Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:52:06 UTC

Tool: SpyC23

Names	SpyC23
Category	Malware
Type	Backdoor, Info stealer, Downloader, Exfiltration
Description	(SentinelLabs) The Arid Viper group has a long history of using mobile malware, including at least four Android spyware families and one short-lived iOS implant, Phenakite. The SpyC23 Android malware family has existed since at least 2019, though shared code between the Arid Viper spyware families dates back to 2017. It was first reported in 2020 by ESET in a campaign where the actor used a third-party app store to distribute weaponized Android packages (APK). That campaign featured several apps designed to mimic Telegram and Android application update managers.
Information	<https://www.sentinelone.com/labs/arid-viper-apts-nest-of-spyc23-malware-continues-to-target-android-devices/> <https://www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1195>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.spyc23>

Last change to this tool card: 28 June 2025

Download this tool card in JSON format

All groups using tool SpyC23

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

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