



# Malware Removal Guide for Windows



Last Updated: April 9, 2012 - [View HTML version](#)

© 2011 Brian Meyer

This guide will help you remove malicious software from your computer. If you think your computer is infected with a virus or trojan, you may want to use this guide. It contains instructions that, if done correctly and in order, will remove most malicious software on a Windows operating system. It highlights free malware removal tools and resources that are necessary to clean your system. Malware is a general term for any malicious software, including viruses, trojans, rootkits, spyware, and adware. [Signs of malicious software](#)

**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, installers (.exe), or screensavers (.scr) because they may be infected by malware. [How do I back up my data?](#)

## Note:

1. In some cases, the only way to remove malicious software is to reformat and reinstall the operating system.
2. This guide is a work in progress and will continue to be updated, so please check back often. - [Revision history](#)
3. If you have any questions or comments regarding this guide, you can contact me by email: **brian4131@gmail.com**

## Index

- Preparation for Removal
- Removal Process
- Step 1 - Scan for and Remove Rootkits
- Step 2 - Scan for and Remove Malicious Software
- Step 3 - Scan Using Antivirus Software
- After the Removal Process
- Fix Post-Disinfection Problems
- Get Expert Analysis
- Can't Boot Into Windows or Safe Mode?
- Conclusion
- Additional Malware Detection/Removal Tools

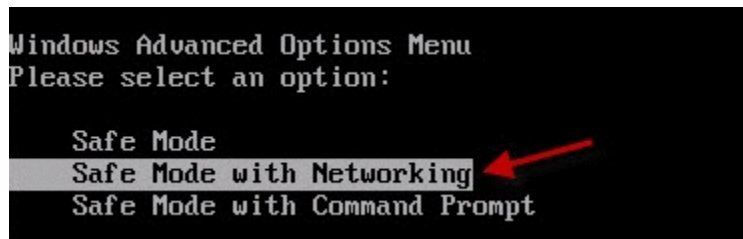
## Preparation for Removal

**Note:** If you are having trouble 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](#). If you use a USB flash drive, you need to disable its autorun file to prevent the malicious software from spreading automatically. [How do I disable the autorun file?](#)

### 1. Boot Into Windows Safe Mode (Cannot Open Programs or No Internet Access)

If you have malicious software that is blocking Internet access or preventing programs from running, you will need to boot into safe mode. Some malicious software will not run in safe mode, thus, allowing easier detection and removal. If you are not experiencing any of the above problems, you can skip safe mode and move on to number 2.

To access safe mode, restart your computer and start tapping the **F8** key before Windows begins to load. You will see a black screen with a number of options. Use the arrow keys to select the **Safe Mode with Networking** option, and then press the **Enter** key. Once you are in **Safe Mode with Networking**, move on to number 2.



**Note:** If safe mode is disabled or corrupted, try fixing it with [Safe Mode Fixer](#). If you still cannot get into safe mode, skip down to **Can't Boot Into Windows or Safe Mode?**

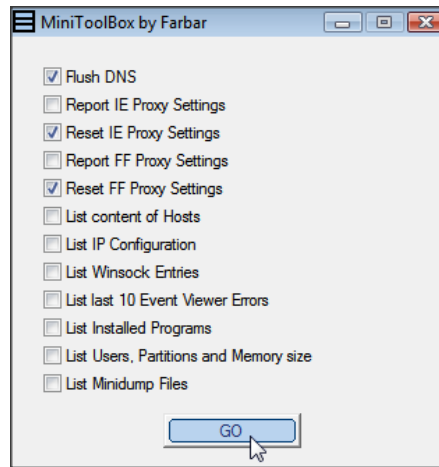
**Note:** If you still cannot open programs in safe mode, follow the instructions on this [page](#).

### 2. Fix Internet Connection Problems

Some malicious software will turn on a proxy setting and corrupt your 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 [MiniToolBox](#) and run it. 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 cannot connect to the Internet after removing the malicious software, follow the instructions on this [page](#).

### Step 1 – Scan for and Remove Rootkits

You need to scan your computer for possible rootkits before running other malware removal software. [What is a rootkit?](#)

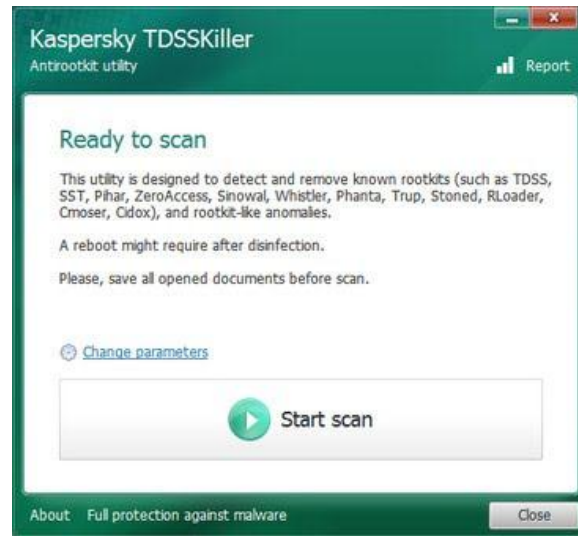
TDSSKiller is a free anti-rootkit tool created by Kaspersky that is designed to remove the TDSS rootkit. This rootkit downloads other malicious software, redirects Google searches, and blocks programs from running. TDSSKiller will also detect and remove other rootkits, such as the ZeroAccess rootkit. TDSSKiller is simple to use and requires no installation.



Download and run **TDSSKiller** - [Download here](#) or [here](#) - [Homepage](#)

To run TDSSKiller, follow these instructions:

When the program opens, click the **Start scan** button. The scan time is very short. If the scan completes with nothing found, click **Close** to exit. If malicious objects are found, the default action will be **Cure** or **Delete**. Click on **Continue**. If suspicious objects are found, the default action will be **Skip**. Click on **Continue**. It may ask you to reboot the computer to complete the rootkit removal process.



**Note:** If TDSSKiller will not run, try running [FixTDSS](#) from Symantec. If FixTDSS does not work, use [RKill](#) to terminate malware processes. After you run RKill, try running TDSSKiller again.

**Note:** If you cannot connect to the Internet after removing the rootkit, follow the instructions on this [page](#).

---

## Step 2 - Scan for and Remove Malicious Software

Many malware removal tools will scan for and remove various malicious software. Unfortunately, none of them will detect and remove 100% of all malicious software; therefore, it is important to use more than one, in the hope that their combined detection is enough to find the problem.

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

### Important notes:

- Make sure the scanners are updated before you scan with them.
- After you have downloaded and updated the scanners, disconnect your Internet connection. This will prevent any further malicious software from installing on your computer. [How do I disconnect my Internet connection?](#)
- 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 you cannot open or run the scanners, follow the instructions on this [page](#).



Download and install **Malwarebytes** - [Download here](#) or [here](#) - [Homepage](#)

Open Malwarebytes and decline the trial. Then 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 will not install, download the randomly named installer from [here](#). Try installing it again. If that does not work, skip down to HitmanPro. After you scan with HitmanPro, try installing Malwarebytes again.



Download and run **HitmanPro** - [Download here \(32-bit\)](#), [\(64-bit\)](#) - [Homepage](#) It requires no installation.

If HitmanPro will not run, use its "Force Breach" mode. To do this, hold down the left **Ctrl** key when you start HitmanPro. Keep the **Ctrl** key pressed until the HitmanPro window appears. This will terminate all non-essential processes, including malware processes. For a detailed tutorial on how to install and use HitmanPro, visit [How to use HitmanPro](#).

**Note:** HitmanPro requires Internet access to detect malware. If you have no Internet access, scan with [SuperAntiSpyware Portable](#).



**Note:** TDSSKiller and HitmanPro are portable programs, which means they can run directly from a USB flash drive. You can take them anywhere and use them on any computer.

---

## Step 3 – Scan Using Antivirus Software

If the malware removal tools find malware that they can't delete, then you should run a full scan with your antivirus program. If the malware removal tools showed no problems, you can skip this step and move on to **After the Removal Process**.

If you currently have antivirus software installed on your computer, make sure it is up to date with the latest virus definitions, and perform a full system scan with it. Remove or quarantine everything that it finds.

**Note:** Before removing anything, make sure it's not a false positive. A false positive occurs when antivirus software falsely identifies a file as malicious. If you suspect a file to be a false positive, go to [VirusTotal](#) or [Jotti's malware scan](#) and upload the file. They will scan the file with several antivirus programs.

If you do not have antivirus software installed, get it immediately. [Avast!](#) and [Microsoft Security Essentials](#) are two highly recommended antivirus programs. Both are free and have excellent malware protection. You should only have one antivirus program running on your computer. [Best Free Security Software for Windows](#)

---

## After the Removal Process

### 1. Remove Temporary Files

Removing your temporary files will delete the remaining malicious files from the 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 icons or folders, skip this step and go on to **Fix Post-Disinfection Problems**.



Download and install **CCleaner** - [Download here](#)

Once installed, simply click on 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

Some malicious software 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 "restore points" may contain malicious software. The only way to remove the malicious software is to delete the restore points. You can use **Disk Cleanup** to remove all but the most recent restore point. Follow these instructions to run Disk Cleanup:

Go to **Start menu > All Programs > Accessories > System Tools** and then click **Disk Cleanup**. Click on the **More Options** tab and locate the section near the bottom labeled **System Restore**. Click on the **Cleanup** button. **Note:** In Windows 7, you need to click on the **Clean up system files** button before the **More Options** tab will appear.

If you cannot find **Disk Cleanup**, you can turn off System Restore, and then turn it back on. This will remove any old points that contain malicious software. [How to turn on/off System Restore](#)

---

## Fix Post-Disinfection Problems

Once you have removed the malicious software from your computer, you may experience some annoying problems, such as Google search redirects and hidden files. Fortunately, there are easy ways to fix these problems.

### 1. Cannot Open or Run Programs (.exe files)

This problem occurs when your .exe file associations are broken. This is usually caused by malware that changes the default file associations in Windows. Follow these instructions to fix this problem:

Download [exeHelper](#). Once downloaded, double-click on **exeHelper** to run the fix. A black window should pop up. Once the fix is complete, press any key to close.



```
C:\Documents and Settings\steiff\Local Settings\Temp\exeHelper.com
exeHelper by Eaktor
Build 2E100P114
Run at 15:57:54 on 11/28/18
Now searching...
Checking for numerical processes...
Checking for sysguard processes...
Checking for bad processes...
Checking for bad files...
Checking for bad registry entries...
Resetting filetype association for .exe
.exe=exefile
.exe=exefile
Resetting filetype association for .com
.com=comfile
.com=comfile
Resetting userinit and shell values...
Resetting policies...
--Finished--
Pokračujte stisknutím libovolné klávesy...
```

### 2. Google Search Redirects (Random Websites)

If you're having a problem with redirects, your hosts file may be corrupted. In order to fix this problem, you have to reset the hosts file back to the default. To reset the hosts file automatically, simply go to [How do I reset the hosts file?](#) and click the **Fix it** button. Then follow the steps in the Fix it wizard.



If you still have redirect issues after resetting the hosts file, try running **GooredFix**. GooredFix fixes **Firefox** browser redirection problems. If you do not use Firefox, you can skip this step. Download GooredFix [here](#). Close Firefox first, and then run the tool. When prompted to run the scan, click Yes. Once the scan is complete, a log will appear; you can close it.

If you still have redirect issues after trying all of the above, your router may be hijacked by malware. In order to fix this problem, you have to reset your router to its default settings. [How do I reset a router?](#)

### 3. Missing Icons and Shortcuts

Some malicious software will hide all the files and shortcuts on your computer. To make your files visible again, download [Unhide](#).



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

### 4. Repair Windows Update and Firewall

If you are having problems updating Windows or turning on Windows Firewall, download and run these tools:



[Repair Windows Update](#), [Repair Windows Firewall](#) or [Error Code 0x80070424](#)

### 5. Other Problems

[Windows Repair](#), by Tweaking.com, allows you to repair or restore various settings, which are often changed by malicious software. It can repair system files, reset file and registry permissions, remove policies set by malicious software, and more. You can find the repair feature by clicking the **Start Repairs** tab.



You may also want to use [Re-Enable](#), which can undo many changes made by a malicious software.



## Get Expert Analysis

### 1. Free Expert Analysis

If you want to be certain that your computer is fully 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 malware removal. 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.

Malware removal forums: [Bleeping Computer](#), [Geeks to Go](#), [What the Tech](#), [Tech Support Forum](#), [MalWare Removal](#), [TnT](#)

### 2. Online Malware Scan

If you believe your computer is still infected with malware, you can perform an online scan of your computer. I recommend using ESET Online Scanner. It can detect and remove malicious software.



[ESET Online Scanner](#)

---


## Can't Boot Into Windows or Safe Mode?

If the malicious software is so severe that you cannot boot into Windows or safe mode, then I recommend using an **antivirus rescue CD**. An antivirus rescue CD can be used to scan your computer for malicious software without having to boot into the operating system. Many antivirus companies provide free rescue CDs. They are extremely effective at removing malicious software.



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

 [Kaspersky Rescue Disk](#) (230 MB) - [How to create and use Kaspersky Rescue Disk](#)

 [Avira AntiVir Rescue System](#) (240 MB) - [How to create and use Avira Rescue CD](#)

 [Dr.Web LiveCD](#) (180 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 Change the Boot Order in BIOS](#)
- Scan the computer with the rescue CD.

If all else fails, you must reformat your hard drive and reinstall Windows. [When should I re-format? How should I reinstall?](#)

---

## Conclusion

Your computer should be completely cleaned of all malicious software after following this guide. If you believe your computer is still infected, seek professional help to remove the malicious software. If you liked this guide, please share it or [leave a comment](#).

- [Prevent Future Infections](#)
  - [How to Stay Safe While Online](#)
- 

### Notable Links:

- [Useful Computer Security Resources](#)
- [Computer and Data Security Guide for Windows](#)
- [Public Block Lists of Malicious IPs and URLs](#)