ZIMPERIUM®
ADVANCED MOBILE SECURITY

The Anatomy of Mobile Attacks

Corporate mobile endpoints, both owned and operating under bring-your-own-device (BYOD) policies, are high-value targets for cybercriminal groups. Mobile devices can access the same company data as a company laptop but generally have significantly less security and more attack vectors.

Most successful mobile attacks use updated versions of existing malicious tools that have been developed in the past, tailored to specific attack goals, and grouped for additional complexity to create an advanced persistent threat. This approach enables attackers to shield the attack from legacy-based threat detection tools early on, giving them the advantage of time to carry out their goals.

To stand up to these advanced mobile toolsets and skilled malicious actors, enterprises must reduce their reliance on legacy, static defenses, as well as end-user training to secure their mobile endpoints. Not only are these legacy systems incapable of preventing advanced attacks, their limited capabilities and reliance on signatures make them all but useless against zero-day threats. To secure the existing endpoints against modern attacks, organizations must adopt a comprehensive solution that can detect known and unknown threats throughout the cyber kill chain and integrate seamlessly into an organization's overall security architecture.

ANATOMY OF CYBERATTACK MODELS

The Cyber Kill Chain (CKC) and MITRE's ATT&CK for Mobile Matrices are tightly coupled case models that provide context around both the strategy and the tactical aspects of the attacks performed. These case models provide the capabilities necessary to detect and defend against attacks that occur at every stage of those models, regardless of when they are started or stopped.

What is the Cyber Kill Chain (CKC) Model?

Stage 1: Discovery & Reconnaissance
Attackers will start off by doing recon on the victim and their devices to uncover details regarding the user and its identity, the device, and/or the related network. Ultimately attackers aim to understand what they can leverage to reach their intended goals.

Stage 2: Weaponization

In this stage, attackers use the information from stage 1 to build a well-suited malware weapon.

Stage 3: Delivery

During the Delivery stage, attackers deliver the malware weapon. Delivery can be realized in many ways, such as:

- Wi-Fi Network
- GSM Network
- USB
- NFC
- Bluetooth
- Message (ex. SMS/MMS/E-Mail)
- Redirect to a site with malicious payload or exploit (ex. Stagefright or Pegasus)
- Malicious image (ex. iMessage)

Once the attackers have delivered their payload and/or established their presence on the device, they can progress to the next/other stages as they see fit.

Stage 4: Exploitation & Stage 5: Installation

During the Exploitation and Installation stages attackers, attackers execute and install the malware to establish their presence. After stage 5, the device is fully compromised.

Stage 6: Command & Control

In principle, at this stage, the attacker sends a command to the device that allows him to control the behavior of the device and be in a position to execute the intended goal.

Stage 7: Actions

Once a device has been compromised the attacker will be able to achieve the ultimate goal of a) creating persistence on the device that the user cannot easily get rid of or detect and b) exfiltrate data that is of interest to the attacker, such as sensitive files and user identity tokens (e.g., certifications, usernames, passwords, etc.).

What are the tactics in MITRE's ATT&CK for Mobile Matrices?

Device Access

- Initial Access (9 techniques)
- Execution (4 techniques)
- Persistence (9 techniques)
- Privilege Escalation (4 techniques)
- Defense Evasion (19 techniques)
- Credential Access (11 techniques)
- Discovery (9 techniques)
- Lateral Movement (2 techniques)
- Collection (17 techniques)
- Command and Control (8 techniques)
- Exfiltration (4 techniques)
- Impact (10 techniques)

Network Access

- Network Effects (9 techniques)
- Remote Service Effects (3 techniques)

BREAKING DOWN THE ANATOMY OF MOBILE ATTACKS

Each test case below covers the different seven stages of the CKC and the use of 13 different MITRE ATT&CK for Mobile technique categories for real-world attacks against mobile endpoints. Although some only cover individual stages, others show how an attack can be chained together to cover the entire model grouping, and some show how the attacks can start later on in the CKC, without being chained together with earlier attacks.

Test Case 1	
Name	**Network Scans**
Platform(s)	Android (all versions), iOS 9.x and below
Description	Scanning on the network allows attackers to discover potential targets and is generally a precursor to an actual attack. These test cases will be aimed at the discovery of Android devices on the network using a variety of scan techniques.
Expected Threat Events	• TCP Scan • IP Scan • ARP Scan • UDP Scan
CKC Stages	Stages = 1
MITRE's ATT&CK for Mobile Tactics	Network Effects, Discovery
Pre-Conditions	• Wi-Fi Network is connected to the internet • No Host-Isolation is present in the Wi-Fi Network • No VPN has been established by the device • Attacker is connected to the Wi-Fi network
Post-Conditions	Attacker has identified the victim in the network
Execution Steps	• Victim connects to the Wi-Fi • Attacker starts network recon scan • Attacker obtains information as a result of the scan

Test Case 2	
Name	**Network Attacks**
Platform(s)	iOS, Android
Description	Attackers can gain control of the network traffic produced by a device running an ARP MitM (Man in the Middle) and subsequently changing the content of the traffic. During the attack, images displayed on webpages will be replaced to demonstrate control of the traffic.
Expected Threat Events	• ARP MitM • SSL Strip • SSL MitM
CKC Stages	Stages = 2, 3
MITRE's ATT&CK for Mobile Tactics	Network Effects, Initial Access
Pre-Conditions	• Wi-Fi network is connected to the internet • No host-isolation is present in the Wi-Fi network • No VPN has been established by the device • Attacker is connected to the Wi-Fi network
Post-Conditions	Victim is connected to the attacker instead of the gateway of the network. The attacker has full control over traffic flow between the victim and network gateway demonstrated by: • Manipulation of http traffic (content injection) • Inspection of http and https traffic (traffic in cleartext) • Browsing various pages which are clearly manipulated by the attacker (e.g. images are replaced)

Execution Steps	• Victim connects to the Wi-Fi
	• Attacker starts Network Attack
	  ○ ARP MitM
	  ○ SSL MitM
	  ○ SSL Strip
	• Victim browses a page on the device

Test Case 3	
Name	**Malware Sideloaded (iOS)**
Platform(s)	iOS (MDM enrolled)
Description	Download and installation of malware from a custom-crafted page
Expected Threat Events	• Suspicious app • Sideloaded app
CKC Stages	Stages = 3, 4
MITRE's ATT&CK for Mobile Tactics	Network Effects, Initial Access, Execution
Pre-Conditions	• Attacker is connected to the Wi-Fi network • Attacker is actively routing traffic to his own host via either Rogue AP or ARP MitM • No host-isolation is present in the Wi-Fi network • No VPN has been established by the device • Wi-Fi network is connected to the internet • A certificate trusted by the device is installed on the web server
Post-Conditions	• Malicious application is installed on the device • Sideloaded application detected on the device
Execution Steps	• Attacker starts DNS poisoning and launches web server hosting malicious payload • Victim connects to the Wi-Fi • Victim browses a page allowing the installation of various apps is shown • The victim taps a link and runs the app installation

Test Case 4	
Name	**Rogue Access Point**
Platform(s)	iOS, Android
Description	Attackers can manipulate and control traffic produced by a device once the device is tricked into connecting to a malicious Wi-Fi with an SSID previously known by the device. After the connection has been established, the traffic can be routed to a malicious captive portal.
Expected Threat Events	Suspicious app
CKC Stages	Stages = 3, 4
MITRE's ATT&CK for Mobile Tactics	Network Effects, Initial Access
Pre-Conditions	• Victim device has previously connected to open Wi-Fis • Victim device Wi-Fi is switched off • Attacker has a rogue access point, also called a "pineapple," running and is actively responding to Wi-Fi probes
Post-Conditions	• Victim device is connected to the rogue access point • Attacker has full control over traffic flow • Control can be demonstrated by routing traffic for specific websites to the attacker's host where a notification page is hosted

Execution Steps	• Attacker
	  ○ Starts a web server on his host serving a notification page
	  ○ Configures DNS route for particular URL to the attacker's host in the pineapple access point
	  ○ Enables a captive portal that notifies anyone connecting to the rogue access point
	  ○ Starts actively responding to Wi-Fi probes
	  ○ Start actively capturing SSIDs that are being requested
	• Victim switches on the Wi-Fi on the device
	• Device connects to the rogue access point
	• Victim gets presented with the captive portal notification and accepts
	• Victim browses a particular URL and is presented with the notification page

Test Case 5	
Name	**Malicious Profile**
Platform(s)	iOS
Description	When the user is connected to the Wi-Fi and browses a page, they will be redirected to a page that tricks them into installing a malicious profile that will connect the device to a VPN service. Within the service, the traffic will be decrypted in order to obtain sensitive information.
Expected Threat Events	• Rogue access point • SSL MitM • Suspicious profile (*MDM only*)
CKC Stages	Stages = 3, 4
MITRE's ATT&CK for Mobile Tactics	Network Effects, Initial Access, Execution
Pre-Conditions	• Attacker is actively routing traffic to his own host using either a rogue access point or ARP MitM • No host-isolation is present in the Wi-Fi network • No VPN has been established by the device • Attacker is connected to the Wi-Fi network • Wi-Fi network is connected to the internet • A certificate trusted by the device is installed on the web server
Post-Conditions	• Malicious profile is installed on the device • VPN is established from the device to an attacker's VPN gateway • The traffic is fully compromised and the attacker has full control
Execution Steps	• Attacker starts DNS poisoning and launches web server hosting malicious payload • Victim connects to the Wi-Fi • Victim browses a page and a warning requesting a profile to be installed • The victim confirms the installation steps in order to proceed • Attacker intercepts the traffic to exfiltrate data and/or inject content

Test Case 6	
Name	**Remote Exploit**
Platform(s)	iOS
Description	A user connects to a Wi-Fi that is hosted by a malicious Wi-Fi access point. When the user browses a page, they will be redirected to a page that will trick the user into installing a malicious application that is undetectable. Once the application runs, it will exploit the device and provide elevated access to the attacker that will be used to exfiltrate data.
Expected Threat Events	• Rogue access point • System tampering /jailbreak
CKC Stages	Stages = 2, 3, 4, 5, 6
MITRE's ATT&CK for Mobile Tactics	Network Effects, Initial Access, Persistence, Privilege Escalation
Pre-Conditions	• Attacker is actively routing traffic to his own host using either a rogue access point or ARP MitM • No host-isolation is present in the Wi-Fi network • No VPN has been established by the device • Attacker is connected to the Wi-Fi network • Wi-Fi network is connected to the internet • A certificate trusted by the device is installed on the Apache server
Post-Conditions	• Malicious application is installed on the device • An exploit is running on the device • The device is fully compromised, and the attacker has full control
Execution Steps	• Attacker starts DNS poisoning and launches web server hosting malicious payload • Victim connects to the Wi-Fi • Victim browses a page and a warning is displayed that requests an app be installed • The victim taps the link and runs the app after installation is completed • Attacker connects to the device to exfiltrate data.

Test Case 7	
Name	**Malicious Charger**
Platform(s)	Android & iOS
Description	Malicious chargers are a strong potential way to exploit devices that are connected to them, including iOS-based A12 chip devices susceptible to Checkm8. Users of mobile devices can get exposed to these in airports, coffee shops, while traveling, when using low-cost chargers manufactured in specific geographic locations, and more. Attackers generally aim to obtain information and access to the connected devices. After connecting to the malicious charger, the users notice nothing but an exploit is pushed to the device and is executed. Following this, the attacker can exfiltrate data and create persistence in the firmware.
Expected Threat Events	• Process anomaly • System tampering • EOP • Persistent O/S modification
CKC Stages	Stages = 2, 3, 4
MITRE's ATT&CK for Mobile Tactics	Initial Access, Persistence, Privilege Escalation
Pre-Conditions	• Victim has accepted the message asking to trust the fingerprint of the connected USB station/device • Developer options & USB debugging enabled • 3rd party app stores enabled • The device is in airplane mode with Wi-Fi disabled
Post-Conditions	The device is fully compromised, and the attacker has full control
Execution Steps	• Victim connects their device to the USB • Attacker pushes an exploit to the device • Attacker runs the exploit(s) and gains elevated privileges

ANATOMY OF COMPREHENSIVE MOBILE SECURITY

Although enterprise mobile devices are often protected by a set of baseline solutions, like mobile device management (MDM) and mobile access management (MAM), these toolsets are not security-centric. Management applications do not provide sufficient detection, prevention, or remediation of malicious attacks through the four most common attack vectors: device, network, application, phishing. These management toolsets also do not provide security teams with the valuable intrinsic threat intelligence data necessary to respond and remediate mobile attacks as they would with traditional endpoints.

Enterprise mobile security solutions must have an advanced technology solution that leverages machine learning to protect against device, network, application, and phishing attacks. They must also fit into existing security ecosystems, integrating with the EPP, UEM, and EDR environment to give a complete picture of endpoints. And flexibility is key to support a wide range of data access laws and compliance needs that can only be met through flexible cloud hosting options.

Ultimately, enterprises need to adopt a security solution that incorporates the data, control, and coverage needed for the distributed workforce while supporting current security workflows.

Zimperium zIPS is an advanced mobile threat defense (MTD) solution built for enterprises, providing persistent, on-device protection to both corporate-owned and BYOD devices. Leveraging Zimperium's machine learning engine, z9, zIPS detects known and zero-day threats on-device and in real-time, without introducing latency or violating user privacy.

Zimperium provides advanced machine learning-based enterprise mobile security, capable of running on any cloud platform (AWS, Azure, Oracle, Google), and integrates seamlessly into existing security infrastructure.

To learn more about how Zimperium can protect your organization's mobile devices, visit www.zimperium.com.

ZIMPERIUM®