Catelites (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:15:49 UTC

Catelites

Catelites Bot (identified by Avast and SfyLabs in December 2017) is an Android trojan, with ties to CronBot. Once the malicious app is installed, attackers use social engineering tricks and window overlays to get credit card details from the victim.
The distribution vector seems to be fake apps from third-party app stores (not Google Play) or via malvertisement. After installation and activation, the app creates fake Gmail, Google Play and Chrome icons. Furthermore, the malware sends a fake system notification, telling the victim that they need to re-authenticate with Google Services and ask for their credit card details to be entered.
Currently the malware has overlays for over 2,200 apps of banks and financial institutions.

References

2017-12-20 · Avast ·
New version of mobile malware Catelites possibly linked to Cron cyber gang
Catelites

2017-12-20 · YouTube · Avast
Video about Catelites Bot - Airbank Example
Catelites

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/apk.catelites