INTEL REPORT 2: CRITICAL INFRASTRUCTURE THREAT ANALYSIS

CLASSIFICATION: UNCLASSIFIED//FOR TRAINING USE ONLY
EXERCISE INTELLIGENCE REPORT 002-25
FROM: Infrastructure Protection Intelligence Unit
DTG: 161200ZJUL25
SUBJECT: Critical Infrastructure Cyber Threats - "Digital Storm"

KEY JUDGMENTS

- EXERCISE - Simulated nation-state actor "Digital Storm" likely planning cyber operations against U.S. critical infrastructure
- Primary targets assessed as power grid and water treatment facilities based on EXERCISE intelligence
- Operations likely timed to coincide with simulated geopolitical events
- Threat actor demonstrates advanced SCADA/ICS exploitation capabilities in EXERCISE scenarios

THREAT ACTOR PROFILE

Group Name: Digital Storm (Simulated)
Assessment: Nation-state sponsored
Primary Objectives: Infrastructure disruption and intelligence collection
Secondary Objectives: Demonstrating cyber capabilities for deterrence

Capabilities:

- Industrial Control System (ICS) exploitation
- SCADA system manipulation
- Custom malware for operational technology (OT) networks
- Social engineering targeting infrastructure operators

TARGET ANALYSIS

Primary Targets (EXERCISE):

1. **Power Generation Facilities**
    - Vulnerability: Aging SCADA systems with limited cybersecurity
    - Impact: Regional power outages affecting military installations
    - Timeline: Likely during simulated crisis periods
2. **Water Treatment Plants**
    - Vulnerability: Internet-connected monitoring systems

    - Impact: Contamination or service disruption
    - Timeline: Coordinated with other infrastructure attacks
3. **Transportation Hubs**
    - Vulnerability: Interconnected traffic management systems
    - Impact: Logistics disruption and public safety concerns
    - Timeline: Peak travel periods for maximum effect

ATTACK VECTORS

Initial Compromise:

- VPN vulnerabilities in OT networks (EXERCISE)
- Phishing campaigns targeting plant operators
- Third-party vendor compromise
- Physical access through insider threats

Lateral Movement:

- Network protocol exploitation (Modbus, DNP3)
- Credential theft from engineering workstations
- Wireless network infiltration

Impact Operations:

- HMI manipulation to confuse operators (EXERCISE)
- Safety system bypass or disabling
- Process parameter modification
- Data destruction or corruption

DEFENSIVE MEASURES

Immediate (EXERCISE):

- Implement network segmentation between IT and OT systems
- Monitor for suspicious remote access activity
- Review vendor access controls and authentication

Short-term:

- Deploy OT-specific security monitoring tools
- Conduct operator training on social engineering
- Test incident response procedures for OT environments

Long-term:

- Modernize legacy SCADA systems with security controls

- Establish threat intelligence sharing with industry
- Develop backup operational procedures

INTELLIGENCE REQUIREMENTS

1. Specific malware samples used in OT environments (EXERCISE)
2. Command and control infrastructure details
3. Insider threat indicators and recruitment methods
4. Timeline for planned operations during simulated scenarios

ASSESSMENT CONFIDENCE: High for capabilities, Medium for intent timing
DISTRIBUTION: Infrastructure protection stakeholders and EXERCISE participants