ATTACKS ON ICS

Ludwig Seitz
(inspired by a course by Justin Searle)
June 2018

RISE ICT
SICS
Control Systems

ICS/SCADA infrastructure -> Controller -> Sensor

Controller -> Actuator
ICS / SCADA

- Industrial Control System
  - General term
  - Systems controlling industrial production

- Supervisory Control And Data Acquisition
  - Hierarchical, distributed architecture
  - High-level management
  - Typically event-driven
  - Focused on data collection

[Image: Wikimedia Commons: Sunilshamnur]
- Digital Control System
  - Controls single factory or plant
  - Process-driven
  - Focused on control
• Programmable Logic Controller
  – Generic, programmable for any purpose
  – Usually runs a real-time operating system
RTU

- Remote Terminal Unit
  - Network gateway
  - Generally used to communicate with multiple field devices such as PLCs
• Human-Machine Interface
  – Used by the operators to observe and interact with a controlled process
  – Range from simple displays with buttons to PCs running advanced control software
Data Historian

- Centralized data repository
  - Collects time-stamped data
  - Input from controllers, HMIs etc.
  - Used for data analysis
  - Main reason why Business IT and Process IT cannot be fully air-gapped
ICS architecture

- Internet DMZ
  - Web Server
  - Mail Server

- Enterprise Level
  - Business Systems
  - Desktop PCs

- Supervisory Level
  - Historian
  - Main HMI
  - Engineering Workstation

- Field Level
  - HMI
  - RTU
  - PLC
Attacking ICS

- Usually starts with classical attacks
  - Social engineering
  - Flaws in the company IT security
  - Insider
- Use the foothold to propagate
  - Move from office IT to operation IT
    → e.g. the through the historian
- ICS part requires deep specialist knowledge
ICS Attack Targets

- Engineering stations
  - Project files (Human readable variable names)
- HMI
  - Fool the operator to think all is fine
- Gateways
  - Intercept and manipulate control traffic
Attack Methodology

• Gather information
  – Public sources (website, news, social media)
  – Scanning and monitoring (nmap, wireshark)

• Analysis
  – Learn how the process works
  – Learn different entities in the system

• Exploit
  – Use the results to gain a foothold
  – Pivot to new subsystems
  – Cover your tracks
No free lunch!

- Delivering a targeted ICS attack is hard!
  - ICS has many safety features
  - Operators good at recognizing abnormal states
  - ICS equipment is fragile
    → Attackers need intimate knowledge of the process to avoid detection

- ICS attack tools show a high level of sophistication
  - Havex malware scans for OPC resources
  - Triton malware targeting system for critical control & safety
Case Study: Havex

1. Attack

2. Software updates + Havex

3. Data exfiltration

4. ???

SCADA system manufacturer

"Waterhole"

Dragonfly

Command & Control Server

Internet

SCADA systems
Case Study: Havex

- Dragonfly: Russian hacker group
- Havex: Remote Access Trojan (RAT)
  - Targets ICS/SCADA systems
  - Communicates with a Command & Control Server
  - Scans for connected network resources using OPC standard
- “Waterhole” attack (2013)
  - Hackers attacked ICS/SCADA manufacturers
  - Customers got infected software updates
- >1000 European / North American energy firms infected
TACK!

Ludwig Seitz
ludwig.seitz@ri.se
+46 703 49 9251

RESEARCH Institutes of Sweden
RISE ICT
SICS
Links

• Homeland Security ICS-CERT
  - https://ics-cert.us-cert.gov/Recommended-Practices
  - https://ics-cert.us-cert.gov/monitors

• MSB
  - https://www.msb.se/ics
  - https://www.cert.se/

• Justin Searle
  - https://www.samuraistfu.org