

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:00:57 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool BoneSpy

Tool: BoneSpy

| | |
|-------------|--|
| Names | BoneSpy |
| Category | Malware |
| Type | Reconnaissance , Backdoor , Info stealer |
| Description | (Lookout) The BoneSpy family showed evidence of continuous development between roughly January and October 2022, after which samples began using consistent lure theming and code structure. Earlier samples from between January and September 2022 used a variety of trojanized apps such as battery charge monitoring apps, photo-gallery apps, a fake Samsung Knox app, and trojanized Telegram apps. Later, Gamaredon largely shifted to using trojanized, fully functional Telegram samples titled as “Beta” versions. |
| Information | < https://www.lookout.com/threat-intelligence/article/gamaredon-russian-android-surveillanceware > |

Last change to this tool card: 27 December 2024

Download this tool card in [JSON](#) format

All groups using tool BoneSpy

| Changed | Name | Country | Observed | |
|-------------------|---------------------------------|---|---------------|---|
| APT groups | | | | |
| | Gamaredon Group |  | 2013-Feb 2025 |  |

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=10958f58-9776-4d97-82f9-fbf37312d0d3>