



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

December 09, 2010



ISOAG December 2010 Agenda

- | | | |
|------|--|--|
| I. | Welcome & Opening Remarks | Michael Watson, VITA |
| II. | Keeping the Bad Guys Out | Michael Watson, VITA, Trey Stevens, NG |
| III. | Commonwealth Security & Risk Management Panel Discussion | Benny Ambler, Bob Baskette, Michael Watson, VITA |
| IV. | Upcoming Events & Other Business | Michael Watson, VITA |
| V. | Partnership Update | Bob Baskette, VITA |



Virginia Information Technologies Agency

Keeping the Bad Guys Out – Security Successes

Trey Stevens and Michael Watson





Overview

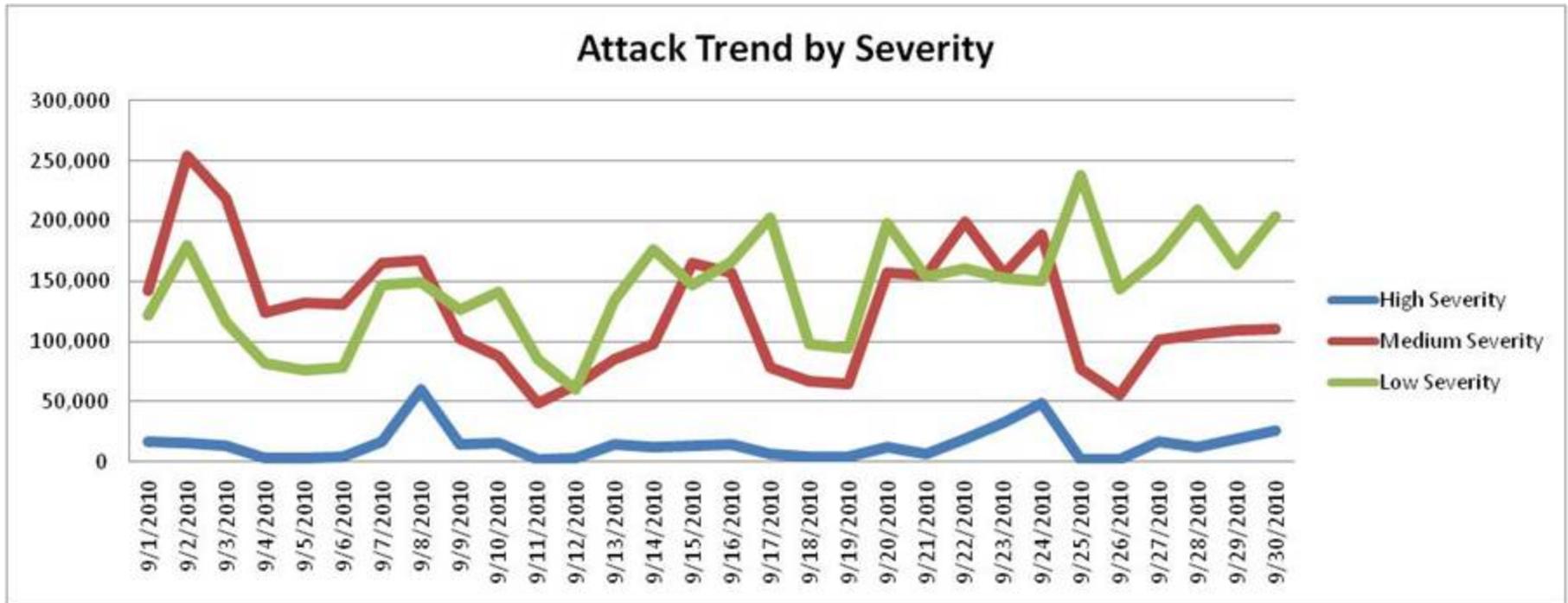
- Intrusion attempts and severity
- Intrusion intelligence
- Security incidents
- Unsolicited e-mail
- Filtered web traffic



Detecting Intrusion Attempts

- Commonwealth systems are constantly under attack
 - 123,657,149 million attacks 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

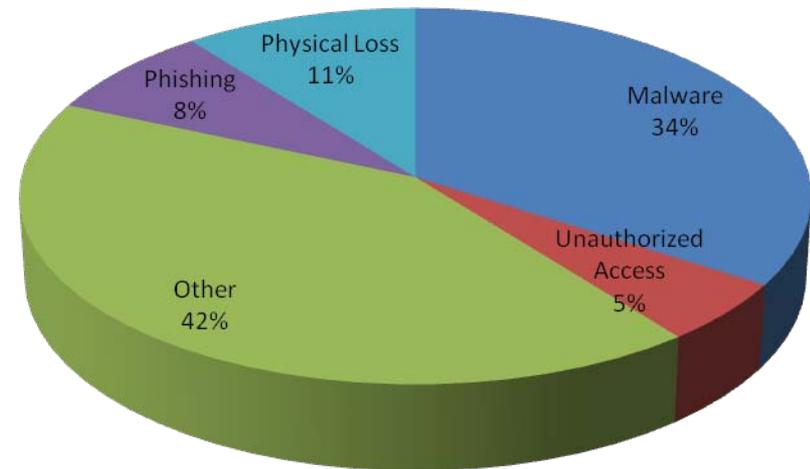
Attack Severity



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



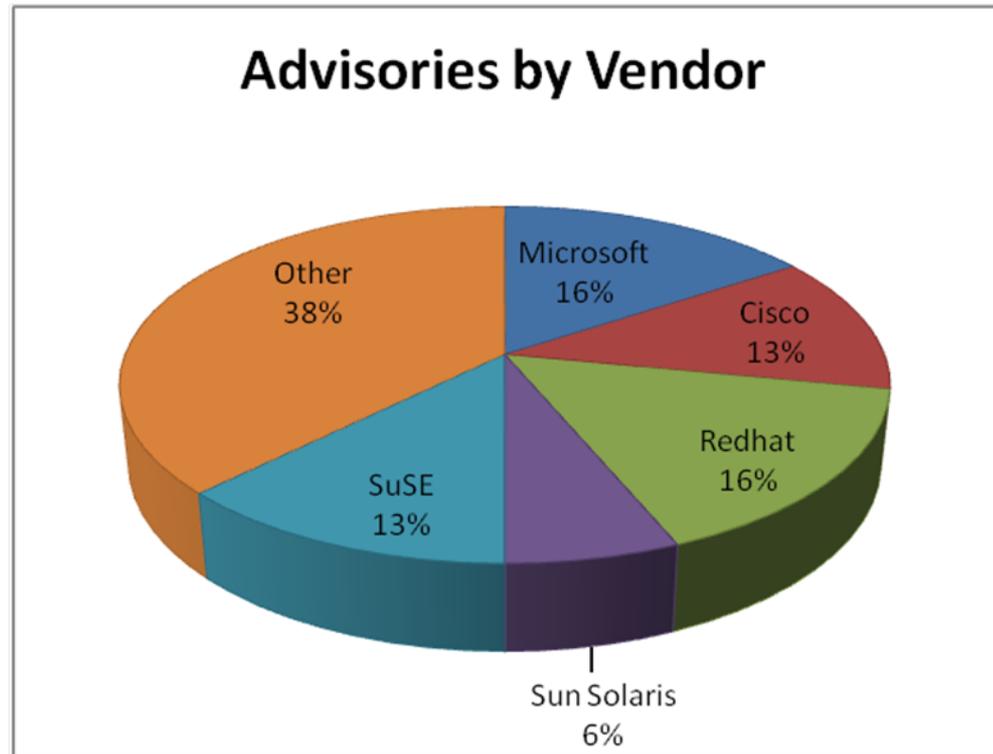


Intrusion Intelligence

- 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% of the infection attempts occurred through removable media

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



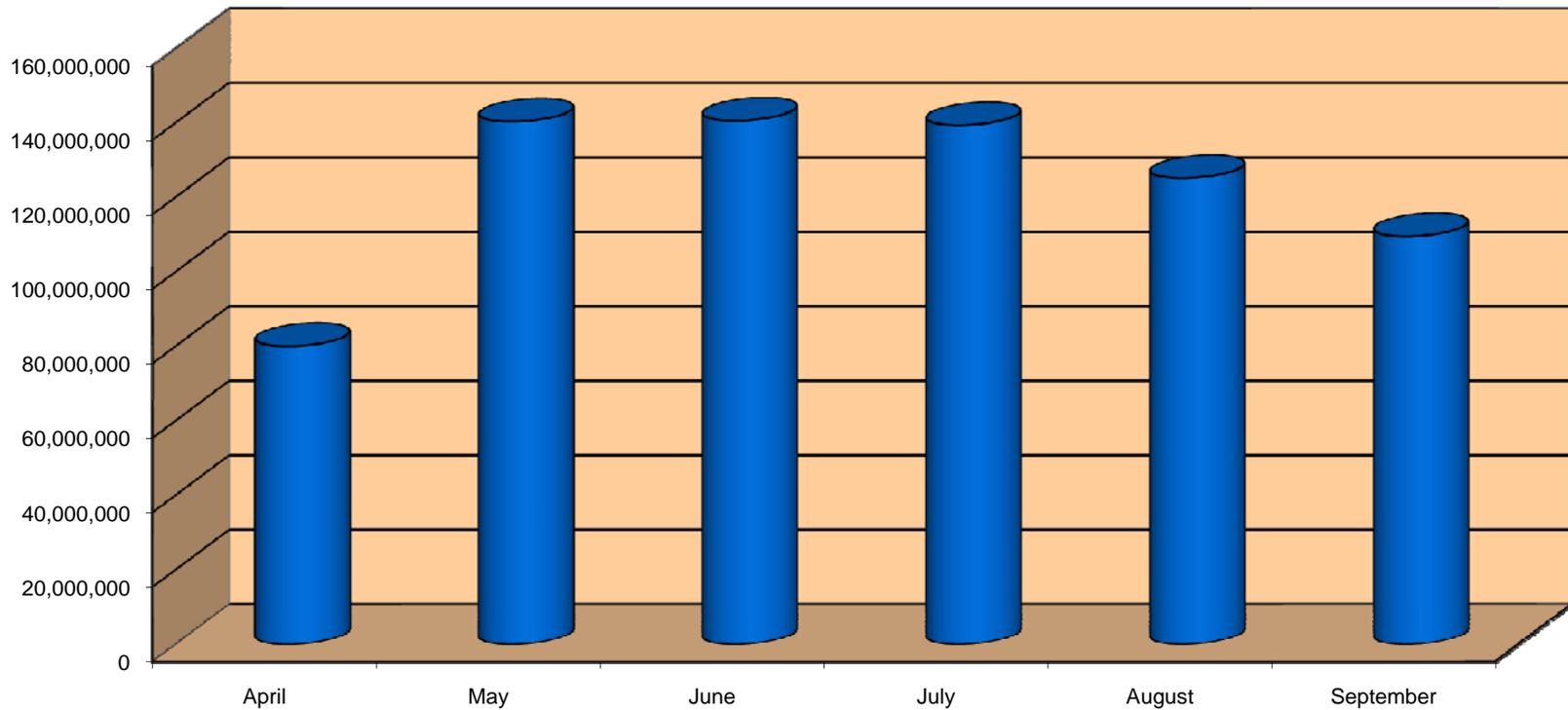
Unsolicited Email

- Spam volumes average between 93% and 94%
 - 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



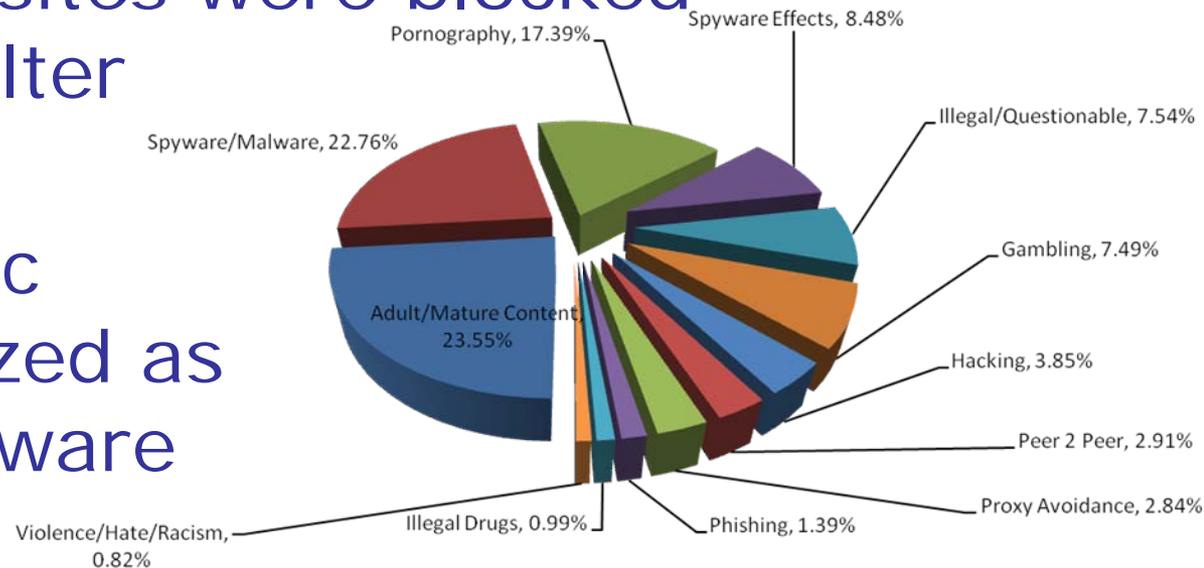
Unsolicited Email

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% 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?



Virginia Information Technologies Agency

CSRM Panel Discussion

Benny Ambler, Sr Mgr Security Governance

Bob Baskette, Sr Mgr Security Operations

Michael Watson, Sr Mgr IT Risk Management



Virginia Information Technologies Agency

Upcoming Events





General Assembly

General Assembly convenes January 12, 2011

(Odd number year = short session)



Future ISOAG's

From 1:00 – 4:00 pm at CESC

ISOAG will be held the 1st Wednesday of each month in 2011

Wednesday - January 5, 2011

Wednesday - February 2, 2011



Future IS Orientation Sessions

Tuesday - January 11, 2011
(CESC)

9:00 – 11:30a

Tuesday - March 8, 2011
(CESC)

1:00 – 3:30p

IS Orientation is now available via webinar!



AITR Meeting

AITR Meeting:

Wednesday, February 9th

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: TBD



Information Security System Association

ISSA meets on the second Wednesday of every month

DATE: Wednesday, January 12, 2011

**LOCATION: Maggiano's Little Italy, 11800 W. Broad St.,
#2204, Richmond/Short Pump Mall**

**TIME: 11:30 - 1:30pm. Presentation starts at 11:45 &
Lunch served at 12.**

COST: ISSA Members: \$10 & Non-Members: \$20

SPEAKER: TBD



MS-ISAC Webcast

National Webcast!

Wednesday, December 15, 2010, 2:00 to 3:00 p.m.

Topic: Security Management

The National Webcast Initiative is a collaborative effort between government and the private sector to help strengthen our Nation's cyber readiness and resilience. A number of vendors have offered their services at no cost, to help develop and deliver the webcasts.

Register @: <http://www.msisac.org/webcast/>



Identity Theft Red Flags Rules Extended Until December 31, 2010

The Red Flags Rule requires many businesses and organizations to implement a written Identify Theft Prevention Program designed to detect the warning signs – or “red flags” – of identity theft in their day-to-day operations.

At the request of members of Congress, the Federal Trade Commission is delaying enforcement of the “Red Flags” Rule until December 31, 2010. Read the FAQ at:

<http://www.ftc.gov/bcp/edu/microsites/redflagesrule/index.shtml>



Virginia Information Technologies Agency

Any Other Business ???????



ADJOURN

THANK YOU FOR ATTENDING

