Andrew Joiner
Computer and Network Security
11 December 2007
R. Vezina

Prevent Infection and Exterminate Spyware

Steve Gibson first established the term spyware. He is currently the president of Gibson Research Corporation. His definition of spyware is "uninvited, unwanted, stealthful, invasive, annoying, exploitive, and potentially privacy-compromising PC add-on software whose ongoing presence in millions of PCs worldwide benefits not the computer's owner and operator, but the interests of the publishers of this troubling new class of software (Walker 42)."

Spyware is installed on the system without the owner or operators knowledge, also known as malware. Spyware is like a private detective to spy on what you do on the computer and internet. Just like private detectives want to gain some information, spyware does the same thing. Credit card numbers, usernames, and passwords are compromised. Common symptoms of spyware running on a computer can include sluggish performances, annoying pop up advertisements, and your homepage changing to another site (Walker 42).

The end user is usually responsible for infecting the system in spyware. End users love to download free applications such as free puzzles, screensavers, toolbars, games, and recipe's. Most of these applications are usually infected with spyware. Additionally, after a machine is infected with spyware and pop-ups, also called adware, users will often find a free pop-up blocker. This is also another way for spyware to infect the system. Although most of these types of downloads can include spyware, not all actually do. There are some programmers out there who do not include spyware in their programs to benefit the community. A simple way to prevent this type of spyware infection is by being more careful when choosing the source for computer entertainment (Walker 43).

Besides regular types of downloadable software, spyware is also obtainable by visiting websites. Visiting naughty sites, or by clicking on links saying you have won a prize often result in obtaining spyware. By not clicking on the links or visiting bad sites such as porn or sites to find serials for programs, it can enhance preventing spyware (Walker 43).

Another interesting way spyware creators generate revenue is by programming their spyware to use the computers modem. This type of spyware uses the computer modem without the user's approval to dial a toll number for premium services like 1-900-###-####. The longer the program can connect to the toll number, the higher the toll charge will be on the phone bill. A simple way in preventing this is by disconnecting the phone line when not in uses if dial-up is still the internet connection, or by considering to switching to broadband internet where available (Walker 48).

Cookies are another form of spyware. Not all cookies are bad, but they contain information about the computer user. When logging in to a website, it will log the username to automatically fill this field on the next visit. Shopping carts use the user cookies to track what the user has put into the shopping cart. By cleaning out cookies frequently from the computer, it will help prevent not only other spyware programs from snooping, but users that use the same computer (Walker 48).

An article which I found interesting was from PC Magazine. This article was about a form of spyware we might not even think about. Microsoft Word in this study, but even other products from Microsoft like Excel, Access, PowerPoint, or Outlook will have the same vulnerabilities. In Microsoft Word in particular, there are many fields which can be created to gain automatically updating content which can be hidden. For example, page numbers can be inserted and automatically updated when the page changes. This feature can also be hidden. Customized dynamic fields can be created to find information about the user or company. If a document is sent to a person on the network with mostly full access to the network drives, the dynamic fields can actually generate information from those files. Even though programs will not flag the file for spyware, I believe it still is a form of spyware. Let's reflect on the definition of spyware, it is information collected without permission from the computer user or computer owner (PC Magazine 2002).

To prevent information from being collected, there is a way to view any fields that are hidden as well as links inside the document. To view links, on the toolbar, choose VIEW, then LINKS. All links visible and hidden are shown in the dialog box. To view hidden visible and hidden fields, choose TOOLS then OPTIONS and then VIEW. Make sure the field shading is checked for the value ALWAYS (PC Magazine 2002).

PC World often provided detailed reviews about particular products on the market. They purchase software and provide laboratory tests on how well they perform. They then compare their results with products that do the same thing. In their article *Die, Spyware, Die!* they provide reviews on different spyware products in their 6 page article. They compared 5 different programs, 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. Since Lavasoft Ad-Aware 2007 Plus is not compatible with Windows Vista; they evaluated its performance on a Windows XP machine (PC World 102).

For this study, the company put both active and inactive spyware and adware objects on the machines. Active spyware objects refer to installed spyware where as inactive spyware pertains to a file downloaded that contains spyware but has not been installed yet (PC World 103).

Spyware Doctor 5.0 rated as number one from *PC World* magazine; found 100% of the active adware and 81% of the inactive adware on the Windows Vista machines. It found 90% of active spyware and 38% of inactive spyware. For removal, it was able to

cleanse 90% of active adware and 70% of active spyware. Spyware Doctor also prevented HKCU and HKLM registry keys from being added or altered. It did not however provide protection against Hosts file. Protection for redirecting webpage is not available but it provides phishing protection on web sites (PC World 103). Spyware Doctor costs $30 and has 24/7 toll free customer support. An extra $10 will also provide virus protection (PC World 104).

AVG Anti-Spyware 7.5 by Grisoft was ranked as number two from *PC World* magazine. This program accounted for the highest number of threats from spyware. What this program is not careful about however is the high number of false positives it included. This program found 100% of the active adware samples, but only found 69% of inactive adware samples. For spyware, it found 90% of active spyware and 38% of inactive spyware. In cleaning the system, it was able to disinfect 30% of active adware and 50% of active spyware. Threats the program did not recognized allowed programs to change the HKLM registry keys. Due to this, the internet browser home page changed exploiting the system (PC World 104).

Spy Sweeper 5.5 by Webroot was ranked as number three. Spy Sweeper was able to find 100% of active adware samples but only 26 % of inactive adware samples. For spyware, it found 10% of inactive spyware and 70% of active spyware. It was able to clean 25% of the active adware but only 15% of active spyware. According to the article, version 5.0 Beta is much better than version 5.5. The program was decent at detecting spyware, but was burdened on actually removing spyware from the actual machine. It was able to detect HKCU and HKLM registry key changes as well as changes to the default webpage. It does not provide scheduled scans and offers limited support. It was able to perform a full system scan at the fastest speed. During installation, the program asks to install four toolbars for the internet browser which are AOL, Das Ortliche, Google, and Quero (PC World 106).

Windows Defender 1.1 by Microsoft was ranked as number three. Windows Defender is available for Windows XP Service Pack 2 and is shipped with all Vista machines. Windows Defender was able to find 100% of active adware samples and 48% inactive adware samples. For spyware, it was able to find 5% of inactive spyware and 0% of active spyware. For cleansing the system, it cleaned 55% of active adware but 0% of active spyware objects. It was also able to find changes to HKCU and HKLM registry keys. This software provides easy scanning with a click of a button. Only two support phone calls are free, after that it will cost $35 each (PC World 106).

Spybot Search & Destroy 1.4 by Safer Networking was ranked as number four. Spybot was able to find 70% of active adware samples and only 2% of inactive adware samples. For spyware, it found 0.4% inactive spyware and 60% of active spyware. For cleaning, it disinfected 5% of active adware and 10% of active spyware. Spybot has a low rate of false positives during the scans. (PC World 106) It was able to detect HKCU and HKLM registry key changes. It is easy to install and provides real-time protection through teatimer.exe (PC World 108).

For part of this final paper, I decided to have a hands on activity to try to mimic the study already performed by PC World. For this study, I downloaded an installed five spyware detection programs and took screenshots of the results. The programs used are Spyware Doctor, AVG Anti-Spyware, Windows Defender, Spybot, and Ad-Aware. Screenshots are found at the end of the report.

Spyware Doctor was an easy program to use and receive definition updates. I was however limited to some features as it was only a trial version of the program. The retail price is roughly $30. During the scan, it found a bunch of cookies, which can be considered an important detail, but it did find two other major sightings. NewdotNet package and a few browser hijacks were reported after the scan. The scan took around forty-five minutes to perform.

AVG Anti-Spyware was also an easy program to use and receive definition updates. It was also a trial, but most of the feature was available. The only limitation was the lack of real-time scanning as well as automatic updating. This program only took thirty five minutes to perform and it was able to find only the NewdotNet spyware package.

Ad-Aware took a significantly long time to scan the machine at a whopping fifty six minutes. After the scan, it found the various cookie files, but it did not find the NewdotNet package. It did find another object, MRU which stands for Most Recently Used. This is a key found in the registry saying what file was recently used. There really is no risk to this finding.

Spybot was able to find all of the cookies the other files were able to find and it was also able to find the NewdotNet spyware package. Spybot did not talk long at all to scan the machine.

Windows Defender was a free package to download and install from Microsoft after validation of Windows XP. After installing, the program wanted to provide real-time scanning of the computer as well as inform the user the definition files are not up to date. After the scan, which did not nearly take as long as the other programs, found the NewdotNet spyware package. Since this program was the last one I tested, I decided to remove the NewdotNet spyware. After removal, I decided to scan the computer again with AVG Anti-Spyware and the NewdotNet spyware package was still installed. After AVG Anti-Spyware removed the package, I scanned with Spyware Doctor and that program determined the NewdotNet was disinfected from the system.

My findings were similar to PC World magazine. Spyware Doctor was able to find the most objects, but since I had a trial, I was not able to determine whether the spyware object was able to be removed effectively. The second best program to my findings was AVG Anti-Spyware. This program was able to detect the spyware object and remove it effectively. Windows Defender was not able to find the hijacks from the browser, but it did find NewdotNet. The program was however unable to successfully remove the object. Spybot was able to find the NewdotNet package and all of the cookies. I was not able to test removal of the package as it was successfully removed

by AVG. The last program was Ad-Aware and it did not find a single threat. As you can see, my findings are similar to those found by PC Magazine.

The threat NewdotNet which was found on my machine is a plug-in for Internet Explorer. It provides pop-up advertisements to the user based on surfing characteristics. The form of spyware also points to a site every time an address is typed incorrectly. This stealth plug-in also is able to update itself on the internet when a new NewdotNet spyware version is available (SpywareRemove 2007).

Preventing spyware is extremely difficult; however, there are a few tools out there which can be of service to the community. After this laboratory testing and research, I decided I will use AVG Anti-Spyware to scan my machine. It is free after all for the limited version; however, it provides the necessary scans. The automatic updating is really not a feature I would use anyway as I like to even update Windows XP manually.

Bibliography

Naraine, Ryan. "Die, Spyware, Die!" PC World 25.10 (Oct 2007): 101-108.

NewDotNet Removal Instructions. 7 December 2007 <http://www.spywareremove.com/removeNewDotNet.html>.

Walker, Andy. Absolute Beginner's Guide to Security, Spam, Spyware and Viruses. Indianapolis: Que, 2005.

"Word as Spyware." PC Magazine 21.22 (Dec 24, 2002): 82.

Appendix Snapshots

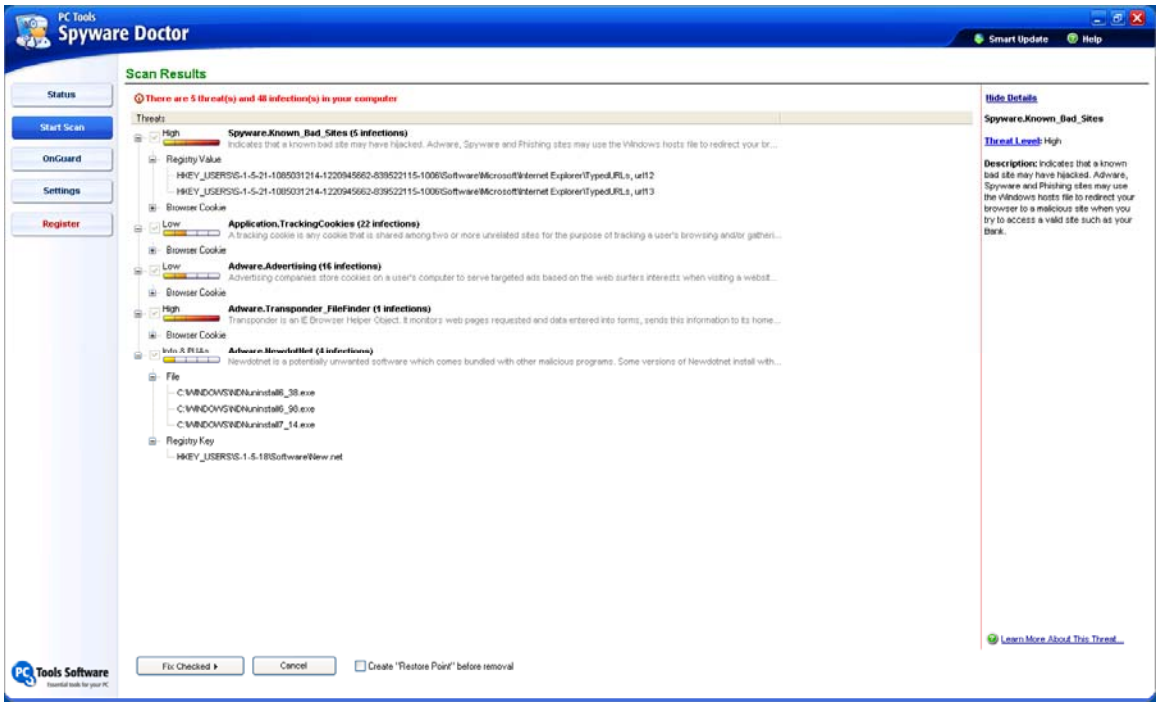

Figure 1. Spyware Doctor

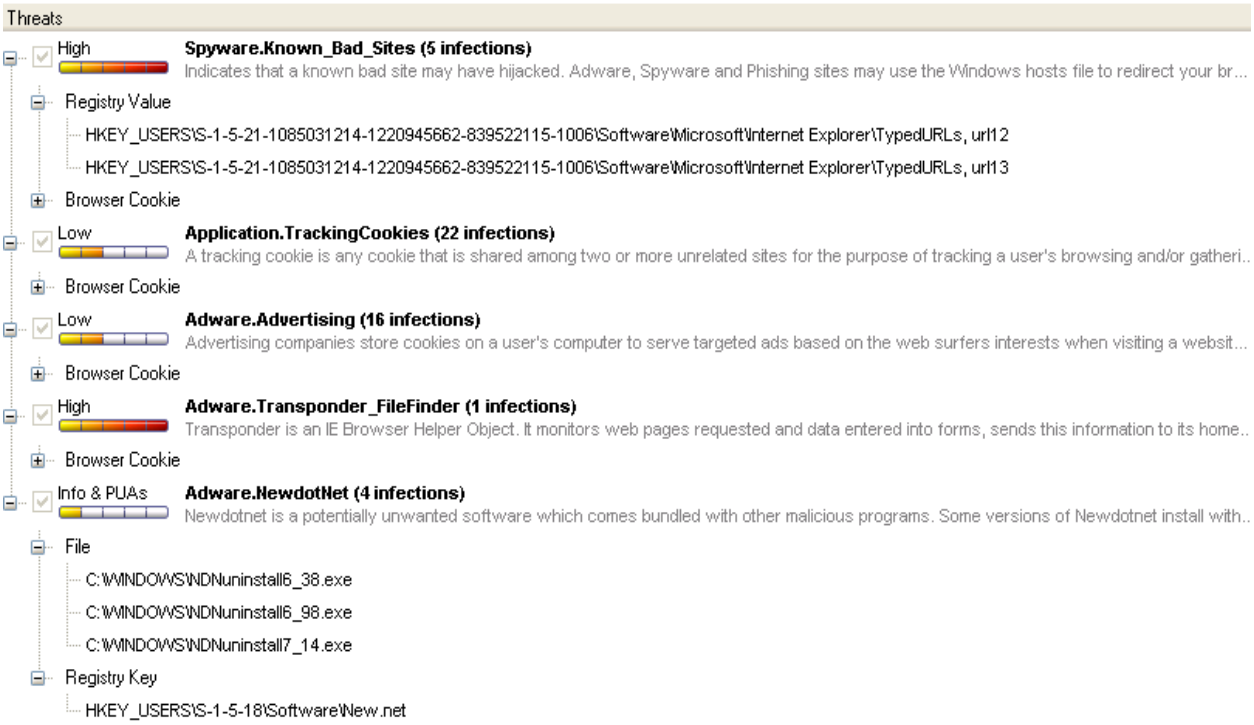

Figure 2. Spyware Doctor Enlarged

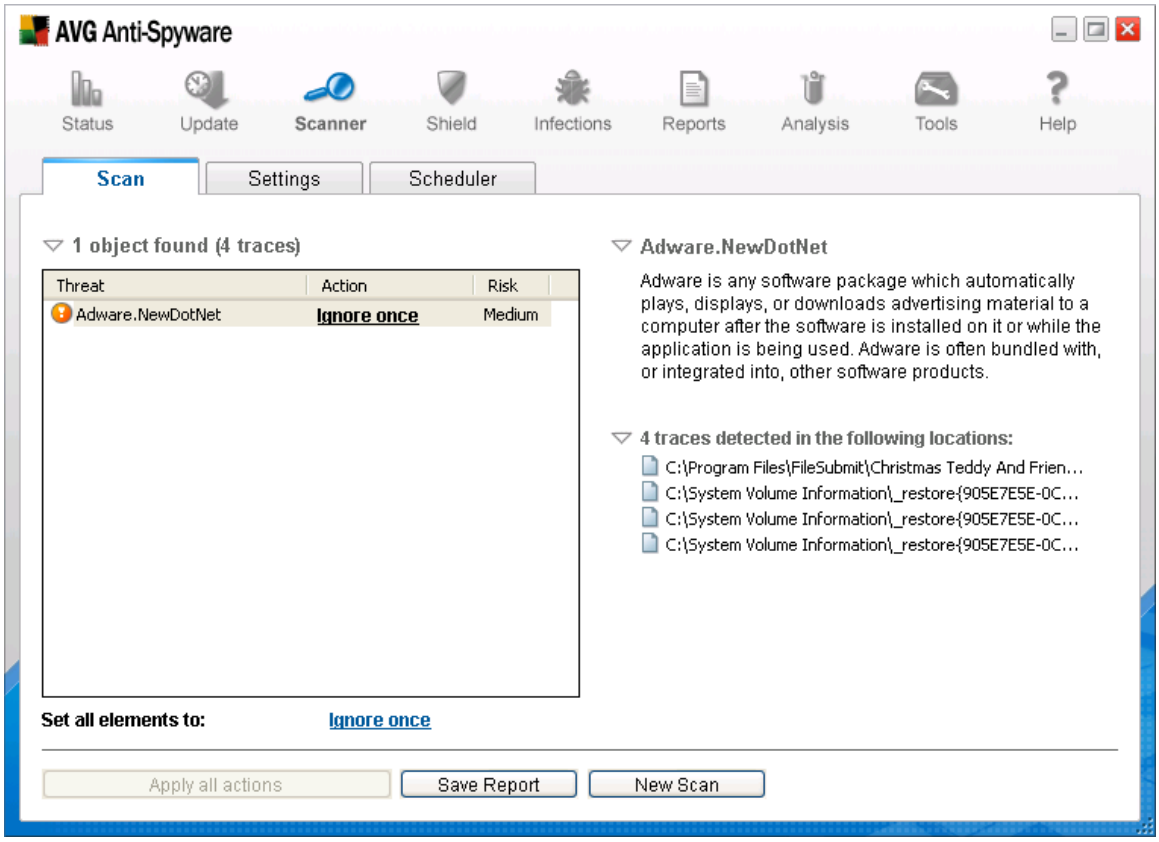

Figure 3. AVG Anti-Spyware

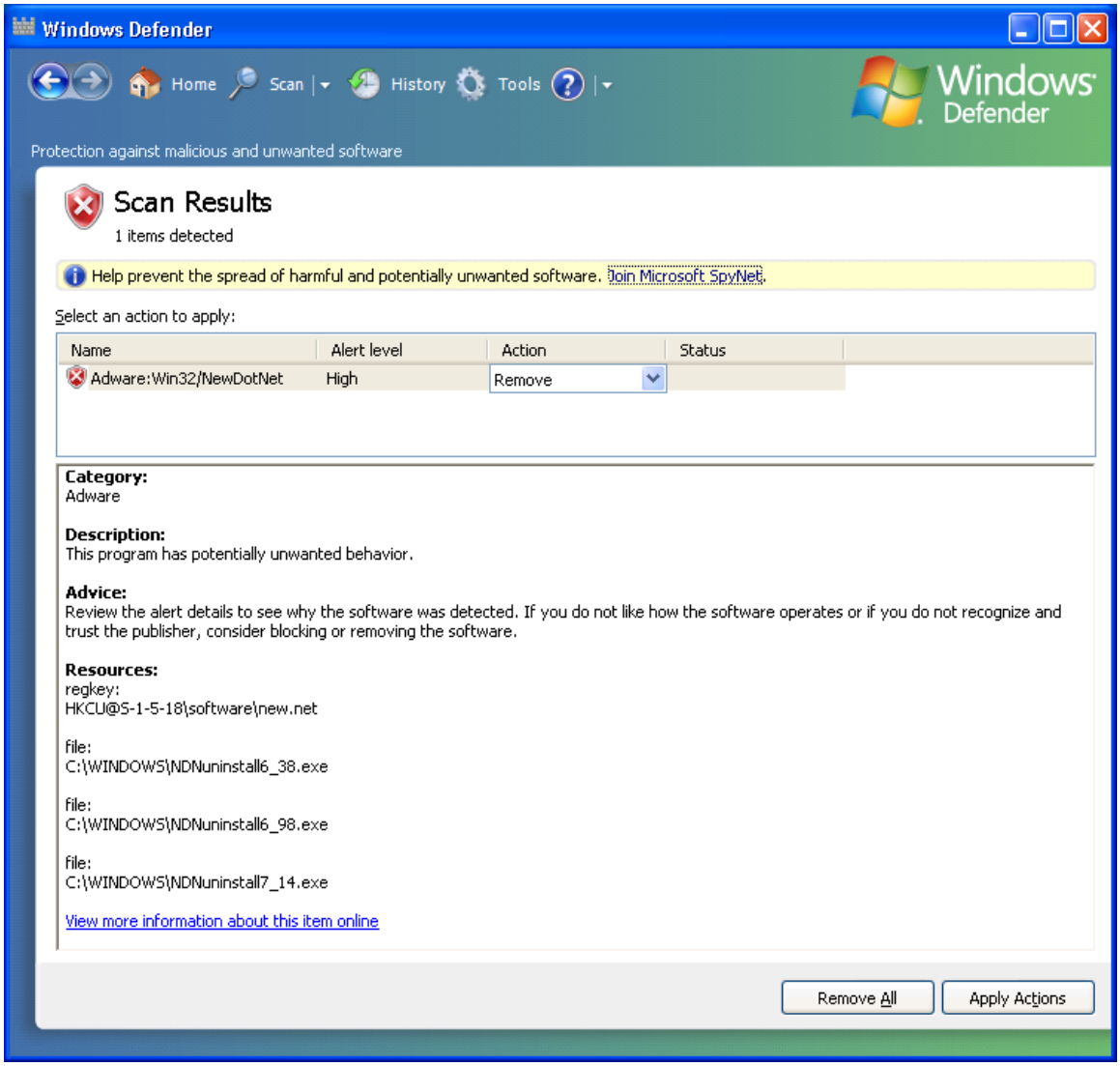

Figure 4. Windows Defender

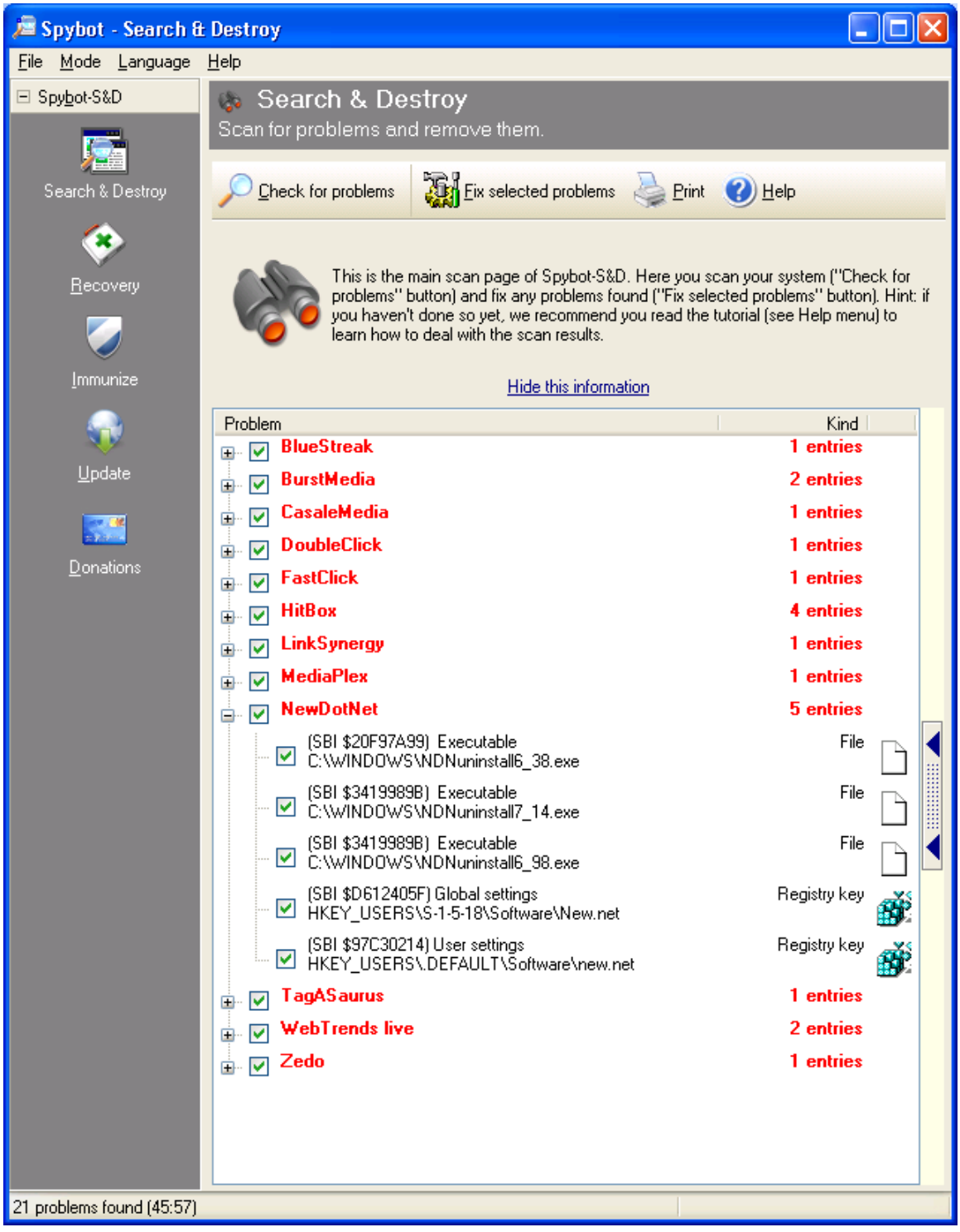

Figure 5. Spybot

Figure 6. Ad-Aware