# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:40:07 UTC



## Tool: MOONSHINE

| | |
|---|---|
| Names | MOONSHINE |
| Category | Malware |
| Type | Backdoor, Info stealer |
| Description | (Citizen Lab) MOONSHINE is designed for stealthy rootless operation, by exploiting popular legitimate Android apps with built-in browsers that request sensitive permissions. MOONSHINE obtains persistence by overwriting an infrequently used shared library (.so) file in one of these apps with itself. When a targeted user opens the legitimate app after exploitation, the app loads the shared library into memory, which causes the spyware to activate. While code in subsequent stages of MOONSHINE suggests that it can be deployed against four apps (Facebook, Facebook Messenger, WeChat, and QQ), the exploit site we tested against did not deliver any exploits for WeChat or QQ User-Agent headers. |
| Information | <https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/> <https://www.trendmicro.com/en_us/research/24/l/earth-minotaur.html> |

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

### All groups using tool MOONSHINE

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Earth Minotaur | | 2019 | |
| | Poison Carp, Evil Eye | | 2018-Jun 2023 | |

*2 groups listed (2 APT, 0 other, 0 unknown)*

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2ea4f916-78e7-4c96-b24d-72a28372ea2c