

Dialup Lockup – HiddenFaxWindow

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-12/3540.html

From: Eric (*none_at_death.to.spammers.now*)

Date: 12/20/03

Date: Fri, 19 Dec 2003 21:33:29 -0500

This message is intended to start a thread for those that have the internet Dialup lockup and "HiddenFaxWindow" problem. This problem, as everyone who has it is aware, has proved to be more than frustrating. Perhaps by comparing various common factors, we can find a fix for it. As everyone who has this problem is very aware of, there is extremely little information to go on — either from Microsoft or elsewhere. A solution has been asked for this problem numerous times on newsgroups (do a deja search), however the answers are always the same — replies from people that think you haven't already tried the OBVIOUS or know how to do a goodle search. Until you have this problem yourself, you won't appreciate how elusive finding a solution has proved to be.

>From my searches and reading, it appears that the nature of this particular problem is somewhat widespread and common, however nobody as of yet has found a clear solution. I believe the newsgroups that I posted this to are appropriate and I wanted to ensure that it achieves maximum proliferation in case someone knows of a solution. If, for any other reason, than perhaps someone in the future will come across the solution through a deja search.

I've been working every angle I can possible think of to find a solution to this problem, but have only achieved working myself in full circles. I will describe each angle I took to find a solution. I will also note specific software installed that may be giving this problem, perhaps when others read this they will begin to see a pattern with specific programs installed.

The problem itself seems simple enough: "WinXP internet connections freezing up while using dialup modem connections"

The symptoms: internet communication locks up completely, no traffic can be received or transmitted. The dialup internet icon in the taskbar (little two terminal looking icon) no longer responds to left or right mouse clicks. Only solution is to shut down WinXP and reboot. Sometimes while shutting down, a dialogue window appears stating that "HiddenFaxWindow" can not shut down properly and must be manually ended. Regardless, after this problem occurs, during the shutdown WinXP can only make itself to the "Saving User Settings" screen and afterwards requires a physical reset. Interestingly, this problem only presents itself while using a dialup internet

connection — it doesn't present itself when only using broadband or wireless connections.

Course of action I have tried:

1. Obviously, the first thing I looked for was any fax (Microsoft or third party) software that may be giving the problem. The only third party software I had installed was "FaxTalk NetOnHold", which operates both as faxing software and a "modem on hold" software interface for my v.92 dialup modem. This, of course, was the prime suspect. However, I seem to recall having this problem before I installed FaxTalk. I did, however, completely remove FaxTalk just to ensure it wasn't the culprit. When I installed it, Norton CleanSweep monitored the installation and I used CleanSweep to remove it completely. I also hand searched the registry to ensure that no entries were left behind, along with hand searching to ensure that all directories and files associated with it were also removed. They all were. Searching through FaxTalk's support web site and also specific searches on web/usenet revealed no known problems with FaxTalk and dialup internet freezing up.
2. Next suspect was perhaps Lucent's "Modem on Hold", however I had previously uninstalled it completely and cleanly to make certain there would be no conflicts with FaxTalk. I ensured that there was nothing of it left laying around in the registry or drive.
3. With that out of the way, my next suspect was perhaps network protocols. I removed, re-installed, and ensured I had the most current TCP/IP. With wireless and broadband working fine, I didn't really think this was the problem but figured it couldn't hurt.
4. I read that WinXP's built-in firewall can sometimes cause conflicts when you have another firewall in use. I have Norton's firewall. I ensured that XP's firewall was disabled for dialup connections, but the problem continued.
5. I read on Microsoft's support web site that DirectX 9.0b causes conflicts with XP's firewall and Microsoft Instant Messenger. While I don't have Microsoft IM set to load on boot, I did check out my DirectX. I have DirectX 9.0a installed, which (based on Microsoft support knowledge base), fixed the conflict problems that DirectX 9.0b had.
6. I begin to expect malware as a possibility. I keep my virus scanner (Norton) continuously updated and frequently do full system scans. I did another full scan, regardless, and it had negative results. I also scanned completely for spyware, using Ad Aware. Nothing beyond Doubleclick cookies were found. Still not completely convinced, I even scanned it with different virus scanners and spyware scanners — thinking perhaps it might've been possible that malware could've attacked Norton or Ad Aware. To do these scans, I scanned the problem PC (laptop) over my wireless network using scanner software physically running on a different machine. No results are found.

7. More web searching leads me to start believing that the "Mofei" worm may be a possibility since some of the symptoms are similar. I see no footprint of this worm, however. Looking at the registry by hand shows no footprint related to this worm being installed, nor do any system files. The system file `/windows/system32/scardsrv32.exe` is a footprint of this worm, however it wasn't in the directory. I did have a few files in that directory that initially caught my attention (`scardsrv.exe`, `scardssp.dll`) mainly because of their file version number (ver: 5.1.2600.0 — that '2600' caught my eye), but after doing some searching against at Microsoft I discovered that these files (Microsoft Smart Card Service Manager) and the version number were legit. To be absolutely sure, I even did a checksum comparison between these files in my directory and known legit files. They checked out fine.

8. Running "Event Viewer" (`/start/Control Panel/Administration Tool/Event` few) raises a few questions. Looking at the Security Log, some questions are raised. I don't believe these are related to this specific internet freezing problem though, but they still kind of bug me. In the log, many entries have been (and continue to be) logged for unsuccessful logon attempts by an "advapi" process. Reason for unsuccessful logon attempts is "unknown user name or password". I had read that this isn't anything major to fret over and have read that this might be caused by the "Administrator" account name being changed. After installing WinXP (full scratch install), I had initially selected "Administrator" for the administrator account name during the setup process, but later changed it to a different name. I wonder if this could be why I am seeing all these log entries and if I could/should change something to clear them up. (WinXP wouldn't let me change the administrator account name back to "Administrator", it says its already in use. From what I read, the names "Administrator", "Guest", etc can't be use for account names. I suppose this holds true even if you had changed the administrator account name from "Administrator" and want to revert back to that name?) I'll hold these questions for later though.

9. Running `msinfo32.exe` raises my most alarming question. In the system history log, there are sometimes an entry for a program that is being added and then immediately removed. The syntax used when it is added is "[program].exe \install". (The "\" might have been a "/", can't remember off-hand which slash it was.) After it is added, it is immediately removed. The reason why I didn't give a name for "[program]" is because I can't using normal ASCII text here! The name of this program is about four (or five) special characters, at least two appearing as a "y" with an accent mark over it. This, of course, raises grave concern of stealthy malware somewhere. I have no idea on how to do a file search for a filename with these special characters. As far as I knew, I didn't even think a filename could contain them?

(*UPDATE*: I find the source of this mysterious entry and it is unrelated and benign.)

10. When these symptoms appear there is a SVCHOST process running at 99 percent. I tried shutting down different ervices from `services.msc` and see which are linked to that SHVHOST process. None had any effect. I also tried disabling services BEFORE symptoms appeared, but that no effect as well.

Malware seems to be one suspect at the moment, but I'm not completely convinced as the only the software I have installed from the internet has been Ad Aware. Everything else has been commercial, packaged, software. It is still possible, I admit, that malware might had found it's way in through email (although I have .exe's, components, even HTML disabled for email) or the web.

I now admit to feeling completely defeated on finding a solution.

Some software I have (and had) installed that may be common with others (read some posts that said some of these were installed on their system as well):

- Lucent's "Modem on Hold" utility for v.92 modems
- FaxTalk NetOnHold
- Microsoft Office 2000 over WinXP
- DirectX 9.0a

If we can find a solution for this, I'm sure many will be pleased -- including us!

–Eric