ICS – Industrial Cyber Scanning, The hidden world of industrial components

Itay Bochner
CYBER Israel - Timeline

2002
NISA

2011
INCB

2016
NCSA

2018
INCD
ICS in a nutshell

- **ICS - Industrial Control System**
  - An automation control system that is used in energy, oil and gas, water, power, etc.
  - Control industrial processes locally or at remote locations
  - Monitor, gather, and process real-time data
  - Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software
## ICS in a nutshell

- **Main components**
  - SCADA – Supervisory Control And Data Acquisition
  - DCS – Distributed Control System
  - PLC - Programmable Logic Controller
  - RTU – Remote Terminal Unit
  - HMI – Human Machine Interface
  - ES – Engineering station
ICS in a nutshell

- How PLC works
  - Cyclic Polling
    - Input – sensors
    - Output - actuators
  - Close to real time ~ 40ms/cycle
  - Embedded logic
    - Ladder diagram
    - Function blocks
  - Process vs. management communication
  - Proprietary protocols and software
    - Modbus/TCP
    - Modbus/RTU
    - S7
    - GESRTP
    - ProfiBus
    - Profinet
    - EtherNet/IP
Attack landscape

- Attacker skills and toolkits
- Attack purpose
  - Immediate vs. overtime damage
  - Physical or disinformation campaign
- How many targets?
  - 1 major target
  - Critical mass

Kali Linux
• Known attacks
• The problem?
  • Exposed devices
  • Opportunistic attackers
  • Distributed attack
• Risk management
  • CI – Critical Infrastructure
  • Big & Small/Medium industrial facilities
  • Cyber Resilience prioritization
  • Influential campaign

National concern

DOS

NY Dam, 2013

DDOS

Industroyer, 2016

Stuxnet, 2011

DDOS

Triton, 2017

Complexity vs. Impact
Needle in a haystack

- Queries & parsing
  - Mix & match
  - Telltale signs
  - Validity of the scan
  - Legacy components

- Challenges of scanning
  - PLCs attribution
  - Scan parameters?
  - Vendor variance
  - Legal limitation
  - No benchmark for scanning
Raising up the guards

• Day2day cyber resilience
  • Remote connections
  • Awareness
  • Supply chain
  • DRP

Thanks you...

ityb@cyber.gov.il