LOCATING AND REMOVING BROWSER HIGHJACKERS

by: C. Hansen, http://famguardian.org

June 24, 2003

1. Run Ad-Aware 6.0 to remove common hijackers.
   1.1. Click on "Web Update", which is the globe in the upper right corner. The "Performing Webupdate…" screen will appear.
   1.2. Click on the "Connect ->" button and get the latest update.
   1.3. After the update occurs, run Ad-Aware on the system.
   1.4. When the list of problems appears, right-click and select all.
   1.5. Click on "Next" and remove all problems.
2. If the above procedure doesn't completely remove the adware, additional manual steps indicated below will be necessary.
3. Next, Clean up the Registry with Registry Editor:
   3.1. START->Run->Command
   3.2. Type in "regedit" and hit "Enter"
   3.3. The Registry Editor will appear.
   3.4. Examine the follow registry entry:
   \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   3.5. Look carefully for suspicious executables that run at startup under the above registry entry.
      3.5.1. Most often, an executable will appear in that list that is not part of your normal install, and it will typically be in the C:|\WINNT\System32\ directory.
      3.5.2. Check each item listed in the "Run" list by going to the executable file and right-clicking on it. A "Version" tab should appear on the properties page, showing the author, version, and copyright. If no Version tab appears, then it is probably a Trojan or virus or spyware.
      3.5.3. Example:
      "mcc.exe" was once found in the C:\WINNT\System32\ directory, and it had no version number. It was running at startup and installing and downloading spyware on the system. Once removed, all returned back to normal.
   3.6. Examine the Internet Explorer toolbars area of the registry at:
   \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Explorer Bars/
   3.7. Examine each entry under the "Explorer Bars" within the location at:
   \HKEY_CLASSES_ROOT\CLSID
   3.8. There should not be any entries under the "Explorer Bar", except perhaps Adobe Acrobat. Most of the time, it is safe to delete all Explorer Bars if you can't identify any other cause of the problem.
4. Run the SYSEDIT utility to look for other startup programs:
   4.1. "START->Run->Command"
   4.2. Type in "sysedit" and hit "Enter". The "Autoexec.bat", "config.sys", "win.ini", and "system.ini" files will open.
   4.3. Examine especially the "autoexec.bat" and "config.sys" files for unnecessary "*.sys" or "*.com" or "*.exe" files that load at startup. It is usually safe to delete any such entries, because they typically are not used within Windows 2000 and later.
5. If a dialog box is popping up at startup, you can run the "Spy++" program and point at the window. Then click on the Process ID to go to the process, and find out the name of the process. Then search for the executable program behind the process. Deleting the program can then help.
6. Next, check the Startup Program Group in the Start->Programs area. There should be no unusual or new programs in the list, because the programs listed will run at startup.
7. After you have done all the above, shut down the machine and bring it back up gracefully.
8. If the above steps still do not work, options remaining include:
   8.1. Go to the Lavasoft Support forum at: http://lavasoftsupport.com/. Post your question there and see who can help.
   8.2. Try another free spyware detection program.
   8.3. Do a virus scan on the machine. It may have a virus.
   8.4. Visit the Symantec security website at: http://symantec.com. See if there is a virus that might demonstrate the symptoms of the problem you are having.
9. Example: Below is a list of changes that a real-life browser hijacker instituted on my system on 6/25/04.
   9.1. "Powerreg schedulerv2.exe" added to program startup group and called from "c:\WINNT\System32\".
   9.2. "mcc.exe" added to registry at:
   \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

And called from C:\WINNT\System32\".

9.3. Extra new DLL's added to C:\WINNT\System32\
  - 9.3.1. "eken.dll"
  - 9.3.2. "jlmn.dll"
  - 9.3.3. "hlmn.dll"

9.4. Several new Explorer Bars added to Internet Explorer at the following locations:
  - 9.4.1. \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Explorer Bars\
  - 9.4.2. \HKEY_CURRENT_USER\ Software\Microsoft\Internet Explorer\Explorer Bars\
  - 9.4.3. \HKEY_USERS*\ Software\Microsoft\Internet Explorer\Explorer Bars\

9.5. "DCPPaid.exe" added to "\WINNT\System32\" at startup.

9.6. "DCPPaid.exe" added under following reg key:
\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

9.7. None of the above problems could be detected by Ad-Aware 6. The following remedies were required in the order listed:
  - 9.7.1. Run Ad-Aware 6.0 as administrator and clean everything out as much as possible. Do not reboot.
  - 9.7.2. Delete "Powerreg schedulerv2.exe" from Startup program group.
  - 9.7.3. Delete all new reg keys under the path below:
    \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - 9.7.4. Delete all added Explorer bars in registry.
  - 9.7.5. Open up Windows Explorer and search C:\WINNT\System32\ for "*.dll"
  - 9.7.6. Sort Windows Explorer window by ascending date and got to end of list. Look at brand new DLLs.
  - 9.7.7. Rename the new Trojan DLLs and then try to delete them. Those that won't delete, log off and log back in and those in the DLL cache will disappear and the others that remain which were renamed can be deleted.
  - 9.7.8. Shutdown and reboot.
  - 9.7.9. Log back in again and do an Ad-Aware 6.0 scan. It should be clean.
  - 9.7.10. Install Spyware Blaster to prevent further problems:
    http://www.javacoolsoftware.com/spywareblaster.html

9.8. Empty the recycle bin to purge all the Trojan spyware permanently.

9.9. Change permissions on normal login so that normal permissions do not include admin permissions. Under this scenario, Ad-Aware 6.0 may only be run as Administrator, because it errors out toward the end of the scan if you do it as a non-privileged user.