

Security Audit – Financial Institution

Introduction

This analysis is based on a security audit that was performed during the 3rd quarter of 2007 for a financial organization. Live Internet access information was gathered during a period of one business day and was based on the surfing activities of 45,000 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. Having its sniffer-based nature, Finjan RUSafe did not terminate Web traffic that was found to include potential risks.

The log files were then analyzed by experts from Finjan's Malicious Code Research Center (MCRC). The main findings are presented below.

Key Findings

Table 1 displays the key finding detected by Finjan RUSafe sniffer.

Category	Violations Count	Business Risk
Zero-day attack infiltrated the network	1	Critical
Websites accessed by users that pose legal liability	3,604	Critical
High-risk website categories accessed by users	3,462	High
Adware and Spyware sites accessed by users	15,190	High
Potentially malicious sites that were accessed by users	1,210	High
Websites accessed by users with potentially malicious code – obfuscated	760	High
Websites accessed by users with potentially malicious code – exploiting 3rd party software	1	Medium

Table 1- Key Audit Findings

Zero-day attack infiltrated the network: **Zero day** attack indicates on a vulnerability that is already exploited in the wild which was not patched by the vendor. As a result, the business has no way to protect itself from such an attack as no signature or patch exists.

Websites accessed by users that pose legal liability: This group displays website categories accessed by users that might have exposed the company to legal liability issues having users watching content from these sites. The categories include: Violence, Adult/Sex, Criminal skills and Weapons

High-risk website categories accessed by users: This group displays website categories with high-risk that were accessed by users. These website categories are marked as high-risk because they may include crimeware and malware trying to infiltrate the network to steal data

Adware and Spyware sites accessed by users: This group displays known Adware and Spyware website categories that were accessed by users.

Potentially malicious sites that were accessed by users: Potentially malicious websites accessed by users. The business risk for visiting these sites is significant as confidential data can be stolen and used by hackers

Websites accessed by users with potentially malicious code – obfuscated: Obfuscated code is a source code that is very hard to read and understand. This can be done in various ways, such as using encryption, or by adding extra tabs, random comments etc. The main legitimate reason someone might want to do this is to prevent reverse engineering. Code obfuscation also works for malicious code writers who want to hide or disguise their code's true purpose.

Websites accessed by users with potentially malicious code – exploiting 3rd party software: Malicious websites accessed by users. The audit found that these malicious websites are exploiting vulnerable applications used by the user. Although businesses patch their operating system when the vendor issues a security update, most of these businesses fail to apply security updates of 3rd party applications used by their users (e.g. WinZip, Apple Quick Time, Adobe Acrobat etc.). Hackers are taking advantage of such vulnerable application to execute Crimeware on the end user PC

Figure 1 displays malicious website distribution by geographic locations, demonstrates a study conducted by Finjan's Malicious Code Research Center which specified that the majority of malicious websites are hosted in the United States (see [Finjan Web Security Trend Report Q1 2007](#))

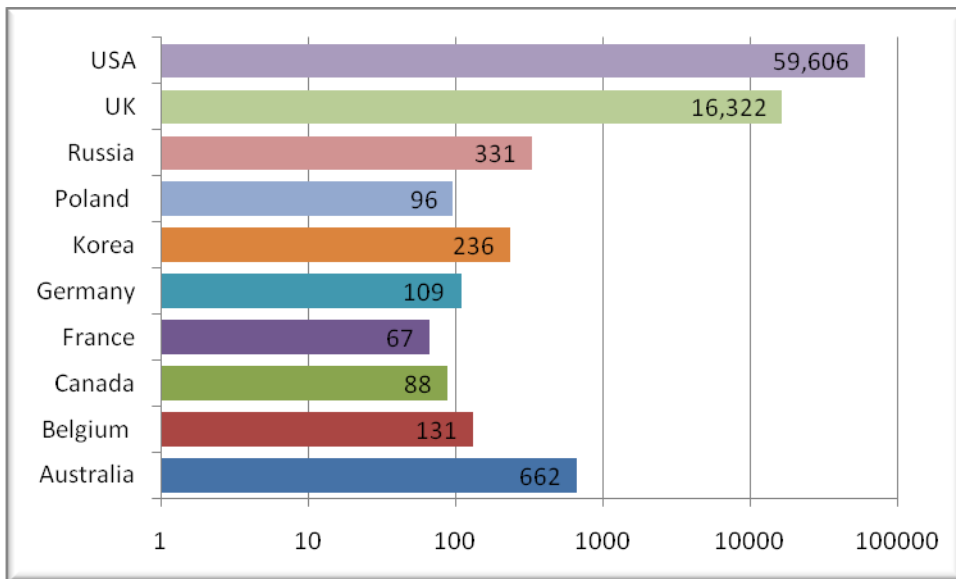


Figure 1 - Geographic Distribution of Malicious Code

Zero Day Attack:

As part of the audit, an instance of Zero-Day attack was detected. Zero-day attack is a newly discovered software security flaw, before the software vendor has made a fix available.

The [Microsoft DirectX Media SDK Vulnerability](#) which was not patched by the software vendors (Adobe and Microsoft) during the audit period were proactively detected by Finjan RUSafe. Finjan's customers are proactively protected against this vulnerability due to the real-time content scanning technology.

The attack was delivered while using two techniques that have emerged as the latest trends in the web security field: evasive technology, and exploitation of un-categorized websites (from the URL categorization stand). The malicious code has been hosted on a domain that all major URL categorization vendors have classified as benign (or failed to classify), and the code had the evasive characteristics described in the [Q2-2007 Web Security Trends Report](#) published earlier by Finjan.

Conclusions

To prevent crimeware and other highly sophisticated web-borne threats, an additional security layer is needed. Today's evasive crimeware attacks pose a significant challenge to 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 being used by today's cybercriminals can be stopped by real-time content inspection techniques. Therefore, enterprises should adopt a multi-layered approach, typically involving both real-time security, as well as reactive (e.g., signature-based) IT security technologies for stopping traditional threats.

Finjan's anti-crimeware with real-time code inspection technology achieves the highest rate of malicious code detection with the lowest false-positives. Finjan's secure web gateway solution analyzes each and every piece of web content in real-time, regardless of its original source, and understand its potential effects before it executes on the end user machine. 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 in use. This prevents any malicious web content from entering the corporate network, protecting enterprises from crimeware that may result in severe business damage.