Spyware and Adware – Threats and Countermeasures

Finjan White Paper

December 2004

For additional information, please visit www.finjan.com or contact one of our regional offices:

USA

2025 Gateway Place
Suite 180
San Jose, CA 95110
Toll Free: 1 888 FINJAN 8
(1 888 346 5268)
Tel: +1 408 452 9700
Fax: +1 408 452 9701
salesus@finjan.com

420 Lexington Avenue,
24th Floor,
Suite 2400
New York, NY 10170
Toll Free: 1 888 FINJAN 8
(1 888 346 5268)
Tel: +1 408 452 9700
Fax: +1 408 452 9701

Europe

2 Milbanke Court
Milbanke Way
Bracknell, Berkshire
RG12 1RP, UK
Tel: +44 (0) 1344 427127
Fax: +44 (0) 1344 425492
saleseu@finjan.com

Haidgraben 2, 85521
Ottobrun, Germany
Tel: +49 89 673 5970
Fax: +49 89 673 597 50

Asia Pacific

2 Karikal Lane
Singapore
427086
Tel: +65 6741 5289
Fax: +65 6842 1327
salesap@finjan.com

Israel

Hamachshev St. 1,
New Industrial Area
Netanya, Israel 42504
Tel: +972 (0)9 865 9440
Fax: +972 (0)9 865 9441

Email: info@finjan.com
Internet: www.finjan.com

Contents

Introduction 1
What is Spyware/Adware? 1
Infection Methods 2
Spyware and Adware Payloads 3
How Does Spyware Threaten Your Business? 3
Examples of Spyware Detected by Finjan 4
Detected Spyware and Adware 5
Detected Dialers 6
Example of Complex Attack Incorporating Spyware: WebMoney 7
Why Traditional Security Solutions Alone Are No Longer Effective 8
Firewall Is Not the Answer 8
Traditional Anti-Virus Alone Is Not Enough 8
Why URL Categorization on Its Own Is Not the Answer for Spyware 9
The Window-of-Vulnerability™ 9
Finjan's Unique Application-Level Behavior Blocking Solution 10
How Finjan Protects Users Against Spyware 10
Finjan Vital Security™ Solutions 11
Vital Security™ for Enterprises 11
1Box™ for Small and Medium-Sized Businesses 12
Conclusion 12
About Finjan Software 13

Introduction

While less visible to users than spam and virus attacks, spyware and adware constitute a serious threat to enterprises. It is estimated that 30% of enterprise desktops are infected with spyware at any given time. The danger in spyware is that users are not even aware of its existence and the potential damage it may be causing. Secretly installed spyware can subject your company and your employees to invasions of personal privacy, loss of confidential information, performance degradation, network congestion, and reduced productivity.

In a recent report, Gartner characterized spyware as a serious security problem:

> *"Spyware is a critical security threat to corporate systems and data. It has evolved from being an occasional nuisance to something that wastes IT user and technical support resources, and compromises the integrity of corporate systems, applications and data. Although many tools can eradicate the resulting system corruption, most tools are not designed for use in corporate environments. In the near term, IT organizations should deploy multiple tools and plan to exploit emerging anti-spyware technologies from major security vendors."* (Source: Gartner report, September 2004)

Most solutions offered today are reactive in nature (e.g., anti-virus, intrusion detection, intrusion prevention, and anti-spyware software that identify known threats) and as such are powerless against new spyware attacks. Finjan delivers proactive content security solutions based on Application-Level Behavior Blocking technology that protect companies from both known as well as new, unknown spyware attacks driven by active content technologies, such as Java applets, ActiveX controls, Java Scripts, VB Scripts, macros or executable files.

Using its patented Application-Level Behavior Blocking technology, Finjan offers the ONLY gateway-based anti-spyware solution capable of proactively identifying and blocking both unknown and known spyware and other types of malicious code before they enter the network and reach any user's computer.

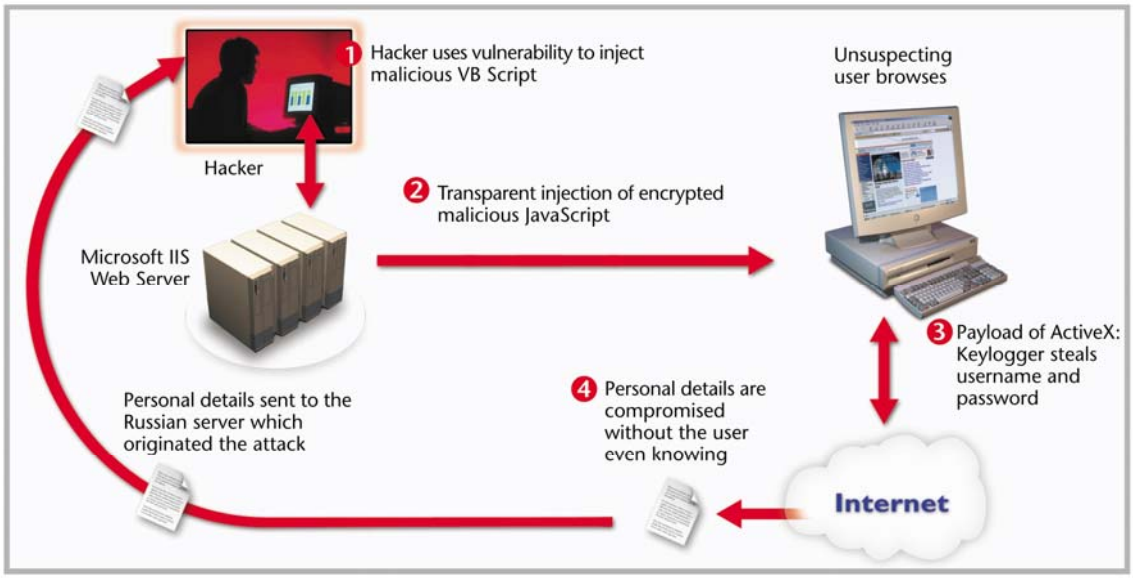
What is Spyware/Adware?

Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, spyware is code that is executed on someone's computer to secretly gather information about the user and relay it to interested parties, often advertisers (hence the term "adware").

Spyware can compromise user names and passwords, send sensitive information to your competitors, open up a back-door to your network, slow down machines and redirect web site access.

The term "spyware" refers to what the code does (its payload) once it infects the victim's computer, rather than how it spreads ("virus"). In this sense, many known viruses, such as Scob and WebMoney, can be considered spyware.

Scob Attack



Scob is an excellent example of a blended or complex attack, which utilizes multiple technologies, stages and angles of attack.

Infection Methods

Exploitation of a Browser Vulnerability

A common method of spyware infection is via the silent installation of a downloader, which exploits a known web browser vulnerability. Once installed, this program can download a wide variety of spyware, including dialers, adware, keyloggers, and programs that capture the Internet history and surfing habits of end-users.

Piggyback Installation

Spyware applications are typically bundled as a hidden component of programs that can be downloaded from the Internet. A common way to become a victim of spyware is to download executable files from common peer-to-peer (P2P) file swapping networks over the Internet. These executable files contain spyware which “piggybacks” on the program being installed without the user even noticing. By connecting users directly, P2P networks bypass normal security barriers, making them easy prey for spyware.

In some instances, spyware/adware will be packaged with “free” programs, requiring the end user to agree to accept the spyware in order to receive the free program. The End User License Agreement informs users of these actions, but most users overlook or choose to disregard this information.

Silent “Drive-by” Download

Today’s spyware no longer requires user “cooperation”, such as opening an email attachment, clicking on a link, or accepting an ActiveX control. Silent “drive-by” downloads, activated by simply visiting a website or reading email via your web browser (e.g., Hotmail), are becoming more prevalent. In such cases, infection is achieved without end user

awareness. In addition, spyware can be installed as a result of clicking an option in a deceptive popup window. **The web has become one of the main "channels" for companies and their users to get infected by spyware.**

Adware

Adware is an application that displays advertisement banners while it is being run. These banners are usually viewed through pop-up windows or through a bar that appears on the screen. Adware can usually be considered spyware, because it almost invariably includes components for tracking and reporting user information. Similar to spyware, adware is sometimes installed without the user's consent or by employing methods that fool the user into thinking he/she is downloading advertisement-free software.

Spyware and Adware Payloads

Spyware/adware may appear in a variety of shapes and forms. Common spyware and adware payloads include:

- Utilities that disconnect the active connection to the Internet, install their own dialing software and use it to go online by dialing one or more highly charged international phone numbers. The entire process is usually performed in a very short period of time, and is often unnoticeable since it gives an illusion of a continuous Internet connection. Utilities of this kind are called "Sex Dialers" since most of them are associated with pay porn sites.

- Utilities that covertly gather personal information and then send it to their "home base", which is one or more web servers on the Internet. Most often, these sites gather data that help create a personal profile on each potential customer. Data of this kind can be the user's browsing history, list of favorite sites, and even the log of keystrokes made while browsing.

- Utilities that unwillingly set the default home page of the browser to a commercial site. These utilities are called "homepage hijackers".

- Browser add-ons, used to display commercial messages. Some of them have a useful functionality as well, e.g., browser search bars.

- Utilities that forcibly open popup windows, which contain advertisements.

Furthermore, spyware can be part of a blended attack that also includes some form of malicious code. Such an attack can deliver spyware that compromises personal details and slows down computer performance, while also delivering more destructive malicious code to infect the computer and destroy files.

How Does Spyware Threaten Your Business?

The vast majority of the world's computers are infected with spyware/adware, resulting in a productivity loss of about $17 per computer in 2004 (Source: mi2g). Based on a survey conducted by McAfee of over 14 million customers, the monthly number of spyware detections rose from 1.5 million to 14.3 million between August 2003 and March 2004. A recent survey by the National Cyber Security Alliance found that nearly 90 percent of all personal computers could be infected with at least one form of spyware.

Spyware producers and distributors are driven by large financial incentives, coming from advertisers and organized crime. The information collected by spyware, such as personal details and market research, as well as the advertisements it distributes, carry significant commercial value and its perpetrators reap noteworthy sums. The huge growth in spyware over the last year is a direct result of the potential financial gain, together with the increasing skills and sophistication of spyware hackers.

Spyware is a serious threat to your company, both due to the potential damage and risks it poses, and to the fact that your computers may already be infected without you even knowing it. Nearly 92% of enterprises acknowledge a serious spyware problem, while estimated infection rates for enterprise desktops is 30% (Web@Work, 2004). This means that if your company does not have effective spyware protection, your corporate systems and data may already be exposed to extensive security, privacy, legal and productivity risks.

Spyware results in a computing resource/bandwidth drain for the company. Complaints from employees about slow computers, program crashes or slow network connections are often an indicator that spyware has infiltrated your network. The presence of spyware consumes valuable CPU or networking bandwidth by downloading information to its “home” site. An additional problem is the increased cost for help desk personnel, who are tasked with cleaning up spyware and its destructive aftermath. The effort required to get your network back up and running after such an attack is both time-consuming and costly, not to mention the amount of business you may lose while your network is down.

The vast majority of enterprises maintain on their internal networks confidential and sensitive information, both regarding their own business and their customers. This information can be compromised using spyware. Imagine the consequences of product design documents or internal price lists falling into the hands of your competitors. In some cases, firms could be held liable for disclosing private information (e.g., medical records). The potential damage to businesses’ customers from leaked account information could be devastating.

Examples of Spyware Detected by Finjan

Finjan continuously monitors the growth and sophistication of spyware, on customer sites as well as in its research laboratories.

During 2004, Finjan conducted several security audits for large enterprises. The purpose of these active content audits was to evaluate the security risk to the organization from providing Internet Web Browsing access to its employees with its existing Internet access infrastructure and security policies.

It should be noted that Finjan’s audits were based on the analysis of content that **had already passed through each organization’s anti-virus (AV) and firewall solutions. No malicious content or spyware was detected by these existing systems**.

Among several viruses and other findings, these security audits discovered multiple spyware/adware applications as well as numerous Internet dialers.

Important to note: one of these audits exposed a malicious dialer that has not yet been identified or recognized by any security company, as well as another different dialer which was not known at the time of the test, and was first announced by AV companies several weeks after the audit took place. These are examples of the value of the proactive protection

that Finjan's products provide **– the malicious code was identified by Finjan before it was either recognized or any patch was issued by an anti-virus company.**

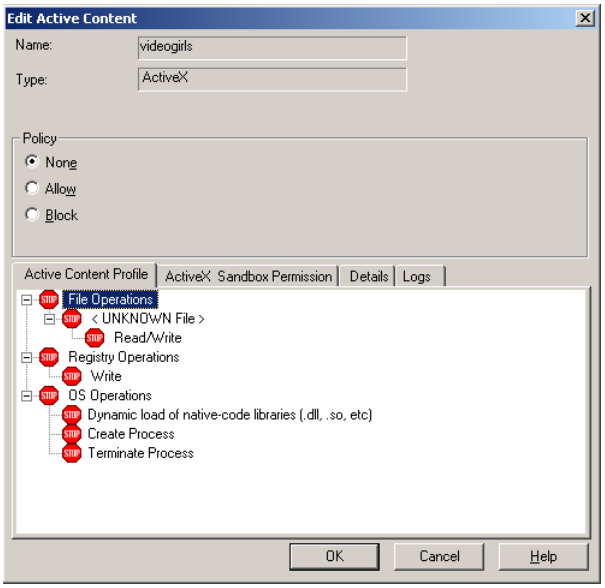
Detected Spyware and Adware

Brief descriptions of the detected spyware and adware appear below. Some screen captures showing violations of the security policy defined in the audit process are presented as they appear in Finjan's security console.

- **AdClicker-BA** - a JavaScript vulnerability activated by a click on an advertisement banner was exploited to silently download and install a Trojan.

- **Adware-Savenow** - an Adware program used to display advertisements in the form of borderless popup windows on top of the browser. Its installer is a "piggyback" rider which is attached to legitimate installation packages.

- **Videogirls** - this is an ActiveX control associated with porn sites.



This ActiveX control communicates via the Internet. As we can see here, this control performs some operations that concern the file system and the registry. It also loads other libraries. By performing these operations, a similar ActiveX control could have complete control of a remote machine.

- **Hotbar** – this is a well-known Spyware application that appends personalized toolbars with built-in keyword-targeted advertisements to Internet applications. It monitors surfing habits and reports back to hotbar.com servers.

Detected Dialers

A dialer is a spyware application which silently dials one of several ISPs to download a hostile executable. The following dialers were detected in this audit:

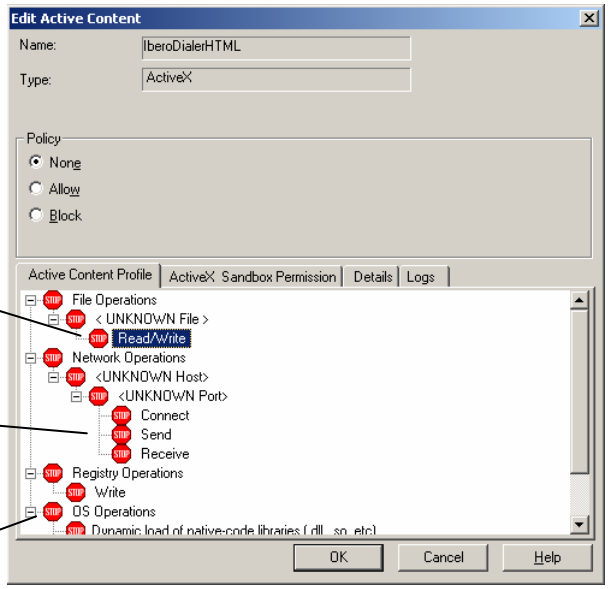
- **Unnamed (probably not yet known) dialer -** A dialer application not yet identified or recognized by any security company (and hence not named yet) was identified in the audit process.
- **QLowZones-5 -** QLowZones-5 is a sex-dialer dropper Trojan. The initial installer consists of a small footprint executable whose size is 15KB.

  At the time of the audit process, no signature-based anti-virus had identified this threat yet. This dialer was first identified and recognized by major Anti-Virus companies 21 days after its detection by Finjan.

  The time it took the AV vendors to identify this virus, plus the time until each enterprise installs the AV upgrade, is a clear demonstration of the Window-of-Vulnerability™, during which enterprises are exposed to attack. Further details of the Window-of-Vulnerability™ are provided later in this document.

The following additional dialers were also detected:

- Dialer-gen
- Dialler-192
- Downloader-JH
- Dialer.DA
- IberoDialerHTML



Accesses the local file system for read and write operations

Opens connections for transmission of data over the network

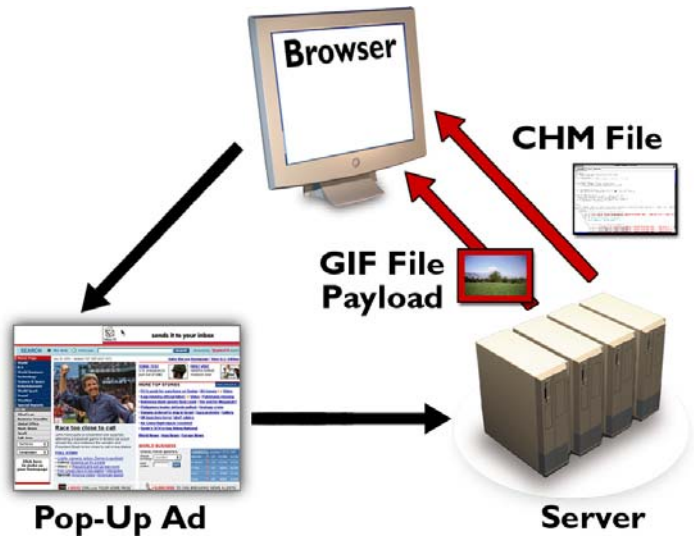
Performs registry-related operations

While not malicious, this ActiveX control is a vivid demonstration of software that might inflict substantial damage to the end user's machine. This ActiveX control updates system files, registry settings, invokes other libraries and executables and communicates via the Internet.

Example of Complex Attack Incorporating Spyware: WebMoney

As the spyware phenomenon evolves, more virus-related propagation techniques are being used by spyware developers. Several of the viruses published by anti-virus companies in 2004 served as vehicles for spyware-like activity. For example, “WebMoney” began to appear in July 2004. It is a Trojan that carries out a multi-stage complex attack. It does not require any human interaction to spread, making it much more dangerous and complex than worms in the past. WebMoney is used to capture private financial information of the user when the user accesses specific secured (HTTPS) financial websites.

As illustrated below, a user innocently browsing the web receives a pop-up ad that leads to the compromised website. The HTML web page that the user is redirected to uses a known Internet Explorer vulnerability to load and execute a .CHM file (an HTML help-file). The HTML web page also downloads a fake GIF file to the desktop, which is used to disguise two bound executable files. The Help file unpacks the fake GIF, which waits for the user to connect to any one of a pre-defined list of financial websites that use SSL encryption. As soon as the user connects to one of these sites, the Help file uses keylogging to capture the user’s personal information.



Webmoney Attack

Finjan’s customers are proactively protected against complex attacks utilizing spyware and other malware technologies. Finjan’s Application-Level Behavior Blocking technology detected the malicious characteristics of these attacks, such as Webmoney, without the need for any patches or new data files. **This was achieved because the proactive behavior-based capabilities of our products defend against both known and unknown (yet to be released) attacks.** Finjan’s Malicious Code Research Center is an industry leader in the detection of dangerous vulnerabilities that could be exploited for Internet and email attacks, helping to protect our customers from today’s and tomorrow’s threats.

Why Traditional Security Solutions Alone Are No Longer Effective

Traditional security solutions were built in the 1990's to safeguard against email attachments and less sophisticated threats than those delivered via active content. Today's malware attacks, such as spyware, take advantage of vulnerabilities in web browsers, which offer greater opportunities for malicious/inappropriate behavior.

The traditional solutions are reactive in nature and thus are not sufficient for combating blended threats, such as Webmoney and Scob, which utilize multiple technologies, stages and angles of attack.

Furthermore, packet inspection products, such as IDS and IPS, operate at the network level and look for patterns at the packet level associated with various attacks. **Spyware, however, is an application-level threat**. Packet inspection products cannot "understand" how a given web page will behave when loaded into a browser, because they never "see" the web page -- they only see individual packets. Packet level solutions have difficulty in identifying complex attacks (particularly ones they have never encountered before), since they are not able to collate information from various sources and understand the overall behavior. Only at the application level (e.g., browser, email application) is it possible to understand the full context of the eventual execution environment and determine accurately what the real behavior is going to be. Spyware attacks underline the need for Application-Level Behavior Blocking solutions.

Firewall Is Not the Answer

Firewalls are capable of protecting networks against packet level attacks but may not detect malware or malicious content entering the network via web traffic, and cannot understand how the content will behave as a whole (at the application level) once it reaches the end user.

While firewalls may still be very useful for intrusion prevention and remote access control, they are no longer efficient for preventing today's malicious code. Blended threats may bypass firewalls, using open ports in the firewall. A system administrator can either block or allow a certain port, but cannot inspect the content allowed to pass through. Needless to say, the system administrator is not aware of the potential behavior of the application bypassing the firewall, including access to system and network resources. The foremost of today's threats enter the network via port 80 (HTTP) and port 443 (HTTPS). In most organizations, opening port 80 is vital to the productivity of the users. Email transportation also opens the door for many complex threats, and the combination of both (web and email transportation) is highly exploited by various risks, as stated earlier.

Traditional Anti-Virus Alone Is Not Enough

Given the proliferation of spyware, anti-virus vendors have begun to add spyware signatures into their scanning engines. While anti-virus software can protect systems against already known spyware, it is reactive in nature and thus incapable of protecting against new, unknown threats. Moreover, recent viruses, such as Mydoom, attack the anti-virus update mechanism, disabling its signature update and increasing the Window-of-Vulnerability™ during which the organization is exposed to attacks.

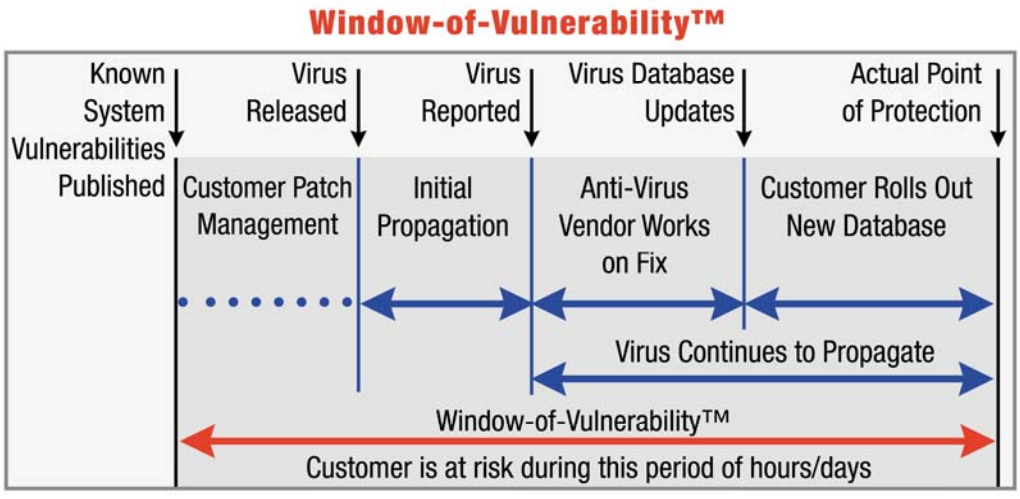
Why URL Categorization on Its Own Is Not the Answer for Spyware

URL Categorization products categorize websites into many different categories and are highly effective for enforcing company policy regarding suitable browsing and keeping high productivity levels by preventing visits to non work-related sites. URL Categorization products categorize websites associated with known spyware (i.e., sites known to infect users with spyware or known to be "phone-home" sites to which known spyware uploads personal information) under categories such as "Spyware" or "Hacking". Requests for URLs that fall into these known categories can therefore be easily blocked.

However, URL Categorization products are not well-suited for blocking new and unknown types of spyware because spyware sites are typically very short-lived in order to avoid detection. This renders URL Categorization solutions less effective. In addition, since this type of "protection" is based on databases of known URLs, it is therefore reactive in nature and cannot block new, unknown spyware, while also being dependent on frequent database updates.

The Window-of-Vulnerability™

The Window-of-Vulnerability™ is the time span from when either a new vulnerability is published or an Internet attack is launched until a signature update or patch to combat that virus is delivered. Even once the patch is issued, studies show that only about 50% of enterprise systems will actually be patched within a period of 21-60 days. Thus, it is hardly surprising that companies without proactive protection against new, unknown attacks are exposed to losses of millions of dollars a year. Enterprises require solutions that close this Window-of-Vulnerability™ through behavior analysis and proactive blocking of malicious and/or inappropriate content (Viruses, worms, Trojan horses, spyware, phishing) the first time it strikes, allowing them to conduct their business safely and without interruption.



Whereas anti-virus companies can only begin to work on an update once the virus has been reported, Finjan's Application-Level Behavior Blocking technology can protect against vulnerabilities from the moment they are published (and in many cases even before they are published). This means that our customers are protected against malicious content throughout the entire Window-of-Vulnerability™.

Finjan's Unique Application-Level Behavior Blocking Solution

Finjan's **Vital Security™ Series**, including the **1Box™ Series** of appliances for small and medium-sized businesses, close the Window-of-Vulnerability™ using patented Application-Level Behavior Blocking technology that protects companies from new, unknown attacks driven by Active Content. Finjan's unique solutions leverage this technology to analyze content, determine the type of behavior and proactively block malicious or inappropriate content, while allowing appropriate content to flow in a transparent manner.

Finjan's Application-Level Behavior Blocking technology determines the full set of behaviors that a given piece of content will exhibit when loaded into the target application, e.g. a web browser or email program. Then, in accordance with each organization's specific security policy, Finjan's system decides whether to pass, block or neutralize the content, ensuring no inappropriate or malicious content can enter the network.

Finjan's scanning technologies inspect the application level traffic that might carry the spyware or malicious mobile code which can infect the computers, and analyzes the behavior of the code itself - **before** it even begins to run on the target computer. Finjan's Application-Level Behavior Blocking technology identifies the combinations of operations, parameters, script manipulations and other exploiting techniques, and can determine that a piece of mobile code is trying to exploit one or more types of vulnerabilities.

Unlike packet-level security solutions, such as IDS and IPS, Finjan's approach is particularly effective at the Application-Level against blended and complex attacks, which use a combination of different technologies and methods, typically exhibiting a mix of virus, worm, and Trojan horse characteristics.. Finjan's products were designed and architected to understand the full context of the eventual execution environment, and handle such situations as a matter of course.

How Finjan Protects Users Against Spyware

Finjan's Application-Level Behavior Blocking technology is extremely effective for fighting spyware. Integrating this technology with best-of-breed anti-virus, URL filtering and anti-spam engines, Finjan offers the world's best and most comprehensive security solution for web and email traffic that provide enterprise and SMB users with superior protection against spyware and other malicious attacks, **without compromising user productivity or performance**.

Finjan's security approach is to provide multiple lines of defense **at the gateway and the desktop**, where each line employs different tools and technologies, in order to detect and block active content that does not adhere to pre-configured security policies.

Lines of defense at the corporate network include:

- At the corporate gateway – the only solution capable of proactively blocking malicious code with Application-Level Behavior Blocking, including blended threats; filtering based on the hash code of known blended threats; and filtering by origin (source URL) and by digital code signatures.
- At the user's desktop - detection of start/stop events of active content objects in the system; runtime monitoring of active content object activities at the operating system

level; runtime monitoring of Java Applets at the Java Virtual Machine level; ability to control (kill) running active content objects; and filtering based on active content hash code and URL.

The following specific features in Finjan's products are used to combat spyware effectively:

- **Block downloads, silent installations and automatic launch** of malicious mobile code (via VB Script, JavaScript, ActiveX, HTML extensions, etc.) that are made during web browsing.
- **Block access of spyware to local information**, files, user details, registry and other local resources. This prevents spyware from being able to collect personal information.
- **Block access of spyware to remote computers and servers**. This prevents spyware from sending back "spied" information obtained from the infected computer.
- The combination of the above allows Finjan's solution to proactively prevent inadvertent installation of spyware and also prevent pre-installed spyware from collecting information and sending it back to its home base. Thus, Finjan's solution is capable of stopping activities performed by unknown spyware that existing Anti-Spyware solutions do not yet recognize.
- **Detect web accesses made by installed spyware** utilities by identifying the "home base" servers they contact. Access to these sites is blocked using an integrated best-of-breed URL Filtering engine (SurfControl or SmartFilter).
- **Scan all content for known spyware signatures** using an integrated third-party Anti-Virus. Finjan offers both Sophos and McAfee as best-of-breed Anti-Virus solutions. Given the proliferation of spyware, these vendors have begun to add spyware signatures into their scanning engines.
- Spyware attacks that use SSL-encrypted content are invisible to most standard gateway scanning applications. Finjan's products **decrypt the SSL-encrypted content** so that it can be scanned for malicious behavior by our web scanning applications.
- Many users are not familiar with browser warnings about problematic certificates or certificate violations and can be fooled into a phishing attack. Finjan's **Vital Security™ for SSL** for enterprises and **SSL 1Box™** for SMBs protect against spyware attacks that use invalid, revoked or otherwise problematic certificates by enforcing your organization's certificate policies at the gateway.

Unlike common clean-up tools, Finjan's solution prevents spyware from arriving in the first place. Finjan's solution does not require a list of known spyware because it identifies spyware by its behavior. Clean-up tools detect and clean known spyware at the desktop, but lack centralized management capabilities and require significant deployment and management efforts by the enterprise. Finjan's centrally managed solution is deployed at the enterprise gateway, facilitating installation and easing management.

Finjan Vital Security™ Solutions

Finjan offers a wide range of solutions via ready-to-use appliances, as well as software packages:

Vital Security™ for Enterprises

- **Vital Security™ Appliance 5100** delivers a comprehensive and scalable security solution for web traffic, meeting enterprises' high performance and zero downtime requirements. Utilizing Finjan's patented Application-Level Behavior Blocking technology together with best-of-breed anti-virus and URL filtering engines, this

solution reduces enterprises' security risks and associated costs. Vital Security™ Appliance 5100 is the ONLY gateway solution capable of proactively blocking spyware and any other malicious attacks from entering your network.

- **Vital Security™ for Web** implements the gateway line of defense for HTTP/FTP traffic. It scans HTML and active content objects at the gateway, away from critical resources, in order to develop a code profile. Active content objects with profiles that do not reconcile with the enforced security policy are not passed to the requesting browser.

- **Vital Security™ for SSL** implements the gateway line of defense for SSL/HTTPS traffic. Vital Security for SSL decrypts SSL traffic and makes it available for malicious code scanning by Vital Security for Web or other third-party software programs. It applies certificate policies at the gateway, preventing users from making security decisions at the desktop.

- **Vital Security™ for E-Mail** implements the gateway line of defense for SMTP, POP3 and Microsoft Exchange traffic and performs the same type of content inspection performed by Vital Security for Web.

- **Vital Security™ for Clients** implements the desktop line of defense. It integrates with the operating system, detecting active content as it begins to run, monitoring it during runtime and enforcing its security policy.

1Box™ for Small and Medium-Sized Businesses

- **Internet 1Box™** is the ultimate security solution for web and email at the gateway and desktop. This easy-to-use product combines Finjan's Application-Level Behavior Blocking technology with best-of-breed anti-virus, URL filtering and anti-spam engines in a single box. Providing enterprise-level security at a price affordable for SMBs, Internet 1Box™ represents a tremendous value for money. Internet 1Box™ is the ONLY solution to effectively combat spyware and other malicious attacks, e.g. phishing, Trojans, worms, and viruses.

- **SSL 1Box™** extends the Internet 1Box™ capability to protect against threats arriving via SSL/HTTPS encrypted content as well as enforcing SSL certificates according to the corporate policies. When implemented together with Internet 1Box™, these products deliver the only solution on the market capable of detecting a new unknown attack arriving via HTTPS/SSL, HTTP and FTP.

- **Documents 1Box™** provides a secure environment for sharing documents within organizations and with partners or customers. Based on pre-defined corporate policies, it protects against unauthorized access, saving, copying, forwarding, printing, or screen-capturing of confidential documents.

Conclusion

The proliferation of spyware, fueled by commercial interests, is already a major concern for enterprises and SMBs. Not only does the presence of spyware hamper your organization's productivity, it may also compromise confidential and private business information.

Due to the ease with which computers can become infected by spyware (often without the user's awareness), businesses require highly intelligent content security solutions which detect any malicious or inappropriate content based on its behavior and block it before it enters their networks and infects their computers. At the same time, this high level of proactive security must be achieved without compromising the productivity or performance of the enterprise's users.

With a field-proven track record, Finjan is the only gateway based Application-Level Behavior Blocking solution on the market capable of **proactively** blocking spyware and all types of malicious code.

About Finjan Software

Finjan Software is the leading provider of proactive, behavior-based secure content management solutions, protecting more than 3 million users from attacks. Finjan uses its Vital Security™ platform to determine actual code behavior and blocks any action that violates predefined security policy, and therefore surpasses the levels of defense typically offered by reactive anti-virus software solutions. This superior technology enables Finjan to protect users proactively by responding to existing, and more importantly, yet to be developed attacks. Finjan's products are currently being used by well-known enterprises with between 1000 to more than 200,000 users. Analyst firm IDC, recognizes Finjan as the leader in the worldwide malicious mobile code security market. For more information, visit http://www.finjan.com.