

microsoft.public.security.virus: Re: 4 Gig worth of packets sent every 12–36 hours

## Re: 4 Gig worth of packets sent every 12–36 hours

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-01/0126.html>

---

**From:** David H. Lipman (*DLipman~nospam~\_at\_Verizon.Net*)

**Date:** 01/05/05

Date: Wed, 5 Jan 2005 11:41:50 -0500

Use WallWatcher to log INCOMING and OUTGOING activity -- <http://www.wallwatcher.com/>

Make sure that the Lavasoft Adaware is Adaware SE v1.05 and its definitions are up-to-date.

1) Download the following three items...

Trend Sysclean Package

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

Latest Trend Pattern File.

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

Adaware SE (free personal version v1.05)

{ if you don't have the latest version }

<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; lpt333.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) Disable System Restore

<http://vil.nai.com/vil/SystemHelpDocs/DisableSysRestore.htm>

4) Reboot your PC into Safe Mode and shutdown as many applications as possible

5) Using both the Trend Sysclean utility 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 both the Trend Sysclean utility and Adaware

Re: 4 Gig worth of packets sent every 12–36 hours

microsoft.public.security.virus: Re: 4 Gig worth of packets sent every 12–36 hours

- 7) 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) Create a new Restore point

\* \* \* Please report your results ! \* \* \*

--

Dave

<http://www.claymania.com/removal-trojan-adware.html>

"hh" <dkblckmr@comcast.net> wrote in message news:eJf%23RR08EHA.3124@TK2MSFTNGP11.phx.gbl...

| When I bring up my network connection, the number of packets sent grows in  
| increments of 4 Gigabytes. I have windows xp home edition w/ up to date  
| Norton. I run lavasoft every so often and find nothing. I am connected via  
| a cable modem. I also use a Linksys Broadband Router. The number of  
| incoming packets seem to be very reasonable.

| This phenomenon seemed to coincide with me continually getting the  
| "Welchia\_ICMP\_Scan" attack indicated by Norton. I have seen hints around the  
| web that Norton LiveUpdate has caused this attack problem. The Norton Alert  
| says it is my IP address that is the source of the attack.

| Whats going on here? Anybody have Any ideas? I have tried 1 documented  
| fix, with no success in correcting the problem. If it is true that the  
| Norton LiveUpdate caused this...you would think that Norton would address  
| this or make a statement about it.

| Thanks,  
|  
|