Malware Removal Guide for Windows

Last Updated: October 1, 2012 – View HTML version

This guide will help you remove malicious software from your computer. If you think your computer might be infected with a virus or trojan, you may want to use this guide. It provides step-by-step instructions on how to remove malware from Windows operating system. It highlights free malware removal tools and resources that are necessary to clean your computer. You will quickly learn how to remove a virus, a rootkit, spyware, and other malware.

Disclaimer: *This malware removal guide is intended to be used as a self-help guide. It is not a substitute for professional malware removal.*

I recommend that you back up all your important data before attempting to perform the malware removal process. In the event of a system failure, you will be able to restore your data. Do not back up any system files, programs (.exe), or screensavers (.scr) because they may be infected with malware. How do I back up my data?

Note:

1. In some cases, the only way to remove malware is to reformat and reinstall Windows.
2. This guide will continue to be updated, so please check back often. – Latest Updates
3. If you have any questions or comments about this guide, please contact me at: **brian4131@gmail.com**

Contents

Preparation for Removal

Note: If you are having problems downloading files, download the files in this guide on another computer, and then transfer them to the infected computer with a CD or USB flash drive.

1. Can't Open Files / Can't Connect to the Internet

If you have malware that is blocking Internet access or preventing programs (exe files) from opening, follow the steps on this page: Stop Malicious Processes and Fix EXE Files

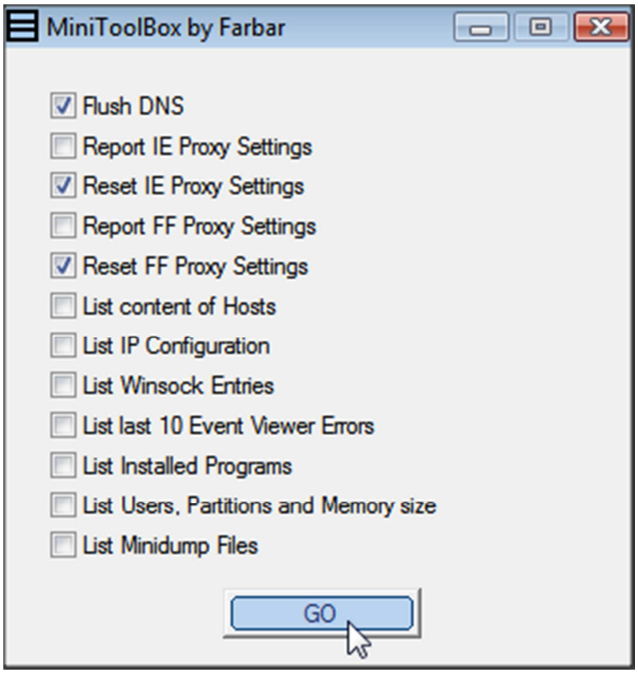
If the instructions do not work, skip down to **Can't Boot Into Windows or Safe Mode?**

2. Fix Internet Connection Problems

Certain types of malware will turn on an Internet proxy setting and corrupt Windows DNS cache, which can prevent you from accessing the Internet or downloading tools required for malware removal. Follow these instructions to fix this problem:

Download and open **MiniToolBox** – Download here – Homepage

Check the following boxes: Flush DNS, Reset IE Proxy Settings, Reset FF Proxy Settings. If you have Firefox open, close it before you click the **Go** button.



Removal Process

Note: If you experience any problems after removing the malware, skip down to **Fix Post-Disinfection Problems**.

Step 1 – Scan for and Remove Rootkits

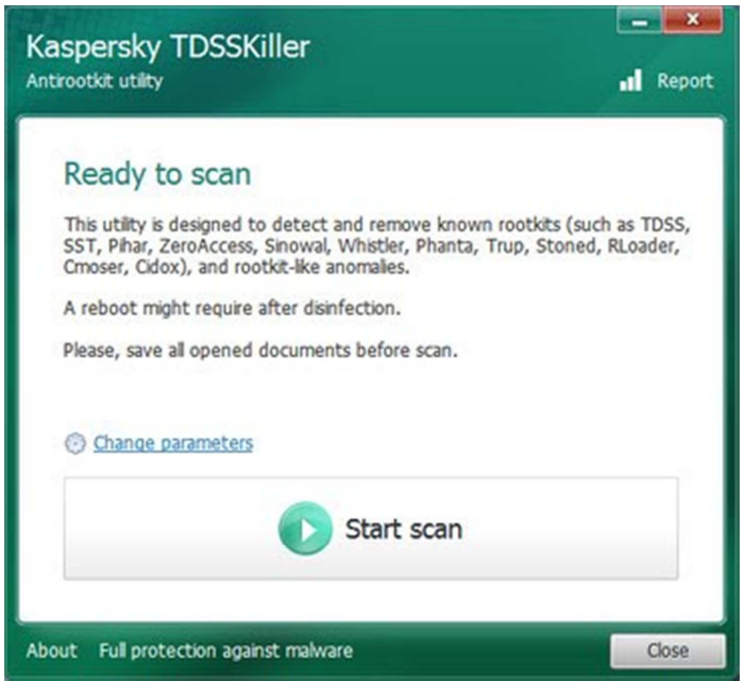
A rootkit is malware that hides itself from Windows and anti-malware software. Most rootkits will download other malware, redirect Google search results, or prevent programs from opening.

Kaspersky TDSSKiller is an effective rootkit removal tool that is easy to use.

Download and open **TDSSKiller** - Download here or here - Homepage

Follow these instructions to use TDSSKiller:

When the program opens, click the **Start scan** button. If the scan finds nothing, click **Close** to exit. If malware or suspicious objects are found, just click **Continue**. Don't change any settings. It may ask you to reboot the computer to complete the rootkit removal process.



Note: If TDSSKiller won't open, try running FixTDSS from Symantec. If FixTDSS won't open, follow the instructions on this page. After you complete the steps, try opening TDSSKiller again.

Step 2 - Scan for and Remove Malware

Many malware removal tools will scan for and remove different types of malware, but unfortunately none of them will find and remove 100% of all malware. Therefore, it's important to use more than one tool to detect and remove all the malware.

The free tools listed below are highly recommended for removing all types of malicious software. They do an excellent job at detecting threats and completely removing them.

Important notes:

- Make sure the malware scanners are up to date before you scan with them.
- Do not use your computer for anything else until the scanning process has finished.
- Do not run more than one scan at a time.
- You may need to restart your computer to complete the malware removal process.
- If the tools won't open, follow the instructions on this page.

 Download and install **Malwarebytes** - Download here or here - Homepage

Uncheck the box that says, "Enable free trial," and then click **Finish**. Perform a quick scan. Once the scan is complete, remove all the listed threats by clicking on the **Remove Selected** button. Make sure that everything is checked.

Note: If Malwarebytes won't update, download and run the offline database installer.

 Download and open **HitmanPro** - Download here (32-bit), (64-bit) - Homepage

When HitmanPro opens, click the **Next** button. Select the box that says **No, I want to perform a one-time scan**, and then click **Next**. Once the scan is complete, click **Next**. Click **Activate free license**, and then click **Next** to remove the malware.

Note: HitmanPro requires Internet access to detect malware. If you can't connect to the Internet, scan with Dr.Web CureIt.

Step 3 – Online Malware Scan

If the automated malware tools can't remove all the malware, scan the computer using an online malware scanner. I recommend using ESET Online Scanner. If the tools ran without any problems, you can skip this step.

After the Removal Process

1. Remove Temporary Files

By removing your temporary files, you will delete any remaining malicious files from Windows temp folders. It will also free up hard disk space, which will help to speed up your computer.

Note: If you are experiencing problems like missing files or icons, skip this step and go on to **Fix Post-Disinfection Problems**.

 Download and install **CCleaner** - Download here

Once installed, simply click the **Run Cleaner** button at the bottom right. You are warned that CCleaner is about to permanently remove files from the system. Click **OK** to proceed.

2. Change All Passwords

Certain types of malware will steal your personal data such as passwords, emails, and banking information. Change all your passwords immediately, especially if you do any banking or other financial transactions on the computer. Password Strength Checker

3. Clean up System Restore

Your system "restore points" may contain malware. The only way to remove the malware is to delete the restore points. To delete the restore points, follow the instructions here: Windows XP - Windows 7

Note: If you are not experiencing any problems that are listed below, skip down to the Conclusion**.**

Fix Post-Disinfection Problems

After the malware is removed, you may experience some annoying problems, such as Windows will not update, Google redirects, and no Internet access. Fortunately, there are simple ways to fix these problems.

1. Can't Connect to the Internet

If you are having problems connecting to the Internet, follow the instructions in this guide: Fix Internet Connection after Malware Removal

2. Google Redirects (Random Websites)

First, try clearing your Java cache. Malware remnants will frequently hide in the Java cache. How do I clear the Java cache? **Note:** If you don't use Java, you should uninstall it. If clearing the Java cache doesn't work, uninstall and reinstall your web browser.

If you are still being redirected after trying all of the above, your computer is likely still infected with malware. Follow the instructions below in the **Get Expert Analysis** section.

3. Missing Icons

Certain types of malware will hide all the icons on your computer. To unhide your files, download Unhide.

Once downloaded, double-click on **Unhide** and allow it to run. It will remove the hidden attribute on all icons and attempt to restore the Start Menu items to their proper location.

4. Fix Windows Update and Firewall

If you are having problems updating Windows or turning on Windows Firewall, follow these instructions:

 Download and install **Windows Repair** - Download here

When Windows Repair opens, click the **Start Repairs** tab, and then click **Start**. Uncheck all the boxes except for the following five:

- Reset Registry Permissions
- Reset File Permissions
- Repair WMI
- Repair Windows Firewall
- Repair Windows Updates

Then click **Start**. Once it's finished, restart your computer.

5. Slow Computer

If your computer is running slow, follow the steps in this guide: How to Speed Up a Slow Computer

6. Windows won't start

Unfortunately, this problem occurs after removing certain rootkits: How to Fix Windows Startup Problems

7. Other Problems

Visit the following websites for more information:

- Microsoft Fix it Solution Center
- Re-Enable a free tool that can undo many changes made by a malware.

Get Expert Analysis

If you want to be certain that your computer is completely cleaned or just want a second opinion, you can create a topic at one of the forums listed below and ask for help. These forums have people who are well trained and experienced in removing malware. Be sure

to mention in your topic that you followed this guide. Please note that it may take a couple of days to receive a reply, so be patient.

Online malware removal forums: Bleeping Computer, Geeks to Go, What the Tech, Tech Support, MalWare Removal, TnT

Can't Boot Into Windows or Safe Mode?

If Windows won't start or your computer won't start in safe mode, I recommend using a **bootable antivirus CD**. A bootable antivirus CD can be used to scan your computer for malware without having to boot into Windows. Many antivirus companies provide free bootable CDs. They are extremely effective at removing malware from a computer.

Below are three highly recommended bootable antivirus CDs. I recommend using Kaspersky Rescue Disk.

Kaspersky Rescue Disk (270 MB) - How to create and use Kaspersky Rescue Disk

Avira Rescue System (250 MB) - How to create and use Avira Rescue CD

Dr.Web LiveCD (190 MB) - How to create and use Dr.Web Live CD

- Burn the antivirus ISO file onto a CD using CD burning software.
- Insert the CD into the infected computer's CD-ROM drive.
- Enter the computer's BIOS, set it to boot from the CD, and reboot the computer. How to Boot from a CD
- Scan for and remove malware using the bootable CD.

Conclusion

Your computer should be completely cleaned of all malware after following this guide. If you believe your computer is still infected, seek professional help to remove the malware. If you like this guide, please share it or leave a comment.

Once your computer is free from malicious software, keep it that way! Follow this security checklist step by step.