

Re: email virus

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-02/0494.html>

From: Malke (malke_at_nospoonnotreally.com)

Date: 02/18/05

Date: Thu, 17 Feb 2005 18:51:38 -0800

Catamount wrote:

> *questionman wrote:*

>

>> *I have been attacked by an email virus which is causing my Outlook*

>> *Express to send out duplicate messages to everyone in my address*

>> *book. I have started to run Microsoft's new Antispyware program*

>> *(Beta), but I have a question. The program quickly notified me that*

>> *it has blocked a "possible Windows Trojan C:\WINDOWS\service.exe." It*

>> *then asks if I want to remove it. Should I remove it despite the word*

>> *"possible"?*

> *"service.exe is a process belonging to the Dell Solution Center which*

> *offers worldwide technical support and training for it's products. "*

>

> *Do you have a dell?*

Actually, you need to run a scan with a full-featured antivirus using updated definitions immediately. Although service.exe may be used by Dell, it is also used by quite a few viruses. MSAS is an antispyware tool, and beta at that. It will not remove viruses. If you do not have an antivirus installed, then start by scanning in Safe Mode with TrendMicro's Sysclean:

TrendMicro's Sysclean is an extensive antivirus tool which has the advantage of not needing to be installed. It requires two parts – the scanning engine and the virus pattern files.

1. Create a new folder on your Desktop or the C: drive named something useful like "Sysclean".
2. Go here and download the two parts of the program to that folder:

<http://www.trendmicro.com/download/dcs.asp> – Sysclean

<http://www.trendmicro.com/download/pattern.asp> – virus pattern files

The pattern files will be zipped – extract them with your unzipper (like WinZip) or if you have XP, you can just open the folder. You need to put the extracted files in the Sysclean folder you made.

3. Restart your computer in Safe Mode. Get into Safe Mode by repeatedly tapping the F8 key as the computer is starting up to get to the proper menu.
4. Go to the Sysclean folder you made and double-click on sysclean.com. Start the scan. After the scan is finished, look at the log. You may need to make a note of where any viruses were found if they were not able to be removed so you can manually delete them.

Then immediately get and install a full-featured av, update its definitions, and run a complete scan in Safe Mode.

In addition to the above, you must have a firewall in place. You didn't say what operating system (including service pack level) you are running; however, I would suggest installing either ZoneAlarm or Sygate's free personal firewall so you can see what is trying to get out.

Malke

--

MS MVP - Windows Shell/User
Elephant Boy Computers
www.elephantboycomputers.com
"Don't Panic!"