

TippingPoint Spyware Protection Solution Brief

IPS-Secured Networks

SOLUTION BRIEF – Spyware



Spyware is software that monitors user activity on the Internet and transmits that information, which can include e-mails, passwords and credit card numbers, in the background to someone else. Spyware is the third greatest threat to network bandwidth and security after viruses and spam. It is estimated that 67% to 90% of computers connected to the Internet are infected by Spyware according to IDC Research. Spyware exposes an enterprise to liability issues and potentially damaging security risks, and halts overall productivity.

Network-Based Spyware Protection

- Block installation of Spyware
- Prevent infected machines from uploading data to Spyware servers
- Detect infected hosts (installed on machines prior to IPS deployment)

"TippingPoint stops spyware from being installed, blocking several hundred spyware attacks each day. What's great about it is that it also blocks outgoing traffic attempting to reach the spyware data collection sites. That means if the spyware got on a laptop while the laptop was at someone's home or at a hotel while the person was on travel, TippingPoint still stops the data from leaving our organization."

Wellstar Health System

How Big is the Spyware Problem?

Spyware presents a number of risks to the organization including:

- End user productivity declines
- IT productivity declines
- Consumption of system and network resources
- Compromised confidentiality and or exposure of trade secrets
- Introduction of secondary vulnerabilities into the network
- Violation of regulatory compliance

Surfing the Web from universities, offices and homes has become more dangerous and annoying due to pop-up ads that display without warning. In turn, these pop-up ads may contain and install Spyware. Spyware often acts as malicious code and secretly gathers information from your computer or network. Frustrating for many IT personnel, Spyware removal is extremely difficult. Using Spyware, attackers can steal passwords, credit card numbers, login data and workstation details such as commonly used applications and services. The problem is so severe that it has moved the U.S government to pass the Internet Spyware Prevention Act (I-SPY).

Many anti-spyware tools are widely available but often have proven to be ineffective in preventing the spyware problem. Requiring continuous

updating, these tools return numerous false positives, impede desktop functionality, and provide little protection as a single tool against the ever-evolving threats of thousands of attacks and intrusive applications.

TippingPoint Spyware Protection

TippingPoint's protection strategy and "defense-in-depth" approach can prevent attempts to install Spyware. To prevent existing infected systems from contaminating the network, the TippingPoint IPS prevents pop-up advertisements and information transfer to and from the enterprise network. Reports and event tracking in the IPS logs provides information to pinpoint infected systems and isolate and eradicate Spyware infections. With its high bandwidth, low latency, easy to use graphical interface and centralized management options, the TippingPoint IPS can be deployed across various divisions in an enterprise's global offices, with minimum impact to thousands of users, offering non-invasive, real-time, proactive protection.

Types of Spyware

The following types of Spyware infiltrate systems through security holes, Adware, socially engineered offers (plugins, toolbars), browser vulnerabilities, and a range of OS misused features. Each type can lead to further infections or loss of private, critical data.

TippingPoint®

TippingPoint Spyware Protection Solution Brief

Browser Hijackers

Malicious programs that, once installed, change a Web browser's default start, search, bookmarks, and error page settings to alternative sites. Browser redirection inflates the Web sites traffic gaining higher advertising revenues, referral fees, and purchase commissions made through the redirected Web site.

Internet Explorer Toolbars

Programs that install and display as toolbars, search bars, or task buttons incorporated into Internet Explorer through browser plug-ins or browser helper objects (BHO). The toolbars display targeted Web sites, some including further Spyware.

Pop-up Advertisements

Malicious program to display advertisements based on entered Web site URLs, browser history, and specific "keywords" entered through a search engine.

Keyloggers

Applications that monitor a user's keystrokes and then send this information back to the malicious user. There are programs commercially available as a "kit" and it is their use or rather mis-use that makes them notorious. The "phone home" frequency, name of the .exe and other options in the kit make attacks customizable by the hacker and difficult for host based protection to block

due to the variable content. The keylogger can be downloaded unwittingly as spyware and executed as part of a rootkit or remote administration Trojan.

Man-in-the-Middle Proxies

Dangerous software that redirects all Web surfing activity, including secure connections, to a man-in-the-middle proxy. The Spyware can potentially harvest sensitive information such as passwords, credit card numbers, bank account information, health care records, and confidential data.

System Monitors and Dialers

Spyware that captures passwords and sensitive information (credit card and social security numbers), monitor usage, and dial long distance phone calls.

Best-of-Breed Network Protection

TippingPoint's IPS is unique in handling Spyware infiltration and infection. The IPS is a network-based hardware device that detects and filters traffic at multi-gigabit speeds with extremely low latencies and extraordinary accuracy. This network-based purpose-built hardware solution protects at the network perimeter or between network segments. The IPS is non-invasive and blocks Spyware before it reaches the end host, protecting and preventing hundreds of hosts from infection while reducing clean-up time and saving help desk costs.

TippingPoint's IPS devices employ filters to block exploits and vulnerabilities, including specific filters for Spyware threats.

TippingPoint's Digital Vaccine service provides weekly and emergency updates to respond to new threats and vulnerabilities. Every week, TippingPoint researches, compiles, tests, and releases updated filters to guard against any intrusions that seek to capitalize on known vulnerabilities including those in Web browsers and Operating Systems. Network administrators can customize protection by modifying action settings for these filters.

The Local Security Manager (LSM) and Security Management System (SMS) provide extensive and easy-to-use reporting features and centralized alerting and log options to review traffic behavior. With these functions, network administrators can pinpoint infected end hosts to quickly isolate and clean up systems or warn users to adhere to the enterprise's security policies.



Corporate Headquarters:

7501B North Capital of Texas Hwy.
Austin, Texas 78731 USA
+1 512 681 8000
+1 888 TRUE IPS

European Headquarters:

World Trade Centre Amsterdam
Zuidplein 36, H-Toren
1077XV Amsterdam
The Netherlands
+31 20 799 7629

Asia Pacific Headquarters:

30, Cecil Street, #18-01
Prudential Tower
Singapore 049712
+65 6213 5999

TippingPoint[®]

www.tippingpoint.com