

Coper (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:56:59 UTC

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

Coper

aka: ExobotCompact, Octo

Coper is an Android banking trojan and RAT descended from ExobotCompact, itself a rewrite of Exobot. It uses a modular architecture, a multi-stage infection chain and (in some variants) a DGA. First observed in Colombia, it has since spread to Europe.

References

2026-01-13 · [Spamhaus](#) · [Spamhaus Malware Labs](#)

Spamhaus Botnet Threat Update July to December 2025

[Coper](#) [FluBot](#) [Joker](#) [Aisuru](#) [Mirai](#) [AsyncRAT](#) [BianLian](#) [Cobalt Strike](#) [DCRat](#) [Havoc](#) [Latrodectus](#) [PureLogs](#) [Stealer](#) [Quasar](#) [RAT](#) [Remcos](#) [Rhadamanthys](#) [Sliver](#) [ValleyRAT](#) [Venom](#) [RAT](#) [Vidar](#) [XWorm](#)

2025-07-14 · [Spamhaus](#) · [Spamhaus Malware Labs](#)

Spamhaus Botnet Threat Update January to June 2025

[Coper](#) [FluBot](#) [Hook](#) [Joker](#) [Mirai](#) [AsyncRAT](#) [BianLian](#) [BumbleBee](#) [Chaos](#) [Cobalt Strike](#) [DanaBot](#) [DCRat](#) [Havoc](#) [Latrodectus](#) [NjRAT](#) [Quasar](#) [RAT](#) [RedLine](#) [Stealer](#) [Remcos](#) [Rhadamanthys](#) [Sliver](#) [ValleyRAT](#) [WarmCookie](#) [XWorm](#)

2025-03-14 · [K7 Security](#) · [Baran S](#)

Android Banking Trojan – OctoV2, masquerading as Deepseek AI

[Coper](#)

2025-01-10 · [Spamhaus](#) · [Spamhaus Malware Labs](#)

Spamhaus Botnet Threat Update July to December 2024

[Coper](#) [FluBot](#) [Hook](#) [Mirai](#) [FAKEUPDATES](#) [AsyncRAT](#) [BianLian](#) [Brute](#) [Ratel](#) [C4](#) [Cobalt Strike](#) [DanaBot](#) [DCRat](#) [Havoc](#) [Latrodectus](#) [NjRAT](#) [Quasar](#) [RAT](#) [RedLine](#) [Stealer](#) [Remcos](#) [Rhadamanthys](#) [Sliver](#) [Stealc](#)

2024-11-21 · [Intrinsec](#) · [CTI Intrinsec](#), [Intrinsec](#)

PROSPERO & Proton66: Uncovering the links between bulletproof networks

[Coper](#) [SpyNote](#) [FAKEUPDATES](#) [GootLoader](#) [EugenLoader](#)

2024-11-20 · [Intrinsec](#) · [Equipe CTI](#)

PROSPERO & Proton66: Tracing Uncovering the links between bulletproof networks

[Coper](#) [SpyNote](#) [FAKEUPDATES](#) [GootLoader](#) [EugenLoader](#) [IcedID](#) [Matanbuchus](#) [Nokoyawa](#) [Ransomware](#) [Pikabot](#)

2024-10-10 · [DomainTools](#) · [Steve Behm](#)

Uncovering Domains Created by Octo2's Domain Generation Algorithm

[Coper](#)

2024-10-04 · [VirusBulletin](#) · [Thibault Seret](#)

Octopus Prime: it didn't turn into a truck, but a widely spread Android botnet

[Coper](#)

2024-09-24 · [ThreatFabric](#) · [ThreatFabric](#)

Octo2: European Banks Already Under Attack by New Malware Variant

[Coper](#)

2024-09-09 · [Cleafy](#) · [Cleafy](#)

Tweet about malware version Octo 2

[Coper](#)

2024-07-09 · [Spamhaus](#) · [Spamhaus Malware Labs](#)

Spamhaus Botnet Threat Update January to June 2024

[Coper](#) [FluBot](#) [Hook](#) [Bashlite](#) [Mirai](#) [FAKEUPDATES](#) [AsyncRAT](#) [BianLian](#) [Cobalt Strike](#) [DCRat](#) [Havoc](#) [NjRAT](#) [OakBot](#) [Quasar](#) [RAT](#) [RedLine](#) [Stealer](#) [Remcos](#) [Rhadamanthys](#) [RisePro](#) [Sliver](#)

2024-03-05 · [Team Cymru](#) · [S2 Research Team](#)

Coper / Octo - A Conductor for Mobile Mayhem... With Eight Limbs?

[Coper](#)

2023-02-08 · [K7 Security](#) · [Baran S](#)

Play Store App Serves Coper Via GitHub

[Coper](#)

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

"In The Box" - Mobile Malware Webinjects Marketplace

[Alien](#) [Cerberus](#) [Coper](#) [ERMAC](#) [Hydra](#)

2022-07-29 · [Trend Micro](#) · [Trend Micro Mobile Team](#)

Examining New DawDropper Banking Dropper and DaaS on the Dark Web

[Coper](#) [DawDropper](#)

2022-07-19 · [Cert-AgID](#) · [Cert-AgID](#)

Analysis and technical insights on the Coper malware used to attack mobile devices

[Coper](#)

2022-06-28 · [Twitter \(@_icebre4ker_\)](#) · [Fr4](#)

Revive and Coper are using similar phishing template and app

[Coper](#)

2022-04-09 · [Bleeping Computer](#) · [Bill Toulas](#)

New Android banking malware remotely takes control of your device

[Coper ExoBot](#)

2022-04-08 · [ThreatFabric](#) · [ThreatFabric](#)

Look out for Octo's tentacles! A new on-device fraud Android Banking Trojan with a rich legacy

[Coper ExoBot](#)

2022-04-07 · [The Hacker News](#) · [Ravie Lakshmanan](#)

New Octo Banking Trojan Spreading via Fake Apps on Google Play Store

[Coper](#)

2022-03-24 · [Cybleinc](#) · [Cyble](#)

Coper Banking Trojan: Android Malware Posing As Google Play Store App Installer

[Coper ExoBot](#)

2021-12-31 · [CERT.PL](#) · [Marcin Dudek](#), [Michał Praszmo](#)

IKO activation - Malware campaign

[Coper](#)

2021-07-21 · [Doctor Web](#) · [@m0br3v](#)

The Coper—a new Android banking trojan targeting Colombian users

[Coper](#)

There is no Yara-Signature yet.

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