

## Re: Internet Traffic

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-10/0913.html>

---

**From:** me\_siyer ([mesiyer\\_at\\_discussions.microsoft.com](mailto:mesiyer_at_discussions.microsoft.com))

**Date:** 10/21/04

Date: Wed, 20 Oct 2004 21:29:07 -0700

Hi Malke..thanks indeed. I use Norton 2003 AV and is uptodate but it isnt locating the virus. I again sat with it for almost 1 hour to find that these two files that I mentioned is now in windows Prefetch folder. This folder is located under c:\Windows\prefetch. I then dowloaded "windows xp prefetch cleaner" to get rid of it. The system was stable for some time but it didnt last much as ZA showed heavy access of internet by these two files which got blocked. Do you suggest that with NAV 2003 I can do the repair work that u suggested (like getting trend software, etc.?). I tried installing AVG and it almost got installed. But then there was a clash between NAV 2003 and i could not complete the installation. Anyways thanks for your help and hope to see your response. Gooday..

"Malke" wrote:

> *me\_siyer wrote:*

>

>> *Hi, I use Win XP, Netscape & zonealarm to connect to my DSL. I hv noticed heavy internet traffic in my pc and have found systemmgr.exe and lsasv2.exe trying to access internet, many a times. I hve blocked its access with Zone Alarm and I think it is some kind of a virus. The registry contains strings relating to these two files under current version/run and runservices as adope file manager – lsasv2.exe and systemmgr – systemmgr.exe. I followed the usual way of manually delete these strings by switching off system restore, and restart in safe mode to delete these files. I tried all possible ways means that I know but these strings still prevail and is trynig to constantly access internet, which is on the other hand is blocked by zone alarm. Can anyone help me out? As u delete these strings under safe mode, it disappears but as you restart XP it comes from no where and sitting nicely back in the registry folders. This also blocks my network service. I request you guys/gals to help me out.. thanks in advance.*

>

> *In the list of items you have on your computer, I don't see a full-featured antivirus. You need to get one, but clean up your computer first before trying to install it:*

- >
- > 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 continue your cleaning by removing other malware:
- >
- > 1) Scan in Safe Mode with current version (not earlier than 2003)
- > antivirus using updated definitions;
- > 2) remove spyware with Spybot Search & Destroy
- > ([www.safer-networking.org](http://www.safer-networking.org)) and Ad-aware ([www.lavasoftusa.com](http://www.lavasoftusa.com)). These
- > programs are free, so use them both since they complement each other.
- > You may also want to run CWShredder and HijackThis from
- > <http://aumha.org/freeware.htm>. Although CWShredder is no longer being
- > updated, it will still clean older variants of the CoolWebSearch
- > malware. If you do not have success with this, there are new removal
- > steps at [http://www.silentrunners.org/sr\\_cwsremoval.html](http://www.silentrunners.org/sr_cwsremoval.html). A combination
- > of HijackThis and About:Buster (<http://www.majorgeeks.com>) works well
- > in removing homepage hijackers. Always read the instructions before
- > running a spyware removal tool. Be sure to update these programs before
- > running, and it is a good idea to do virus/spyware scans in Safe Mode.
- > Make sure you are able to see all hidden files and extensions (View tab
- > in Folder Options);
- > 3) If you are running Windows ME or XP, you should disable/enable System
- > Restore because malware will be in the Restore Points. With ME, you
- > must disable System Restore completely. With XP, you can delete all but
- > the most recent (presumably clean) System Restore point from the More
- > Options section of Disk Cleanup (Run>cleanmgr).
- > 4) make sure you've visited Windows Update and applied all security
- > patches. Do not install driver updates from Windows Update;
- >
- > Malke

microsoft.public.security.virus: Re: Internet Traffic

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