

Re: Internet explorer has been "modified"

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-05/0207.html>

From: Marc A. Donges (*filter.marc.usenet-200212_at_defiant.hadiko.de*)

Date: 05/13/03

Date: Tue, 13 May 2003 05:53:56 +0200

Hi autocol!

autocol wrote:

- > *Hi guys. I use zone alarm at home as a firewall, and here at work I*
- > *can't remember exactly what we use but apparently it failed to work.*
- > *I've visited some website, either accidentally or not, I'm not sure,*
- > *but they've installed all sorts of stuff into my internet explorer. It*
- > *totally overwrote my favourites with a bunch of crap, put some foreign*
- > *toolbar in and changed my homepage, etc...*
- >
- >
- > *I've manually reset the favourites and homepage, but even if I hide*
- > *the toolbar, it's still there, in the list. This makes me worry that*
- > *perhaps they've installed a whole bunch of other stuff that I'm*
- > *unaware of, too. I've searched my computer using the freebie ad-aware,*
- > *but this hasn't removed it...*
- >
- > *Can anyone tell me if I can remove the stuff these people installed*
- > *without my permission, or do I just have to be happy with hiding the*
- > *toolbar?*

No. Your system has been compromised. The changed toolbar and bookmarks are a visible consequence of that and are probably annoying. But what is worse is that you cannot know what else has been changed. Your system could very well be in control of someone else and there is a good chance that your system can now be used to launch all sorts of attacks against other networks. That is, of course, only in addition to the (not so important) fact that your own personal data is at risk of being stolen, destroyed or maliciously modified.

Disconnect your system from the internet. You should then backup all data that cannot possibly contain malicious code (MPEG audio files, JPEG images, for instance) but **nothing** else (including the operating system, installed programs, Word Documents etc.), then erase all permanent storage of that system and reinstall from scratch. You should also install all security related patches (hotfixes, service packs etc.) for any software you are using, especially Windows and Internet Explorer and Outlook Express. You should also configure them not to execute just

comp.security.misc: Re: Internet explorer has been "modified"....

anything without asking (and restrain yourself from blindly clicking "Yes" on any available occasion). After that you can reconnect your system to other networks and restore your backed up data.

Marc

--

_ _ Marc A. Donges +49 721 6904-2130
'v' Klosterweg 28 / E110
/ \ 76131 Karlsruhe PGP-Key(RSA): 1024R/429D9719
W W <http://www.hadiko.de/~marc/marc.asc>