

MobileOrder, Software S0079 | MITRE ATT&CK®

Archived: 2026-04-05 15:41:57 UTC

Domain	ID	Name	Use
Enterprise	T1217	Browser Information Discovery	MobileOrder has a command to upload to its C2 server victim browser bookmarks. ^[1]
Enterprise	T1005	Data from Local System	MobileOrder exfiltrates data collected from the victim mobile device. ^[1]
Enterprise	T1041	Exfiltration Over C2 Channel	MobileOrder exfiltrates data to its C2 server over the same protocol as C2 communications. ^[1]
Enterprise	T1083	File and Directory Discovery	MobileOrder has a command to upload to its C2 server information about files on the victim mobile device, including SD card size, installed app list, SMS content, contacts, and calling history. ^[1]
Enterprise	T1105	Ingress Tool Transfer	MobileOrder has a command to download a file from the C2 server to the victim mobile device's SD card. ^[1]
Enterprise	T1057	Process Discovery	MobileOrder has a command to upload information about all running processes to its C2 server. ^[1]
Enterprise	T1082	System Information Discovery	MobileOrder has a command to upload to its C2 server victim mobile device information, including IMEI, IMSI, SIM card serial number, phone number, Android version, and other information. ^[1]

Source: <https://attack.mitre.org/software/S0079/>