

Forum:[Hack Forums](#)

Thread: [snaware.com](#)

Vendorss - August 1, 2018, 6:31 pm

Hello, I keep getting a tab opening with "snaware com/products/facebookposterandscheduler" and it is really annoying me. Lmk.

ItsJigSaw - August 1, 2018, 6:40 pm

Best solution is to just wipe the whole HDD tbh

Anyway, first of all download an ad blocker to disable pop up ads. Then turn off your PC and start it in Safe Mode with Networking. Then when it boots just go to your web browser and remove any search engine(except google) etc. Then go to run > msconfig > startup and check every program that turns on on startup, disable everything u see suspicious. Boot PC normally, go to Task Manager and check processes, anything u see suspicious right click and go to location. Check the folder if u think thats the adware first scan it with malwarebytes and then delete/dont delete. After all of that run a full PC scan with malwarebytes and hope they didnt crypt it and it gets flagged.

Vendorss - August 1, 2018, 6:43 pm

(Aug 1, 2018 06:40 PM)ItsJigSaw Wrote: [\[CITE\]](#) Best solution is to just wipe the whole HDD tbh
Anyway, first of all download an ad blocker to disable pop up ads. Then turn off your PC and start it in Safe Mode with Networking. Then when it boots just go to your web browser and remove any search engine(except google) etc. Then go to run > msconfig > startup and check every program that turns on on startup, disable everything u see suspicious. Boot PC normally, go to Task Manager and check processes, anything u see suspicious right click and go to location. Check the folder if u think thats the adware first scan it with malwarebytes and then delete/dont delete. After all of that run a full PC scan with malwarebytes and hope they didnt crypt it and it gets flagged.
you're a funny one :D.

Yeah no. Im waiting on Sigma to hmu with fixbar. hes solved it before.
I've tried all above steps but not wiping whole hdd.

Vanilla - August 1, 2018, 6:43 pm

I had this awhile back, forgot what it was. What I do now is just reinstall windows and install all my software then backup and whenever stuff like this happens just restore the backup.

ItsJigSaw - August 1, 2018, 6:47 pm

(Aug 1, 2018 06:43 PM)Vendorss Wrote: [\[CITE\]](#) you're a funny one :D.

Yeah no. Im waiting on Sigma to hmu with fixbar. hes solved it before.
I've tried all above steps but not wiping whole hdd.

Well i cant know what u tried or u didnt try bcs u didnt specify anything. Mine was to respond with some basic virus removal stuff.

Unless u like HDD wiping u can always make a backup of your PC and problems like this are fixed super fast.

Clysic - August 1, 2018, 9:01 pm

Hey, I am pretty sure MalwareBytes/HitMan Pro can remove Snaware?

Why not try running a scan with those 2 if you haven't already? Last I remember, Snaware isn't anything crazy to remove.

(Aug 1, 2018 06:40 PM)ItsJigSaw Wrote: [\[CITE\]](#) Best solution is to just wipe the whole HDD tbh Anyway, first of all download an ad blocker to disable pop up ads. Then turn off your PC and start it in Safe Mode with Networking. Then when it boots just go to your web browser and remove any search engine(except google) etc. Then go to run > msconfig > startup and check every program that turns on on startup, disable everything u see suspicious. Boot PC normally, go to Task Manager and check processes, anything u see suspicious right click and go to location. Check the folder if u think thats the adware first scan it with malwarebytes and then delete/dont delete. After all of that run a full PC scan with malwarebytes and hope they didnt crypt it and it gets flagged.

I am pretty sure a wipe isn't even needed. It's just Ad-ware which isn't anything crazy to worry about.

Sigma - August 2, 2018, 6:30 am

I'm Sigma, I'm one of the leaders of the Security Malware Removal Team and will be assisting you throughout this thread. Before we start just take a second to read through these few requests - these are to ensure we can help you quickly and safely: Only use this thread for help. Please don't create multiple threads, accounts, PM me or post on other forums - if you do just let me know.

Only follow my guidance.

Don't run tools I haven't asked you to run. If you do just let me know so I can take that into consideration when viewing logs.

DO NOT install any other software while we are attempting to clean your machine. It can get quite confusing especially if you are downloading questionable tools.

Please be prompt in responding. I'll do my best to do so. If >48hrs has passed, please either PM me or ask "Are you there, I still need help" in this thread.

Please stick with me until I give you the 'All Clean'. I'll help you cleanup quickly and offer some tips to make you more secure and get your system running faster.

Your malware related tools will be removed. I don't support the tools often distributed on these forums. Scanners will generally remove these - I take no responsibility for any malicious software that is lost.

I (nor does the forum) support pirated software.

If you don't understand something, don't be afraid to ask - I'm here to help. ?

You'll notice the logs are pretty big and you won't be able to post a reply containing it all. Please use ONLY either: <https://hastebin.com> - here you can upload the .txt file directly. <- I prefer this.

<http://pasted.co/> - here you can set a password if you wish to protect your data. Just PM me the password.

And paste the link to the logs in your reply. Post each log separately (each with a separate link). If you're a new member and can't paste links you can fool the forums system by removing the beginning of the link.

e.g. If you can't post this: <https://hastebin.com/raw/epaduvuyic>

Post: I used hastebin, here is the ending /raw/epaduvuyic

If I request you to post an image please use a service like <https://imgur.com>

=====

Malwarebytes - Clean ModeDownload and install the free version of [Malwarebytes](#)

Note: If you have Malwarebytes already installed, you don't need to install it again. Simply start from the next bullet point

Once Malwarebytes is installed, launch it and let it update his database. You might have to click on the little arrow by Scan Status in the middle right pane for it to do so

Once the database update is complete, click on the Scan tab, then select the Threat Scan button and click on Start Scan

Let the scan run, the time required to complete the scan depends of your system and computer specs

Once the scan is complete, make sure that the first checkbox at the top is checked (which will automatically check every detected item), then click on the Quarantine Selected buttonIf it asks you to restart your computer to complete the removal, do so

Click on Export Summary after the deletion (in the bottom-left corner) and select Copy to Clipboard. Paste the content in your next reply

=====

Download the right version of [RogueKiller](#) for your Windows version (32 or 64-bit)

Once done, move the executable file to your Desktop, right-click on it and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10 users)

Click on the Start Scan button in the right panel, which will bring you to another tab, and click on it again (this time it'll be in the bottom right corner)

Wait for the scan to complete

On completion, the results will be displayed. Click on the Open Report button in the bottom left corner, followed by the Open TXT button (also in the bottom left corner)

This will open the report in Notepad. Copy/paste its content in your next reply

=====

Please read the guide [AsSaSs@iN](https://hackforums.net/showthread.php?tid=5772641) constructed here before continuing:
<https://hackforums.net/showthread.php?tid=5772641>

Post the logs in THIS THREAD

Let's get to it!

Franz Hopper - March 17, 2019, 5:03 pm

Hello, I have the same issues as you and finally, I was looking to update my GatherProxy app and I saw this:

DOWNLOAD LINK:

[www\(.\)snaware\(.\)com/download/GP/GatherProxy.rar](http://www(.)snaware(.)com/download/GP/GatherProxy.rar)

Source:

[www\(.\)gatherproxy\(.\)com/gptool](http://www(.)gatherproxy(.)com/gptool)

Reverse app:

Memory Forensics- snaware. com Domain/IP reference

12683f462645a4a152a7bc579856b0f9-60002af-GPGC~Updates

This is why we get to: l(.)snaware(.)com/l/1029577412/1047

Gatherproxy did this whitehat adware, we can declare GatherProxy as a MALWARE SITE

Link to reverse scan:

[www\(.\)reverse\(.\)it/sample/62e2f0198859120c64ecab5a0c034cff7db3b222b621f2a87c375351bdb3f26b](http://www(.)reverse(.)it/sample/62e2f0198859120c64ecab5a0c034cff7db3b222b621f2a87c375351bdb3f26b)

and:

[www\(.\)reverse\(.\)it/sample/9c1c87abf7a1fbff43007f4310f3a722ad6798ec4c42d599509c5c3e3d214284?environmentId=120](http://www(.)reverse(.)it/sample/9c1c87abf7a1fbff43007f4310f3a722ad6798ec4c42d599509c5c3e3d214284?environmentId=120)

Seems it's not detected by the most popular antivirus (Eset, avast, McAfee).

Finally, with this research, we solved this unknown adware case.

Hope a lot of people will get rid of this adware with this comment.