

Federal Bureau of Investigation



Prepared by SA: Jorge A. Aliaga

UNCLASSIFIED

The FBI San Juan Division



The Federal Bureau of Investigation's San Juan Field Office operates from its Headquarters Office located in Hato Rey, Puerto Rico. The San Juan Field Office covers 78 municipalities, and the US Virgin Islands. To effectively cover this territory, the San Juan Field Office has five Resident Agencies located in Aguadilla, Fajardo, Ponce, St. Thomas, and St. Croix.



Federal Office Building

Suite 526

150 Carlos Chardon Ave.

Hato Rey, PR 00918

Telephone Number: (787) 754-6000



UNCLASSIFIED

What do we investigate?



National Security Priorities

1. Terrorism

- International Terrorism
- Domestic Terrorism
- Weapons of Mass Destruction

2. Counterintelligence

- Counterespionage
- Counterproliferation
- Economic Espionage

3. Cyber Crime

- Computer Intrusions
- Online Predators
- Piracy/Intellectual Property Theft
- Internet Fraud
- Identity Theft

Criminal Priorities

4. Public Corruption

- Government Fraud
- Election Fraud
- Foreign Corrupt Practices

5. Civil Rights

- Hate Crime
- Human Trafficking
- Color of Law
- Freedom of Access to Clinics

6. Organized Crime

- Italian Mafia/LCN
- Eurasian
- Balkan
- Middle Eastern
- Asian
- African
- Sports Bribery

7. White-Collar Crime

- Antitrust
- Bankruptcy Fraud
- Corporate/Securities Fraud
- Health Care Fraud
- Insurance Fraud
- Mass Marketing Fraud
- Money Laundering
- Mortgage Fraud
- More White-Collar Frauds

8. Violent Crime and Major Thefts

- Art Theft
- Bank Robbery
- Cargo Theft
- Crimes Against Children
- Cruise Ship Crime
- Gangs
- Indian Country Crime
- Jewelry and Gem Theft
- Retail Theft
- Vehicle Theft



UNCLASSIFIED

What do we investigate?



National Security Priorities

1. Terrorism

- International Terrorism
- Domestic Terrorism
- Weapons of Mass Destruction

2. Counterintelligence

- Counterespionage
- Counterproliferation
- Economic Espionage

3. Cyber Crime

- Computer Intrusions
- Online Predators
- Piracy/Intellectual Property Theft
- Internet Fraud
- Identity Theft

Criminal Priorities

4. Public Corruption

- Government Fraud
- Election Fraud
- Foreign Corrupt Practices

5. Civil Rights

- Hate Crime
- Human Trafficking
- Color of Law
- Freedom of Access to Clinics

6. Organized Crime

- Italian Mafia/LCN
- Eurasian
- Balkan
- Middle Eastern
- Asian
- African
- Sports Bribery

7. White-Collar Crime

- Antitrust
- Bankruptcy Fraud
- Corporate/Securities Fraud
- Health Care Fraud
- Insurance Fraud
- Mass Marketing Fraud
- Money Laundering
- Mortgage Fraud
- More White-Collar Frauds

8. Violent Crime and Major Thefts

- Art Theft
- Bank Robbery
- Cargo Theft
- Crimes Against Children
- Cruise Ship Crime
- Gangs
- Indian Country Crime
- Jewelry and Gem Theft
- Retail Theft
- Vehicle Theft



UNCLASSIFIED

Transportation



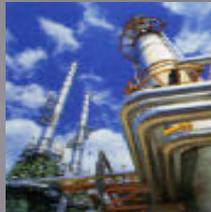
Water



Defense
Industrial
Base



Chemical
Industry



Banking
and
Finance



Government Services



Critical
Infrastructures



Telecommunications



Postal & Shipping



Energy



Public
Health



Emergency
Services



Agriculture



Food

Cyber Concerns Are On The Rise



Cyber Division Focus

The Cyber Division supports investigations dedicated to any of the following violations:

1. Cyber Terrorism
2. Cyber Threats to National Security
3. Computer Hacking
4. IPR Matters
5. Identity Theft
6. Internet Fraud

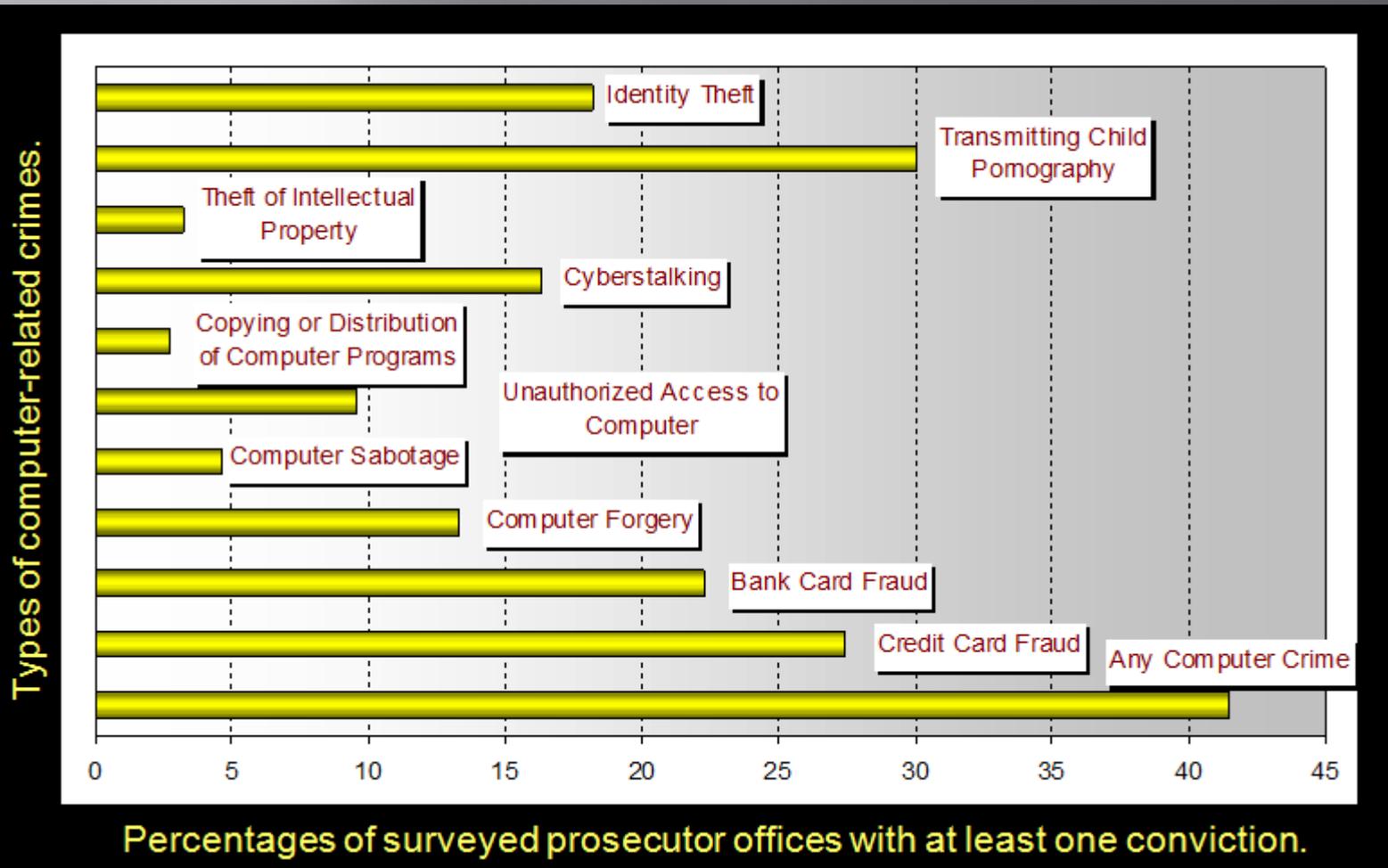


Cyber Division Strategy



- ▣ Identify and disrupt...
 - the most significant individuals, groups and foreign powers conducting computer intrusions, the dissemination of malicious code, or other computer supported network operations.
 - operations targeting U.S. intellectual property.
 - the most significant perpetrators of Internet fraud.

Computer-related Crimes



Computer Intrusion

- ▣ **FBI Cyber Priority 1:** Identify and disrupt individuals and foreign powers conducting intrusions
 - Counterterrorism
 - ▣ Jihad Forums
 - ▣ Cyber Terrorism
 - Counterintelligence
 - ▣ Telecommunication Companies
 - ▣ Universities / Government Agencies
 - Criminal
 - ▣ Banks
 - ▣ Private Sector



Counter-Terrorism

- ▣ WMD
- ▣ Facebook / Twitter
- ▣ Jihad Forums
- ▣ Cyber “Dark” Net / Black market
- ▣ Cyber Terrorism



UNCLASSIFIED

Counter-Intelligence

- ▣ ISP / Telecommunications Companies
- ▣ Government Agencies
- ▣ Universities

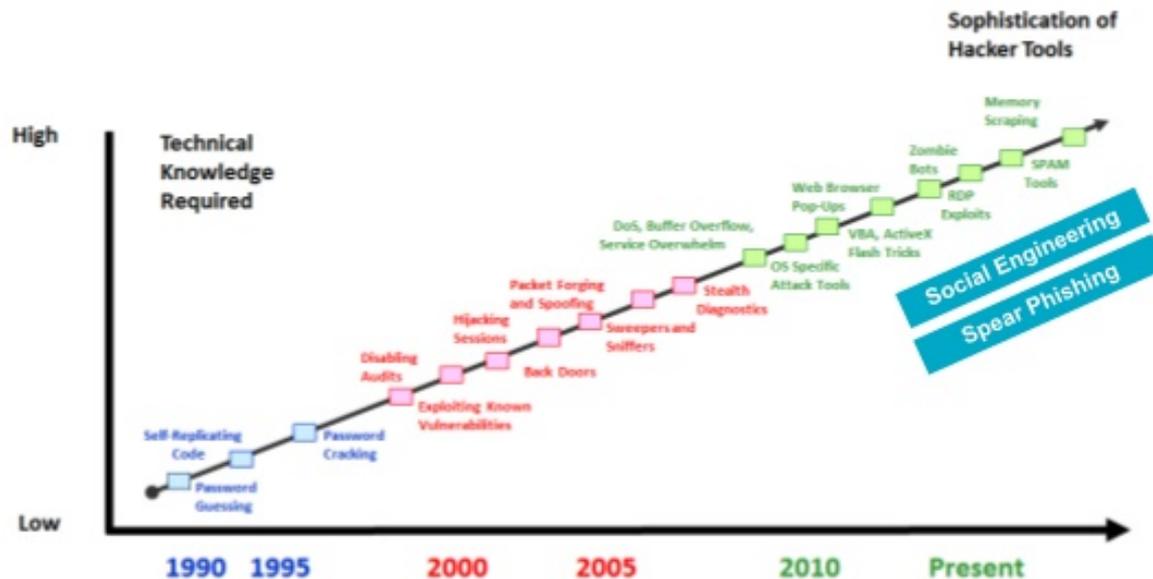


Criminal

- Financially Driven Intrusion
- Private Sector
- Identification Theft



Cyber Security Threat Landscape – Sophistication of Attacks



Threat Vectors / Techniques

- ▣ Virus
- ▣ Worms
- ▣ Botnets
- ▣ APT!!!!
- ▣ Rootkits
 - User
 - Kernel



Most Recent Malware Threat

- ▣ **Shamoon Virus**
- ▣ Comprised of four files



- `trksrv.exe` initial infection agent
- `Netint.exe` communication with remote host
- `Drdisk.sys` provides raw access to disk
- `Dnslookup.exe` wiper component



"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012



IC3



- ❑ Internet Crime Complaint Center
- ❑ The IC3 was established as a partnership between the FBI and the National White Collar Crime Center to serve as a means to receive Internet related criminal complaints.
- ❑ Complaint is researched and referred to federal, state, local, or international law enforcement agencies.
- ❑ Access IC3 at → www.ic3.org

Actions To Take When You Have Been Victimized

- ▣ Contact your local FBI Field Office and report the following:
 - How access was gained
 - Evidence of physical damage
 - Level of access obtained
 - Which programs/files were accessed
 - Which operating systems were involved
 - Value of data exploited
 - Point(s) of origin, dates and times

- ▣ Do NOT contact the suspected perpetrator

What a Special Agent from the FBI Computer Crime Squad Can Do?

- ▣ Combine technical skills and investigative experience
- ▣ Preserve evidence
- ▣ Identify avenues of attack and attackers
- ▣ Provide local, national and global response
- ▣ Apply traditional investigative techniques
- ▣ Integrate law enforcement and national security concerns
- ▣ Develop pattern analysis
- ▣ Suggest mitigation

What a Special Agent from the FBI Computer Crime Squad Cannot Do

- ❑ Take over your system
- ❑ Provide information beyond your need to know
- ❑ Share proprietary information with competitors
- ❑ Become involved in civil action
- ❑ May not keep you advised of status of investigation
- ❑ Provide investigation-related information to the media
- ❑ React with the speed you expect
- ❑ Recover your data

What Can You Do To Combat Computer Crime?

- ▣ Develop and implement security policies and procedures such as the use of:
 - Audit features, antivirus software, and firewalls
 - Automatic intrusion detection software
 - Complex and frequently changing passwords
 - Warning banners on networked computers
 - Monitoring computer access
 - Encryption products
 - Retain logs
 - Be careful with opening your emails
 - ▣ Attachments
 - ▣ Hyperlinks

- ▣ **Your safety begins with your awareness!!!!**



What is InfraGard?

- ❑ A partnership between the FBI and the private sector
- ❑ An association of businesses, academic institutions, state and local law enforcement agencies, and other participants
- ❑ It is dedicated to sharing information and intelligence to prevent hostile acts against the U. S.
- ❑ Chapters are geographically linked with FBI Field Office territories.

www.infragard.net

Learn About Internet Scams & Warnings



A-Z INDEX • SITE MAP

Search Site SEARCH

CONTACT US

ABOUT US

MOST WANTED

NEWS

STATS & SERVICES

SCAMS & SAFETY

JOBS

FUN & GAMES

New E-Scams & Warnings

[Get FBI Updates](#)

[Home](#) • [Scams & Safety](#) • [New E-Scams & Warnings](#)

To report potential e-scams, please go the Internet Crime Complaint Center and file a report. Note: the FBI does not send mass e-mails to private citizens about cyber scams, so if you received an e-mail that claims to be from the FBI Director or other top official, it is most likely a scam.

If you receive unsolicited e-mail offers or spam, you can forward the messages to the Federal Trade Commission at spam@uce.gov.

Below are some recent scams and warnings.

Situational Alert Regarding Charitable Contribution Schemes

08/26/11—In light of Hurricane Irene, the public is reminded to beware of fraudulent e-mails and websites claiming to conduct charitable relief efforts. To learn more about avoiding online fraud, please see "Tips on Avoiding Fraudulent Charitable Contribution Schemes" at: <http://www.ic3.gov/media/2011/110311.aspx>.

Malicious Software Features Usama bin Laden Links to Ensnare Unsuspecting Computer Users

The Internet Crime Complaint Center (IC3) urges computer users to not open unsolicited (spam) e-mails, including clicking links contained within those messages. Even if the sender is familiar, the public should exercise due diligence. Computer owners must ensure they have up-to-date firewall and anti-virus software running on their machines to detect and deflect malicious software.

The IC3 recommends the public do the following:

- Adjust the privacy settings on social networking sites you frequent to make it more difficult for people you know and do not know to post content to your page. Even a "friend" can unknowingly pass on multimedia that's actually malicious software.
- Do not agree to download software to view videos. These applications can infect your computer.
- Read e-mails you receive carefully. Fraudulent messages often feature misspellings, poor grammar, and nonstandard English.
- Report e-mails you receive that purport to be from the FBI. Criminals often use the FBI's name and seal to add legitimacy to their fraudulent schemes. In fact, the FBI does not send unsolicited e-mails to the public. Should you receive unsolicited messages that feature the FBI's name, seal, or that reference a division or unit within the FBI or an individual employee, report it to the Internet Crime Complaint Center at www.ic3.gov.

Reporting E-Scams
File a complaint with the FBI's Internet Crime Complaint Center or contact your local FBI office.

Fake FBI E-mails
Have you received an e-mail from the FBI? It might be a fake. Details

Internet Fraud Advice
Get tips, read victim stories, and test your fraud savvy on LooksTooGoodToBeTrue.com.

UNCLASSIFIED

Questions?



FBI Laboratory, Quantico, VA

UNCLASSIFIED