

# ERMAC (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:18:41 UTC

apk.ermac ([Back to overview](#))

## ERMAC



According to Intel471, ERMAC, an Android banking trojan enables bad actors to determine when certain apps are launched and then overwrites the screen display to steal the user's credentials

### References

2025-08-14 · [Hunt.io](#) · [Hunt.io](#)

Hunt.io Exposes and Analyzes ERMAC V3.0 Banking Trojan Full Source Code Leak

[ERMAC](#)

2025-03-11 · [ThreatMon](#) · [Aziz Kaplan](#), [ThreatMon](#), [ThreatMon Malware Research Team](#)

New Ermac Variant - Android Banking Trojan & Botnet

[ERMAC](#)

2023-10-03 · [Twitter \(@ShilpeshTrivedi\)](#) · [Shilpesh Trivedi](#)

Tweet about possible Rebranding/Derivate for ERMAC called Rusty Droid

[ERMAC](#)

2023-09-11 · [NCC Group](#) · [Alberto Segura](#), [Joshua Kamp](#)

From ERMAC to Hook: Investigating the technical differences between two Android malware variants

[ERMAC Hook](#)

2022-12-08 · [ThreatFabric](#) · [ThreatFabric](#)

Zombinder: new obfuscation service used by Ermac, now distributed next to desktop stealers

[ERMAC Xenomorph](#)

2022-11-25 · [Resecurity](#) · [Resecurity](#)

"In The Box" - Mobile Malware Webinjects Marketplace

[Alien Cerberus Coper ERMAC Hydra](#)

2022-08-31 · [Intel 471](#) · [Intel 471 Malware Intelligence team](#)

ERMAC 2.0: Perfecting the Account Takeover

[ERMAC](#)

2022-05-25 · [cyble](#) · [Cyble Research Labs](#)

ERMAC Back In Action: Latest Version Of Android Banking Trojan Targets Over 400 Applications

[ERMAC](#)

2021-10-06 · [Twitter \(@ESETresearch\)](#) · [ESET Research](#)

Tweet on ERMAC android malware

[ERMAC](#)

2021-09-22 · [ThreatFabric](#) · [ThreatFabric](#)

ERMAC - another Cerberus reborn

[AmpleBot Cerberus ERMAC](#)

There is no Yara-Signature yet.

---

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