Combating the New Generation of Malware: Spyware, Phishing and Active Content

Finjan White Paper

October 2004
Contents

New Era of Internet Attacks.................................................................................................................. 1
What is Active Content? .......................................................................................................................... 1
Threatening Businesses’ Bottom Line...................................................................................................... 2
The Need for Proactive Security ............................................................................................................. 3
Finjan’s Unique Behavior Blocking Solution ......................................................................................... 3
Combating the New Generation of Malware Attacks .............................................................................. 4
  Spyware ............................................................................................................................................... 5
  Phishing ............................................................................................................................................. 6
  Blended Threats – Viruses, Worms and Trojans .................................................................................. 8
Finjan Vital Security™ Solutions ........................................................................................................... 8
  Vital Security™ for Enterprises ........................................................................................................... 9
  Vital Security 1Box™ Series for Small and Medium-Sized Businesses .............................................. 9
Conclusion ........................................................................................................................................... 10
About Finjan Software ............................................................................................................................ 10
New Era of Internet Attacks

Several key trends point to the fact that we have entered a new era of Internet attacks. First, the frequency of viruses traveling through the Internet has increased significantly, while the time between the identification of a vulnerability and the time an exploit appears has decreased. There are tools and Web sites that teach people how to hack into a computer or create a virus or worm, which gives any person with malicious intentions the potential to become the author of the next computer threat.

Second, hackers are becoming more ingenious in how they introduce malware to potential victims. Recent tactics, such as spyware and phishing, are cleverly disguised and use social engineering to trick a user into launching a malicious payload. Even worse, the new genre of “drive-by” downloads can be activated without any user action at all.

“Another cause for the high incidence of the virus infection is the increasing sophistication of viruses and malicious code. Organizations are now facing blended threats that possess characteristics of viruses, worms and Trojans, and blend these with hacking techniques.” (PWC, April 2004)

Moreover, recent viruses (such as 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. As a result, the Window of Vulnerability is extended well beyond the normal 24-76 hours, exposing users to sever damage, while a special tool may be required to clean this complex infection.

Lastly, the intentions behind Internet attacks have changed. Hackers of the past introduced viruses to shut down systems or destroy files, mostly as an adolescent challenge or ways to gain notoriety with the public or underground hacker communities. Hackers today are motivated more by financial gain and aggressively attempt to steal personal information, such as usernames, passwords, bank account numbers and credit card numbers, through the use of malicious code and Trojans that have key-logging and backdoor capabilities.

Despite their widespread deployment, traditional anti-virus and firewall solutions have not succeeded in preventing major outbreaks of highly destructive attacks, such as MyDoom, Sobig and Sasser, the first time they strike, but only reactively after the patch.

What is Active Content?

Active Content refers to components that are embedded in applications which can carry out or trigger actions automatically (and dynamically), often without the user's approval or even knowledge. Active Content is delivered to the user's computer while browsing the web, enabling web sites to provide increased functionality, such as interacting dynamically with visitors, delivering animation and interactive applications, and much more. Of course, active content can be delivered also via email, instant messaging and other means of communication.

Active content technologies include:

- Java applets, ActiveX controls, Java Scripts or Visual Basic Scripts (either as embedded files or as an integral part of a web page) contained in web pages.
• Macros, spreadsheet formulas, or other interpretable or executable code contained in proprietary desktop-application formatted files.
• Executable files.

Active content has become part of common business practices, and is used in business applications such as web conferencing, e-learning, e-commerce and others. However, at the same time, active content technology may be exploited to carry malicious mobile code, which is downloaded and executed on a local system without the explicit knowledge or consent of the user. This dichotomy creates a difficult security challenge for enterprises and businesses.

The figure below illustrates how active content can be used for both business (left side) and malware (right side) purposes.

Security solutions must be capable of detecting and analyzing the behavior of active content in order to block malicious and inappropriate content, while allowing appropriate content to flow in a transparent manner.

**Threatening Businesses’ Bottom Line**

Attacks by active content are growing exponentially and account for the vast majority of today’s malware. These attacks have a direct impact on businesses’ bottom line, as they result in a massive loss of valuable time and resources, reduced productivity and lost revenue. In addition, active content can expose or even lead to theft of confidential or
competitive information. The overall damage created by malware is estimated at over $10 billion annually worldwide.

According to 2004 CSI/FBI Computer Crime and Security Survey of companies and organizations in the United States, the cost of damages caused by viruses alone more than doubled in 2004, reaching an estimated cost of $55,053,900. This fact is all the more alarming given the fact that virtually all of the organizations surveyed use anti-virus software (99 percent) and firewalls (98 percent).

Unsolicited email, or spam, is another growing concern for large and small businesses. In businesses without anti-spam solutions, the average amount of time lost by email users each day due to spam is 10 minutes. This translates into a total of $4.1 million in lost productivity each year for an enterprise with 5,000 email users (Source: IDC, March 2004).

According to mi2g intelligence Unit (UK digital risk management firm: http://www.mi2g.com), the big three malware families of 2004, i.e., all variants of Bagle, MyDoom and NetSky combined, have caused the loss or misallocation of 72 million Equivalent Person Days (EPDs) worldwide over the last two months across corporations, government organizations and homes. This is an average of 1.2 million EPDs daily sustained loss worldwide, the highest ever. These damages are estimated in $55bn in 2003, compared to $20-30bn in 2002 and $13bn in 2001.

The Need for Proactive Security

Traditional security solutions, such as anti-viruses, are reactive in nature and, as such, are powerless against new unknown attacks, which may utilize multiple technologies, stages and angles of attack. These attacks underline the need for application-level behavior blocking solutions.

Today's attacks are ever-increasing in complexity, and simply cannot be identified at the packet-level. Indeed, even anti-virus products are hard-pressed to identify complex threats, which may require multiple steps in order to instigate an attack, each using a different technology. Traditional solutions are not able to collate information from various sources and understand the overall behavior. Only at the application-level (e.g., browser, email app) is it possible to determine accurately what the real behavior is going to be with regard to a specific context.

In light of the above, security experts and analysts everywhere agree that organizations must implement a multi-layered set of security solutions to effectively guard against current and future generations of computer attacks. Proactive security solutions, such as behavior-blocking software, must be leveraged and used to complement traditional signature-based anti-virus software to adequately defend against unknown virus, worm and malicious code attacks at the moment of outbreak, and block them the first time they strike.

Finjan’s Unique Behavior Blocking Solution

Finjan’s Vital Security™ series, including the 1Box™ Series of appliances for small and medium-sized businesses, delivers proactive content security solutions based on Finjan’s patented Behavior Blocking technology that protects companies from new, unknown attacks driven by active content. Finjan offers the only solution on the market that uses application-level behavior-based technology to analyze content, deduce the type of behavior and proactively block malicious or inappropriate content while allowing appropriate content to flow
in a transparent manner. This analysis is carried out in accordance with each business’ security policy which defines what content to trust, authorize and deem appropriate or inappropriate.

Finjan’s Behavior Blocking technology works at the application level, which means that it determines the full set of behaviors that a given piece of content will exhibit when loaded into the target application, e.g. a web browser or email program, and with the help of our policy engine, decides whether to pass, block or neutralize the content. Unlike packet-level security solutions, such as IDS and IPS, Finjan’s approach is particularly effective against blended threats and complex attacks, which use a combination of different technologies and methods, typically exhibiting a mix of virus, worm, and Trojan horse characteristics. Packet inspection products cannot know how a given web page will behave when loaded into a browser, because they never see the web page -- they only see individual packets. Finjan’s products were designed and architected to handle such situations as a matter of course.

Finjan’s scanning technologies will scan the application-level traffic that might carry the malicious mobile code which can infect the computers, and analyzes the behavior of the code itself - before it even begins to run on the target computer. Finjan behavior analysis and blocking technology identifies the combinations of operations, parameters, script manipulations and other exploiting techniques, and can determine that a piece of mobile code is trying to exploit one or more of types of vulnerabilities.

Industry experts are in agreement regarding the need for behavior blocking:

- At RSA Conference 2004 on behavior blocking: “You can really think of this as taking the notion of secure-by-default to the next level. The system will truly know what actions are allowed for operating-system components and the applications that are running”, Bill Gates, Chairman & Chief Security Architect, Microsoft – at RSA Conference 2004.

- “If the AV Industry were getting started today, we would not choose the approach that we currently pursue….The pot of gold at the end of the rainbow AV detection is day-zero detection: to be able to detect and prevent an item of malware or other undesired attacks (rather than move it post infection). In order to achieve this, reactive action will have to become a thing of the past, making way for generic and behavior based blocking,” Paul Gartside, McAfee Inc. – Virus Bulletin Comment, September 2004 Issue.

**Combating the New Generation of Malware Attacks**

Finjan offers the world’s best and most comprehensive content security solution for web and email traffic. Integrating Finjan’s patented application-level behavior blocking technology with best-of-breed anti-virus, URL filtering and anti-spam engines, these layered solutions provide enterprise and SMB users with Day-Zero protection against malware attacks, both known and unknown.

Finjan’s security approach is to provide multiple lines of defense, where each line employs different tools and technologies, in order to detect and block active content that does not adhere to pre-configured security policies.
Lines of defense at the corporate network include:

- At the corporate gateway - proactive content analysis and blocking of malicious code, including complex threats, and filtering by origin (source) and by digital code signatures.
- At the user’s desktop - detection of start/stop events of active content objects in the system; runtime monitoring of active content object activities at the operating system level; runtime monitoring of Java Applets at the Java Virtual Machine level; ability to control (kill or restrict) running active content objects; and filtering based on active content hash code and URL.

**Spyware**

Spyware is any program that aids in gathering information about a person or organization without their knowledge. Secretly installed spyware can subject your company and your employees to invasions of personal privacy, loss of confidential information, performance degradation, network congestion, and reduced productivity.

Finjan’s Vital Security™ proactive security solutions effectively combat spyware and adware using multiple lines of defense at the gateway and the desktop, where each line employs different security tools and technologies, to detect and block active content that does not adhere to pre-configured security policies. Finjan’s comprehensive security solutions utilize its patented Behavior Blocking technology, which detects malicious or inappropriate content and blocks such content the first time it strikes.

The key advantage of Finjan’s patented solution lies in its ability to proactively scan code coming from the Internet, profile the code to determine what operations it may attempt to perform, and proactively block code that attempts to perform operations that are not allowed according to the predefined policy.

The following specific features in Finjan’s products are used to combat spyware effectively:

- Block silent installations of hostile content that are made during web browsing. The aim here is at identifying and blocking malicious mobile code, which is embedded in HTML (VBS, JS, ActiveX, HTML extensions etc.).
- Block access of spyware to local information, files, user details, properties and registry. This prevents spyware from being able to accumulate data and information that the spyware is interested in.
- Block access of spyware to remote computers and servers. This prevents spyware from sending back spied information that may be obtained from local computer.
- The combination of the above, allows Finjan solution to proactively prevent spyware from collecting information and sending it back to its home base. This is done to known and unknown spyware, i.e., Finjan’s solution is capable stopping activities performed by spyware that existing Anti-Spyware solutions do not yet recognize.
- Detect web accesses made by installed spyware utilities by identifying the “home base” servers they contact. This is performed by integrating best-of-breed URL-filtering engines (SurfControl and SmartFilter).
- Scan all content for known spyware signatures using a third-party anti-virus integrated in Finjan solution. Finjan offers both McAfee and Sophos as best-of-breed anti-virus solutions.
By proactively preventing malicious operations, such as remote code execution, using patented real-time behavior monitoring technology and centrally managed security policies, Finjan’s Vital Security™ solutions protect users from the Scob and WebMoney Trojans, as well as other malicious mobile code attacks traveling via the Internet, e-mail, peer-to-peer (P2P) applications, Instant Messaging applications, IRC, etc., without the need to frequently download patches or updates.

**Phishing**

One of the fastest growing scams on the Internet, phishing uses social engineering techniques, such as spoofed emails and fraudulent websites, to trick recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. Phishing attacks send emails that appear to be from a bank or other legitimate institution, asking the user to provide personal details. The email usually contains a link to an online form, branded to look exactly like the organization's website. In many cases, the user might never be aware that his/her details have been stolen. Recent examples of phishing attacks include IPSpoof-B and Exploit-URLSpoof.

Exact statistics on the number of phishing attacks are difficult to ascertain. There is a general consensus that these attacks have dramatically increased since their emergence in mid 2003. The Anti-Phishing Working Group (APWG) reported a 50% average monthly growth rate of phishing attacks through July 2004. The number of monthly unique phishing attacks is shown in the chart below:

![Monthly Unique Phishing Attacks](chart.png)

The following specific features in Finjan’s Vital Security™ solutions are used to combat phishing:

**Email Level:**

- Scanning of emails for known Internet Explorer vulnerabilities, hackers tricks and other malicious behavior (examples: <object Data, URL Spoofing, IFrame bugs, etc.).
- 3rd party anti-virus engine blocks these exploits without checking the content of the emails.
- Known phishing emails will be also labeled as spam.
- Anti-fraud detection of the Anti-spam engines.
Web Level:

- Scanning for code that is capable of replacing the web browser address bar with a fake one, including malicious JavaScript and Java applets, and proactively blocking such attempts.
- 3rd party URL Categorization engine is used to label known phishing sites under "hacking", and block them if defined. However, this is a temporary solution since phishing sites are typically brought down soon after the emails are sent.
- If the fraudulent site also contains malicious code (e.g., Trojan, spyware) inside the web pages, such code will be detected and blocked by Finjan’s solution.

A harmless demo of the well-known phishing attack against Citibank can be found on Finjan’s website: [http://www.finjan.com/mcrc/demos/fakeaddress/](http://www.finjan.com/mcrc/demos/fakeaddress/). Finjan’s Vital Security™ identifies the JavaScript that tries to capture personal information and blocks it as illustrated in the screen below:
**Blended Threats – Viruses, Worms and Trojans**

A blended threat is an attack using multiple methods and technologies to infect or propagate to other systems and networks, resulting in high and extremely rapid compromise of millions of systems.

Bugbear, one of the more complex worms that appeared in September 2002, emails itself to addresses found on the infected system (this technique is called "mass mailing"), copies itself through network shares, leaves a file for later execution (Trojan) for propagating through remote access, logging key strokes for getting other systems' passwords, and finally, changing its shape with each infection ("polymorphic").

The Nimda virus (that appeared in late 2000) is considered very sophisticated, employing five different methods for replicating and infecting systems, including email, JavaScript execution (while web browsing) and network shares. The Win32.Livra.A Trojan seen in the beginning of 2003, used mass-mailing to propagate, as well as shared folders, instant messages, KaZaa peer-to-peer networks, and IRC (Internet Relay Chat). The Sobig worm (January 2003) used a built-in SMTP client and network shares to spread.

Finjan’s Vital Security™ solutions proactively detected and blocked 100% of the viruses in the monthly Sophos top 10 lists in 2004, as well as all of the worms (e.g., Sasser, Scob and MyDoom) appearing in McAfee’s listings for 2004. **Finjan stopped these viruses before the anti-virus vendors even knew they existed!**

**Finjan Vital Security™ Solutions**

Finjan products close the Window-of-Vulnerability™ — the period of time spanning from when a new virus outbreak first occurs, until an anti-virus update is delivered. Traditional anti-virus software leaves enterprises and SMBs exposed and vulnerable for hours and frequently for days, before a signature update is delivered. Instead of relying on reactive database updates, Finjan provides proactive, real-time protection against new virus outbreaks and malicious code with the patented behavior blocking technology available in its Vital Security™ and 1Box™ solutions.

Integrating Finjan’s patented behavior blocking technology with best-of-breed anti-virus (McAfee®, Sophos®), URL filtering (SurfControl®, Secure Computing®) and anti-spam (Mailshell™) engines, Finjan’s layered solution provides enterprise users with superior protection against malicious and inappropriate content. Finjan’s integrated solution presents customers with a highly effective “all-in-one” solution, reducing businesses’ total cost-of-ownership. **Finjan’s Vital Security™ solutions are transparent to enterprise users, providing unsurpassed security without compromising work productivity.**

Utilizing its unique application-level behavior blocking technology, Finjan provides security solutions that are optimized for both enterprises (250 up to an unlimited number of users) and SMBs (up to 250 users).

Finjan’s products are currently being used by well-known enterprises with between 1000 to more than 200,000 users.
**Vital Security™ for Enterprises**

Finjan offers a wide range of solutions via ready-to-use appliances, as well as software packages:

- **Vital Security™ for Web** implements the gateway line of defense for HTTP and FTP traffic. It scans HTML and active content objects at the gateway, away from critical resources, in order to develop a behavior profile. Active content objects with profiles that do not reconcile with the enforced security policy are not passed to the requesting browser. This product integrates best-of-breed anti-virus (McAfee or Sophos) and URL filtering (SurfControl or SmartFilter) engines.

- **Vital Security™ for SSL** implements the gateway line of defense for SSL/HTTPS traffic. Vital Security for SSL decrypts SSL traffic and makes it available for malicious code scanning by Vital Security for Web or other third-party software programs. Encrypted content is secure from eavesdropping but may carry malicious content (e.g., webmail).

- **Vital Security™ for E-Mail** implements the gateway line of defense for SMTP and POP3 traffic and performs the same type of content inspection performed by Vital Security for Web. This product integrates best-of-breed anti-spam (Mailshell) engine.

- **Vital Security™ for Clients** implements the desktop line of defense and is particularly suitable for laptop users connecting to the Internet from outside the enterprise network. It integrates with the operating system, detecting active content as it begins to run, monitoring it during runtime and enforcing its security policy.

**Vital Security 1Box™ Series for Small and Medium-Sized Businesses**

- **Internet 1Box™** is the ultimate security solution for web and email at the gateway and desktop. This easy-to-use product combines Finjan’s Behavior Blocking technology with best-of-breed anti-virus, URL filtering and anti-spam engines in a single box. Providing enterprise-level security at a price affordable for SMBs, Internet 1Box™ represents a tremendous value for money.

- **SSL 1Box™** extends the Internet 1Box™ capability to protect against threats arriving via SSL/HTTPS encrypted content as well as enforcing SSL certificates according to the corporate policies. When implemented together with Internet 1Box™, these products deliver the only solution on the market capable of detecting a new unknown attack arriving via HTTPS/SSL, HTTP and FTP.

- **Documents 1Box™** provides a secure environment for sharing documents within organizations and with partners or customers. Based on pre-defined corporate policies, it protects against unauthorized access, saving, copying, forwarding, printing, or screen-capturing of confidential documents.
Conclusion

The increasingly sophisticated nature of malware attacks, including blended threats, necessitates highly advanced security capabilities beyond those provided by traditional anti-virus or intrusion protection solutions, which are reactive in nature.

In light of this new generation of attacks, enterprises require highly intelligent security solutions that block malicious or inappropriate content before it enters their networks and infects their computers. Finjan’s behavior-blocking technology is the only solution on the market that can identify the “true” behavior of malicious code and protect against unknown threats the first time they strike; before they reach any computer in the network.

About Finjan Software

Finjan Software is the leading provider of proactive, behavior-based secure content management solutions, protecting more than 3 million users from attacks. Finjan uses its Vital Security™ platform to determine actual code behavior and blocks any action that violates predefined security policy, and therefore surpasses the levels of defense typically offered by reactive anti-virus software solutions. This superior technology enables Finjan to protect users proactively by responding to existing, and more importantly, yet to be developed attacks. Analyst firm IDC, recognizes Finjan as the leader in the worldwide malicious mobile code security market. For more information, visit http://www.finjan.com.