# Learn and use the Windows Malicious Software Removal Tool

The Microsoft Windows Malicious Software Removal Tool (MSRT) helps remove malware from Windows computers. This tutorial will show you how to open and use the Malicious Software Removal Tool to scan and remove specific common malware in Windows.

Microsoft Windows Malicious Software Removal Tool (MSRT) helps remove malware from computers running Windows 10, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows Server 2012 R2, Windows 8, Windows Server 2012, Windows 7 or Windows Server 2008.

Microsoft typically releases MSRT monthly as part of Windows Update or a standalone tool. Use this tool to find and remove specific common threats and reverse the changes they have made. For comprehensive malware detection and removal, consider using Microsoft Safety Scanner.

The Microsoft Malicious Software Removal Tool does not replace antivirus software. Therefore, you should still install and use up-to-date antivirus software. If you like, you can use Windows Defender on Windows 10 to kill viruses.

Microsoft Malicious Software Removal Tool differs from some antivirus products in three following points:

1. The tool removes malware from computers that have been infected with a virus. Antivirus software blocks malware from running on your computer. Preventing malware from running on your computer is more useful than removing it after being infected with a virus.
2. The tool only removes certain specific common malware. Specific malware is a small subset of malware today.
3. The tool focuses on detecting and removing active malware, which means that malware is running on the computer. Malware removal tool cannot run. However, antivirus software can perform this task.

Malicious Software Removal Tool runs in silent mode in the background. If you detect malware on your computer, the next time you log on to your computer as an administrator, you'll see a notification in the notification area that says your computer is infected with a virus.

**Perform a full computer scan**

If the tool finds malware, you should perform a full scan of the computer. This process will perform a quick scan first and then a full scan of the computer whether or not a quick scan finds malware. This process can take several hours as it will scan all fixed and removable drives. However, it does not scan mapped network drives.

**Remove malicious files**

If the malware modifies files on the computer, the tool will notify the user to remove malware from these files. If malware modifies browser settings, the homepage may be changed automatically to a page that provides instructions on how to restore this setting.

You can delete specific files or all the infected files found by the tool. However, you should be aware that some data may be lost during this process. In addition, the tool may not be able to restore some files to their original, uninfected original state.

The tool may require you to restart your computer to complete the removal of some malware or notify users to take manual steps to complete the malware removal process. To completely remove malware, you should use anti-virus software.

**Report malware infection information to Microsoft**

Malicious Software Removal Tool will send basic information to Microsoft if it detects malware or finds an error. This information is used to monitor the rate of virus infection. You do not need to worry as it will not send personally identifiable information related to you and the computer in this report.

This tutorial will show you how to open and use the Malicious Software Removal Tool (MSRT) to scan and remove specific specific malware in Windows.

**Note:** Get the scanning signature of the Malicious Software Removal Tool stored in C: WindowsDebugmrt.log.

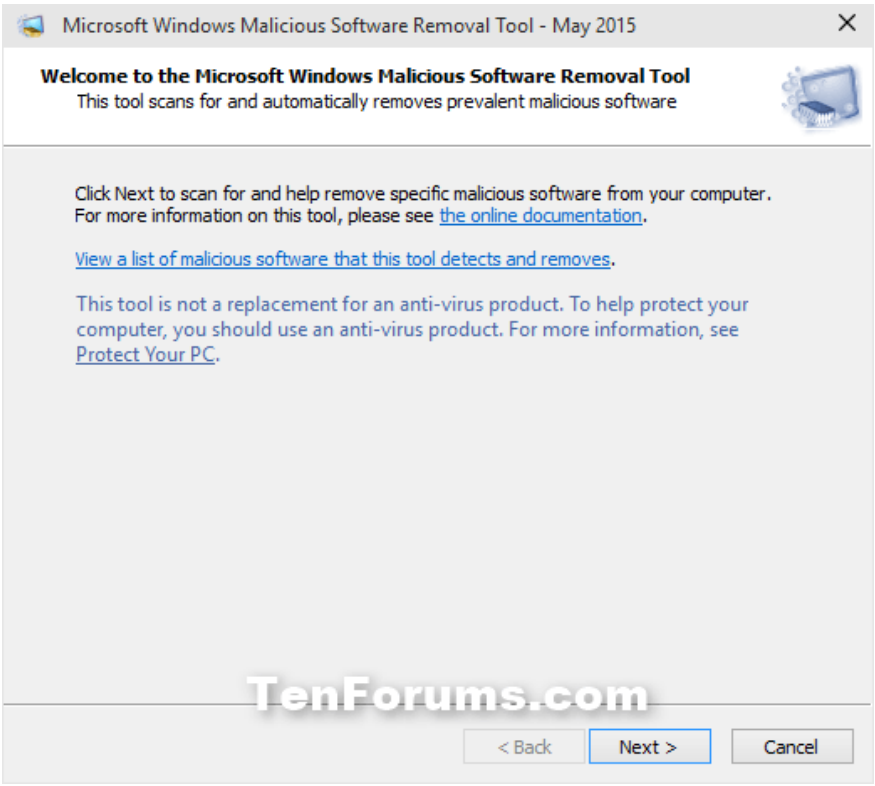
Microsoft releases a new version of the Malicious Software Removal Tool on the second Tuesday of each month. MSRT is updated in Windows with Windows Update KB890830. You can download and install MSRT for 32-bit Windows (x86) or 64-bit (x64).

`https://www.microsoft.com/en-us/download/malicious-software-removal-tool-details`

# 1. Open and use the Malicious Software Removal Tool

**Step 1** . Type **mrt** (C: WindowsSystem32MRT.exe) in the search box ( `Windows` + `S` ) on the Start menu or Taskbar and press **Enter** to open the Malicious Software Removal Tool.

**Step 2** . Click on **Next** .

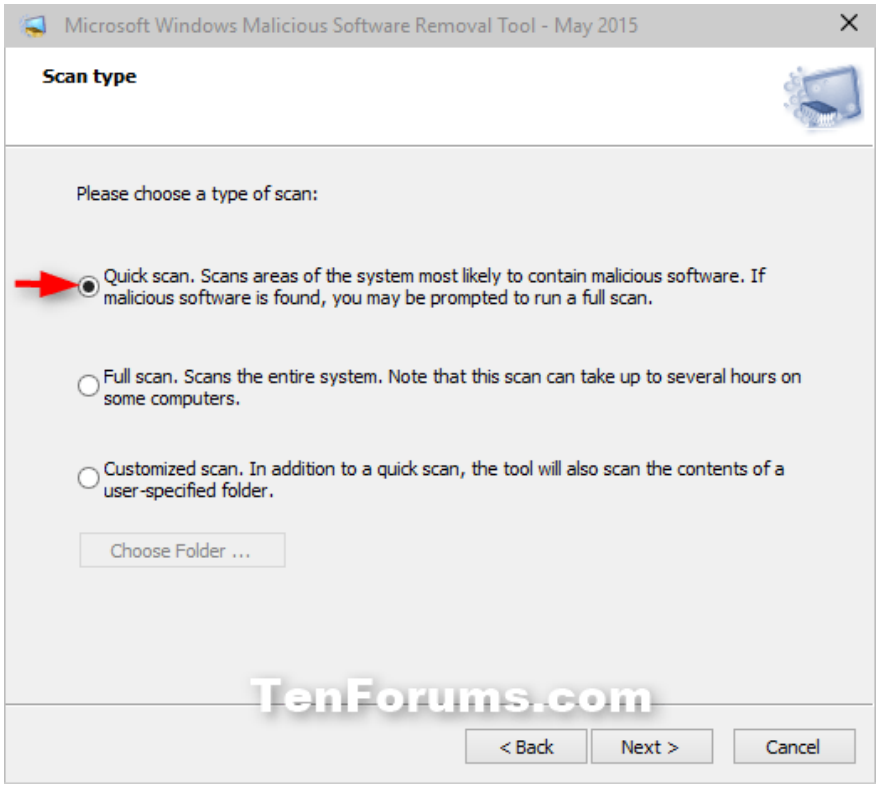



**Step 3** . Perform **Step 4** (Quick Scan), **Step 5** (Full System Scan) or **Step 6** (Custom Scan).

**Step 4.** Perform a quick scan with MSRT

**Note:** This option scans areas of the system that may contain malware. If malware is detected, it will notify users to perform a full system scan.

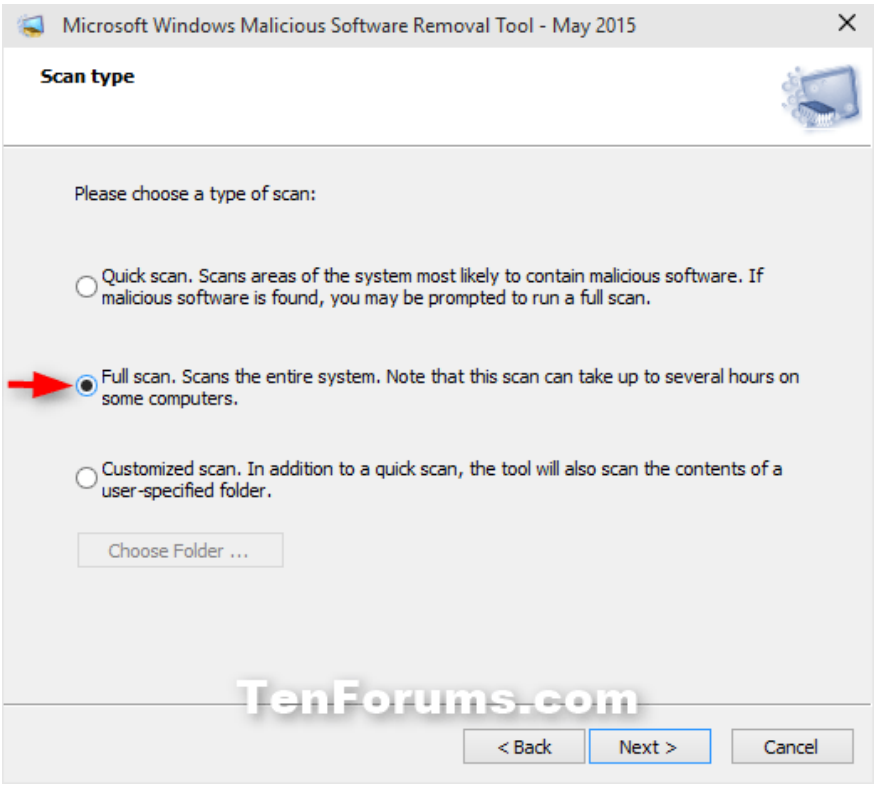
Select **Quick scan** , click on **Next** and go to **Step 7** .




**Step 5** . Perform a full system scan with MSRT

**Note:** This option will scan your entire system and this may take several hours depending on how much data you want to scan.

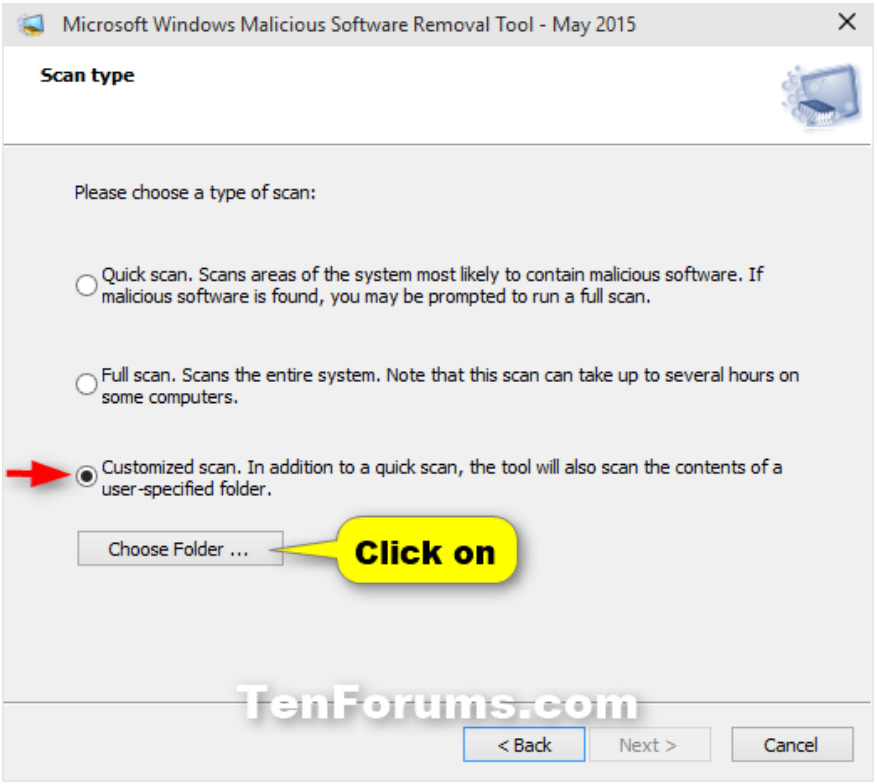
Select **Full scan** , click **Next** and go to **Step 7** .



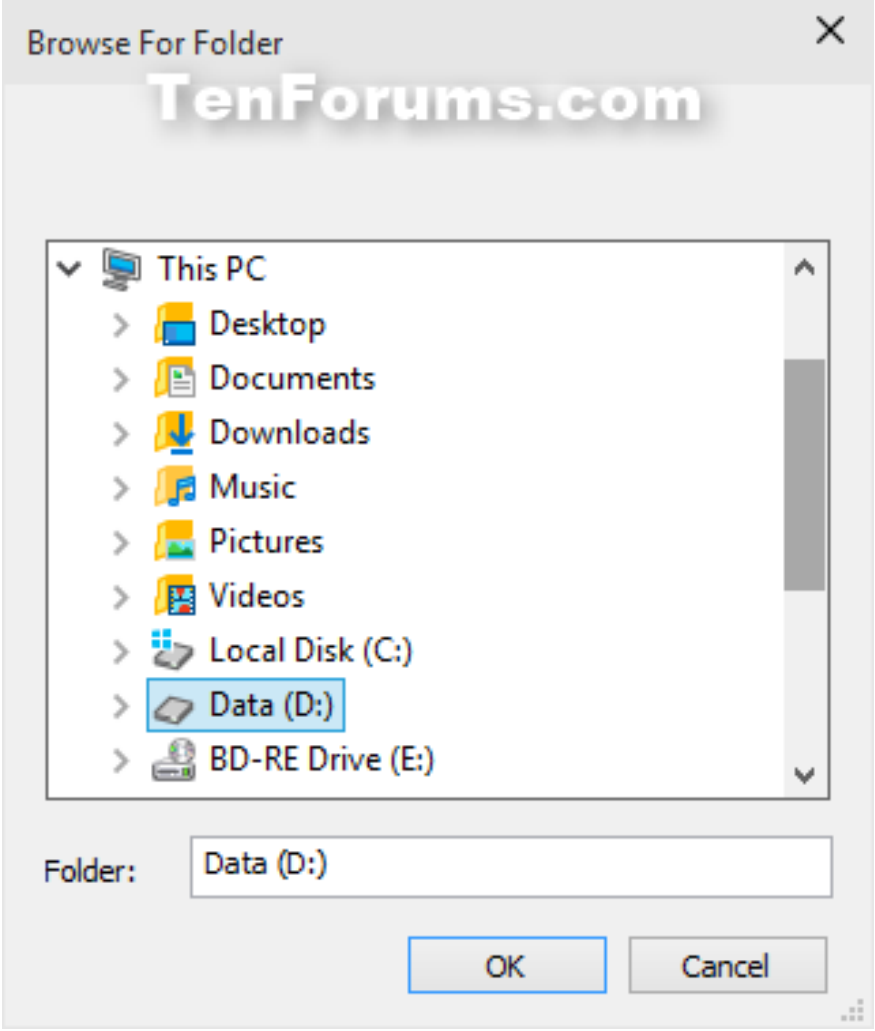

**Step 6.** Perform custom scans with MSRT

**Note** : This option will perform a quick scan first, then scan the contents of the folder or hard drive you specify.

Select **Customized scan** and click on **Choose Folder** .

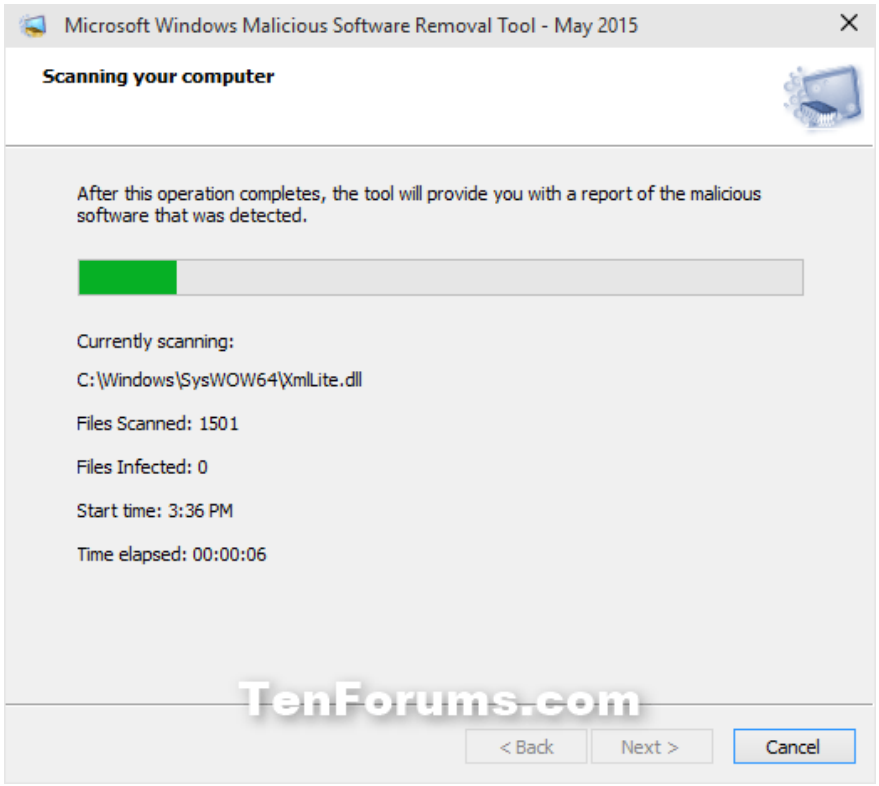


Browse and select the folder or hard drive you want to scan, click on **OK** .

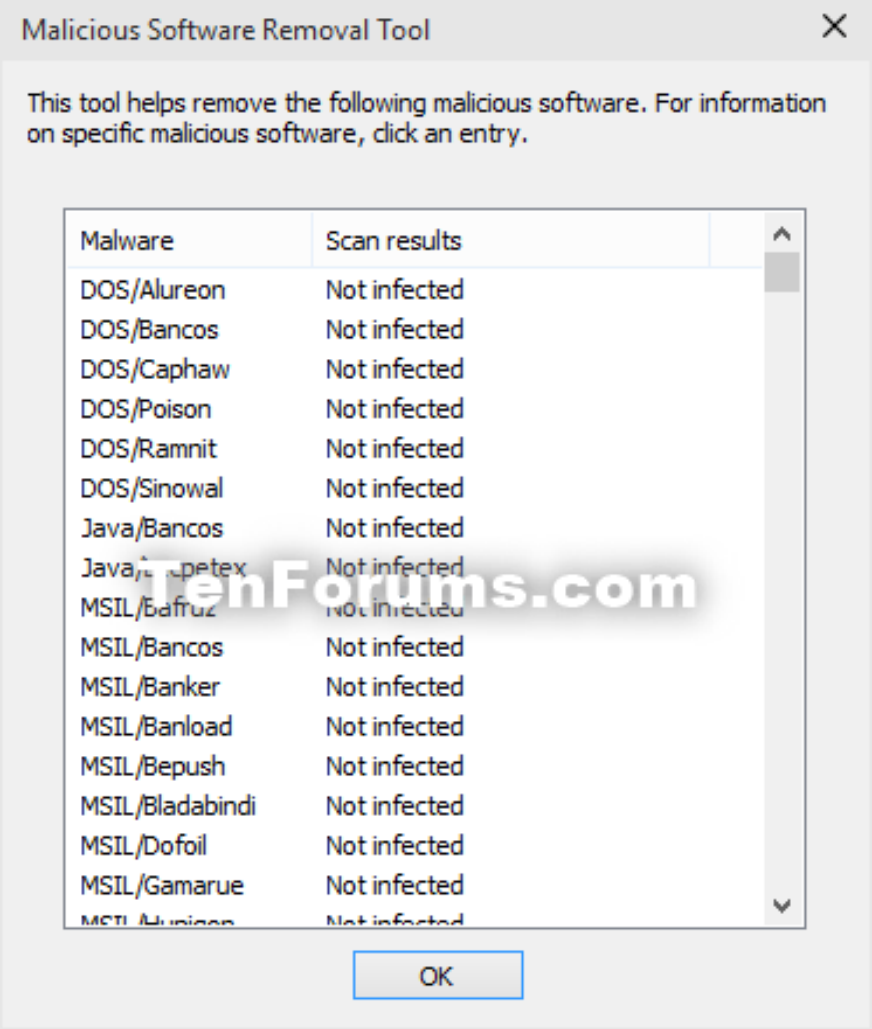



Click **Next** and go to **Step 7** .

**Step 7** . MSRT will start scanning the computer.




**Step 8** . When done, you will see the results, click on the **View detailed results of the scan link** . When done, click on **Finish** .




## 2. Run the Malicious Software Removal Tool in the Command Prompt

**Step 1** . Open Command Prompt as admin.

**Step 2** . In the Command Prompt, copy and paste the command below you want to use and press **Enter** .

1. **MRT / F** : Open the MSRT user interface and perform a full system scan.
2. **MRT / F / Q** : Perform a full system scan without opening the MSRT user interface.
3. **MRT / F: Y** : Open the MSRT user interface, perform a full system scan and automatically delete infected files.
4. **MRT / F: Y / Q** : Performs a mandatory full scan on automatically deleting infected files without opening the MSRT user interface.

I wish you successful implementation!