



How to Minimize the Impact of Cybercrime on Your Business

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.dot 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 Web as the primary attack vector for cybercriminals	2
3. The business impact of Cybercrime	3
4. Emerging Crimeware Trends	4
<i>4.1 Evasive attacks</i>	<i>4</i>
<i>4.2 Dynamic code obfuscation</i>	<i>5</i>
<i>4.3 Web 2.0 exploits</i>	<i>6</i>
5. Finjan’s Secure Web Gateway solution uses active real-time content inspection	7
<i>5.1 Key features of Finjan’s active real-time content inspection technology</i>	<i>7</i>
<i>5.2 Benefits to the enterprise</i>	<i>9</i>
5.2.1 Anti-Crimeware using active real-time content inspection technology	9
5.2.2 Deploying active real-time content inspection technology within Finjan Secure Web Gateway Solutions	9
<i>5.3 Advantages over other security solutions</i>	<i>10</i>
5.3.1 Anti-Virus	10
5.3.2 Reputational databases.....	11
5.3.3 Intrusion detection and intrusion prevention systems.....	11
5.3.4 Heuristic technologies are prone to false-positives	12
5.3.5 Gateway-base URL filtering (including dynamic URL filtering)	12
6. What do industry experts say?	13
7. Conclusion	14
8. About Finjan	15

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).

Illustrating the magnitude of this trend are the following examples:

- The FBI's Internet Crime Complaint Center (IC3) registered its one-millionth official complaint in June 2007 after seven years of operations. Many of these complaints involved reports of identity theft, such as loss of personal identifying data and unauthorized use of credit cards or bank accounts.
- The retailer Marshalls and TJ Maxx (part of the TJX Companies) disclosed in January 2007 that computer hackers broke into its systems and stole customer data. The stolen credit card and debit card information was used by cybercriminals in several US States and overseas. As a result, the Company recorded an after-tax cash charge of approximately **\$118 million**, or \$.25 per share, with respect to the computer intrusions.
- In December 2007, more than 10,000 websites in the US were infected by a new variant of Crimeware toolkit. The attack consisted of an extremely elusive Crimeware trojan that infected end users' machines and then sent data from these machines via the Internet to its "master" – the cybercriminal.
- In December 2007, director-general of MI5 sends letter to British companies warning them of an **electronic espionage attack** against their systems. This new **wave** of attacks generating from **China**, distributed malicious content using obfuscated code and a network of websites to bypass traditional information security technologies.

Enterprises and organizations are becoming more and more dependent on the Web for online business applications, access to information, and communication with the public. This offers cybercriminals lots of opportunities to invisibly inject and propagate malicious code. 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.

This white paper takes a look at the Crimeware industry and examines Web-based techniques and methods currently used to sustain cybercrime. It also focuses on the business impact of these attacks. The paper also outlines the benefits of active real-time content inspection technology as a solution to help secure enterprises, corporations, businesses and governmental agencies from this growing Crimeware threat.

2. The Web as the primary attack vector for cybercriminals

The Web has become a primary attack vector, as confirmed by Gartner in its June 2007 report:

“The Internet and Internet applications will be the primary sources of malware infections in the enterprise in 2008 and beyond (0.8 probability).”

“Malware filtering in the Web gateway will increase from a penetration level of 10% to 15% of enterprises in 2006 to 70% of enterprises by 2011, driven by the emerging supply of more consolidated and scalable solutions and the increasing threat of Web applications (0.8 probability).”

Source: Gartner Secure Web Gateway Magic Quadrant, June 2007

Statistics from January 2008 by [Websense](#) confirm the growing use of the Web as an attack vector.

- 51% of websites with malicious code are *legitimate* sites that have been compromised, rather than sites specifically commissioned by hackers
- 18% of malicious websites were created using a *toolkit*
- 65% of unwanted messages contain malicious URLs (including links to spam and malicious sites)

Moreover, malicious code on websites is constantly being altered.

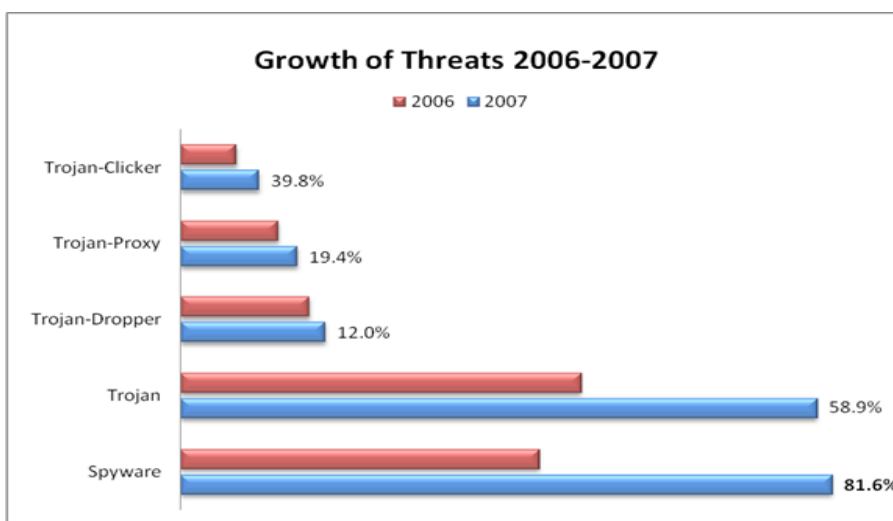


Figure 1 - Malware evolution in 2007 (based on data from Kaspersky Security Bulletin 2007)

3. The business impact of Cybercrime

Attacks are typically targeting internal user systems within the corporate network, using invisible “Web-borne” techniques to take control.

With the necessary tools readily available on the Internet, gaining remote access to an internal workstation only requires determination from the cybercriminal. It only takes a few hours for the criminal to stealthily gain access and take control of the critical internal business systems and data of a company and use them for profit.

Organized crime cells are especially focused on infiltrating businesses and personal computers, using the services of highly-skilled professional Crimeware writers. These crime pros need little time to access the personal information and data of the end-user. This of course significantly increases the security risk and thus places a huge burden on security experts.

Using a \$100-\$200 “Do It Yourself” **toolkit**, cybercriminals can achieve the following for significant profit:

- 1) Gain access to the balance sheets of companies and manipulate stock behavior.
- 2) Locate payroll information.
- 3) Get hold of business’ bank statements and transfer money from that business or make transfers between accounts.
- 4) Gain access to company’s budgets and private financial statements.
- 5) Steal company’s product roadmap and R&D work-plan for industrial espionage.
- 6) Capture company’s credit card numbers for purposes of fraud.
- 7) Intellectual property theft

Needless to say, the damage to a business or organization from any of the above-mentioned illegal activities could be devastating. Any corporations’ or organizations’ confidential information and intellectual property have substantial business value. With such an easy and profitable “return on investment”, it is clear why organizations, governmental agencies, corporations, enterprises and businesses alike have become prime targets.

The estimated total amount of annually losses due to computer-related crimes runs in the billions of US\$. To illustrate, the total loss for the e-crime victims of cases referred to the FBI in 2006 was \$198.44 million.

(Source: Internet Crime Report **2006** of the FBI/National White Collar Crime Center)

4. Emerging Crimeware Trends

Crimeware has become a business and its evolution is being driven by commercial and financial interests.

As we have seen above, a real market exists for malicious code, governed by the market forces of supply and demand. Vulnerabilities are being traded in online auctions, and commercialized malicious products, such as toolkits, are being developed and packaged to serve this market. Criminals are willing to pay large sums of money for bank account details, credit card numbers and confidential business data collected by trojans, keyloggers and other types of malicious code. As a result, profit-motivated and highly skilled crimeware writers are continuously finding new ways to mask, disguise and obfuscate their crimeware attacks. The rationale is simple – the longer their malicious code remain undetected, the larger the amount of users that can be infected, and the higher are their revenues.

Finjan examines these trends in its quarterly [Web Security Trends Reports](#). Some of the trends initially identified by Finjan during 2006 and 2007 (such as evasive attacks and dynamic code obfuscation) have become de facto standards for current Crimeware attacks. These attacks often combine multiple propagation methods and anti-forensic techniques, which significantly improves the chances of going *undetected* by traditional security systems. A few of these key trends are described below.

4.1 Evasive attacks

Security research by Finjan's Malicious Code Research Center uncovered a new genre of highly sophisticated attacks **designed to evade signature-based and database-reliant security methods**. These attacks represent a quantum leap in terms of their technological sophistication, going far beyond drive-by downloads and code obfuscation.

Using advanced techniques, these evasive attacks significantly reduce the malicious code's exposure, thus lowering the likelihood of detection while maximizing opportunities for infection. By keeping track of the actual IP addresses of visitors to a particular website or webpage, these attacks expose malicious code to innocent website visitors only once. The next time any of these visitors accesses that same webpage, benign content is displayed while all traces of the malicious code have completely vanished. This minimizes the exposure of the malicious code to forensic analysis or security research, as there is only a onetime opportunity for the visitor to be exposed to the malicious code.

Moreover, evasive attacks can not only identify the IP addresses of crawlers used by URL filtering, reputation services and search engines, but they can also reply to these engines with legitimate content. This way, these toolkits increase the probability of mistakenly being classified as a legitimate category. The combination of evasive attacks with code obfuscation techniques significantly enhances the capability of sophisticated malicious code to go undetected for a longer period of time.

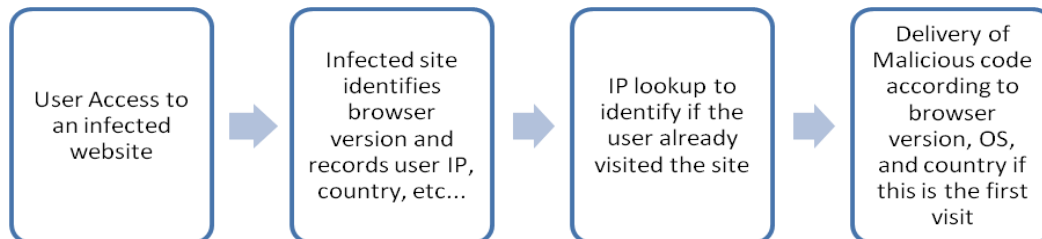


Figure 2 - Evasive Attack Flow

4.2 Dynamic code obfuscation

First emerged at the end of 2006, dynamic code obfuscation has become a standard tool in the Crimeware arena during 2007.

Dynamic code obfuscation is a technique that basically scrambles any malicious code into what seems to be incomprehensible gibberish. It has become one of the favorite weapons for propagating malicious code due to its **effectiveness in bypassing signature-based and database-reliant solutions**.

Dynamic code obfuscation serves each visitor to a malicious site with a different instance of the obfuscated malicious code (based on random functions, parameter name changes, and the actual content). In order to detect the existence of such a particular piece of malicious code and block it, a signature-based security solution would need millions of signatures to be effective. Dynamic code obfuscation enables the reuse of multitude of older attacks as it can bypass anti-virus systems and still be effective on unpatched PCs.

Dynamic code obfuscation, automated code obfuscation utilities and other encoding methods enable attackers to plant “invisible” malicious code that infects a user’s machine as soon as that user visits the malicious site.

4.3 Web 2.0 exploits

While Web 2.0 offers many advantages in terms of enriching the Internet and improving user experience, it also opens the door to new propagation methods for malicious code. Since Web 2.0 platforms (such as MySpace, Wikipedia, blogs) enable anyone to upload content, these sites are easily susceptible to hackers wishing to upload malicious content.

A striking example is the online banner advertisement that ran on MySpace.com and other sites in 2006. It used a known Windows security flaw to infect more than a million users with Crimeware. The vast majority of these popular websites is still considered to be “trusted” by URL Filtering/Categorization products, and will not be blocked even if they contain malicious code.

Research conducted by NetBenefit in the UK in **May 2007** found that 60% of computer users are actively using Web 2.0 technologies in the form of blogs, AJAX-enabled websites and mash-ups.

Finjan researchers discovered that hackers use AJAX queries to create “invisible” attacks. (See also Finjan’s **MPOM** of March 2007). This technique is especially effective, since the code is never revealed on the site and can be encrypted in transit using SSL. It is therefore likely, that URL filtering solutions will remain unaware that a given site is malicious, since they don’t know which parameters will activate the malicious AJAX request. This scenario is illustrated in the diagram below:

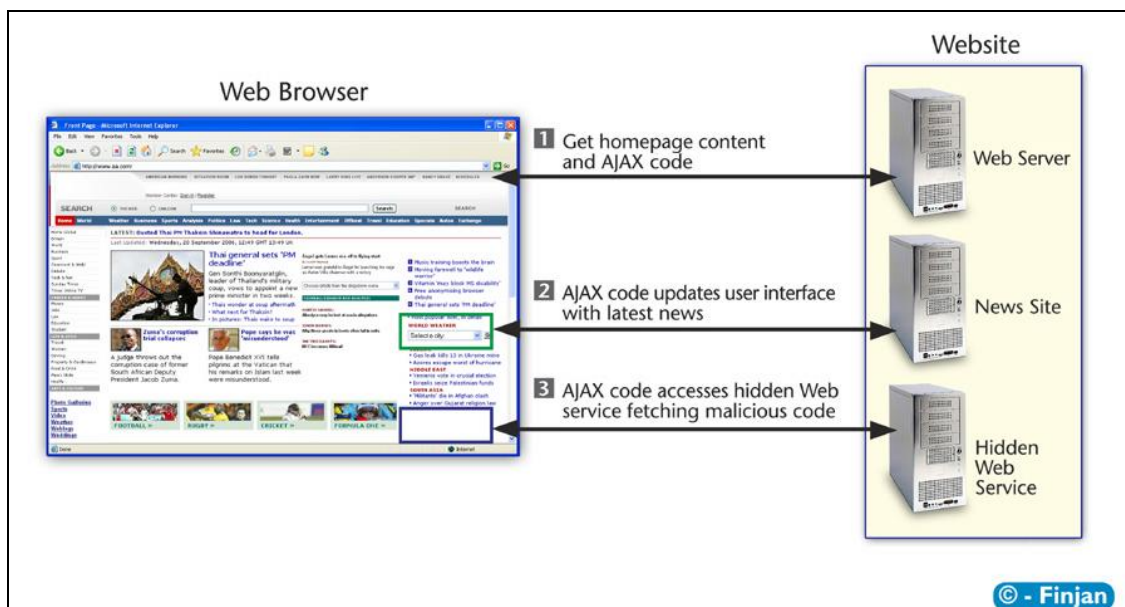


Figure 3 - Using AJAX to access the hidden web

5. Finjan's Secure Web Gateway solution uses active real-time content inspection

In order to safeguard information assets from malicious Web threats, security technologies need to be able to analyze each piece of incoming and outgoing Web content *regardless* of its origin, context, and appearance *in real time*.

Active real-time content inspection techniques are capable of identifying malicious code the first time it is seen. These solutions are able to analyze incoming and outgoing Web content in real-time, understand its intent, and block Crimeware when detected.

Finjan's patented active real-time content inspection technology scans each and every piece of incoming and outgoing Web content in HTTP/HTTPS/FTP, analyzes it in real time regardless of its originating URL and without signature matching. It therefore detects and blocks Crimeware, targeted attacks and other malicious web content, also when hiding in SSL traffic, from entering corporate networks.

Finjan's active real-time code analysis approach is highly effective in handling *unknown, dynamic and rich* Web content (that cannot be detected by reactive signature- and database-reliant security technologies) as well as traditional threats.

5.1 Key features of Finjan's active real-time content inspection technology

When the Web content is processed by Finjan's active real-time scanning engine, its analysis consists of several steps:

- **True content type detection** to identify multiple types of content. The type detection algorithms identify different file type variations, spoofed file types, archived executables and encoded script files.
- **Inspecting all inbound and outbound content** including HTTP/HTTPS/SSL content.
- **Detection and decoding obfuscated code** that tries to "bypass" security scanners.
- **Dissecting HTML code into individual components** (HTML commands, text sections, style sheets, URI, scripts, external object activation, etc.)
- **Scanning each active content component** using a sub-engine that analyzes Java, ActiveX, JS/VB Scripts, HTML, XML, CSS, and HTTP/HTTPS/SSL in context.
- **Constructing a behavior profile** that encompasses the combined operational behavior of the active content components.
- **Comparing the behavior profile** against a comprehensive list of security profiles. In case the behavior profile violates any of them, it is immediately blocked.
- If the case of a "blocked" decision, **a fix-up attempt is performed**, sanitizing the malicious portions and serving the Webpage with as much functionality as possible.

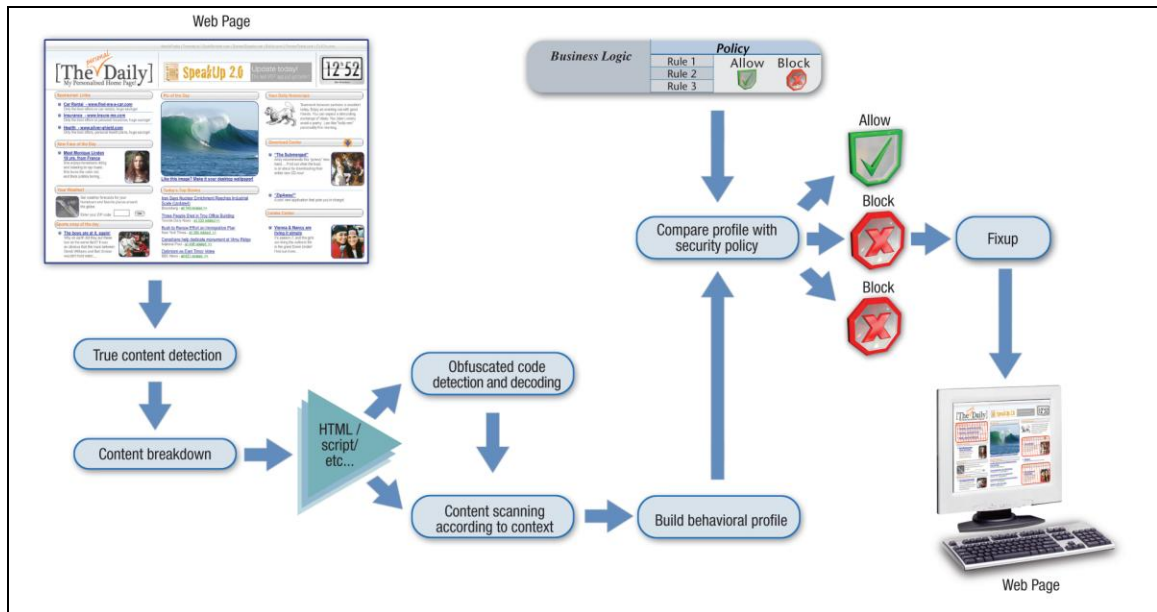


Figure 4 – Active Real-Time Content Inspection Technology Workflow

By deploying its analysis approach, Finjan's active real-time behavior-based security engine understands the programmatic connections among the various bits and pieces of code. Each individual piece of code can be quite benign, and easily avoid network-level scanning devices, as well as signature-based scanning technologies. Deep scanning of the combined operations (resembling a compiler working with a runtime interpreter) can detect the *true* intended action that the code will perform when it reaches the user's desktop.

Finjan's scanning engine is not affected by programmatic variances, such as changing names of objects and variables in the scripts, cross-calls between scripts, and alternating calling sequences.

5.2 Benefits to the enterprise

5.2.1 Anti-Crimeware using active real-time content inspection technology

- An optimal solution able to detect and prevent Crimeware and Web 2.0 attacks despite the advanced propagation techniques and anti-forensic methods (code obfuscation, evasive attacks, random file names and URLs) being used.
- Analyzing each and every piece of web content in real time, regardless of its originating URL and without signature-matching.
- Increased knowledge and awareness of the incoming and outgoing content itself and its associated behavior when it enters/exits the organization. This results in more educated security policy definitions and risk analyses.
- Deep code analysis to reveal malicious combinations of individually innocent functions.
- Exposes Crimeware that tries to extract private information and publish it to the Internet or that tries to access private and unprivileged information.
- Transparent handling of Web traffic reduces transmission costs and downloading time.
- External reporting and logging system provides a flexible and scalable data analysis platform for internal use, audits, and compliance requirements.
- Assistance in **complying** with regulations such as SOX (COBIT) DS5, HIPAA, GLB Act, PCI DSS 1.1., and FISMA.
- For increased Web 2.0 and productivity control, URL filtering engines from IBM Internet Security Systems and Websense are available as an extra option.

5.2.2 Deploying active real-time content inspection technology within Finjan Secure Web Gateway Solutions

- Inspecting all Inbound and outbound content including HTTP/HTTPS/SSL content.
- Finjan provides a comprehensive list that includes actions on the 'File Access' level, 'Processes' level, 'Registry' level, 'Network Access' level, 'Windows' level, etc. In each category, Finjan offers a long list of actions.
- Wizard-driven security policy decision-making system with a single-click rules refinement enhancement.
- Integrated dashboard provides instant information on the system's performance and its risk level, using an extensive set of graphs and views for quick and accurate insight.
- Flexibility to create rules with connections between all types of filters.
- Granular security policies enable any rule to be attributed to any user or group of users.
- True content type detector identifies multiple types of content, regardless of: variations and spoofed types; archived executables; or encoded script files.
- Supporting Cisco WCCPv2 and ICAP standards to ensure interoperability with various networking and caching systems.

5.3 Advantages over other security solutions

Signature- and database-reliant Internet security solutions are limited in preventing new types of dynamic Web-borne attacks. Due to the volatility of website content and the evasive nature of modern attacks, the task of “tracking” or categorizing malicious web content is virtually impossible. Obfuscated malicious codes lurk behind innocent-looking websites, ready to infect corporate networks and systems long before a signature-based anti-virus solution can be updated or a software patch can be installed.

The main types of signature- and database-reliant Internet security solutions are discussed below.

5.3.1 Anti-Virus

Anti-virus solutions are reactive in nature and are mainly effective against *known* threats. They are quite powerless against dynamically obfuscated and zero-day attacks, which may utilize multiple technologies, stages and angles of attack. Hackers are also clever enough to test their malicious code against anti-virus products *before* releasing them to make sure that the code will be undetected. The traditional anti-virus solutions block known viruses and worms by comparing content against signature databases, which need to be updated each time a new virus is discovered. Since viruses spread at tremendous speed, anti-virus vendors traditionally receive new attack samples, create new patches (or signatures), and deliver them to their anti-virus products databases. While these updates take place, virus writers are already busy working on the next viruses for which signatures don't exist yet. The result of this endless loop is exposure to dangerous attacks.

5.3.2 Reputational databases

Similar to URL categorization, reputation services use Web crawlers to map the Web and assign a reputation score for each website. Parameters consist of the IP of the hosted site, the owner of the site (such as a Fortune 500 company), how long the domain is registered, and whether the URL appears in mass spam emails.

Although the resulting database is substantial, it doesn't cover the entire Web and cannot be updated in real time.

New infected webpages are often found on legitimate websites and Web 2.0 sites that normally carry a favorable reputation score.

Reputation services will probably *not block* the malicious content on these sites, since they have a good reputation, have valid owners and a long registration.

Vital Security takes a completely different approach, using real-time code inspection of each webpage. It reads the program code in real time, and determines what this code intends to do. Both known and unknown malicious code is detected using this technology without the need to rely on any database. By analyzing the program code in real time, Vital Security provides a level of security that can never be matched by any of the current reputation services.

5.3.3 Intrusion detection and intrusion prevention systems

Intrusion Detection System (IDS) products are designed to detect situations once the network has ***already been infected***. It identifies patterns of network traffic behavior (involving one computer or a group of computers) that may indicate the spread of a worm or other anomalies. When this happens, they perform "damage control" by cutting off the network traffic, isolating a group of computers and alerting the administrator, resulting in decreased user experience and productivity.

Intrusion Prevention Systems (IPS) and similar "smart packet filtering" solutions usually operate at Layers 2 through 4 of the OSI networking model, and attempt to identify communication patterns (such as rate of transmission) of packets coming into the network. However, powerful and sophisticated attacks cannot be identified at the single-packet level, since such attacks are constructed of high-level scripting and HTML operations within the context of whole webpages. A pattern identified in a *single packet* cannot determine if this packet is a part of a code that will try to exploit the target PC or not. In addition, IPS is not effective against social engineering techniques that simply trick users into clicking "OK" to install Crimeware and all kinds of malware without their knowledge.

5.3.4 Heuristic technologies are prone to false-positives

Heuristic-based technologies detect infections by scrutinizing a program's overall structure, its computer instructions and other data contained in the file. The heuristic scanner then makes an assessment of the likelihood that the program is malicious based on the logic's apparent intent. Anti-virus engines often use heuristics to identify variations of known viruses. They often fail to detect new infections since there are too many ways to obfuscate malicious code, and the only sure way to know if content is malicious or not is watching it run in real-time. This accounts for the high rate of false-positives that users of such heuristic-based systems receive.

In contrast, Finjan's **real-time behavior-based engine** identifies "concrete" behavior and as such is able to minimize overblocking. It detects and identifies the true behavior of obfuscated code which might be used for malicious purposes.

5.3.5 Gateway-base URL filtering (including dynamic URL filtering)

Gateway-based URL filtering products check URLs in a database which clusters URLs in categories and requires constant updates. URL categorization vendors use Web crawlers to map the Web and assign a category to each URL, such as advertisement, finance, gambling.

It is almost impossible to map the entire Web this way, also since websites are highly dynamic and keep constantly changing. As a result, such databases can only be as accurate at their latest scan.

URL filtering blocks non-productive sites, making it a good solution for companies to control their employees' browsing habits to enhance productivity and network performance.

However, it is very limited in protecting users that are surfing the Web from being attacked.

Dynamic URL filtering tries to classify websites (which are not in the database) based on text and graphics.

However, legitimate text and graphics are no guarantee for a 100% Crimeware-free website, also since most infected webpages are on hacked *legitimate* websites.

Finjan's Vital Security takes a completely different approach, using **real-time code inspection** of each webpage. This solution understands the *intended* malicious behavior of Web content based on the actual code, regardless of its URL. It detects Crimeware on websites by analyzing the program code in real time, thus providing a level of security unmatched by any URL filtering technology.

6. What do industry experts say?

Industry players are in agreement regarding the need for real-time, behavior-based security:

- *“URL Filtering was primarily designed to monitor employees Internet activity and enforce acceptable usage policy in order to avoid hostile workplace litigation. However URL Filtering suffers a fundamental flaw to be an effective security filter; it does not monitor threats in real-time.”*
Peter Firstbrook, Gartner Analyst, “The growing Web Threat” (April 13, 2007)
- *“Malware filtering is increasingly important and provides an immediate return on investment (ROI) ...”*
Gartner, Secure Web Gateway Magic Quadrant, June 2007
- *“The evolution of the threats has made protection based on behavioral detection techniques indispenseable”*
Frost & Sullivan AV report 2006
- *“Based on signatures, anti-virus software is dying - we need Behavior-based Interception”*
John Pescatore, Gartner Analyst at Network World
- *“Traditional signature-based antivirus products can no longer protect companies from malicious code attacks. Vendors must execute product and business strategies to meet the new market requirements for broader malicious code protection.”*
Gartner, February 2005 Magic Quadrant
- *“Reactive, signature-based protection is becoming less effective. The time from software patch to exploit is dropping below the time needed for companies to install the patch. Even if you start when the patch is released, most IT departments will take 30 days to test and patch a system and hackers are faster than that now. Therefore we need more proactive security”,...“behavior-blocking looks promising”*
Robert Clyde, Symantec CTO, Vnunet.com
- *“Behavioural-based anti-malware with smart algorithms is the best way to detect and block such attacks [on Web 2.0 sites]”*
Nigel Stanley, Bloor Research - IT Week, Nov 30, 2006
- *“The consensus seems to be either don't let your employees use these [Web 2.0] sites at work, or make sure you have some form of real time, behaviour-based content security in place”*
Phil Muncaster - IT Week blog, November 30, 2006

7. Conclusion

Financial gain is the driving force behind the explosive growth of Crimeware such as phishing, 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.

8. 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.