

Re: Start Page Attack?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2004-04/7833.htm>

From: Shenan Stanley (*news_helper_at_hushmail.com*)

Date: 04/24/04

Date: Sat, 24 Apr 2004 02:52:01 -0500

Mark wrote:

- > Please note contents of findings after running Ad Aware with the
- > latest updates. I have also done a full scan with Norton with latest
- > updates.
- >
- > Basically something is making the start page go to the start.chm file
- > as below. I have deleted the file so now I get the page not found
- > sheet.
- >
- > Strangely the browser seems to get hijacked either the second time it
- > is opened from startup or after a certain period of time there seems
- > to be something that changes it.
- >
- > Vendor: Possible Browser Hijack attempt
- > Category: Data Miner
- > Object Type: RegData
- > Size: -
- > Location: Software\Microsoft\Internet Explorer\Main "Start Page"
- > ("mk:@MSITStore:C:\WINDOWS\start.chm::start.html")
- > Last Activity: 24-04-2004
- > Risk Level Medium
- > Comment: Possible browser hijack attempt
- > Description: Possible attempt to control\redirect the browser. This
- > object refers to a "blacklisted" site.

You cannot depend on a single anti-spyware application.

Secure your system and keep it protected/updated by following these tips:

You may have spyware/adware infesting your machine, follow the appropriate section for that, making sure you use at least THREE of the tools I list to scan and clean your machine AFTER updating them. Cleaning up spyware/adware/malware usually solves home page hijackers as well.

Please Notice that if you use AOL, you should at least upgrade to 9.0 or greater before doing any of the fixes. I know you can get AOL 9.0 at almost

microsoft.public.windows.inetexplorer.ie6.browser: Re: Start Page Attack?

any convenience store, gas station, super market or other retail outlet in the world, so this should not be a problem.

Turn on that firewall...

<http://www.microsoft.com/WindowsXP/home/using/howto/homenet/icf.asp>

(It has been reported that it now works with AOL 9.0+)

Make sure you have all the updates (critical) installed from:

<http://windowsupdate.microsoft.com/>

(Scan for updates, Review and Install)

Get rid of the spy/ad/mal-ware..

(Yes – using MORE than one of these..

I recommend at least the first three. Also..

UPDATE the definitions for them before using.)

Spybot Search and Destroy

<http://www.safer-networking.net/>

Lavasoft AdAware

<http://www.lavasoft.de>

CWSShredder

<http://www.spywareinfo.com/~merijn/downloads.html>

Hijack This!

<http://mjc1.com/mirror/hjt/>

I also like "The Cleaner" and "SpywareBlaster" and "SpywareGuard".

– <http://www.moosoft.com/>

– <http://www.javacoolsoftware.com/>

The first is a PAY product, but useable for 30 days – it has found and eliminated problems in the past the others did not. The latter two are prevention mechanisms. I like SpywareGuard for those with enough processor to have something running like antivirus software – and it prevents browser hijacking quite well. SpywareBlaster is a FANTASTIC free product, I suggest getting this after you cleanup and keeping it updated as well....

And Assortment of Others:

<http://spywareinfo.com/>

After you cleanup your PC somewhat of spy/ad/mal-ware, verify your antivirus software is updated and run a full scan of your computer. If you have no antivirus software – get one NOW! Grisoft AntiVirus:

http://www.grisoft.com/us/us_dwnl_free.php

Empty your Temporary Internet Files and shrink the size it stores to about 80 to 120MB (seems to be an optimal size for the normal user)

microsoft.public.windows.inetexplorer.ie6.browser: Re: Start Page Attack?

- Open ONE copy of Internet Explorer.
- Select TOOLS -> Internet Options.
- Under the General tab in the "Temporary Internet Files" section, do the following:
 - Click on "Delete Cookies" (click OK)
 - Click on "Settings" and change the "Amount of disk space to use:" to something between 80MB and 120MB. (Betting it is MUCH larger right now.)
 - Click OK.
 - Click on "Delete Files" and select to "Delete all offline contents" (the checkbox) and click OK. (If you had a LOT, this could take 2-10 minutes or more.)
- Once it is done, click OK, close Internet Explorer
- Re-open Internet Explorer.

Uninstall any software you do not use often/ever. (If you have something installed but never use it, uninstall it.) If you go through Control Panel -> Add/Remove Programs and see things you seldom if ever use, it is to your advantage to remove it.

Also, if you are tired of Web Page Pop-Ups/Unders.. You could try the Google Toolbar.

<http://toolbar.google.com/>

Stop loading applications at logon.. run MSCONFIG and look under the startup tab for things you DON'T want to startup! Search the Internet with Google to discover what things are safe to remove and what things may even be malware infecting your computer.

Better control your email and lessen the amount of time you spend dealing with SPAM:

SpamBayes

<http://sourceforge.net/projects/spambayes/>

or

Spamihilator.

<http://www.spamihilator.com>

--
<- Shenan ->
--