Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:41:20 UTC

Tool: lightSpy

Names	lightSpy
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Trend Micro) The iOS malware, which we named 'lightSpy' (detected by Trend Micro as IOS_LightSpy.A), is a modular backdoor that allowed the attacker to remotely execute a shell command and manipulate files on the infected device. It is also implemented with several functionalities through different modules for exfiltrating data from the infected device including: • Hardware information • Contacts • Keychain • SMS messages • Phone call history • GPS location • Connected Wi-Fi history • Browser history of Safari and Chrome The malware also reports the surrounding environment of the device by: • Scanning local network IP address • Scanning available Wi-Fi network The campaign also employs modules specifically designed to exfiltrate data from popular messenger applications such as QQ, WeChat, and Telegram.
Information	<https://documents.trendmicro.com/assets/Tech-Brief-Operation-Poisoned-News-Hong-Kong-Users-Targeted-with-Mobile-Malware-via-Local-News-Links.pdf> <https://securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407/> <https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/> <https://blogs.blackberry.com/en/2024/04/lightspy-returns-renewed-espionage-campaign-targets-southern-asia-possibly-india>

	<https://www.threatfabric.com/blogs/lightspy-implant-for-macos> <https://www.threatfabric.com/blogs/lightspy-implant-for-ios> <https://www.lookout.com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41> <https://blogs.blackberry.com/en/2024/11/lightspy-apt41-deploys-advanced-deepdata-framework-in-targeted-southern-asia-espionage-campaign> <https://hunt.io/blog/lightspy-malware-targets-facebook-instagram>
MITRE ATT&CK	<https://attack.mitre.org/software/S1185>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ios.lightspy>

Last change to this tool card: 28 June 2025

Download this tool card in JSON format

All groups using tool lightSpy

Changed	Name	Country	Observed	
APT groups				
	Operation Poisoned News, TwoSail Junk		2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=4c9d4f77-ee82-4452-b187-84072275951e