Instructions for Aurora removal

You don't need to reformat your computer to remove **aurora**! It only took me two hours to delete **aurora**/nail, while I was writing this guide. Reformatting takes forever, especially replacing all of your files.

Here is a list of most of the files from the **aurora** virus (If you don't know what to do with these files, see below) (If you use windows2000, replace C:\WINDOWS with C:\WINNT)

Main executables:

C:\Documents and Settings\(User Name)\Local Settings\Temp\toc_0032.exe (main installer)
C:\Documents and Settings\(User Name)\Local Settings\Temp\tp7543.exe (main installer)
C:\WINDOWS\vwzailkubk.exe
C:\WINDOWS\Nail.exe
C:\WINDOWS\tdtb.exe
C:\WINDOWS\svcproc.exe
C:\windows\system32\elitealp32.exe
C:\WINDOWS\system32\adlinstallwin32.exe
C:\adlinstallwin32.exe

These are malicious files, but I'm not positive if these are from **aurora**. Either way delete them if you have them.

C:\WINDOWS\TASKMAN.exe
C:\WINDOWS\ilaijn.exe
C:\WINDOWS\ieuninst.exe
C:\WINDOWS\Q330994.exe

delete these directories (if they exist):
C:\temporary
C:\windows\browserxtras
C:\WINDOWS\EliteToolBar

main registry directory:
HKCU\Software\aurora

The **aurora** Virus (yes, it is a virus) is a quite a pest. Many people have tried ridding themselves of it by using antimalware/virus/spyware programs to no avail. The reason for this is because **aurora** has a self duplicating, randomly named executable. This file is located in C:\windows\system32 and the name of it is six characters long (example: qwxogr.exe). The solution to this post is as follows.

I'm assuming you are computer literate and know how to use Microsofts's regedit.exe. If not, search this forum on how to use it. Some files (exes, dlls) can be hidden from regedit.exe. I suggest you use Reglite instead.

To make this process easier, follow these two steps:

1. Boot to safe mode
    a. Restart you computer
    b. Press the F8 key continuously until the Safe Mode screen appears
    c. Choose: Safe mode, with networking (If you need the references of the internet)
2. Show hidden and system files
   Start > My Computer > Tools Menu > Folder Options > View Tab
   Under the Hidden files and folders heading select Show hidden files and folders
   Uncheck the Hide protected operating system files (recommended) option

It is not necessary, but if you wish to disable the annoying popup: "Windows File Protection" (which will appear many times during this process), navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon and modify the key "SFCDisable" from 0 to ffffff9d. If you would like to turn it back on later, just change the value back to 0.

C:\Documents and Settings\(User Name)\Local Settings\Temp\toc_0032.exe could possibly be the **aurora** installer, delete this ASAP. (it could also be in your Temporary Internet Files folder)

Deleting Harmful Files

1. Clear temp dirs (temp AND temp internet files) and cookies
2. Navigate to HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run using regedit.exe or reglite (Some of the entries in this directory are required for certain programs to start when Windows starts (example: antivirus) I prefer to have only require Windows files load at startup, so I deleted these registry entries. If you wish to have the programs start when Windows does (which will take up CPU cycles and RAM) leave them there.

It will take you a while to figure out which entries are harmful, and which are not. (If you see any random numbers or letters (example: alsh2lhjasl), they are harmful. Some of the malicious processes will be masked with names that look legitimate such as "rundll32.exe". Under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run there will be some registry keys that are dlls, not exes. If you modify the key, you will see:

a. A mask (example: rundll32.exe)
b. The actual dll name to delete (located in c:\windows\system32)

3. Once you figure out which entries are harmful, right click them, select "modify" to find out where they are located.
4. After locating the files, delete them, then go back and delete the registry entries they were linked to. You must be in safe mode to delete some of the files, however, there is an alternative. Killbox will allow you to delete them in normal mode, but I will not provide instructions.
5. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. Modify key: "Shell", Remove "C:\WINDOWS\Nail.exe" from "Explorer.exe C:\WINDOWS\Nail.exe" (There is a major vulnerability in windows' registry. Many executables listed in the registry do not contain the full pathname. The registry entry could therefore be point to a "fake" explorer.exe. To fix this change the "Shell" key from: "Explorer.exe" to "C:\WINDOWS\explorer.exe" Now you know for a surety that it points to the right executable.)

The following files are on a reciprocal duplicating system (meaning, when you delete one, the other one recreates it)

C:\WINDOWS\Nail.exe
C:\Documents and Settings\(User Name)\Local Settings\Temp\toc_0032.exe (main installer)
C:\Documents and Settings\(User Name)\Local Settings\Temp\tp7543.exe (main installer)
C:\WINDOWS\system32\adlinstallwin32.exe
C:\adlinstallwin32.exe

To permanently delete these files, follow these steps:

1. Create new text document and rename it to XXXX.exe or whatever you choose.
2. copy the the name of the file (example: Nail.exe)
3. shift+delete the file
4. Rename xxxx.exe by pasting the text Nail.exe before Nail.exe remakes itself
5. Right click the new Nail.exe and click read only
6. Leave this file in place, it is not harmful, it contains no code. Confirm this by checking the size of the file. It should be 0 bytes. Repeat these steps for all five of the reciprocating files.

Delete these directories (if they exist):
C:\temporary
c:\windows\browserxtras

Delete the main **aurora** registry directory:
HKCU\Software\aurora

Once you are finished, none of these files or directories should exist:

Files:
C:\Documents and Settings\(User Name)\Local Settings\Temp\toc_0032.exe (main installer)
C:\Documents and Settings\(User Name)\Local Settings\Temp\tp7543.exe (main installer)
C:\WINDOWS\vwzailkubk.exe
C:\WINDOWS\Nail.exe
C:\WINDOWS\tdtb.exe
C:\WINDOWS\svcproc.exe
C:\windows\system32\elitealp32.exe
C:\WINDOWS\system32\adlinstallwin32.exe
C:\adlinstallwin32.exe
C:\WINDOWS\TASKMAN.exe
C:\WINDOWS\ilaijn.exe
C:\WINDOWS\ieuninst.exe
C:\WINDOWS\Q330994.exe

Directories:
C:\temporary
c:\windows\browserxtras
C:\WINDOWS\EliteToolBar

Main registry directory:
HKCU\Software\aurora

The file that Windows File Protection keeps saying was replaced was Windows Media Player. If, after you have removed all of the harmful files, WMP doesn't work run the following program: C:\Program Files\Windows Media Player\setup_wm.exe

If that doesn't update and fix WMP, then go to the Add/Remove Programs list and uninstall WMP. Once you restart your computer WMP should be reinstalled. If not insert your windows cd and install it.

Prevention
Use a secure browser: Firefox or Opera (I actually prefer Opera).
Use Spybot and Ad-aware weekly. Keep the spyware definitions updated!
Use AVG Antivirus weekly. Keep the virus definitions updated!

Teach people who use your computer how to kill popups. (Clicking "yes" on popups will download malware, but so will clicking "no". Teach them to use CTRL+SHIFT+ESC to "end task".)

Further **prevention**

This is the best guide on prevention: »www.silentrunners.org/sr_disinfection...

Conclusion

Malware sucks! Hopefully this guide has helped you destroy the crux of your dismay, which is the sadist **aurora**.

This was written by MSimcox at asatt@hotmail.com and reformatted by Condoman@snet.net from a posting on www.broadbandreports.com