

Re: Need Help Removing SpyWare and Agobot.spoolsrv32

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-03/1193.html

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

Date: 03/14/05

Date: Mon, 14 Mar 2005 12:29:52 -0500

From: "Rona" <Rona@discussions.microsoft.com>

| Good day,

|

| I'm trying to help my Dad with a SpyWare and virus problem. He has a
| Windows XP system. Here's what I've tried so far:

|

- | (1) Disconnected PC from Internet
- | (2) Installed beta version of Microsoft Anti-Spyware software
- | (3) Disabled System Update
- | (4) Ran the Anti-Spyware program -- this identified two problematic "items"
| (Lookingfor (dialer) and Agobot.spoolsrv32). I removed each of these.
- | (5) I rebooted and re-ran the Anti-Spyware software. No problems detected.
- | (6) Re-enabled System Update
- | (7) Turned PC off, reconnected to the Internet
- | (8) Rebooted.

|

| After these steps, everything seemed fine as my Dad used the machine
| yesterday (he had turned on and off a couple of times after things were
| fixed, and no problems cropped up). This morning, the problem is back. His
| desktop is black with the Spyware message box and the Anti-Spyware software
| is flagging the Lookingfor (dialer) and Agobot.spoolsrv32 issues again.

|

| Help! Any suggestions on how to fix this problem more permanently would be
| most welcome. I can't figure out if the PC is getting reinfected by sites
| that my Dad is visiting after we cleaned it, or if it's a different problem
| in play. Thanks in Advance.

MS Anti Spware is insufficient and is not a virus removal software adequate for AGOBot worms.

Dump the contents of the IE Temporary Internet Folder cache (TIF)

start --> settings --> control panel --> internet options --> delete files

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>

Ad-aware 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; lpt492.zip

Extract the contents of the ZIP file and place the contents in the same directory as SYSCLEAN.COM .

2) Update Ad-aware with the latest definitions.

3) Disable System Restore

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

4) Reboot your PC into Safe Mode [F8 key during boot]
and shutdown as many applications as possible.

5) Using Trend Sysclean, Stinger and Ad-aware, 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) 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>