

Security Audit – Government Agency

Introduction

This analysis is based on a security audit performed during the 1st quarter of 2009 for a government agency company. Live Internet access information was gathered during a period of 1 week and was based on the surfing activities of 6000 users.

Finjan's RUSafe™ appliances were installed as sniffers in a network using a default security policy utilizing Finjan patented Active Real-Time Content Inspection. Finjan 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 type of malicious content detected by the appliances.

The resulting log files were analyzed by experts from Finjan. Key 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	22,742	Critical
High-risk websites	33,188	Medium
Potential data breach	219,125	Critical
Spyware / Adware	210,015	Critical
Malicious Code	5,950	Critical
3 rd party software vulnerability	3,109	Critical
Viruses	51	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 has detected more than 210,015 incidents of Spyware, Spyware sites and adware 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 with its patented technology has detected more than 5,950 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 3,109 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: ~51 incidents of known viruses were detected by 3rd party Anti-Virus application.**

Summary

79% of the security incidents of potential data breaches were detected by Finjan's patented technologies. Different attack vectors were used. Only a small proportion (20%) of web-based malware which potentially causes data breaches, was detected by traditional security technologies.

76% of incidents presenting as high-risk websites were attempts to use proxy avoidance tools to bypass installed security technologies. By using proxy avoidance tools, employees (internal users) are trying to hide their internet activities and surfing habits and to access improper sites which may result in financial or legal consequences

Several 'Zero Day' viruses detected by Finjan core technology, before antivirus signatures were available

Evidence of workstations being compromised by highly sophisticated Trojan (Drive-By Trojan) which was hosted on legitimate web sites (e.g. travel sites). The functionality of these types of Trojans includes the ability to run arbitrary commands, monitor user and system activity, operate an HTTP proxy, make changes to the system registry and perform denial-of-service attacks.

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 (ZDNet.co.uk, 30-Jun 2008)
- "Given that malicious software (malware) filtering is a key requirement, products must offer proactive "zero day" malware detection techniques that do not rely on previous knowledge of the malware (Gartner, Magic Quadrant for Secure Web Gateway, Sep 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.