

microsoft.public.security: Re: My home page has changed to "CoolWWWSearch" variant

Re: My home page has changed to "CoolWWWSearch" variant

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-04/1878.html>

From: thejd (*thejd_at_uk2.net*)

Date: 04/27/04

Date: Tue, 27 Apr 2004 10:52:52 +0100

Good points. Im learning how to use "Process Explorer" by SysInternals, looks good.

Last night after much examination I discovered alg.exe running, but only while the WARNING pop-ups appeared from winpatrol telling me that the IE settings were being changed. alg.exe = Application Layer Gateway Service.

alg.exe turned out to be related to ICS, Internet connection sharing. Thats strange I thought, seeing as I dont use ICS, nor is it enabled.

So I "disabled" Application Layer Gateway Service from "manual" startup in "Services" and it seems to have worked!!! WinPatrol is no longer reporting IE changes and my home page is no longer being changed nor is the CWS addon helper appearing in the IE Settings.

So what is alg.exe? Accoring to MS it: "Provides support for 3rd party protocol plug-ins for Internet Connection Sharing and the Internet Connection Firewall"

Im not aware of any problems disabling this Service as yet, any other idea or comments appreciated....

Was the reason I could not clear the CWS source file because it was not resident on my PC? Did CWS hijack my internet connection (via alg.exe) to download itself again and again??

Yes I have a firewall, yes Im using a NAPT fireall router, No Im not using any file sharing, Guest acc is disabled etc etc.

Pretty scary stuff! Perhaps someone from MS would like to comment on the security alg.exe?

"N. Miller" <nsm@blackhole.aosake.net> wrote in message news:MPG.1af718c17ef0fb89989eff@msnews.microsoft.com...

> In article <ug7Gv14KEHA.3852@TK2MSFTNGP10.phx.gbl>, thejd@uk2.net says...
>

Re: My home page has changed to "CoolWWWSearch" variant

microsoft.public.security: Re: My home page has changed to "CoolWWWSearch" variant

>> *WinXP SP1 fully patched with IE security settings all at default.*
>
>> *I was running as administrator (silly) whilst surfing the internet.*
>
>> *:::My home page has changed to "CoolWWWSearch" variant.::.*
>
>> *Ive tried absolutly everything in the way of adware, trojen and virus*
>> *remove*
>> *tools including CWSredder.*
>
>> *I have even tried installing XP SP2–beta, but to no avail.*
>
>> *Where is the resident CWS file? Every few minutes WinPatrol reports the*
>> *changes to my IE settings, but is unable to stop them.*
>
>> *I try disabling (new XP SP2 feature) the "IE Helper" but it simply*
>> *returns*
>> *in to the enabled list after a few minutes.*
>>
>> *After spending 3 days on this now, I am wondering whether their is a*
>> *cure, I*
>> *am also curious that there seems to be little open debate on the MS–Home*
>> *site regarding the FACT that this trojan can infect a FULLY patched XP*
>> *OS!!!! Without me ever agreeing to a download or similar numpty activity*
>> *(other than being logged in as admin)*
>
> *Welcome to the commercial Internet, where many commercial interests*
> *believe*
> *that they own your computer. A fully patched system won't stop them. If*
> *they*
> *pop up sneaky windows, telling you that you should download a "small*
> *plugin" so your browser will work on their site, and if you click "Ok", no*
> *patches will help you. Some popups are even sneakier; they ignore your*
> *choice of "No", and install anyway, treating the "No" button click as an*
> *affirmation.*
>
> *The authors of the Cool Web Search browser hijacker are in an arms race*
> *with*
> *the spyware killers. They are trying to stay three steps ahead of the*
> *spyware removers, to make it harder for you to regain control of your*
> *computer. Remember what I said; they want to possess your computer for*
> *their*
> *ends. Maybe, if you contact the CWS people, they have recent updates, or*
> *may*
> *even be interested in finding out if yours is a new variant that they*
> *haven't seen, yet.*
>
> *I live in California. I wish that Sen. Liz Figueroa (D–Fremont) would drop*
> *her proposed legislation against Google, for their "Gmail", and pursue*
> *legislation against Cool Web Search type browser hijackers instead. Google*
> *is up front about what they intend to do; more so than Hotmail, or Yahoo!,*

Re: My home page has changed to "CoolWWWSearch" variant

microsoft.public.security: Re: My home page has changed to "CoolWWWSearch" variant

- > *which are just as significant in their privacy issues.*
- >
- > *Cool Web Search is downright sneaky and malicious.*
- >
- > --
- > *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*