# MITRE ATT&CK® Mobile Matrix – Complete Expanded TTP Report

**Objective:**
This document outlines standardized operational instructions for conducting and understanding cybersecurity activities aligned with the 14 tactical objectives of the MITRE ATT&CK® Mobile Matrix.
Each tactic is supported by **three distinct techniques (with MITRE IDs)**, and each technique is implemented through **two realistic, step-by-step procedures**.
The goal is to provide operational clarity, promote consistency across mobile security operations, and enhance threat detection and response.

---

## 1. Reconnaissance (TA0043)

**Tactic Description:**
The attacker gathers information to plan future operations against mobile targets.

---

**Technique 1: Network Information Gathering (T1420)**
**Procedure 1:** Use a mobile terminal app (like Termux) to run `whois targetdomain.com` to gather domain registration info for mobile services.
**Procedure 2:** Run `nslookup` or `dig` on subdomains to identify backend services such as `api.targetdomain.com`.
**Connection:** Provides insight into mobile backend endpoints for targeting.

**Technique 2: Phishing for Information via SMS (T1421)**
**Procedure 1:** Send SMS messages impersonating a mobile service provider asking users to verify their account.
**Procedure 2:** Include a shortened malicious link leading to a fake

verification page capturing IMEI and login credentials.
**Connection:** Builds a victim profile for future targeted attacks.

**Technique 3: Contact List Gathering (T1422)**
**Procedure 1:** Distribute a malicious Android app requesting contact read permissions.
**Procedure 2:** Exfiltrate contacts to an attacker-controlled cloud database for lateral targeting.
**Connection:** Expands attack surface by mapping a target's social network.

---

## 2. Resource Development (TA0042)

**Tactic Description:**
The attacker acquires, builds, or compromises infrastructure to support future mobile attacks.

---

**Technique 1: Develop Malicious Mobile Application (T1408)**
**Procedure 1:** Embed spyware modules into a legitimate open-source app.
**Procedure 2:** Repackage and sign the APK, distributing it via file-sharing platforms.
**Connection:** Provides a persistent delivery vehicle for mobile malware.

**Technique 2: Acquire C2 Infrastructure (T1583)**
**Procedure 1:** Rent a VPS under a false identity to host malware updates.
**Procedure 2:** Use domain fronting to mask the C2's IP address through legitimate cloud services.
**Connection:** Ensures stable, hidden communication channels.

**Technique 3: Obtain SMS Gateway Access (T1608.003)**
**Procedure 1:** Purchase access to an SMS API using cryptocurrency.
**Procedure 2:** Configure the gateway to send phishing messages in

bulk.
**Connection:** Facilitates large-scale mobile phishing campaigns.

---

## 3. Initial Access (TA0001)

**Tactic Description:**
The attacker delivers malicious payloads or gains entry to the mobile system.

---

**Technique 1: Drive-by Compromise (T1476)**
**Procedure 1:** Inject malicious JavaScript into an ad network serving mobile sites.
**Procedure 2:** Exploit mobile browser flaws to force-download a malicious APK.
**Connection:** Enables compromise without direct user interaction.

**Technique 2: Malicious App from Third-Party Store (T1475)**
**Procedure 1:** Trojanize a popular game APK with a backdoor.
**Procedure 2:** Upload it to unofficial app stores like Aptoide or APKPure.
**Connection:** Avoids stricter Play Store vetting, increasing infection rates.

**Technique 3: Service-based Spearphishing (T1476)**
**Procedure 1:** Send WhatsApp messages with malicious shortened links.
**Procedure 2:** Redirect victims to a fake mobile banking login page.
**Connection:** Steals credentials directly via social engineering.

---

## 4. Execution (TA0002)

**Tactic Description:**
The attacker runs malicious code or commands on the mobile device.

---

**Technique 1: Command and Scripting Interpreter (T1623)**
**Procedure 1:** Use Termux to execute shell scripts for data theft.
**Procedure 2:** Deploy malicious Python scripts for automated credential exfiltration.
**Connection:** Executes payloads directly on the mobile OS.

**Technique 2: Exploitation for Client Execution (T1620)**
**Procedure 1:** Deliver a malicious PDF exploiting a mobile viewer vulnerability.
**Procedure 2:** Use crafted media files to trigger code execution in gallery apps.
**Connection:** Leverages vulnerabilities to gain code execution.

**Technique 3: Dynamic Code Loading (T1407)**
**Procedure 1:** Deploy a base app that downloads extra malicious code at runtime.
**Procedure 2:** Encrypt secondary payloads to evade detection until execution.
**Connection:** Delivers flexibility and evasion in executing malicious features.

# 5. Persistence (TA0003)

**Tactic Description:**
The attacker ensures ongoing access to the mobile device, even after reboots or app restarts.

---

**Technique 1: Abuse Device Administrator Permissions (T1401)**
**Procedure 1:** Request `DEVICE_ADMIN` permission during malicious app installation.
**Procedure 2:** Block the uninstall process by intercepting removal requests.
**Connection:** Prevents removal and maintains long-term control over the device.

**Technique 2: Boot or Logon Autostart Execution (T1547)**
**Procedure 1:** Register the malicious app to start automatically via

`BOOT_COMPLETED` broadcast receiver.
**Procedure 2:** Use hidden services to restart malware after force stop.
**Connection:** Ensures malware survives restarts and user attempts to close it.

**Technique 3: Account Manipulation (T1098)**
**Procedure 1:** Add a rogue Google account to sync data with attacker-controlled servers.
**Procedure 2:** Change the primary sync account to redirect backups and cloud storage.
**Connection:** Grants persistent cloud access even after local cleanup.

---

# 6. Privilege Escalation (TA0004)

**Tactic Description:**
The attacker gains higher-level permissions to access restricted features or sensitive data.

---

**Technique 1: Exploitation for Privilege Escalation (T1404)**
**Procedure 1:** Deploy a root exploit targeting outdated Android kernel.
**Procedure 2:** Use privilege escalation to disable security settings.
**Connection:** Provides full system control beyond app sandbox restrictions.

**Technique 2: Access Token Manipulation (T1134)**
**Procedure 1:** Hook Android API calls to impersonate system apps.
**Procedure 2:** Replace security tokens to bypass permission prompts.
**Connection:** Grants access to privileged operations without explicit approval.

**Technique 3: Abuse of Accessibility Features (T1546)**
**Procedure 1:** Request `ACCESSIBILITY_SERVICE` to read screen content.
**Procedure 2:** Automate clicks to bypass security dialogs.
**Connection:** Uses legitimate OS features to gain powerful capabilities.

## 7. Defense Evasion (TA0005)

**Tactic Description:**
The attacker avoids detection and security controls to prolong their access.

**Technique 1: Obfuscated Files or Information (T1027)**
**Procedure 1:** Encode malicious payloads in Base64 before execution.
**Procedure 2:** Encrypt C2 communication using AES with hardcoded keys.
**Connection:** Makes it harder for AV tools to detect malicious content.

**Technique 2: Deactivate Security Software (T1089)**
**Procedure 1:** Disable Google Play Protect via accessibility automation.
**Procedure 2:** Force-stop AV apps using root privileges.
**Connection:** Removes protective layers that could detect or stop the attack.

**Technique 3: Hide App Icon (T1418)**
**Procedure 1:** Modify the launcher intent to hide the app from home screen.
**Procedure 2:** Trigger the app only via secret dial codes.
**Connection:** Keeps malicious app hidden from the user.

## 8. Credential Access (TA0006)

**Tactic Description:**
The attacker steals credentials stored on or entered into the mobile device.

**Technique 1: Credential Dumping (T1003)**
**Procedure 1:** Extract stored Wi-Fi credentials from Android settings

database.
**Procedure 2:** Dump saved email logins from mobile browser storage.
**Connection:** Provides direct access to accounts without phishing.

**Technique 2: Keylogging (T1056)**
**Procedure 1:** Implement a background service to log keyboard inputs.
**Procedure 2:** Hook input events via accessibility features to capture credentials.
**Connection:** Captures sensitive input in real time.

**Technique 3: Harvest Authentication Tokens (T1528)**
**Procedure 1:** Access mobile app cache files to retrieve JWTs or OAuth tokens.
**Procedure 2:** Replay tokens to bypass MFA and session logins.
**Connection:** Enables account takeover without needing passwords.

---

## 9. Discovery (TA0007)

**Tactic Description:**
The attacker identifies device details, apps, and network information to guide next steps.

---

**Technique 1: Network Service Scanning (T1046)**
**Procedure 1:** Use a port scanning app to find open services on the local network.
**Procedure 2:** Identify weakly secured IoT devices for lateral attacks.
**Connection:** Finds exploitable entry points in connected environments.

**Technique 2: System Information Discovery (T1082)**
**Procedure 1:** Query Android API for OS version, kernel, and build.
**Procedure 2:** Retrieve device model and manufacturer info for exploit targeting.
**Connection:** Tailors payloads to specific OS vulnerabilities.

**Technique 3: Application Discovery (T1418)**
**Procedure 1:** Enumerate installed apps to identify mobile banking

software.
**Procedure 2:** Check running services to locate security tools.
**Connection:** Helps in planning specific targeting.

---

## 10. Lateral Movement (TA0008)

**Tactic Description:**
The attacker moves from one compromised device to other systems or accounts.

---

**Technique 1: Remote Service Exploitation (T1210)**
**Procedure 1:** Exploit unpatched SMB/FTP servers on the same Wi-Fi network.
**Procedure 2:** Deploy payload to connected laptops.
**Connection:** Expands attack beyond the initial device.

**Technique 2: Pass-the-Hash (T1550.002)**
**Procedure 1:** Use stolen NTLM hashes from synced Windows credentials.
**Procedure 2:** Authenticate to corporate systems without passwords.
**Connection:** Bypasses authentication without cracking credentials.

**Technique 3: Credential Reuse (T1078)**
**Procedure 1:** Test harvested mobile credentials on corporate VPN.
**Procedure 2:** Use the same credentials for email compromise.
**Connection:** Gains access to additional accounts.

---

## 11. Collection (TA0009)

**Tactic Description:**
The attacker gathers data from the mobile device for later exfiltration.

---

**Technique 1: Screen Capture (T1513)**
**Procedure 1:** Take periodic screenshots of banking apps.
**Procedure 2:** Capture OTP codes displayed on-screen.
**Connection:** Provides visual intelligence for fraud.

**Technique 2: Audio Capture (T1417)**
**Procedure 1:** Activate microphone during calls without consent.
**Procedure 2:** Record ambient room conversations.
**Connection:** Collects sensitive voice data.

**Technique 3: Clipboard Data Harvesting (T1414)**
**Procedure 1:** Monitor clipboard for copied passwords or payment details.
**Procedure 2:** Store captured clipboard data in local cache for later exfiltration.
**Connection:** Steals transient but sensitive information.

---

## 12. Command and Control (TA0011)

**Tactic Description:**
The attacker communicates with compromised devices to issue commands and receive data.

---

**Technique 1: Web Service: Social Media (T1102.002)**
**Procedure 1:** Create a Telegram bot for C2 communication.
**Procedure 2:** Send and receive encoded commands through chat.
**Connection:** Blends in with normal encrypted traffic.

**Technique 2: Application Layer Protocol: HTTPS (T1071.001)**
**Procedure 1:** Use HTTPS POST requests to send stolen data to C2.
**Procedure 2:** Employ self-signed certificates for traffic encryption.
**Connection:** Conceals C2 within normal web browsing.

**Technique 3: Domain Fronting (T1090.004)**
**Procedure 1:** Route malicious traffic through CDN domains.

**Procedure 2:** Hide true C2 server address behind legitimate hosts.
**Connection:** Makes blocking malicious comms difficult.

---

## 13. Exfiltration (TA0010)

**Tactic Description:**
The attacker steals data from the device to a controlled location.

---

**Technique 1: Exfiltration Over HTTPS (T1041)**
**Procedure 1:** Send encrypted data chunks to an HTTPS endpoint.
**Procedure 2:** Use innocuous POST variables to hide payloads.
**Connection:** Avoids detection via encrypted channels.

**Technique 2: Cloud Storage Exfiltration (T1537)**
**Procedure 1:** Upload stolen files to Google Drive using API keys.
**Procedure 2:** Sync data periodically to avoid large spikes in traffic.
**Connection:** Uses legitimate services to store stolen data.

**Technique 3: Exfiltration Over Bluetooth (T1011)**
**Procedure 1:** Pair with a hidden Bluetooth receiver.
**Procedure 2:** Send sensitive files to nearby device.
**Connection:** Works even without internet access.

---

## 14. Impact (TA0040)

**Tactic Description:**
The attacker manipulates, disrupts, or destroys device functionality or data.

---

**Technique 1: Data Destruction (T1485)**
**Procedure 1:** Wipe `/sdcard` directory contents.

**Procedure 2:** Overwrite files with random data.
**Connection:** Prevents recovery of user data.

**Technique 2: Disk Encryption for Ransom (T1486)**
**Procedure 1:** Encrypt storage partitions with AES.
**Procedure 2:** Display ransom demand for decryption key.
**Connection:** Extorts payment from victim.

**Technique 3: Resource Hijacking (T1496)**
**Procedure 1:** Deploy XMRig miner to use device CPU/GPU.
**Procedure 2:** Keep miner throttled to avoid overheating detection.
**Connection:** Generates revenue for attacker using victim hardware.