ICS Down! ... It’s Go Time

Jason Dely
Practice Director, ICS and Critical Infrastructure
ICS DISRUPTORS - 2017

WannaCry
NotPetya
CrashOverride
Triton/Trisis
RESPONSE

Pay Ransom

Containment

Mass Remediation to all Systems

Mass Patch Roll-out to all Systems

Restore Infected Machines from Backups
ICS IR Response

- Farther System Impact
- Extended Time to Recovery
  - Reduced Trust

Safety / Public Trust / $$$

DETECT and DEFLECT => ? CHOICE ? <= BLOCK and TACKLE
ICS INCIDENT DISCOVERY AND TRIAGE

- Do you have established relationships with contacts into each business unit?
- Do you have an existing escalation and communication structure?
- Are you able to measure actual impact and execute existing contingencies?
Do you have established and trusted data sources?
- IDS, Firewall, Syslogs, SCCM Logs, DNS Logs, etc.
- Accurate time source

Do you have established metrics in place?
- Usable for current mission
- Scalable for the environment
- Accessible to those that require it
ICS PATCHING / REMEDIATION / RECONFIGURATION

- Do you have IT tools and capabilities (PPT) in place?
  - Has these tools ever been performed in your ICS?
  - Validation and testing processes
- Do you truly know what is in your environment?
  - Knowledge of all business units assets across all networks
  - Knowledge of all networks?
  - Accurate list of all assets, systems (Inc. OS types, manufactures, etc.)
  - Understanding of uptime and availability requirements
  - Understanding of critical dependencies, communication paths and data flows
- Does the ICS perimeter operate as a router or a sentry?
ICS BACKUP AND RESTORE

- Do you have backups?
  - Current and available
  - Validated with tested procedures
- Do you understand what restoring to ’normal’ operations entails?
  - Critical systems/communications in operation
  - Order of system startup
  - Associated assets and data
During an incident is a **BAD** time to build a response!
WHY?

Ooooooh

SHINY!!!!!
ICS FACTS

- ICS contain multiple systems
- Every interaction is engineered
- Every system has various levels of criticality
- Each system is unique (PPT)
- Attack != BOOM
  - … well, depends on definition of boom
IT TAKES THREE TO PLAY

SECURITY

IT

OPERATIONS
PERCEPTION AND RESPONSE

Operation Related Issues

vs

Attacker Related Concerns

THINK LIKE THE OPERATOR & ADVERSARY
THREAT ACTORS

Intent

Foreign Intel Services
Military / Funded Teams
Traditional Cyber Criminals
Low Level/Script Kiddies

Capability

Intelligence
Active Defense
Passive Defense
Architecture
Weak Security
Design for Response!
KNOWLEDGE GAIN

- Drawing and Documentation
- Asset Inventory
- Configuration Reviews
  - ICS and Network Devices
- Communications and Data Flows
- Vulnerability Assessments
- Critical Assets and Bad Day
NIST CYBERSECURITY FRAMEWORK

IDENTIFY
- Truly know all environments

PROTECT
- Implement and maintain effective safeguards

DETECT
- Monitor safeguards in all environments

RESPOND
- Responsibly act on events

RECOVER
- Restore services impaired by events
ATTACK PATHS

Identify initial attack vectors to ICS
Identify plausible attacks to ICS

Traditional computing devices will be involved
Document unfixed vulnerabilities (i.e. Legacy)
Identify manipulation and containment capabilities

C2 Channels
ATTACK PATHS = BUSINESS NEEDS?

Architecture
1. Flat; everything can reach everything
   Prevention
1. Minimal; everything trusts everything
   Monitoring
1. Inadequate; advanced threats will win
   Response
1. Extremely difficult; failure is likely

Internet

Office Network
- Remotes
  - Reservoirs
  - Distribution
  - Etc.
- Phishing
- Weak Communication Protection

Firewall

Third Party
- Sub-Systems
  - Power
  - Generation
  - Etc.
- Rogue Internet & USB
- Weak Access Control
- Firmware
- Legacy Unmanaged
- Third Party Reservoirs

Processing
- Flocculation
- Filtration
- Chlorination
- Etc.
- Processing Distribution
- Processing Chlorination

Operations
- Control Room
- Workstations
- Servers
- Etc.
- Operations Control Room
- Operations Workstations
- Operations Servers

ISA95 PURDUE REFERENCE MODEL

Enterprise Zone
- Enterprise Network (Level 5)
- Site Business Planning and Logistics Network (Level 4)

Demilitarized Zone

Manufacturing Zone
- Site Manufacturing Operations and Control (Level 3)
- Area Supervisory Control (Level 2)
- Basic Control (Level 1)
- Process (Level 0)

Cell/Area Zone

Safety Zone
- Safety-Critical
VALUE OF TARGETS

Value to the Business

vs

Value to the Threat

DO THEY ALIGN
TOOLS

Triage – Passive and non invasive
Forensics Gathering – Will likely disrupt ICS
Test and validate in lab
Involve operations staff for approval
TECHNIQUES

Initial triage to narrow initial scope
Identify level of severity
ICS vs non-ICS related attack concerns
Manipulation, Recovery or Forensics?
PROCEDURES

Allow continued, safe operation

Isolation of ICS

Isolation of Critical Assets

Engage Response to the Threat
RECOVERY

More then just rebuilding...

Reinstate integrity and confidence within operations
POSITIVE TAKE AWAY

Prepared for an ICS Incident

Good ICS Security Hygiene

Attacks will stand out, IF engineered to stand out
QUESTIONS
AND
ANSWERS
CylancePROTECT leverages the power of machines, not humans, to dissect malware’s DNA. Artificial intelligence then determines if the code is safe to run.
BREAK THE KILL CHAIN

- **MEMORY PROTECTION**
  - MEMORY EXPLOITS
  - MALICIOUS SCRIPTS
  - MALICIOUS MACROS

- **FILE SYSTEM**
  - WATCH FOR NEW FILES
  - BACKGROUND THREAT DETECTION

- **EXECUTION CONTROL**
  - MONITOR PROCESS EXECUTION
  - MONITOR LIBRARY LOADS
  - BLOCK MALWARE PRE-EXECUTION
  - APPLICATION CONTROL
Risk Mitigation Cost

- **RESPOND**
  - **RISK**
    - **Lowest Risk**
      - **Lowest Cost**
      - **Limited Liability**
    - **Highest Risk**
      - **Highest Cost**
      - **Most Liability**
  - Focus is on minimizing damage – only variables are time to detect and time to contain.
- **DETECT**
  - **Control**
    - **Friction**
- **PREVENT**
  - **Control Approaches**
    - **Automated**
    - **Semi-Automated**
    - **Manual**
  - Focus is on minimizing vulnerability and potential for harm.

THANK YOU