Zone Labs
Integrity

Enterprise Endpoint
Security

// Trusted Zone //

How to Stop Spyware

A White Paper Presented
by Zone Labs

> **"Spyware authors are always looking for new, better-hidden places in the system to anchor themselves."**
>
> *-Spybot creator Patrick Kolla*

There used to a be a time when Spyware was nothing more than a passing nuisance to IT decision-makers. No one paid much attention to a few unauthorized desktop additions that provided a slight boost to employee morale. However, Spyware has been known to consume up to 37% of a typical enterprise network's bandwidth. More often than not this becomes a formidable resource allocation issue and can also lead to overhead in desktop troubleshooting.

In an age of lightening-speed technological innovation, Spyware has become a potent threat, using subterfuge, social engineering and cutting edge techniques to infiltrate enterprise networks by way of third party applications. According to a recent article in Information Security magazine, the number of remote control software tools in the wild, which includes both Trojan horses and spyware, has climbed from 2,944 in the year 2000 to 4,519 thus far in 2003. The end result is open doors leading to potential theft of corporate data and exposure to a wide array of vulnerabilities.

What makes Spyware so dangerous is its ability to transmit data from a host to the Internet. That amounts to each Spyware infected machine acting as a server on your enterprise network to the outside world. Data sent off the machine is encrypted and can potentially be anything garnered from the system, including e-mail, other confidential documents and even keystroke logs. Once Spyware embeds itself, neither end users or any egress filters IT administrators may have on their network can control unauthorized data being sent. What's worse, Spyware has the ability to install additional software onto a host without consent. There are typically no opt-out capabilities. Thus is the insidious and sophisticated nature of today's Spyware.

Spyware is Evasive

Just about any software download from the Internet has the potential to be bundled with Spyware. Typically, it is unclear who is responsible for deploying the Spyware or what they do with your information once it is collected. This practice amounts to significant unauthorized network activity going on behind the back of IT departments.

Spyware gains access to a system through habitual every day tools such as web browsers. "Drive by" downloads via HTTP ActiveX is a common method of infiltration as is instant messaging, streaming audio and video and a variety of third party programs that may or not be considered legitimate business applications. In addition, even if users are not utilizing programs such as peer to peer file sharing and other freeware, just by installing the programs, your network is put at risk. Users are typically unaware of the dangers of installing such programs.

Typical security technologies cannot counter Spyware:

- Antivirus solutions typically don't include signatures for even well-known Spyware since it is not regarded to be in the same class as viruses and worms.
- Spyware removal tools are not a complete solution because they can not be centrally managed, leaving it up to the des top support staff to ensure that each workstation has up to date signatures.

- Perimeter firewalls are ineffectual against Spyware since the problem originates internal to the network through habitual Internet use.
- Intrusion Detection Systems do not have signatures to detect Spyware activity on a network.
- Adware prevention software are not robust enough to eliminate much more than pop-up ads.

> **"The top two concerns of IT professionals with regard to employee computing behavior are web surfing and software downloads."**
>
> *– Emerging Internet Threats Survey 2003*

Once on a system, Spyware behaves similar to worms, vulnerabilities and exploits published in the wild, opening up entry points for other forms of vulnerabilities such as exposing network shares. Each day dozens of vulnerabilities are published on the Internet, covering a wide range of software, hardware and operating systems. The majority of these published vulnerabilities are intended for the vendor to fix a security problem. However, more often than not, security vulnerabilities are used by those with malicious or surreptitious intent as a means to bypass enterprise as well as home networks. In fact, Spyware is equally as dangerous as the exploits and vulnerabilities because they incorporate those published techniques into their software as an edge in attempting to defeat security defenses.

Coping with Spyware Problems

It's no surprise that IT departments are hard-pressed to keep pace with end-user machine maintenance as a result of Spyware infestation. The problem of Spyware often goes unnoticed until a problem occurs. Even after workstations are cleaned, problems re-occur due to the embedded and sophisticated nature of today's Spyware which enables it to re-infect computers. The cycle of repeat infections is costly to IT departments in terms of troubleshooting overhead and lost productivity of employees, not to mention the frustration of tracing deeply hidden problems within the operating system.

To combat Spyware proactively requires the ability to flush out Spyware on computers in order to negate unauthorized network traffic that consumes bandwidth and cause troubleshooting headaches.

How to Stop Spyware

The process of detecting and blocking applications that seek to transmit data off of infected machines to the Internet requires a series of steps:

Step One

Deploy a centrally managed endpoint security solution capable of detecting all applications and services utilizing your network. Unless you know what's trafficking on your network, you have no control over it.

Zone Labs Integrity™ is a best-in-class, centrally-managed endpoint security solution that provides robust protection against Spyware. Combining Zone Labs' patented, multi-layered PC firewall technology with efficient, central policy management controls, Integrity enables fast, flexible security deployment and enforcement across the enterprise. Proven in over seven hundred enterprises, Zone Labs Integrity provides the most secure defense for endpoint PCs and enterprise data in today's highly-vulnerable networked environments.

Step Two

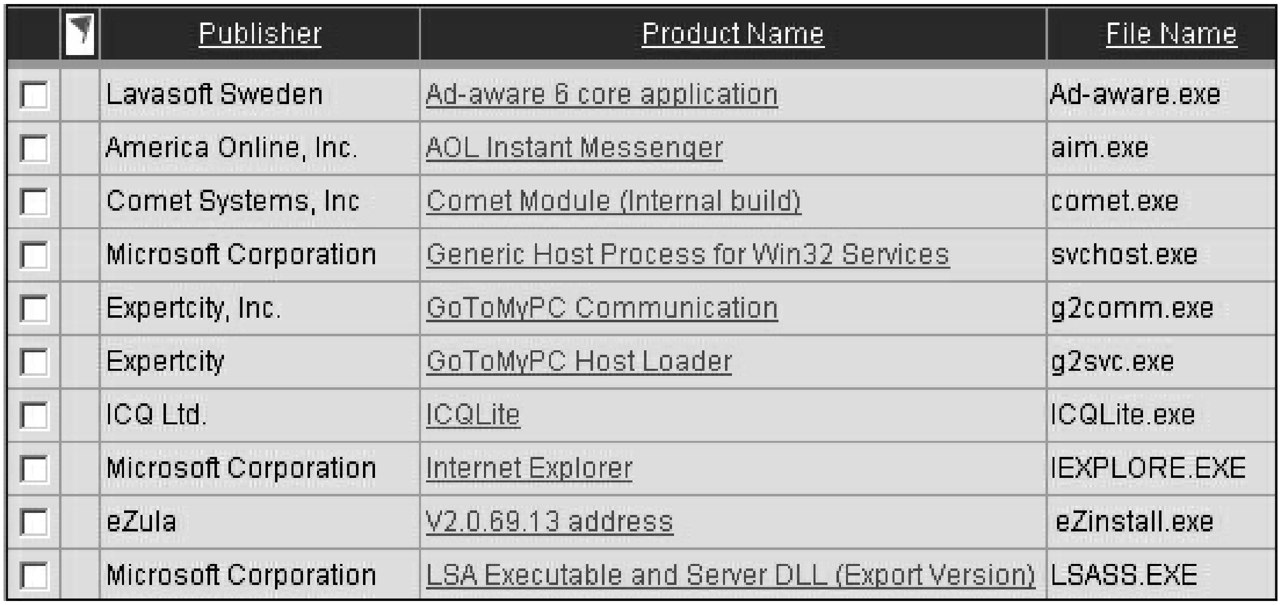
Configure Integrity clients to discover all running applications and services on endpoints that attempt network access. Integrity will then collate them into in a Programs List for Administrators to view and organize.

Step Three

Once programs accessing your network or the Internet are discovered, groups can be established with targeted policies permitting known applications and services of your choosing to have configurable levels of network access. By excluding known Spyware and other undesirable applications from your permissible program groups, you will have taken a giant step forward in defending your enterprise against Spyware. Establishing groups within the Integrity environment is a key to preventing Spyware from propagating and trafficking across your network and also eliminates the need for end-users to make permission decisions on individual applications.

Step Four

Create and deploy an Integrity security policy to your enterprise users. Administrators can configure policies to either display or suppress blocked program alerts so users can co-exist harmoniously with security protection and enforcement on their desktop. Program events are centrally logged so administrators can generate reports to see what programs are attempting access on the network.



		Publisher	Product Name	File Name
□		Lavasoft Sweden	Ad-aware 6 core application	Ad-aware.exe
□		America Online, Inc.	AOL Instant Messenger	aim.exe
□		Comet Systems, Inc	Comet Module (Internal build)	comet.exe
□		Microsoft Corporation	Generic Host Process for Win32 Services	svchost.exe
□		Expertcity, Inc.	GoToMyPC Communication	g2comm.exe
□		Expertcity	GoToMyPC Host Loader	g2svc.exe
□		ICQ Ltd.	ICQLite	ICQLite.exe
□		Microsoft Corporation	Internet Explorer	IEXPLORE.EXE
□		eZula	V2.0.69.13 address	eZinstall.exe
□		Microsoft Corporation	LSA Executable and Server DLL (Export Version)	LSASS.EXE

Figure 1: Integrity Discovered Programs List

Benefits of Using Integrity to Protect Your Enterprise from Spyware

Translating application permission policies and standards into real-world mechanisms requires a next-generation security tool. Zone Labs Integrity™ ensures continuous improvement of security practices by encouraging centralized application monitoring while enforcement takes place in the background, transparent to users so as to not impact their productivity. Establishing and monitoring a consistent desktop security policy across the entire enterprise allows the notion of the weakest link to be drastically minimized. Within the Integrity™ environment, all endpoints are configured in a consistent manner with regard to such attributes as program and network permissions and other common safe usage parameters. This alone makes it more difficult for Spyware to find a niche to remain on your network.

Zone Labs Integrity™ provides centralized manageability advantages that make it the best choice for overall endpoint protection.

- Integrity detects and blocks Spyware so it can be neutralized, preventing conflict with other system resources, preventing consumption of bandwidth on your network and reducing IT staff maintenance overhead for help desk and on-site support.
- Integrity helps organizations discover and counter ongoing Spyware risks by assigning a mitigating policy to users and groups.
- Integrity generates reports, making it simple and time efficient for IT staff to review policy needs.
- Integrity enables organizations achieve better security through creating and maintaining efficient control over des top security policy. This facilitates smoother system upgrades across the enterprise.
- Integrity mitigates additional security risks such as port scanning, Trojan horses and other forms of malware.

Zone Labs Integrity™ operates from the perspective that Spyware proliferation and development in the wild will continue to increase over time. That's why Integrity enables IT staff to create security policies that can be distributed throughout an organization based on known permissible applications, without having to be concerned with ever-increasing strains and variants of Spyware. All unauthorized programs and services are blocked through policy enforcement.

Empowering administrators to centrally monitor applications on the endpoints enables desktop-usage enforcement rules to be sufficiently maintained within an overall corporate network security program.

About Zone Labs

Zone Labs, Inc. is a leading creator of endpoint security solutions that millions of customers trust to protect their PCs from the risk posed by hackers and data theft. Zone Labs' proven technology is deployed by global enterprises, service providers, small business and consumers.

US Headquarters
Zone Labs, Inc.
475 Brannan Street, Suite 300
San Francisco, CA 94107
tel 415.633.4500
fax 415.633.4501

European Headquarters
Zone Labs, GmbH
Düsseldorfer Str. 40a
65760 Eschborn, Germany
tel +49 6196 773 670
fax +49 6196 773 6777