



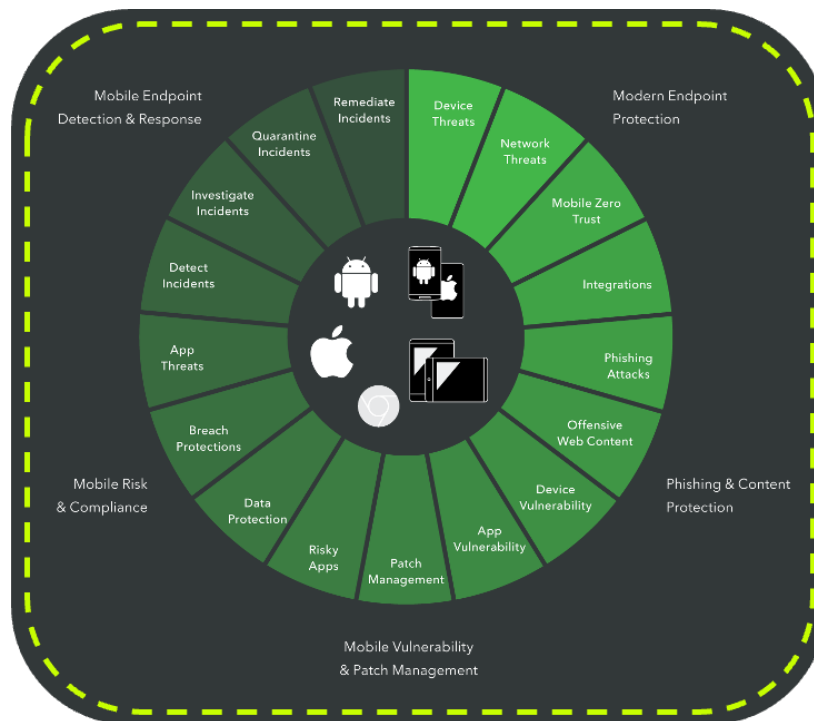
Enhance Your Mobile Cybersecurity Posture with MITRE ATT&CK[®] Matrix for Mobile

Lookout Mobile Endpoint Security

MITRE | ATT&CK[®]

MITRE ATT&CK®

The MITRE ATT&CK® framework is a globally recognized knowledge base of adversary tactics and techniques that are used for cyber-attacks. Cybersecurity professionals use the framework to understand attackers' tactics and techniques to develop effective defense strategies. Recently, MITRE has expanded its ATT&CK® framework to include mobile platforms. The MITRE ATT&CK® Mobile Matrix is a comprehensive guide that outlines the tactics, techniques, and procedures (TTPs) used by attackers to carry out mobile-based cyber-attacks. This white paper will provide an overview of the MITRE ATT&CK® Mobile Matrix and its significance in mobile security.



Overview of MITRE ATT&CK® Mobile Matrix:

The MITRE ATT&CK® Mobile Matrix is a comprehensive guide that outlines the tactics, techniques, and procedures (TTPs) used by attackers to carry out mobile-based cyber-attacks. The matrix is divided into three main categories: pre-attack, attack, and post-attack. The pre-attack category includes techniques that attackers use to gather information about the target and plan the attack. The attack category includes techniques that attackers use to gain access to the target device, steal data, or carry out other malicious activities. The post-attack category includes techniques that attackers use to maintain access to the target device or cover their tracks.

The MITRE ATT&CK® Mobile Matrix is designed to be used by security professionals to understand the various tactics and techniques used by attackers to carry out mobile-based cyber-attacks. The matrix is also useful for developing effective defense strategies and identifying vulnerabilities in the mobile environment. The matrix provides a comprehensive overview of the various TTPs used by attackers, and it can be used to develop targeted defense strategies that address specific vulnerabilities.

Significance of MITRE ATT&CK® Mobile Matrix:

Mobile devices have become an essential part of our daily lives, and they are increasingly being used for sensitive activities such as online banking, shopping, and communication. As a result, mobile devices have become a prime target for cyber-attacks. The MITRE ATT&CK® Mobile Matrix is significant because it provides a comprehensive guide to the tactics and techniques used by attackers to carry out mobile-based cyber-attacks.

The matrix is useful for security professionals because it provides a framework for understanding the various TTPs used by attackers. This information can be used to develop effective defense strategies that address specific vulnerabilities in the mobile environment. The matrix can also be used to identify gaps in existing security measures and to develop targeted mitigation strategies.

MITRE ATT&CK® for Mobile Matrix

Below are the tactics and techniques representing the two MITRE ATT&CK® Matrices for Mobile. The Matrices cover techniques involving device access and network-based effects that can be used by adversaries without device access. The Matrix contains information for the following platforms: Android, and iOS.

Initial Access 4 techniques	Execution 3 techniques	Persistence 7 techniques	Privilege Escalation 3 techniques	Defense Evasion 14 techniques	Credential Access 5 techniques	Discovery 8 techniques	Lateral Movement 2 techniques	Collection 13 techniques	Command and Control 8 techniques	Exfiltration 2 techniques	Impact 9 techniques
Drive-By Compromise	Command and Scripting Interpreter (0/1)	Boot or Logon Initialization Scripts	Abuse Elevation Control Mechanism (0/1)	Download New Code at Runtime	Access Notifications	File and Directory Discovery	Exploitation of Remote Services	Access Notifications	Application Layer Protocol (0/1)	Exfiltration Over Alternative Protocol (0/1)	Account Access Removal
Lockscreen Bypass	Native API	Compromise Application Executable	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Clipboard Data	Location Tracking (0/2)	Replication Through Removable Media	Adversary-in-the-Middle	Call Control	Exfiltration Over C2 Channel	Call Control
Replication Through Removable Media	Scheduled Task/Job	Compromise Client Software Binary	Process Injection (0/1)	Foreground Persistence	Credentials from Password Store (0/1)	Network Service Scanning		Archive Collected Data	Dynamic Resolution (0/1)		Data Encrypted for Impact
Supply Chain Compromise (0/3)		Event Triggered Execution (0/1)		Hide Artifacts (0/2)	Input Capture (0/2)	Process Discovery		Audio Capture	Encrypted Channel (0/2)		Data Manipulation (0/1)
		Foreground Persistence		Hooking	Steal Application Access Token (0/1)	Software Discovery (0/1)		Call Control	Ingress Tool Transfer		Endpoint Denial of Service
		Hijack Execution Flow (0/1)		Impair Defenses (0/3)		System Information Discovery		Clipboard Data	Non-Standard Port		Generate Traffic from Victim
		Scheduled Task/Job		Indicator Removal on Host (0/3)		System Network Configuration Discovery		Data from Local System	Out of Band Data		Input Injection
				Input Injection		System Network Connections Discovery		Input Capture (0/2)	Web Service (0/3)		Network Denial of Service
				Native API				Location Tracking (0/2)			SMS Control
				Obfuscated Files or Information (0/2)				Protected User Data (0/4)			
				Process Injection (0/1)				Screen Capture			
				Proxy Through Victim				Stored Application Data			
				Subvert Trust Controls (0/1)				Video Capture			
				Virtualization/Sandbox Evasion (0/1)							

See the full-size ATT&CK® Matrix for Mobile diagram at attack.mitre.org/matrices/mobile

In the below, we will look to provide a thorough breakdown of each tactic and technique, including definitions, impacted operating systems, mitigation recommendations, and the associated solutions.

Possible mitigation strategies:


Antivirus/Antimalware	Filter Network Traffic
Application Developer Guidance	Limit Hardware Installation
Application Isolation and Sandboxing	Lock Bootloader
Attestation	Operating System Configuration
Audit	Privileged Account Management
Behavior Prevention on Endpoint	Privileged Process Integrity
Boot Integrity	Security Updates
Code Signing	Software Configuration
Deploy Compromised Device Detection Method	System Partition Integrity
Disable or Remove Feature or Program	Update Software
Enterprise Policy	Use Recent OS Version
Execution Prevention	User Guidance
Exploit Protection	Vulnerability Scanning





Possible solutions include:

Lookout Mobile Endpoint Security (MES) — A Mobile Threat Defense solution that detects and prevents mobile device, network, phishing, and malicious app attacks.

MDM/UEM — A Mobile Device Management solution allows compliant devices to access corporate email, apps via the corporate app store, and data, and it secures data-in-transit between the mobile device and the corporate network.

Initial Access				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Drive-By Compromise	Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior, such as acquiring an Application Access Token.		Security Updates, Antivirus/Antimalware, Filter Network Traffic	Lookout MES
Lockscreen Bypass	An adversary with physical access to a mobile device may seek to bypass the device's screen lock. Several methods exist to accomplish this, including biometric spoofing, unlock code bypass, or a vulnerability exploit.		Enterprise Policy, Security Updates, Use Recent OS Version, Attestation, System Partition Integrity, Lock Bootloader, Exploit Protection, Limit Hardware Installation	Lookout MES & MDM/UEM
Replication Through Removable Media	Adversaries may move onto devices by exploiting or copying malware to devices connected via USB. In the case of Initial Access, adversaries may attempt to exploit the device via the connection to gain access to data stored on the device.		Enterprise Policy, Lock Bootloader, Security Updates, Use Recent OS Version, User Guidance, Attestation, System Partition Integrity, Exploit Protection, Limit Hardware Installation, Antivirus/Antimalware	Lookout MES & MDM/UEM
Supply Chain Compromise	Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.		Application Developer Guidance, Security Updates, Use Recent OS Version, Deploy Compromised Device Detection Method, Audit, Boot Integrity	Lookout MES
Compromise Software Dependencies and Development Tools	Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Applications often depend on external software to function properly.		Application Developer Guidance, Deploy Compromised Device Detection Method, Enterprise Policy, Code Signing, Behavior Prevention on Endpoint, Audit, Antivirus/Antimalware	Lookout MES
Compromise Hardware Supply Chain	Adversaries may manipulate hardware components in products prior to receipt by a final consumer for the purpose of data or system compromise. By modifying hardware or firmware in the supply chain, adversaries can insert a backdoor into consumer networks.		Security Updates, Use Recent OS Version, System Partition Integrity, Deploy Compromised Device Detection Method, Attestation, Lock Bootloader, Antivirus/Antimalware, Audit, Code Signing	Lookout MES


Initial Access				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Compromise Software Supply Chain	Adversaries may manipulate application software prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise of software can take place in a number of ways, including manipulation of the application source code, manipulation of the update/distribution mechanism for that software, or replacing compiled releases with a modified version.		Security Updates, Use Recent OS Version, System Partition Integrity, Deploy Compromised Device Detection Method, Attestation, Lock Bootloader, Antivirus/Antimalware, Audit, Code Signing	Lookout MES





Execution				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Command and Scripting Interpreter	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities.		Attestation, Deploy Compromised Device Detection Method, Enterprise Policy, Code Signing, Execution Prevention, Limit Software Installation, Antivirus/Antimalware	Lookout MES
Unix Shell	Adversaries may abuse Unix shell commands and scripts for execution. Unix shells are the underlying command prompts on Android and iOS devices. Unix shells can control every aspect of a system, with certain commands requiring elevated privileges that are only accessible if the device has been rooted or jailbroken.		Attestation, Deploy Compromised Device Detection Method, Enterprise Policy, Code Signing, Execution Prevention, Limit Software Installation, Antivirus/Antimalware	Lookout MES
Native API	Adversaries may use Android's Native Development Kit (NDK) to write native functions that can achieve execution of binaries or functions. Like system calls on a traditional desktop operating system, native code achieves execution on a lower level than normal Android SDK calls.		Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Scheduled Task/Job	Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. On Android and iOS, APIs and libraries exist to facilitate scheduling tasks to execute at a specified date, time, or interval.		Antivirus/Antimalware	Lookout MES

Persistence				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Boot or Logon Initialization Scripts	<p>Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence. Initialization scripts are part of the underlying operating system and are not accessible to the user unless the device has been rooted or jailbroken.</p>		<p>Attestation, Lock Bootloader, Security Updates, System Partition Integrity, Deploy Compromised Device Detection Method, Use Recent OS Version, Antivirus/Antimalware, Behavior Prevention on Endpoint, Boot Integrity, Code Signing, Execution Prevention, Exploit Protection, Operating System Configuration</p>	Lookout MES & MDM/UEM
Compromise Application Executable	<p>Adversaries may modify applications installed on a device to establish persistent access to a victim. These malicious modifications can be used to make legitimate applications carry out adversary tasks when these applications are in use.</p> <p>Adversaries may also rebuild applications to include malicious modifications.</p> <p>Adversaries may also take action to conceal modifications to application executables and bypass user consent.</p>		<p>Security Updates, Use Recent OS Version, Antivirus/Antimalware</p>	Lookout MES
Compromise Client Software Binary	<p>Adversaries may modify system software binaries to establish persistent access to devices.</p> <p>Adversaries may make modifications to client software binaries to carry out malicious tasks when those binaries are executed.</p>		<p>Attestation, Lock Bootloader, Security Updates, System Partition Integrity, Use Recent OS Version, Deploy Compromised Device Detection Method, Enterprise Policy, Antivirus/Antimalware, Application Isolation and Sandboxing, Audit, Behavior Prevention on Endpoint, Boot Integrity, Code Signing, Execution Prevention, Exploit Protection</p>	Lookout MES
Event Triggered Execution	<p>Adversaries may establish persistence using system mechanisms that trigger execution based on specific events. Mobile operating systems have means to subscribe to events such as receiving an SMS message, device boot completion, or other device activities.</p> <p>Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via automatically and repeatedly executing malicious code.</p>		<p>Use Recent OS Version, Antivirus/Antimalware</p>	Lookout MES

Persistence				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Broadcast Receivers	Adversaries may establish persistence using system mechanisms that trigger execution based on specific events. Mobile operating systems have means to subscribe to events such as receiving an SMS message, device boot completion, or other device activities.		Use Recent OS Version, Application Developer Guidance, Antivirus/Antimalware	Lookout MES
Foreground Persistence	Adversaries may abuse Android's startForeground() API method to maintain continuous sensor access. Beginning in Android 9, idle applications running in the background no longer have access to device sensors, such as the camera, microphone, and gyroscope. Applications can retain sensor access by running in the foreground, using Android's startForeground() API method.		User Guidance, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Hijack Execution Flow	Adversaries may execute their own malicious payloads by hijacking the way operating systems run applications. Hijacking execution flow can be for the purposes of persistence since this hijacked execution may reoccur over time.		Attestation, System Partition Integrity, Deploy Compromised Device Detection Method, Security Updates, System Partition Integrity, Use Recent OS Version, Antivirus/Antimalware, Behavior Prevention on Endpoint, Boot Integrity, Code Signing, Execution Prevention, Exploit Protection, Privileged Process Integrity	Lookout MES
System Runtime API Hijacking	Adversaries may execute their own malicious payloads by hijacking the way an operating system run applications. Hijacking execution flow can be for the purposes of persistence since this hijacked execution may reoccur at later points in time.		Attestation, System Partition Integrity, Deploy Compromised Device Detection Method, Security Updates, System Partition Integrity, Use Recent OS Version, Antivirus/Antimalware, Behavior Prevention on Endpoint, Boot Integrity, Code Signing, Execution Prevention, Exploit Protection, Privileged Process Integrity	Lookout MES
Scheduled Task/Job	Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. On Android and iOS, APIs and libraries exist to facilitate scheduling tasks to execute at a specified date, time, or interval.		Antivirus/Antimalware	Lookout MES

Privilege Escalation				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control elevated privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can gain on a machine. Authorization has to be granted to specific users in order to perform tasks that are designated as higher risk.		Application Developer Guidance, Enterprise Policy, Deploy Compromised Device Detection Method, Antivirus/Antimalware	Lookout MES
Device Administrator Permissions	Adversaries may abuse Android's device administration API to obtain a higher degree of control over the device. By abusing the API, adversaries can perform several nefarious actions, such as resetting the device's password for Endpoint Denial of Service, factory resetting the device for File Deletion and to delete any traces of the malware, disabling all the device's cameras, or to make it more difficult to uninstall the app		Use Recent OS Version, User Guidance, Enterprise Policy, Deploy Compromised Device Detection Method, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Exploitation for Privilege Escalation	Adversaries may exploit software vulnerabilities in order to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in an application, service, within the operating system software, or kernel itself to execute adversary-controlled code. Security constructions, such as permission levels, will often hinder access to information and use of certain techniques. Adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.		Attestation, Deploy Compromised Device Detection Method, Security Updates, Enterprise Policy, Use Recent OS Version, Application Isolation and Sandboxing, Audit, Antivirus/Antimalware, Behavior Prevention on Endpoint, Boot Integrity, Code Signing, Execution Prevention, Exploit Protection, Update Software, Software Configuration, Privileged Process Integrity, Privileged Account Management, Operating System Configuration	Lookout MES
Process Injection	Adversaries may inject code into processes in order to evade process-based defenses or even elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.		Attestation, Deploy Compromised Device Detection Method, System Partition Integrity, Use Recent OS Version, Security Updates, Audit, Behavior Prevention on Endpoint, Code Signing, Privileged Process Integrity, Vulnerability Scanning, Antivirus/Antimalware	Lookout MES

Privilege Escalation				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Ptrace System Calls	Adversaries may inject malicious code into processes via ptrace (process trace) system calls in order to evade process-based defenses as well as possibly elevate privileges. Ptrace system call injection is a method of executing arbitrary code in the address space of a separate live process.		Attestation, Deploy Compromised Device Detection Method, System Partition Integrity, Use Recent OS Version, Security Updates, Audit, Behavior Prevention on Endpoint, Execution Prevention, Code Signing, Privileged Process Integrity, Vulnerability Scanning, Antivirus/Antimalware	Lookout MES

Defense Evasion				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Download New Code at Runtime	Adversaries may download and execute dynamic code not included in the original application package after installation. This technique is primarily used to evade static analysis checks and pre-publication scans in official app stores. In some cases, more advanced dynamic or behavioral analysis techniques could detect this behavior. However, in conjunction with Execution Guardrails techniques, detecting malicious code downloaded after installation could be difficult.		Use Recent OS Version, Filter Network Traffic, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Execution Guardrails	Adversaries may use execution guardrails to constrain execution or actions based on adversary-supplied and environment-specific conditions that are expected to be present on the target. Guardrails ensure that a payload only executes against an intended target and reduces collateral damage from an adversary's campaign.		Use Recent OS Version, User Guidance, Antivirus/Antimalware	Lookout MES
Geofencing	Adversaries may use a device's geographical location to limit certain malicious behaviors. For example, malware operators may limit the distribution of a second stage payload to certain geographic regions.		Use Recent OS Version, User Guidance, Antivirus/Antimalware	Lookout MES
Foreground Persistence	Adversaries may abuse Android's startForeground() API method to maintain continuous sensor access. Beginning in Android 9, idle applications running in the background no longer have access to device sensors, such as the camera, microphone, and gyroscope. Applications can retain sensor access by running in the foreground, using Android's startForeground() API method.		User Guidance, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM



Defense Evasion				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Hide Artifacts	Adversaries may attempt to hide artifacts associated with their behaviors to evade detection. Mobile operating systems have features and developer APIs to hide various artifacts, such as an application's launcher icon. These APIs have legitimate usages, such as hiding an icon to avoid application drawer clutter when an application does not have a usable interface. Adversaries may abuse these features and APIs to hide artifacts from the user to evade detection.		Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Suppress Application Icon	A malicious application could suppress its icon from being displayed to the user in the application launcher. This hides the fact that it is installed, and can make it more difficult for the user to uninstall the application. Hiding the application's icon programmatically does not require any special permissions.		Deploy Compromised Device Detection Method, Application Isolation and Sandboxing, Audit, Behavior Prevention on Endpoint, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
User Evasion	Adversaries may attempt to avoid detection by hiding malicious behavior from the user. By doing this, an adversary's modifications would most likely remain installed on the device for longer, allowing the adversary to continue to operate on that device.		Use Recent OS Version, User Guidance, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Hooking	Adversaries may utilize hooking to hide the presence of artifacts associated with their behaviors to evade detection. Hooking can be used to modify return values or data structures of system APIs and function calls. This process typically involves using 3rd party root frameworks, such as Xposed or Magisk, with either a system exploit or pre-existing root access. By including custom modules for root frameworks, adversaries can hook system APIs and alter the return value and/or system data structures to alter functionality/visibility of various aspects of the system.		Attestation, Deploy Compromised Device Detection Method, Enterprise Policy, System Partition Integrity, Antivirus/Antimalware, Behavior Prevention on Endpoint, Code Signing, Privileged Process Integrity	Lookout MES
Impair Defenses	Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may span both native defenses as well as supplemental capabilities installed by users or mobile endpoint administrators.		Deploy Compromised Device Detection Method, Enterprise Policy, Security Updates, System Partition Integrity, User Guidance, Use Recent OS Version, Operating System Configuration, Privileged Account Management, Privileged Process Integrity, Software Configuration, Antivirus/Antimalware	Lookout MES & MDM/UEM






Defense Evasion				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Prevent Application Removal	Adversaries may abuse the Android device administration API to prevent the user from uninstalling a target application. Adversaries may also abuse the device accessibility APIs to prevent removal. This set of APIs allows the application to perform certain actions on behalf of the user and programmatically determine what is being shown on the screen.		Enterprise Policy, Use Recent OS Version, User Guidance, Attestation, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Device Lockout	An adversary may seek to inhibit user interaction by locking the legitimate user out of the device. This is typically accomplished by requesting device administrator permissions and then locking the screen using DevicePolicyManager.lockNow() . Other novel techniques for locking the user out of the device have been observed, such as showing a persistent overlay, using carefully crafted "call" notification screens, and locking HTML pages in the foreground.		Enterprise Policy, Use Recent OS Version, User Guidance, Attestation, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Indicator Removal on Host	Adversaries may delete, alter, or hide generated artifacts on a device, including files, jailbreak status, or the malicious application itself. These actions may interfere with event collection, reporting, or other notifications used to detect intrusion activity. This may compromise the integrity of mobile security solutions by causing notable events or information to go unreported.		Attestation, Security Updates, User Guidance, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Uninstall Malicious Application	Adversaries may include functionality in malware that uninstalls the malicious application from the device		Attestation, Security Updates, User Guidance, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
File Deletion	Adversaries may wipe a device or delete individual files in order to manipulate external outcomes or hide activity. An application must have administrator access to fully wipe the device, while individual files may not require special permissions to delete depending on their storage location.		User Guidance, Attestation, Enterprise Policy, Deploy Compromised Device Detection Method, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Disguise Root/Jailbreak Indicators	An adversary could use knowledge of the techniques used by security software to evade detection.		Antivirus/Antimalware	Lookout MES
Input Injection	A malicious application can inject input to the user interface to mimic user interaction through the abuse of Android's accessibility APIs.		Enterprise Policy, User Guidance, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Native API	Adversaries may use Android's Native Development Kit (NDK) to write native functions that can achieve execution of binaries or functions. Like system calls on a traditional desktop operating system, native code achieves execution on a lower level than normal Android SDK calls.		Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM







Defense Evasion				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Obfuscated Files or Information	Adversaries may attempt to make a payload or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the device or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.		Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Steganography	Adversaries may use steganography techniques in order to prevent the detection of hidden information. Steganographic techniques can be used to hide data in digital media such as images, audio tracks, video clips, or text files.		Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Software Packing	Adversaries may perform software packing to conceal their code. Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory.		Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Process Injection	Adversaries may inject code into processes in order to evade process-based defenses or even elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges.		Attestation, Deploy Compromised Device Detection Method, System Partition Integrity, Use Recent OS Version, Security Updates, Audit, Behavior Prevention on Endpoint, Code Signing, Privileged Process Integrity, Vulnerability Scanning, Antivirus/Antimalware	Lookout MES
Ptrace System Calls	Adversaries may inject malicious code into processes via ptrace (process trace) system calls in order to evade process-based defenses as well as possibly elevate privileges. Ptrace system call injection is a method of executing arbitrary code in the address space of a separate live process.		Attestation, Deploy Compromised Device Detection Method, System Partition Integrity, Use Recent OS Version, Security Updates, Audit, Behavior Prevention on Endpoint, Execution Prevention, Code Signing, Privileged Process Integrity, Vulnerability Scanning, Antivirus/Antimalware	Lookout MES



Defense Evasion				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Proxy Through Victim	Adversaries may use a compromised device as a proxy server to the Internet. By utilizing a proxy, adversaries hide the true IP address of their C2 server and associated infrastructure from the destination of the network traffic. This masquerades an adversary's traffic as legitimate traffic originating from the compromised device, which can evade IP-based restrictions and alerts on certain services, such as bank accounts and social media websites.		User Guidance, Enterprise Policy, Filter Network Traffic, Restrict Web-Based Content, Limit Access to Resource Over Network, Limit Software Installation, Network Intrusion Prevention, SSL/TLS Inspection, Filter Network Traffic, Audit, Antivirus/Antimalware, Disable or Remove Feature or Program, Restrict Web-Based Content, SSL/TLS Inspection	Lookout MES & MDM/UEM
Subvert Trust Controls	Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted applications. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust.	 	Enterprise Policy, Use Recent OS Version, User Guidance, Attestation, Antivirus/Antimalware	Lookout MES
Code Signing Policy Modification	Adversaries may modify code signing policies to enable execution of applications signed with unofficial or unknown keys. Code signing provides a level of authenticity on an app from a developer, guaranteeing that the program has not been tampered with and comes from an official source. Security controls can include enforcement mechanisms to ensure that only valid, signed code can be run on a device.	 	Enterprise Policy, Use Recent OS Version, User Guidance, Attestation, Antivirus/Antimalware	Lookout MES
Virtualization / Sandbox Evasion	Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors after checking for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox.	 	Antivirus/Antimalware	Lookout MES
System Checks	Adversaries may employ various system checks to detect and avoid virtualization and analysis environments. This may include changing behavior after checking for the presence of artifacts indicative of a virtual environment or sandbox. If the adversary detects a virtual environment, they may alter their malware's behavior to disengage from the victim or conceal the core functions of the implant. They may also search for virtualization artifacts before dropping secondary or additional payloads.	 	Antivirus/Antimalware	Lookout MES






Credential Access				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Access Notifications	Adversaries may collect data within notifications sent by the operating system or other applications. Notifications may contain sensitive data such as one-time authentication codes sent over SMS, email, or other mediums. In the case of Credential Access, adversaries may attempt to intercept one-time code sent to the device. Adversaries can also dismiss notifications to prevent the user from noticing that the notification has arrived and can trigger action buttons contained within notifications.		Application Developer Guidance, Enterprise Policy, User Guidance, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Clipboard Data	Adversaries may abuse clipboard manager APIs to obtain sensitive information copied to the device clipboard. For example, passwords being copied and pasted from a password manager application could be captured by a malicious application installed on the device.	 	Use Recent OS Version, Enterprise Policy, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Credentials from Password Store	Adversaries may search common password storage locations to obtain user credentials. Passwords can be stored in several places on a device, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.		Attestation, Deploy Compromised Device Detection Method, Security Updates, Application Developer Guidance, Antivirus/Antimalware	Lookout MES
Keychain	Adversaries may collect keychain data from an iOS device to acquire credentials. Keychains are the built-in way for iOS to keep track of users' passwords and credentials for many services and features such as Wi-Fi passwords, websites, secure notes, certificates, private keys, and VPN credentials.		Attestation, Deploy Compromised Device Detection Method, Security Updates, Antivirus/Antimalware	Lookout MES
Input Capture	Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal device usage, users often provide credentials to various locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. Keylogging) or rely on deceiving the user into providing input into what they believe to be a genuine application prompt (e.g. GUI Input Capture).	 	Enterprise Policy, Use Recent OS Version, User Guidance, Antivirus/Antimalware	Lookout MES
Keylogging	Adversaries may log user keystrokes to intercept credentials or other information from the user as the user types them.	 	Enterprise Policy, Use Recent OS Version, User Guidance, Antivirus/Antimalware	Lookout MES
GUI Input Capture	Adversaries may mimic common operating system GUI components to prompt users for sensitive information with a seemingly legitimate prompt. The operating system and installed applications often have legitimate needs to prompt the user for sensitive information such as account credentials, bank account information, or Personally Identifiable Information (PII). The constrained display size of mobile devices may impair the ability to provide users with contextual information, making users more susceptible to this technique's use.	 	Enterprise Policy, Use Recent OS Version, User Guidance, Antivirus/Antimalware	Lookout MES

Credential Access				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Steal Application Access Token	Adversaries can steal user application access tokens as a means of acquiring credentials to access remote systems and resources. This can occur through social engineering or URI hijacking and typically requires user action to grant access, such as through a system "Open With" dialogue.		Application Developer Guidance, Use Recent OS Version, User Guidance, Antivirus/Antimalware	Lookout MES
URI Hijacking	Adversaries may register Uniform Resource Identifiers (URIs) to intercept sensitive data.		Application Developer Guidance, Use Recent OS Version, User Guidance, Antivirus/Antimalware	Lookout MES

Discovery				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
File and Directory Discovery	Adversaries may enumerate files and directories or search in specific device locations for desired information within a filesystem. Adversaries may use the information from File and Directory Discovery during automated discovery to shape follow-on behaviors, including deciding if the adversary should fully infect the target and/or attempt specific actions.		Use Recent OS Version, Antivirus/Antimalware	Lookout MES
Location Tracking	Adversaries may track a device's physical location through the use of standard operating system APIs via malicious or exploited applications on the compromised device.		Enterprise Policy, Interconnection Filtering, Use Recent OS Version, User Guidance, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Remote Device Management Services	An adversary may use access to cloud services (e.g. Google's Android Device Manager or Apple iCloud's Find my iPhone) or to an enterprise mobility management (EMM)/mobile device management (MDM) server console to track the location of mobile devices managed by the service.		Enterprise Policy, User Guidance, Antivirus/Antimalware	Lookout MES
Impersonate SS7 Nodes	Adversaries may exploit the lack of authentication in signaling system network nodes to track the location of mobile devices by impersonating a node.		Interconnection Filtering, Antivirus/Antimalware	Lookout MES
Network Service Scanning	Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans from the mobile device. This technique may take advantage of the mobile device's access to an internal enterprise network either through local connectivity or through a Virtual Private Network (VPN).		Antivirus/Antimalware	Lookout MES

Discovery				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Process Discovery	Adversaries may attempt to get information about running processes on a device. Information obtained could be used to gain an understanding of common software/applications running on devices within a network. Adversaries may use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.		Attestation, Use Recent OS Version, Deploy Compromised Device Detection Method, Antivirus/Antimalware	Lookout MES
Software Discovery	Adversaries may attempt to get a listing of applications that are installed on a device. Adversaries may use the information from Software Discovery during automated discovery to shape follow-on behaviors, including whether or not to fully infect the target and/or attempts specific actions.		Use Recent OS Version, User Guidance, Antivirus/Antimalware	Lookout MES
Security Software Discovery	Adversaries may attempt to get a listing of security applications and configurations that are installed on a device. This may include things such as mobile security products. Adversaries may use the information from Security Software Discovery during automated discovery to shape follow-on behaviors, including whether or not to fully infect the target and/or attempt specific actions.		Use Recent OS Version, User Guidance, Antivirus/Antimalware	Lookout MES
System Information Discovery	Adversaries may attempt to get detailed information about a device's operating system and hardware, including versions, patches, and architecture. Adversaries may use the information from System Information Discovery during automated discovery to shape follow-on behaviors, including whether or not to fully infect the target and/or attempts specific actions.		Antivirus/Antimalware	Lookout MES
System Network Configuration Discovery	Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of operating systems they access or through information discovery of remote systems.		Use Recent OS Version, Antivirus/Antimalware	Lookout MES
System Network Connections Discovery	Adversaries may attempt to get a listing of network connections to or from the compromised device they are currently accessing or from remote systems by querying for information over the network.		Antivirus/Antimalware	Lookout MES







Lateral Movement				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Exploitation of Remote Services	Adversaries may exploit remote services by taking advantage of a mobile device's access to an internal enterprise network through local connectivity or through a Virtual Private Network (VPN).		Enterprise Policy, Audit, Behavior Prevention on Endpoint, Filter Network Traffic	Lookout MES
Replication Through Removable Media	Adversaries may move onto devices by exploiting or copying malware to devices connected via USB. In the case of Lateral Movement, adversaries may utilize the physical connection of a device to a compromised or malicious charging station or PC to bypass application store requirements and install malicious applications directly.		Enterprise Policy, Lock Bootloader, Security Updates, Use Recent OS Version, User Guidance, Attestation, System Partition Integrity, Exploit Protection, Limit Hardware Installation, Antivirus/Antimalware	Lookout MES & MDM/UEM


Collection				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Access Notifications	Adversaries may collect data within notifications sent by the operating system or other applications. Notifications may contain sensitive data, such as one-time authentication codes sent over SMS, email, or other mediums.		Application Developer Guidance, Enterprise Policy, User Guidance, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Adversary-in-the-Middle	Adversaries may attempt to position themselves between two or more networked devices to support follow-on behaviors such as Transmitted Data Manipulation or Endpoint Denial of Service.		Encrypt Network Traffic, Use Recent OS Version, Network Intrusion Prevention, Antivirus/Antimalware	Lookout MES
Archive Collected Data	Adversaries may compress and/or encrypt data that is collected prior to exfiltration. Compressing data can help to obfuscate its contents and minimize the use of network resources. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.		Antivirus/Antimalware	Lookout MES
Audio Capture	Adversaries may capture audio to collect information by leveraging standard operating system APIs of a mobile device.		Use Recent OS Version, Application Developer Guidance, Antivirus/Antimalware	Lookout MES
Call Control	Adversaries may make, forward, or block phone calls without user authorization. This could be used for adversary goals such as audio surveillance, blocking or forwarding calls from the device owner, or C2 communication.		User Guidance, Use Recent OS Version, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM



Collection				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Clipboard Data	Adversaries may abuse clipboard manager APIs to obtain sensitive information copied to the device clipboard.		Use Recent OS Version, Enterprise Policy, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Data from Local System	Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to exfiltration.		Antivirus/Antimalware	Lookout MES
Input Capture	Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal device usage, users often provide credentials to various locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. Keylogging) or rely on deceiving the user into providing input into what they believe to be a genuine application prompt (e.g. GUI Input Capture).		Enterprise Policy, Use Recent OS Version, User Guidance, Antivirus/Antimalware	Lookout MES
Keylogging	Adversaries may log user keystrokes to intercept credentials or other information from the user as the user types them.		Enterprise Policy, Use Recent OS Version, User Guidance, Antivirus/Antimalware	Lookout MES
GUI Input Capture	Adversaries may mimic common operating system GUI components to prompt users for sensitive information with a seemingly legitimate prompt. The operating system and installed applications often have legitimate needs to prompt the user for sensitive information such as account credentials, bank account information, or Personally Identifiable Information (PII). The constrained display size of mobile devices may impair the ability to provide users with contextual information, making users more susceptible to this technique's use.		Enterprise Policy, Use Recent OS Version, User Guidance, Antivirus/Antimalware	Lookout MES
Location Tracking	Adversaries may track a device's physical location through the use of standard operating system APIs via malicious or exploited applications on the compromised device.		Enterprise Policy, Interconnection Filtering, Use Recent OS Version, User Guidance, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Remote Device Management Services	An adversary may use access to cloud services (e.g. Google's Android Device Manager or Apple iCloud's Find my iPhone) or to an enterprise mobility management (EMM)/mobile device management (MDM) server console to track the location of mobile devices managed by the service.		Enterprise Policy, User Guidance, Antivirus/Antimalware	Lookout MES
Impersonate SS7 Nodes	Adversaries may exploit the lack of authentication in signaling system network nodes to track the location of mobile devices by impersonating a node.		Interconnection Filtering, Antivirus/Antimalware	Lookout MES

Collection				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Protected User Data	Adversaries may utilize standard operating system APIs to collect data from permission-backed data stores on a device, such as the calendar or contact list. These permissions need to be declared ahead of time.		Use Recent OS Version, User Guidance, Deploy Compromised Device Detection Method, Antivirus/Antimalware	Lookout MES
Calendar Entries	Adversaries may utilize standard operating system APIs to gather calendar entry data.		User Guidance, Deploy Compromised Device Detection Method, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Call Log	Adversaries may utilize standard operating system APIs to gather call log data.		User Guidance, Use Recent OS Version, Deploy Compromised Device Detection Method, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Contact List	Adversaries may utilize standard operating system APIs to gather contact list data.		User Guidance, Use Recent OS Version, Deploy Compromised Device Detection Method, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
SMS Messages	Adversaries may utilize standard operating system APIs to gather SMS messages.		User Guidance, Use Recent OS Version, Deploy Compromised Device Detection Method, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Screen Capture	Adversaries may use screen capture to collect additional information about a target device, such as applications running in the foreground, user data, credentials, or other sensitive information.		Application Developer Guidance, Enterprise Policy, User Guidance, Use Recent OS Version, Antivirus/Antimalware	Lookout MES
Stored Application Data	Adversaries may try to access and collect application data resident on the device. Adversaries often target popular applications, such as Facebook, WeChat, and Gmail.		Use Recent OS Version, Application Developer Guidance, Antivirus/Antimalware	Lookout MES
Video Capture	An adversary can leverage a device's cameras to gather information by capturing video recordings. Images may also be captured, potentially in specified intervals, in lieu of video files.		Use Recent OS Version, Application Developer Guidance, Antivirus/Antimalware	Lookout MES

Command and Control				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Application Layer Protocol	Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the mobile device, and often the results of those commands, will be embedded within the protocol traffic between the mobile device and server.		Antivirus/Antimalware	Lookout MES
Web Protocols	Adversaries may communicate using application layer protocols associated with web protocols traffic to avoid detection/network filtering by blending in with existing traffic. Commands to remote mobile devices, and often the results of those commands, will be embedded within the protocol traffic between the mobile client and server.		Antivirus/Antimalware	Lookout MES
Call Control	Adversaries may make, forward, or block phone calls without user authorization. This could be used for adversary goals such as audio surveillance, blocking or forwarding calls from the device owner, or C2 communication.		User Guidance, Use Recent OS Version, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Dynamic Resolution	Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. This algorithm can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control.		Antivirus/Antimalware	Lookout MES
Domain Generation Algorithms	Adversaries may use Domain Generation Algorithms (DGAs) to procedurally generate domain names for uses such as command and control communication or malicious application distribution.		Antivirus/Antimalware	Lookout MES
Encrypted Channel	Adversaries may explicitly employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol.		Antivirus/Antimalware	Lookout MES
Symmetric Cryptography	Symmetric encryption algorithms use the same key for plaintext encryption and ciphertext decryption. Common symmetric encryption algorithms include AES, Blowfish, and RC4.		Antivirus/Antimalware	Lookout MES
Asymmetric Cryptography	Asymmetric cryptography, also known as public key cryptography, uses a keypair per party: one public that can be freely distributed, and one private that should not be distributed.		Antivirus/Antimalware	Lookout MES
Ingress Tool Transfer	Adversaries may transfer tools or other files from an external system onto a compromised device to facilitate follow-on actions.		Antivirus/Antimalware	Lookout MES

Command and Control				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Non-Standard Port	Adversaries may generate network traffic using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088 or port 587 as opposed to the traditional port 443.		Antivirus/Antimalware	Lookout MES
Out of Band Data	Adversaries may communicate with compromised devices using out of band data streams. This could be done for a variety of reasons, including evading network traffic monitoring, as a backup method of command and control, or for data exfiltration if the device is not connected to any Internet-providing networks (i.e. cellular or Wi-Fi). Several out of band data streams exist, such as SMS messages, NFC, and Bluetooth.		User Guidance, Antivirus/Antimalware	Lookout MES
Web Service	Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media, acting as a mechanism for C2, may give a significant amount of cover.		Antivirus/Antimalware	Lookout MES
Dead Drop Resolver	Adversaries may post content, known as a dead drop resolver, on Web services with embedded (and often obfuscated/encoded) domains or IP addresses. Once infected, victims will reach out to and be redirected by these resolvers.		Antivirus/Antimalware	Lookout MES
Bidirectional Communication	Those infected systems can then send the output from those commands back over that Web service channel. The return traffic may occur in a variety of ways, depending on the Web service being utilized. For example, the return traffic may take the form of the compromised system posting a comment on a forum, issuing a pull request to development project, updating a document hosted on a Web service, or by sending a Tweet.		Antivirus/Antimalware	Lookout MES
One-Way Communication	Those infected systems may opt to send the output from those commands back over a different C2 channel, including to another distinct Web service. Alternatively, compromised systems may return no output at all in cases where adversaries want to send instructions to systems and do not want a response.		Antivirus/Antimalware	Lookout MES

Exfiltration				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Exfiltration Over Alternative Protocol	Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.		Antivirus/Antimalware	Lookout MES

Exfiltration				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Exfiltration Over Unencrypted Non-C2 Protocol	Adversaries may opt to obfuscate this data, without the use of encryption, within network protocols that are natively unencrypted (such as HTTP, FTP, or DNS). Adversaries may employ custom or publicly available encoding/compression algorithms (such as base64) or embed data within protocol headers and fields.		Antivirus/Antimalware	Lookout MES
Exfiltration Over C2 Channel	Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.		Antivirus/Antimalware	Lookout MES

Impact				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Account Access Removal	Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: credentials changed) to remove access to accounts.		User Guidance, Use Recent OS Version, Deploy Compromised Device Detection Method, Enterprise Policy, Antivirus/Antimalware	Lookout MES
Call Control	Adversaries may make, forward, or block phone calls without user authorization. This could be used for adversary goals such as audio surveillance, blocking or forwarding calls from the device owner, or C2 communication.		User Guidance, Use Recent OS Version, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Data Encrypted for Impact	An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.		Antivirus/Antimalware	Lookout MES
Data Manipulation	Adversaries may insert, delete, or alter data in order to manipulate external outcomes or hide activity. By manipulating data, adversaries may attempt to affect a business process, organizational understanding, or decision-making.		Use Recent OS Version, Enterprise Policy, Antivirus/Antimalware	Lookout MES
Transmitted Data Manipulation	Adversaries may alter data en route to storage or other systems in order to manipulate external outcomes or hide activity. By manipulating transmitted data, adversaries may attempt to affect a business process, organizational understanding, or decision-making.		Use Recent OS Version, Enterprise Policy, Antivirus/Antimalware	Lookout MES

Impact				
MITRE ATT&CK® Technique	Technique Details	Platforms	MITRE Mitigation Recommendations	Solutions
Endpoint Denial of Service	Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users.		User Guidance, Use Recent OS Version, Deploy Compromised Device Detection Method, Enterprise Policy, Antivirus/Antimalware	Lookout MES
Generate Traffic from Victim	Adversaries may generate outbound traffic from devices. This is typically performed to manipulate external outcomes, such as to achieve carrier billing fraud or to manipulate app store rankings or ratings. Outbound traffic is typically generated as SMS messages or general web traffic, but may take other forms as well.		User Guidance, Antivirus/Antimalware	Lookout MES
Input Injection	A malicious application can inject input to the user interface to mimic user interaction through the abuse of Android's accessibility APIs.		Enterprise Policy, User Guidance, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM
Network Denial of Service	Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth that services rely on, or by jamming the signal going to or coming from devices.		Antivirus/Antimalware	Lookout MES
SMS Control	Adversaries may delete, alter, or send SMS messages without user authorization. This could be used to hide C2 SMS messages, spread malware, or various external effects.		User Guidance, Use Recent OS Version, Antivirus/Antimalware, Disable or Remove Feature or Program	Lookout MES & MDM/UEM

MITRE | ATT&CK®

About MITRE ATT&CK®

The MITRE ATT&CK® Mobile Matrix is a comprehensive guide that outlines the tactics, techniques, and procedures (TTPs) used by attackers to carry out mobile-based cyber-attacks. The matrix is designed to be used by security professionals to understand the various TTPs used by attackers and to develop effective defense strategies. Mobile devices have become a prime target for cyber-attacks, and the MITRE ATT&CK® Mobile Matrix is significant because it provides a framework for understanding the various TTPs used by attackers and developing targeted defense strategies. As mobile devices continue to play an increasingly important role in our daily lives, it is essential that security professionals have access to comprehensive guides like the MITRE ATT&CK® Mobile Matrix to help them protect against mobile-based cyber-attacks.



About Lookout

Lookout, Inc. is the endpoint-to-cloud cybersecurity company that delivers zero trust security by reducing risk and protecting data wherever it goes, without boundaries or limits. Our unified, cloud-native platform safeguards digital information across devices, apps, networks and clouds and is as fluid and flexible as the modern digital world. Lookout is trusted by enterprises and government agencies of all sizes to protect the sensitive data they care about most, enabling them to work and connect freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our [blog](#), [LinkedIn](#), and [Twitter](#).

If you'd like to get a **free evaluation of your risk**, we can help.

© 2023 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, and LOOKOUT with Shield Design® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, the 4 Bar Shield Design, and the Lookout multi-color/multi-shaded Wingspan design.

© 2015–2023, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.