

Re: Help with CWS trojan

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-06/1522.html>

From: taff (taff_at_the-valleys.com)

Date: 06/22/04

Date: Tue, 22 Jun 2004 21:24:57 +0100

On Tue, 22 Jun 2004 15:03:02 -0400, "Rob Conklin"

<robconklin@worldnet.att.net> wrote:

>I find that my system keeps getting infected with the Cool Web Search trojan
>malware. Specifically, the variant that hijacks the default HOME webpage,
>and redirects to the Cool Web Search site.
>
>I have downloaded and run (and run, and re-run, again and again) the
>CWShreader program, getting the latest updates of CWShreader, closing all
>explorer windows, closing all connections, rebooting, running CWShreader
>again, etc...very meticulously. CWShreader "seems" to get rid of it, but at
>some point I get reinfected again.
>
>I am running Windows XP Professional on computer (home usage) with a dial-up
>internet connection only. I have the latest Java virtual machine. I've
>seen instructions on getting rid of Microsoft's version, but get error(s)
>when attempting to follow them, suggestive somewhat that maybe I no longer
>have MS's java stuff, (which is where the vulnerability is sometimes said to
>exist), but I don't know if I have it or not (since there is no simple tool
>to install/uninstall it...)
>
>My questions:
>
>1. does Microsoft regard the vulnerability of Windows XP to infection with
>this to be a problem for which a specific security patch should be applied?
>Does a specific patch already exist? (If so, which one?)
>
>2. In simple, clear terms, what is the vulnerability in XP leading to
>infection with CWS?
>
>3. Is there any way (preferably quite simple) to make my system
>invulnerable to this infection?
>
>4. Is this infection thought to constitute a true "back door" onto one's
>system, allowing the t