

Forum:[Hack Forums](#)

Thread: [Fairly sure there's SOME type of infection.](#)

justg - November 27, 2014, 9:25 pm

Came home from college, and the desktop I usually used when I was home (Family Desktop) was running at a snail's pace. There are certain times it will run fine, and then others the usage is very choppy and slow.

I asked my mother about it, and learned that the three smaller girls we have (ages 7-10) had been on the computer a lot while I've been gone. I figured they probably downloaded something that infected the computer with some adware or malware.

Run CCleaner to clear out temporary system files, just in case it was just that. However, it gets stuck at 34% under System temp files. I stop the CCleaner scan and run a Malwarebytes scan, and find 2 Trojan's and quite a few file registry/key/value errors. I let malwarebytes handle that, run the CCleaner again, and the same thing happens.

Next I check under task manager and check for open processes. I notice that with only One tab in google chrome open that there are 98 processes, so I end a few. Even after ending a few, CPU Usage has stayed up near 100%, while physical memory in between 40 and 60.

If I run Malwarebytes now, it ALWAYS comes up with the same 5 errors - which is from the Sweetpacks Adware, which after multiple tries, I can not seem to get rid of. I also figured it couldn't be the Sweetpacks slowing this computer down and making CPU usage 100%. Also, on top of this, at least once a day there is a pop up that tells me Windows Powershell has stopped working.

Any help here guys?

Aura - November 27, 2014, 9:30 pm

Follow the instructions here :

<https://hackforums.net/showthread.php?tid=4486298>

Post the log either here or there. Give me a few to reply to it since I'm on my phone.

desynk - November 28, 2014, 1:36 am

Sounds like it's infected with Poweliks. If you are awake right now I can remove it if you pm me your TeamViewer details, otherwise you'll have to wait for tomorrow unless someone else gets to you first.

ven0m - November 28, 2014, 6:09 am

Have resolved the issue or require further assistance?

-Hyperion - November 28, 2014, 8:18 am

If you are only using MWB it will not remove it. Please follow these instructions here

<http://malwaretips.com/blogs/remove-sweetpacks-toolbar/>

justg - November 28, 2014, 10:50 am

I will be following Aura's advice when I get back to the PC later after work.

Aura - November 28, 2014, 12:43 pm

(Nov 28, 2014 11:50 AM)justg Wrote: [\[CITE\]](#) I will be following Aura's advice when I get back to the PC later after work.

That's fine with me. If ven0m's wants to jump in however, I strongly recommend you to follow his instructions over the instructions of anyone else here since he's way more qualified than me in that domain. For now, I'm good with that :smile:

justg - November 28, 2014, 1:15 pm

<http://pastebin.com/ZaYqp8zF>

That's the log.

Aura - November 28, 2014, 1:18 pm

(Nov 28, 2014 02:15 PM)justg Wrote: [\[CITE\]](#) <http://pastebin.com/ZaYqp8zF>

That's the log.

Alright let's see :Uninstall Catalina Savings Printer;

Uninstall Coupon Printer for Windows;

Uninstall Java 7 Update 67 - You'll have to install the latest version from Java.com, do not Accept the Ask Toolbar;

Uninstall Internet Explorer Toolbar 4.8 by SweetPacks;

Uninstall QuickTime;

Update Sandboxie;

Update Skype - We are on v6.22;

Uninstall Skype Click to Call;

Update WinRAR - From RARLabs, install the 64-bits version;

The Updates can wait, go with the Uninstalls.

justg - November 28, 2014, 1:42 pm

(Nov 28, 2014 02:18 PM)Aur? Wrote: [\[CITE\]](#) Alright let's see :Uninstall Catalina Savings Printer;

Uninstall Coupon Printer for Windows;

Uninstall Java 7 Update 67 - You'll have to install the latest version from Java.com, do not Accept the Ask Toolbar;

Uninstall Internet Explorer Toolbar 4.8 by SweetPacks;

Uninstall QuickTime;

Update Sandboxie;

Update Skype - We are on v6.22;

Uninstall Skype Click to Call;

Update WinRAR - From RARLabs, install the 64-bits version;

The Updates can wait, go with the Uninstalls.

Can not find the Catalina Savings Printer in "uninstall a program".

When I attempt to remove the Sweetpacks toolbar, it comes up with this:

<https://gyazo.com/1a60c5f9f84e3e7baa45d93fabf91c12>

Updated Skype and Java, decided to remove Sandboxie and WinRAR, will decide if I want them back at a later time.

Aura - November 28, 2014, 1:47 pm

(Nov 28, 2014 02:42 PM)justg Wrote: [\[CITE\]](#) Can not find the Catalina Savings Printer in "uninstall a program".

When I attempt to remove the Sweetpacks toolbar, it comes up with this:

<https://gyazo.com/1a60c5f9f84e3e7baa45d93fabf91c12>

Updated Skype and Java, decided to remove Sandboxie and WinRAR, will decide if I want them back at a later time.

Was expecting that error from Sweetpack, since the previous deletion of it's files by Malwarebytes most likely corrupted it's installation.

Do you have CCleaner (I don't remember) ?

justg - November 28, 2014, 1:49 pm

(Nov 28, 2014 02:47 PM)Aur? Wrote: [\[CITE\]](#) Was expecting that error from Sweetpack, since the previous deletion of it's files by Malwarebytes most likely corrupted it's installation.

Do you have CCleaner (I don't remember) ?

I do. I have ran it several times, and always comes up with file/registry errors (The same 5) when I run it.

Aura - November 28, 2014, 1:56 pm

(Nov 28, 2014 02:49 PM)justg Wrote: [\[CITE\]](#) I do. I have ran it several times, and always comes up with file/registry errors (The same 5) when I run it.

When you try to uninstall Sweetpack via CCleaner or when you try to start it ?

justg - November 28, 2014, 1:59 pm

(Nov 28, 2014 02:56 PM)Aur? Wrote: [\[CITE\]](#) When you try to uninstall Sweetpack via CCleaner or when you try to start it ?

When you try to Uninstall via CCleaner it just gives and error saying access is denied. When you run the cleaner it comes up with 5 Errors, all based around sweetpacks.

Aura - November 28, 2014, 2:01 pm

(Nov 28, 2014 02:59 PM)justg Wrote: [\[CITE\]](#) When you try to Uninstall via CCleaner it just gives and error saying access is denied. When you run the cleaner it comes up with 5 Errors, all based around sweetpacks.

Right-click on CCleaner and select "Run as Admin". Then try to uninstall it.

justg - November 28, 2014, 2:08 pm

(Nov 28, 2014 03:01 PM)Aur? Wrote: [\[CITE\]](#) Right-click on CCleaner and select "Run as Admin". Then try to uninstall it.
Actually updated CCleaner to the newest version while there,
However it still gives the same error as when attempting to Uninstall from the "uninstall a program" menu under windows.

Aura - November 28, 2014, 2:12 pm

(Nov 28, 2014 03:08 PM)justg Wrote: [\[CITE\]](#) Actually updated CCleaner to the newest version while there,
However it still gives the same error as when attempting to Uninstall from the "uninstall a program" menu under windows.
Alright, download the portable version of [Revo Uninstaller](#) and try to uninstall it. Set the scan type to Advanced.

desynk - November 28, 2014, 2:12 pm

While running through these steps are excellent for normal PUP's/infections and generally cleaning up and securing your system, if it truly is infected with Poweliks these steps will not help. There is a very strong indication you are infected with Poweliks. My offer for assistance still stands if the issue persists.

Aura - November 28, 2014, 2:13 pm

(Nov 28, 2014 03:12 PM)desynk Wrote: [\[CITE\]](#) While running through these steps are excellent for normal PUP's/infections and generally cleaning up and securing your system, if it truly is infected with Poweliks these steps will not help. There is a very strong indication you are infected with Poweliks. My offer for assistance still stands if the issue persists.
I didn't ignore your post, just trying to get these out of the ways first, then there's a quick scan that will allow us to detect Poweliks.

justg - November 28, 2014, 2:17 pm

(Nov 28, 2014 03:12 PM)Aur? Wrote: [\[CITE\]](#) Alright, download the portable version of [Revo Uninstaller](#) and try to uninstall it. Set the scan type to Advanced.
Gave that same error about halfway through when the application asked if I wanted to uninstall this product.

Aura - November 28, 2014, 2:18 pm

(Nov 28, 2014 03:17 PM)justg Wrote: [\[CITE\]](#) Gave that same error about halfway through when the application asked if I wanted to uninstall this product.
If you cancel the installation, does it still proceed to the scan ? If so, click "Select All" for Registry and Files/Folders and delete them.
If it doesn't, we'll move to Poweliks identification.

justg - November 28, 2014, 2:23 pm

(Nov 28, 2014 03:18 PM)Aur? Wrote: [\[CITE\]](#) If you cancel the installation, does it still proceed to the scan ? If so, click "Select All" for Registry and Files/Folders and delete them.
If it doesn't, we'll move to Poweliks identification.
It does continue and came up with 50 registry items. I have selected them all and deleted them.

It now does not appear on my "uninstall a program" list.
When I check CPU Usage now it's not at a 100% constant, but fluctuates greatly, anywhere from 6% to 97%.

Problem seems to be resolved. Closing.

