The Cyber Threat: Securing Cyber Infrastructure

Overview

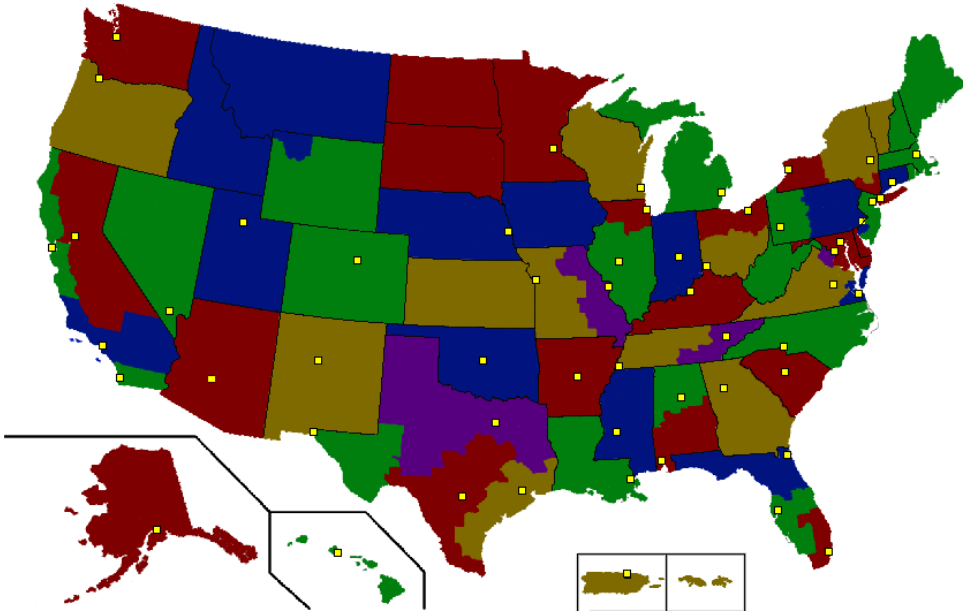
- What are the FBI's Priorities?
- What is the FBI's Cyber Structure?
  - HQ Division
  - Dedicated Cyber squads in all 56 field offices, including satellite locations overseas.
  - Cyber Identity Crisis
- Who works the Cyber Threat?
  - Special Agents, Intelligence Analysts, Support, Computer Scientists, Linguists, Contractors

Cyber Mission

- What does the FBI's Cyber Mission look like?
  - Goals:
    - Investigate and collect evidence NOT secure networks.
    - Disrupt threats through arrests, technical ops, intel sharing, etc
      - Benefits victims
    - Change how we share information with the Private Sector, make it a smoother and faster process.

Resources

- Local Field Office
  - Intake
  - Complaints
  - Liaison
- FLASH
- Strategic Outreach
  - Briefings
- Infraguard
- IC3
- NCFTA



What Do We Investigate?

TARGET

YAHOO!

ebay

THE HOME DEPOT

WENDY'S

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Anthem BlueCross

LinkedIn

JPMorganChase

SONY PICTURES

Cyber Threats

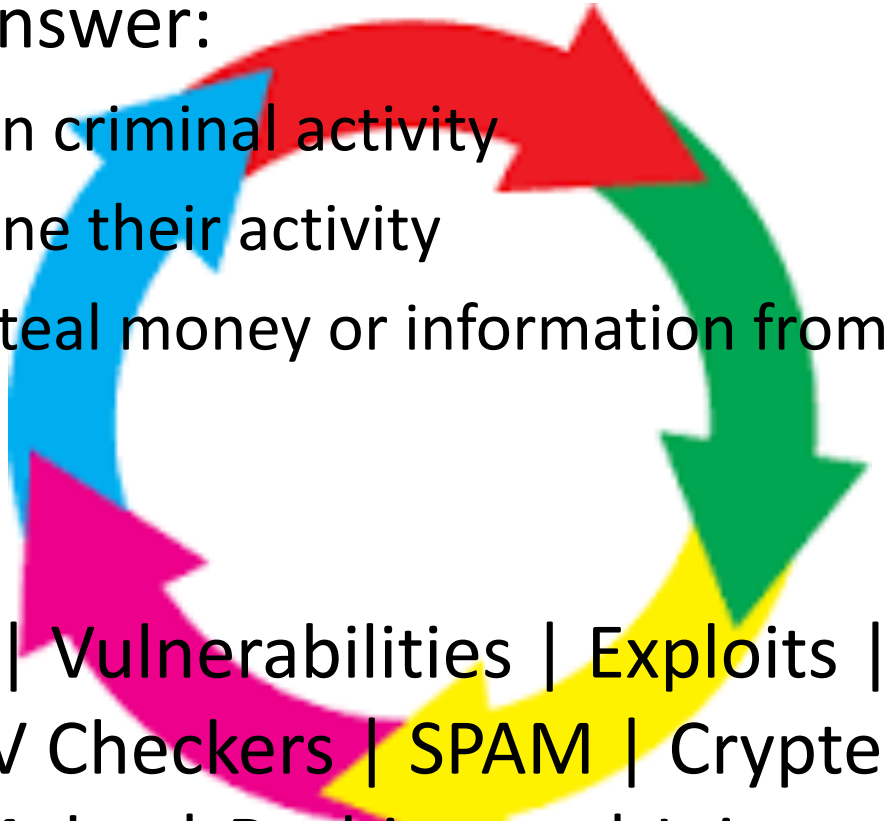
- Hacktivist
- Criminal
- Insider
- Lone Wolf
- Nation State
- Military
- Terrorist

Cyber Crime Landscape

- Borderless
- Complex global problem
- Criminal can be anywhere
- Victims can be everywhere
- Endless possibilities
- Applies to BOTH Criminal and Nation State hacking groups

How Do They Do It?

- General answer:
  - Engage in criminal activity
  - Streamline their activity
  - Simply steal money or information from their victims.



Malware | Vulnerabilities | Exploits | Loaders | Botnets | AV Checkers | SPAM | Crypters | Cash out services | Mules | Reshippers | Injects | BP Hosting

Criminal

- Goal:
  - Make Money through:
    - Data breaches
    - Malware
    - Money Laundering
    - ID Theft
    - Stolen Credit Cards
- Who:
  - Hacking groups, typically located outside the U.S.

Hennadiy Kapkanov

Joint Cyber Operation Takes Down Avalanche Criminal Network

FBI took part in a successful multi-national operation to dismantle Avalanche, alongside our law enforcement partners representing 40 countries and with the cooperation of private sector partners. The investigation involved arrests and searches in four countries, the seizing of servers, and the unprecedented effort to sinkhole more than 800,000 malicious domains associated with the network

Nation State/Military

- Goal:
  - Obtain information from Private Sector companies, or Government entities.
  - High-Tech Espionage
  - Cyber Warfare
- Who:
  - Military
  - Intelligence Services
  - Government sponsored hackers

Insider/Lone Wolf

- Goal:
  - To disrupt or destroy company infrastructure
- Who:
  - Employee/Former Employee
  - Expert Knowledge

THE UNITED STATES ATTORNEY'S OFFICE
WESTERN DISTRICT of PENNSYLVANIA

FOR IMMEDIATE RELEASE
Thursday, June 1, 2017
Houston Man Admits Hacking and Damaging Computers of Pittsburgh-area Health Care Facility

Prosecutors: NSA contractor may have had plans for more leaks

Hacktivist

- Goal:
  - To Promote Ideology
  - For Publicity and/or Disruption
- Who:
  - Non-Specific
  - Often Part of a Group

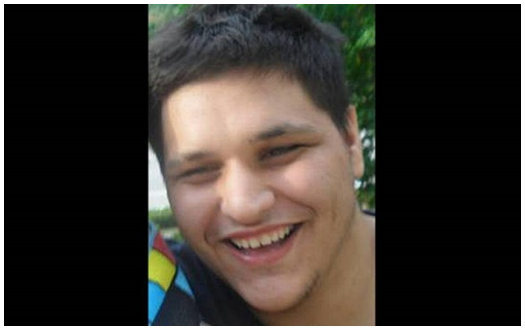
Terrorist

- Goal:
  - Trying to cause harm/terrorize
- Who:
  - Non-Specific, Domestic/International

Hacker charged with cyber terrorism gets 20 years

By: Matthew Barakat, The Associated Press, September 23, 2016

ALEXANDRIA, Va. — A computer hacker who helped the Islamic State group by providing names of more than 1,000 U.S. government and military workers as potential targets has been sentenced to 20 years in prison.



Open Discussion & Questions

- SA Abigail Smith- FBI Pittsburgh
  - Abigail.Smith@ic.fbi.gov
- IA Andrew Czyzewski – FBI Pittsburgh
  - Andrew.Czyzewski@ic.fbi.gov