@hackinarticles

https://github.com/Ignitetechnologies

https://in.linkedin.com/company/hackingarticles

MITRE ATT&CK Mobile Tactics

ID:TA0032 - Discovery
- T1420 - File and Directory Discovery
- T1430 - Location Tracking
  - Remote Device Management Services
  - Impersonate SS7 Nodes
- T1423 - Network Service Scanning
- T1424 - Process Discovery
- T1418 - Software Discovery
  - Security Software Discovery
- T1426 - System Information Discovery
- T1422 - System Network Configuration Discovery
- T1421 - System Network Connections Discovery

ID:TA0031 - Credential Access
- T1517 - Access Notifications
- T1414 - Clipboard Data
- T1634 - Credentials from Password Store
  - Keychain
- T1417 - Input Capture
  - Keylogging
  - GUI Input Capture
- T1635 - Steal Application Access Token
  - URI Hijacking

ID:TA0030 - Defense Evasion
- T1407 - Download New Code at Runtime
- T1627 - Execution Guardrails
  - Geofencing
- T1541 - Foreground Persistence
- T1628 - Hide Artifacts
  - Suppress Application Icon
  - User Evasion
- T1617 - Hooking
- T1629 - Impair Defenses
  - Prevent Application Removal
  - Device Lockout
  - Disable or Modify Tools
- T1630 - Indicator Removal on Host
  - Uninstall Malicious Application
  - File Deletion
  - Disguise Root/Jailbreak Indicators
- T1516 - Input Injection
- T1575 - Native API
- T1406 - Obfuscated Files or Information
  - Steganography
  - Software Packing
- T1631 - Process Injection
  - Ptrace System Calls
- T1604 - Proxy Through Victim
- T1632 - Subvert Trust Controls
  - Code Signing Policy Modification
- T1633 - Virtualization/Sandbox Evasion
  - System Checks

ID:TA0029 - Privilege Escalation
- T1626 - Abuse Elevation Control Mechanism
  - Device Administrator Permissions
- T1404 - Exploitation for Privilege Escalation
- T1631 - Process Injection
  - Ptrace System Calls

ID:TA0028 - Persistence
- T1398 - Boot or Logon Initialization Scripts
- T1577 - Compromise Application Executable
- T1645 - Compromise Client Software Binary
- T1624 - Event Triggered Execution
  - Broadcast Receivers
- T1541 - Foreground Persistence
- T1625 - Hijack Execution Flow
  - System Runtime API Hijacking
- T1603 - Scheduled Task/Job

ID:TA0041 - Execution
- T1575 - Native API
  - T1623 - Command and Scripting Interpreter
    - Unix Shell
- T1603 - Scheduled Task/Job

ID:TA0027 - Initial Access
- T1456 - Drive-By Compromise
- T1461 - Lockscreen Bypass
- T1458 - Replication Through Removable Media
- T1474 - Supply Chain Compromise
  - Compromise Software Dependencies and Development Tools
  - Compromise Hardware Supply Chain
  - Compromise Software Supply Chain

ID:TA0033 - Lateral Movement
- T1428 - Exploitation of Remote Services
- T1458 - Replication Through Removable Media

ID:TA0035 - Collection
- T1517 - Access Notifications
- T1638 - Adversary-in-the-Middle
- T1532 - Archive Collected Data
- T1429 - Audio Capture
- T1616 - Call Control
- T1414 - Clipboard Data
- T1533 - Data from Local System
- T1417 - Input Capture
  - Keylogging
  - GUI Input Capture
- T1430 - Location Tracking
  - Remote Device Management Services
  - Impersonate SS7 Nodes
- T1636 - Protected User Data
  - Calendar Entries
  - Call Log
  - Contact List
  - Messages
- T1513 - Screen Capture
- T1409 - Stored Application Data
- T1512 - Video Capture

ID:TA0037 - Command and Control
- Web Protocols
  - T1437 - Application Layer Protocol
- T1616 - Call Control
- Domain Generation Algorithms
  - T1637 - Dynamic Resolution
- T1521 - Encrypted Channel
  - Symmetric Cryptography
  - Asymmetric Cryptography
- T1544 - Ingress Tool Transfer
- T1509 - Non-Standard Port
- T1644 - Out of Band Data
- T1481 - Web Service
  - Dead Drop Resolver
  - Bidirectional Communication
  - One-Way Communication

ID:TA0036 - Exfiltration
- Exfiltration Over Unencrypted Non-C2 Protocol
  - T1639 - Exfiltration Over Alternative Protocol
- T1646 - Exfiltration Over C2 Channel

ID:TA0034 - Impact
- T1640 - Account Access Removal
- T1616 - Call Control
- T1471 - Data Encrypted for Impact
- Transmitted Data Manipulation
  - T1641 - Data Manipulation
- T1642 - Endpoint Denial of Service
- T1643 - Generate Traffic from Victim
- T1516 - Input Injection
- T1464 - Network Denial of Service
- T1582 - SMS Control

ID:TA0038 - Network Effects
The adversary is trying to intercept or manipulate network traffic to or from a device

ID:TA0039 - Remote Service Effects
The adversary is trying to control or monitor the device using remote services