

Re: repeated failure of store – security hack?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-11/msg03657.html>

- *From:* "Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]" <sbradcpa@xxxxxxxxxxx>
 - *Date:* Thu, 24 Nov 2005 22:16:08 -0800
-

I don't run Antispyware on my server because I don't surf there. Thus I don't have the threat.

Yes on a DC like this you will have lots of logons/offers.

Truly call PSS, ask for an analysis they can put your mind at ease [or not] but their analysis has to be done one on one with your event logs, It's not something that can be done in a newsgroup.

John McCombe wrote:

Thanks for your posts, they are helpful.

Latest update I have the same MO appearing on another server, not related to or connected to the first one (I am the only common denominator, I visited this new one the day after the first).

This server has been running ok for three years, it has been running ok 72 days since last reboot. I received email alerts regarding the store start pending, this afternoon. Mail delivery had ceased. Security logs show repeated logon logoff events, Store log files were corrupted.

lsass.exe process is taking up 35 - 50% processor activity. This is a 1 processor 2.8GHz system. (The first system is a 2X dual processor 2.8GHz and shows no noticeable change in processor activity, but for high disc activity)

I have antivirus software running at the webhost for email, and for each workstation - not a free one. I have the MS firewall, and a hardware firewall on the router.

I will remove the beta software, but why was it recommended on the Microsoft security site?

Re: repeated failure of store – security hack?

Note that the situation occurred prior to the installation of the software.

Is it normal to have so many logon/logoff events and to have attempts to change permissions? How can address this?

I am still not convinced that it is hardware - not on two different systems, one after the other.

How can I monitor and restrict the logon activity? Note that this is not user activity.

I understand that I may not be doing best practice, but what I need now is a strategy to sort this out. I would appreciate more advice

John McCombe

"Susan Bradley, CPA aka Ebitz - SBS Rocks" wrote:

You can always call Microsoft product support - Security and discuss the issues.

Lanwench [MVP - Exchange] wrote:

In news:05004143-60D4-45E8-B0E4-7E2E874BDCDD@xxxxxxxxxxxxxxxx,
John McCombe <JohnMcCombe@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> typed:

Hi

I have a problem with a sbs 2003 server runnig fine since commissioning August 05. On last Monday morning 08:39 ther were 50+ attempts to log in to the server from a (win98) client using the wrong password and the user was locked out.

Re: repeated failure of store – security hack?

Disable account lockout - it's a bad idea.

I received an email warning. Then the users came in at 9:00 and advised me that noone could log in. I am remote from the server, and could not access it either.

I recommended a soft re-boot, but unfortunately they could not do so, and powered off & on.

At this stage, login was allowed, but email delivery was not working. I checked in the event logs and was told that stor could not stsrst as the exxx log file was corrupt

Using the MS KB I restored the log files form backup and the store stsrtd ok - email traffic ok.

This lasted about 28 hours, and the same symptoms occured - store not mounted emails received (by pop3) but not delivered.

I went to visit the server - re-booted restored the log files all ok. I ran MS malicious software removal tool nothing found I ran MS antispysware tool nothing found. (it is now running in the background).

I left site at 2pm will all messages tracked as delivered ok.

At 2:06 the sam happened and email delivery went down

I got the following events logged:

Re: repeated failure of store – security hack?

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
User: N/A
Computer: COULTER-MAIN

Re: repeated failure of store – security hack?

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 dics 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!

Re: repeated failure of store – security hack?

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