Mandrake, Software S0485 | MITRE ATT&CK®

Archived: 2026-04-05 14:16:21 UTC

Mobile T1517 Access Notifications

Mandrake can capture all device notifications and hide notifications from the user.[1]

Mobile T1407 Download New Code at Runtime

Mandrake can download its second (Loader) and third (Core) stages after the dropper is installed.[1]

Mobile T1637 .001 Dynamic Resolution: Domain Generation Algorithms

Mandrake has used domain generation algorithms.[1]

Mobile T1541 Foreground Persistence

Mandrake uses foreground persistence to keep a service running. It shows the user a transparent notification to evade detection.[1]

Mobile T1628 .001 Hide Artifacts: Suppress Application Icon

Mandrake can hide its icon on older Android versions.[1]

Mobile T1629 .001 Impair Defenses: Prevent Application Removal

Mandrake can abuse device administrator permissions to ensure that it cannot be uninstalled until its permissions are revoked.[1]

.003 Impair Defenses: Disable or Modify Tools

Mandrake can disable Play Protect.[1]

Mobile T1630 .002 Indicator Removal on Host: File Deletion

Mandrake can delete all data from an infected device.[1]

Mobile T1544 Ingress Tool Transfer

Mandrake can install attacker-specified components or applications.[1]

Mobile T1417 .002 Input Capture: GUI Input Capture

Mandrake can manipulate visual components to trick the user into granting dangerous permissions, and can use phishing overlays and JavaScript injection to capture credentials.[1]

Mobile T1516 Input Injection

Mandrake abuses the accessibility service to prevent removing administrator permissions, accessibility permissions, and to set itself as the default SMS handler.[1]

Mobile T1430 Location Tracking

Mandrake can collect the device's location.[1]

Mobile T1655 .001 Masquerading: Match Legitimate Name or Location

Mandrake can mimic an app called "Storage Settings" if it cannot hide its icon.[1]

Mobile T1509 Non-Standard Port

Mandrake has communicated with the C2 server over TCP port 7777.[1]

Mobile T1406 Obfuscated Files or Information

Mandrake obfuscates its hardcoded C2 URLs.[1]

Mobile T1636 .003 Protected User Data: Contact List

Mandrake can access the device's contact list.[1]

.004 Protected User Data: SMS Messages

Mandrake can access SMS messages.[1]

Mobile T1513 Screen Capture

Mandrake can record the screen.[1]

Mobile T1582 SMS Control

Mandrake can block, forward, hide, and send SMS messages.[1]

Mobile T1418 Software Discovery

Mandrake can obtain a list of installed applications.[1]

Mobile T1409 Stored Application Data

Mandrake can collect all accounts stored on the device.[1]

Mobile T1632 .001 Subvert Trust Controls: Code Signing Policy Modification

Mandrake can enable app installation from unknown sources.[1]

Mobile T1426 System Information Discovery

Mandrake can access device configuration information and status, including Android version, battery level, device model, country, and SIM operator.[1]

Mobile T1633 .001 Virtualization/Sandbox Evasion: System Checks

Mandrake can evade automated analysis environments by requiring a CAPTCHA on launch that will prevent the application from running if not passed. It also checks for indications that it is running in an emulator.[1]

Mobile T1481 .002 Web Service: Bidirectional Communication

Mandrake has used Firebase for C2.[1]
