Skygofree, Software S0327 | MITRE ATT&CK®

Archived: 2026-04-05 15:51:04 UTC

Domain	ID		Name	Use
Mobile	T1437	.001	Application Layer Protocol: Web Protocols	Skygofree can be controlled via HTTP, XMPP, FirebaseCloudMessaging, or GoogleCloudMessaging in older versions.[1]
Mobile	T1429		Audio Capture	Skygofree can record audio via the microphone when an infected device is in a specified location.[1]
Mobile	T1407		Download New Code at Runtime	Skygofree can download executable code from the C2 server after the implant starts or after a specific command.[1]
Mobile	T1404		Exploitation for Privilege Escalation	Skygofree has the capability to exploit several known vulnerabilities and escalate privileges.[1]
Mobile	T1430		Location Tracking	Skygofree can track the device's location.[1]
Mobile	T1644		Out of Band Data	Skygofree can be controlled via binary SMS.[1]
Mobile	T1409		Stored Application Data	Skygofree has a capability to obtain files from other installed applications.[1]
Mobile	T1512		Video Capture	Skygofree can record video or capture photos when an infected device is in a specified location.[1]

Source: https://attack.mitre.org/software/S0327