

## Security Audit – Financial Institution

### Introduction

This analysis is based on a security audit that was performed during the first quarter of 2006 for a financial organization. Live Internet access information was gathered during a period of 2 weeks and was based on the surfing activities of 5,000 users.

Finjan’s Vital Security™ web security solution was installed using a security policy customized to the organization’s specific needs. All content downloaded during this period was scanned by Finjan’s Vital Security™ product.

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

### Main Findings

The following charts and tables display the percentage of each content type that violated the security policy (total of 67,916 instances of code violating the selected security policy).

Figure 1 clearly demonstrates current trends, where Spyware constitutes a major security threat to businesses and organizations.

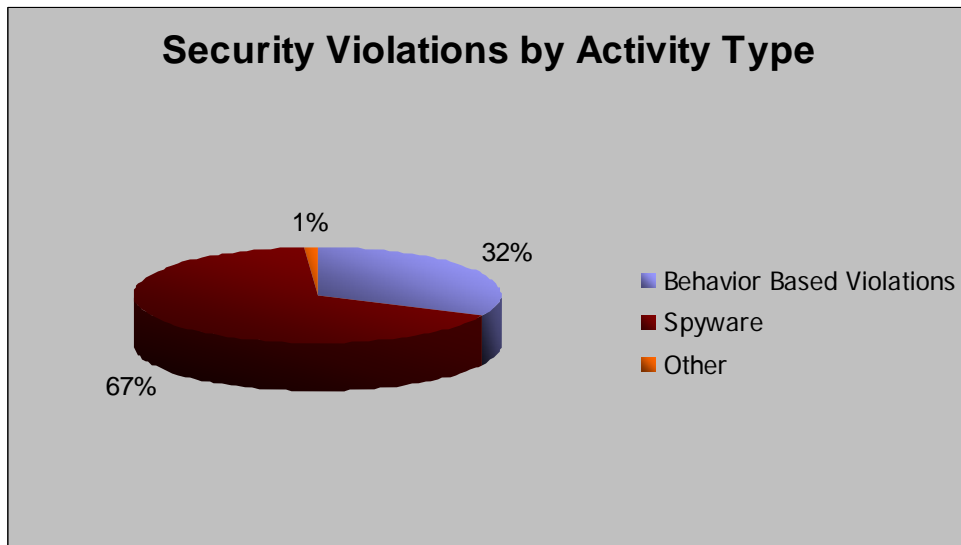


Figure 1

Behavior-based violations comprise:

- Malicious scripts: File system operations, registry operations, operating system operations
- Malicious ActiveX, Java Applets and executables: Get user information, registry access, spoofed file types
- Others

Spyware comprises:

- Known Spyware
- Attempt to access websites which are categorized as Spyware sites
- Attempt to access websites which try to execute Spyware applications
- Others

According to the 2005 FBI Computer Crime Survey, 79.5% of the surveyed organizations reported as having been affected by Spyware at least once during the year.

### Security Violation Breakdown

The following table provides quantitative information regarding the nature of the security violations:

Quantity	Nature of Violation
45,316	Spyware
21,847	Behavior-based violations
559	Known viruses
194	Attempt to exploit operating system or browser vulnerabilities

### Conclusions

Traditional signature-based Anti-Virus products and heuristic-based Anti-Virus products are incapable of preventing complex malicious code attacks which may use multiple propagation techniques.

Since Active Content is being used by legitimate business applications as well as malware, behavior-based gateway security solutions, such as Vital Security™, are required to analyze Active Content in order to determine its true behavior. With Finjan's Vital Security solutions, enterprises can achieve intelligent behavior analysis without compromising the productivity or performance of their users.