



# Keeping the Bad Guys Out – Security Successes

**Trey Stevens and Michael Watson**

---

AITR Meeting  
December 2, 2010



## Overview

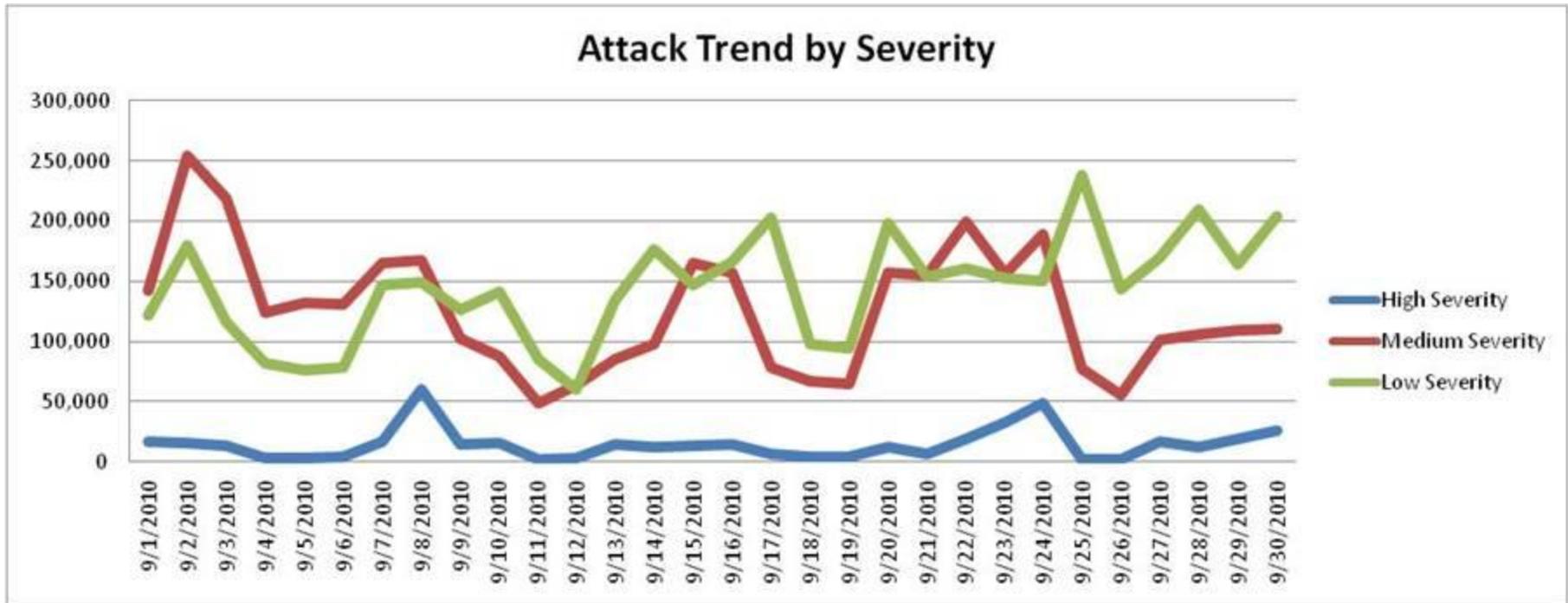
- Intrusion attempts and severity
- Intrusion intelligence
- Security incidents
- Unsolicited e-mail
- Filtered web traffic



# Detecting Intrusion Attempts

- Commonwealth systems are constantly under attack
  - 123,657,149 million attacks this year as of Nov. 28
- Attack types vary each month
  - September's top targets were the file transfer protocol (FTP) and web services
  - Brute force attacks are constant
  - Structured query language (SQL) injections common
- Sources of attack
  - Number one source is consistently United States-based hosts
  - The top foreign sources vary but are primarily Eastern Europe and China

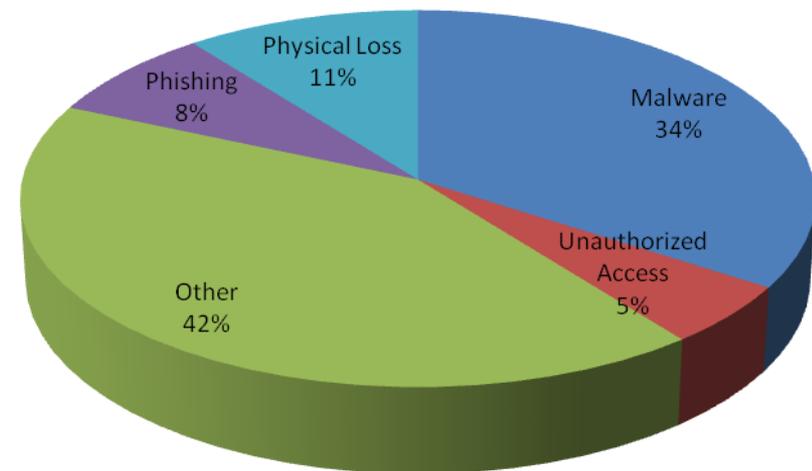
# Attack Severity



# Security Incidents

- Partnership customers seeing a downward trend
  - Averaging 40 incidents per month
  - Mean time between incidents 15h 12m 31s for the year
- Malware is the single biggest threat
  - Best defense is user education
- 42 security incidents in September

September 2010  
Security Incidents



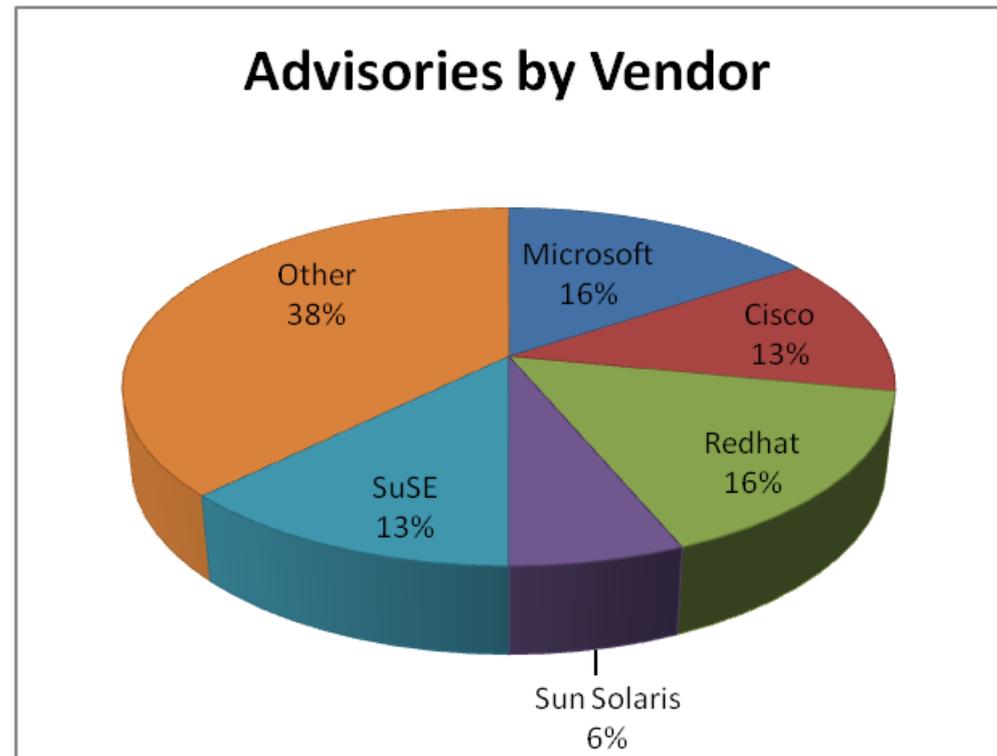


## Intrusion Intelligence

- Intrusion attempts that are not stopped are investigated
- Attacks can be complex
  - Evidence of stealth attack attempts
- Protect Internet facing systems first
- Be aware of attempts to gain footholds on systems
- Least privilege

# Vulnerability Analysis

- 63 vulnerability notifications issued in September
- Three issues involved attacks occurring prior to patches being available
- Applications are primary attack vector
  - Agencies should be monitoring agency specific applications





# Malicious Software

- Infection attempts are consistent throughout the environment
- Successful attempts have declined as security controls block malicious traffic
- Removable media is primary vector for infection attempts detected at the desktop
  - 30 percent of the infection attempts occurred through removable media

Desktop	Server	Mail	Proxy	Total
246	82	1,022	1,147	2,497

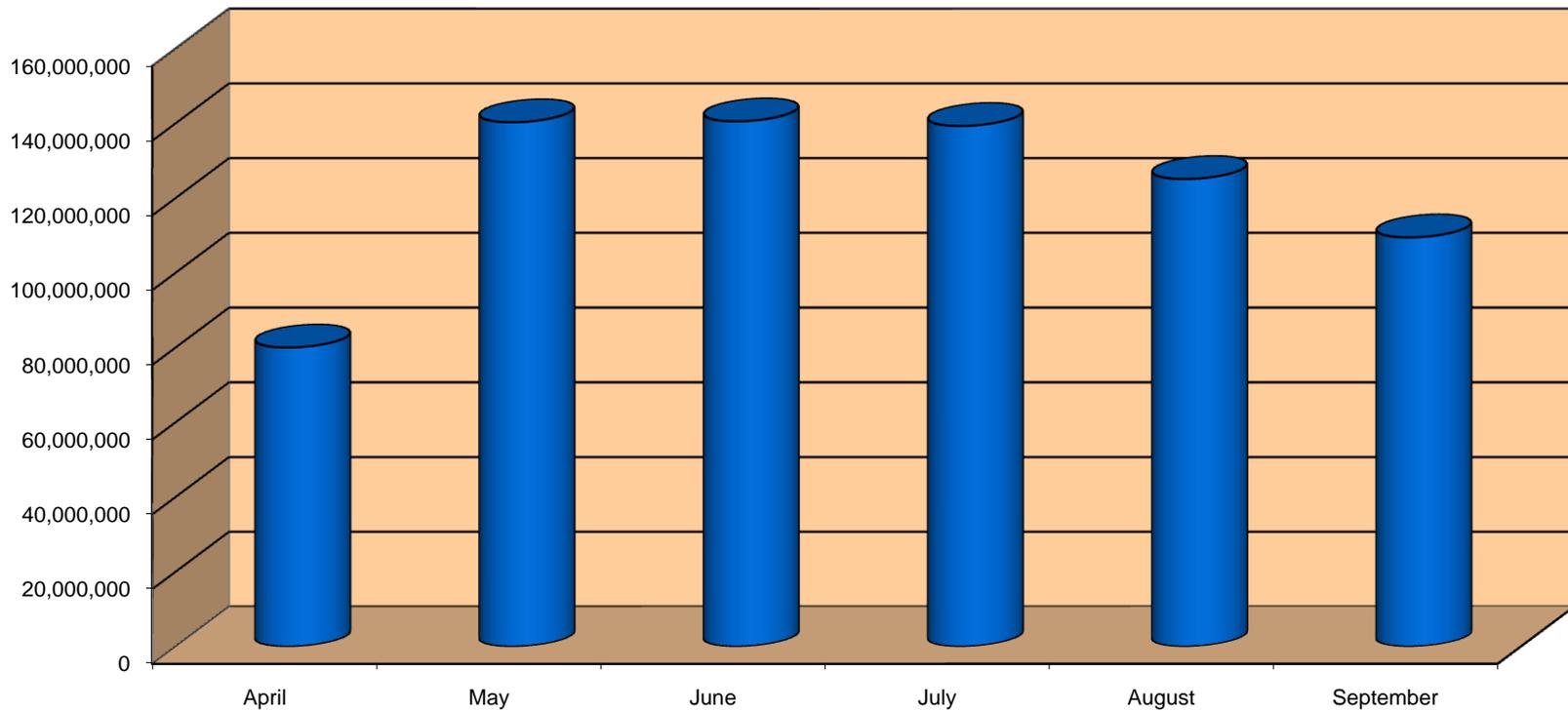


## Unsolicited E-mail

- Spam volumes average between 93 percent and 94 percent
  - Above the global spam percentage published by Symantec
- Commonwealth noticed drops in spam levels when law enforcement activities shutdown spam operators
- The Commonwealth blocks approximately 120 million spam messages a month

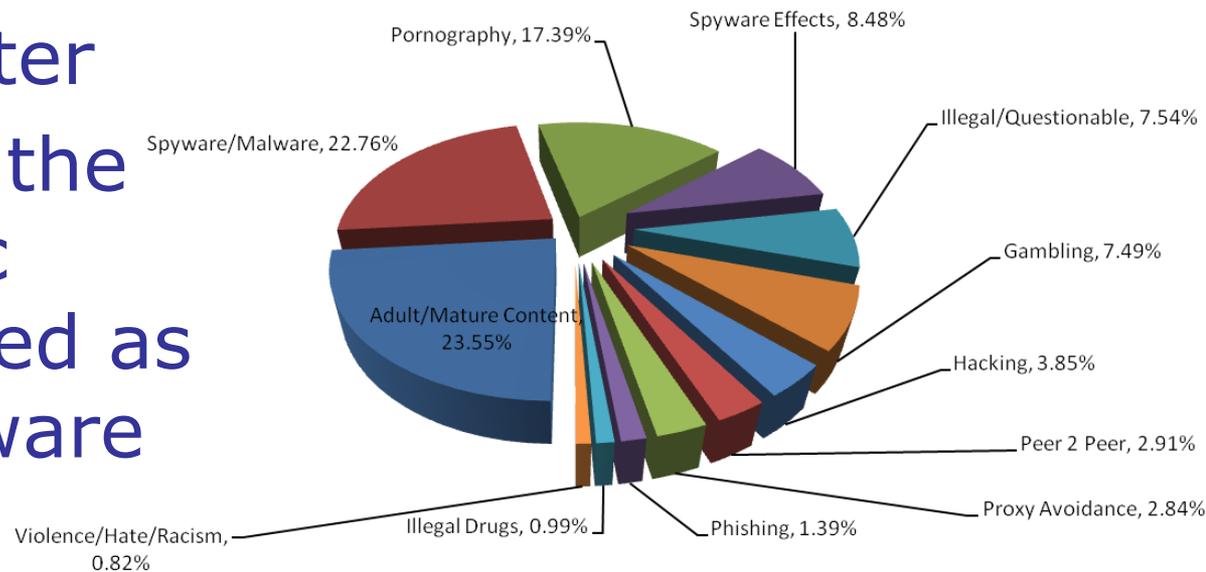
# Unsolicited E-mail

Spam Blocking Trend



# Web Traffic Security Analysis

- The Commonwealth had approximately 111.9 million page views for the month of September
- 19,382 total sites were blocked by the web filter
- 32 percent of the blocked traffic was categorized as malware/spyware





## Review

- Intrusion attempts and severity
- Intrusion intelligence
- Security incidents
- Unsolicited e-mail
- Filtered web traffic



# Questions

Questions?