



# Anti-Spyware

## How to Prevent Spyware with Finjan's Active Real-Time Code Inspection

---

### Finjan White Paper

*April 2008*

---

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

© Copyright 1996 - 2008. Finjan Software Inc. and its affiliates and subsidiaries ("Finjan"). All rights reserved.

All text and figures included in this publication are the exclusive property of Finjan and are for your personal and non-commercial use. You may not modify copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, use or sell any part of its content in any way without the express permission in writing from Finjan. Information in this document is subject to change without notice and does not present a commitment or representation on the part of Finjan.

The Finjan technology and/or products and/or software described and/or referenced to in this material are protected by registered and/or pending patents including U.S. Patents No. 6092194, 6154844, 6167520, 6480962, 6209103, 6298446, 6353892, 6804780, 6922693, 6944822, 6993662, 6965968, 7058822, 7076469, 7155743, 7155744, 7185358 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, Vital Security, Vulnerability Anti.dote and Window-of-Vulnerability are trademarks or registered trademarks of Finjan. Sophos is a registered trademark of Sophos plc. McAfee is a registered trademark of McAfee Inc. Kaspersky is a registered trademark of Kaspersky Lab. SurfControl and Websense are registered trademarks of Websense, Inc. IBM Proventia Web Filter technology is a registered trademark of IBM Internet Security Systems. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation. All other trademarks are the trademarks of their respective owners.

For additional information, please visit [www.finjan.com](http://www.finjan.com) or contact one of our regional offices:

<p><b>USA</b> 2025 Gateway Place Suite 180 San Jose, CA 95110, USA Toll Free: 1 888 FINJAN 8 Tel: +1 408 452 9700 Fax: +1 408 452 9701 <a href="mailto:salesna@finjan.com">salesna@finjan.com</a></p>	<p><b>Europe</b> Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 <a href="mailto:salesuk@finjan.com">salesuk@finjan.com</a></p>
<p>Chrysler Building 405 Lexington Avenue, 35th Floor New York, NY 10174, USA Tel: +1 212 681 4410 Fax: +1 212 681 4411 <a href="mailto:salesna@finjan.com">salesna@finjan.com</a></p>	<p>Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 <a href="mailto:salesce@finjan.com">salesce@finjan.com</a></p>
<p><b>Israel/APAC</b> Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 <a href="mailto:salesint@finjan.com">salesint@finjan.com</a></p>	<p>Printerweg 56 3821 AD Amersfoort The Netherlands Tel: +31 33 4543555 Fax: +31 33 4543550 <a href="mailto:salesne@finjan.com">salesne@finjan.com</a></p>

Email: [info@finjan.com](mailto:info@finjan.com)  
Internet: [www.finjan.com](http://www.finjan.com)

## Table of Contents

1. Introduction.....	1
2. Spyware.....	1
3. Finjan’s Anti-Spyware Solution.....	5
4. Conclusion.....	7
5. About Finjan.....	8

## 1. Introduction

Cybercrime is booming and money is the driving force behind the growth of targeted attacks against corporate networks that steal business data that can be sold on to other criminals.

Cybercriminals use the web as a highly effective attack vector for a wide range of illegitimate and malicious activities, including identity theft through keylogging, financial fraud, espionage, and intelligence gathering.

Security vendor reported that 51% of the malicious sites found in the second half of 2007 were legitimate sites that were compromised by attackers. They also point out that these sites pose a significant risk to companies who rely on website reputation to protect their users.

Spyware has evolved from an online nuisance to a dire web threat.

Cybercriminals use Spyware programs to hijack users' sensitive personal information at will for profit. Spyware distributors use evasive techniques to avoid detection.

Spyware presents a problem for corporations. If their employees' machines are not sufficiently protected, Spyware attacks can result in employee login information being compromised, allowing access to an employee's network account and thus accessing confidential and business information.

## 2. Spyware

Spyware is any computer program designed and used by Cybercriminals to gather information from a personal or business computer, without the computer user's knowledge or permission.

Spyware consists of malicious code, designed to obtain data for financial gain.

Cybercriminals use Spyware such as keyboard loggers (or keyloggers) to capture information entered at legitimate websites, such as Internet banking sites.

This type of spyware can be planted on a user's computer using a Trojan infection. Any information the spyware captures is sent to a predetermined computer on the Internet.

Another method of Spyware infection is using silent installation of a downloader, which exploits known web browser vulnerability. Once this program is installed on the targeted computer, it starts to download its Spyware.

Spyware applications are typically bundled into a hidden component of programs that can be downloaded from the Internet. Especially executable files from popular peer-to-peer (P2P) file swapping networks are used by Cybercriminals.

Since users normally connect directly to these P2P networks, normal security barriers are bypassed, making them a prime target for the distribution of Spyware. Spyware distribution is also spread via silent drive-by downloads, that don't need any end user activity.

A classic example of Spyware and its malicious effects is Movieland, also known as Moviepass.tv or Popcorn.net.

Movieland is a movie download service that has been the subject of thousands of consumer complaints. Its repeated pop-up windows (figure 1) and demands for payment (figure 1) made its consumers feel that they were held hostage. Numerous complaints were filed at the Federal Trade Commission (FTC), the Washington State Attorney General's Office and the Better Business Bureau. (The full text can be downloaded in pdf form from the FTC's website at <http://www.ftc.gov>)

The FTC filed a [complaint](#) against Movieland.com and eleven other defendants, charging them with having "*engaged in a nationwide scheme to use deception and coercion to extract payments from consumers.*"

The complaint alleges that the defendants downloaded software that repeatedly opened oversized pop-up windows that could not be closed or minimized, accompanied by music that lasted nearly a minute.

The complaint further alleges that the pop-ups demanded payment of at least \$29.95 to end the pop-up cycle, claiming that consumers had signed up for a three-day free trial but did not cancel their membership before the trial period was over, and were thus obligated to pay.

Movieland's pop-up windows, which display both textual and audiovisual payment demands, significantly disrupt consumers' use of their computers, since once these pop-up payment demands were displayed on a particular computer for the first time, they caused them to redisplay again and again with ever-increasing frequency.



Figure 1– "3 DAY TRIAL EXPIRED" pop-up window with dark background as illustrated in the FTC complaint

The pop-ups have a large dark background and take up much of the screen, blocking access to other windows.

They lack the familiar "X" or "-" symbols to close or minimize, leaving the user with only one option: to click "Continue".

The first pop-up (figure 2) shows the date and time "our content access software was installed on your system and your 3 day free trial began", the text "Click 'Continue' to purchase your license and stop these reminders", and a graphic reading "STOP THESE REMINDERS NOW" and "CLICK CONTINUE". The only option offered is a button labeled "Continue".

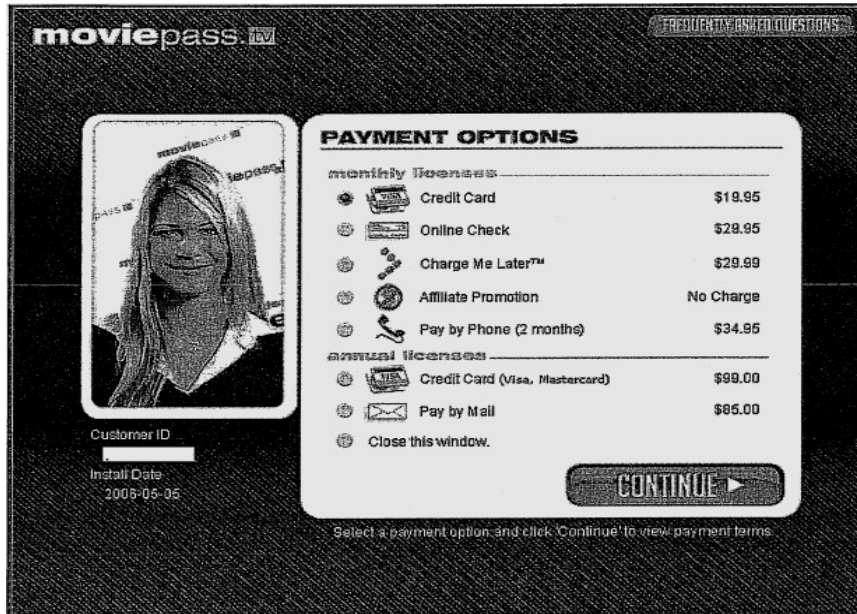


Figure 2 – "PAYMENT OPTIONS" pop-up window as illustrated in the FTC

Clicking "CONTINUE" brings up the next pop-up (figure 3) - an audiovisual file featuring a woman who introduces herself as "your personal customer service representative" and states "Because you did not cancel during your trial period, you are now legally obligated to make your payment as per the terms and conditions you agreed to when you installed our content delivery software."

As the video clip nears its conclusion (approximately 40 seconds after it begins), a dialog box entitled "PAYMENT OPTIONS" appears. Choosing its "Close this window" option closes the pop-ups until the cycle begins again.

It was extremely difficult or impossible for consumers to uninstall the software. Those attempting to remove it through the Windows Control Panel "Add or Remove Programs" function were redirected to a web page telling them that they had to pay the \$29.95 fee to stop the pop-ups. The only way many consumers could regain control of their computers was to pay the fee, or pay a computer technician to remove the software.

Digital Enterprises, which does business as California-based Movieland.com, settled with the FTC in September 2007. As part of the consent agreement, Movieland had to pay more than \$501,000 in consumer redress; had to ban future downloads without consent and had to offer a way to remove the adware.

As this example illustrates, fighting Spyware (and Adware) is not an easy feat. The best option is to prevent Spyware from entering the network by using proactive content inspection technologies.

Finjan's active real-time code inspection analyzes the behavior of applications arriving from the Internet and determines whether they violate the security policy as defined by the network administrator. It therefore provides a highly effective way to detect and block Spyware and Adware at the gateway, before it even has a chance to enter the network and execute on end users' computers.

### 3. Finjan's Anti-Spyware Solution

As shown above, attacks have become more evasive and obfuscated. This poses a challenge for traditional security, since anti-virus, reputation-based services and URL filtering solutions were not designed to handle these threats. Active real-time content inspection protects the networks and vital information assets of organizations around-the-clock.

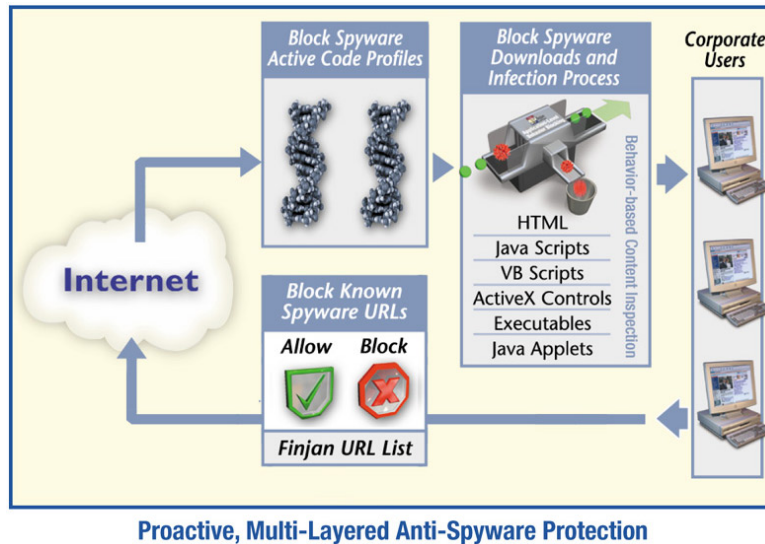
Finjan's Secure Web Gateway products utilize active real-time content inspection to understand the intended criminal behavior of web content. Each and every piece of incoming and outgoing web content in HTTP/HTTPS/FTP is analyzed in real time regardless of its originating URL and without signature matching.

It therefore detects and blocks Spyware (also when hiding in SLL traffic) from entering corporate networks. It thus prevents malicious web content from entering the corporate network, thus protecting enterprises from Spyware that may result in severe business damage.

Finjan's comprehensive and fully integrated Vital Security™ Web Appliances leverage patented active real-time security technologies to achieve the highest level of protection against incoming and outgoing Spyware.

Finjan's Secure Web Gateway products utilize active real-time content inspection to understand the intended criminal behavior of web content. Each and every piece of incoming and outgoing web content in HTTP/HTTPS/FTP is analyzed in real time regardless of its originating URL and without signature matching. It therefore detects and blocks phishing attacks, thus protecting enterprises from any phishing that may result in severe business damage.

Finjan's Anti-Spyware Solution utilizes Finjan's active real-time content inspection technology to provide superior protection against Spyware attacks. It identifies malicious active content and blocks it at the gateway. It therefore provides excellent protection against sophisticated Crimeware attacks, including Spyware.



Features include:

- Proactive real-time content inspection solution that detects and blocks both unknown and known Spyware.
- Comprehensive solution, including Anti-Spyware, Anti-virus and URL filtering.
- Detects and blocks Spyware that tries to exploit known vulnerabilities.
- Detects Spyware attacks that use **SSL-encrypted content** which are invisible to most standard gateway scanning applications.
- Detects and blocks Spyware that tries to access local information, files, user details, registry and other local resources to prevent collection of personal information.
- Detects installed Spyware (on previously infected machines) trying to access the Internet and blocks it from sending back "spied" information to its home site using integrated URL blacklist functionality.
- Protects against Spyware attacks that use invalid, revoked or otherwise problematic certificates by enforcing your organization's certificate policies at the gateway.
- Prohibits access to and downloads from known Spyware sites based on Finjan's URL blacklists.
- If the fraudulent site also contains malicious Web content (such as Crimeware, Spyware, Trojans and other types of malware), such content is detected and blocked by Finjan's active real-time content inspection technology.
- Blocks downloads, silent installations and automatic launch of Spyware (including drive-by downloads) during web browsing.
- Blocks malicious content matching Finjan's extensive list of known Spyware behavior profiles.

## 4. Conclusion

Financial gain is the driving force behind the explosive growth of Crimeware such as Spyware, obfuscated code methods, and targeted attacks. Professional hackers use sophisticated Crimeware to evade signature- and database-reliant security tools. Website content is becoming more and more volatile and domain names can be set up for brief periods of time. As a result, “keeping track” of the malicious content has become extremely difficult. Attempts to pattern malicious code and create signatures, or to categorize known malicious sites, are not enough to sufficiently defend against the wave of dynamic Web threats. It is clear that an additional security layer is needed.

Evasive Crimeware attacks are hard to stop by products designed to prevent employees from visiting known non-productive sites (URL filtering), known malicious sites (reputation services) or downloading known malicious programs (anti-virus). The answer is the use of real-time content inspection techniques. More and more enterprises and organizations are looking at a multi-layered approach, consisting of real-time security and reactive (e.g., signature-based) IT security technologies.

Finjan’s **Vital Security™** with **active real-time code inspection** technology achieves the highest rate of malicious code prevention. Finjan’s secure web gateway solution analyzes each and every piece of incoming and outgoing Web content in real-time, regardless of its original source, and understand its potential effects before it executes itself. By understanding the true intent of Web content, Finjan’s active real-time content inspection technology detects and prevents Crimeware despite the propagation techniques and anti-forensics methods in use. This prevents any malicious Web content from entering or exiting the corporate network, thus protecting enterprises from Crimeware that may result in severe business damage.

## 5. About Finjan

Finjan is a global provider of secure web gateway solutions for the enterprise market. Our real-time, appliance-based web security solutions deliver the most effective shield against Web-borne threats, freeing enterprises to harness the Web for maximum commercial results. Finjan's real-time web security solutions utilize its patented behavior-based technology to repel all types of threats arriving via the Web, such as Crimeware, phishing, trojans, obfuscated codes and other malicious codes, thus securing businesses against unknown and emerging threats, as well as known Crimeware. Finjan's security solutions have received industry awards and recognition from leading analyst houses and publications, including IDC, Butler Group, SC Magazine, eWEEK, CRN, ITPro, PCPro, ITWeek, Network Computing, and Information Security. With Finjan's award-winning and widely used solutions, businesses can focus on implementing Web strategies to realize their full organizational and commercial potential.

For more information about Finjan, please visit [www.finjan.com](http://www.finjan.com).