

Kill Spyware

Can Microsoft's free Windows Defender protect you from attacks? Experiment with 5 other antispware programs to find the best tool.

Initially, specialized antivirus and antivirus software, spyware and adware antispware software. This clear distinction is now gone. Macro and worm email degradation has forced antivirus software companies to look for other targets to fight, and the complexity of spyware makes it an extremely dangerous enemy. In recent tests, anti-virus tools have proved effective in fighting Trojan horses, 'back-end' programs (often classified as spyware) as well as adware. We will answer the question about the effectiveness of spyware removal tools.



For answers, we will look at six popular software: 5 software running on Windows Vista system including Grisoft AVG Anti-Spyware 7.5, Microsoft Windows Defender 1.1, PC Tools Spyware Doctor 5.0, Safer Networking Spybot Search & Destroy 1.4 and Webroot Spy Sweeper 5.5; and the 6th software - Lavasoft Ad-Aware 2007 Plus runs on Windows XP SP2 because at the time of this evaluation test, Ad-Aware did not have a version running on Vista, for this reason its results directly compared with other software.

German company AV-Test.org takes on the part of testing malware, attacking software with current adware and spyware patterns. AV-Test measures the ability to identify about 110,000 adware, spyware and rootkits in an inactive state. The template does not work like an application downloaded from the Internet but has not been run

or installed. Antispyware software should detect the pattern based on known identity data before it is activated. AV-Test also checks each software for behavioral identification and then cleans up 20 active adware and spyware. Since each threat can be subdivided into less than 100 components, cleaning is quite complex. Experimental group (NTN) checks software for the ability to clean up registry changes and important files. NTN also tested behavior-based features to detect and prevent changes to critical areas of the system without any information about the intruder. Spy writers constantly offer new threats, and security companies often need time to come up with data that identifies those threats. The detection feature is based on the behavior of antispyware protection software users during this critical period. NTN also evaluates false detection and working speed; about design, price and ease of use.

Result: Spyware Doctor 5.0 of PC Tools outperforms competitors running on Windows Vista. AVG Anti-Spyware 7.5 of Grisoft and Spy Sweeper 5.5 of Webroot are far below. Neither Spybot Search & Destroy nor Windows Defender are effective against current threats. On Windows XP, Lavasoft Ad-Aware did not impress on performance.

Spyware Doctor 5.0



The large and clearly designed function buttons of Spyware Doctor allow Easily set up real-time protection mode

In tests conducted by AV-Test, Spyware Doctor proved excellent in adware detection and removal. The results of dealing with spyware are less impressive but still better than other software. Spyware Doctor found 81% of adware models inactive and 100% of adware models worked, successfully removing almost all active adware templates. However, when dealing with other intruders, Spyware Doctor only detected 27% of inactive spyware related to banks and 43% of spyware steals passwords. It detects all spyware samples except the Trojan horse that steals the PSW.Maram password, and successfully eliminates 70% of the "vandals".

Spyware Doctor also performs behavioral detection tests, detects behavior that adds "Run" keys in HKCU and HKLM to prevent adware and spyware from changing IE's search pages and home pages. However, it does not detect changes to the Hosts file (spyware can be used to redirect to phishing websites).

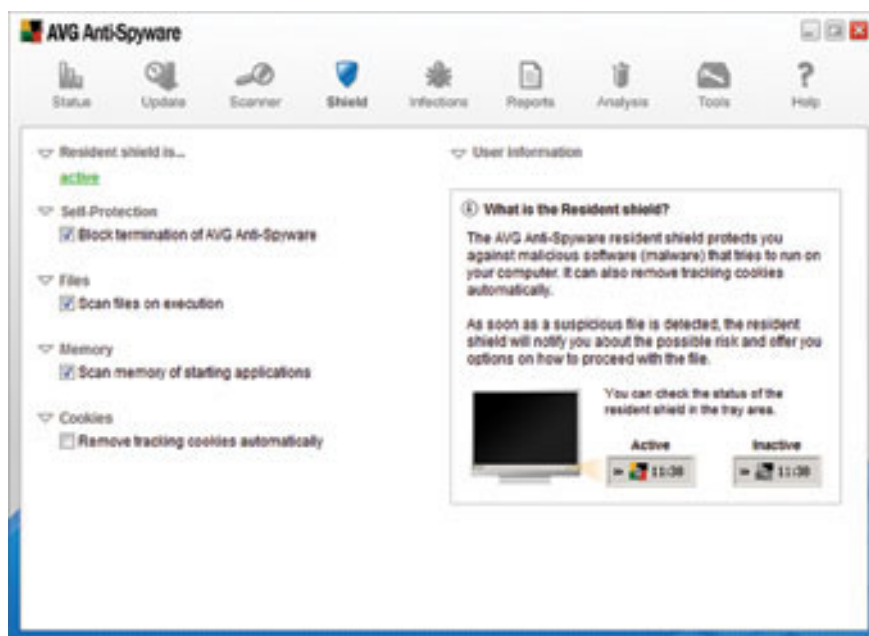
By default, Spyware Doctor does not turn on the anti-rootkit feature, which aims to increase scanning speed and minimize false detection (Spyware Doctor found 8 out of 9 inactive rootkit models). When this feature is turned on, it misrepresents 387 Google ad monitoring cookies, the New York Times website and other major sites.

PC Tools provides free telephone support for customers in the US. For an additional \$ 10, you have additional antivirus features.

Although there is a slight improvement in the interface and anti-spyware features, Spy Doctor is still the best option if you are looking for comprehensive adware and spyware protection and accept a \$ 30 price tag.

AVG Anti-Spyware 7.5

Grisoft, famous for its AVG Anti-Virus software, bought Ewido Networks last year and reworked its antispysware technology to launch AVG Anti-Spyware. This beautiful interface software is able to identify the highest threats (average%). Unfortunately it detects based on poor behavior and high level of false detection.



Despite good design and ease of use, AVG Anti-Spyware there is a high level of false detection

In the test, AVG Anti-Spyware did well for known adware and spyware detection. This software detects 19 of the 20 active templates (installed on the computer), only omitted Trojan horse Banbra specialized in collecting bank accounts. AVG software is also the best software so far to identify a large number of inactive adware, keyloggers, banking and rootkit spyware - a proof of full identity database.

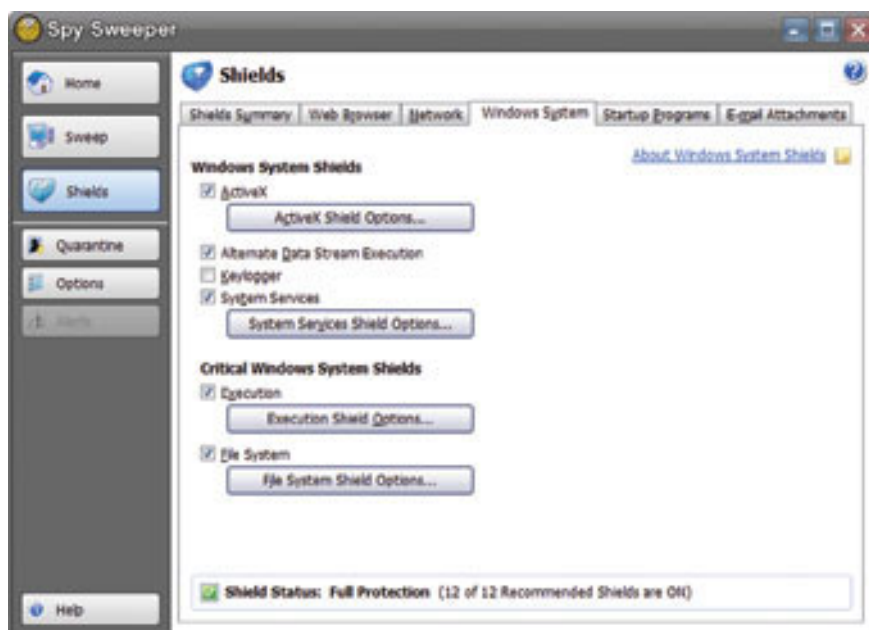
But when AVG does not recognize the threat, its behavior-based detection feature does not signal suspicious behavior that adds to the "Run" key in HKLM, changes to the default search page and home page of IE, and changes to the Hosts file. Therefore, this software may allow unknown threats to penetrate critical areas of the computer.

AVG Anti-Spyware is easy to use with easy-to-understand icons. But it lacks the anti-phishing feature to prevent users from accessing fake financial sites that collect personal information, and it does not have POP3, IMAP and SMTP scans to block email threats. In addition, you cannot set up a system restore point in case important files are accidentally deleted while killing spyware.

If you choose AVR Anti-Spyware, consider purchasing it through a distributor that provides telephone support. Grisoft only provides customer support via email. In short, AVG Anti-Spyware is powerful software with the most complete identity database, but is poor in behavior-based protection against unknown threats.

Spy Sweeper 5.5

Last year, Webroot Spy Sweeper 5.0 Beta was nominated for Best Buy product. The incident has changed with version 5.5. This software excelled at behavior-based detection, but disappointed with the ability to remove adware and spyware.



The Shields feature in Spy Sweeper prevents it change IE and other components.

When AV-Test gave Spy Sweeper a response to 20 active adware and spyware models, the software detected 85% of infected files and registry keys. However, when tested against adware and inactive spyware, the software only detected 26% of adware, 14% of spyware stole passwords and less than 2% of keylogger related to the bank. This software is also very poor in decontamination, only cleaning up 25% of adware infected files and registry keys and 15% of files and registry infections.

However, Spyware Sweeper excels in behavior-based detection. It successfully detects the behavior of adding 'Run' (HKCU and HKLM) and Startup folders with IE's default search and home page changes and Hosts file.

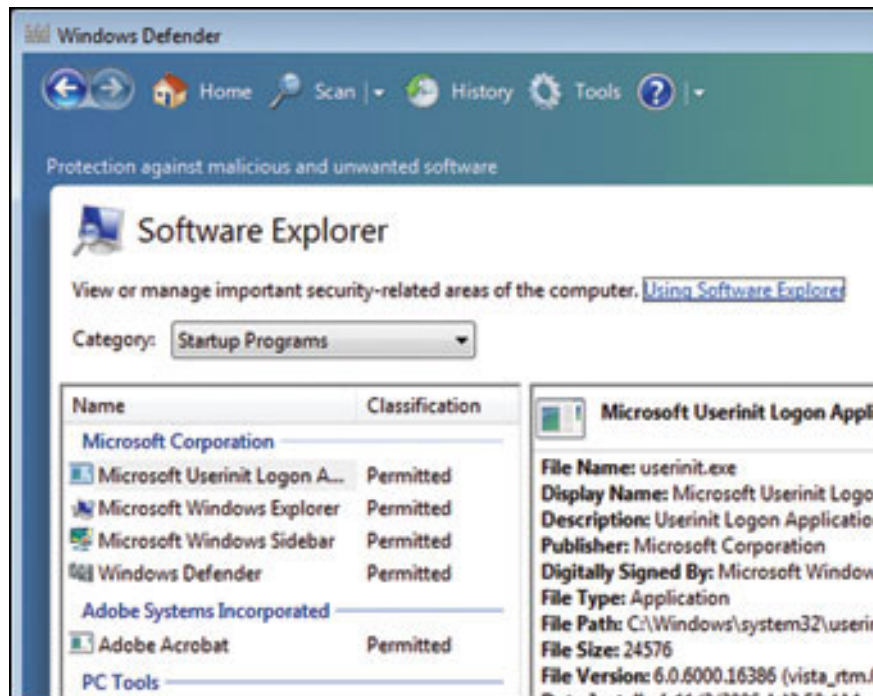
Spy Sweeper provides one-click access to system scanning, in testing, this function in the default setting is completed half faster than the fastest competitor. The company offers 10 hours of free phone support each week.

And antivirus protection will be provided if you pay 10USD more.

One annoying thing is that this software asks all the time during the installation of 4 popular browser toolbars (AOL, Das Ortliche, Google and Quero); 5 other software in the test 'know' these toolbars legally.

Windows Defender 1.1

Free Windows Defender from Microsoft comes with Windows Vista and has a free download version for Windows XP SP2. If the software introduced it directly as an anti-adware expert, NTN would have been less hard-working, but Defender's website claimed that the software provided 'free antispyware protection', but in this respect it failed. .



Windows Defender is free, but not capable support some form of spyware.

Windows Defender detected all 10 active adware threats, found that less than 50% of adware models were inactive - the results were average. In decontamination tests, this software successfully removed 55% of adware infected files and registry keys, does not eliminate PremiumSearch (adware fixes IE home and Favorites pages) and Starware (adware creates search bar in IE).

But for spyware, things are different. Testing showed that the software did not detect and did not remove 10 active spyware threats. It only found that 7% of spyware stolen passwords do not work.

Windows Defender excelled in behavior-based protection. It detected all the behavior of adding the "Run" (HKCU and HKLM) keys and the Startup folder, as well as all changes to IE's search and home pages and the Hosts file.

Windows Defender is easy to configure. It requires less user impact, in addition to choosing a low, medium or high security level, and this is the only stand-alone antispyware software out of 6 default test products with scan mode. according to the regular schedule. On Vista, it is the only antispyware tool integrated with IE 7 Protected Mode that allows scanning of downloaded files before saving to the computer and executing.

Note : the phone support service for this software is quite expensive. After 2 free calls, you pay \$ 35 for each call.

Windows Defender is good at adware and has strong behavior-based protection, but if there's a spyware that surpasses Defender's first line of defense, you'll need another tool to eliminate it.

Spybot Search & Destroy 1.4

Safer Networking's Spybot Search & Destroy is considered to be the first antispyware software to offer free real-time protection for loyal users. But recent tests show that this software is no longer effective antispyware.

Spybot overcame all misidentification tests, correctly detected legitimate toolbars and 6285 other sample files. Its Resident TeaTimer feature provides good behavior-based protection. It correctly detects the behavior of adding "Run" keys in HKCU and HKLM, changes to the home page and IE's default search page and Hosts file (but does not detect additions to the Startup folder).



Spybot is free and popular software, but no longer protects effectively.

However, Spybot discovered less than 2% of the threat of adware and spyware, indicating that the database identifies its threats is not enough. Dealing with active threats on the computer, it misses three of the 10 active adware and 4 out of 10 active spyware. Finally, it only kills 8% of active threats.

Spybot is easy to install and easy to use, but its interface seems to be aimed at technical savvy users. These users will like the feature to list BHOs (Browser Helper Objects) and installed ActiveX controls and secure file deletion. But they will not like the lack of automatic software updates.

Safer Networking does not provide telephone support, but NTN is impressed with the quality of web support services with forums.

For many years this free software has been the benchmark in antispyware, but unfortunately it has lost its competitiveness.

Lavasoft Ad-aware 2007 Plus



Ad-Aware blocks threats well but does not kill well. Ad-Aware 2007 Plus commercial version of Ad-Aware 2007 Free software. Despite its name, Lavasoft said that this software to remove spyware is as good as adware removal. For \$ 27, you get automatic updates, scheduled scanning and real-time protection not available for free software, however, in the test, Ad-Aware's work speed Plus does not meet the basic requirements.

In tests conducted by AV-Test.org, Ad-Aware failed to detect 9 out of 10 active spyware samples. Although 10 adware samples were detected, it killed only 35% of infected adware in files and registry keys.

Confronted with the huge amount of inactive 110,380 adware and spyware samples, the software's on-demand scanning feature found less than 2%. Ad-Aware 2007 Plus also has no anti-rootkit feature.

Compared to the detection feature based on the identification data, the software's behavior-based system blocking feature works much better. It blocks behavior that adds to the Registry's HKCU and HKLM keys, and detects changes to the Hosts and Startup files. Ad-Aware also features TrackSweep, which allows users to delete browsing history from Internet Explorer, Mozilla Firefox and Opera.

Unfortunately, the 2-branch design of this software creates unnecessary complexity. You must configure the Ad-Watch component (real-time monitoring and proactive protection) separate from the rest of the program.

Ad-Aware Plus has a certain improvement over the free version, but its performance is inferior to other anti-spyware tools.

At the time of the test, Ad-Aware Plus did not have a version of Windows Vista (currently available).

Ad-Aware 2007 Plus | Lavasoft, 77 good

With real-time protection and scheduled scanning, Ad-Aware 2007 Plus outperforms the same free software, but it is not the best antispysware available.

Nguyen Le

You finished reading the article "**Kill Spyware**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.