What Will Your Attack Look Like?

Adversary campaigns often use similar and recognizable techniques. As an ICS defender, your defensive actions (or lack of actions) will determine what your next attack will look like.

### System Variables

**The various cyber, physical, and support components found in an environment.**

1. **System Vendor**
   - Third-party applications required for operational function.

2. **Applications**
   - Productivity.
   - Training.
   - Patches.
   - Access control.

3. **Infrastructure**
   - Physical system.
   - Configuration.
   - HW, SW, and network.

4. **Cyber Maturity Variables**
   - Organization culture, investment, and management programs that shape cybersecurity capability.

5. **Adversary Capabilities**
   - A many-casts, multi-vector, phishing, and social engineering will determine system requirements.

### Cyber Maturity Variables

Your actions as the system owner will affect the attacker's strategy and possibly the outcome.

**Your cyber environment includes many elements specific to your implementation, engineering, and operational needs. These elements combine to create a unique environment to defend and protect.**

### External Drivers

- **Infrastructure**
  - Physical system.
  - Configuration.
  - HW, SW, and network.

- **Finance**
  - Electronic and financial applications.

- **Regulatory**
  - Regulatory and compliance frameworks.

- **Mission**
  - Mission and business goals.

- **Adversary Intent**
  - External party may identify the attack.
  - Privileged accounts obtained.
  - Multiple access points obtained.

### Adversary Campaigns

- **Stage 1**
  - The adversary may identify the attack.
  - Privileged accounts obtained.
  - Multiple access points obtained.

- **Stage 2**
  - The adversary may disrupt adversarial actions with the goal of minimizing the impact of the attack on the process or operation.

### Take Action!

ICS defenders must consider opportunities to disrupt adversarial actions with the goal of minimizing the impact of the attack on the process or operation.

**The adversary tactics, techniques, and procedures (TTP) used in your attack will be influenced by the maturity of your cybersecurity program, the effectiveness of your processes, and the capabilities of your defenders.**

---

**What an attack at this maturity will look like:**
- **Initial Stage**
  - Organizations at this maturity level may have already undergone an extended enterprise-targeted Stage 1 attack or an ICS-focused Stage 2 attack and are working on mitigation.

- **Defined Stage**
  - Organizations at this maturity level may have already undergone an extended enterprise-stage Stage 1 attack or an ICS-focused Stage 2 attack and are working on mitigation.

- **Optimized Stage**
  - Organizations at this maturity level may have already undergone an extended enterprise-stage Stage 1 attack or an ICS-focused Stage 2 attack and are working on mitigation.
Adversary campaigns often use similar and recognizable techniques. As an ICS defender, your defensive actions (or lack of actions) will determine what your next attack will look like.

**Adversary Capabilities**

As an ICS defender, you can’t control whether your organization becomes the target of a capable adversary.

**Adversary Methods**

ICS defenders do not control the intent, objectives, or scope of the campaign.

**External Drivers**

Adversary objectives and scope can be fluid and may change with external drivers such as geopolitical or economic events.

---

**Stage 1:** Cyber Intrusion Preparation and Execution

<table>
<thead>
<tr>
<th>Planning</th>
<th>Reconnaissance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparation</td>
<td>Weaponization</td>
</tr>
<tr>
<td>Cyber Intrusion</td>
<td>Targeting</td>
</tr>
<tr>
<td>Management &amp; Enablement</td>
<td>Sustainment, Entrenchment, Development &amp; Execution</td>
</tr>
</tbody>
</table>

- Remote Access
  - Footprint
  - Support personnel
  - Attack surface
  - Build-up
  - Monitoring
  - Legal engineering

- System Mgmt
  - Physical
  - Network
  - Backup
  - Configuration
  - Traffic management

- System Use
  - Data storage
  - Environmental reporting
  - Process performance
  - Billing
  - Powering

- Plan A
  - Utilize existing connections, credentials, and tools

- Plan B
  - Install tools, escalate privileges, and manipulate the environment

- Plan C
  - Utilize physical access approaches to deliver autonomous attacks or "phone home" when connectivity allows

**Stage 2:** ICS Attack Development and Execution

- Attack Development & Tuning
- Validation

- Attack
- Develop
- Test

- ICS Attack
- Deliver
- Install/Modify
- Execute ICS Attack

- Enabling Attack
- Trigger
- Deliver

- Initiating Attack
- Modify
- Impact

- Supporting Attack
- Hide
- Amplify

---

**Successes**

- Information sharing following Ukraine electric system attack
- Information sharing following German steelmaker attack
- Emerging and improving standards and certifications

**Failures**

- Not patching assets
- No inventory of ICS components
- Lack of segmentation
- Internet-facing devices
- Auto run and unapproved removable media use
- No antivirus or malicious code detection
- No logging

**Out of Balance**

- Important opportunities to share, learn, and improve

---

"Adversaries have managers and PowerPoint too" - Robert M. Lee

---

**Seven Habits of an Effective APT**

1. **Start with the Why**
   - Define the goal of the campaign and what success looks like: data sets, project files, operational data, and capability demonstration.

2. **Flexibility**
   - Target environments change — maintain a variety of accessible tools and capabilities to adapt to changes.

3. **Avoid Discovery by Appearing Normal**
   - Eliminate reliance on initial attack footholds and blend in to behave like a trusted user utilizing existing communication paths and tools.

4. **Understanding Human Behavior**
   - Targeted employees generally have a desire to do a good job and help others, but they typically do not assess technical risks very well and may have a limited understanding of the interconnectedness of cyber systems.

5. **Lead**
   - Stay several steps ahead of the ICS defender. Anticipate defensive responses upon discovery to ensure continuation of attack.

6. **Test to Win**
   - Validate the exploits will achieve desired outcomes in target environment. Limit damage to non-target environments.

7. **Execute**
   - Perform final-stage attacks systematically, create collateral impacts to confound and confuse recovery efforts, and follow up on ICS defender’s defensive actions.

---

"Adversaries have managers and PowerPoint too" - Robert M. Lee

---

**Flexibility**

- Target environments change — maintain a variety of accessible tools and capabilities to adapt to changes.

- Understanding Human Behavior
  - Targeted employees generally have a desire to do a good job and help others, but they typically do not assess technical risks very well and may have a limited understanding of the interconnectedness of cyber systems.

- **Test to Win**
  - Validating the exploits will achieve desired outcomes in target environment. Limit damage to non-target environments.

- **Execute**
  - Perform final-stage attacks systematically, create collateral impacts to confound and confuse recovery efforts, and follow up on ICS defender’s defensive actions.

---

**Adversary Capabilities**

- Avoid Discovery by Appearing Normal
- Understanding Human Behavior
- Test to Win
- Execute
- Start with the Why

---

**Cyber Maturity Variables**

1. External Drivers
   - Adversary objectives and scope can be fluid and may change with external drivers such as geopolitical or economic events.

2. System Variables
   - Adversary Capabilities
     - As an ICS defender, you can’t control whether your organization becomes the target of a capable adversary.

3. Adversary Methods
   - ICS defenders do not control the intent, objectives, or scope of the campaign.

4. External Drivers
   - Adversary objectives and scope can be fluid and may change with external drivers such as geopolitical or economic events.

---

**Stage 1:**

- Cyber Intrusion Preparation and Execution

**Stage 2:**

- ICS Attack Development and Execution

**Advantages:**

- Systematic approach
- Continuity of attack
- Confusion and delay in recovery efforts

**Out of Balance:**

- Important opportunities to share, learn, and improve

---

**Attacker Capabilities:**

- Physical access
- Covert channel
- Hardware manipulation
- Physical tampering

---

**Cyber Intrusion Preparation and Execution**

- Remote Access
  - Footprint
  - Support personnel
  - Attack surface
  - Build-up
  - Monitoring
  - Legal engineering

- System Mgmt
  - Physical
  - Network
  - Backup
  - Configuration
  - Traffic management

- System Use
  - Data storage
  - Environmental reporting
  - Process performance
  - Billing
  - Powering

**Plan A**

- Utilize existing connections, credentials, and tools

**Plan B**

- Install tools, escalate privileges, and manipulate the environment

**Plan C**

- Utilize physical access approaches to deliver autonomous attacks or "phone home" when connectivity allows

---

**ICS Attack Development and Execution**

- Plan A
  - Validate and expand tools to deliver autonomous attacks on ICS targets

- Plan B
  - Develop attack tools and tactics within an organization

- Plan C
  - Utilize physical access approaches to deliver autonomous attacks or "phone home" when connectivity allows

---

**Cyber Maturity**

- Cyber Intrusion Preparation and Execution
- ICS Attack Development and Execution

**Advantages:**

- Systematic approach
- Continuity of attack
- Confusion and delay in recovery efforts

**Out of Balance:**

- Important opportunities to share, learn, and improve