# Operation Poisoned News, TwoSail Junk

Archived: 2026-04-05 23:02:23 UTC



## APT group: Operation Poisoned News, TwoSail Junk

| | |
|---|---|
| Names | Operation Poisoned News *(Trend Micro)*<br>TwoSail Junk *(Kaspersky)* |
| Country | China |
| Motivation | Information theft and espionage |
| First seen | 2020 |
| Description | (Kaspersky) A watering hole was discovered on January 10, 2020 utilizing a full remote iOS exploit chain to deploy a feature-rich implant named LightSpy. The site appears to have been designed to target users in Hong Kong based on the content of the landing page. Since the initial activity, we released two private reports exhaustively detailing spread, exploits, infrastructure and LightSpy implants.<br><br>We are temporarily calling this APT group “TwoSail Junk”. Currently, we have hints from known backdoor callbacks to infrastructure about clustering this campaign with previous activity. And we are working with colleagues to tie LightSpy with prior activity from a long running Chinese-speaking APT group, previously reported on as Lotus Blossom, Spring Dragon, Thrip, known for their Lotus Elise and Evora backdoor malware. Considering that this LightSpy activity has been disclosed publicly by our colleagues from TrendMicro, we would like to further contribute missing information to the story without duplicating content. And, in our quest to secure technologies for a better future, we reported the malware and activity to Apple and other relevant companies. |
| Observed | Countries: Hong Kong. |
| Tools used | dmsSpy, lightSpy. |
| Information | <https://securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407/><br><https://documents.trendmicro.com/assets/Tech-Brief-Operation-Poisoned-News-Hong-Kong-Users-Targeted-with-Mobile-Malware-via-Local-News-Links.pdf> |

Last change to this card: 01 May 2020

Download this actor card in PDF or JSON format

---