WaterISAC

Cybersecurity Incidents and Emerging Threats

September 10, 2014

Topics

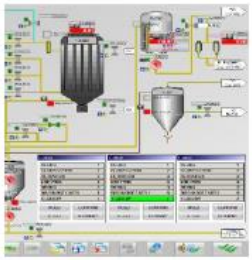
- Recent incidents
  - (U//FOUO) Breach at water utility
  - Ransomware infections
  - Theft of sensitive computer equipment
  - Social engineering attempt at water utility
- Emerging threats
  - Targeted attacks
  - Havex Trojan
  - Zero-day vulnerabilities vs. known vulnerabilities
  - Password security

(U//FOUO) Breach at Water Utility

COMPROMISE

Threat actor attempts to infiltrate U.S. water utility

Threat actor gains access to control system network



- Sophisticated actor
- Brute-force attack

- Multiple Internet-accessible remote access services
- Simple password protection

- System exposed to numerous security threats
- Previous intrusion activity

MITIGATION

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Initial Response

- ICS-CERT notified by third party vendor
- ICS-CERT contacted utility and performed analysis of intrusion
- Analysis revealed:
  - No indication of ICS changes
  - No impacts to system
- ICS-CERT conducted cybersecurity evaluation and design architecture review

Corrective Actions

- Security measures increased
- Additional controls established on remote access capabilities
- Networks segmented
- WaterISAC provided sector awareness of incident and lessons learned/recommendations

Recommendations

- Minimize network exposure for all control system devices
- Employ secure methods, such as VPNs
- Remove, disable, or rename default system accounts
- Implement strong passwords
- Implement account lockout policies
- Monitor administrator level accounts by third-party vendors
- Apply patches as necessary
- Scan networks for vulnerabilities (e.g., Shodan)
- "I'm not a target" mentality must be dismissed

Ransomware Infections

- Cryptolocker encrypted one terabyte of a water utility's business data files
  - No industrial control systems were affected
  - Utility recovered files through a backup
- Other ransomware infections were reported thereafter
- Nexus to GameOver Zeus (GOZ) botnet
- Ransomware threat likely to continue

Theft of Sensitive Computer Equipment

- Computers containing sensitive information were stolen from a water utility's administrative office
  - Occurred around the same time as thefts of other items (cell phones, tablets, money, etc.)
  - Insider involvement deemed likely

Social Engineering Attempt

- Water utility administrative office received call from someone claiming to be from “corporate IT”
- Asked for a process control engineer by name
  - Requested PCE’s “username and password for the main system”
- Caller hang up after being refused this information

Targeted Attacks

- Increases in the length and sophistication of attacks
  - If an organization is exposed, it will very likely be targeted
- Certain individuals within organizations may be targeted given their responsibilities

Havex Trojan

- ICS software vendor websites compromised
  - Legitimate software infected with Havex Trojan
- So far, this malware has only been observed scanning networks and sending information back to servers
  - What else is to come?

Zero-Day Vulnerabilities vs. Known Vulnerabilities

- Zero-day vulnerabilities get much attention, but known vulnerabilities are the most exploited
- Emphasis needs to be placed on maintaining awareness of and implementing patches, as necessary

Password Security

- Recent incidents have undermined trust in the traditional password
  - OpenSSL Heartbleed vulnerability
  - Russian hackers amass 1.2 billion online credentials
  - Numerous database breaches
- Possible future alternatives
  - Biometrics?
  - More two-factor authentication?

WaterISAC

Thank You

WaterISAC Contact Information:

Charles Egli
Lead Analyst
analyst@waterisac.org

1-866-H2O-ISAC