

microsoft.public.win2000.general: Re: Virus that causes a lot of traffic ?

Re: Virus that causes a lot of traffic ?

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.general/2004-11/3042.html>

From: David H. Lipman (*DLipman~nospam~_at_Verizon.Net*)

Date: 11/27/04

Date: Sat, 27 Nov 2004 18:26:34 -0500

Paul:

All viruses are malware but not all malware are viruses.

Adaware looks for non-viral malware (browser hijackers, adware, spyware, data miners, etc)

Stinger looks for some Trojans but mostly Internet worms.

Trend Sysclean is a broad-spectrum; virus, worm and Trojan cleaner.

Running the suggested utilities in Safe Mode increases the effectiveness of all the scanners to both detect and to clean.

Trend Housecall is a web based scanner while Trend sysclean is a Command Line scanner and they share the same Pattern Files. However, Sysclean it is not dependent upon a browser and because it can run in Safe Mode it is more effective.

Yes, Trend Sysclean is free.

Dave

"Paul fpvt2" <anonymous@discussions.microsoft.com> wrote in message news:96a401c4d4d6\$50455f30\$a401280a@phx.gbl...

| Thank you very much.

| I will suggest it to my office.

|

| May I ask, is it correct that Adaware only look for
| spyware type of viruses ?

|

| Before I run Trend Sysclean, Stinger and Adaware, is it
| necessary to boot in safe mode ?

|

| What do you think of virus check from

| http://housecall.trendmicro.com/housecall/start_corp.asp

| compare to the Trend Sysclean Package ? Is Trend Sysclean

| Package a free utility ?

|

| Thanks again.

|

Re: Virus that causes a lot of traffic ?

|>-----Original Message-----

|>Paul:

|>

|>That's what Ethereal is for. Determination of what the
| traffic is, what port and what is
|>the actual traffic.

|>

|>Dave

|>

|>

|>

|>

|>"Paul fpvt2" <anonymous@discussions.microsoft.com> wrote
| in message

|>news:9fd101c4d4bf\$ec3736a0\$a601280a@phx.gbl...

|>| Thank you very much for your reply. I will suggest that
|>| to our network administrator.

|>|

|>| My boss is convinced that we have SQL Slammer, but we
|>| told him that we have installed SQL Server 2000 SP3 on
|>| those machines that have a lot of traffic. I am
| wondering

|>| if there is any other virus that can cause heavy
| traffic

|>| to the server besides SQL Slammer, so that I can
| suggest

|>| to them to look at other viruses, not only SQL Slammer.

|>|

|>| Also, if we have 3 servers, 2 of them have SQL Server
|>| 2000 SP3 installed, and 1 does not have it, is it
|>| possible the SQL Slammer comes from this 1 server and
|>| cause the heavy traffic on the other 2 servers ?

|>|

|>| Thank you.

|>|

|>|>-----Original Message-----

|>|>You will have to use Ethereal or some other packet
|>| analysis tool and examine the traffic

|>|>to/from the server to see what's going on. In the
| mean

|>| time, I suggest performing the

|>|>following...

|>|>

|>|>1) Download the following four items...

|>|>

|>|> McAfee Stinger

|>|> <http://vil.nai.com/vil/stinger/>

|>|>

|>|> Trend Sysclean Package

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

|>|>

microsoft.public.win2000.general: Re: Virus that causes a lot of traffic ?

|> > Latest Trend Pattern File.
|> >
|> <http://www.trendmicro.com/download/pattern.asp>
|> >
|> > Adaware SE (free personal version v1.05)
|> > <http://www.lavasoftusa.com/>
|> >
|> > Create a directory.
|> > On drive "C:"
|> > (e.g., "c:\New Folder")
|> > or the desktop
|> > (e.g., "C:\Documents and Settings\lipman\Desktop\New
|> Folder")
|> >
|> > Download Sysclean.com and place it in that directory.
|> > Download the Trend Pattern File by obtaining the ZIP
|> file.
|> > For example; lpt265.zip
|> >
|> > Extract the contents of the ZIP file and place the
|> contents in the same directory as
|> sysclean.com.
|> >
|> > 2) Update Adaware with the latest definitions.
|> > 3) If you are using WinME or WinXP, disable System
|> Restore
|> >
|> >
|> <http://vil.nai.com/vil/SystemHelpDocs/DisableSysRestore.ht>
|> m
|> > 4) Reboot your PC into Safe Mode
|> > 5) Using Trend Sysclean, Stinger and Adaware,
|> perform a Full Scan of your
|> platform and clean/delete any
|> infectors/parasites found.
|> > (a few cycles may be needed)
|> > 6) Restart your PC and perform a "final" Full Scan
|> of your platform using the three
|> utilities; Trend Sysclean, Stinger and
|> Adaware
|> > 7) If you are using WinME or WinXP, Re-enable
|> System
|> Restore and re-apply any
|> > System Restore preferences, (e.g. HD space to
|> use suggested 400 ~ 600MB),
|> > 8) Reboot your PC.
|> > 9) If you are using WinME or WinXP, create a new
|> Restore point
|> >
|> >
|> > * * * Please report your results ! * * *

Re: Virus that causes a lot of traffic ?

microsoft.public.win2000.general: Re: Virus that causes a lot of traffic ?

|>|>
|>|>Dave
|>|>
|>|>
|>|>
|>|>
|>|>
|>|>
|>|>
|>|>"Paul fpvt2" <anonymous@discussions.microsoft.com>
|>| wrote
|>| in message
|>|>news:0ac601c4d49b\$07adda30\$a501280a@phx.gbl...
|>|> Recently some of our servers received many traffic
|>| that
|>|> it caused the servers to go down. We have installed
|>| SP3
|>|> for SQL Server 2000, so I don't think it is related
|>| with
|>|> the W32/SQLSlammer.worm. We also installed Symantec
|>|> antivirus software in all our servers. Is there any
|>| other
|>|> viruses that would case a lot of traffic to your
|>| machine ?
|>|>
|>|> Thank you.
|>|>
|>|>
|>|>.
|>|>
|>
|>
|>.
|>