

Re: repeated failure of store – security hack?

- > At 2:06 the sam happened and email delivery went down
- >
- > I got the following events logged:
- >
- >
- > Event Type: Warning
- > Event Source: ESE
- > Event Category: Performance
- > Event ID: 508
- > Date: 23/11/2005
- > Time: 14:06:16
- > User: N/A
- > Computer: COULTER–MAIN
- > Description:
- > Information Store (3196) First Storage Group: A request to write to
- > the file "D:\exchsrvr\mdbdata\E00tmp.log" at offset 0
- > (0x0000000000000000) for 1048576 (0x00100000) bytes succeeded, but
- > took an abnormally long time (244 seconds) to be serviced by the OS.
- > This problem is likely due to faulty hardware. Please contact your
- > hardware vendor for further assistance diagnosing the problem.
- >
- > For more information, click
- > <http://www.microsoft.com/contentredirect.asp>.
- >
- >
- > Event Type: Warning
- > Event Source: ESENT
- > Event Category: Performance
- > Event ID: 508
- > Date: 23/11/2005
- > Time: 14:06:15
- > User: N/A
- > Computer: COULTER–MAIN
- > Description:
- > wins (1656) A request to write to the file
- > "C:\WINDOWS\system32\wins\j50.log" at offset 389632
- > (0x0000000000005f200) for 512 (0x00000200) bytes succeeded, but took
- > an abnormally long time (60 seconds) to be serviced by the OS. This
- > problem is likely due to faulty hardware. Please contact your
- > hardware vendor for further assistance diagnosing the problem.
- >
- > For more information, see Help and Support Center at
- > <http://go.microsoft.com/fwlink/events.asp>.
- >
- >
- > Event Type: Warning
- > Event Source: ESENT
- > Event Category: Performance
- > Event ID: 508
- > Date: 23/11/2005
- > Time: 14:06:15

Re: repeated failure of store – security hack?

Re: repeated failure of store – security hack?

- > User: N/A
- > Computer: COULTER–MAIN
- > Description:
- > tcpsvcs (2064) A request to write to the file
- > "C:\WINDOWS\System32\dhcp\j50.log" at offset 15360
- > (0x0000000000003c00) for 512 (0x00000200) bytes succeeded, but took
- > an abnormally long time (60 seconds) to be serviced by the OS. This
- > problem is likely due to faulty hardware. Please contact your
- > hardware vendor for further assistance diagnosing the problem.
- >
- > For more information, see Help and Support Center at
- > <http://go.microsoft.com/fwlink/events.asp>.
- >
- > when I checked the counters it doe show discs idle time low and
- > transfer rate low, which suggests hardware – but considering recent
- > events (and the fact that the driv is new) I am not sure.t

Well, I'd be inclined to believe it. What's your disk setup? Hardware RAID is the best. Got good backups? Take a full backup now.

- > Also, on checing the security logs I get repeated logon/logoff evenmt
- >
- <snip>
- >
- > I have successfully restored the store again;but for how long?
- >
- > I am thinking rootkit trojan – I have not come across one before and
- > do not want to!
- >

> Please help, I am getting overwhelmed here!

You need good antivirus software running on your whole network. Do you have a separate 'edge' firewall in place or are you using ISA?
Don't run beta software on your server. And spyware is unlikely to be on it unless someone's using it as a workstation, which they shouldn't be. I think you have hardware problems, myself.

- >
- > Many thanks
- >
- > John

.

• *Follow-Ups:*

Re: repeated failure of store – security hack?

Re: repeated failure of store – security hack?

◆ **Re: repeated failure of store – security hack?**

◇ From: Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]

• **References:**

◆ **repeated failure of store – security hack?**

◇ From: John McCombe

- Prev by Date: **Re: SBS 2003 & NT Server**
- Next by Date: **Re: SBS2003 and VPN / Terminal services**
- Previous by thread: **repeated failure of store – security hack?**
- Next by thread: **Re: repeated failure of store – security hack?**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**