

Re: MSN Hijack

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-04/0742.html>

From: Mike Burgess (winhelp2002_at_spamthis.com)

Date: 04/12/04

Date: Sun, 11 Apr 2004 21:59:26 -0400

sobyrne,

> "in regards to MSN hijacking"

Well no wonder

[O4 - HKLM\..\Run: [MSNSysRestore] C:\WINDOWS\SYSTEM\pc32.exe bg]

Restart in Safe Mode (see below) and delete "pc32.exe"

Note: it may be a hidden file, so make sure that option is enabled (see below)

Run HijackThis while in Safe Mode, and "Fix" the following:

O2 - BHO: (no name) - {CBA523B2-1906-4D14-95A2-CD8E233701C7} - (no file)

O3 - Toolbar: (no name) - {11F6B95F-0774-4B8D-8C9E-6B552CBCAD14} - (no file)

O3 - Toolbar: (no name) - {0AAF602E-72A1-45FE-BAB1-06971E07EAA2} - (no file)

O4 - HKLM\..\Run: [MSNSysRestore] C:\WINDOWS\SYSTEM\pc32.exe bg

Restart normally, make *sure* your Ad-Aware\SpyBot is properly updated as the 3 "(no file)" entries are from "I-Lookup" and should have been removed.

How to start the computer in Safe Mode (98\ME\2K\XP)

http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001052409420406?OpenDocument&src=sec_doc_nam

How To: Show hidden files

<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2002092715262339?Open&src=ent&docid=2002092514>

Mike Burgess [MVP Windows Shell\User] <http://www.mvps.org/winhelp2002/>

Blocking Spyware, Adware, Parasites, Hijackers, Trojans, with a HOSTS file

<http://www.mvps.org/winhelp2002/hosts.htm> [updated 04-09-04]

Please post replies to this Newsgroup, email address is invalid

--

"sobyrne" <anonymous@discussions.microsoft.com> wrote in message news:1b01301c41fc9\$cd3337f0\$a301280a@phx.gbl...

> Mike,

>

> I appreciate you taking the time to respond to my question
> on the discussion board in regards to MSN hijacking my
> browser. I have tried restting the browser to comcast.net

Re: MSN Hijack

microsoft.public.security: Re: MSN Hijack

> but everytime I reboot it just resets back to MSN. As I
> had stated in my earlier post I have spybot, ad-aware and
> nortons and none of them detect anything wrong but I still
> can't stop my browser from being reset to MSN. Any
> suggestions you might have would be greatly appreciated.
> Below is the log file from Hijackthis, I hope you can
> understand my frustration.
>
> Beste Regards,
>
> Steve
<snip>