download windows 10 malicious removal tool

What is the Malicious Software Removal Tool and Do I Need It?

Once a month, a new version of the Malicious Software Removal tool appears in Windows Update. This tool removes some malware from Windows systems, particularly those systems without antivirus programs installed.

Bear in mind that this tool is no substitute for a solid antivirus program. It doesn't run automatically in the background at all times, and only detects a few specific and widespread types of malware.

What is the Malicious Software Removal Tool?

Microsoft releases a new version of this tool on the second Tuesday of every month — in other words, on "Patch Tuesday." It appears as just another patch in Windows Update. If you have your computer set to automatically install Windows Updates, it will be installed automatically. If you install updates manually, you've probably been installing it as part of the manual update process — it's considered an important update, not just a recommended one.

After Windows downloads the newest version of the Microsoft Malicious Software Removal tool, it will automatically run it in the background. This tool checks for specific, widespread types of malware and removes them if it finds them. If everything is fine, Windows will run the tool silently in the background without bothering you. If it finds a infection and fixes it, the tool will display a report telling you which malicious software was detected and will be removed after you restart your computer.

Microsoft introduced this tool back in the days of Windows XP, when Windows was very insecure — the first release of Windows XP didn't even have a firewall enabled by default. Microsoft's Malicious Software Removal Tool page says "This tool checks your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps to remove the infection if it is found." Note the three types of malware still described here in 2014 — these were widespread worms that infected many Windows XP systems back in 2003 and 2004, ten years ago. Microsoft introduced this tool to purge these widespread worms and other popular types of malware from Windows XP system without antivirus software installed.

Do I Need to Run This Tool?

You shouldn't need to worry about this tool. Set Windows to automatically install updates, or have Windows alert you to updates and install it along with the other new security updates when they appear every month. The tool will check your computer in the background and stay silent if everything is fine.

All you need to do is ensure the update is installed from Windows Update. You don't have to worry about running the tool manually, although you can. This tool doesn't stay running in the background and scan everything you open, so it's compatible with other antivirus programs and won't interfere with them.

Why You Still Need an Antivirus.

This tool is nowhere near a replacement for an antivirus. It only covers specific types of malware, so it won't purge all infections. It also only quickly scans the normal locations for the malware and won't scan your entire system. Worse yet, the tool only runs once every month and doesn't scan in the background. This means your computer could become infected and it wouldn't be fixed until a month later when a new version of the tool arrives.

The Malicious Software Removal Tool is a weapon Microsoft uses to purge worms and other nasty malware from infected systems so they don't stay infected for years. It's not a tool that will help protect you in your day-to-day computer use. If you'd like to see the full list of malware it removes, you can download the tool, run it manually, and click the "View detailed results of the scan" link after running a scan to see all the different types of malware it checked for.

Microsoft will continue updating this tool for Windows XP until July 14, 2015, even though they're ending support for Windows XP on April 8, 2014. But it's no substitute for having a patched operating system and using a solid antivirus program.

Manually Running the Tool and Viewing Logs.

You don't need to run the tool manually. If you suspect your computer is infected, you're better off scanning it with a dedicated antivirus program that can detect much more malware. If you really want to run the tool manually, you can download it from Microsoft's download page and run it like any other .exe file.

When you run the tool in this way, you'll see a graphical interface. The tool performs a Quick scan when you run it in the background, but you can also perform a Full scan or Customized scan to scan your entire system or specific folders if you run it manually.

After the tool runs — either manually or automatically in the background — it will create a log file you can view. This file is located at %WINDIR%\debug\mrt.log — that's C:\Windows\debug\mrt.log by default. You can open this file in Notepad or any other text editor to see the results of the scan. If you see a mostly empty log file with no problem reports, the tool didn't detect any problems.

So that's why the Malicious Software Removal Tool keeps popping up in Windows Update. You shouldn't ever have to pay attention to this tool. As long as you're running a good antivirus program, it will do a quick double-check in the background every month and not bother you.

Remove specific prevalent malware with Windows Malicious Software Removal Tool (KB890830)

The Windows Malicious Software Removal Tool (MSRT) helps remove malicious software from computers that are running any of the following operating systems:

Windows Server 2019.

Windows Server 2016.

Windows Server 2012 R2.

Windows Server 2012.

Windows Server 2008 R2.

Windows Server 2008.

Microsoft releases the MSRT on a monthly cadence as part of Windows Update or as a standalone tool. Use this tool to find and remove specific prevalent threats and reverse the changes they have made (see covered malware families). For comprehensive malware detection and removal, consider using Windows Defender Offline or Microsoft Safety Scanner.

This article contains information about how the tool differs from an antivirus or antimalware product, how you can download and run the tool, what happens when the tool finds malware, and tool release information. It also includes information for the administrators and advanced users, including information about supported command-line switches.

In compliance with the Microsoft Support Lifecycle policy, the MSRT is no longer supported on Windows Vista or earlier platforms. For more information, go to Microsoft Support Lifecycle.

If you are having problems in regards to an MSRT update within Windows Update, see Troubleshooting problems updating Windows 10.

More information.

The MSRT does not replace an antivirus product. It is strictly a post-infection removal tool. Therefore, we strongly recommend that you install and use an up-to-date antivirus product.

The MSRT differs from an antivirus product in three important ways:

The tool removes malicious software from an already-infected computer. Antivirus products block malicious software from running on a computer. It is significantly more desirable to block malicious software from running on a computer than to remove it after infection.

The tool removes only specific prevalent malicious software. Specific prevalent malicious software is a small subset of all the malicious software that exists today.

The tool focuses on the detection and removal of active malicious software. Active malicious software is malicious software that is currently running on the computer. The tool cannot remove malicious software that is not running. However, an antivirus product can perform this task.

For more information about how to protect your computer, go to the Microsoft Safety & Security Center website.

Note The MSRT focuses on the detection and removal of malicious software such as viruses, worms, and Trojan horses only. It does not remove spyware.

You do not have to disable or remove your antivirus program when you install the MSRT. However, if prevalent, malicious software has infected your computer, the antivirus program may detect this malicious software and may prevent the removal tool from removing it when the removal tool runs. In this case, you can use your antivirus program to remove the malicious software.

Because the MSRT does not contain a virus or a worm, the removal tool alone should not trigger your antivirus program. However, if malicious software infected the computer before you installed an up-to-date antivirus program, your antivirus program may not detect this malicious software until the tool tries to remove it.

Note: Starting November 2019, MSRT will be SHA-2 signed exclusively. Your devices must be updated to support SHA-2 in order to run MSRT. To learn more, see 2019 SHA-2 Code Signing Support requirement for Windows and WSUS.

The easiest way to download and run the MSRT is to turn on Automatic Updates. Turning on Automatic Updates guarantees that you receive the tool automatically. If you have Automatic Updates turned on, you have already been receiving new versions of this tool. The tool runs in Quiet mode unless it finds an infection. If you have not been notified of an infection, no malicious software has been found that requires your attention.

Enabling automatic updates.

To turn on Automatic Updates yourself, follow the steps in the following table for the operating system that your computer is running.

If your computer is running:

Follow these steps:

Select the Start button, then select Settings > Update & security > Windows Update . If you want to check for updates manually, select Check for updates.

Select Advanced options , and then under Choose how updates are installed , select Automatic (recommended) .

Note Windows 10 is a service. This means that automatic updates are turned on by default and your PC always has the latest and best features.

Open Windows Update by swiping in from the right edge of the screen (or, if you're using a mouse, pointing to the lower-right corner of the screen and moving the mouse pointer up), select Settings > Change PC settings > Update and recovery > Windows Update . If you want to check for updates manually, select Check now .

Select Choose how updates get installed , and then under Important updates , select Install updates automatically (recommended) .

Under Recommended updates , select the Give me recommended updates the same way I receive important updates check box.

Under Microsoft Update , select the Give me updates for other Microsoft products when I update Windows check box, and then select Apply .

Click Start , point to All Programs , and then click Windows Update .

In the left pane, click Change settings .

Click to select Install updates automatically (recommended) .

Under Recommended updates , click to select the Give me recommended updates the same way I receive important updates check box, and then click OK . If you are prompted for an administrative password or for confirmation, type the password or provide confirmation. Go to step 3.

Download the MSRT. You must accept the Microsoft Software License Terms. The license terms are only displayed for the first time that you access Automatic Updates.

Note After you accept the one-time license terms, you can receive future versions of the MSRT without being logged on to the computer as an administrator.

The MSRT runs in Quiet mode. If it detects malicious software on your computer, the next time that you log on to your computer as a computer administrator, a balloon appears in the notification area to make you aware of the detection.

Performing a full scan.

If the tool finds malicious software, you may be prompted to perform a full scan. We recommend that you perform this scan. A full scan performs a quick scan and then a full scan of the computer, regardless of whether malicious software is found during the quick scan. This scan can take several hours to complete because it will scan all fixed and removable drives. However, mapped network drives are not scanned.

Removing malicious files.

If malicious software has modified (infected) files on your computer, the tool prompts you to remove the malicious software from those files. If the malicious software modified your browser settings, your homepage may be changed automatically to a page that gives you directions on how to restore these settings.

You can clean specific files or all the infected files that the tool finds. Be aware that some data loss is possible during this process. Also, be aware that the tool may be unable to restore some files to the original, pre-infection state.

The removal tool may request that you restart your computer to complete the removal of some malicious software, or it may prompt you to perform manual steps to complete the removal of the malicious software. To complete the removal, you should use an up-to-date antivirus product.

Reporting infection information to Microsoft The MSRT sends basic information to Microsoft if the tool detects malicious software or finds an error. This information will be used for tracking virus prevalence. No identifiable personal information that is related to you or to the computer is sent together with this report.

The MSRT does not use an installer. Typically, when you run the MSRT, it creates a randomly named temporary directory on the root drive of the computer. This directory contains several files, and it includes the Mrtstub.exe file. Most of the time, this folder is automatically deleted after the tool finishes running or after the next time that you start the computer. However, this folder may not always be automatically deleted. In these cases, you can manually delete this folder, and this has no adverse effect on the computer.

How to receive support.

Help protect your computer that is running Windows from viruses and malware: Virus Solution and Security Center.

Local support according to your country: International Support.

Microsoft Download Center.

Note: Starting November 2019, MSRT will be SHA-2 signed exclusively. Your devices must be updated to support SHA-2 in order to run MSRT. To learn more, see 2019 SHA-2 Code Signing Support requirement for Windows and WSUS.

You can manually download the MSRT from the Microsoft Download Center. The following files are available for download from the Microsoft Download Center:

For 32-bit x86-based systems:

For 64-bit x64-based systems:

Release Date: June 8, 2021.

For more information about how to download Microsoft support files, see How to obtain Microsoft support files from online services.

Microsoft scanned this file for viruses. Microsoft used the most current virus-detection software that was available on the date that the file was posted. The file is stored on security-enhanced servers that help prevent any unauthorized changes to the file.

Deploying the MSRT in an enterprise environment.

If you are an IT administrator who wants more information about how to deploy the tool in an enterprise environment, see Deploy Windows Malicious Software Removal Tool in an enterprise environment.

This article includes information about Microsoft Systems Management Server (SMS), Microsoft Software Update Services (MSUS), and Microsoft Baseline Security Analyzer (MBSA).

Except where noted, the information in this section applies to all the ways that you can download and run the MSRT:

The Microsoft Download Center.

The MSRT website on Microsoft.com.

To run the MSRT, the following conditions are required:

The computer must be running a supported version of Windows.

You must log on to the computer by using an account that is a member of the Administrators group. If your logon account does not have the required permissions, the tool exits. If the tool is not being run in quiet mode, it displays a dialog box that describes the failure.

If the tool is more than 215 days (7 months) out of date, the tool displays a dialog box that recommends that you download the latest version of the tool.

Support for command-line switches.

The MSRT supports the following command line switches.

Uses quiet mode. This option suppresses the user interface of the tool.

Displays a dialog box that lists the command-line switches.

Runs in detect-only mode. In this mode, malicious software will be reported to the user, but it will not be removed.

Forces an extended scan of the computer.

Forces an extended scan of the computer and automatically cleans any infections that are found.

Usage and release information.

When you download the tool from Microsoft Update or from Automatic Updates, and no malicious software is detected on the computer, the tool will run in quiet mode next time. If malicious software is detected on the computer, the next time that an administrator logs on to the computer, a balloon will appear in the notification area to notify you of the detection. For more information about the detection, click the balloon.

When you download the tool from the Microsoft Download Center, the tool displays a user interface when it runs. However, if you supply the /Q command-line switch, it runs in quiet mode.

Release information.

The MSRT is released on the second Tuesday of each month. Each release of the tool helps detect and remove current, prevalent malicious software. This malicious software includes viruses, worms, and Trojan horses. Microsoft uses several metrics to determine the prevalence of a malicious software family and the damage that can be associated with it.

This Microsoft Knowledge Base article will be updated with information for each release so that the number of the relevant article remains the same. The name of the file will be changed to reflect the tool version. For example, the file name of the February 2020 version is Windows-KB890830-V5.80.exe, and the file name of the May 2020 version is Windows-KB890830-V5.82-ENU.exe.

The following table lists the malicious software that the tool can remove. The tool can also remove any known variants at the time of release. The table also lists the version of the tool that first included detection and removal for the malicious software family.

How to Uninstall Malware Programs Using "Add/Remove Programs" Tool.

The instructions below describe how to manually remove malicious programs using the Windows "Add/Remove Programs" tool. It is recommended that before uninstalling malicious programs that you back up your computer (or sensitive applications or documents) before removing any software from your hard drive. Check for programs that you don't remember installing, or are related to the program you found on the System Tray. Be careful not to remove system files or patches! Keep in mind that some malicious parasites do not come with an uninstall program, therefore the malware program will not appear in the "Add/Remove Programs" panel.

To uninstall a malware program, you must do the following:

Note: This process is NOT 100% effective. It is likely that malicious files or folders still remain in your PC after manual removal. To prevent further infection, please use this spyware detection tool as an automatic solution.

For Windows XP in the default XP view.

Click on the Windows "Start" button and click on the "Control Panel" . In the "Control Panel" window, double-click "Add/Remove Programs" icon. When the "Add/Remove Programs" window has fully populated, locate the malware program you wish to uninstall in the list of currently installed programs. Click on the entry to select it, and then click the "Add/Remove" or "Change/Remove" button. To finish the removal process, just follow the simple instructions in the wizard screen that comes up.

Once you've completed the removal process, it's recommended that you reboot your computer and go back to the "Add/Remove Programs" to check whether the malicious program is still present.

For Windows 95, 98, Me, NT, 2000, and XP in the classic view.

Click on the Windows "Start" button, select "Settings" , and then click on the "Control Panel" . In the "Control Panel" window, double-click "Add/Remove Programs" icon. When the "Add/Remove Programs" window has fully populated, locate the malware program you wish to uninstall in the list of currently installed programs. Click on the entry to select it, and then click the "Add/Remove" or "Change/Remove" button. To finish the removal process, just follow the simple instructions in the wizard screen that comes up.

Once you've completed the removal process, it's recommended that you reboot your computer and go back to the "Add/Remove Programs" to check whether the malicious program is still present.

One Comment.

I REALLY NEED AN ANSWER ON THIS. I want Spyhunter OFF my computer. How do I uninstall it? I hate this program and it does me no good at all. All it does is slow down my computer. I WANT IT OFF NOW. This is a total scam.

How to Remove Malware.

This article was co-authored by Jeremy Mercer. Jeremy Mercer is the Manager and Head Technician at MacPro-LA in Los Angeles, CA. He has over ten years of experience working in electronics repair, as well as retail stores that specialize in both Mac and PC.

The wikiHow Tech Team also followed the article's instructions and verified that they work.

This article has been viewed 91,400 times.

This wikiHow teaches you how to scan for (and remove) malware from your PC or Mac without purchasing additional software. Windows comes with a free antivirus/anti-malware tool called Windows Defender that works great to remove viruses, adware, and spyware. If malware is preventing you from running a scan, you can use the Malicious Software Removal Tool, which can be downloaded from Microsoft. Mac malware can be removed by dragging the app to the Trash.

Why no windows malicious software removal tool download on September 2019 patch Tuesday for win 10 1903?

My name is Anthony, an Independent Advisor trying to help.

The Windows Malicious Software Removal Tool (MSRT) helps keep Windows computers free of frequent malware. MSRT finds and eliminates threats and reverses the changes they have made.

In this case, these are the compatible operating system:

Windows 10; Windows 10 Tech Preview; Windows 7; Windows 8; Windows 8.1; Windows Server 2008; Windows Server 2008 R2; Windows Server 2012; Windows Server 2012 R2; Windows Server 2016; Windows Server Tech Preview.