

Security Audit – Retail Company

Introduction

This analysis is based on a security audit that was performed during the 2nd quarter of 2008 for a retail company. Live Internet access information was gathered during a period of 2 weeks and was based on the surfing activities of 10,000 users.

Finjan's RUSafe™ was installed using a default security policy. 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 that was 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 Secure Web Gateway solution.

Category	Violations Count	Business Risk
Websites accessed by users that pose (potential) legal liability	709,348	Critical
High-risk website categories accessed by users	20,643	High
Potentially malicious sites that were accessed by users	143,784	Critical
Spyware & Spyware sites accessed by users	33,633	High
Websites accessed by users with potentially malicious code - exploiting 3rd party software	42	High
Websites accessed by users with potentially malicious code – obfuscated	55,925	High
Viruses	47	Medium

Table 1 - Key Audit Findings

Websites accessed by users that pose (potential) legal liability

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

High-risk website categories accessed by users

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

Potentially malicious sites that were accessed by users

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.

During this audit more than 100 cases of usage of shell commands (Shellcode) were frequently used by attackers which enabled them to control compromised machines and steal sensitive information.

Spyware and Spyware sites accessed by users

This group 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.

Websites accessed by users with potentially malicious code - exploiting 3rd party software

The audit also found that these malicious websites are exploiting vulnerable applications used by the end-users (systems/browsers vulnerabilities). 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 their end-users' PCs.

Websites accessed by users with potentially malicious code – obfuscated

This group displays in great detail one of the major risks for any business working online. Dynamic code obfuscation techniques are the latest salvo from hackers in their constant battle of wits against security vendors. In response to security vendors' efforts to detect encrypted malicious code, hackers have developed dynamic code obfuscation techniques, which basically scramble malicious code in a different way each time a new visitor enters the malicious website.

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.

During the audit, around 56,000 instances of obfuscated code (table 1) were detected by Finjan's RUSafe.

Viruses

This category includes blocked pages which contained known viruses that were detected by an up-to-date 3rd party Anti-Virus application.

Figure 1 show how malicious websites which were detected by Finjan real-time content scanning and were categorized as legitimate websites by URL Filtering system.

URL filtering is an effective way to enforce corporate policy and enhance productivity by blocking non-productive sites. However, URL Filtering is limited in detecting and blocking web based threats.

Sophisticated cybercriminals are taking advantage of the weak spots of reactive database technologies.

In a recent report by Sophos, an average of **more than 15,000 newly infected web pages** are detected each day, the majority of these poisoned sites (**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**”

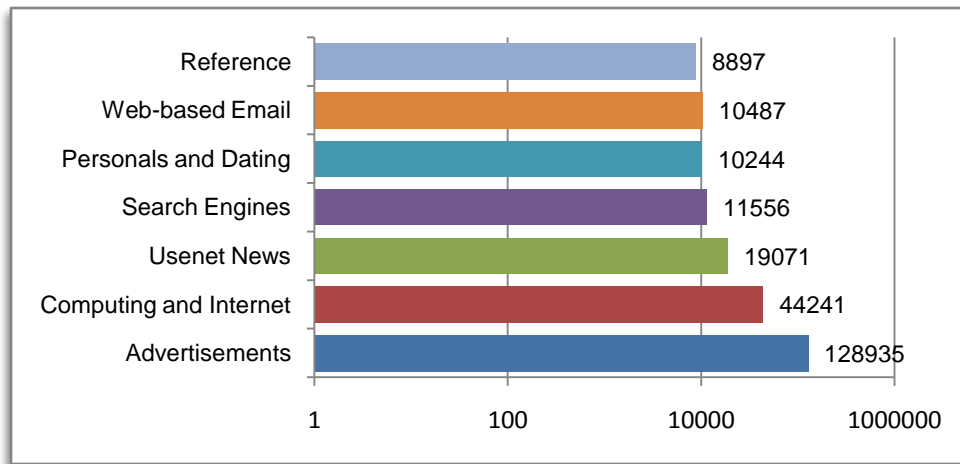


Figure 1 - Malicious websites are categorized as legitimate by URL Filtering

Conclusions

During this audit, a significant number of Trojans and malicious scripts were detected by Finjan's RUSafe. The detected malware is capable of remote code execution, arbitrary code execution, file and network access and performing other activities.

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 rate 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.