Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:40:36 UTC

Tool: DragonEgg

Names	DragonEgg LightSpy
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Credential stealer, Exfiltration
Description	(Lookout) Similar to WyrmSpy, DragonEgg appears to rely on additional payloads to implement the full scale of its surveillance functionality. At launch, the malware acquires — either from C2 infrastructure or a bundled file within the APK — a payload often named “smallmload.jar” which attempts to acquire and launch additional functionality. Like WyrmSpy, the DragonEgg samples request extensive permissions for services that are not directly exploited in the core app. We suspect that by trojanizing legitimate chat apps like Telegram, APT41 is trying to remain inconspicuous while requesting access to extensive device data. Messaging apps typically request access to sensitive device data, and by hiding its surveillance functionality within a large, fully-functional app, the threat actor is better able to remain inconspicuous while the app is running on the device or statically analyzed by a researcher.
Information	<https://www.lookout.com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41> <https://www.threatfabric.com/blogs/lightspy-mapt-mobile-payment-system-attack>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.dragonegg>

Last change to this tool card: 13 October 2023

Download this tool card in JSON format

All groups using tool DragonEgg

Changed	Name	Country	Observed

APT groups

	APT 41		2012-Jul 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b92e627c-2e0f-4d95-90f1-798028d00ba1