



Vulnerability Anti.dote™

Zero-Day Protection Against Known Vulnerabilities

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 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 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>	<p>Printerweg 56 3821 AD Amersfoort The Netherlands Tel: +31 33 4543555 Fax: +31 33 4543550 salesne@finjan.com</p>

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

Table of Contents

1. Introduction	1
2.The Window-of-Vulnerability™	2
3. Finjan’s Vulnerability Anti.dote™	3
<i>3.1 Solution Highlights.....</i>	<i>3</i>
<i>3.2 How It Works</i>	<i>4</i>
4. Conclusion	6
5. About MCRC.....	6
6. About Finjan.....	6

1. Introduction

Today's cybercriminals are motivated by *financial gain*, and their main vector of attack has become the Web. They understand too well that signature- and database-reliant solutions are not designed to protect against obfuscated malicious codes served on compromised legitimate sites, Web 2.0 -based attacks, and other dynamic attack vectors that use the Web.

These sophisticated Web-based attacks are specifically designed to hit the "blind spots" of traditional security systems that rely on signatures or databases (such as anti-virus, URL filtering and reputation based security).

The latest generation of sophisticated malware, including Crimeware, Web 2.0 attacks, Spyware, Trojans and blended threats, exploit vulnerabilities (such as software flaws and security holes) in standard software to deliver payloads that cause major damage to organizations and enterprises.

Enterprise vendors need time to develop a patch, which creates a Window-of-Vulnerability™ (the time between the exploit and availability of the patch against it).

This leaves organizations and enterprises vulnerable to cybercriminals out to steal their valuable personal, financial and business data.

Enterprises, corporations, organizations and governmental agencies alike realize that they need to adopt a security strategy that protects their network systems and data from malicious content, also during the Window-of-Vulnerability™.

This white paper outlines the benefits of active real-time content inspection technology and in particular the benefits of Vulnerability Anti.dote, as a solution to prevent enterprises, corporations, businesses and governmental agencies to be vulnerable, especially during the time between the exploit and the patch against it.

2. The Window-of-Vulnerability™

The latest generation of sophisticated malware, including Crimeware, Web 2.0 attacks, Spyware, Trojans and blended threats, exploit vulnerabilities (such as software flaws and security holes) in standard software to deliver payloads that cause major damage to organizations and enterprises.

Enterprise vendors need time to develop a patch against Crimeware that exploits vulnerabilities in standard software. This creates a Window-of-Vulnerability™ - the time between the exploit and availability of the patch against it.

According to [Symantec](#) the window of exposure was 55 days during the first half of 2007. This was based on an average exploit development time of 5 days and an average patch development time of 61 days. The enterprise window of exposure during the second half of 2006 was 47 days.

This leaves organizations and enterprises vulnerable to cybercriminals out to steal their valuable personal, financial and business data.

With the multitude of operating systems, service packs, applications and security settings each organization has to maintain, IT managers are under constant pressure to patch their systems at the same rate that new vulnerabilities are discovered.

To address this need, Finjan provides them with its Vulnerability Anti.dote solution. It is an integral part of Finjan's [Vital Security™ Web Appliances](#).

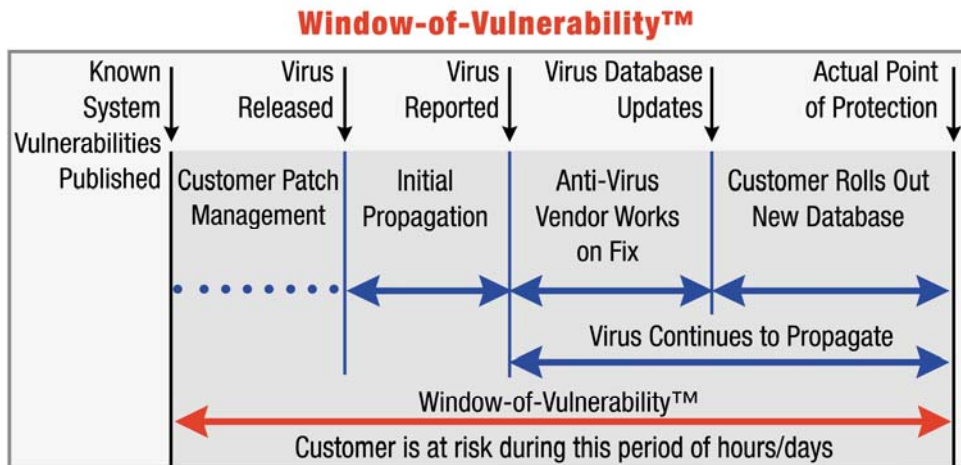


Figure 1 – Window-of-Vulnerability™

3. Finjan's Vulnerability Anti.dote™

Vulnerability Anti.dote provides an optimal balance between powerful proactive security and minimal patch management overhead.

Based on Finjan's extensive knowledge of new software vulnerabilities, Finjan's security experts at its **Malicious Code Research Center** (MCRC specializes in research, analysis and detection of web threats) create behavioral rules that enable the Vulnerability Anti.dote scanning engines to identify and block content that tries to exploit one or more vulnerabilities.

This enables organizations to immunize their desktops from these vulnerabilities that are blocked at the gateway without having to constantly issue emergency patches. It therefore reduces the resources required for patch management. It also allows companies to benefit from Finjan's early discovery of new software vulnerabilities.

3.1 Solution Highlights

- Protects organizations, enterprises, companies and businesses from the next virus/exploit outbreak
- Finjan's technology identifies the underlying program structure of the vulnerability, which allows Finjan's scanners to block attacks
- Blocks any attack trying to exploit the known vulnerabilities as well as their variants
- Utilizes extensive databases of known and newly discovered vulnerabilities, that are constantly updated by Finjan's Malicious Code Research Center (MCRC)
- No need to worry about frequent patches
- Automatic update mechanism for new vulnerabilities, including "hot updates" pushed by Finjan as required
- Optimal balance between proactive behavior-based security and minimal management costs
- Vulnerabilities are logically arranged into categories, for ease of management. Vulnerability Anti.dote is managed using the unified, web-based Vital Security™ management console.

3.2 How It Works

Vulnerability Anti.dote provides zero-day protection against known vulnerabilities that could be exploited by unknown viruses, Crimeware, Web 2.0 attacks and other dangerous web-based threats. Vulnerability Anti.dote proactively protects against spoofing attacks, Phishing attacks, denial of service attacks, silent “drive-by” Crimeware installations, obfuscated malicious code, and remote code execution attacks, all of which exploit unpatched vulnerabilities.

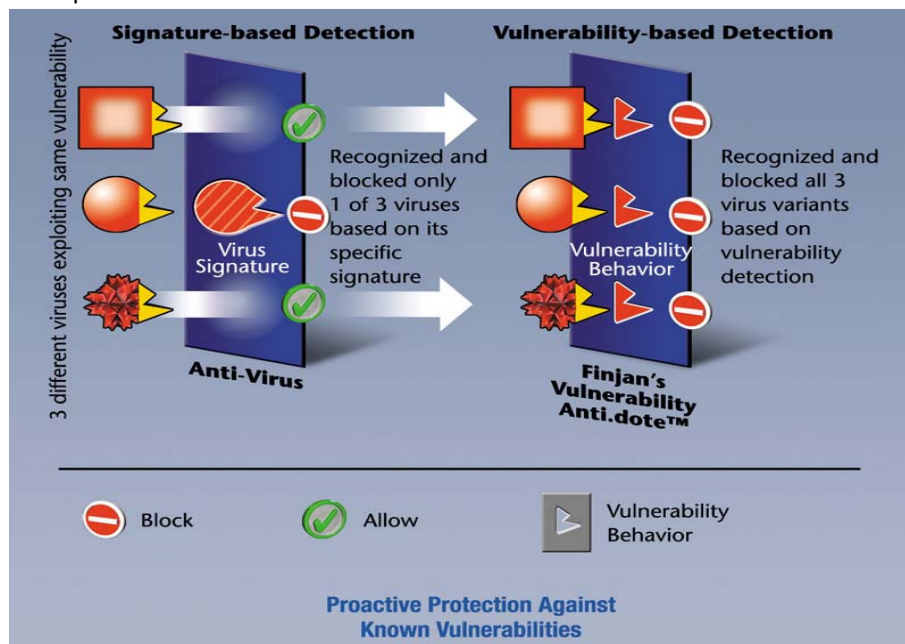


Figure 2 – Vulnerability-based vs. Signature-based Detection

Vulnerability Anti.dote utilizes a multi-layered rule-based engine that can “understand” HTML, scripts and other program components that compose HTTP-based content, at a level similar to compiler analysis.

This engine is driven by highly detailed rules created by Finjan’s MCRC experts.

Finjan creates these rules using its unique, proprietary Vulnerability Description Language (VDL). These rules enable the scanners to identify a wide range of possible attacks that will try to exploit a vulnerability (or a combination of several vulnerabilities). Once a vulnerability has been encoded in Finjan’s VDL and fed into the engine, Crimeware that is targeted to exploit this vulnerability will be discovered and blocked in real time.

In short, Vulnerability Anti.dote captures the essence of the various possible vulnerabilities in browser applications, Windows operating system and services, and other applications that can be accessed by active content such as FTP, Windows Media Player, etc.

As a result, any attempt to exploit one or more vulnerabilities is detected and blocked before such malicious content can enter the network.

The vulnerabilities are logically arranged into categories for ease of management. A full list of a sub-category normally contains hundreds of items that are continuously updated and maintained by Finjan.

Finjan's unique scanners allow the customer to be protected from vulnerabilities starting at the point of discovery – even before any exploit or Crimeware has been written based on these specific vulnerabilities. Cybercriminals are keen to exploit these vulnerabilities for their attacks, especially when related to frequently-used applications such as Microsoft Internet Explorer.

The following screenshot shows the Vital Security™ management console displaying the Vulnerability Anti.dote™ panel.

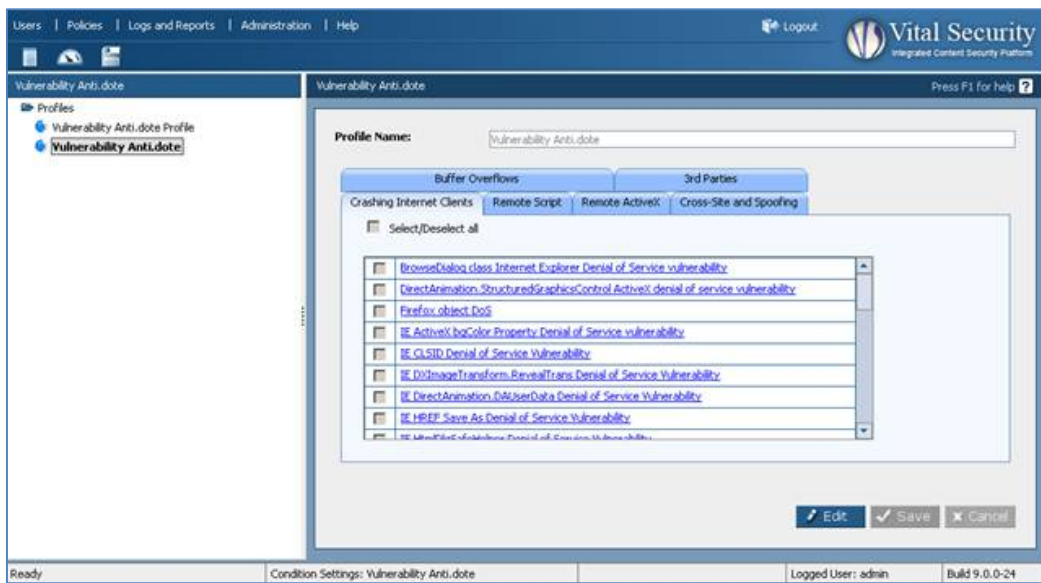


Figure 3 – Vulnerability Anti.dote™ panel

4. Conclusion

Crimeware attacks by nature exploit vulnerabilities.

Finjan's Vulnerability Anti.dote identifies specific vulnerabilities and their variants, using its patented **active real-time code inspection** technology.

Using Vulnerability Anti.dote, organizations, enterprises, companies and businesses are now also protected against Crimeware exploits before software vendors issue a patch for new vulnerabilities.

They can be assured that the Window-of Vulnerability™ that normally remains open until the new patch is released, will stay firmly closed. This prevents malicious Web content from entering or exiting the corporate network, thus protecting enterprises from Crimeware that may result in severe business damage.

By using Finjan's Vulnerability Anti.dote, organizations also benefit from the significant reduction in resources and costs required for patch management.

5. About MCRC

Malicious Code Research Center (MCRC) is the leading research department at Finjan, dedicated to the research and detection of security vulnerabilities in Internet and email applications as well as other popular applications. MCRC's goal is to continue to be steps ahead of hackers attempting to exploit open platforms and technologies to develop malicious code such as Spyware, Trojans, Phishing attacks, worm and viruses. MCRC researchers work with the world's leading software vendors to help patch their security holes, as well as contribute to the development of next generation defense tools for Finjan's real-time secure web gateway solutions.

For more information, visit our [MCRC subsite](#).

6. 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.