Cyber Threats and Countermeasures

David Landry, CISSP
US-CERT

- U.S. Computer Emergency Readiness Team
- Cybersecurity lead for U.S. government
- Protect .gov
ICS-CERT

• Industrial Control Systems
• Respond to water, power, and manufacturing cyber issues
• Supervisory Control and Data Acquisition (SCADA)
NCCIC

- National Cybersecurity and Communications Integration Center
- Coordinate U.S. government responses to physical and cyber threats
- Includes Law Enforcement and Information Sharing and Analysis Center (ISAC) reps
Threats

• Criminal
  – $$$$  
  – Distributed Denial of Service (DDOS)  
  – Cryptolocker  
  – Bots  
    • DDOS, Spam, mine BitCoin, click-fraud  
  – Credential Stealing  
    • Keyloggers
Threats

• Insider
  – Violate trust relationship
Threats

• Advanced Persistent Threat
  – Advanced
    • Custom malware
    • Zero Day use
    • Establish link to Command and Control (CnC)
  – Persistent
    • Multiple infections
    • Hard to find / eradicate
  – Use established accounts
    • “look like an insider”
Source - Mandiant
Intrusion Steps

• Reconnaissance
• Attack
• Lateral Movement
• Escalate Privileges
• Maintain Access
• Exfil
Countermeasures
Goal

Minimize time between intruder’s first unauthorized access and your discovery / eradication

“typical advanced attack is unnoticed for nearly 8 months” - Mandiant
Network Architecture

• Log everything
  – 30 days Netflow
  – Account access date/time

• Segmentation
  – Private Virtual Local Area Networks (VLANS) with port restriction

• 2 Factor Authentication
Top 4 Strategies

• Applications whitelisting
• Patch applications
• Patch Operating System
• Minimize admin privileges
Large Organizations

• Priorities
  – Protect the crown jewels
    • Encryption
  – Manage risk
• Dedicated network security personnel
• Beware the FEAR of the butterfly effect
• Blue team yourself
Personal

• Don’t get Phished
• 2 accounts minimum on your laptop
  – Admin
  – The one you actually use
• Protect your PII
  – Password protect docs