ICS Threat Intelligence and Active Defense

Robert M. Lee
Twitter: @RobertMLee
Email: rlee@dragos.com
Web: www.dragos.com
Agenda

• ICS Threat Intelligence
• Case-Studies: ICS Activity Groups
• ICS Active Defense
• The Four Types of Detection
ICS Threat Intelligence

@_LittleBobby_
www.LittleBobbyComic.com
Fact: No ICS were harmed in the making of this “report”
2008 Turkey Pipeline Explosion
Bloomberg published “Mysterious ‘08 Turkey Pipeline Blast Opened New Cyberwar” in December, 2014

Fact: BTC Pipeline was attacked
Reality: No “cyber” involved
10-hour Power Failure reported by Bloomberg, CNN, and major media outlets as possible Iranian Cyber Attack

Fact: Aging infrastructure caused outage
Reality: “Cyber” linked through previous reports
Israeli Power Grid Suffers Massive Cyber Attack
Overarching Problem

Few People Know How to Protect the ICS that Run Our World

And the Threat Landscape is Mostly Unknown
The Three Pillars of Security

Know Thyself

Know The Adversary

Know What to Do
Intelligence’s Purpose

1. Know Thyself
2. Know The Adversary
3. Know What to Do
The Intelligence Lifecycle

Relationship of Data, Information, and Intelligence

Operational Environment | Data | Information | Intelligence
Collection | Processing and Exploitation | Analysis and Production
What is a Threat?

• Organizations must know what their threats are to accurately collect and use threat intelligence

• Threats can be established by evaluating Capability + Intent + Opportunity
Threat Modeling and Intelligence Requirements

Acme Power

- Website Availability
- Employee PII
- Financial Data
- R&D / Intellectual Property
- HMI
- Data Historians
- Final Control Elements

- Hacktivists
- Financially Motivated Actors
- Espionage

- SANDWORM
  - Black Energy
  - SCADA Hijack

- ELECTRUM
  - CRASH OVERRIDE
  - SCADA Hijack

- DRAGONFLY
  - HAVEX
  - Trojanized ICS Software
# Build a Collection Management Framework

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Endpoint Protection System</th>
<th>Windows Systems</th>
<th>Network</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kill Chain Coverage</td>
<td>Exploitation &amp; Installation</td>
<td>Exploitation, Installation, and Actions on Objectives</td>
<td>Internal Reconnaissance, Delivery, and C2</td>
<td>Internal Reconnaissance, Deliver, and C2</td>
</tr>
<tr>
<td>Follow on Collection</td>
<td>Malware sample</td>
<td>Files and timelines</td>
<td>Packet Capture</td>
<td>Netflow</td>
</tr>
<tr>
<td>Typical Storage in Days</td>
<td>30 days</td>
<td>60 days</td>
<td>23 days</td>
<td>60 days</td>
</tr>
</tbody>
</table>
The Four Paths to Attribution

- Adversary Admission
- Leaks
- Direct Access
- Intrusion Analysis

True Attribution
Adversary Intent vs. Perceived Intent

• Early 2017 WannaCry ransomware worm infected 300k+ computers
• The National Security Agency (NSA) assessed that the adversary behind WannaCry was North Korea
  • Many in the community supported this with their own analysis
• Despite the attribution (right or wrong) questions formed
  • Why did North Korea do this?
  • Would North Korea do this?
  • What was their intention?
• Focus on perceived intent do not pretend we can know it
What Intelligence Should Provide

How do I reduce dwell time of the adversary? (Detection/Remediation)

What do I need to focus on to reduce risk? (Vulnerabilities, news, hype, adversaries, etc.)

Do my investments match my threat landscape and requirements?
Case Studies: ICS Activity Groups

**LITTLE BOBBY**

AND ALL OF THIS ELECTRIC GRID IS YOURS TO SECURE LITTLE BOBBY!

WHAT IS THAT DARK SPOT THERE?

**ELECTRICIAN**

THAT IS THE DC BUBBLE!

YOU MUST PROMISE TO NEVER GO THERE!

**LITTLE BOBBY**

THEY BELIEVE THE POWER GRID IS ON THE VERGE OF CRASHING AND THAT MEETINGS WILL KEEP IT RUNNING.

by Robert M. Lee and Jeff Haas

DRAGOS
The Making of an Activity Group

- Group
  - Campaign 1
    - Victim Organization
    - Intrusion Analysis
  - Campaign 2
    - Victim Organization
    - Intrusion Analysis
  - Campaign 3
    - Victim Organization
    - Intrusion Analysis
The Diamond Model

Adversary

Infrastructure

Capability/TTPs

Victim
ELECTRUM

- Dual-use infrastructure such as TOR to host C2
- Internal proxies setup
- Ukrainian Utility Companies
  - Electric
  - Water
- Long term access to ICS
- CRASHOVERRIDE
- ICS Specific Modules
- Operations Knowledge

Links: Development team for Sandworm
DYMALLOY

- Compromise ISP IPs
- Compromised business connections for initial infection and subsequent implants

Multi-State Adversary Interests

- North American electric operators
- Turkish energy providers
- Western Europe electric operators

- Malicious docs w/ credential harvesting via external SMB connections
- RATs from publicly available toolkits
- Custom-developed information theft toolkits built on public tools
- One non-public toolkit

Links: Dragonfly 2.0
Not Dragonfly 1.0
CHRYSENE

- Arabian gulf region
- Saudi Arabia petrochemical focus
- Oil/gas, petro, and electric generation

Iranian State Interests

- Actor owned infrastructure
- Domain patterns after legitimate resources
- Custom DNS server as authoritative for the domain to enable C2

- 64-bit malware using DNS for C2
- Greenbug malware with HTTP C2
- OilRig as evolution of Greenbug
- Unique DNS C2 system
  - Initial beacon AAAA request
  - IPv6 encoded commands

Links: “OilRig” Actor
MAGNALIUM

- Spoofed domains of relevance to victim
- Dynamic DNS for C2
- IT services and aerospace themed

Iranian State Interests

- Commodity and non-public malware combination
- Publicly available crimeware
- Specific malware encoding routine

- Saudi Arabian petrochemical
- Aerospace companies
- North America and South Korean targets only with Saudi business

Links: APT 33
COVELLITE

- Sophisticated implant with secure communication channels
- Similar features to malware used against South Korean targets
- Specific session key used for payload and second encrypted layer
- 41 minute and 30 second sleep

Legitimate infrastructure
- University IPs for C2

Electric utility companies in the United States

North Korean State Interests

Links: Unknown
ICS Active Defense

LITTLE BOBBY
WHAT ARE YOU DOING?
INSTALLING NEXT-GEN SOFTWARE TO PROTECT ME AGAINST FOREIGN GOVERNMENTS.

WHY IS THERE A POPUP SAYING YOU STILL NEED TO PATCH YOUR SYSTEM?

I'LL GET TO THAT LATER.

by Robert M. Lee and Jeff Haas
The Sliding Scale of Cyber Security

Ref: https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240
Understand Adversary Intrusions

Stage 1 mimics a targeted and structured attack campaign.

Based on the Cyber Kill Chain® model from Lockheed Martin
Stage 2 shows the steps associated with a material attack that requires high confidence.
Understand Your Data and What Questions You Can Ask Of It

<table>
<thead>
<tr>
<th>Common Data Sources in ICS Environments and Relative Ease to Gather</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netflows (IPFIX, Sflow, AppFlow, etc.)</td>
</tr>
<tr>
<td>Network traffic (pcap)</td>
</tr>
<tr>
<td>Process controller logs (syslog)</td>
</tr>
<tr>
<td>Process/Data Historian</td>
</tr>
<tr>
<td>Host based logs (Windows and Linux supervisory systems)</td>
</tr>
<tr>
<td>ICS Software Events and Alarms</td>
</tr>
<tr>
<td>Specialized Equipment logs (e.g. digital relay logs, CCTV, physical security systems, etc.)</td>
</tr>
</tbody>
</table>
Hypothesis Generation

Friendly or Threat Intelligence

Situational Awareness

Domain Expertise

Ref: https://www.sans.org/reading-room/whitepapers/threats/generating-hypotheses-successful-threat-hunting-37172
Sample Hypotheses for ICS Environments

- Malware will initiate internet checks
- Malicious updates and patches will occur out of cycle
- An adversary in the network will exfil process historian data
- Adversaries will gravitate towards HMIs
- Targeted threat groups will steal engineering documents
The Four Types of Detection

LITTLE BOBBY

I NEED YOU TO ENSURE NO ATTACKS OCCUR.

OKAY--WHAT'S THE SECURITY BUDGET?

OH, WE HAD TO CUT IT ALL.

I ASSURE YOU WE WILL NEVER SEE ANY ATTACKS.

by Robert M. Lee and Jeff Haas
Problems Today

- Failure to generate good requirements
- Alert fatigue
- Language confusion (anomaly vs. analytics)
- Marketing driving the narrative
- Environmental vs. Threat based approaches
# The Four Methods to Detect Threats

<table>
<thead>
<tr>
<th>Environment</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Unknowns**

**Knowns**

- Configuration Analysis
The Four Methods to Detect Threats

<table>
<thead>
<tr>
<th>Environment</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistical Modeling</td>
<td></td>
</tr>
<tr>
<td>Configuration Analysis</td>
<td></td>
</tr>
</tbody>
</table>

Unknowns

Knowns
# The Four Methods to Detect Threats

<table>
<thead>
<tr>
<th>Environment</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknowns</td>
<td></td>
</tr>
<tr>
<td>Statistical Modeling</td>
<td></td>
</tr>
<tr>
<td>Knowns</td>
<td></td>
</tr>
<tr>
<td>Configuration Analysis</td>
<td>Indicators</td>
</tr>
</tbody>
</table>
## The Four Methods to Detect Threats

<table>
<thead>
<tr>
<th>Environment</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistical Modeling</td>
<td>Behavioral Analytics</td>
</tr>
<tr>
<td>Configuration Analysis</td>
<td>Indicators</td>
</tr>
</tbody>
</table>

- **Unknowns**
  - Statistical Modeling
  - Behavioral Analytics
- **Knowns**
  - Configuration Analysis
  - Indicators
# The Four Methods to Detect Threats

<table>
<thead>
<tr>
<th>Environment</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unknowns</strong></td>
<td></td>
</tr>
<tr>
<td>Statistical Modeling</td>
<td>Behavioral Analytics</td>
</tr>
<tr>
<td><strong>Knowns</strong></td>
<td></td>
</tr>
<tr>
<td>Configuration Analysis</td>
<td>Indicators</td>
</tr>
</tbody>
</table>

Requires Deep System Knowledge (DPI, Vendors Specifics, etc.)
The Four Methods to Detect Threats

<table>
<thead>
<tr>
<th>Environment</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknowns</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Statistical Modeling</td>
</tr>
<tr>
<td>Knowns</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration Analysis</td>
</tr>
</tbody>
</table>

Requires Deep Threat Knowledge (Incident Response, Intrusion Analysis, etc.)
Recommendations Moving Forward

Active Defense is Required
- Target rich environments demand an active approach
- Defensible networks make hunting extremely viable

Intelligence to Guide Efforts
- Prioritize efforts and understand *your* threat landscape with intelligence
- Threat intel isn’t threat feeds, pew-pew maps, or vendor marketing

Threat vs. Environmental
- Understand the difference in value in threat vs. environmental approaches
- Identify adversary behaviors specific to industrial environments
LITTLE BOBBY

WE SHOULD COLLECT AND ANALYZE THE ICS SERIAL TRAFFIC FOR APTS.

HAVE YOU ALREADY DONE ANALYSIS OF THE OT SYSTEMS?

NO!

START WITH THE MOST LIKELY TARGETED SYSTEMS—LIKE THE HMI OR REMOTE VPN CLIENT.

by Robert M. Lee and Jeff Haas

Questions?

Robert M. Lee
Twitter: @RobertMLee
Email: rlee@dragos.com
Web: www.dragos.com