

Security Audit – Insurance Sector

Introduction

This analysis is based on a security audit that was performed by Finjan during Q4/ 2007 for an insurance company. Live Internet data traffic, based on the surfing activities of 20,000 users, was gathered over a period of 4 weeks.

Finjan’s Vital Security™ Web Appliance, a Secure Web Gateway, was installed at the corporate network. The appliance inspected all incoming and outgoing Web users’ activities.

Following the 4 week-audit, the experts at Finjan’s Malicious Code Research Center (MCRC) analyzed the product log. Their main findings are presented below.

Key Findings

Table 1 displays the key findings detected by Finjan’s Vital Security™.

Category	Violations Count	Business Risk
Websites accessed by users violating company’s policy	96,240	Critical
Zero-day attack attempted to infiltrated the network	1	Critical
Websites accessed by users with potentially malicious content	18,635	High
Websites accessed by users with potentially malicious code exploiting vulnerabilities of 3 rd party’s product (WinZip, QuickTime, AIM etc.)	8,680	High
Websites accessed by users with obfuscated malicious code	1,008	High
Spyware Objects	202	High
Viruses	433	Medium

Table 1 - Key Audit Findings

The key audit findings are grouped in seven major categories that are explained below.

Websites accessed by users violating company's policy

This category displays websites accessed by users that are defined as *prohibited* by the company. Accessing these websites violate company policy.

Zero-day attack attempted to infiltrate the network

Zero day attack indicates on a vulnerability that is already exploited "in the wild" and was not patched by the vendor. As a result, the company has almost no way to protect itself from such an attack since no signature or patch exists.

Finjan's Vital Security™ stopped this attack from entering the corporate network, and thus prevented serious criminal activities from taking place against the organization.

Websites accessed by users with potentially malicious content

This category displays malicious code detected by Finjan's patented real-time content inspection technology:

- **Potential Malicious Binary files**
Malicious or potential malicious ActiveX, Java Applets and Executables
- **Malicious Scripts**
Malicious behavior detected in scripts
(file system operation, registry operation)
- **Potential Malicious Files**
Blocked files considered as potentially malicious based on true-type detection such as suspicious file types and spoofed executable files

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 obfuscated malicious code

[Obfuscated code](#) is a source code that is purposely very hard to read and understand. This can be achieved in various ways, including using encryption or adding extra tabs, random comments, etc.

The main *legitimate* reason for obfuscating code in to prevent reverse engineering.

However, code obfuscation also works for *malicious* code writers who want to hide or disguise their code's true purpose from anti-virus signatures.

Spyware objects

This category displays known spyware objects that were detected on websites accessed by end-users:

- Attempt to download known Spyware
- Attempt to access websites that try to execute Spyware applications

Viruses

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

The following graph displays malicious website distribution by geographic location

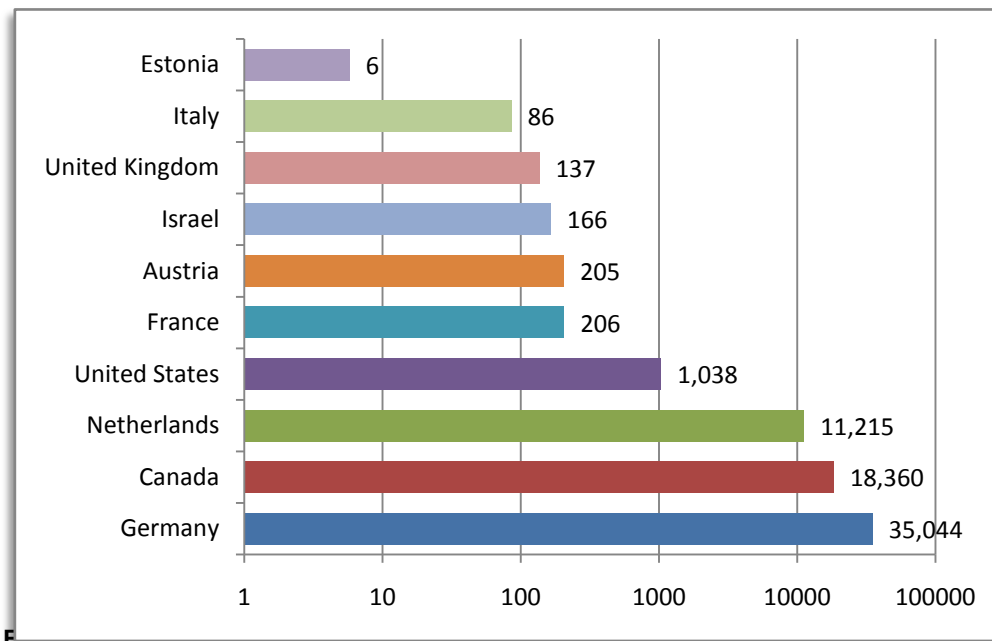


Figure 2 - Geographic Distribution of Malicious Code

Zero-Day Attack

As part of the audit, the occurrence of a zero-day attack was detected.

A zero-day attack is defined as a newly discovered software security flaw, for which no patch was provided yet by the software vendor.

The logs show a page that was blocked by Finjan despite the fact that the latest hacking techniques were applied:

1. Usage of Google cache to deliver malicious code.
Accessing the site in Google cache to bypass URL filtering and reputation services detection.
(For more information on this topic, please refer to [Web Security Trends Report - Q3/2006](#))
2. Dynamic code obfuscation to bypass Anti-virus detection.
(For more information please refer to [Web Security Trends Report - Q4/2006](#))
3. A **zero-day attack on a common 3rd party software component offered by Apple** allows remote attackers to execute arbitrary code on the end-user's PC and install Trojans.
This code was not patched by the software vendors during the entire audit. During the audit period this code was proactively detected and blocked by Finjan Secure Web Gateway.
4. Installation of a Crimeware.
In this case a Bank-Trojan to collect online banking data as well as user's files
(For more information, please read our press release "[When Trojans Go Phishing – 500,000 Users Already Infected](#)")

When decoding the obfuscated code, it was revealed that:

5. Attackers made usage of a Crimeware toolkit called *NeoSploit* to manage the malicious code.
6. The malicious code contained exploits for several vulnerabilities, among them the zero-day vulnerability.
7. Upon successful execution of the exploit, a Bank-Trojan is downloaded and installed on the end-user machine:
 - The Trojan "phones home" to get commands from the attacker/criminal.
 - Information regarding the logged-on user and his infected PC are being sent over an encrypted connection to the attacker.
 - The Trojan monitors files and Web-browsing activities and sends the collected information to the hacker.
 - The Trojan collects credentials for online banking applications that the user is using. These credentials are sent to the hacker who controls the sites.

It is imperative to understand that this attack took place as part of *standard* usage of the Internet by company employees.

This attack was successfully detected and stopped in real-time by Finjan Vital Security™ technology.

If such an attack would have taken place in an organization that does **not** have the adequate protection from such Web-borne threats, such an attack could have resulted in grave financial loss and identity theft.

Conclusions

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.