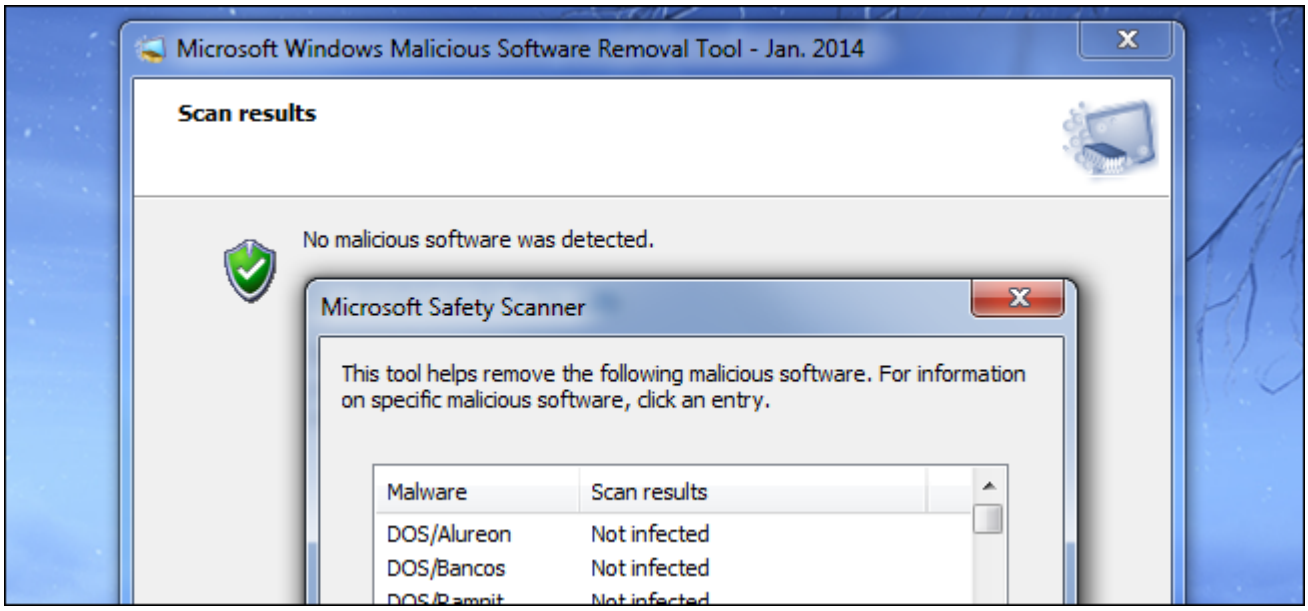
What is the Malicious Software Removal Tool and Do I Need It?

By Chris Hoffman on January 29th, 2014

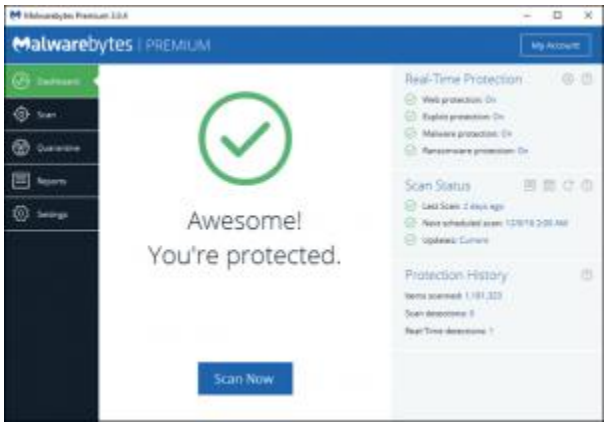


Once a month, a new version of the Malicious Software Removal tool appears in Windows Update. This tool removes some malware from Windows systems, particularly those systems without antivirus programs installed.

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.

Run Malwarebytes Alongside Your Antivirus for Maximum Protection

---



Running antivirus is still very important, but these days the really active threats are from spyware, adware, crapware, and the worst of all: ransomware. That's where Malwarebytes comes in.

Malwarebytes not only protects your computer from malware, but does a better job of cleaning up an infected computer than anything else on the market. And it doesn't just work on PCs — they have a Mac version too.

And to protect your browser against zero-day exploits, Malwarebytes also includes Anti-Exploit and Anti-Ransomware features, which can stop drive-by attacks cold. And best of all, you can run Malwarebytes alongside your existing antivirus to keep yourself fully protected.

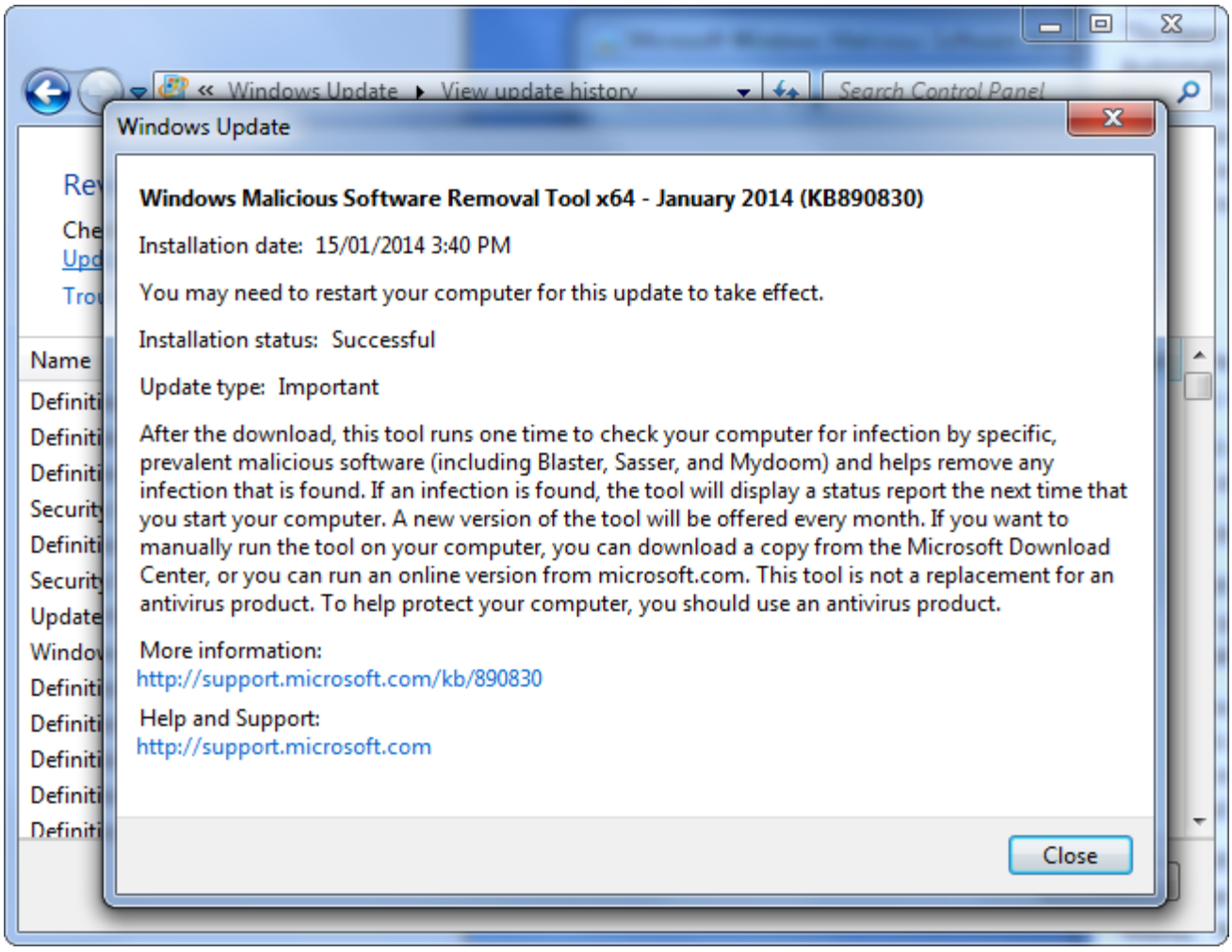
Download Malwarebytes Today

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.

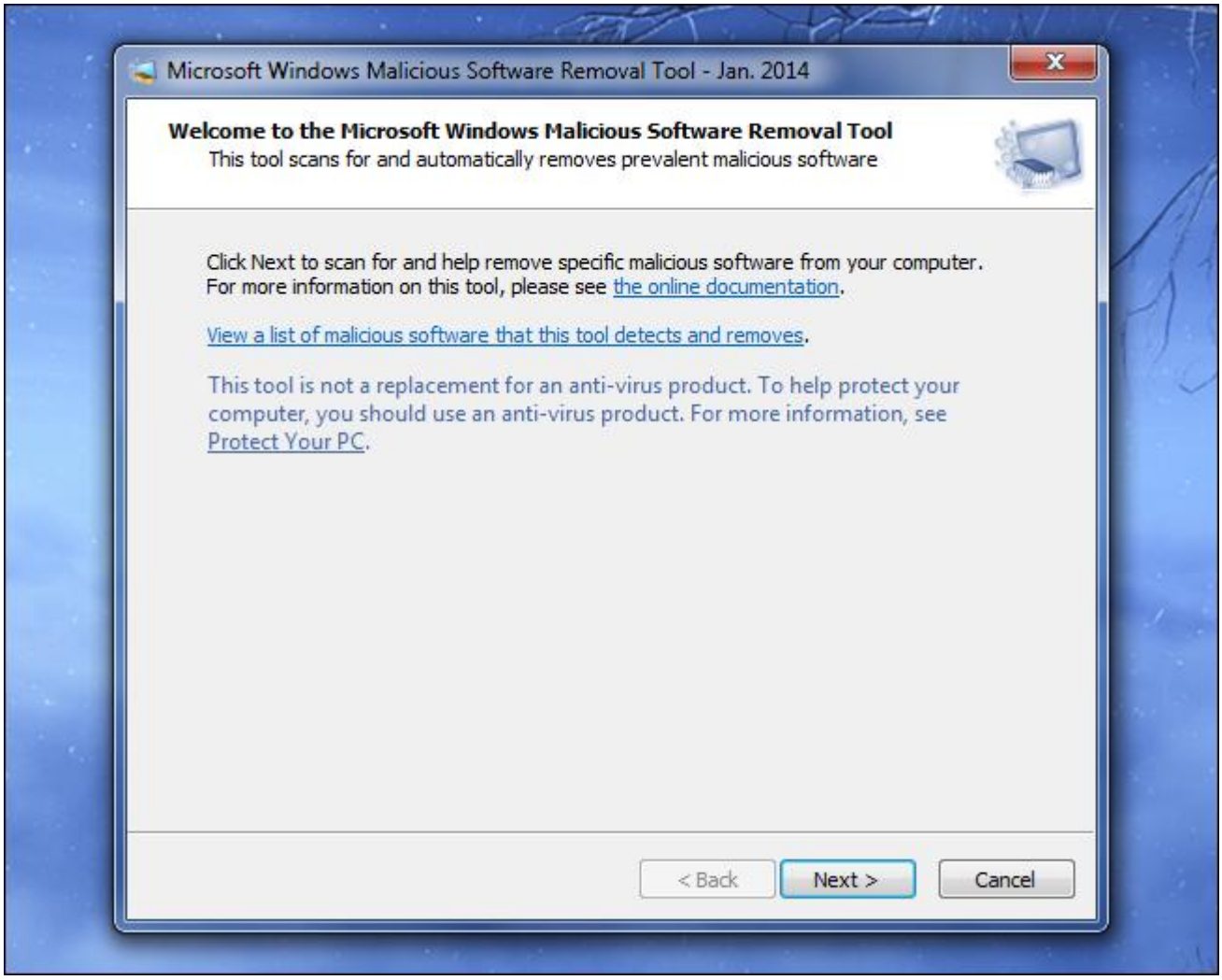
Microsoft introduced this tool back in the days of Windows XP, when Windows was very insecure — the first release of Windows XP didn't even have a firewall enabled by default. Microsoft's Malicious Software Removal Tool page says "This tool checks your computer for infection by specific, prevalent malicious 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.

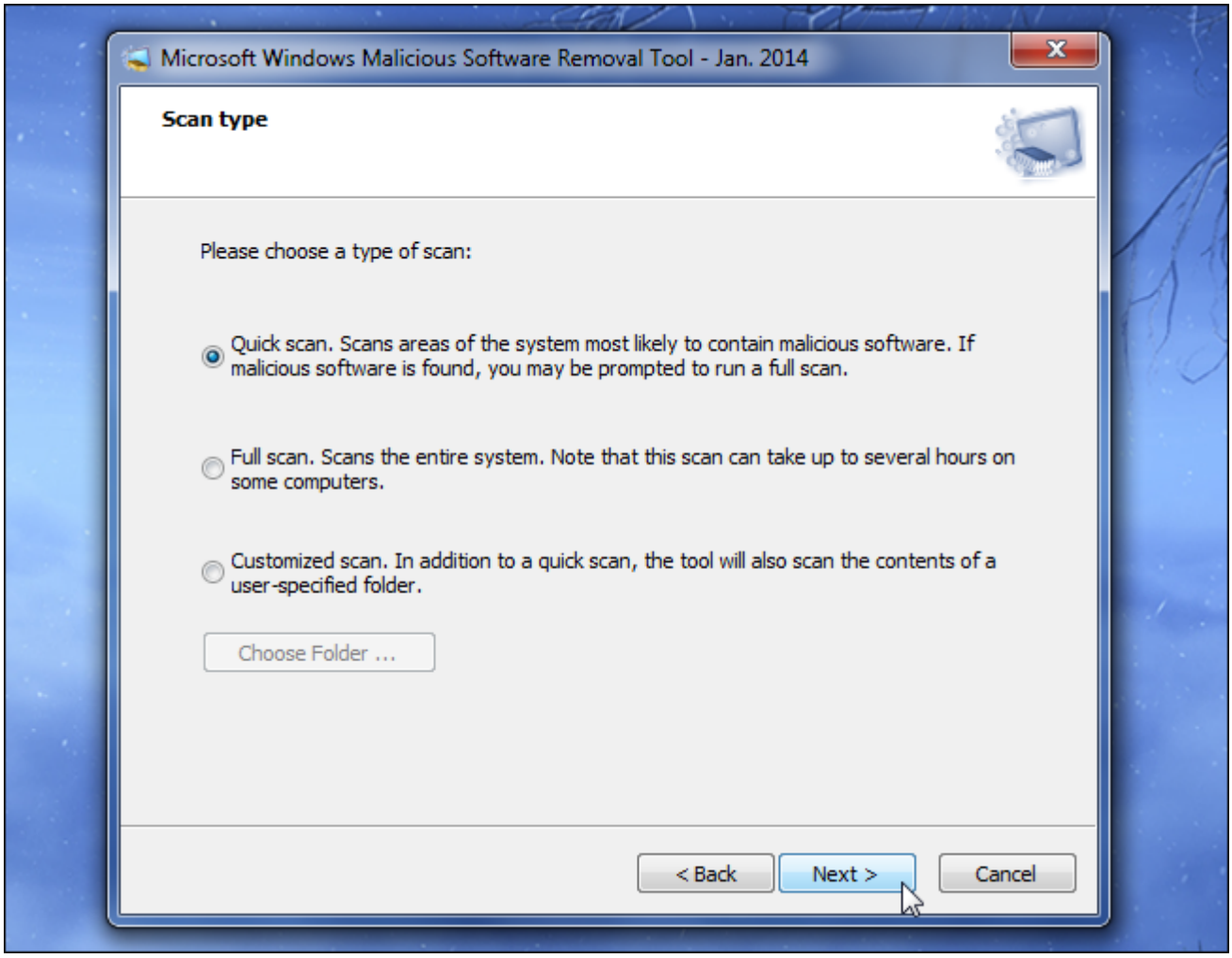


Why You Still Need an Antivirus

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.

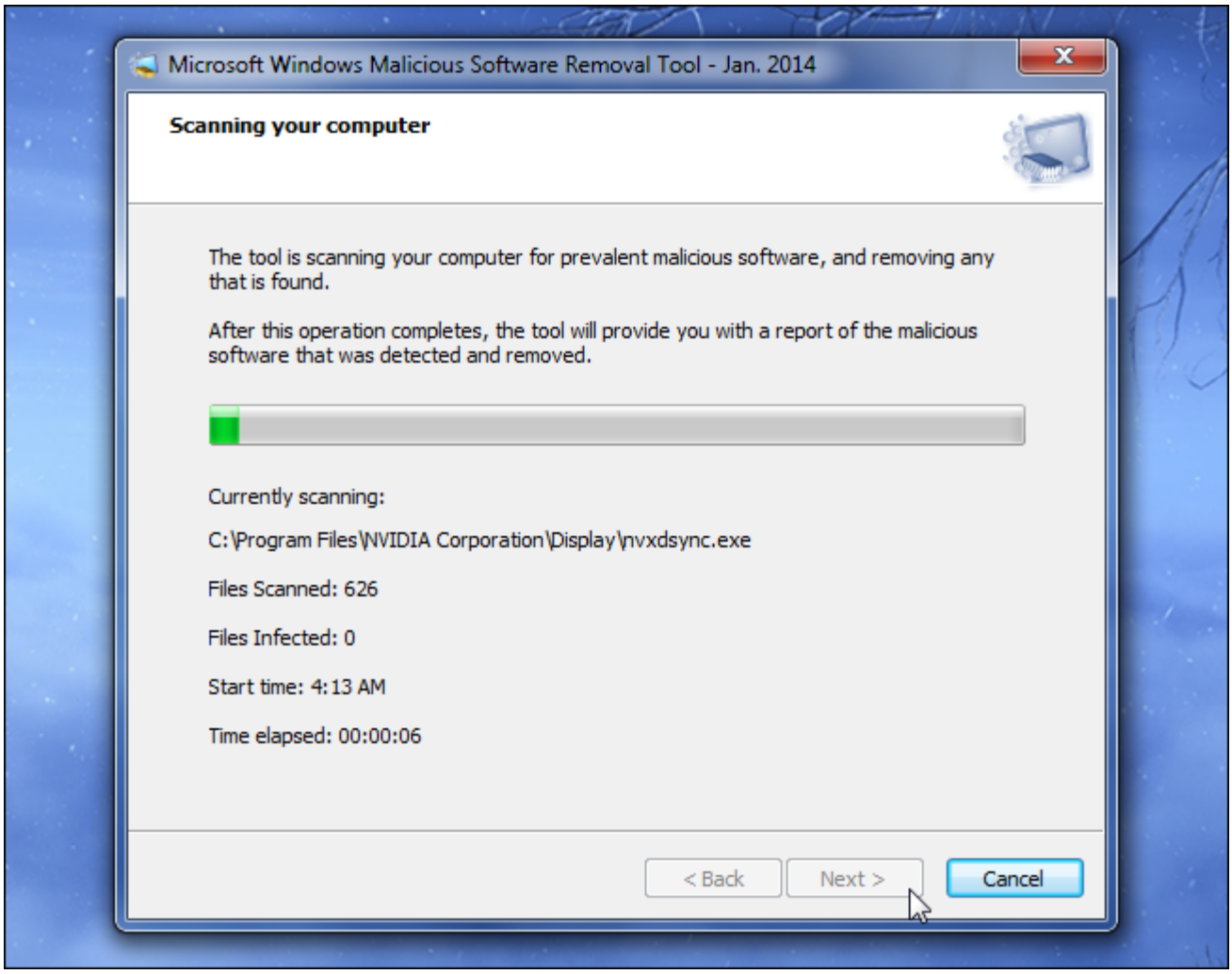
Microsoft will continue updating this tool for Windows XP until July 14, 2015, even though they're ending support for Windows XP on April 8, 2014. But it's no substitute for having a patched operating system and using a solid antivirus program.



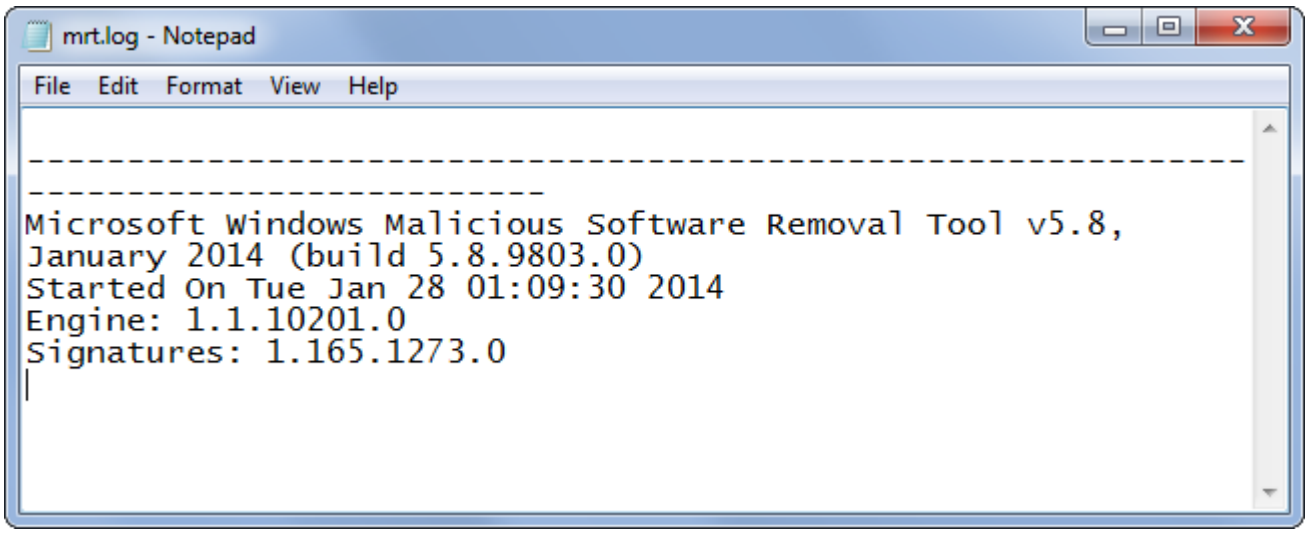
Manually Running the Tool and Viewing Logs

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.