

IE6 Search Hijack

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2004-11/0501.htm>

From: Sun Chong Hong (*valid43monthsonly_at_hotmail.com*)

Date: 11/03/04

Date: 3 Nov 2004 05:46:56 -0800

(Warning – readers are cautioned not to try to reach the URL mentioned in this post, especially the IP address unless they are sure of what they are doing.)

There have been many similar posts about the search hijack. In my case I noticed that my IE6 browser search behaved differently following the RuneScape Windows Client download from the Internet to play the Web-based Active X control game. Since then my pc always try to connect IP 69.26.170.37 whenever I am on line.

I am not sure if RuneScape is the cause of the problem (it has a trust certificate to show), but my Zone Alarm Personal Internet Log shows that if I deny access to programs such as Internet Explorer or Windows Explorer, the ZA log will show that access to IP 69.26.170.37:80 is denied too.

My computer had Spywareblaster installed. Scanning using resident Adaware and Spybot with latest undates produced negative results. Scanning with Antivirus Avast! (autoupdate) also revealed nothing.

Free online scans provided by Pest Petrol and F-Secure removed some trojan key loggers, adware and dialers. Further online scan using Symantec and Yahoo Antispy showed that there is nothing left, but the problem remained.

The effect of the problem is shown when I use the IE Address bar. For example, if I type uob and <enter>, I get a web page showing uob.com with links to other sites (the code appears to be java code). The address bar will show <http://uob/>.

Similarly, if I type 69.29.170.37 in the Address Bar, I will get a bogus web page called Seek2.com, again with links to other sites. Sometimes a popup message asks me whether I want to set a bogus <http://search.net> as my home page. However, if there is a legitimate address such as dbs, the correct web page will be displayed. The behavior of the search has been changed since then and I can't get

back the default.

I have try using HijackThis, removing suspicious entries without success.

CWS shredder showed nothing.

Scanning in the safe mode also turned up nothing.

Newsgroups have similar postings on the seek2.com but they are not much of a help to me.

Using WHOIS traced the IP to unknown.xeex.com. This is sometimes shown in my ZA internet log.

I have included the IP in my hosts file. But I am not sure whether it works. In any case I learned that the hosts file can be hijacked too.

I installed Sygate Personal Firewall which can block individual IP. With ZA deactivated and this IP blocked from all applications, I typed the IP in the address bar and got the message that "the message cannot be displayed....", with the status bar showing that I was in Local Intranet Zone!

If I click on the Search button, it will trigger an attempt to connect to 69.26.170.37:80 via IE, in addition to Yahoo and MSN. But at least the Search functions appear to work according to the Advanced tab in the Internet Options.

And now my Sygate Firewall Packet Log shows that practically every application that goes on line, and some window services are blocked trying to connect to 69.26.170.37. Examples are, besides IE, Avast Antivirus, WinWord, Windows Media Player, Realplayer, MSN Messenger, Spybot's TeaTimer, svchost.exe, ntoskrnl.exe, lsass.exe, services.exe, csrss.exe, etc.

By the way, my internet access is through an ADSL Ethernet modem (Aztech DSL 305E) and a SMC 5 port switch. I wonder whether these can be exploited? I am using XP Professional SP1 with all the latest updates (SP2 uninstalled because of compatibility issue).

After struggling to find a solution for over a month, I now find that my computer also tries to contact 64.15.205.xxx (svchost.exe) for no apparent reason.

Any comments would be appreciated.

Sun Chong Hong