

BusyGasper, Software S0655 | MITRE ATT&CK®

Archived: 2026-04-05 16:38:21 UTC

Mobile [T1429 Audio Capture](#)

[BusyGasper](#) can record audio.^[1]

Mobile [T1616 Call Control](#)

[BusyGasper](#) can open a hidden menu when a specific phone number is called from the infected device.^[1]

Mobile [T1623 .001 Command and Scripting Interpreter: Unix Shell](#)

[BusyGasper](#) can run shell commands.^[1]

Mobile [T1645 Compromise Client Software Binary](#)

[BusyGasper](#) can abuse existing root access to copy components into the system partition.^[1]

Mobile [T1533 Data from Local System](#)

[BusyGasper](#) can collect images stored on the device and browser history.^[1]

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

[BusyGasper](#) can download a payload or updates from either its C2 server or email attachments in the adversary's inbox.^[1]

Mobile [T1639 .001 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol](#)

[BusyGasper](#) can download text files with commands from an FTP server and exfiltrate data via email.^[1]

Mobile [T1628 .001 Hide Artifacts: Suppress Application Icon](#)

[BusyGasper](#) can hide its icon.^[1]

[.002 Hide Artifacts: User Evasion](#)

[BusyGasper](#) can utilize the device's sensors to determine when the device is in use and subsequently hide malicious activity. When active, it attempts to hide its malicious activity by turning the screen's brightness as low as possible and muting the device.^[1]

Mobile [T1417 .001 Input Capture: Keylogging](#)

[BusyGasper](#) can collect every user screen tap and compare the input to a hardcoded list of coordinates to translate the input to a character.^[1]

Mobile [T1430 Location Tracking](#)

[BusyGasper](#) can collect the device's location information based on cellular network or GPS coordinates.^[1]

Mobile [T1644 Out of Band Data](#)

[BusyGasper](#) can perform actions when one of two hardcoded magic SMS strings is received.^[1]

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

[BusyGasper](#) can collect SMS messages.^[1]

Mobile [T1513 Screen Capture](#)

[BusyGasper](#) can use its keylogger module to take screenshots of the area of the screen that the user tapped.^[1]

Mobile [T1582 SMS Control](#)

[BusyGasper](#) can send an SMS message after the device boots, messages containing logs, messages to adversary-specified numbers with custom content, and can delete all SMS messages on the device.^[1]

Mobile [T1409 Stored Application Data](#)

[BusyGasper](#) can collect data from messaging applications, including WhatsApp, Viber, and Facebook.^[1]

Mobile [T1512 Video Capture](#)

[BusyGasper](#) can record from the device's camera.^[1]

Mobile [T1481 .002 Web Service: Bidirectional Communication](#)

[BusyGasper](#) can be controlled via IRC using freenode.net servers.^[1]

Source: <https://attack.mitre.org/software/S0655>