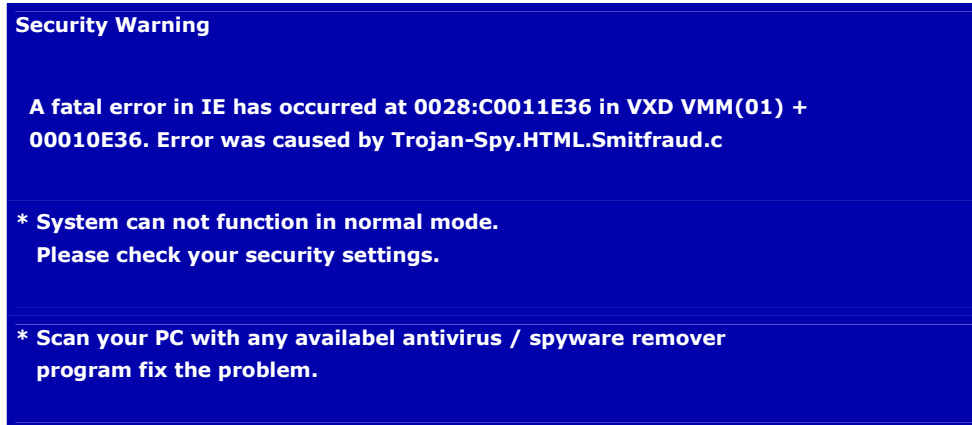


What this program does:

These infections change your desktop to say an alert which acts as a goad to use the antispyware software it installs (usually Security iGuard) and disables the screens that allow you to change your desktop. They also hijack your Internet Explorer start page, produce popups, and hijack search queries at popular search engines.



Smitfraud Desktop Background

Tools Needed for this fix:

- [HijackThis](#)
- [Killbox](#)
- [Smitfraud.reg](#)
- [Hoster](#)
- [Deldomains.inf](#)
- [Cleanup!](#)
- [Ewido Security Suite](#)
- [ActiveScan](#)

Symptoms in a HijackThis Log:

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
http://www.quicknavigate.com/search.php?qq=%1

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar = http://www.quicknavigate.com/bar.html

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
http://www.quicknavigate.com/search.php?qq=%1

R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
http://www.quicknavigate.com/search.php?qq=%1

R1 - HKCU\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
http://www.quicknavigate.com/search.php?qq=%1

R1 - HKCU\Software\Microsoft\Internet Explorer\SearchURL,(Default) =
http://www.quicknavigate.com/search.php?qq=%1

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Local Page =http://www.quicknavigate.com/

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = about:blank

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
http://www.startsearches.net/search.php?qq=%1

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar = http://www.startsearches.net/bar.html

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
http://www.startsearches.net/search.php?qq=%1

R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
http://www.startsearches.net/search.php?qq=%1

R1 - HKCU\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
http://www.startsearches.net/search.php?qq=%1

R1 - HKCU\Software\Microsoft\Internet Explorer\SearchURL,(Default) =
http://www.startsearches.net/search.php?qq=%1

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Local Page = http://www.startsearches.net/

O2 - BHO: VMHomepage Class - {FFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF} -
C:\WINDOWS\System32\hp6DD8.tmp

O4 - HKCU\..\Run: [WindowsFY] c:\wp.exe

O4 - HKCU\..\Run: [WindowsFY] c:\bsw.exe

O4 - HKLM\..\Run: [WindowsFZ] C:\WINDOWS\ZLOADER3.EXE

O4 - HKLM\..\Run: [Security iGuard] C:\Program Files\Security iGuard\Security iGuard.exe

O9 - Extra button: Microsoft AntiSpyware helper - {D5BC2651-6A61-4542-BF7D-84D42228772C} -
C:\WINDOWS\System32\wldr.dll

O9 - Extra 'Tools' menuitem: Microsoft AntiSpyware helper - {D5BC2651-6A61-4542-BF7D-84D42228772C} -
C:\WINDOWS\System32\wldr.dll

O9 - Extra button: Microsoft AntiSpyware helper - {D5BC2651-6A61-4542-BF7D-84D42228772C} -
C:\WINDOWS\System32\wldr.dll (HKCU)

O9 - Extra 'Tools' menuitem: Microsoft AntiSpyware helper - {D5BC2651-6A61-4542-BF7D-84D42228772C} -
C:\WINDOWS\System32\wldr.dll (HKCU)

Note: Not all these O4 entries may be present. The O2 entry may have a different name but will start with hp.

Removal Instructions:

Update: There is now an automated tool, created by noahdfear, that can get rid of most variations of these infections. Please attempt this method first and only attempt Method 2 if this fails.

Method 1 Instructions:

1. Print out these instructions as we will need to shutdown every window that is open later in the fix.
2. Download [HijackThis](#) and save it to your C:\ folder. Extract the hijackthis.zip file to c:\hijackthis. We will use this program later.
3. Download [smitRem.exe](#) and save the file to your desktop.
4. Double click on the file to extract it to c:\smitrem.
5. Place a shortcut to [Panda ActiveScan](#) on your desktop.

6. Please download the trial version of Ewido Security Suite here: <http://www.ewido.net/en/download/>
7. Please read [Ewido Setup Instructions](#)
8. Install Ewido, and update the definitions to the newest files. Do **NOT** run a scan yet.
9. If you have not already installed Ad-Aware SE 1.06, follow these download and setup instructions, otherwise, check for updates:

[Ad-Aware SE Setup](#)

Don't run it yet!

10. Next, please reboot your computer in [SafeMode](#) by doing the following:
 1. Restart your computer
 2. After hearing your computer beep once during startup, but before the Windows icon appears, press F8.
 3. Instead of Windows loading as normal, a menu should appear
 4. Select the first option, to run Windows in Safe Mode.
11. When your computer has started in safe mode and you see the desktop, close all open Windows.
12. Now navigate to the folder that you extracted HijackThis to in an earlier step and double-click on HijackThis.exe.
13. When the program, press the **Scan** button has started put a checkmark next to each of these entries if they are present:

**R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
http://www.quicknavigate.com/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar =
http://www.quicknavigate.com/bar.html**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
http://www.quicknavigate.com/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
http://www.quicknavigate.com/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
http://www.quicknavigate.com/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\SearchURL,(Default) =
http://www.quicknavigate.com/search.php?qq=%1**

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Local Page =http://www.quicknavigate.com/

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = about:blank

**R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
http://www.startsearches.net/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar =
http://www.startsearches.net/bar.html**

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
http://www.startsearches.net/search.php?qq=%1

R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
http://www.startsearches.net/search.php?qq=%1

R1 - HKCU\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
http://www.startsearches.net/search.php?qq=%1

R1 - HKCU\Software\Microsoft\Internet Explorer\SearchURL,(Default) =
http://www.startsearches.net/search.php?qq=%1

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Local Page = http://www.startsearches.net/

O2 - BHO: VMHomepage Class - {FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFFF} -
C:\WINDOWS\System32\hp6DD8.tmp

O4 - HKCU\..\Run: [WindowsFY] c:\wp.exe

O4 - HKCU\..\Run: [WindowsFY] c:\bsw.exe

O4 - HKLM\..\Run: [WindowsFZ] C:\WINDOWS\ZLOADER3.EXE

O4 - HKLM\..\Run: [Security iGuard] C:\Program Files\Security iGuard\Security iGuard.exe

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

O4 - HKCU\..\Run: [Windows installer] C:\wininstall.exe

O4 - HKLM\..\Run: [AntivirusGold] C:\Program Files\AntivirusGold\AntivirusGold.exe /h

O4 - HKCU\..\Run: [Intel system tool] C:\WINDOWS\System32\winnook.exe

O4 - HKCU\..\Run: [Intel system tool] C:\WINDOWS\System32\hookdump.exe

O4 - HKLM\..\Run: [AdwareDelete] C:\Program Files\AdwareDelete\adwaredelete.exe /h

O4 - HKLM\..\Run: [Daily Weather Forecast] C:\Program Files\Daily Weather Forecast\weather.exe

O9 - Extra button: Microsoft AntiSpyware helper - {D5BC2651-6A61-4542-BF7D-84D42228772C} -
C:\WINDOWS\System32\wldr.dll

O9 - Extra 'Tools' menuitem: Microsoft AntiSpyware helper - {D5BC2651-6A61-4542-BF7D-
84D42228772C} - C:\WINDOWS\System32\wldr.dll

O9 - Extra button: Microsoft AntiSpyware helper - {D5BC2651-6A61-4542-BF7D-84D42228772C} -
C:\WINDOWS\System32\wldr.dll (HKCU)

O9 - Extra 'Tools' menuitem: Microsoft AntiSpyware helper - {D5BC2651-6A61-4542-BF7D-
84D42228772C} - C:\WINDOWS\System32\wldr.dll (HKCU)

14. Once you have put a checkmark in each of the above entries, press the Fix button, and then close HijackThis.
15. Open the **c:\smitrem** folder and double click the **RunThis.bat** file to start the tool.
16. Follow the prompts on screen and wait for the tool to complete and disk cleanup to finish.
17. When the tool is finished, it will will create a log named smitfiles.txt in the root of your drive, eg; Local Disk C: or the partition where your operating system is installed. Examining that log should show that the infection was cleaned.
18. Open Ad-aware and do a full scan. Remove all it finds.
19. Run Ewido:
 - o Click on scanner

- Click on Complete System Scan and the scan will begin.

NOTE: During some scans with ewido it is finding cases of false positives.

- You will need to step through the process of cleaning files one-by-one.
- If ewido detects a file you KNOW to be legitimate, select none as the action.
- DO NOT select "Perform action on all infections"
- If you are unsure of any entry found select none for now.
- When the scan is finished, click the Save report button at the bottom of the screen.

20. Close Ewido

21. Next go to **Control Panel** click Display > Desktop > Customize Desktop > Web > Uncheck "**Security Info**" if present.

22. Reboot back into Windows and click the Panda ActiveScan shortcut, then do a full system scan. Make sure the **autoclean** box is checked!

You should now be clean of the Smitfraud infection.

Removal Method 2:

In order to remove this infection we will need to use HijackThis to manually remove the infection:

1. Print out these instructions as we will need to shutdown every window that is open later in the fix.
2. Download **HijackThis** and save it to your **C:** folder. Extract the hijackthis.zip file to **c:\hijackthis**. We will use this program later.
3. Enter the Windows Control Panel and double-click on **Add/Remove Programs**.
4. When the installed programs list appears, double-click on the following entries if they exists and allow them to uninstall.

Security IGuard

Virtual Maid

Search Maid

PSGuard

Then exit the Add/Remove Programs screen and the Control Panel.

5. Right-click: **HERE** and select **Save As** (in Internet Explorer it's labeled **Save Target As**) in order to download the Smitfraud.reg file. Save this file to your desktop.

Locate the **smitfraud.reg** file on your desktop and double-click it. When asked if you want to merge with the

registry, click the **YES** button. Wait for the "**merged successfully**" prompt then follow the rest of the instructions below.

6. Configure your computer so you can see all hidden files.

[How to see hidden files in Windows](#)

7. Download the **[Killbox by Option^Explicit](#)** and save it to your desktop. Extract killbox.zip to your desktop. Then double-click on the **killbox.exe** program.
8. When the program is open, select the option labeled **Delete on reboot**.
9. **Do not** close killbox, and open open notepad, by clicking on **Start**, then **Run**, and typing **notepad.exe** and pressing the **OK** button.
10. When notepad is open, copy and paste the following bolded text into the notepad screen. You do this by highlighting each of the below bolded filenames and then pressing **Control-C** on your keyboard. Then click on the open notepad windows and press **Control-V** to paste the contents into the notepad.

C:\wp.exe
C:\wp.bmp
C:\bsw.exe
C:\Windows\sites.ini
C:\Windows\popuper.exe
C:\Windows\zloader3.exe
C:\Windows\system32\wp.bmp
C:\Windows\System32\hhk.dll
C:\Windows\System32\wldr.dll
C:\Windows\System32\helper.exe
C:\Windows\System32\intmon.exe
C:\Windows\System32\shnlog.exe
C:\Windows\system32\perfci.ini
C:\Windows\System32\intmonp.exe
C:\Windows\System32\msmsgs.exe
C:\Windows\system32\msole32.exe
C:\Windows\System32\ole32vbs.exe
C:\WINDOWS\system32\oleadm.dll
C:\WINDOWS\system32\oleadm32.dll

11. Return to Killbox, go to the **File** menu and select **Paste from Clipboard**.
12. Still in Killbox, click the red-and-white **Delete File** button. Click **Yes** at the Delete on Reboot prompt. Click No at the Pending Operations prompt.

If your computer does not restart automatically, please restart it manually.

13. While your computer is restarting, tap the F8 key continually until a menu appears. Use your up arrow key to highlight **Safe Mode**, then press the enter button on your keyboard.
14. Using **Windows Explorer**, delete the following files, if found, (**please do NOT try to find them by "search" because they will not show up that way**)
 FOLDERS to delete (in bold) if found:
 C:\Program Files**Search Maid**
 C:\Program Files**Virtual Maid**
 C:\Windows\System32**Log Files**
 C:\Program Files**Security IGuard**
 C:\Program Files**PSGuard**
15. While still in Safe Mode, do the following:
 Make sure all programs and windows are closed. Double-click on **C:\hijackthis\hijackthis.exe** that you had downloaded and extracted earlier. When the program starts place a check next to each of the following bolded entries, if found, then click **FIX CHECKED** button.

**R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
 http://www.quicknavigate.com/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar =
 http://www.quicknavigate.com/bar.html**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
 http://www.quicknavigate.com/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
 http://www.quicknavigate.com/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
 http://www.quicknavigate.com/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\SearchURL,(Default) =
 http://www.quicknavigate.com/search.php?qq=%1**

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Local Page =http://www.quicknavigate.com/

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = about:blank

**R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
 http://www.startsearches.net/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar =
 http://www.startsearches.net/bar.html**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
 http://www.startsearches.net/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
 http://www.startsearches.net/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
 http://www.startsearches.net/search.php?qq=%1**

**R1 - HKCU\Software\Microsoft\Internet Explorer\SearchURL,(Default) =
 http://www.startsearches.net/search.php?qq=%1**

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Local Page = http://www.startsearches.net/

**O2 - BHO: VMHomepage Class - {FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFFF} -
 C:\WINDOWS\System32\hp6DD8.tmp**

- O4 - HKCU\..\Run: [WindowsFY] c:\wp.exe
- O4 - HKCU\..\Run: [WindowsFY] c:\bsw.exe
- O4 - HKLM\..\Run: [WindowsFZ] C:\WINDOWS\ZLOADER3.EXE
- O4 - HKLM\..\Run: [Security iGuard] C:\Program Files\Security iGuard\Security iGuard.exe
- O4 - HKLM\..\Run: [PSGuard] C:\Program Files\PSGuard\PSGuard.exe
- O9 - Extra button: Microsoft AntiSpyware helper - {D5BC2651-6A61-4542-BF7D-84D42228772C} - C:\WINDOWS\System32\wldr.dll
- O9 - Extra 'Tools' menuitem: Microsoft AntiSpyware helper - {D5BC2651-6A61-4542-BF7D-84D42228772C} - C:\WINDOWS\System32\wldr.dll
- O9 - Extra button: Microsoft AntiSpyware helper - {D5BC2651-6A61-4542-BF7D-84D42228772C} - C:\WINDOWS\System32\wldr.dll (HKCU)
- O9 - Extra 'Tools' menuitem: Microsoft AntiSpyware helper - {D5BC2651-6A61-4542-BF7D-84D42228772C} - C:\WINDOWS\System32\wldr.dll (HKCU)

16. When it is done fixing the entries, exit the HijackThis program and restart your computer so its back into normal mode.
17. Download [The Hoster](#) and run **hoster.exe**. Press the **Restore Original Hosts** button and then press the press **OK** button. When it is done, exit the program.
18. Right-Click [HERE](#) and select **Save As** to download DelDomains.inf to your desktop.
19. Now **RIGHT-CLICK** on the **DelDomains.inf** file on your desktop and select the **Install** option.

Note: This will remove all entries in the "Trusted Zone" and "Ranges" also.

20. Download, install, and run [CleanUp!](#)
21. Run this online virus scan [ActiveScan](#) to clean up any left over traces of these infections.
22. Follow the steps here:

[Simple and easy ways to keep your computer safe and secure on the Internet](#)

Your computer should now be free of the Smitfraud / Quicknavigate / VirtualMaid infections.

Important Note:

This infection tends to be linked, or installed, with 3 other infections. It is advised that you click on each of the following links to determine if there are any further malware that needs to be removed.

[How to remove SpySheriff / Winstall.exe / Spysheriff.exe](#)

[How to remove Antivirus Gold or AVGold](#)

[How to remove AdwareDelete](#)

How to remove Antivirus Gold / AVGold

Credits: Metallica for original fix and Miekimoes for guiding me through it

What this program does:

Antivirus Gold is a supposed AntiSpyware application that gets installed **by Spyware/malware** without asking for permission. This infection hijacks your desktop to display an ad stating you need to buy an antispware program.

Tools Needed for this fix:

- [HijackThis](#)
- [Killbox](#)
- [Avgoldfix.reg](#)

Related Tutorials:

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

Symptoms in a HijackThis Log:

O4 - HKLM\..\Run: [AntivirusGold] C:\Program Files\AntivirusGold\AntivirusGold.exe /h

O4 - HKCU\..\Run: [Intel system tool] C:\WINDOWS\System32\winnook.exe

O4 - HKCU\..\Run: [Intel system tool] C:\WINDOWS\System32\hookdump.exe

Note: All of these O4 entries may not be present.

Removal Instructions:Update: New automated procedure can be found [here](#). Try that automated procedure first and fall back to this manual one if it fails.

In order to remove this infection we will need to use HijackThis to manually remove the infection:

1. Print out these instructions as we will need to shutdown every window that is open later in the fix.
2. Download [HijackThis](#) and save it to your **C:** folder. Extract the hijackthis.zip file to **c:\hijackthis**. We will use this program later.
3. Right-click: [HERE](#) and select **Save As** (in Internet Explorer it's labeled **Save Target As**) in order to download the Smitfraud.reg file. Save this file to your desktop.
4. Configure your computer so you can see all hidden files.

[How to see hidden files in Windows](#)

5. Download the [Killbox by Option^Explicit](#) and save it to your desktop. Extract killbox.zip to your desktop. Then double-click on the **killbox.exe** program.
6. When the program is open, select the option labeled **Delete on reboot**.
7. **Do not** close killbox, and open open notepad, by clicking on **Start**, then **Run**, and typing **notepad.exe** and pressing the **OK** button.

- When notepad is open, copy and paste the following bolded text into the notepad screen. You do this by highlighting each of the below bolded filenames and then pressing **Control-C** on your keyboard. Then click on the open notepad windows and press **Control-V** to paste the contents into the notepad.

C:\Program Files\AntivirusGold\AntivirusGold.exe

C:\WINDOWS\System32\winnook.exe

C:\WINDOWS\System32\hookdump.exe

C:\Windows\desktop.html

C:\Windows\screen.html

C:\Windows\windows.html

- Return to Killbox, go to the **File** menu and select **Paste from Clipboard**.
- Still in Killbox, click the red-and-white **Delete File** button. Click **Yes** at the Delete on Reboot prompt. Click No at the Pending Operations prompt.

If your computer does not restart automatically, please restart it manually.

- While your computer is restarting, tap the **F8** key continually until a menu appears. Use your up arrow key to highlight **Safe Mode**, then press the enter button on your keyboard.
- Using **Windows Explorer**, delete the following files, if found, (**please do NOT try to find them by "search" because they will not show up that way**)

FOLDERS to delete (in bold) if found:

C:\Program Files**AntivirusGold**

- While still in Safe Mode, do the following:

Make sure all programs and windows are closed. Double-click on **C:\hijackthis\hijackthis.exe** that you had downloaded and extracted earlier. When the program starts place a check next to each of the following bolded entries, if found, then click **FIX CHECKED** button.

O4 - HKLM\..\Run: [AntivirusGold] C:\Program Files\AntivirusGold\AntivirusGold.exe /h

O4 - HKCU\..\Run: [Intel system tool] C:\WINDOWS\System32\winnook.exe

O4 - HKCU\..\Run: [Intel system tool] C:\WINDOWS\System32\hookdump.exe

- Locate the **avgoldfix.reg** file on your desktop that we downloaded earlier and double-click it. When asked if you want to merge with the registry, click the **YES** button. Wait for the "**merged successfully**" prompt then follow the rest of the instructions below
- Enter your **Control Panel** and double-click on the **Display** control panel, then select the **Desktop** tab and then press the **Customize Desktop** button.
- Select the **Website** tab and uncheck **Security Info**
- Reboot your computer back to normal mode.

18. Follow the steps here:

[Simple and easy ways to keep your computer safe and secure on the Internet](#)

Your computer should now be free of the Antivirus Gold infection.

Important Note:

This infection tends to be linked, or installed, with 3 other infections. It is advised that you click on each of the following links to determine if there are any further malware that needs to be removed.

[How to remove SpySheriff / Winstall.exe / Spysheriff.exe](#)

[How to remove AdwareDelete](#)

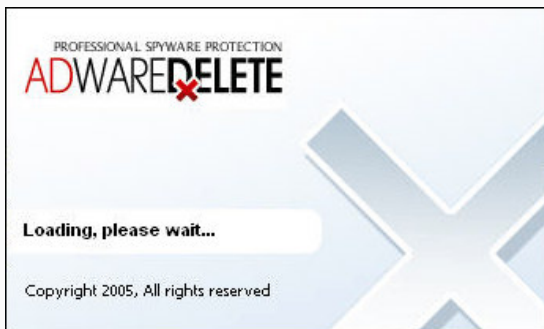
[How to remove the Smitfraud / Quicknavigate / VirtualMaid](#)

How to remove the AdwareDelete

Credits: Miekemoes

What this program does:

AdwareDelete is a supposed AntiSpyware application that gets installed **by Spyware/malware** without asking for permission. If you have this program on your machine you will see this image when you start your computer:



Tools Needed for this fix:

[HijackThis](#)

Related Tutorials:

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

Symptoms in a HijackThis Log:

O4 - HKLM\..\Run: [AdwareDelete] C:\Program Files\AdwareDelete\adwaredelete.exe /h

Removal Instructions:Update: New automated procedure can be found **[here](#)**. Try that automated procedure first and fall back to this manual one if it fails.

In order to remove this infection we will need to use HijackThis to manually remove the infection:

1. Print out these instructions as we will need to shutdown every window that is open later in the fix..

2. Reboot your computer into **Safe Mode**
3. Delete the following folder:

C:\Program Files\AdwareDelete

4. Reboot your computer back to normal mode.
5. Download HijackThis from the above link and extract it to **c:\hijackthis**.
6. Close all windows, even this Internet Explorer window.
7. Navigate to the c:\hijackthis directory and double-click on **HijackThis.exe**
8. When the program starts, click on the **Scan** button.
 1. Put a checkmark next to the following entry (There may be more than one of each):
O4 - HKLM\..\Run: [AdwareDelete] C:\Program Files\AdwareDelete\adwaredelete.exe /h
 2. Then click the **Fix** button
9. Still in HijackThis, click on the **Config** button.
10. Then click on the **Misc Tools** button.
11. Then click on the **Open Uninstall Manager** button.
12. Select the entry for **AdwareDelete** and press the **Delete this entry** button.
13. Exit HijackThis.
14. Download the following file by right-clicking on the link and selecting **Save As**. Then save this file to your desktop.

[AdwareDelete Reg Fix](#)

15. Once the file is downloaded, double-click on the **adwaredelete.reg** file on your desktop and allow it to merge the information into your registry.
16. Delete the **adwaredelete.reg** file from your desktop.

Your computer should now be free of AdwareDelete.