

Re: Ongoing Virus problem

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-08/9871.html>

From: Lanwench [MVP – Exchange] (lanwench_at_heybuddy.donotsendme.unsolicitedmail.atyahoo.com)

Date: 08/30/04

Date: Mon, 30 Aug 2004 18:57:44 -0400

Kevin Weilbacher [SBS-MVP] wrote:

> *what do you mean when you say -- "except exchange of course"?*

I presume he meant except the dangerous Exchange folders one should never scan with file-based software.

>

> *If you are not running an Exchange based mail scanner, then you're not*

> *catching anything until it gets into the user's mailbox and they pick*

> *it up with Outlook. Not quite the optimal situation, in my view.*

eTrust is an Exchange aware AV product, I believe – and if he's getting some attachments stripped, he has it.

>

> *"susan" <smcrey@mindspring.com> wrote in message*

> *news:egpsmCujEHA.3348@TK2MSFTNGP12.phx.gbl...*

>> *I'm having a problem in that we receive 5-15 virus infected emails*

>> *every day. Yes, I do have antivirus and sometimes it strips the*

>> *attachment and sometimes it doesn't (eTrust antivirus by CA).*

>> *Sometimes the virus identified is Netsky.P and sometimes Netsky.C*

>> *and i've had a few id'd as Netsky.Z -- some say "trojan", some say*

>> *"worm" ! I have virus scanned (and online scanned using Symantec's online*

>> *scanner) every workstation, laptop and the server (except exchange*

>> *of course) and can*

>> *find NOTHING! I've researched the virus'es and know what to look for*

>> *in the*

>> *registry etc. and find nothing indicating infection at any station.*

>>

>> *These infected emails sometimes have a "sender" address that is*

>> *familiar, but most often not.*

>>

>> *I check the headers and what's puzzling is that they read: sent from*

>> *"mydomain.org" received by "mail.mydomain.org".... does this*

>> *automatically mean that they are happening WITHIN the network??? The*

>> *ip address of the supposed "sender" is not a valid internal address,*

>> *but i realize all this stuff could be spoofed...*

>>

>> *I'm puzzled and don't know what else to do. I just have to find out*

microsoft.public.windows.server.sbs: Re: Ongoing Virus problem

>> *what I can do about this as babysitting the mail is tiring.*

>>

>> *Any ideas, suggestions, advice??*