



Anti-Spyware Testing Methodology

Methodology for Comparing Anti-Spyware Products

Table of Contents

Anti-Spyware Testing Methodology	3
Introduction	3
Evaluate the Underlying Technology	3
Evaluate the Dynamic Element: Today’s Anti-Spyware Content	4
Objective Testing Methodology	5
Snapshot Tools	5
Test Proactive Protection	5
Test Reactive Protection	5
Evaluating the Results	6
What to Do with the Reds and Yellows?	6
Resources	6

Methodology for Comparing Anti-Spyware Products

Anti-Spyware Testing Methodology

Introduction

A variety of consumer, shareware, and business-class anti-spyware products are available today. Unlike the mature anti-virus market, where vendors have standardized on naming conventions and share collections to provide the widest protection to their customers, each anti-spyware product has a closed database and uses unique naming schemes. Spyware (including not only malicious code but also adware, jokes, etc.)¹ tends to be more complex than “traditional” malware in the sheer number of registry entries, files, self-protection mechanisms, and other tools that it employs. These factors make it difficult for organizations wanting to evaluate anti-spyware products to measure one against another.

This document presents a methodology for comparing anti-spyware products in as objective a manner as possible, showing steps to eliminate bias toward one product over another. It recognizes that there are two aspects to evaluate when determining how well an anti-spyware product will protect your organization’s productivity and computing and information assets.

First, you should evaluate the underlying technology of the anti-spyware product. This is the component that will not change over time, and that limits or enables the overall effectiveness of the product.

Second, you should review the dynamic element: a specific anti-spyware product’s database of unwanted programs and the vendor’s processes, resources, and ability to update that database on a regular basis.

Evaluate the Underlying Technology

The technology foundation underlying an anti-spyware product determines its long-term effectiveness and

capabilities, as well as your costs of owning and managing it. When reviewing the technology of an anti-spyware product take into account the following topics/questions.

- **How critical is information security to your organization?**

Some anti-spyware products provide true on-access, proactive capabilities for preventing PUPs from installing on a computer in the first place. Others provide “real-time,” reactive, protection that cleans off a PUP when they have detected its installation.

Both approaches work well to remove known threats, but the latter carries more risk. In the period between the installation of a PUP and its detection by the anti-spyware product, there is opportunity for downloading additional unknown PUPs or transmitting your confidential information to the Internet.

- **How does the anti-spyware product identify spyware?**

Some products rely on file names only. This has obvious benefits in that it is easy to create a large database quickly and perform rapid system scans. It is also very prone to false positives and is easy to fool with a changed file name.

Some products rely on MD5 hashes to identify the contents of a PUP’s executable files. Hashes also allow rapid system scans and are more reliable than name matching, but PUP writers can still outwit it by changing as little as one byte in their files.

Some products, notably those from established anti-virus companies, perform deep scans of files to identify PUPs. Deep scanning does take longer to perform on-demand system scans, but you can have more confidence in the results. Also, since the scans usually are also looking for viruses, the total scan time for both functions is not appreciably longer than separate anti-virus and anti-spyware scans.

- **Are you willing to accept reboots to ensure full cleaning?**

Many anti-spyware products are able to identify unwanted processes in running memory, but not all can unload DLLs without requiring a system reboot or application exit. If your environment requires maximum uptime and minimal system

¹ This document will use the term potentially unwanted program or PUP to refer to the various categories of spyware, adware, etc.

or user interruption, you will weight this capability higher.

- **How does the anti-spyware product protect against unknown threats?**

The better anti-spyware products provide some form of access protection or shielding to protect key files and directories on your computer from compromise. As with detection of known threats, these functions can be either proactive or reactive.

Proactive access protection prevents PUPs from performing certain steps such as modifying host files, executing from temp directories, initiating outbound communication on certain ports, and other files. Reactive shields monitor application behavior and trigger when a set of rules has been broken. The difference is in preventing a behavior or reacting to an accomplished fact.

Look at the whole anti-spyware solution to determine what protection or shielding it provides, how extensible that capability is: can you add your own rules? Can you exclude wanted programs?

- **How can you manage the anti-spyware product in your organization?**

As the size of an organization grows, so too does the importance of centralized management. When considering an anti-spyware solution, look not just at the desktop component but also your ability to manage those desktop agents. What facilities does the solution provide for remote deployment and updating of agents as well as reporting on detections and cleaning? Can you create, deploy, and enforce anti-spyware policies?

- **What does it cost?**

Many of the anti-spyware products on the market are freeware or shareware. This is appropriate since they were launched as consumer products.

It is easy to assume that a low license cost translates into a low overall cost. However, you will need to evaluate the operations costs associated with “free.” Factor in such elements as the cost to deploy, upgrade, gather reports, and so on. Also factor in costs of onsite support and lost productivity while your staff cleans and reboots systems.

Evaluate the Dynamic Element: Today's Anti-Spyware Content

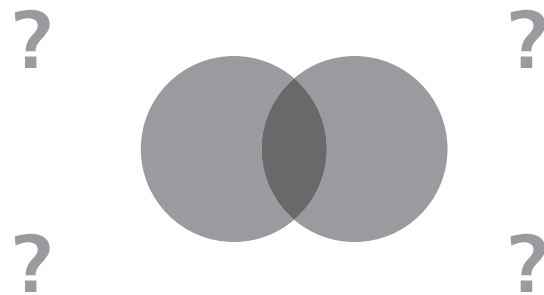
An anti-spyware product will have abilities to detect and protect against both unknown and known threats. Known threats are those for which the vendor's research team has created detections (signatures, heuristic drivers, MD5 hashes, name tables). In addition to providing PUPs detection, the vendor distributes instructions that allow the anti-spyware product to clean or remove PUPs from your computer.

PUPs are complex products, often integrating tightly into your operating system or applications, and relying on a variety of tactics to avoid detection and removal. Some PUPs are well behaved, and provide uninstall scripts. Others create multiple registry keys with many values, load watcher processes into memory to reload (or redownload) each other, or mimic operating system files.

For these reasons, as well as the relative youth of the anti-spyware market, it is often hard for any single anti-spyware product to clean every component of PUPs off your computer. All anti-spyware vendors rely on their user communities to submit samples of suspected PUPs in order to grow their databases. McAfee is taking a leadership position in working with other vendors to create a consortium for sample sharing, common naming, and counting such as exists today in the more mature anti-virus market.

Given that no single anti-spyware product today will detect and remove all PUPs, how can you objectively test the effectiveness of any of them?

One common methodology is to compromise a computer with as many PUPs as possible, then run several anti-spyware products on the computer in sequence. No matter which product is run first, the second always finds some set of missed PUPs. If you then run a third anti-spyware product on the same computer, you'll detect another set of PUPs missed by both of the first two scans.



Two anti-spyware products catch some of the same PUPs, but what do they both miss?

It is also tempting to assume that the second anti-spyware product would have detected everything caught by the first, plus what it caught that the first missed. This is a trap. As the diagram above shows, the detection capabilities of any two anti-spyware products will overlap, but each will detect items missed by the other.

If you are going to compare anti-spyware products head-to-head you must run at least two tests. Create your test environment and run Product A then Product B. Repeat the test with Product B then Product A. Compare all logs. In this way you will get a more balanced view of each product's detection and removal capabilities.

Objective Testing Methodology

A better method to compare anti-spyware products is to use some objective tool to quantify and detail the state of your computer (files, registry) before attempting to compromise it, apply a single anti-spyware product, then take a second snapshot of the system and compare it to the original. Differences between these reports will show you exactly what the PUPs you installed did to the computer and how much of that was prevented, eliminated, or corrected by the anti-spyware product.

An objective test will also compare both proactive/preventative protection as well as “after-the-fact,” clean-up capabilities of the anti-spyware product. The “recipes” that follow suggest a plan you can adapt to your needs and environment.

Snapshot Tools

Several products exist that take before and after snapshots of critical components of the Windows® operating system and file system to expose the effects of a software installation. Two readily available examples are Inctrl5 (from *PC Magazine*)² and Tracker (from Evans Programming)³.

Test Proactive Protection

Test the ability of an anti-spyware product to prevent PUPs from installing themselves and other software on a computer. This test reflects the anti-spyware product’s ability to protect your systems and information by keeping an otherwise clean computer clean.

1. Begin with a clean computer (e.g., standard Windows installation, never been connected to the Internet).
2. Install a snapshot product like one of those noted above.
3. Image the system at this point so you can run subsequent tests from the identical starting state.
4. Install the anti-spyware product and update its database to ensure that you are testing the most current content. Make sure the product is running with all default features enabled.⁴
5. Take a snapshot of your operating and file systems.
6. Compromise the computer by launching Internet Explorer and downloading PUPs from the Internet. See <http://spywarewarrior.com/asw-test-guide.htm#test> for a well-designed test methodology and test sets. Note that these tests were run against various consumer anti-spyware

products in late 2004. The content is therefore somewhat dated, but the methodology is sound and repeatable).

7. Allow a few minutes to pass. During this time the downloaded PUPs may in turn attempt to download and install other applications. When disk and network activity has ceased, proceed.
8. Take a second system snapshot. Review the state of the system as compared to snapshot 1.

Test Reactive Protection

Test the ability of an anti-spyware product to clean PUPs from an already compromised computer. This test reflects the anti-spyware product’s ability to clean up a computer that has already become compromised by users surfing to sites that download PUPs.

1. Begin with a clean computer (e.g., standard Windows installation, never been connected to the Internet)
2. Install a snapshot product like one of those noted above.
3. Image the system at this point so you can run subsequent tests from the identical starting state.
4. Install the anti-spyware product and update its database to ensure that you are testing the most current content. Make sure the product is *disabled* so it will neither prevent nor clean anything.
5. Take a snapshot of your operating and file systems.
6. Compromise the computer by downloading PUPs from the Internet. See <http://spywarewarrior.com/asw-test-guide.htm#test> for a well-designed test methodology and test sets. Note that these tests were run against various consumer anti-spyware products in late 2004. The content is therefore somewhat dated, but the methodology is sound and repeatable.
7. Allow a few minutes to pass. During this time the downloaded PUPs may in turn attempt to download and install other applications. When disk and network activity has ceased, proceed.
8. After compromising the computer, reboot and restart your browser (Internet Explorer—IE) before attempting to scan and remove the PUPs. This ensures the PUPs are fully installed and functional: some will launch extra processes when Windows starts and others require IE to load them. This also tests the anti-spyware product’s ability to remove active PUPs.

² <http://www.pcmag.com/article2/0,4149,25126,00.asp>

³ <http://www.evansprogramming.com/tracker.asp>

⁴ For up-to-the-minute content from McAfee, download the latest daily DAT file. You may also want to download the latest McAfee beta DAT file from the Virus Information Library site (<http://vil.nai.com/vil/averttools.asp>). Beta DATs contain early visibility into malware drivers before they appear in the officially released DAT files.

9. Activate the anti-spyware product and scan the computer to detect and remove the PUPs you have downloaded.
10. Take a second system snapshot. Review the state of the system as compared to snapshot 1.

Evaluating the Results

When reviewing the system snapshots following each test cycle above, you will find it useful to set goals and metrics so that you can compare the ability of each anti-spyware product to protect your system, as well as rate the risk imposed by those items the product missed.

There are no standards for quantifying the things an anti-spyware product detects. Some itemize every single registry key, key value, file, directory and other information PUPs create on your system. Others count only the names of the PUPs, while still others range anywhere in between. A useful categorization for counting leftovers is:

- The PUP itself. How many full or partial PUPs did the anti-spyware product leave behind on your test computer?
- If the anti-spyware product only partially removed the PUPs, identify what was left behind of each:
 - Files
 - Folders
 - Registry keys (values are less important—if the anti-spyware product removes the key, its associated values will also be removed. Counting values is an artificial way to boost “detections”)

A useful metric to apply to these leftovers might be as follows:

Red	.EXEs, .DLLs, .coms, scripts, or other executable code that could reload the PUP or cause other damage.
Yellow	Registry keys, folders, text files, or other non-executable code that should have been cleaned but that do not represent a security threat to your computer or information.
Green	Temporary files, IE cache files, etc., that are left behind by the operating system or software installer, but that don't represent pieces of the PUP itself.

You may want to apply a numeric rank to the categories Red, Yellow, and Green. You may also want to apply a multiplier to differentiate between those items associated with a PUP the anti-spyware product missed entirely from those left after a partial removal.

What to Do with the Reds and Yellows?

To help enhance the protection capabilities of each anti-spyware product you evaluate, please send samples and logs of all missed PUPs to each of the anti-spyware vendors so they can update their databases. In addition to being good for the vendor and user community, it also gives you another way to evaluate the vendors: how easy is it to submit samples and how quickly do the vendors add the new PUP to their databases?

McAfee accepts malware and PUP submissions via e-mail or the WebImmune system. You can find information about how to submit samples at the Virus Information Library: <http://vil.nai.com/vil/default.asp>.

Resources

For more details about the varying methods anti-spyware companies use to count unwanted programs in their databases and on your computer, contact your McAfee Account Manager and ask for the following white paper *Counting Spyware Detections*.

For more details on matching anti-spyware products to your business needs, contact your McAfee Account Manager and ask for the following white paper *Anti-Spyware: Choosing the Right Solution for Your Business*.

To speed your testing, consider a virtual PC program such as Microsoft® Virtual PC (<http://www.microsoft.com/windows/virtualpc/default.mspx>). This kind of tool saves reconfiguration time compared to re-imaging the entire PC.

For more information on designing specific ePO reports on PUP activity, ask for the white paper titled Tracking Potentially Unwanted Programs.