

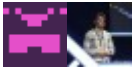
Anubis (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:57:23 UTC

Anubis

aka: BankBot, android.bankbot, android.bankspy



BleepingComputer found that Anubis will display fake phishing login forms when users open up apps for targeted platforms to steal credentials. This overlay screen will be shown over the real app's login screen to make victims think it's a legitimate login form when in reality, inputted credentials are sent to the attackers.

In the new version spotted by Lookout, Anubis now targets 394 apps and has the following capabilities:

- Recording screen activity and sound from the microphone
- Implementing a SOCKS5 proxy for covert communication and package delivery
- Capturing screenshots
- Sending mass SMS messages from the device to specified recipients
- Retrieving contacts stored on the device
- Sending, reading, deleting, and blocking notifications for SMS messages received by the device
- Scanning the device for files of interest to exfiltrate
- Locking the device screen and displaying a persistent ransom note
- Submitting USSD code requests to query bank balances
- Capturing GPS data and pedometer statistics
- Implementing a keylogger to steal credentials
- Monitoring active apps to mimic and perform overlay attacks
- Stopping malicious functionality and removing the malware from the device

References

2025-05-19 · [cocomelonc](#) ·

AIYA - Mobile malware development book. First edition

[AndroRAT](#) [Anubis](#) [CraxsRAT](#) [Dendroid](#) [FakeGram](#) [Hydra](#) [IPStorm](#) [SpyNote](#)

2022-07-11 · [Security Affairs](#) · [Pierluigi Paganini](#)

Anubis Networks is back with new C2 server

[Anubis](#)

2022-05-29 · [muha2xmad](#) · [Muhammad Hasan Ali](#)

Full Anubis android malware analysis

[Anubis](#)

2022-03-01 · [VirusTotal](#) · [VirusTotal](#)

VirusTotal's 2021 Malware Trends Report

[Anubis AsyncRAT BlackMatter Cobalt Strike DanaBot Dridex Khonsari MimiKatz Mirai Nanocore RAT Orcus RAT](#)

2021-08-27 · [0x1c3n.tech](#) · [0x1c3N](#)

Anubis Android Malware Analysis

[Anubis](#)

2021-04-28 · [ThreatFabric](#) · [ThreatFabric](#)

The Rage of Android Banking Trojans

[Anubis Gustuff Medusa](#)

2021-02-24 · [RiskIQ](#) · [Jordan Herman](#)

Turkey Dog: Cerberus and Anubis Banking Trojans Target Turkish Speakers

[Anubis Cerberus](#)

2020-12-10 · [Intel 471](#) · [Intel 471](#)

No pandas, just people: The current state of China's cybercrime underground

[Anubis SpyNote AsyncRAT Cobalt Strike Ghost RAT NjRAT](#)

2020-11-21 · [Medium Intel-Honey](#) · [Twitter \(@intel_honey\)](#)

Reversing Anubis Malware

[Anubis](#)

2020-07-04 · [N1ght-W0lf Blog](#) · [Abdallah Elshinbary](#)

Deep Analysis of Anubis Banking Malware

[Anubis](#)

2020-05-09 · [BushidoToken](#) · [BushidoToken](#)

Turkey targeted by Cerberus and Anubis Android banking Trojan campaigns

[Anubis Cerberus](#)

2020-04-23 · [Youtube \(Lukas Stefanko\)](#) · [Lukáš Štefanko](#)

Android banking Trojan Anubis | Malware demo | infected device | covid19 | targets Italy

[Anubis](#)

2020-03-26 · [Bitdefender](#) · [Liviu Arsene](#)

Android Apps and Malware Capitalize on Coronavirus

[Anubis Joker](#)

2020-02-25 · [Kaspersky Labs](#) · [Victor Chebyshev](#)

Mobile malware evolution 2019

[Anubis Asacub Dvmap FlexNet HiddenAd Marcher Sypeng Triada](#)

2020-02-01 · [ThreatFabric](#) · [ThreatFabric](#)

2020 - Year of the RAT

[Anubis Cerberus Ginp Gustuff Hydra](#)

2019-04-07 · [Eybisi](#) · [Eybisi](#)

Mobile Malware Analysis : Tricks used in Anubis

[Anubis](#)

2019-03-13 · [Pentest Blog](#) · [Ahmet Bilal Can](#)

N Ways to Unpack Mobile Malware

[Anubis](#)

2019-01-17 · [Trend Micro](#) · [Kevin Sun](#)

Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics

[Anubis](#)

2018-09-10 · [Security Boulevard](#) · [Gary Warner](#)

Android Malware Intercepts SMS 2FA: We have the Logs

[Anubis](#)

2018-08-30 · [Random RE](#) · [sysopfb](#)

Manually unpacking Anubis APK

[Anubis](#)

2018-03-13 · [PhishLabs](#) · [Joshua Shilko](#)

New Variant of BankBot Banking Trojan Ups Ante, Cashes Out on Android Users

[Anubis](#)

2017-11-21 · [ESET Research](#) · [Lukáš Štefanko](#)

New campaigns spread banking malware through Google Play

[Anubis](#)

2017-09-19 · [Fortinet](#) · [Dario Durando](#)

A Look Into The New Strain Of BankBot

[Anubis](#)

2017-07-27 · [Security Intelligence](#) · [Limor Kessem](#), [Shachar Gritzman](#)

After Big Takedown Efforts, 20 More BankBot Mobile Malware Apps Make It Into Google Play

[Anubis](#)

2017-05-30 · [Koodous](#) · [entdark](#)

Bankbot on Google Play

[Anubis](#)

2017-05-09 · [Lukáš Štefanko](#)

Tracking Android BankBot

[Anubis](#)

2017-04-26 · [Fortinet](#) · [Dario Durando](#), [David Maciejak](#)

BankBot, the Prequel

[Anubis](#)

2017-04-13 · [Koodous](#) · [Koodous Blog](#)

Decrypting Bankbot communications.

[Anubis](#)

There is no Yara-Signature yet.

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/apk.anubis>