

## Security Audit – Media Company

### Introduction

This analysis is based on a security audit performed during the 3<sup>rd</sup> quarter of 2008 for a media company. Live Internet access information was gathered during a period of 3 months and was based on the surfing activities of 10,000 users.

Finjan's RUSafe™ appliances were installed using a default security policy with Finjan patented Active Real-Time Content Inspection with add-on modules of Anti-Virus and URL filtering enabled. RUSafe sniffs live traffic from the switch, scans the content using Finjan's real-time content inspection technologies, and generates summary-level and detailed-level reports which specify the magnitude and type of malicious content detected by the appliance. Due to its sniffer-based nature, Finjan RUSafe did not terminate if Web traffic found included *potential* risks.

The resulting log files were analyzed by experts from Finjan. Their main findings are presented below.

### Key Findings

Table 1 displays the key findings detected by Finjan Technology.

Business Risks	Violations Count	Business Risk
Potential legal liability	<b>485,903</b>	Critical
High-risk websites	<b>135,852</b>	Medium
Potential data breach	<b>514,394</b>	Critical
Spyware / Adware	380,048	Critical
Code Obfuscation	523	Critical
3 <sup>rd</sup> party software vulnerability	133,770	Critical
Viruses	53	Low

**Table 1 - Key Audit Findings**

#### Potential legal liability

This group displays website categories accessed by users that might have exposed their companies to legal liability issues. These categories include: Violence, Adult/Sex, Criminal Skills and Weapons (as detected by URL Filtering engine)

*Misuse of internet resources at work may result in financial consequences*

#### High-risk websites

This group consists of website categories that pose a high risk when accessed by users. These website categories are marked as high-risk because they may include crimeware and malware trying to infiltrate corporate networks and steal data.

### Potential Data Breach

This group incorporates potentially malicious websites that were accessed by users. The business risk of visiting these sites is significant, since confidential data can be stolen and used by hackers (medical information, email communication, user/password information, disclosing private information, disclosing confidential data to competition).

#### *Data Breach Could Lead to Class Action Lawsuit*

- Finjan Secure Web Gateway **has detected more than 60 cases of usage of shell commands (Shellcode)**. Shell commands are frequently used by attackers to control compromised machines and steal sensitive information.
- **Finjan Secure Web Gateway has detected more than 380,000 incidents of Spyware and Spyware sites which were accessed by users:** this group of incidents includes known Spyware objects and Spyware website categories that were accessed by users. These websites categories are known to include Spywares to track user's online activity.
- **Finjan Secure Web Gateway has detected ~510,000 incidents of websites accessed by users containing potentially malicious code - exploiting 3rd party software:** Although businesses patch their operating system when leading vendors (such as Microsoft) issue security updates, most of these companies fail to apply security updates of 3rd party applications used by their end-users (e.g. WinZip, Apple Quick Time, Adobe Acrobat). Hackers are taking advantage of these vulnerabilities to execute Crimeware on end-users' PCs.
- **Finjan Secure Web Gateway has detected more than 500 incidents of websites accessed by users with potentially malicious code which was obfuscated:** Cybercriminals are using dynamic code obfuscation techniques in order to hide the malicious code itself and execute it dynamically. This way, they increase the probability of bypassing traditional security products (e.g. antivirus) and accomplish their attacks successfully.
- **Viruses: ~50 incidents of known viruses were detected by 3<sup>rd</sup> party Anti-Virus application.**

According to a survey conducted by Finjan conducted during July 2008, 73% of responding **CIOs and CSOs** were **more concerned about data theft** (Crimeware stealing their business data) **than about downtime and loss of productivity** due to virus infections ([Finjan Web Security Survey,2008](#))

## Detected Attack Techniques

### Evasive Techniques

Cybercriminals quickly realized that in order to avoid detection by URL filtering or reputation services products, they need to avoid detection by deploying several new techniques, such as:

- Storing IP addresses of web crawlers in their attack databases. This method enables cybercriminals to serve legitimate content to these Web crawlers while serving malicious content to all other website visitors. Since these Web crawlers are the main feed for updating URL filtering and reputation services databases, the result is a false rating or categorization of infected websites.
- Using random webpage names. This method prevents „black listing“ of malicious pages. Each time users visit an infected site; a new unique URL is created and served dynamically ([Malicious Page of the Month, Jan 2008](#))
- Code obfuscation. This method “breaks” anti-virus signatures to avoid detection.

Evasive techniques including Fragmentation, Substitution, Escape Characters and Obfuscation are used to disguise the appearance and intent of the code.

These types of attacks **were detected by Finjan Patented Active Real-Time Content inspection** technology and **bypass Anti-Virus engines**

### Compromised Legitimate Websites

Finjan’s patented Active Real-Time Content Inspection technology has detected cases of legitimate website which served malicious code.

In a recent report by Sophos, an average of **more than 15,000 newly infected webpages** are detected each day; the majority of these poisoned webpages (**79%**) are found **on legitimate** websites that have been hacked (Sophos Security Threats Report, Q1 2008).

According to Websense “Compromises and misuses of legitimate Web sites **make reputation security systems much less effective**”

**Traditional security solutions are limited in handling such incidents.**

## Conclusions

During this audit, a significant number of incidents presenting potential data breaches were detected by Finjan's RUSafe. Different attack vectors were used. **Only a small proportion of web-based malware was detected by traditional anti-virus engines.**

"Organizations are increasingly demanding Secure Web Gateway solutions that go beyond traditional URL filtering to **provide real-time inspection of malicious Web content** and granular Web application control." (Lawrence Orans, research director at Gartner)

"The Web Has Changed ... Reputable Websites are becoming compromised and used to distribute malicious code ... Categorizing Web 2.0 is nearly impossible task ... Static URL Databases are increasingly ineffective" (Mark Guntrip, Websense, June 2008)

To prevent Crimeware and other highly sophisticated Web-borne threats, an *additional* security layer is needed. Today's evasive Crimeware attacks cannot be successfully stopped by only using 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 used by today's cybercriminals are best handled by *real-time content inspection techniques*. The best option for enterprises is to adopt a *multi-layered* approach. Such an approach ideally consists of both real-time and reactive (such as signature-based) IT security technologies.

Finjan's anti-Crimeware technology incorporates real-time code inspection. It therefore achieves one of the highest rates of malicious code detection with the lowest false-positives available. Finjan's secure Web gateway solution analyzes each and every piece of Web content in real-time regardless of its original source. It understands potential effects *before* it has a chance to execute the end-users' machines. 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 currently popular among cybercriminals. This prevents any malicious Web content from entering the corporate network, thus effectively protecting enterprises from Crimeware that may result in severe business damage.