

## Hijack??My log

**Source:**

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network\\_web/2004-06/2465.html](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network_web/2004-06/2465.html)

---

**From:** Jerry Arzin (h974483\_at\_graduate.hku.hk)

**Date:** 06/18/04

Date: 17 Jun 2004 22:55:09 -0700

From: h974483@graduate.hku.hk (Jerry Arzin)

Newsgroups: microsoft.public.windows.inetexplorer.ie6.browser

Subject: Hijack??MY LOG

NNTP-Posting-Host: 202.180.83.6

Message-ID: <33b5a863.0406172153.8afef42@posting.google.com>

ello,

My computer was hijacked by a ebook website a few days ago. Everything I clicked was connected to a search engine called www.ntsearch.com. Some of my freinds tell me that the virus was called Torjan and it was orginated from a Java Script.As my knowledge is so limited, I cannot gain any advantages from downloading and running adware, spybot and Hijack this to my computer. However, I did a scan from Hijack this and here is the log:

Logfile of HijackThis v1.97.7

Scan saved at PM 05:31:37, on 2004/6/18

Platform: Windows 98 SE (Win9x 4.10.2222A)

MSIE: Internet Explorer v6.00 SP1 (6.00.2800.1106)

Running processes:

C:\WINDOWS\SYSTEM\KERNEL32.DLL

C:\WINDOWS\SYSTEM\MSGSRV32.EXE

C:\WINDOWS\SYSTEM\MPREXE.EXE

C:\WINDOWS\SYSTEM\mmtask.tsk

C:\WINDOWS\SYSTEM\MSTASK.EXE

C:\PROGRAM FILES\NORTON INTERNET SECURITY\NISSERV.EXE

C:\WINDOWS\EXPLORER.EXE

C:\PROGRAM FILES\NORTON INTERNET SECURITY\NISUM.EXE

C:\PROGRAM FILES\NORTON INTERNET SECURITY\SYMPROXYSVC.EXE

C:\WINDOWS\SYSTEM\INTERNAT.EXE

C:\WINDOWS\TASKMON.EXE

C:\WINDOWS\SYSTEM\SYSTRAY.EXE

C:\WINDOWS\SOUNDMAN.EXE

C:\PROGRAM FILES\COMMON FILES\REAL\UPDATE\_OB\REALSCHED.EXE

C:\WINDOWS\LOADQM.EXE

C:\PROGRAM FILES\NORTON INTERNET SECURITY\IAMAPP.EXE  
C:\PROGRAM FILES\NORTON ANTIVIRUS\NAVAPW32.EXE  
C:\WINDOWS\SYSTEM\KHOOKER.EXE  
C:\WINDOWS\SYSTEM\DDHELP.EXE  
C:\PROGRAM FILES\MSN MESSENGER\MSNMMSGGR.EXE  
C:\WINDOWS\SYSTEM\WMIEXE.EXE  
C:\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE  
C:\PROGRAM FILES\COMMON FILES\REAL\UPDATE\_OB\RNATHCHK.EXE  
C:\WINDOWS\SYSTEM\RNAAPP.EXE  
C:\WINDOWS\SYSTEM\TAPISRV.EXE  
C:\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE  
C:\PROGRAM FILES\WINZIP\WINZIP32.EXE  
C:\WINDOWS\TEMP\HIJACKTHIS.EXE

O2 – BHO: (no name) – {02478D38–C3F9–4efb–9B51–7695ECA05670} –  
C:\WINDOWS\DOWNLOADED PROGRAM FILES\YCOMP5\_1\_6\_0.DLL  
O2 – BHO: (no name) – {06849E9F–C8D7–4D59–B87D–784B7D6BE0B3} –  
C:\PROGRAM FILES\ADOBE\ACROBAT 5.0\READER\ACTIVEX\ACROIEHELPER.OCX  
O2 – BHO: (no name) – {BDF3E430–B101–42AD–A544–FADC6B084872} –  
C:\Program Files\Norton AntiVirus\NavShExt.dll  
O3 – Toolbar: ????? – {8E718888–423F–11D2–876E–00A0C9082467} –  
C:\WINDOWS\SYSTEM\MSDXM.OCX  
O3 – Toolbar: Norton AntiVirus –  
{42CDD1BF–3FFB–4238–8AD1–7859DF00B1D6} – C:\Program Files\Norton  
AntiVirus\NavShExt.dll  
O3 – Toolbar: &Yahoo! Companion –  
{EF99BD32–C1FB–11D2–892F–0090271D4F88} – C:\WINDOWS\DOWNLOADED PROGRAM  
FILES\YCOMP5\_1\_6\_0.DLL  
O4 – HKLM\..\Run: [internat.exe] internat.exe  
O4 – HKLM\..\Run: [ScanRegistry] C:\WINDOWS\scanregw.exe /autorun  
O4 – HKLM\..\Run: [TaskMonitor] C:\WINDOWS\taskmon.exe  
O4 – HKLM\..\Run: [SystemTray] SysTray.Exe  
O4 – HKLM\..\Run: [LoadPowerProfile] Rundll32.exe  
powrprof.dll,LoadCurrentPwrScheme  
O4 – HKLM\..\Run: [SoundMan] SOUNDMAN.EXE  
O4 – HKLM\..\Run: [TkBellExe] C:\Program Files\Common  
Files\Real\Update\_OB\realsched.exe –osboot  
O4 – HKLM\..\Run: [LoadQM] loadqm.exe  
O4 – HKLM\..\Run: [iamapp] C:\Program Files\Norton Internet  
Security\IAMAPP.EXE  
O4 – HKLM\..\Run: [NAV Agent] C:\PROGRA~1\NORTON~1\NAVAPW32.EXE  
O4 – HKLM\..\Run: [P2P NETWORKING] C:\WINDOWS\SYSTEM\P2P  
NETWORKING\P2P NETWORKING.EXE /AUTOSTART  
O4 – HKLM\..\Run: [SiS KHooker] C:\WINDOWS\SYSTEM\khooker.exe  
O4 – HKLM\..\Run: [Mirabilis ICQ] C:\Program Files\ICQ\ICQNet.exe  
O4 – HKLM\..\RunServices: [LoadPowerProfile] Rundll32.exe  
powrprof.dll,LoadCurrentPwrScheme  
O4 – HKLM\..\RunServices: [SchedulingAgent] mstask.exe  
O4 – HKLM\..\RunServices: [ScriptBlocking] "C:\Program Files\Common  
Files\Symantec Shared\Script Blocking\SBServ.exe" –reg  
O4 – HKLM\..\RunServices: [nisserv] C:\Program Files\Norton Internet

Security\NISSERV.EXE

O4 – HKCU\..\Run: [MsnMsgr] "C:\Program Files\MSN Messenger\MsnMsgr.Exe" /background

O4 – HKCU\..\Run: [Spyware Doctor] "C:\PROGRAM FILES\SPYWARE DOCTOR\SPYDOCTOR.EXE" /Q

O4 – HKCU\..\RunOnce: [ICQ] C:\PROGRAM FILES\ICQ\ICQ.EXE –trayboot

O4 – Startup: Windows &#27284;&#26696;&#32317;&#31649;.lnk

O4 – Startup: MS–DOS &#27169;&#24335;.pif

O4 – Startup: Outlook Express.lnk

O4 – Startup: Internet Explorer.lnk

O4 – Startup: RealOne Player.lnk

O4 – Startup: Acrobat Reader 5.1.lnk

O4 – Startup: MSN Messenger 6.1.lnk

O4 – Startup: Windows Media Player.lnk

O4 – Startup: Ad–aware 6.lnk

O8 – Extra context menu item: Download with GetRight – C:\Program Files\GetRight\GRdownload.htm

O8 – Extra context menu item: Open with GetRight Browser – C:\Program Files\GetRight\GRbrowse.htm

O9 – Extra button: ICQ Pro (HKLM)

O9 – Extra 'Tools' menuitem: ICQ (HKLM)

O16 – DPF: {D27CDB6E–AE6D–11CF–96B8–444553540000} (Shockwave Flash Object) – <http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab>

O16 – DPF: {9F1C11AA–197B–4942–BA54–47A8489BB47F} (Update Class) – <http://v4.windowsupdate.microsoft.com/CAB/x86/ansi/iuctl.CAB?37689.2697800926>

O16 – DPF: {8EF27A70–DD04–11D6–B7F6–00A0C9CD5F8A} – <http://www.quikshield.com/qshsetup.exe>

O16 – DPF: {2B323CD9–50E3–11D3–9466–00A0C9700498} (Yahoo! Audio Conferencing) – <http://us.chat1.yimg.com/us.yimg.com/i/chat/applet/v45/yacscom.cab>

O16 – DPF: Yahoo! Chat – <http://us.chat1.yimg.com/us.yimg.com/i/chat/applet/c381/chat.cab>

O16 – DPF: {7D1E9C49–BD6A–11D3–87A8–009027A35D73} (Yahoo! Audio UI1) – <http://chat.yahoo.com/cab/yacsui.cab>

O16 – DPF: {EF99BD32–C1FB–11D2–892F–0090271D4F88} (&Yahoo! Companion) – [http://us.dll.yimg.com/download.companion.yahoo.com/dl/toolbar/yiebio5\\_1\\_6\\_0.cab](http://us.dll.yimg.com/download.companion.yahoo.com/dl/toolbar/yiebio5_1_6_0.cab)

---

This log is done by Spybot:

DSO Exploit: Data source object exploit

(&#30331;&#37636;&#27284;&#35722;&#26356;, fixed)

HKEY\_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1004!=W=3

--- Spybot – Search && Destroy version: 1.3 ---

2004–05–25 Includes\Cookies.sbi

2004–05–29 Includes\Dialer.sbi

2004–05–28 Includes\Hijackers.sbi

2004–05–28 Includes\Keyloggers.sbi

2004–05–28 Includes\Malware.sbi

2004–05–04 Includes\Revision.sbi

2004-04-12 Includes\Security.sbi

2004-05-28 Includes\Spybots.sbi

2004-05-28 Includes\Trojans.sbi

2004-05-12 Includes\LSP.sbi

2004-05-24 Includes\Tracks.uti

The problem is I have two systems in my computer, one is Window 98 and another is XP. For XP that was the infected one because everything I read was linked to a search website called [www.ntsearch.com](http://www.ntsearch.com) and all the chinese characters become question marks like this ??????. It is a great nuisances to me and all other users in my family. Can somebody please read this log and interpret it?

Many thanks.

--JA