Update: Tools to remove almost any malware

By Fred Langa on April 14, 2016 in On Security

Special-purpose anti-malware scanners not only clean up some of the worst forms of malware, they can also be used for routine *deep scans* .

Here are 12 tools you can use to verify that your full-time anti-malware tool is truly keeping your PC malware-free

This article starts where a pair of earlier articles leaves off. To get the most out of the information below, please take a moment to skim through those earlier, foundational stories.

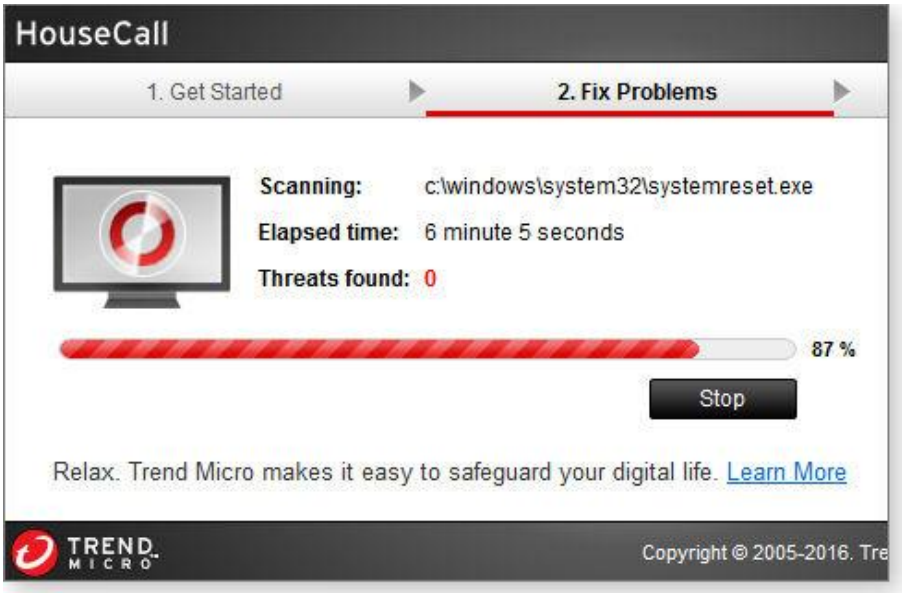
Start with the April 4, 2013, Top Story , "Microsoft's six free desktop security tools," which explains how Microsoft defines two main categories of malware: ***malicious software*** and ***potentially unwanted software*** **.** The article then discusses the built-in and free-download Windows tools that combat each type of malware. The article also clarifies some confusing Microsoft nomenclature. For example, **Windows Defender,** built into Win8 and Win10, is completely different from the identically-named "Windows Defender" in Vista and Win7. The former is a relatively good front-line anti-malware application; the latter is a much simpler tool that should ***never*** be relied on as your primary defense against malware. The aforementioned Top Story has more details. New versions of two other Microsoft tools discussed in that article — Microsoft Safety Scanner (aka "System Sweeper") and Windows Defender Offline — are covered in this update.

Next, see "A dozen tools for removing almost any malware" (April 11, 2013, Top Story), which provides an introduction to the topic of using standalone, self-contained anti-malware scanners either to clean up difficult infections or for periodic ***deep scans*** to verify that your primary anti-malware defenses have left your PC truly malware free. I won't repeat those introductory details here; please review the article.

This update article discusses current anti-malware–scanning tools, replacing some of the previously-recommended tools with new ones and, in all cases, noting how these special-purpose scanners now work with Win8.1 and Win10 (neither of which was released when the original articles ran).

Anti-malware for routine cleanup/verification

Trend Micro's HouseCall (free; http://housecall.trendmicro.com/) has been around for years and has an excellent reputation. It's available in 32-bit and 64-bit versions for all current versions of Windows — Vista, Win7, Win8, and Win10. HouseCall, shown in Figure 1, is known for its speed, making it an excellent choice for routine use to verify that a PC is malware-free.



Scanning: c:\windows\system32\systemreset.exe

Elapsed time: 6 minute 5 seconds

Threats found: 0

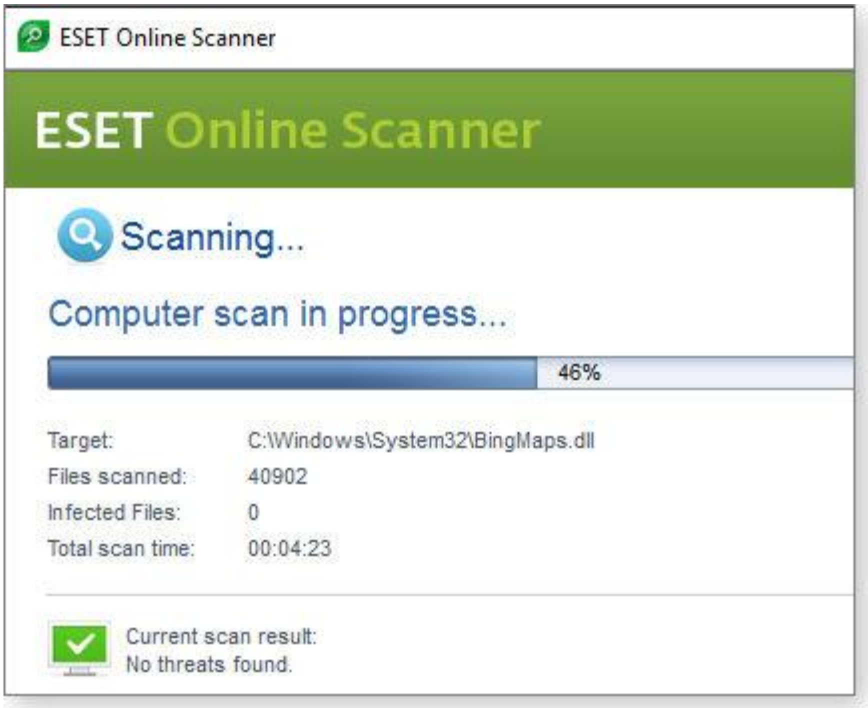
Relax. Trend Micro makes it easy to safeguard your digital life. Learn More

Copyright © 2005-2016. Tre

Figure 1. Trend Micro's *HouseCall* scanner is small, simple, and quick.

HouseCall has the three standard levels of scans offered by most anti-malware tools — "Quick," "Full," and "Custom" — but, unique among the products I looked at, it also offers the optional **HomeDevice Guard** feature that scans your local network, checking whether your attached devices are vulnerable to common types of network-based attack.

ESET's Online Scanner (free; http://www.eset.com/us/online-scanner/) is another tool with a long pedigree and a well-deserved reputation for excellence. There are two flavors of Online Scanner: browser-based and standalone. If you download the application via Internet Explorer, and you have ActiveX enabled, you'll get the in-browser version. On the other hand, if you download the Scanner through Chrome, Firefox, Opera, and so forth, you get the standalone edition that runs outside the browser. Once launched, both versions operate identically.
ESET's Online Scanner is available in 32- and 64-bit versions. Although the ESET site only promises compatibility for Windows XP, Vista, and Win7, I've run it on Win8 and Win10 systems without trouble.
You can select scan type ("Quick," "Full," or "Custom"), and target which drives to scan (local and/or remote/networked). You can also have Online Scanner look inside archives such as ZIP files — something only a few other scanners can do. Moreover, the scanner will look for ***potentially unwanted programs*** (aka PUPs).



Computer scan in progress...

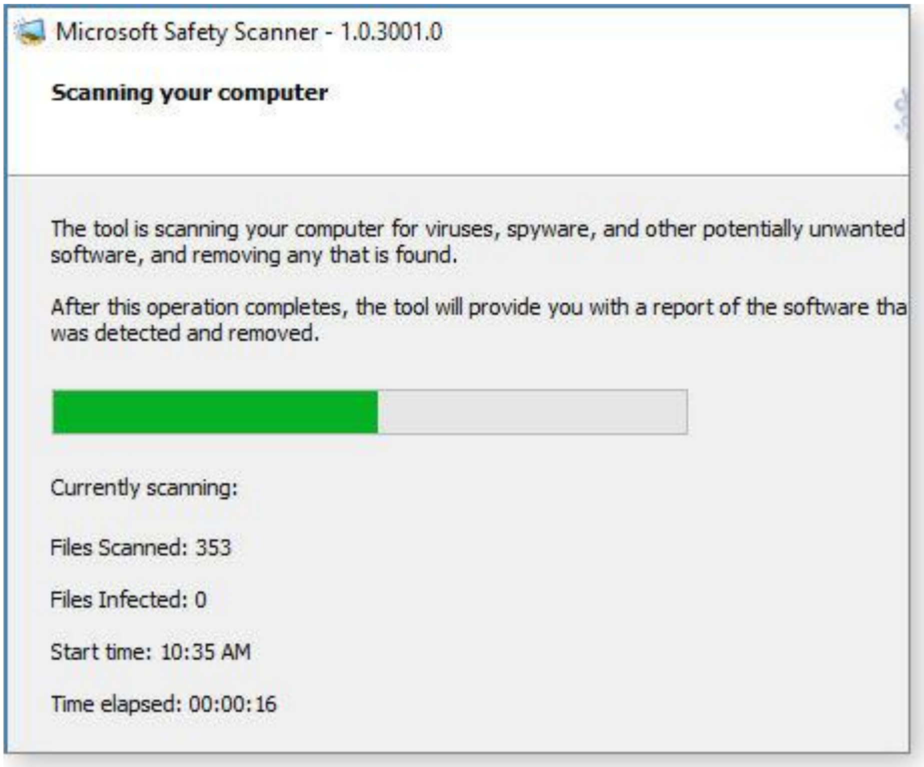
Target: C:\Windows\System32\BingMaps.dll
Files scanned: 40902
Infected Files: 0
Total scan time: 00:04:23

Current scan result:
No threats found.

Figure 2. ESET's highly configurable *Online Scanner* comes in both standalone (shown) and browser-based versions.

For very deep malware scans, I typically run Online Scanner overnight, with all options enabled; it thoroughly examines all files on a PC's local and network-attached drives.

Microsoft Safety Scanner (Figure 3) is fast, free, and easy to use, and it can find/remove both malicious software and PUPs. Microsoft states it's compatible with XP, Vista, and Win7, but I've had no trouble running it on Win8 and Win10 PCs. You'll find 32- and 64-bit versions on its info/download page (http://www.microsoft.com/security/scanner/en-us/)


Microsoft Safety Scanner - 1.0.3001.0

Scanning your computer

The tool is scanning your computer for viruses, spyware, and other potentially unwanted software, and removing any that is found.

After this operation completes, the tool will provide you with a report of the software tha was detected and removed.

Currently scanning:

Files Scanned: 353

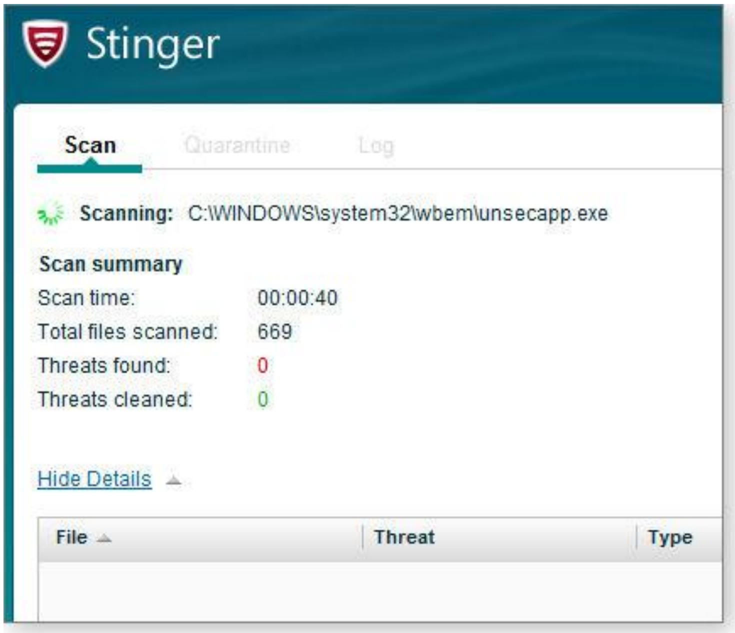
Files Infected: 0

Start time: 10:35 AM

Time elapsed: 00:00:16

Figure 3. Microsoft's *Safety Scanner* is extremely easy to use.

McAfee's Stinger (free; http://www.mcafee.com/us/downloads/free-tools/stinger.aspx) is a far more specialized tool. Rather than scan for all known forms of malware, it looks for rootkits; it then scans running processes, loaded modules, and the Registry and folder locations most commonly used by malware.
Stinger's narrower focus means that scans are ***very*** fast, making this tool a good choice for malware first-aid. It can find and cure many of the most common types of malware problems in short order. However, Stinger's limited focus makes it less thorough than the other tools in this article.
Stinger is available in 32- and 64-bit versions, and McAfee says it's compatible with XP, Vista, and Win7/8. I also ran it successfully on Win10 without trouble.
Note: There's also a beta (experimental) 64-bit Stinger version that includes "Real Protect," a real-time, malware-behavior detection technology that should detect for suspicious activity — even if there's no associated malware signature.
This sounds promising, but I couldn't get the beta software to run properly on a Win10 Pro x64 test PC. (Again, the official 64-bit standard version of Stinger ***without*** Real Protect ran flawlessly.)



Scanning: C:\WINDOWS\system32\wbem\unsecapp.exe

Scan summary

Scan time:	00:00:40
Total files scanned:	669
Threats found:	0
Threats cleaned:	0

File	Threat	Type

Figure 4. McAfee's *Stinger* is exceptionally fast, and it targets both rootkits and common types of Malware.

If these relatively simple, on-demand scanners/cleaners don't work, or if an infection has crippled Windows, it's time to roll out the big guns.

Heavy-duty, self-booting, malware-cleaning tools

Some forms of malware — rootkits, for example — are especially adept at playing hide-and-seek with anti-malware apps. Infections also have been known to actually disable anti-malware tools and scanners, and to block Windows Update and browsers.

The solution is a self-contained, self-booting system scanner that operates entirely ***outside*** of Windows. These tools are typically offered as downloadable ISO files that you use to create bootable CD, DVD, or flash drives — commonly called ***rescue disks*** — that contain both a minimal operating system and a malware scanner.

When you start and run a PC from a rescue disc, your Windows setup — and any infections it might harbor — remains inert and inactive. Malware can't hide itself, and it's considerably easier for the scanner to look everywhere it needs to.

The one drawback with rescue disks is setup and use; you have to take the time to create the bootable CD/DVD or flash drive. You also have to be able to boot your system from that disc or drive, which can be difficult on newer PCs with UEFI BIOSes and "Secure Boot" technology.

How to make a bootable DVD/CD: Assuming you have an optical drive, Windows 10/8/7 all have built-in tools for creating bootable CDs and DVDs (See Appendix A)). Or you can use a third-party CD/DVD burning app such as Free ISO Burner (http://www.freeisoburner.com.)

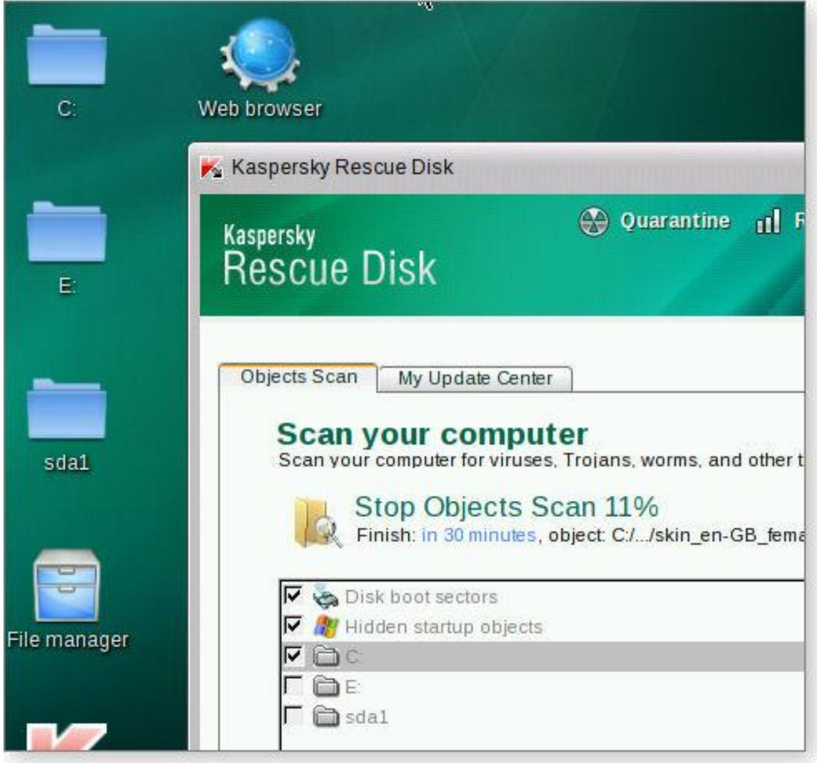
How to make a bootable flash drive: On Win10/8/7, use Microsoft's free Windows USB/DVD Download Tool (See Appendix B); or any of the many available third party tools.

For help booting from your rescue disc or flash drive:

- "How to solve UEFI boot and startup problems" – Dec. 11, 2014, Top Story
- "Emergency access to your PC's UEFI settings" – Jan. 15, 2015, LangaList Plus
- "Emergency repair disks for Windows: Part 1" – April 10, 2014, Top Story
- "Emergency repair disks for Windows: Part 2" – April 17, 2014, Top Story

Here are three free, self-booting rescue disks to consider:

The **Kaspersky Rescue Disk** (free; https://support.kaspersky.com/viruses/rescuedisk) is a self-booting, Linux-based cleaning tool. Note that you don't have to know anything about Linux — the tool has a complete, ready-to-run, point-and-click, Windows-like desktop environment (see Figure 5). It's about as easy to use as any good Windows application.



Scan your computer

Scan your computer for viruses, Trojans, worms, and other t

Stop Objects Scan 11%

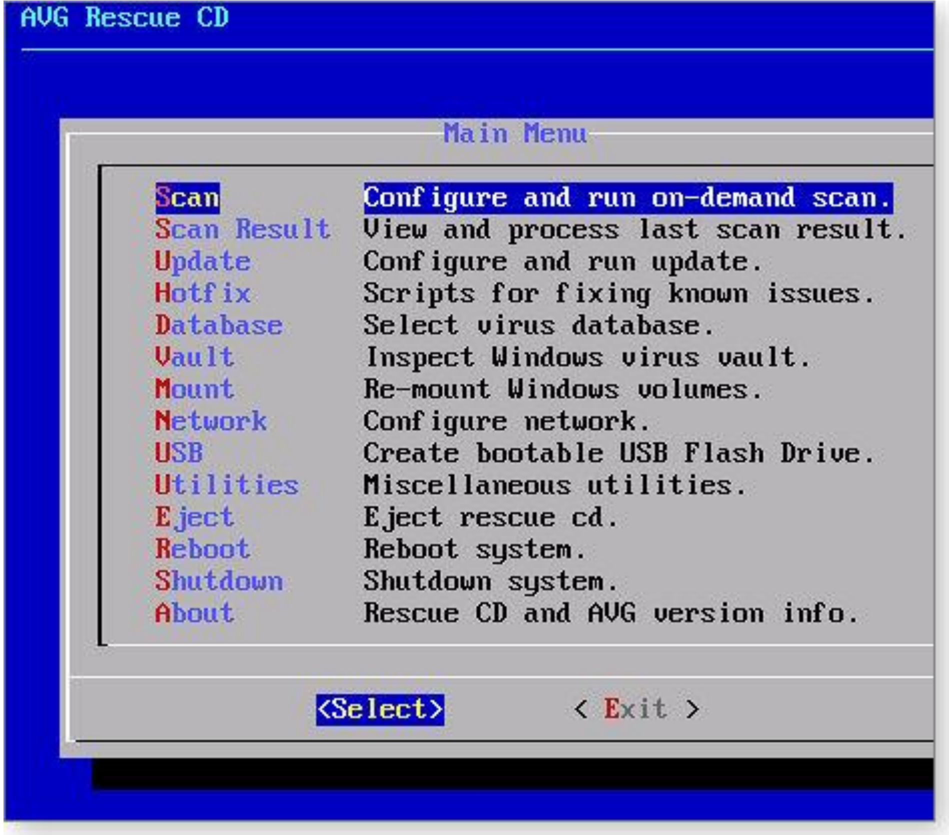
Finish: in 30 minutes, object: C:/.../skin_en-GB_fema

☑ Disk boot sectors
☑ Hidden startup objects
☑ C:
□ E:
□ sda1

Figure 5. Linux based, the Kaspersky *Rescue Disk* has a familiar graphical interface.

I now recommend the **AVG Rescue CD** (free; http://www.avg.com/us-en/download), a Linux-based, anti-malware tool that includes additional rescue/scan/repair options.

It boots to a minimalistic, text-based environment (see Figure 6), though it simulates a graphical environment via ASCII graphics, reminiscent of old-school DOS apps. It's easy to use; you navigate with the keyboard's arrow keys and make selections with the Enter key.

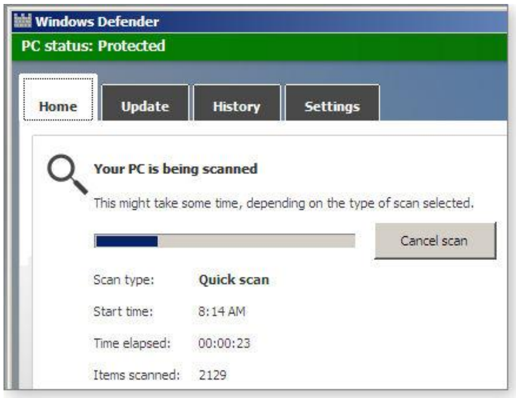


```
AVG Rescue CD

                     Main Menu

   Scan          Configure and run on-demand scan.
   Scan Result   View and process last scan result.
   Update        Configure and run update.
   Hotfix        Scripts for fixing known issues.
   Database      Select virus database.
   Vault         Inspect Windows virus vault.
   Mount         Re-mount Windows volumes.
   Network       Configure network.
   USB           Create bootable USB Flash Drive.
   Utilities     Miscellaneous utilities.
   Eject         Eject rescue cd.
   Reboot        Reboot system.
   Shutdown      Shutdown system.
   About         Rescue CD and AVG version info.

          <Select>         < Exit >
```

Figure 6. The AVG *Rescue CD* has an extremely simple, DOS-like interface.

With minimal graphics and no mouse support required, AVG's Rescue CD should operate on just about any hardware — including very old, damaged, or otherwise hardware-constrained PCs.

Windows Defender Offline (WDO) is a stripped-down, locked-down, bootable version of Windows that has one function: running a self-contained version of Win10/8's Windows Defender. It looks and operates much like the built-in versions of Windows Defender — and, for that matter, much like the Win7/Vista versions of Microsoft Security Essentials.



PC status: Protected

Your PC is being scanned

This might take some time, depending on the type of scan selected.

Scan type: Quick scan

Start time: 8:14 AM

Time elapsed: 00:00:23

Items scanned: 2129

You'll find free 32- and 64-bit versions of WDO that work on all current Windows versions (through Win10) on an MS site at http://windows.microsoft.com/is-is/windows/what-is-windows-defender-offline

Figure 7. *Windows Defender Offline* is effectively a bootable, standalone version of Win8/10's built-in Windows Defender.

Other Linux-based tools worth a look

If the above tools don't meet your needs or won't work on your PC (no software works on all systems), consider using any of the following free, well-regarded, self-booting, Linux-based anti-malware scanners. I've tried them all on various Windows versions up to and including Win10 Pro x64. They all offer something worthwhile.

- **Bitdefender Rescue CD** (http://www.bitdefender.com/support/how-to-create-a-bitdefender-rescue-cd-627.htm) offers a beautiful and fully graphical interface.
- **Vba32 Rescue** (http://www.anti-virus.by/en/vba32rescue.shtml) uses a simple, text-based (ASCII graphics) interface that you navigate via the arrow keys. This tool can also help you to recover/copy files from a system that will no longer boot Windows.
- **Comodo Rescue Disk** (https://help.comodo.com/topic-170-1-493-5214-.html) offers a choice of graphical or text-mode operation.
- **Panda SafeCD** (http://www.pandasecurity.com/mediacenter/products/panda-safecd-4-4-3-0/) is the oldest tool in this lineup, but it still downloads and uses the very latest malware signatures. It has a simple, graphical interface that's extremely easy to use.
- **Sophos Bootable Anti-Virus** (https://www.sophos.com/en-us/support/knowledgebase/52011.aspx) uses a slightly unusual, multi-step download process. You first download a small executable program that then downloads and builds the ISO for you.
-

All cleaned? Now keep your PC that way!

If an anti-malware scan finds an infection on your system, it's an indication that your current, full-time anti-malware defenses might not be up to the job. Consider installing and using a different tool — ASAP!

Whether your system is infected or clean, use one or more of the special-purpose scanners discussed above to verify that your regular anti-malware tool is keeping your PC safe.

With a good, full-time anti-malware tool, buttressed by a periodic ***deep scan*** with a separate anti-malware scanner, you can help ensure that your PC is truly clean — and stays that way!

APPENDIX A
Burn a CD or DVD from an ISO file

Applies to Windows 7

An ISO file, also called a disc image, is a single file that’s a copy of an entire data CD or DVD. When you burn a CD or DVD from an ISO file, the new disc has the same folders, files, and properties as the original disc. The most common way to get an ISO file is to download it from a website. For example, you might download and then use an ISO file to update software on your computer.

You can burn a disc image file, which often has either an .iso or .img file name extension, to a recordable CD or DVD by using Windows Disc Image Burner. Whether you can burn it to a recordable CD, DVD, or Blu-ray Disc depends on your disc burner and the type of discs it can burn, the size of the disc image file, as well as the device on which you plan to use the disc.

1. Insert a recordable CD, DVD, or Blu-ray Disc into your disc burner.
2. Open Computer by clicking the **Start** button, and then clicking **Computer**.
3. In Windows Explorer, find the disc image file, and then double-click it.
4. If you have more than one disc burner, from the **Disc burner** list in Windows Disc Image Burner, click the burner that you want to use.
5. (Optional) If you want to verify that the disc image was burned correctly to the disc, select the **Verify disc after burning** check box.
6. If the integrity of disc image file is critical (for example, the disc image file contains a firmware update), you should select this check box.
7. Click **Burn** to burn the disc.

Notes
If a third-party CD or DVD burning program is installed on your computer, that program might open when you double-click the disc image file. If this happens, and you want to use Windows Disc Image Burner to burn the CD or DVD from the disc image file instead, right-click the disc image file, and then click **Burn disc image**.

You can't create disc image files using Windows Disc Image Burner. To create a disc image file, you need to install and use a third-party CD or DVD burning program or other program that lets you create disc image files from a CD or DVD.

APPENDIX B

Windows USB/DVD Download Tool

When you download Windows from Microsoft Store, you have two options: You can download a collection of compressed files, or you can download an ISO file. An ISO file combines all the Windows installation files into a single uncompressed file.

If you choose to download an ISO file so you can create a bootable file from a DVD or USB drive, copy the Windows ISO file onto your drive and then run the Windows USB/DVD Download Tool. Then simply install Windows onto your computer directly from your USB or DVD drive.

When you download the ISO file, you must copy it onto a USB or DVD. When you're ready to install Windows, insert the USB drive or DVD with the ISO file on it and then run Setup.exe from the root folder on the drive.

This allows you to install Windows onto your machine without having to first run an existing operating system. If you change the boot order of drives in your computer's BIOS, you can run the Windows installation directly from your USB drive or DVD when you first turn on your computer. Please see the documentation for your computer for information about how to change the BIOS boot order of drives.

Making copies

- To install the software, you can make one copy of the ISO file on a disc, USB flash drive, or other media.

- After you’ve installed the software and accepted the license terms that accompany the software, those license terms apply to your use of the software. The license terms for Windows permit you to make one copy of the software as a back-up copy for re-installation on the licensed computer. If you do not delete your copy of the ISO file after installing the Windows software, the copy of the ISO file counts as your one back-up copy.

If you need to download the software again, you can go to your Download Purchase History in your Microsoft Store account and access the download there.

Installation

To install the Windows USB/DVD Download Tool:
1. Click to open the Windows USB/DVD Download Tool page.
2. Click **Download** then **Run.**
3. Follow the steps in the setup dialogs. You'll have the option to specify where to install the Windows USB/DVD Download Tool.

You must be an administrator on the computer on which you are installing the Windows USB/DVD Download tool. It requires the Microsoft .NET Framework version 2.0 or higher.

System requirements

- Windows XP SP2, Windows Vista, or Windows 7 (32-bit or 64-bit)
- Pentium 233-megahertz (MHz) processor or faster (300MHz is recommended)
- 50MB of free space on your hard drive

- DVD-R drive or 4GB removable USB drive

Using the Windows USB/DVD Download Tool
Before you run the Download Tool, make sure you have purchased the Windows ISO download from Microsoft Store and downloaded the Windows ISO file to your drive. If you have purchased Windows but have not yet downloaded the ISO file, you can download the ISO file from your Microsoft Store Account.

To make a copy of your Windows ISO file:

1. Click the Windows START button, and click WINDOWS USB/DVD DOWNLOAD TOOL in the ALL PROGRAMS list to open the Windows USB/DVD Download Tool.

2. In the SOURCE FILE box, type the name and path of your Windows ISO file, or click BROWSE and select the file from the OPEN dialog box. Click NEXT.

3. Select USB DEVICE to create a copy on a USB flash drive or select DVD disk to create a copy on a DVD disk.

4. If you are copying the file to a USB flash drive, select your USB device in the drop-down list and click BEGIN COPYING. If you are copying the file up to a DVD, click BEGIN BURNING.

When your Windows ISO file is copied to your drive, install Windows by moving to the root folder of your DVD or USB drive, and then double-click Setup.exe.