

Re: CWS searchx strain won't go away

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-05/2129.html>

From: PA Bear (PABear_at_mvps.org)

Date: 05/25/04

Date: Tue, 25 May 2004 17:10:52 -0400

Here's MVP Mike Burgess' recent fix, posted in a number of forums (and in IE6 Browser and this NG).

<paste>

Ok, here goes ... this is my "How To:" (Hint: print out the below)

[Tools and files needed]

Download: "RepairAppInit.reg" (XP\2K only!)

<http://www.mvps.org/winhelp2002/RepairAppInit.reg>

Do not do anything with this file yet, it will be needed later.

Download: CWS shredder

<http://www.spywareinfo.com/~merijn/files/hijackthis.zip>

Unzip, but do not run it yet, it will be needed later.

Download: Ad-Aware

<http://www.lavasoft.de/software/adaware/>

Install, but do not run it yet, it will be needed later.

Download: Find-All.zip

<http://www.10.brinkster.com/exploit0iter/freetlast/pvtool.htm>

Unzip, but do not run it yet, it will be needed later.

Download: WINFILE.zip

<http://www.10.brinkster.com/exploit0iter/freetlast/WINFILE.zip>

Unzip, but do not run it yet, it will be needed later.

Download: Registrar Lite [freeware]

<http://www.resplendence.com/download>

Install, but do not run it yet, it will be needed later.

[Step1]

Double-click the included "Find-All.bat" file from Find-All.zip.

Generates: "output.txt"

Note: if infected you will see:

Locked file(s) found...

C:\WINDOWS\System32\

Where "<filename>" is the hidden invisible installer.

Note: "+++ File read error" is not an error, this just identifies the culprit.

[Step2]

Run "Registar Lite" and navigate to:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows]

Double click on "AppInit_DLLs" entry (right pane)

The size will likely be something other than "1" (if infected)

IMPORTANT: Make a note of the filename and location (folder)

[Step3]

Rename the highlighted "Windows" key (left pane)

To rename: Right-click and select: Rename

(type) NoWindows

Double-click "AppInit_DLLs" again (right pane)

Clear (delete) the "Value" containing the .dll and click Ok.

IMPORTANT: Rename the "NoWindows" key (left pane)

To rename: Right-click and select: Rename

(type) "Windows" (no quotes) and close RegLite.

[Step 4]

Using Windows Explorer go to your root drive: (typically) "C:\\"

Click File (up top) select: New > Folder

(type) "Junk" (no quotes)

Open Winfile

Navigate to System32 folder.

Click File (up top) select: Move

Copy and paste this into the 'From' box: C:\WINDOWS\System32\

Copy and paste this into the 'To' box: C:\Junk\

Note: where "<filename>" = culprit dll from "output.txt"

Click OK. Close Winfile

Open Windows Explorer and check in C:\Junk for the "<filename>.dll" file.

At this point see if you can rename the "<filename>.dll"

Do this several time, changing the name and extension each time.

Then see if you can "Move" to "A:\" (floppy)

[Step 5]

Re: CWS searchx strain won't go away

Locate: "RepairAppInit.reg" right-click and select: Merge
Ok the prompt

[Step 6]

Open Regedit (Start | Run (type) "regedit" (no quotes)
Use the Search function for the <filename>.dll
Click: Edit (up top) select: Find
(type) <filename>.dll, click: Find Next

Note: where "<filename>" = culprit dll from "output.txt"

Remove all instances found.Press "F3" to continue searching
until you see the "Completed" message.

Next repeat the above steps, substitute the "secondary dll"
From: "text/html" as seen in the "output.txt"

[Step 7]

Run CWShredder and reboot.

[Step 8]

Run Ad-Aware

Reconfigure Ad-Aware for Full Scan:

Please update the reference file following the instructions here:

<http://www.lavahelp.com/howto/updref/index.html>

Launch the program, and click on the Gear at the top of the start screen.

Click the "Scanning" button.

Under Drives & Folders, select "Scan within Archives".

Click "Click here to select Drives + folders" and select your installed hard
drives.

Under Memory & Registry, select all options.

Click the "Advanced" button.

Under "Log-file detail", select all options.

Click the "Tweaks" button.

Under "Scanning Engine", select the following:

"Include additional Ad-aware settings in logfile" and

"Unload recognized processes during scanning."

Under "Cleaning Engine", select the following:

"Let Windows remove files in use after reboot."

Click on 'Proceed' to save these Preferences.

Please make sure that you activate IN-DEPTH scanning before you proceed.

After the above post a fresh log ...

microsoft.public.security: Re: CWS searchx strain won't go away

```
--
Disclaimer: Renaming the "Windows" key modified some security settings.
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows]
Right-click the "Windows" key, select: Permissions
[Example]
Before renaming the "Windows" key:
"Path"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows"
"Read":
*"Administrators
*Power Users
*Users"
"Write"
*"Administrators"
--
[Example]
After Renaming the key:
"Path"
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows"
"Read":
***"Everyone"***
"Write"
*"Administrators
--
You need to check that and if 'Everyone' was added (as seen above)
You need to reset your original settings as follows:
Note: do this after removing the infection.
Right-click "Windows", select: Permissions
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows]
Click Advanced [button]
If the "inherit permissions" box is checked = Uncheck it.
Then select "COPY" on the prompt.
Select "Everyone Group" (if listed) and remove. (only the group)
You can individually view/edit each group settings.
Be sure "Administrators" and "System" have full control on all.
Note: Creator owner full control on Sub keys only.
"Power users" and "users" = "read control".
</paste>
--
HTH - Please Reply to This Thread
~Robear Dyer (PA Bear)
MS MVP-Windows (IE/OE), AH-VSOP
AumHa Forums
http://forum.aumha.org
What You Should Know About Spyware
http://www.microsoft.com/mscorp/twc/privacy/spyware.mspx
Maggie wrote:
> HELP!! I have followed the instructions below and still can't shake
> this thing. I'm wondering if I have a new strain/variant.
>
> 1. I do have the "homeoldsp=about:blank" present when I run HiJack
> this. I keep electing to fix and it keeps coming back.
>
> 2. I found the "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
> NT\CurrentVersion\Windows\AppInit_DLLs" and deleted it. When I hit F5
> it never came back but I still had the same problem (hijacked start
> page instead of about:blank). So I did a search while in regedit and
> found the AppInit_Dlls hidden elsewhere. This time I followed the
> instructions on renaming the folder, deleting, changing the name back,
> etc. I then ran AdAware 6, CWSredder, Spybot, and rebooted. My
> about:blank start page is still some bastard Search Spyware but I
> can't find AppInit_DLLs anywhere within regedit now.
```

microsoft.public.security: Re: CWS searchx strain won't go away

>
> 3. I have also run PestPatrol and keep getting nailed with "CWS -
> Hijacker" hkey_classes_root\protocols\filter\text/html. I delete
> repeatedly and it's back withing minutes. I'm assuming the two are
> related or the same. Anybody seen this thing as a variant?
>
> Thanks for the help!