One-pager

The invisible hand of digital fraud: PlayPraetor's silent setup

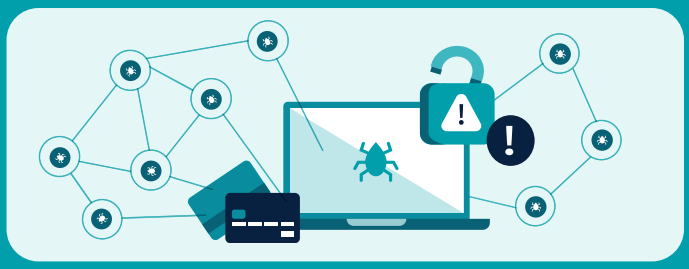
Fraud that looks like fraud is easy to catch. The danger now is **malware that doesn't behave like malware**. It hides behind permission trickery, sideloaded apps, and subtle user manipulation.

PlayPraetor isn't built to steal money directly. It's built to **own access** - devices, apps, and users - before any transaction occurs. It signals a clear shift in how cybercriminals prepare attacks, and why banks must rethink where they look for fraud.

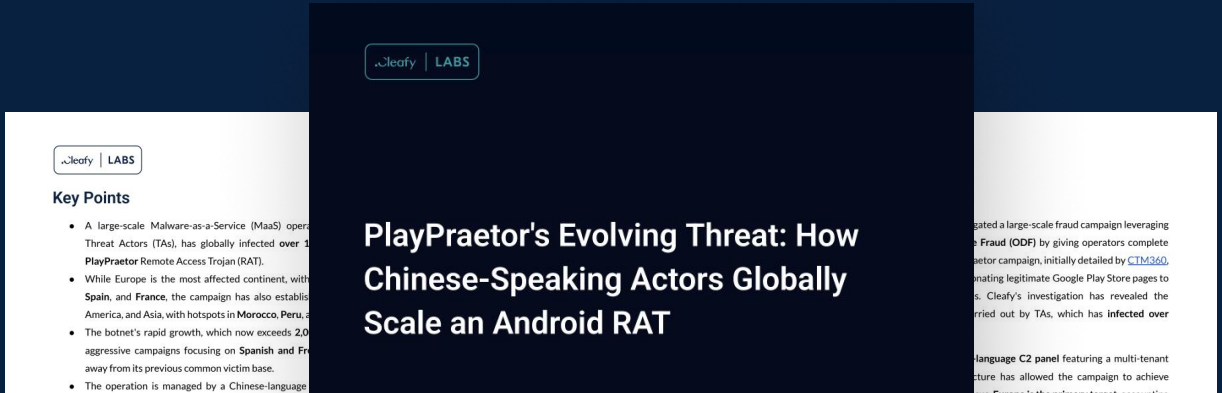
PlayPraetor isn't just another Android Trojan. It's a **Remote-Access Toolkit** being scaled by organised, Chinese-speaking operators who rent and adapt it globally. When a RAT like PlayPraetor gains persistence on a **mobile device,** it doesn't just collect credentials. It turns that device into a permanent bridge into your financial services ecosystem.That means authenticated fraud, executed from trusted devices, bypassing traditional defences.

Fraud begins upstream

PlayPraetor is part of a **new generation of Android malware** built for scale and subtlety. It doesn't rush to steal. It quietly builds access, manipulates permissions, and sets up attacks that look legitimate when they finally hit. Transaction scoring and signature feeds only see the aftermath. Cleafy sees the setup.



Deep dive into our Cleafy LABS technical findings about PlayPraetor to learn more about how this malware actually works against digital banking customers.



Malware-as-a-Service: modular, fast, cheap, scalable

PlayPraetor isn't a one-off. It's modular, rebranded, and rented to local criminal groups who adapt it by language, lure, and market. Campaigns active in **Southern and Eastern Europe** can pivot to other countries overnight. The same distribution networks that delivered TeaBot, **FluBot**, and **Vultur** are being reused - faster, quieter, more effective. When it lands, it won't be new, but refined.

Invisible, until it's not

PlayPraetor hides behind permissions, accessibility abuse, and sideloaded apps that look harmless. **Traditional security tools** see nothing out of place. **Cleafy** spots the behavioural anomalies inside the session - overlays, remote access, device manipulation - even when the user experience appears genuine.

Android under pressure

Mobile banking Trojans **surged 196% in 2024,** hitting 1.24 million incidents globally. Nearly all mobile malware, 99%, targets **Android.** PlayPraetor exploits that flexibility to stay dormant, waiting for the right moment. Without session visibility, banks are blind until money moves.

Real Malware. Real Intelligence.

Cleafy confirms malware activity inside customer environments, including OTP interception, remote control, and evolving capabilities like overlays. We don't just flag apps, we map permissions, device access, and potential attack vectors. Banks get **actionable intelligence,** not theory, for prioritising risk and briefing executives.

From detection to anticipation

Cleafy turns hidden activity into early warning:

Real malware inside customer sessions

Capabilities and permissions mapped

Reports ready for executive decision-making

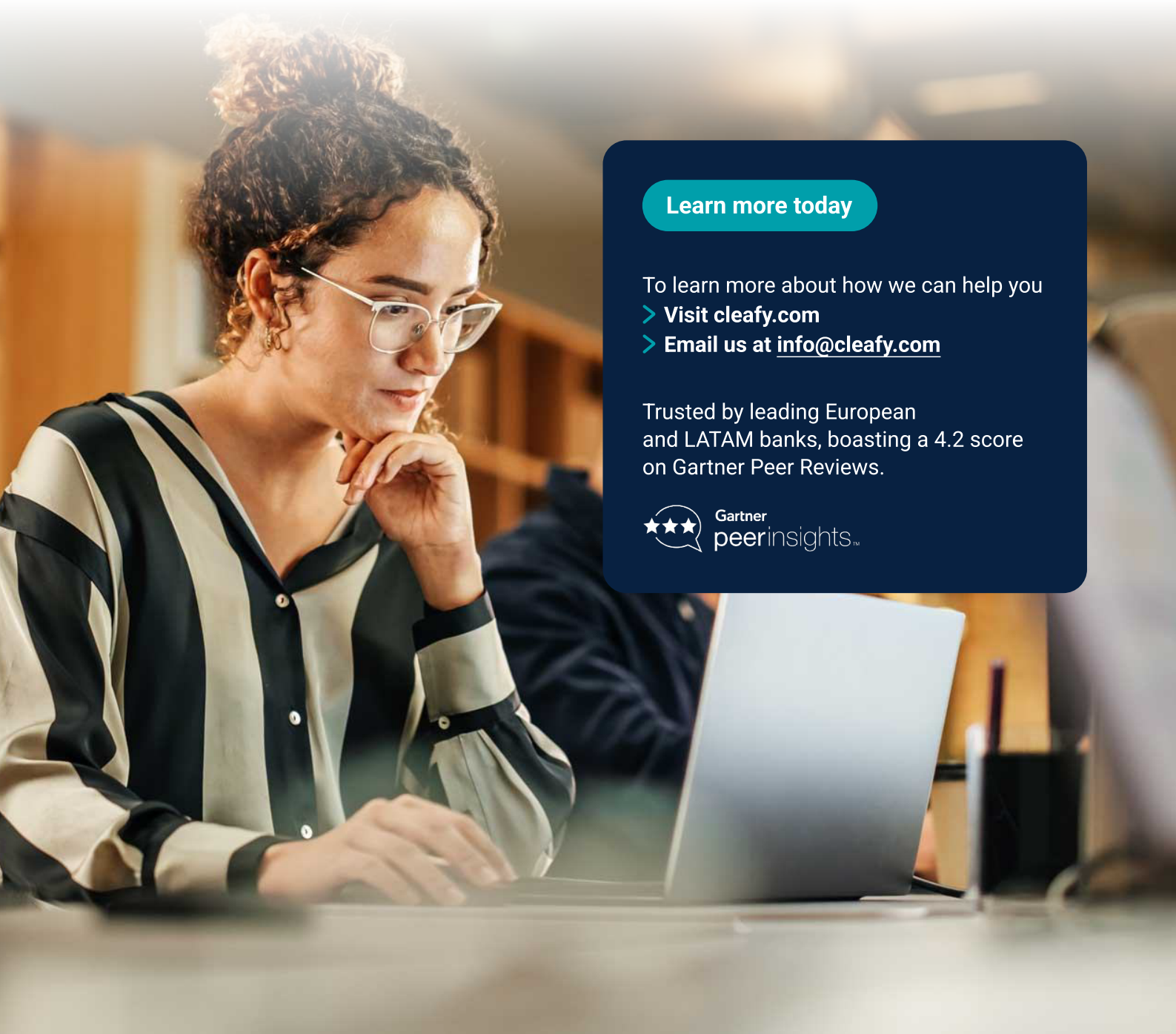
Fraud begins before the fraud. Cleafy sees that moment.

Why it matters now

PlayPraetor shows how the rules have changed. Fraud starts when a device quietly joins the attacker's playbook, not at login or payment. The **UK banking ecosystem** is deeply connected to Europe; threats rarely stay contained. **Cleafy customers** already see and stop these behaviours in real-time. The question isn't if PlayPraetor will hit UK banks. It's who will see it first.

See it sooner. Stop it earlier.

Cleafy doesn't just provide malware detection; our **cyber-fraud defence platform** provides banks and financial institutions with early warnings, before the transaction, before the fraud, before the alert storm hits.



Learn more today

To learn more about how we can help you
- **Visit cleafy.com**
- **Email us at info@cleafy.com**

Trusted by leading European and LATAM banks, boasting a 4.2 score on Gartner Peer Reviews.

Gartner peerinsights™

Cleafy – Italy | UK | Spain | Netherlands | Brazil | Colombia