

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/2004-12/0012.html>

From: Paul fpvt2 (*anonymous_at_discussions.microsoft.com*)

Date: 11/30/04

Date: Tue, 30 Nov 2004 06:32:14 -0800

Hi Dave,

Yesterday, our network administrator ran the Stinger and Trend Housecall (albeit not in a safe mode) on our Win2000 servers.

The following were the viruses that can not be cleaned. Do you know the best way to clean these viruses ? Do we need to reboot the machine in a safe mode, go to DOS prompt, unhide the directory and files, and delete them ?

- . Bkdr./bounce.a. It is in c:\winnt\system32\config\services.exe. Housecall can not clean it.
- . Troj SQLSpida.B. It is in c:\winnt\system32\drivers\services.exe. This is a hidden file that was only shown when when "Show all hidden files and directories" in Windows explorer was selected. Housecall can not clean it.
- . HTML_Netsky.P. It is in c:\program files\..\RYGJYXY0* Layer2 nonamefl*. In Windows explorer, even after "Show all hidden files and directories" was selected, you still can not see this directory. Housecall can not clean it.
- . IRC/Flood.ap Trojan at c:\winnt\system32\OCXDLL.EXE\DLL32NT.HLP. Stinger can not clean this file.

The following were viruses that were successfully cleaned:

- . Malware.pe_parite.a
- . malware.worm_agobot-2
- . W32/Sdbot.worm.gen.T
- . W32/Sdbot.worm.gen.R

Do you think any of the malware that were found above could cause the high bandwidth traffic on the servers ?

Thanks again in advance.

Re: Virus that causes a lot of traffic ?

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

>-----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>

>

> *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.htm>

>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

Re: Virus that causes a lot of traffic ?

