Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

January 12, 2010

January

Happy New Year

Virginia Information Technologies Agency

ISOAG January 2010 Agenda

I.	Welcome & Opening Remarks	John Green, VITA
II.	Semi-Annual Information Security Update	Goran Gustavsson, APA
III.	Channel Surfing – A Guide to Covert Communications	Bob Baskette, VITA
IV.	Where's the BeEF? XSS Demo	Eric Taylor, NG
V.	COV 2009 Threat Report	Michael Watson, VITA
VI.	Upcoming Events & Other Business	John Green, VITA

October Semi-Annual Update

Semi-Annual Information Security Update

January 12, 2010

Goran Gustavsson, Audit Director
Auditor of Public Accounts

Objectives

- Determine whether agencies and institutions of higher education have developed a security program based on the Commonwealth's Information Security Standard (SEC501) or industry best practices (ISO 27002, NIST)

Objectives

- Determine whether agencies and institutions of higher education are following their information security programs

Objectives

- Analyze the progress made by agencies and institutions of higher education

Scope

- Audit reports issued between December 1, 2008 and September 30, 2009 (10 months)
- Coverage since last “Statewide Security Review” follow-up report, issued December 2008
- 54 agencies and institutions of higher education

Scope

- Small Agencies

Board of Accountancy
Board of Bar Examiners
Department for the Aging
Department of Business Assistance
Department of Fire Programs
Department of Human Resource Management
Department of Minority Business Enterprises
State Board of Elections
State Council for Higher Education for Virginia
Virginia College Savings Plan
Virginia Commission for the Arts
Virginia Office for Protection and Advocacy
Virginia State Bar

- Medium and Large Agencies

Attorney General and Department of Law
Christopher Newport University
College of William and Mary (Incl. Richard Bland College and Virginia Institute of Marine Science)
Department of Accounts
Department of Agriculture and Consumer Services (Incl. Division of Charitable Gaming)

- Medium and Large Agencies (cont'd)

Department of Alcoholic Beverage Control
Department of Behavioral Health & Developmental Svcs
Department of Correctional Education
Department of Corrections
Department of Criminal Justice Services
Department of Emergency Management
Department of Forestry
Department of General Services
Department of Health
Department of Health Professions
Department of Medical Assistance Services
Department of Mines, Minerals, and Energy
Department of Motor Vehicles
Department of Rehabilitative Services (Incl. Department for the Deaf and Hard of Hearing, Department of the Blind and Vision Impaired, Virginia Board for People with Disabilities, Virginia Industries for the Blind, Virginia Rehabilitation Center for the Blind and Vision Impaired, Woodrow Wilson Rehabilitation Center.)
Department of Social Services
Department of Taxation
Department of the Treasury

Scope

- Medium and Large Agencies (cont'd)

Department of Transportation
Department of Veterans Services
George Mason University
Indigent Defense Commission
James Madison University
Library of Virginia
Longwood University
Marine Resources Commission
Norfolk State University
Old Dominion University
Radford University
State Lottery Department
Supreme Court (Incl. Board of Bar Examiners and Virginia State Bar)
University of Mary Washington
Virginia Commonwealth University
Virginia Community College System
Virginia Employment Commission
Virginia Military Institute
Virginia State University

Methodology

- Risk Management & Continuity Plans
  - Business Impact Analysis (BIA)
  - Risk Assessment (RA)
  - Continuity of Operations Plan (COOP)
  - Disaster Recovery Plan (DRP)

Methodology

- Essential Policies and Procedures
  - Authority of the Information Security Officer
  - Training Program
  - Logical Access Controls
  - User Authentication Requirements
  - Password Controls
  - Physical Access Controls
  - Monitoring

Methodology

- Objective 1: Does the Agency have an Information Security Program that complies with best practices?

- **Yes:** The agency has performed a security analysis and documented a program that includes all risk management and continuity of operations plans and all seven essential policy and procedure components.

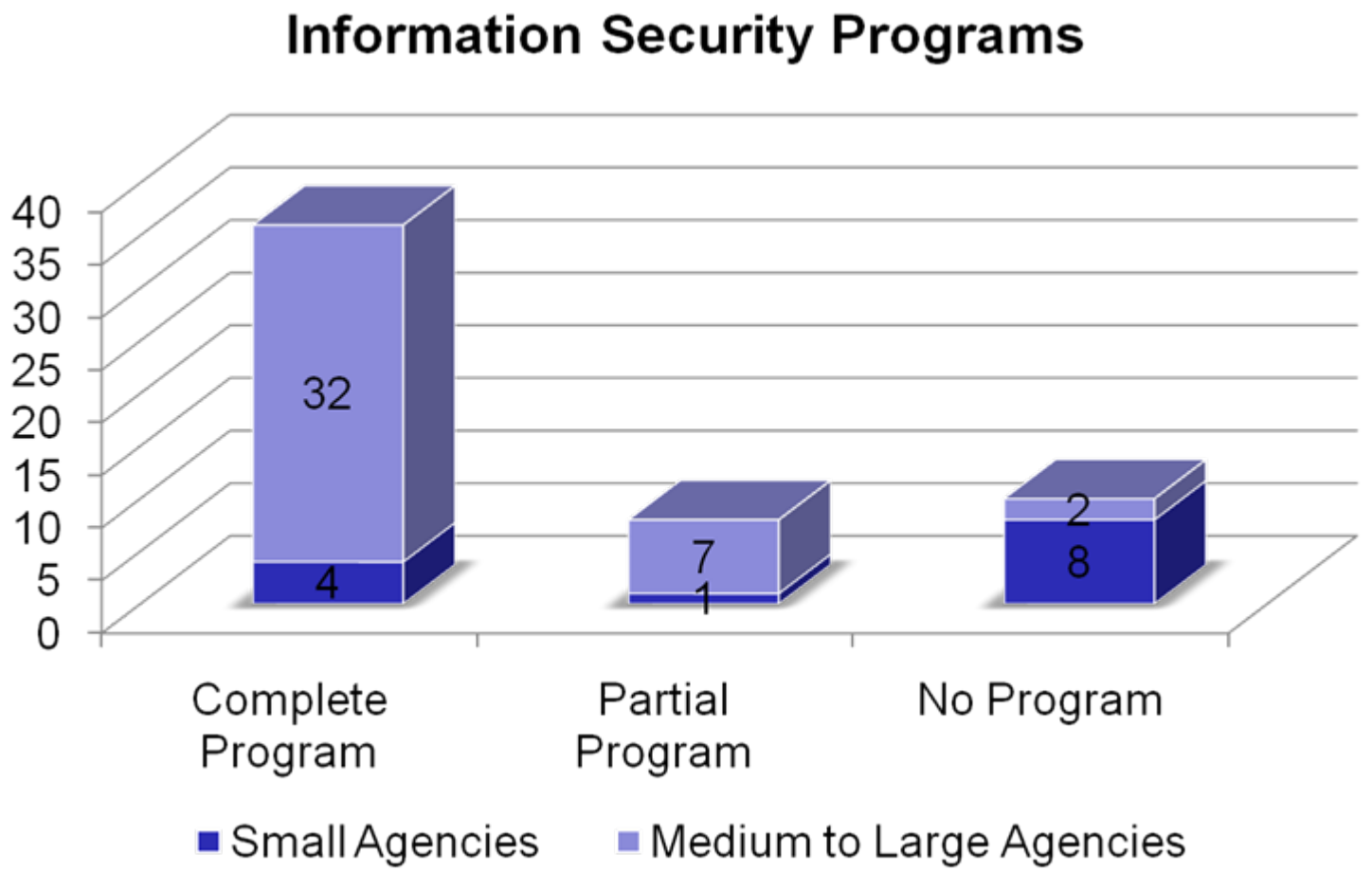
- **No:** The agency is missing one or more of the risk management plans, continuity of operations plan, or essential policy and procedures components.

Methodology

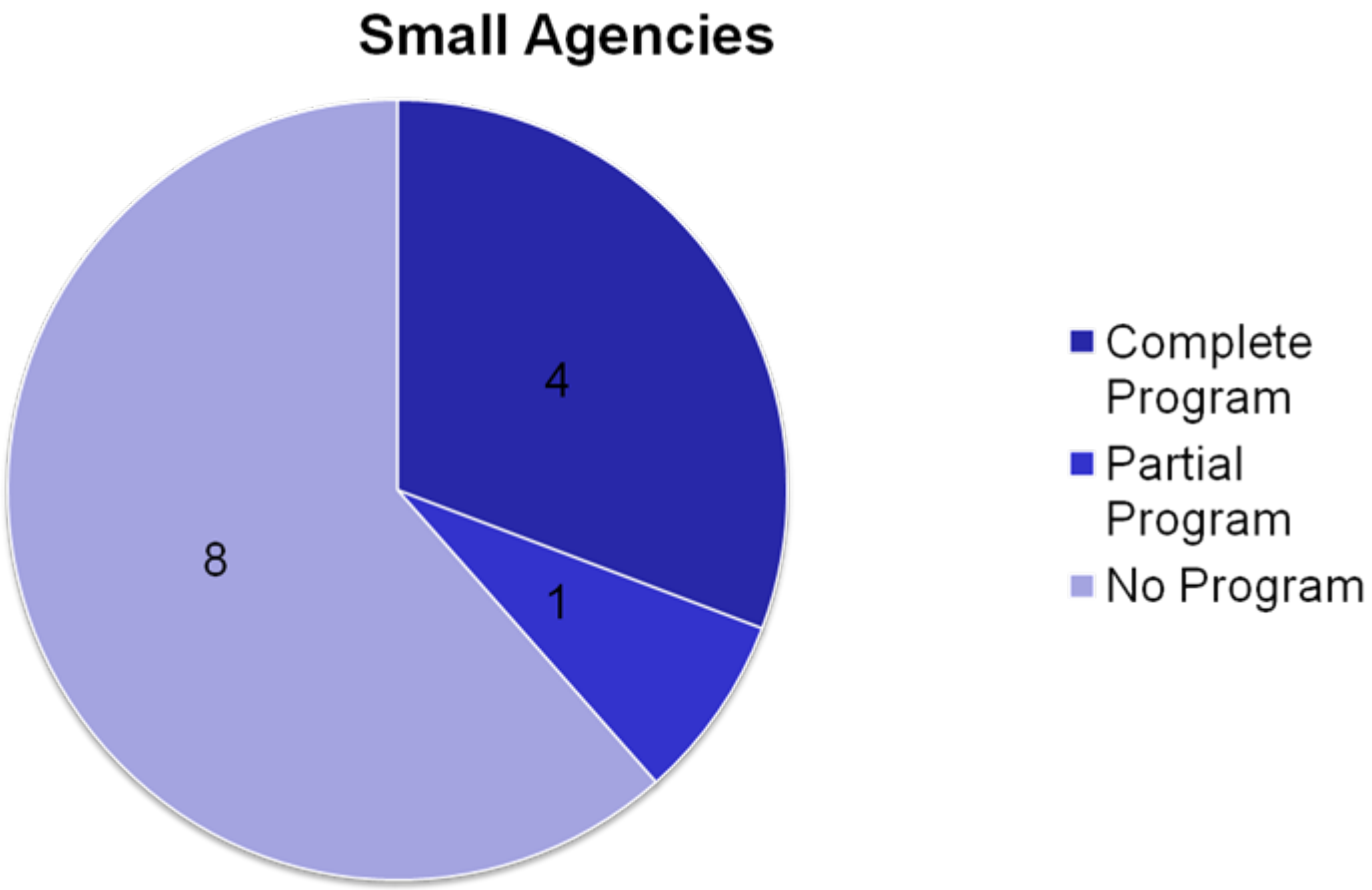
- Objective 2: Does the Agency follow its Information Security Program?

- **Yes:** The agency is following and has established a process to update its information security program and provide adequate training to its employees.
- **No:** The agency is not fully following the requirements of its information security program.
- N/A: The agency does not have a security program that complies with best practices, and the agency has a “No” rating for Objective 1, “Does the agency have an Information Security Program that complies with best practices?”

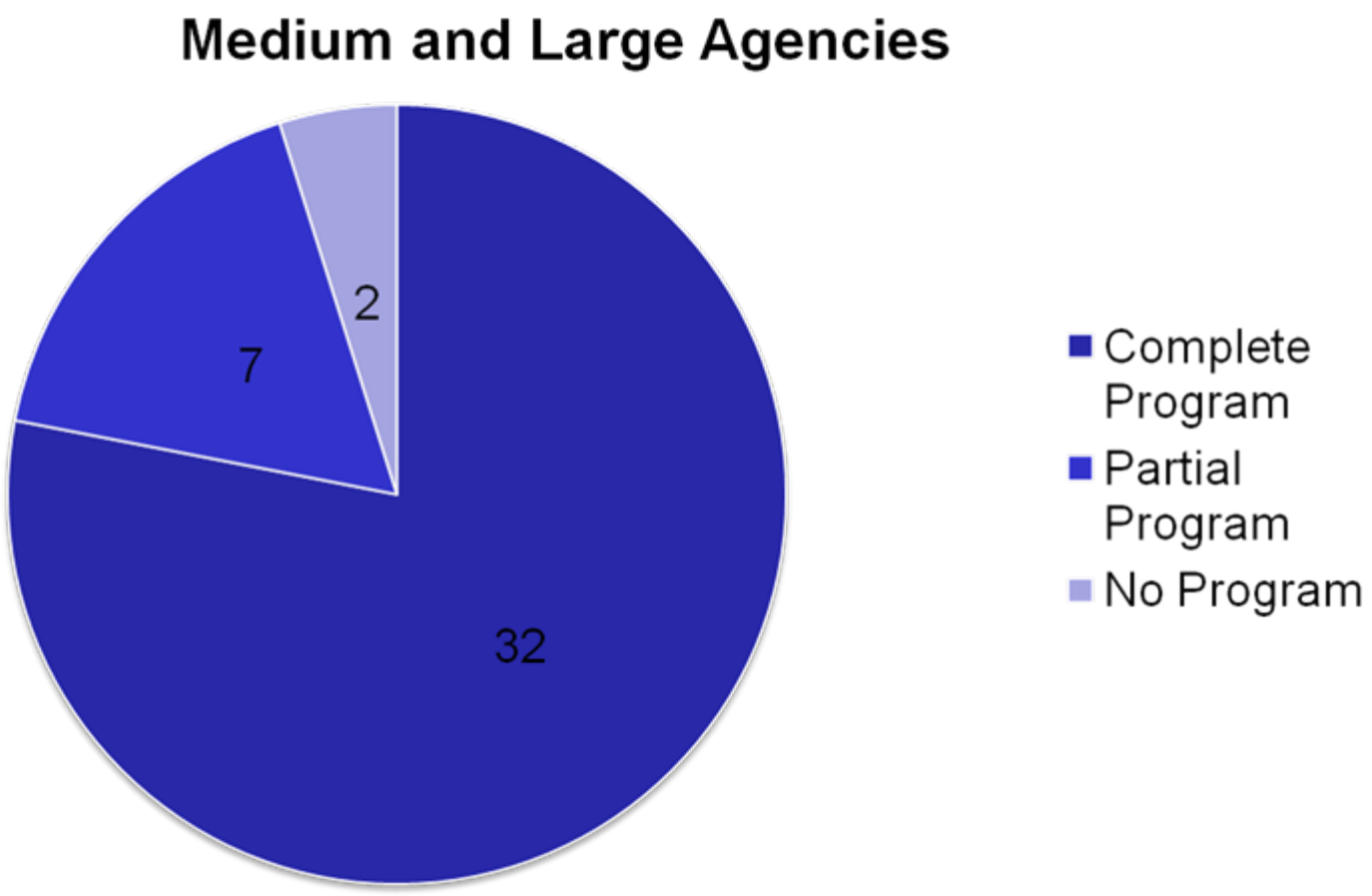
Results


Information Security Programs
40
35
30
25
20
15
10
5
0
32
4
7
1
2
8
Complete Program
Partial Program
No Program
Small Agencies
Medium to Large Agencies

Results


Small Agencies
4
1
8
Complete Program
Partial Program
No Program

Results


Medium and Large Agencies
2
7
32
Complete Program
Partial Program
No Program

Results

- Complete Programs
  - 78% of medium and large agency population (32 of 41)
  - 31% of small agency population (4 of 13)

Next Semi-Annual Update

- Release Date: April, 2010
- Audits issued October 1, 2009 through March 30, 2010

Questions?

Goran Gustavsson

Audit Director

Information Systems Security Specialty Team

Auditor of Public Accounts

(804) 225-3350 ext. 306

Goran.Gustavsson@apa.virginia.gov

Virginia Information Technologies Agency

Channel Surfing: A Guide to Covert Communications

Bob Baskette
CISSP-ISSAP, CCNP/CCDP, RHCT
Commonwealth Security Architect

Generic Covert Channel Definitions

- A covert channel is any method that can be utilized by an entity to receive information in an unauthorized manner
- A covert channel allows two cooperating processes to transfer information in such a way that violates the security policy
- A covert channel creates information flows that are not controlled by any security mechanism
- A covert channel is hidden from the access control mechanisms since it does not use the legitimate data transfer mechanisms of the computer system

Environmental Factors

- Covert Channels can be established as the result of one of the following conditions:
  - Improper oversight in the development of the software product
  - Improper implementation of access controls within the software
  - The existence of a shared resource between two or more entities

TCSEC Definition

- The Trusted Computer Security Evaluation Criteria (TCSEC) is a set of criteria established by the National Computer Security Center

- The TCSEC defines two kinds of covert channels:
  - Storage channels
    - Communicate by modifying a stored object
  - Timing channels
    - Perform operations that affect the relative timing of events

- The information is transferred using a signaling mechanism via entities or objects

Covert Storage Channel Attacks

- Uses one process to write data to a storage area and another process to read the data
- Uses storage system to hide or move data
- Performed by changing the amount or pattern of free space on the disk
- Sharing disk space between two subjects at different security levels

Covert Timing Channel Attacks

- One process signals information to another process by modulating its own use of system resources
- Influence the rate that some other process is able to acquire resources (CPU/Memory/IO)
- Variation in rate may be used to pass signals
- Manipulation affects the real response time observed by the second process
- A program can open and close a file in a specific, timed pattern that can be detected by another program. This pattern can be interpreted as a string of bits, forming a covert channel.

Modern Covert Channel Methods

- Port Forwarding
  - Works by listening on certain ports and then forward the packets to a secondary target
  - Port Forwarding tools do not care about protocols used simply act as a pipe to more data
    - Data pipe
      - Unix port redirection tool
      - data pipe <local port> cremate port> <host>
    - Fpipe
      - Port redirection on Windows
      - Fpipe -l 69 -r 53 -u IP-address
    - Netcat
      - Command-line utility written for Unix and Windows
      - Can use both TCP and UDP connections
      - Can be used for port redirection
      - Can read and write data over the connections

Modern Covert Channel Methods

- Protocol Manipulation
  - Uses an established protocol for a purpose not defined in the approved design
  - Insert data into the payload section of a common protocol such as HTTP, IM, IRC, or SMTP
  - Can be used to bypass a firewall
    - Reverse WWW shell
    - Compromise internal host
    - Use internal host to connect to an outside host on port 80
    - Appear to be just client web traffic

Modern Covert Channel Methods

- Packet Manipulation
  - IP, TCP and ICMP Header manipulation
  - IP and TCP contain options fields that can be used to carry fragmented data
  - Can bypass the firewall by using a covert channel tunnel via ICMP or in TCP-ACK packet

Internet Control Message Protocol

- Used to:
  - Deliver status messages
  - Reports errors
  - Reply to certain requests
  - Report on routing information
  - Test connectivity

- ICMP header contains an Optional Data field
  - Was designed to be filler to make the ICMP packet the minimum legal length
  - Linux operating systems will fill the Optional Data field with numeric values to a total size of 56 bytes in addition to the 8 octet header.
  - Microsoft Windows will fill the Optional Data field with characters to a total size of 32 bytes in addition to the 8 octet header.
  - Hackers will fill the Optional Data field with fragments of data

TCP Header Information

- A TCP segment consists of a segment header and a data section.
- The TCP header contains 10 mandatory fields and an optional extension field
- The data section follows the header
- Its contents are the payload data carried for the application

TCP Header Manipulation

- TCP Acknowledgment number (32 bits)
  - If the ACK flag is set then the value of this field is the next sequence number that the receiver is expecting
  - This acknowledges receipt of any prior bytes
  - The first ACK sent by each end acknowledges the other end's initial sequence number itself

- Data offset (4 bits)
  - Specifies the size of the TCP header in 32-bit words
  - The minimum size header is 5 words and the maximum is 15 words resulting in the minimum size of 20 bytes and maximum of 60 bytes, allowing for up to 40 bytes of options in the header
  - This field gets its name from the fact that it is also the offset from the start of the TCP segment to the actual data

IP Header Information

- The maximum packet size 65535 bytes
- Typical MTU for Ethernet 1500 bytes
- The IP packet consists of a header section and a data section
- The IPv4 packet header consists of 13 fields
  - 12 Fields are required
  - The 13th field is optional and is called Options Field

IP Header Option Information

- Optional header fields may follow the destination address field, but these are not often used
- The value in the IHL field must include enough extra 32-bit words to hold all the options
- Must also include any padding needed to ensure that the header contains an integral number of 32-bit words

IP Header Option Information

- The possible options that can be put in the header are as follows:
  - Copied
    - 1-bit
    - Set to 1 if the options need to be copied into all fragments of a fragmented packet
  - Option Class
    - 2-bits
    - General options category. 0 is for "control" options, and 2 is for "debugging and measurement“ (1 and 3 are reserved)
  - Option Number
    - 5-bits
    - Specifies an option
  - Option Length
    - 8-bits
    - Indicates the size of the entire option
  - Option Data
    - Variable
    - Option-specific data

Covert Channel Programs

- **007 Shell**
  - Shell tunneling program
  - Allows covert channels
- **ICMP Shell**
  - Similar to telnet
  - Used to make a connection to target using just ICMP commands
- **ACKCmd**
  - Client/server program
  - Communicates using only TCP-ACK packets
- **Covert_TCP**
  - Used to send files through firewall one byte at a time
  - Hide data in he IP-header

Covert Communication Tools

- **Loki**
  - Originally designed to show how ICMP traffic can be insecure and dangerous
  - Purpose is to be a backdoor or covert channel
  - Does not encrypt traffic
  - Can be detected since it generates many more ICMP requests than replies
  - Client/server program
  - Used by hackers to setup backdoors
  - Server code housed on the compromised computer
  - Hacker sends commands as data inside ICMP

Covert Communication Tools

- **Reverse WWW Tunneling shell**
  - Proof of concept Perl script
  - Imitates web traffic to by-pass firewalls
  - Program run at preset time every day
- **ICMP Backdoor**
  - Uses only ping reply packets
  - Can be detected since it does not pad up short messages or divide large messages
- **Ackland**
  - Provides a command shell on Windows
  - Communicates via TCP ACK packets

Steganography Basics

- The art and science of writing hidden messages such that that only the sender and intended recipient know of the existence of the message
- The term is Greek in origin and means "concealed writing"
- Messages are not encrypted, just obscured by other data
- Classic form of security through obscurity

Steganography Basics

- Provides concealment of information within computer files
- Typically the message will appear to be another object
  - Images
  - Articles
  - Shopping lists
- The least-significant bit of each byte in an image file can be altered to encode a message without causing any significant change to the image

Steganography Verses Cryptography

- The advantage of steganography over cryptography is that messages do not attract attention to themselves
- Encrypted messages or files can arouse suspicion and may be incriminating in countries where encryption is illegal
- Cryptography protects the contents of a message
- Steganography can protect both the message and communicating parties
- Media files are ideal for steganography because of their large size.
  - Adjust the color of every 100th pixel to correspond to a letter in the alphabet within an image file. The change is so subtle it is unlikely to be noticed

Ancient Steganography Methods

- The first recorded uses of steganography can be traced back to 440 BC:
  - Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were in common use then as reusable writing surfaces
  - Histiaeus shaved the head of his most trusted servant and tattooed a message on it. After the servant's hair grew back the message was hidden

Physical Steganography

- In WWII, the French Resistance sent some messages written on the backs of couriers using invisible ink
- Messages written in Morse code on knitting yarn and then knitted into a piece of clothing worn by a courier
- Messages written on the back of postage stamps
- During World War II, a spy for Japan living in New York City sent information to addresses in neutral South America. The spy was a toy doll dealer and the information sent to South America discussed how many of each doll model to ship. The hidden message in the doll orders gave information about ship movements

Digital Steganography Techniques

- Concealing messages within the lowest bits of noisy images or sound files
- Concealing data within encrypted data or within random data
  - The data to be concealed is first encrypted before being used to overwrite part of a much larger block of encrypted data or a block of random data
  - Unbreakable cipher text like one-time pad generated cipher text will appear perfectly random without the decryption key
- Mimic functions
  - Convert one file to have the statistical profile of another
  - Used to defeat statistical methods that help brute-force attacks identify the solution in a cipher text-only attack

Digital Steganography Techniques

- Concealed messages in tampered executable files
  - Exploits redundancy in the i386 instruction set
- Injecting imperceptible delays to packets sent over the network from the keyboard
  - Delays in key presses in some applications such as telnet or remote desktop software can create a delay in packets
  - The delays in the packets can be used to encode data
- Blog-Steganography
  - Messages are fractionalized and the encrypted pieces are added as comments of orphaned web-logs on social network platforms
  - In this case the selection of blogs is the symmetric key that sender and recipient are using
  - The carrier of the hidden message is the whole blogosphere

Digital Steganography Techniques

- Chaffing and Winnowing
  - A cryptographic technique to achieve confidentiality without using encryption when sending data over an insecure channel
  - The technique was conceived by Ron Rivest
  - The name is derived from agriculture where the grain must be separated from the chaff after harvesting by winnowing
  - A third party can make their communication confidential by simultaneously sending specially crafted messages through the same channel

How Chaff and Winnowing Works

- The sender enumerates the bits in the message and sends out each bit in a separate packet to a third party
- Each packet contains the bit's serial number in the message, the bit itself, and a Message Authentication Code (MAC) (secret key)
- The third party interleaves the packets with corresponding bogus packets known as the "chaff“ with corresponding serial numbers, the bits inverted, and a random number in place of the MAC.
- The third party then forwards each packet of the message to the recipient
- The recipient uses the MAC to find the authentic packets and drops the "chaff" packets

How Chaff and Winnowing Works

- The third party does not need to know the secret key
- An eavesdropper located between the sender and the third party could read the sender's message
- An eavesdropper located between the third party and the recipient would need the secret key and process the message have to determine which packets are "chaff"

How Steganography Works In Images

- The greater the difference in the size between the cover message and the protected data in total the easier it is to hide the protected data
- Most digital pictures contain enormous amounts of data and can be used to hide messages on many types of media
- A 24-bit bitmap will utilize 8-bits to represent each of the three base color values (red, green, and blue) for each pixel
- This results in 28 different values for each base color

How Steganography Works In Images

- The difference between 11111111 and 11111110 in the value for blue intensity will most likely be undetectable by the human eye
- Therefore the least significant bit could be altered to store the protected data without detection
- One letter of ASCII text could be encoded for every three pixels if all three base color values are utilized

Additional Steganography Usage

- Digital watermarking
  - The message is simply an identifying object that is hidden in an image so that its source can be tracked or verified
- Printer steganography
  - Used by Printer Manufactures including HP and Xerox
  - Color laser printers insert tiny yellow dots to each page to record the encoded printer serial numbers and time stamps

Steganography Image

Hidden in Plain Sight

- Image of a tree from the Wikipedia page on Steganography (http://en.wikipedia.org/wiki/Steganography)
- Removing all but the last 2 bits of each color component produces an almost completely black image
- Making that image 85 times brighter produces the image below

Hidden Image

Steganography Programs

- **Stegger, PHP Steganography**
  - Open source secure implementation of image steganography written in PHP
- **StegoShare**
  - Software which can be used for anonymous file sharing
- **Hiding Glyph: Bytewise Image Steganography**
  - Freeware software which hides any file or folder inside any lossless compressed image file such as BMP or PNG
- **ImageSpyer**
  - GUI tool which hides any file inside any image

Steganography Programs

- **FreeOTFE Free**
  - Open-source disk encryption software that supports hiding one encrypted volume inside another
- **OpenStego**
  - Open-source library written in Java used for embedding any type of file into images
- **PCopy**
  - Command-line tool that can produce lossless images such as PNG and BMP. Special features are Huffman compression, strong XOR encryption and the Hive archiving format which enables the injection of entire directories
- **Thumbnail Steganography**
  - Open-source program written in Java that is designed to increase the complexity required when attempting to automate steganography detection. It requires the original image (jpg, gif, etc) as well as the thumbnail (png) to extract the file from the thumbnail

Steganography Programs

- **TrueCrypt**
  - Windows/Linux disk encryption software that supports hiding one encrypted volume inside another
- **NetTools**
  - Program used to hide data in pictures, archives, sounds, text files, html, and lists
- **SteganoG**
  - Simple program to hide a text file in a .bmp file

Steganography Programs

- **ImageHide**
  - Steganography program that hides large amounts of text in images
  - Does not increase the file size
  - Can by used to bypass email filters
- **Blindside**
  - Steganography application that hides information inside BMP images
- **MP3Stege**
  - Hides information in MP3 files during compression
  - Data is compressed, encrypted, and hidden in the MP3 data stream
- **Snow**
  - White space steganography
  - Conceals messages in ASCII text by appending white spaces to the end of a line of text

Steganalysis Tools

- **StegAlyzerAS**
  - An automated tool used to detect the presence of steganography applications by matching artifacts of known files and registry keys on suspect computer media
- **Steganography Analysis and Research Center**
  - A Backbone Security Center of Excellence providing tools for steganography detection and extraction as well as Certified Steganography Examiner Training
- **StegDetect**
  - A tool to automatically find hidden messages in images embedded by seven steganography applications

Steganalysis Tools

- **StegSpy**
  - A tool that will detect hidden messages embedded by five steganography applications

- **StegSecret**
  - A java-based multiplatform steganalysis tool
  - Allows detection of hidden information by using the most known steganographic methods
  - Detects EOF, LSB, DCTs and other techniques

Steganography Countermeasures

- The simplest method to detect modified files is to compare them to known original files through a Hash comparison
- Once detected, the differences between the two files will comprise the payload
- Using extremely high compression rate on a file makes performing steganographic manipulation difficult but not impossible
- High compression rates reduce the amount of data available to hide the payload by raising the encoding density and facilitating easier detection of encoded information

File Hiding in Microsoft Windows

- The Microsoft attrib command
  - Will enable the Hidden file attribute for the filenames listed in the command syntax
    - attrib +h filename
  - File will not be displayed in a directory listing unless the display hidden file option is enabled

File Hiding in Microsoft Windows

- NTFS Alternate Data Stream Facility
  - Utilizes the $DATA attribute in the NTFS Master File Table
  - $DATA attribute is used to store any form of data and does not have a required format or defined value
  - A $DATA attribute is allocated for each file in the Master File Table to hold the contents of the file
  - Also allows additional data such as summary information and system information to be stored with the base file

NTFS Alternate Data Stream Facility

- Any additional $DATA attributes associated with a file will not be displayed when the contents of a directory are listed
- Information can be hidden from view simply by adding text to the base file name
  - Text.txt:hidden.txt
- Makestrm.exe = utility that moves data from file to an alternate data stream linked to the original file

NTFS Alternate Stream Detection

- Most file system forensic tools will record Alternate Data Streams by displaying all $DATA attributes associated with a file in the Master File Table
  - Encase
  - The Sleuth Kit
  - FTK

- To delete the stream file
  - Copy first file to a FAT partition
  - Copy file from FAT to NTFS partition
  - Stream feature does not exist in FAT

Trojan Programs

- Trojans can communicate via overt or covert channels
- Trojans that communicate via covert channels are classified as Backdoor programs
- Backdoor program is any type of program that will allow an attacker to connect to a computer without going through the normal authentication process

Trojan Infection Mechanisms

- **Peer-to-Peer Networks (PZP)**
  - Kazaa
  - Imesh
  - Aimster
  - gnutella
- **Instant Messaging (IM)**
- **Internet Relay Chat (IRC)**
- **Email Attachments**
- **Physical access**
- **Software Vulnerabilities**

Trojan Program Examples

- **Tini**
  - Simple and small backdoor Trojan written fear Windows
  - Coded in Assembler
  - Listens on TCP port 7777
  - Provides a remote command prompt

- **Qaz**
  - Backdoor Trojan
  - Renames Notepad.exe to Note. com
  - Copies itself to the system as Notepad.exe
  - Will call the original Notepad.exe to remain hidden
  - Uses Winsock and connects on port 7597

Remote Access Trojans

- **Donald Dick**
  - Can use IP or SPX on default ports of 23476 and 23477
  - Attacker can access the local file system browse, create, remove directories, edit the registry
  - Will add Lsasup.exe, pruss.exe, samcfg.exe and bootexec.exe to the system32 folder under Windows 2000 or XP
  - Will be added to the registry for automatic restart
  - Can use either GUI or command-line for control

Remote Access Trojans

- **Net Bus**
  - Server portion of the Trojan named patch.exe and has a default size of 483KB
  - Will install a file called KeyHook.dll on the target system
  - Listens on TCP port 12345 for remote clients responds on TCP port 12346
  - Once the Net Bus server (on the victim's computer) is contacted, will create two files
    - Hosts.txt = Lists hosts that have contacted the server if logging enabled
    - Memo.txt = Remote user can leave a note

Remote Access Trojans

- **Back Orifice / Back Orifice 2000**
  - Designed to accept a variety of specially designed plug-ins
  - Supports encryption between client and server
  - Can use TCP, more robust protocol
  - Can use UDP to traverse a firewall
  - Provides Keystroke logging
  - HTTP file system browsing
  - Management of network file shares
  - Registry editing
  - Port redirection

Remote Access Trojans

- **Sub Seven**
  - Can mutate to avoid fingerprint detection
  - Has a server component 'installed on the target
  - Uses client installed on attacker's computer
  - Will copy file called Watching.dll on the target
  - Server uses TCP ports 6711, 6712, and 6713
  - Provides keystroke logging
  - Provides Web cam access
  - Provides Microphone access
  - Provides File access
  - Provides Local network sniffing

Remote Access Trojans

- **Let Me Rule**
  - Remote access trojan
  - Written in Delphi
  - Uses TCP port 260971

- **RECUB**
  - Unix or Windows
  - Provides RC4 encryption
  - Provides code injection
  - Provides encrypted ICMP communications

- **Phatbot**
  - Variant of Agobot / IRC bot
  - Can steal information
  - Forwards information using P2P
  - Can kill antivirus or software firewalls

Trojan And Backdoor Countermeasures

- Antivirus
- Education
- Integrity checking software
- Intrusion Detection Systems
- Honeypots

Covert Channel Countermeasures

- The possibility of covert channels cannot be completely eliminated, although it can be significantly reduced by careful design and analysis.

Questions???

For more information, please contact:
CommonwealthSecurity@VITA.Virginia.Gov

Thank You!

Where's the BeEF? XSS Demo

Eric Taylor

Northrop Grumman Enterprise Security Architect

INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Where's the BeEF? XSS Demo

- Hacker's view of the web
- Cross-site Scripting in depth
- Live Demo - browser exploitation framework (BeEF) and metasploit
- Defenses
- References

Hacker's view of the web

- Web applications are attack vectors for targeting clients and the server.
  - **All that is needed**; a web browser, Internet connection… and a clear mind.
- Web applications are the most likely place to find security issues.
- SSL only prevents us from listening or manipulating request or responses on the network. Control either side and SSL is useless.
  - SSL hides attacks from network-based IDS/IPS sensors (usually)
- Session state is a major target.
- Authentication is a major target.

Hacker's view of the web

Web Hacks fall under the following categories:

- URL Interpretation attacks
- Input Validation attacks
- Injection attacks
  - SQL, File & Code..
- Impersonation attacks
- Buffer Overflow attacks

Cross-site Scripting in depth

- Cross-site Scripting (a.k.a XSS) is an injection attack
- Targets the client using the application
- Two types
  - **Persistent** - it occurs when the data provided by the attacker is saved by the server, and then permanently displayed on "normal" pages returned to other users in the course of regular browsing, without proper HTML escaping
  - **Reflective** - These holes show up when data provided by a web client—most commonly in HTTP query parameters or in HTML form submissions—is used immediately by server-side scripts to generate a page of results for that user, without properly sanitizing the response.
- Typical Attacks
  - Reading Cookies
  - Redirecting a user
  - Modifying content on a page

Cross-site Scripting in depth

- XSS allows for running any client-side code the browser supports
- Using JavaScript

  `Onload`

  - Change content on the page after it loads

  `Onunload`

  - Launch a pop-under window to retain control of a zombie browsers

  `Onmouseover`

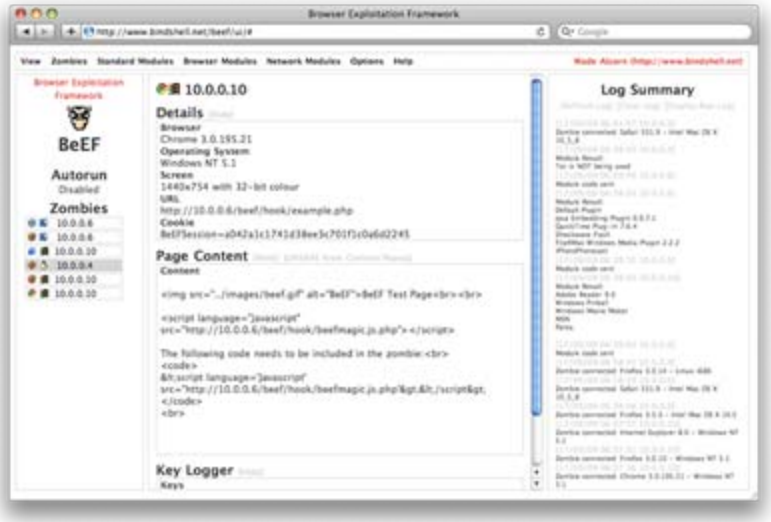
  - Track the movement of the mouse across a page

  `Onblur`

  - Send the contents of a form field to an attacker
- Document Object Model (DOM)
  - Interacting with Cookies
  - Provide form and window objects

BeEF (Browser Exploitation Framework)

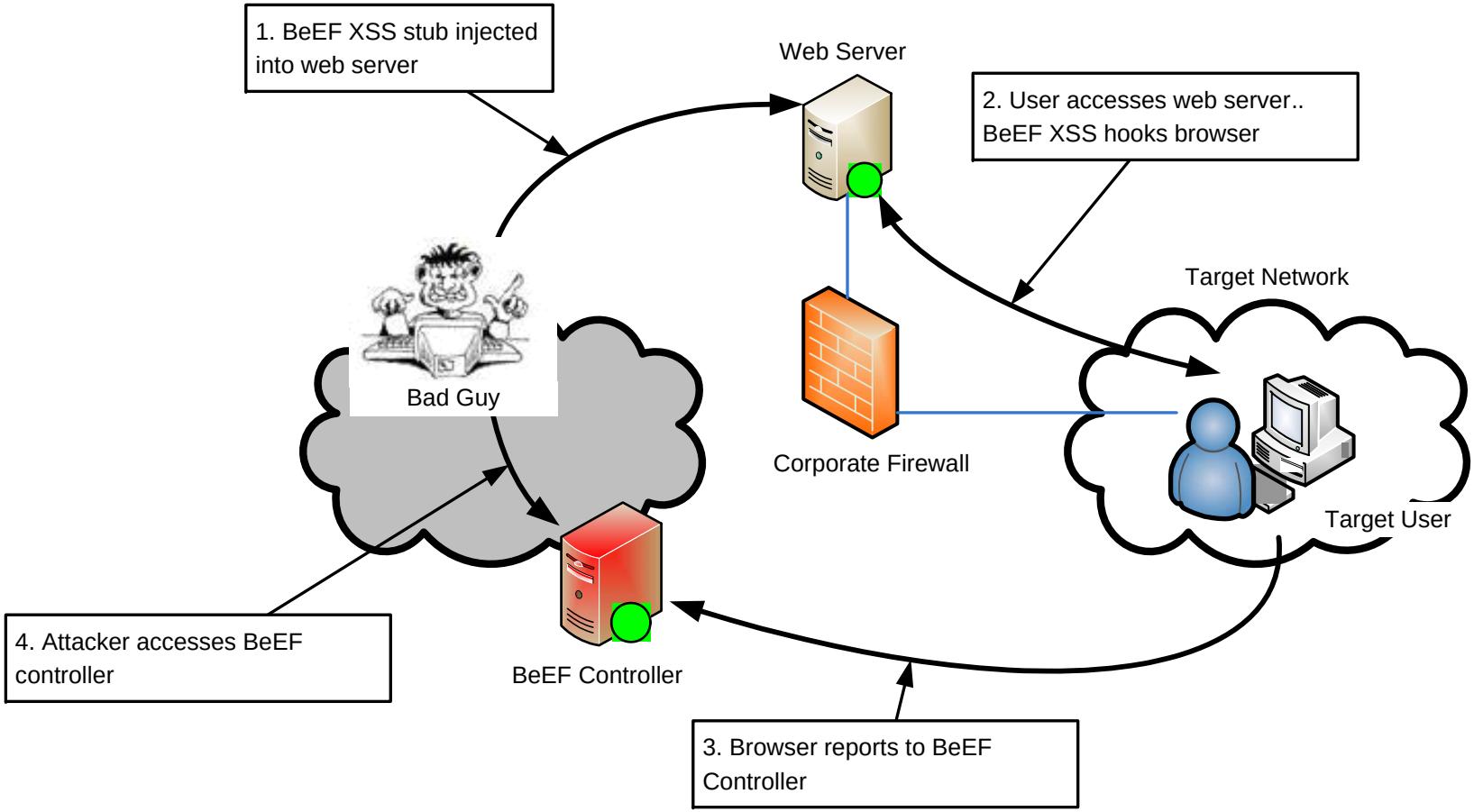
- BeEF provides an easily integratable framework that demonstrates the impact of browser and Cross-site Scripting issues in real-time. Development has focused on creating a modular framework. This has made module development a very quick and simple process.
  - Browser exploitation modules
  - Keystroke logging
  - Distributed Port Scanning
  - Integration with Metasploit via XML-RPC
  - Mozilla extension exploitation support
  - Browser functionality detection modules
- www.bindshell.net



BeEF - Inter-Protocol Communication

- Inter-Protocol Communication is the communication between two distinct protocols.
- The potential of two different protocols meaningfully communicating commands and data.
- **HTTP and IMAP3 Example:** Inter-Protocol Communication can be performed from a HTTP carrier protocol to an IMAP3 target protocol. It is possible to encapsulate IMAP3 within a web request so that valid commands can be passed to an IMAP3 server.
- Inter-Protocol Exploitation - http://www.ngssoftware.com/research/papers/InterProtocolExploitation.pdf

DEMO


1. BeEF XSS stub injected into web server
Web Server
2. User accesses web server.. BeEF XSS hooks browser
Target Network
Bad Guy
Corporate Firewall
Target User
4. Attacker accesses BeEF controller
BeEF Controller
3. Browser reports to BeEF Controller

Defenses

- End Point Security
  - Host based Intrusion Prevention
  - IE8 with XSS Filtering enabled
  - Firefox w/NoScript
  - Antivirus with Buffer Overflow protection
  - Least Privilege
- Application Protections
  - Take XSS seriously
  - Turn off HTTP TRACE support
  - OWASP **XSS (Cross Site Scripting) Prevention Cheat Sheet**
  - Keep middleware up to date!
- Web Application Firewalls

References

- BeEF – www.bindshell.net
- HTML Code Injection and Cross-site scripting http://www.technicalinfo.net/papers/CSS.html
- OWASP - **XSS (Cross Site Scripting) Prevention** http://www.owasp.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet
- How To: Prevent Cross-Site Scripting in ASP.NET http://msdn.microsoft.com/en-us/library/ms998274.aspx
- Archive of reported XSS vulnerable websites *www.**xssed**.com*

Virginia Information Technologies Agency

Commonwealth of Virginia 2009 Threat Report

Michael Watson
Director of Security Incident Management

ISOAG
1/12/10

Threat Report

- Layout the threats that are seen throughout the Commonwealth
- Identify the best methods to mitigate threats
- Establish patterns or indications that may be concerning
- Attempt to identify coordinated attacks on the Commonwealth government

Sources of Information

- Partnership Monitoring
  - Intrusion detection data
  - Electronic communication monitoring devices
  - Web content filtering
- Reported security incidents
  - Intelligence derived from these incidents
- Honeynet Data
- Web application scanning pilot
- Some data from third parties

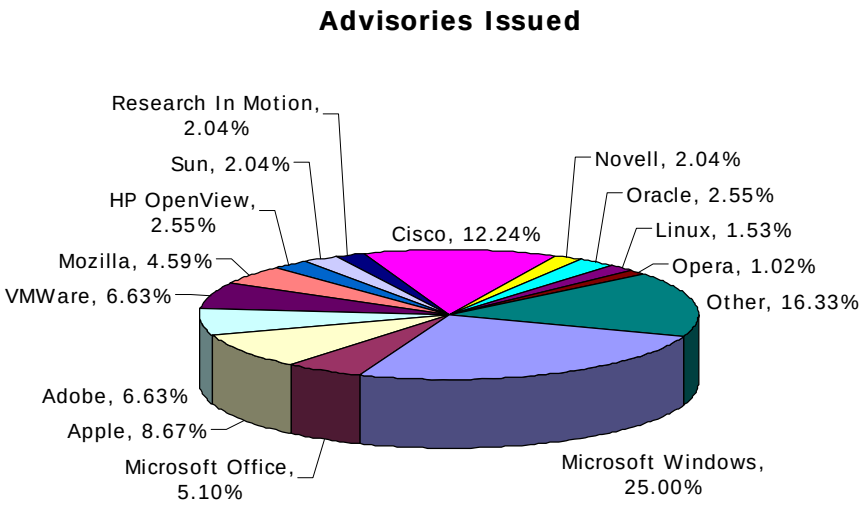
Report Overview

- Data collected is between January 1st and October 31st of 2009
- Vulnerability analysis
  - Types of advisories
  - What they mean for the Commonwealth
- Security incident trends
  - Security incidents that are frequently seen
  - Indications of future issues that are likely to become wide spread
- Data breach analysis
  - Data breaches that were recognized by the media
  - Analysis of the cause for COV breaches
- Sources of attacks on the Commonwealth
- Threats involving electronic communication

Vulnerability Analysis

- Based on number of advisories issued by Commonwealth Security

- Top 5
  - Microsoft Windows
  - Cisco
  - Microsoft Office
  - Apple
  - Adobe and VMWare



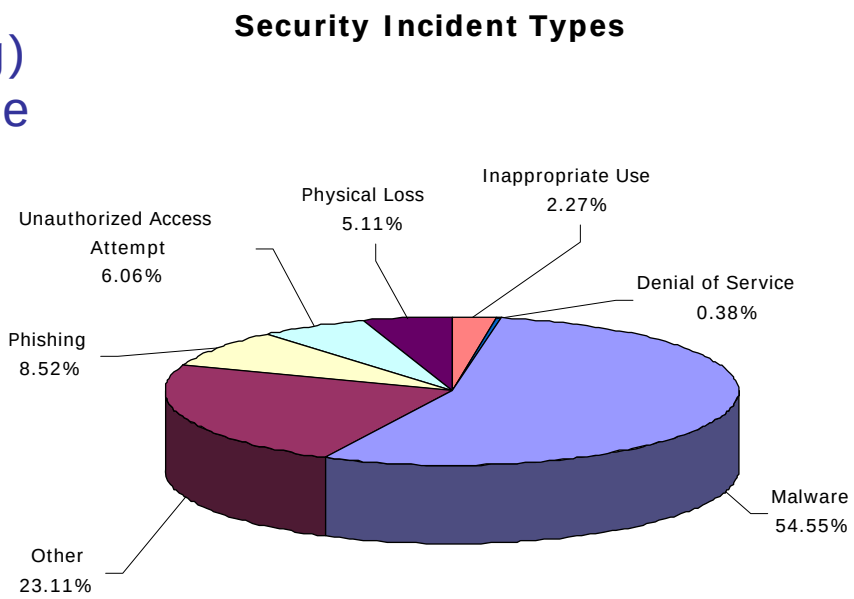
- NOTE: Linux and Oracle may appear skewed

Security Incident Trends

- Malware
  - This category identifies security incidents that involve the execution of malicious code on a system. Malware may lead to unauthorized access attempts to Commonwealth data. In that case the category of the security incident is unauthorized access.
- Phishing
  - Activity associated with theft of information from a user. Typically this type of security incident involves requesting account credentials from a user via email.
- Physical Loss
  - Any Commonwealth resource that is lost or stolen and contains Commonwealth data will be part of this category.
- Denial of Service
  - A Commonwealth service that becomes unavailable for normal use due to malicious activity.
- Unauthorized Access
  - Successful unauthorized access to Commonwealth data to Commonwealth data using another security incident category is part of Unauthorized Access Attempts. This category includes any security incident where it is unclear whether a malicious party accessed Commonwealth data.
- Inappropriate Use
  - Security incidents that involve the misuse of Commonwealth resources are part of this category.
- Other
  - Reports where the investigation determines the reported event is not truly a security incident are part of this category.

Security Incident Trends

- Rogue AV
  - Increased 585% in the first half of 2009 (antiphishing.org)
  - Most common type of malware within the Commonwealth
  - A 3 month sample of Rogue AV malware
    - 1335 infection attempts
    - 1143 cleaned or stopped automatically
    - 192 needed intervention
- Phishing
  - Spear phishing increase affecting Commonwealth entities
    - Password and account change notifications

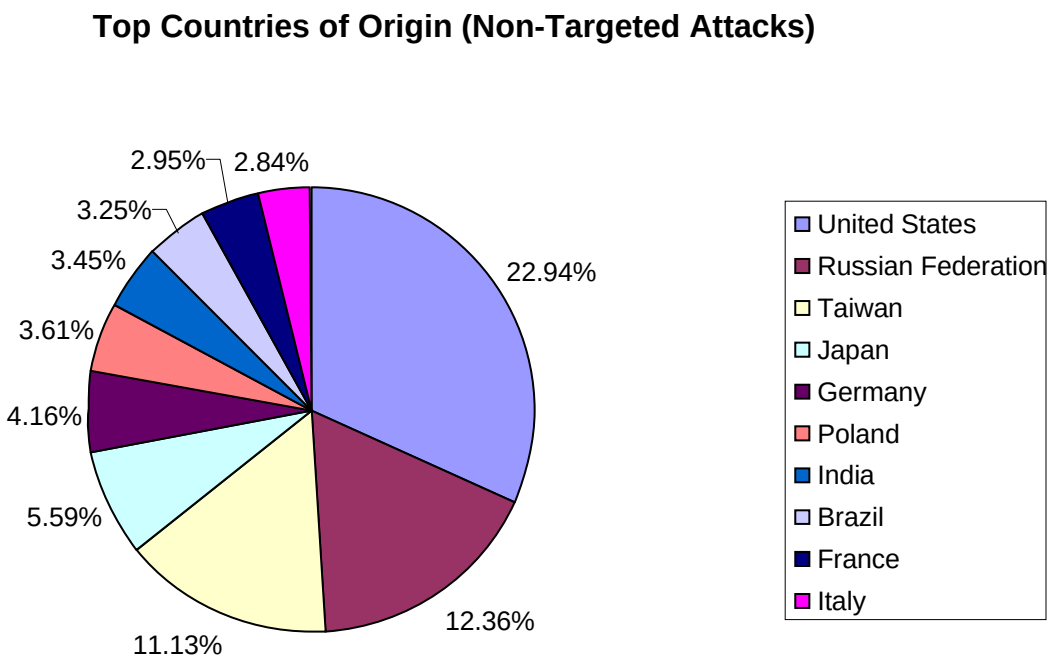


Data Breach Analysis

- Three data breaches that made the data breach repositories
- Approximately 660,000 records affected by these breaches
- Two of the three breaches were due to physical theft
- Cost in notifications alone approximately $330,000

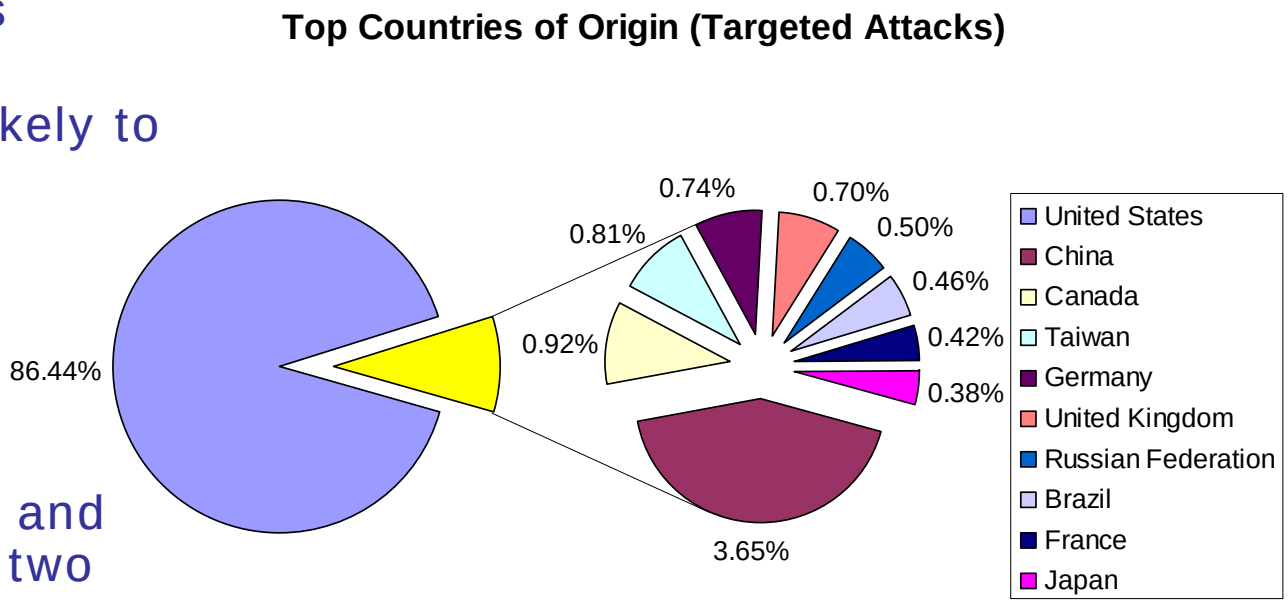
Origin of Attacks

- Autonomous malware infection attempts
- No actual infections occurred
- Most traffic due to Korgo / Padobot worm
- The United States, Russian Federation, and Taiwan are the top three sources



Origin of Attacks

- Targeted malware infection attempts
- Some infections likely to have occurred
- Traffic includes application level attacks
- The United States and China are the top two significant sources

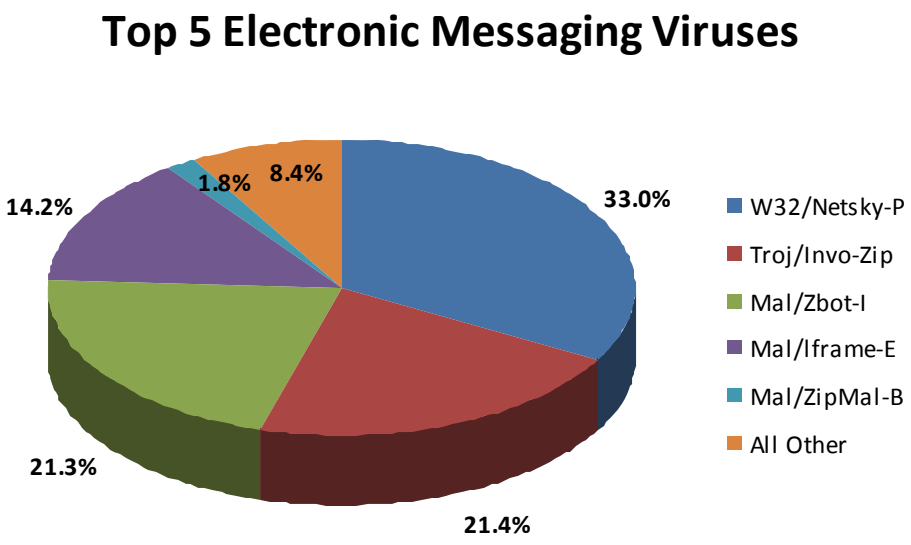


Origin of Attacks

- Origin recorded is not definitive
  - Proxies, zombies, etc.
- United States has the most unique number of IPs associated with attacks
  - Most attacks associated with applications
    - Internet Explorer
    - QuickTime
    - RealPlayer
- China was the source for a significant number of SQL injection attacks
  - Mostly unsuccessful
  - Modified behavior throughout the year
    - Fragmentation of SQL injection attacks to evade perimeter defenses
- China also primary source of Conficker worm exploit attempts
  - Likely due to unauthorized Microsoft software
- Majority of probing attempts originated in China
  - 15% of total probes belonged to a Chinese address

Electronic Messaging

- Viruses associated with electronic messaging
- Commonwealth does not receive a significant number of infected messages
- Mostly well known trojans and viruses
- Spain was the largest contributor to malicious messages



Web Application Vulnerability Pilot

- Applications varied in how long they were in production
  - Some were brand new and some were in use for many years
  - Majority of the scans were pages newly put into production or still in testing
- 25 web applications were reviewed in total
- Testing primarily for XSS and SQL injection vulnerabilities
- Most agencies mitigated vulnerabilities discovered quickly
- The small sample size did not indicate that there was a systemic problem with the public facing web applications, however there was not a significant representation of legacy applications in the sample
- Demand and number of vulnerabilities found does indicate an application vulnerability program would be beneficial

Conclusion

- Security integration has made significant progress, however much more to do
  - Establish additional points to reach
- Web application vulnerability assessment program should be established
  - Specifically addressing sensitive or internet facing web applications
- Implement methods to detect cyber attack
  - Share IDS data or summary data
  - Expand the scope of security incident reporting to include non-executive branch agencies

Questions

?

Upcoming Events

General Assembly

General Assembly convenes January 13, 2010

Future ISOAG's

From 1:00 – 4:00 pm at CESC

(please let us know if you want to host in the Richmond area!)

Wednesday -	**February 10, 2010**
Wednesday -	**March 10, 2010**
Wednesday -	**April 14, 2010**

Future IS Orientation Sessions

Monday -	March 1, 2010	1:00 – 3:30 (CESC)
Monday -	May 3, 2010	1:00 – 3:30 (CESC)
Tuesday -	July 6, 2010	1:00 – 3:30 (CESC)
Monday -	September 7, 2010	9:00 – 11:30 (CESC)

Information Security System Association

ISSA meets on the second Wednesday of every month

DATE: Wednesday, January 13, 2010
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.

PRESENTATION: Security Issues with Cloud Computing
COST: ISSA Members: $15 & Non-Members: $30 (After January 6th)

MS-ISAC Webcast

National Webcast!

Wednesday, February 24, 2010, 2:00 to 3:00 p.m.

Topic: Emerging Trends and Threats for 2010

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/

Virginia Information Technologies Agency

Commonwealth IT Security Audit Class

When: February 23, 2010
Where: James Monroe Building, 101 N. 14th Street, Richmond, VA (DGS Conference Room B, located near the Va. Credit Union, 1st Floor)
Time: 8:15 a.m. – 4:45 p.m.
Cost: $50.00 (Participants will earn 8 CPEs)
Registration: https://secure.doa.virginia.gov/hrtraining/login.cfm

Speaker: Matthew Teasdale, Dept. of Accounts. Matt retired in 2003 from the Air Force with over 26 years experience in IT Operations and Management Training. He has 3 ½ years experience in State Internal Auditing.

For questions or problems registering please contact:
Tim Sadler, Audit Manager (804-225-3106, ext. 23 or tim.sadler@doa.virginia.gov)

Identity Theft Red Flags Rules Extended Until June 1, 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 June 1, 2010. Read the FAQ at: http://www.ftc.gov/bcp/edu/microsites/redflagesrule/index.shtml

Security Awareness Tools

For those of you here in Chester, we have Security Awareness Tools available for you!

Security Bookmarks!
Security Brochures!
Security Posters!
Duh's of Security DVD!

– All of these tools and many more can be downloaded from the toolkit website

http://www.vita.virginia.gov/security/default.aspx?id=5146

Any Other Business ??????

ADJOURN

THANK YOU FOR ATTENDING