8/11/2025

intern id 341

MITRE ATT&CK® TTPs poc

# MITRE ATT&CK® TTPs – Proof of Concept Report

## 1. Scope

This Proof of Concept (PoC) covers the mapping of adversary behaviors to the MITRE ATT&CK® framework across three matrices: Enterprise, Mobile, and ICS. The report focuses on demonstrating tactics, techniques, and procedures (TTPs) in a simulated attack scenario, with a detailed emphasis on the Execution tactic (TA0002).

## 2. Objective

The objective of this PoC is to understand and simulate real-world adversary behaviors by applying MITRE ATT&CK TTPs in a controlled environment. The goal is to develop the ability to map observed activities to specific tactics and techniques, improving detection and mitigation strategies.

## 3. Definitions

**Tactics:** The high-level goals or objectives attackers aim to achieve during an intrusion ('why').

**Techniques:** The specific methods used to achieve those goals ('how').

**Procedures:** The concrete steps, tools, or configurations used in real attacks.

Understanding these relationships helps defenders anticipate attacker goals, recognize their methods, and implement effective defenses.

**4.MITRE ATT&CK® – Enterprise**

**1) Reconnaissance (TA0043)**

Definition: Gathering information about the target before launching attacks, using active or passive methods.

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

* **Sub-technique:** Vulnerability Scanning (T1595.002)
* **Procedures:**
  + APT41 used Acunetix to identify SQL injection flaws in web apps.
  + Sandworm Team scanned for unpatched Microsoft Exchange servers vulnerable to ProxyShell.

**Technique 2:** Gather Victim Identity Information (T1589)

* Sub-technique: Employee Names (T1589.003)
* **Procedures:**
  + Kimsuky scraped LinkedIn to identify government researchers.
  + APT28 cloned NATO profiles to impersonate staff.

Technique 3: Search Open Websites/Domains (T1593)

* **Sub-technique:** Search Open Websites (T1593.001)
* Procedures:
  + Kimsuky used news sites to identify organizations for targeting.
  + Sandworm queried Ukraine’s EDRPOU registry to plan NotPetya.

**2) Resource Development (TA0042)**

Definition: Preparing tools, accounts, and infrastructure before attacks.

**Technique 1:** Compromise Accounts (T1586)

* **Sub-technique**: Compromise Email Account (T1586.002)
* **Procedures:**
  + APT28 compromised Microsoft 365 accounts to send phishing.
  + TA453 performed password spraying to hijack academic accounts.

**Technique 2:** Obtain Capabilities (T1588)

* **Sub-technique**: Obtain Malware (T1588.001)
* **Procedures:**
  + FIN7 purchased BlackBasta ransomware from MaaS markets.
  + Lazarus modified open-source RATs for supply-chain attacks.

**Technique 3:** Stage Capabilities (T1608)

* **Sub-technique:** Upload Malware (T1608.001)
* **Procedures:**
  + TA505 hosted FlawedGrace RAT on compromised university sites.
  + FIN11 used Azure Blob Storage to deliver Qbot.

**3) Initial Access (TA0001)**

**Definition:** Methods used to gain entry into the target network.

**Technique 1:** Phishing (T1566)

* **Sub-technique:** Spearphishing Attachment (T1566.001)
* **Procedures:**
  + Emotet sent macro-enabled Word docs to install trojans.
  + APT29 delivered weaponized PDFs to deploy Cobalt Strike.

**Technique 2:** Exploit Public-Facing Application (T1190)

* **Procedures:**
  + Hafnium exploited Exchange Server vulnerabilities for shells.
  + Magecart injected skimmers into Magento sites.

**Technique 3:** Valid Accounts (T1078)

* **Sub-technique:** Domain Accounts (T1078.002)
* **Procedures:**
  + APT33 used stolen VPN credentials to bypass defenses.
  + FIN4 accessed OWA with credentials from phishing.

**4) Execution (TA0002)**

**Definition:** Running malicious code on a compromised system.

**Technique 1:** Command and Scripting Interpreter (T1059)

* **Sub-technique:** PowerShell (T1059.001)
* **Procedures:**
  + APT34 downloaded malware via encoded PowerShell.
  + FIN11 disabled Windows Defender using PowerShell before ransomware.

**Technique 2:** User Execution (T1204)

* **Sub-technique:** Malicious File (T1204.002)
* **Procedures:**
  + APT32 sent Excel files with malicious macros.
  + TA505 delivered JavaScript attachments installing RATs.

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

* **Sub-technique:** Scheduled Task (T1053.005)
* **Procedures:**
  + APT28 created tasks to run scripts at logon.
  + Carbanak scheduled malware execution during business hours.

**5) Persistence (TA0003)**

**Definition:** Techniques for maintaining access over time.

**Technique 1:** Account Manipulation (T1098)

* **Sub-technique:** Add Account (T1098.005)
* **Procedures:**
  + APT33 created local admin accounts.
  + FIN7 added hidden service accounts.

**Technique 2:** Boot or Logon Autostart Execution (T1547)

* **Sub-technique:** Registry Run Keys (T1547.001)
* **Procedures:**
  + TrickBot set registry keys for auto-execution.
  + APT29 placed DLLs in startup folders.

**Technique 3:** Web Shell (T1505.003)

* **Procedures:**
  + APT41 deployed China Chopper web shells.
  + Equation Group used custom web shells for persistence.

**6) Privilege Escalation (TA0004)**

**Definition:** Obtaining higher-level permissions for more control.

**Technique 1:** Exploitation for Privilege Escalation (T1068)

* **Procedures:**
  + Equation Group exploited kernel vulnerabilities.
  + APT41 used unpatched privilege escalation flaws.

**Technique 2:** Access Token Manipulation (T1134)

* **Sub-technique:** Token Impersonation (T1134.001)
* **Procedures:**
  + Cobalt Strike impersonated admin tokens.
  + APT29 stole tokens to move laterally in cloud systems.

**Technique 3:** Process Injection (T1055)

* **Sub-technique:** DLL Injection (T1055.001)
* **Procedures:**
  + FIN7 injected malicious DLLs into svchost.exe.
  + APT32 used DLL injection for stealth.

**7) Discovery (TA0007)**

**Definition:** Mapping out the victim environment after access.

**Technique 1**: System Information Discovery (T1082)

* **Procedures:**
  + APT28 used systeminfo to check OS and patches.
  + FIN7 ran PowerShell scripts to enumerate systems.

**Technique 2:** Account Discovery (T1087)

* **Sub-technique:** Domain Account (T1087.002)
* **Procedures:**
  + APT33 listed domain accounts using net user /domain.
  + Cobalt Strike queried Active Directory via LDAP.

**Technique 3:** Network Service Scanning (T1046)

* **Procedures:**
  + APT41 used Nmap for internal scanning.
  + Carbanak located database servers.

**8) Lateral Movement (TA0008)**

**Definition:** Moving within the network to compromise additional systems.

**Technique 1:** Remote Services (T1021)

* **Sub-technique:** RDP (T1021.001)
* **Procedures:**
  + APT29 used RDP with stolen creds.
  + FIN7 tunneled RDP sessions covertly.

**Technique 2:** Pass the Hash (T1550.002)

* **Procedures:**
  + APT33 reused NTLM hashes.
  + Cobalt Strike accessed admin shares using hashes.

**Technique 3:** Windows Admin Shares (T1077)

* **Procedures:**
  + APT41 copied malware to C$ shares.
  + Carbanak deployed trojans to ATMs.

**9) Collection (TA0009)**

**Definition:** Gathering sensitive files and data.

**Technique 1**: Screen Capture (T1113)

* **Procedures:**
  + APT28 took screenshots periodically.
  + Lazarus captured credentials shown on screen.

**Technique 2:** Clipboard Data (T1115)

* **Procedures:**
  + FIN7 stole copied passwords.
  + APT41 captured crypto wallet addresses.

**Technique 3:** Input Capture (T1056)

* **Sub-technique:** Keylogging (T1056.001)
* **Procedures:**
  + Carbanak logged keystrokes of bank staff.
  + APT33 collected VPN credentials via keyloggers.

**10) Command and Control (TA0011)**

**Definition:** Communication between adversary and compromised systems.

**Technique 1:** Application Layer Protocol (T1071)

* **Sub-technique:** Web Protocols (T1071.001)
* **Procedures:**
  + APT29 sent encrypted C2 via HTTPS.
  + FIN11 disguised C2 as normal web traffic.

**Technique 2:** Remote Access Software (T1219)

* **Procedures:**
  + APT32 installed TeamViewer.
  + TA505 used AnyDesk.

**Technique 3:** Encrypted Channel (T1573)

* **Sub-technique:** Asymmetric Cryptography (T1573.002)
* **Procedures:**
  + APT41 secured C2 with RSA.
  + Equation Group used custom PKI.

**11) Exfiltration (TA0010)**

**Definition:** Removing stolen data from the victim network.

**Technique 1:** Exfiltration Over Web Service (T1567)

* **Sub-technique:** Cloud Storage (T1567.002)
* **Procedures:**
  + APT29 uploaded data to Dropbox.
  + FIN4 used Google Drive.

**Technique 2:** Exfiltration Over C2 Channel (T1041)

* **Procedures:**
  + APT28 sent data over HTTPS C2.
  + Lazarus embedded data in heartbeat packets.

**Technique 3:** Automated Exfiltration (T1020)

* **Procedures:**
  + Carbanak automated SQL dumps to attacker servers.
  + APT33 scheduled file uploads at night.

**12) Impact (TA0040)**

**Definition:** Disrupting operations, destroying data, or manipulating systems.

**Technique 1:** Data Destruction (T1485)

* **Procedures:**
  + Shamoon wiped drives in oil companies.
  + NotPetya overwrote MBRs.

**Technique 2:** Data Encrypted for Impact (T1486)

* **Procedures:**
  + Ryuk ransomware encrypted hospital data.
  + Conti targeted corporate shares.

**Technique 3:** Defacement (T1491)

* **Sub-technique:** Internal Defacement (T1491.001)
* **Procedures:**
  + APT33 altered ICS HMI displays.
  + Iranian actors defaced political sites.

**13) Defense Evasion (TA0005)**

**Definition:**  
Defense evasion tactics are used to avoid detection, hide malicious activity, or disable security tools. This allows attackers to operate without being stopped by antivirus, EDR, or network monitoring systems.

**Technique 1:** Obfuscated Files or Information (T1027)

* **Sub-technique:** Software Packing (T1027.002)
* **Procedures:**
  + Lazarus Group packed malware with UPX to evade static analysis.
  + APT29 used custom packers to hide backdoor payloads from antivirus.

**Technique 2:** Impair Defenses (T1562)

* **Sub-technique:** Disable or Modify Tools (T1562.001)
* **Procedures:**
  + FIN7 disabled Windows Defender using PowerShell scripts.
  + APT33 modified firewall rules to allow malicious outbound connections.

**Technique 3:** Masquerading (T1036)

* **Sub-technique:** Match Legitimate Name or Location (T1036.005)
* **Procedures:**
  + APT41 renamed malware to mimic svchost.exe.
  + Turla placed malicious executables in C:\Windows\System32 to blend in.

**14) Credential Access (TA0006)**

**Definition:**  
Credential access techniques are used to steal usernames, passwords, authentication tokens, and other secrets to expand access within a network.

**Technique 1:** Brute Force (T1110)

* **Sub-technique:** Password Spraying (T1110.003)
* **Procedures:**
  + APT33 used low-frequency password spraying to avoid account lockouts.
  + TA505 tested common passwords like Winter2025! across multiple accounts.

**Technique 2:** Credential Dumping (T1003)

* **Sub-technique:** LSASS Memory (T1003.001)
* **Procedures:**
  + APT29 dumped LSASS process memory to extract NTLM hashes.
  + FIN7 used Mimikatz to obtain domain admin credentials.

**Technique 3:** Unsecured Credentials (T1552)

* **Sub-technique:** Credentials in Files (T1552.001)
* **Procedures:**
  + Lazarus searched for .txt files containing passwords on desktop folders.
  + Carbanak found unencrypted config files with database logins.

## 5. MITRE ATT&CK® – Mobile Coverage

## The Mobile ATT&CK matrix includes tactics specific to mobile devices, such as Initial Access, Execution, and Persistence.

**1) Initial Access (TA0027 – Mobile)**  
Gaining unauthorized access to a mobile device through malicious apps, phishing, or exploiting vulnerabilities.

**Technique 1:** Drive-by Compromise (T1456)

* **Procedures:**
  + OceanLotus infected Android devices via malicious websites with browser exploits.
  + Pegasus spyware exploited Safari vulnerabilities on iOS devices without user interaction.

**Technique 2:** Malicious App Installation (T1476)

* **Procedures:**
  + Joker malware embedded in apps on Google Play Store to steal SMS and contact data.
  + Xamalicious disguised as a legitimate utility app, granting remote control after installation.

**Technique 3:** Exploit via Phishing (T1471)

* **Procedures:**
  + APT-C-23 sent WhatsApp messages with malicious APK links.
  + Dark Caracal distributed fake secure messaging apps to activists.

**2) Credential Access (TA0028 – Mobile)**  
Stealing authentication information from mobile devices.

**Technique 1:** Input Capture (T1417)

* **Sub-technique:** Keylogging (T1417.001)
* **Procedures:**
  + **Anubis banker malware** captured typed banking credentials.
  + **Cerberus Trojan** logged keystrokes and sent them to C2 servers.

**Technique 2:** Credential Dumping (T1402)

* **Procedures:**
  + **Pegasus** extracted authentication tokens from messaging apps.
  + **GnatSpy** accessed stored Wi-Fi credentials.

**Technique 3:** Two-Factor Interception (T1625)

* **Procedures:**
  + **FluBot** intercepted SMS-based OTPs for bank logins.
  + **EventBot** stole MFA tokens from financial apps.

**3) Exfiltration (TA0037 – Mobile)**  
Stealing data from a mobile device and sending it to attacker-controlled infrastructure.

**Technique 1:** Exfiltration Over Alternative Protocol (T1646)

* **Procedures:**
  + **FinSpy** used covert DNS tunneling for data theft.
  + **Skygofree** used encrypted MQTT channels to evade detection.

**Technique 2:** Cloud Storage Exfiltration (T1537 – adapted)

* **Procedures:**
  + **Triout** uploaded photos and call logs to Google Drive accounts.
  + **GnatSpy** stored exfiltrated contacts in Dropbox folders.

**Technique 3:** Audio/Video Capture (T1513)

* **Procedures:**
  + **Chrysaor** recorded audio via the microphone and exfiltrated it.
  + **Monokle** activated the camera in stealth mode.

## 6. MITRE ATT&CK® – ICS (Industrial Control Systems) Coverage

The ICS ATT&CK matrix includes tactics for industrial control systems, covering aspects like Initial Access, Inhibit Response Function, and Impact.

**1) Initial Access (TA0108 – ICS)**

**Definition:**  
Techniques used to gain entry into ICS environments.

**Technique 1:** External Remote Services (T0890)

* **Procedures:**
  + **Dragonfly 2.0** accessed ICS networks via poorly secured VPN gateways.
  + **Xenotime** exploited remote access solutions for engineering workstations.

**Technique 2:** Supply Chain Compromise (T0862)

* **Procedures:**
  + **NotPetya** spread via infected accounting software in Ukraine.
  + **Industroyer** was deployed after trojanized software updates.

**Technique 3:** Spearphishing Attachment (T0865)

* **Procedures:**
  + **Sandworm** sent malware-laced Word documents to energy sector employees.
  + **APT33** used spearphishing emails to gain foothold in oil and gas ICS.

**2) Execution (TA0104 – ICS)**

Running malicious code within ICS systems to manipulate, disrupt, or gain deeper access.

**Technique 1:** Command-Line Interface (T0807)

* **Procedures:**
  + Industroyer issued direct control commands to circuit breakers.
  + Triton used engineering software command consoles to disable safety systems.

**Technique 2:** Scripting (T0853)

* **Procedures:**
  + Stuxnet used PLC scripts to alter centrifuge operations.
  + CrashOverride used custom scripts to execute load-shedding events.

**Technique 3:** Graphical User Interface (T0828)

* **Procedures:**
  + BlackEnergy interacted with ICS HMIs to manually shut down systems.
  + Iran-linked actors used HMI access to falsify operational data.

**3) Impact (TA0105 – ICS)**

**Definition:**  
Causing damage, disruption, or manipulation in ICS environments.

**Technique 1:** Manipulation of Control (T0831)

* **Procedures:**
  + Stuxnet altered PLC logic to damage centrifuges.
  + Industroyer manipulated circuit breaker controls to cause blackouts.

**Technique 2:** Inhibit Response Function (T0809)

* **Procedures:**
  + Triton disabled SIS controllers, risking unsafe plant conditions.
  + CrashOverride disrupted protective relay functions.

**Technique 3:** Damage to Property (T0820)

* **Procedures:**
  + Stuxnet physically destroyed uranium enrichment equipment.
  + Iran’s cyberattacks caused pump failures in industrial facilities.