

Re: Problem with Win32.trojan.spy.agent.kb

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2008-05/msg00102.html>

- *From:* "David H. Lipman" <DLipman~nospam~@Verizon.Net>
 - *Date:* Mon, 26 May 2008 13:53:21 -0400
-

From: <David Williams>

| I just googled the virus, was led to this page, am having the exact same problem. In CA
| Yahoo Anti-Spy, the virus is called Konvoy B, with absolutely no practical removal
| instructions that can be understood. Although it could just be my computer, many
| anti-malware sites and their forums are inaccessible, as well as Notepad.exe and
| msnmsgr.exe failing on activation, immediately. AntiSpywareMaster is advertised continuously
| while surfing Firefox, even when in Safe Mode. I'll help in any ways I can, but please help
| me get this infection off of my computer. Just as well, I am running a Vista with Zone
| Alarm Security Suite with all of the newest updates.

| Again, I am posting only what I'm told by ZA.

1. Download and execute HiJack This! (HJT)

http://www.trendsecure.com/portal/en-US/threat_analytics/HJTInstall.exe

2. Disable Notepad's word wrap:

In Notepad.exe; Format --> uncheck; "Word wrap"

3. Download/run Deckard's System Scanner:

<http://www.techsupportforum.com/sectools/Deckard/dss.exe>

4. Save the scan results (Main.txt and Extra.txt)

5. And then post the contents of Main.txt and Extra.txt in your post in one of the below expert forums...

{ Please – Do NOT post the HJT and Deckard's System Scanner Logs here ! }

Forums where you can get expert advice for HiJack This! (HJT) and Deckard's System Scanner Logs.

NOTE: Registration is REQUIRED in any of the below before posting a log

Suggested primary:

<http://www.thespykiller.co.uk/index.php?board=3.0>

Re: Problem with Win32.trojan.spy.agent.kb

Suggested secondary:

<http://www.bleepingcomputer.com/forums/forum22.html>

<http://castlecops.com/forum67.html>

<http://www.malwarebytes.org/forums/index.php?showforum=7>

Suggested tertiary:

<http://www.dslreports.com/forum/cleanup>

<http://www.cybertechhelp.com/forums/forumdisplay.php?f=25>

<http://www.atribune.org/forums/index.php?showforum=9>

http://www.geekstogo.com/forum/Malware_Removal_HiJackThis_Logs_Go_Here-f37.html

<http://gladiator-antivirus.com/forum/index.php?showforum=170>

<http://forum.networktechs.com/forumdisplay.php?f=130>

<http://forums.maddoktor2.com/index.php?showforum=17>

<http://www.spywarewarrior.com/viewforum.php?f=5>

<http://forums.spywareinfo.com/index.php?showforum=18>

<http://forums.techguy.org/f54-s.html>

<http://forums.tomcoyote.org/index.php?showforum=27>

<http://forums.subratam.org/index.php?showforum=7>

<http://www.5starsupport.com/ipboard/index.php?showforum=18>

<http://aumha.net/viewforum.php?f=30>

<http://makephpbb.com/phpbb/viewforum.php?f=2>

<http://forums.techguy.org/54-security/>

<http://forums.security-central.us/forumdisplay.php?f=13>

--

Dave

<http://www.claymania.com/removal-trojan-adware.html>

Multi-AV - <http://www.pctipp.ch/downloads/dl/35905.asp>