CELAES Conference

September 15, 2011

USSS Robert Villanueva

FBI Monica Horvath

AUSA Aurora Fagan

Southern District of Florida

- Five Offices
  - –Miami (main)
  - –Ft. Pierce
  - –WPB
  - –FLL
  - –Key West

U.S. Secret Service

- Access Device Fraud
- Bank Fraud
- ID Theft
- Miami Electronic Crimes Taskforce

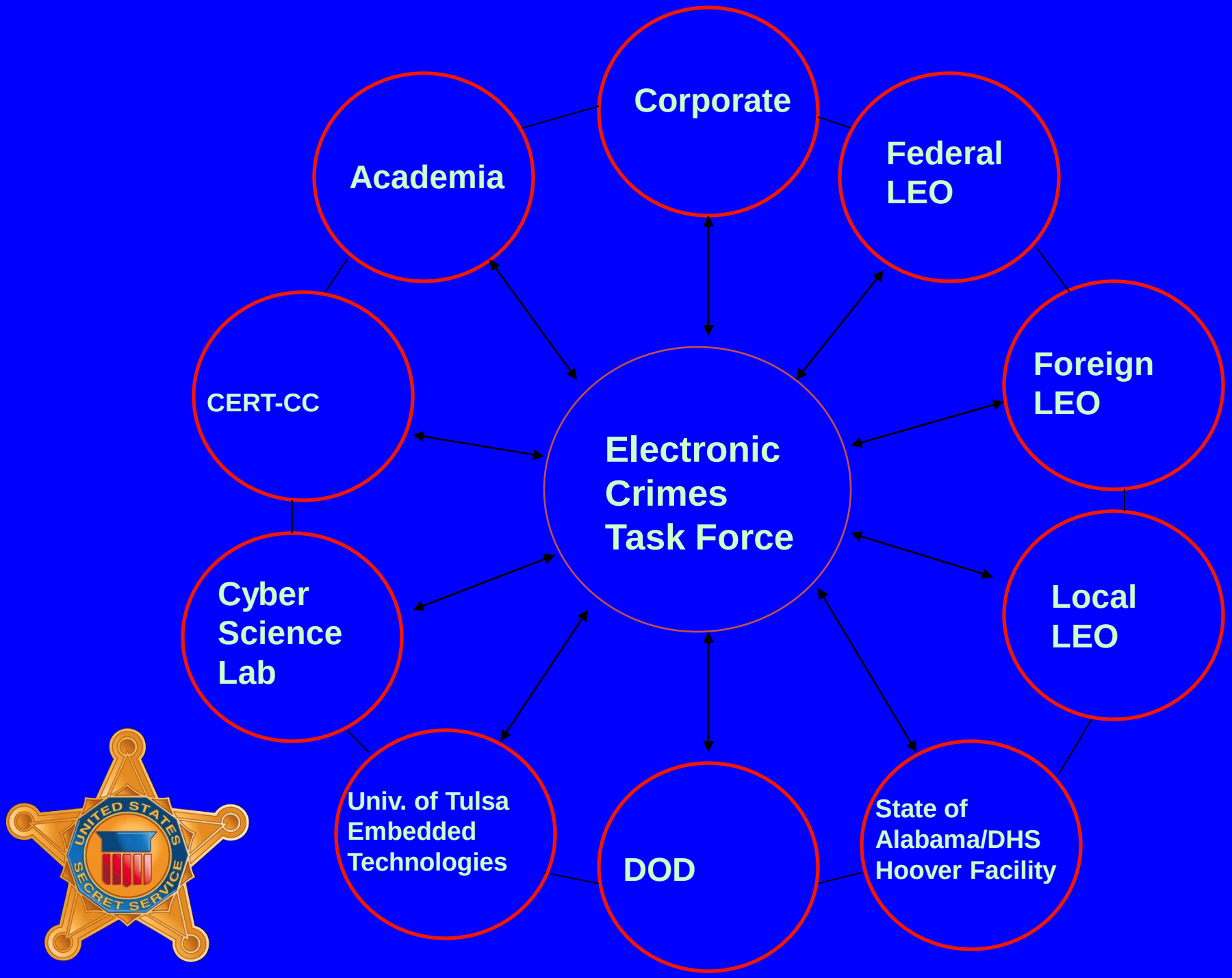
USSS Enhanced Mission

The Director of the United States Secret Service shall take appropriate actions to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

Public Law 107-56, Section 105

U.S. Department of Homeland Security

United States Secret Service


Corporate
Academia
Federal LEO
CERT-CC
Electronic Crimes Task Force
Foreign LEO
Cyber Science Lab
Local LEO
Univ. of Tulsa Embedded Technologies
DOD
State of Alabama/DHS Hoover Facility
UNITED STATES SECRET SERVICE

Intrusiones en Computadoras y Las Instituciones Financieros

SSA Melissa Horvath

División de Ciberneticos

Sección de Ciber Criminal/

Unidad 1 de Ciber Criminal

202 651-3206

melissa.horvath@ic.fbi.gov

Intrusiones en Computadoras y el sector Financiero últimas tendencias y amenazas

1. **Bancarias a través de dispositivos móviles**
   - Las vulnerabilidades
   - Tendencias del mercado
   - Quien estan involucrado en los financieros móviles, Que se hace para controlarlas y asegurarlas (transacciones)
   - Telco Initiative at the Cyber Initiative and Resource Fusion Unit in Pittsburgh, PA

2. **ACH – Zeus Botnet**
   - Operacion “Trident Breach” y “ACHing Mules”
   - más que 390 casos total en el FBI, $70 Milliones en pérdidas
   - Coordinada barridos/arrestos en el Londres, Ucrania, los EE.UU. Y Moldavia.
   - Los grupos de Trabajo para atacar la ameneza.

Vulnerabilidades de los dispositivos Móviles

- **Malware para dispositivos móviles** utilizados para obtener la información de identificación personal (PII) o intercepción / iniciar la comunicación con las instituciones financieras;

- **Vulnerabilidades de las nuevas tecnologías** en el ámbito de los servicios de pago, tales como la identificación por radiofrecuencia (RFID) y Near Field Communication (NFC);

- **El aumento de la ingeniería social** a través del servicio de mensajes cortos (SMS), voz sobre IP (VoIP) y servicios de transmisión;

- **La explotación de los servicios** de comprometer centralita privada (PBX) y las líneas de la conferencia, realizar los ataques de la negación de servicio de teléfono (TDoS) , para llevar a cabo el tráfico de bombeo, facilitar el robo de la tarjeta SIM y / o re-envío, y lograr la clonación de cable módem.

Tendencias del Mercado

February 8, 2011

The New York Times

Smartphones Outsell PCs

By SARAH PEREZ of ReadWriteWeb

According to IDC, smartphone manufacturers shipped 100.9 million devices in the fourth quarter of 2010, while PC manufacturers shipped 92.1 million units worldwide. Or, more simply put, smartphones just outsold PCs for the first time ever.

The number of smartphones sold in Q4 2010 was up 87.2% from the 53.9 million sold in Q4 2009. For the year, vendors shipped 302.6 million smartphones - an increase of 74.4% from the 173.5 million in 2009.

Mobile Content Usage
3 Month Avg. Ending Feb. 2011 vs. 3 Month Avg. Ending Nov. 2010
Total U.S. Mobile Subscribers Ages 13+
Source: comScore MobiLens

	Share (%) of Mobile Subscribers		
	Nov-10	Feb-11	Point Change
Total Mobile Subscribers	*100.0%*	*100.0%*	*N/A*
Sent text message to another phone	67.1%	68.8%	1.7
Used browser	35.3%	38.4%	3.1
Used downloaded apps	33.4%	36.6%	3.2
Accessed social networking site or blog	23.5%	26.8%	3.3
Played Games	22.6%	24.6%	2.0
Listened to music on mobile phone	15.0%	17.5%	2.5

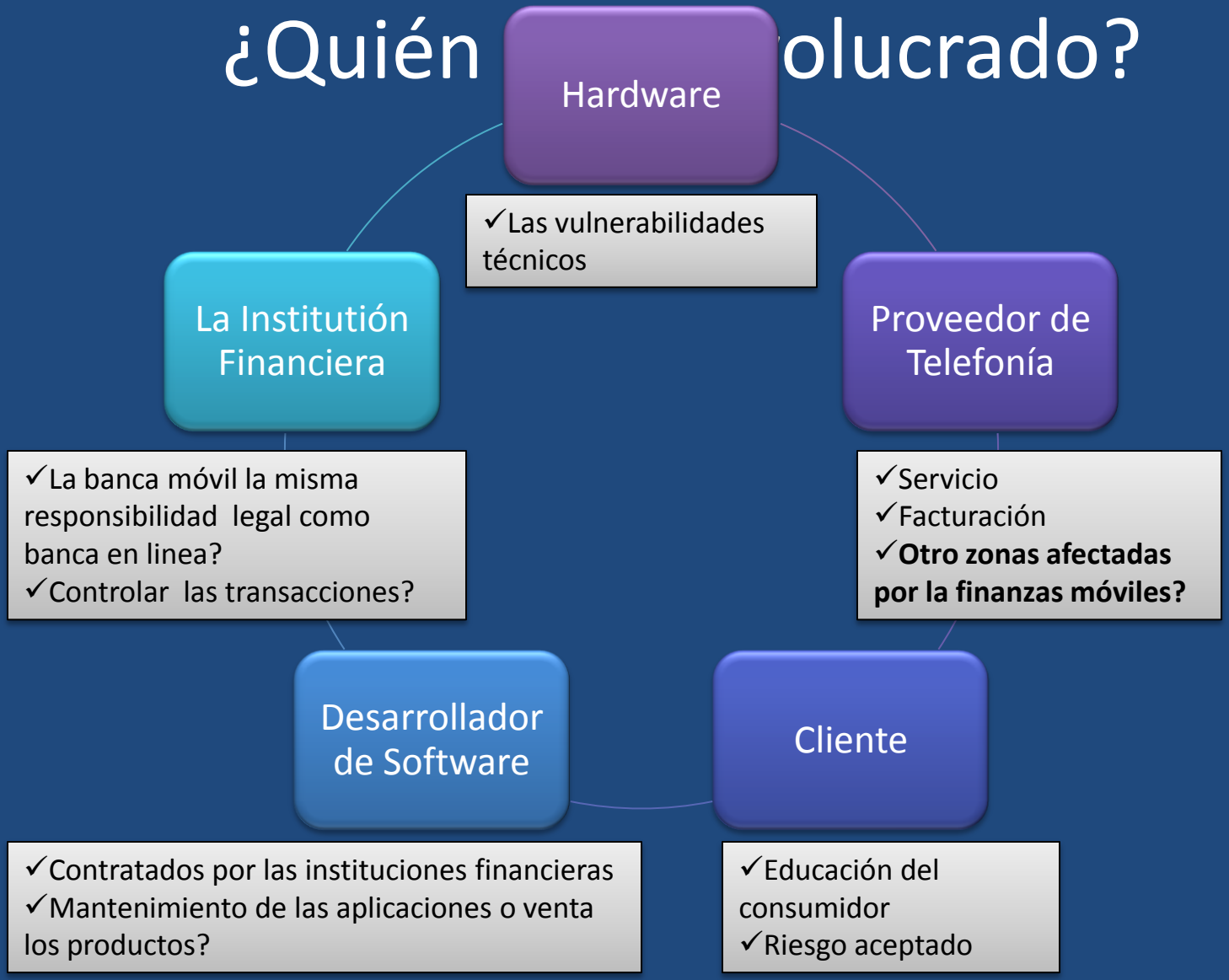
About comScore
comScore, Inc. (NASDAQ: SCOR) is a global leader in measuring the digital world analytics. For more information, please visit www.comscore.com/companyinfo.

"BlackBerry maker Research In Motion Ltd., has said **most new BlackBerrys will have NFC chips by later this year.**

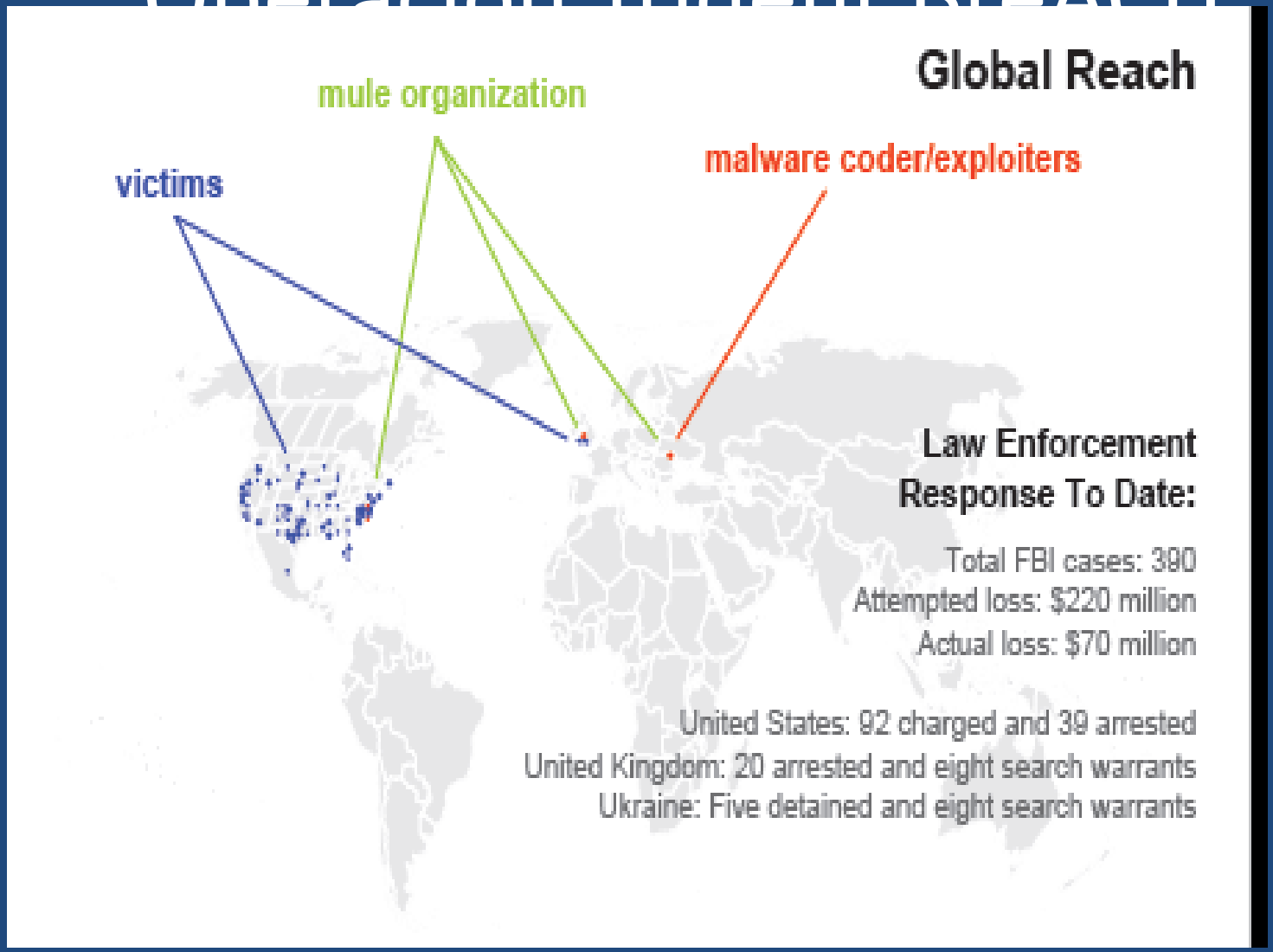
Google Inc.'s Nexus S already has one, and the company's **latest Android software for that and other phones has NFC support**. Nokia Corp., the world's largest maker of phones, has committed to putting NFC chips in all its next-generation smart phones.

There's also speculation the **new iPhone model due this summer will have an NFC chip,** though Apple isn't commenting.

Aplicaciones para Smartphones: ¿Quién olucrado?



Operación Trident BreACH



Operación ACHing MULAS

La organización de las mulas de la visas J-1 en Nueva York:

- **90+ victimas**
- **$3,000,000 en U.S. dolares en los transferencias de ACH exitosas.**
  - **30+ los reclutadores y las mulas acusadas**
  - **Fraude bancario, fraude de pasaportes, la conspiración**
  - **Principalmente portadores de la visa J1 de Ucrania, Moldavia y Rusia**

Overview

- CHIP Program and Network
- Computer Crimes
  - Statutes/Scenarios
- Recent Trends
- Law Enforcement Contacts

What is the CHIP Program?

- Nationwide CHIP Network
- At least one CHIP prosecutor in each of 93 U.S. Attorney's Offices
  - More than 230 CHIP attorneys nationwide
- CHIP Units in 25 U.S. Attorney's Offices
  - San Francisco, Los Angeles, Sacramento, San Diego, Seattle Denver, New Haven, Tampa, Miami, Atlanta, Chicago, Baltimore, Boston, Detroit, Kansas City, Newark. Brooklyn, New York, Philadelphia, Pittsburgh, Nashville, Dallas, San Antonio, Alexandria, and Washington, D.C.

Cybercrime.gov

- Public Page
- Latest News Releases
- Policies & Programs
- Legal Resources
- Contact Info
- Cases

Computer Crime Cases

- Hacking/unauthorized access
  - Theft/Destruction of Data
  - Denial of service attacks
- Computer fraud
- Internet Fraud/ ID Theft

Computer Crimes

- Trespassing
- Theft of Information
- Damaging computers and networks
- Passwords and "Access Devices"

We Want You!

CSI 2009/10 Computer Crime and Security Survey*

- 443 computer security practitioners
- 15 % financial sector
- 15.7 % consulting
- 12.3 % information technology
- 9.5 % government
- 7.7 % health services

CSI Survey

- Types of e-crimes:
  - 64.3% were victims of malware
  - 34% victim fraudulently represented as a sender of email
  - 29.7% victims of insider abuse
  - 42.2% victims of laptop theft
  - 29.2% victims of DOS attacks
  - 19.5% financial fraud

Average loss:

$234,244/organization

Financial Fraud:

$463,100

“Bot” victims:

$345,600

Concerns

- “Professionalization” of computer crime
- Security measures imperfect
  - –Can respond only to known threats
- Targeted Attacks

Degradation of services

- How to tell that intruder's activity is what degraded integrity or function of system?
  - DDoS
  - Any other virus, worms launched at same time
  - Capacity of victim's system
    - Look at what victim did in response to activity- i.e., did they add patches in response to activity.

Issues

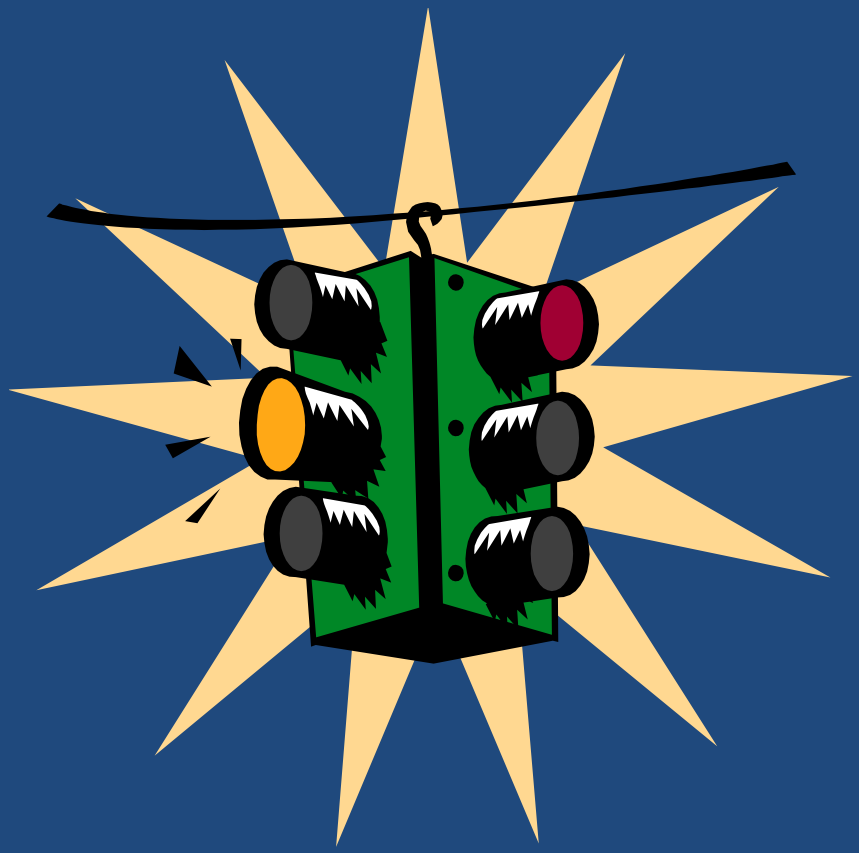
- Can you trace software source code?
- Do you meet monetary thresholds?
  - How to calculate cost of site being down?
  - How to calculate loss of business?
  - Does your statute account for any other disruption of service?
- Compromised machine- universities
  - Will they allow you access to machines?

Website Defacements- Issues

- Victim company repairs site before we can gather evidence
- Source of activity out of the U.S.
- Target may use exploit to get in and do it again,

  and again,

  and again……..



Identity Theft

- Hacker intrusion or insider compromise
- Gumshoe detective work
- Insider vs. Outsider
- Disclosure Requirements

WHAT CAN YOU DO
Protection against Insiders

- Careful record keeping and auditing of computer access
- Regular backups
- Secure passwords (require changes every 120 days; passwords should have capitals, numbers and punctuation)
- Restricted access (need to know)
- Check employee backgrounds (be mindful of employees with financial problems)

What will happen if I call the Feds?

- We will want your system administrator to recover network logs for us.
- We will work with you and your system administrator to find out who attacked you
- We are sensitive to your concerns of negative publicity
- We may not tell you what is going on all the time, but we will try not to disclose without your knowledge
- If you prefer, we will try to keep you out of the news

Law Enforcement Contacts

U.S. Secret Service

Electronic Crimes Squad

305-863-5450

SA Gerald “Mick” Walsh

FBI

Computer Crimes Squad

305- 787-6165

SSA Raymond Goergen

Questions?

AUSA Aurora Fagan
561-820-8711
Aurora.Fagan@usdoj.gov

www.cybercrime.gov
Computer Crime and Intellectual Property Section
U.S. Department of Justice