

CarbonSteal, Software S0529 | MITRE ATT&CK®

Archived: 2026-04-05 17:27:36 UTC

Mobile [T1429 Audio Capture](#)

[CarbonSteal](#) can remotely capture device audio. ^[1]

Mobile [T1616 Call Control](#)

[CarbonSteal](#) can silently accept an incoming phone call. ^[1]

Mobile [T1407 Download New Code at Runtime](#)

[CarbonSteal](#) can dynamically load additional functionality. ^[1]

Mobile [T1521 .002 Encrypted Channel: Asymmetric Cryptography](#)

[CarbonSteal](#) has performed rudimentary SSL certificate validation to verify C2 server authenticity before establishing a SSL connection. ^[1]

Mobile [T1420 File and Directory Discovery](#)

[CarbonSteal](#) has searched device storage for various files, including .amr files (audio recordings) and superuser binaries. ^[1]

Mobile [T1630 .002 Indicator Removal on Host: File Deletion](#)

[CarbonSteal](#) has deleted call log entries coming from known C2 sources. ^[1]

Mobile [T1430 Location Tracking](#)

[CarbonSteal](#) can access the device's location and track the device over time. ^[1]

Mobile [T1655 .001 Masquerading: Match Legitimate Name or Location](#)

[CarbonSteal](#) has impersonated several apps, including official Google apps, chat apps, VPN apps, and popular games. ^[1]

Mobile [T1575 Native API](#)

[CarbonSteal](#) has seen native libraries used in some reported samples ^[1]

Mobile [T1406 Obfuscated Files or Information](#)

[CarbonSteal](#) has used incorrect file extensions and encryption to hide most of its assets, including secondary APKs, configuration files, and JAR or DEX files. ^[1]

Mobile [T1644 Out of Band Data](#)

[CarbonSteal](#) has used specially crafted SMS messages to control the target device.^[1]

Mobile [T1636 .004 Protected User Data: SMS Messages](#)

[CarbonSteal](#) can access the device's SMS and MMS messages.^[1]

Mobile [T1418 Software Discovery](#)

[CarbonSteal](#) has looked for specific applications, such as MiCode.^[1]

Mobile [T1409 Stored Application Data](#)

[CarbonSteal](#) can collect notes and data from the MiCode app.^[1]

Mobile [T1426 System Information Discovery](#)

[CarbonSteal](#) has gathered device metadata, including model, manufacturer, SD card size, disk usage, memory, CPU, and serial number.^[1]

Mobile [T1422 System Network Configuration Discovery](#)

[CarbonSteal](#) has collected device network information, including 16-bit GSM Cell Identity, 16-bit Location Area Code, Mobile Country Code (MCC), and Mobile Network Code (MNC). [CarbonSteal](#) has also called `netcfg` to get stats.^[1]

[.001 Internet Connection Discovery](#)

[CarbonSteal](#) has gathered device metadata, including model, manufacturer, SD card size, disk usage, memory, CPU, and serial number.^[1]

Source: <https://attack.mitre.org/software/S0529/>