Goals

- Cyber – It’s a team sport!
- Authorities
- Trends
- Case discussions

Cyber as an FBI Priority

- To protect the United States against:

- Terrorist attack
- Foreign intelligence
- operations and espionage
- Cyber-based attacks and
- high technology crimes

- As the only U.S. agency with the authority to investigate both criminal and national security cybersecurity threats, the FBI is following a number of emerging trends.

Cyber as an FBI Priority

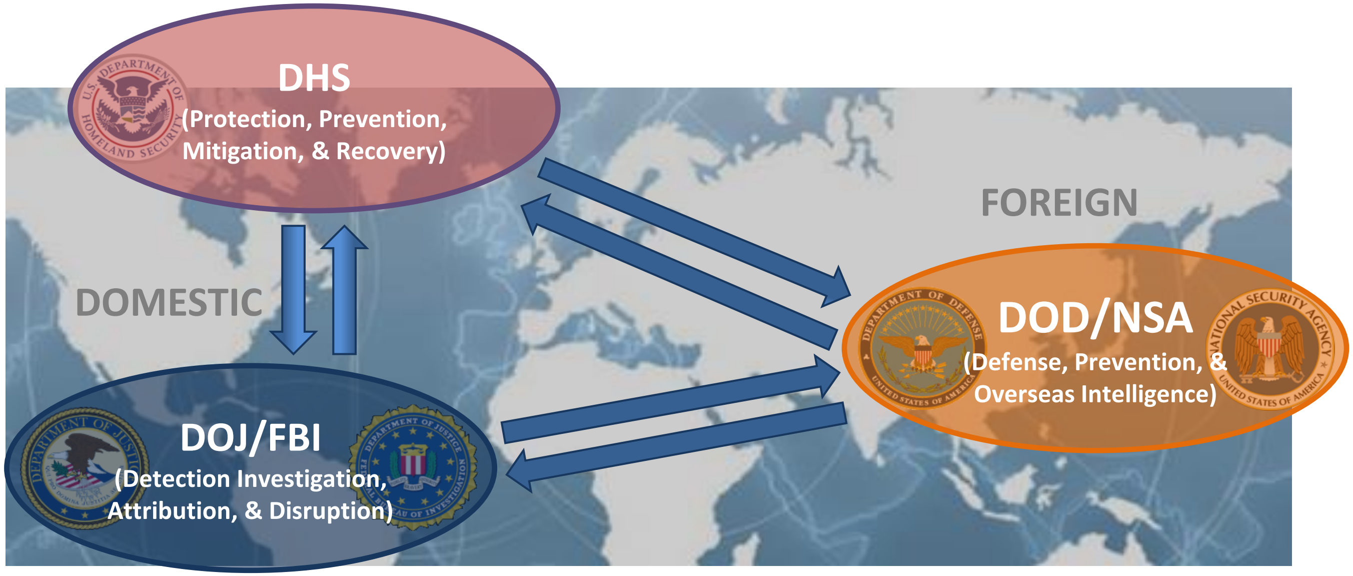
- 2002
  - Cyber placed as number three priority for the FBI
- 2003
  - President’s National Strategy to Secure Cyberspace
- 2012
  - Realignment of resources, hiring initiative
- 2014
  - Restructuring of National Security threats

FBI - Cyber ALATs

- FBI Operates LEGAT offices in 79 locations
- In 2010, FBI Cyber Division instituted Cyber ALAT Program
  - Embed ALATs with host nation counterparts
    - Bucharest, Romania
    - Kyiv, Ukraine
    - Riga, Latvia
    - Tallinn, Estonia
    - The Hague, Netherlands

USG Cybersecurity Responsibilities

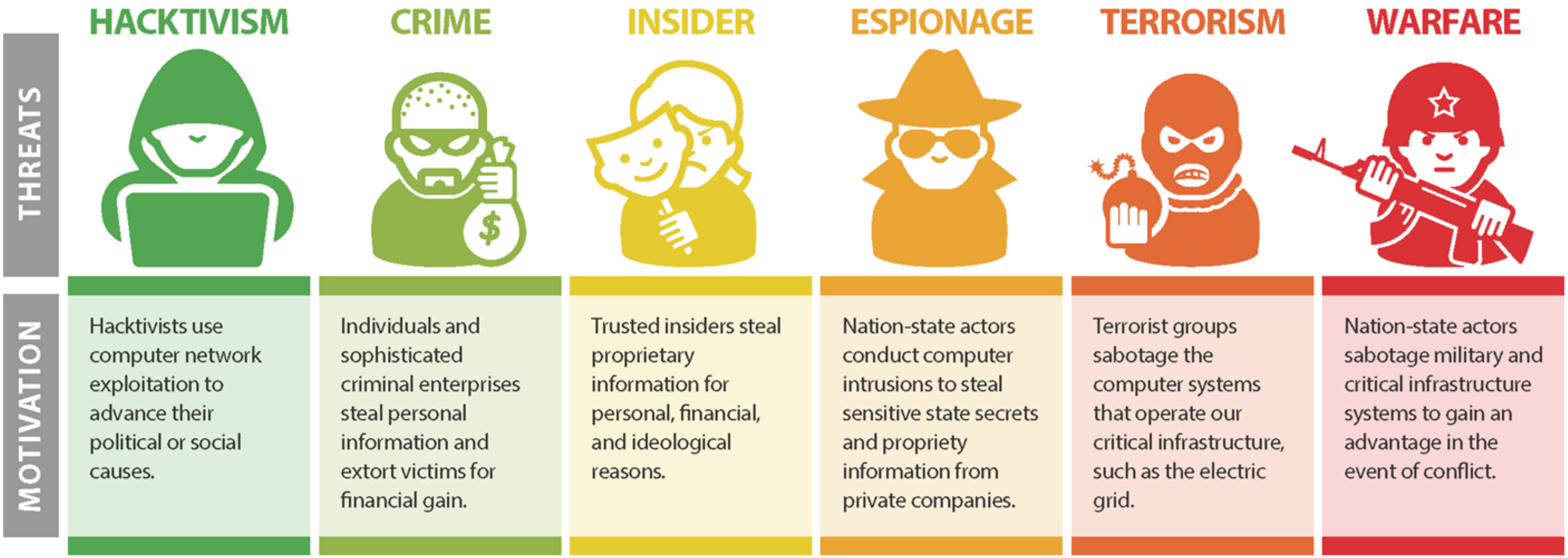
- Coordinate the national protection, prevention, mitigation of, and recovery from cyber events
- Disseminate domestic cyber threat and vulnerability analysis
- Protect critical infrastructure
- Secure federal civilian systems
- Investigate cyber crimes under DHS' jurisdiction


DHS
(Protection, Prevention, Mitigation, & Recovery)
FOREIGN
DOMESTIC
DOD/NSA
(Defense, Prevention, & Overseas Intelligence)
DOJ/FBI
(Detection Investigation, Attribution, & Disruption)

- Investigate, attribute, disrupt, and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate cyber threat investigations

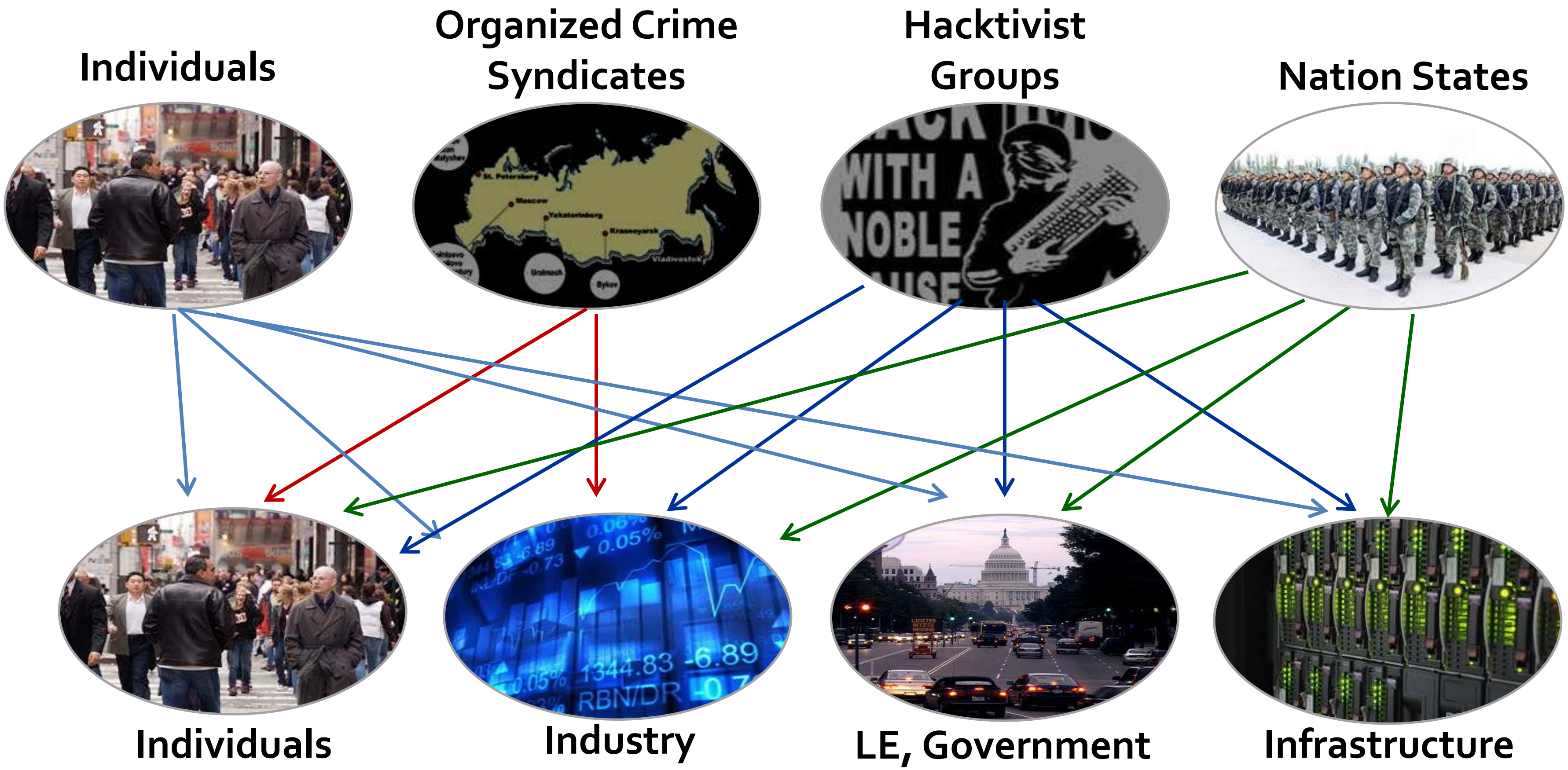
- Defend the nation from attack
- Gather foreign cyber threat intelligence and determine attribution
- Secure national security and military systems
- Support the national protection, prevention, mitigation or, and recovery from cyber incidents
- Investigate cyber crimes under military jurisdiction

Top Cyber Threats



THREATS	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

Current and Emerging Criminal Trends



Individuals

Organized Crime Syndicates

Hacktivist Groups

Nation States

Individuals

Industry

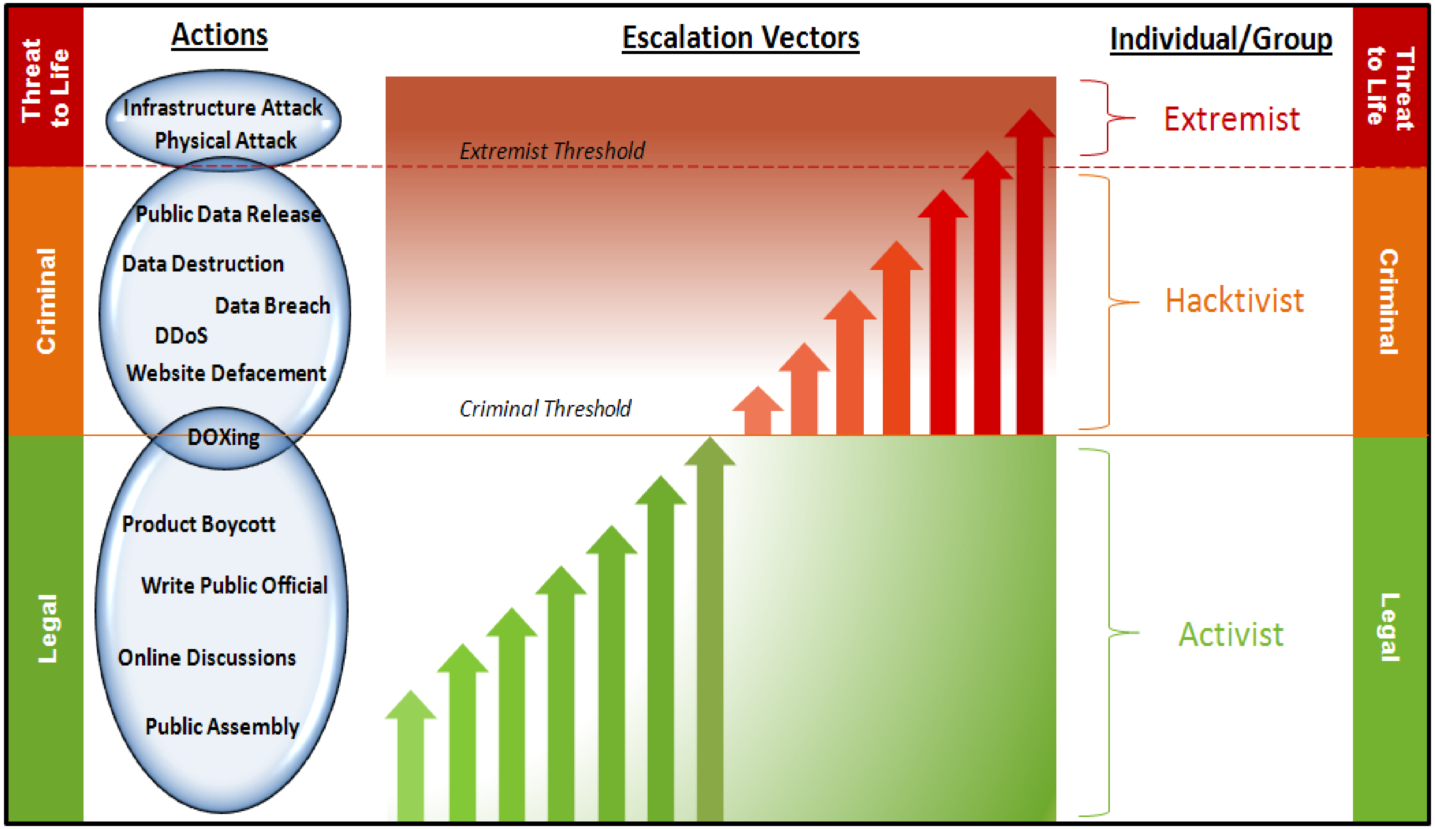
LE, Government

Infrastructure

Hacktivism

Hacktivism: Computer network exploitation or attack to advance a political or social cause.

Hacking for activism = hacktivism



Advanced Persistent Threat (APT)

APT refers to nefarious cyber activity with national security implications. As opposed to criminally based cyber attacks, this intrusion activity more closely resembles espionage with actors stealing information from networks, as well as priming relevant systems to enable ongoing access to them.

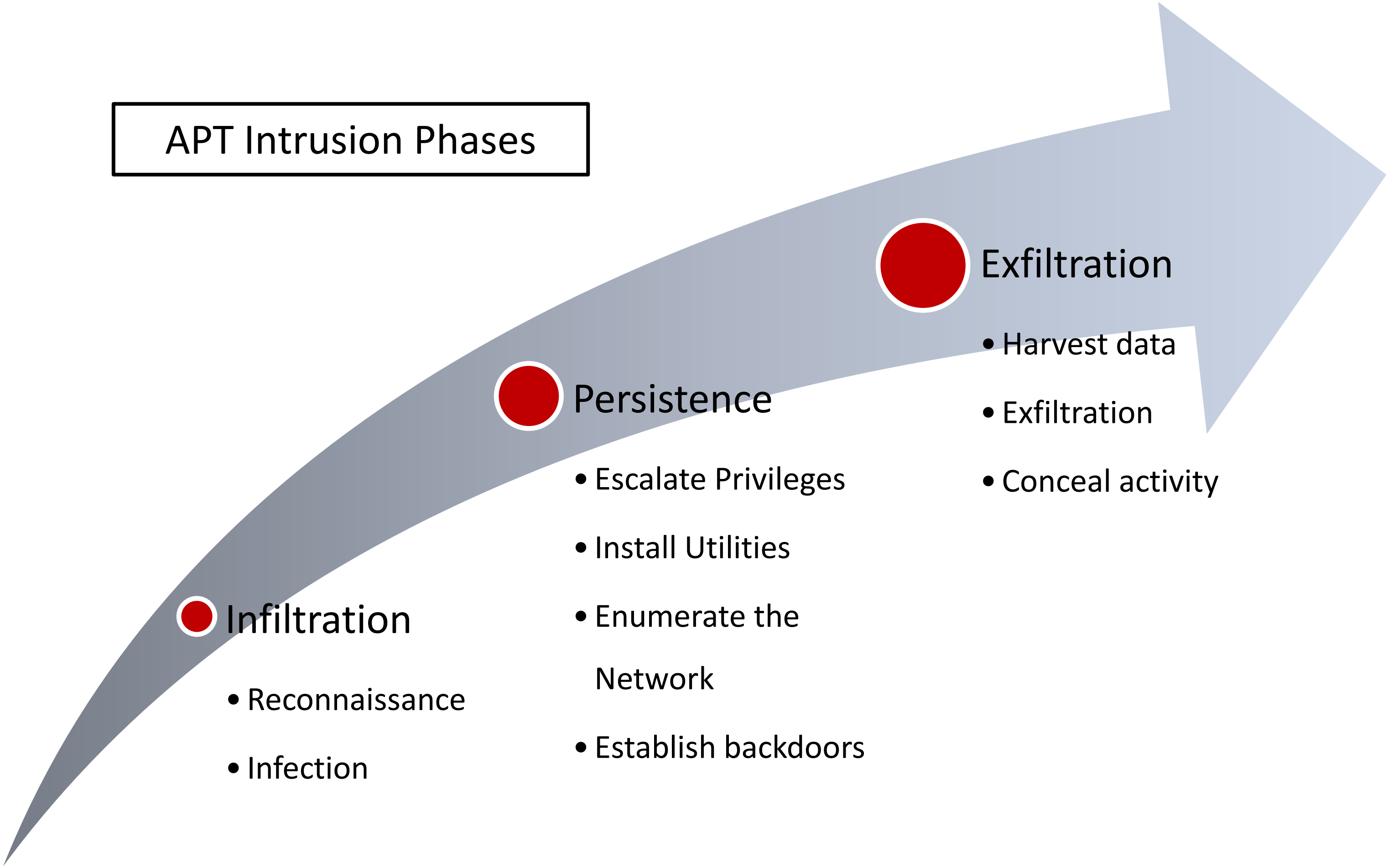
Goals:

1. Steal information that can provide advantage
2. Establish and maintain network presence

- Actors are successful in harvesting enormous amounts of critical information including proprietary data, source code, negotiation tactics, and strategic operational plans.

Advanced Persistent Threat (APT)

APT Intrusion Phases



Infiltration

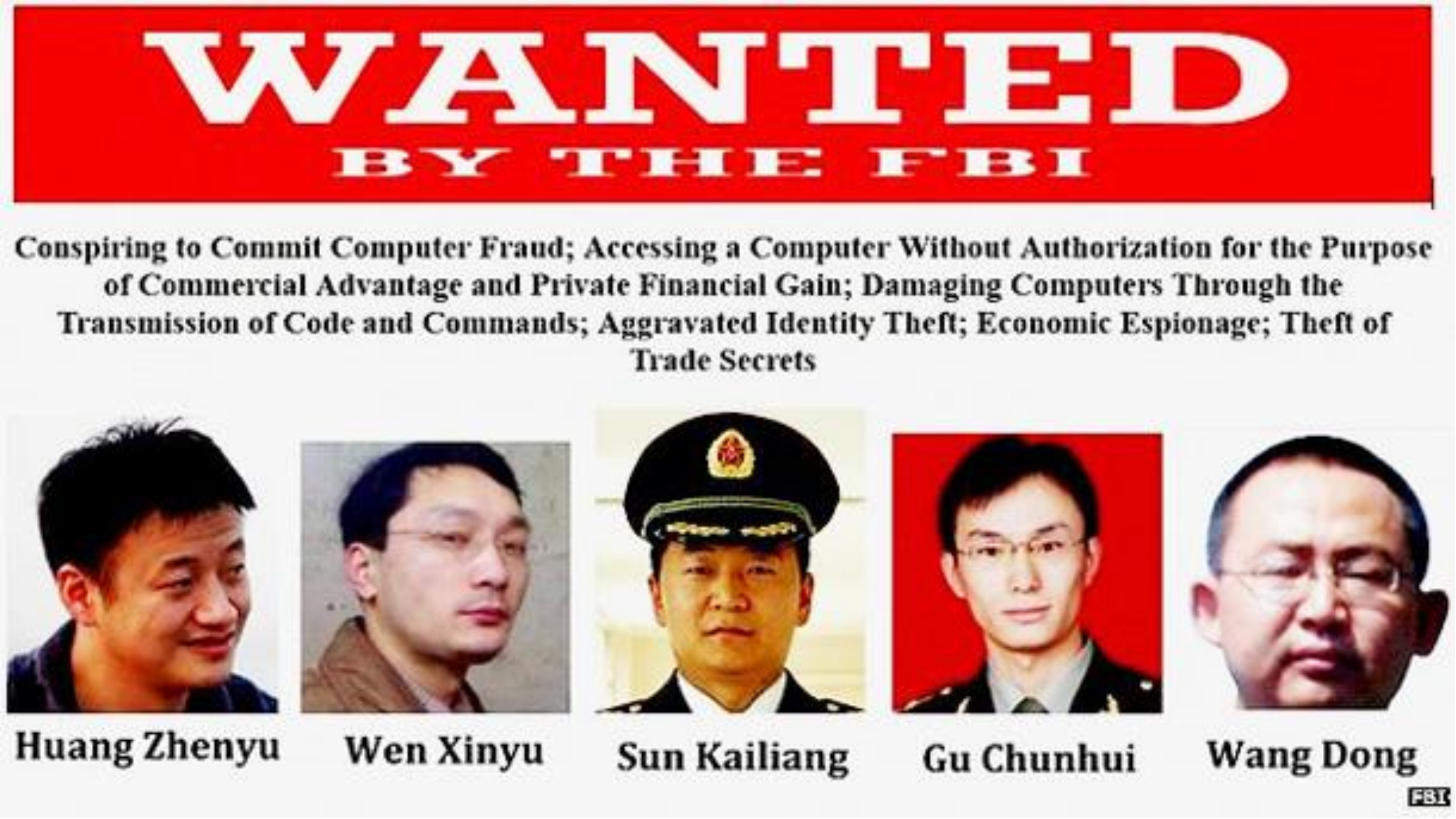
- Reconnaissance
- Infection

Persistence

- Escalate Privileges
- Install Utilities
- Enumerate the Network
- Establish backdoors

Exfiltration

- Harvest data
- Exfiltration
- Conceal activity



WANTED

BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Huang Zhenyu **Wen Xinyu** **Sun Kailiang** **Gu Chunhui** **Wang Dong**

FBI

FBI Cyber – trends

- Insider v Outsider
  - Deterrence, not detection
  - Case examples
- Team Cyber
  - Info sharing, attribution, collaboration, action
  - Citizens Academy, InfraGard, Outreach
- Don’t click the email, backup, PWD
- Ransomware v email spoofing

InfraGard
www.infragard.org

What is InfraGard

“ A cooperative undertaking between the U.S. Government (the FBI) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. “

National InfraGard

- Over 50,000 members nationwide and 86 Chapters
- A non-profit association of businesses, academic institutions, and state and local government offices
- Improves information-sharing and cooperation between government and private industry
- Establishes meaningful liaisons at all levels of law enforcement and private sector
- Provides members access to FBI, DHS and DoD analytical products and threat advisories
- Encourages private sector cooperation with law enforcement

Spearfishing – Don’t open!

- **From:** MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
  Sent: Thursday, October 16, 2014 4:45 PM
  To: William Pelgrin
  Subject: CIS CYBER ALERT - Invoice Phishing Spam Campaign Distributing Dyre Banking Trojan - TLP: WHITE
-
- **TLP: WHITE**
- **CIS CYBER ALERT**
-
- **TO**: All Members
-
- **DATE ISSUED**: October 16, 2014
-
- **SUBJECT**: Invoice Phishing Spam Campaign Distributing Dyre Banking Trojan
-
- CIS recently became aware of a massive spam campaign targeting users in various sectors. Phishing emails used in the campaign contains a PDF attachment named Invoice621785.pdf. This attachment is a weaponized PDF document exploiting a vulnerability in Adobe Reader (CVE-2013-2729). After successful exploitation, user’s system will download additional malware from hxxp://rlmclahore.com/Resources/Search/1510out[.]exe. This is a banking trojan similar to Zeus/Citadel that it targets sensitive user information including banking credentials. As of this writing, all of the major AV products are detecting this malware as Tojan Dyre/Zbot/Fondu.
-
- **Phishing Email Characteristics:**
- • Subject: "Unpaid invoic” [Please note the typo in the subject line]
- • Attachment: Invoice621785.pdf
-
- **System Level Indicators (If successful in exploitation):**
- • Copies itself under C:\Windows\[RandomName].exe
- • Created a Service named ""Google Update Service” by setting the following registry keys:
- o HKLM\SYSTEM\CurrentControlSet\Services\googleupdate\ImagePath: "C:\WINDOWS\pfdOSwYjERDHrdV.exe"
- o HKLM\SYSTEM\CurrentControlSet\Services\googleupdate\DisplayName: "Google Update Service"