

---

## Security Audit - Government Sector

### Introduction

This analysis is based on a security audit that was performed during the 2<sup>nd</sup> quarter of 2007 for a government organization. Live Internet access information was gathered during a period of four weeks and was based on the surfing activities of approximately 20,000 users.

Finjan's RUSafe™ Vital Security™ Sniffer Tool was installed using a default security policy.

All content downloaded during this period was scanned by Finjan's Vital Security™ technology. The log files were then analyzed by experts from Finjan's Malicious Code Research Center (MCRC). The main findings are presented below.

### Main Findings

- **Spyware and Adware:** 27% of malicious behavior content detected during the audit was related to Spyware & Adware, this includes the following violations:
  - Attempt to download known Spyware
  - Attempt to access websites which are categorized as Spyware sites
  - Attempt to access websites which try to execute Spyware applications
- **Malicious Scripts and Binary Content:**
  - **Malicious Scripts** - malicious behavior detected in scripts (File system operation, registry operation) and attempts to exploit systems/browsers vulnerabilities.
  - **Malicious Binary Content** - malicious or potential malicious ActiveX, Java Applets and Executables.
  - **Potential Malicious Files** - blocked files considered as potentially malicious based on true type detection such as suspicious file types and spoofed executable files.
  - **Known Viruses** - as detected by Anti-Virus solution integrated in Vital Security Web Appliance
- **High-Risk Site Categories** - sites which were blocked by URL Filtering module such as Adults, Hacking, etc. Majority of the sites blocked were adults related.

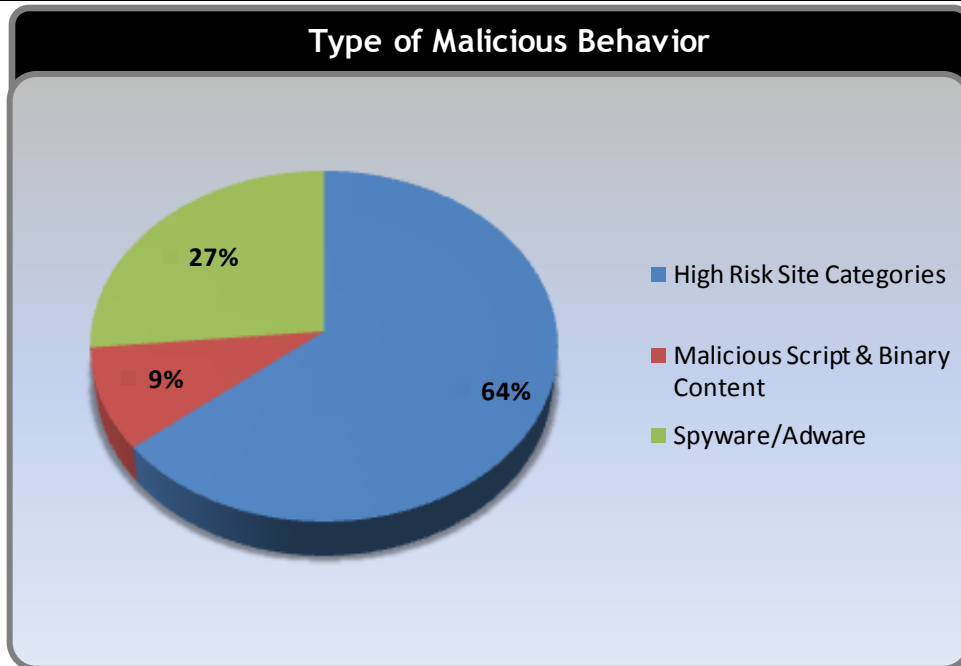


Figure 1 - Main Security Violations

### Security Violations Breakdown

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

Nature of Violation	Quantity	%
Block Access to High-Risk Site Categories (SurfControl)	2,691,217	64%
Block Access to Adware Sites	991,967	27%
Block Access to Spyware Sites	116,807	
Block Spoofed Content	286,135	9%
Block Application Level Vulnerabilities	30,949	
Block IM Tunneling	25,628	
Block Binary Exploits in Textual Files	15,710	
Block Malicious ActiveX, Java Applets and Executables	11,007	
Block Illegitimate Archives (Including Password-Protected Archives)	5,958	
Block Files with Suspicious Multiple Extensions	4,621	
<b>Total</b>	<b>4,179,999</b>	

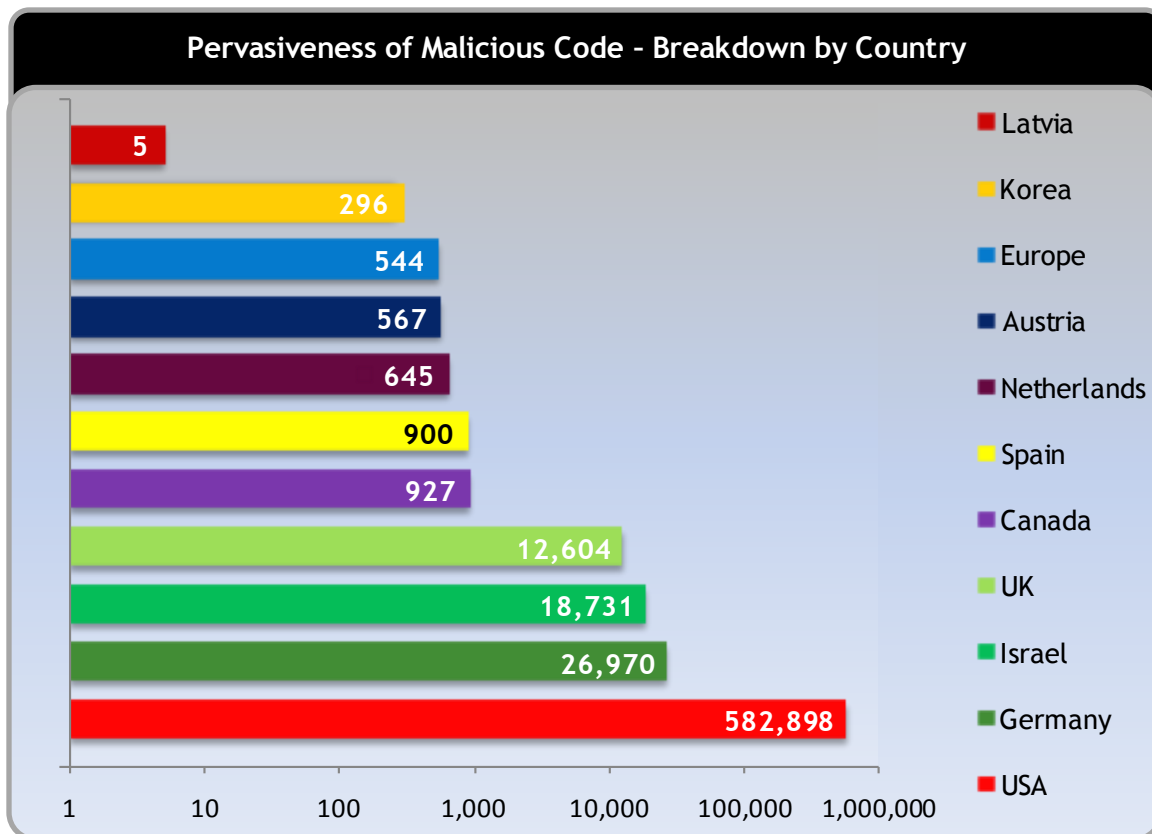


Figure 2 - Pervasiveness of Malicious Code - Breakdowns by Country

### Conclusions

This audit supports the research results as presented in Web Security Trend Report Q1 2007 that United States is on the top of the list of countries hosting malicious code.

Spyware and malicious behavior have significant part of security incidents in this type of network. Malicious code was detected by Finjan’s Vital Security technology, based on behavior analysis and without using signatures.

The assumption that an Anti-Virus lab can put its hands on each and every piece of malicious code and create a signature does not play well in the dynamic web scenario (very few malicious pages were detected by anti-virus products). Only proactive, behavior-based security can analyze web content on-the-fly and detect whether or not it is legitimate.

Finjan’s Vital Security Web Appliance utilizes patented behavior-based security to detect and block unknown, new and emerging threats that cannot be detected by traditional reactive security technologies. This type of proactive security is akin to having an “expert system in a box,” safeguarding corporate users from malicious web content.