2025 Mobile Fraud Intelligence Briefing: What We're Seeing Across the Threat Landscape

Throughout 2025, our teams have analysed Cleafy's discoveries across the mobile threat ecosystem, and the direction of travel is unmistakable: mobile fraud has entered a fully industrialised, on-device era. The four principal malware families identified this year—Albiriox, Klopatra, PlayPraetor, and SuperCard X—signal a decisive shift in how fraud is orchestrated, delivered, and scaled globally.

Malware Family	Primary Function	Operator Profile	Key Capabilities	Geographical Footprint	Strategic Risk
Albiriox	Android RAT + Banking Trojan (MaaS)	Russian-speaking operators; affiliate-driven	Accessibility abuse, remote control, screen streaming, large targeting catalogue (>400 apps)	Early activity in Central Europe; capability to scaleglobally	High-volume, scalable on-device fraud with a commercialised delivery pipeline
Klopatra	Advanced Android Banking RAT	Turkish-speaking group	Strong obfuscation (packer use), hidden VNC, native-code evasion	Southern Europe (Spain/Italy)	Hard-to-detect RAT designed to bypass static mobile defences
PlayPraetor	RAT delivered via Chinese-speaking MaaS	Highly structured, multi-tenant operation	Live video session streaming, WebSocket orchestration, mass distribution through fake store pages	Europe, LATAM, parts of Africa and Asia	Rapid botnet expansion and session-level takeover at global scale
SuperCard X	NFC Relay Malware	Chinese-speaking operators	NFC harvesting and real-time relay for POS/ATM cash-outs	Initially Italy-centred	Exploits card rails directly, circum-venting account-level fraud engines

2025 Malware Set Through Our Lens

Albiriox

A highly commercialised MaaS platform enabling affiliates to operate inside authenticated banking and crypto sessions. Its breadth of targeting and modular infrastructure represents a mature fraud supply chain.

Read the Technical Analysis

Klopatra

A technically sophisticated banking RAT engineered for stealth. The depth of its obfuscation stack and its hidden remote-access functionality place it firmly in the “next-generation” category of mobile threats.

Read the Technical Analysis

PlayPraetor

A rapidly scaling MaaS ecosystem with botnet growth far exceeding typical Android fraudware. Its real-time device-streaming capability redefines the adversary’s operational control within a customer session.

Read the Technical Analysis

SuperCard X

A notable expansion of the attack surface beyond banking apps. By weaponising NFC, it introduces a new class of mobile-enabled payment fraud that challenges conventional card-fraud controls.

Read the Technical Analysis

Implications for the Financial Sector

We are witnessing a shift from transactional interference to full-session compromise, where adversaries utiliseseeing a transition from transactional interference to full-session compromise, where adversaries use the device itself as the point of execution. Accessibility misuse, remote device management, and relay techniques underpin attacks that operate as legitimate usersremote-device management, and relay techniques underpin attacks that operate as the legitimate user within trusted environments.

This requires a structural shift in defensive strategy. Fraud controls built around transaction scoring are no longer sufficient, and mobile-security solutions reliant on signatures are outpaced by increasingly professionalised obfuscation pipelines.

To counter the 2025 threat model, financial institutions must move decisively towards session-layer intelligence, combining behavioural analytics, device integrity insights, malware-specific telemetry, and fused cyber–fraud response.

The Narrative We Are Driving

The message we are taking to market is simple: 2025 marks the point at which **on-device fraud** becomes the standard operating model for threat actors. The malware families uncovered this year show a deliberate, scalable **engineering approach** aligned to sustained financial exploitation.

Our objective is to anchor industry attention on the session as the **strategic control point.** Protecting payments alone is no longer sufficient; the future of fraud prevention lies in protecting the full digital experience.

As we look ahead, it's clear the market has entered a new phase of **mobile-led fraud** where adversaries are no longer probing the edges of digital banking—they are operating squarely within it.

The findings from 2025 reinforce a simple truth: **meaningful resilience** now depends on understanding and controlling the customer session end to end. Our commitment is to ensure the industry stays ahead of this shift, translating intelligence into **actionable defence** and enabling organisations to protect their customers with confidence in an increasingly contested digital landscape.