

Security Audit – Financial Institute

Introduction

This analysis is based on a security audit that was performed during the 1st quarter of 2008 for a financial institute. Live Internet access information was gathered during a period of 2 weeks and was based on the surfing activities of 2500 users.

Finjan's Secure Web Gateway was installed using a default security policy in an X-Ray mode to detect crimeware. X-Ray Mode allows enterprises to test the affect of new rules within the live Web traffic environment, and monitor the effects before actually applying a new rule. This approach enables 'what if' scenarios to be modeled, and the effects of different rule variations to be measured.

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 Secure Web Gateway.

Category	Violations Count	Business Risk
Websites accessed by users that pose legal liability	38,994	Critical
High-risk website categories accessed by users	5,578	High
Potentially malicious sites that were accessed by users	1,127	Critical
Adware and Spyware sites accessed by users	1,031	High
Websites accessed by users with potentially malicious code – obfuscated	1,746	High

Table 1- Key Audit Findings

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 (as detected by URL Filtering engine)

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 your network to steal data

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

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

Websites accessed by users with potentially malicious code – obfuscated: This group displays, in great details, 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 security products and accomplish the attack successfully.

During the audit, more than 1,700 instances of obfuscated code (table 1); it was found that in a specific attack, the cybercriminal used several different types of vulnerabilities. The use of several vulnerabilities is to assure the infections of the victim machine. Successful exploitation yields the downloading and running of a crimeware Trojan on the victim machine.

Figure 1 shows how malicious websites were categorized 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 percent** – 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**"

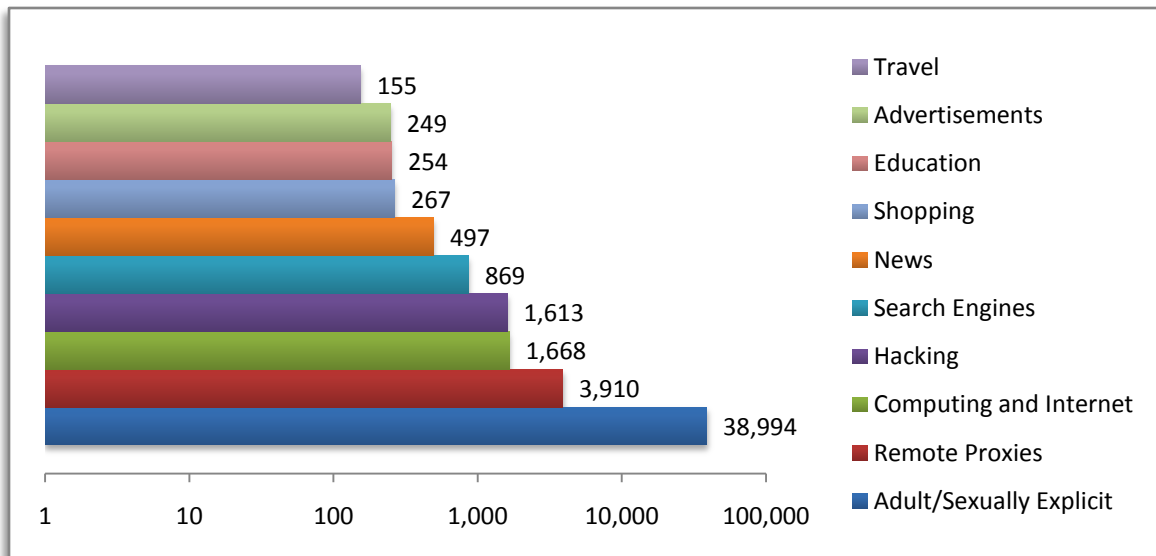


Figure 1 - Categorization of Malicious Websites by URL Filtering

Conclusions

Today's cybercriminals are motivated by financial gain, and their main vector of attack has become the Web. They understand too well that signature- and database-reliant solutions are not designed to protect against obfuscated malicious codes served on compromised legitimate sites, Web 2.0 -based attacks, and other dynamic attack vectors that use the Web. These sophisticated Web-based attacks are specifically designed to hit the "blind spots" of traditional security systems that rely on signatures or database (such as anti-virus and URL filtering).

Evasive Crimeware attacks are hard to stop by 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 answer is the use of active real-time content inspection techniques.

More and more enterprises and organizations are looking at a multi-layered approach, consisting of active real-time security and reactive (e.g., signature-based) IT security technologies

Finjan's Vital Security™ with active real-time code inspection technology provides optimal protection against malicious content.

Finjan's secure web gateway solution analyzes each and every piece of web content in real-time, regardless of its original source, and understands its potential effects before it executes itself on the end user machine. By understanding the true intent of web content, Finjan's active 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, thus protecting enterprises from Crimeware that may result in severe business damage.