Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:10:37 UTC

Tool: SpyWaller

Names	SpyWaller
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Lookout) The latest SpyWaller variants are capable of accessing the sensitive data of over 20 different apps, in addition to being able to record calls, capture surrounding audio, track a device's location, take pictures with the camera, and retrieve a list of installed packages. Initial infection is followed by requests to command and control infrastructure for the latest native code component that contains the bulk of SpyWaller's surveillanceware functionality. While we found the native code that is bundled up in the app is somewhat obfuscated, the latest binary served up by attacker infrastructure was not, and contains new code to target Facebook and Google Hangouts. These improvements in capability suggest that the actor behind SpyWaller may be deploying it in campaigns outside of China, where we believe the majority of previous activity to have been conducted.
Information	<https://blog.lookout.com/spywaller-mobile-threat>

Last change to this tool card: 02 July 2020

Download this tool card in JSON format

All groups using tool SpyWaller

Changed	Name	Country	Observed	
APT groups				
	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3153ac82-3419-4d2b-8702-1e621e0bab17