

Security Audit - Internet Service Provider Company

Introduction

This analysis is based on a security audit that was performed during the first quarter of 2007 for an ISP (Internet Service Provider) organization. Live Internet access information was gathered during a period of one day and was based on the surfing activities of approximately 10,000 users.

All web pages recorded on company's proxy, were re-scanned and analyzed by Finjan's Vital Security™ technology. The data was then analyzed by experts from Finjan's Malicious Code Research Center (MCRC). The main findings are presented below.

Main Findings

- **Spyware and Adware:** 18% 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

- 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:**
 - **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) and attempts to exploit systems/browsers vulnerabilities.
 - **Potential Malicious Files** - blocked files considered as potentially malicious based on true type detection such as suspicious file types and spoofed executable files.

- **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.

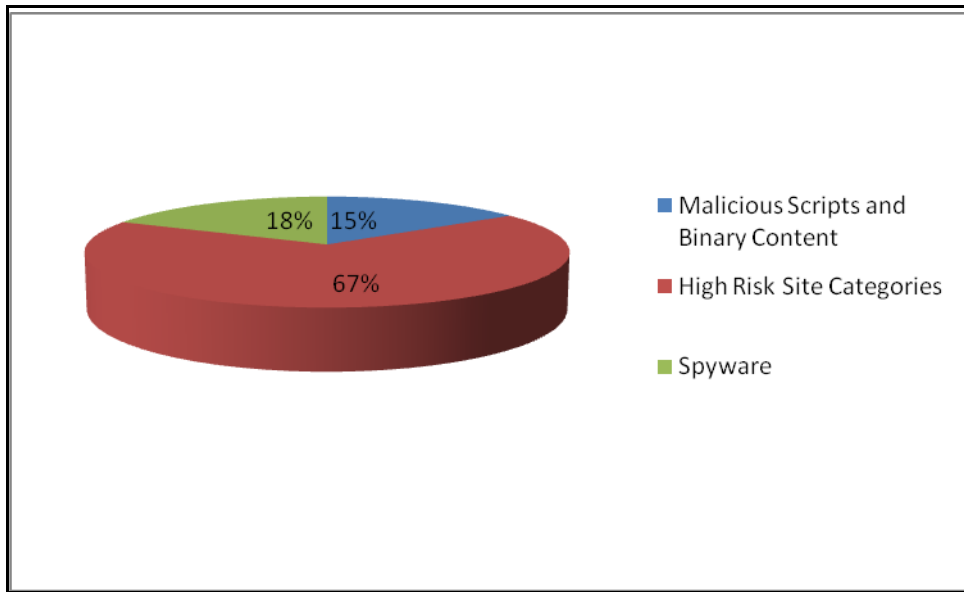


Figure 1 - Main Security Violations

Security Violations Breakdown

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

Nature of Violation	Quantity	%
High Risk Site Categories	191,783	67%
Spyware Site and Spyware Objects	51,249	18%
Malicious Scripts	40,165	15%
Potential Malicious File Types	2,168	
Potential Malicious Binary Files	1,689	
Known Viruses	938	
Grand Total	287,992	100%

Pervasiveness of Malicious Code - Breakdown by Country

The following table provides malicious web sites breakdown by countries:

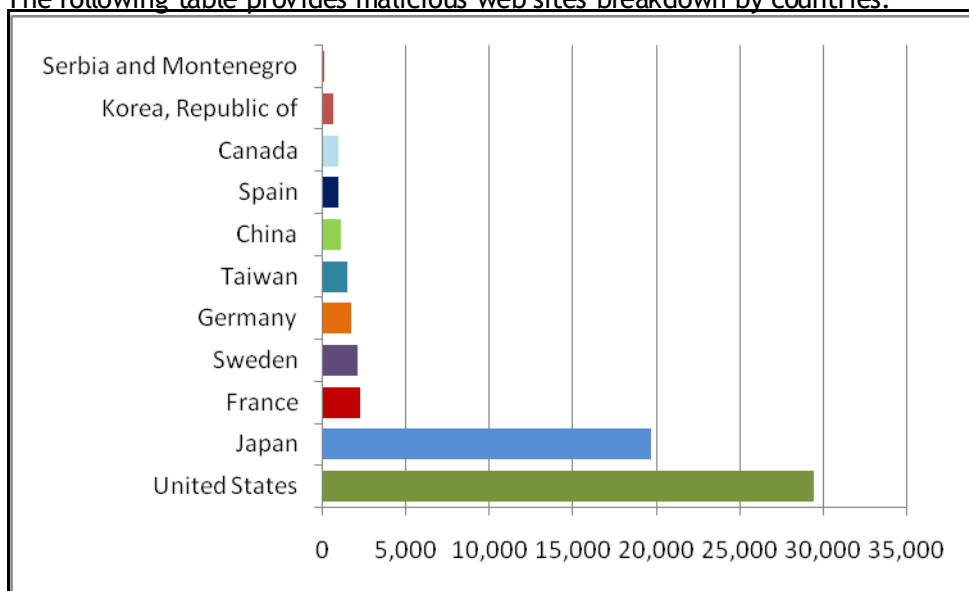


Figure 2 - Malicious Sites Breakdown by Country

Conclusions

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.

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.

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.