ToxicPanda (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:52:02 UTC

apk.toxic_panda (Back to overview)

ToxicPanda

ToxicPanda is an Android banking RAT first identified by Cleafy in October 2024. It shows similarity to the TgToxic campaign, but appears to be a new development rather than a derivative. The threat actors are likely Chinese speakers. ToxicPanda initially made use of hardcoded C2 domains only, but started to incorporate a DGA in late 2024.

References

2025-07-28 · BitSight · Pedro Falé
ToxicPanda: The Android Banking Trojan Targeting Europe
TgToxic ToxicPanda

2024-11-04 · Cleafy · Alessandro Strino, Federico Valentini, Michele Roviello
ToxicPanda: a new banking trojan from Asia hit Europe and LATAM
ToxicPanda

There is no Yara-Signature yet.
