



APCO  
International

Leaders in Public Safety Communications®

UNCLASSIFIED



Kansas City Terrorism Early Warning  
Inter-Agency Analysis Center  
Cyber Threat Intelligence Program

# **EMERGING TECHNOLOGY FORUM CYBER BRIEFING**

March 15, 2016

UNCLASSIFIED

# Agenda

- What is a Fusion Center?
- CTIP program
- Cyber Threat Landscape
- Cyber Threat Trends

# National Network of Fusion Centers



## Fusion centers are on the front lines of the Nation's homeland security efforts

- **Facilitate sharing** of homeland security and criminal-related information and intelligence
- **Collaborate** to create a shared view of homeland and national security as well as criminal threats within a region
- Facilitating the sharing of information; **common operating picture** between Federal and regional partners
- **Produce** and **disseminate** actionable intelligence against those threats

# Fusion Centers are NOT

**Focused only on Terrorism:** FCs have broader capabilities to assist in counterterrorism as well as all-crimes and all-hazards missions

**Owned by the Federal Government:** FCs are owned and operated by state and local entities with support from federal partners

**A Base for Domestic Spies:** FCs are committed to protecting the privacy, civil rights, and civil liberties of Americans

UNCLASSIFIED

# Information flow



UNCLASSIFIED

UNCLASSIFIED

# Expansive Homeland Intelligence Mission

Cybersecurity

Counterterrorism

Criminal

Border Security and Immigration

Critical Infrastructure

Health Intelligence

UNCLASSIFIED

# National Network Priorities

1. **Receive**: Ability to receive classified and unclassified information from federal partners
2. **Analyze**: Ability to assess local implications of that threat information through the use of a formal risk assessment process
3. **Disseminate**: Ability to further disseminate that threat information to other state, local, tribal, territorial and private sector entities within their jurisdiction
4. **Share**: Ability to gather locally generated information, aggregate it, analyze it, and share it with federal partners as appropriate



# CTIP program

## KCTEW Cyber Threat Information Program - CTIP

- **Formation**

- On October 26, 2011 the KCTEW launched its Cyber Threat Information Program.
- The program's purpose is to gather and produce threat and risk analysis products from and to its Federal, State, Local, Tribal and Private partners regarding various cyber threats.
- A key component of that initiative was the formation of the Missouri Cyber Working Group. The MO-CWG is composed of Federal, State, Local and Private Sector subject matter experts.

## KCTEW Cyber Threat Information Program - CTIP

- **Threats/Risks**

- **Cyber Terrorism** would include threats or attacks that would, if successful, damage or incapacitate IT systems or Critical Infrastructure served by those systems. *(Applicable directives: PDD-63, PPD-21, EO-13636)*
- **Cyber Crime** threats would include theft of information, identity theft, privacy invasion, system alteration, system subversion and others. *(Applicable directives: US Code Title 18-1030, various applicable state and local laws and ordinances)*

## KCTEW Cyber Threat Information Program - CTIP

- **Scope of Program**
  - Does not provide consulting, remediation or investigative services.
  - Supplies information about specific threats, analysis and other information to enable it's Federal, State, Local, Tribal and Private Industry partners to use for their Cyber Terrorism/Cyber Crime prevention efforts.

# KCTEW Cyber Threat Information Program - CTIP

- **Sources**
  - **Open Source**
  - **Partnerships**
    - Cyber ILOs
    - Industry Sector partners
    - Federal ( FBI, DHS, USSS, US-CERT)
    - ISACs (MS\_ISAC, FS\_ISAC, ES\_ISAC, etc)
  - **Internal**
    - KCTEW Analysts
  - **Classified**

## KCTEW Cyber Threat Information Program - CTIP

- **Products**
  - **CTIP Bulletin**
    - As needed
  - **“Urgent” or “Specials Bulletins”**
  - **Threat/Risk Analysis**
  - **Briefings**

UNCLASSIFIED

# CYBER THREAT LANDSCAPE

UNCLASSIFIED

# Cyber Threat Landscape

- **Cyber Threat Actors**
  - State Sponsored
  - Terrorist/Violent Extremists
  - Insider Threat
  - Hackers
  - Hacktivists
  - Criminals / Organized Crime



# Cyber Targets

- **Government Networks**
  - Federal
  - State
  - Local
  - Tribal and Territorial
- **Critical Infrastructure and Key Resources (CIKR) Networks**
  - Over 85% owned by private sector
  - Industrial Control Systems/SCADA
  - Embedded systems
- **Business and Home Networks**



# Cyber Threats to Critical Infrastructure

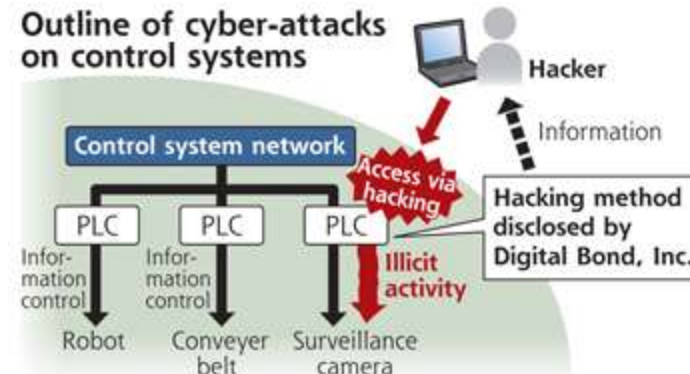
- **Supply Chain Exploitation**
- **Disruption**
- **Cyber Crime**
- **Corporate Espionage**
- **Advanced Persistent Threat**
- **Industrial Control Systems/SCADA**

# Devices, Systems and Networks

- Desktops/Laptops
  - OS/App
- Servers
  - OS/App
- Printers
- Routers
- VPN
- **DNS system**
- Mobile devices

# Targeting and Attack Techniques

- Social engineering
- Spear phishing
- Spoofing e-mail accounts
- Exploiting vulnerabilities
- Malware
  - Downloaders, Trojans, Keyloggers, etc.
- External memory devices (USB)
- Supply-chain exploitation
- Leveraging trusted insiders
- Denial of Service
- Mobile Device Attacks




# Spear-Phishing

- Targeted e-mails containing malicious attachments or links
- E-mails forged to look as if they came from a legitimate source and have a subject that the victim is likely to open
- Target e-mail addresses can be harvested from Web sites, social networks, etc.
- Targeting of CEOs, executives is called “whaling”

# Sample Phishing Website

← → ↻ http://npamail.svpnpa.gov.in/sitekey/online/sslencrypt218bit/online\_banking/

**Bank of America**  **Higher Standards** Online Banking

---


**Sign In**

**Enter Online ID:**   
(5 - 25 numbers and/or letters)  
☐ Save this online ID ([How does this work?](#))

**Enter Passcode:**   
(4 - 12 numbers and/or letters)

[Sign In](#)

[Reset passcode](#)  
[Forgot or need help with your ID?](#)

 **Stop writing checks  
and you could save \$53**  
[Learn more >>](#)

Not using Online Banking?  
[Enroll now  
for Online Banking >>](#)


[Learn more  
about Online Banking >>](#)

[Service Agreement >>](#)


[Pay By Phone user's guide >>](#)


[Go to Online Banking for  
a state other than California](#)

---

 **Secure Area**

[Home](#) ▪ [Locations](#) ▪ [Contact Us](#) ▪ [Help](#) ▪ [Sign in](#) ▪ [Site Map](#)  
[Personal Finance](#) ▪ [Small Business](#) ▪ [Corporate & Institutional](#)  
[About the Bank](#) ▪ [In the Community](#) ▪ [Finance Tools & Planning](#) ▪ [Privacy & Security](#)

Bank of America, N.A. Member FDIC. Equal Housing Lender   
© 2007 Bank of America Corporation. All rights reserved.

Official Sponsor 2000-2004  
U.S. Olympic Teams 

(Via fsecure.com)

# Sample Phishing Website

The image shows a web browser window with a URL bar containing the address `http://npamail.svpnpa.gov.in/sitekey/online/sslencrypt218bit/online_banking/`. A red oval highlights this URL, and a red arrow points from it to a text box that reads "Compromised police academy server in India". The website itself has a header with the text "Online Banking" and a red horizontal bar. Below this is a "Sign In" section with two input fields: "Enter Online ID:" (containing "asdasd") and "Enter Passcode:". The "Enter Online ID:" field has a note "(5 - 25 numbers and/or letters)" and a checkbox labeled "Save this online ID" with a link "(How does this work?)". The "Enter Passcode:" field has a note "(4 - 12 numbers and/or letters)". A "Sign In" button is located below the passcode field. On the right side of the page, there is a sidebar with links: "Not using Online Banking? Enroll now for Online Banking >>", "Learn more about Online Banking >>", "Service Agreement >>", and "Pay By Phone user's guide >>".

Compromised police academy server in India

Online Banking

Sign In

Enter Online ID:   
(5 - 25 numbers and/or letters)  
☐ Save this online ID ([How does this work?](#))

Enter Passcode:   
(4 - 12 numbers and/or letters)

[Sign In](#)

Not using Online Banking?  
[Enroll now for Online Banking >>](#)

[Learn more about Online Banking >>](#)

[Service Agreement >>](#)

[Pay By Phone user's guide >>](#)

(Via fsecure.com)

## Sample Spearphishing Email



(Via nytimes.com)

## Advanced Persistent Threat (APT)

- Category of cyber attack against political, business, or economic targets
  - Federal agencies
  - State agencies
  - City governments
- Commercial and non-profit organizations
- Actors use full spectrum of computer intrusion techniques and technology
- Characterized by focus on specific information objectives rather than immediate financial gain
- Stealthy, coordinated, focused activity over a long period of time



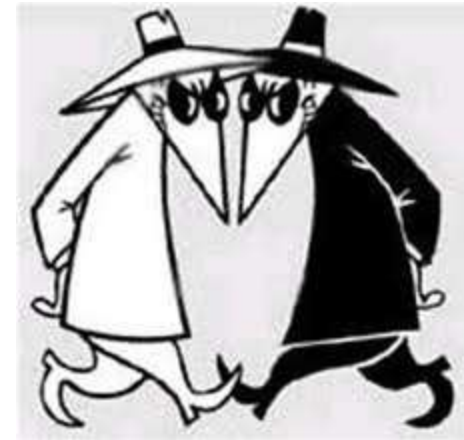
**Operators are skilled, motivated, organized, well-funded**

# Recent Cyber Events

- Shamoon (aka: Wiper) – Steals credentials wipes boot record from 30,000 to 50,000 computers at Saudi Aramco and RasGas.
- Banking DDOS against JP Morgan/Chase, PNC, Wells Fargo, Bank Of America. Total of 8 banks attacked.
- South Carolina DOR. – 3.8 million SSNs stolen and tax returns exposed.

# So What ?

- **Computer network exploitation by threat actors enables:**
  - Massive financial losses
  - Degradation/disruption of services
  - Extortion
  - Intellectual property theft
    - Counterfeiting
    - Theft of proprietary data
- Identity theft (personally identifiable information)
  - Access to credit
  - Loss of money and credibility



UNCLASSIFIED

# CYBER THREAT TRENDS

UNCLASSIFIED

# Trends

- **ENORMOUS** increase in Cyber Attacks/Crime both in numbers and sophistication.
  - State sponsored attacks likely to increase. (Cyber Warfare is real now.)
  - Stuxnet /DUGU is reportedly a U.S. Cyberweapon



Cyberweapon toolkits using FLAME, Stuxnet, DUGU will be utilized by not only state sponsored attackers, but by any entity with medium/high skills.



## Trends

### Nation-States That Have Declared Offensive Cyber Capability

- Iran
- India
- UK
- China
- Russia
- U.S.A.
- Australia
- Italy
- France
- Syria
- Germany
- Israel

# Trends

## Hactivists

- Alliances with ideologically similar groups
- More Skilled
- More Organized
- More Aggressive
- More of them

# Trends

## Cyber Criminals

- Can occasionally approach the sophistication if not the endurance of State sponsored attackers
- Adding much more emphasis to mobile devices.
- Adds a physical dimension to the Cyber realm.

# SCENARIO

## Cyber Attack **DURING** A Disaster

When combined like this, the event would be known as a “blended attack” each attack amplifying the others.

Intent of attacker is to cause harm – as much harm as possible.

This is Cyber Terrorism

# SCENARIO

## Cyber attack During a disaster



## SCENARIO

### Cyber attack During a disaster

- The EM infrastructure is “DDOSed”
  - Distributed Denial of Service attacks are made periodically against the WEBEOC servers and gateways.
  - TDOS attacks are made against LEO, Fire and Health Service PSAP exchanges.
  - Trunking communications are compromised/incapacitated with DDOS attacks.

## SCENARIO

### Cyber attack During a disaster

- The “Cryptolocker” virus is spread to large segments of responders via an email with an attached infected PDF document entitled “Incident Response Plan”.
  - Anyone opening the document has all their files irrevocably encrypted.
  - A number of users are attached directly or through a VPN connection to shared storage and all THOSE files are encrypted as well, affecting hundreds of users.

## SCENARIO

### Cyber attack **During** a disaster

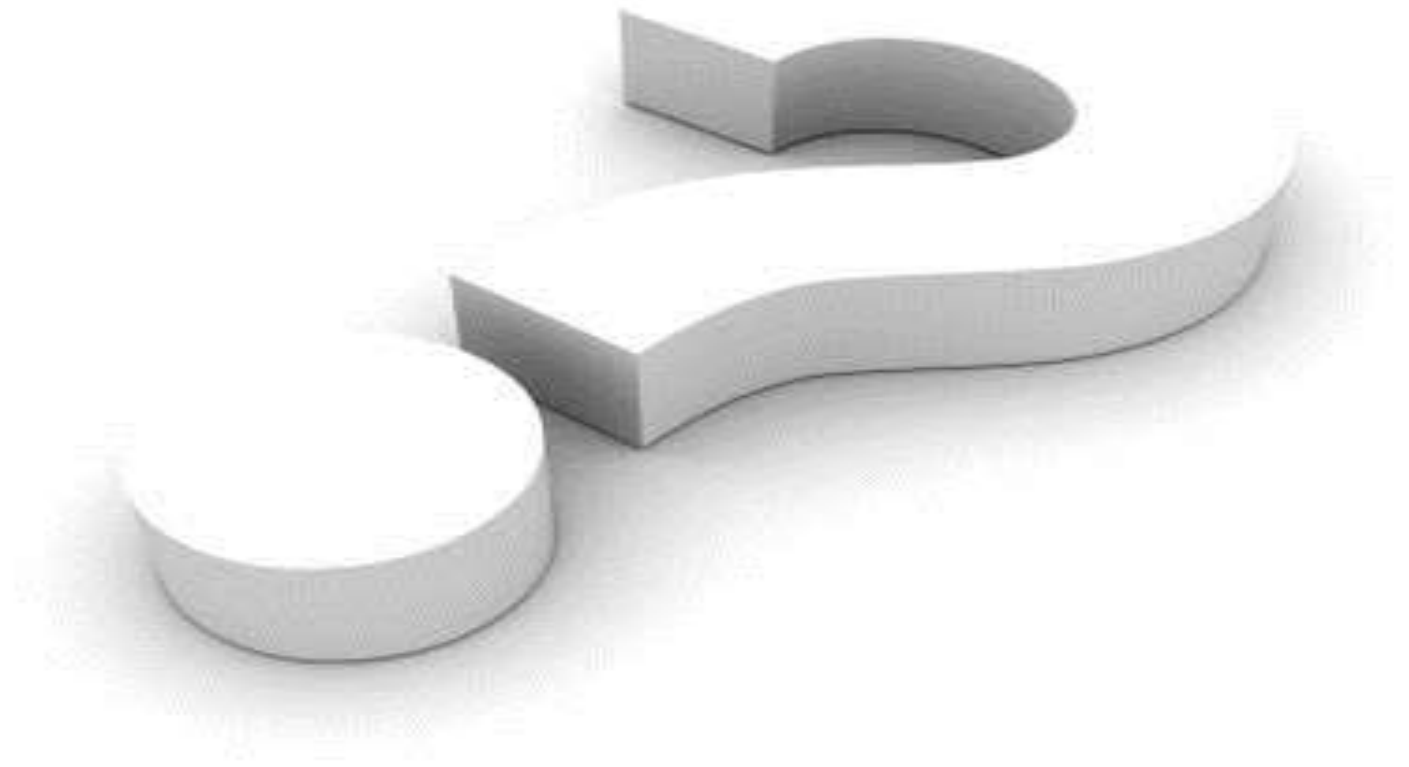
- **Strategic systems are Infiltrated with a “RAT” – Remote Access Trojan, another type of APT. (RAT was installed via spear phishing email.)**
  - Response plans, emails, credit cards, account credentials, responder PII are exfiltrated (stolen) and published on hacker websites.
  - CAMJacker is turned on. Any webcam or microphone is tapped.

## SCENARIO

### Cyber attack During a disaster

- Masses of user computers are attacked by Wiper (“Wiper” is a virus that destroys the boot track and format table of a hard disk – Installed along with the RAT or Cryptolocker).
  - Forty eight hours after the start of the initial Cryptolocker attack, the Wiper virus renders hundreds of hard disk drives unusable, forcing the replacement or reformatting of all the drives.

# Questions



UNCLASSIFIED



**Kansas City Terrorism Early  
Warning Fusion Center  
Cyber Threat Intelligence Program (CTIP)**

**[troy.campbell@kcpd.org](mailto:troy.campbell@kcpd.org)  
(816) 413-3588**

UNCLASSIFIED