Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:12:40 UTC

Tool: WyrmSpy

Names	WyrmSpy AndroidControl
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Credential stealer, Exfiltration
Description	(Lookout) After it's installed and launched, WyrmSpy uses known rooting tools to gain escalated privileges to the device and perform surveillance activities specified by commands received from its C2 servers. These commands include instructing the malware to upload log files, photos stored on the device, and acquire device location using the Baidu Location library. Although we were not able to acquire additional modules from the C2 infrastructure at the time of discovery, we assess with high confidence that a secondary payload is used by the malware to perform additional surveillance functionality. This is based on the permissions that WyrmSpy obtains but does not use in the code contained in the app, which indicates abilities to exfiltrate additional data, such as SMS and audio recordings. Configuration files used by the malware to execute instructions received by the C2 further support this hypothesis, with references to "AudioRecord" and "Files" set to true or false based on received commands.
Information	<https://www.lookout.com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.wyrmspy>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool WyrmSpy

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=fc5f26a3-382f-498c-982d-b9a165c301bf