



Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

June 18, 2008





ISOAG June 2008 Agenda

- | | | |
|-------|--|---|
| I. | Welcome and Opening Remarks | Peggy Ward, VITA |
| II. | JCOTS SSN Collection Survey | Peggy Ward, VITA |
| III. | Chesterfield County Information Security Program | Sandy Graham, Chesterfield County |
| IV. | VITA Help Desk | Chad Carter, VITA |
| V. | Partnership Security Update | Don Kendrick, Matt Slaight, COV IT Infrastructure Partnership |
| VI. | IT Security Standard & Guideline Revisions | Cathie Brown, VITA |
| VII. | IT Security Audit Resources | Cathie Brown, VITA |
| VIII. | Commonwealth Security Annual Report | Ed Miller, VITA |
| IX. | Honeypot Visualization | Cathie Brown, Michael Watson, VITA |
| X. | Upcoming Events & Other Business | Peggy Ward, VITA |



JCOTS SSN Collection Survey

Peggy Ward

**Chief Information Security Officer
of the Commonwealth**



New Legislatively Required Survey HB 634/SB132

**Government Data Collection and Dissemination Practices Act;
disclosure of personal information.** Joe T. May & R. Edward Houck, Patrons

“...requires state agencies to study their own collection and use of SSNs and report to the FOIA Council and JCOTS on such collection and use by October 1, 2008. The bill also contains a fourth enactment clause providing for the gathering of similar information about the use and collection of SSNs by cities, counties and towns with a population greater than 15,000.”

<http://leg1.state.va.us/cgi-bin/legp504.exe?ses=081&typ=bil&val=hb634>

JCOTS = the Joint Commission on Technology and Science



State Agency Survey of SSN Collections

3. “That every state agency subject to the provisions of the Government Data Collection and Dissemination Practices Act (§ [2.2-3800](#) et seq.) shall conduct an analysis and review of its collection and use of social security numbers, to be completed by October 1, 2008. Each such agency shall submit, no later than October 1, 2008, to the chairmen of the Freedom of Information Advisory Council and the Joint Commission on Technology and Science, on forms developed by the Council and the Commission, (i) a list of (a) all state or federal statutes authorizing or requiring the collection of social security numbers by such agency and (b) instances where social security numbers are voluntarily collected or (ii) in the absence of statutory authority to collect social security numbers, written justification explaining why continued collection is essential to its transaction of public business. In conducting such a review, each agency shall be encouraged to consider whether such collection and use is essential for its transaction of public business and to find alternative means of identifying individuals. The chairmen of the Council and the Commission may withhold from public disclosure any such lists or portions of lists as legislative working papers, if it deems that the public dissemination of such lists or portions of lists would cause a potential invasion of privacy.”



Localities Survey of SSN Collections

4. "That every county and city, and any town with a population in excess of 15,000 shall, no later than September 10, 2008, provide the Virginia Municipal League or the Virginia Association of Counties, as appropriate, information on a form agreed upon by the Virginia Municipal League, the Virginia Association of Counties and staff of the Freedom of Information Advisory Council and the Joint Commission on Technology and Science identifying (i) all state or federal statutes authorizing or requiring the collection of social security numbers by such county, city or town and (ii) instances where social security numbers are voluntarily collected or (iii) in the absence of statutory authority to collect social security numbers, written justification explaining why continued collection is essential to its transaction of public business. In conducting such a review, each such county, city or town shall be encouraged to consider whether such collection and use is essential for its transaction of public business and to find alternative means of identifying individuals. The information required by this enactment shall be submitted no later than October 1, 2008 to the chairmen of the Freedom of Information Advisory Council and the Joint Commission on Technology and Science, on forms developed by the Council and the Commission. "



Next Steps

JCOTS is developing the forms and other logistics!

Lisa Wallmeyer, Executive Director of JCOTS will

present these at the July 16 ISOAG meeting!



Questions?





Chesterfield County

**Providing a FIRST CHOICE community through excellence
in public service.**



**Information Security outside the Sandbox:
Interacting Safely & Securely with the Outside World (WWW)**

*Presented By: Sandra Graham, Chesterfield County
June 18, 2008*



Demographics



- A little background about us...
 - 5 Districts, each represented by a Board of Supervisors (BOS) elected official
 - County operations governed by the BOS
 - County Administrator, Deputy County Administrators and Constitutional Officers represent County Leadership Team
 - Information Systems Technology led by CIO



Information Security is Everyone's Business



Information Systems Technology (IST)



- IST Leadership Team
 - CIO, Chief Information Officer*
 - Barry Condrey
 - Deputy Chief Information Officer
 - Paul Hendricks
 - Applications & Web Services Director
 - Ted Maxwell

** Information Security reports to the CIO*

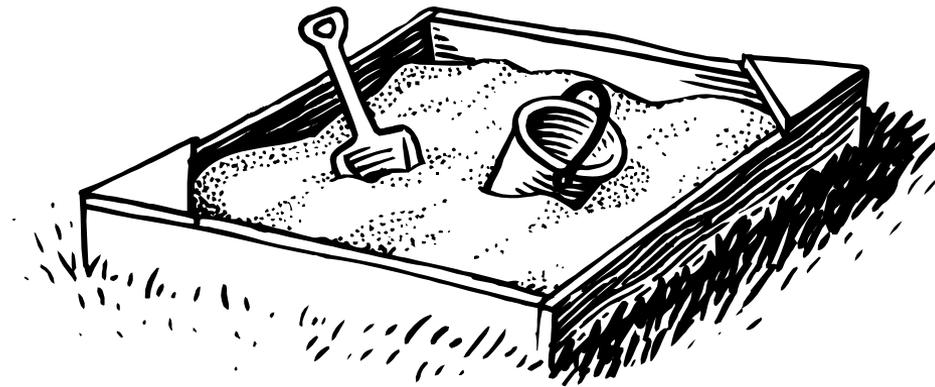
Information Security is Everyone's Business



The Security Sandbox Challenge



- *“It’s not your father’s county anymore!” Barry Condrey, CIO, Chesterfield County*
 - It’s time to learn how to play well with others...



Information Security is Everyone's Business



The Security Sandbox Challenge



- Small localities as with large government agencies, are challenged with cyber security opportunities daily.
 - *Local CISO's can no longer isolate and fully control their destiny within a small township, village, county, or city; We must now...*
 - 1. Interact outside our boundaries**
 - 2. Continue to secure our internal assets**
 - 3. Partner for success.**
 - 4. Provide Education & Awareness**

Information Security is Everyone's Business



1) Interact Outside Our Boundaries



- WWW generates business unit opportunities for improvement, growth & innovation but security controls are still necessary
 - Credit Card Processing (PCI)
 - Sensitive Communications (PII Privacy)
 - Electronic Health Records (HIPAA)
 - Electronic Transactions (Contracts) (UETA)



Information Security is Everyone's Business



2) Secure our Internal Assets



- ***Use a Security Framework to Accelerate Maturation***

- ***Good is not good enough! You need to plan for a mature Information Security Program.***

- Information Security is the front line of defense in thwarting against cyber threats and vulnerabilities, investigating and responding to cyber incidents, implementing and planning remediation of security controls, and promoting workforce security awareness for new and emerging cyber threats.



- ***Mature your security framework by mapping to ITIL, COBIT's, ISO270005, CISSP Domains (or other frameworks) to formalize best practice adoption***

Information Security is Everyone's Business

3) Partner for Success



- *MS-ISAC and VITA have provided such a partnership that is strategically preparing Chesterfield County with world-class security expertise at little or no cost; primarily built upon the framework and tool sets provided by MS-ISAC and relationship building activities with the Commonwealth of Virginia Technology office (VITA)*
 - *Provides freely available resources to states and localities for security education, incident alerting and assistance services, mentoring, and communication strategies for introducing first responder relationships with partner organizations*

Information Security is Everyone's Business

4) Provide Education & Awareness



- ***Get Leadership Buy-in***
 - Engage executive leaders in the security conversation
- ***Tailor your message for different audiences***
 - Educate those responsible for security operations
 - Promote Awareness for those who use the systems and applications
- ***Provide useable tools & resources***
 - Ensure tools and resources are not only fit for use, they are desirable resources that fulfill a need! And they are in a user-friendly cookie-cutter format. A locality doesn't need to understand new software, new methodologies, or new terminology to use the tool. In most cases it is just a cut and paste of a useful template. Chesterfield County is specifically using the MS-ISAC templates provided in the Security Awareness Toolkits



Information Security is Everyone's Business

IST Leadership Support is Key!

- ***Changing of the Guard...***

- Retirement Transition

- 30 Years+ under previous Director & Asst. Director
- CIO Strategy – Closer Alignment with Business Leaders
- Commitment to Growth & Innovation
- Increased Understanding and Support of Information Security Issues & Opportunities

- Renewed Focus on Information Security

- ISSC Re-vitalized
- All Information Security policies being Renovated
- Renewed Awareness Efforts
- Revived SDLC & Change Management Integration
- Responsible Vendor Management
- Improved automation of security processes (on-boarding, etc.)
- Accountability through Focused Reporting & Metrics

Information Security is Everyone's Business





Information Security Strategy



- **1) Interact Outside Our Boundaries**
 - ISSC (Information Security Steering Committee)
 - TIP (Technology Improvement Plan)
 - Business Risk Assessment
 - Incident Response
- **2) Continue to Secure our Internal Assets**
 - 26 Processes Identified for Improvement
 - Mapping to ITIL, Cobit's, NIST & ISO-27005
 - SAR (Security Architecture Review)
 - Acquisitions (Boiler Plate Language for Security)
 - Penetration Testing (Quarterly)
 - Change Management
- **3) Partner for Success**
 - MS-ISAC
 - VITA
 - InfraGard
 - Other Localities (Va. Beach – Secure Communications)
- **4) Provide Education & Awareness**
 - MOAT
 - Cyber-Month Activities, Newsletters, Monthly Tips
 - Chesterfield University Information Security Training
 - NEO (New Employee Orientation Program)



Information Security is Everyone's Business

Information Security Outlook



- ***Our outlook is great! With use of mature resources, tools, processes, and partnerships, Chesterfield County will become a first-class Information Security Program, modeled after world class leaders in security.***
 - ***Chesterfield and it's partners did it collectively but we will benefit as a whole. Our partners are putting expertise in dealing with national issues in the hands of local government so we do not become the weakest link in our nation's cyber security efforts.***

Information Security is Everyone's Business

Questions?

- Thank You!
-



Help Desk Overview

Chad Carter

June 18, 2008



NORTHROP GRUMMAN

Help Desk Introduction

<p>Project Description</p>	<p>The Partnership is responsible for providing a first-point-of-contact (FPOC) Help Desk and for providing end-to-end ownership (e.g., logging, tracking, resolution and reporting) of Help Desk Trouble Tickets and Service Requests.</p> <p>Types of issues to be handled include:</p> <ul style="list-style-type: none"> • Requests for information • Help Desk Trouble Tickets (Break fix) • Service Requests • IMACs (Install, Move, Add, and Change) • Password Resets • Logging and routing of out-of-scope applications (i.e. Agency applications)
<p>Purpose and Benefits</p>	<ul style="list-style-type: none"> • Improve end-to-end tracking, resolution management, and performance reporting • Improve the Commonwealth of Virginia’s efficiency and effectiveness by adopting vendor leveraged knowledge databases and best practices in the areas of customer reporting, logging, tracking, resolving of IT problems and Service Requests • Support availability 24 X 7 X 365 • Single point of contact • Web based portal for end user with self help content • Agency applications tracking (<i>optional feature</i>)

Help Desk Implementation

Occurs in two phases:

Phase I – Implementation of ServiceCenter 6.1
(Peregrine)

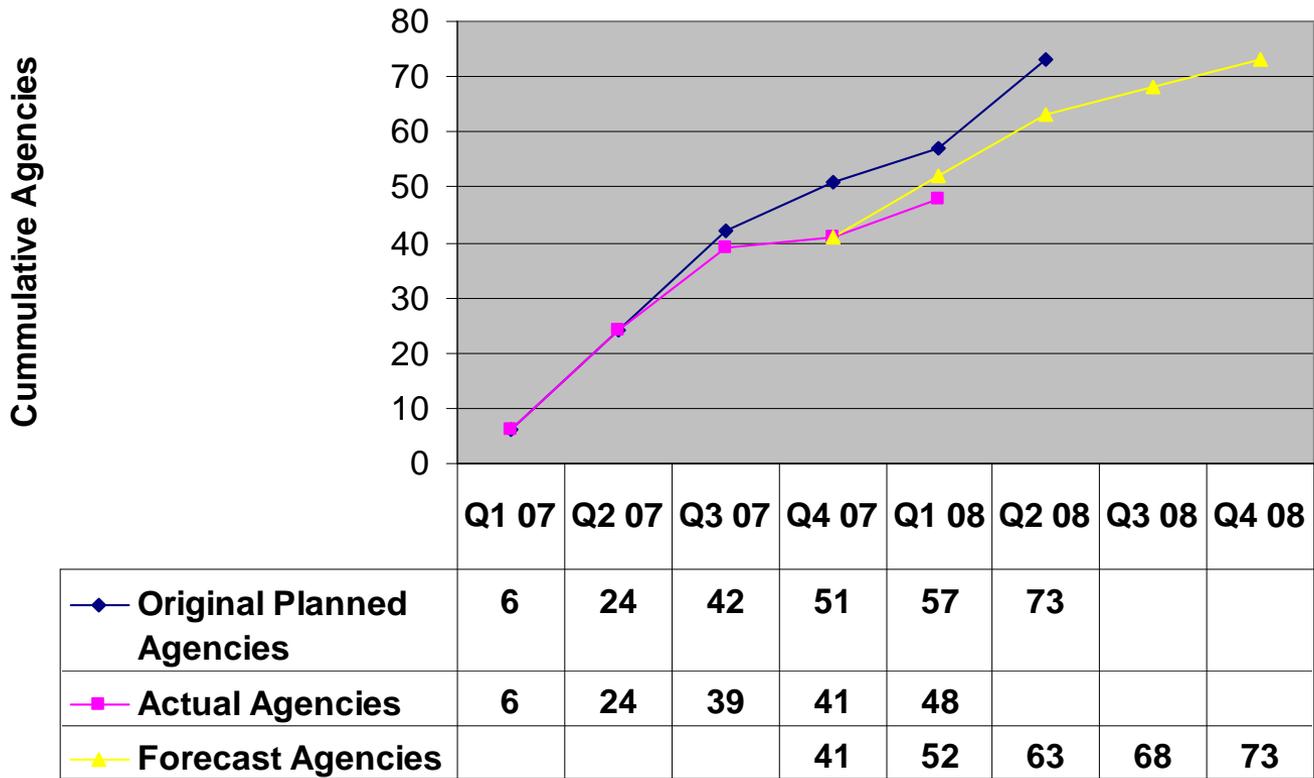
- * Training onsite personnel
- * Configuration of tool
- * Gathering reporting requirements

Phase 2 – End-users start calling the Help Desk

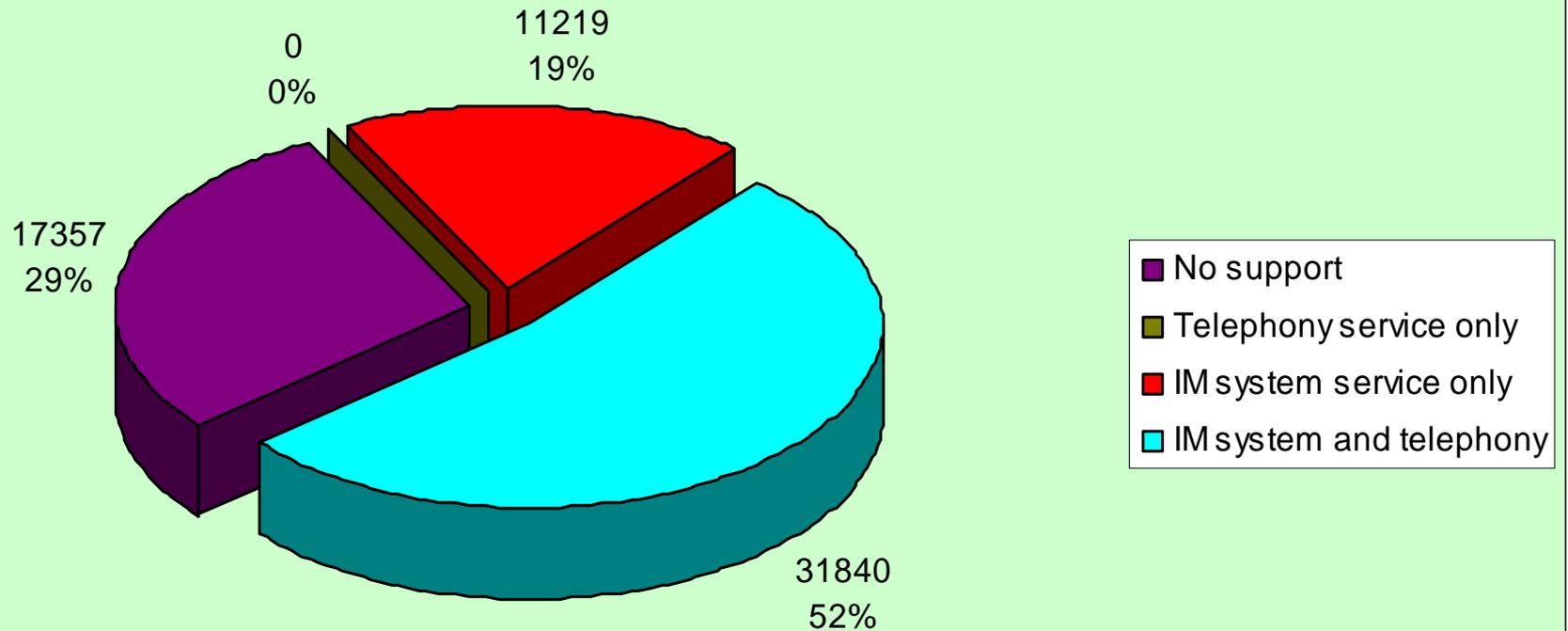
- * Configuration of VRU
- * Capturing solutions/processes in Knowledgebase

Peregrine Rollout Status

Peregrine Rollout Plan



Coverage of End-Users by July 1st



Security Related Issues

Peregrine resides in a MSP environment meaning that multiple clients are on the same instance.

- * Mitigated risk of shared data via Mandanten Security.
- * Peregrine has received VAR (VITA Architectural Review) approval.
- * Risk Assessment complete.

Identity Management

- * Legacy process of verifying last four of social and ‘special’ word still in use.
- * Work around to use P-Synch as an alternate way of entitling callers has not been approved.

Questions???



Partnership Security Update

Don Kendrick, Senior Manager of Security Operations, VITA

Matt Slaight, Senior Information Security Manager, Northrop Grumman

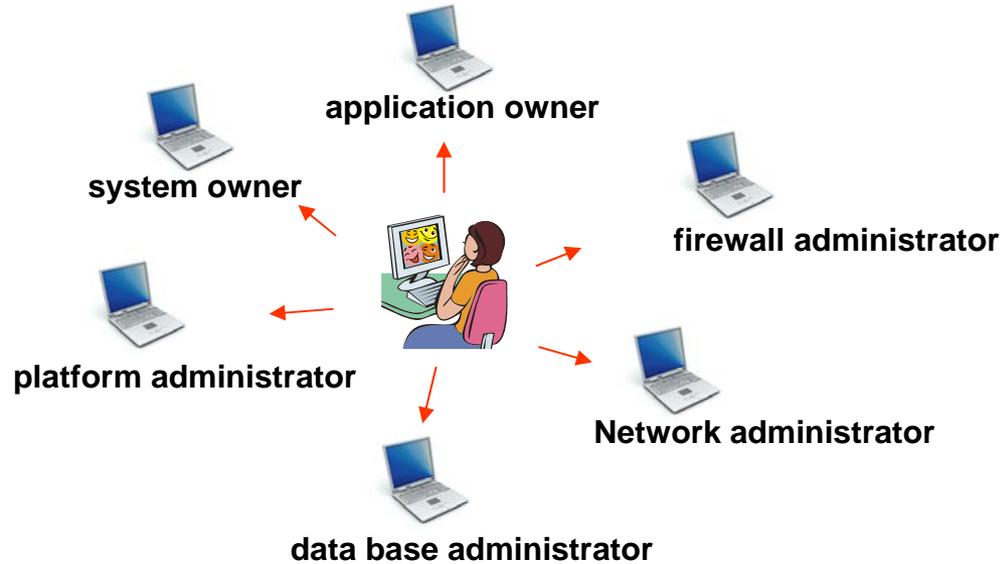


AGENDA

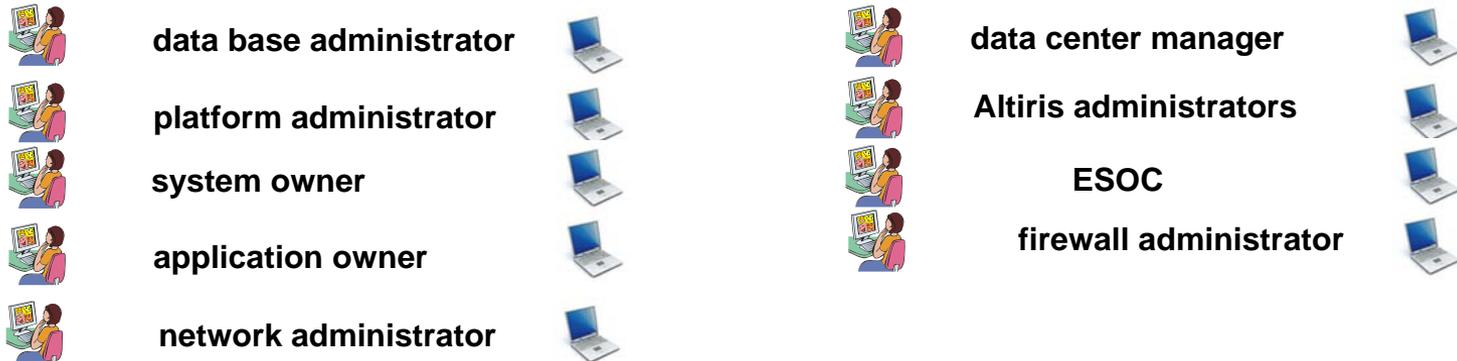
1. Altiris update
2. Questions

Altiris checks and balances

Pre partnership



Post partnership



The issue under post partnership is that COV Agencies might not know these people



Altiris checks and balances II

Environment Oversight and control

Partnership trust

- Highly respected corporation working with great COV employees for the citizens of Virginia

Access control

- Granular system restrictions based on roles and functions to be performed on a server or work station. For example, an Altiris admin DOES NOT have Windows admin privileges

Separation of duties (SOD)

- Given the information on last slide, SOD is more defined than ever before. Access control methods defining rights and privileges restricted to admin designated function

Monitoring, logging and auditing

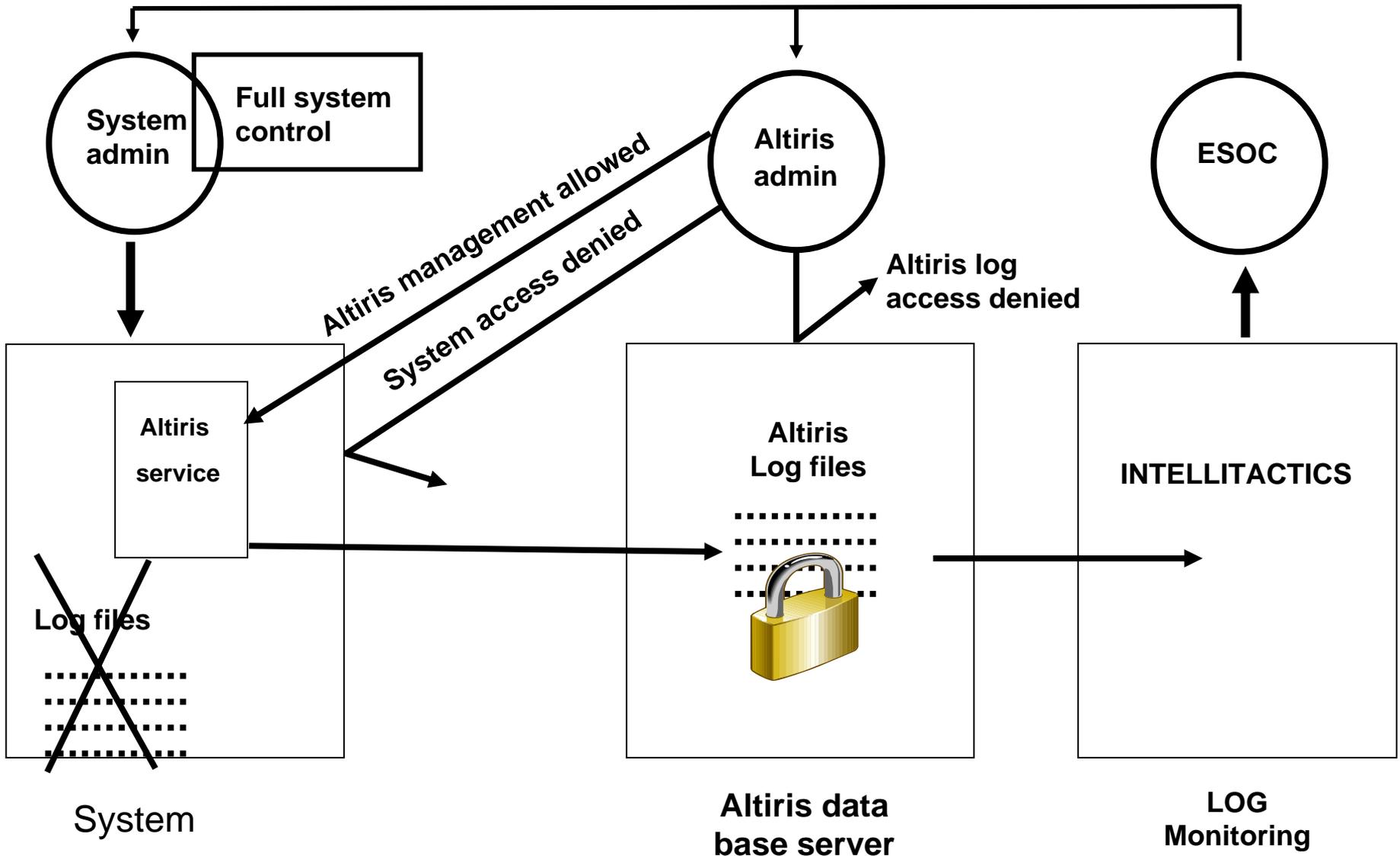
- User actions logged using native platform logging and additional technical means
- ESOC monitors information 24x7x365 for anomaly indicators, breach detection, and policy violation
- Altiris security expressions will ensure compliance to VITA security standards
- Pen tests and vulnerability scanning will reveal weaknesses
- Extensive external auditing

Staffing

- Extensive background checks and highly skilled talent
- Numerous prior COV employees



Sys admin vs Altiris admin rights



QUESTIONS?





Revisions IT Security Standard ITRM SEC 501-01

Cathie Brown, CISM, CISSP
Deputy Chief Information Security Officer



Standard - Revision 4 – July 1, 2008

- Aligns with changes to the Code of Virginia
- Documents additional and revised standards
- Includes a new section for Application Security
- Compliance date is January 1, 2009



IT Security Roles & Responsibilities

Section 2.2.2

1. As required by Section 2.3 of the *COV IT Security Policy* (ITRM Policy SEC500-02), via e-mail to VITASecurityServices@vita.virginia.gov, designate an Information Security Officer (ISO) for the agency, and provide the person's name, title and contact information to VITA no less than biennially. The Agency Head is strongly encouraged to designate at least one backup for the ISO. **Agencies with multi-geographic locations or specialized business units should consider designating deputy ISOs as needed.**



Business Impact Analysis

Section 2.3.2

4. **Determine and document any additional functions on which each essential business function depends. These identified functions are essential functions as well as previously identified.**

5. **For each essential business function:**
 - a. Determine **and document** the required recovery time for each essential business function, based on agency and COV goals and objectives.
 - b. **Determine and document the Recovery Point Objectives (RPO) for each essential business function.**
 - c. Identify the **IT** resources that support each essential business function.

Glossary

Recovery Point Objective: The measurement of the point in time to which data must be restored in order to resume processing transactions. Directly related to the amount of data that can be lost between the point of recovery and the time of the last data backup.

Recovery Time Objective (RTO): The period of time in which systems, applications or functions must be recovered after an outage.



IT System and Data Sensitivity Classification

8. Require that the agency prohibit posting any data classified as sensitive based on **confidentiality** on a public web site unless a written exception is approved by the Agency Head identifying the business case, risks, mitigating logical and physical controls, and any residual risk.



IT System and Data Backup and Restoration

For every IT system identified as sensitive **relative to availability**, each agency shall or shall require that its service provider implement backup and restoration plans to support restoration of systems and data in accordance with agency requirements. At a minimum, these plans shall address the following:

2. **Store off-site backup media in an off-site location that is geographically/separately distinct from primary location.**



Application Security

- *Purpose*

Application security requirements define the high level specifications for securely developing and deploying Commonwealth applications.

- *4.7.2 Requirements*

Each agency ISO is accountable for ensuring the following steps are followed and documented:



Application Planning

- **Data Classification** - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data. (Section 2.4)
- **Risk Assessment** – If the data classification identifies the system as sensitive a risk assessment shall be conducted before development begins and after planning is complete. (Section 2.6.2)
- **Security Requirements** – Identify and document the security requirements of the application early in the development lifecycle. For a sensitive system, this shall be done after a risk assessment is completed.
- **Security Design** – Use the results of the Data Classification process to assess and finalize any encryption, authentication and access control, and logging requirements.
- **Security shall be addressed at all life cycle stages of the software development lifecycle (SDLC).**



Application Development

The following requirements represent a minimal set of coding practices, which shall be applied to all applications which utilize untrusted data.

- **Input Validation** – Validate input from all sources. Input validation should always consider only expected input and not block input based on an arbitrary criteria.
- **Default deny** – Base access control on specific permission rather than exclusion. By default all access should be denied.
- **Principal of Least Privilege** – All processes should be performed with the least set of privileges required to complete the process.
- **Quality Assurance** – Quality assurance is one of the single most effective means of identifying and eliminating software vulnerabilities. Internal testing shall include at least one of the following: penetration testing, fuzz testing, or source code auditing. External source code auditing and/or penetration testing shall be conducted commensurate with sensitivity and risk.

Glossary

Fuzz Testing: is a software testing technique that provides random data ("fuzz") to the inputs of a program. If the program fails (for example, by crashing, or by failing built-in code assertions), the defects can be noted.



Application Development – con't

Note: Source code auditing techniques include:

- Manual code review can identify vulnerabilities as well as functional flaws, but most companies do not have the skilled security resources or time available within the software lifecycle that a manual code review requires, and therefore many companies who decide to perform manual code reviews can only analyze a small portion of their applications.
- Application penetration testing tries to identify vulnerabilities in software by launching as many known attack techniques as possible on likely access points in an attempt to bring down the application.
- Automated source code analysis tools make the process of manual code review more efficient, affordable, and achievable. This technique of code audit results in significant reduction of analysis time, actionable metrics, significant cost savings, and can be integrated into all points of the development lifecycle.



Production and Maintenance

- Applications shall be hosted on servers compliant with the Commonwealth Security requirements for host hardening. (Section 4.3.2)
- Applications classified as sensitive shall at a minimum have quarterly vulnerability assessments run against the applications and supporting server infrastructure and when any significant change to the environment or application has been made.



Logical Access Control

Account Management

- Configure systems to clear cache upon logoff.

Password Management

2. Require passwords on mobile devices such as PDAs and smart phones. For mobile phones, use a 4 to 5 digit pin number.
3. Require password complexity
 - utilize special characters,
 - not be based on a single dictionary word (ex. Bad Password: P4\$sw0rD vs. Good Password: t0YtR4p!), and utilize at least two of the following three:
 - at least eight characters in length,
 - a mix of alphabet characters and numeral,
 - combination of upper case and lower case letters.



Logical Access Control – con't

8. Require users of IT systems to change their passwords after a period of **42 days**.
 - **Note: Microsoft and Center for Internet Security are moving to 42 days = 6 weeks, notifications begin 2 weeks out - thus the user gets a 30 day password rotation for those that change at the first notification.**

10. **Maintain the last 24 passwords used in the password history files to prevent the reuse of the same or similar passwords, commensurate with sensitivity and risk.**
 - **Note: Reference CIS standards for Windows - http://www.cisecurity.org/tools2/windows/CIS_Win2003_DC_Benchmark_v2.0.pdf**



Logical Access Control – con't

17. Implement a screen saver lockout period after a minimum of 30 minutes of inactivity for COV devices. COV devices with access to sensitive systems or those devices in less physically secure environments must have a lower time out interval documented and enforced.



Data Storage Media Protection

2. Prohibit the storage of sensitive data on **any non-network storage device or media**, except for backup media, unless the data is encrypted and there is a written exception approved by the Agency Head...
Note: Non-network storage device or media, includes removable data storage media and the fixed disk drives of **all desktops** and mobile workstations, such as laptop and tablet computers, **USB drives, CDs, etc.**
5. Prohibit the auto forwarding of emails.
7. Procedures must be implemented and documented to safeguard handling of all backup media containing sensitive data. Encryption of backup media shall be considered where the data is Personal Health Information (PHI) or Personally Identifiable Information (PII). Where encryption is not a viable option, mitigating controls and procedures must be implemented and documented.



Encryption

3. Require encryption during transmission of data **that is sensitive relative to confidentiality and integrity.**



IT Personnel Security

1. Perform background investigations of **all internal IT System users** based on access to sensitive IT systems or data. **Existing users may be grandfathered under the policy and may not be required to have background investigations.**
6. Document practices to temporarily disable physical and logical access rights when personnel are out for prolonged period in excess of 30 days due to disability or other authorized purpose.
7. Disable physical and logical access rights upon suspension of personnel for disciplinary purposes.



Email Communications

Purpose

Unsecured email shall not be used to send sensitive data if there is no encryption. As stated in section 6.3.2 of this standard, encryption is required for the transmission of data that is sensitive relative to confidentiality and integrity. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus. An email disclaimer is a set of statements that are either prepended or appended to emails. These statements are frequently used to create awareness of how to treat the data in the email. An email disclaimer is not a substitute for judgment on what content to put into an email.



Email Communications – con't

Email Disclosure Requirements

The ISO must consult with the agency's legal counsel before adopting an email disclaimer. Emails sent from Commonwealth systems are public records of the Commonwealth of Virginia and must be managed as such. Following is an example of an email disclaimer for consideration when meeting with your agency's legal counsel.

The information in this email and any attachments may be confidential and privileged. Access to this email by anyone other than the intended addressee is unauthorized. If you are not the intended recipient (or the employee or agent responsible for delivering this information to the intended recipient) please notify the sender by reply email and immediately delete this email and any copies from your computer and/or storage system. The sender does not authorize the use, distribution, disclosure or reproduction of this email (or any part of its contents) by anyone other than the intended recipient(s).

No representation is made that this email and any attachments are free of viruses. Virus scanning is recommended and is the responsibility of the recipient.



IT Security Incident Handling

Requirements

Each agency shall **document IT security incident handling practices and where appropriate the agency shall incorporate** its service provider's **procedures for** incident handling practices that include the following components, at a minimum:



Data Breach Notification

Requirements

Each agency shall:

- Identify all agency systems, processes, and logical and physical data storage locations (whether held by the agency or a third party) that contain **Personal Information** which means a combination of a first name, **or first initial, last name**, and any of the following:
 - Social security number
 - Drivers license or state identification card number
 - Financial account number, credit or debit card number **and/or the corresponding password, security, or access codes.**



Data Breach Notification – con't

3. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted **and/or unredacted Personal Information** by any mechanism, including, but not limited to:
 - Theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's, tapes, USB drives, SD cards, etc.;
 - Theft or loss of physical hardcopy
 - Security compromise of any system.
- **If the unauthorized release includes data that will allow or facilitate the decryption of data, the entity must treat the data as it is unencrypted.**
- **If a data custodian is the entity involved in the data breach they must alert the data owner so that the data owner can notify the affected individuals.**



Data Breach Notification – con't

4. In the case, a computer is found to be infected with malware that exposes data to unauthorized access, individuals that may have had their information exposed due to use of that computer must be alerted in accordance with data breach rules.

5. Provide notification that consists of:
 - a. A general description of what occurred and when;
 - b. The type of **personal information** that was involved;
 - c. What actions have been taken to protect the individual's personal information from further unauthorized disclosure;
 - d. What, if anything, the agency will do to assist affected individuals, including **a telephone number, if one exists, and additional contact information** for more information and assistance; and
 - e. What actions the agency recommends that the individual take. **The actions recommended should be in addition to monitoring the affected parties credit report and reviewing their account statements.**



Data Breach Notification – con't

6. Provide this notification by one or more of the following methodologies, listed in order of preference:
 - a. Standard mailing for any affected individuals to their last known postal address.
 - b. Electronic **Notice**
 - c. **Telephone Notice**
 - d. **Substitute Notice** - In the case of large scale data breaches the entity can use substitute notice to inform the affected individuals. Substitute notice consists of notice by email, conspicuous posting on the entity's website, and notice to major statewide media including newspaper, radio, and television. A breach may use substitute notice if it meets any of the following requirements:
 - i. Where the forms of communication listed above will incur costs exceeding \$50,000 and they affect more than 100,000 individuals
 - ii. Sufficient contact information is not available
 - iii. Legal consent is necessary to release or access the information required to contact the involved individuals.



Data Breach Notification – con't

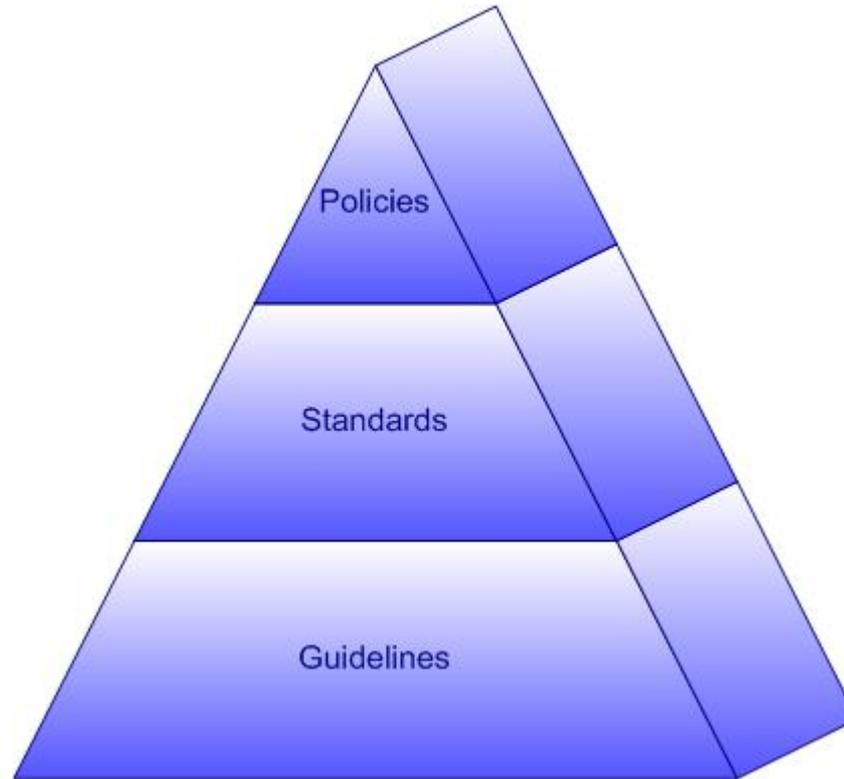
- 7. Provide notice to the OAG if unencrypted and/or unredacted personal information is exposed. Personal information is considered redacted if the following applies to the exposed information:**
 - Five digits of a SSN are visible.
 - The last four digits of a driver's license number or state identification card are visible.
 - The last four digits of an account number are visible.



IT Systems Security Guideline

- ITRM SEC514-00
 - 24 Comments Received on ORCA
 - 16 relate to formatting (changed)
 - 2 request additional definitions (changed)
 - 1 duplicate
 - 4 changes under consideration
 - Response to Comments by 6/20/08
 - Publish by 6/30/08

Questions and/or Comments?



Thank you!



IT Security Audit Resources

Cathie Brown, CISSP, CISM
Deputy Chief Information Security Officer



Purpose

To provide agencies with information regarding identifying resources to conduct Information Technology (IT) Security Audits to meet the requirements of the Commonwealth IT Security Audit Standard, SEC 502-00.



IT Security Audit Alternatives

IT Security Audits may be performed by a variety of sources that, in the judgment of the Agency management, have the experience and expertise required to perform IT security audits. These resources may include:

- Agency Internal Auditors,
- Internal Auditors from other agencies in the Agency's Secretariat,
- Internal Auditors from other agencies, states or localities in similar business lines (Example: Lottery IT system auditor from Maryland conducts an IT lottery system audit in Virginia,
- Internal Auditors from other agencies with leave accrued that would allow them to be hired as a wage employee,
- the Auditor of Public Accounts for IT systems they audit,
- the Commonwealth IT Infrastructure Partnership independent auditors for the IT Infrastructure component,
- a private auditing company, or
- staff of a private firm



IT Security Audit Alternatives

If an agency wishes to contract with a private auditing firm or for IT auditors from the private sector there are two contract methods within the Commonwealth that can be used:

- Supplier Managed Staff Augmentation (SMSA) and
- Advanced IT Resources Contracts.

NOTE: IT Security Audits should not be performed by the IT Systems Operations staff.



SMISA

- An hourly rate based method to augment agency staff on an as-needed basis
- Recommended for use when an agency already has existing internal audit management and staff, or the ability to design and manage the audit but needs additional personnel and/or expertise to perform one or more IT Security Audits.
- Activities must be thoroughly defined and be closely supervised by agency personnel.

Contact:

Cindy Sullivan

110 S. 7th Street, Suite 101

Richmond, VA 23219

Phone: 804-343-3840 Fax: 804-343-3843

E-mail: Cindy_Stonich@compaid.com



Advanced IT Resources Contracts

- A contract based on specified deliverables at a set price
- Recommended for use in situations where the agency has no audit project management expertise or experience available
- Advanced IT Resources are available from various firms under state contract that are able to provide a full range of IT auditing services



Advanced IT Resources Contracts

Contracts for **AIT Resources** are with the following Vendors:

- CGI
- BearingPoint
- CACI
- Northrup Grumman

Find out more about IT Advanced Resources at <http://www.vita.virginia.gov/procurement/contractBrowse.cfm?qsCat=3>



Additional Information

- How to use the resources
- Example Statement of Work

IT Security Audit Resource document is available on the [VITA Website](#) as a template for download



Questions?





Commonwealth Security Annual Report

Ed Miller

Information Security Assurance Manager





Title of Slide

§ 2.2-2009. (Effective until July 1, 2008) Additional duties of the CIO relating to security of government information.

- C. The CIO shall report to the Governor and General Assembly by December 2008 and annually thereafter, those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch and independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to the (i) Information Technology Investment Board, (ii) affected cabinet secretary, (iii) Governor, and (iv) Auditor of Public Accounts. Upon review of the security audit results in question, the Information Technology Investment Board may take action to suspend the public bodies information technology projects pursuant to subdivision 3 of § 2.2-2458, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.



Secretariat: Finance

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
DOA	NO	YES	YES	ADEQUATE	YES	NO
DPB	Extension Expired	Yes	YES	INADEQUATE	YES/UPD	NO
TRS	YES	YES	NO	INADEQUATE	YES	NO
TAX	YES	YES	YES	ADEQUATE	YES	YES



Secretariat: Administration

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
SCB	YES	NO	NO	INADEQUATE	YES	NO
CHR	NO	YES	NO	NOT SURVEYED	YES	NO
SBE	YES	NO	YES	INADQUATE	YES	NO
EDR	YES	YES	YES	NO PROGRAM	YES/UPD	NO
DGS	YES	YES	NO	ADEQUATE	YES	NO
DHRM	YES	YES	NO	INADEQUATE	YES/UPD	NO
DMBE	NO	YES	YES	NO PROGRAM	YES	NO



Secretariat: Commerce & Trade

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
BOA	YES	YES	YES	INADEQUATE	YES	NO
DBA	NO	YES	YES	INADEQUATE	YES	NO
VEDP/VTA	NO	YES	NO	INADEQUATE	YES	NO
VEC	YES	YES	YES	INADEQUATE	YES/UPD	NO
DHCD	YES	YES	NO	INADEQUATE	YES	NO
DOLI	NO	YES	YES	INADEQUATE	YES	NO
DMME	YES	YES	YES	INADEQUATE	YES	YES
DPOR	YES	YES	YES	INADEQUATE	YES	NO
VRC	EXTENSION EXPIRED	YES	YES	INADEQUATE	YES	NO
VRA	NO	NO	NO	NOT SURVEYED	NA	NO
VNDIA	NO	NO	NO	NOT SURVEYED	NA	NO
VHDA	NO	NO	NO	NOT SURVEYED	NA	NO
TIC	NO	NO	NO	NOT SURVEYED	NA	NO



Secretariat: Health & Human Resources

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
VDA	YES	YES	YES	NO PROGRAM	YES	NO
DHP	YES	YES	NO	ADEQUATE	YES	NO
VDH	YES	YES	NO	INADEQUATE	YES	YES
DMAS	YES	YES	YES	INADEQUATE	YES	NO
DMHMRSAS (CBR)	YES	YES	YES	INADEQUATE	YES	NO
DRS (VBPD, VDBVI, VDDHH, WWRC)	YES	YES	NO	ADEQUATE	YES	NO
DSS (CSARYF)	YES	YES	YES	INADEQUATE	YES/UPD	NO
TSF	NO	NO	NO	NOT SURVEYED	NO	NO



Secretariat: Education (excluding Higher Ed)

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
DOE	YES	YES	NO	INADEQUATE	YES	NO
FCMV	NO	YES	NO	NO PROGRAM	NO	NO
GH	NO	NO	NO	NO PROGRAM	NO	NO
SCHEV	EXTENSION EXPIRED	YES	NO	INADEQUATE	YES	NO
JYF	YES	YES	YES	INADEQUATE	YES	NO
LVA	YES	YES	YES	INADEQUATE	YES	NO
VMFA	EXTENSION EXPIRED	YES	YES	INADEQUATE	YES	NO
SMV	NO	YES	NO	INADEQUATE	YES	NO
VCA	NO	NO	NO	INADEQUATE	YES	NO



Secretariat: Education (Higher Ed only)

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
CNU	YES	YES	NO	ADEQUATE	NA	N/A
VMI	YES	YES	NO	ADEQUATE	NA	N/A
VCCS	YES	YES	NO	ADEQUATE	NA	YES
GMU	YES	YES	YES	INADEQUATE	NA	YES
JMU	YES	YES	NO	ADEQUATE	NA	YES
LU	YES	YES	YES	INADEQUATE	NA	YES
NSU	NO	YES	NO	INADEQUATE	NA	NO
ODU	YES	YES	YES	INADEQUATE	NA	YES
RU	YES	YES	NO	INADEQUATE	NA	YES
VSU	YES	YES	YES	INADEQUATE	NA	NO
RBC	YES	NO	NO	INADEQUATE	NA	YES
UMW	YES	YES	YES	INADEQUATE	NA	NO



Secretariat: Executive (Governor)

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
GOV	Extension Expired	YES	YES	INADEQUATE	YES	NO
OAG	NO	YES	YES	INADEQUATE	NA	NO



Secretariat: Agriculture & Forestry

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
VADACS (DCG)	YES	YES	YES	NO PROGRAM	YES	NO
DOF	YES	YES	NO	INADEQUATE	YES	N/A



Secretariat: Natural Resources

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
DCR	YES	YES	YES	INADEQUATE	YES	NO
DEQ	YES	YES	YES	INADEQUATE	YES	YES
DGIF	NO	YES	YES	INADEQUATE	YES	NO
DHR	YES	YES	YES	INADEQUATE	YES	NO
MRC	YES	YES	YES	INADEQUATE	YES/UPD	NO
VMNH	NO	YES	NO	INADEQUATE	YES	NO



Secretariat: Transportation

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
DOAV	NO	YES	YES	INADEQUATE	YES	NO
MVDB	NO	YES	NO	INADEQUATE	YES	NO
DMV	YES	YES	YES	INADEQUATE	YES	NO
DRPT	YES	YES	YES	INADEQUATE	YES	NO
VDOT	YES	YES	YES	INADEQUATE	YES	YES
VPA	NO	NO	NO	ADEQUATE	N/A	NO



Secretariat: Technology

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
CIT	YES	YES	YES	Adequate	YES	NO
VITA	YES	YES	YES	Adequate	YES	YES



Secretariat: Public Safety

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
ABC	YES	YES	YES	INADEQUATE	YES	YES
CASC	NO	NO	NO	NO PROGRAM	NO	NO
DOCE	NO	YES	NO	INADEQUATE	YES	NO
DOC	YES	YES	YES	ADEQUATE	YES	NO
DCJS	YES	YES	NO	INADEQUATE	YES	NO
DFS	YES	YES	YES	NO PROGRAM	N/A	N/A
VDEM	NO	YES	NO	INADEQUATE	YES	NO
DFP	NO	YES	YES	INADEQUATE	NO	NO
DJJ	YES	YES	YES	INADEQUATE	YES	NO
DMA	NO	NO	NO	INADEQUATE	YES	NO
VSP	YES	YES	YES	INADEQUATE	YES	N/A
DVS	NO	YES	NO	NO PROGRAM	YES	NO



Independent Branch Agencies

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
VCSP	NO	NO	NO	ADEQUATE	N/A	NO
LOTTERY	NO	YES	YES	INADEQUATE	N/A	NO
VRS	NO	YES	YES	ADEQUATE	N/A	NO
SCC	NO	NO	YES	NO PROGRAM	N/A	NO
VCU-HSA	NO	NO	NO	NOT ASSESSED	N/A	NO
VOPA	NO	NO	NO	NO PROGRAM	N/A	NO
IDC	NO	YES	NO	NO PROGRAM	N/A	NO
VWCC	NO	NO	YES	INADEQUATE	N/A	NO



Questions?





Honeypot Visualization

Michael Watson, Incident Management Director
Cathie Brown, Deputy Chief Information Security Officer





What is a honeypot/honeynet?

*A **honeypot** is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.*

*Typically a **honeynet** is used for monitoring larger and more diverse networks in which one honeypot is not sufficient.*

-wikipedia.org



Why run a honeypot?

- To better know your enemy
 - Who, where, what, how...
 - Targeted, Automated, Capture
- To better know your landscape
 - Network, OS, Applications
 - Vulnerabilities, Defenses
- Early warning & deterrence
 - Internal and external
 - Catch and capture malware.
- Research
 - Geopolitical, ISP, Prevalence
 - Worst offenders, rampant code

So it is said that if you know your enemies and know yourself, you will fight without danger in battles.

If you know only yourself, but not your opponent, you may win or you may lose.

If you know neither yourself nor your enemy, you will always endanger yourself.

- Sun Tzu



What information can be captured?

- IP Addresses – Source and Destination
- Corporate owner of the IP (ISP/Net block)
- Geolocation – Country, City, Lat & Long
- Timestamps – When did this occur
 - How many times? Histogramming...
- Type of attack – Exploit/Vulnerability
- Malicious Code – Infected with...?
 - MD5/SHA-256 Hash



Honeypot Visualization

Unique IP Count: 1188

IP Address	Block Owner	First Seen Date	Last Seen Date	Ticket #
1.150.23.140	Lotus Sp. z o.o.	2007-11-12 15:15:06	2008-05-10 23:51:58	
78.218.1.1	Ya.com Internet Factory	2008-02-06 02:19:46	2008-05-10 23:51:58	
148.132.103	JSC CenterTelecom Kaluga branch	2008-03-26 16:30:01	2008-05-10 23:51:58	
109.238.175		2008-05-01 04:32:19	2008-05-10 23:51:58	
141.242.10		2008-05-03 15:48:06	2008-05-10 23:51:58	
1236.11.100	Hanaro Telecom Co.	2008-05-08 12:11:08	2008-05-10 23:51:58	
237.166.151		2008-05-08 21:26:38	2008-05-10 23:51:58	
1255.24.155	Telefonica de Argentina	2008-05-10 23:01:33	2008-05-10 23:51:58	
209.58.1		2008-05-10 23:51:58	2008-05-10 23:51:58	
146.156.1		2008-05-10 23:51:58	2008-05-10 23:51:58	
209.116.199		2008-05-10 23:51:58	2008-05-10 23:51:58	
192.33.1	WideOpenWest	2008-05-10 23:51:58	2008-05-10 23:51:58	
10.0.0		2007-10-01 04:23:53	2008-05-10 23:46:51	
126.52.1	SoftLayer Technologies	2008-03-07 15:46:20	2008-05-10 23:46:51	
1127.11.155	SingNet Pte Ltd	2008-03-28 06:41:50	2008-05-10 23:46:51	
236.92.1	Turk Telekom	2008-05-10 23:46:51	2008-05-10 23:46:51	
1217.10.167	Office National des Postes et Telecommunications (2008-05-10 23:46:51	2008-05-10 23:46:51	
15.189.1	Telemar Norte Leste S.A.	2008-05-10 23:46:51	2008-05-10 23:46:51	
237.166.151		2008-05-10 23:46:51	2008-05-10 23:46:51	
114.78.1	Kujtesa	2008-05-10 23:46:51	2008-05-10 23:46:51	
221.26.1		2008-05-10 23:46:51	2008-05-10 23:46:51	
41.147.1	Telewest Broadband	2008-05-10 23:46:51	2008-05-10 23:46:51	
1141.76.151	sunrise	2008-05-10 23:46:51	2008-05-10 23:46:51	
146.17.15		2008-05-10 23:46:51	2008-05-10 23:46:51	

IP Address

Link to IP specific detail. Including IP history, dropped malware, relationships, etc...

ISP/Block Owner

Instant visual identification of the corporation which owns the IP address space

First/Last Seen Dates

Is this the first time the address has been seen? How old is the infection?

Honeypot Visualization

Google Mapping



OPTIONS

- Real Time
- Event Driven
- Historical
- Query Specific

LIMITATIONS

Geolocation database accuracy;
browser heavy;
data overload.



Moving Beyond Honeypot Visualization

Putting it all together... Through the use of other technologies such as sandboxing, we can start to build real profiles, stories, and relationships between malicious code, negligent and criminal networks, and the criminals that utilize them.

- Sandbox Visualization
- Command & Control Visualization
- Relationship Visualization



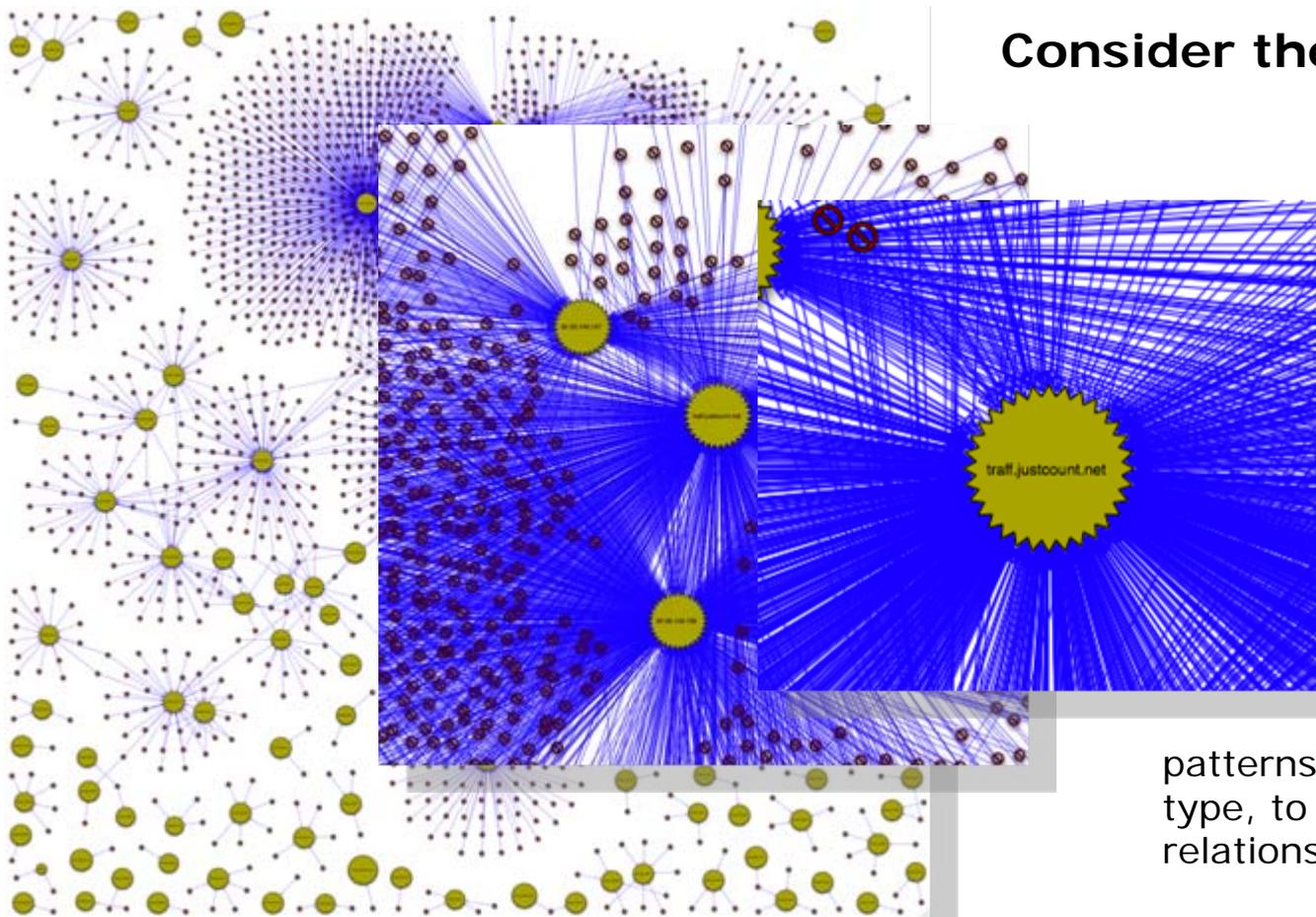
What is a sandbox?

*“In computer security, a **sandbox** is security mechanism for safely running programs. It is often used to execute untested code, or untrusted programs from unverified third-parties...”*

-wikipedia.org

Sandbox Visualization

Consider the following...



Of the thousands of malicious binaries these sandboxes and other tools capture, all are run through sandboxes. All of the malicious code's activities are captured and stored in a database. Through database queries you begin to enumerate

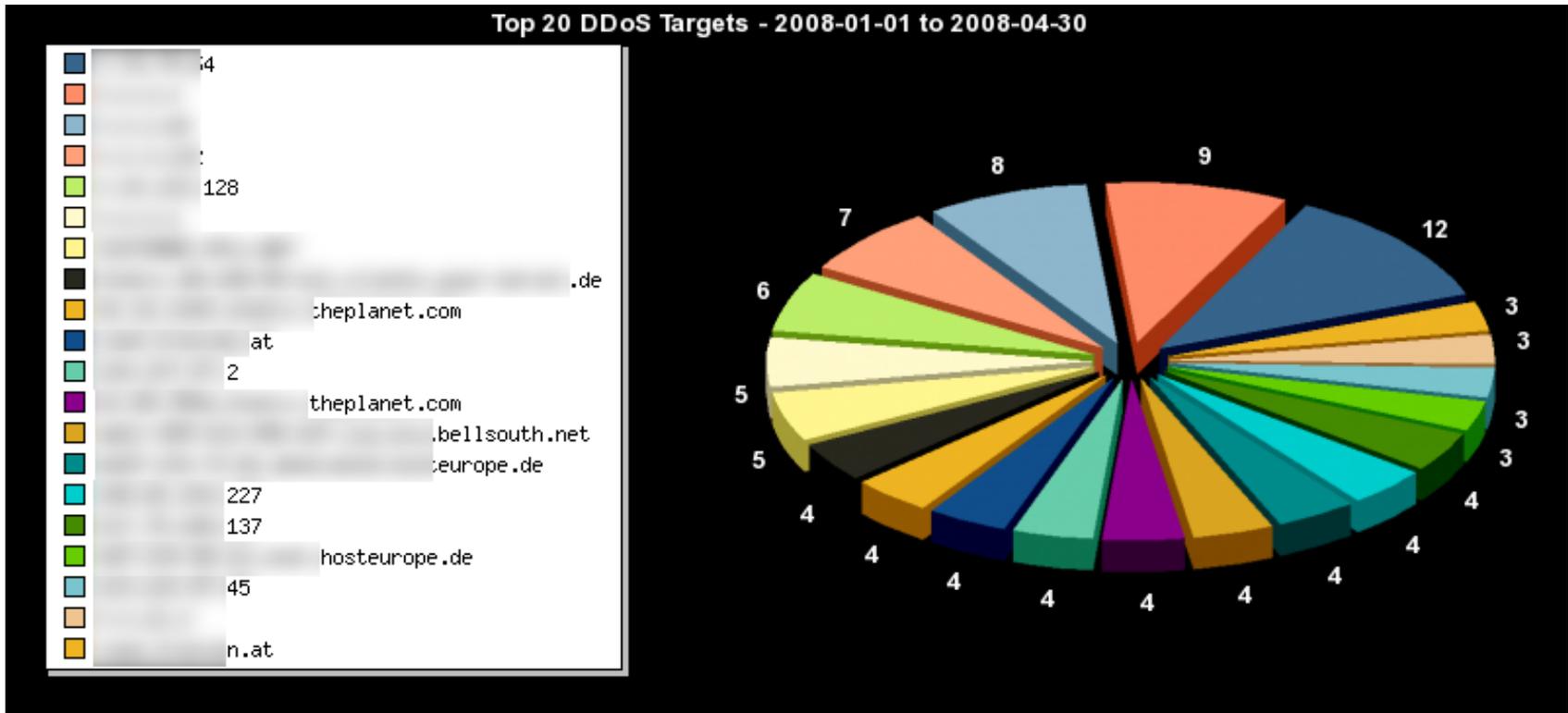
patterns of behavior. From traffic type, to network destination, to host relationships within those networks



What is Command & Control?

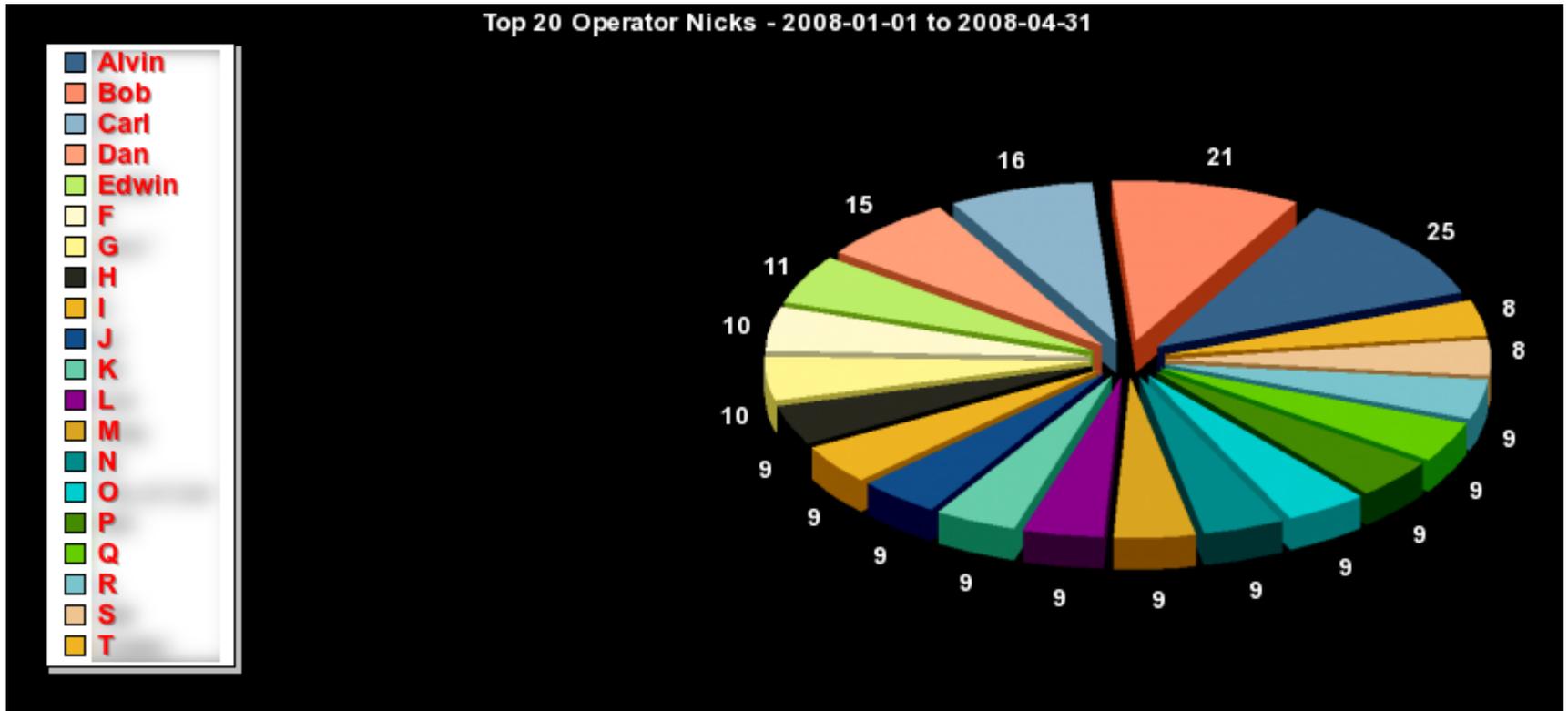
*In botnet terminology, **command and control** refers to a control point and/or control methodology used to dictate operating orders to nodes within the botnet.*

Command & Control Visualization



CAN BE IMAGE MAP LINKABLE TO COMMAND AND CONTROL ENUMERATION

Relationship Visualization



Tracking the most prevalently seen herder aliases across monitored networks.



Putting It All Together

The screenshot shows the homepage of the Commonwealth Computer Security Resource Center. At the top, it features the VITA logo and the text "Virginia Information Technologies Agency" and "Commonwealth Computer Security Resource Center". Below this is a navigation menu with links for Home, Security Bulletins, News, Weblog, and Login/Register. There are also sections for Guidance & Exchange, CCSRC (What is CCSRC, Analysis Center, Services, News/Press, Papers), and VITA (VITA Home). The main content area is titled "Security Log - Alerts, News, Blog" and contains several news items and alerts, such as "News - 02/19/07 - More Stormy Love", "Alert - 02/18/07 - Microsoft Vulnerability", "News - 02/18/07 - Spam Exploits Election?", "Blog - 02/17/07 - Malware Analysis", and "Alert - 02/15/07 - Microsoft Vulnerability". There are also sections for "Today's Most Active Malware" and "Today's Most Active Attackers".

Commonwealth Computer Security Resource Center

Portal Features

- Blog-style Informative Posts
- Statistical Analysis
- News & Alerts
- White Papers
- Subscription Alerts
- Security Resources for:
 - Home
 - Business
 - Government

Putting It All Together

Commonwealth Computer Security Resource Center

Analysis Center

- Open High Level 'World View'
- Authorized 'Net Specific Views'
- More detailed issue analysis
- Live historical analysis
- Client Sandbox Access
- Instant 'Net Alerting'



Welcome!

That image to your left is a map representing our visibility into the geographic locations from which computers are currently attacking Commonwealth of Virginia network infrastructure. If that sounds interesting to you, please feel free to look around and see what we do here! Or, if you are feeling confident feel free to jump right into the public [Analysis Center Console](#).

The [What is CCSRC](#) page gives a good oversight into what we do and why we do it. Or if you need some advice try [Guidance and Exchange](#) for helpful computer security information.

- Home
 - Security Bulletins
 - News
 - Weblog
 - Login/Register
- Guidance & Exchange
 - Home Users
 - Business Managers
 - Network Engineers/SA
 - Security Engineers
- CCSRC**
 - What is CCSRC
 - Analysis Center
 - Services
 - News/Press
 - Papers
- VITA
 - VITA Home

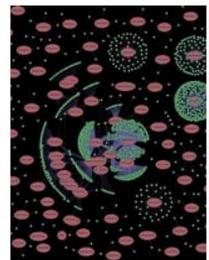


CCSRC
[Analysis Center](#)
[Public Console](#)
 (click to register or login)

The Russian Business Network Tuesday, February 19, 2008

Thanks to the diligent analysis of CCSRC staff engineers and some great security organizations and individuals, the CCSRC Analysis Center is today releasing a paper detailing the full range of...

[Read more...](#)





Questions?

Thank you!



Upcoming Events





UPCOMING EVENTS

IS Orientation

Wednesday, June 25th, 2 to 4:30 pm @ CESC

Wednesday, July 30th, 1 to 3:30 pm @ CESC

IS Orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV IT Security Policy and Standards and is open to all Commonwealth state and local government persons interested in Information Security.

To register email VITASecurityService@VITA.Virginia.gov



UPCOMING EVENTS!

NEXT ISOAG MEETING!

July 16th, 1:00 – 4:00 pm

- SSN Survey JCOTS! – Lisa Wallmeyer, JCOTS
- Roanoke County Information Security Program – Elton Ghee, Roanoke County
- eSupport – COV IT Infrastructure Partnership
- Citizens Awareness Banner – Michael Watson, VITA
- Commonwealth IT Security Policy & Standard – Cathie Brown, VITA

@ CESC



UPCOMING EVENTS

Commonwealth Information Security Council Meeting

Monday, July 21, 12:00 - 2:00 p.m. @ CESC with
Committee meetings from 2:00 - 3:30 p.m.

If you would like to attend or be on the agenda for either the Council meeting or a Committee meeting please either contact a Committee co-chair or send an email to VITASecurityServices@vita.Virginia.Gov (not vendors please)

Find out more about your Commonwealth Information Security Officer's Council at

<http://www.vita.virginia.gov/security/default.aspx?id=5128>



Any Other Business ???????



ADJOURN

THANK YOU FOR ATTENDING!!

