



bleepingcomputer.com

Home

Forums

Tutorials

Startup List

Spyware Removal

Uninstall List

File Database

Bleeping Computer

Welcome Guide Blogs Chat Help Search RSS

Welcome Guest ([Log In](#) | [Create Account](#))

New Member? [Join for free.](#)

► [BleepingComputer.com](#) -> [Virus, Spyware, & Malware Removal Guides](#)

[Remove Internet Security 2010 \(Uninstall Guide\)](#)

Posted by [Grinler](#) on December 10, 2009 @ 11:37 AM · Views: 355,215

What this programs does:

Internet Security 2010 is a rogue [anti-spyware](#) program that is installed through the use of malware. Once installed, Internet [Security](#) will be configured to start automatically when you login to Windows. It will then scan your [computer](#) and display numerous infections, but will not remove anything until you purchase the program. These infections, though, are all fake and are only being shown to trick you into thinking you are infected so that you then purchase the program. It goes without saying that you should definitely not purchase this program.



[Internet Security](#) 2010 is typically bundled with numerous Trojans that display fake security alerts on your computer. For example, one Trojan will display a message when you login into Windows before you see your desktop. This message will state:

[Security Warning!](#)
[Worm.Win32.NetSky detected on your machine.](#)

It will then recommend that you purchase the program to remove the infection. When you start certain programs, another Trojan will display a

message and then terminate the program. The message it will display is:

[Application cannot be executed. The file is infected. Please activate your antivirus software.](#)

Some of the programs that will cause this message to be shown include Notepad, the CMD prompt, Freecell, Minesweeper, Nero, Windows Messenger, [Microsoft](#) Word, Microsoft Excel, Window calculator, Skype, and PowerPoint. This same Trojan will also display a warning when you try to run programs, such as Windows [Media Player](#) or WinAmp, that play audio and video files. This error message is:

[Windows can't play the following media formats: AVI;WMV;AVS;FLV;MKV;MOV;3GP;MP4;MPG;MPEG;MP3;AAC;WAV;WMA;CDA;FLAC;M4A;MID. Update your video and sound codec to resolve this issue.](#)

It will then prompt you to purchase VSCodec Pro, which is another rogue program, to fix the supposed problem. Just like the scan results, these security warnings are fake and are only being shown to try and convince you that your computer has a security problem.

As you can see, Internet Security 2010 was created to scare you into purchasing the program. Without a doubt, you should definitely not do so, and if you have, you should [contact](#) your credit card company and dispute the charges stating that the program is a scam. Finally, to remove Internet Security 2010 and any related [malware](#) please use the removal guide to remove it for free.

[Tools Needed for this fix: Malwarebytes' Anti-Malware](#)

[Automated Removal Instructions for Internet Security 2010 using Malwarebytes' Anti-Malware:](#)

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

2. Before we can do anything we must first end the processes that belong to Internet Security 2010 so that it does not interfere with the cleaning procedure. To do this, download the following file to your desktop.

[rkill.com Download Link](#)

3. Once it is downloaded, double-click on the rkill.com in order to automatically attempt to stop any processes associated with Internet Security 2010 and other Rogue programs. Please be patient while the program looks for various malware programs and ends them. When it has finished, the black window will automatically close and you can continue with the next step. If you get a message that rkill is an infection, do not be concerned. This message is just a fake warning given by Internet Security 2010 when it terminates programs that may potentially remove it. If you run into these infections warnings that close Rkill, a trick is to leave the warning on the screen and then run Rkill again. By not closing the warning, this typically will allow you to bypass the malware trying to protect itself so that rkill can terminate Internet Security 2010 . So, please try running Rkill until malware is no longer running. You will then be able to proceed with the rest of the guide.

Do not reboot your computer after running rkill as the malware programs will start again.

Now you should download Malwarebytes' Anti-Malware,

4. Once downloaded, close all programs and Windows on your computer, including this one.
5. Double-click on the icon on your desktop named mbam-setup.exe. This will start the installation of MBAM onto your computer.
6. 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 and is at the last screen, make sure you uncheck both of the Update Malwarebytes' Anti-Malware and Launch Malwarebytes' Anti-Malware check boxes. Then click on the Finish button. If Malwarebytes' prompts you to reboot, please do not do so.

If you receive a code 2 error while installing Malwarebytes's, please press the OK button to close these errors as we will resolve them in future steps. The code 2 error will look similar to the image below.



7. As this infection deletes a core executable of Malwarebytes' we will need to download a new copy of it and put it in the C:\program files\Malwarebytes' Anti-Malware\ folder. To download the file please click on the following link:

[Malwarebytes' EXE Download](#)

When your browser prompts you where to save it to, please save it to the C:\program files\Malwarebytes' Anti-Malware\ folder. When [downloading](#) the file, it will have a random filename. Please leave the filename the way it is as it is important that it is not changed. You may want to write down the name of the file as you will need to know the name in the next step.

Once the file has been downloaded, open the C:\program files\Malwarebytes' Anti-Malware\ folder and double-click on the file you downloaded in step 8. MBAM will now start and you will be at the main program screen as shown below.



8. Before you can perform a scan, you must first update the program. To do this click on the Update tab, and that at the new screen click on the Check for Updates button. Malwarebytes' will now check for new updates and download and install them as necessary. When the update is completed, you will be prompted with a message stating either that you already have the latest updates or that they have been updated. Either way, you should now click on the OK button to continue.
9. Now click on the Scanner tab and make sure the the Perform

full scan option is selected. Then click on the Scan button to start scanning your computer for Internet Security 2010 related files.

10. 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.



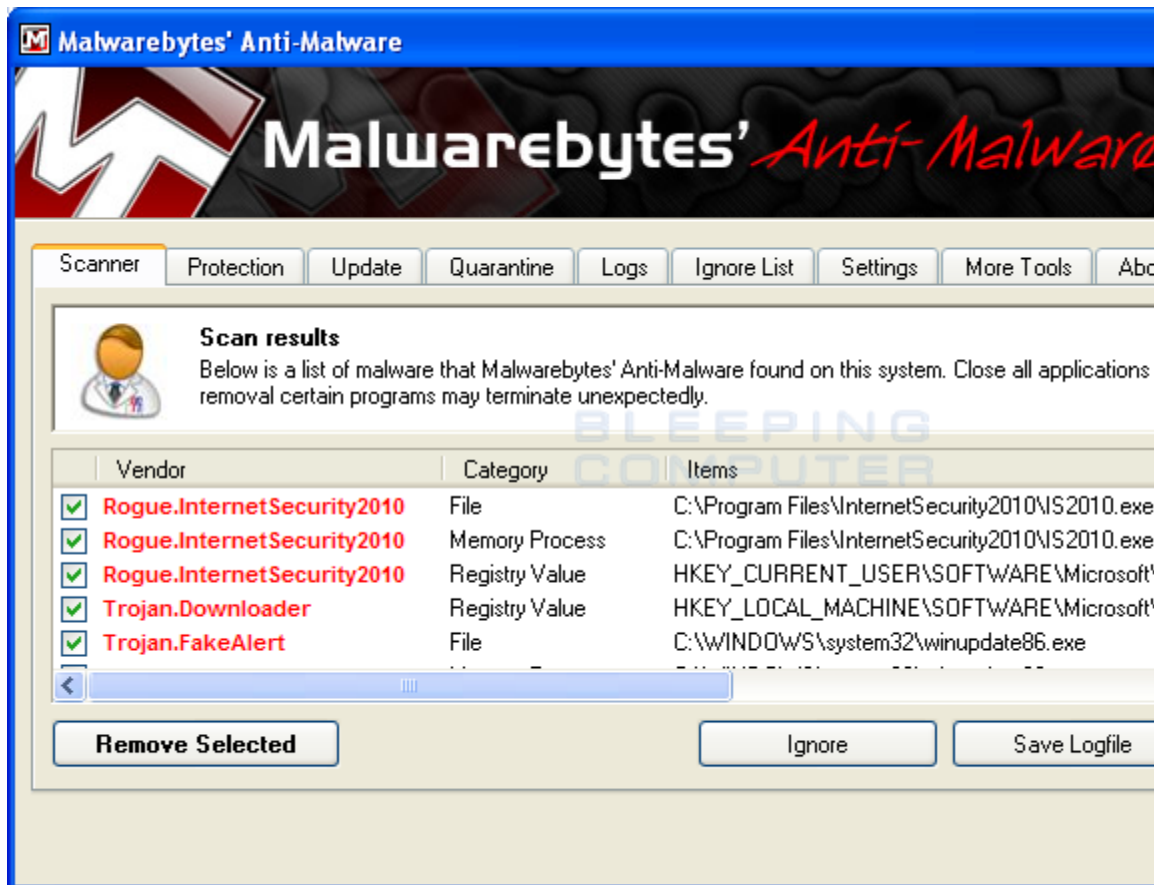
11. When the scan is finished a message box will appear as shown in the image below.



You should click on the OK button to close the message box and

continue with the Internet Security 2010 removal process. You will now be back at the main [Scanner](#) screen. At this point you should click on the Show Results button.

12. 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.

13. 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.

14. You can now exit the MBAM program.
15. Due to the fact that this infection deletes certain MalwareBytes' files, and we had to work around this, if you wish to continue using MalwareBytes' Anti-Malware, which we suggest you do, then you should uninstall and then install it again so that the files are created properly.

Your computer should now be free of the Internet Security 2010 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.