Drinik, Software S1054 | MITRE ATT&CK®

Archived: 2026-04-05 16:56:17 UTC

Domain	ID		Name	Use
Mobile	T1437		Application Layer Protocol	Drinik has code to use Firebase Cloud Messaging for receiving C2 instructions.[1]
Mobile	T1616		Call Control	Drinik can use the Android `CallScreeningService` to silently block incoming calls.[1]
Mobile	T1533		Data from Local System	Drinik can request the `READ_EXTERNAL_STORAGE` and `WRITE_EXTERNAL_STORAGE` Android permissions.[1]
Mobile	T1646		Exfiltration Over C2 Channel	Drinik can send stolen data back to the C2 server.[1]
Mobile	T1541		Foreground Persistence	Drinik has C2 commands that can move the malware in and out of the foreground. [1]
Mobile	T1628	.001	Hide Artifacts: Suppress Application Icon	Drinik can hide its application icon.[1]
Mobile	T1629	.003	Impair Defenses: Disable or Modify Tools	Drinik can use Accessibility Services to disable Google Play Protect.[1]
Mobile	T1417	.001	Input Capture: Keylogging	Drinik can use keylogging to steal user banking credentials.[1]
		.002	Input Capture: GUI Input Capture	Drinik can use overlays to steal user banking credentials entered into legitimate sites.[1]

Domain	ID		Name	Use
Mobile	T1406		Obfuscated Files or Information	Drinik has used custom encryption to hide strings, potentially to evade antivirus products.[1]
Mobile	T1636	.002	Protected User Data: Call Log	Drinik can request the `READ_CALL_LOG` permission.[1]
		.004	Protected User Data: SMS Messages	Drinik can collect user SMS messages.[1]
Mobile	T1513		Screen Capture	Drinik can record the screen via the `MediaProjection` library to harvest user credentials, including biometric PINs.[1]
Mobile	T1582		SMS Control	Drinik can steal incoming SMS messages and send SMS messages from compromised devices. [1]
