RedDrop, Software S0326 | MITRE ATT&CK®

Archived: 2026-04-02 10:35:55 UTC

Domain	ID		Name	Use
Mobile	T1437	.001	Application Layer Protocol: Web Protocols	RedDrop uses HTTP requests for C2 communication.[1]
Mobile	T1429		Audio Capture	RedDrop captures live recordings of the device's surroundings.[1]
Mobile	T1646		Exfiltration Over C2 Channel	RedDrop uses standard HTTP for exfiltration.[1]
Mobile	T1643		Generate Traffic from Victim	RedDrop tricks the user into sending SMS messages to premium services and then deletes those messages.[1]
Mobile	T1544		Ingress Tool Transfer	RedDrop uses ads or other links within websites to encourage users to download the malicious apps using a complex content distribution network (CDN) and series of network redirects. RedDrop also downloads additional components (APKs, JAR files) from different C2 servers.[1]
Mobile	T1426		System Information Discovery	RedDrop exfiltrates details of the victim device operating system and manufacturer.[1]
Mobile	T1422		System Network Configuration Discovery	RedDrop collects and exfiltrates information including IMEI, IMSI, MNC, MCC, nearby Wi-Fi networks, and other device and SIM-related info.[1]

Domain	ID		Name	Use
		.001	Internet Connection Discovery	RedDrop collects and exfiltrates information including IMEI, IMSI, MNC, MCC, nearby Wi-Fi networks, and other device and SIM-related info.[1]
		.002	Wi-Fi Discovery	RedDrop collects and exfiltrates information including IMEI, IMSI, MNC, MCC, nearby Wi-Fi networks, and other device and SIM-related info.[1]
