

advice about a worm intrusion alert

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2006-11/msg00136.html>

- *From:* Robert M Jones <robert53newsgroups-ms2@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 24 Nov 2006 18:03:07 +0000
-

XP Home, limited user account. Newbie to this group – I know next to nothing about ports but am an experienced computer user otherwise.

Can anyone interpret this for me – just started to get these recently – this is only the second one. Got it while using a user account in my XP Home machine.

Security Alert – Medium Risk

Norton Internet Worm Protection has detected and blocked an intrusion attempt.

The text in More Info was as follows:

Intrusion: MS SQL PacketResolution DoS

Intruder: 192.168.1.1 (domain(53))

Risk Level: Medium.

Protocol: UDP

Attacked IP: COMPUTER NAME (192.168.1.2)

Attacked Port: ms-sql-m(1434)

The Intruder address was my router, to which one Win98SE computer is connected by ethernet (not mentioned in report) and the other on the 192.168.1.2 address is my XP Home machine, wirelessly connected to the router.

I clicked OK and then the wireless connection lost its IP and connectivity – and I had no internet access on the wireless XP machine. Router was still connected to internet fine – all lights glowing properly.

Computer upstairs 192.168.1.3 was on and could connect to the internet – no one was using it at the time of the alert. It has Zone Alarm free version to prevent any outgoing stuff, and also NAV and Spybot S&D resident (teatimer). It is on Win98SE. No alerts showing.

This machine runs Windows XP Home (user account) has NAV, Counterspy and Zone Alarm free. Wireless network is WPA-PSK with 63 character pw.

Log off and on did not restore the wireless (always does usually).

Log off and then on to Admin acct – again wireless network did not work but I got a windows error – windows is recovering from a serious error.

Still no connection.

Did a warm reboot and then everything was back to normal.

I do a Norton AV and Counterspy scan daily. Clear.

I think all the Windows/wireless hassle was due to the Norton blocking the request, and I think the "intrusion"

advice about a worm intrusion alert

was legitimate – but I don't want to "allow" it unless someone can explain the details to me. Many thanks to any network gurus who can interpret please.

--

Rev Robert M Jones, Wimborne Baptist Church, UK

<http://www.wimborne-baptist.org.uk>

Free trial of Mailwasher Pro – effective email spam filter – (commission goes to our partners in Bulgaria)

<http://fta.firetrust.com/index.cgi?id=420>

.