THREAT PICTURE OF OPERATIONAL TECHNOLOGY AND CONTROL SYSTEMS

Adam Akridge, Senior Cybersecurity Program Manager
Engineer Research and Development Center (ERDC)
Information Technology Lab (ITL)

Federal Facilities Council
Standing Committee on Cyber and Physical Security and Hazard Mitigation

Disclaimer: The views expressed during this presentation do not represent official or enforceable US Government, USACE, or ERDC Policy. The presenter is not committing or obligating the government in any way.

U.S. ARMY

US Army Corps of Engineers®

ERDC
ENGINEER RESEARCH & DEVELOPMENT CENTER

ADVERSARIAL TARGETING OF OT/CS SYSTEM

Adversaries demonstrate capabilities and intent of targeting Operational Technology (OT) and Control Systems (CS) through cyber means to impact physical processes

- This presents risk to mission readiness, production, and safety.

OT/CS Attacks

Volt Typhoon Threat Group

Joint CISA Alert-State Sponsored Compromise and Persistent across US. Critical Infrastructure

22 Danish Power Organizations breached in 2023

Required shift to local control

6 Hours and 230k people

Time Ukraine lost power due to Cyberattack

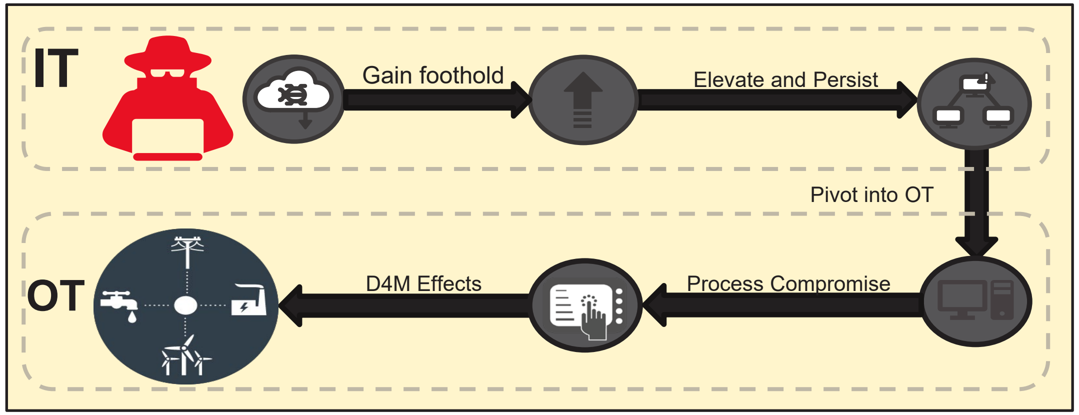
$5M

Paid in ransom by Colonial Pipeline

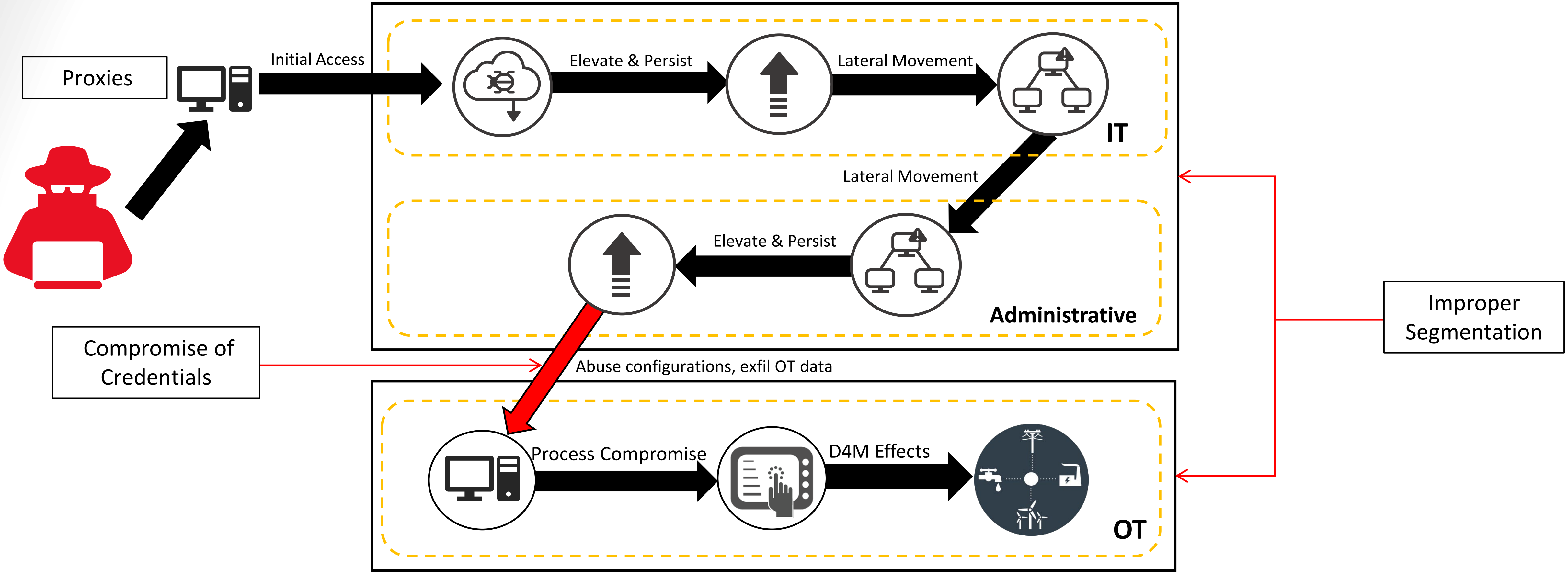
OBSERVED TTPS

Adversary goal: Gain and Maintain persistence to the environment for future action

- Extensive reconnaissance conducted against organization, network, and staff
- Initial access gained to IT or OT network
  - Network appliances
  - Engineer Workstations
- Harvesting credentials targeting domain controllers, remote access tools, and administrators
- Network Discovery and mapping using Live of the Land binaries (LoLBins) or tailored malware
- Maintain, expand, and fortify access to persist on network
- File obfuscation, log clearing
- Slow exfiltration of OT documents, diagrams, process data for attack development
- Effects: process change/manipulation, Ransomware, wiping, physical damage



Attacking OT/CS Networks



PERSPECTIVES ON SECURE ARCHITECTURE NETWORK DESIGN

- Design your architecture with the knowledge you are being targeted (and they may know how your systems work)
- Design with system resilience in mind
- Limit surface area
- Be prepared to operate in degraded operations/ local control (islanding)
  - Test your Defensive Cyber Plan
  - Backup and restoration capability
- Auditing & logging (network and host), and time sync
  - Log offloading
- Plan for failures, know what will happen when they do.

PERSPECTIVES ON OT CYBER PROGRAM DESIGN

- Create ownership
  - Establish roles, responsibilities, and duties.
  - If no one is assigned that task no one is doing it
- Define your boundaries and know what you have
  - Understand dependencies on other systems and what systems depend on you
- Choose a framework (Nist 800-53r5 RMF, NIST 800-82r3, 800-171r2, NIST CSF, CIS)
- Find the engineer workstations! How is media moved between domains?
- Locate your project files/logic files determine ownership
- If compromise is detected assume full domain compromise

SOURCES AND REFERENCES

- *Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems (ICS)*, US Cyber Command, https://apps.dtic.mil/sti/citations/AD1056116

- *Guide to Industrial Control Systems (ICS) Security*. SP 800-82, rev. 3., NIST (National Institute of Standards and Technology), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

- *Identifying and Mitigating Living Off the Land Techniques*, Joint Publication led by DHS CISA multiple co-authors, https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques

- *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Joint Publication led by DHS CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

- *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, Joint Publication led by DHS CISA multiple co-authors, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

- The attack agasint Danish, critical infrastructure, SEKTORCert, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

- *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure,* Joint Publication led by DHS CISA multiple co-authors, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a

Questions?