New Android RAT Klopatra Targets Financial Data - Against Invaders - Not

Data: 2025-10-01 12:39:52

Autor: Inteligência Against Invaders

A previously unknown Android Remote Access Trojan (RAT) has been identified by security

researchers, marking a significant advancement in the evolution of mobile banking threats.

The malware, named “Klopatra,” was uncovered by Cleafy’s Threat Intelligence team in late August 2025 and is already being used in large-scale campaigns targeting financial institutions in Europe.

Unlike most mobile malware, Klopatra employs commercial-grade protection techniques rarely seen in Android attacks.

Its developers integrated Virbox, a professional software protection suite, and shifted much of its functionality from Java to native code. This combination creates substantial obstacles for analysts, allowing the malware to evade detection and resist reverse engineering.

At its core, Klopatra is a sophisticated banking Trojan. It enables attackers to seize control of infected devices using Hidden VNC for remote operations, dynamic overlays to steal credentials and abuse of Accessibility Services to execute transactions without the victim’s awareness.

Read more on Android banking trojans: Android Malware Targets Banking Users Through Discord Channels

Campaigns, Operators and Risks

Two primary botnets have been linked to Klopatra so far. Together, they have compromised more than 3000 devices, with most victims located in Spain and Italy. Researchers observed tailored targeting of major banking apps in these regions, confirming a focus on financial fraud.

Analysis also points strongly toward a Turkish-speaking criminal group. Linguistic traces in the malware’s code, field names in command-and-control (C2) infrastructure and even direct operator notes left in server logs all suggest a cohesive team managing development and monetization.

Klopatra’s activity since March 2025 shows an unusually fast development cycle, Cleafy said, with over 40 distinct builds recorded. Early versions lacked many of the capabilities seen today, but recent updates demonstrate a layered defense strategy that includes string encryption and advanced permission abuse.

The malware has already been tied to real-world fraud attempts. Operators often strike at night while victims’devices are charging and unattended. They use stolen unlock patterns or PINs to access banking apps, transferring funds under the cover of a blacked-out screen that convinces the user the phone is off.

Advanced Mobile Malware

Klopatra highlights a growing trend of mobile malware adopting techniques once reserved for desktop threats.

By investing in commercial protection tools and agile updates, its operators ensure the malware remains both effective and resilient.

Security experts warn that Klopatra may serve as a model for future threats, raising the stakes for financial institutions.

“This is not an experiment but a fully operational fraud tool,”Cleafy warned.

“For financial institutions and anti-fraud teams, the emergence of Klopatra underscores the need for threat detection solutions that go beyond static analysis and focus on device-level behavioral monitoring. For the threat intelligence community, continuous monitoring of this group and its infrastructure will be essential to anticipate their next moves and protect users from this evolving threat.”