How to Minimize the Impact of Cybercrime on Your Business

With Finjan's Real-Time Code Inspection

Finjan White Paper

July 2007

For additional information, please visit www.finjan.com or contact one of our regional offices:

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	**Europe** Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com
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	Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com
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	Printerweg 56 3821 AD Amersfoort The Netherlands Tel: +31 33 4543555 Fax: +31 33 4543550 salesne@finjan.com

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

Contents

Introduction

Consider the following scenario: As the owner of a large US-based international chain of retail stores, your company just suffered an unauthorized intrusion into the computer systems that process and store information related to customer transactions. As a result, stolen credit card and debit card information from your stores' customers is being used by fraudsters in several states, as well as overseas. Days after the breach was published, your stock price has already begun to drop. Your first-quarter earnings dipped significantly -- the result of $12 million in charges related to the breach. A hypothetical nightmare? Hardly. This is what actually happened to TJX Companies, the owner and operator of thousands of retail stores, including TJ Maxx and Marshalls, in the United States and Canada.

In January 2007 TJX Companies disclosed that computer hackers broke into its systems in 2006 and stole customer data. TJX expected to incur additional costs related to the breach, including the enhancement of its computer security and systems, as well as technical, legal and other fees. "It is pretty obvious that it was a very well orchestrated, **targeted attack**," commented Avivah Litan, an analyst with Gartner.

The evolution of the Internet has had a profound effect on the way businesses and individuals work and communicate. Enterprises and organizations are increasingly dependent on the web for online business applications, access to information, Web 2.0 technology such as blogs, and the like. Unfortunately, while these technological advancements have added important business functionality, they have also introduced opportunities for cybercriminals to invisibly inject and propagate malicious code. As cybercrime continues to grow and focus on the business sector, enterprises realize that they must adopt a security strategy that protects their network systems and data from malicious content arriving via the web, as well as preventing data leakage in outbound web traffic.

This whitepaper explores the emerging crimeware industry, examining web-based techniques and methods being used to perpetrate cybercrime, with a focus on the business impact of these attacks. The paper also explains the benefits of real-time content inspection technology as a solution which can help secure enterprises from the growing crimeware threat.

World Wide Web Is the Primary Attack Vector for Cybercriminals

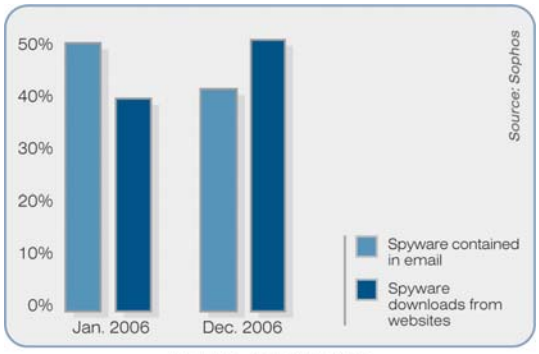
Today's **professional hackers are motivated by financial gain**, and **their main vector of attack has become the web**. They understand that signature- and database-reliant solutions are not designed to counter obfuscated malicious code, Web 2.0/AJAX platforms and technologies, and other dynamic attack vectors in today's web scenario. As a result, new sophisticated web-based attacks are being developed specifically to attack the "blind spots" of traditional security systems which rely on signatures or database (e.g. anti-virus, URL filtering, heuristic-based security).

Illustrating the magnitude of this trend, 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, unauthorized use of credit cards or bank accounts, and the like. According to the McAfee, the number of keyloggers—a favorite software tool used by cybercriminals to track typing activity to capture passwords and other private information—increased by 250 percent between January 2004 and May 2006. For purposes of comparison, phishing attacks increased by "only" 100%.

Gartner confirms this trend in its 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, Introducing the Secure Web Gateway, Peter Firstbrook, et al., March 2007*

Statistics from Sophos support the growing use of the web as an attack vector. While the number of emails containing infected attachments significantly decreased in 2006, the percentage of email that linked to websites infected with downloadable Spyware has reached an astounding 51% (Sophos Security Threat Report 2007). Moreover, malicious code on websites is being altered on average seven times a day in order to evade detection. In Q1 2007, Sophos identified an average of 5,000 new infected web pages (e.g., hosting malicious software or drive-by downloads of unwanted content) being created every day.



Spyware - Email vs. Web

In this context, code obfuscation has become the biggest and most serious threat on the web. In an analysis of live end user traffic in the UK including more than 10 million (>10,000,000) unique URLs, Finjan found that over 80% of the detected malicious code was obfuscated in an attempt to evade signature-based products like anti-virus, IDS/IPS and URL filtering.

The Business Impact of Cybercrime

Attacks typically target internal user systems within the corporate perimeter, using invisible "web-borne" techniques to take control of internal 'endpoints' from the Internet. With the necessary tools readily available on the Internet, gaining remote access to an internal workstation is only a matter of determination. From there, it often takes as little as a few hours to "invisibly" gain access and take control of a company's critical internal business systems and data.

In fact, organized crime has assembled cadres trained to infiltrate businesses and personal PCs. It is enough that a few hundred users are vulnerable for 20 minutes in order to allow hackers access to their personal information and data. These facts of life significantly raise the security risk and place the burden on security experts.

The following examples, any of which could be carried out using a $200 "Do It Yourself" toolkit, show the potential business impact of targeted crimeware attacks:

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

It is clear that the damage to a business from any of the above illegal activities could be devastating. In today's highly competitive market, corporations' confidential information and intellectual property also have a huge business value. With such a return on investment, it is easy to understand why businesses have become prime targets for cybercriminals.

Cybercrime has a direct impact on bottom lines, as well as exposing businesses to identity theft, data leakage, privacy liability issues and compromised intellectual property. Cybercrime in its various forms -- computer crime, identity theft and phishing -- costs the U.S. economy some US$117.5 billion a year, according to a Government Accountability Office (GAO) report in July 2007.

Emerging Crimeware Trends

Crimeware has become a business and its evolution is being driven by commercial and financial interests. A real market exists for malicious code, governed by the forces of supply and demand. Vulnerabilities are being traded in online auctions, and commercialized products, such as toolkits, are being developed and packaged to serve this market. Criminals are willing to pay large sums of money for the bank account details, credit card numbers and confidential business data collected by Trojans, keyloggers and other types of malicious code. Accordingly, commercially-motivated and highly skilled hackers continue to raise the technological bar to find new ways to mask, disguise and obfuscate malware attacks. The rationale is simple – the longer their malicious code remains undetected, the greater the number of users that can be infected. And now that malicious code has commercialized, large numbers of infected users means higher revenues for the attackers.

Finjan has been examining these trends in its quarterly Web Security Trends Reports. Interestingly, some of the trends initially identified by Finjan during 2006-2007 (such as evasive attacks and dynamic code obfuscation) have already become de facto standards for crimeware attacks. Often attacks combine multiple propagation methods and anti-forensic techniques, which significantly improves the chances of cybercriminals going undetected by traditional security systems. Some of these key trends are described below.

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, hence lowering the likelihood of detection and maximizing opportunities for infection. By keeping track of the actual IP addresses for visitors to a particular website or web page, these attacks expose malicious code to innocent website visitors only once. The second time a visitor tries to access the same page, benign content is displayed while all traces of the malicious code vanish completely. This minimizes the exposure of the malicious code to forensic analysis or security research, as there is just one opportunity for a visitor to actually see the code.

Moreover, evasive attacks can identify the IP addresses of crawlers used by URL filtering, reputation services and search engines, replying to these engines with legitimate content and increasing the probability of mistakenly being classified by them 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 longer.

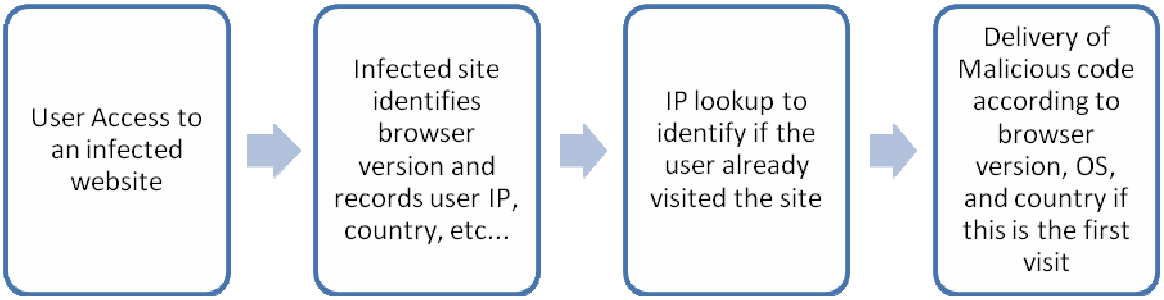


Figure 1- Evasive Attack Logic

Dynamic Code Obfuscation

An emerging security trend towards the end of 2006, dynamic code obfuscation has become a standard tool in the crimeware arena in 2007. Dynamic code obfuscation is a technique that basically scrambles any malicious code into what seems to be completely 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**.

Using dynamic code obfuscation, each visitor to a malicious site will receive a different instance of the obfuscated malicious code, based on random functions and parameter name changes, etc. Theoretically, a signature-based security solution would need millions of signatures just to detect the existence of this particular piece of malicious code and to block it. As a side effect, dynamic code obfuscation "revived" a plethora of older attacks that can now be obfuscated and reused to bypass anti-virus systems on unpatched PCs.

Dynamic code obfuscation, soon-to-be-released automated code obfuscation utilities and other encoding methods enable hackers to plant "invisible" malicious code that infects a user's machine as soon as he/she visits the malicious site.

Web 2.0/AJAX Exploits

While Web 2.0 and AJAX offer many advantages in terms of enriching the Internet and improving the user experience, they also open the door to new propagation methods for malicious code. Since Web 2.0 platforms (e.g., Myspace, Wikipedia) enable anyone to upload content, these sites are easily susceptible to hackers wishing to upload malicious content. In July 2006, for example, an online banner advertisement ran on MySpace.com and other sites, using a known Windows security flaw to infect more than a million users with spyware. What makes matters worse is that the vast majority of these popular websites is considered "trusted" by URL Filtering/Categorization products, and as such will not be blocked despite the fact that they contain malicious code. Research conducted by NetBenefit in the UK in May 2007 found that 60 per cent of users are actively using Web 2.0 technologies in the form of blogs, AJAX-enabled websites and mash-ups.

Asynchronous JavaScript and XML (AJAX) comprises a set of web technologies that are combined to enable web browsers to refresh content (e.g., stock quotes) in real time without requiring pages to reload or refresh. In the security context, Finjan researchers have discovered that AJAX can query back-end web services automatically, or, in other words,

"query the hidden web." This provides an opening for hackers to create "invisible" attacks using AJAX queries, since the code is never revealed on the site and more specifically can be encrypted in transit using SSL. URL Filtering solution will probably be unaware that a given site is malicious, because it doesn't know which parameter will activate the malicious AJAX script. This scenario is illustrated in the diagram below:

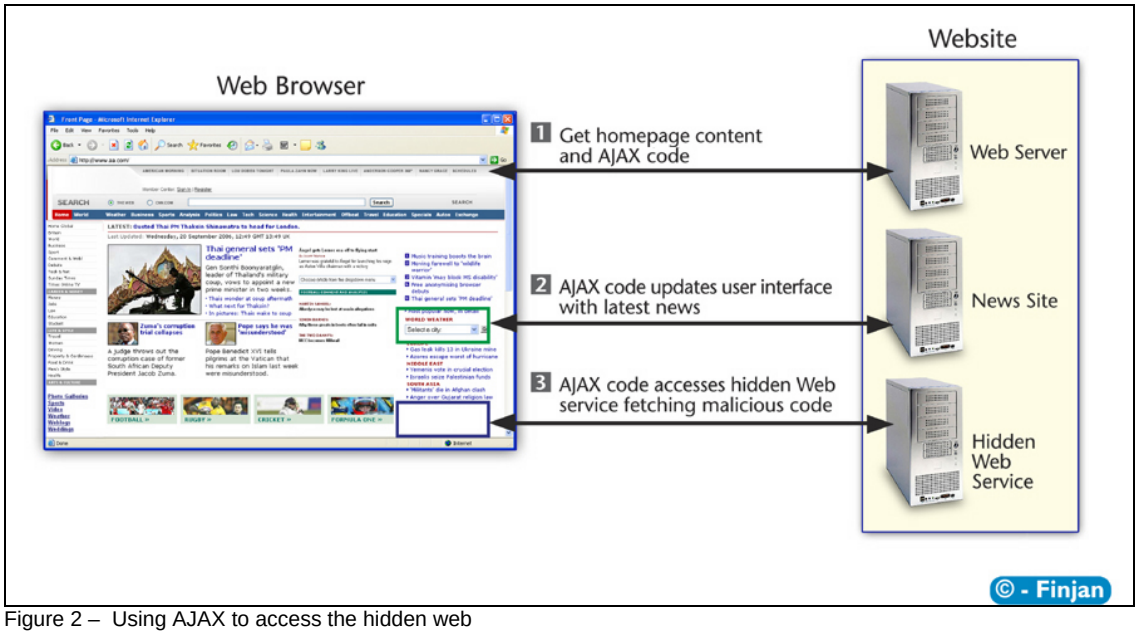


Figure 2 – Using AJAX to access the hidden web

Finjan Anti-Crimeware Security Uses Real-Time Content Inspection to Protect Your Business against Sophisticated Crimeware

In order to safeguard information assets from malicious web threats, businesses require security technologies that analyze each piece of web content regardless of its origin, context, and appearance, when it occurs. The methods being used by today's cybercriminals can only be stopped by real-time content inspection techniques capable of identifying malicious code the first time it is seen. Solutions that are able to analyze web content in real-time, understand the intent and make a decision on the fly are needed to protect users from sophisticated crimeware.

Finjan's unique approach to protecting businesses against crimeware is to understand what the underlying code in each piece of web content intends to do, before it does it. Finjan's anti-crimeware security utilizes real-time content inspection technology which scans each and every piece of web content in real-time (regardless of its source), breaking down the code and understanding its potential effects before it begins to run on the target computer. In this way, it identifies the true intent of the code and blocks only that content which needs to be blocked in accordance with each organization's security policy. Finjan's real-time code analysis approach is highly effective in handling unknown, dynamic and rich web content – such as targeted attacks, Web 2.0 exploits and dynamically obfuscated code - that cannot be detected by reactive signature- and database-reliant security technologies.

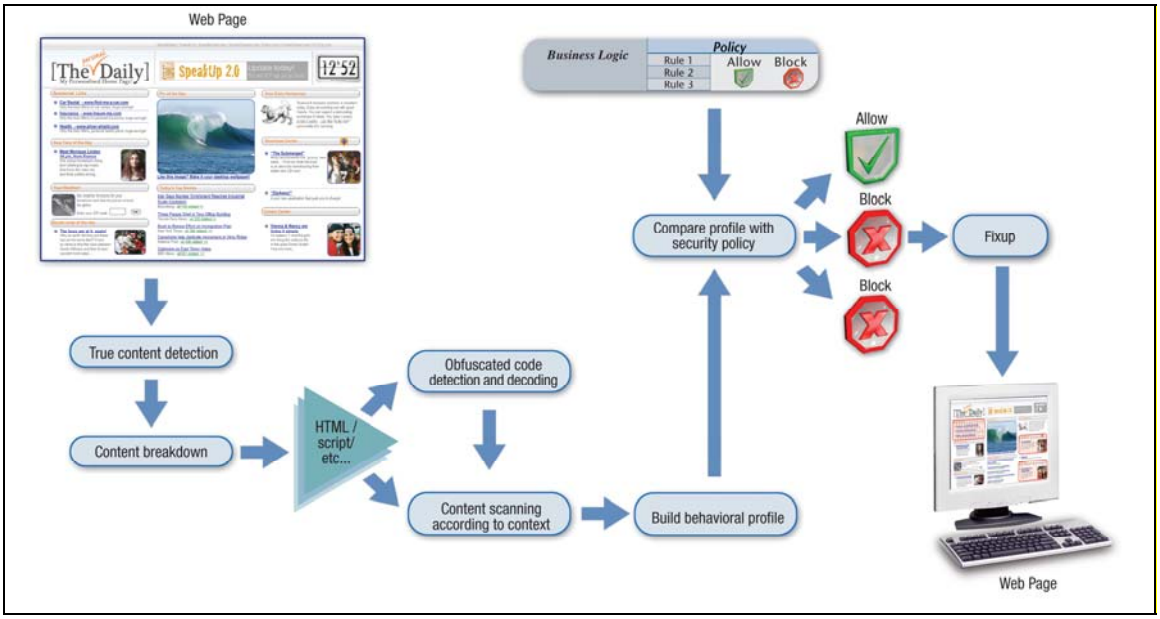
Using this patented real-time code inspection technology, Finjan's anti-crimeware solution detects crimeware based on its intended criminal operation, rather than trying to identify the URL (known or unknown) from which it originates or using signature matching with known malicious programs.

How Finjan's Real-Time Content Inspection Technology Works

When the web content is processed by Finjan's real-time scanning engine, the analysis progresses along the following logical steps:

- **True content type detection** is used to identify multiple types of content. The type detection algorithms can identify file type variations, spoofed file types, archived executables, encoded script files and more.
- **Detection and decoding of obfuscated code**, a technique often used to "bypass" security scanners
- **Breaking up HTML code into components** (HTML commands, text sections, style sheets, URI, scripts, external object activation, etc.)
- **Scanning each Active Content component** in-context by a sub-engine specialized at analyzing that type (Java, ActiveX, Scripts, HTML, CSS and so on)
- **Building a behavior profile** that encompasses the combined operational behavior of the active code components
- **Comparing the behavior profile** against a comprehensive list of security profiles, and if it violates any of them, it is blocked

- If the case of a "block" decision**, performing a fixup attempt** which sanitizes the malicious portions and serves the webpage with as much functionality as possible**.**

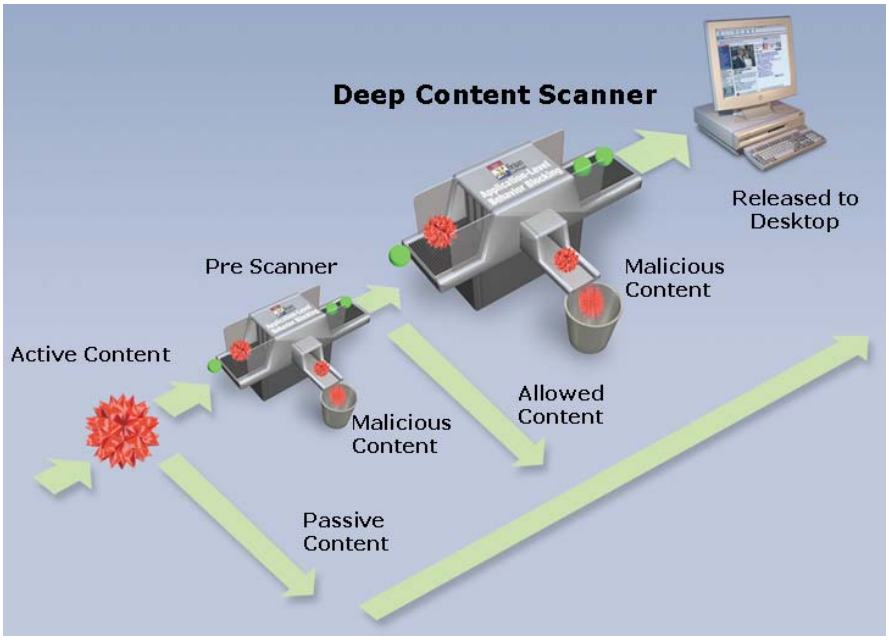


Real-Time Content Inspection Technology Workflow

By employing this holistic analysis approach, Finjan's real-time behavior-based security engine can understand the programmatic connections among the various bits and pieces of code. Each individual piece of code can be quite benign, and easily slip through network-level scanning devices, as well as signature-based scanning technologies. Only by deep scanning of the combined operations in a way that resembles a compiler working with a runtime interpreter, can the engine detect the true intended action that the code will perform when it reaches the user's desktop.

Based on these principles of operation, 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.

To further accelerate the scanning process, Finjan's engines keep a unique mathematically-computed key that identifies each active code object, and cache the behavior profile of the active code object indexed by that key. Therefore when the same piece of active code will be examined by the scanners again, its cached behavior profile will be used. These cached behavior profiles are called *Active Content Lists (ACL)*, and Finjan manages and distributes updates of Malware ACLs to the multiple installations of the Vital Security™ Web Appliance solutions worldwide. ACLs are also used as one of the building blocks of Finjan's *Anti-Spyware* engine.



Two-Step Scanning Approach for Highest Performance

When deployed on a customer's site, an administrator or security officer can use Active Content Lists to white-list particular Active Code objects which are known to the company and proven to be safe; for example, a stock-ticker and financial information Java Applet that communicates information in and out of the user's PC and pops up message windows, can be identified by its unique key and behavior profile, and can be placed on the "white" Active Content List.

Behavioral Rules

The rules that drive the operation of the real-time security engine are not signatures. Rules at various levels define Active Content program and language tokens, semantic patterns of Active Code, permitted combinations of operations, parameters and programming techniques. These rules are created by security experts from Finjan's Malicious Code Research Center (MCRC) group, and fed into the real-time behavior-based security and Vulnerability Anti.dote™ scanning engines, enabling the identification of Active Content that may try to exploit a given vulnerability. Vulnerability Anti.dote is a unique technology that protects computers against known vulnerabilities without the need for software patches. Finjan's Malicious Code Research Center (MCRC) is a leader in the detection of dangerous vulnerabilities that could be exploited for malicious attacks, keeping our customers steps ahead of the hacker community.

Benefits to the Enterprise

Anti-Crimeware using Real-Time Content Inspection Technology

- Only solution able to detect and prevent crimeware despite the advanced propagation techniques and anti-forensic methods (code obfuscation, evasive attacks, random file names and URLs) being used

- Additional security layer against crimeware, spyware, malicious code and complex attacks, leading to a significant increase in ROI from your security investment
- Reduction in 'false positives' that may occur if relying on heuristics based techniques, leading to a reduced cost of solution management
- Minimized overblocking enables users to leverage the full power of Internet as a business tool
- Increased knowledge and awareness of the content (and associated behavior) entering your organization, leading to more educated security policy definition and risk analysis
- Deep code analysis to reveal malicious combinations of individually innocent functions
- Scanners use cached behavior profiles (Active Content Lists) for accelerated performance
- Expose malware that tries to extract private information and publish it to the Internet, or other forms of trying to access private and unprivileged information (HIPAA and Sarbanes-Oxley compliance)

Deploying Real-Time Content Inspection Technology within Finjan Secure Web Gateway Solutions

- Advanced and rich categorization of Active Content actions
- 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.
- 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 – Can identify multiple types of content, regardless of variations and spoofed types; archived executables; encoded script files and more
- Ability to scan encrypted content that travels over HTTPS through our integrated SSL Inspection feature

Advantages over Other Security Solutions

Signature- and database-reliant Internet security solutions, such as anti-virus, URL filtering, firewall, intrusion detection, intrusion prevention and heuristic-based systems, are in most cases incapable of preventing today's 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 code lurking behind the façade of innocent-looking websites can infect your network and systems long before a signature-based anti-virus solution can be updated or a software patch can be installed. Based on the results of the CSI/FBI 2006 Computer Crime Survey, 24% of US companies incurred six (6) or more security incidents (e.g., viruses, Spyware, information theft and other computer crimes) in 2006, despite the fact that virtually all of the organizations surveyed use firewalls (98%), anti-virus software (97%) and anti-spyware (79%).

Anti-Virus

Anti-virus solutions are reactive in nature and, as such, are mainly effective against known threats. However, these solutions are powerless against today's dynamically obfuscated and zero-day attacks, which may utilize multiple technologies, stages and angles of attack. Moreover, today's hackers test their malicious code against anti-virus products before

releasing them in order to ensure that they will not be detected. 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. Given the prolific speed at which viruses spread today, companies know they have very limited protection from new attacks until their anti-virus vendor receives the new attack sample, creates a new patch (or signature), and delivers that patch to the antivirus product's database. The paradox is that while the anti-virus vendor is updating its signature database, the virus writers are busy working on the next new virus for which a signature does not exist. This endless loop always has the same result - the end user is exposed to dangerous attacks.

Reputational Databases

Reputational database technology is one of the newest developments in the security industry. The technology uses a "crawler" to automatically visit a website, and identify its content. However, like other database-reliant solutions, reputational analysis faces the key problem: pure volume. Many URL filtering companies are now promoting their Reputational Databases, and state that they are visiting up to 80 million URLs a day. To put this figure into perspective, though, Gartner has recently stated that the average length of time that a phishing attack is live on the website is only 20 minutes (before the authors themselves remove it to reduce the risk of being detected).

Based on the largest crawling capacity currently published, the technology is only capable of viewing 1,111,111 sites, or 1.38 per cent of the 80 million websites within a 20 minute window. This means there is a 98.61 per cent chance of it not seeing the malware. But with the current number of registered domain names now in excess of 100 million and the estimated number of sites between 200 million and 400 million, the effectiveness and scalability of this technology to address the threat is a serious question mark. Currently, it clearly falls short.

Remediation is also an issue. Once the Reputational analysis solution has tagged a site as being malicious, how long does it take for the crawlers to come back and reassess? Keeping accurate intelligence of all the bad apples is challenging to say the least.

Firewall

Firewalls traditionally operate at Layers 2, 3 and 4 of the OSI model and effectively isolate corporate networks from the Internet as well as hide IP addresses and protect ports from the outside world. While firewalls may still be very useful for intrusion prevention and remote access control, they are no longer efficient for preventing today's malicious code. This is because today's complex threats, such as Spyware and Phishing, enter the network via port 80 (HTTP) and port 443 (HTTPS) which are left open in the firewall. In most organizations, these ports cannot be closed without severely hampering the productivity of the users. Firewalls can either block or allow a certain port, but cannot inspect the content allowed to pass through. Email transportation also opens the door to many threats, and the combination of web and email transportation is highly exploited by various types of threats, such as Phishing. The ineffectiveness of firewalls against such threats is evidenced by the rapid increase in worm penetration in 2006 (such as Mytob and Netsky), despite the extremely wide deployment of firewalls (98% of respondents to 2006 CSI/FBI Computer Crime Survey).

Intrusion Detection and Intrusion Prevention Systems

Intrusion Detection System (IDS) products are designed to detect situations when the network has ***already been infected***, by identifying patterns of network traffic behavior (of 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.

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 (e.g., rate of transmission) of packets coming into the network, rather than analyzing the code entering the network. The problem is that powerful, sophisticated attacks cannot be identified at the single-packet level - such attacks are made up of high-level scripting and HTML operations within the context of whole web pages, so any 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. In addition, IPS is not effective against social engineering techniques that simply trick users into clicking “OK” to install malware without their knowledge.

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. However, since these schemes don’t actually observe full execution of the scanned software, they often fail to detect new infections; there are simply too many ways to obfuscate malicious code, and often the only way to know content is malicious is to watch it run in real-time. This accounts for the high rate of false-positives when using such heuristic-based systems. In contrast, Finjan’s real-time behavior-based engine identifies “concrete” behavior and as such is able to minimize overblocking. It is well-equipped to detect and identify the true behavior of obfuscated code which might be used for malicious purposes. Finjan reduces false-positives, reducing the cost of solution management.

What Do the 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

Conclusion

Financial gain is the driving force behind the explosive growth of crimeware (e.g. spyware, phishing, obfuscated code methods, and targeted attacks), cleverly crafted by professional hackers to evade signature- and database-reliant security tools. As website content is becoming more volatile, and domain names can be set up for brief periods of time, the task of "keeping track" of the malicious content on the World Wide Web is becoming ever more difficult. Attempts to pattern malicious code and create signatures, or to categorize known malicious sites, are clearly insufficient to defend against today's dynamic web threats.

To prevent crimeware and other highly sophisticated web-borne threats, an additional security layer is needed. Today's evasive crimeware attacks cannot be stopped 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 methods being used by today's cybercriminals can only be stopped by real-time content inspection techniques. Therefore, enterprises should adopt a multi-layered approach, typically involving both real-time security, as well as reactive (e.g., signature-based) IT security technologies for stopping traditional threats.

Finjan's anti-crimeware with real-time code inspection technology achieves the highest rate of malicious code detection with virtually zero false-positives. Finjan's secure web gateway solution analyzes each and every piece of web content in real-time, regardless of its original source, and understand its potential effects before it executes on the end user machine. By understanding the true intent of web content, Finjan's 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 the corporate network, protecting enterprises from crimeware that may result in severe business damage.

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 patented behavior-based technology to repel all types of threats arriving via the web, such as spyware, phishing, Trojans, obfuscated code and other malicious code, securing businesses against unknown and emerging threats, as well as known malware. 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.

