# Antispyware

BY KONSTANTINOS KARAGIANNIS

## Spy Sweeper 3.5

$29.95 direct. Webroot Software Inc.,

**PC MAGAZINE EDITORS' CHOICE**

www.webroot.com. ●●●●◐

The best just keeps getting better. Webroot's Spy Sweeper 3.5, which once shared the spotlight with Lavasoft's Ad-aware SE Plus, is now the sole champ of the antispyware arena. The latest version, with its slight but effective improvements, is easily the best choice for protecting PCs from spyware and for cleaning machines that are already infected.

Scan time is improved in the new version. Because it was revised during our test cycle, we were able to run both versions 3.0 and 3.5 on the same test system, and we verified that Spy Sweeper 3.5 is approximately 30 percent faster, in line with Webroot's claims. Accuracy is up as well; the program got perfect scores on all but one of our tests.

Other improvements include the ability to remove both CoolWebSearch and TV Media completely. We found one pest that remains less than fully curable by Spy Sweeper's means, however. The program was unable to delete a key component of Istbar, although it did block the spyware bar from working. Spy Sweeper wrongly suggests that a user can delete the file; Windows claims Istbar is in use, making deletion via Windows Explorer impossible. You need to kill Istbar either via a command line, by removing dependencies on the file, or with Spybot Search & Destroy. Even the best occasionally needs a little help.

Of course, with all its Shields active, Spy Sweeper will prevent Istbar and almost every other pest from getting on your system in the first place. If version 3.0 got on your nerves with frequent requests for user interaction, you'll like 3.5's ability to block browser-hijack attempts without asking for advice.

Many antispyware packages offer users a chance, on a case-by-case basis, to block a program from running. After a few
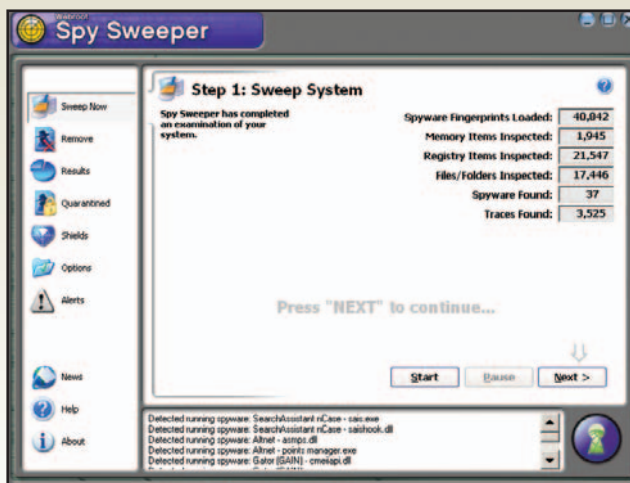


**FAST, FLEXIBLE, AND EFFECTIVE,** Webroot's Spy Sweeper is our reigning champ.

times, you may get fed up and simply delete it. As a safeguard against removing a program that another app, such as one for file-sharing, relies on, Spy Sweeper gives users the option of blocking apps permanently instead.

When looking at traces found during a scan, you can still take advantage of the expandable tree view, complete with summary information about each threat. A previous gripe of ours has been resolved, too: You can now ignore tracking cookies, making it easier to focus on the more immediate threats posed by spyware apps.

After experiencing the huge improvements Webroot made in the past few versions, we're eager to see the next incremental revision. We'd like to see Spy Sweeper update its abilities to handle Istbar and a couple of other pests that weren't part of our official test batch, and get better at cleaning annoying desktop shortcuts and folders deposited by adware. This product is so close to five stars we can taste it.

# Antispyware: Spy Sweeper 3.5

Spyware isn't like spam or viruses. It typically enters your PC with little enough fanfare that you can miss it until it's so entrenched that your machine crawls through basic tasks, displays browser home pages you didn't choose and can't change, and pops up ads, even when you're not on the Web, that seem to know you eerily well.

Spyware is often the surprise payload hidden in a temptingly "free" download. And it seems like this year, everyone's got it—a nasty spyware infection, that is. We saw competition heat up in the antispyware arena this year, at last, reflecting the extremely high rate of infestation. To cap the year, the word *spyware* was added to the Oxford English Dictionary in December. Spyware has truly arrived.

Amid the newly fierce competition, one of our previous Editors' Choices, Webroot's Spy Sweeper, recently updated to version 3.5, continues to excel. Spy Sweeper now stands alone, our single Editors' Choice for detecting and removing spyware. In this version, we found a marked improvement in scanning speed, tremendous performance in our real-time prevention and "torture system" removal tests, and a few new specialized removal tools. Although no antispyware app is truly "there" yet, Spy Sweeper is really closing in on the target.

The defensive-security field is no place to rest on your laurels. Antispyware developers have to adapt quickly to keep up with the competition and stay ahead of spyware creators. Although we can't predict how long it will maintain the designation, Webroot's Spy Sweeper 3.5 is currently the best defense against a tide of spyware.

## PERFORMANCE TESTS: ANTISPYWARE

To gauge the effectiveness of these applications against adware and spyware, we created two test-system images. One was heavily infested with dozens of malware applications. We analyzed this system via InCtrl5 logs to isolate nine adware and 13 spyware applications likely to be encountered in the wild. We also created another clean system image to infect in real time with ten chosen adware and spyware applications.

The pests we chose are among the trickiest, including CoolWebSearch, TV Media, and Istbar. We also used two keyloggers—RedHand SpyPC and Spector Pro—to see how the apps would fare against something more devious than pop-ups.

For the cleaning tests, scores reflect the number of cleaning successes out of a maximum total of adware or spyware applications installed. We measured success by whether an antispyware program removed enough of a pest's components to render it inoperable. The maximum total reflects how many total pests we audited, not the number of traces involved.

For the prevention tests, total scores were generated in a similar fashion. Each positive result or number means that an antispyware program was able to block enough of the components of a spyware app to keep it from running. This means that an antispyware package either totally stopped an install in real time or was able to block installed spyware immediately, with a warning to do a full subsequent scan. We also counted as successful a scan that launched automatically—either afterwards or on reboot—to fix a new problem.

Our prevention testing represents worst-case, not-quite-real-world scenarios, to test raw protection abilities. In some cases, you would get better results by using Windows XP's pop-up blocker and refusing to install unknown ActiveX controls.

*— Analysis written by Konstantinos Karagiannis*

| ANTISPYWARE<br>Higher scores are better.<br>■ YES □ NO | CLEANING | | | PREVENTION | | |
|---|---|---|---|---|---|---|
| | Adware cleaned<br>Out of 9 | Spyware cleaned<br>Out of 13 | Keyloggers cleaned<br>Out of 2 | Spyware install stopped<br>Out of 10 | Keylogger install stopped | Homepage change stopped |
| **DEDICATED ANTISPYWARE** | | | | | | |
| Ad-aware SE Plus 1.05 | 7 | 10 | 0 | 5 | □ | ■ |
| CounterSpy 1.0.22 | 5 | 10 | 1 | 5 | □ | ■ |
| eTrust PestPatrol 2005 Anti-Spyware | 6 | 9 | 1 | 8 | ■ | □ |
| McAfee AntiSpyware | 1 | 5 | 1 | 3 | ■ | □ |
| Spybot Search & Destroy 1.3 | 4 | 9 | 0 | 9 | □ | ■ |
| SpySubtract Pro 2.6 | 7 | 10 | 1 | 7 | ■ | ■ |
| **Spy Sweeper 3.5** | 9 | 12 | 2 | 10 | ■ | ■ |
| Spyware Doctor 3.0 for Windows | 7 | 11 | 0 | 10 | □ | ■ |
| **SECURITY SUITES** | | | | | | |
| Authentium Curtains for Windows 1.60 | 4 | 8 | 0 | 2 | □ | □ |
| BitDefender 8 Professional Plus | 5 | 3 | 0 | 4 | □ | □ |
| F-Secure Internet Security 2005 | 6 | 9 | 0 | 7 | □ | ■ |
| McAfee Internet Security 2005 | 4 | 7 | 0 | 6 | □ | ■ |
| Norman Internet Control 5.7 | 4 | 3 | 0 | 2 | □ | □ |
| Norton Internet Security Suite 2005 | 5 | 6 | 0 | 6 | □ | □ |
| Panda Platinum Internet Security 2005 | 8 | 11 | 1 | 8 | ■ | □ |
| Trend Micro PC-cillin Internet Security 2005 | 3 | 7 | 0 | 2 | □ | □ |
| ZoneAlarm Security Suite 5.5 | 1 | 0 | 0 | 0 | □ | □ |

RED denotes Editors' Choice.

**webroot®**
SOFTWARE, INC.

www.webroot.com • 800-772-9383