Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:04:20 UTC

Tool: Antidot

Names	Antidot
Category	Malware
Type	Banking trojan
Description	(Cyble) A new Android Banking Trojan, “Antidot,” masquerading as a Google Play update application, displays fake Google Play update pages in multiple languages, indicating a wide range of targets. Antidot incorporates a range of malicious features, including overlay attacks and keylogging, allowing it to compromise devices and harvest sensitive information. Antidot maintains communication with its Command and Control (C&C) server through WebSocket, enabling real-time, bidirectional interaction for executing commands. The malware executes a wide range of commands received from the C&C server, including collecting SMS messages, initiating USSD requests, and even remotely controlling device features such as the camera and screen lock. Antidot implemented VNC using MediaProjection to remotely control infected devices.
Information	<https://cyble.com/blog/new-antidot-android-banking-trojan-masquerading-as-google-play-updates/>

Last change to this tool card: 18 June 2024

Download this tool card in JSON format

All groups using tool Antidot

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

1 group listed (0 APT, 0 other, 1 unknown)