



# **Vulnerability Anti.dote™ - Zero-Hour Protection Against Known Vulnerabilities**

---

Finjan White Paper

*September 2006*

---

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 - 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 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](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>                  4<sup>th</sup> Floor, 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>Haidgraben 2, 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>	

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

## Executive Summary

Web-based threats are getting more sophisticated and dangerous, as developers of malicious code are constantly seeking new ways to exploit business and personal computing systems. Bill Gates, Microsoft Chairman, said in January 2005, “You can never underestimate the level of malicious people out there who are going to try to take advantage of whatever things there are.”<sup>1</sup> In other words, there will always be vulnerabilities and weaknesses in operating systems, web browsers and other Internet-related applications, and there will always be people that will try to exploit them for malicious purposes.

Moreover, modern hackers are familiar with the workings of traditional security systems such as Firewalls, Anti-Virus and Intrusion Prevention/Detection products, and are crafting their malicious code to “outsmart” such systems.

On the other hand, as Microsoft releases several new patches and alerts each week to the Windows operating system in an attempt to out-race malicious code developers and “plug the holes”, companies are facing two problematic facts:

- Deploying patches across multiple PCs running mission-critical business applications is a painful process, quite often error-prone, and must be carefully tested to assure no software conflicts or errors in the business systems will result from the Operating System updates. Deploying a new patch every few days, or even weeks, disrupts business and requires special IT attention (and cost).
- In every OS patch, new vulnerabilities are always discovered sooner or later, and even as the patch is being deployed, users are already exposed to new possible attacks.

**Finjan has redefined the concept of proactive protection against attacks exploiting vulnerabilities in Windows-based operating systems and applications by targeting the root cause of the problem.** The revolutionary **Vulnerability Anti.dote™** engine represents the culmination of a decade of researching malicious code and security technologies.

The **Vulnerability Anti.dote** engine identifies any attempt by mobile code to exploit known and new vulnerabilities from the moment they are published or discovered by Finjan, with no need to update desktop PCs or install operating system patches. Since every virus, Spyware or Phishing attack exploits one or more vulnerabilities, Finjan’s **Vulnerability Anti.dote** prepares your organization to stop these inevitable attacks, even before they are unleashed by the hackers.

---

<sup>1</sup> Source: BBC News Online, [http://news.bbc.co.uk/2/hi/programmes/click\\_online/4215183.stm](http://news.bbc.co.uk/2/hi/programmes/click_online/4215183.stm)

# Contents

- Introduction..... 1
  - The Window-of-Vulnerability™ ..... 1
  - What is the Magnitude of the Threat? ..... 2
    - Spyware ..... 2
    - Phishing ..... 3
    - Fraud ..... 4
- The Inherent Danger of Software Vulnerabilities ..... 4
  - “Speed of Light” Infection..... 5
  - Patch Management Is Ineffective against Today’s Threats ..... 6
- The Solution: Finjan’s Vulnerability Anti.dote™ ..... 7
  - How It Works..... 8
  - Benefits ..... 10
  - Complete Protection Against the Most Dangerous Types of Malware Attacks..... 10
- Examples of Vulnerability Exploits..... 11
  - IFRAME Vulnerability (Bofra)..... 11
  - HHCTRL.OCX Vulnerability ..... 11
- Conclusion ..... 12
- About Finjan ..... 12

## Introduction

Today's new generation of "Malware" attacks (e.g., Spyware, Phishing, viruses, Trojans and combinations of these, sometimes referred to as blended threats) are characterized by their complexity and the speed at which they propagate. The frequency and volume of new virus outbreaks has also increased significantly, while the time between the identification of a software vulnerability (i.e., a weakness that could be exploited by malicious code to gain unauthorized access to information or process) and the time an exploit of that vulnerability appears has decreased. Very often an exploit is published along with the vulnerability description (as proof of concept code), leaving no chance to fix the security hole before the threat has begun to spread.

While signature-based anti-virus software can protect systems against known viruses, it is incapable of protecting against new, unknown threats. Anti-virus software is reactive in nature as it depends on signature file updates, which are only made available once the new threat is detected by one of the anti-virus vendors.

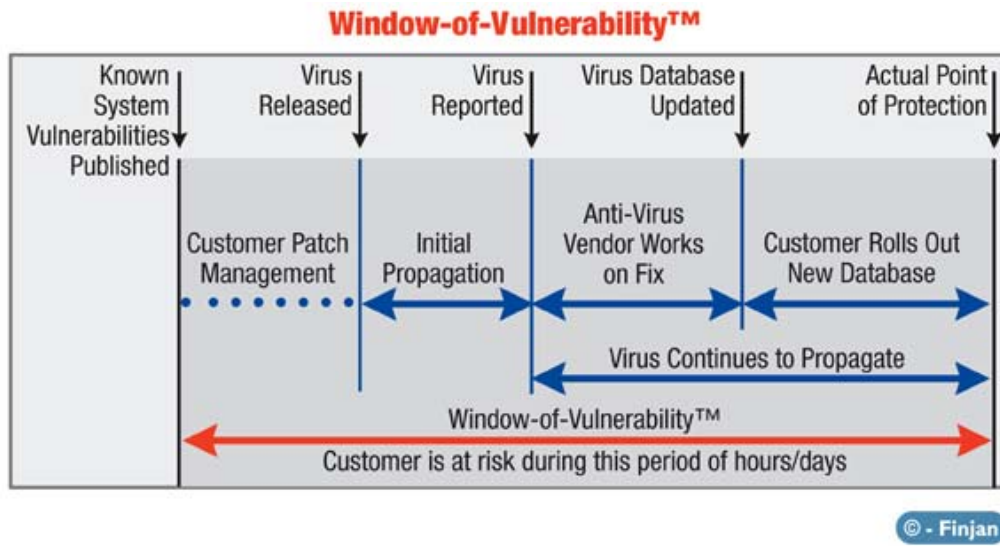
Moreover, even with the latest anti-virus update, enterprises are still exposed to major potential damage. This is because virus and worm attacks typically spread faster than the distribution of anti-virus signatures, as well as the fact that virus-signatures can be easily bypassed using mutations, executable packers, text encoders, etc.

Finally, some viruses (e.g. MyDoom) actually attack the installed anti-virus to disable its update mechanism, so as to prevent the anti-virus vendor from delivering the signature of that virus. Some viruses even shut down the operation of the anti-virus process itself. As a result, the period of time that computers are exposed to viruses is extended well beyond the normal 24-76 hours, exposing users to severe damage and costly cleanup procedures.

Due to their volume and speed, along with new financially-driven motivation and focus of attackers, today's and tomorrow's threats are more dangerous and more costly than ever, presenting a new level of challenge for IT professionals and business owners.

### ***The Window-of-Vulnerability™***

The Window-of-Vulnerability™ is the time from when either a new vulnerability is published or an Internet attack is launched (exploiting a vulnerability not previously known) until protection is delivered, either via a signature update or a software patch, and deployed across the corporate network. 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.



## What is the Magnitude of the Threat?

Based on information collected from over 2,000 companies and organizations in the United States, the total business loss due to computer security incidents in the US alone is conservatively estimated at \$67.2 billion per year (2005 FBI Computer Crime Survey). These statistics are even more alarming given the fact that the vast majority of organizations use anti-virus software (98.2%) and firewalls(90.8%). According to this survey, the top three categories of losses are 1) viruses, 2) unauthorized access and 3) theft of proprietary information.

Looking beyond 2006 in terms of vulnerability exploitation, Sophos expects that “although Microsoft will continue to have its vulnerabilities exploited by malware authors, we will see an increase in attacks taking advantage of security holes in other products (for instance, desktop tools, alternative web browsers, email gateway software, etc) which are widely used.” (Sophos Security Threat Management Report 2005).

## Spyware

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

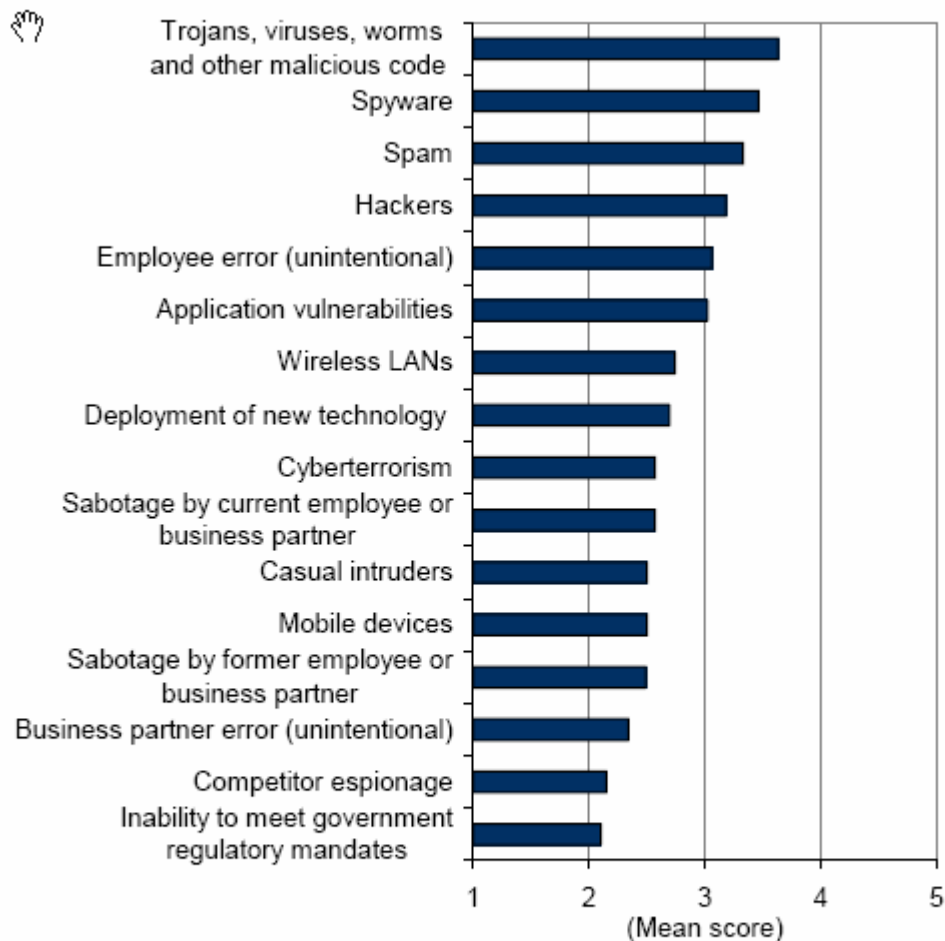
*“Spyware continues to move up the priority list of corporate security concerns. Spyware is now considered to be the second-greatest threat to enterprise network security, according to IDC’s 2005 Enterprise Security Survey. IDC believes more than three-quarters of all corporate machines are infected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

*“Spyware looks set to rise in 2006 and we are now seeing hackers beginning to use zombies to install adware and potentially unwanted software across the network.” (Sophos Security Threat Management Report 2005)*

*“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



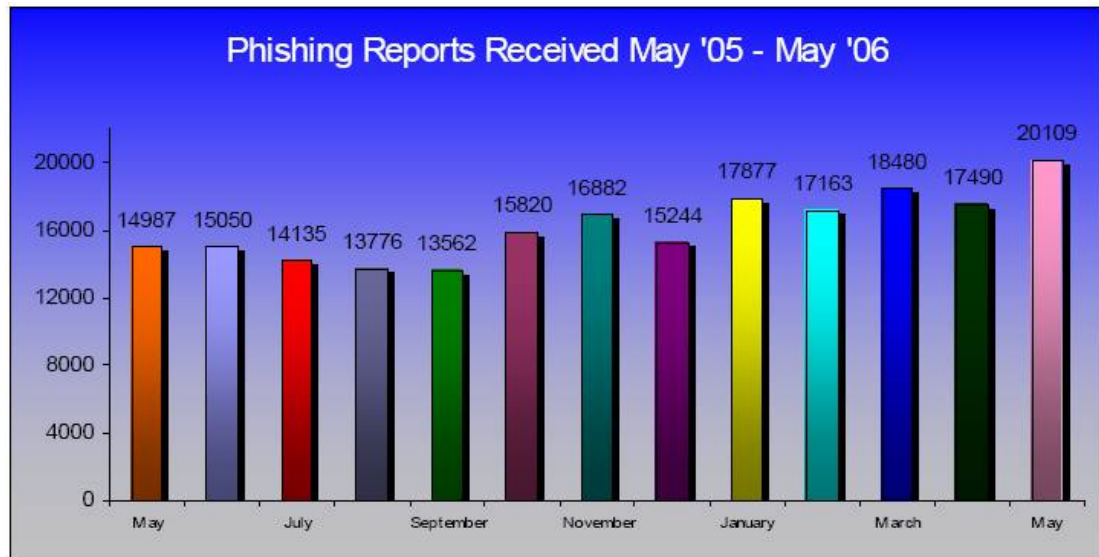
n = 435

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

## Phishing

- There was 34% increase in the number of unique Phishing attacks reported to the Anti-Phishing Working Group between May 2005 and May 2006.



*Source: Anti-Phishing Working Group*

- According to Gartner, an estimated 2.4 million Americans were victims of phishing attacks during this 12-month period, resulting in financial losses estimated at \$929 million.
- “The continued rise in Phishing attacks shows increasing sophistication in strategy as well as more organized efforts among online criminals” (Dave Jevans, APWG chairman)
- Until recently most phishers used the names of financial institutions (i.e., banks) to deceive people into giving away their account information. They also have started to use the names of other organizations such as eBay, Apple, etc.
- The exclusive motivation of phishers is financial gain.

## Fraud

- Spyware-related thefts, based on illegal access to checking accounts, resulted in \$2.4 billion in direct fraud losses (Gartner).
- A survey released in August 2004 by the US Federal Trade Commission reveals that 25 million Americans have been hit by fraud in the past year. The top ten fraud scams include Internet and Information Services fraud.
- In the above survey, it was reported that Americans lost at least \$548 million to identity theft and consumer fraud in 2004 via the Internet.

## The Inherent Danger of Software Vulnerabilities

Vulnerabilities appear within software over time, usually after the software vendor has released the software product to market. These vulnerabilities can be exploited by various forms of malware. A single vulnerability can be “exploited” by multiple types of attacks and variants (mutations). Vulnerabilities, once discovered, are fixed by a patch issued by the relevant software vendor.

Each bug, security hole, misaligned feature or even combinations of legitimate operations that, when put together in a certain order with certain data, will deliver the attack that the hackers intended to launch, is actually a vulnerability of the user’s system. There are several sources on the web that publish such vulnerabilities; some of these sources come from Microsoft and

other software vendors, and some from independent groups (e.g., Secunia, Security Focus). The vulnerabilities are typically published along with exploits that are “proof of concept” pieces of code that constitute some form of attack or malicious behavior based on the specific vulnerability that has been just discovered.

Hackers and producers of malicious code are always on the search for new techniques by which to exploit vulnerabilities. “Security firm Imperva claims a large portion of Web applications are vulnerable, even after developers took a look at them with the goal of fixing security errors. Cisco security architect Martin Nystrom claimed that 95 percent of web applications have flaws (<http://www.vnunet.com>).

Some attacks cause immediate interference and damage, some will silently implant themselves on the user’s computer, and cause cumulative damage over time, while compromising the user’s private data and resources, and possibly also distributing itself over the network.

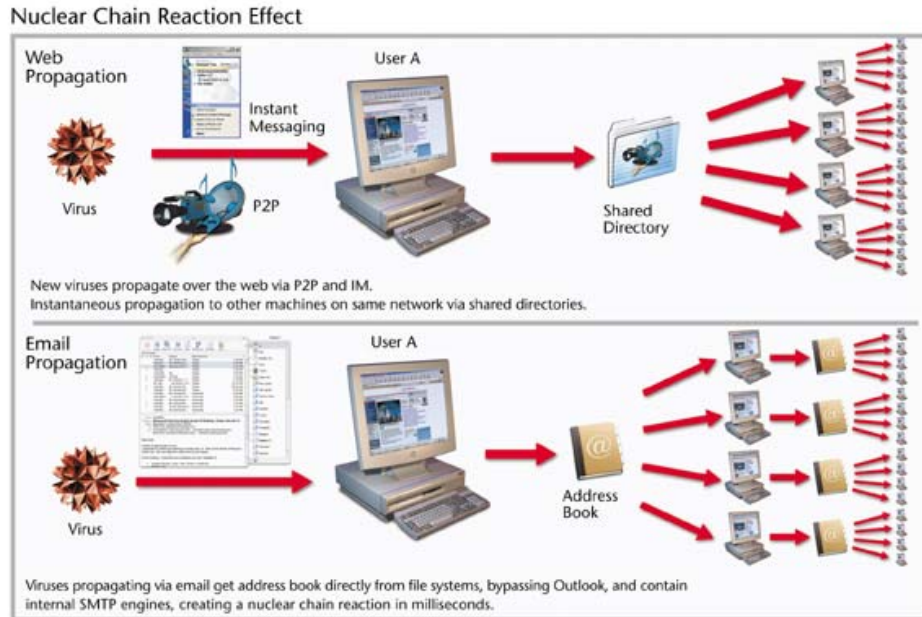
“Organizations that don’t include security as a criterion when building or buying software will see system downtime caused by security vulnerabilities grow from 5% of downtime in 2004 [to 15% of downtime in 2008](#),” according to Gartner’s Strategic Planning Report (Sept 2004), “Building a Sound Security Infrastructure: New Defenses for a New World of Threats.”

### ***“Speed of Light” Infection***

Like many biological pathogens, Internet worms typically spread exponentially until their growth levels off. The speed of these attacks necessitates sophisticated security solutions with capabilities beyond those provided by traditional anti-virus or other reactive, signature based solutions.

When a virus or a worm creates damage of enormous magnitude, it is said to have a “nuclear effect”. The effect can be manifested either by the harm it inflicts to the victim machine, or by the aggressiveness of its distribution. Examples of such attacks include Distributed-Denial-of-Service attacks (DDOS), in which a server is brought to its knees by simultaneous attacks from multiple sources (like the attack in August 2004 that brought down Google). In addition, such attacks often incorporate a major surprise factor, not allowing traditional defensive measures to be set in time to prevent the attack or the damage they inflict.

The rapid proliferation of worms and malicious code targeting known vulnerabilities on unpatched systems, and the resultant downtime and expense they bring, is probably the biggest reason that organizations and vendors are focusing on proactive, behavior-based security solutions.



## ***Patch Management Is Ineffective against Today's Threats***

Patch management is an important element of any enterprise's overall security strategy. In an average week, vendors and other tracking organizations announce about one hundred and fifty alerts (Lynda McGhie, *Secure Business Quarterly*, Q2/2003). The near-absolute majority of users are working in a typical Windows Office environment, running operating systems such as Win/98, Win/ME, Win/NT, Win/2000 and Win/XP, surf the web using Internet Explorer, and read email using Outlook or Outlook Express. There are innumerable combinations of operating system versions, service packs, and Windows patches, with multiple versions and patching levels of Internet Explorer and security settings.

During 2005, for example, Microsoft published 55 security updates, many of which were cumulative patches containing more than one fix. Carnegie Mellon University's CERT Coordination Center states that the number of vulnerabilities each year has been doubling since 1998. As a result, patch management has become an increasingly burdensome issue for IT organizations in terms of people, process, and technology.

**Gartner reports that over 90% of the security exploits are carried out through vulnerabilities for which there are known patches. (Lynda McGhie, *Secure Business Quarterly*, Q2/2003).** Remember the Mimail worm that wreaked havoc worldwide in August 2003? It was exploiting an Internet Explorer vulnerability, published in August 2002, for which Microsoft released a patch in April 2003. Mimail attacked four months after the patch's release and a full 12 months after proof-of-concept!

Due to the multitude of operating systems, service packs, applications and security settings each organization has to maintain, IT managers are hard pressed to patch their systems at the rate that new vulnerabilities are discovered. This is the classic Window-of-Vulnerability™ that leaves enterprises exposed to malware attacks for intolerably long periods of time.

Patch management involves the laborious process of sorting through growing volumes of alerts, figuring out applicability to unique IT environments and configurations, testing patches

prior to implementing and finally orchestrating the process of timely updates. System administrators don't have the bandwidth to deal with the sheer magnitude of patches and hot fixes, and don't have time for the constant review and system changes required by patching.

Even new "automated patch management" products will not solve the problem for most organizations. It is too risky to automatically deploy each new patch across the whole organization, as it may cause problems or conflict with business applications used by the organization. Therefore, each update must be first tested in an isolated environment for smooth interaction with all the business applications – a task that takes time.

Patch management is performed because vulnerabilities exist in software. When a credible threat can target a vulnerability, then you have an identifiable risk that will remain as long as the threat exists. However, once the vulnerability has been successfully patched, then the risk has been removed for that patched device even though the threat remains in place.

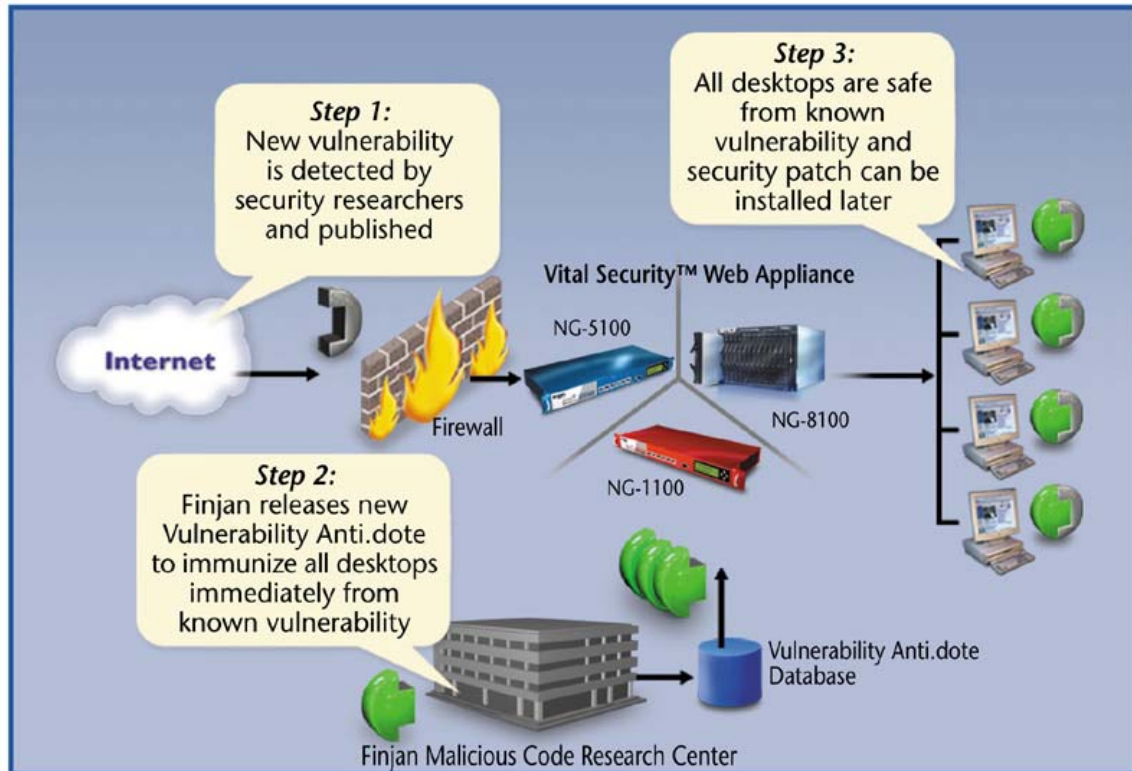
## The Solution: Finjan's Vulnerability Anti.dote™

Finjan's breakthrough **Vulnerability Anti.dote™** technology represents an optimal balance between powerful proactive web security and minimal security and patch management overhead.

Finjan's dedicated team of Malicious Code Research Center (MCRC) experts specialize in the discovery and analysis of new vulnerabilities in Windows-based operating systems and applications. A vulnerability refers to any bug, security hole, maligned feature or combination of operations that can constitute a malicious attack. In 2005 Finjan has reported high risk vulnerabilities to Microsoft and other software vendors. Based on Finjan's extensive database of published vulnerabilities, as well as unpublished vulnerabilities discovered by MCRC researchers (and disclosed by Finjan only to the vendors of the relevant products), Finjan creates behavioral rules that enable the Vulnerability Anti.dote scanners to identify and block content that tries to exploit one or more vulnerabilities.

Finjan has built and is constantly maintaining a database that contains samples and technical details of numerous vulnerabilities. The sources of this database are publicly known vulnerabilities and attacks, internal research conducted at the MCRC in Finjan and collaboration with security vendors and security researchers. For each vulnerability, the database determines several key elements, including:

- Core elements of the vulnerability
- A description of the damage or malicious operation made available by the vulnerability
- Systems exposed to this vulnerability (Operating System, service pack, patch etc.).



*Vulnerability Anti.dote™ Workflow*

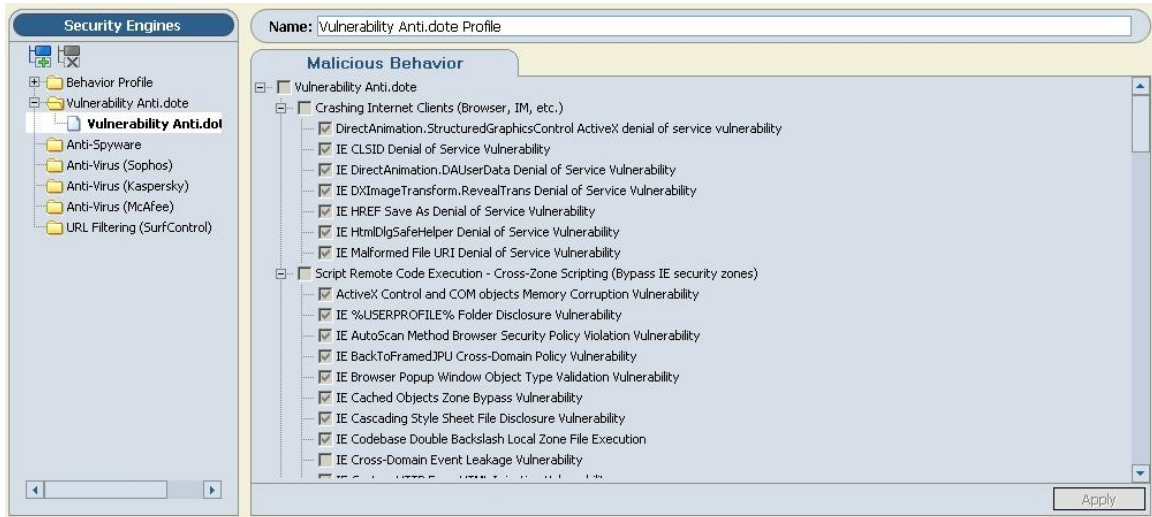
## How It Works

**Vulnerability Anti.dote** utilizes a multi-layered rule-based engine that can “understand” HTML, Scripts and other programmatic components that make up HTTP-based content, at a level similar to compiler analysis. This engine is driven by highly detailed rules that capture the essence of the various possible vulnerabilities in any of the following software applications or systems:

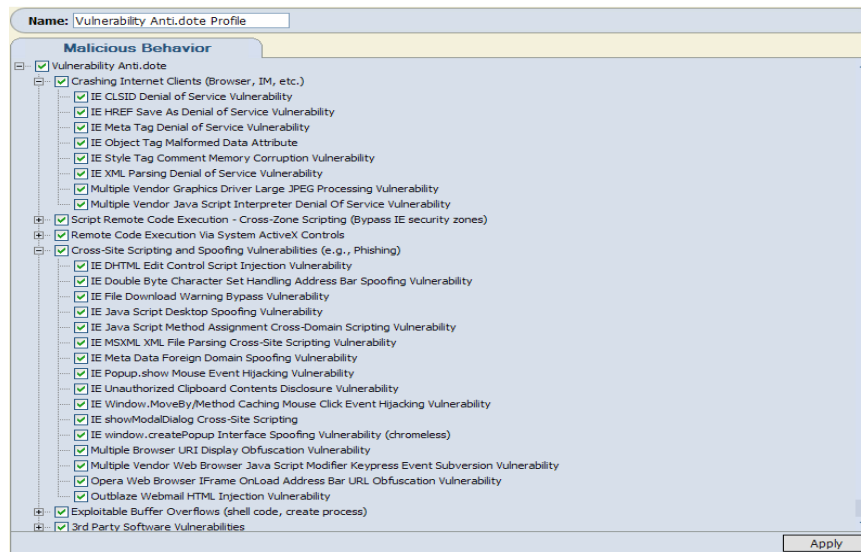
- Internet-related applications, such as Internet Explorer and Microsoft Outlook
- Windows operating system, services, file system and runtime libraries
- Various protocols or applications that can be accessed by any type of Active Content coming into the user’s PC over the network such as FTP, Windows Media Player, etc.

MCRC analyses the vulnerabilities and using Finjan’s unique, proprietary **Vulnerability Description Language (VDL)**, Finjan creates behavioral rules which translate into operational instructions that feed the **Vulnerability Anti.dote** scanning engines. These rules enable the scanners to identify, for a given vulnerability, a wide range of possible attacks that will try to exploit this vulnerability, or a combination of two or more vulnerabilities. Thus, from inception, once a certain vulnerability has been encoded in Finjan VDL and fed into the engine, the engine can discover and protect against multiple viruses that will inevitably be written to exploit this vulnerability. This is the core of Finjan’s breakthrough **Vulnerability Anti.dote** technology.

The vulnerabilities are logically arranged into categories, for ease of management. The following example is a screen-shot of the Vital Security management console, showing the **Vulnerability Anti.dote** panel, with some of the vulnerability categories partially expanded.



The following screen-shot shows an example of just one of the sub-categories (URI Vulnerabilities) fully expanded. The full list contains hundreds of items, and is 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 virus has been written based on these specific vulnerabilities, and naturally before a patch is released. Such vulnerabilities often evolve into the next virus, especially when related to frequently-used applications, such as Microsoft Internet Explorer.



*Vulnerability Anti.dote Protection over Time*

## Benefits

- Protects you **before** the next virus/exploit outbreak, based on known vulnerabilities in any mainstream software system (e.g., Microsoft, Netscape)
- Frees you of the need to worry about patching your systems since it requires almost no management (only automatic updates).
- Virtually eliminates false positives for optimal transparency and user productivity
- Breakthrough technology identifies the underlying programmatic structure of the vulnerability which allows scanners to block any potential attack based on the known vulnerability as well as all of its variants.
- Extensive database includes information on numerous known and newly discovered vulnerabilities, many of which have been discovered by Finjan Malicious Code Research Center (MCRC).
- Weekly update mechanism for new vulnerabilities, with possible “hot updates” pushed out more frequently by Finjan as required
- Optimal balance between proactive behavior-based web security and minimal management costs – protection starts at the point of vulnerability discovery

## Complete Protection Against the Most Dangerous Types of Malware Attacks

Vulnerabilities covered by the **Vulnerability Anti.dote** range from bugs that can crash the system or consume CPU resources to exploits that could lead to remote code execution. Vulnerability Anti.dote proactively protects against a large number of:

- Spoofing attacks, in which the actual email or web page viewed by the user is different than what is claimed to be presented. For example, the user could browse a web page from a hacking site, yet the page’s address, which is shown to the user, would be a different well-known site.
- Phishing attacks, in which typically an innocent-looking email is sent to the victim. Allegedly, the email comes from a respectable or a known source, yet when it is opened or when the user clicks on a link in it, he/she is redirected to a web page that entices the user to provide personal details. For more information, read our white paper entitled “Phishing – Threats and Countermeasures”.

- Denial of service attacks, in which either the web browser or the email client erroneously parses and executes a malicious active code object, thereby limiting the speed or functionality of Internet browsing or causing the termination of the web browser or the email client application. Another harmful effect could be a complete machine freeze.
- Silent “drive-by” installations of spyware, in which a malicious applications are installed on the victim’s machine without any user interaction and without any prompt. For more information, read our white paper entitled “Spyware – Threats and Countermeasures”.
- Remote code execution attacks, in which an attacker successfully exploits a bug that allows him/her to plant and execute his/her own code on the victim’s machine and gain complete control over it.

## Examples of Vulnerability Exploits

### ***IFRAME Vulnerability (Bofra)***

The IFRAME vulnerability, published in November 2004, allows an attacker to execute arbitrary code remotely on Windows operating systems and gain complete control of the victim's computer. The most prominent vulnerable application is Internet Explorer, although other programs (e.g., Outlook, Outlook Express, AOL, Lotus Notes) that use the WebBrowser ActiveX control were also in danger of being affected by this vulnerability. Confirmed vulnerable systems are fully patched Windows 2000 and Windows XP machines using Internet Explorer 6.0.

On November 7, the date that Finjan issued an alert, there were no worms or viruses that had yet exploited this vulnerability. Since that time, several exploits of the IFRAME vulnerability were reported:

- November 11, 2004: Two new Mydoom worm variants were found that exploited this vulnerability. Both Mydoom.ag and Mydoom.ah worms, also known as Bofra/A and Bofra/B, send e-mail messages which include a malicious URL. The URL exploits the IFrame vulnerability to automatically download and launch an executable. The e-mail messages do not include an attachment. The URL is actually a link to one of the compromised machines which serves as a web server following the infection.
- November 21, 2004: The IFRAME exploit was found to be spreading through banner ads. Web site visitors who clicked on banner ads on some web sites could have been automatically infected with variants of the Bofra worm. Incident information can be found in the SANS report at: <http://isc.sans.org/diary.php?date=2004-11-20>

Finjan’s products blocked all possible variants of this dangerous Internet Explorer (IE) remote code execution exploit.

### ***HHCTRL.OCX Vulnerability***

The most recent version of the HHCTRL.OCX vulnerability was published in October 2004. This vulnerability allows an attacker to remotely execute script code when the victim browses a malicious web page. By exploiting this vulnerability in conjunction with several others, a hacker could execute arbitrary code on the victim’s machine. The bug applies to several systems, including Windows XP SP2. More information on this vulnerability can be found at <http://www.kb.cert.org/vuls/id/25249>. Research conducted at Finjan’s Malicious Code

Research Center indicates that this vulnerability has already been exploited in several spyware and phishing scams.

Finjan's products blocked all possible variants of this dangerous Internet Explorer (IE) remote code execution exploit.

## Conclusion

Every malware attack, by definition, exploits a vulnerability. Finjan's **Vulnerability Anti.dote** identifies specific vulnerabilities and their variants, and using advanced behavior analysis proactively blocks any Active Content trying to exploit such vulnerability. This means that you are protected against malware exploits, such as IFrame, even before software vendors have issued a patch for a new vulnerability, thus closing the Window-of-Vulnerability™ that leaves enterprises exposed to potentially hazardous malware attacks for intolerably long periods of time.

While virtually eliminating the risk of being hit by an attack, **Vulnerability Anti.dote** also significantly reduces the resources and costs required for patch management since you don't need to patch your systems as frequently in order to be protected against malicious Active 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, 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](http://www.finjan.com).