Out of Control: Ransomware in Industrial Control Systems

David Formby
PhD Candidate, Georgia Institute of Technology
www.ece.gatech.edu/cap

CEO/CTO, Fortiphyd Logic
www.fortiphyd.com
Putting on the Black Hat

- Most malware authors and attackers are in it for the money
- Ransomware is the hot new business model
  - $209 Million profit in Q1 2016  
    - Source: CNN, “Cyber-extortion losses skyrocket, says FBI”
- High profile ransomware attacks
  - San Francisco’s light rail system
  - Hospitals
- Where might an enterprising young hacker attack next?
Brief History of Ransomware

- **Locker Ransomware**
  - Renew software license
  - Fake AV
  - FBI threats
  - Awareness and security tools decreased effectiveness

- **Crypto Ransomware**
  - No false pretense, clear extortion
  - No easy recovery

Symantec Whitepaper “The Evolution of Ransomware”
Brief History of Ransomware

Booz Allen Industrial Cybersecurity Threat

Holding the HMI Hostage—The Growing Threat of Ransomware
By Del Rodillas
06/07/2016 Palo Alto Networks

Move over Healthcare, Ransomware Has Manufacturing In Its Sights


Europe

Hackers Use New Tactic at Austrian Hotel: Locking the Doors
By DAN BILEFSKY JAN. 30, 2017

Ransomware locks up San Francisco transportation ticket machines
now restored; attacker demanded $73,000.
The Ransomware Races
Overview of Industrial Control Systems

- Internet
- Web Server
- Email
- Business Workstations
- Corporate Network
- PLCs, controllers
- Historian
- Engineering Station
- HMI
- Control Network
- Physical Plant
ICS Security

- Most protocols have no message authentication
  - Accept any command injected on the network

- Most PLC programming interfaces lack solid password authentication
  - Nonexistent
  - Misleading
  - Poor protection against brute forcing

- Rely on fallacies
  - Security through obscurity
  - “Airgaps”
What Makes a Ransomware Attack Successful?

Hospitals

- Easier targets
  - Old equipment
  - Traditionally weak security posture
- Increasing time pressure
- Lives at stake
- Crown jewels = patient data

ICS Networks

- Easier targets
  - Old equipment
  - Traditionally weak security posture
- Increasing time pressure
- Lives at stake
- Crown jewels = safe operation
# Market Size Analysis

## Businesses Hit by Ransomware
- 70% paid the ransom
- Median payout approx. $10k
- Small, medium sized businesses less prepared

Source: IBM, “Ransomware: How consumers and businesses value their data”

## PLCs on the Internet
- MicroLogix 1400
  - 1,300
- Schneider Modicon M221
  - 200

\[
1,500 \times \$10,000 \times 50\% = \$7.5 \text{ Million}
\]

Trivial PLCs  Expected payout  Conservative success rate
Attack
Typically mixed with chlorine to kill bacteria

We use iodine because it’s safer to handle and cooler looking

Testbed simulates the Disinfection and Storage stages

Source: CDC, “Water Treatment”
Recon

Search engine for connected ICS devices
Common protocol, Modbus

Over 13,000 results

Plenty of choices to choose from, just pick one
Initial Foothold

- Schneider Modicon M241
  - Running CODESYS V3
  - Third party PLC runtime environment used by over 200 vendors
  - Password
    - No brute force checks
    - No strength policy
  - Controlling the water input and monitoring the storage levels
Reprogram the M241 to scan the internal network and grab model numbers

- Allen Bradley MicroLogix 1400
- Modicon M221
Internal Network Scan

Allen Bradley MicroLogix 1400
- Password only checked in engineering software, **NOT** the PLC
- SMTP mail client
- Controlling the addition of chlorine (iodine)

Schneider Modicon M221
- Password only checked in engineering software, **NOT** the PLC
- Controlling the final output of treated water
Actual Network

**Allow:**
- External to A
- Internal to Internal

Water from previous stage

Storage Tank

Water used by customers

Monitor levels, input

Mix with chlorine

Pump output
Actual Network

Input water valve

Mixing valve to control ratio of water/iodine

Level sensors

Programmable logic controllers

Output water valve
How Can We Maximize Success Rate

- Pick targets with high downtime costs
- Understand the process behind the PLCs
- Threaten to screw things up if they don’t meet deadline
  - What if they just unplug everything?
- Covertly move system into critical state **before** notifying them
  - Allow reserve storage tank to get low first, blinding operators
  - Make continued operation by attacker more attractive than shutting everything down
Water Treatment Testbed

https://youtu.be/KTKRjvTgTQI
Attack

https://youtu.be/t4u3nJDXwes
Discussion
Apply: Lessons Learned

- ICS networks and devices are STILL very vulnerable
  - Poor/nonexistent password protection
  - Vendors slow to fix obvious problems
  - A lot of exposed devices on the Internet

- Ransomware trend is likely to jump to ICS
  - Early signs attacking corporate networks of ICS
  - Easy targets
  - Money and lives at stake
Apply: Defenses

- Know your network
  - Devices, remote vendor connections

- Security assessment
  - Firewall rules, segmented network, proper remote access
  - Passwords

- Monitor at the ICS level
  - Communication patterns
  - PLC programming events

- Pressure vendors to build more security into their products
Thank You!

David Formby
www.cap.gatech.edu
djformby@gatech.edu
@gtcapgroup @davidjf12

Fortiphyd Logic
www.fortiphyd.com
info@fortiphyd.com
@fortiphyd