(U) Cyber Threats to the Homeland

October 2016

The overall classification of this briefing is:

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Warning: This product may contain US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. US person information is highlighted with the label USPER and should be protected in accordance with constitutional requirements and all federal and state privacy and civil liberties laws.

Threat

Capability x Intent = Threat

- Capability – Resources that permit a successful attack
  - People – Well-trained? Single actor? Team? Backed by nation-state?
  - Tools – Malware, hardware, infrastructure
  - Tactics – Established techniques, practiced, new or poorly understood?
- Intent – The will to undertake an attack
  - Target
  - Desired end-state
  - Doctrine/Redlines

A "Zero " in either category is "Zero" Threat. Many terrorist groups have Intent with no capability. Friendly Nation States, Universities, Researches, and National labs have capability with no intent.

State Actors

- **Most capable, active, and dangerous cyber adversaries**
  - Advanced tradecraft and technical expertise
  - Indigenously developed exploitation tools
  - Well resourced
  - Social engineering (spear phishing), extensive research and target profiling, DDoS attacks

- **Exploitation supports, political, military, economic strategy planning and intelligence collection**
  - Persistent compromise, access, and exfiltration
  - Industrial espionage focused on emerging technologies
  - Competitive advantage in trade negotiations and corporate mergers
  - Some have incorporated cyber operations into military doctrine

Use comprehensive, well-honed tactics to gain persistent access throughout networks.

Cybercriminals

Chronic cyber threat

- One of the most capable
- Capability of some organized criminal rings exceeds many state actors
- Tool development values exploitation over disruption/destruction

Profit is only motivator

- Commoditization of malware and exploit tools reduces technical barriers to carrying out criminal activity
- Target vulnerable systems (e.g., point-of-sale, automated teller machines) for sensitive information
  - Employ Ransomware to exploit victims
  - Steal PII for financial gain

Seek to exploit networks for financial gain, not attack for the purpose of disruption or damage. Threat will increase due to robust underground marketplace and ongoing tool development.

Criminal Hackers

Low-to-moderate-level capabilities

- Poor command and control and varying capability
- Lack of funds and resources

Engage in criminal activity to advance political or ideological agenda

- Goals include publicity and exposing targets
- Limited lasting effect on actual operations
  - Website defacements
  - DDoS attacks
  - "Doxing"

(U//FOUO) Seek high-profile "ops," conducting nuisance attacks with limited effectiveness. An unpredictable actor, little threat of a damaging or destructive attack.

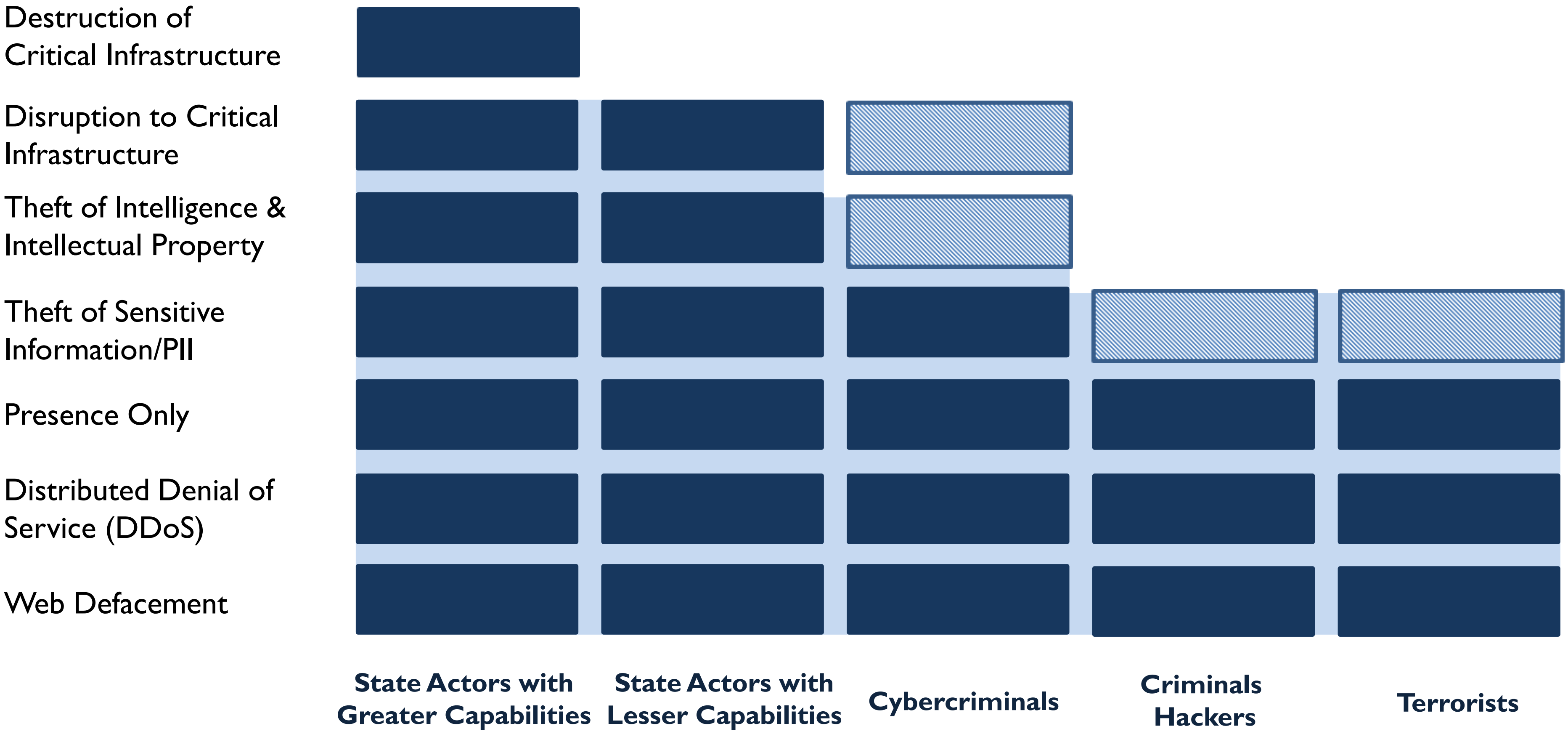
Terrorists

Least capable cyber actors

- Limited indigenous capability
- Use internet for recruitment & propaganda
- Using simple online tools to steal PII and conduct "Doxing"
- Targets of opportunity/non-persistent
- Promote violent extremism

A high-impact cyber attack from terrorists has a lower probability due to rudimentary understanding, but possible targets of opportunity hold the potential for a high-profile event.

Assessing Cyber Actor Capabilities



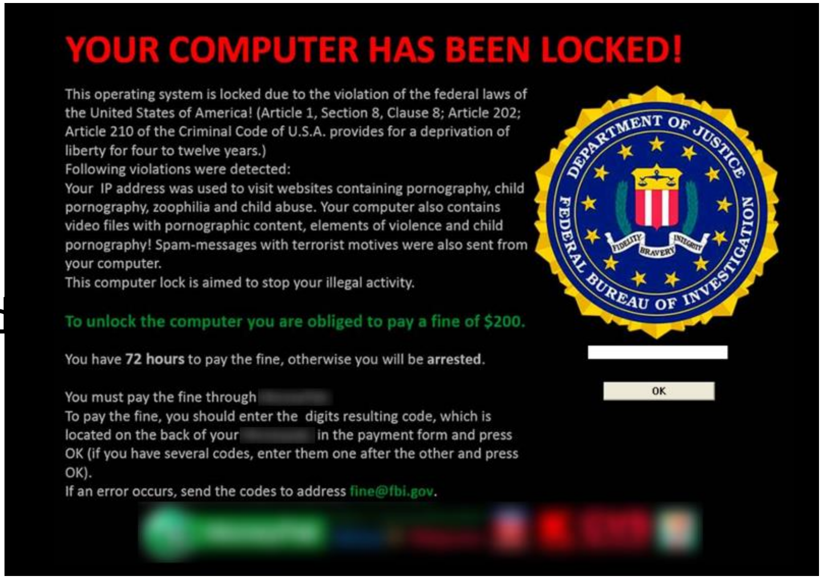
	State Actors with Greater Capabilities	State Actors with Lesser Capabilities	Cybercriminals	Criminals Hackers	Terrorists
Destruction of Critical Infrastructure	■				
Disruption to Critical Infrastructure	■	■	▨		
Theft of Intelligence & Intellectual Property	■	■	▨		
Theft of Sensitive Information/PII	■	■	■	▨	▨
Presence Only	■	■	■	■	■
Distributed Denial of Service (DDoS)	■	■	■	■	■
Web Defacement	■	■	■	■	■

Motivation and resources drive development of cyber capabilities

Recent Threats to State, Local, and Private Sector

Ransomware

- Criminal actor-associated
- Around since 2005
- Encrypts systems and/or key files
- Demands a ransom be paid to decrypt files
- Infection vectors: phishing, compromised websites, other malware
- Can target any computer
- Proliferation of adaptations and variants
- Recent events of note:
  - Spread through interconnected healthcare facilities across 3 states
  - Focused campaign against MA state gov, 71 attempts in a short timeframe



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested**.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

[redacted]

Noteworthy Vulnerability

Internet of Things

- Increasing number of endpoint devices
- Endpoint devices are poorly protected
  - Medical devices
  - Children's toys
  - Kitchen appliances
  - Baby monitors and cameras
- Recent event of note:
  - 25,000+ Internet-connected CCTV units compromised, used in botnet DDoS attack
  - University printers at 12 universities set to print racist and anti-Semitic propaganda

Recent Threats to North Carolina

Scanning and Reconnaissance

- Preparatory activity
- High levels of activity, low threat

Barrage of Attempts

- SQL injection attempts against public-facing websites
- Brute force password attempts

More Successful Incidents

- State agency ransomware infection
- DDoS against NC legislative body
- CEO spoofing emails for money transfers
- Phishing/spearphishing

Takeaways & Resources

Threats to SLTT networks and data

- Best-case: Low-level disruptions and nuisance-type activity (website defacements and denial-of-service,)
- Worst-case: Intent to severely deny, degrade, disrupt SLTT and CI networks
- Most likely: Exfiltration and release of data (PII), and nuisance-type activity to exploit targets of opportunity

Resources – mitigation/recovery/info sharing, investigations, best practices

- Mitigation/recovery/info sharing:
  - National Cybersecurity and Communications Integration Center (NCCIC) NCCIC@hq.dhs.gov
  - US-Computer Emergency Readiness Team (US-CERT) SOC@us-cert.gov
  - Multi-State Information Sharing and Analysis Center info@msisac.org
- Criminal investigations: US Secret Service (USSS) and US Immigration and Customs Enforcement (ICE)
- Best practices: National Institute of Standards and Technology (NIST) Cybersecurity Framework
  - Cyber Security Self-Assessment Tool: Baldrige Cybersecurity Excellence Builder

SLTT Law Enforcement Cyber Incident Reporting

Organization	What to Report?
National Protection and Programs Directorate (NPPD)	
National Cybersecurity and Communications Integration Center (NCCIC) (http://www.dhs.gov/about-national-cybersecuritycommunications-integration-center) NCCIC@hq.dhs.gov or (888) 282-0870	Suspected or confirmed cyber incidents that may impact critical infrastructure and require technical response and mitigation assistance
United States Secret Service (USSS)	
Secret Service Field Offices (http://www.secretservice.gov/field_offices.shtml) Electronic Crimes Task Forces (ECTFs) (http://www.secretservice.gov/ectf.shtml)	Cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment Information
Immigration and Customs Enforcement Homeland Security Investigations (ICE HSI)	
ICE HSI Field Offices (http://www.ice.gov/contact/inv/) ICE HSI Cyber Crimes Center (http://www.ice.gov/cyber-crimes/)	Cyber-based domestic or international cross-border crime, including child exploitation, money laundering, smuggling, and violations of intellectual property rights
Federal Bureau of Investigation (FBI)	
FBI Field Offices (http://www.fbi.gov/contact-us/field) Cyber Task Forces (http://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1) Law Enforcement Online Portal (https://www.cjis.gov/CJISEAI/EAIController) or (888) 334-4536	Cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity

Questions?

The overall classification of this briefing is:

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Warning: This product may contain US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. US person information is highlighted with the label USPER and should be protected in accordance with constitutional requirements and all federal and state privacy and civil liberties laws.