2026 Mobile Banking Heist Report

Fraud Now Starts on the Device

www.zimperium.com

ZIMPERIUM®

Index

Introduction

Financial institutions globally have spent years hardening their backend banking infrastructure, strengthening authentication, improving transaction monitoring, and investing in fraud analytics. Those investments were necessary — and they worked, for the threat they were built to address.

The threat has changed. Cybercriminals have a mobile-first attack strategy.

The mobile app now is the bank for most customers. Today, 54% of consumers cite mobile apps as their primary method for managing bank accounts, a figure that has more than doubled since 2017. As the channel shifted, so did the attack surface — faster than any institution could reasonably have anticipated.

The numbers make the target obvious. Banking trojan attacks on Android smartphones increased 56% in 2025. The number of unique trojan banker installation packages rose to 255,090 — a 271% increase over 2024 alone. Online fraud within financial services increased 21% between 2024 and 2025, with one in every 20 verification attempts now deemed fraudulent. Critically, **80% of fraud events now occur through online or mobile platforms.**

The mobile banking app is not just one of many attack surfaces. It is the largest and most lucrative one.

A Note on Our Research Methodology

The findings in this report are based on our analysis of malware samples across multiple threat families. Our research examines how these malware families behave, who they target, and how they operate — it is not an analysis of any specific mobile banking application or institution.

In 2026, Zimperium's zLabs research team analyzed 34 active mobile malware families targeting 1,243 financial brands across 90 countries — covering apps with more than three billion downloads worldwide. These weren't isolated incidents. They were industrialized campaigns, engineered at scale, moving faster than traditional defense cycles can match.

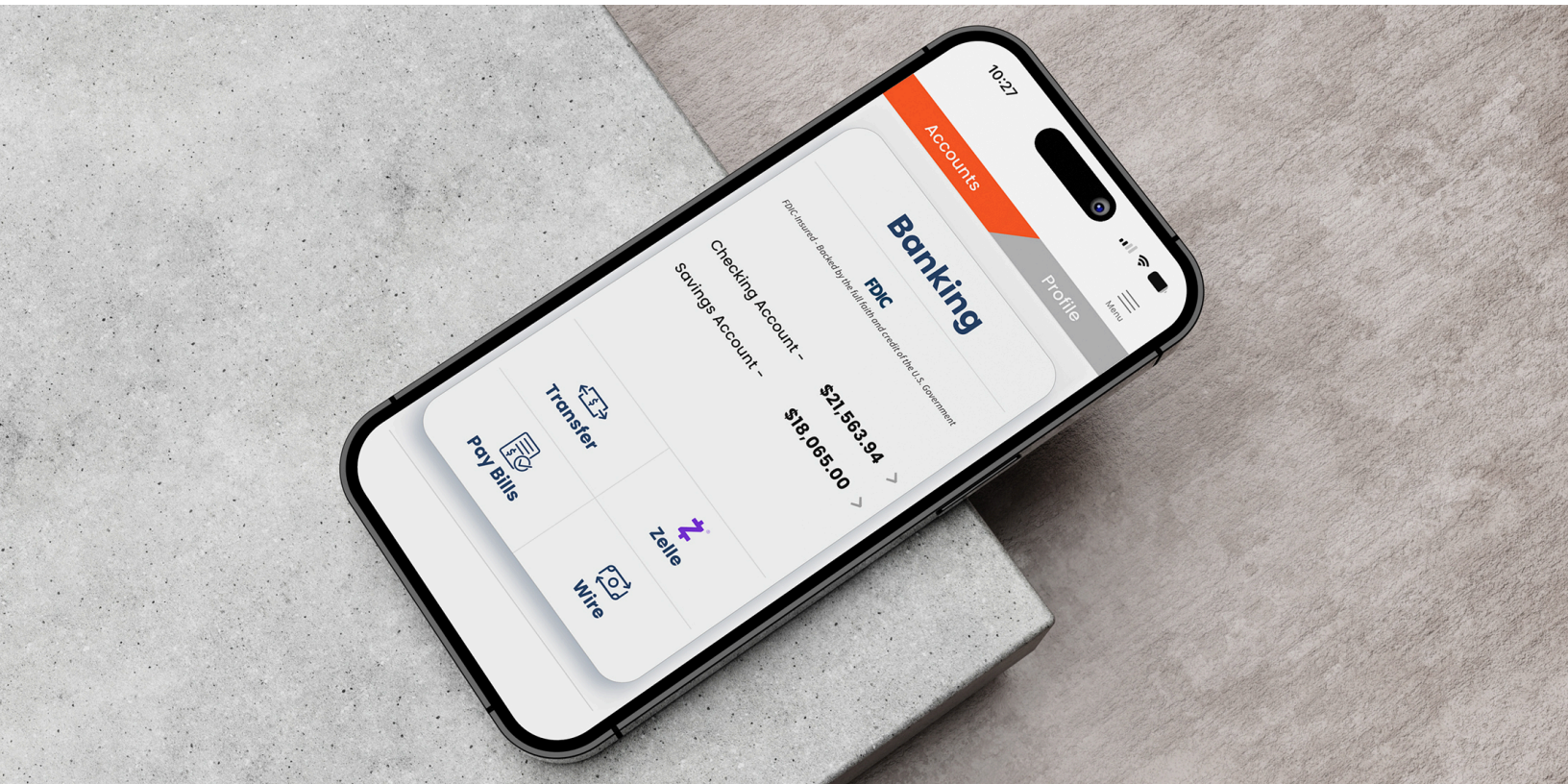
This report exists to help financial institutions understand the capabilities, scale, and sophistication of today's mobile malware — so they can identify the gaps in their current defenses and build a stronger foundation for protecting their mobile banking apps.

Executive Summary

What Zimperium's 2026 Research Found

- Infrastructure-as-a-service and code sharing has driven the cost of entry to near zero, industrializing attacks at a scale no single institution can outpace alone.
- Three malware families, TsarBot, CopyBara, and Hook collectively target more than 60% banking and fintech apps.
- Overlay attacks, session hijacking, and full device remote access are no longer advanced capabilities, they are accessible by even less sophisticated fraudsters.
- The United States alone has 162 banking apps under active targeting, the highest concentration of any single country globally.
- Ukraine, Russia, and the United States are the top three countries hosting command-and-control infrastructure across the malware families analyzed.
- In 2026, banking malware has escalated to deploy ransomware, encrypting device files and demanding Bitcoin, evolving from fraud into extortion.

The mobile banking app is now the primary attack surface for financial fraud. Many institutions are struggling to defend their app in what is often a hostile and compromised environment: their own customer's personal device.



Banking Malware Now Bypasses Traditional Defenses

Banking malware has evolved from credential harvesting into full device control. Android malware transactions increased by 67% year-over-year, fueled by sophisticated spyware and banking trojans. Modern banking trojans are highly sophisticated pieces of software. They persist on the customer's device, evade detection, impersonate a real user, invisibly hijack live mobile banking sessions, and can silently execute fraudulent transactions inside the official banking app. To backend systems, the activity appears legitimate. The fraud has already happened by the time it is detected.

The implication is direct: strong authentication and server side security alone is not sufficient when malware can intercept the one-time passcode and impersonate the user. Device trust must be established first.

Attackers Know How Your App Works

Before a single customer account is compromised, attackers have already downloaded the legitimate mobile banking app, reverse engineered it on their own infrastructure, and built malware tailored to bypass controls. They understand API structure, authentication logic, and transaction workflows. This is not hypothetical — more than 60% of mobile banking apps lack basic code protection, leaving their architecture openly readable to anyone who downloads them. Because their tools replicate legitimate mobile banking traffic patterns, API security and traffic inspection alone cannot distinguish a fraudulent request from a genuine one.

Transaction monitoring and API security cannot detect fraud that looks identical to a legitimate session — because the attacker is manipulating the real app. Both the app and the API layer must be attested to ensure nothing is being manipulated.

AI Is Accelerating Every Stage of the Attack Chain

Reverse engineering a mobile banking app that once took weeks can now be completed in a fraction of the time and without the exceptional technical skill that was once needed. Overlay screens are customized at scale. Malware now leverages AI-generated deepfakes to bypass eKYC verification — defeating the onboarding controls banks have invested in to establish customer trust from the first interaction. The attacks are more precise, more scalable, and harder to detect with each cycle of AI advancement and 76% of security teams report they cannot keep pace.

What This Means for Security and Fraud Leaders

These are not opportunistic attacks. They are engineered campaigns — systematic, sustained, and global. And regulatory scrutiny is increasing. Institutions that lack visibility into device-level compromise of their mobile banking channel are becoming audit targets. The ability to measure and verify compliance, rather than assume it, is no longer optional.

Backend controls were built for a different threat. Reducing exposure now requires extending security to the mobile banking app itself across three areas: hardening the app against reverse engineering, protecting app runtime integrity on customer devices, and gaining visibility into device risk before fraud reaches your systems.

The core conclusion of this report is straightforward: mobile banking fraud no longer begins at the server. **It begins on the mobile device.**

Research Findings

In 2025, Zimperium's zLabs tracked 34 active malware families targeting 1,243 financial brands across 90 countries. This report is a summary of what a full year of that research revealed.

The data below captures the operational scale of banking malware in 2026. It reflects the number of active malware families, the financial applications targeted, and the global distribution of these campaigns. All data presented in this report comes from Zimperium's zLabs research organization.

These metrics illustrate how systematically mobile banking is being targeted across regions and institutions.

Quick Summary

Malware Families Researched

34

Traditional Banking Apps Targeted

1,131

New Malware Families

2

(Sturnus, Crocodilus)

Fintech (Payments, Crypto and Trading) Apps Targeted

112

Countries Impacted

90

Targeted Mobile Banking App Downloads

3 Billion +

The Most Active Banking Malware Families

The ten families below are not opportunistic tools built by isolated actors. They are scalable fraud infrastructure — distributed through Malware-as-a-Service platforms, accelerated by code sharing across cybercriminal networks, and continuously updated to bypass app security and evade detection. This is what has driven the cost of entry for new malware and variants to near zero and enabled campaigns to scale across institutions, geographies, and payment systems simultaneously.

The table below outlines the ten most active banking malware families so far in 2026, ranked by the number of financial applications targeted and their geographic reach. The data illustrates the scale and global coordination of modern banking trojans.

TsarBot	CopyBara	Hook	Teabot	Hydra	ExobotCompact	Ermac	GodFather	Anubis II	Blackrock
711 Traditional Banking Apps Targeted	696 Traditional Banking Apps Targeted	600 Traditional Banking Apps Targeted	407 Traditional Banking Apps Targeted	413 Traditional Banking Apps Targeted	338 Traditional Banking Apps Targeted	346 Traditional Banking Apps Targeted	283 Traditional Banking Apps Targeted	241 Traditional Banking Apps Targeted	194 Traditional Banking Apps Targeted
90 Fintech Apps Targeted	88 Fintech Apps Targeted	55 Fintech Apps Targeted	9 Fintech Apps Targeted	32 Fintech Apps Targeted	5 Fintech Apps Targeted	30 Fintech Apps Targeted	32 Banking Apps Targeted	14 Banking Apps Targeted	27 Banking Apps Targeted
Stolen Data Exfiltrated to: Russia	Stolen Data Exfiltrated to: Germany	Stolen Data Exfiltrated to: Russia	Stolen Data Exfiltrated to: Netherlands UK France Ukraine	Stolen Data Exfiltrated to: Ukraine South Africa United States	Stolen Data Exfiltrated to: Ukraine Japan France United States Russia Switzerland	Stolen Data Exfiltrated to: Ukraine South Africa United States	Stolen Data Exfiltrated to: USA Turkey Spain Canada France Germany UK Italy Poland	Stolen Data Exfiltrated to: Lithuania Russia UK Ukraine	Stolen Data Exfiltrated to: Russia UK Ukraine

Malware Capabilities Observed

Banking malware has advanced to focus on manipulating how the banking app behaves on a mobile device. When attackers control app behavior, authentication no longer guarantees trust, and fraud detection becomes more complex.

Early generation banking trojans focused on credential theft, account takeover and evading detection. In 2025, they have grown exponentially in sophistication and the ability to control both the victim's account and their device. Screen overlays, which invisibly capture all data entered into the device, have become a persistent tactic of new and modified malware families. Meanwhile, these bad actors are now expanding their tactics to enable the ability to extort the user or financial institution, including ransomware.

The table below provides details of how key malware capabilities have expanded in the last year from what was seen in previous generations:

Earlier-Generation Banking Trojans	Additional Capabilities Observed in 2025
Account Takeover • Intercept notifications • Bypass one time passwords • Automatic Transfer Systems (ATS) • Remote screen sharing and recording **Stealth and Evasion** • Detect and evade emulators • Obfuscate and open source code reuse • Domain Generation Algorithms (DGA)	**Account and Transaction Takeover** • Intercept codes from authentication apps • Steal session cookies • Bypass biometric and eKYC requirements • Present overlay screens to capture credentials • NFC relay to hijack a transaction • Executes invisible transactions while the screen appears frozen or off • Capture keystrokes **Context Hijacking** • Read WhatsApp/Telegram/Signal for social engineering • Interception of incoming and outgoing calls • Fraudulent voice calls to extract PII **Full Device Control** • Full device takeover (DTO) • Remotely control the device • Pretend to be a corporate device management tool **Persistence and Evasion** • Obfuscate malicious code • Evade analysis tools • Evade detection mechanisms • Hide its app icon **Financial Extortion** • Demand Bitcoin to unlock the device • Ransomware module to encrypt on device files

The table below maps the 34 malware families analyzed against five capability categories — revealing not just how many families possess each capability, but how comprehensively the attack chain has been engineered.

Capability	Malware	Prevalence
Account and Transaction Takeover	29	**85%**
Persistence and Evasion	29	**85%**
Full Device Control	25	**73%**
Financial Extortion	17	**50%**
Context Hijacking	13	**38%**

Introducing Sturnus, Crocodilus

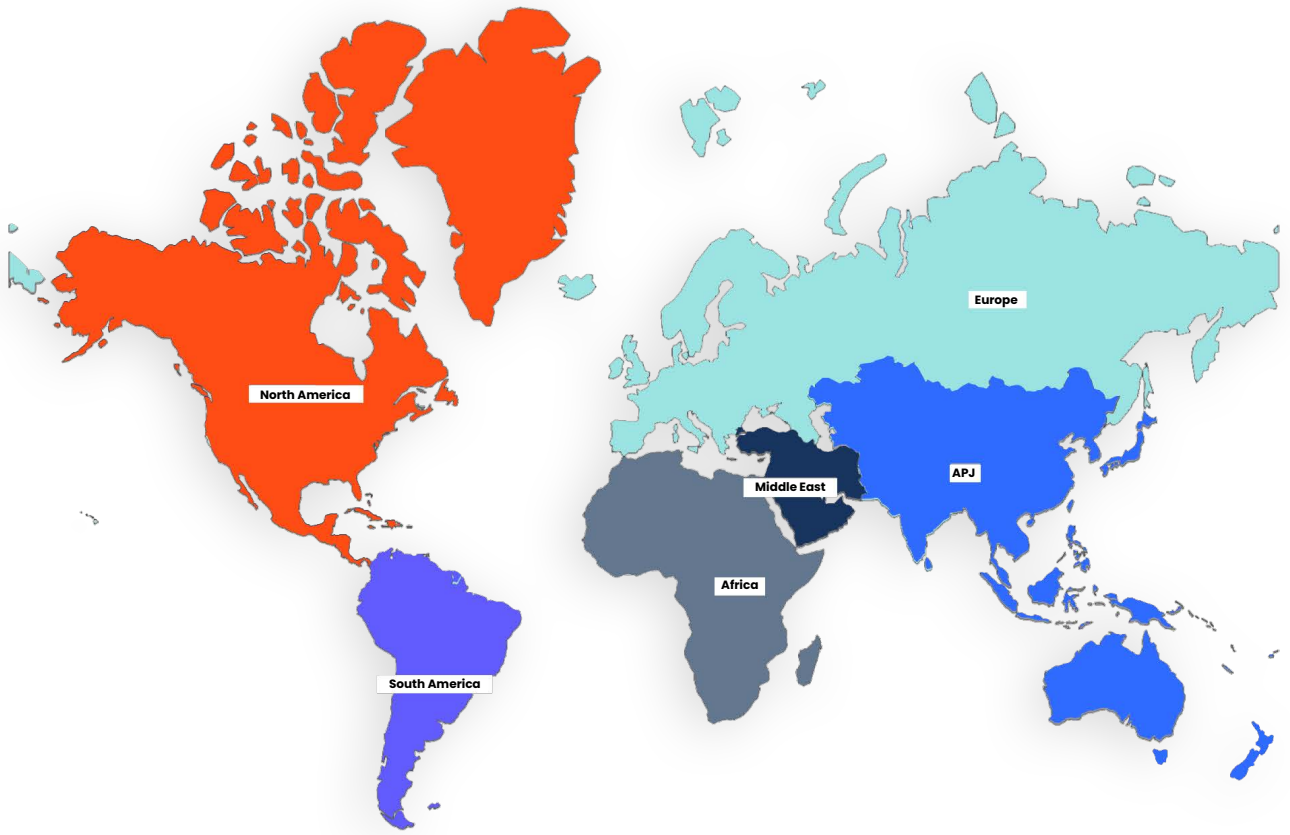
Sturnus is a sophisticated, Android banking Trojan that targets financial institutions and users, particularly in Southern and Central Europe.

Crocodilus is also a new Android banking Trojan which specializes in device takeover, banking credential theft, and stealing cryptocurrency assets.

Countries Targeted In Each Region

The table below shows the countries where banking apps were targeted by the malware families analyzed. This data demonstrates not just global scale but deliberate regional targeting, with each malware family adapted to the language and banking environment of its victims.

It also shows that banking malware campaigns operate across both highly regulated and less regulated markets. Regulatory maturity alone does not prevent device-driven fraud, underscoring the need for consistent mobile app security controls regardless of regulatory guidelines or mandates.

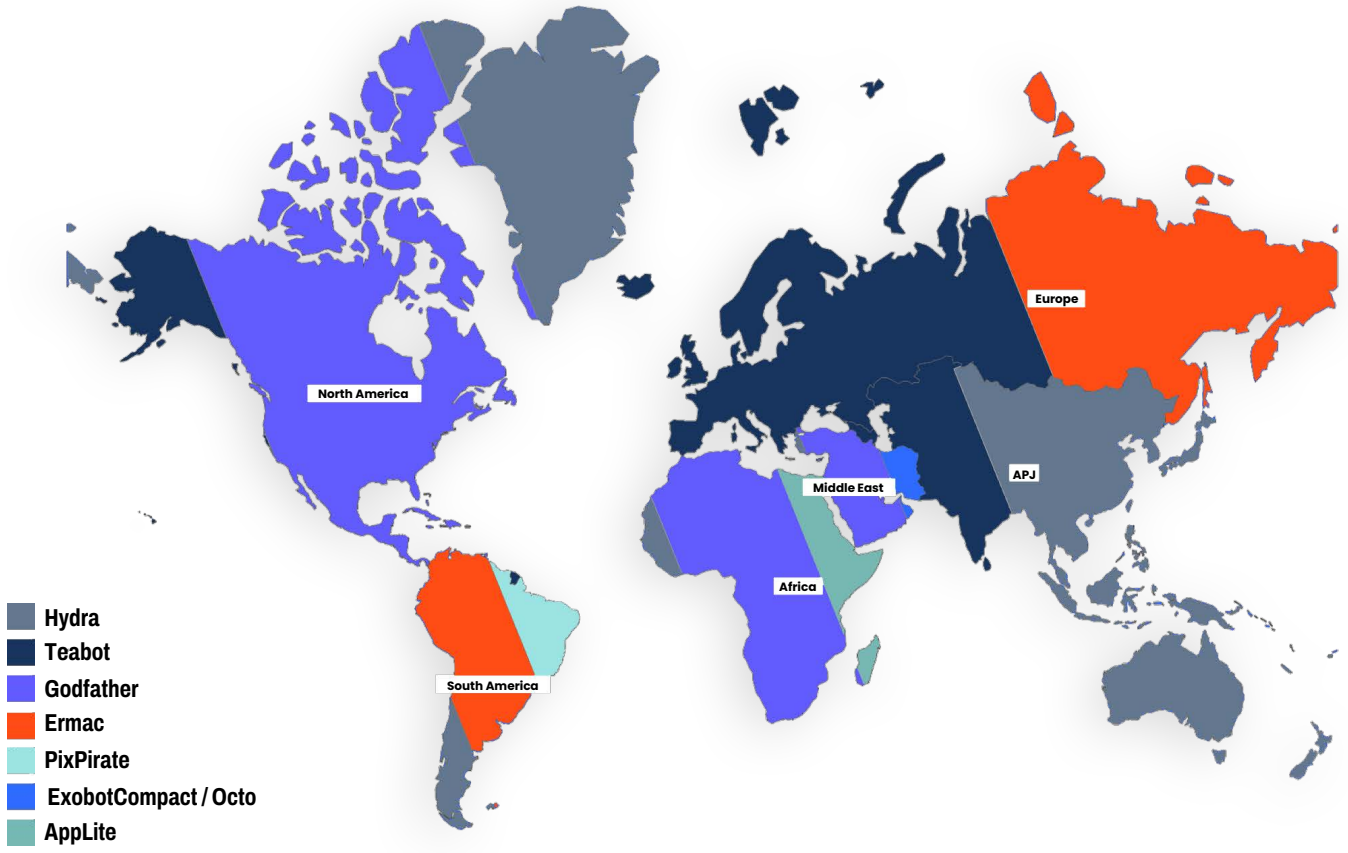


North America	South America	Europe		APJ	Middle East	Africa
Canada	Argentina	Andorra	Ireland	Australia	United Arab Emirates	Nigeria
United States	Brazil	Austria	Italy	Cambodia	UAE	Egypt
Mexico	Chile	Belarus	Latvia	China	Saudi Arabia	Morocco
Belize	Colombia	Belgium	Lithuania	Hong Kong	Qatar	Kenya
Dominican Republic	Ecuador	Bosnia Herzegovina	Luxembourg	India	Kuwait	Angola
Haiti	Peru	Croatia	Malta	Indonesia	Oman	Senegal
	Uruguay	Cyprus	Netherlands	Japan	Israel	Seychelles
	Venezuela	Czech Republic	Norway	Malaysia	Jordan	Cape Verde
	Guatemala	Denmark	Poland	New Zealand	Turkey	Pan African HQ Togo
		Estonia	Portugal	Pakistan		
		Finland	Romania	Papua New Guinea		
		France	Scotland	Philippines		
		Georgia	Slovakia	Singapore		
		Germany	Spain	South Korea		
		Greece	Switzerland	Sri Lanka		
		Hungary	United Kingdom	Thailand		
				Vanuatu		

Malware Families Prevalent By Region

TsarBot, Copybara, Hydra, and Hook dominate the global volume of attacks across all regions.They use overlay attacks, accessibility abuse, and command-and-control infrastructure to steal financial credentials and enable account takeover on infected devices. But there are other malware families that are pervasive within specific regions.

North America and Europe are heavily targeted by sophisticated 2FA-bypass tools like **Teabot and Godfather**, whereas **South America** faces bespoke threats, like **PixPirate,** tailored to exploit regional payment systems. **Hydra** has emerged as the most pervasive non-global threat, reflecting a worldwide shift toward remote access and direct account takeover. This "Global for Volume, Local for Success" approach means that while banks must defend against a universal baseline of risk, their most critical task is neutralizing the specific regional malware designed to bypass local security protocols.



North America

Focus on **device takeover and session manipulation** to bypass strong banking authentication such as MFA and behavioral fraud controls.

South America

Built to exploit **instant payment systems such as PIX,** allowing attackers to initiate and authorize real time fraudulent transfers.

Europe

Campaigns designed to **bypass strong authentication frameworks like PSD2,** relying heavily on overlays and session hijacking.

Middle East

High prevalence of **Remote Access Trojans enabling real time device control** to execute transactions inside trusted sessions.

APJ

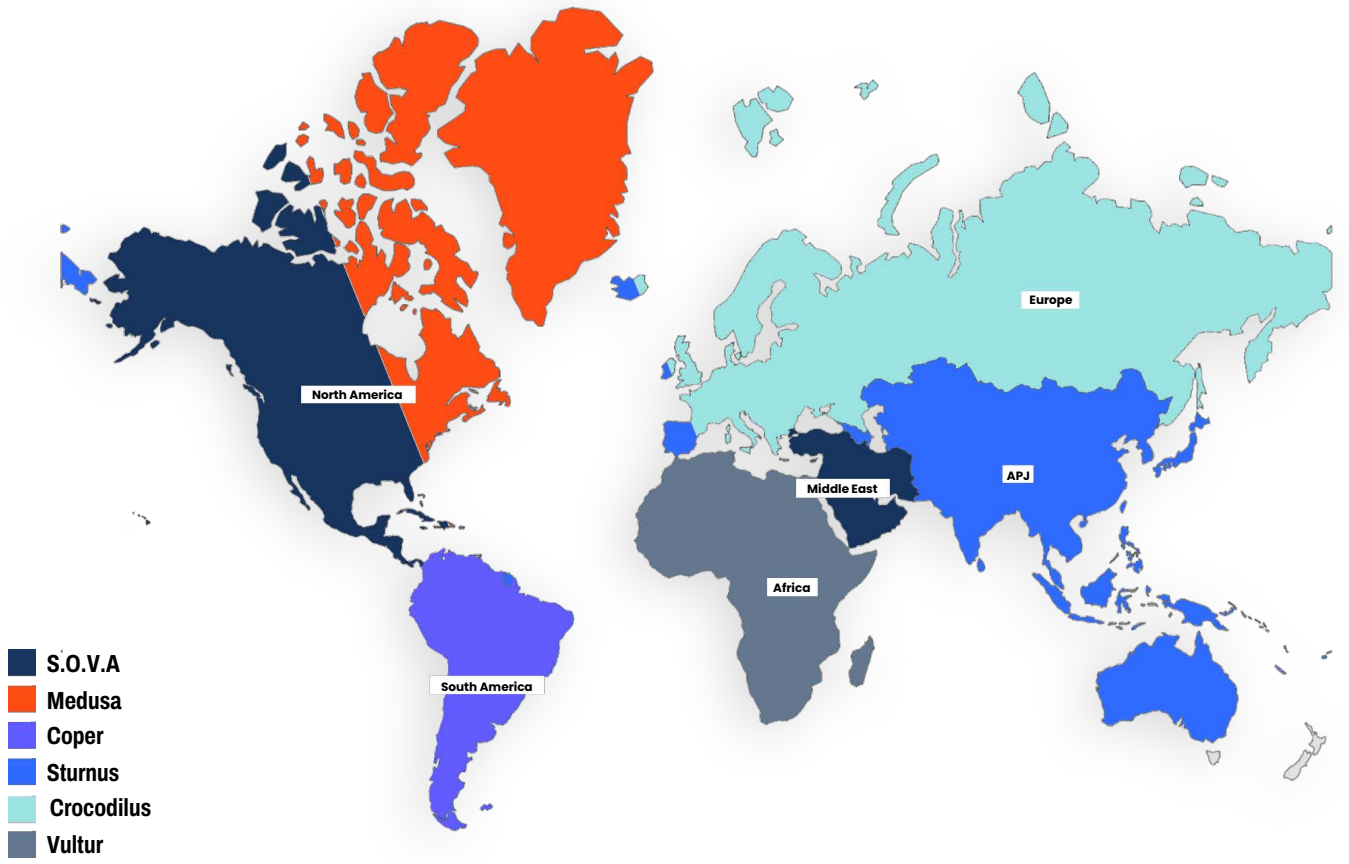
Strong focus on **credential harvesting and SMS interception** due to widespread use of SMS OTP based authentication.

Africa

Mix of **advanced RATs targeting high value crypto and banking users** alongside lightweight malware used for large scale credential harvesting.

Emerging Malware Families By Region

Emerging families such as **Sturnus** and **Crocodilus** utilize advanced "Blackout" modes to execute high-speed heists while the device appears to be off, while **S.O.V.A.** bypasses traditional MFA by hijacking active session cookies. These threats are increasingly regionalized, leveraging encrypted chat surveillance in Europe and APJ, automated payment fraud (ATS) in South America, and real-time VNC surveillance in Africa to automate fraud in total silence.



North America

- **Cookie/Session Stealing:** Bypasses MFA by hijacking active sessions.
- **Anti-Uninstall:** Blocks access to settings to prevent removal.
- **Semi-ATS:** Automates transfer steps to speed up theft.

South America

- **Disable Security:** Disables Google Play Protect and grants itself "Device Admin" rights.
- **Persistence:** Specifically prevents security and banking apps from launching.

Europe

- **Contextual Hijacking:** Reads WhatsApp/ Telegram/Signal for social engineering.
- **Blackout Mode:** Executes invisible transactions while the screen appears frozen or off.

Middle East

- **Session Takeover:** Focuses on stealing active login tokens (Cookies) to enter accounts "already logged in."
- **Persistence:** Aggressive anti-uninstall and notification blocking.

APJ

- **Contextual Hijacking:** Reads WhatsApp/ Telegram/Signal for social engineering.

Africa

- **Real-Time VNC:** Streams the device screen to attackers.
- **Disguised Payloads:** Masquerades as legitimate security software (e.g., McAfee) to bypass trust.
- **Lock-Out:** Can disable lock screen to perform fraud while the user is locked out.

Top Countries With The Most Targeted Apps

The distribution of targeted banking apps shows that **malware operators follow digital maturity, not geography.** The highest concentrations appear in markets with strong mobile banking adoption, high transaction volume, and Android dominated device ecosystems. This includes large economies like the United States and United Kingdom, but also fast digitizing markets such as Vietnam, Peru, Malaysia, and the UAE. These regions combine rapid mobile growth with fragmented device security and uneven runtime protections, creating attractive conditions for scalable fraud. The pattern reinforces a clear trend. As banking becomes mobile first, attackers shift from perimeter exploitation to device level compromise, targeting the customer endpoint where credentials, sessions, and transaction logic reside.

The table below highlights the top countries with the greatest number of targeted banking applications.

North America	 United States: 162	 Canada: 27	 Mexico: 9				
South America	 Brazil: 18	 Peru: 16	 Colombia: 10	 Argentina: 7			
Europe	 UK: 69	 Spain: 65	 Italy: 52	 Germany: 48	 France: 38	 Poland: 35	
Middle East	 Turkey: 55	 United Arab Emirates: 35	 Saudi Arabia: 17	 Kuwait: 11	 Qatar: 9		
APJ	 Australia: 50	 India: 42	 Vietnam: 23	 Malaysia: 17	 Japan: 15	 China: 14	 Indonesia: 12
Africa	 Nigeria: 9	 Egypt: 4	 Kenya: 3				

Regulatory Mandates Driven By Malware-Driven Fraud

Across Singapore, India, the EU, UAE, Malaysia, Hong Kong, Kuwait, and Australia, regulators are shifting from perimeter controls to device level enforcement. The common thread is mobile first banking combined with real time payments and rising fraud losses. Wealth-dense markets focus on device binding and strong authentication. High volume digital economies mandate code protection and rapid patching. Europe emphasizes resilience and session integrity as open banking expands exposure. The economic signal is clear. As mobile becomes core financial infrastructure, regulators are codifying a simple reality: Fraud starts on the device, not the server.

Country / Region	Regulatory Guidance & Mandates	Key Mobile App Security Focus
Singapore	**MAS TRM Guidelines / Safe App Standard 2.0**	Focus on **Malware Detection**, Anti-Screen Capture, and secure device binding.
Malaysia	**RMiT / Fraud Detection Standards**	Mandates "One Device per User" binding and **Accessibility Service** monitoring.
India	**RBI Digital Payment Security Controls**	Explicitly requires **Code Obfuscation, Anti-Tampering (RASP)**, and de-registration of inactive devices.
European Union	**DORA (Digital Operational Resilience Act)**	Focuses on **Threat-Led Penetration Testing (TLPT)** and resilience against session hijacking.
Hong Kong	**HKMA SPM TM-E-1 (Risk Mgmt of E-banking)**	Requires blocking **Screen Mirroring**, detecting root/ jailbreak, and malicious accessibility hooks.
UAE	**CBUAE Consumer Protection / Cybersecurity**	Mandatory transition from SMS OTPs to **App-based Authenticators** and Device-Bound Passkeys by 2026.
EU	**PSD2 / PSD3 (Strong Customer Authentication)**	Defines **Dynamic Linking** (linking the authentication to a specific amount/payee) and secure execution environments.
India	**SEBI Cybersecurity Framework (CSCRF)**	Mandates **VAPT (Vulnerability Assessment)** for all client-facing apps and strict patching of critical bugs within 24 hours.
Kuwait	**CBK Cybersecurity Framework**	Standardized protocols for **Operational Resilience** and standardization of cyber defense across the banking sector.
Australia	**APRA CPS 234 (Information Security)**	Requires regular **Control Effectiveness Testing** specifically for mobile assets and third-party supply chain security.

New Malware Capabilities

The scale of targeting is only part of the story. The new capabilities embedded in these modern banking malware fundamentally change how fraud is executed and detected.

1. Account and Transaction Takeover

Modern banking malware no longer relies solely on stolen passwords

Attackers can:

- Steal active session cookies
- Reads encrypted messages from WhatsApp, Telegram, and Signal
- NFC relay to hijack transactions
- Bypass biometric and eKYC requirements
- Execute invisible transactions while screen appears frozen or off

Key Takeaway: These techniques allow attackers to execute fraud from within legitimate, authenticated sessions.

2. Full Device Control

Some banking trojans now operate as remote access tools

Attackers can:

- Take full control of the device without rooting the device
- Remotely control taps, swipes, and inputs to the app
- Masquerade as device management software

Key Takeaway: When attackers control the device, they can mimic legitimate user behavior in real time, making fraud difficult to distinguish from normal activity.

3. Persistence and Evasion

Modern malware is built to remain undetected and operational

Attackers can:

- Detect and bypass analysis environments
- Disable or evade security tooling
- Hide the app icon to avoid user discovery
- Installed through dropper applications to overcome OS limitations

Key Takeaway: The longer malware remains undetected on a device, the greater the window for repeated fraud and sustained exploitation.

4. Financial Extortion

Some families now incorporate ransomware-style modules

Attackers can:

- Encrypt files on the device
- Demand cryptocurrency payments to restore access
- Change device unlock patterns to effectively lock the user out of its own device

Key Takeaway: Mobile compromise can escalate beyond fraud into direct customer disruption and reputational damage.

The Strategic Implication of New Malware Capabilities

Banking malware has evolved from stealing credentials to controlling the mobile device itself.

When the endpoint is compromised, authentication no longer guarantees trust. Transactions can be manipulated inside legitimate sessions, and fraud is executed within the bank's application environment.

For security and fraud leaders, this requires a shift in the threat model. Backend controls alone are insufficient. Device integrity must now be treated as a core component of fraud prevention and risk governance.

Key Takeaways for Financial Organizations

1. Protect the App from Reverse Engineering

Neutralizes: Precision attack construction, API exploitation, authentication logic bypass, business workflow abuse.

Attackers routinely download mobile banking apps from public app stores and reverse engineer them to uncover APIs, authentication logic, embedded secrets, and transaction workflows. The malware families analyzed in this report are engineered to exploit the specific controls of the institutions they target. That intelligence comes from the app itself.

Banks should implement controls that:

- Harden code against reverse engineering and static analysis
- Protect embedded keys and sensitive business logic
- Prevent tampering and repackaging
- Detect instrumentation and hooking frameworks

By limiting application transparency to attackers, banks close the reconnaissance window that precision attacks depend on.

2. Protect the App's Runtime Integrity

Neutralizes: Overlay attacks, key logging, OTP and authenticator code interception, session cookie theft, biometric and eKYC bypass, NFC relay, invisible transaction execution.

Modern malware interacts with the banking app during execution — injecting overlays, intercepting authentication factors, hijacking active sessions, and executing transactions while the app appears to function normally. These capabilities are present across every major malware family analyzed and every region. They do not break into the bank. They operate inside it.

Banks should deploy runtime protections that:

- Detect code injection and hooking at the process level
- Detect overlay, keylogging and screen capture abuse in real time
- Identify and terminate session manipulation before transactions execute
- Detect NFC relay attempts and transaction hijacking

These controls prevent fraud from being executed inside trusted application flows closing the visibility gap that makes mobile fraud invisible to backend detection.

3. Detect and Respond to Device-Level Risk

Neutralizes: Full device takeover, remote access and control, persistence and evasion, ransomware, deepfake-assisted eKYC bypass.

Mobile banking apps run on devices the bank does not own or control. Full device remote access allows attackers to control taps, swipes, and inputs inside the banking app in real time. Ransomware modules can encrypt device files and lock customers out entirely. When the device is compromised at this level, every downstream control weakens.

Banks should implement controls that:

- Identify rooted, jailbroken, or compromised devices
- Detect active malware and fraud-related behaviors on the device
- Monitor for ransomware activity
- Apply adaptive session controls based on real-time device risk posture
- Terminate or step up authentication for high-risk sessions before fraud executes

Visibility into device risk allows banks to act before fraud reaches backend systems — not after.

Conclusion

Mobile banking fraud has shifted from credential abuse to device-level compromise. Modern malware operates inside trusted sessions, impersonates legitimate users, adapts in real time, and scales globally. For financial institutions, the mobile device is no longer a peripheral channel.

It is a primary execution environment for fraud. Reducing exposure requires extending security beyond backend systems to include mobile application hardening, runtime protection, and device risk visibility.

Banking institutions that treat mobile app security as a core component of fraud prevention and technology risk governance will be better positioned to reduce financial loss and maintain regulatory trust.

About Zimperium

Zimperium is the world leader in AI-empowered mobile security. Purpose-built for mobile, Zimperium provides unparalleled protection for mobile applications and devices, leveraging the power of AI to deliver autonomous mobile security that counters evolving threats including mobile phishing (mishing), malware, app vulnerabilities, app tampering, device compromise, and even zero-day attacks. Cybercriminals have adopted a mobile-first attack strategy, targeting your most vulnerable attack surface - the mobile apps and devices that your organization and customers depend upon.

Headquartered in Dallas, Texas, Zimperium is backed by Liberty Strategic Capital and SoftBank. Learn more at **zimperium.com** and connect on LinkedIn and X (@Zimperium).

Affiliations

Zimperium is a member of the App Defense Alliance and an active partner in the malware mitigation program, which aims to quickly find Potentially Harmful Applications (PHAs) and stop them before they ever make it onto Google Play.

Appendix

Documented Banking Malware Campaigns from zLabs

The techniques and new malware capabilities discussed in this report are not hypothetical. The following zLabs research publications document active mobile banking malware campaigns that illustrate use of the techniques discussed in this report.

1. **Extended IOCs for TaxiSpy Android Banking Malware**
   zLabs uncovered 60 additional TaxiSpy samples beyond those initially reported — an Android banking RAT that intercepts OTPs, harvests credentials, and hands attackers full remote control of the infected device.
   https://zimperium.com/blog/extended-iocs-for-taxispy-android-banking-malware

2. **Tap-and-Steal: The Rise of NFC Relay Malware on Mobile Devices**
   Demonstrates how attackers use NFC relay techniques to enable unauthorized contactless payments and ATM withdrawals.
   https://zimperium.com/blog/tap-and-steal-the-rise-of-nfc-relay-malware-on-mobile-devices

3. **Mishing in Motion: Uncovering the Evolving Functionality of FakeCall Malware**
   Highlights the use of mobile phishing and call interception to socially engineer victims and bypass traditional controls.
   https://zimperium.com/blog/mishing-in-motion-uncovering-the-evolving-functionality-of-fakecall-malware

4. **Hook Version 3: The Banking Trojan with The Most Advanced Capabilities**
   Examines advanced runtime manipulation, session hijacking, and device control techniques.
   https://zimperium.com/blog/hook-version-3-the-banking-trojan-with-the-most-advanced-capabilities

5. **NGate: NFC Relay Malware Enabling ATM Withdrawals Without Physical Cards**
   Documents real-world abuse of mobile devices to bypass card-present safeguards.
   https://zimperium.com/blog/ngate-nfc-relay-malware-enabling-atm-withdrawals-without-physical-cards

6. **PixRevolution: The Agent-Operated Android Trojan Hijacking Brazil's PIX Payments in Real Time**
   Android banking trojan specifically targeting Pix payment system and implicitly targeting most Brazilian financial institutions.
   https://zimperium.com/blog/pixrevolution-the-agent-operated-android-trojan-hijacking-brazils-pix-payments-in-real-time

External References

- **ABA/Morning Consult — 54% mobile primary channel, more than doubled since 2017**
  https://bankingjournal.aba.com/2025/11/aba-survey-bank-apps-continue-to-be-most-popular-option-among-customers/
- **Fraudulent activity in financial services up 21%, 1 in 20 verification attempts fraudulent — Veriff Future of Finance Report**
  https://www.globenewswire.com/news-release/2024/12/03/2990577/0/en/Veriff-2025-Identity-Fraud-Report-Online-Fraud-is-Up-by-21.html
- **80% of fraud occurs via online/mobile channels**
  https://coinlaw.io/digital-payment-fraud-statistics/

Regulatory References

- Monetary Authority of Singapore
  https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines
- Safe App Standard 2.0
  https://www.mas.gov.sg/regulation/standards/safe-app-standard
- Bank Negara Malaysia- RMiT
  https://www.bnm.gov.my/documents/20124/761679/RMiT.pdf
- Reserve Bank of India - Framework for Digital Payment Security Controls
  https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11666
- Digital Operational Resilience Act (DORA) - Official EU regulation text
  https://eur-lex.europa.eu/eli/reg/2022/2554/oj
- Hong Kong Monetary Authority - Risk Management of E-banking
  https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-E-1.pdf
- Central Bank of the UAE - Consumer Protection Regulation
  https://www.centralbank.ae/en/regulation/consumer-protection/
- UAE Information Assurance / Cybersecurity Standards
  https://www.centralbank.ae/en/regulation/cybersecurity/
- Payment Services Directive 2
  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366
- Payment Services Directive 3 (proposal)
  https://finance.ec.europa.eu/publications/proposal-payment-services-directive-psd3_en
- Securities and Exchange Board of India
  CSCRF Framework
  https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities_85690.html
- Australian Prudential Regulation Authority
  https://www.apra.gov.au/prudential-standard-cps-234-information-security

Indicators of Compromise

You can find the IOCs for banking trojans in the GitHub repository link below.
https://github.com/Zimperium/IOC/tree/master/2026-Banking-Heist

Authors & Research

Authored by Krishna Vishnubhotla, Vice President of Product Strategy, Zimperium, with research conducted by Zimperium s zLabs threat intelligence team.

zLabs Research Team: Aazim Bill Se Yaswant, Vishnu Pratapagiri, Rajay Goyal, Fernando Sanchez Ortega, Gianluca Braga.

ZIMPERIUM®