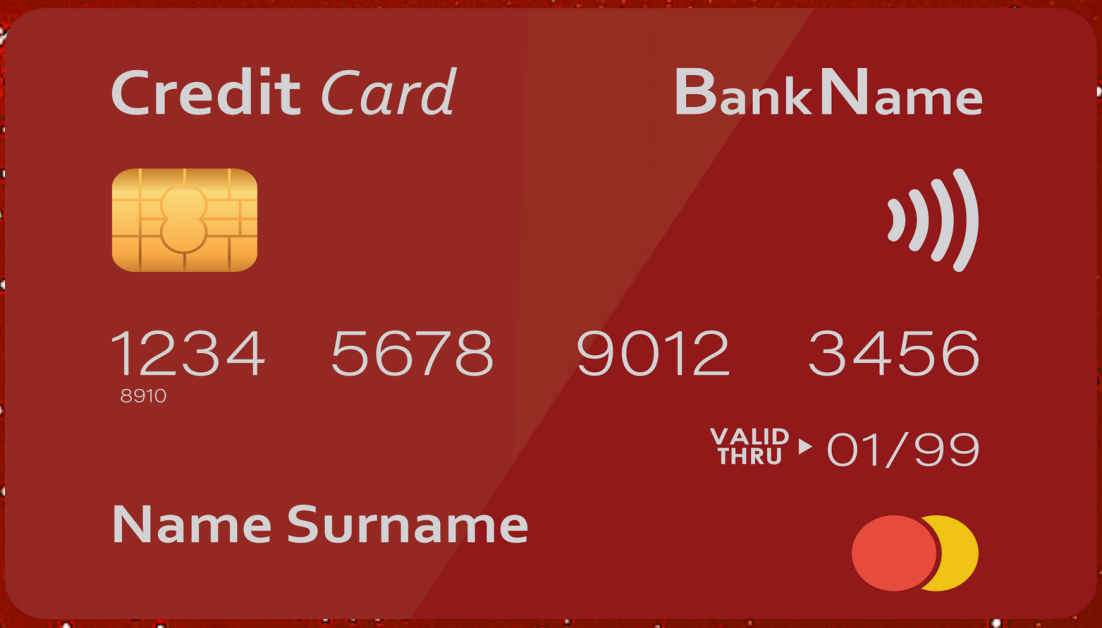
CyHawk

2025

THREAT INTELLIGENCE REPORT



Telegram Underground Market Fuels Payment Card Fraud Across Africa

By
Hassanat Oladeji

Executive Summary

Recent investigations by CyHawk Africa uncovered a Telegram-based underground marketplace distributing stolen payment card data belonging to African banks. While the platform operates globally, CyHawk's analysis highlights the African exposure, with banks in West, East, Central, Southern, and North Africa all affected.

The platform is run through an automated Telegram bot that allows criminals to query stolen cards by country, BIN (Bank Identification Number), card scheme (Visa/Mastercard), and type (Classic, Gold, Platinum, Prepaid, Business, Infinite). This accessibility lowers the barrier for cybercriminals to commit card-not-present (CNP) fraud, identity theft, and money laundering at scale.

Adversary Infrastructure and Operations

The operations behind this underground carding ecosystem rely on a blend of technical enablers and criminal supply chains that sustain the marketplace. The elements identified are:

1. Telegram Bot Ecosystem

- The core of the criminal infrastructure is an automated Telegram bot that acts as a searchable marketplace.
- Buyers can filter data by country, BIN, card type, or issuer bank, effectively turning stolen card data into a consumer-like catalog.
- Payment and delivery are instant, allowing anonymous transactions with minimal barriers.

2. Compromised Data Sources

- The stolen payment card data appears to originate from:
  - Infostealer malware infections on end-user devices (harvesting browser-stored payment credentials).
  - Compromised Point-of-Sale (POS) terminals in retail and hospitality sectors.
  - Card skimming hardware attached to ATMs and payment terminals, capturing magnetic stripe data.
  - Breaches of merchant databases where payment details were stored insecurely.

Adversary Infrastructure and Operations (Cont'd)

3. Cryptocurrency Payment Channels

- The marketplace is sustained by cryptocurrency transactions, primarily Bitcoin and USDT (Tether).
- These digital currencies provide pseudo-anonymity, making tracing criminal transactions difficult.

4. Underground Hosting and Evasion

- Hosting is decentralized, with threat actors leveraging bulletproof hosting providers and content delivery networks (CDNs) to evade takedowns.
- Redundant mirrors ensure that even if one Telegram bot is banned, operations migrate to another with minimal downtime.

5. Operational Security (OpSec) Measures

- Vendors use multiple layers of anonymity, including disposable Telegram accounts, encrypted communications, and crypto mixers for payments.
- Use of affiliates and resellers spreads distribution and reduces exposure of core operators.

6. Regional and Global Links

- Although CyHawk Africa's focus is on African banks, the infrastructure clearly serves a global customer base, with card data from North America, Europe, Asia, and Latin America also circulating.
- This highlights a transnational cybercrime operation where African financial institutions are just one segment of the targeted ecosystem.

African Exposure by Geography

North Africa

- Libya: National Commercial Bank
- Tunisia: UBCI, Société Monétique-Tunisie
- Algeria, Morocco: (also observed in dumps)

West Africa

- Nigeria: First Bank, Zenith, GTBank, UBA, Access, Fidelity, Sterling, Wema, Polaris, Providus
- Ghana: UT Bank, First Atlantic Bank
- Togo: Ecobank Togo, Network International
- Liberia: Ecobank Liberia
- Guinea-Bissau: Banco da Africa Ocidental
- Mali: BSIC Mali, BICIM
- Cabo Verde: SISP, Banco Caboverdiano de Negocios, Caixa Economica

East Africa

- Kenya: KCB, Equity Bank, Standard Chartered, Co-operative, NCBA, Absa/Barclays, National Bank of Kenya, I&M, Citibank, SBM, Gulf African Bank, Commercial Bank of Africa
- Uganda: Centenary Bank, Absa Uganda, Equity Bank Uganda, DFCU Bank, Diamond Trust Bank
- Tanzania: CRDB, NMB, KCB Tanzania, NBC, UBA Tanzania, Stanbic, Exim, DTB Tanzania, Standard Chartered Tanzania
- Burundi: KCB Burundi
- Somalia: Premier Bank

African Exposure by Geography (Cont'd)

Central Africa

- Cameroon: Société Générale Cameroun, UBA Cameroon
- Congo-Brazzaville: Banque Commerciale Internationale, BGFIBank Congo
- Congo-Kinshasa (DRC): Rawbank, Equity BCDC, Access Bank RDC
- Gabon: Union Gabonaise de Banques, BGFI, UBA Gabon

Southern Africa

- South Africa:
  - Investec Bank (Visa Platinum)
  - FirstRand Bank (Visa Classic)
  - Discovery Bank (Visa Gold)
  - Standard Bank of South Africa (MC Gold)
  - Capitec Bank (MC Standard)
- Zambia: Stanbic Zambia, FNB Zambia, Standard Chartered Zambia, Barclays Zambia, Indo Zambia Bank
- Angola: Banco BIC, Banco Angolano de Investimentos, Banco de Comercio e Industria

Top Targeted Banks
(Based on Recurrence & BIN Volume)

Analysis of the BIN dataset extracted from the Telegram marketplace highlights clear patterns of recurrence (the number of times a bank or group appears across different African countries) and BIN volume (the number of unique card BINs tied to that institution). Together, these factors provide a reliable measure of which financial institutions are targeted by threat actors.

1. P**an-African Banking Groups**
    - Ecobank and United Bank for Africa (UBA) stand out as the most frequently recurring institutions. Their presence across multiple West and Central African countries makes them attractive to carding groups seeking scale and repeatability.
    - Standard Bank/Stanbic, Absa/Barclays, and Société Générale affiliates also feature prominently across Southern and Central Africa, reflecting the geographical reach of their customer bases.

2. **High BIN Volume in East Africa**
    - Institutions such as KCB Bank, Equity Bank, CRDB Bank, and NMB Bank in Kenya and Tanzania show a high concentration of BIN listings, suggesting attackers repeatedly target them, either due to their market dominance or perceived vulnerabilities.
    - In Uganda, Centenary Bank, DTB, and Absa Uganda also appear multiple times, reinforcing East Africa as a high-visibility region for card fraud operations.

Top Targeted Banks (Cont'd)
(Based on Recurrence & BIN Volume)

3. **Premium Tier Cards as a Target Vector**
    - Several banks show repeated exposure in Platinum, Gold, and Business card tiers, particularly in South Africa (Investec, FirstRand, Discovery, Capitec, and Standard Bank). This suggests criminals are deliberately prioritizing higher-value accounts with larger credit limits, which provide more lucrative returns per compromised card.

4. **Rawbank and BGFI Group (Central Africa)**
    - Rawbank (DR Congo) and BGFI (Congo-Brazzaville and Gabon) each show multiple BIN exposures across different card schemes. Both institutions serve as dominant players in their markets, making them natural high-priority targets in Central Africa.

5. **Interpretation of Recurrence vs. Volume**
    - Recurrence shows breadth of targeting (how many different markets a bank is exposed in).
    - Volume shows depth (how many card products or BIN ranges are consistently compromised).
    - Banks such as Ecobank, UBA, and Standard Bank are prominent in both measures, making them strategic priority targets for monitoring and counter-fraud initiatives.

Mitre Att&ck Mapping

The Telegram-based underground marketplace for stolen card data reflects multiple ATT&CK techniques spanning initial access, collection, exfiltration, infrastructure use, and monetization. The ecosystem sources data from infostealer malware, compromised POS terminals, and card skimming operations, before reselling it through automated Telegram bots.

1. Initial Access & Collection

- T1566.002 – Phishing: Spearphishing Link
- Delivery of infostealers via phishing emails or malicious links to compromise endpoints where card data is stored.
- T1555.003 – Credentials from Web Browsers
- Infostealer malware extracts stored payment card details directly from web browsers.
- T1005 – Data from Local System
- Cardholder data captured from infected endpoints and applications.
- T1056.001 – Input Capture: Keylogging
- Some malware captures keystrokes, including manual card entry into web forms.
- T1056.004 – Network Sniffing
- POS malware variants intercept card data in transit between POS terminals and payment processors.
- T1056.002 – Input Capture: GUI Input Capture
- Some malicious tools grab on-screen card details during online payments.

Mitre Att&ck Mapping (Cont'd)

- T1190 – Exploit Public-Facing Application
- Compromised POS terminals often result from vulnerabilities in payment software or poor segmentation.
- T1005/T1056 – Card Skimming (Physical Device Compromise)
- Hardware skimmers attached to ATMs or POS terminals record magnetic stripe data, later sold through Telegram marketplaces.

2. Exfiltration

- T1041 – Exfiltration Over C2 Channel
- POS malware and infostealers send dumps to attacker-controlled servers.
- T1567.002 – Exfiltration to Cloud Storage

Conclusion

The discovery of a Telegram-based underground marketplace trading stolen payment card data highlights the persistent and evolving threat to Africa's financial sector. By leveraging infostealer malware, compromised POS terminals, and physical skimming devices, cybercriminals are feeding a global fraud ecosystem that exploits African financial institutions alongside other financial institutions worldwide.

The use of Telegram bots as automated distribution platforms lowers the barrier to entry for cybercriminals, making the trade in sensitive financial data faster, cheaper, and more scalable than ever before. This trend represents a significant escalation in the accessibility of financial cybercrime, moving illicit operations away from hidden forums into mainstream encrypted applications.

For Africa, the threat is acute: banks in Nigeria, South Africa, Ghana, Uganda, Zambia, and others have emerged as frequent targets, exposing vulnerabilities in both digital banking infrastructure and physical payment ecosystems. The concentration of BINs linked to Ecobank, UBA, Standard Bank, and other top regional players underscores the strategic focus of adversaries on high-value institutions with widespread customer bases.

Mitigating this threat requires a multi-layered defense, integrating cyber threat intelligence, advanced fraud monitoring, endpoint detection, and physical security measures. Financial institutions must collaborate regionally to share threat data, enforce stricter PCI DSS compliance, and coordinate law enforcement action against underground operators.

CyHawk Africa will continue to monitor these underground markets, with a focus on Africa's exposure, ensuring that stakeholders across the continent remain informed and equipped to counter emerging financial cyber threats.

Recommendations

To mitigate the risks posed by the Telegram-based underground carding marketplace and strengthen defenses against financial cybercrime, CyHawk Africa recommends the following:

1. Enhanced Fraud Monitoring and Threat Intelligence

- Deploy advanced fraud detection systems that leverage machine learning to flag unusual spending patterns and cross-border transactions.
- Subscribe to real-time threat intelligence feeds on compromised BINs, card dumps, and Telegram-based marketplaces to proactively block fraudulent transactions.

2. Strengthen Endpoint and Network Security

- Enforce strict monitoring of endpoints for infostealer malware, which remains one of the primary sources of stolen card data.
- Harden ATM and POS terminals against skimming and tampering, with regular inspections and physical security controls.
- Isolate payment processing environments from the wider enterprise network to limit attacker movement.

3. Card Issuer Security Enhancements

- Encourage the adoption of chip-and-PIN (EMV) over magnetic stripe technology to reduce skimming risks.
- Enable two-factor authentication (2FA) and real-time transaction alerts for cardholders to detect and block unauthorized activity quickly.
- Regularly rotate BIN ranges and enforce velocity limits on high-risk card categories (e.g., prepaid cards).

Recommendations (Cont'd)

4. Regulatory and Compliance Measures

- Ensure compliance with PCI DSS, focusing on encryption of cardholder data in transit and at rest.
- Regulators should coordinate cross-border intelligence sharing among African banks and telecom providers to track and disrupt fraud operations.
- Establish regional task forces to investigate underground markets and take legal action against threat actors.

5. Customer Awareness and Education

- Launch awareness campaigns warning customers about risks of phishing, fraudulent merchants, and compromised POS terminals.
- Encourage cardholders to regularly review bank statements and promptly report suspicious activity.

6. Collaboration and Information Sharing

- Foster collaboration between banks, telecom operators, payment processors, and law enforcement to combat card fraud.
- Leverage platforms such as FS-ISAC Africa or create regional equivalents to facilitate structured cyber threat intelligence sharing.