

## Security Audit – Manufacturing Company

### Introduction

This analysis is based on a security audit performed during the 4<sup>th</sup> quarter of 2008 for a manufacturing 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	591,710	Critical
High-risk websites	92,371	Medium
Potential data breach	109,267	Critical
Unknown Potential Malicious Code	53,571	Critical
Spyware / Adware	26,116	Critical
Code Obfuscation	20,907	Critical
3 <sup>rd</sup> party software vulnerability	8,536	Critical
Viruses	137	Medium

**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 with its patented technology has detected more than 53,571 incidents of malicious code which has being unknown at the time of detection** for example: malicious binary files (e.g. ActiveX, Java Applets, Executables), binary exploits in textual files, malicious scripts, exploit codes before an AV signature was available, etc.
- **Finjan Secure Web Gateway has detected more than 26,116 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 more than 20,907 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.
- **Finjan Secure Web Gateway has detected 8,536 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.
- **Viruses: ~137 incidents of known viruses were detected by 3<sup>rd</sup> party Anti-Virus application.**

## Data Breach Attack

During the audit, Finjan Secure Web Gateway detected and logged an attack which caused serious data breach. Company employees' information was uploaded to external web server maintained by cyber criminals.

Cybercriminals quickly realized that in order to avoid detection by traditional security solutions, they need to avoid detection by deploying several techniques by distributing malicious code on legitimate websites to bypass URL categorization solutions that allow access to these sites or by using obfuscating their malicious code to avoid detection by signatures of Anti-Virus solutions).

The described incidents, cybercriminals created malicious script exploiting 3<sup>rd</sup> party product vulnerability (patched by the vendor more than 3 years ago) however, still managed to bypass traditional security solutions. The malicious code managed to download Trojan. The Trojan uploaded employees' information to cyber criminals' server. The Trojan uploaded user's data as site visited, searches performed, credentials used, etc.

These types of attacks **were detected by Finjan Patented Active Real-Time Content inspection** technology and **bypass traditional security solutions**.

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](#))

Malicious Code Research Center outlook for 2009 ([Web Security Trends Report Q4/2008](#)), in terms of cybercriminals stealing valuable data, **the focus will remain on leveraging Trojan technologies since Trojans enable cybercriminals maximum flexibility in terms of command and control**.

## Conclusions

During this audit, 76% of incidents presenting potential data breaches were detected by Finjan's patented technologies. Different attack vectors were used. **Only a small proportion (24%) of web-based malware which potentially causes data breaches, was detected by traditional security technologies.**

Traditional security solution (antivirus, URL filtering, reputation technology) are limited to cope with the sheer volume of new and sophisticated malware being developed by cybercriminals:

- "In the antivirus business, we have been lying to customers for 20 years, people thought that virus protection protected them, but we cannot block all viruses" Eva Chen – CEO of Trend Micro.
- "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 highly sophisticated 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.