TTPs for Threat Hunting in Refineries

Dan Gunter | Twitter: @dan_gunter
Principal Threat Analyst @ Dragos
October 2018
Talk Overview

• Start theoretical, end applied
• What to do?
• How to do it?
• Useful Open Source Tools
Threat Hunt Model

- Proactive
- Behavioral & IOC Driven
- Prevention & Detection
  - Leads to Response
- Not Red Teaming Data
- Key Players:
  - Operations
  - OT/IT
  - Engineers
Threat Hunt Model

- Purpose
- Goals
- Outcomes
Threat Hunt Model

• Phase 1: Location
• Phase 2: Hypothesis Generation
Threat Hunt Model

- Phase 1: Collection Management Framework (CMF)
- Phase 2: Resource Allocation
Threat Hunt Model

- Viability
- Fit to Purpose
- Scope modifications
Threat Hunt Model

- Carry out Hunt
- Additional Hypotheses
- Generate Report
Threat Hunt Model

- Feedback
  - Automation where possible
  - Objectives met?
  - Discussion with stakeholders
Applied Threat Hunting
Purpose

- Protect critical parts of refining
- Gain visibility and understanding
- Chose to focus on desalination
  - Focus varies by engagement
Scope: Phase 1

- Desalination Process
- ABB Freelance DCS
  - Freelance Operation Center
  - All Controllers communicating with Caustic Solution Dosing DM Water, and Crude Oil pumps
    - Profibus, Modbus (RTU and TCP)
ABB: Freelance DCS

- Modernized Control System
- Variety of implementations
- Integrations with many other applications
- Hundreds of IOs and field devices
- Controllers:
  - AC 700F, AC 800F, AC 900F
  - Remote IO: S700, S800, S900
- Freelance Operations
- Freelance Engineering
Scope: Phase 2: Hypotheses

- Hypotheses
  - Attackers are leveraging Freelance Operation Center login information to do reconnaissance on pump functions in desalination process.
  - Attackers also are using vendor access
  - Attackers are leveraging web shells to maintain access
  - Attackers are sending malicious commands to AC 900F, AC 700F, and AC 800F controllers to manipulate pumps associated with desalination process.
    - Might be too late if you see ^
    - Worth analyzing defenses still
Equip: Phase 1: Collection Management Framework

- Freelance Operations center
  - Asset Management
  - Process information
  - User logging + Timestamps
  - System Changes

- Freelance Engineering
  - Database
  - Project configurations

- Network Traffic to Controllers
- Historian Assets
## Collection Management Framework

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Desalination Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Logs</td>
<td>2 Days</td>
</tr>
<tr>
<td>Freelance Operations Windows Event Logs</td>
<td>30 Days</td>
</tr>
<tr>
<td>FreeLance Engineering Windows Event Logs</td>
<td>30 Days</td>
</tr>
<tr>
<td>Full Network Capture</td>
<td>7 Days</td>
</tr>
<tr>
<td>Process Historian Windows Event Logs</td>
<td>60 Days</td>
</tr>
<tr>
<td>Controllers</td>
<td>None Available</td>
</tr>
</tbody>
</table>
Equip: Phase 2: Resource Allocation

- Team members
  - Senior & Junior
  - IT & OT
- Tools
  - Approved
  - Custom vs General
- Time
  - Dev
  - Execution
Plan Review

- Stakeholder awareness
- Potential issues with achieving purpose success
- Any alterations
Execute

- Use hypotheses to structure hunts with relevant data sources
- Discussions with Subject Matter Experts on what is “normal”
- Hunt to find what does not fit the expected normal
- Observables of known adversary behavior
Composite Events Are More Powerful than Atomic Indicators
What is behavioral data?

• A chain of events rooted in observables with high confidence in activity

- VPN connection established to network
- RDP session to Historian machine
- Malicious download executes code
- Data exfiltration to external source

• Tactics, Techniques, and Procedures of attacker activity
• Rooted in observable evidence in network and host
• Abstracted from too specific information to what can be shared
What does a malicious vendor or physical attack look like?
Behavioral Tracking of Malicious Access & Devices

New Device Appears

Social Media Tracking Cookies

NMAP Scan

Transient Device Disappears Hour Later

Finding NMAP: https://dragos.com/blog/20171121ThreatHuntingWithPythonPt2.html
How Does A Web Shell Behave?
Web Shell Behavior

- Web Server File Modification
- New URIs and User Agents
- Host Log Activity
- New HTTP Traffic Patters
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>AppleScript</td>
<td>bash_profile and bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>AppleScript</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>CMSTP</td>
<td>Command-Line Interface</td>
<td>Accessibility Features</td>
<td>BITS Jobs</td>
<td>Brute Force</td>
<td>Application Discovery</td>
<td>Application</td>
<td>Automated Collection</td>
<td>Data Compressed</td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Command-Line Interface</td>
<td>AppCert DLLs</td>
<td>Accessibility Features</td>
<td>Binary Padding</td>
<td>Credential Dumping</td>
<td>Deployment Software</td>
<td>Deployment</td>
<td>Data Staged</td>
<td>Data Encrypted</td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Dynamic Data Exchange</td>
<td>AppCert DLLs</td>
<td>Bypass User Account Control</td>
<td>Clear Command History</td>
<td>Credentials in Files</td>
<td>Distributed Component Object Model</td>
<td>Distributed</td>
<td>Data Transfer Size Limits</td>
<td></td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>Execution through API</td>
<td>DLL Search Order Hijacking</td>
<td>Component Firmware</td>
<td>Component Object Hijacking</td>
<td>Forcing Authentication</td>
<td>Forcing Access</td>
<td>Forcing</td>
<td>Data from Information Repositories</td>
<td></td>
</tr>
<tr>
<td>Spearphishing Link</td>
<td>Execution through Module Load</td>
<td>DLL Search Order Hijacking</td>
<td>Forcing</td>
<td>Control Panel Hijacking</td>
<td>Exploitation for Credential Access</td>
<td>Network Service Discovery</td>
<td>Network</td>
<td>Data from Network</td>
<td>Exfiltration Over Alternate Protocol</td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>Change Default File Execution</td>
<td>DCShadow</td>
<td>Network</td>
<td>Keychain</td>
<td>Keychain</td>
<td>Password Policy Discovery</td>
<td>Password Policy</td>
<td>Data from Removable Media</td>
<td>Exfiltration Over Other Network Media</td>
</tr>
<tr>
<td>Trusted Relationship</td>
<td>Graphical User Interface</td>
<td>LLNM/IPS/NS</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process</td>
<td>Data from Network</td>
<td>Exfiltration Over Physical Medium</td>
</tr>
<tr>
<td>Valid Accounts</td>
<td>InstallUtil</td>
<td>DLL Search Order Hijacking</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process</td>
<td>Data from Network</td>
<td>Exfiltration Over Physical Medium</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td>DLL Search Order Hijacking</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process</td>
<td>Data from Network</td>
<td>Exfiltration Over Physical Medium</td>
</tr>
<tr>
<td></td>
<td>Start</td>
<td>DLL Search Order Hijacking</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process</td>
<td>Data from Network</td>
<td>Exfiltration Over Physical Medium</td>
</tr>
<tr>
<td></td>
<td>Local Job Scheduling</td>
<td>DLL Search Order Hijacking</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process</td>
<td>Data from Network</td>
<td>Exfiltration Over Physical Medium</td>
</tr>
<tr>
<td></td>
<td>Malware</td>
<td>DLL Search Order Hijacking</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process</td>
<td>Data from Network</td>
<td>Exfiltration Over Physical Medium</td>
</tr>
<tr>
<td></td>
<td>PowerShell</td>
<td>DLL Search Order Hijacking</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process</td>
<td>Data from Network</td>
<td>Exfiltration Over Physical Medium</td>
</tr>
<tr>
<td></td>
<td>Regsvr32</td>
<td>DLL Search Order Hijacking</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process</td>
<td>Data from Network</td>
<td>Exfiltration Over Physical Medium</td>
</tr>
<tr>
<td></td>
<td>Scheduled Task</td>
<td>DLL Search Order Hijacking</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process</td>
<td>Data from Network</td>
<td>Exfiltration Over Physical Medium</td>
</tr>
<tr>
<td></td>
<td>Scripting</td>
<td>DLL Search Order Hijacking</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process Discovery</td>
<td>Process</td>
<td>Data from Network</td>
<td>Exfiltration Over Physical Medium</td>
</tr>
</tbody>
</table>
Useful Threat Hunting Tools

- EvtxToElk: https://github.com/dgunter/evtxtoelk
- ParseBroLogs: https://github.com/dgunter/ParseBroLogs
- Jupyter Notebooks: https://jupyter.org/
- Security Onion
  - ELK Dashboarding
Quick overview of what critical events are present

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Created (Count)</td>
<td>3</td>
</tr>
<tr>
<td>User Privilege Elevation (Count)</td>
<td>7</td>
</tr>
<tr>
<td>User Account Modified (Count)</td>
<td>9</td>
</tr>
<tr>
<td>Failed Logins (Count)</td>
<td>3,561</td>
</tr>
<tr>
<td>Type 3 Logins (Count)</td>
<td>48</td>
</tr>
<tr>
<td>Failed Type 3 Logins (Count)</td>
<td>3,561</td>
</tr>
<tr>
<td>RDP Logins (Count)</td>
<td>0</td>
</tr>
<tr>
<td>Failed RDP Logins (Count)</td>
<td>0</td>
</tr>
<tr>
<td>Logins with Alternate Credentials (Count)</td>
<td>47</td>
</tr>
<tr>
<td>Event Log Clearing (Count)</td>
<td>0</td>
</tr>
<tr>
<td>Service Created (Count)</td>
<td>66</td>
</tr>
<tr>
<td>Scheduled Task Created, Enabled, Updated (4958, 4790, 4702, Security) (Count)</td>
<td>0</td>
</tr>
<tr>
<td>Command Line Auditing (Count)</td>
<td>8,408</td>
</tr>
<tr>
<td>Image or Page Hash Not Valid (5038, 6281, Security) (Count)</td>
<td>0</td>
</tr>
<tr>
<td>Event</td>
<td>Computer Keyword</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
<tr>
<td>E10W17</td>
<td>Win7</td>
</tr>
</tbody>
</table>
Critical Assets and Connections

- AC900F
- Crude Oil Pump
- Master AC Unit for sending commands, firmware updates, and configuration changes
- Freelance Operations, Historian

HMI, Supervisory Devices, Freelance Engineering
Hypothesis #1

• Attackers are leveraging Freelance Operation Center login information to do reconnaissance on desalination process.

• Data Source
  • Freelance Operation Center
    • Weird logons
    • Unknown users
    • Timestamps during non-working hours
    • Un-successful logon attempts in high frequency and volume

• Data Source
  • Network Capture
    • Timestamps during non-working hours
    • Unknown addressing space
    • Scanning activity
    • Exfiltration of data
Hypothesis #2

• Attackers are sending malicious commands to AC 900F and AC 700F controllers to manipulate desalination process.

• Freelance Operation Center
  • Trend Analysis
  • Normal operations as baseline
  • Event logs
  • User Authentication

• Network Capture
  • Controller Command Responses
  • Controller Status

• Freelance Engineering
  • Understanding of PLC configuration files
  • Stateful analysis

• Process Historian
  • Alarm Events
  • Trend Analysis
Execute: Report

- Summary of all findings
- Hypothesis confirmation or falsification
- Better understanding of environment
- Establish baseline of operations for follow on hunts with new scopes
Feedback

- **Purpose**: How was the report received?
- **Scope**: Too broad or narrow? Follow on hunts?
- **Equip**: Data sources? Team Experience?
- **Plan Review**: Any blatant issues missed?
- **Execute**: Did we prove or disprove hypothesis with confidence?
Other Threat Hunting Resources

• Dragos Talk: Consequence Driven Threat Hunting in Industrial Environments
  • https://vimeo.com/288414762

• Dale Peterson discussed Consequence with Andy Bochman of INL

• Dragos Blog: Threat Hunting
  • https://dragos.com/blog/20170831-ImproveThroughHunting.html
  • https://dragos.com/blog/20171003-ThreatHuntingSeriesPart2.html
Wrapping Up

• Lots of great open source tools
• Use behaviors where possible
  • Look for bad behaviors
  • Understand environment better
• Get comfortable with larger data volumes
• Make a plan to avoid biases
Questions?

Dan Gunter | dgunter@dragos.com | Twitter: @dan_gunter

If you ever just want to talk about threat hunting, please reach out. No cost involved.