Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:09:26 UTC

Tool: AridSpy

Names	AridSpy
Category	Malware
Type	Backdoor
Description	(ESET) ESET Research discovered three-stage Android malware, which we named AridSpy, being distributed via five dedicated websites. AridSpy's code is in some cases bundled into applications that provide legitimate functionality. While the first stage of AridSpy has been documented previously, here we also provide a full analysis of its previously unknown later stages. AridSpy is a remotely controlled trojan that focuses on user data espionage. We detected six occurrences of AridSpy, in Palestine and Egypt. We attribute AridSpy with medium confidence to the Arid Viper APT group.
Information	<https://www.welivesecurity.com/en/eset-research/arid-viper-poisons-android-apps-with-aridspy/> <https://www.zimperium.com/blog/new-advanced-android-malware-posing-as-system-update/>

Last change to this tool card: 19 June 2024

Download this tool card in JSON format

All groups using tool AridSpy

Changed	Name	Country	Observed	
APT groups				
	Desert Falcons	[Gaza]	2011-Oct 2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=45b4cf25-3d0c-4a30-982a-00daa6fc4c3d