Corona Updates, Software S0425 | MITRE ATT&CK®

Archived: 2026-04-05 16:14:41 UTC

Domain	ID		Name	Use
Mobile	T1517		Access Notifications	Corona Updates can collect messages from GSM, WhatsApp, Telegram, Facebook, and Threema by reading the application's notification content.[1]
Mobile	T1437	.001	Application Layer Protocol: Web Protocols	Corona Updates communicates with the C2 server using HTTP requests.[1]
Mobile	T1429		Audio Capture	Corona Updates can record MP4 files and monitor calls.[1]
Mobile	T1533		Data from Local System	Corona Updates can collect voice notes, device accounts, and gallery images.[1]
Mobile	T1639	.001	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	Corona Updates has exfiltrated data using FTP.[1]
Mobile	T1430		Location Tracking	Corona Updates can track the device's location.[1]
Mobile	T1636	.002	Protected User Data: Call Log	Corona Updates can collect the device's call log.[1]
		.003	Protected User Data: Contact List	Corona Updates can collect device contacts.[1]

Domain	ID		Name	Use
		.004	Protected User Data: SMS Messages	Corona Updates can collect SMS messages. [1]
Mobile	T1582		SMS Control	Corona Updates can send SMS messages.[1]
Mobile	T1426		System Information Discovery	Corona Updates can collect various pieces of device information, including OS version, phone model, and manufacturer.[1]
Mobile	T1422		System Network Configuration Discovery	Corona Updates can collect device network configuration information, such as Wi-Fi SSID and IMSI.[1]
		.001	Internet Connection Discovery	Corona Updates can collect device network configuration information, such as Wi-Fi SSID and IMSI.[1]
		.002	Wi-Fi Discovery	Corona Updates can collect device network configuration information, such as Wi-Fi SSID and IMSI.[1]
Mobile	T1512		Video Capture	Corona Updates can take pictures using the camera and can record MP4 files.[1]

Source: https://attack.mitre.org/software/S0425