

Re: Spyware

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-04/1497.html

From: Leo (*Leo_at_discussions.microsoft.com*)

Date: 04/28/05

Date: Thu, 28 Apr 2005 13:53:19 -0700

I have had good luck using Microsoft's anti spywarebeta in conjunction with Lavasoft's ad-aware. It took two or three runs to get a badly infected computer clean but did not require the skills needed for search and destroy or hijack this. good luck

leo

"Malke" wrote:

> *Stressed Tech* wrote:

>

> > *I have been seeing alot of issues with spyware. I am a desktop*

> > *support tech and the main issue is there is some sort of pop up*

> > *blocker installed and I cannot get rid of it. Anythime I try to bring*

> > *up a page that requires another instance of IE to come up it will not.*

> > *ALso it is preventing me from rolling out application to this*

> > *particular desktop. I ran ANtispyware, adaware and virusscan and it*

> > *picks up things I delete them and issue still remains.*

> > *Nothing shows up in Control Panel either. Something seems to be*

> > *preventing*

> > *pop ups and blocking anything from coming in . PLEASE HELP!*

>

> *Here are general malware removal steps. Do everything with updated tools*

> *in Safe Mode:*

>

> *First delete all Temporary and Temporary Internet Files. To do this, go*

> *to Control Panel>Internet Options>General tab. You'll see where you can*

> *delete cookies and files. For Temporary files, Start>Run cleanmgr*

> *[enter] and then:*

>

> *1) Scan in Safe Mode with current version (not earlier than 2004)*

> *antivirus using updated definitions.*

>

> *Before you remove malware, get LSPFix or WinSockFix for XP – see links*

> *below.*

>

> *2) Remove spyware with Spybot Search & Destroy and Ad-aware. These*

- > *programs are free, so use them both since they complement each other.*
- > *There is a new version of CWShredder from Intermute. I would not*
- > *install the other Intermute programs, however. Alternately, there are*
- > *CoolWebSearch malware removal steps at SilentRunners.*
- >
- > *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).*
- >
- > *If the malware remains even after you used Ad-aware and Spybot, you can*
- > *scan with HijackThis. HijackThis is an excellent tool to discover and*
- > *disable hijackers, but it requires expert skill. See below for*
- > *HijackThis links, including sites where you can post your HJT logs. A*
- > *combination of HijackThis and About:Buster works well in removing the*
- > *About:Blank homepage hijacker. Again, this is an expert tool and*
- > *novices should get help with it.*
- >
- > *3) If you are running Windows ME or XP, you should disable/enable System*
- > *Restore after the system is clean 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.*
- >
- > *5) Run a firewall.*
- >
- > *Links to help with malware:*
- >
- > *Software/Methods:*
- > *<http://www.safer-networking.org> – Spybot Search & Destroy*
- > *<http://www.lavasoftusa.com> – Ad-aware*
- > *<http://www.intermute.com/products/cwshredder.html>*
- > *<http://www.tomcoyote.com/hjt/> – HijackThis*
- > *http://www.intermute.com/spysubtract/cwshredder_download.html*
- > *http://www.silentrunners.org/sr_cwsremoval.html. – SilentRunners*
- > *<http://www.cexx.org/lspfix.htm> – Repair Winsock 2 settings after*
- > *removing spyware*
- > *<http://www.spychecker.com/program/winsockxpfix.html> – WinsockXPFix.exe*
- >
- > *HijackThis:*
- > *<http://www.aumha.org/a/hjttutor.htm> – HijackThis tutorial by Jim*
- > *Eshelman*
- > *<http://aumha.net> – forums*
- > *<http://spywarewarrior.com/viewforum.php?f=5> – Spyware Warrior HijackThis*
- > *forum*
- > *<http://www.wilderssecurity.com/>*
- > *<http://forums.tomcoyote.org/>*
- >

- > *General:*
- > <http://aumha.net> – look under "Security" for various forums
- > <http://rgharper.mvps.org/cleanit.htm>
- > <http://mvps.org/winhelp2002/unwanted.htm>
- > <http://www.aumha.org/a/parasite.htm> – The Parasite Fight
- > http://www.spywarewarrior.com/rogue_anti-spyware.htm
- >
- > *Malke*
- > --
- > *Elephant Boy Computers*
- > www.elephantboycomputers.com
- > *"Don't Panic!"*
- > *MS-MVP Windows – Shell/User*
- >