How to Remove Windows Malware for Free

Posted 04/06/2015 at 1:25pm | by Paul Lilly

Return a bug-infested PC to pristine condition

Your smartphone begins to vibrate. Not the quick vibration that would indicate it's an incoming text message, but a longer one associated with a phone call. Yes, people still communicate via voice, and thanks to Caller ID, you know it's your parents on the other end. It's been a few weeks since you've heard from them and a funny feeling begins to fill the pit of your stomach. You know what's coming next.

A plea for PC help. You listen intently as your folks describe hijacked web searches, a toolbar they don't recognize, and sluggish behavior. Oh, and there are pop-ups. Lots and lots of pop-ups. The list of ailments goes on like a kid reciting a Christmas list to Santa Clause. Only instead of toys and candy, it's rogue programs and malware. It's a good thing you installed TeamViewer because trying to fix the problem over the phone is a time-consuming process that always ends the same way—"I'll be over in the morning."

Or maybe you didn't install TeamViewer and you really will be over in the morning. Either way, the task at hand is to rid a system of malware. Perhaps it's your own system, especially if you let little Billy and sweet little Suzy hop on for a spell. Whatever the case may be, don't panic. **Removing malware, while seemingly daunting, isn't all that difficult. Like anything else, you just need the proper know-how and tools, both of which we'll provide here**. Be sure to read the entire guide before embarking on your malware removal journey.

Scrub the Browser(s)

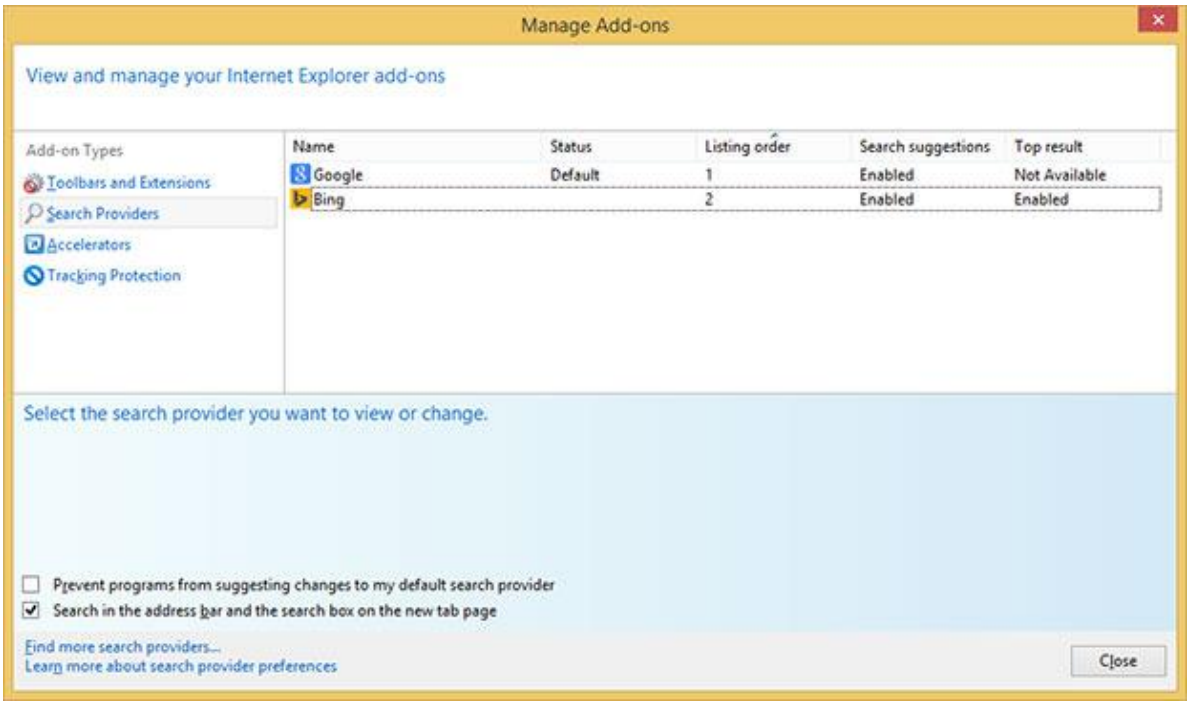
Toolbars, hijacked web searches, and pop-ups are often the result of malware, adware, and or other unwanted-ware that was either installed without permission, or sneaked in through a legitimate application through the fine print, usually when installing a free program. That Spongebob screensaver pack that little Billy installed from a site he can't remember? Yeah, we're guessing he mashed the "Okay" or "Next" button throughout the process, at one point agreeing to change your browser's settings. Cut him some slack, the kid still eats his boogers.

Luckily, these are usually easy fixes. Here's what you need to do.

Internet Explorer

Let's start with Internet Explorer. Click the **Gear (Tools)** icon in the upper-right corner and select **Manage add-ons**. On the left-hand side is a column of categories: Toolbars and Extensions, Search Providers, Accelerators, and Tracking Protection. It's the first three that are of interest, starting with Toolbars and Extensions.

See anything you don't recognize? Maybe something like "DealBuddy" or some other descriptor that's a clear giveaway? Click it and select **Remove** or **Disable**. If it's an entry you don't recognize, look it up on Google or your search engine of choice. In most cases, however, unwanted entries will stick out like a pimple on prom night.

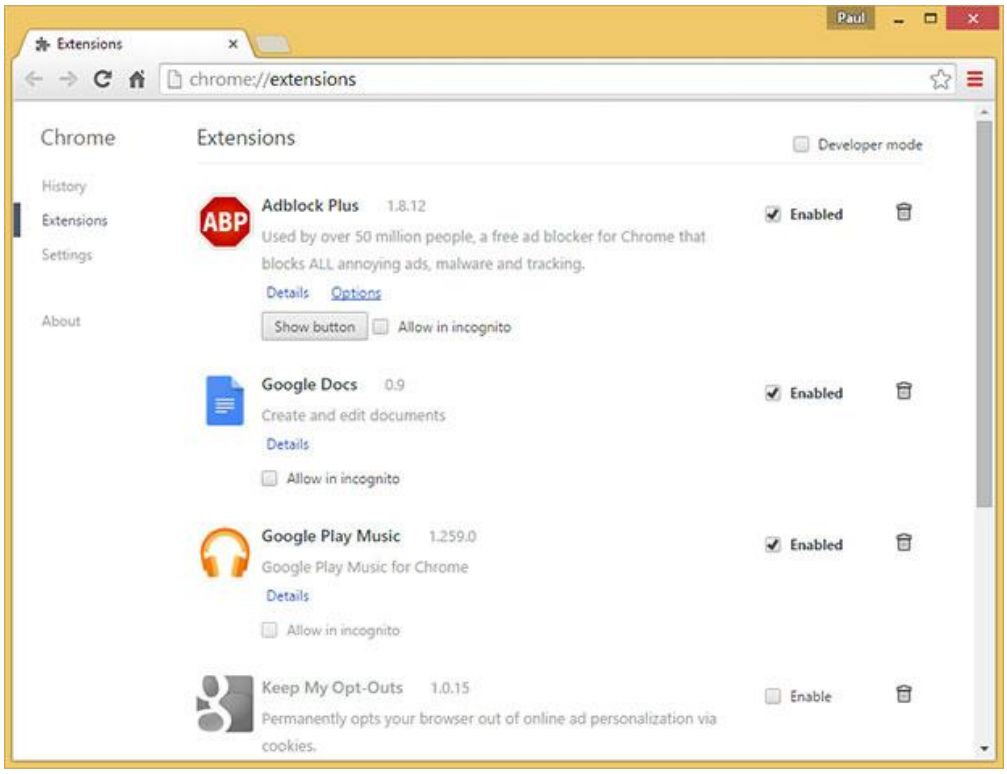


The same goes for the Search Providers category. The only thing you should see is Bing unless you've added another search provider, like Google. We're making this up (we think), but let's say the default entry is "CouponPal." The option to remove is grayed out, but that's only because it's the default search option. Click on one of the other options—Bing, Google, Yahoo, etc.—and punch the **Set as default button**, then return to CouponPal and click **Remove**.

Now let's rinse and repeate for the Accelerators category. Is there a rogue entry? Remove or disable it. When you're finished with all these, close out the Manage add-ons window. Return to the **Gear (Tools)** icon and select Internet **Options**. Navigate to the **General** tab if you're not already there and look at the Home page section. Oftentimes adware will replace the default homepage with its own entry, which will load each time you fire up IE. Highlight the hijacked entry and change it to whatever you want, like http://www.maximumpc.com (c'mon, show us some love!) and click **Apply**. Now hit **OK**, close IE, and reload it. If you haven't missed anything, it should work as new again. And if not, you may have a deeper malware problem, which we'll get to in a moment.

Chrome

The steps are similar in Chrome. To check if the default search engine's been changed, click the **three horizontal lines (Chrome Menu)** in the upper-right corner and select **Settings**. Under the Search heading, click **Manage search engines**. Hover your mouse over whichever one you want to be the default and click **Make default**. Next, hover over the rogue entry and click the X button on the right to remove it.



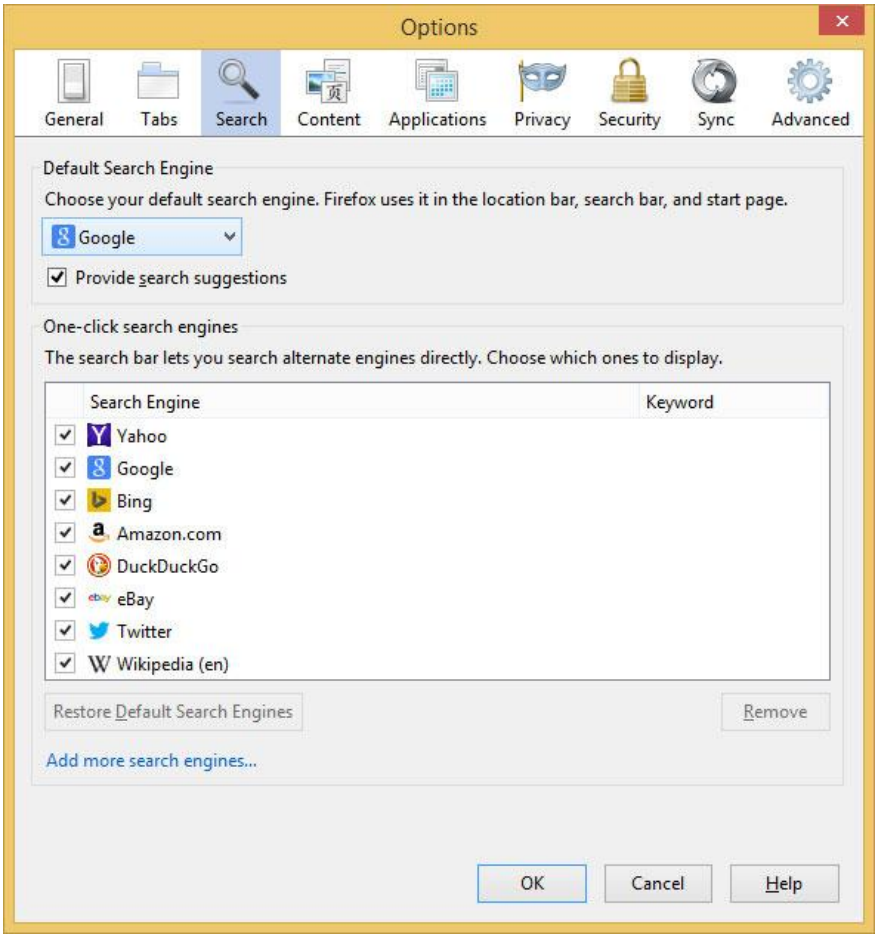
Also in the Settings menu is an **On startup** heading with three options: Open the New Tab page, Continue where you left off, and Open a specific page or set of pages. If your homepage has been taken over, click the **Set Pages** hyperlink next to the Open a specific page or set of pages option. Go ahead and delete the rogue entry and/or enter whichever page you'd like to load at startup. Alternately, you can use one of the other options.

Go back to the Chrome menu and select **More Tools > Extensions**. Here is where you'll see a list of installed add-ons, like Adblock (which we hope you've disabled on Maximum PC—we've gotta eat!), Google Play Music, or whatever. See any entries that shouldn't be there? Click the trash icon to dispose of them.
Remember to close Chrome and reload it.

Firefox

In Firefox, click the **three horizontal lines (Firefox Menu)** and select **Options**. Under the **Search** tab, you'll see a pull-

down menu with your default search option, and under that a list of search engines. Highlight any rogue entries and click **Remove**.



Next, navigate to the **General** tab to make changes to your homepage. If it's been taken over, you'll most likely see the address here. Change it to whatever you want, or click the **Restore to Default** button.

Firefox has long supported extensions and plugins. To access them, go back to the **Firefox menu** and select **Add-ons**. Remove any rogue extensions, or if you're unsure, click the disable button to see how it affects your browser. You can always come back and remove it.

Following the above steps will help restore your browser(s) to the way it was operating before adware dug its claws in. However, it might not remove the root cause if there's a deeper malware infection. Let's move on.

Just Uninstall It

Not all malware is highly sophisticated. Many of them can be uninstalled just like any other program, so before you go any further, bring up the Control Panel and head over to Programs and Features. Scan the list for any signs of adware, toolbars, or anything else that's obviously unwanted software and simply uninstall it. Is your system back to normal? If so, then great, you got off easy! If not, blurt out a few curse words (you'll feel better) and then continue reading.

Fight Software with Software

One of our favorite and most reliable anti-malware programs is Malwarebytes. There's both a free and paid version, the latter of which adds proactive protection like real-time monitoring and conveniences like scheduled scanning. For removing existing malware, the free version is sufficient.

What's neat about Malwarebytes is that it scans for a wide range of rogue software, like spyware, adware, some viruses, and even rootkits. Be advised that Malwarebytes isn't intended as a standalone antivirus program, but as a supplement. Or, in this case, as a cleanup tool.

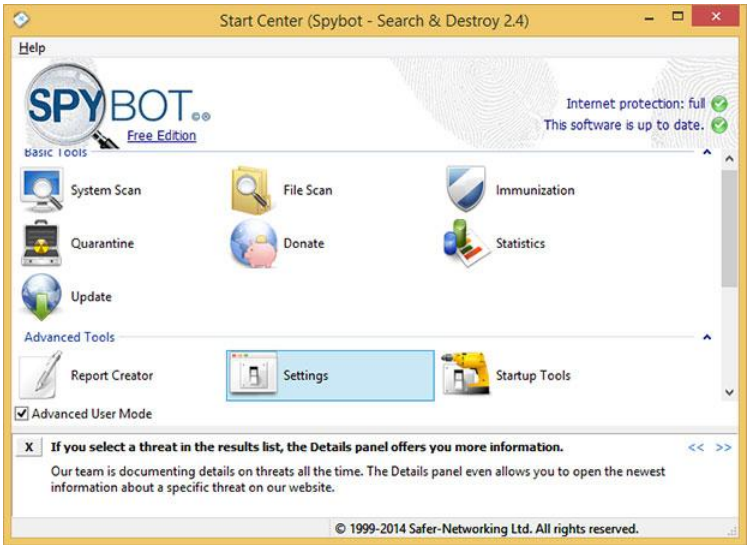
The first thing you should do when running Malwarebytes is to update the database so that it can scan for the latest threats. Just click the **Update Now** now link and let it do its thing.

See that big **Scan Now** button at the bottom? Don't click it just yet. First, click the **Settings** option and navigate to **Detection and Protection**. Even though Malwarebytes scans for rootkits, you first have to enable the option, and this is where you'll find it—check the **Scan for rootkits** box.

Now, go to the Scan heading and select **Threat Scan**, which is the recommended option. This will run a comprehensive sweep of your system and could take a long time to finish. Find something else to do for a bit—ride a bike, catch up on some reading, make love, play a console game, grab some lunch, or anything else you can think of that's more fun than watching a system scan. When it's finished, audit the list of threats for any false positives and uncheck them, then click **Remove Selected**.

Solicit a Second (or Third) Opinion

As much as we like Malwarebytes, there's no single program out there capable of detecting and removing every piece of malicious software. For a machine that's in particularly bad shape, it pays to run multiple spyware sweeps. Which ones? There are several out there, and one that we still like is Spybot Search and Destroy (http://www.safer-networking.org/).

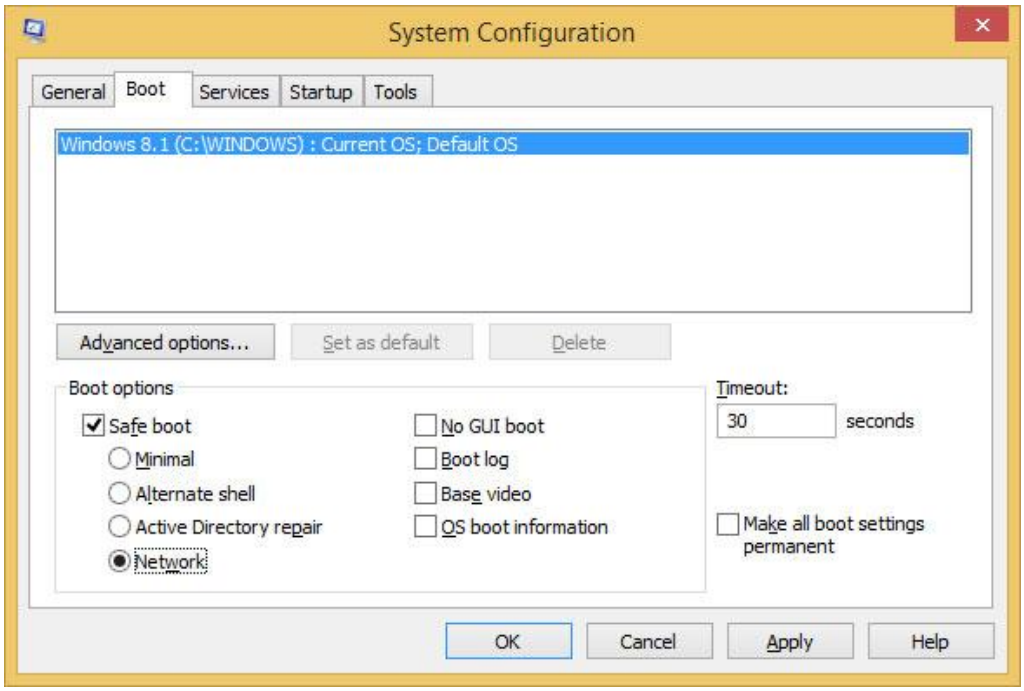


As with all of these programs, be sure to update the definitions database first—just click the **Update** icon. The first update can take a few minutes, even on a fast Internet connection, so be patient. Once it's finished, click **System Scan** and let it sweep your system for junk.

As you can see, these programs are pretty self explanatory, so rather than walk you through each one, here's a list of software we recommend running on badly infected machines:
Comodo Antimalware BOClean
Hitman Pro
AdwCleaner
Kaspersky TDSSKiller (rootkit removal tool)

There are others out there, and if you have a favorite, feel free to add it to the list. Remember, it might not always be necessary to run several different programs, but for a machine that's in really rough shape, it doesn't hurt to blitz the opposition using multiple tools.

Better Safe Mode than Sorry
In some cases, you may not be able to run or even install the aforementioned malware removal software. Some of the more sophisticated malware will block them outright, and if that's the case, you should try booting into Safe Mode. The same is true if a piece of malware manages to reinstall itself after you've already removed it.
To boot into Safe Mode, shut down your system, turn it back on, and start tapping the F8 key. Instead of booting into Windows, you should see an **Advanced Boot Options** menu. Select the **Safe Mode with Networking** option. This will load just the essential Windows drivers while also giving you Internet access so that you can download, install, and update anti-malware software.



If you're having trouble booting into Safe Mode, another way in there is to boot into Windows as you normally would. Click the **Start menu**, select **Run**, and type **msconfig**. Select the **Boot tab** and under the **Boot options** heading, check the **Safe boot** box. Mark the **Network** radio bubble and click Apply, then reboot your system.

Scan for Viruses
Microsoft's built-in Windows Defender in Windows 8.1 (separate download in prior versions) does a good job overall of detecting viruses, and if that's what you're rolling with, update the database and scan your system. Otherwise, do the same with whichever antivirus software you're using. If you're not using one, either enable Windows Defender or seek out a free AV such as Avast, AVG, Avira, Bitdefender, Comodo, or Panda, to name a few of the no-cost options. Be sure

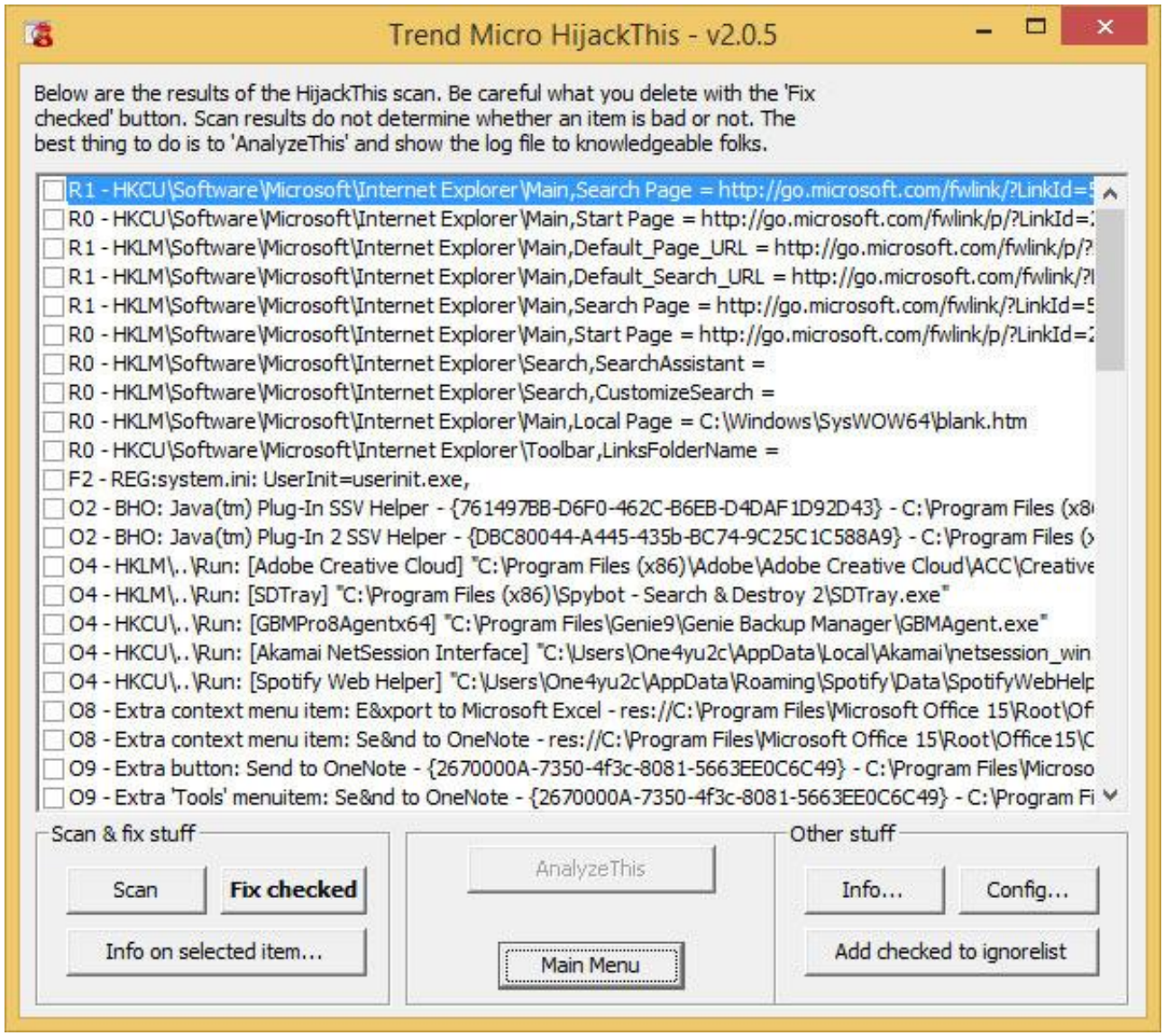
to install only one, as multiple AV programs can conflict with each other (though it's okay to run them with malware removal tools like Malwarebytes).

Bring Out the Big Guns

At this point, you've scanned for viruses, run multiple anti-malware programs, rooted out any rootkits, and cleaned up your browsers, yet your system is still acting up. That's bad news, but don't go throwing in the towel just yet. Instead, download HijackThis.

HijackThis

HijackThis is a simple little utility that audits your registry, browser settings, and system services. It only takes a few seconds to run, however, it doesn't discern between good and malicious entries, so don't go deleting entries willy-nilly. There's no installation required here—just fire up HijackThis and select the top option so that it saves the results to a log file. In a few seconds, you'll see a long list of entries. Scroll through them and look for any obviously malicious entries. For example, if you know you've been infected by a particular piece of malware and you see references to it in the HijackThis results, check the box.



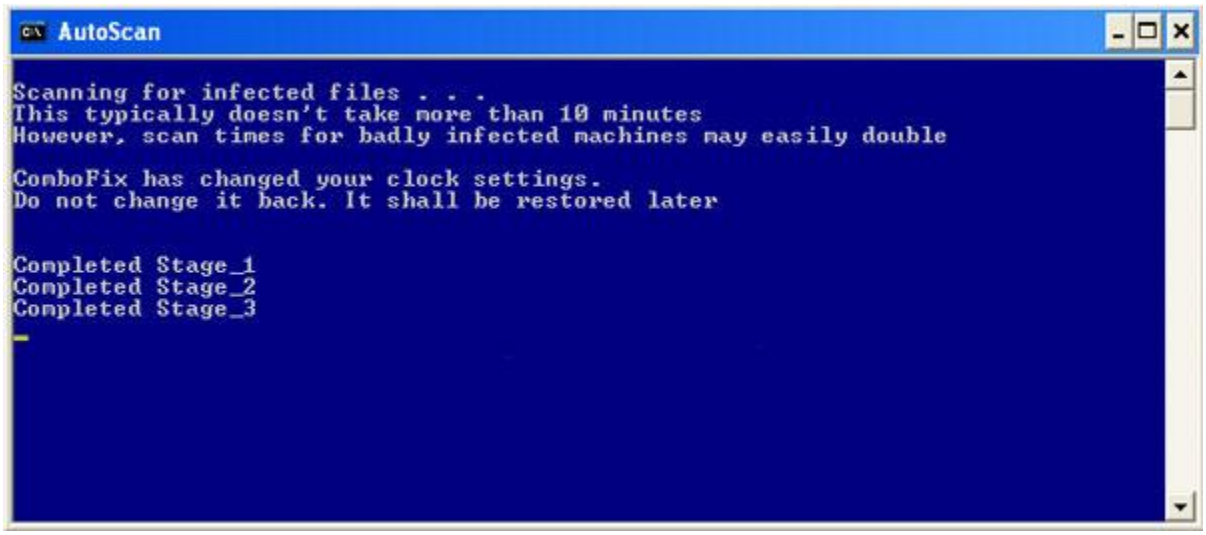
Most of the entries will be safe, so be careful what you check. You could even break functionality of a legitimate program or cause other problems by checking certain entries. This is where the log comes in handy. When the scan finished, it should have populated a Notepad file with the results. Highlight the entire text and copy it to your clipboard.

Now head to I Am Not A Geek, paste the contents in the box, and click Parse. Potentially malicious entries will be highlighted red, but before you click the check box in HijackThis, look up each one in Google so that you're sure of what you're removing.

There are several other online analyzers, such as HiJackThis.de Security and HiJackThis.co. Try using at least two, and if you still need help, solicit advice from a forum such as *Bleeping Computer*.

ComboFix

As a last resort before wiping your system clean and starting anew, there's ComboFix, an aggressive program that hunts for persistent infections and attempts to remove them. It was developed by the folks at *Bleeping Computer* and they recommend not running it unless specifically requested, so keep that in mind. It's also worth noting that ComboFix doesn't yet work in Windows 8.1 or Windows 2000, though it does run in Windows 8, 7, Vista, and XP.



If it's finally come to this, follow the instructions in *Bleeping Computer's* guide and when it's finished running, see if your system is back to normal. Should problems remain, post a copy of the log ComboFix generated into the forum thread where it was recommended that you run it.