Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:52:29 UTC

Tool: PlainGnome

Names	PlainGnome
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer
Description	(Lookout) PlainGnome consists of a two-stage deployment in which a very minimal first stage drops a malicious APK once it’s installed. While the first and second stages use some variation on the Telegram package name, the actual functionality presented to the user is essentially the same as that observed in previous BoneSpy samples using the “image gallery” theme. This lure theme continued through most of PlainGnome’s deployment throughout 2024.
Information	<https://www.lookout.com/threat-intelligence/article/gamaredon-russian-android-surveillanceware>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool PlainGnome

Changed	Name	Country	Observed	
APT groups				
	Gamaredon Group		2013-Feb 2025	

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