



REI Stops Spyware Attacks Using Finjan's Proactive Web Security Solution

*Behavior-Based Security Detects Dynamic Web Threats and
Targeted Attacks at the Gateway*

Case Study



November 2006

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

© Copyright 1996 - 2006. Finjan 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 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 is a registered trademark of SurfControl plc. 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 or contact one of our regional offices:

<p>USA 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 salesna@finjan.com</p>	<p>Europe 4th Floor, Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com</p>
<p>Chrysler Building 405 Lexington Avenue, 35th Floor New York, NY 10174, USA Tel: +1 212 681 4410 Fax: +1 212 681 4411 salesna@finjan.com</p>	<p>Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com</p>
<p>Israel/APAC Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 salesint@finjan.com</p>	

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

Contents

Background.....	1
Meeting the Spyware Challenge.....	1
Finjan’s Vital Security™ Web Appliance Solution	1
The Results: Proactive Prevention of Spyware at the Gateway	2
Conclusion	3
About Finjan.....	4

Background

Founded in 1938, REI is the largest consumer cooperative in the US, with over 2.8 million member-owners. REI is a retailer of high end outdoor gear and apparel for climbing, skiing, bicycling, camping and more, with sales in 2005 topping \$1 billion. Originally set up by a group of Pacific Northwest mountaineers, REI has been named to FORTUNE magazine's list of the "Best 100 Companies to Work For" eight consecutive years.

With over 8,000 employees and business operations distributed over 80 retail outlets nationwide and two online stores, REI devotes substantial resources to ensuring the efficiency and security of its network infrastructure, which is critical to the success of its ongoing business operations.

Meeting the Spyware Challenge

Aware of the potential damage Spyware could cause to its business operations due to network downtime, performance degradation and reduced productivity, REI sought a proactive web security solution that blocks these types of threats before they infiltrate end-user PCs. Since web-based threats enter network firewalls through port 80 (the same port used for web browsing and other web-based applications), REI required the ability to differentiate between legitimate and malicious/inappropriate content. In other words, it needed a solution that blocks Spyware and other malicious content, while at the same time enabling web-enabled business activities.

REI understood that while traditional, signature-based solutions are effective against known viruses and malware, these types of solutions are not sufficient for detecting unknown malware and stealthy Spyware attacks. Moreover, as hackers are familiar with the workings of traditional security systems such as firewalls, anti-virus and IDS/IPS products, they are crafting malicious code and targeted attacks to "outsmart" such systems.

To meet its needs for a proven and intelligent web security solution that would protect its network from Spyware and other potential web-based threats, REI chose Finjan's Vital Security™ Web Appliance.

Finjan's Vital Security™ Web Appliance Solution

Finjan's Vital Security™ Web Appliance features patented behavior-based technology to proactively detect and block all types of malicious web threats at the Internet gateway. This unique solution scans all incoming and outgoing web traffic, proactively blocking Spyware and other web-based attacks in real-time, enabling REI's users to continue to conduct business safely and without interruption.

Finjan's solution includes dedicated anti-spyware functionality, which blocks downloads, silent installations and automatic launch of Spyware (including drive-by installations) performed during web browsing. It prohibits access to known Spyware sites as well as preventing Spyware already installed on end-users' workstations from "calling home" to Spyware websites. During the first three months of live operations, Finjan's solution detected and blocked over 2100 attempts per day to access Spyware sites and download Spyware objects. **"Finjan's behavior-based technology is unique in its ability to analyze web content at the gateway and determine its behavior before it begins to run on users' computers. This provides us with the best possible protection against Spyware and other malicious web threats,"** stated Brad Brown, REI Vice President of Information Services.

Finjan's solution gave REI full control over content entering and leaving its network via the web. Using a centralized management console, REI's administrators can create and set granular security policies per user groups and control which transactions are scanned by Vital Security Web Appliance and which go out directly. By proactively stopping all Spyware at the enterprise gateway, the solution enabled REI to improve network performance, maximize user productivity and reduce support/helpdesk overhead resulting from security incidents.

The Results: Proactive Prevention of Spyware at the Gateway

This case study provides a detailed analysis of the web traffic entering REI's network over three months of live operations, based on the activities of 600 users with Internet access. All content downloaded during this period was scanned by Finjan's Vital Security™ Web Appliance at REI's Internet gateway. The log files were then analyzed by experts from Finjan's Malicious Code Research Center (MCRC).

About 94% of the malicious content detected and blocked by Finjan's gateway appliance was related to Spyware, including the following violations:

- Attempt to download known Spyware
- Attempt to access websites which are categorized as Spyware sites
- Attempt to access websites which try to execute Spyware applications

In addition to Spyware, there were several other types of malicious behavior detected and blocked during the three-month period. These types of threats include:

- **Potential Malicious Binary files** - malicious or potential malicious ActiveX, Java Applets and Executables.
- **Malicious Scripts** - malicious behavior detected in scripts (File system operation, registry operation) and attempts to exploit systems/browsers vulnerabilities.
- **Potential Malicious Files** - blocked files considered as potentially malicious based on true type detection such as suspicious file types and spoofed executable files.
- **High-Risk Site Categories** - sites which were blocked by URL Filtering module such as Adults, Hacking, Advertisements, etc.

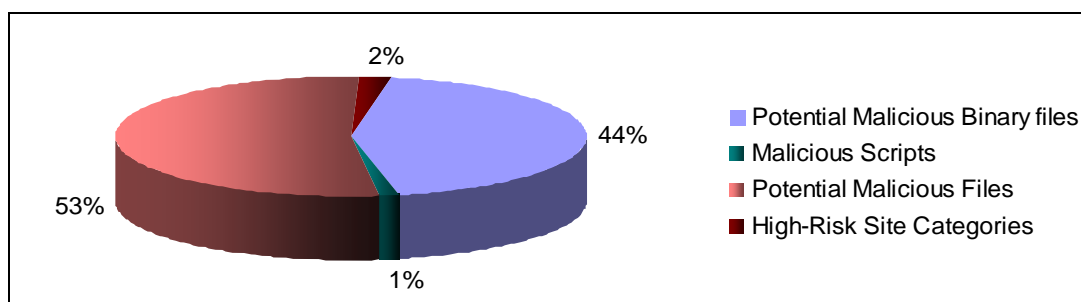


Figure 1 – Other Types of Malicious Behavior

Security Violations Breakdown

The following table provides quantitative information regarding the nature of the security violations:

Nature of Violation	Quantity
Access to Spyware Sites	191,886
Detection of Spyware Objects	482
Potential Malicious Files	6,888
Potential Malicious Binary files	5,777
High-Risk Site Categories	299
Malicious Scripts	177

According to the results of this analysis, it is clear that Spyware represents the most prevalent security threat to REI's network and business productivity. In terms of the other types of security violations (excluding access to Spyware sites) detected over this three-month period, more than 80% could be attributed to Finjan's unique behavior-based security engines. Based on the nature of these violations, it is reasonable to assume that the vast majority of the blocked content would not have been detected by traditional security methods, such as anti-virus and URL Filtering.

Conclusion

As demonstrated in this case study, Spyware and malicious behavior represent the vast majority of security incidents in enterprise networks. Malicious code was detected and blocked by Finjan's Vital Security Web Appliance, based on behavior analysis and without using signatures.

The assumption that an Anti-Virus lab can put its hands on each and every piece of malicious code and create a signature does not play well in the dynamic web scenario. Only proactive, behavior-based security can analyze web content on-the-fly and detect whether or not it is legitimate.

Finjan's Vital Security Web Appliance utilizes patented behavior-based security to detect and block unknown, new and emerging threats that cannot be detected by traditional reactive security technologies. This type of proactive security is akin to having an "expert system in a box", safeguarding corporate users from malicious web content.

About Finjan

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, CRN, SC Magazine, ITWeek, Information Security, and PCPro. For more information about Finjan and its proactive protection solutions against threats driven by mobile malicious code, please visit: www.finjan.com.