



***e*nabling *e*businessTM**

- T: +44 (0) 1483-227600
- F: +44 (0) 1483-227700
- E: info@wickhill.co.uk
- W: www.wickhill.com

Wick Hill Ltd. River Court, Albert Drive, Woking, Surrey, GU21 5RP



Spyware and Adware – Threats and Countermeasures

Finjan White Paper

January 2006

THIS DOCUMENT INCLUDES PROPRIETARY AND CONFIDENTIAL INFORMATION OF FINJAN INC.
AND/OR ITS AFFILIATES AND MAY NOT BE USED, CIRCULATED OR QUOTED EXCEPT IN
ACCORDANCE WITH EXPLICIT WRITTEN AUTHORIZATION FROM FINJAN

Contents

| | |
|--|-----------|
| Introduction..... | 1 |
| What is Spyware/Adware?..... | 3 |
| Infection Methods | 3 |
| Spyware and Adware Payloads | 4 |
| How Does Spyware Threaten Your Business?..... | 5 |
| Examples of Spyware Detected by Finjan | 7 |
| Detected Spyware and Adware..... | 8 |
| Detected Dialers | 8 |
| Example of Complex Attack Incorporating Spyware: WebMoney | 9 |
| Why Traditional Security Solutions Alone Are No Longer Effective..... | 10 |
| Firewall Is Not the Answer | 10 |
| Traditional Anti-Virus Alone Is Not Enough | 11 |
| Why URL Categorization on Its Own Is Not the Answer for Spyware | 11 |
| The Window-of-Vulnerability™..... | 11 |
| Finjan’s Unique Behavior-Based Security | 12 |
| How Finjan Protects Corporate Networks from Spyware | 13 |
| Finjan Vital Security™ Solutions | 15 |
| Large Enterprise Solutions | 15 |
| Enterprise Solutions | 15 |
| Small and Medium-sized Business Solutions..... | 16 |
| Conclusion | 16 |
| About Finjan Software | 16 |

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.

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)

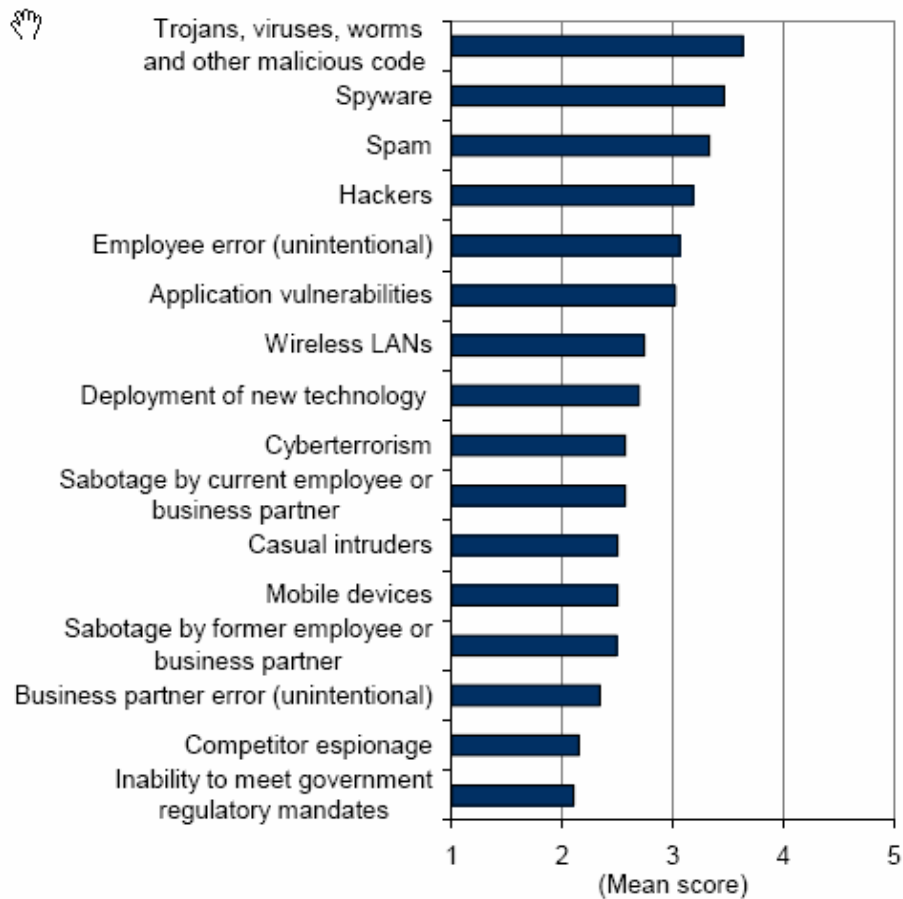
According to IDC, Spyware is perceived as the second most dangerous threat to enterprise security (see graph below):

“Spyware continues to move up the priority list of corporate security concerns. Spyware is now considered to be the second-greatest threat to enterprise network security, according to IDC’s 2005 Enterprise Security Survey. IDC believes more than three-quarters of all corporate machines are infected with various forms of Spyware.”

“Theft of confidential information, loss of employee productivity, consumption of large amounts of bandwidth, damage to corporate desktops, and a spike in the number help desk calls related to Spyware are forcing corporations of all sizes to take action.”

“Financial gain is the number 1 driving force behind the global spam epidemic, the outbreak of “phishing” scams, and the explosive growth of Spyware.” (IDC, Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam and Malicious Code Continue to Wreak Havoc, November 2005)

Threats to Enterprise Security



n = 435

Note: Scores are based on a scale from 1 to 5, with 1 being no threat and 5 being a significant threat.

Source: IDC's Enterprise Security Survey, 2005

Most Anti-Spyware 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, behavior-based web security solutions 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 behavior-based 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?

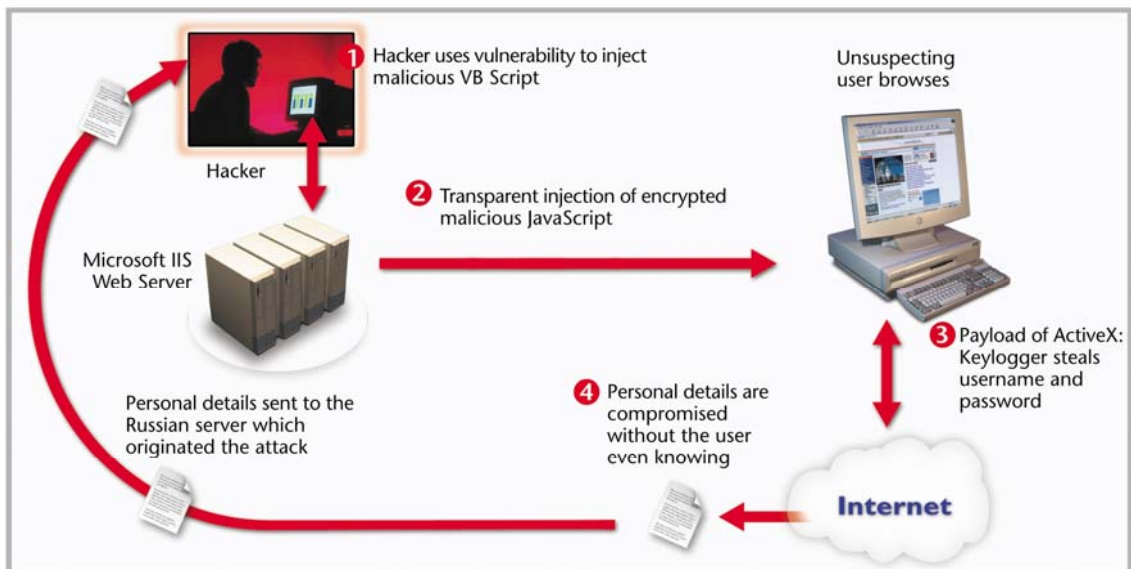
Spyware is any computer program that is designed to gather information from a person's computer (personal or organizational classified information) without his knowledge or consent. Spyware is malicious code that exploits infected computers for commercial gain. This malicious code sometimes takes control over the person's computer, monitors the user's activities or uses the computer for the benefit of 3rd party (advertisers or competitors).

Spyware can reveal 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.

The term "Adware" refers to any software which displays advertisements, with or without the user's approval. Some Adware may also behave like Spyware, such as reporting user's surfing habits to build up marketing profiles.

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.**

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.

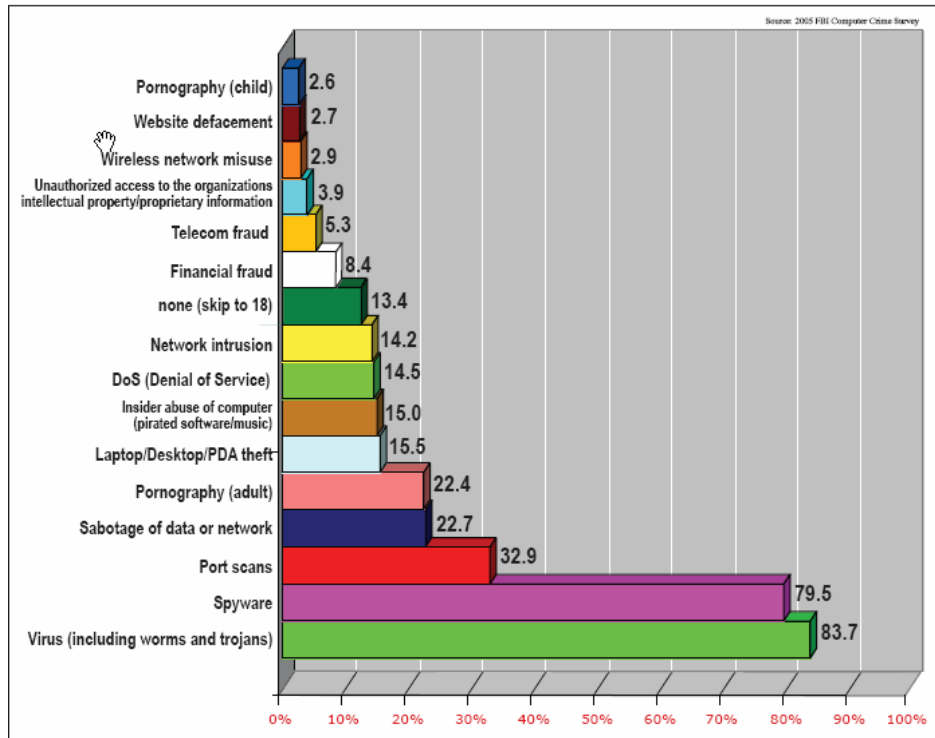
Furthermore, Spyware can be part of a blended attack that also includes some form of malicious code. Such an attack can deliver Spyware that compromises personal details and slows down computer performance, while also delivering more destructive malicious code to infect the computer and destroy files.

How Does Spyware Threaten Your Business?

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. Sophos Labs predicts that quantity of Spyware will increase in 2006 and the threat from Spyware and Adware will continue to grow during 2006. 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.

Consider the following facts:

- Sophos reports that the number of keylogging Trojans has tripled in the first six months of 2005 compared to the first half of 2004.
- IDC estimates that more than 75% of all corporate machines are infected with various forms of Spyware (Source IDC's 2005 Enterprise Security Survey).
- McAfee AVERT research center has reported a 12 percent increase in the number of new potentially unwanted programs (PUP) created in Q2 2005 as compared to Q1 2005.
- The number of new malware threats (i.e., Spyware, virus, worm, and Trojan horse) rose by 48% between January-November 2005 (Sophos Security Threat Management Report 2005). The quantity of reported Spyware as a percentage of total malware rose from 54.2% in January 2005 to 66.4% in November 2005.
- As indicated in the chart below, over 79% of companies surveyed had been affected by Spyware and almost 84% had been affected by a virus attack at least one time within the last 12 months (2005 FBI Computer Crime Survey). These facts speak even louder given the fact that 98.2% of the surveyed companies were protected by Anti-virus software and 90.7% of the companies were protected by Firewall.



Types of Computer Incidents Detected in Last 12 Months

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. 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 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 and 2005, 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 was not identified or recognized for months 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 security solutions 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.

- **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** - an ActiveX control associated with porn sites.
- **Hotbar** - 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 (not known at time of audit) dialer** - A dialer application not yet identified or recognized by any security company (and hence not named) 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.

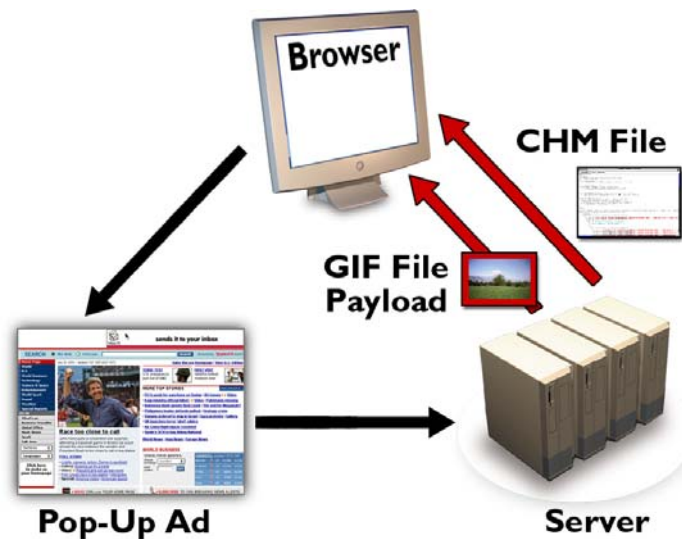
The following additional dialers were also detected:

- Dialer-gen
- Dialler-192
- Downloader-JH
- Dialer.DA
- IberoDialerHTML
- Dialer.Trafficadvance
- Trojan.AdminCash

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 behavior-based security 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 web-borne 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) 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 behavior-based 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.

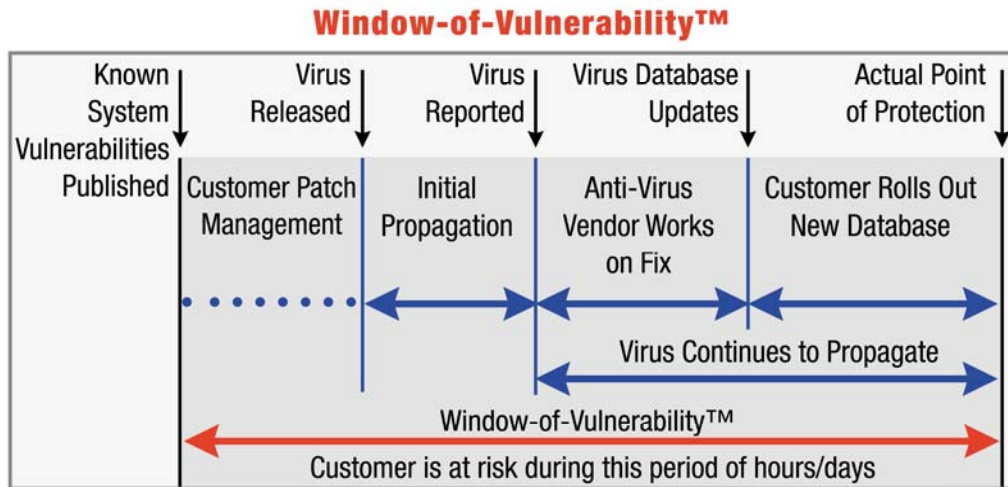
Why URL Categorization on Its Own Is Not the Answer for Spyware

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 attack is launched until a signature update or patch to combat that virus is delivered. Even once the patch is issued, studies show that about one-half of enterprise systems remain unpatched for a period of between 21-60 days. Thus, it is hardly surprising that companies without proactive protection against new, unknown attacks are in danger of compromising their network security and valuable business assets. 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, etc.) 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 behavior-based technologies can provide zero-hour protection 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 Behavior-Based Security

Finjan's **Vital Security™ solutions** close the Window-of-Vulnerability™ using patented behavior-based 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 behavior-based security engine 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. 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 behavior-based 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.

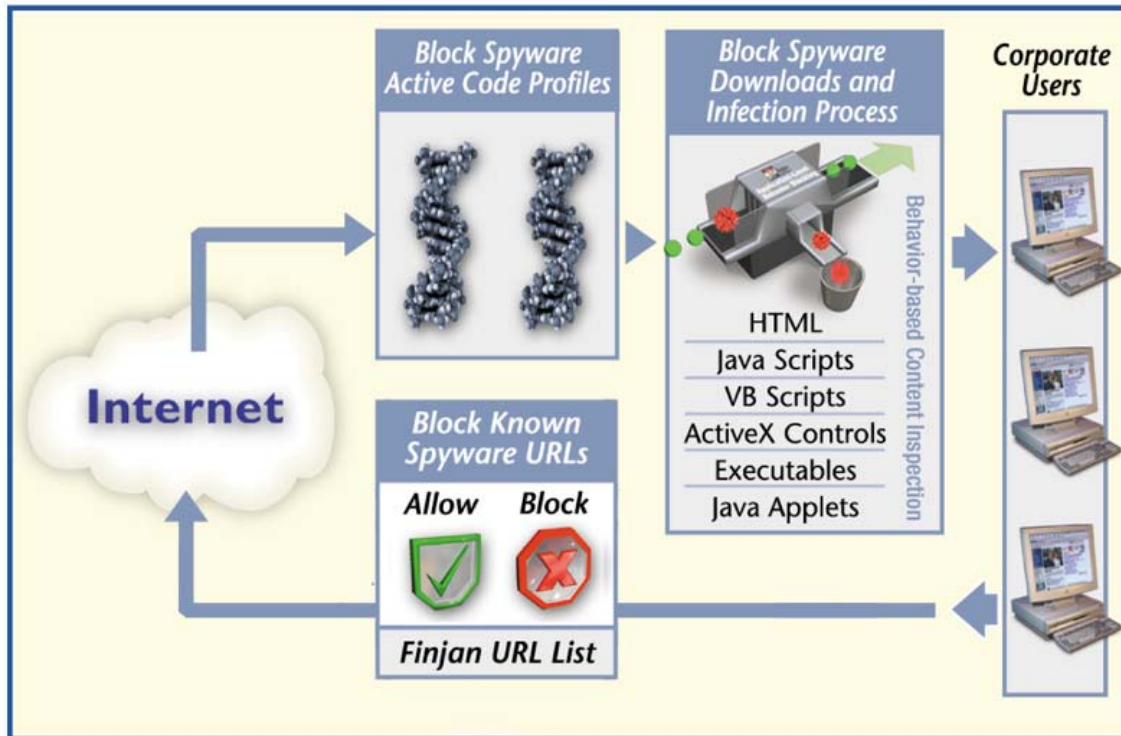
Unlike packet-level security solutions, such as IDS and IPS, Finjan's approach is particularly effective at stopping blended and complex attacks, which use a combination of different technologies and methods, typically exhibiting a mix of virus, worm, and Trojan horse characteristics.. Finjan's products 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 Corporate Networks from Spyware

Finjan's web security solutions proactively detect known and unknown Spyware through multiple methods and block it at the gateway. The Anti-Spyware engine leverages patented behavior-based technology, customized specifically to block Spyware attacks, together with URL blacklists and Active Content behavior profiles. This solution operates at the application-level, providing comprehensive and layered protection against Spyware at the gateway. Granular security policies are provided to block known and unknown Spyware **without compromising user productivity or performance.**

The following specific features in Finjan's Anti-Spyware solution are used to keep Spyware out of corporate networks:

- **Blocks downloads/silent installations/automatic launch** of malicious mobile code (via VB Script, JavaScript, ActiveX, HTML extensions, etc.) performed during web browsing
- **Blocks active content** matching Finjan's extensive list of known Spyware behavior profiles, as generated by our scanning engines
- **Blocks access of Spyware to local information**, files, user details, registry and other local resources to prevent collection of personal information
- **Detects Spyware already on your computer**, blocks it from "calling home" using integrated URL blacklisting and provides identification details for cleanup
- **Blocks access of Spyware (on previously infected machines) to remote computers and servers** to prevent Spyware from sending back "spied" information
- **Detects Spyware attacks that use SSL-encrypted content** which are invisible to most standard gateway scanning applications, when used in conjunction with Vital Security™ Appliance NG-5400
- Protects against Spyware attacks that use invalid, revoked or otherwise problematic certificates by **enforcing your organization's certificate policies at the gateway**, when used in conjunction with Vital Security™ Appliance NG-5400.



Proactive, Multi-Layered Anti-Spyware Protection

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 proactive, behavior-based web security solutions for businesses and organizations. Our proactive, appliance-based solutions deliver zero-hour protection against web-borne threats, freeing enterprises to harness the web for maximum commercial results. Finjan's web security solutions utilize patented **behavior-based technology** to proactively repel all types of threats arriving via the web, such as *Spyware*, *Phishing*, *Trojans* and *other malicious code*, securing businesses against unknown and emerging threats, as well as known malware.



Finjan's Family of Best-of-Breed Web Security Appliances

Large Enterprise Solutions

Vital Security™ Web Appliance NG-8100 is Finjan's proactive web security solution for enterprises/organizations with between 10,001-250,000 users. This solution delivers the world's best web security in a high performance, scalable and high availability integrated blade server appliance. This appliance utilizes Finjan's patented behavior-based technology to proactively secure corporate networks against all types of web-borne attacks, including even new, unknown threats. The fully integrated NG-8100 includes our behavior-based security engine, Vulnerability Anti.dote™, Anti-Spyware and a choice of leading Anti-Virus engines. URL Filtering is also available as an optional module. This solution can be integrated with various Security Load Balancing options to ensure compliance with the high performance and availability requirements of large enterprise networks.

Enterprise Solutions

Vital Security™ Web Appliance NG-5100 is Finjan's proactive web security solution for enterprises/organizations with between 501-10,000 users. This solution utilizes Finjan's patented behavior-based technology to proactively secure corporate networks against all types of web-borne attacks, including even new, unknown threats. Finjan's web security solution enables enterprises to leverage the web for maximum business results, free from security worries. The comprehensive NG-5100 includes our behavior-based security engine, Vulnerability Anti.dote™, Anti-Spyware and a choice of leading Anti-Virus engines. URL Filtering is also available as an optional module. This solution can be integrated with a number of Security Load Balancing options to ensure compliance with the high performance and availability requirements of enterprise networks.

Small and Medium-sized Business Solutions

For businesses with up to 500 users, Finjan offers its Vital Security Web Appliance NG-1100. This best-of-breed, proactive web security solution features Finjan's behavior-based security engine, Vulnerability Anti.dote™, Anti-Spyware and a choice of leading Anti-Virus engines. URL Filtering is also available as an optional module. Specially designed for smaller and medium-sized organizations, this solution delivers the world's best and most comprehensive web security in an all-in-one, easy to install and "self-managing" appliance.

Conclusion

The proliferation of Spyware, fueled by commercial interests, is already a major concern for enterprises networks. 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 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.

An integral part of the comprehensive Vital Security™ Web Appliance, Finjan's Anti-Spyware solution is the only gateway solution capable of blocking known and unknown Spyware before it infiltrates your network.

About Finjan Software

Finjan is a global provider of best-of-breed web security solutions for businesses and organizations, protecting millions of users from known and unknown threats. Finjan uses its patented behavior-based security technologies to determine actual code behavior and block any action that violates an organization's predefined security policy, therefore surpassing the levels of defense offered by reactive and signature-based anti-virus and intrusion detection solutions. This superior technology enables Finjan to proactively repel all types of web-borne attacks, securing businesses against known, unknown and emerging threats. Finjan's security solutions have received industry awards and recognition from leading analysts and publications including IDC, Butler Group, SC Magazine, PCPro, ITWeek, and Information Security. For more information about Finjan and its proactive protection solutions against threats driven by mobile malicious code, please visit: www.finjan.com.