

Re: Crude Popups and Un-Changeable Homepage Can Someone Help? Could This Be A Virus?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-07/1981.html>

From: N. Miller (*anonymous_at_discussions.microsoft.com*)

Date: 07/30/04

Date: Thu, 29 Jul 2004 17:17:33 -0700

In article <4eee01c473ea\$8f8a8d20\$a601280a@phx.gbl>, Thea says...

> *Ive recently gone to a site, *a normal site ran by one or
> two people, it wasnt a corparation site or anything* and
> now my homepage has changed to a search engine that
> delivers a lot of pop-ups to my computer. It wont let me
> change it, and it bothers me because there was some crude
> information on the page. Ive tried going to Internet
> Properties and sites that offer you to change your page,
> but nothing works, and now it wont let my toolbar that
> has a pop-up blocker come on. Some of the pop ups are
> inapropriate and crude. Could I have a virus? My computer
> is still as fast as it used to be, and it hasnt effected
> any other part of my computer. Has this happened to
> anyone? Can someone please help.*

It is a browser hijacker. There are steps you can take, but some can be pretty extreme. Start with these two:

Ad Aware: <http://www.lavasoftusa.com/software/adaware/>
Spybot S&D: <http://www.safer-networking.org/en/index.html>

After installation, check for updates first, then run them. Spybot is the more aggressive and finds a few things which I don't consider threatening. It has a backup, though, so if you break something, just restore from the Spybot backup.

If the hijacker is one of the more insidious versions that resists cleaning by those two, try CWShredder.

<http://www.spywareinfo.com/~merijn/>

I don't think the author is keeping it current any longer. He has a real life, and CW Shredder was an unpaid side job, if I recall. Get the latest version available and try it. If you have an older CoolWebSearch variant, CWShredder will probably deal with it. But later variants, well...

This is the "heavy artillery", and your best step is to run a scan with it, and ask it for a report. Then post your report to their forum. Hijack This:

<http://www.spychecker.com/program/hijackthis.html>

I have never had to resort to this one, myself, but I keep my MSIE6 locked down tight, and only let it out on the Windows Update site, rarely, one or two others. Read the directions carefully. I don't hang out on the forums where the logs get posted; but you should be able to find a link on the site. You post your log, and, hopefully, somebody who actually knows about your hijacker will come along and assist you.

--

Norman

~Win dain a lotica, En vai tu ri, Si lo ta

~Fin dein a loluca, En dragu a sei lain

~Vi fa-ru les shutai am, En riga-lint