Desert Scorpion - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:40:06 UTC

Tool: Desert Scorpion

Names	Desert Scorpion
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Lookout) The malicious capabilities observed in the second stage include the following: • Upload attacker-specified files to C2 servers • Get list of installed applications • Get device metadata • Inspect itself to get a list of launchable activities • Retrieves PDF, txt, doc, xls, xlsx, ppt, pptx files found on external storage • Send SMS • Retrieve text messages • Track device location • Handle limited attacker commands via out of band text messages • Record surrounding audio • Record calls • Record video • Retrieve account information such as email addresses • Retrieve contacts • Removes copies of itself if any additional APKs are downloaded to external storage. • Call an attacker-specified number • Uninstall apps • Check if a device is rooted • Hide its icon • Retrieve list of files on external storage • If running on a Huawei device it will attempt to add itself to the protected list of apps able to run with the screen off • Encrypts some exfiltrated data
Information	<https://blog.lookout.com/desert-scorpion-google-play>

MITRE ATT&CK	<https://attack.mitre.org/software/S0505/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Desert Scorpion

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=98d061ee-cea8-4987-9ae5-554d09404413