Cybersecurity Adventure: Adversary Emulation, Purple Teaming, and ICS

Tim Schulz, SCYTHE
Table of Contents

01 Cyber Archeology
   Brief journey through big cybersecurity events

02 Adversary Emulation
   Building a better training system

03 Purple Teaming
   Collaborative, transparent testing

04 ICS/OT Testing
   Finding a balance between realism and safety
Cyber Archeology
A long long time ago*

Jan 2010
Google posts a blogpost on Aurora hack

*In the information security world…
Operation Aurora

- January 12, 2010 official blog
- “If Google can get hacked, so can anyone”
- APT17

https://googleblog.blogspot.com/2010/01/new-approach-to-china.html
Unearthing Attribution

Feb 2013

APT1 report is publicly released

Jan 2010

Google posts a blogpost on Aurora hack
Highlights of the report include:

- Evidence linking APT1 to China's 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (Military Cover Designator 61398).

- A timeline of APT1 economic espionage conducted since 2006 against 141 victims across multiple industries.

- APT1's modus operandi (tools, tactics, procedures) including a compilation of videos showing actual APT1 activity.

- The timeline and details of over 40 APT1 malware families.

- The timeline and details of APT1's extensive attack infrastructure.

Adversary Rosetta Stone

Feb 2013
APT1 report is publicly released

Jan 2010
Google posts a blogpost on Aurora hack

May 2015
MITRE ATT&CK® Released
## MITRE ATT&CK®

### ATT&CK Matrix for Enterprise

<table>
<thead>
<tr>
<th></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>Command and Control</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Techniques</td>
<td>12</td>
<td>19</td>
<td>13</td>
<td>42</td>
<td>16</td>
<td>30</td>
<td>9</td>
<td>17</td>
<td>16</td>
<td>9</td>
<td>13</td>
</tr>
</tbody>
</table>

- **Execution** Techniques:
  - Command and Scripting Interpreter (9)
  - Container Administration Command
  - Deploy Container
  - Exploitation for Client Execution
  - Inter-Process Communication (2)
  - Native API
  - Scheduled Task/Job (3)
  - Shared Modules
  - Software Deployment Tools
  - System Services

- **Persistence** Techniques:
  - Account Manipulation (5)
  - BITS Jobs
  - Boot or Logon Autostart Execution (14)
  - Boot or Logon Initialization Scripts (3)
  - Browser Extensions
  - Compromise Client Software Binary
  - Create or Modify System Process (4)
  - Domain Policy Modification (2)
  - Event Triggered Execution (15)
  - Event Triggered

- **Privilege Escalation** Techniques:
  - Account Manipulation (5)
  - Access Elevation Control Mechanism (4)
  - Access Token Manipulation (6)
  - BITS Jobs
  - Build Image on Host
  - Boot or Logon Autostart Execution (14)
  - Boot or Logon Initialization Scripts (3)
  - Debug Evasion
  - Deobfuscate/Decode Files or Information
  - Deploy Container
  - Direct Volume Access
  - Domain Policy Modification (2)
  - Execution Guards (1)
  - Forge Authentication

- **Defense Evasion** Techniques:
  - Account Manipulation (5)
  - Access Elevation Control Mechanism (4)
  - Access Token Manipulation (6)
  - BITS Jobs
  - Build Image on Host
  - Boot or Logon Autostart Execution (14)
  - Boot or Logon Initialization Scripts (3)
  - Debug Evasion
  - Deobfuscate/Decode Files or Information
  - Deploy Container
  - Direct Volume Access
  - Domain Policy Modification (2)
  - Execution Guards (1)
  - Forge Authentication

- **Credential Access** Techniques:
  - Adversary-in-the-Middle (2)
  - Brute Force (4)
  - Credentials from Password Stores (3)
  - Exploitation for Credential Access
  - Forced Authentication
  - Forge Credentials (2)
  - Input Capture (4)
  - Modify Authentication Process (5)
  - Multi-Credential

- **Discovery** Techniques:
  - Account Discovery (4)
  - Application Discovery (4)
  - Application Window Discovery
  - Browser Bookmark Discovery
  - Cloud Infrastructure Discovery
  - Cloud Service Dashboard
  - Cloud Service Discovery
  - Cloud Storage Object Discovery
  - Container and Resource Discovery
  - File and Directory Discovery
  - Multi-Credential

- **Lateral Movement** Techniques:
  - Exploitation of Remote Services
  - Internal Spearphishing
  - Lateral Tool Transfer
  - Remote Service Session Hijacking (2)
  - Remote Services (3)
  - Remote Service Session Hijacking (2)
  - Root Cause Analysis
  - Software Installation
  - Software Deployment Tools
  - Taint Shared Context

- **Collection** Techniques:
  - Adversary-in-the-Middle (3)
  - Archive Collected Data (3)
  - Communication Through Removable Media
  - Data Encoding (2)
  - Data Obfuscation (3)
  - Dynamic Resolution (3)
  - Encrypted Channel (2)
  - Data from Cloud Storage Object
  - Data from Configuration Repositories
  - Data from Information Repositories (2)

- **Command and Control** Techniques:
  - Application Layer Protocol (4)
  - Automated Collection
  - Browser Session Hijacking
  - Clipboard Data
  - Data from Cloud Storage Object
  - Data from Configuration Repositories
  - Data from Information Repositories (2)

- **Exfiltration** Techniques:
  - Automated Exfiltration (1)
  - Account Access Removal
  - Communication Through Removable Media
  - Data Encryption
  - Data Obfuscation (3)
  - Dynamic Resolution (3)
  - Encrypted Channel (2)
  - Data from Cloud Storage Object
  - Data from Configuration Repositories

- **Impact** Techniques:
  - Automated Exfiltration (1)
  - Account Access Removal
  - Data Encryption
  - Data Obfuscation (3)
  - Dynamic Resolution (3)
  - Encrypted Channel (2)
  - Data from Cloud Storage Object

### Website
https://attack.mitre.org/
Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required).

### Procedure Examples

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0677</td>
<td>AADInternals</td>
<td>AADInternals is written and executed via PowerShell.[^6]</td>
</tr>
<tr>
<td>S0622</td>
<td>AppleSeed</td>
<td>AppleSeed has the ability to execute its payload via PowerShell.[^7]</td>
</tr>
<tr>
<td>G0073</td>
<td>APT19</td>
<td>APT19 used PowerShell commands to execute payloads.[^8]</td>
</tr>
</tbody>
</table>

[^6]: https://attack.mitre.org/techniques/T1059/001/
[^7]: https://attack.mitre.org/techniques/T1059/001/
[^8]: https://attack.mitre.org/techniques/T1059/001/
### MITRE ATT&CK: APT 1

#### Techniques Used

<table>
<thead>
<tr>
<th>Domain</th>
<th>ID</th>
<th>Name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>T1087</td>
<td>Account Discovery: Local Account</td>
<td>APT1 used the commands <code>net localgroup</code>, <code>net user</code>, and <code>net group</code> to find accounts on the system.(^1)</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1583</td>
<td>Acquire Infrastructure: Domains</td>
<td>APT1 has registered hundreds of domains for use in operations.(^1)</td>
</tr>
</tbody>
</table>

#### Software

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>References</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0017</td>
<td>BISCUIT</td>
<td>(^1)</td>
<td>Command and Scripting Interpreter: Windows Command Shell, Encrypted Channel: Asymmetric Cryptography, Fallback Channels, Ingress Tool Transfer, Input Capture: Keylogging, Process Discovery, Screen Capture, System Information Discovery, System Owner/User Discovery</td>
</tr>
<tr>
<td>S0119</td>
<td>Cachedump</td>
<td>(^1)</td>
<td>OS Credential Dumping: Cached Domain Credentials</td>
</tr>
</tbody>
</table>

[1] https://attack.mitre.org/groups/G0006/
Shift in Business

Feb 2013
- APT1 report is publicly released

March 2016
- Petya debuts
- Ransomware-as-a-Service

Jan 2010
- Google posts a blogpost on Aurora hack

May 2015
- MITRE ATT&CK® Released
Rise of Ransomware

Ransomware As A Service

- More collaboration in the cybercrime world
- Focus on scale
- Distributed payments
Rise of Ransomware

Ransomware As A Service

- More collaboration in the cybercrime world
- Focus on scale
- Distributed payments

Rise of Cryptocurrencies

- Easier for victims to pay
- Global use
- Value increases meant more ROI

https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time
Jan 2010
Google posts a blogpost on Aurora hack

Feb 2013
APT1 report is publicly released

March 2016
Petya debuts Ransomware-as-a-Service

May 2010
Colonial Pipeline attacked by Darkside Ransomware Group

May 2015
MITRE ATT&CK® Released
Cyber attack shuts down U.S. fuel pipeline ‘jugular,’ Biden briefed

Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate
Where does this leave us?

Increasing number of cyber attacks

Attackers that most organizations are concerned about has shifted from nation state to cybercrime
Where does this leave us?

**Increasing number of cyber attacks**
Attackers that most organizations are concerned about has shifted from nation state to cybercrime

**Higher business impact**
Ransomware can grind business to a halt and cost organizations millions of dollars
Where does this leave us?

Increasing number of cyber attacks
Attackers that most organizations are concerned about has shifted from nation state to cybercrime

Higher business impact
Ransomware can grind business to a halt and cost organizations millions of dollars

More information than ever
Vendor reports and tooling allows us to see more than ever before
Adversary Emulation
What is Adversary Emulation?

“Security tests using adversary emulation identify gaps, verify defensive assumptions, and prioritize resources.”

“Data Driven Red Teaming”

https://www.scythe.io/library/introduction-to-adversary-emulation
Becoming Data Driven

Adversary Data
- Threat Reports
- Internet Sensors
- Community Frameworks

Security Testers (Red Teams)
- Experts on security controls
- Already well established
- Active community for research & development
What is Adversary Emulation?

Security Testing + ATT&CK

Cyber Threat Intelligence (CTI)
Pyramid of (Adversary) Pain

David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
TTP Pyramid

Procedures
How the technique was carried out. For example, the attacker used `procdump -ma lsass.exe lsass_dump`

Techniques
Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics
Tactics represent the strategic goal of the adversary. For example, TA006 - Credential Access

David Bianco’s Pyramid of Pain (2013)

Getting Started with CTI

- **Red Canary Threat Detection Report** (yearly)
- **Verizon DBIR Report** (yearly)
  - [https://www.verizon.com/business/resources/reports/dbir/](https://www.verizon.com/business/resources/reports/dbir/)
- **Dragos Year in Review** (yearly) (ICS specific)
  - [https://www.dragos.com/year-in-review/](https://www.dragos.com/year-in-review/)
- **Mandiant M-Trends** (yearly)
  - [https://www.mandiant.com/m-trends](https://www.mandiant.com/m-trends)
- CrowdStrike, SentinelOne, Cybereason, etc. (EDR/CTI vendors) all have publicly released reports
- **Katie Nickels CTI Self Study Plan**
  - [Part 1, Part 2](https://www.redcanary.com/threat-detection-report/)

Where do we start?

Questions for CTI

Who is potentially targeting us?

Who should we prioritize to defend against?

What are the behaviors of those we need to defend against?
Where do we start?

**Questions for CTI**

- Who is potentially targeting us?
- Who should we prioritize to defend against?
- What are the behaviors of those we need to defend against?

**Questions for Testing**

- Would we block them?
- Would we detect them?
- Can we respond to them?
Leveraging Prior Work

TRITON
ICS Evaluation 2021

https://attackevals.mitre-engenuity.org/ics
Test Scope

Technique Scope

For the TRITON evaluation, 17 ATT&CK techniques across 10 ATT&CK tactics are in. You can view the in-scope Techniques for the TRITON evaluation below:

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Evasion</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Inhibit Response Function</th>
<th>Impair Process Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Historian</td>
<td>Change Operating Mode</td>
<td>Exploitation for Privilege Escalation</td>
<td>Hooking</td>
<td>Change Operating Mode</td>
<td>Exploitation for Evasion</td>
<td>Indicator Removal on Host</td>
<td>Escalating Privilege</td>
<td>Commonly Used Port</td>
<td>Activate Firmware Update Mode</td>
<td>Broke Force I/O</td>
<td>Damage to Property</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Command-Line Interface</td>
<td>Exploitation for Privilege Escalation</td>
<td>Hooking</td>
<td>Network Connection Enumeration</td>
<td>Default Credentials</td>
<td>Automated Collection</td>
<td>I/O</td>
<td>Attack</td>
<td>Denial of Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Engineering Workstation Compromise</td>
<td>Graphical User Interface</td>
<td>Exploitation for Privilege Escalation</td>
<td>Hooking</td>
<td>Network Connection Enumeration</td>
<td>Data from Information</td>
<td>Exploitation of Remote Services</td>
<td>Denial of View</td>
<td>Authentication</td>
<td>Module Firmware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Execution Through API</td>
<td>Exploitation for Privilege Escalation</td>
<td>Hooking</td>
<td>Network Connection Enumeration</td>
<td>Remote System Discovery</td>
<td>Remote System Information Discovery</td>
<td>Denial of Access</td>
<td>Block</td>
<td>Spoofer Reporting Message</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

https://attackevals.mitre-engenuity.org/ics
ATT&CK Evaluations: Triton

**Attack Flow**

1. Engineering Workstation Compromise
2. Initial Discovery
3. Access Safety System
4. Disable Safety Functions
5. Manipulate Process Controls
6. Destroy Infrastructure

[Diagram: TRITON Environment]

https://attackevals.mitre-engenuity.org/ics
Testing the Industry

Results

Detection Categories
How close am I to the test?

DRAGOS CONFIGURATION

The following product description and configuration information was provided unedited form. Any MITRE Engenuity comments are included in italics.

Product Version
- Dragos Platform SiteStore version: 7.2
- Dragos Platform Sensor version: 7.2
- Dragos Knowledge Pack: April 2020

Product Configuration
Each of the Windows hosts used the Microsoft Sysmon tool and forwarded logs to the Dragos Platform which can passively collect network data off of the environment and optionally leverage host-based logs. The network traffic was monitored by one Dragos network sensor monitoring the SPAN port of the switch. With this deployment, Windows host and network data were our two data sources.

Dragos Platform Configuration
- Network Traffic Ingestion by Dragos Sensor
- Windows Events ingested using the SYSLOG via Dragos Platform Sitestore
Deciphering the Results

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Telemetry</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command and Control (TA0101)</td>
<td></td>
<td>Evidence of an established network connection over TCP port 3389 between the control EWS (10.0.100.20) and the safety EWS</td>
</tr>
<tr>
<td>Technique</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commonly Used Port (T0885)</td>
<td>General (Correlation)</td>
<td></td>
</tr>
</tbody>
</table>

10.B.1
ATT&CK Evals is Great for Research Data!

Defender Policy Evaluation and Resource Allocation With MITRE ATT&CK Evaluations Data

Alexander V. Outkin, Patricia V. Schulz, Timothy Schulz, Thomas D. Tarman, and Ali Pinar, Senior Member, IEEE
How do I do that?
Purple Teaming
Why Purple Team?

- Train defenders
- Test TTPs
- Test process between teams
- Replay Security Tests

Foster a collaborative culture and mentality!
Purple Team Process

Exercise Coordinator (EC)

Present adversary, TTPs, and technical details

All

Table-top discussion of security controls and expectations for TTP execution

Red Team

Emulate the TTP while sharing the screen so everyone sees and learns what an attack looks like

Blue Team

Follow process to detect and respond to TTPs, share screen to confirm identification of artifacts

Detection Engineering

Can any adjustments or tuning to security controls and/or logging be made to increase visibility

All

Repeat procedure and record new results, move to next TTP
The Defender Challenge

Process
Discovery
T1057
Same Goal, Different Paths

- tasklist
- Get-Process
- `wmic process get /format:list`
- `CreateToolhelp32Snapshot Function`
- Process Discovery T1057
Same Goal, Different Paths

- tasklist
- Get-Process
- Process Discovery T1057
- wmic process get /format:list
- CreateToolhelp32Snapshot Function
Logs?
Are there any logging/telemetry/data for the TTPs executed?
Defender Questions

Logs?
Are there any logging/telemetry/data for the TTPs executed?

Alerts?
Were any alerts generated by the test behaviors? Were they info/high/med/low?
Defender Questions

Logs?
Are there any logging/telemetry/data for the TTPs executed?

Response?
What was the team response to any alerts?

Alerts?
Were any alerts generated by the test behaviors? Were they info/high/med/low?
Defender Questions

Logs?
Are there any logging/telemetry/data for the TTPs executed?

Alerts?
Were any alerts generated by the test behaviors? Were they info/high/med/low?

Response?
What was the team response to any alerts?

Expectations?
Were the responses appropriate for the alerts? Do we need to recalibrate?
Alert Response Process

1. SOC Receives Alert
2. Alert Analyzed & Elevated
3. Incident Response Initiated
4. Incident Remediation

How are we evaluating people and process?
Detection Engineering

Dissemination
Distributing to Stakeholders
SOC, Management, Red Team, etc

Processing
Processing Logs for Query Development

Collection
Collect Emulation Logs

Direction
Cyber Threat Intelligence (CTI) & Threat Understanding

Detection Engineering Process
Measurable Improvement

Overall Score

Lower

- Campaigns Aggregated: 5
- Test Cases Completed: 65
- Test Cases Passed: 3
  - Blocked: 1
- Test Cases Failed: 61
  - Not Detected: 61
- Test Cases Not Completed: 0
  - To Be Determined: 0

Not Detected: 94%

Overall Score

Above Average

- Campaigns Aggregated: 5
- Test Cases Completed: 69
- Test Cases Passed: 44
  - Blocked: 1
- Test Cases Failed: 24
  - Not Detected: 24
- Test Cases Not Completed: 0
  - To Be Determined: 0

Detected: 84%
Good Purple Team Talks & Resources

- Casey Smith and Ross Wolf - Fantastic Red-Team Attacks and How to Find Them
  - https://www.youtube.com/watch?v=9bUrVgP8Duk&feature=youtu.be
- Ian Anderson from OG&E: “A Path Towards Adversary Emulation in OT Environments”
  - https://www.youtube.com/watch?v=I8v6shditZE&list=PLscfLWU3es1XmQRTcobQ-E_rEEn6DTt-w&index=10
- Jorge Orchilles - Operationalized Purple Teaming
  - https://www.sans.org/webcasts/operationalized-purple-teaming/
- SANS Purple Team Poster:
  - https://www.sans.org/posters/purple-concepts-bridging-the-gap/?msc=purple-team-lp
ICS / OT Testing
Purdue Model

Enterprise IT Systems & Networks (Level 4)

“Beachhead” between legacy IT and OT operations introduce points of entry (Levels 2/3)

Strictly OT (Levels 0/1)

https://www.garlandtechnology.com/blog/ot-segmentation-best-practices-for-a-more-secure-industrial-network
Understanding the Threat
Threat Vector Overlap

Initial Access
Phishing / Credentials

Recon
External IT Systems

Other IT Threat Vectors
Gain situational awareness of hosts/network
Threat Vector Overlap

**Initial Access**
- Phishing / Credentials

**Actions on Objectives**
- Identify bridge systems

**Recon**
- External IT Systems

**Other IT Threat Vectors**
- Gain situational awareness of hosts/network

**ICS/OT Actions on Objectives**
Threat Vector Overlap

Initial Access
- Phishing / Credentials

Actions on Objectives
- Identify bridge systems

Recon
- External IT Systems

Other IT Threat Vectors
- Gain situational awareness of hosts/network

Catch ICS/OT Threats here too!
# Actions on Objectives

<table>
<thead>
<tr>
<th>Created file c:\perflogs\pa.pay</th>
<th>This file is used as a binary blob that is decrypted and loaded into memory in the Industroyer2 campaign.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download an executable payload to C:\perflogs\vatt.exe</td>
<td>This executable is used to decrypt the pa.pay payload into process memory. The binary used for vatt.exe in this campaign is a benign executable.</td>
</tr>
<tr>
<td>Perform PowerShell Active Directory GPO enumeration</td>
<td>Some components of Industroyer2 were deployed via GPO. It is believed the PowerShell enumeration was used to locate GPOs to use for deployment and optionally to confirm that new GPOs created were visible to a sample target.</td>
</tr>
</tbody>
</table>

# Actions on Objectives

<table>
<thead>
<tr>
<th>Created file c:\perflogs\pa.pay</th>
<th>This file is used as a binary blob that is decrypted and loaded into memory in the Industroyer2 campaign.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download an executable payload to C:\perflogs\vatt.exe</td>
<td>This executable is used to decrypt the pa.pay payload into process memory. The binary used for vatt.exe in this campaign is a benign executable.</td>
</tr>
<tr>
<td>Perform PowerShell Active Directory GPO enumeration</td>
<td>Some components of Industroyer2 were deployed via GPO. It is believed the PowerShell enumeration was used to locate GPOs to use for deployment and optionally to confirm that new GPOs created were visible to a sample target.</td>
</tr>
</tbody>
</table>

## Actions on Objectives

<table>
<thead>
<tr>
<th>Created file c:\perflgs\pa.pay</th>
<th>This file is used as a binary blob that is decrypted and loaded into memory in the Indestroyer2 campaign.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download an executable payload to C:\perflgs\vatt.exe</td>
<td>This executable is used to decrypt the pa.pay payload into process memory. The binary used for vatt.exe in this campaign is a benign executable.</td>
</tr>
<tr>
<td>Perform PowerShell Active Directory GPO enumeration</td>
<td>Some components of Indestroyer2 were deployed via GPO. It is believed the PowerShell enumeration was used to locate GPOs to use for deployment and optionally to confirm that new GPOs created were visible to a sample target.</td>
</tr>
</tbody>
</table>

# Actions on Objectives

<table>
<thead>
<tr>
<th>Created file <code>c:\perflogs\pa.pay</code></th>
<th>This file is used as a binary blob that is decrypted and loaded into memory in the Industroyer2 campaign.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download an executable payload to <code>C:\perflogs\vatt.exe</code></td>
<td>This executable is used to decrypt the <code>pa.pay</code> payload into process memory. The binary used for <code>vatt.exe</code> in this campaign is a benign executable.</td>
</tr>
<tr>
<td>Perform PowerShell Active Directory GPO enumeration</td>
<td>Some components of Industroyer2 were deployed via GPO. It is believed the PowerShell enumeration was used to locate GPOs to use for deployment and optionally to confirm that new GPOs created were visible to a sample target.</td>
</tr>
</tbody>
</table>

Safely Demonstrating Impact

- Ransomware: Behaviors prove the point
- Generated Files

- HMI: Network conns prove the point
- PLC
# Stages of Testing

<table>
<thead>
<tr>
<th>Stages of Testing</th>
<th>Lab</th>
<th>Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Passive</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2 Active</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>
## Stages of Testing

<table>
<thead>
<tr>
<th>Stages of Testing</th>
<th>Lab</th>
<th>Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Passive</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2 OT Vendor Tools with Industrial Protocols</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3 Active</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>
Living Off the Land

From the Github:

● A LOLBin/Lib/Script must:
  ○ Be a Microsoft-signed file, either native to the OS or downloaded from Microsoft.
  ○ Have extra "unexpected" functionality. It is not interesting to document intended use cases.
  ○ Exceptions are application whitelisting bypasses
  ○ Have functionality that would be useful to an APT or red team

https://lolbas-project.github.io/
Living Off the Land: ICS Edition

From the Github:

● A LOLBin/Lib/Script must:
  ○ Be a OT Vendor application, either native to the device ecosystem and/or downloaded from the vendor.
  ○ Have device-specific functionality. It is not interesting to document intended use cases.
  ○ Exceptions are application whitelisting bypasses
  ○ Have functionality that would be useful to an APT or red team
Detection Engineering

Dissemination
Distributing to Stakeholders
SOC, Management, Red Team, etc

Processing
Processing Logs for
Query Development

Collection
Collect Emulation Logs

Direction
Cyber Threat Intelligence
(CTI) & Threat Understanding

Detection Engineering Process
Building Trust

OT Circle of Trust

Security Testers
Trust Through Testing

- Validate in a lab
- Purple Team for transparency

Production decides OT scope
You decide!*  
*Regulations may decide for you
ICS/OT Cybersecurity Resources

- Anyone that does manufacturing
- Anyone that owns or operates critical infrastructure
- ICS/OT Vendors - SEL, etc..
- DHS - CISA/TSA
- FFRDCs/National Labs - SNL, PNNL, ORNL, INL, MITRE
- Dragos (https://www.dragos.com)
- Nozomi (https://www.nozominetworks.com/)
- GRIMM (https://www.grimm-co.com)
- SCYTHE (https://www.scythe.io)
- ICS Village (https://www.icsvillage.com/)
- Also look for VCs and their portfolios in this space (Energy Impact Partners, etc..)
THANK YOU

@teschulz

scythe.io