# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:12:28 UTC



## Tool: AnubisSpy

| | |
|---|---|
| Names | AnubisSpy |
| Category | Malware |
| Type | Backdoor, Info stealer, Exfiltration |
| Description | (Trend Micro) AnubisSpy can steal messages (SMS), photos, videos, contacts, email accounts, calendar events, and browser histories (i.e., Chrome and Samsung Internet Browser). It can also take screenshots and record audio, including calls. It can spy on the victim through apps installed on the device, a list of which is in its configuration file that can be updated. This includes Skype, WhatsApp, Facebook, and Twitter, among others.<br><br>After the data are collected, they are encrypted and sent to the (C&C) server. AnubisSpy can also self-destruct to cover its tracks. It can run commands and delete files on the device, as well as install and uninstall Android Application Packages (APKs).<br><br>AnubisSpy has several modules, each of which has a separate role. AnubisSpy's code is well constructed, indicating the developer/s' know-how. |
| Information | <https://blog.trendmicro.com/trendlabs-security-intelligence/cyberespionage-campaign-sphinx-goes-mobile-anubisspy/><br><https://documents.trendmicro.com/assets/tech-brief-cyberespionage-campaign-sphinx-goes-mobile-with-anubisspy.pdf> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/apk.anubisspy> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:anubisspy> |

Last change to this tool card: 21 May 2020

Download this tool card in JSON format

### All groups using tool AnubisSpy

| Changed | Name | Country | Observed |
|---|---|---|---|

## APT groups

| | | | | |
|---|---|---|---|---|
| | Sphinx | [Unknown] | 2014 | |

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

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=808cf3ae-bce9-40a5-a4e9-14bb9c1c8424