YinkoShield

June 30, 2025

The New Frontier: How advanced malware from Asia is Targeting Africa's Financial Sector

Presented by
Yinkozi's engineering team

Contents

The New Frontier: How Migrating Threat Actors and Advanced Mobile Malware are Reshaping Risk in Africa's Financial Sector

I. Executive Summary

The African financial sector is no longer a secondary target but a primary battleground for some of the world's most sophisticated, financially motivated cybercrime syndicates. The period between June 2024 and June 2025 was defined by two converging and deeply concerning trends: the deployment of highly advanced Android and iOS banking trojans and the strategic migration of mature threat actors from Asia into Africa. This evolution marks a fundamental shift in the continent's risk profile, demanding an immediate and proportional response from financial institutions, regulators, and cybersecurity bodies.

The central finding of this report is the confirmation of a direct threat migration corridor from Asia to Africa. Evidence confirms that well-organized, Chinese-speaking cybercrime groups, such as the notorious **GoldFactory**, are actively expanding their operations from their traditional hunting grounds in Southeast Asia into African nations.[1]

The deployment of the **Gigabud** trojan, a sibling malware to the Asia-focused **GoldDigger**, in **South Africa and Ethiopia** provides a direct, traceable link, demonstrating that Africa is the new operational frontier for these mature syndicates.[3] This is not opportunistic spillover; it is a calculated expansion into a region perceived as having a high-growth, target-rich, and less-defended mobile financial ecosystem.

Compounding this trend is the unprecedented level of malware sophistication being deployed. Threat actors are not using legacy tools but are bringing their most advanced and innovative arsenals to bear on the African market. The **GoldPickaxe** trojan, a key component of the GoldFactory malware suite, introduces a paradigm-shifting threat: the harvesting of facial recognition data from both Android and iOS users to create AI-powered deepfakes.[5] This technique, capable of bypassing modern biometric authentication systems, was perfected in response to enhanced security measures in Asia and is now poised for widespread deployment in Africa.[5]

The mobile threat landscape during this period was dominated by several key malware families and incidents. Beyond the groundbreaking GoldFactory suite, established Android banking trojans like **Anatsa** and **Grandoreiro** continued to inflict significant financial damage through on-device fraud and sophisticated overlay attacks (a technique where malware places a fake, often invisible, window over a legitimate app to steal credentials or trick the user into performing unintended actions).

Simultaneously, hyper-localized threats such as the **Tria Stealer** in Nigeria leveraged trusted mobile messaging platforms like WhatsApp for distribution, effectively bypassing traditional app store security controls and exploiting social trust networks.[28]

The financial impact of this new wave of attacks is severe and paradoxical. While some metrics, such as the rate of simple fraudulent transactions, show a decline in certain markets, the overall financial *losses* from cybercrime are skyrocketing.[33] This indicates a strategic shift by adversaries away from high-volume, low-value fraud towards targeted, high-impact attacks that cause catastrophic losses per incident.

The strategic imperative for African financial institutions is clear and urgent. The defensive posture must evolve from guarding against opportunistic, localized threats to countering persistent, well-resourced, and globalized adversaries. This necessitates a fundamental shift towards mobile-centric security architectures, investment in advanced threat intelligence capabilities, and the deployment of defenses capable of thwarting AI-driven and biometric-focused attacks. This technological adaptation must also contend with a market where zero-rated services for popular applications are common and a majority of users rely on low-end devices, creating unique security constraints and opportunities for exploitation. The battle for the future of Africa's digital financial services is underway, and the front line is the mobile device.

II. Africa's Mobile Financial Ecosystem: A Confluence of Opportunity and Risk

The escalating cyber threat targeting Africa's financial sector is not occurring in a vacuum. It is a direct consequence of the continent's explosive, mobile-led digital transformation, which has created an environment of unprecedented opportunity for both economic development and criminal exploitation. This confluence of rapid growth and inherent vulnerabilities has made Africa an irresistible target for global cyber adversaries.

The Mobile-First Revolution

The scale and pace of Africa's adoption of mobile financial services are staggering, establishing the primary "pull" factor for threat actors. In 2024, the global mobile money industry achieved two monumental milestones: surpassing two billion registered accounts and reaching over half a billion monthly active accounts.[35] The engine of this growth was Sub-Saharan Africa. The number of registered mobile money accounts in the region doubled in just four years, from 2020 to 2024, to exceed one billion. This growth in user base corresponds directly with transaction value, which globally

surpassed $1.68 trillion in 2024, with Africa being a principal driver.[35] This hyper-growth has created a vast and lucrative pool of potential targets for financially motivated criminals.

The Widening Attack Surface

This rapid, often leapfrogging, adoption of digital services has outpaced the development of commensurate security infrastructure and user awareness, creating a uniquely vulnerable ecosystem. The direct correlation between usage and risk is stark. A 2024 survey revealed that 85% of respondents across several African nations use mobile financial services, while in Kenya, the Communications Authority reported a 333% surge in detected mobile application threats in a single quarter of 2024, primarily aimed at stealing user credentials.

Several factors exacerbate this vulnerability:

- **Device Security:** Financial transactions are frequently conducted on secondhand or less-secure devices that may lack the latest security patches or contain pre-existing vulnerabilities, elevating both the risk and potential impact of an attack.
- **Blurred Digital Boundaries:** The distinction between personal and professional device usage has effectively vanished. A 2025 survey found that 93% of respondents use mobile messaging platforms like WhatsApp for work-related communication. This trend creates a dangerous bridge for attackers, allowing them to compromise a less-secure personal device and pivot to attack corporate financial systems and data.
- **User Awareness Gaps:** While concern about cybercrime is rising, user understanding of security best practices lags. A 2025 survey noted that user comprehension of what constitutes a strong password slightly decreased, and the percentage of users "very unlikely" to give away personal information was halved compared to 2023, indicating a worrying level of ease with which sensitive data is shared.[10]

The convergence of these factors creates a perfect storm for cybercriminals. On one hand, there is a target-rich environment characterized by a massive, rapidly expanding user base and high transaction volumes. On the other hand, this environment is comparatively less defended. Reports from INTERPOL and other security bodies consistently highlight that many African nations still lack mature cybersecurity infrastructure, comprehensive legal frameworks, and streamlined international cooperation capacity to effectively combat cross-border cybercrime.[7]

This dynamic is further amplified by external pressures on threat actors. As law enforcement in traditionally targeted regions like Southeast Asia intensifies, criminal syndicates are actively seeking new territories where they can operate with a higher probability of success and a lower risk of disruption.[1] Africa, with its unique combination of high growth and developing defenses, presents not just an opportunity but a strategic imperative for these groups. Their migration is not a random drift but a calculated business decision, pushed by enforcement in Asia and pulled by the immense economic potential of Africa's digital frontier.

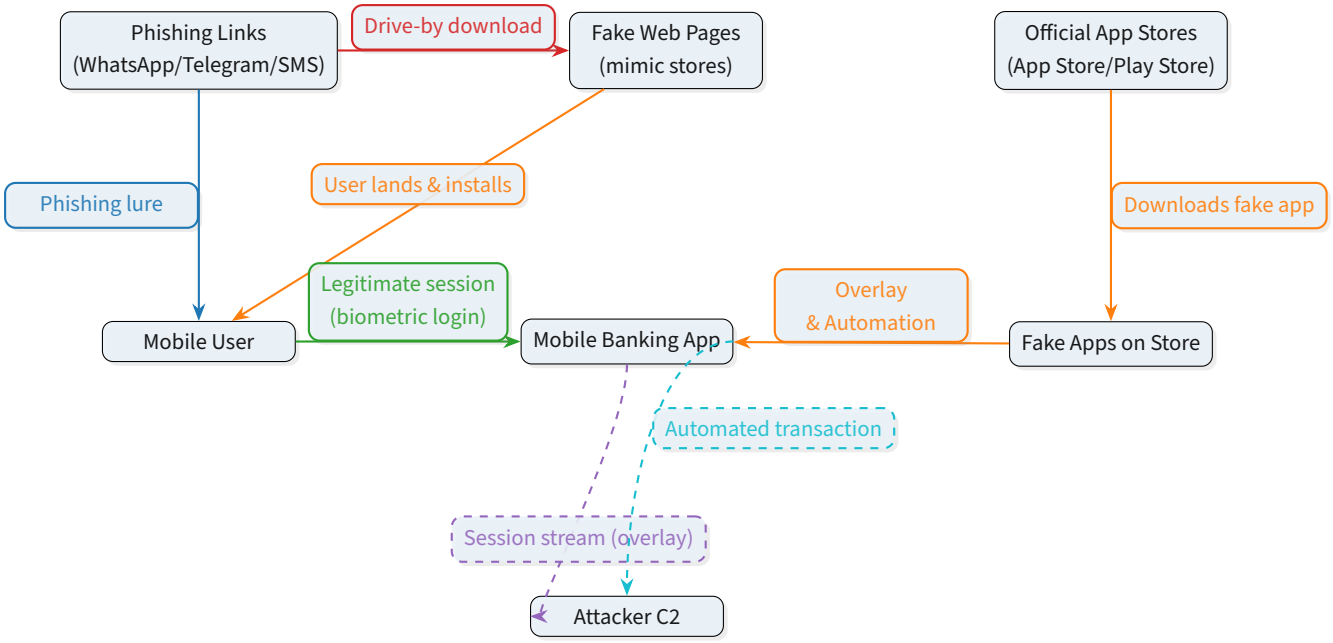

Figure 1: Expanded attack surface in Africa's mobile financial ecosystem, showing phishing vectors, fake pages/apps, and malware modus operandi (session overlay streaming and automation).

III. The Evolving Mobile Threat Arsenal: A Deep Dive into Prevalent Malware Families

The adversaries targeting Africa's financial sector are deploying a diverse and increasingly sophisticated arsenal of mobile malware. The threat landscape is characterized by the continued prevalence of established banking trojans, the introduction of groundbreaking malware families with novel capabilities, and the emergence of hyper-localized threats that exploit regional communication habits.

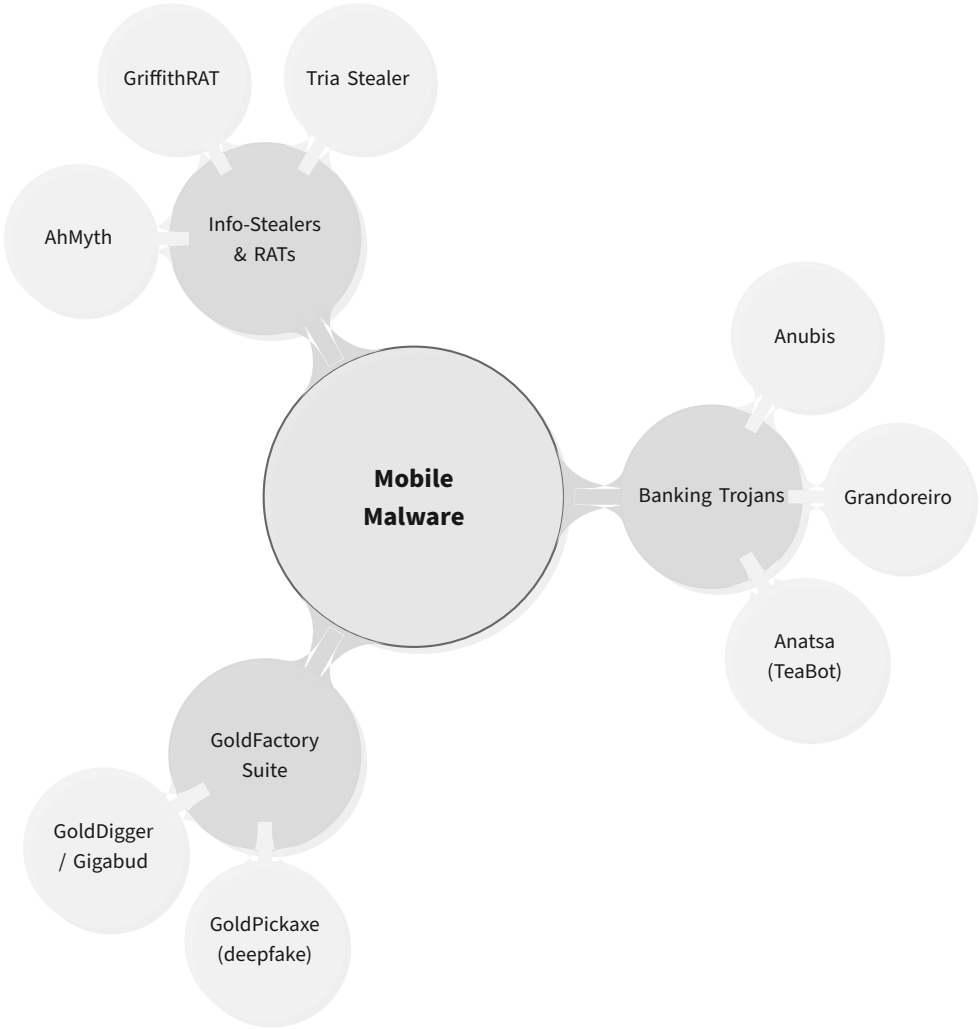

Figure 2: Taxonomy of major mobile malware families targeting Africa.

A. Established Android Banking Trojans: The Persistent Threat

Even as new threats emerge, well-known Android banking trojans remain a potent and persistent danger, causing significant financial losses through proven attack methodologies.

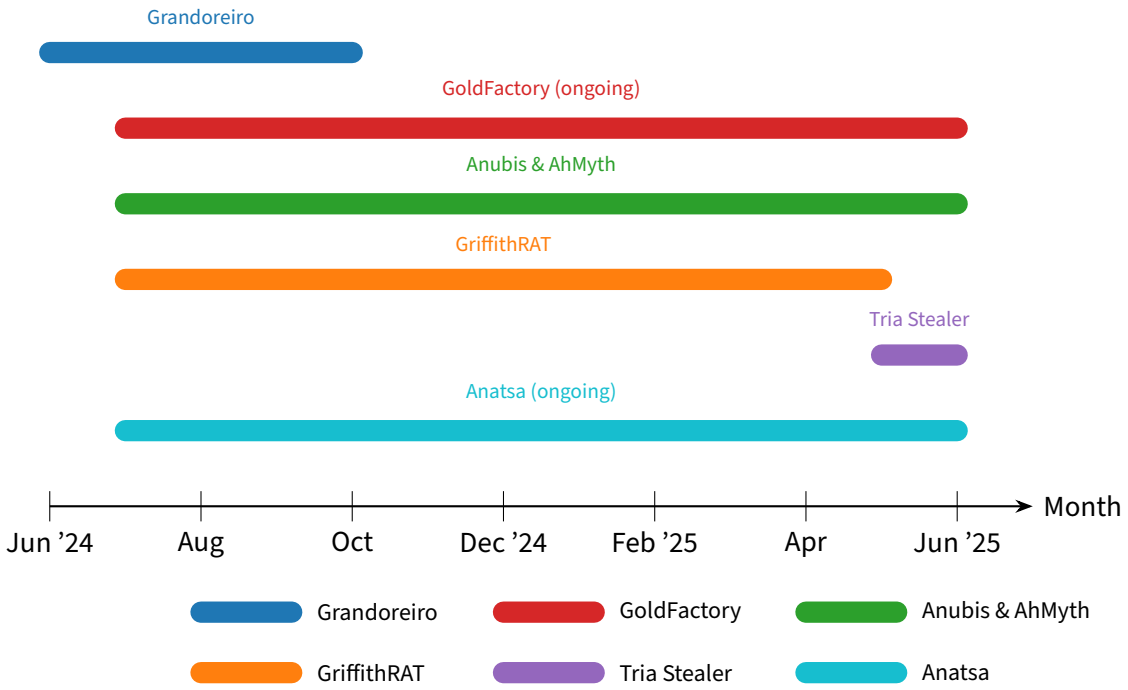

Figure 3: Timeline of key mobile malware activity (June 2024–June 2025).

- **Anatsa (TeaBot/Toddler):** This powerful Android banking trojan continues to pose a severe threat across the continent. In July 2024, Nigeria's Computer Emergency Response Team (ngCERT) issued a specific advisory warning of Anatsa campaigns targeting Android users in the country. Anatsa's primary modus operandi involves abusing Android's Accessibility Services. Once a user is tricked into granting these powerful permissions, the malware can perform overlay attacks, where it displays a fake login screen on top of a legitimate banking app to steal credentials. More dangerously, it can conduct full Device Takeover (DTO) fraud, allowing the attacker to remotely control the device to initiate and authorize transactions. This technique is particularly insidious because, from the bank's perspective, the fraudulent transactions appear to originate from the victim's legitimate, trusted device, making them exceptionally difficult for traditional anti-fraud systems to detect.
- **Grandoreiro:** This banking trojan, often distributed as part of a Malware-as-a-Service (MaaS) model under the "Tetrade" umbrella, has also been highly active. An ngCERT advisory from May 2024 noted that Grandoreiro was targeting over 41 banking applications in Nigeria. Earlier in 2024, campaigns involving the trojan were observed impersonating South African government entities, a tactic used to lend credibility to phishing lures. Grandoreiro is typically distributed via phishing emails and is designed to steal banking credentials and search for cryptocurrency wallets on compromised devices. Its operators employ technical evasion techniques such as binary padding, inflating the malware's file size with large images to bypass security scanners,

demonstrating a continuous effort to outwit defenses.

B. The GoldFactory Arsenal: A New Caliber of Threat

The arrival of the GoldFactory malware suite represents a significant escalation in the sophistication of threats facing the African financial sector. Attributed to a well-organized, Chinese-speaking cybercrime group, this family of malware introduces advanced evasion techniques and novel attack vectors previously unseen on the continent.[5]

- **GoldDigger & GoldDiggerPlus:** These are the foundational Android trojans in the GoldFactory suite.
  - **GoldDigger** was first identified in mid-2023 targeting over 50 financial institutions in Vietnam.[13] It is distributed through fake websites that impersonate the Google Play Store or legitimate corporate portals.[19]
  - Like Anatsa, it heavily abuses the Accessibility Service to scrape on-screen text, including usernames, passwords, and intercept SMS-based one-time passcodes.[19]
  - A key indicator of its sophistication is its use of **Virbox Protector**, a legitimate commercial software packer. This tool significantly complicates reverse engineering and allows the trojan to evade detection by many security products.[3]

  GoldDiggerPlus marks an evolution of this malware family. It embeds a secondary trojan, **GoldKefu**, which introduces:
  - Overlay attacks with highly convincing fake banking UIs
  - Real-time, interactive voice calls to victims, enhancing social engineering techniques and increasing the likelihood of account compromise.[5]
- **GoldPickaxe: The Biometric Game-Changer:** GoldPickaxe is arguably the most alarming innovation from the GoldFactory group. It is a novel trojan designed to attack both **iOS and Android** platforms—a significant advancement given the robust security of Apple's ecosystem.[13]
  - On iOS, it bypasses App Store protections using social engineering to distribute the app via Apple's **TestFlight** platform (intended for beta testing) or through installation of a malicious **Mobile Device Management (MDM)** profile.[18]
  - The MDM profile grants attackers sweeping control over the device, including the ability to silently install applications and intercept network traffic.

- GoldPickaxe introduces a new threat category: the harvesting of **biometric data**. Rather than stealing credentials alone, the malware tricks users into recording a video of their face—typically under the guise of identity verification.[5]
- This facial video is processed by AI to create highly realistic **deepfakes**, which are used to bypass *liveness checks* in banking applications. This allows attackers to access the victim's bank account from their own devices and approve transactions.[5]
- This technique was reportedly developed specifically to defeat enhanced facial recognition measures deployed by banks in Thailand, showing the group's rapid adaptation to emerging security defenses.[5]

C. Other Emerging Mobile Threats

Alongside these major malware families, other potent threats have emerged, often tailored to specific regional contexts.

- **Tria Stealer (Nigeria):** In June 2025, ngCERT issued an alert regarding a highly evasive malware campaign in Nigeria dubbed Tria Stealer.[28]
  - This info-stealer spreads through fake wedding or event invitations shared via **WhatsApp and Telegram**. This distribution method bypasses app store vetting entirely and leverages social trust networks, as users are more likely to open files from known contacts.
  - Once installed, Tria Stealer hijacks messaging accounts, intercepts OTPs, steals data from financial apps, and communicates with its command-and-control (C2) server via Telegram bots—blending malicious activity with legitimate traffic.[28]
- **Anubis & AhMyth:** According to a 2025 threat report, these two malware families were among the most prevalent mobile threats active in Africa.[4]
  - **Anubis** is a mature and versatile Android banking trojan. While initially focused on credential theft, it has evolved to include keylogging, ransomware features, and full Remote Access Trojan (RAT) functionality.[4]
  - **AhMyth** is an open-source Android RAT, widely adopted due to its accessibility. Typically disguised as a utility or game, it grants attackers deep access to a victim's device, including screen capture, camera and microphone surveillance, and SMS interception.[4]

The following table provides a consolidated overview of the major mobile-focused malware campaigns that characterized the threat landscape between June 2024 and June 2025.

Table 1: Inventory of Major Mobile-Focused Malware Campaigns Targeting African Financial Sector (June 2024 - June 2025)

Campaign/ Malware Name	Malware Type	Primary African Countries Targeted	Known Financial Sector Targets	Key Modus Operandi	Attributed Threat Actor(s)	Period of Peak Activity/ Reporting
GoldFactory Suite (GoldDigger, GoldPickaxe, Gigabud)	Android/ iOS Banking & Biometric Trojan	South Africa, Ethiopia (Gigabud); Threat expanding from APAC	Banking customers, mobile banking apps	Abuse of Accessibility Services, AI-driven deepfakes for biometric bypass, MDM profile abuse, TestFlight distribution, Virbox packer for evasion. [3]	**Gold-Factory** (Chinese-speaking cyber-crime group)	2024 - 2025
Tria Stealer	Android Info-Stealer	Nigeria	WhatsApp, Telegram, and banking app users	Distribution via malicious APKs on WhatsApp/ Telegram, OTP interception, credential theft, C2 via Telegram bots. [28]	Un-specified	June 2025

Campaign/ Malware Name	Malware Type	Primary African Countries Targeted	Known Financial Sector Targets	Key Modus Operandi	Attributed Threat Actor(s)	Period of Peak Activity/ Reporting
Anatsa (TeaBot/ Toddler)	Android Banking Trojan	Nigeria	Mobile banking app users	Dropper apps on Google Play, abuse of Accessibility Services, overlay attacks, Device Takeover (DTO) fraud.	Un-specified for Nigerian campaign	July 2024 (Nigeria advisory), ongoing
Grandoreiro	Banking Trojan	Nigeria, South Africa	Over 41 Nigerian banking apps; impersonated SA government entities	Phishing emails, credential theft, binary padding, DLL sideloading.	MaaS operators ("Tetrade" umbrella)	Early - Mid 2024
GriffithRAT	Remote Access Trojan (RAT)	Africa (unspecified countries)	Fintech companies, online trading platforms	Spread via Skype/ Telegram disguised as financial reports; credential theft, keylogging, screen/ webcam capture.	Cyber mercenaries	Late 2024 - May 2025

Campaign/ Malware Name	Malware Type	Primary African Countries Targeted	Known Financial Sector Targets	Key Modus Operandi	Attributed Threat Actor(s)	Period of Peak Activity/ Reporting
Anubis & AhMyth	Android Banking Trojan /RAT	Africa (general)	Mobile banking users	Distribution via malicious apps, keylogging, screen capture, SMS interception, ransomware functions (Anubis). [4]	Various operators	2025

IV. The Migration of Malice: Tracing Threat Corridors from Asia to Africa

The emergence of highly sophisticated malware like the GoldFactory suite in Africa is not an isolated phenomenon. It is the most visible evidence of a broader, strategic migration of organized cybercrime syndicates from Asia to the African continent. This section presents a layered, evidence-based analysis of this threat migration, tracing the macro trends and specific malware trajectories that connect these two regions.

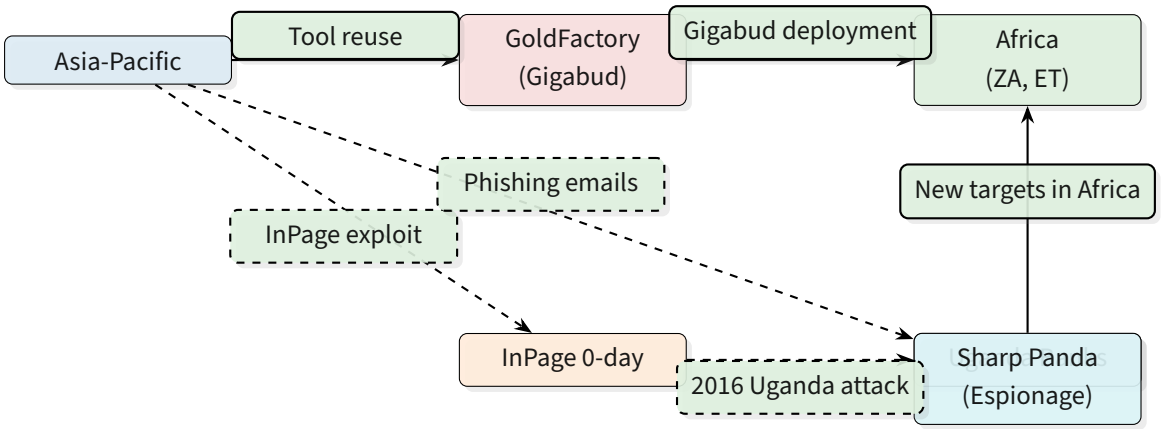

Figure 4: Traceable corridors of threat migration from Asia into Africa, including GoldFactory's Gigabud deployment, the 2016 InPage attack in Uganda, and state-aligned phishing by Sharp Panda.

A. The Macro Trend: Asian Crime Syndicates Go Global

High-level intelligence from international bodies provides the strategic context for this migration. Reports from the United Nations Office on Drugs and Crime (UNODC) published in 2025 confirm a deliberate global expansion of East and Southeast Asian organized crime groups.[1] This expansion is fueled by two primary drivers. First, the immense profitability of their operations, with cyberfraud generating an estimated $37 billion in losses in East and Southeast Asia in 2023 alone, provides the capital for global expansion.[1] Second, increasing and coordinated law enforcement pressure in their traditional operating zones such as Cambodia, Laos, and Myanmar is forcing these syndicates to hedge their bets and establish new, less-contested bases of operation.[1]

Crucially, the UNODC has explicitly identified Africa as a key destination for this expansion, naming nations such as **Zambia, Angola, and Namibia** as new footholds for these syndicates.[1] This is not a future possibility but a current reality. These groups are actively establishing a presence on the continent, bringing with them their operational maturity, technical expertise, and vast financial resources.

B. Primary Evidence - The Gigabud Trajectory: A Smoking Gun

While the UN reports provide the strategic overview, malware analysis provides the forensic proof. The most compelling evidence of this direct migration comes from tracing the operational path of the Gigabud trojan.

The first step in establishing this link is understanding the connection between the GoldDigger and Gigabud malware families. Cybersecurity researchers have confirmed that these two trojans share significant portions of their source code and utilize the same distinct technical components, such as the "libstrategy.so" library for UI interaction and the Virbox packer for evasion.[3] This level of similarity indicates with high confidence that they are developed and operated by the same threat actor: the GoldFactory group.[3]

The second step is to map their deployment. The GoldDigger trojan was first discovered with a narrow focus, targeting financial applications almost exclusively in Vietnam.[13] In contrast, the Gigabud trojan, while also active in Asia (targeting Thailand and the Philippines), saw its attack scope rapidly expand. Analysis has confirmed that Gigabud campaigns have been actively deployed against targets in **South Africa and Ethiopia**.[3]

This trajectory provides a direct, traceable path of a threat actor's expansion from Asia into Africa. It is not a case of different groups imitating tactics. It is one specific, highly sophisticated Asian threat actor (GoldFactory) taking a toolset proven in one region (GoldDigger in Vietnam) and deploying a variant of it (Gigabud) in a new target region (Africa). This serves as the "smoking gun" that validates the threat migration thesis, demonstrating a clear and deliberate extension of operations.

C. Historical Precedent: The InPage Zero-Day Attack

This intercontinental attack corridor is not an entirely new phenomenon, though its scale and sophistication have increased dramatically. A 2016 report from Kaspersky provides a historical precedent for this trend.[25] The report detailed a series of attacks that leveraged a zero-day vulnerability in

InPage, a specialized text editor software package popular among Urdu and Arabic speakers. The software's primary user base is in South Asia, particularly India and Pakistan.[25]

The attackers used this zero-day exploit, delivered via spear-phishing emails, to target banks. The campaign was not limited to Asia, where organizations in Myanmar and Sri Lanka were attacked. The very same exploit was used to compromise banking targets in **Uganda**.[25] This incident, nearly a decade ago, demonstrates that threat actors have long understood the potential of using tools and exploits common in the Asian threat landscape to attack targets within the African financial sector. It establishes that this attack vector has existed for years, and the current wave of migration represents a massive escalation along this pre-existing corridor.

D. The Broader Influx: Beyond Financially Motivated Crime

The migration of malicious actors from Asia to Africa extends beyond purely financial cybercrime, encompassing state-aligned espionage activities that also pose a significant risk to the financial sector. The China-linked cyber espionage group known as **Sharp Panda** (or Sharp Dragon) has been observed expanding its targeting to include governmental organizations in Africa and the Caribbean.[26]

These espionage campaigns often align with China's broader strategic and technological initiatives in the region, such as the Digital Silk Road project. Consequently, their targets frequently include critical sectors like telecommunications, government bodies, and financial institutions.[26] The modus operandi of groups like Sharp Panda involves using compromised email accounts in Southeast Asia to send phishing emails to new targets in Africa, further cementing the Asia-to-Africa attack vector.[26] The presence of these state-aligned actors demonstrates that the "migration of malice" is a multifaceted trend. It involves a complex ecosystem of actors, from profit-driven criminals to intelligence-gathering spies, all of whom view Africa as a strategic priority and whose activities can directly or indirectly impact the stability and security of the continent's financial institutions.

V. Threat Actor Spotlight: Profiling the Adversaries

Understanding the threats to Africa's financial sector requires profiling the diverse array of actors behind the attacks. The landscape is not monolithic; it is a complex ecosystem of adversaries with different origins, motivations, and capabilities. These range from highly sophisticated international syndicates and state-sponsored groups to specialized access brokers and local criminal networks.

A. GoldFactory (The Innovators)

- **Profile:** GoldFactory is a highly sophisticated, resourceful, and well-organized Chinese-speaking cybercrime group that has been active since at least mid-2023.[5] They are considered an emerging group whose AI-driven attack methods have the potential to disrupt the financial systems of targeted countries.[17]
- **Motivation:** Their primary motivation is direct financial gain through advanced banking fraud.[17]
- **Signature TTPs:** GoldFactory's hallmark is innovation. They are responsible for developing and deploying a complex suite of mobile trojans, including GoldDigger, GoldDiggerPlus, and the groundbreaking GoldPickaxe.[5] Their most notable TTP is pioneering the use of AI-driven deepfakes to bypass biometric authentication, a technique previously unseen in mobile banking malware.[18] They also demonstrate technical prowess through their use of legitimate software packers like Virbox for evasion and their ability to target multiple platforms, including both Android and iOS.[13]
- **Significance:** The presence of GoldFactory in the African threat landscape represents a significant escalation. They are not simply using off-the-shelf malware but are developing and deploying top-tier, custom tools. Their activity elevates the baseline threat level for all financial institutions on the continent.

B. Initial Access Brokers - e.g., CL-CRI-1014 (The Door Openers)

- **Profile:** Tracked by Palo Alto Networks' Unit 42, CL-CRI-1014 is an intrusion set that has been actively targeting financial organizations across Africa since at least 2023.[8]
- **Motivation:** This group operates as an Initial Access Broker (IAB). Their business model is not to conduct the final fraud themselves but to gain the initial foothold into a corporate network and then sell that access to other criminal groups on dark web markets.[8]
- **Signature TTPs:** CL-CRI-1014 employs a consistent and effective playbook that relies on open-source and publicly available tools rather than custom malware. Their toolkit includes the

PoshC2 attack framework, the **Chisel** tunneling utility for bypassing firewalls, and remote administration tools like **Classroom Spy** for reconnaissance and control.[8] They focus on stealth and functionality, using techniques like signing their tools with stolen certificates to evade detection.[21]

- **The Symbiotic Threat Supply Chain:** The existence of distinct actor types like GoldFactory (the specialists in financial theft) and CL-CRI-1014 (the specialists in network intrusion) points to a disaggregated and highly efficient cybercrime supply chain. An IAB can breach an African bank's network and then sell that privileged access to an affiliate of a MaaS operation like Grandoreiro or a sophisticated group like GoldFactory, who then deploys their specialized malware to extract funds. This division of labor lowers the barrier to entry for conducting high-impact attacks, increases operational efficiency for the criminals, and makes attribution incredibly challenging for defenders.

C. State-Sponsored & State-Aligned Actors (The Spies)

- **Sapphire Sleet:** Microsoft's designation for Bluenoroff, a subgroup of the Lazarus Group, also known as APT38. This notorious North Korean state-sponsored group is infamous for conducting large-scale financial heists to generate revenue for the Pyongyang regime. Its specialized subgroup, **Bluenoroff**, focuses exclusively on attacking financial institutions worldwide.[6] Their victimology explicitly includes entities in Africa, and their motivations make any financial institution a potential target for a major cyber-heist.[6]
- **Sharp Panda:** As detailed previously, this China-linked espionage group has expanded its operations into Africa, targeting government and other strategic sectors.[26] While their primary goal is intelligence gathering, their targeting of government bodies can have direct spillover effects on the financial sector, particularly state-owned banks or institutions involved in national critical infrastructure. Their use of phishing and exploitation of 1-day vulnerabilities to deploy backdoors like Cobalt Strike represents a persistent, advanced threat.[26]

D. Cyber Mercenaries & Local Criminal Networks

- **GriffithRAT Operators:** The discovery of GriffithRAT highlights the role of "cyber mercenaries" in the African threat landscape. These are for-hire threat actors who conduct targeted attacks on behalf of a third-party client. GriffithRAT, a sophisticated RAT spread via mobile messaging apps like Skype and Telegram, was used to target fintech companies, online trading platforms, and betting operators in Africa, demonstrating a clear mobile-centric attack vector against the financial sector by these hired guns.

- **Operation Red Card Networks:** The dismantling of several criminal networks by INTERPOL's Operation Red Card provides a ground-level view of mobile-focused crime in Africa. These cross-border syndicates relied heavily on less technically complex but highly effective mobile vectors. This included groups in Zambia using malware spread via malicious links in mobile messages to take over phones and access banking apps, Rwandan groups using social engineering via mobile calls for fraud, and South African syndicates using SIM boxes for mass SMS phishing (smishing) attacks.

The following table provides a comparative profile of these key adversary types.

Table 2: Threat Actor Profile Matrix

Actor/Group	Likely Origin/Affiliation	Primary Motivation	Signature Mobile-Relevant TTPs	Known African Targets
GoldFactory	Chinese-speaking cybercrime	Direct Financial Gain	AI-driven biometric deepfakes, iOS malware via TestFlight/MDM, advanced Android trojans with Virbox packer. [3]	Financial Institutions (South Africa, Ethiopia)
CL-CRI-1014	Initial Access Broker (IAB)	Access-as-a-Service	Use of open-source tools (PoshC2, Chisel) for network intrusion; not directly mobile-focused but enables mobile malware deployment. [8]	General Financial Sector (Africa-wide)
Lazarus (Bluenoroff)	North Korean State-Sponsored	State Funding /Financial Heist	Sophisticated malware frameworks, targeting of financial infrastructure (e.g., SWIFT), trojanized crypto apps. [6]	Financial Institutions (Africa included in global targeting)
Sharp Panda	China-linked Espionage	Intelligence Gathering	Phishing via compromised emails, deployment of backdoors like Cobalt Strike. [26]	Government, Financial Institutions
GriffithRAT Operators	Cyber Mercenary	Hired-to-Attack	Sophisticated RATs (GriffithRAT) distributed via mobile messaging apps (Skype, Telegram).	Fintechs, Online Trading Platforms

Actor/Group	Likely Origin/Affiliation	Primary Motivation	Signature Mobile-Relevant TTPs	Known African Targets
Operation Red Card Syndicates	Local/Regional Criminal Networks	Direct Financial Gain (Fraud)	Social engineering via mobile calls, malware via SMS links (smishing), SIM box fraud.	Mobile Banking Users (Zambia, Rwanda, SA, etc.)

VI. Regional Deep Dive: Nigeria and South Africa as Threat Epicenters

As Africa's two largest economies with rapidly growing digital populations, Nigeria and South Africa serve as bellwethers for the continent's mobile security challenges. While both are prime targets, their specific threat landscapes exhibit distinct characteristics, reflecting different stages of digital maturity and unique criminal ecosystems.

A. Nigeria: A Hub for Social Engineering and Mobile Fraud

Nigeria's vibrant and rapidly expanding digital economy makes it a focal point for cybercrime that often preys on user trust and exploits communication platforms.

- **Scale of the Problem:** The financial impact of fraud is staggering. According to the Nigeria Inter-Bank Settlement System (NIBSS), financial institutions lost an estimated ₦52.26 billion (approximately $32 million) to fraud in 2024.[14] This represents a monumental 350% increase in losses since 2020. This surge occurred even as the total number of reported fraud incidents *decreased*, a clear indicator that criminals are succeeding in fewer, but far more lucrative, high-impact attacks.[14]
- **Key Malware Campaigns:** Nigeria has been a key target for major international banking trojan campaigns. ngCERT issued specific advisories for both the **Anatsa** and **Grandoreiro** trojans, which were actively targeting Nigerian mobile banking users and applications. The more recent emergence of the **Tria Stealer** campaign in June 2025 highlights a trend towards hyper-localized threats. Tria Stealer's distribution via fake invitations on **WhatsApp** is particularly insidious in the Nigerian context, where the app is a primary tool for both personal and business communication, making the malware's propagation highly effective.[28]
- **Dominant Threat Landscape:** The Nigerian threat landscape is heavily characterized by phishing, smishing (SMS phishing), and various forms of banking and fintech fraud that rely on social engineering.[11] The use of AI to generate deepfake audio for voice phishing (vishing) scams, where criminals impersonate bank officials over mobile calls, has been flagged as a significant and growing concern. The success of these methods was further evidenced by Nigeria's inclusion in INTERPOL's Operation Red Card, which dismantled numerous scams facilitated through mobile messaging and applications.

B. South Africa: A Target for Advanced International Actors

With a more mature digital banking market, South Africa is increasingly in the crosshairs of the world's most sophisticated international threat actors, who deploy their advanced toolsets against its financial institutions.

- **Scale of the Problem:** The financial losses are substantial. The South African Banking Risk Information Centre (SABRIC) reported that digital banking and mobile app crime resulted in over R1 billion being stolen from consumers in 2023. Another report cited losses of over $180 million for local banks and their customers in the same year.[7] SABRIC's data for 2023 showed a 47% year-on-year rise in financial losses attributable to digital fraud, with fraud on banking apps accounting for 60% of all digital banking crime.[33]
- **Key Malware Campaigns & Indicators:** South Africa serves as a clear landing point for the Asia-to-Africa threat migration. It was explicitly named as a target country for the Asia-linked **Gigabud** trojan, a sibling of GoldDigger.[3] The country has also been heavily affected by the **Android.VO1D** botnet, with over 200,000 Android TV devices compromised by early 2025, creating a massive, indirect risk to mobile banking activities conducted on shared home networks. Other significant indicators include campaigns by the **Grandoreiro** trojan impersonating government entities and the dismantling of a large-scale SMS phishing operation by authorities during Operation Red Card.
- **The Deceptive Decline in Fraud Rates:** An analysis of conflicting data points from South Africa reveals a critical evolution in adversary tactics. On the surface, data from TransUnion shows an encouraging trend: the *rate* of suspected digital fraud in South Africa has fallen significantly, from 9.0% of transactions in 2020 to 4.6% in 2024, now below the global average.[12] However, this is directly contradicted by SABRIC's data, which shows that the financial *losses* from this same category of crime have surged.[33]

  This paradox is not a data error; it is a signal of a fundamental shift in criminal strategy. Attackers are moving away from easily detected, high-volume, low-value fraud attempts (such as basic card testing), which tend to inflate the overall "rate" of suspicious transactions. Instead, they are focusing on stealthy, sophisticated, low-volume, high-value attacks that are designed to bypass traditional fraud detection systems. Malware like Anatsa, which performs Device Takeover (DTO) fraud, and the techniques of GoldFactory, which use deepfakes to defeat biometric checks, are engineered to appear legitimate.

  These attacks are not flagged as suspicious by conventional rate-based models, yet they result in catastrophic losses per incident. This means that risk models based solely on transaction fraud rates are becoming obsolete and dangerously misleading. The greatest threat now lies not in the noise of frequent, low-level fraud, but in the silence of the successful, high-impact compromise.

The following table contrasts the key characteristics of the mobile threat landscapes in these two economic powerhouses.

Table 3: Regional Threat Snapshot: Nigeria vs. South Africa

Metric	Nigeria	South Africa
Mobile Banking Penetration	Rapidly growing user base with high adoption of mobile payments and fintech apps. [11]	High mobile banking usage (50% of surveyed individuals).
Reported Financial Losses	₦52.26bn (approx. $32m) lost to fraud in 2024, a 350% increase since 2020. [14]	>R1bn stolen via digital/mobile app crime in 2023; 47% rise in digital fraud losses. [33]
Key Active Malware	Anatsa, Grandoreiro, Tria Stealer. [28]	Gigabud, Grandoreiro, Android.VO1D. [3]
Dominant Attack Vectors	Social engineering, malware via WhatsApp/Telegram, phishing, vishing. [28]	Advanced trojans, large-scale SMS phishing, biometric attacks (emerging), indirect IoT threats. [3]
National CERT/Industry Body Focus	ngCERT advisories on Anatsa, Grandoreiro, Tria Stealer, and Android.VO1D. [28]	SABRIC warnings on rising digital fraud losses and mobile app crime; Operation Red Card dismantling of SIM box fraud. [33]

VII. The Future Battlefield: AI, IoT, and the Next Wave of Mobile Attacks

The mobile threat landscape is not static; it is a dynamic battlefield where adversaries continuously innovate to overcome defenses. Looking ahead, two interconnected trends are set to define the next wave of attacks against Africa's financial sector: the operationalization of Artificial Intelligence for fraud and the exploitation of the insecure Internet of Things (IoT) ecosystem that surrounds the mobile user.

A. AI-Driven Fraud: From Theory to Reality

For years, AI-driven fraud was a theoretical concern. In 2024 and 2025, it became an operational reality. The use of AI by threat actors has moved beyond automating phishing campaigns to fundamentally compromising the integrity of identity verification systems.

The most potent example of this is the **GoldPickaxe** trojan. Its ability to steal facial video data from victims and use it to generate deepfakes to bypass banking authentication is a real-world, in-the-wild capability.[5] This is not a proof-of-concept; it is a deployed weapon. The implications for Africa are profound. As financial institutions across the continent invest heavily in biometric authentication as a cornerstone of their security strategy, threat actors are already deploying tools specifically designed to defeat it.

This is corroborated by on-the-ground data. The Lagos-based digital identity verification company Smile ID reported a staggering sevenfold increase in the use of deepfake videos for impersonation attempts in Africa during the second half of 2024.[7] The company's 2025 report further states that generative AI is fueling a new wave of fraud across the continent, enabling criminals to create hyper-realistic fake documents and images with unprecedented precision.[34] This trend moves the threat beyond simple credential theft or overlay attacks to the compromise of "what you are" biometric factors, attacking the very foundation of modern digital trust.

B. The Compromised Personal Ecosystem: Mobile-Adjacent IoT Risk

The security of a mobile financial transaction no longer depends solely on the security of the mobile device itself. The proliferation of insecure, interconnected IoT devices, particularly those running versions of the Android operating system, has dramatically expanded the attack surface and created new vectors for compromising mobile users.

The **Android.VO1D** (also known as LinkDoor) botnet serves as a prime case study. This malware created a massive botnet by infecting Android-based TV boxes and smart TVs, with South Africa being one of the most heavily affected countries, home to over 200,000 compromised devices. While the botnet's

primary purpose may be ad fraud or serving as a proxy network, its presence on a user's home network poses a critical, indirect threat to their mobile banking activities.

This development signals the death of the traditional "castle and moat" security model for mobile banking. In this outdated model, the mobile device is the "castle," and security efforts are focused on hardening the device and the banking app within it. However, the Android.VO1D botnet compromises another device—a smart TV—that resides *inside* the trusted home network, effectively inside the moat. An attacker in control of a device on the same local Wi-Fi network as the user's mobile phone can launch a variety of devastating attacks. These include Man-in-the-Middle (MitM) attacks to intercept and alter communication between the phone and the bank, DNS spoofing to redirect the user to a malicious server, or direct credential harvesting from unencrypted traffic.

This forces a paradigm shift in how risk is assessed. Financial institutions can no longer consider the mobile device in isolation. The security of a banking transaction conducted on a smartphone now depends, in part, on the security posture of the user's smart TV, their connected speakers, and every other IoT gadget on their home network. This creates a vastly more complex risk environment that challenges traditional security models and requires a new approach to both technical controls and user education.

VIII. Fortifying the Front Lines: Strategic Recommendations for Mobile Security Resilience

To counter the sophisticated and evolving threats detailed in this report, African banks and fintechs must adopt a multi-layered, threat-informed, and forward-looking security strategy. The following recommendations are designed to build resilience against the specific tactics, techniques, and procedures (TTPs) being deployed by modern adversaries.

- **1. Evolve Authentication Beyond Static Biometrics:** The demonstrated ability of the GoldPickaxe trojan to defeat facial recognition with AI-generated deepfakes makes it imperative to move beyond simple biometric checks.[5] Institutions must invest in and deploy **dynamic liveness detection** technologies. These systems challenge the user with real-time, unpredictable prompts (e.g., "turn your head to the left," "smile") that are significantly more difficult for a static deepfake video or image to spoof.[34] Layering multiple authentication factors, including behavioral biometrics that analyze how a user interacts with their device, can further strengthen defenses against these advanced impersonation attacks.
- **2. Secure the Application Layer against Prevalent TTPs:** Mobile banking applications must be hardened from within to counter the specific methods used by prevalent malware. This includes:
  - **Countering Accessibility Service Abuse:** This is the core TTP for dominant trojans like Anatsa and GoldDigger.[13] Applications should incorporate mechanisms to detect and flag or block anomalous activity originating from Android's Accessibility Services, especially for high-risk actions like transaction authorization or credential entry.
  - **Implementing Anti-Overlay Detection:** To combat malware like GoldKefu and other trojans that use overlay attacks to display fake login screens, applications must have the ability to detect when another app is attempting to draw over their interface and alert the user or terminate the session.[13]
  - **Robust Code Protection:** Employing techniques like code obfuscation and anti-tampering mechanisms makes it more difficult for attackers to reverse-engineer the application to find vulnerabilities or build effective malware.
- **3. Adopt an "Ecosystem" Approach to User Education:** Customer awareness campaigns must evolve beyond generic advice like "use a strong password." Education must address the specific, modern threats users face and acknowledge that their risk extends beyond their phone. Campaigns should explicitly warn customers about:
  - **Social Engineering on Messaging Apps:** The distribution of malware like Tria Stealer via WhatsApp highlights the need to teach users to be skeptical of unsolicited files and links, even from known contacts.[28]

  - **Advanced Phishing Tactics:** Users must be educated about the dangers of installing MDM profiles from untrusted sources (the vector for GoldPickaxe on iOS) and malicious QR codes.[31]
  - **Home Network and IoT Security:** Users need to understand that the security of their mobile banking is linked to the security of their entire home network. Simple guidance on changing default passwords on routers and smart devices (like the TVs targeted by Android.VO1D) is now a crucial part of financial security education.

- **4. Enhance Proactive Threat Intelligence Capabilities:** Given the clear evidence of threat migration, a reactive security posture is insufficient. Financial institutions must develop proactive threat intelligence programs that specifically monitor for TTPs emerging from other regions, particularly the Asia-Pacific (APAC). TTPs seen in Vietnam and Thailand today are leading indicators of the threats that will target Africa tomorrow.[1] Fostering intelligence-sharing partnerships with regional and international bodies, such as INTERPOL and national CERTs, is critical for gaining early warning of new campaigns and malware.
- **5. Re-evaluate and Augment Fraud Detection Models:** The paradox of falling fraud *rates* and rising financial *losses* in markets like South Africa demonstrates the limitations of traditional risk models.[33] Institutions must augment transaction-based fraud detection with more sophisticated behavioral analytics capable of identifying the subtle signals of on-device fraud and Device Takeover (DTO) scenarios. Risk models must be updated to recognize that the absence of frequent, low-level fraud alerts may not signify safety, but could instead indicate the presence of a stealthy, high-impact adversary who has successfully bypassed initial defenses.

IX. Conclusion: Africa as the New Frontier for Global Cyber Threats

The evidence presented in this report leads to an unequivocal and urgent conclusion: the mobile threat landscape in Africa has fundamentally and irrevocably matured. The continent is no longer a peripheral target for opportunistic or low-level cybercrime but has become a strategic priority for organized, well-resourced, and technically advanced international threat actors. The era of viewing Africa as a secondary market for cyber threats is over.

The documented migration of sophisticated syndicates like **GoldFactory** from their traditional strongholds in Asia to new operational zones in Africa, bringing with them their most innovative tools like the **Gigabud** and **GoldPickaxe** trojans, marks a significant inflection point.[1] These adversaries are not merely exporting malware; they are exporting battle-tested tactics, techniques, and procedures developed in highly contested digital environments. This includes the pioneering of AI-driven biometric fraud, a method specifically designed to defeat the very security measures that African financial institutions are now implementing as their next-generation defense.[5]

The result is a highly complex and dangerous threat environment where localized, socially engineered scams coexist and may even collaborate with state-of-the-art banking trojans deployed by global syndicates. The immense financial losses, which continue to climb even as the volume of simple fraud declines in some areas, underscore the severe and disproportionate impact of these advanced, targeted attacks.[33] This new reality renders many traditional risk and fraud models dangerously obsolete.

For Africa's financial sector, this evolution demands a paradigm shift in security strategy. Survival and success in this new frontier require moving beyond legacy thinking. The approach must be mobile-first, intelligence-driven, and ecosystem-aware. Defenses must be architected not just to stop a fraudulent transaction, but to prevent a device takeover, to detect a deepfake, and to account for vulnerabilities in a user's home network. The battle for Africa's digital financial future is on, and the front lines are no longer confined to data centers or corporate networks; they are on the millions of mobile devices in the hands of its citizens. The time for strategic preparation is now.

References

[1] *A Cancer: UN warns Asia-based cybercrime syndicates expanding worldwide - Al Jazeera*. Accessed: 2025-06-30. ALJAZEERA. 2025. URL: https://www.aljazeera.com/news/2025/4/21/a-cancer-un-warns-asia-based-cybercrime-syndicates-expanding-worldwide.

[2] *Africa extends its smartphone growth streak, but 2025 projected to see moderate 3% growth*. Accessed: 2025-06-30. CANALYS. 2025. URL: https://www.canalys.com/newsroom/africa-smartphone-market-q1-2025.

[3] *Breaking News: Golddigger and Gigabud Android Banking Trojans ...* Accessed: 2025-06-30. VNCS. 2025. URL: https://vncs.vn/en/tin-tuc/detail-breaking-news-golddigger-and-gigabud-android-banking-trojans-same-cybercriminal-new-tricks-phat-hien-moi-ve-an-ninh-mang-lien-ket-giua-golddigger-va-gigabud-rojan-ngan-hang-android-364.

[4] *Check Point: April 2025 Most Wanted Malware - 8 African countries ...* Accessed: 2025-06-30. ITEDGENEWS. 2025. URL: https://www.itedgenews.africa/check-point-april-2025-most-wanted-malware-8-african-countries-among-worlds-most-targeted/.

[5] *Chinese Hackers Using Deepfakes in Advanced Mobile Banking Malware Attacks*. Accessed: 2025-06-30. THEHACKERNEWS. 2024. URL: https://thehackernews.com/2024/02/chinese-hackers-using-deepfakes-in.html.

[6] *Cyber threats impacting the financial sector in 2024 - focus on the main actors*. Accessed: 2025-06-30. BLOG. 2025. URL: https://blog.sekoia.io/cyber-threats-impacting-the-financial-sector-in-2024-focus-on-the-main-actors/.

[7] *Cybercrime threat rises in Africa as mobile banking grows: Interpol Semafor*. Accessed: 2025-06-30. SEMAFOR. 2025. URL: https://www.semafor.com/article/06/23/2025/cybercrime-threat-rises-in-africa-as-mobile-banking-grows-interpol.

[8] *Cybercriminals Abuse Open-Source Tools To Target Africatextquotesingle s Financial Sector - Unit 42*. Accessed: 2025-06-30. UNIT42. 2025. URL: https://unit42.paloaltonetworks.com/cybercriminals-attack-financial-sector-across-africa/.

[9] *Cyberfraud in the Mekong reaches inflection point, UNODC reveals*. Accessed: 2025-06-30. UNODC. 2025. URL: https://www.unodc.org/unodc/frontpage/2025/April/cyberfraud-in-the-mekong-reaches-inflection-point--unodc-reveals.html.

[10] *Cybersecurity Concerns Increase in Africa as Mobile Banking and AI Threats Surge*. Accessed: 2025-06-30. TECHAFRICANEWS. 2025. URL: https://techafricanews.com/2025/02/18/knowbe4-report-highlights-digital-risks-in-africa-amid-growing-use-of-technology/.

[11] *Cybersecurity Threats Facing Nigerians in 2025—and How to Stay Safe - GreenWare Tech*. Accessed: 2025-06-30. GREENWARE-TECH. 2025. URL: https://greenware-tech.com/cybersecurity-threats-facing-nigerians-in-2025-and-how-to-stay-safe/.

[12] *DIGITAL FRAUD TRENDS IN AFRICA - FAnews*. Accessed: 2025-06-30. FANEWS. 2025. URL: https://www.fanews.co.za/assets/Marilyn_2025_2/TransUnion12062025.pdf.

[13] *Face Off: Group-IB identifies first iOS trojan stealing facial recognition data*. Accessed: 2025-06-30. GROUP-IB. 2025. URL: https://www.group-ib.com/blog/goldfactory-ios-trojan/.

[14] *Fraud follows fintech - AB magazine*. Accessed: 2025-06-30. ABMAGAZINE. 2025. URL: https://abmagazine.accaglobal.com/global/articles/2025/apr/business/fraud-follows-fintech.html.

[15] *GoldDigger Android Trojan Targets Banking Apps in Asia Pacific Countries*. Accessed: 2025-06-30. THEHACKERNEWS. 2023. URL: https://thehackernews.com/2023/10/golddigger-android-trojan-targets.html.

[16] *GoldDigger Android trojan targets Vietnamese banking apps - The Register*. Accessed: 2025-06-30. THEREGISTER. 2023. URL: https://www.theregister.com/2023/10/06/golddigger_android_trojan_vietnam_attacks/.

[17] *GoldFactory - Group-IB*. Accessed: 2025-06-30. GROUP-IB. 2025. URL: https://www.group-ib.com/masked-actors/goldfactory/.

[18] *GoldPickaxe Trojan Uses Biometric Data and Deepfake Tech to Scam Banks*. Accessed: 2025-06-30. INFOSECURITY-MAGAZINE. 2025. URL: https://www.infosecurity-magazine.com/news/goldpickaxe-trojan-biometric/.

[19] *Group-IB Uncovers GoldDigger Trojan Targeting 50+ Vietnamese Banks*. Accessed: 2025-06-30. CYBERSECURITYASIA. 2025. URL: https://cybersecurityasia.net/group-ib-uncovers-golddigger-trojan-targeting-50-vietnamese-banks/.

[20] *Group-IB Uncovers the First iOS Trojan Harvesting Facial Recognition Data - Security Insight*. Accessed: 2025-06-30. SECURITYINSIGHT. 2025. URL: https://securityinsight.nl/blog/group-ib-uncovers-the-first-ios-trojan-harvesting-facial-recognition-data.

[21] *Hackers Use Open-Source Offensive Cyber Tools to Attack Financial Businesses in Africa*. Accessed: 2025-06-30. INFOSECURITY-MAGAZINE. 2025. URL: https://www.infosecurity-magazine.com/news/hackers-financial-businesses-africa/.

[22] *How to protect Android apps from overlay attacks - Build38*. Accessed: 2025-06-30. BUILD38. 2025. URL: https://build38.com/blog/solutions/protect-android-apps-from-overlay-attacks/.

[23] *Interpol warns of rise in cybercrime in Africa - Atalayar*. Accessed: 2025-06-30. ATALAYAR. 2025. URL: https://www.atalayar.com/en/articulo/new-technologies-innovation/interpol-warns-of-rise-in-cybercrime-in-africa/20250628190000216267.html.

[24] *Is Facebook undermining African alternatives?* Accessed: 2025-06-30. AFRICAN. 2015. URL: https://african.business/2015/11/technology-information/is-data-free-facebook-in-africa-really-such-a-good-thing.

[25] *Kaspersky Lab Reports Asian and African Banks Attacked Using a Zero-day Vulnerability*. Accessed: 2025-06-30. USA. 2025. URL: https://usa.kaspersky.com/about/press-releases/kaspersky-lab-reports-asian-and-african-banks-attacked-using-a-zero-day-vulnerability.

[26] *New Frontiers, Old Tactics: Chinese Espionage Group Targets Africa & Caribbean Govts*. Accessed: 2025-06-30. THEHACKERNEWS. 2024. URL: https://thehackernews.com/2024/05/new-frontiers-old-tactics-chinese-cyber.html.

[27] *New INTERPOL report warns of sharp rise in cybercrime in Africa*. Accessed: 2025-06-30. INTERPOL. 2025. URL: https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa.

[28] *ngCERT alerts Nigerians to new Android malware targeting ...* Accessed: 2025-06-30. NAIRAMETRICS. 2025. URL: https://nairametrics.com/2025/06/11/ngcert-alerts-nigerians-to-new-android-malware-targeting-whatsapp-and-banking-apps/.

[29] *Open-source tools leveraged to compromise African financial sector SC Media*. Accessed: 2025-06-30. SCWORLD. 2025. URL: https://www.scworld.com/brief/open-source-tools-leveraged-to-compromise-african-financial-sector.

[30] *Overlay Attacks: Protect Your Digital Assets Group-IB*. Accessed: 2025-06-30. GROUP-IB. 2025. URL: https://www.group-ib.com/resources/knowledge-hub/overlay-attacks/.

[31] *Public should beware of GoldDigger malware targeting iOS devices - HKCert*. Accessed: 2025-06-30. HKCERT. 2025. URL: https://www.hkcert.org/security-bulletin/malware-alert-public-should-beware-of-golddigger-malware-targeting-ios-devices_20240220.

[32] *SABRIC Reports Increase in Financial Crime Losses - 2023*. Accessed: 2025-06-30. BANKING. 2025. URL: https://www.banking.org.za/news/sabric-reports-significant-increase-in-financial-crime-losses-for-2023/.

[33] *SABRIC reports significant increase in financial crime losses in 2023 - BankservAfrica Blog*. Accessed: 2025-06-30. BANKSERVAFRICA. 2025. URL: https://www.bankservafrica.com/blog/post/7b44561f-7926-4f6c-8c25-d15a10f2450a_sabric-reports-significant-increase-in-financ.

[34] *Smile ID Releases 2025 Digital Identity Fraud in Africa Report*. Accessed: 2025-06-30. USESMILEID. 2025. URL: https://usesmileid.com/blog/2025-digital-identity-fraud-in-africa-report.

[35] *The State of the Industry Report on Mobile Money 2025 - GSMA*. Accessed: 2025-06-30. GSMA. 2025. URL: https://www.gsma.com/sotir/wp-content/uploads/2025/04/The-State-of-the-Industry-Report-2025_English.pdf.

YinkoShield:
Protecting the Most Impactful Apps Across Africa

YinkoShield is the trusted mobile protection platform behind some of the largest and most sensitive applications in Africa, including those used in finance, digital identity, and government services. Built specifically to address the realities of the African mobile landscape, YinkoShield is optimized for low-end devices and limited connectivity environments—without compromising on security or performance.

From anti-tampering and runtime integrity to advanced overlay and accessibility protection, YinkoShield brings multiple layers of defense across Android, iOS, and hybrid applications. Its seamless integration and compatibility with thousands of devices ensure that security is not a barrier to adoption or user experience.

With native support for OpenTelemetry and integration into major APMs, YinkoShield also empowers development and support teams to respond to threats in real time—turning security into a business enabler.

YinkoShield: Empowering developers. Delighting users. Defending the future.

YinkoShield