BRATA, Software S1094 | MITRE ATT&CK®

Archived: 2026-04-05 14:14:54 UTC

Mobile T1437 .001 Application Layer Protocol: Web Protocols

BRATA can use both HTTP and WebSockets to communicate with the C2 server.[2]

Mobile T1532 Archive Collected Data

BRATA has compressed data with the `zlib` library before exfiltration.[2]

Mobile T1616 Call Control

BRATA can hide incoming calls by setting ring volume to 0 and showing a blank screen overlay.[3]

Mobile T1662 Data Destruction

BRATA can perform a factory reset.[2]

Mobile T1533 Data from Local System

BRATA has collected account information from compromised devices.[1]

Mobile T1641 .001 Data Manipulation: Transmitted Data Manipulation

BRATA has injected string contents into the device clipboard.[3]

Mobile T1407 Download New Code at Runtime

BRATA has used an initial dropper to download an additional malicious application, and downloads its configuration file from the C2 server.[2][3]

Mobile T1627 .001 Execution Guardrails: Geofencing

BRATA has performed country and language checks.[3]

Mobile T1646 Exfiltration Over C2 Channel

BRATA has exfiltrated data to the C2 server using HTTP requests.[2]

Mobile T1664 Exploitation for Initial Access

BRATA has abused WhatsApp vulnerability CVE-2019-3568 to achieve initial access.[1]

Mobile T1628 .002 Hide Artifacts: User Evasion

BRATA can turn off or fake turning off the screen while performing malicious activities.[1]

Mobile T1629 .003 Impair Defenses: Disable or Modify Tools

BRATA can remove installed antivirus applications as well as disable Google Play Protect.[2][3]

Mobile T1630 .001 Indicator Removal on Host: Uninstall Malicious Application

BRATA can uninstall itself and remove traces of infection.[1][3]

Mobile T1417 .001 Input Capture: Keylogging

BRATA can log device keystrokes.[1][2][3]

.002 Input Capture: GUI Input Capture

BRATA can use tailored overlay pages to steal PINs for banking applications.[2]

Mobile T1516 Input Injection

BRATA can insert a given string of text into a data field. BRATA can abuse the Accessibility Service to interact with other installed applications and inject screen taps to grant permissions.[1][3]

Mobile T1430 Location Tracking

BRATA can track the device's location.[2]

Mobile T1461 Lockscreen Bypass

BRATA can request the user unlock the device, or remotely unlock the device.[1]

Mobile T1655 .001 Masquerading: Match Legitimate Name or Location

BRATA has masqueraded as legitimate WhatsApp updates and app security scanners.[1][3]

Mobile T1406 Obfuscated Files or Information

BRATA has employed code obfuscation and encryption of configuration files.[2][3]

.002 Software Packing

BRATA has utilized commercial software packers.[3]

Mobile T1660 Phishing

BRATA has been distributed using phishing techniques, such as push notifications from compromised websites.[1]

Mobile T1663 Remote Access Software

BRATA can view a device through VNC.[2]

Mobile T1513 Screen Capture

BRATA can capture and send real-time screen output.[1][3]

Mobile T1418 .001 Software Discovery: Security Software Discovery

BRATA can search for specifically installed security applications.[2]

Mobile T1426 System Information Discovery

BRATA can retrieve Android system and hardware information.[1]

Mobile T1633 .001 Virtualization/Sandbox Evasion: System Checks

BRATA can check to see if it has been installed in a virtual environment.[3]
