

HenBox, Software S0544 | MITRE ATT&CK®

Archived: 2026-04-05 17:43:01 UTC

Domain	ID	Name	Use
Mobile	T1429	Audio Capture	HenBox can access the device's microphone. ^[1]
Mobile	T1623	Command and Scripting Interpreter: Unix Shell	HenBox can run commands as root. ^[1]
Mobile	T1533	Data from Local System	HenBox can steal data from various sources, including chat, communication, and social media apps. ^[1]
Mobile	T1407	Download New Code at Runtime	HenBox can load additional Dalvik code while running. ^[1]
Mobile	T1624	Event Triggered Execution: Broadcast Receivers	HenBox has registered several broadcast receivers. ^[1]
Mobile	T1430	Location Tracking	HenBox can track the device's location. ^[1]
Mobile	T1655	Masquerading: Match Legitimate Name or Location	HenBox has masqueraded as VPN and Android system apps. ^[1]
Mobile	T1575	Native API	HenBox has contained native libraries. ^[1]
Mobile	T1406	Obfuscated Files or Information	HenBox has obfuscated components using XOR, ZIP with a single-byte key or ZIP/Zlib compression wrapped with RC4 encryption. ^[1]

Domain	ID	Name	Use
Mobile	T1424	Process Discovery	HenBox can obtain a list of running processes. ^[1]
Mobile	T1636	Protected User Data: Call Log	HenBox has collected all outgoing phone numbers that start with "86". ^[1]
		Protected User Data: Contact List	HenBox can access the device's contact list. ^[1]
		Protected User Data: SMS Messages	HenBox can intercept SMS messages. ^[1]
Mobile	T1418	Software Discovery	HenBox can obtain a list of running apps. ^[1]
Mobile	T1426	System Information Discovery	HenBox can collect device information and can check if the device is running MIUI on a Xiaomi device. ^[1]
Mobile	T1512	Video Capture	HenBox can access the device's camera. ^[1]
Mobile	T1633	Virtualization/Sandbox Evasion: System Checks	HenBox can detect if the app is running on an emulator. ^[1]

Source: https://attack.mitre.org/software/S0544/