Windows Secrets
Everything Microsoft forgot to mention

A dozen tools for removing almost any malware

By Fred Langa on April 10, 2013 in Top Story

Need to get a system clean of malware and/or verify that it's completely malware-free?

Use one or more of these free tools to clean up even the worst malware infections — and keep PCs clean.

Here's a typical scenario for a veteran computer user. Having established best-security practices on your PC, you've been free of malware infections for a long time. But every so often, a friend or family member says those dreaded words: "I think I might have a problem with my PC." Typically, by then the infection — a bogus antivirus popup, for example — is well established.

If it's been a while since you had to clean someone's machine, it can be
difficult to remember the best techniques and apps for restoring a system to good health. We suggest you keep this story handy for future reference — bookmark it or print it out. It should provide all the information needed to remove even the most tenacious malware infestation.

"Hi! I think I have a virus. Can you help?

A Windows infection shows up in many ways: strange system behavior such as excessive, unexplained activity; odd warning; or that aggressive popup you can't remove. Sometimes the infection is more subtle: It feels like Windows or installed apps just aren't working as they should. Or maybe the system seems to be working fine, but you'd still like to verify that malware hasn't taken hold and is working silently in the background.

Whatever the signs, experienced Windows users typically resort to one or more anti-malware scanners/cleaners. Unfortunately, it can be far easier to detect malware than to remove it. Thoroughly cleaning a system might require the use of multiple AV products, multiple scan/clean cycles, and even Linux-based tools running outside Windows.

Best AV practices also include proactive planning — preparing for infections, rather than scrambling for the right malware cleaner after the fact. With just a little work — literally a few minutes — you can equip yourself with the tools needed to rid a PC of most malware or verify that a system isn't actually infected.

Last week, I covered AV tools from Microsoft in the Top Story, "Microsoft's six free desktop security tools." This article adds a selection of third-party tools, a dozen of the best-regarded and most popular anti-malware cleanup tools currently available. All these tools find and eliminate common worms, viruses, and Trojans. Some also target hard-to-find and hard-to-remove **rootkits** and **bootkits** — malware that hides deep in the system, in some cases launching even before the OS and full-time anti-malware tools boot.

I've run all these tools on my XP, Vista, Windows 7, and Windows 8 PCs — and I use many of them regularly. But this is far from a definitive list; there are hundreds of other anti-malware applications available. That's good, because no single AV app works on all Windows systems all the time. Feel free to explore other options via your favorite search engine and download sites.

It's not the lack of AV tools that results in malware infections; it's the lack of application by users!

AV apps for routine cleanup and verification

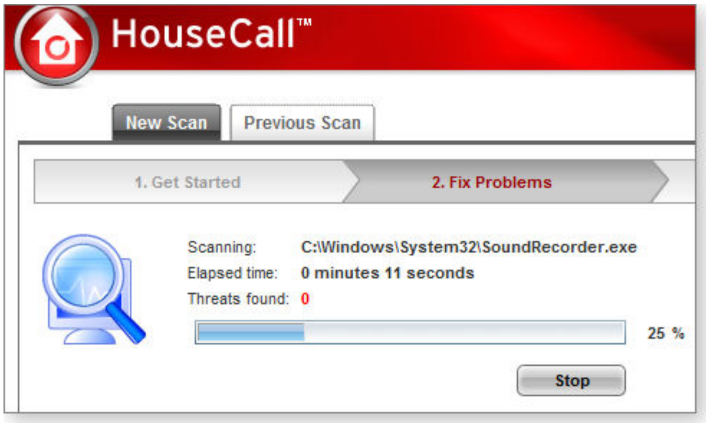
Most Windows users know they should run some sort of full-time anti-malware software. Malware authors are clever programmers and depend on staying one step ahead of AV developers. ***On-demand scanners*** are a second line of defense. Use them if your full-time scanner fails or when you wish to verify that a PC is malware-free. (It's like getting a second medical opinion.)

On-demand scanners are typically quick to download and easy to run. Usually self-contained (i.e., operating independently of your full-time AV tool), they might detect and remove malware your regular scanner missed. On-demand scanners are active only when specifically launched, so they rarely conflict with full-time scanners. In other words, you don't need to disable your full-time scanner to run an on-demand scanner/cleaner. If you strongly suspect an infection and one on-demand tool doesn't work, run others from different AV companies.

Here are my recommendations for free on-demand AV tools:

- Trend Micro's **HouseCall** (site) has been around for years and has earned an excellent reputation. It's available in a 32-bit version for XP and in both 32-bit and 64-bit versions for Vista, Win7, and Win8.

  HouseCall, shown in Figure 1, is known for its speed, making it an excellent choice for routine use. I use HouseCall often on my PCs for quickly verifying that a system is malware-free. Its **Settings** link offers three levels of scans: Quick, Full, or Custom.

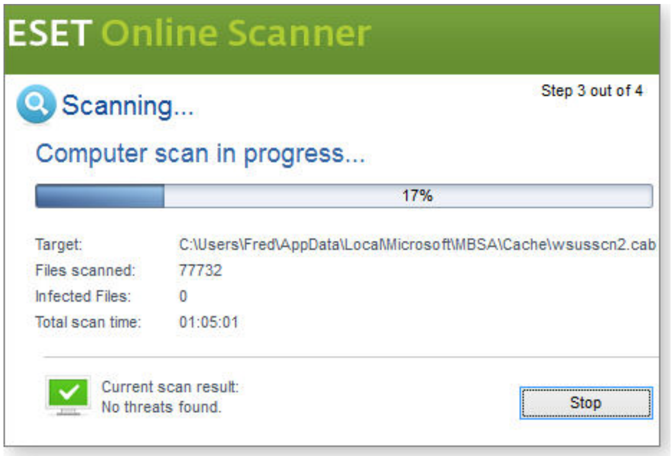


Scanning: C:\Windows\System32\SoundRecorder.exe
Elapsed time: 0 minutes 11 seconds
Threats found: 0

Figure 1. HouseCall is exceptionally simple and quick — ideal for routine malware-checking and cleanups.

- ESET's **Online Scanner** (site) is another tool with a long pedigree and a well-deserved reputation for excellence. It's not particularly fast, but it is nicely configurable. For example, the scanner's **Advanced** settings let you select which drives to scan — even remote networked drives. It will also scan inside archives (e.g., **.zip** files), which not all scanners can do. You can select the depth of the scan, such as looking for potentially unwanted and/or unsafe applications.

  ESET's scanner (Figure 2) runs on all current versions of Windows (XP through Win 8) and comes in both 32- and 64-bit flavors. Unlike its competitors, it's also available in two versions based on your choice of browser. If you download Online Scanner via Internet Explorer, you'll get an in-browser, ActiveX version. Downloading the scanner with another browser (e.g., Chrome or Firefox) installs a non-ActiveX version that runs outside the browser. Both versions work identically.



Computer scan in progress...

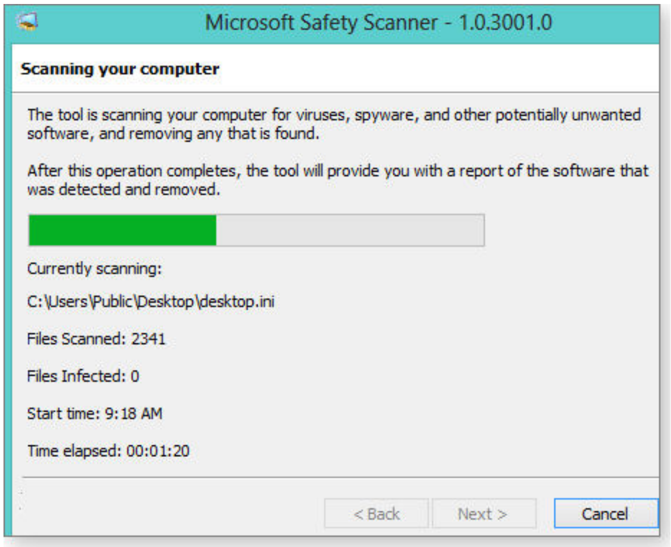
Target: C:\Users\Fred\AppData\Local\Microsoft\MBSA\Cache\wsusscn2.cab
Files scanned: 77732
Infected Files: 0
Total scan time: 01:05:01

Current scan result:
No threats found.

Figure 2. ESET's Online Scanner is exceptionally configurable and comes in both a browser-based and a standalone version (shown).

When something's gone wrong with a system and it needs a deep scan to determine whether it's infected, I run Online Scanner overnight with all options enabled.

- I covered the **Microsoft Safety Scanner** in last week's Top Story. But it's worth mentioning again because it's fast, free, and easy to use. Safety Scanner (Figure 3) finds and removes both malicious software and potentially unwanted software. It's compatible with XP, Vista, Win7, and Win8. You'll find both 32- and 64-bit versions on its info/download page.


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 that was detected and removed.

Currently scanning:

C:\Users\Public\Desktop\desktop.ini

Files Scanned: 2341

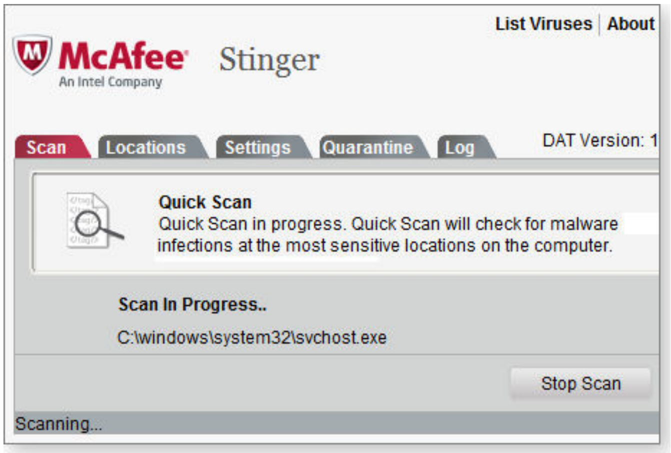
Files Infected: 0

Start time: 9:18 AM

Time elapsed: 00:01:20

Figure 3. Microsoft's extremely simple-to-use Safety Scanner checks for a variety of viruses and other malware.

- McAfee's **Stinger** (site) scans for about 5,000 common types of malware — and for those often difficult-to-remove **rootkits.** It offers Quick (see Figure 4), Full, and Custom scans, and McAfee updates the tool several times a week so the download is always reasonably current. (Many on-demand scanners must go through an update cycle immediately after installing or launching the app.)



DAT Version: 1

Quick Scan

Quick Scan in progress. Quick Scan will check for malware infections at the most sensitive locations on the computer.

Scan In Progress..

C:\windows\system32\svchost.exe

Scanning...

Figure 4. The easy-to-use McAfee Stinger targets rootkits, along with many other 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 malware — rootkits, for example — is especially adept at playing hide-and-seek with AV apps, making them especially difficult to detect and remove. Infections have been known to actually disable full-time AV scanners — and even Windows Update.

The solution is a self-contained, self-booting system scanner that operates entirely outside Windows.

These tools are typically offered as downloadable **.iso** files used to create bootable CD, DVD, or flash drives — commonly called ***rescue discs*** — that contain both an operating system and a malware scanner.

When you start and run a PC from a rescue disc, everything on your system's hard drive(s) — Windows, applications, your data files — remains inactive, unused, and for the most part unlocked to the disc-based scanner. That makes it considerably harder for malware to hide itself and considerably easier for an AV scanner to look for suspect code. There's also no chance that the rescue-disk scanner will conflict with any other installed anti-malware software.

The drawback with rescue discs is their setup. Unlike the download-and-run simplicity of the on-demand scanners mentioned above, you have to ***build*** a rescue disc before you can use it. That typically means downloading the **.iso** file and burning it to media. Assuming you have an optical drive, Windows 7 and 8 can create bootable CDs and DVDs natively (more MS info); Vista and XP need a little help from a third-party CD/DVD burning app such as Free ISO Burner (site).

Next, your system must be configured to boot from the rescue disc. You might have to press a specific key during power-up or change BIOS settings. The PC's owner manual or the vendor's website should have the information you need.

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

- The **Kaspersky Rescue Disk** (info/download) is my favorite standalone, self-booting cleaning tool. Although it's Linux-based, you don't have to know anything about Linux — everything is preconfigured as a complete, ready-to-run, point-and-click, Windows-like environment, as shown in Figure 5. It's about as easy as can be.

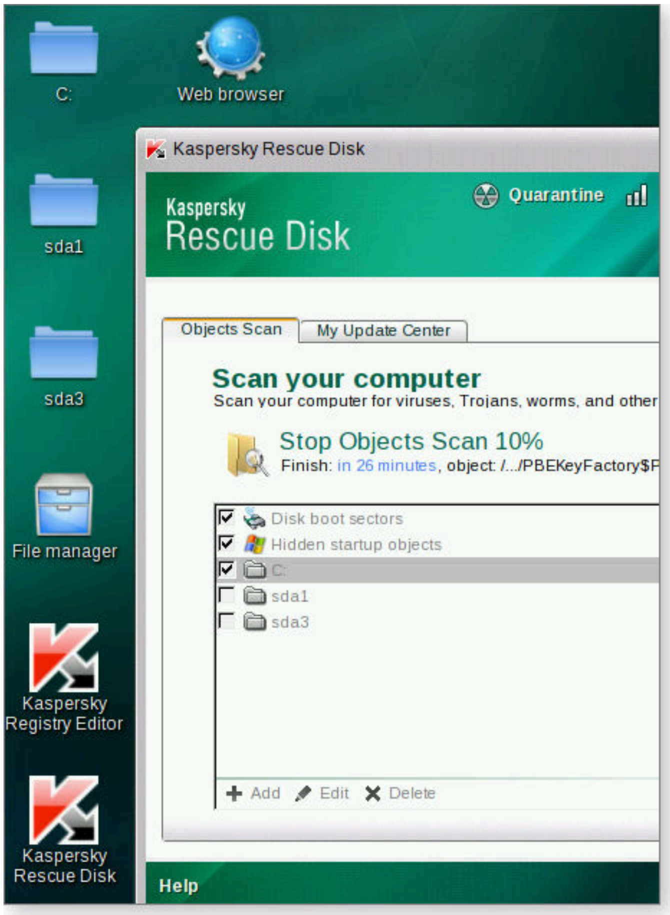
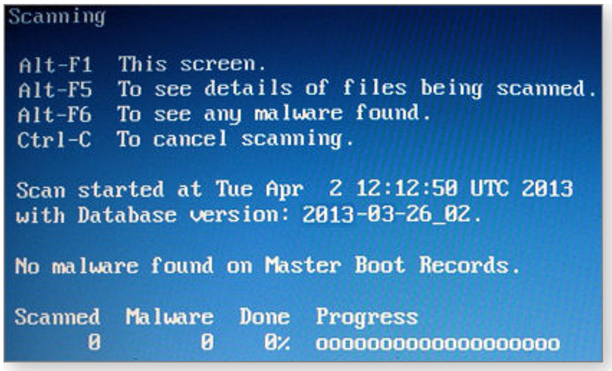


Figure 5. Linux-based, the *Kaspersky Rescue Disk* is a polished disk-scanning and recovery tool with a familiar graphical interface.

Removing some malware requires a more specialized tool. Kaspersky's Utilities page has downloadable malware-removal tools for specific viruses.

- F-Secure's **Rescue CD** (site) is at the other end of the usability spectrum. It's a Linux-based tool with a minimalistic, DOS-style text interface (see Figure 6). It's not point-and-click; you navigate with arrow-key and keystroke entries.



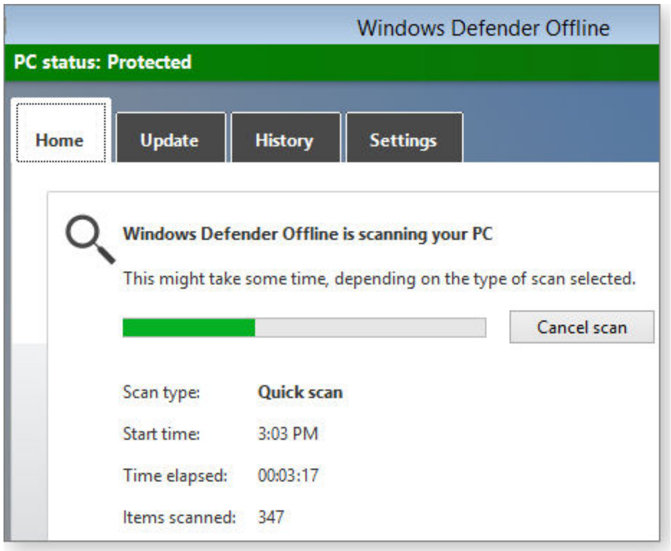
```
Scanning

 Alt-F1   This screen.
 Alt-F5   To see details of files being scanned.
 Alt-F6   To see any malware found.
 Ctrl-C   To cancel scanning.

 Scan started at Tue Apr  2 12:12:50 UTC 2013
 with Database version: 2013-03-26_02.

 No malware found on Master Boot Records.

 Scanned  Malware  Done  Progress
       0        0    0%  oooooooooooooooooooo
```

Figure 6. F-Secure's Rescue CD has a simple, text-based interface.

The lack of a graphical interface might be jarring for some Windows users, but Rescue CD's extremely simple, compatible, and robust. With minimal graphics support and no mouse support, Rescue CD should operate on just about any hardware, including very old or otherwise hardware-constrained PCs.

- I covered **Windows Defender Offline** (WDO) in last week's Top Story, so I'll be brief here. WDO falls in between the Kaspersky and F-Secure tools: It's more polished than F-Secure's Rescue CD but doesn't offer a complete GUI operating environment like Kaspersky's Rescue Disk.

  In operation, WDO is a near-clone of Microsoft Security Essentials or the Win8 version of Windows Defender (see Figure 7) — and it targets a similar range of malicious and potentially unwanted software.



PC status: Protected

Windows Defender Offline is scanning your PC

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

Scan type: Quick scan
Start time: 3:03 PM
Time elapsed: 00:03:17
Items scanned: 347

Figure 7. Windows Defender Offline is effectively a bootable, standalone version of Microsoft Security Essentials and Win8's Windows Defender.

  You'll find free 32- and 64-bit versions of WDO for all current Windows versions (XP through Win 8) on its info/download page.

A few other free, self-booting cleaning tools worth noting:

- **AVG Rescue CD** (site) is a general-purpose, Linux-based, rescue/scan/repair CD with a solid reputation.
- **Bitdefender Rescue CD** (site) offers excellent instructions and additional free tools to assist in creating a bootable CD/DVD or flash drive.
- **Avira AntiVir Rescue CD** (site) is available either as a standard **.iso** file or as an **.exe** version that can automatically create a burnable CD or DVD for you.

All cleaned? How to keep your PC that way!

If an AV scan finds malware on your system, it's an indication that your current full-time, anti-malware defenses might not be up to the job. (However, as already noted, no AV product will catch all malware for all time.) You can switch to another full-time scanner/cleaner: the Feb. 16, 2012, Top Story, "Is your free AV tool a 'resource pig?'," mentions several, or you can do a search online. What's more, you can add a second full-time scanner that will be compatible with the AV product you're currently using.

Two examples:

- **Malwarebytes' Anti-Malware** (free; site) is an excellent anti-malware utility that scans your system on demand — or on whatever schedule you choose. A **hybrid tool,** Malwarebytes installs like a standard Windows application and is specifically designed to coexist with other anti-malware tools. A Pro version (U.S. $25) offers additional real-time protection not available in the free version. I use the Pro version along with Microsoft Security Essentials on my own primary PC.
- **Safer Networking's Spybot Search & Destroy** (basic version is free for home use; advanced and commercial versions available; site) is another hybrid tool that you can leave running for ongoing, secondary protection.

Your choice: 16 known-good options. There are hundreds of anti-malware tools available — both paid and free. The products in this story, along with the Microsoft tools discussed in last week's Top Story, should give you all the information you need to keep or remove malware from your system(s) — or from PCs you (sometimes reluctantly) support!

All Windows Secrets articles posted on 2013-04-10:

= Paid content

TOP STORY	**A dozen tools for removing almost any malware**
LOUNGE LIFE	How to network various Windows versions
BONUS DOWNLOAD	If you want to write Windows 8 apps
WACKY WEB WEEK	Riding on the ridge of the world in Nepal
LANGALIST PLUS	Assessing Win8 File History — and its weaknesses

Show all articles on a single page

About Fred Langa

Fred Langa is senior editor. His LangaList Newsletter merged with Windows Secrets on Nov. 16, 2006. Prior to that, Fred was editor of Byte Magazine (1987 to 1991) and editorial director of CMP Media (1991 to 1996), overseeing Windows Magazine and others.

View all posts by Fred Langa →