

Forum:[Hack Forums](#)

Thread: [\[MRT-X Academy\] Malwarebytes Anti-Malware Tutorial](#)

Tha Sneak - February 16, 2025, 10:51 pm

Malwarebytes Anti-Malware Tutorial

1. Introduction

Malwarebytes Anti-Malware is one of the most popular and effective tools for detecting and removing malware, viruses, spyware, and other malicious software from your computer. It is known for its robust detection engine, ability to remove stubborn threats, and user-friendly interface. This tutorial will guide you through how to download, install, and use Malwarebytes Anti-Malware to keep your system secure.

2. Features

Malwarebytes Anti-Malware offers a variety of features: Real-time protection against malware, viruses, and spyware (Premium version).

- Comprehensive scanning to detect and remove malware.

- Ransomware protection (Premium version).

- Automatic updates to keep malware definitions current.

- Lightweight and easy-to-use interface.

- Compatible with other antivirus software.

- Malware removal in free mode.

3. Download and Installation

To get started with Malwarebytes Anti-Malware, follow these steps:

Go to the official [Malwarebytes website](#) and download the latest version of Malwarebytes Anti-Malware.

- Save the installation file (mbsetup.exe) to a location that is easy to access, such as your desktop.

- Double-click the installation file to start the installation process.

- Follow the on-screen instructions to install Malwarebytes. You can choose between the free version (manual scans only) or the Premium version (real-time protection).

- Once the installation is complete, Malwarebytes will automatically update its malware definitions.

4. How to Use Malwarebytes Anti-Malware

Step 1: Launching Malwarebytes

After installation, Malwarebytes Anti-Malware will automatically launch. If it doesn't, you can start it by double-clicking the Malwarebytes icon on your desktop or finding it in the Start menu.

When the application opens, you will see the main dashboard displaying your protection status, last scan, and other features.

Step 2: Running a Scan

In the main dashboard, click the Scan button to begin a system scan.

Malwarebytes will start scanning your system for malware, viruses, spyware, and other potentially unwanted programs (PUPs).

You can monitor the progress of the scan, including the number of files scanned and any threats detected.

The scan will take a few minutes to complete, depending on the number of files on your system.

Step 3: Reviewing the Scan Results

Once the scan is complete:

Malwarebytes will display the scan results, showing any detected malware or potentially unwanted programs (PUPs).

You can click on any detected item for more details, such as the file path and threat type.

By default, all detected items will be selected for removal. If you wish to keep any item, uncheck the corresponding box.

Once you have reviewed the list, click Quarantine to move the detected items to quarantine and neutralize the threats.

Step 4: Quarantine and Removal

After quarantining threats:

Malwarebytes will prompt you to reboot your computer to complete the removal of certain threats. Click Yes to reboot if needed.

After the reboot, open Malwarebytes again and go to the Quarantine tab in the left-hand menu to review the quarantined items.

You can either delete the quarantined files permanently or restore them if needed (only recommended for false positives).

Step 5: Updating Malwarebytes

To ensure that Malwarebytes can detect the latest malware threats:

Malwarebytes automatically updates its database of malware definitions, but you can manually check for updates.

From the main dashboard, click the Settings tab on the left menu.

Click on the Check for Updates button under the General section.

Malwarebytes will download and install any available updates.

5. Real-Time Protection (Premium Feature)

For users with the Premium version, Malwarebytes offers real-time protection: The Real-Time Protection feature blocks malware, ransomware, and other malicious programs before they can cause harm.

This feature runs in the background and actively monitors your system.

If Malwarebytes detects suspicious activity, it will automatically quarantine the threat.

You can toggle real-time protection on and off in the dashboard.

6. Troubleshooting

If you encounter any issues while using Malwarebytes: Ensure that Malwarebytes is updated to the latest version.

If Malwarebytes fails to remove certain threats, try running the scan in Safe Mode by rebooting

your computer and pressing F8 repeatedly during startup.

Check for conflicting antivirus software and temporarily disable them if necessary.

Reboot your system if Malwarebytes prompts you to do so after removing malware.

For persistent issues, visit the [Malwarebytes Support Center](#).

7. Additional Tips

Here are some extra tips to help you get the most out of Malwarebytes Anti-Malware: Run regular scans even if you have real-time protection enabled to ensure maximum security.

Schedule automatic scans by going to Settings > Scan Schedule (Premium version only).

Review the Quarantine section regularly to delete old or unnecessary files.

Keep your operating system and all other software updated to reduce vulnerabilities.

8. Conclusion

Malwarebytes Anti-Malware is a powerful tool for keeping your system protected against malware, viruses, and other threats. Whether you use the free version for manual scans or the Premium version for real-time protection, Malwarebytes provides an extra layer of defense that complements your existing antivirus software.

Tha Sneak - February 19, 2025, 3:22 pm

Tha Sneak - February 22, 2025, 8:32 am

Malwarebytes Anti-Malware Clean Log:

Malwarebytes

www.malwarebytes.com

-Log Details-

Scan Date: 2/19/2025

Scan Time: 5:06 AM

Log File: 3d758cd2-eea9-11ef-acee-1091d15cef30.json

-Software Information-

Version: 5.2.6.163

Components Version: 1.0.5146

Update Package Version: 1.0.96112

License: Trial

-System Information-

OS: Windows 10 (Build 19045.2965)

CPU: x64

File System: NTFS

User: DESKTOP-9L7LAU3\Tha Sneak

-Scan Summary-

Scan Type: Threat Scan

Scan Initiated By: Manual

Result: Completed

Objects Scanned: 173030

Threats Detected: 1

Threats Quarantined: 0

Time Elapsed: 6 min, 46 sec

-Scan Options-

Memory: Enabled

Startup: Enabled

File system: Enabled

Archives: Enabled

Rootkits: Enabled
Heuristics: Enabled
PUP: Detect
PUM: Detect

-Scan Details-

Process: 0
(No malicious items detected)

Module: 0
(No malicious items detected)

Registry Key: 0
(No malicious items detected)

Registry Value: 0
(No malicious items detected)

Registry Data: 0
(No malicious items detected)

Data Stream: 0
(No malicious items detected)

Folder: 0
(No malicious items detected)

File: 1
Malware.AI.3594256008, C:\USERS\THA SNEAK\DESKTOP\MALWARE REMOVAL
TOOLS\DELFIX\DELFIX_1.010.EXE, No Action By User, 17, 0, 1.0.96112, 17, dds, 03227584,
E0C27AAD0A97444BB001C0F2B976A6EA,
8A22C1EBD3ACBFD7BA443A950D1A7903C27EB63FE0722585CBAB2D56D2AD2D9C

Physical Sector: 0
(No malicious items detected)

WMI: 0
(No malicious items detected)

(end)

Infected Log:

Malwarebytes
www.malwarebytes.com

-Log Details-

Scan Date: 2/26/2025
Scan Time: 4:43 AM
Log File: 805bc69f-f42e-11ef-8dfb-1091d15cef30.json

-Software Information-

Version: 5.2.7.167

Components Version: 1.0.5160

Update Package Version: 1.0.96396

License: Trial

-System Information-

OS: Windows 7 Service Pack 1

CPU: x64

File System: NTFS

User: System

-Scan Summary-

Scan Type: Threat Scan

Scan Initiated By: Scheduler

Result: Completed

Objects Scanned: 124326

Threats Detected: 11

Threats Quarantined: 11

Time Elapsed: 0 min, 57 sec

-Scan Options-

Memory: Enabled

Startup: Enabled

File system: Enabled

Archives: Enabled

Rootkits: Disabled

Heuristics: Enabled

PUP: Detect

PUM: Detect

-Scan Details-

Process: 0

(No malicious items detected)

Module: 0

(No malicious items detected)

Registry Key: 6

Trojan.Tasker, HKLM\SOFTWARE\MICROSOFT\WINDOWS

NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TREE\SearchFilterHost, Quarantined, 5741, 955239, 1.0.96396, , ame, , ,

Trojan.Tasker, HKLM\SOFTWARE\MICROSOFT\WINDOWS

NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{3C22E77B-1DAD-47F6-81A8-D8A83525C816}, Quarantined, 5741, 955239, 1.0.96396, , ame, , ,

Trojan.Tasker, HKLM\SOFTWARE\MICROSOFT\WINDOWS

NT\CURRENTVERSION\SCHEDULE\TASKCACHE\LOGON\{3C22E77B-1DAD-47F6-81A8-D8A83525C816}, Quarantined, 5741, 955239, 1.0.96396, , ame, , ,

Trojan.Tasker, HKLM\SOFTWARE\MICROSOFT\WINDOWS

NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TREE\System, Quarantined, 5741, 906855, 1.0.96396, , ame, , ,

Trojan.Tasker, HKLM\SOFTWARE\MICROSOFT\WINDOWS

NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{820F5FC6-37D7-4025-83CE-96014B

7A49B3}, Quarantined, 5741, 906855, 1.0.96396, , ame, , ,
Trojan.Tasker, HKLM\SOFTWARE\MICROSOFT\WINDOWS
NT\CURRENTVERSION\SCHEDULE\TASKCACHE\LOGON\{820F5FC6-37D7-4025-83CE-96014B
7A49B3}, Quarantined, 5741, 906855, 1.0.96396, , ame, , ,

Registry Value: 2

Trojan.Agent,
HKU\S-1-5-21-325657282-3775987751-4064538032-1000\SOFTWARE\MICROSOFT\WINDOWS\
CURRENTVERSION\RUN|WINLOGON, Quarantined, 9, 195982, 1.0.96396, , ame, , ,
Trojan.Agent,
HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN|WINLOGON,
Quarantined, 9, 196487, 1.0.96396, , ame, , ,

Registry Data: 1

Hijack.Shell, HKLM\SOFTWARE\MICROSOFT\WINDOWS
NT\CURRENTVERSION\WINLOGON|SHELL, Replaced, 1928, 1005206, 1.0.96396, , ame, , ,

Data Stream: 0

(No malicious items detected)

Folder: 0

(No malicious items detected)

File: 2

Trojan.Tasker, C:\WINDOWS\SYSTEM32\TASKS\SearchFilterHost, Quarantined, 5741, 955239,
1.0.96396, , ame, , 4D36A84571C825AA64C780C23EC44F23,
1EC9868362AEDEF935174F22B65B59A5E52FF0222C30567CB14BF9583BDFEB1D
Trojan.Tasker, C:\WINDOWS\SYSTEM32\TASKS\System, Quarantined, 5741, 906855, 1.0.96396,
, ame, , FC6772FEAF11688E6BB133F640F03437,
D0D8313B2D337D9EB47A96D3F25D54F7BBC06980B821388CAFB4197217DC1E98

Physical Sector: 0

(No malicious items detected)

WMI: 0

(No malicious items detected)

(end)

Tha Sneak - March 1, 2025, 8:45 pm

Please do NOT reply to this thread in case information needs to be added or edited.

If you have a questions about the contents of the thread or other tutorials please go to this thread and post your question in this thread: <https://hackforums.net/showthread.php?tid=6293473>

Thanks,

Tha Sneak