



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

October 5, 2011



Governor's Proclamation

Governor McDonnell has proclaimed
October 2011
as

Cyber Security Awareness Month

Proclamation can be located at the Governor's Porthole:

<http://www.governor.virginia.gov/OurCommonwealth/Proclamations/>

or VITA Information Security Awareness Toolkit:

<http://www.vita.virginia.gov/security/toolkit/default.aspx?id=9930>



MS-ISAC Cyber Security Pledge

- The Multi-State Information Sharing and Analysis Center (MS-ISAC) is celebrating Cyber Security Awareness Month with a “Cyber Pledge” contest.
- The Pledge aims to raise awareness about staying safe online and encourages individuals to confirm their commitment to doing their part to keep cyber space safe.
- The state with the most submitted pledges will be awarded seats to “Securing the Human” from SANS.
- Sign the pledge by visiting www.msisac.org and clicking on the Cyber Pledge icon.



ISOAG October 2011 Agenda

- | | | |
|------|--|---|
| I. | Welcome & Opening Remarks | Michael Watson, VITA |
| II. | Emerging Cyber Threats | SA David Crisafi, FBI |
| III. | Indirect Reconnaissance:
Information Gathering Techniques | Bob Baskette, VITA |
| IV. | 2011 Commonwealth Security
Annual Report | Michael Watson, VITA |
| V. | Upcoming Events & Other Business | Michael Watson, VITA |
| VI. | Partnership Update | Bob Baskette, VITA
Michael Clark, NG |

CYBER CRIME



Emerging Cyber Threats



FBI Richmond Division Cyber Investigations

SA David M. Crisafi
Squad 11 – Cyber
Richmond Field Office

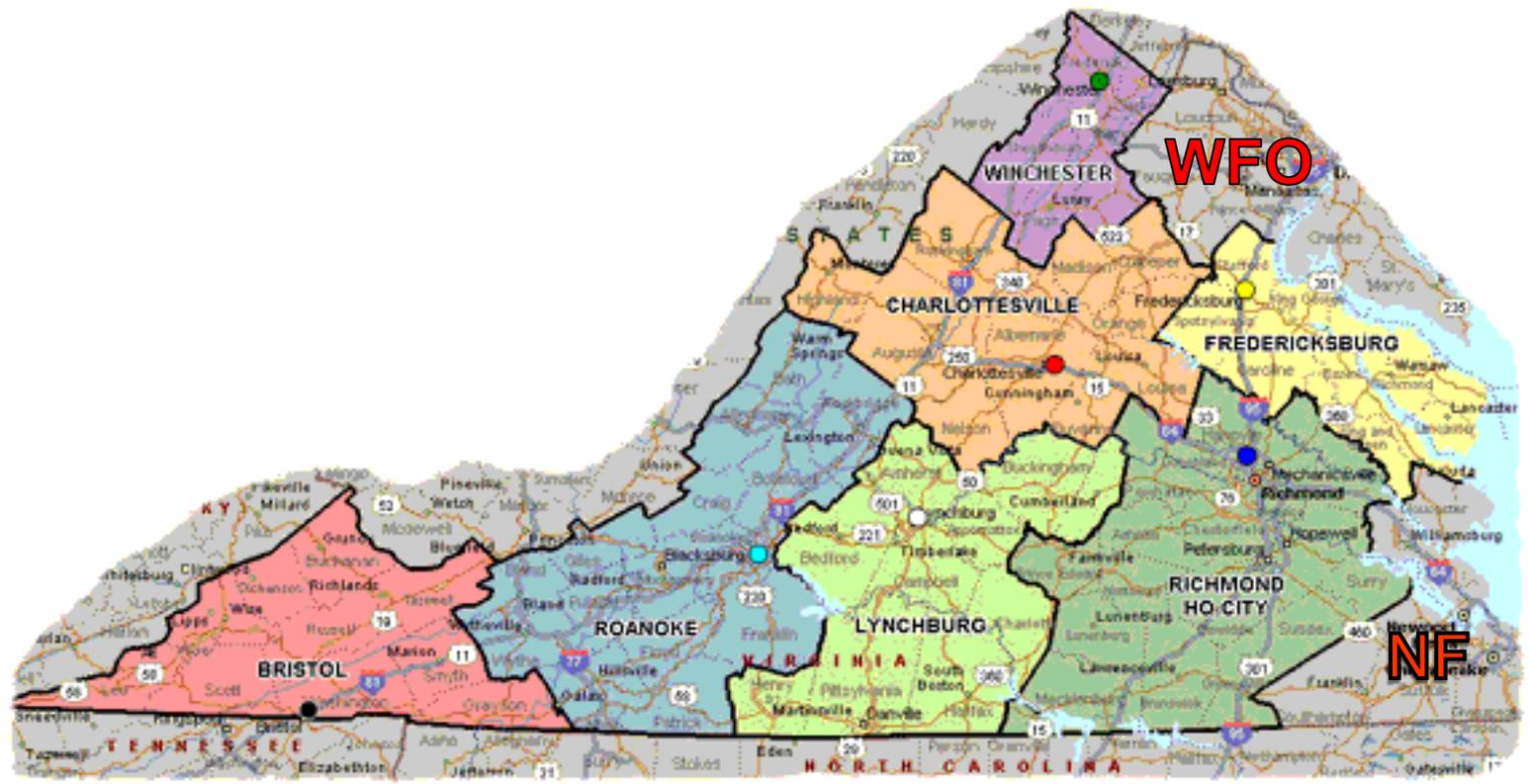
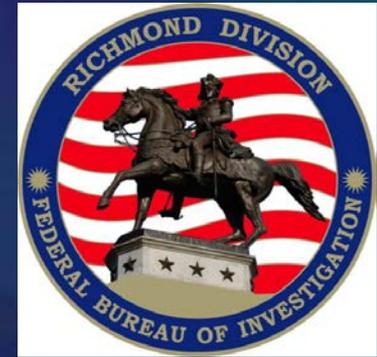


FBI Structure

- *FBIHQ in Washington, D.C.*
 - *Provides administrative, oversight, coordination, program management and investigative support functions*
- *56 Field Offices in the U.S.*
 - *Conduct investigations*
 - *Resident Agencies (Satellite Offices)*
- *> 75 Legal Attache (Legat) offices overseas*
 - *Perform liaison functions*
 - *Conduct investigations with host country authorization*



Richmond Division Territory





Richmond Field Office Squad 11 – Cyber



Supervisory Special Agent (SSA)

Melissa W. McRae

- 8 Special Agents (SA)
- 2 Intelligence Analysts (IA)
- 2 SA and 1 Support Computer Forensic Examiners
- Task Force Officers.



FBI Priorities

- Protect U.S. from terrorist attack
- Protect U.S. against foreign intelligence operations/espionage
- Protect U.S. against cyber-based attacks and high-technology crimes
- Combat public corruption
- Protect civil rights
- Combat transnational/national criminal organizations
- Combat major white-collar crime
- Combat significant violent crime
- Support federal, state, local and international partners
- Upgrade technology to support FBI's missions



FBIHQ Cyber Division



- The Cyber Division at FBIHQ was created in 2002 to consolidate the following programs:
 - *Computer Intrusion (Hacking, Denial of Service, Phishing, Botnet, Identity Theft)*
 - *Child Pornography (Enticement, Production, Distribution, Possession)*
 - *Intellectual Property Rights (Theft of Trade Secrets, Criminal Copyright/Trademark Infringement, Counterfeit Items). Emphasis on health and safety.*
 - *Internet Fraud (Credit Card, Auction)*



Cyber Division Strategy



- Four strategic objectives set by FBI Director to reduce the cyber threat in the US.
- Cyber Division's strategy is focused on achieving these four objectives while protecting the freedom, privacy, and civil liberties of Americans:
 - Identify and disrupt the most significant individuals, groups and foreign powers conducting computer intrusions, the dissemination of malicious code, or other nefarious computer supported network operations.



Cyber Division Strategy (cont.)



- Identify and disrupt online predators or groups that sexually exploit and endanger children for personal or financial gain.
- Identify and disrupt operations targeting U.S. intellectual property.
- Identify and disrupt the most significant perpetrators of Internet fraud.



Cyber Division Investigative Priorities



1. Computer Intrusions
Counterterrorism Intrusions
Counterintelligence Intrusions
Criminal Intrusions

2. Innocent Images

3. Intellectual Property

4. Internet Fraud



Attackers

Who is behind cyber attacks?

- *Computer geeks looking for bragging rights*
- *Businesses trying to gain an upper hand in the marketplace by hacking competitor websites.*
- *Criminal organizations wanting to steal your personal information and selling it on black markets*
- *Spies and terrorists looking to rob our nation of vital information or launch cyber strikes.*



Sophistication

Level One

Ankle biter or Script Kiddies

The careless Beginner

Obvious publicly available tools.

NOISY

Level Two

Black Hat Criminal Hacker

Sophisticated and crafted tools with some
"Zero Day" use.

The careful expert

QUIET

Level Three

State Actor, Insider with Valid Credentials,
Higher sophistication.

Working at multiple network layers

Zero-Day, supply chain, and worse...

SILENT



Impact of Illicit Use of Cyberspace

National Security Implications

Compromise of:

- Critical Government/Military Networks
- Government Contractor Networks
- Weapons Systems Under Development
- Financial Industry Networks

Threat to National Critical Infrastructure



Impact of Illicit Use of Cyberspace

Economic implications could result in:

- Financial losses in the Billions (?)
- Lost confidence in
 - Internet Based Commerce
 - Information Infrastructure
 - Data Integrity
- Increased security costs
- Job security
- Increased costs to businesses and consumers.

Personal safety implications:

- Health care
- Transportation
- Etc.



Computer Intrusion Statistics

- 48% of compromises take less than a day
- 75% of intrusions not detected for at least a week
- 94% require 7-31 days for containment
- Attackers have a lot of time to operate
 - Defenders are inherently disadvantaged



5 Stages of Intrusion Response

Denial

"We have a firewall and IDS installed..."

"An AV scan didn't detect anything. We're safe."

Anger

"We weren't given enough information to detect the threat."

"The FBI is hiding something..."

Bargaining

"If we re-image these boxes, we'll be safe, right?"

"Can't we just buy something that will solve this problem?"

Depression

"My job is hopeless. I give up."

"I'm going to go work for someone with a secure network."

Acceptance

"How can I limit my window of exposure?"

"How do I re-write policy to be successful in this environment?"



Investigative Process Initial Phase

- *Receive complaint (Citizens, industry groups, other agencies)*
- *Triage complaint (Violation of federal laws, venue, loss)*
- *Contact US Attorney's Office (USAO)*
- *If appropriate, open case (USAO concurrence, FBI priority, investigative resources, other factors)*
- *If not open, may refer complaint to other FBI divisions or government agencies*



Investigative Process

Investigation Phase

- *Purpose: To collect evidence*
- *Tools:*
 - *Interview*
 - *Electronic Surveillance*
 - *Physical Surveillance*
 - *Open Source/Public Database Research*
 - *Subpoena (Grand Jury/Administrative)*
 - *Court Order (2703, Pen/Trap, Title III)*
 - *Undercover Operations*
 - *Warrants (Search, Arrest)*



Investigative Process Prosecution Phase

- *Provide results of investigation to USAO*
 - *Must be able to prove all elements of a statute to prosecute*
- *If prosecute, USAO may:*
 - *Issue target letters to subject/defendant to begin plea negotiation*
 - *Seek grand jury indictment -> arrest/summon*
 - *Have agent file complaint -> arrest*
- *Plea/Trial*
- *Sentencing*



Federal Statutes

- **18, USC, Section 1030 (Fraud and Related Activity in Connection with Computers)**
- **18, USC, Section 1029 (Fraud and Related Activity in Connection with Access Devices)**
- **18, USC, Section 1832 (Theft of Trade Secrets)**
- **17, USC, Section 506 / 18, USC, Section 2319 (Criminal Copyright Infringement)**
- **18, USC, Section 2320 (Trafficking in Counterfeit Goods and Services)**
- **18, USC, Section 1341 (Mail Fraud)**
- **18, USC, Section 1343 (Wire Fraud)**
- **18, USC, Section 371 (Conspiracy)**
- **Etc...**



Working with U.S. Federal Law Enforcement

- *Tell you what we can but may be restricted by:*
 - *Grand Jury restrictions*
 - *Court order restrictions (sealed orders)*
 - *Privacy rights*
 - *Classification*
- *Press Concerns*



Internal vs. External Cyber Threats





Internal Threat Vectors

- Supply Chain / Vendor
 - Hardware, software
 - Design, Manufacture, Delivery, Installation, Upgrade/Patches, Repair.
 - Pirated SW and HW
- Remote
 - Hacking
 - DDoS



Internal Threat Vectors

cont.

- Close Access (Proximate Access)
 - Wireless sniffing
 - Hands-on installation
 - Theft of hardware
- Insider Threat
 - Foreign Intelligence Operatives
 - Industrial Spies
 - Disgruntled Employees
 - Unwitting, well-intentioned employees who violate security



Internal Threats

- E-mail
 - “Spear Phishing”
 - Phishing
 - Viruses / Malware
- Websites
 - Cross Site Scripting
 - Remote Code Execution
- Applications / Services
 - Unnecessary Open Ports
 - Un-patched Software
 - Zero Day Exploits
- Users
 - Weak Passwords
 - Social Engineering
- Wireless
 - Open Access Points
 - Unauthorized Access Points
- Unauthorized Hardware
 - Thumb Drives
 - Media players
- Etcetera



Example: HBGary Federal





Anatomy of the Attack

- SQL Injection of the Content Management System
- Username/Password DB exposed
- Basic MD5 encrypted password DB easily decrypted
- CEO and COO used simple 8 character passwords
- Same passwords used on multiple accounts including email, Twitter, and LinkedIn
- Linux server accessed with COO's stolen password, but the account only had basic system privileges
- Root access gained with unpatched exploit
- Anonymous gained accessed to gigabytes of backups and research data



Continued...



- HBGary email hosted with Google (Gmail)
- CEO's email accessed with cracked password
- CEO had administrator access to all of the company's email boxes
- Password reset on email box of HBGary Federal parent company, HBGary, CEO Greg Hogland
- Hogland's email account contained the root password for the company's website www.rootkit.com
- Social engineering ensues to gain ssh access to the system
- Access is gained, the user/password DB is exposed for all registered users



Analysis Summary

- The intrusion was not exceptional
- Standard, widely known techniques used
- Attack highly effective
- Well executed
- ***If a well respected computer security firm is susceptible to this type of attack, what does that mean for the rest of us?***



Other Recent High Profile Attacks



MySQL.com:

- SQL Injection



RSA:

- Spear Phishing
- Adobe Flash
Zero-Day Exploit



External Cyber Threats

- End Users
- Hackers
- Attack Kits
- Carder Forums
- Insecure business partners
- New technologies





Attack Kits

- Examples:
 - Zeus
 - SpyEye
- Commoditized and sold for a few thousand \$'s
- Used to steal PII and login credentials
- Commercial bank accounts targeted
- Often spread via spear phishing
- Responsible for hundreds of millions of \$ is loss



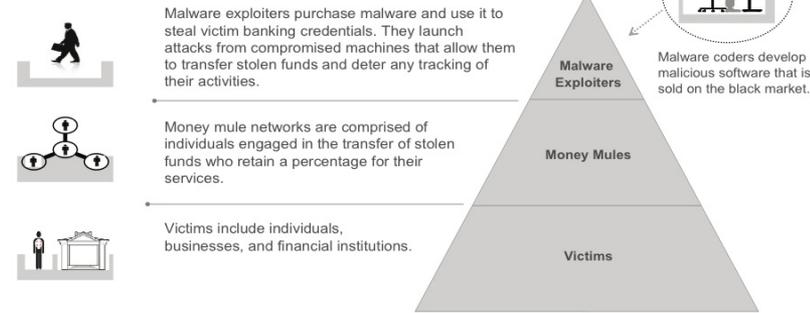
Money Mules

- Required to move stolen funds from US bank accounts to accounts controlled by attack kit operator
- Often hired via “Work-at-Home” job postings
- Reshipping scams
- Need for mules in 2011 to rise

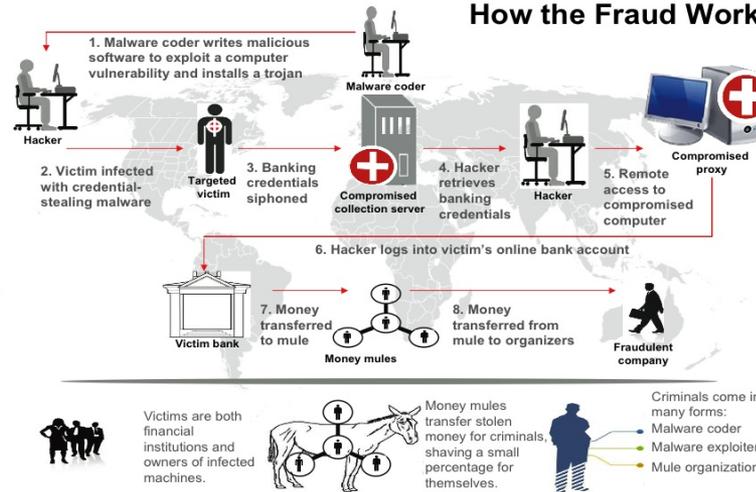




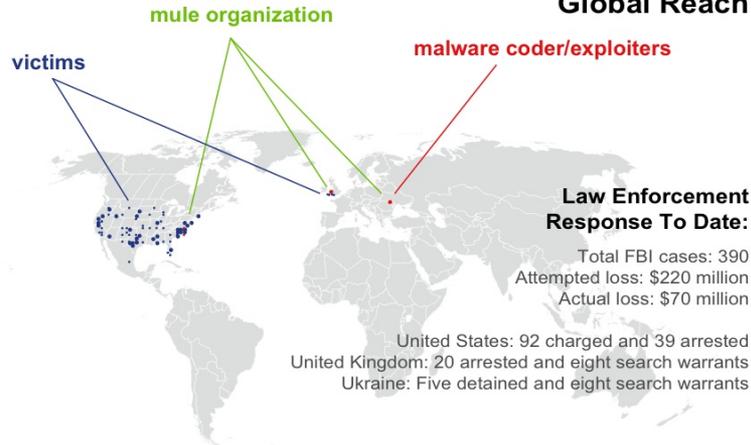
Cyber Theft Ring



How the Fraud Works



Global Reach





1. Malware coder writes malicious software to exploit a computer vulnerability and installs a trojan



2. Victim infected with credential stealing malware



3. Banking credentials siphoned



4. Hacker retrieves banking credentials



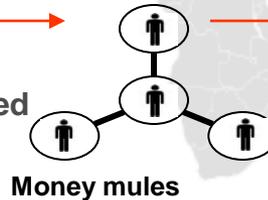
5. Remote access to compromised computer



6. Hacker logs into victim's online bank account



7. Money transferred to mule



8. Money transferred from mule to organizers

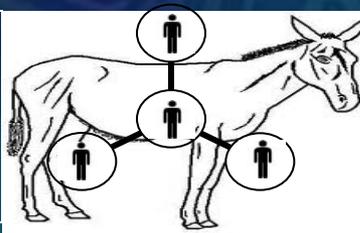


Federal Bureau of Investigation

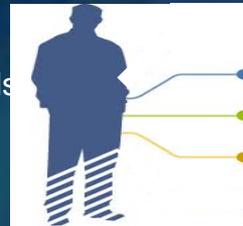
The FBI has 390 ACH cases of which have resulted in an attempted loss of ~220 million dollars and actual loss of ~70 million dollars. These cases represent over 300 victims and 3500 mules.



Victims are both financial institutions and owners of infected machines.



Money mules transfer stolen money for criminals shaving a small percentage for themselves.



Criminals come in many forms:
Malware coder
Mule organization
Malware exploiters

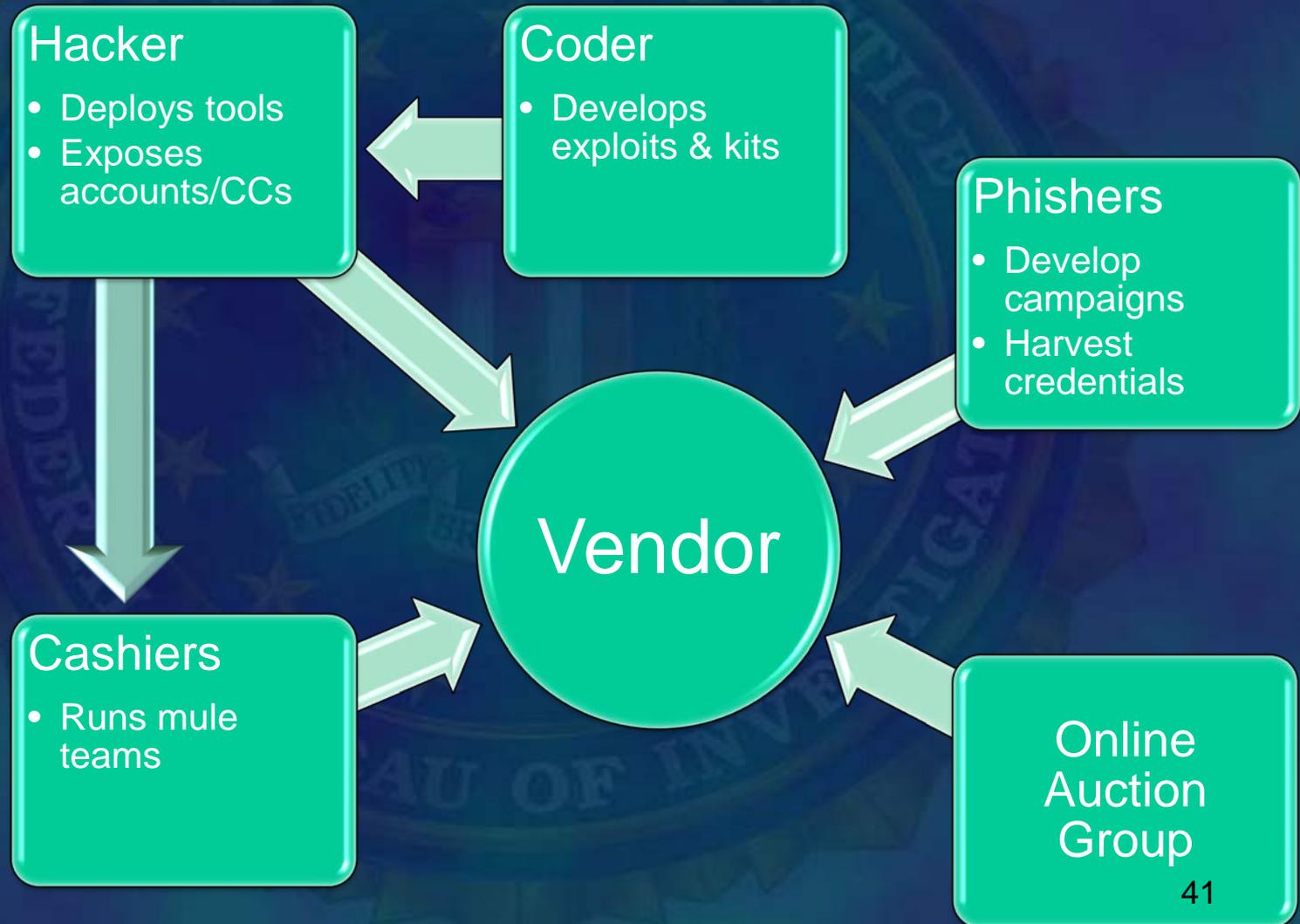


Carder Forums

- Online forums used by cyber criminals to buy/sell stolen credit card information
- Several hundred forums around the world currently operating
- Stolen magnetic stripes, aka “dumps”, can be transferred to blank cards for use at retailers



Efficiency Through Integration of Functions





Organized Crime

- Admins
- Supermoderators
- Moderators
- VIP Users
- Verified Vendors
- Authenticated sellers
- Vouched user
- Forum member



What is for Sale?

- CVV and Virtual Credit Cards
- RATs
- Dumps
- Account logins (ebay, amazon, apple, etc)
- Skimmers for ATMs
- Viruses/malware
- Crypters and FUD (fully undetectable)
- Bank Trojans
 - gozi
- Botnets
 - zeus
 - spyeye
- Binary uploads to botnets



The New Currency

- Liberty Reserve
- Webmoney
- Bartercheque
- Western Union
- Moneygram



Iceman Investigation

- Max Butler, aka “Iceman”
 - Background info on Butler
- Iceman operated Cardersmarket.com starting in late 2005
- August 2006, Iceman hacks the 4 major carding sites and moves all of the users to cardersmarket.com
- 6,000+ users on cardersmarket.com making it the largest on the Internet
- FBI agent a high level member on DarkMarket until Iceman shut it down and absorbed it into Cardersmarket
- In May 2007, Chris Aragon arrested at a retailer with fake cards



Iceman Contd...

- FBI and Secret Service worked together to identify Butler
- Butler arrested at his safe house in Sept 2007
- Butler's data encrypted, by LE prepared and perform a live capture of his computer systems
- Butler found to be in possession of more than 1 million dumps
- Butler sentenced to 13 years incarceration and \$27.5 million in restitution



The Crew





Iceman's Lair





Aragon's Factory





Capital One Meets Iceman



- Sept 29, 2006: Approx 500 Capital One employees receive a spear phishing email from g.reily@lendingnewsgroup.com
- More than 125 employees click on the link
- A blank page loads, but a trojan payload arrives and the computers are compromised
- Capital One Security contacts the FBI
- Domain financialedgenews.com registered using the same account info as CardersMarket.com



Contd.

- FBI realizes Iceman is more than just a carder forum operator

From: Gordon Reily [mailto:g.reily@lendingnewsgroup.com]
Sent: Friday, September 29, 2006 9:25 PM
To: Casby, Thomas (CONT)
Subject: CapitalOne customer information leak?

Thomas,

I am a reporter for Lending News doing a follow up story on the recent leak of customer records from Capital One. I saw the name Thomas Casby come up in the article from Financial Edge and would like to interview you for a follow up piece.

XXXhttp://financialedgenews.com/news/09/29/Disclosure_CapitalOneXXX

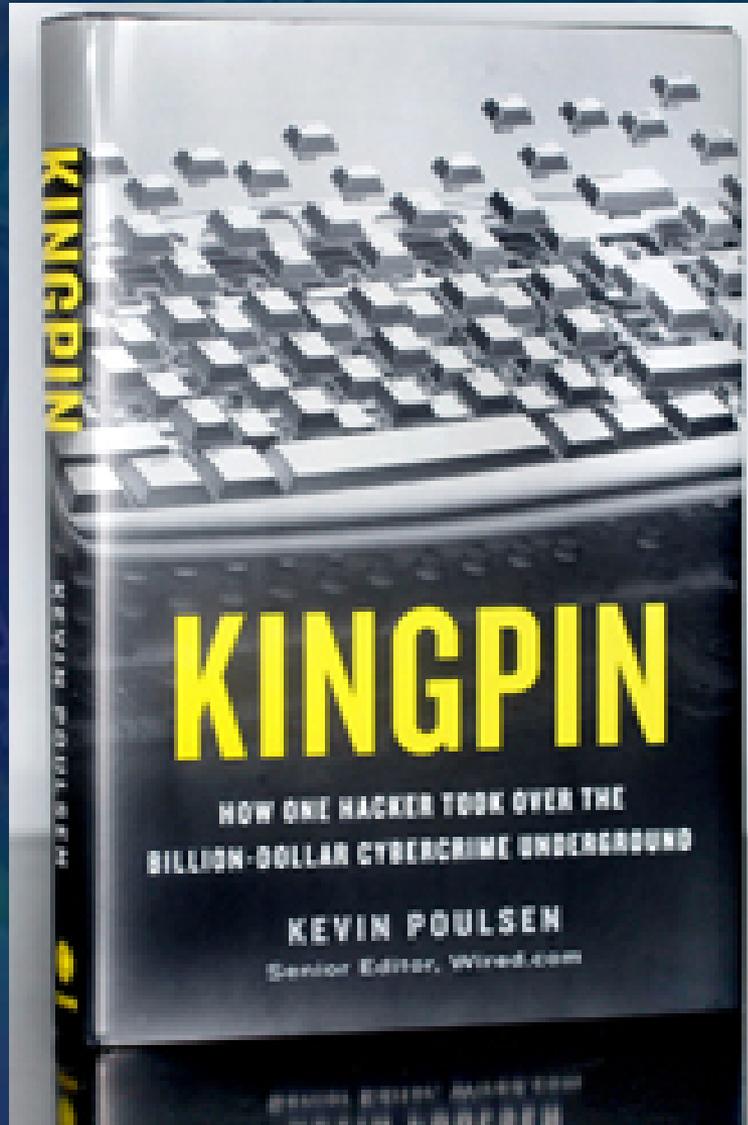
If you have time I would greatly appreciate an opportunity to further discuss the details of the above article.

Regards,

Gordon Reily



More Information



Kingpin
By: Kevin Poulsen



Rise of the Smartphone

- Mobile Banking apps
- Mobile malware
 - Steal PII
- Mobile payments, coming to a smartphone near you!



Google Pulls 21 Apps In Android Malware Scare



March 1, 2011 by [Jolie O'Dell](#) 94

[Google](#) has just pulled 21 popular free apps from the [Android Market](#). According to the company, the apps are malware aimed at getting root access to the user's device, gathering a wide range of available data, and downloading more code to it without the user's knowledge.

Although Google has swiftly removed the apps after being notified (by the ever-vigilant [Android Police](#) bloggers), the apps in question have already been downloaded by at least 50,000 Android users.



The apps are particularly insidious because they look just like knockoff versions of already popular apps. For example, there's an app called simply "Chess." The user would download what he'd assume to be a chess game, only to be presented with a very different sort of app.

These apps are all pirated versions of popular games and utilities — an expeditious solution for busy hackers. Once downloaded, the apps root the user's device using a method like `rageagainstthecage`, then use an Android executable file (APK) to nab user and device data, such as your mobile provider and user ID. Finally, the app acts as a wide-open backdoor for your device to quietly download more malicious code.

Below is a complete list of the bad apps, all of which were made by an entity called Myournet. If you've downloaded one of these apps, it might be best to take your device to your carrier and exchange it for a new one, since you can't be sure that your device and user information is truly secure. Considering how much we do on our phones — shopping and mobile banking included — it's better to take precautions.

- Falling Down
- Super Guitar Solo
- Super History Eraser
- Photo Editor
- Super Ringtone Maker
- Super Sex Positions
- Hot Sexy Videos
- Chess
- 下坠滚球_Falldown
- Hilton Sex Sound
- Screaming Sexy Japanese Girls
- Falling Ball Dodge
- Scientific Calculator
- Dice Roller
- 躲避弹球
- Advanced Currency Converter
- APP Uninstaller
- 几何战机_PewPew
- Funny Paint
- Spider Man
- 蜘蛛侠

Remember, the Android Market is open, which can be great and unfortunate in different circumstances. Always read user reviews before you download; and if you have any doubts, play it safe.

[Email Story](#)



NFC = New Threat

- Near Field Communications
- Distance of 4cm or less
- Trials under way in US cities
- Google supports NFC in Android now
- Citigroup, VeriFone working towards trials with Google providing the readers to retailers for free
- 35 million NFC phones to ship in 2011
- 340 million global wireless users will use mobile payments by 2014 (Gartner study)





What You Can Do

■ Implement Good Security Practices

- Firewalls, Virus Protection, Physical Security, Strong Passwords, ...
- Employee Awareness
 - Use caution with e-mails and visiting sites
 - Social Engineering Tactics
 - Shoulder Surfing





What You Can Do

■ Implement Measures for Identifying Intruders

- Good Logging
- Banners
- Intrusion Detection Systems
- Know your networks / systems
- Know what you are allowed to do
 - Monitor

■ Working with the FBI

- Early Notification (data is perishable)
- Consent to Search & Consent to Monitor
- Preservation of Data
- Make employees available for interviews



Intrusion cases are already won
or lost long before law
enforcement arrives



InfraGard[®]
a collaboration for
infrastructure protection



HOME

29-Aug-2008

27,165 MEMBERS (Including FBI)

ABOUT INFRAGARD

LEARN MORE ABOUT INFRAGARD[®]

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the [Federal Bureau of Investigation](#) and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. [InfraGard Chapters](#) are geographically linked with FBI Field Office territories. [Learn more about InfraGard](#)

BECOME A MEMBER

ELEVATED
significant risk of terrorist attacks

FIND YOUR CHAPTER

BECOME A MEMBER

[APPLY FOR MEMBERSHIP](#)

Attend a local chapter meeting, meet FBI officials from your area, and help protect your nation's infrastructure today.

NEWS ROOM

LINKS

CONTACT

SPECIAL INTEREST GROUPS

INFRASTRUCTURE PROTECTION

It is our goal to improve and extend information sharing between private industry and the government, particularly the FBI, when it comes to critical national infrastructures.



IN THE NEWS

[The International Association of Campus Law Enforcement Administrators \(IACLEA\)](#)

FEATURED CHAPTER

NATIONS CAPITAL



InfraGard Benefits

FBI Program vs Private Sector



- Trusted membership and Network of professionals
- Timely/Non-public Intelligence Products
- Secure forum to share information & discuss issues.
- Avenue to provide positive intelligence
- Ongoing relationship with the FBI

- Industry sector Subject Matter Experts
- Initiation of new investigations
- Early indication of sector specific attacks
- Avenue to obtain feedback on intelligence
- Ability to identify significant crime problems

Also, It is "FREE!"



Access to Secure Website

Home

Mission

This secure web site is designed to provide InfraGard members information about recent intrusions and infrastructure protection measures, access to original research issues, and the capability for members to communicate with each other about similar security interests.

The [sector](#) and [chapter news](#) pages provide members with up-to-date news on issues that affect the critical infrastructures, and upcoming events sponsored by local InfraGard chapters. As a member of InfraGard, you are a key partner in the vital effort to protect our nation's critical infrastructures. InfraGard started as a pilot project sponsored by the FBI's Cleveland Field Office and has now evolved into a national program managed by FBI Headquarters in Washington, D.C.

Unlike in the past, when national security was solely a government responsibility, today the responsibility has to be a shared one, with the private sector taking an increasingly important role. Thank you for accepting this role in protecting our nation.

Recent Alerts & Advisories

-  [Force Protection Intelligence Summary - Dover AFB - January 01 - 08](#)
U.S. Air Force
January, 2009
-  [Strategic Implications of Global Health](#)
National Intelligence Council
January, 2009
-  [Malicious Code In The Virtual World, Second Life, Stealing Currency](#)
FBI
January 6, 2009
-  ['Preoff-Bot' Malware Present on an University's Networks, January to June 2008](#)
FBI
January 6, 2009
-  [Hackers By-Passed Token Authentication System On Widely Used Online Banking Software](#)
FBI
January 6, 2009

 **ELEVATED**
significant risk of terrorist attacks

RECENT INTELLIGENCE

Hackers By-Passed Token Authentication System On Widely Used Online Banking Software

Welcome to InfraGard

- [LES Guidelines](#)
- [Alerts & Advisories](#)
- [Calendar](#)
- [Change Password](#)
- [Computer Security](#)
- [Cyber News Summary](#)
- [Cyber Threat Media Highlights](#)
- [DHS Open Source Reports](#)
- [Government Reports](#)
- [Homeland Security Newsletters](#)
- [Listserv Instructions](#)
- [Public Site](#)

Restricted Access

- [Request Access to SIGs](#)
- [Food-Agriculture InfraGard](#)
- [Chemical InfraGard](#)
- [Research and Technology Protection InfraGard](#)

62

External Links

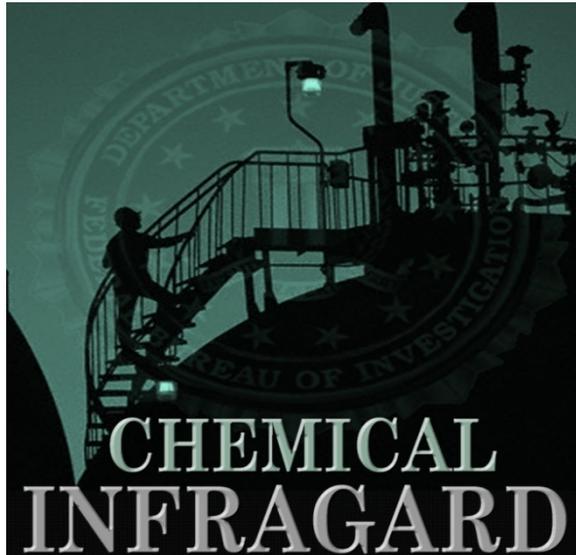
Special Interest Groups



The Food/Agriculture InfraGard Special Interest Group (SIG) is a resource dedicated to the safeguarding of the food and agriculture sectors of both private industry and government through information-sharing networks and a private secure portal of communication. It is a collaborative effort of the Counterterrorism and Cyber Divisions of the FBI. The Food/Agriculture InfraGard SIG is intended to enhance the sharing of information among private sector stakeholders who can be called on to assist the FBI in detecting, deterring, assessing, and preventing threats and attacks targeting the food and agriculture sectors of our nation's critical infrastructures. It aims to be a consortium of agriculture security professionals and law enforcement officials with the common goal of protecting America's farmland, food products, animals, and industry.

Participation in the Food/Agriculture InfraGard SIG requires membership in the national InfraGard Program and affiliation with the agriculture industry. Visit www.infragard.net for national membership. Once a participant in the national program, a member may request access to the Food/Agriculture InfraGard SIG by submitting an e-mail containing answers to questions about his/her association with the agriculture industry.

Assessments, news, relevant links, and up-to-date information on protection issues related to the agriculture community are available to Food/Agriculture InfraGard SIG members. Members may submit articles for posting on the site, and communicate on the message board about food and agriculture sector issues in a secure environment. The site is also broken into areas specific to law enforcement, industry, food/agriculture agencies, animal/human health organizations and academia. The Food/Agriculture InfraGard SIG is a unique opportunity for you to belong to the fastest growing network dedicated to agriculture-specific information sharing, driven to protect the food and agriculture infrastructure of the United States. To belong to the Food/Agriculture InfraGard SIG, visit www.infragard.net. For questions, please contact infragardteam@infragard.org.



The Chemical InfraGard Special Interest Group (SIG) is a resource directed to the safeguarding of the chemical sector of both private industry and government through information-sharing networks and a private secure portal of communication. It is a collaborative effort of the Counterterrorism and Cyber Divisions of the FBI. The Chemical InfraGard SIG is intended to enhance the sharing of information among private sector stakeholders who may be called upon to assist the FBI in detecting, deterring, assessing, and preventing threats and attacks targeting the chemical sector of our nation's critical infrastructures. It aims to be a consortium of chemical security professionals and law enforcement officials with the common goal of protecting America's chemical plants and industry.

Participation in the Chemical InfraGard SIG requires membership in the national InfraGard Program and affiliation with the chemical industry. Visit www.infragard.net for national membership. Once a participant in the national program, a member may request access to the Chemical InfraGard SIG by submitting an e-mail containing answers to questions about his/her association with the chemical industry.

Assessments, news, relevant links, and up-to-date information on protection issues related to the chemical community are available to Chemical InfraGard SIG members. Members may submit articles for posting on the site, and communicate on the message board about chemical sector issues in a secure environment. There is also a Chemical InfraGard SIG listserv which allows SIG moderators the ability to correspond upcoming events and important announcements directly to SIG members via secure e-mail. The Chemical InfraGard SIG is a unique opportunity for you to belong to the fastest growing network dedicated to chemical-specific information sharing, driven to protect the chemical infrastructure of the United States. To belong to the Chemical InfraGard SIG, visit www.infragard.net. For questions, please contact infragardteam@infragard.org.



The Research and Technology Protection InfraGard Special Interest Group (SIG) is a resource dedicated to the safeguarding of our new and developing technologies from illegal acquisition by foreign adversaries. Although innovation in the United States benefits from a globalized economy, these international relationships make our technology increasingly vulnerable to foreign adversaries covertly acquiring and illegally transferring U.S. technology including proprietary information and trade secrets. The Research and Technology Protection InfraGard SIG enhances the efforts to protect research and technology made by private industry, academia and government through information-sharing networks with a private secure portal of communication.

The Research and Technology Protection InfraGard SIG is a collaborative effort of the Foreign-Counterintelligence and Cyber Divisions of the FBI. It is intended to enhance the sharing of information among private sector stakeholders who, in partnership with the FBI, can assist in detecting, deterring, assessing, and preventing threats and attacks targeting the innovation that drives our national economy. It is the consortium of members representing U.S. firms, universities, national laboratories, sensitive government facilities and law enforcement with the common goal of protecting our country's research and technology.

Participation in the Research and Technology Protection InfraGard SIG requires membership in the national InfraGard Program and affiliation with the scientific and technological research and development fields. Visit www.infragard.net for national membership. Once a participant in the national program, a member may request access to the Research and Technology Protection InfraGard SIG by submitting an e-mail containing answers to questions about the member's association with these fields.

Assessments, news, relevant links and up-to-date information on protection issues related to the research and technology communities are available to Research and Technology Protection InfraGard SIG members. This is a unique opportunity for you to belong to the fastest growing information-sharing network dedicated to research and technology protection.



Research and Technology Protection



HOME PUBLICATIONS NEWS MEMBERSHIP DIRECTORY FBI COORDINATORS

IG Home > Research and Technology Protection InfraGard

Quick Links



Workforce Education
- a collection of workforce education documents



Online Resources
- links to a variety of govt and private sources



Publications
- a comprehensive list of publications from a variety of sources



FBI Research and Technology Protection InfraGard

Welcome to the Research and Technology Protection Special Interest Group (RTP SIG). The mission of the RTP SIG is to provide actionable and relevant information to cleared defense contractors, private industry and academia so that they are better able to protect their research, technology and information. While our main concern is the protection of classified information, the same principles can be applied to the protection of trade secrets and other intellectual property.

The FBI's preventative initiative in this realm is called the Counterintelligence Domain Program. In partnership with other U.S. government agencies we have collaborated to better protect key technologies in the U.S. domain. One result of this collaboration is the RTP SIG website. As you look through the site you will notice that our content comes from a variety of sources including the Defense Security Service, Naval Criminal Intelligence Service as well as private industry. If you're interested in learning more about the Domain Program please [click here](#) for our purple brochure.

In addition to the wide array of information available on the InfraGard main site, the RTP SIG supplements that with information that we think will be helpful to the individual who has responsibility for protecting research and technology. The buttons provided above are a quick way to go directly to the most commonly referred to items. For example, in the [Publications](#) section you can:

- Curious about China's cyber activities? Here are some perspectives:
 - [Chinese Military Hacked into Pentagon](#)
 - [China Denies Hacking Pentagon Computers](#)
 - [What is Behind the Chinese Cyber Offensive?](#)
- Learn more about a [U.S. District Court convicts businessperson of conspiracy to commit money](#)

- Home
- Publications
- News
- Workforce Education
- Counterintelligence/Domain Mission
- FBI Domain Coordinators
- Online Resources
- Meetings/Conferences
- Membership Directory
- LES Guidelines
- Message Boards
- Contact Us
- Submit Content
- FBI Tips

Research and Technology Protection



[HOME](#)

[PUBLICATIONS](#)

[NEWS](#)

[MEMBERSHIP DIRECTORY](#)

[FBI COORDINATORS](#)

Home > Research and Technology Protection InfraGard > **Mission**

FBI's Counterintelligence Mission Statement

 [Business Alliance and Academic Alliance](#)

As the lead counterintelligence agency in the United States, the FBI is responsible for identifying and neutralizing ongoing national security threats. The Counterintelligence Division provides centralized management and oversight for all Foreign Counterintelligence (FCI) investigations. It ensures that offensive operations and investigations are fully coordinated with the U.S. Intelligence Community, and focused on those countries, foreign powers, or entities which pose the most significant threat to the United States. The Counterintelligence Division integrates law enforcement with intelligence efforts to investigate violations of the espionage statutes under Title 18 of the US Criminal Code. The investigative priorities of the FCI Program are to:

- Prevent or neutralize the foreign acquisition of weapons of mass destruction (WMD) technology or equipment
- Prevent the penetration of the U.S. Intelligence Community
- Prevent the penetration of U.S. Government agencies or contractors
- Prevent the compromise of U.S. Critical National Assets.
- Conduct aggressive CI operations focusing on those countries that constitute the most significant threat to U.S. Strategic interests.



- [Home](#)
- [Publications](#)
- [News](#)
- [Workforce Education](#)
- [Counterintelligence/Domain Mission](#)
- [FBI Domain Coordinators](#)
- [Online Resources](#)
- [Meetings/Conferences](#)
- [Membership Directory](#)
- [LES Guidelines](#)
- [Message Boards](#)
- [Contact Us](#)
- [Submit Content](#)
- [FBI Tips](#)



Access to other Resources

National Cyber-Forensics & Training Alliance

http://www.ncfta.net/default2.asp



National Cyber-Forensics & Training Alliance

About
Facilities
Partnerships
Submit a Tip
White Papers
Archived Articles
Contact
Privacy Policy

The National Cyber-Forensics and Training Alliance provides a neutral collaborative venue where critical confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia and law enforcement.



The Alliance facilitates advanced training, promotes security awareness to reduce cyber-vulnerability, and conducts forensic and predictive analysis and lab simulations.

These activities are intended to educate organizations and enhance their abilities to manage risk and develop security strategies and best practices.

Objectives
NCFTA will bring together local, state, and federal law enforcement, businesses, and academic institutions to functionally collaborate on cybercrime issues.

It will establish jointly developed and staffed facilities, where program participants will benefit from cyber-forensic analysis, tactical response development, technological simulation/modeling analysis, and the development of advanced training.

TOP ALERTS

- Micro Deposits
- Limbo 2 Trojan
- BlackBerry Users at Risk
- Phantom Merchants
- UPS Spam Trojan
- The Coreflood Trojan
- Silentbanker Trojan Strikes Again
- Malware Infected Multimedia Files
- Malware Plays on Olympic Games
- Turkish Botnet Infects Cartoon Fans

[view all scams / threats](#)

NEWS & RESEARCH

8/29/2007
Cyber-Security Issues: Congressional Testimony
Good afternoon Chairman Akin, ranking member Bordallo, and members of the committee [read more](#)



Home > Resources > **DHS Reports**

DHS Daily Open Source Infrastructure Report



About the DHS Daily Open Source Infrastructure Report

The DHS Daily Open Source Infrastructure Report (Daily Report) is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. Each Daily Report is divided by the critical infrastructure sectors and key assets defined in the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.

October

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#)
[7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#)
[14](#) [15](#) [16](#) [17](#) [18](#) [19](#) [20](#)
[21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#)
[28](#) [29](#) [30](#) [31](#)

September

[1](#)
[2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#)
[9](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#)
[16](#) [17](#) [18](#) [19](#) [20](#) [21](#) [22](#)
[23](#) [24](#) [25](#) [26](#) [27](#) [28](#) [29](#)
[30](#)

August

[1](#) [2](#) [3](#) [4](#)
[5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#)
[12](#) [13](#) [14](#) [15](#) [16](#) [17](#) [18](#)
[19](#) [20](#) [21](#) [22](#) [23](#) [24](#) [25](#)
[26](#) [27](#) [28](#) [29](#) [30](#) [31](#)

July

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#)
[8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#)
[15](#) [16](#) [17](#) [18](#) [19](#) [20](#) [21](#)
[22](#) [23](#) [24](#) [25](#) [26](#) [27](#) [28](#)
[29](#) [30](#) [31](#)

June

[1](#) [2](#)
[3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)
[10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#)

May

[1](#) [2](#) [3](#) [4](#) [5](#)
[6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#)
[13](#) [14](#) [15](#) [16](#) [17](#) [18](#) [19](#)

April

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#)
[8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#)
[15](#) [16](#) [17](#) [18](#) [19](#) [20](#) [21](#)



Resources

- [DHS Open Source Reports Help Section](#)
- [List-Serv Instructions](#)
- [Membership](#)
- [Member Contributions](#)
- [Presentations](#)
- [Reports](#)
- [SBA/NIST](#)
- [Whitepapers](#)
- [FBI Tips](#)
- [USP3 Global Snapshot](#)

DHS Open Source Reports

- [Current](#)
- [2006 Archive](#)
- [2005 Archive](#)



Chapter Meetings Valuable Speakers

InfraGard - Richmond, VA Chapter

http://www.infragard.net/chapters/richmond/announcements.php?mn=1

Google



InfraGard®
Richmond, VA



RICHMOND HOME 29-Aug-2008

Home | Find Your Chapter | **Richmond, VA**

Meetings

May 19, 2008

The next Richmond InfraGard Chapter meeting will be on May 19, 2008 from 1pm to 3pm. It will be held at Virginia Commonwealth University (VCU) in their new Engineering and Business School building, Snead Hall, Room B1115. The building is located at the intersection of Main St and Belvedere, just before you get to Cary St. It is located on the East side of Belvedere. and the address is 301 W. Main St, Richmond, VA 23284.

The focus of the meeting will be on the new Chemical Security Legislation, CFATS. In addition to the main speakers, who will be speaking about CFATS, we will also have a panel of experts in WMD and Export Control who will be available for a question/answer session. Please see the link below for additional information regarding this meeting.

Please extend the invitation to anyone else in your organization or outside your organization who would benefit from this meeting. Please note that all attendees must bring a valid ID for vetting.



**RESEARCH
& TECHNOLOGY**

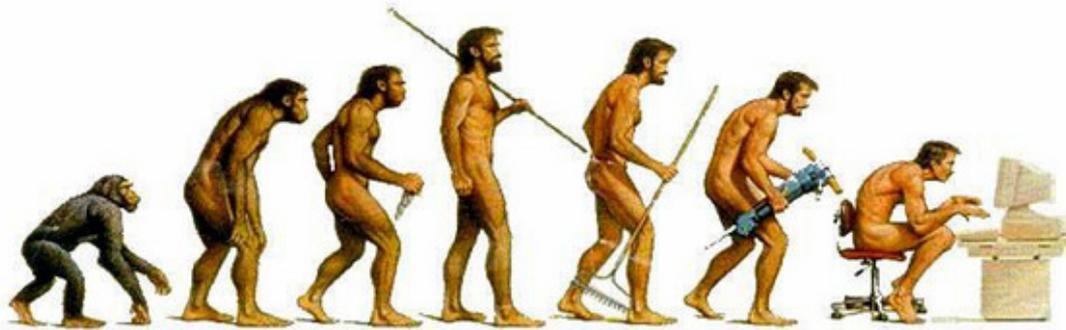


Conclusion

- Technology heavily favors the criminals today.
- Success requires long term commitment, data sharing and ongoing cooperation.



Evolution of Cyber Crime... Still Changing...





Questions?

SA Michael P. French
SA Michael R. Schuler

FBI Richmond Division
1970 E. Parham Rd
Richmond, VA 23228
Phone: (804)261-1044
Fax: (804) 627-4494



Indirect Reconnaissance: Information Gathering Techniques

Bob Baskette
Senior Manager, Security Operations
and Architect



The Importance of Information

- Information Gathering is a critical step in launching an attack against a system
- All of the information collected will be used to shape the attack and will directly impact the success of the attack
- The more information gathered, the higher probability of a successful attack



Information Gathering Tools

- The Internet has become a vast database of user activity and server information since this information is indexed by everyone and is rarely deleted
- Several tools have emerged to extract the data
 - Google (or any major search engine)
 - Netcraft
 - Whois



Information Takes Many Forms

- Remember any piece of information can be of importance:
 - Exposed email addresses allow for directed client-side attacks and phishing
 - Banners provide software version numbers that can be used to research and deploy vulnerabilities
 - Organizational information can be used for social engineering



Search Engine Data Mining

- Google and other search engines are valuable sources of information concerning web servers and user information available on the Internet
- Every piece of information stored in Google's cache (simply a database index of sites) can be extracted and viewed using Google's special search operators.



Google Base Search Criteria

- Based on the syntax of the Uniform Resource Locator (URL) structure
- Should be as unique as possible in order to get the most specific results.
Remember, garbage in, garbage out
- Result pages are dynamic and created on the fly



Google Base Search

- Every Google query can be represented with a URL that points to a result page
- Can bookmark the query URL used in the search for future use
- The URL can be directly modified to alter the search options

Research using Google

- The only parameter required for the search URL is the query = q parameter
 - www.google.com/search?q=google
- Google search returns
 - Name of the site
 - Summary of the site
 - URL of the page
 - Size and date the page was last crawled
 - Cached link that shows the page as it appeared on the last crawl



Google Search Operators

- To find all of the pages available from a web service

`site:www.vita.virginia.gov`

- To find all of the web services available from a domain

`site:vita.virginia.gov`



Google Search Operators Cont.

- To find documents available from the domain

`filetype:pdf site:vita.virginia.gov`

- Can use a combination of search terms and special operators to check for unwanted pages or links

`SSN site:vita.virginia.gov -filetype:doc -
filetype:pdf`



Google Search Operators

- Can be used to find login portals, software version numbers, or exposed authentication credentials
- Can also use the filetype operator to scan for exposed configuration files on a web server or cached in the environment
`config admin filetype:cfg site:vita.virginia.gov`



Exploring the use of Recorded Data

- Email address harvesting is very valuable since most people use the same email address for most contact pages
- Email address can be used to build a profile of an individual and locate other emails in use



Exploring the use of Recorded Data

- The secondary email addresses can be used in phishing attacks against information related to the primary email address:
 - Lower security controls
 - Lower situational awareness
 - False sense of trust from profiled information



Other Fun with Google

- Use the site and filetype operators to find login pages.
password site:domainname.domain -filetype:pdf
– filetype:doc
- Use the inurl operator and the Boolean operators to search the banner information
"Banner" inurl:"marker" OR inurl:"marker"



Boolean Operators and Special Characters

- Used to perform advanced queries and help specify the results that are returned from a query
- To properly segment the various parts of an advanced query, must use visual grouping techniques that use parenthesis characters



Boolean Operators and Special Characters

- Queries with a combination of AND, NOT, OR are simply processed from left to right
- Each operator has the same weight
- Can use parenthesis to combine multiple search terms inside a single operator



Boolean AND Operators

- Operator is used to include multiple terms in a query and is the default Boolean operator in Google searches
- Google automatically searches for all terms in the query
- Note, to force Google to search for common words, preface the word with a plus sign



Boolean NOT Operator

- Opposite of the AND operator
- Excludes a word from the search
- Best way to use the operator is to preface the search word with a minus sign

password site:vita.virginia.gov -filetype:pdf



Boolean OR Operator

- Represented by the pipe symbol or simply the word OR
- Instructs Google to locate either one term or another in a query

site:vita.virginia.gov password | admin



URL information

- Uniform Resource Locator
- Address of a web page
- Components
 - Protocol
 - Address of resource
 - Path to file
 - Filename
 - List of parameters to be passed to or into the filename?q=



URL information

- Google does not effectively search the protocol field of the URL
- Google also has issues parsing through the special characters in the URL
- The site and filetype operators are more effective in parsing data inside the URL string than the inurl operator



Additional Google Operators

- Allintext
 - Simplest operator to use
 - Locates a term within the text of the page
 - Used when the search text should only be found in the text of the page
 - Can also be used as "find this string anywhere except in the title, URL, or links"



Additional Google Operators

- Intitle and Allintitle
 - Used to search within the title of a page
 - Title of a page can be described as the text that it is found within the TITLE tags of the HTML document
 - Must consider what text is actually from the website title and what text may have been inserted by the browser during download



Additional Google Operators

- Intitle and Allintitle
 - Title will be the text that appears at the top of the web page
 - Intitle will search for the word or phrase directly after the colon
 - Allintitle will use every single word or phrase in the match and all search terms must appear in the title

Additional Google Operators

- Daterange Operator
 - Used to locate pages indexed by Google within a certain date range
 - Each time Google crawls a page the date changes
 - Operator can be used to limit the search and filter out obsolete or obscure pages



Additional Google Operators

- Daterange Operator
 - Parameter must always be expressed as a range of two dates separated by a dash to specify a specific date
 - Must provide the same date twice separated by a dash to specify a single day
 - Dates must be in the form of Julian dates (the number of days that have passed since January 1, 4713 B.C.)



Additional Google Operators

- Cache Operator
 - Shows the cached version of a page
 - Does not require Google to perform a query or return a results page
 - Must supply a complete URL or hostname otherwise the partial/invalid URL will be treated as a phrase search

Google Cache

- Provides a certain anonymity by browsing the cached version of a web page
- If used properly the target system may not receive a single packet
- Not all images are cached so the requesting system's IP address may be exposed to the target system during image retrieval



Additional Google Operators

- Link operator
 - Search for pages that link to other pages
 - Requires a URL or server name as an argument
 - Result will contain HTML links to the search term
 - The more specific URL will return more specific and few results



Additional Google Operators

- Inanchor Operator
 - Used to locate text within the link text
 - Companion to the link operator
 - Searches the text representation of a link not the actual URL
 - Accepts a word or phrase as the search term



Story Time

- This slide has been intentionally left blank



Netcraft

- Internet monitoring company based in England
 - <http://searchdns.netcraft.com>
- Best known for monitoring up times and providing server operating system information and web server version
- If the server has been indexed, Netcraft can provide a detailed report



Whois

- Database maintained by the InterNic
- Contains name server, registrar, full contact information for the domain web-based tools
 - <http://whois.domaintools.com>
 - <http://www.networksolutions.com/whois/index.jsp>



Whois

- Can provide the following information for a domain
 - IP address
 - Registrar
 - Name server
 - Update date
 - Creation date
 - Expiration date
 - Company address
 - Company contact information



Additional Whois Information Concerns

- Can extract the total IP address range for a site given a single IP address.
- Allows for an expanded attack surface.
- Provided DNS server information for the domains allowing DNS harvesting activities



Additional Whois Information Concerns

- Provides domain contact information simplifying social engineering attacks
 - Need to review who is listed and train on what to do when the call comes
- Provides important domain listing dates
 - How often is the information checked and updated
 - Can allow the domain be stolen on expire



Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!



Virginia Information Technologies Agency

2011
Commonwealth Security Annual Report
as of
October 5, 2011

Michael Watson
Acting Chief Information Security Officer



§ 2.2-2009

§ 2.2-2009. Additional duties of the CIO relating to security of government information.

C. The CIO shall annually report to the Governor, the Secretary, and General Assembly 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 or 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 (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the public body's information technology projects pursuant to § 2.2-2015, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.



Explanation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011 - Percentage of CAPs Received	2011 - Percentage of Quarterly Updates Received	3 year - Percentage of Audit Obligation Completed
XYZ	Yes	5	Current	90%	75%	100%

Acronyms:

- ISO:** Information Security Officer
- IS:** Information Security
- CAP:** Corrective Action Plan
- CISO:** Chief Information Security Officer of the Commonwealth

ISO Designated: The Agency Head has

- Yes** - designated an ISO with the agency within the past two years
- No** – not designated an ISO for the agency since 2006
- Expired** –designated an ISO more than 2 years ago or the designated ISO is no longer with the agency

Attended IS Orientation:

The number indicates agency personnel that have attended the optional Information Security Orientation sessions within the last 2 years. Their attendance indicates they are taking additional, voluntary action to improve security at their agency akin to “Extra Credit!”



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- Percentage of CAPs Received	2011- Percentage of Quarterly Updates Received	3 year - Percentage of Audit Obligation Completed
XYZ	Yes	5	Current	90%	75%	100%

Security Audit Plan Received: The Agency Head has

Current - submitted a Security Audit Plan for the period of fiscal year (FY) 2011-2013 or 2012-2014 for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2011, Audit Plans submitted shall reflect FY 2012-2014)

No - not submitted a Security Audit Plan since 2006

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

Expired –submitted a Security Audit Plan on file that does not contain the current three year period FY FY 2011-2013 or FY 2012-2014

Pending –submitted a Security Audit Plan that is currently under review

2011 - Percentage of CAPs Received: The Agency Head or designee has

% – submitted % of CAPs for planned audits listed on submitted Audit Plan

N/A - not had Security Audits scheduled to be completed

Pending –submitted a Corrective Action Plan that is currently under review



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- Percentage of CAPs Received	2011- Percentage of Quarterly Updates Received	3 year - Percentage of Audit Obligation Completed
XYZ	Yes	5	Current	90%	75%	100%

2011 - Percentage of Quarterly Updates Received: The Agency Head or designee has % – submitted % of quarterly status updates received for corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

N/A - no open Security Audit findings

Pending - submitted quarterly status update that is currently under review



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- Percentage of CAPs Received	2011- Percentage of Quarterly Updates Received	3 year - Percentage of Audit Obligation Completed
XYZ	Yes	5	Current	90%	75%	100%

3 year - Percentage of Audit Obligation Completed:

Percent of sensitive systems reported **by 2008** (according to IT Security Audit Plans) that have been audited to date. This datapoint is based on the IT Security Audit Standard requirement: *“At a minimum, databases that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years.”*

Agencies that did not submit an IT Security Audit Plan **by 2008** were not in compliance and therefore there is no data to report on for **2011**.

Systems that have been removed from audit plans within the three year period due to retirement of the system or reclassification to non-sensitive are not counted.

N/C – agency not in compliance by 2008, agency did not submit an IT Security Audit Plan **by 2008**

Pending – currently under review

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved



FAQ!

What should an agency do if they conduct a Security Audit that results in no findings?

In the event that a Security Audit was performed and there were no findings and, therefore, no Corrective Action Plan is due, the Agency Head should notify Commonwealth Security via email or letter stating what audit was conducted and that there were no findings.

What is the cutoff date to submit documentation for the Commonwealth Security Annual Report?

December 31, 2011



Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
CB	Yes	1	Expired	0	N/A	0
DGS	Yes	3	Current	N/A	N/A	0
DHRM	Yes	1	Current	0	N/A	100
DMBE	Yes	1	Expired	N/A	N/A	0
EDR	Yes	1	Current	100	100	100
HRC	Yes	0	Current	N/A	N/A	100
SBE	Yes	1	Expired	N/A	0	50

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Agriculture & Forestry

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
DOF	Yes	1	Current	0	N/A	0
VDACS	Yes	1	Current	Pending	Pending	100

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Commerce & Trade

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
BOA	Yes	1	Expired	0	N/A	0
DBA	Yes	0	Expired	N/A	N/A	0
DHCD	Yes	0	Pending	Pending	Pending	Pending
DMME	Yes	4	Current	50	0	57.14
DOLI	Yes	0	Expired	0	N/A	0
DPOR	Yes	1	Expired	N/A	0	100
TIC	Yes	0	Expired	0	N/A	0
VEC	Yes	0	Expired	Pending	Pending	Pending
* VEDP	Yes	1	Expired	0	N/A	0
VRA	No	0	No	N/A	N/A	N/C
VRC	Yes	1	Expired	N/A	N/A	0

* VEDP includes VTA and VNDIA

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
CNU	Yes	0	Current	N/A	N/A	0
DOE	Yes	1	Current	N/A	N/A	100
FCMV	Yes	0	Expired	N/A	N/A	100
GH	Yes	1	Expired	N/A	N/A	0
JYF	Yes	1	Current	N/A	100	100
LVA	Yes	0	Expired	0	N/A	100
NSU	Yes	4	Expired	N/A	N/A	0
RBC	Yes	1	Pending	Pending	Pending	Pending
SCHEV	Yes	0	Expired	0	N/A	0
SMV	Yes	0	Expired	0	N/A	0
SVHEC	No	0	No	N/A	N/A	N/C
UMW	Yes	0	Current	50	33.33	80
VCA	Yes	0	Expired	N/A	N/A	100
VMFA	Yes	2	Expired	N/A	0	50
VSDB	Yes	1	Current	0	N/A	0
VSU	Yes	0	Expired	Pending	Pending	Pending

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CS&RM](#).



Secretariat: Finance

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
DOA	Yes	1	Current	0	0	25
DPB	Yes	0	Expired	N/A	0	100
TAX	Yes	1	Current	Pending	Pending	Pending
TD	Yes	0	Current	0	N/A	0

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Health & Human Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
*DBHDS	Yes	3	Current	N/A	0	100
DHP	Yes	2	Expired	0	N/A	0
DMAS	Yes	2	Current	N/A	N/A	0
*DRS	Yes	4	Current	100	18.92	47.83
DSS	Yes	5	Current	Pending	Pending	Pending
VDH	Yes	2	Current	N/A	58.33	3.57
VFHY	Yes	0	Current	N/A	N/A	100

* DBHDS includes VCBR

* DRS includes DBVI, VDA, VDDHH,VBPD and WWRC

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Natural Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
DCR	Yes	0	Current	0	50	20
DEQ	Yes	1	Current	0	0	75
DGIF	Yes	3	Current	0	N/A	0
DHR	Yes	0	Expired	0	N/A	0
MRC	Yes	1	Current	100	0	100
VMNH	Yes	1	Expired	0	N/A	0
VOF	No	0	No	N/A	N/A	N/C

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Public Safety

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
ABC	Yes	3	Current	75	36.36	100
CASC	Yes	0	Expired	N/A	N/A	100
DCE	Yes	2	Current	0	57.14	33.33
DCJS	Yes	1	Expired	0	N/A	0
DEM	Yes	1	Current	N/A	N/A	0
DFP	Yes	0	Current	N/A	50	100
DFS	Yes	0	Pending	N/A	N/A	0
DJJ	Yes	2	Current	N/A	33.33	66.67
DMA	Yes	0	No	N/A	N/A	N/C
*DOC	Yes	4	Expired	71.43	100	58.82
*DVS	Yes	1	Pending	0	N/A	0
VSP	Yes	0	Current	Pending	Pending	Pending

*DOC includes VPB

*DVS includes VWM

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Technology

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
IEIA	Yes	2	Expired	0	N/A	0
VITA	Yes	2	Current	100	72.22	54.55

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Transportation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
DMV	Yes	1	Current	0	0	100
DOAV	Yes	0	Expired	0	N/A	0
DRPT	Yes	0	Expired	N/A	N/A	0
MVDB	Yes	0	Expired	N/A	N/A	100
VDOT	Yes	7	Expired	Pending	Pending	Pending
VPA	No	0	No	N/A	N/A	N/C

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Independent Branch Agencies

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
IDC	Yes	4	Current	N/A	53.33	100
SCC	Yes	2	Current	40	25	40
SLD	Yes	2	Expired	0	N/A	0
VCSP	Yes	1	Current	N/A	N/A	100
VOPA	Yes	1	Current	0	N/A	0
VRS	Yes	0	Expired	0	15	42.86
VWC	Yes	0	Current	Pending	Pending	Pending

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Others

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
GOV	Yes	0	Current	N/A	N/A	N/A
OAG	Yes	2	Expired	N/A	N/A	0

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Virginia Information Technologies Agency

Upcoming Events





2011 VA SCAN CONFERENCE

Virginia Alliance for Secure Computing and Networking
(VA SCAN) annual conference.

WHEN: October 6 - 7, 2011

WHERE: College of William and Mary in Williamsburg, Virginia

“SECURITY WITH OUT BORDERS”

Don't miss this opportunity to hear
leaders in the security field discuss current issues
And effective security practices

Conference will include a SANS class for those who want the opportunity to receive formal security training and/or earn CPE's. SEC567: Power Packet Crafting with Scapy taught by SANS instructor, Judy Novak. Seats for the SANS course are limited to 68 so register early if you want to take the course!

Details / Register: <http://wmpeople.wm.edu/site/page/pckell>

Questions? Contact Pete Kellogg at pckell@wm.edu or 757-221-1822.



MS-ISAC

National Webcast Initiative

Thursday, Oct 6
2:00 pm – 3:00 pm EDT

Topic: **Cyber Security & You: Top 10 Tips**

Visit MS-ISAC web for more information:

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



Information Security System Association

ISSA

DATE: Wednesday, Oct 12, 2011

LOCATION: Maggiano's Little Italy

11800 West Broad Street, #2204, Richmond, VA 23233

TIME: 11:30 - 1:00pm. Presentation starts at 11:45.

Lunch served at 12.

COST: ISSA Members: \$20 & Non-Members: \$25

SPEAKER: TBA

TOPIC: TBA



AITR Meeting

AITR Meeting:

Wednesday, October 12th

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: CESC



ISACA Fall 2011 CISM Review Course

The Virginia Information Systems Audit and Control Association (ISACA) Chapter will be hosting a 3 day CISM review class for all interested participants.

John Karabaic Director of Certification for the Virginia Chapter
ISACA will be teaching this course.

WHEN: October 29, November 5 & 12

TIME: 8:30am – 5:00pm

WHERE: DMAS, 600 E. Broad St., Richmond, VA

There are a limited number of spots available so please sign up and pay as soon as possible!

Register here:

<http://www.cvent.com/events/fall-2011-cism-review-course/event-summary87f5735971b947edb23faf91698b32f6.aspx>



2011 Information Security Awareness Tools

The Information Security Toolkit has been updated with new materials!

<http://www.vita.virginia.gov/security/toolkit/>

For printing cost estimates you can contact DMV's
Damian McInerney at (804)367-0925
or email: damian.mcinerney@dmv.virginia.gov

Thank you DMV!



Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - November 2, 2011

Wednesday - December 7, 2011

ISOAG will be held the 1st Wednesday of each month in 2012



Future IS Orientation Sessions

Tuesday - November 8, 2011

1:00 – 3:30p
(CESC)

Tuesday - February 7, 2012

1:00 – 3:30p
(CESC)

IS Orientation is now available via webinar!



Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:
Kathryn.Merhout@VITA.Virginia.Gov



ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

October 5, 2011



NORTHROP GRUMMAN



ADJOURN

