

Re: Event 26. Your computer may be infected.

Re: Event 26. Your computer may be infected.

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-10/msg00040.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Thu, 12 Oct 2006 15:47:41 -0700
-

I think you may be examining the wrong machine. The message is claimed to be sent from/by the DC. The MRP member is just the recipient of the message. There are two alternatives here. The DC is actually sending the message, in which case it may have been compromised (unless you can recognize the as an alert something you have installed would send); or some other machine may be originating the message so that it appears as if it comes from the DC.

There is some defined need that you have so the you have the messenger service running? It is pretty easy to cause a machine to receive a message if it is running. However you need to verify that it is not originating from something that is on the DC.

"Bunert" <rizenbone@xxxxxxxxxx> wrote in message news:e1Ujhhg7GHA.4304@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

I have a W2k3 domain controller and a W2k member server.

Both have been running fine for weeks, months, years.

There have been no changes to either machine in the last few days.

All of a sudden today, I am getting a messenger application pop-up from the domain controller that says:

Message from DC to Server at XX:XX:XX AM on XX/XX/2006.

Your computer may be infected by a virus and may be attacking other computers on the network.

Please check your antivirus pattern and your software.

It logs even ID 26 with the same description on the W2k member server – nothing is logged on the W2k3 controller.

I've scanned the W2k member with the latest antivirus and it comes up clean. I've reviewed services, run registry entries, startup, etc and nothing is there out of the ordinary. This server has not changed, been

Re: Event 26. Your computer may be infected.

rebooted, had anything done to it in the last week. HAVe not received these messages in the 3 years its been in place. This server sits there and provides access to an MRP app. No changes have happened on the MRP app.

I can't find any info on an event id 26 with the description above anywhere. I'm not seeing any abnormal traffic to or from that server.

It does run Backup Exec overnight, but its run that to the same target servers for 3 years. Otherwise this box has no other function.

Anyone with any ideas or things to look at? It's looking fine, but I got about 10 of those popups in 2 hours this morning. Then they have since stopped (so far). The times of the events do not correlate with anything running at that time.