Android/SpyAgent, Software S1214 | MITRE ATT&CK®

Archived: 2026-04-05 16:29:04 UTC

Domain	ID		Name	Use
Mobile	T1616		Call Control	Android/SpyAgent can execute an automated phone call.[1]
Mobile	T1629	.003	Impair Defenses: Disable or Modify Tools	Android/SpyAgent has attempted to detect anti-spam call applications.[1]
Mobile	T1655	.001	Masquerading: Match Legitimate Name or Location	Android/SpyAgent has used the official icon of the Korean police application and the package name "kpo," which contain references related to the Korean police.[1]
Mobile	T1406		Obfuscated Files or Information	Android/SpyAgent has used the Tencent packer to hide its malicious payload.[1]
Mobile	T1636	.004	Protected User Data: SMS Messages	Android/SpyAgent has exfiltrated SMS and MMS messages.[1]
Mobile	T1422		System Network Configuration Discovery	Android/SpyAgent has collected device network information, such as the IMEI and the phone number.[1]
Mobile	T1481		Web Service	Android/SpyAgent's payload has obtained the C2 address via Twitter accounts.[1]
		.001	Dead Drop Resolver	Android/SpyAgent has used the Tencent Push Notification Service to receive commands from the C2 server.[1]

Source: https://attack.mitre.org/software/S1214