

IE6 Search Hijack

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2005-02/3549.htm>

From: Sun (*valid43monthsonly_at_hotmail.com*)

Date: 02/21/05

Date: 21 Feb 2005 00:48:37 -0800

About 3 months ago (3 Nov 2004) I wrote a long post under the same subject heading, detailing my futile efforts to deal with suspected spyware/trojan in my pc, using the commonly recommended disinfection tools, such as Spybot, Adaware, CWS shredder, HijackThis, etc.

The pc with XP Pro was then always trying to send tcp packets to IP 69.29.170.37. This was then replaced by IP 64.15.205.xxx (where xxx stands for 132, 155, 180, 182, 183, 202, 240 and 241) some 2 weeks later. The sending of packets were revealed by Sygate Personal Firewall as each individual IP could be blocked, whereas the ZoneAlarm Personal lacked such feature (I learnt later that some trojans/keyloggers self-delete after pre-determined time). The sending of the tcp packets were triggered by applications such as IE, Winword, Windows Media Player, Realplayer, etc, and services such as svchost, ntoskrnl, lsass, services, csrss, etc.

After 3 months of tweaking with various settings with the help of internet resources, I finally managed to stop the sending of tcp packets to the IPs mentioned. To share my experience with others who may be similarly affected, the followings were the steps I tried:

a) Specified my ISP's DNS Servers in the Network and Internet Connections. I did this because the symptoms seemed DNS related. For those who are interested in the explanations and the exact steps involved, here is the link:

<http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/docume>

.

The tweak was not successful.

b) Adjusted Windows XP DNS Cache Settings. There is a known Windows security issue where an unauthorised DNS server might pass along invalid resource records to misdirect DNS queries. For explanations see link : <http://www.helpwithwindows.com/WindowsXP/tune-24.html>

There was no noticeable difference after the tweak.

c) Re-installed XP Service Pack 2 and all security updates.

d) Tweaked an Advanced Setting in Sygate Firewall for the svchost.exe, so that the host machine (my pc) did not act as server. Blocked all ports from ntoskrnl.exe. This improves the speed of loading of web pages in IE. Before the tweak they took ages to load.

And finally, the one that did the trick:

e) Uncheck the *Automatically detect settings* in the LAN Settings for the Internet Options. This was done after I noticed on one occasion that the status bar in IE showed briefly the message *detecting proxy setting* or something like that. Now there is no more time delay of nine seconds for the IE to load web pages at the start of every IE session. Previously, there were always three tcp packets sent to IP 64.15.205.xxx at an interval of 3 seconds between the first and second packets, and an interval of 6 seconds between the second and third packets (these are recorded in the Sygate packet log).

However, life does not end happily thereafter, there are still something left behind in my pc. If I use the nslookup command and query, say, singnet.com.sg, I will get a response:

Non-authoritative answers

Name:singnet.com.sg.Hasbani.com

Addresses: 64.15.205.132, 64.15.205.155, 64.15.205.180, 64.15.205.182, 64.15.205.183, 64.15.205.202, 64.15.205.240, 64.15.205.241.

(My LAN is provided by a SMC 5-port switch and connects to Internet through an Aztec ADSL modem and has a Hasbani Web server)

Is it possible to delete this record? If so what are the commands to be used. Grateful if those who know provide the exact syntax or point to the relevant resource.

Sun Chong Hong