

bleepingcomputer.com

Home Forums Tutorials Startup List Spyware Removal Uninstall List File Database Glossary Resources

Bleeping Computer Welcome Guide Blogs Chat Help Search RSS

Welcome Guest ([Log In](#) | [Create Account](#)) New Member? [Join for free.](#)

Malware & Trojan Remover

Free Malware Scan. Multiple Winner of Best Anti-Malware. Rated 5 Stars
www.pctools.com

Top Malware Removal Tool

Removes All Malware For You! Less than 5 minutes, Scan 100% Free
MalwareRemovalBot.com

Clean Windows XP Registry

Fix All Windows Errors in 1 Min. Feel The Difference. Free Download!
quad-cleaner.com

Ads by Google



Ads by Google

⚠ Have a problem and would like to ask us for help? To learn how to ask your question [Click Here!](#)

✖ Do you have popups or other malware infecting your computer? If so, [Start Here!](#)

❓ Are you having trouble using this site? Then you should visit the [New User Orientation Center!](#)

► [BleepingComputer.com](#) -> [Malware and Spyware Removal Guides](#)

How to remove XP Antivirus 2008, XP Antivirus 2009, and XPAntiVirus (Removal Instructions)

Posted by [Grinler](#) on July 22, 2008 @ 01:07 PM · Views: 627,090

★ [Add to Favorites!](#) 🖨 [Print Guide!](#)

What this programs does:

XP Antivirus 2008, XP Antivirus 2009, and XPAntiVirus are rogue [antivirus](#) programs that, when run, display false results as a tactic to scare you into purchasing the [software](#). Older versions of XP Antivirus would create 9 entries in your Windows Registry that impersonate infections on your machine. In reality, though, these registry entries were harmless and had absolutely no effect on your [computer](#). Instead, these entries were set so that XP AntiVirus can find them when scanning your computer and report them as infections. The newer versions of the program, such as XP Antivirus 2008 and XP Antivirus 2009, instead just display false results when scanning your computer that state infections were found. In order to remove these fake infections, though, you would first need to purchase the software as the trial does not allow you to remove them.

While running, XP Antivirus will also display fake alerts stating that you are infected or under attack from some type of threat. These alerts are fake and can be ignored. If you do click on the alert, though, it will prompt you to purchase the software. Examples of text contained in these alerts can be found below.

Privacy Violation alert!

XP antivirus detected Privacy Violation. Some program is secretly sending your private [data](#) to untrusted [internet](#) host. Click here to block this activity by removing threats (Recommended).

or

System files modification alert!

Some critical system files of your computer were modified by malicious program. It may cause system instability and [data loss](#). Click here to block unauthorised <sic> modification by removing threats (Recommended).

As you can see these programs are fraudware because they make changes to your computer and then state these changes are infections as a scare tactic to have you purchase the software. It goes without saying that under no circumstances should you buy it. The older program, XPAntiVirus, does come with a removal option in the computer's Add or Remove Programs list, but when you attempt to uninstall it, all that happens is the entry is removed from the list and program's process is terminated. Next time you reboot, XP AntiVirus will start up again. The newer versions of the program do not contain an entry in the Add or Remove Programs list at all.



XP Antivirus 2008 screenshot
For more screen shots of this infection click on the image above.
There are a total of 7 images you can view.

The guide below will walk you through the steps necessary to remove this software and any entries it installed in your Windows Registry for free.

Threat Classification:

- [Information on Rogue Programs](#)

Advanced information:

[View XP Antivirus 2008, XP Antivirus 2009, and XPAntiVirus files.](#)

[View XP Antivirus 2008, XP Antivirus 2009, and XPAntiVirus Registry Information.](#)

Entries for this program found in the Add or Remove Programs control panel:

[XP antivirus 1.0.1](#)

Threat Descriptions

- Rogue Programs
- Trojan Horses
- Worms

Search Guides

Google™ Custom Se

Search

Subscribe

- RSS
- MY YAHOO!
- Google
- Windows Live
- Technorati
- NEWSBURST

BlogRoll

- MalwareBytes Blog

Tools Needed for this fix:

- [Malwarebytes' Anti-Malware](#)

Symptoms that may be in a HijackThis Log:

```
O2 - BHO: (no name) - {4e7bd74f-2b8d-469e-dcf7-f96da086b434} - (no file)
O2 - BHO: (no name) - {6C6B8C69-9285-4D94-8492-9E920C8C2B65} - (no file)
O2 - BHO: (no name) - {74f25a2c-22b3-4023-8f1a-ca616c30a8b5} - (no file)
O2 - BHO: (no name) - {9a19966f-ae0e-4699-8cce-9b6f5f1c352c} - (no file)
O2 - BHO: (no name) - {D714A94F-123A-45CC-8F03-040BCAF82AD6} - (no file)
O4 - HKLM\...\Run: [System] C:\WINDOWS\krln32.exe
O4 - HKLM\...\Run: [Windows Framework] C:\WINDOWS\system32\scvh0st.exe
O4 - HKLM\...\Run: [mmnext06] C:\Program Files\Common Files\trjdwnl.dll
O4 - HKLM\...\Run: [shellbn] C:\WINDOWS\shlxt32.exe
O4 - HKCU\...\Run: [XP Antivirus] C:\Program Files\XPAntivirus\XPAntivirus.exe
O4 - HKCU\...\Run: [10181281926292389167514053783761] C:\Program Files\XP
Antivirus\xpa.exe
```

Guide Updates:

10/10/07 - Initial guide creation.
07/22/08 - Updated with information on new variants

Automated Removal Instructions for XP Antivirus 2008, XP Antivirus 2009, and XPAntivirus using Malwarebytes' Anti-Malware:

1. [Print](#) out these instructions as we will need to close every window that is open later in the fix.
2. Download Malwarebytes' Anti-Malware, or MBAM, from the following location and save it to your [desktop](#):

[Malwarebytes' Anti-Malware Download Link](#)
3. Once downloaded, close all programs and Windows on your computer, including this one.
4. Double-click on the icon on your desktop named **Download_mbam-setup.exe**. This will start the installation of MBAM onto your computer.
5. When the installation begins, keep following the prompts in order to continue with the installation process. Do not make any changes to default settings and when the program has finished installing, make sure you leave both the **Update Malwarebytes' Anti-Malware** and **Launch Malwarebytes' Anti-Malware** checked. Then click on the **Finish** button.
6. MBAM will now automatically start and you will see a message stating that you should update the program before performing a scan. As MBAM will automatically update itself after the install, you can press the **OK** button to close that box and you will now be at the main program as shown below.



7. On the **Scanner** tab, make sure the the **Perform quick scan** option is selected and then click on the **Scan** button to start scanning your computer for **XP Antivirus 2008**, **XP Antivirus 2009**, and **XPAntiVirus** related files.
8. MBAM will now start scanning your computer for malware. This process can take quite a while, so we suggest you go and do something else and periodically check on the status of the scan. When MBAM is scanning it will look like the image below.

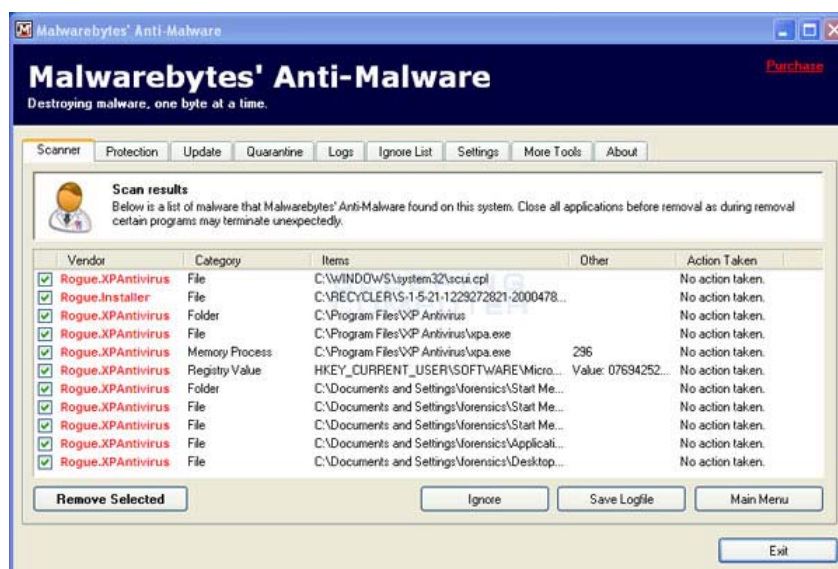


9. When the scan is finished a message box will appear as shown in the image below.



You should click on the OK button to close the message box and continue with the **XP Antivirus 2008**, **XP Antivirus 2009**, and **XPAntiVirus** removal process.

10. You will now be back at the main [Scanner](#) screen. At this point you should click on the **Show Results** button.
11. A screen displaying all the malware that the program found will be shown as seen in the image below. Please note that the infections found may be different than what is shown in the image.



You should now click on the **Remove Selected** button to remove all the listed malware. MBAM will now delete all of the files and registry keys and add them to the programs quarantine. When removing the files, MBAM may require a reboot in order to remove some of them. If it displays a message stating that it needs to reboot, please allow it to do so. Once your computer has rebooted, and you are logged in, please continue with the rest of the steps.

12. When MBAM has finished removing the malware, it will open the scan log and display it in Notepad. Review the log as desired, and then close the Notepad window.
13. You can now exit the MBAM program.

Your computer should now be free of the **XP Antivirus 2008**, **XP Antivirus 2009**, and **XPAntiVirus** program. If your current [anti-virus](#) solution let this infection through, you may want to consider [purchasing the PRO version of Malwarebytes' Anti-Malware](#) to protect against these types of threats in the future.

If you are still having problems with your computer after completing these instructions, then please follow the steps outlined in the topic linked below:

[Preparation Guide For Use Before Posting A Hijackthis Log](#)

Associated XP Antivirus 2008, XP Antivirus 2009, and XPAntiVirus Files:

```
c:\Program Files\XP Antivirus
c:\Program Files\XP Antivirus\vipa.exe
C:\Program Files\XPAntiVirus\
C:\Program Files\XPAntiVirus\XPAntiVirus.exe
c:\WINDOWS\system32\scui.cpl
%UserProfile%\Desktop\XP Antivirus 2008.Ink
%UserProfile%\Start Menu\XP Antivirus 2008
%UserProfile%\Start Menu\XP Antivirus 2008\Uninstall XP Antivirus 2008.Ink
%UserProfile%\Start Menu\XP Antivirus 2008\XP Antivirus 2008.Ink
%UserProfile%\Application Data\Microsoft\Internet Explorer\Quick Launch\XP Antivirus 2008.Ink
C:\WINDOWS\krnl32.exe
C:\WINDOWS\system32\scvh0st.exe
C:\Program Files\Common Files\trjdownl.dll
C:\WINDOWS\shlex32.exe
```

Associated XP Antivirus 2008, XP Antivirus 2009, and XPAntiVirus Windows Registry Information:

```
HKEY_CURRENT_USER\Software\XP antivirus
HKEY_CURRENT_USER\Software\
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\XPAntivirusFilter
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\XPAntivirusFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{4e7bd74f-2b8d-469e-dcf7-f96da086b434}\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{6C6B8C69-9285-4D94-8492-9E920C8C2B65}\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{74f25a2c-22b3-4023-8f1a-ca616c30a8b5}\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{9a19966f-ae0e-4699-8cce-9b6f5f1c352c}\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{D714A94F-123A-45CC-8F03-040BCAF82AD6}\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\XP antivirus_is1\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "XP Antivirus"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "mmnext06"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "shellbn"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "System"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Windows Framework"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run ""
```



This is a self-help guide. Use at your own risk.

BleepingComputer.com can not be held responsible for problems that may occur by using this information. If you would like help with any of these fixes, you can post a HijackThis log in our [HijackThis Logs and Analysis forum](#).

If you have any questions about this self-help guide then please post those questions in our [AntiVirus, Firewall and Privacy Products and Protection Methods forum](#) and someone will help you.

[Advertise](#) | [About Us](#) | [Terms of Use](#) | [Privacy Policy](#) | [Contact Us](#) | [Site Map](#) | [Chat](#) | [Tutorials](#)
[Discussion Forums](#) | [The Computer Glossary](#) | [Resources](#) | [RSS Feeds](#) | [Startups](#) | [The File Database](#) | [Malware Removal Guides](#)

© 2003-2009 All Rights Reserved [Bleeping Computer LLC](#).
PGT: 0.08289 Queries: 12