

## Re: sticky trojan

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-12/0489.html>

---

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

**Date:** 12/22/04

Date: Wed, 22 Dec 2004 06:42:45 -0500

1) Download the following two items...

Trend Sysclean Package

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

Latest Trend signature files.

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

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 signature files (pattern files) by obtaining the ZIP file.

For example; lpt313.zip

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

2) If you are using WinME or WinXP, disable System Restore

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

3) Reboot your PC into Safe Mode

4) Using the Trend Sysclean utility, perform a Full Scan of your platform and clean/delete any infectors found

5) Restart your PC and perform a "final" Full Scan of your platform

6) 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),

7) Reboot your PC.

8) If you are using WinME or WinXP, create a new Restore point

9) Please report back your results

Dave

"Li'l Roberto" <whoisit@nospam.net> wrote in message  
news:%23eIBonA6EHA.2196@TK2MSFTNGP11.phx.gbl...

| Have just come across a particularly stubborn trojan, after spending

Re: sticky trojan

microsoft.public.security.virus: Re: sticky trojan

| almost two hours in a fruitless attempt to remove it, regretablely I had  
| to format and start over. [clients insistance]

| Here are the symptoms:

| The desktop was hijacked as web page with the warning that the  
| system had been compromised and displayed a link to the following web  
| site: for a "cure" [www.topantispyware.com/overview.php?30](http://www.topantispyware.com/overview.php?30). Right  
| clicking on the "desktop" and choosing properties showed  
| C:\Windows\Web\desktop.html not the normal properties sheet.

| Panda would detect the trojan downloader.small.11.BU and heal it on each  
| reboot, but always came back with a different file name, EG  
| C:\windows\system32\jgglaaaa.dll and wisadwsfndos.exe, plus there was  
| always a file r.exe on the root of C:.

| I ran uptodate versions of FPROTDOS, sysclean, AD-Aware, Hijackthis and  
| Spybot S and D, but just couldn't remove it. Anyone come across this  
| and have a fix? for next time

| rgds

| Li'l Roberto

|  
|  
|  
|  
|  
|  
|  
|  
|  
|