Why You Should Not Play the Numbers Game with Anti-Spyware Vendors

Ed English

Security technology vendors relish throwing out numbers: We have “X” more pattern files or “Y” more algorithms than any other vendor. We have more >>fill in this blank with your most-often-heard sales pitch<< to make you more secure.

But if you inquire about what is actually being counted, you often find the impressive totals may not be as relevant as they first sound. One such case is the number of spyware threats some anti-spyware vendors claim to overcome. This is one numbers game that should not be played.

Some anti-spyware providers boast they can eliminate almost 100,000 spyware traces. At first mention, that sounds impressive, right? If you’re a member of an IT department — help desk, operations, security, system management, desktop management, network admin, etc. — don’t you feel your company is better protected knowing that you have an anti-spyware defense system that combats those legions of threats? After all, the larger the number, the more secure you feel. You can report to your CIO, CTO, or even CEO that you purchased a comprehensive anti-spyware solution that protects your organization’s thousands of PCs and laptops from a whopping number of intrusive malware threats. Executives, even product reviewers and IT analysts, naturally, may think “bigger is better.”

But that big number has one big problem: What are the anti-spyware vendors counting as a threat or spyware trace?

If you sent out your army to disarm the rebels, when they reported their success capturing the rebels’ weapons, you would want to know whether they were counting guns, bullets, rope, stones, rocket launchers, or rockets, right? It’s the same with spyware.

Many anti-spyware vendors count both folders and the individual files in a folder as countable “threats.” A folder could contain 1 or 100 files and even more folders inside the folder, all associated with a single spyware product. Although deleting the one

ED ENGLISH is Trend Micro’s general manager of consumer products, North America. Ed was the CEO and founder of InterMute, which focused on anti-spyware and online ad-blocking technologies. InterMute was acquired by Trend Micro in May 2005. Trend Micro, Inc., is a leader in network antivirus and Internet content security software and services. The Tokyo-based corporation has business units worldwide. Trend Micro products are sold through corporate and value-added resellers and managed service providers. For additional information and evaluation copies of all Trend Micro products, visit its Web site, www.trendmicro.com.
root folder might eliminate that spyware problem, some vendors choose to count each file and folder individually for the sole purpose of upping the “threat deleted count.”

Additionally, how many Internet cookies or “false positives” are included in a vendor’s gargantuan threat-detection number? Unfortunately, several notable anti-spyware offerings identify useful personalization cookies from Web sites such as The Wall Street Journal and TV Guide as spyware. Alarms go off in these vendors’ products when such cookies are detected, wasting both end-user and help-desk time dealing with these noninvasive “threats.” An optimal anti-spyware solution minimizes false positives by adhering to a more responsible and mature approach to defining a legitimate spyware threat.

When evaluating anti-spyware solutions, don’t be tempted to ask, “How many spyware threats do you remove, or how large is your definitions database?” Instead, ask more qualitative (rather than quantitative) questions, such as those presented here, to get the anti-spyware solution that meets your needs.

HOW DOES THE PROVIDER DEFINE SPYWARE?
Spyware is any program that monitors or subverts users’ computer or online activities without their explicit consent. Spyware installations often employ deceitful tactics, such as a silent install or presenting users with lengthy and cumbersome end-user license agreements (EULAs). Some spyware EULAs are 50 or more screens long. The average user about to install a software program cannot be reasonably expected to read or understand such lengthy license agreements. Spyware marketers know this and often include sections in the agreement that grant them permission to do just about anything they want with users’ computers or data.

WHAT ARE THE PERFORMANCE CHARACTERISTICS OF THE ANTI-SPYWARE PRODUCT?
How large is the download file size of the product? How much computer resources are consumed by the anti-spyware product? Does it use excessive amounts of memory, disk, or CPU processing? Investigate whether the product has been designed to use minimal computer resources while providing extremely high-speed scanning. How much of the hard disk does the anti-spyware product actually scan? This can vary widely. Some products skip portions of the hard drive, perhaps to shorten their scan times. Check to see if the product delivers both full-disk scanning and quick-scan options.

WHAT TYPES OF SPYWARE DOES THE APPLICATION REMOVE?
Most anti-spyware products can remove standard spyware threats. The usual suspects include key loggers, adware, browser helper objects (BHOs), browser toolbars, and so forth. However, ask the vendors how they handle threats from the new generation of “polymorphic spyware” — examples include CoolWebSearch, HomeSearch, and Look2Me. These are among the most challenging forms of spyware to remove.

By continually modifying their own filenames and file contents, polymorphic spyware escapes traditional filename and signature scanning detection methods. Even the location where the spyware is installed may be random, thus making every installation unique. Due to its continuous morphing and mutating, polymorphic spyware cannot be removed with conventional anti-spyware tools.

Because of the vibrant spyware economy, new variations are being released almost every week. Some anti-spyware products can deal with the older, simpler versions of these now complex threats; however, they cannot deal with the newer, more tenacious spyware threats.
HOW DOES THE PROVIDER CONDUCT ITS SPYWARE RESEARCH?
To deliver and maintain the best-of-breed anti-spyware solution, a provider must construct and utilize a comprehensive set of methods, tools, and tactics to detect and analyze new spyware threats in a timely manner. Some anti-spyware vendors claim use of Web crawlers to build their spyware databases. Such techniques may make for nice press releases but are akin to combing the entire Atlantic Ocean for fish, rather than focusing on George’s Bank. Some automation in a spyware harvesting methodology is appropriate, but detailed analysis of individual programs is required to construct and maintain a quality anti-spyware database with minimum false positives.

Anti-spyware products should allow end users to easily generate spyware reports — with a push of a button — so the symptoms and negative impact the spyware caused on a PC or laptop can be thoroughly and properly investigated. To devise a proper remedy, researchers need to know how the spyware behaves on a system.

To build and maintain a top-quality anti-spyware database requires a talented engineering team to harvest, analyze, and classify new spyware threats. It is important to receive spyware reports from a diverse range of PC end users, including corporate IT professionals, knowledgeable help-desk technicians, as well as home and home-office users. Consumers surf to different Internet Web sites than business users and tend to pick up the newest spyware releases before they appear in the corporate environment.

WHAT TECHNOLOGIES DOES THE PROVIDER USE TO IDENTIFY THE ORIGIN OF THE SPYWARE AND PROVIDE REAL-TIME PREVENTION?
If you know how spyware infected a system, you can take steps to prevent reinfection. Spyware is often quietly installed onto a computer by a carrier program. By unmasking the source of spyware, users can blacklist carrier programs to avoid reinfections. (Both blacklist and whitelist capabilities are

HOW DOES THE PROVIDER LOOK FOR SPYWARE INFECTIONS?
Is detection “dumb,” looking for filenames only? Lightweight or casual detection methods can result in deleting the wrong programs. Confirm that the product employs a methodology to identify spyware on a computer, including a database of MD5 spyware signatures of every known variant of every spyware threat monitored. Make sure the solution detects and defeats polymorphic spyware, which can reside in numerous places on a system. As spyware creators focus more on getting around anti-spyware tools, more sophisticated detection and removal techniques are required. It is inadequate to check just the Windows registry keys, the Windows system directories, or the desktop for spyware. Anti-spyware products need to scan the entire system to thoroughly protect users from spyware.

WHAT TYPES OF SPYWARE SCANNING TECHNIQUES DOES THE APPLICATION EMPLOY?
It is important for an anti-spyware solution to provide fast and accurate detection. Some products seem fast; however, they may identify spyware simply by filenames. To efficiently minimize false positives and properly test suspect files, expansive detection techniques must be employed. These include MD5 checksum matching, file and folder name searching, registry key scanning, and monitoring an extensive list of known spyware intrusion points on a system, such as changes made to the startup group, new BHOs, or layered service providers (LSPs) inserted in the network stack.

HOW OFTEN DOES THE PROVIDER UPDATE ITS SPYWARE DEFINITIONS?
Spyware definitions should be delivered frequently and on a timely basis. Spyware is continually evolving with frequent new releases. Your anti-spyware vendor needs to be committed to prompt releases to address new spyware threats.
required for a robust anti-spyware solution.) Real-time protection intercepts known spyware before it is installed, actively protecting against spyware, reducing the risk of compromise of confidential information, instead of relying on a manual scanning-and-cleaning process.

DOES THE ANTI-SPYWARE SOLUTION REQUIRE ANY INTERVENTION ON THE PART OF THE END USER OR AFFECT HIS OR HER PRODUCTIVITY IN ANY WAY?
A best-in-class anti-spyware solution will be transparent or have a minimal impact on the end user. A user-centric anti-spyware solution will dynamically manage scan-engine CPU utilization, ensuring that owners’ use of the PC is granted priority over disk-scanning activities.

WITH A CENTRALLY MANAGED ANTI-SPYWARE SOLUTION, CAN MEMBERS OF THE IT DEPARTMENT LOG ON TO ANY PC ON THE NETWORK AND CHECK THE STATUS OF SPYWARE SCANS OR ACTIVITIES?
IT staffers, especially in large organizations, frequently are responsible for systems in geographically diverse locations and often use someone else’s PC to service a computer. A dedicated anti-spyware console that can be operated from only a single machine is unproductive and inconvenient. Your anti-spyware solution should support the roaming nature of IT departments, providing IT staff with the ability to manage spyware defenses and settings via a Web-based console, accessible from any desktop in the organization.

CONCLUSION
Remember, by eliminating the “how many” types of questions and honing in on the “what types of …” and “how do you …” questions, you will obtain more useful information, which will help you select the anti-spyware solution that meets the needs of your organization. The best solutions will not impair the productivity of your employees or network, while protecting your organization from the many costs associated with spyware.