 Connector issue, did you apply 835734?

>

> 835734 Many unexpected outbound e-mail messages appear in the SMTP queue in

> <http://support.microsoft.com/?id=835734>

>

> Did you check the q in Exchsrvr\Mailroot\vs1\Queue folder? Do you have

> lots of files there?

>

> Ray Fong

> Microsoft SBS Product Support

The results of my crash dump !analyze -v are at the end of this message...but first....

Regarding the pop3 issue. I have installed the patch already. I did so after the before mentioned NDR problem. All the queues were emptied and the queue folder was also empty. However, the patch did not work. I was able to test it with some more of the problematic e-mails, and NDRs were still generated for users not in my domain.

<http://groups.google.com/groups?hl=en&lr=&ie=UTF-8&frame=right&th=22b8bb415807d60b&seekm=79f36727.04>

That thread discusses the particular message that was affecting me and some others. From what I gathered, the pop3 fix does not work for this message. But this problem is not as important as the stop messages I'm getting. I just brought it up because the crashes first began during/after this event.

On to the stop error and debug. The only changes I had recently made, that I can remember, are one of the more recent critical update for what I think was an IE security issue(automatically notified by

microsoft.public.windows.server.sbs: Re: Stop 0x50 occurring after Exch SP1 and e-mail bomb

windows update), a windows media services update (at the update website), and Exchange 2003 SP1...not necessarily in that order. Since the problems started, I updated my LAN driver via the windows update website.

I have run memtest86 v3.1 on my RAM. Maybe 2-3 passes on the default tests, and almost 3 passes on all tests and no errors reported.

No devices seem faulty. The only additional hardware connected to the mobo besides one HD is an AGP nVidia FX 5200. Although I know this is not the smartest thing, I stressed the system with some 3d games, and all was fine. One note, the processor is a hyperthreading P4 w/ hyperthreading enabled (cpu usage history shows 2 graphs).

I only have one full dump to work with now. This one says win32k.sys faulted. The other full dump (gone now) said ntkrnlmp.exe was faulting. I have renamed this dump in order to keep it for comparison in the future. Am I correct in assuming you can't do full analyzing of mini-dumps? I have a few of those, but windbg shows symbol errors and says it can't determine the name of the faulty driver name when I try to analyze them. So, here's the latest full dump !analyze -v. I downloaded the server 2003 symbols package and use the symbol path of "SRV\*c:\symbols\*<http://msdl.microsoft.com/download/symbols>". I'm using the latest version of debugging tools from the MS website.

```
*****
*
*
* Bugcheck Analysis
*
*
*
*****
```

PAGE\_FAULT\_IN\_NONPAGED\_AREA (50)  
Invalid system memory was referenced. This cannot be protected by try-except, it must be protected by a Probe. Typically the address is just plain bad or it is pointing at freed memory.  
Arguments:  
Arg1: e04392ec, memory referenced.  
Arg2: 00000001, value 0 = read operation, 1 = write operation.  
Arg3: bf900804, If non-zero, the instruction address which referenced the bad memory address.  
Arg4: 00000000, (reserved)

Debugging Details:  
-----

microsoft.public.windows.server.sbs: Re: Stop 0x50 occurring after Exch SP1 and e-mail bomb

WRITE\_ADDRESS: e04392ec Nonpaged pool

FAULTING\_IP:

win32k!HMAssignmentUnlock+9  
bf900804 ff4804 dec dword ptr [eax+0x4]

MM\_INTERNAL\_CODE: 0

IMAGE\_NAME: win32k.sys

DEBUG\_FLR\_IMAGE\_TIMESTAMP: 3e801611

MODULE\_NAME: win32k

FAULTING\_MODULE: bf800000 win32k

DEFAULT\_BUCKET\_ID: DRIVER\_FAULT

BUGCHECK\_STR: 0x50

CURRENT\_IRQL: 1

LAST\_CONTROL\_TRANSFER: from bf8ce635 to bf900804

TRAP\_FRAME: ed32870c --- (.trap ffffffffed32870c)

ErrCode = 00000002

eax=e04392e8 ebx=00000000 ecx=bc6332b8 edx=00000000 esi=bc633270

edi=e11fb588

eip=bf900804 esp=ed328780 ebp=ed328790 iopl=0 nv up ei ng nz

na po nc

cs=0008 ss=0010 ds=0023 es=0023 fs=0030 gs=0000

efl=00010286

win32k!HMAssignmentUnlock+0x9:

bf900804 ff4804 dec dword ptr [eax+0x4]

ds:0023:e04392ec=????????

Resetting default scope

STACK\_TEXT:

ed32877c bf8ce635 e11fb610 00000000 8637cc60

win32k!HMAssignmentUnlock+0x9

ed328790 bf903076 e11fb610 00000001 e12e5aa0 win32k!DestroyClass+0x7f

ed3287a0 bf901def e11fb588 859d7388 00000000

win32k!DestroyProcessesClasses+0x27

ed3287e8 bf8ebce3 00000001 bf8ebd2b 859d7388

win32k!xxxDestroyThreadInfo+0x252

ed3287f0 bf8ebd2b 859d7388 00000001 00000000

win32k!UserThreadCallout+0x48

ed328808 805922d0 859d7388 00000001 859d7388

win32k!W32pThreadCallout+0x37

ed3288a0 805dfe6a c0000354 859c2840 804f3251 nt!PspExitThread+0x3a2

ed3288ac 804f3251 859c2840 ed3288f8 ed3288ec nt!PsExitSpecialApc+0x1b

Re: Stop 0x50 occurring after Exch SP1 and e-mail bomb

microsoft.public.windows.server.sbs: Re: Stop 0x50 occuring after Exch SP1 and e-mail bomb

ed3288fc 804dfda8 00000001 00000000 ed328914 nt!KiDeliverApc+0x1c6  
ed3288fc 77f43855 00000001 00000000 ed328914 nt!KiServiceExit+0x56  
00fefcf8 77d06718 77d067e0 00fedf6c 00000000  
ntdll!KiUserCallbackDispatcher  
ed328bd0 8058ebe5 ed328c44 ed328c48 00000000 nt!KiCallUserMode+0x4  
ed328c28 bf86c669 0000004d 00000000 00000000  
nt!KeUserModeCallback+0x85  
ed328c4c bf8e57af 00000200 e12e5aa0 00000000  
win32k!ClientDeliverUserApc+0x1e  
ed328c94 bf8e5db1 000025ff 00000000 00000001  
win32k!xxxSleepThread+0x109  
ed328cec bf8e6721 ed328d18 00000000 00000000  
win32k!xxxRealInternalGetMessage+0x471  
ed328d4c 804dfd24 00fedf6c 00000000 00000000  
win32k!NtUserGetMessage+0x27  
ed328d4c 7ffe0304 00fedf6c 00000000 00000000 nt!KiSystemService+0xd0  
00fefcf8 77d06718 77d067e0 00fedf6c 00000000  
SharedUserData!SystemCallStub+0x4  
00fedf18 748f15df 00fedf6c 00000000 00000000  
USER32!NtUserGetMessage+0xc  
00fed90 748f281c 748f0000 00000000 000100cc  
stobject!SysTrayMain+0x17e  
00feffb8 77e4a990 00000000 00000000 00000000  
stobject!CSysTray::SysTrayThreadProc+0x4d  
00feffec 00000000 748f27cf 00000000 00000000  
kernel32!BaseThreadStart+0x34

FOLLOWUP\_IP:

win32k!HMAssignmentUnlock+9  
bf900804 ff4804 dec dword ptr [eax+0x4]

SYMBOL\_STACK\_INDEX: 0

FOLLOWUP\_NAME: MachineOwner

SYMBOL\_NAME: win32k!HMAssignmentUnlock+9

STACK\_COMMAND: .trap ffffffffed32870c ; kb

BUCKET\_ID: 0x50\_W\_win32k!HMAssignmentUnlock+9