

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/msg00073.html>

- *From:* "Gregg Hill" <bogus@xxxxxxxxxxxx>
 - *Date:* Wed, 25 Oct 2006 13:10:49 -0700
-

Bunert,

I just found this on Trend's site.

<http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-125968&id=EN-125968>

Gregg Hill

"Bunert" <rizenbone@xxxxxxxx> wrote in message
<news:e1Ujhgh7GHA.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 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.

Re: Event 26. Your computer may be infected.

Re: Event 26. Your computer may be infected.

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.