ICS, SCADA, and Non-Traditional Incident Response

Kyle Wilhoit
Threat Researcher, Trend Micro
$whoami

• Threat Researcher, FTR, Trend Micro
  • Threat Researcher at Trend Micro- research and blogger on criminal underground, advanced persistent threats, and vulnerabilities/exploits.

• Research:
  • Malware detection/reversing
  • Persistent Threats (Malware based espionage)
  • ICS/SCADA Security
  • Vulnerabilities and the “Underground”
  • Offensive Exploitation
Agenda

- Honeynet
- Forensics
- SCADA
- DNP3
- Pro-Active
- ICS Incident
- Honeypot
- Modbus
What are ICS devices?

- Used in production of virtually anything
- Used in water, gas, energy, automobile manufacturing, etc.
- Notoriously insecure…in every way
- Software is sometimes embedded, sometimes not
- Typically proprietary
Glossary

- **HMI**: Human Machine Interface
- **IED**: Intelligent Electronic Device
- **SCADA**: Supervisory Control And Data Acquisition
- **RTU**: Remote Terminal Unit
- **Historian**: Data Historian
- **Modbus**: Most common ICS Protocol
- **DNP3**: Very common ICS Protocol
Typical ICS Environment
Security Concerns - ICS vs. Traditional IT Systems

ICS
- Correct Commands Issued (Integrity)
- Up-time (Availability)
- Protection of data (Confidentiality)

IT
- Protect the data (Confidentiality)
- Protect communication (Integrity)
- Limit interruptions (Availability)
ICS Vulnerabilities

• In 2012, 171 unique vulnerabilities affecting ICS products.
  • 55 Vendors…

Figure 4. Incidents by Sector – Fiscal Year 2012
Unique ICS Concerns - Incident Response

• Remote...
• Lack of INFOSEC knowledge
• Lack of engineer knowledge of INFOSEC
• Unknown embedded/proprietary OS
• Lack of network layout knowledge
• Lack of logical access
Unique ICS Concerns- Forensics

• Remote…
  – Imaging?!?!?

• Embedded/Proprietary operating systems

• WAN/LAN Links
BUT WHAT CAN WE DO?
Story Time…

• Small town in rural America
• Water pump controlling water pressure/availability
• Population 18,000~
Story Time...

- Water pressure system Internet facing
- No firewalls/security measures in place
- Could cause catastrophic water pressure failures
Story Time…

Attacked several times…During Q3-Q4
Attackers successfully gained access
Has not been made public

This is not a story…
Real life event..
This Happened.
In my basement...
Enter Pro-Active Incident Response

HONEY
Not always the best diet
Honeypot Overview

- Two low-interaction
- One high-interaction
- Ran for 28 days in total
- One Windows Server 08
- Two Ubuntu 12.04 Servers

THIS IS A PRODUCTION UNIT- MAKING CHANGES WILL VIOLATE THE INTEGRITY OF THE WATER MONITORING SYSTEMS, AND COULD ADVERSELY AFFECT WATER CONTAINMENT.
What They See
What is an Attack?

- **ONLY** attacks that were targeted
- **ONLY** attempted modification of pump system (FTP, Telnet, etc.)
- **ONLY** attempted modification via Modbus/DNP3
- **DoS/DDoS** will be considered attacks
Attacks

1 Spear Phishing Attempt...
Attacks

- Vxworks exploitation attempt
- Attempt to shutdown pump system
- Modify temperature output
- Modify pump pressure
- Secured area access attempt
- Modbus traffic modification
- Modification of CPU fan speed
Need for ICS Incident Response

• No focused interest seen...anywhere...

• Needed to understand attacks.
  – Are we even attacked???

• Need to understand differences
  – Security event
  – Engineering event
  – Hardware event
  – Etc.

• Educated response leads to decreased risk

• CRITICAL INFRASTRUCTURE!!!
“Traditional” Incident Response

- Preparation
- Detection & Analysis
- Containment Eradication & Recovery
- Post-Incident Activity
ICS/SCADA Incident Response

- Must include forensics
- Must be dynamic enough to diversify
- Must have SME’s
- Must follow documented process
- Must have a wide range of expertise
- Must utilize threat intelligence
ICS INCIDENT RESPONSE APPROACHES
Asset Identification

• Identify all assets deemed “ICS”
• Perform criticality assessment
• Logically map all equipment
• Map connectivity points to LAN/WAN segments
• Identify make, model, and manufacturer or ICS equipment
Pro-Active Identification

- Honeypots
- IDS (Not IPS in active mode!)
  - Must be placed parallel to other ICS equipment
- IOC’s
- Threat Intelligence (HUMINT, SIGINT)
- Offensive Incident Response
- Network Segmentation
Incident Identification/Investigation

• Identify Incident
  – Engineering mistake?
  – Security Incident?
  – Hardware Incident?

• In the ICS world- take off network (Likely)

• Primary business priority- get back online
Threat-Actor Identification

• Why care? Especially during incident.
• Helps look for parallel attackers
• Can help planning of offensive IR (Offensive countermeasures)
• Use OSINT!!!
OSINT Case Study
Containment

• Typical Containment Methods:
  – Firewalls
  – IPS/IDS
  – Take device off net
  – ACL’s
  – Bastion hosts
  – Whitelisting
  – IOC development
  – Increased logging
  – Sniffer deployment

The list goes on…
ICS Forensics

- Done to understand incident on micro level
- Will allow classification of future “events”
Recommendations

• Implement forensics and incident response into ICS environments

• Have SME’s for threat intelligence, malware, incident response, and forensics

• Have pro-active protections in place

• Utilize logging!!!

• Take devices off the Internet

• Utilize network segmentation
Thanks!

kylewilhoit@gmail.com
Kyle_wilhoit@trendmicro.com
@lowcalspam