Malwarebytes Techbench User Guide

Version 1.07

19 November 2013

Notices

Malwarebytes products and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. You may copy and use this document for your internal, reference purposes only.

This document is provided "as-is." The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, we would appreciate your comments; please report them to us in writing.

The Malwarebytes logo and Malwarebytes Techbench are trademarks of Malwarebytes Corporation. Windows, Windows Vista, Windows 7, Windows 8 and Internet Explorer are registered trademarks of Microsoft Corporation. Firefox is a registered trademark of Mozilla Foundation. Chrome and Google are registered trademarks of Google, Inc. All other trademarks or registered trademarks listed belong to their respective owners.

Contents

Getting Started

Malwarebytes Techbench is a portable product which runs from a special USB drive created to provide a solution for PC repair shops to be able to service their customers' systems to rid them of malware using powerful detection and removal technologies found in Malwarebytes Anti-Malware.

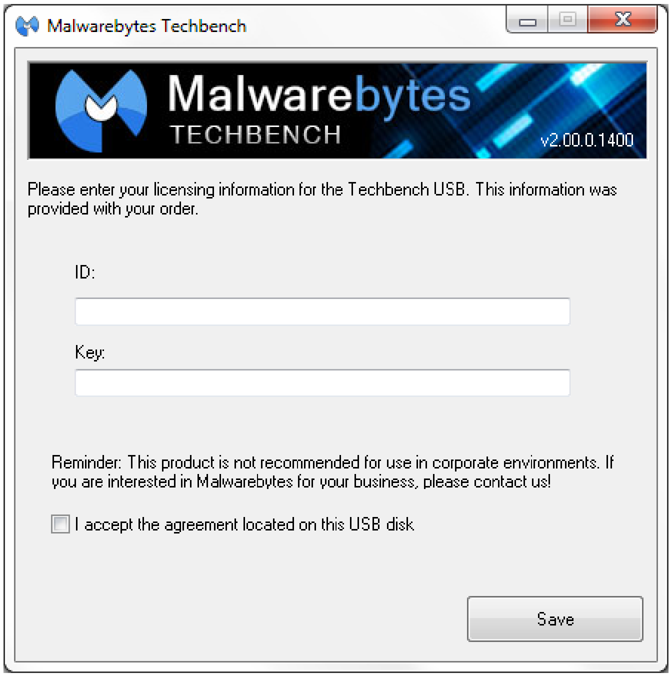
Malwarebytes Anti-Malware is considered to be the next step in the detection and removal of malware. We have compiled a number of new technologies that are designed to quickly detect, destroy, and prevent malware. Malwarebytes Anti-Malware can detect and remove malware that even the most well-known antivirus and antimalware applications on the market today cannot.

In addition to Malwarebytes Anti-Malware, Malwarebytes Techbench also includes our cutting edge Malwarebytes Chameleon technology, designed to allow Malwarebytes Anti-Malware to run in hostile environments where other anti-malware applications and tools are helpless.

Product Registration

Before you can begin using Malwarebytes Techbench to clean up your customers' systems, you must activate it using license information provided to you at time of purchase. It is recommended that this step be performed from a known clean PC, such as the one used by your tech shop for research and storage of tools (assuming you have such a PC). This only needs to be done once, and must be done prior to using the product.

1. Insert the Malwarebytes Techbench USB drive into the clean PC.
2. Run the **mbtechbench.exe** application included in the root directory of the drive.
3. In the fields provided, enter the ***ID*** and ***Key*** provided to you at time of purchase, and check the box indicating that you accept the agreement located on the USB disk.



Please enter your licensing information for the Techbench USB. This information was provided with your order.

ID:

Key:

Reminder: This product is not recommended for use in corporate environments. If you are interested in Malwarebytes for your business, please contact us!

□ I accept the agreement located on this USB disk

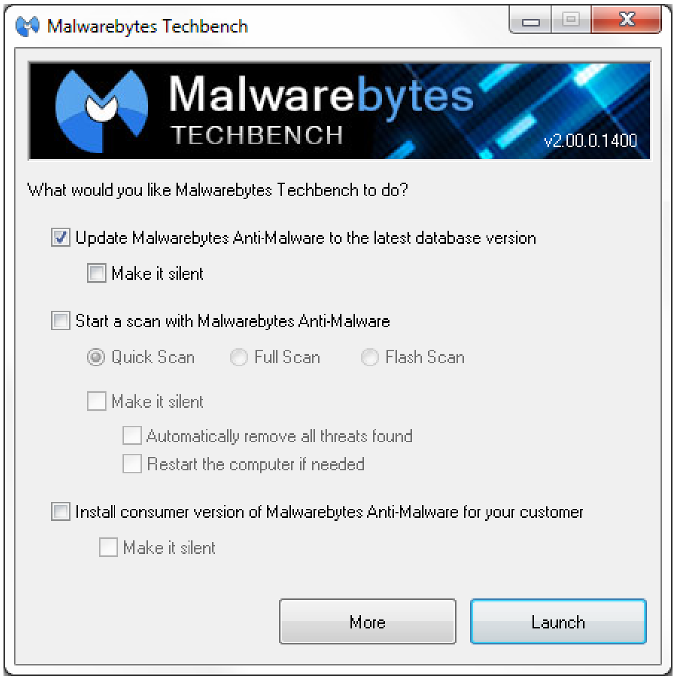
4. Click the ***Save*** button.
5. Close the program and eject the drive from your system unless you have other tasks to perform, such as ensuring that you have the latest version and database by checking for updates

WARNING: You may damage the USB drive by removing it without first ejecting it. Use the ***Eject*** command from Explorer's right-click context menu, or in the Windows taskbar.

Updating the Database

Before using Malwarebytes Techbench to clean a customer PC, you want to have the most effective malware detection and removal technology at your disposal. Downloading the latest threat definition database helps to assure this. It is recommended that this step be performed from a known clean PC, such as the one used by your tech shop for research and the storage of tools (assuming you have such a PC). This is because an infected PC may not have internet access or may have an infection which blocks access to Malwarebytes' update servers.

1. Insert the Malwarebytes Techbench USB drive into the PC.
2. Run the **mbtechbench.exe** application included on the drive.
3. Check the box next to ***Update Malwarebytes Anti-Malware to the latest database version***.



What would you like Malwarebytes Techbench to do?

☑ Update Malwarebytes Anti-Malware to the latest database version

☐ Make it silent

☐ Start a scan with Malwarebytes Anti-Malware

● Quick Scan ○ Full Scan ○ Flash Scan

☐ Make it silent

☐ Automatically remove all threats found

☐ Restart the computer if needed

☐ Install consumer version of Malwarebytes Anti-Malware for your customer

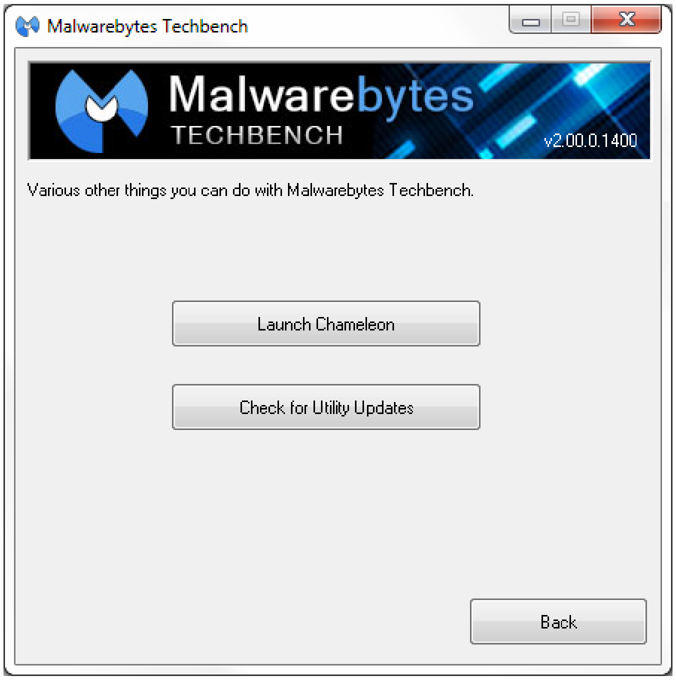
☐ Make it silent

4. Click the ***Launch*** button.
5. The updater will now run, and will notify you when the database has been successfully updated. Click ***OK***.
6. Eject the drive from your system when prompted (unless you have other tasks to perform first),

You may choose to make this update silent and use it as part of the cleaning process for an infected PC. To do this, follow the steps above except check the box next to ***Make it silent*** when you check the box next to ***Update Malwarebytes Anti-Malware to the latest database version***. This ensures that no prompts are displayed. Once the update is complete, it will perform any other tasks you selected, such as scanning the system for malware using the ***Start a scan with Malwarebytes Anti-Malware*** option, which can also be made silent if you choose.

Updating the Malwarebytes Techbench Utility

You may check for Techbench application updates at any time by clicking the ***More*** button and then clicking the ***Check for Utility Updates*** button.



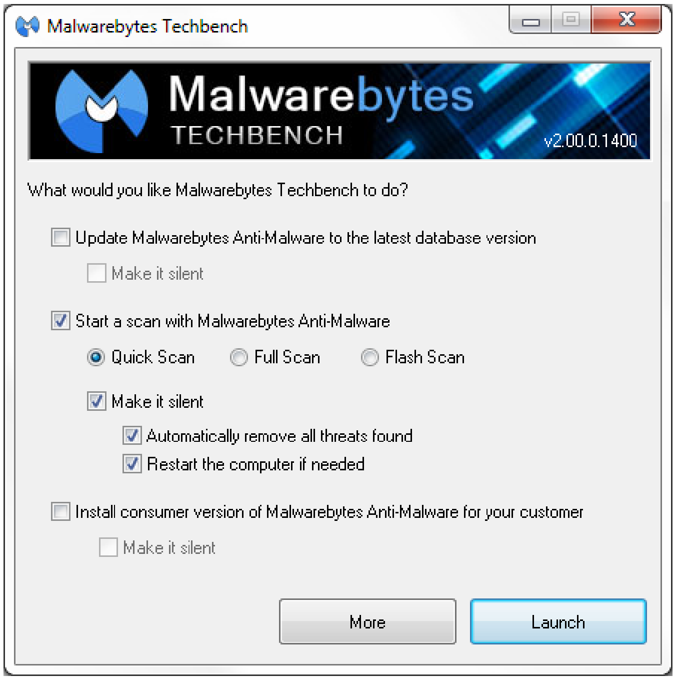
Various other things you can do with Malwarebytes Techbench.

Malwarebytes Techbench will then check our update servers for a newer version of the product, and download it if one is available. Once a utility update has been downloaded, it will launch automatically. Just follow onscreen instructions to upgrade the application.

Performing Scans

Scans may be run on infected systems using the ***Start a scan with Malwarebytes Anti-Malware*** checkbox, and choosing from any of the options below:

- **Quick Scan:** Scans all system locations where malware is known to install itself. This is the scan type recommended by Malwarebytes.
- **Full Scan:** Scans every file on the drives you selected, in addition to all areas checked by the Quick Scan.
- **Flash Scan:** Scans system memory and startup locations for active infections. It also checks key locations using heuristics.
- **Make it silent:** This option makes your scan run silently rather than displaying the user interface and scan progress. This is a good choice if you wish to have the scan run automatically and clean the PC while you perform other tasks.
- **Automatically remove all threats found:** This option – which is only available if you made the scan silent – will have Malwarebytes Anti-Malware remove detected threats automatically.
- **Restart the computer if needed:** This option – which is only available if you made the scan silent and used the ***Automatically remove all threats found*** option – will cause Malwarebytes Anti-Malware to reboot the system if required to complete threat removal.



Malwarebytes Techbench

Malwarebytes TECHBENCH v2.00.0.1400

What would you like Malwarebytes Techbench to do?

□ Update Malwarebytes Anti-Malware to the latest database version

□ Make it silent

☑ Start a scan with Malwarebytes Anti-Malware

● Quick Scan ○ Full Scan ○ Flash Scan

☑ Make it silent

☑ Automatically remove all threats found

☑ Restart the computer if needed

□ Install consumer version of Malwarebytes Anti-Malware for your customer

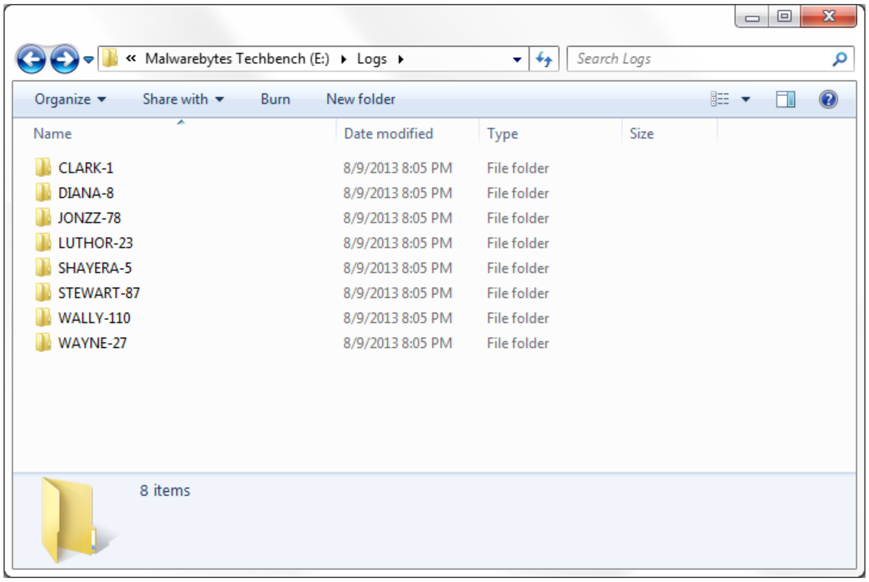
□ Make it silent

Malwarebytes Anti-Malware Settings and Features

All settings and functions of Malwarebytes Anti-Malware may be accessed by running **mbam.exe** located within the **mbam** folder on the USB drive. To find out in detail what those settings and features are and what functions they serve, refer to the included **mbam.chm** help file, also located within the **mbam** folder on the USB drive. Any changes made to Malwarebytes Anti-Malware settings here will only remain in effect until you exit Malwarebytes Anti-Malware. If you wish to run a scan using modified settings, you should do that prior to exiting the program.

Scan Logs

Logs generated by scans are stored on the USB drive itself, within folders in the root of the drive, with each subfolder named after the system upon which the scan was performed. This allows you to easily keep track of which scan logs came from which of your customers' systems.

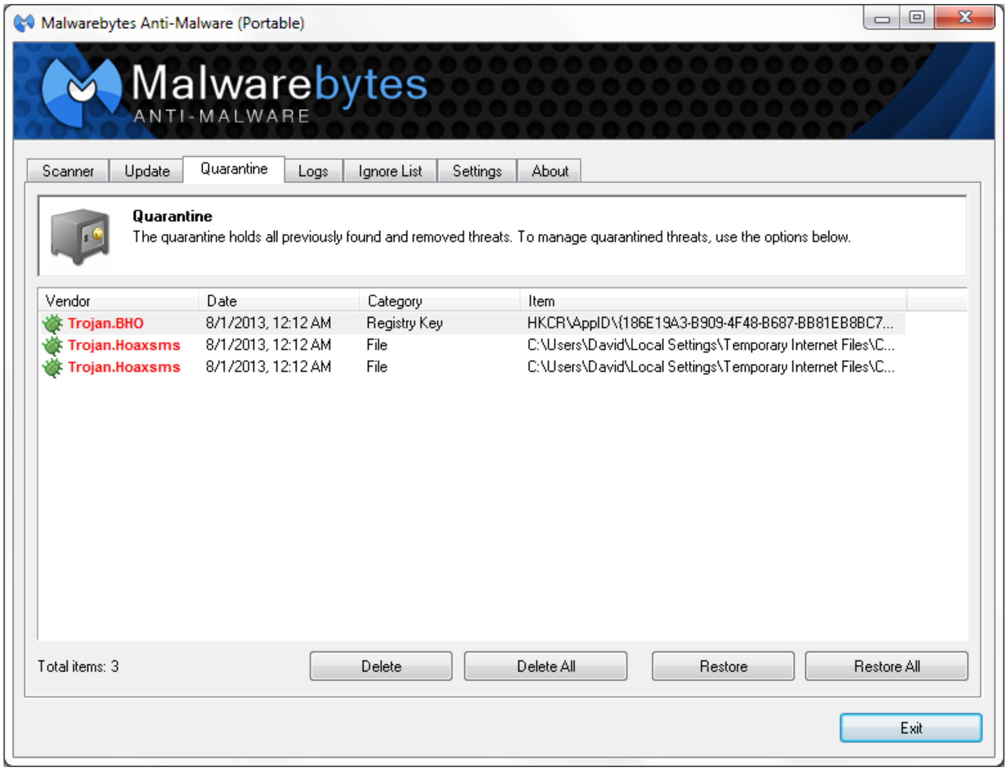


Name	Date modified	Type	Size
CLARK-1	8/9/2013 8:05 PM	File folder	
DIANA-8	8/9/2013 8:05 PM	File folder	
JONZZ-78	8/9/2013 8:05 PM	File folder	
LUTHOR-23	8/9/2013 8:05 PM	File folder	
SHAYERA-5	8/9/2013 8:05 PM	File folder	
STEWART-87	8/9/2013 8:05 PM	File folder	
WALLY-110	8/9/2013 8:05 PM	File folder	
WAYNE-27	8/9/2013 8:05 PM	File folder	

8 items

Quarantine

Quarantined threats are all stored on the USB drive and may be viewed by launching Malwarebytes Anti-Malware itself which may be found on the USB drive under the folder **\mbam**. Simply run **mbam.exe**, access the **Quarantine** tab, and use the available controls to restore objects from quarantine or to delete the quarantined backup copies from the drive. If you do need to restore anything, be sure that you only restore threats to the system of the customer from which they were quarantined. Use the scan logs, which are all stored in folders named after each customer PC (as described previously) to determine which threats came from which system.



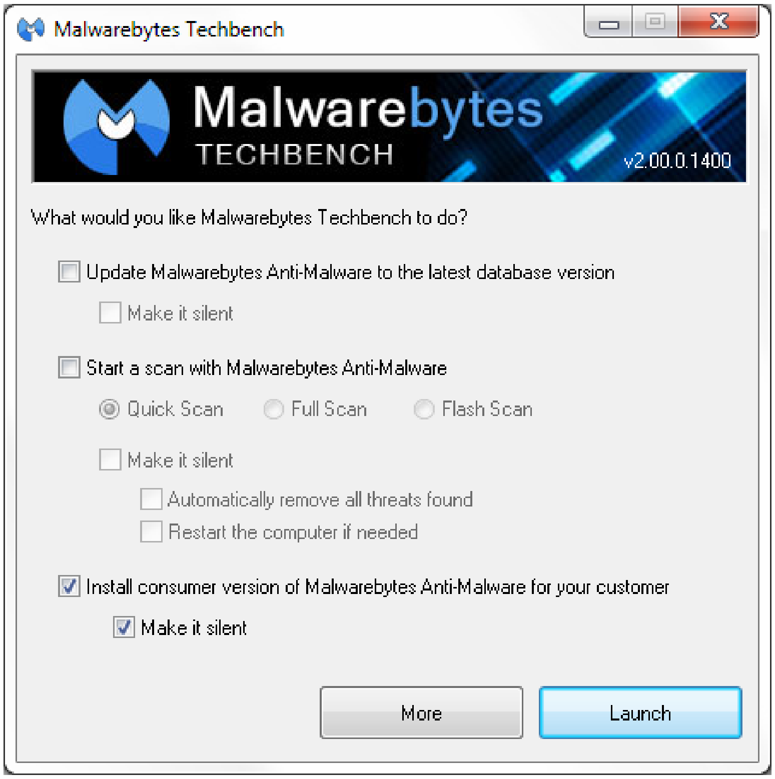
Quarantine
The quarantine holds all previously found and removed threats. To manage quarantined threats, use the options below.

Vendor	Date	Category	Item
Trojan.BHO	8/1/2013, 12:12 AM	Registry Key	HKCR\AppID\{186E19A3-B909-4F48-B687-BB81EB8BC7...
Trojan.Hoaxsms	8/1/2013, 12:12 AM	File	C:\Users\David\Local Settings\Temporary Internet Files\C...
Trojan.Hoaxsms	8/1/2013, 12:12 AM	File	C:\Users\David\Local Settings\Temporary Internet Files\C...

Total items: 3

Installing Malwarebytes Anti-Malware for Your Clients

Once you've finished cleaning up your customer's PC, you may wish to install Malwarebytes Anti-Malware for them. You may do so by checking the box next to ***Install consumer version of Malwarebytes Anti-Malware for your customer*** and then clicking ***Launch***.



What would you like Malwarebytes Techbench to do?

□ Update Malwarebytes Anti-Malware to the latest database version

□ Make it silent

□ Start a scan with Malwarebytes Anti-Malware

● Quick Scan ○ Full Scan ○ Flash Scan

□ Make it silent

□ Automatically remove all threats found

□ Restart the computer if needed

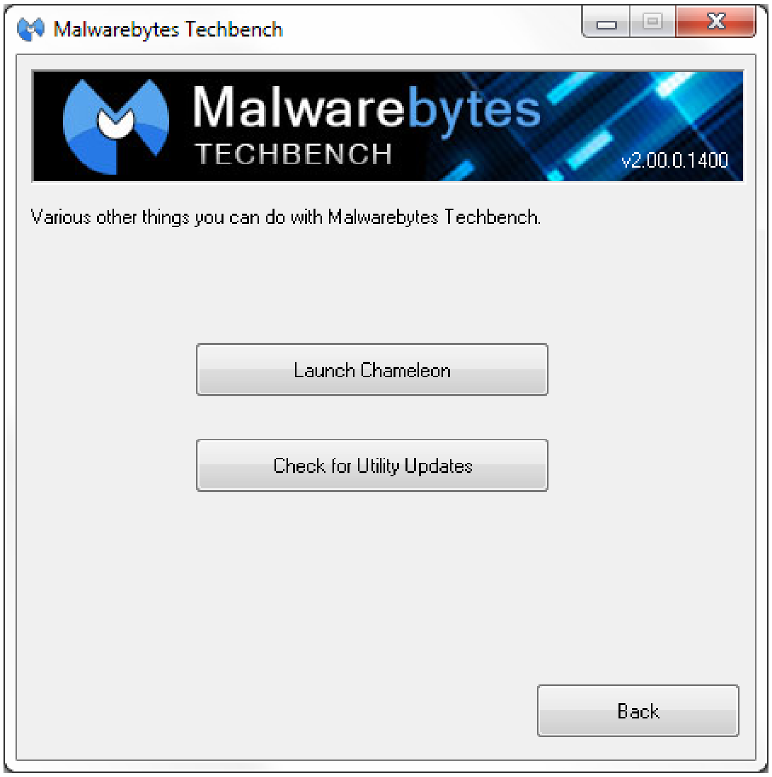
☑ Install consumer version of Malwarebytes Anti-Malware for your customer

☑ Make it silent

You may also make the installation process silent if you would like it to happen automatically without requiring you to navigate through the installation wizard.

Malwarebytes Chameleon

Malwarebytes Chameleon is a set of new technologies to help get Malwarebytes Anti-Malware up and running on a system when prevented from doing so by specific malware infections. To access Chameleon, simply click on the ***More*** button and then click the ***Launch Chameleon*** button.



Various other things you can do with Malwarebytes Techbench.

If **mbtechbench.exe** will not execute due to infections present on the system, you'll need to launch Chameleon manually. To do this, access the **mbam** folder on the USB drive, then the **Chameleon** subfolder. You then have several options as far as what to do next to get it to run, which all depend on what the infection you're dealing with allows, and even getting to that folder may be difficult, if say Windows explorer isn't running:

Using the Chameleon.chm Help File via Explorer

1. On the USB drive, go to **mbam\Chameleon** and double-click on the **chameleon.chm** help file.
2. Once the "Help" file opens, click each **Chameleon #** button until you see a black DOS/command prompt window that remains open and says MBAM-chameleon ver. # at the top. If your host operating system is Windows Vista, Windows 7 or Windows 8, you may see a User Account Control prompt. If so, click **Yes**.
3. Press any key to continue.
4. Malwarebytes Chameleon will then update Malwarebytes Anti-Malware. Please ensure that you are connected to the internet if possible. Once the update completes and it says your database has been updated, click **OK.**
5. Malwarebytes Chameleon will then terminate threats running in memory. Please be patient…this may take a while. Upon completion, Malwarebytes Anti-Malware will open automatically and perform a Quick Scan.
6. Once the scan is complete, click on **Show Results.** You may remove any threats which have been found by clicking **Remove Selected**.
7. If prompted to restart the computer to complete the removal process, click **Yes**.
8. After the computer restarts, open Malwarebytes Anti-Malware and perform one last Quick Scan to verify that no threats remain.

Using the Chameleon.chm Help File via Task Manager

1. Press **Ctrl**+**Shift**+**Esc** on the keyboard.
2. Once **Task Manager** opens, click on **File** at the top and choose **New Task (Run...)**.
3. Click the **Browse...** button.
4. Navigate to the **mbam\Chameleon** folder.
5. Click on the drop-down menu that says **Programs** and choose **All Files**.
6. Double-click on the **Chameleon.chm** help file.
7. Once the "Help" file opens, click each **Chameleon #** button until you see a black DOS/command prompt window that remains open and says MBAM-chameleon ver. # at the top.
8. Press any key to continue.
9. Malwarebytes Chameleon will then update Malwarebytes Anti-Malware. Please ensure that you are connected to the internet if possible. Once the update completes and it says your database has been updated, click **OK**.
10. Malwarebytes Chameleon will then terminate threats running in memory. Please be patient…this may take a while. Upon completion, Malwarebytes Anti-Malware will open automatically and perform a Quick Scan.
11. Once the scan is complete, click on **Show Results**. You may remove any threats which have been found by clicking **Remove Selected**.
12. If prompted to restart the computer to complete the removal process, click **Yes**.
13. After the computer restarts, open **Malwarebytes Anti-Malware** and perform one last Quick Scan to verify that no threats remain.

Using the Chameleon.chm Help File via Internet Browser

1. Open the internet browser (for example, **Internet Explorer**, **Firefox** or **Google Chrome**).
2. Press the **Alt** key on the keyboard.
3. In the menu that appears at the top, click on **File** and choose **Open** or **Open File**.
4. In the browse window that opens, navigate to the **mbam\Chameleon** folder on the USB drive.
5. Double-click on the **Chameleon.chm** help file. If you do not see it, click on the drop-down menu that says **Web Documents** and choose **All Files**.
6. Once the "Help" file opens, click each **Chameleon #** button until you see a black DOS/command prompt window that remains open and says MBAM-chameleon ver. # at the top. If your host operating system is Windows Vista, Windows 7 or Windows 8, you may see a User Account Control prompt. If so, click **Yes**.
7. Press any key to continue.
8. Malwarebytes Chameleon will then update Malwarebytes Anti-Malware. Please ensure that you are connected to the internet if possible. Once the update completes and it says your database has been updated, click **OK**.
9. Malwarebytes Chameleon will then terminate threats running in memory. Please be patient…this may take a while. Upon completion, Malwarebytes Anti-Malware will open automatically and perform a Quick Scan.
10. Once the scan is complete, click on **Show Results.** You may remove any threats which have been found by clicking **Remove Selected**.
11. If prompted to restart the computer to complete the removal process, click **Yes**.
12. After the computer restarts, open **Malwarebytes Anti-Malware** and perform one last Quick Scan to verify that no threats remain.

Chameleon.chm Will Not Open Due to Infection

1. Open the **mbam\Chameleon** folder.
2. Next, double-click on each file one by one until you find one that works, which will be indicated by a black DOS/command prompt window. If your host operating system is Windows Vista, Windows 7 or Windows 8, you may see a User Account Control prompt when attempting to open the files. If so, click **Yes**

Warning: Do not attempt to open file **mbam-killer.exe.** This file serves a different purpose.

3. Press any key to continue.
4. Malwarebytes Chameleon will then update Malwarebytes Anti-Malware. Please ensure that you are connected to the internet if possible. Once the update completes and it says your database has been updated, click **OK**.
5. Malwarebytes Chameleon will then terminate threats running in memory. Please be patient…this may take a while. Upon completion, Malwarebytes Anti-Malware will open automatically and perform a Quick Scan.
6. Once the scan is complete, click on **Show Results**. You may remove any threats which have been found by clicking **Remove Selected**.
7. If prompted to restart the computer to complete the removal process, click **Yes**.
8. After the computer restarts, open **Malwarebytes Anti-Malware** and perform one last Quick Scan to verify that no threats remain.

Other Methods

You may also mix the techniques described above. For example, if the CHM help file will not open via Task Manager or an internet browser, you can use that same method to try and run the Chameleon executables one by one. You can also try booting the computer into Safe Mode with Networking (so that you have internet access for downloading updates).