

Follow these removal steps to remove this **Ad-Ware** from your computer:

1. Close all open Internet Explorer windows.
2. Click Start > Run, type 'regedit', and click Ok to open the Registry editor.
3. Navigate to the following key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

In the right pane find and delete the entry named "**SurfSideKick**", "**SurfSideKick 2**" or "**SurfSideKick 3**" that points to the file "**sks.exe**".

Find and delete the entry named "**CU1**" that points to "C:\Program Files\Common Files\VCClient\VCClient.exe".

Find and delete the entry named "**CU2**" that points to " C:\Program Files\Common Files\VCClient\VCMain.exe"

4. Navigate to the following key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

In the right pane find and delete the entry named "**SurfSideKick**", "**SurfSideKick 2**" or "**SurfSideKick 3**" that points to the file "**sks.exe**".

Find and delete the entry named "**CU1**" that points to "C:\Program Files\Common Files\VCClient\VCClient.exe".

Find and delete the entry named "**CU2**" that points to " C:\Program Files\Common Files\VCClient\VCMain.exe".

5. Find and delete the following keys:

HKEY_CURRENT_USER\Software\SurfSideKick

HKEY_CLASSES_ROOT\CLSID\ {000AB005-FF12-42C2-8DF5-39E12E5F9C91}

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Surf Sidekick_is1

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\URLSearchHooks

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SurfSideKick

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\URLSearchHooks\ {000AB005-FF12-42C2-8DF5-39E12E5F9C91}

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SurfSideKick

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\URLSearchHooks\ {000AB005-FF12-42C2-8DF5-39E12E5F9C91}

6. Exit Registry Editor.
7. Delete the following directories if they exist:

C:\Program Files\SurfSideKick

C:\Program Files\SurfSideKick 2\

C:\Program Files\SurfSideKick 3\

C:\Program Files\Common Files\VCClient\

8. Search for and delete the following files (if exist):

Ssknwrddll

Ssk.log

SskUpdater.exe

SskCore.dll



First make a folder In C:\ & call it BFU then

please download BFU from

http://www.majorgeeks.com/Brute_Forc...BFU_d4714.html

and save it to the folder you have just made
Open the folder & double click BFU.exe to run it

Run the program and click the Web button.

Use this URL below and copy it into the address bar of the Download script window:

<http://metallica.geekstogo.com/alcanshorty.bfu>

Execute the script by clicking the Execute button.
Note that you should see a progress bar while the script is being executed.

If you have any questions about the use of BFU please read here:
<http://metallica.geekstogo.com/BFUinstructions.html>

Download the pocket killbox

<http://www.bleepingcomputer.com/files/killbox.php>

Please download WebRoot SpySweeper from HERE (It's a 2 week trial):

<http://www.webroot.com/consumer/prod...de=af1&rc=4129>

- * Click the Free Trial link under "Downloads/SpySweeper" to download the program.
- * Install it. Once the program is installed, it will open.
- * It will prompt you to update to the latest definitions, click Yes.
- * Once the definitions are installed, click Options on the left side.
- * Click the Sweep Options tab.
- * Under What to Sweep please put a check next to the following:
 -
 - Sweep Memory

- o Sweep Registry
- o Sweep Cookies
- o Sweep All User Accounts
- o Enable Direct Disk Sweeping
- o Sweep Contents of Compressed Files
- o Sweep for Rootkits
- o Please UNCHECK Do not Sweep System Restore Folder.
- * Click Sweep Now on the left side.
- * Click the Start button.
- * When it's done scanning, click the Next button.
- * Make sure everything has a check next to it, then click the Next button.
- * It will remove all of the items found.
- * Click Session Log in the upper right corner, copy everything in that window.
- * Click the Summary tab and click Finish.
- * Paste the contents of the session log you copied into your next reply.

After running spysweeper run these scans!

- * Download the trial version of Ewido Security Suite here

<http://www.ewido.net/en/>

- * Install ewido.
- * During the installation, under "Additional Options" uncheck "Install background guard" and "Install scan via context menu".
- * Launch ewido
- * It will prompt you to update click the OK button and it will go to the main screen
- * On the left side of the main screen click update
- * Click on Start and let it update.
- * DO NOT run a scan yet. You will do that later in safe mode.

- * Click here to download ATF Cleaner by Atribune and save it to your desktop.

http://majorgeeks.com/ATF_Cleaner_d4949.html

- * Double-click ATF-Cleaner.exe to run the program.
- * Under Main choose: Select All
- * Click the Empty Selected button.
- o If you use Firefox:
 - + Click Firefox at the top and choose: Select All
 - + Click the Empty Selected button.
 - + NOTE: If you would like to keep your saved passwords, please click No at the prompt.
- o If you use Opera:
 - + Click Opera at the top and choose: Select All
 - + Click the Empty Selected button.
 - + NOTE: If you would like to keep your saved passwords, please click No at the prompt.
- * Click Exit on the Main menu to close the program.

* Click here for info on how to boot to safe mode if you don't already know how.

http://service1.symantec.com/SUPPORT...rc=sec_doc_nam

* Now copy these instructions to notepad and save them to your desktop. You will need them to refer to in safe mode.

* Restart your computer into safe mode now. Perform the following steps in safe mode:

have hijack this fix these entries. close all browsers and programmes before clicking FIX.

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = about:blank
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar = about:blank
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page =
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant = about:blank
R3 - URLSearchHook: (no name) - {02EE5B04-F144-47BB-83FB-A60BD91B74A9} - C:\Program Files\SurfSideKick 3\SskBho.dll
O3 - Toolbar: &Google - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - blank (file missing)
O4 - HKLM\..\Run: [AutoTKit] C:\hp\bin\AUTOTKIT.EXE
O4 - HKLM\..\Run: [Recguard] C:\WINDOWS\SMINST\RECGUARD.EXE
O4 - HKLM\..\Run: [keyboard] C:\windows\keyboard11.exe
O4 - HKLM\..\Run: [mousepad] C:\windows\mousepad11.exe
O4 - HKLM\..\Run: [newname] C:\windows\newname11.exe
O4 - HKLM\..\Run: [webHancer Survey Companion] C:\Program Files\webHancer\Programs\whsurvey.exe
O4 - HKLM\..\Run: [SurfSideKick 3] C:\Program Files\SurfSideKick 3\Ssk.exe
O4 - HKCU\..\Run: [MessengerPlus3] "" /WinStart
O4 - HKCU\..\Run: [Notn] "C:\WINDOWS\WNSXS~1\wuauclt.exe" -vt mt
O4 - HKCU\..\Run: [Jjl] C:\WINDOWS\system32\?icrosoft.NET\winpool.exe
O4 - HKCU\..\Run: [rfmf] C:\PROGRA~1\COMMON~1\rfmf\rfmf.exe
O4 - HKCU\..\Run: [SurfSideKick 3] C:\Program Files\SurfSideKick 3\Ssk.exe
O20 - AppInit_DLLs: repairs303169572.dll
O20 - Winlogon Notify: igfxcui - C:\WINDOWS\SYSTEM32\igfxsrv.dll
O20 - Winlogon Notify: SideBySide - C:\WINDOWS\system32\rZsadhlp.dll (file missing)
O20 - Winlogon Notify: winrkq32 - C:\WINDOWS\SYSTEM32\winrkq32.dll

Double-click on Killbox.exe to run it. Now put a tick by Standard File Kill. In the Full Path of File to Delete box, copy and paste each of the following lines one at a time then click on the button that has the red circle with the X in the middle after you enter each file. It will ask for confirmation to delete the file. Click Yes. Continue with that same procedure until you have copied and pasted all of these in the Paste Full Path of File to Delete box.

Note: It is possible that Killbox will tell you that one or more files do not exist. If that happens, just continue on with all the files. Be sure you don't miss any.

C:\Program Files\SurfSideKick 3\SskBho.dll
C:\Program Files\SurfSideKick 3
C:\WINDOWS\SMINST\RECGUARD.EXE
C:\windows\keyboard11.exe
C:\windows\mousepad11.exe
C:\windows\newname11.exe
C:\Program Files\webHancer\Programs\whsurvey.exe
C:\Program Files\webHancer
C:\Program Files\SurfSideKick 3\Ssk.exe
C:\WINDOWS\WNSXS~1\wuauclt.exe
C:\WINDOWS\system32\?icrosoft.NET\winpool.exe
C:\PROGRA~1\COMMON~1\rfmf\rfmf.exe
C:\PROGRA~1\COMMON~1\rfmf
C:\Program Files\SurfSideKick 3\Ssk.exe
C:\WINDOWS\SYSTEM32\winrkq32.dll

* Run Ewido:

- * Click on scanner
- * Click Complete System Scan and the scan will begin.
- * During the scan it will prompt you to clean files, click OK
- * When the scan is finished, look at the bottom of the screen and click the Save report button.
- * Save the report to your desktop

reboot to normal mode and run a few online scans!

Run ActiveScan online [virus](#) scan here

<http://www.pandasoftware.com/products/activescan.htm>

When the scan is finished, anything that it cannot clean have it delete it. Make a note of the file location of anything that cannot be deleted so you can delete it yourself.

- Save the results from the scan!

post another hijack this log, the ewido, spysweeper and active scan logs



- [How to use HijackThis to remove Browser Hijackers & Spyware](#)

Symptoms in a HijackThis Log (Maybe different entries but will contain the same domains and hostnames):

R3 - URLSearchHook: (no name) - {000AB005-FF12-42C2-8DF5-39E12E5F9C91} - C:\Program Files\SurfSideKick\SskBho.dll

O4 - HKLM\..\Run: [SurfSideKick] C:\Program Files\SurfSideKick\Ssk.exe

O4 - HKCU\..\Run: [SurfSideKick] C:\Program Files\SurfSideKick\Ssk.exe

O4 - HKLM\..\Run: [SurfSideKick 3] C:\Program Files\SurfSideKick 3\Ssk.exe

O4 - HKCU\..\Run: [CU1] C:\Program Files\Common Files\VCClient\VCClient.exe

O4 - HKCU\..\Run: [CU2] C:\Program Files\Common Files\VCClient\VCMain.exe

O20 - AppInit_DLLs: repairs.dll

O20 - AppInit_DLLs: repairs302972943.dll

Removal Instructions:

1. [Download](#) HijackThis from the above link and extract it to c:\hijackthis.
2. Print out these instructions.
3. Close Internet Explorer and keep it closed throughout the entire removal process.
4. Enter the control panel by clicking on the **Start** menu, then clicking on **Run**.
5. Now type **control** in the **Open** field and press the **OK** button.
6. Double-click on the **Add/Remove Programs** icon.
7. Look for and uninstall the following entries if found in the **Add/Remove Programs** window.

Surf Sidekick
Surf Sidekick 2
Surf Sidekick 3

It may prompt about whether or not you are sure you want to remove this program. Reply **Yes** to this prompt. It will then uninstall the program.

If there is no **Add/Remove Programs** entry for this programs, click on **Start**, then **Run** and type the followin in the **Open:** field:

C:\Program Files\SurfSideKick 3\Ssk.exe /u

and press the **OK** button. A code will be displayed that it will ask you to enter. Enter this code and reboot.

Once back to your desktop continue with the rest of the fix.

8. Navigate to the c:\hijackthis directory and double-click on HijackThis

9. When the program starts, double-click on the HijackThis icon and then click on the **Scan** button.

10. Put a checkmark next to the following entries if they exist:

R3 - URLSearchHook: (no name) - {000AB005-FF12-42C2-8DF5-39E12E5F9C91} - (no file)

R3 - URLSearchHook: (no name) - {000AB005-FF12-42C2-8DF5-39E12E5F9C91} - C:\Program Files\SurfSideKick\SskBho.dll

O4 - HKLM\..\Run: [SurfSideKick] C:\Program Files\SurfSideKick\Ssk.exe

O4 - HKCU\..\Run: [SurfSideKick] C:\Program Files\SurfSideKick\Ssk.exe

O4 - HKLM\..\Run: [SurfSideKick 3] C:\Program Files\SurfSideKick 3\Ssk.exe

O4 - HKCU\..\Run: [CU1] C:\Program Files\Common Files\VCClient\VCClient.exe

O4 - HKCU\..\Run: [CU2] C:\Program Files\Common Files\VCClient\VCMain.exe

O20 - AppInit_DLLs: repairs.dll

O20 - AppInit_DLLs: repairs302972943.dll

11. Then click the **Fix** button

12. Exit HijackThis.

13. Reboot your computer

14. Delete the following directories if they exist:

C:\PROGRAM FILES\SurfSideKick

C:\Program Files\SurfSideKick 3

C:\Program Files\Common Files\VCClient

15. Search for the following files and if found delete them:

Sskknwrd.dll

Ssk.log

SskUpdater.exe

Ssk.exe