G

Godfather Android Malware: Banking Theft and Recovery

Godfather is Android banking malware associated with credential theft, overlays, remote control, and newer on-device application virtualization techniques.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 How Godfather attacks banking apps
02 How infection begins
03 Warning signs
04 What to do if Godfather is suspected
05 Prevention
06 Sources

Quick answer: Godfather is Android banking malware that targets financial and cryptocurrency applications. Documented versions have used fake login overlays, accessibility permissions, screen or input capture, and remote-control functions. Researchers reported a newer 2025 variant using on-device virtualization to run selected legitimate apps inside an attacker-controlled environment.

01 How Godfather attacks banking apps

Earlier reporting described Godfather monitoring which app was open and presenting a counterfeit login page over a targeted bank or wallet app. Information entered into the overlay went to the attacker. Powerful Android accessibility permissions could help the malware observe the screen, perform actions, or grant additional access.

In 2025, researchers documented a different approach: a malicious host application incorporated a virtualization framework and launched a copy of a targeted legitimate app inside that controlled environment. Because the victim interacted with a real app running inside the container, visual inspection alone became less reliable than with a simple fake overlay.

Capabilities and targets vary by version and operator. A list of targeted brands from one campaign does not prove that every customer or region is affected, and an absent brand does not make an unknown APK safe.

02 How infection begins

The victim still has to receive and install a malicious application or dropper. Delivery can use impersonated apps, deceptive sites, messages, or third-party stores, followed by instructions to enable installation from an unknown source or grant accessibility and other sensitive permissions. A legitimate banking app is not itself infected merely because Godfather targets it.

03 Warning signs

- An app installed from a link or outside the expected official store.
- A utility, media, or security app requesting accessibility, notification, SMS, screen-capture, or device-administration access without a clear need.
- Play Protect or mobile-security alerts, disabled protection, hidden app icons, or an app resisting removal.
- Unexpected login screens, repeated credential prompts, screen overlays, or banking notifications for unknown activity.

- New linked devices, changed recovery details, or fraudulent transactions.

04 What to do if Godfather is suspected

1. Enable airplane mode and turn off Wi-Fi. Stop banking, email, password-manager, and cryptocurrency activity on the phone.
2. From another trusted device, contact the bank through its official number, secure the account, and review pending and completed transactions.
3. Change exposed passwords, starting with email and financial accounts; revoke sessions and check MFA, recovery information, and linked devices.
4. Record suspicious app names, installation source, permissions, alerts, and times. For a managed phone, contact the security team before resetting it.
5. Remove device-administrator or accessibility privileges from the malicious app only if safe, then uninstall it. Run updated Play Protect or the approved mobile-security scan.
6. Factory-reset the phone when removal or integrity is uncertain. Reinstall apps manually from official sources and avoid restoring unknown APKs or unsafe settings.

A factory reset does not reverse stolen credentials or fraudulent transfers, so account recovery is required even after the device is cleaned.

05 Prevention

Keep Android and apps supported and updated, leave Play Protect enabled, and install apps only from verified stores and publishers. Treat accessibility as a high-impact permission. Review it regularly along with device administrators, notification access, VPN profiles, and installation privileges. Use a strong screen lock, unique passwords, transaction alerts, and phishing-resistant authentication where supported.

06 Sources

Original targeting and capability research is from Group-IB’s Godfather analysis. The virtualization development is summarized in Recorded Future’s H1 2025 malware trends report.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com