PUBLIC RELEASE EDITION

AFRIWEALTH NATIONAL INTELLIGENCE BRIEF SERIES

Ghana Cyber Threat Intelligence Brief

Q1 2026

January – March 2026

AfriWealth Cyber Intelligence

Built for Defense. Driven by Intelligence.

Document Reference: ACI-NIB-2026-Q1-001

PUBLIC RELEASE

April 2026

Series: AfriWealth National Intelligence Brief Series

Accra, Ghana

DOCUMENT INFORMATION

Document Notice

CLASSIFICATION: PUBLIC RELEASE — NO HANDLING RESTRICTIONS APPLY

Document Title	Ghana Cyber Threat Intelligence Brief
Series	AfriWealth National Intelligence Brief Series
Reporting Period	Q1 2026 · January – March 2026
Edition	Public Release Edition
Document Reference	ACI-NIB-2026-Q1-001
Classification	PUBLIC — No handling restrictions apply
Organisation	AfriWealth Cyber Intelligence
Publication Date	April 2026
Next Edition (Est.)	Q2 2026 Brief

PUBLIC RELEASE SCOPE

This edition provides structured national-level intelligence assessment derived from open-source monitoring, regional pattern analysis, and public reporting review. It does not include technical indicators of compromise, detailed infrastructure mapping, actor attribution analysis, or TLP-restricted intelligence content. AfriWealth Subscriber Editions contain the full technical intelligence product.

CONTENTS

Table of Contents

OVERVIEW

Executive Summary

This brief provides a structured national-level intelligence assessment of cyber threat activity affecting Ghana during Q1 2026.

Ghana's Q1 2026 cyber threat environment is defined by financially motivated activity achieving scale through social engineering rather than advanced technical exploitation.

Key Findings — Q1 2026

KIT-1 — Social Engineering as the Dominant Attack Vector

Financially motivated adversaries continued to achieve operational success through social engineering rather than advanced technical exploitation. This pattern is structural, not incidental, and reflects the configuration of Ghana's mobile-first financial ecosystem.

KIT-2 — Mobile Financial Infrastructure as the Primary Attack Surface

Phishing, smishing, SIM swap fraud, and credential compromise operations were observed at sustained levels, with targeting patterns consistent with adversary familiarity with Ghana's telecom and banking environment.

KIT-3 — Absence of National-Level Disruption Events

No publicly confirmed large-scale cyber incident was recorded during the reporting period. The assessed threat environment is characterised by persistent sub-threshold financial fraud activity, not acute crisis conditions.

KIT-4 — Detection Gaps as the Primary Risk Amplifier

The most significant assessed vulnerability across Ghanaian institutional sectors is not the absence of patches or perimeter controls — it is the absence of detection capability. Adversaries are assessed as operating within environments where their activity would not trigger available monitoring controls.

STRATEGIC ASSESSMENT

The Q1 2026 threat landscape reflects persistent financially motivated adversary activity operating below national disruption thresholds yet above baseline nuisance levels. The structural conditions sustaining this activity — high mobile financial penetration, variable authentication maturity, and limited institutional detection capability — remain present across the assessed sectors.

The Q1 threat environment is characterised by four primary observations: social engineering as the dominant observed attack vector; increased mobile-first targeting patterns; underground ecosystem references to Ghana-linked financial accounts; and regional ransomware operator activity presenting assessed indirect exposure risk to Ghanaian sectors.

CONFIDENCE ASSESSMENT: MODERATE

Based on structured OSINT monitoring, regional pattern comparison, and public reporting review.

This assessment is intended to support institutional awareness, defensive prioritisation, and strategic decision-making across financial, telecom, and public-sector environments.

ANALYTICAL JUDGEMENTS

Key Judgements

The following structured judgements represent AfriWealth's principal analytical conclusions derived from Q1 2026 intelligence observations. Each judgement is explicitly assessments-based, not descriptive. Confidence ratings reflect the quality and breadth of the underlying source base.

#	KEY JUDGEMENT	CONFIDENCE
1	Social engineering is assessed as the primary operational pathway for financially motivated adversaries in Q1 2026. Advanced technical exploitation is not assessed as a prerequisite for achieving operational impact in Ghana's current threat environment.	HIGH
2	Mobile money and mobile banking users are assessed as the highest-exposure population category, reflecting convergence of high penetration rates, SMS-based authentication reliance, and variable platform monitoring maturity.	HIGH
3	No publicly confirmed large-scale national cyber disruption event was recorded in Q1 2026. The assessed threat environment is characterised by persistent sub-threshold financial fraud activity rather than acute crisis conditions.	HIGH
4	Underground ecosystem references to Ghana-linked financial accounts are assessed as consistent with sustained adversary interest. The observed availability of SIM swap services and credential listings is assessed as lowering operational barriers for financially motivated actors.	MODERATE
5	A moderate probability environment for targeted ransomware activity affecting Ghanaian SME and healthcare sectors is assessed within the 6-12 month horizon, contingent on current structural exposure conditions persisting without remediation.	MODERATE
6	Detection capability gaps are assessed as a more significant risk amplifier than unpatched technical vulnerabilities. Intelligence-led detection engineering is assessed as the higher-priority defensive investment for most Ghanaian institutional sectors.	MODERATE TO HIGH
7	Investment fraud operations targeting Ghanaian citizens and diaspora communities are assessed as likely to persist. Citizen-level financial loss, not institutional compromise, remains the primary assessed impact category.	HIGH

SCOPE NOTE

Key Judgements are derived exclusively from open-source intelligence monitoring, regional pattern analysis, and public reporting review. They do not reflect classified source material, confirmed breach data, or proprietary subscriber intelligence. All judgements carry inherent analytical uncertainty.

AT A GLANCE

Sector Risk Summary — Q1 2026

The following matrix presents AfriWealth's assessed exposure levels by sector and threat category for Q1 2026. Ratings reflect observed adversary targeting patterns and assessed institutional exposure conditions. They do not represent confirmed incident volumes or verified breach data.

SECTOR	PHISHING	MOBILE MONEY	RANSOMWARE	BEC	INVEST. FRAUD	OVERALL
Financial Services	HIGH	HIGH	MODERATE	HIGH	HIGH	HIGH
Government / MDAs	HIGH	LOW	ELEVATED	HIGH	LOW	ELEVATED
Healthcare	MODERATE	LOW	ELEVATED	MODERATE	LOW	ELEVATED
Telecoms	MODERATE	HIGH	MODERATE	MODERATE	LOW	MODERATE
SME / Enterprise	HIGH	MODERATE	MODERATE	HIGH	MODERATE	HIGH
Individual Citizens	HIGH	HIGH	LOW	LOW	HIGH	HIGH

Risk levels represent AfriWealth's structured intelligence assessment based on observed adversary targeting patterns and assessed exposure conditions during the reporting period. These ratings do not indicate confirmed incident volumes or verified breach data.

Level definitions — HIGH: sustained observed targeting with elevated assessed impact potential; ELEVATED: persistent exposure conditions with moderate-to-high impact potential; MODERATE: observable activity with manageable impact under assessed current controls; LOW: limited direct observed targeting in this category during the period.

ASSESSMENT BASIS

Risk classifications in this matrix represent AfriWealth's structured intelligence assessment for Q1 2026. They are derived from observed adversary targeting patterns and assessed institutional exposure conditions. All classifications carry inherent analytical uncertainty and do not constitute confirmed incident data.

Risk Rating Methodology

Each sector-level rating is derived from the structured combination of three assessment components applied consistently across the reporting period.

Component	Definition	Source Basis
Observed Adversary Targeting	Frequency and consistency of observed campaign activity directed at the sector, derived from OSINT monitoring, underground references, and public incident reporting.	OSINT / Public Reporting
Structural Exposure Conditions	Persistent configuration or operational characteristics creating sustained adversary-accessible risk: authentication posture, remote access configuration, backup integrity, and detection coverage.	Structural Analysis

Component	Definition	Source Basis
Impact Potential	Assessed consequence of successful adversary activity: operational disruption, financial loss, data exposure, and service continuity impact.	Analytical Judgement

Ratings reflect the assessed intersection of all three components. A sector with low observed targeting but high structural exposure will not automatically receive a high rating. All ratings carry inherent analytical uncertainty.

ANALYTICAL UNCERTAINTY LIMITATION

Absence of observed targeting does not confirm absence of activity. Ratings should be interpreted as structured analytical benchmarks derived from a public-source collection base, not as quantitative risk scores or confirmed incident records.

Analytical Terminology Reference

The following terms carry specific analytical meaning throughout this brief. Consistent interpretation is required for accurate reading of risk ratings and assessments.

Term	Analytical Definition
National disruption threshold	The assessed severity level at which a cyber incident constitutes widespread concurrent impact across critical national infrastructure or essential services. Sub-threshold activity is financially damaging but operationally contained.
Mobile-first targeting	Adversary campaign design optimised for delivery via mobile devices: SMS-based phishing, mobile-optimised credential harvesting pages, and mobile application attack vectors reflecting the predominant digital access pattern of the target population.
Detection capability gap	The difference between adversary activity level and institutional ability to detect, alert on, and respond. A gap exists when adversary techniques would not trigger available monitoring controls.
Structural exposure condition	A persistent configuration or operational characteristic creating sustained adversary-accessible risk, independent of specific targeting activity.
Assessed persistence	AfriWealth's judgement that an observed pattern is likely to continue beyond the reporting period, based on enabling structural conditions and the absence of mitigating changes in the assessed environment.

SECTION 01

Ghana Threat Environment Context

Structural risk factors and primary threat drivers

01

SECTION 01

Ghana Threat Environment Context

Ghana's digital expansion continues to reshape its risk profile. The following structural conditions are assessed as the primary enabling factors for adversary activity observed during Q1 2026.

Contextual Risk Factors

– High mobile money penetration expanding the population of individuals accessible through digitally-delivered fraud
– Increasing reliance on mobile banking applications with variable authentication security
– SME digital adoption proceeding without proportional growth in security maturity
– Cloud integration across enterprise and government sectors expanding assessed exposure surface
– Cross-border financial integration within West Africa widening the operational reach of assessed fraud networks

These structural conditions are assessed as enabling adversaries to achieve scale through social engineering without requiring advanced technical exploitation capability. This pattern is both the defining characteristic of the Q1 threat environment and consistent with observations across prior reporting periods.

Primary Risk Drivers Observed in Q1 2026

Risk Driver	Threat Category	Primary Targets	Assessed Persistence
Credential harvesting	Phishing / BEC	Financial users, corporate finance staff	High
SIM swap-linked fraud	Mobile money fraud	Individual subscribers, telecom customers	High
BEC-oriented phishing	Business Email Compromise	Corporate finance functions	Moderate to High
Underground account refs	Fraud ecosystem	Financial account holders	Moderate

STRUCTURAL ASSESSMENT

Observed Q1 activity patterns suggest that social engineering represents the primary assessed pathway to adversary success in Ghana's current threat environment. Advanced technical sophistication is not assessed as a requirement for achieving operational impact. This characterisation should inform how institutions prioritise defensive investment.

SECTION 02

Phishing and Social Engineering

Campaign patterns, delivery mechanisms, and institutional impact

02

SECTION 02

Phishing and Social Engineering Landscape

Phishing remained the most observable attack vector during Q1 2026. Observed campaigns demonstrated improved localisation, impersonation of Ghanaian financial institutions, and optimisation for mobile interaction — patterns consistent with adversary adaptation to Ghana's mobile-first financial user base.

Observations

– SMS-based phishing (smishing) targeting mobile banking and mobile money users
– Banking-themed account verification lures optimised for mobile display
– Invoice-themed phishing linked to Business Email Compromise intent
– Government service impersonation messages
– **Infrastructure indicators:** short-lived domain registrations; SSL certificate use to increase perceived legitimacy; rapid hosting rotation cycles

Assessment

Financial institutions and corporate finance teams remain assessed as primary institutional targets based on observed campaign characteristics. Individual citizens are assessed as disproportionately affected by mobile-first phishing operations, reflecting the alignment between observed adversary tactics and Ghana's predominant financial access patterns. The combination of credible lure content, SSL-enabled harvesting infrastructure, and SMS delivery is assessed as materially increasing campaign credibility to targeted recipients.

Outlook

Phishing activity is assessed as likely to persist throughout Q2 2026. Potential escalation drivers include regulatory update communications, tax period activity, and financial product announcements — each of which provides credible impersonation themes for campaign operators.

CONFIDENCE ASSESSMENT: HIGH

Based on structured OSINT monitoring and observed campaign pattern consistency across the reporting period.

SECTION 03

Mobile Money Fraud Intelligence

Fraud typologies, actor behaviour, and structural risk factors

03

SECTION 03

Mobile Money Fraud Intelligence

Mobile money fraud continues to represent a high-impact threat category affecting Ghanaian citizens and the broader telecom financial ecosystem. Observed fraud patterns are consistent with strong localisation capability and operational familiarity with Ghana's mobile financial infrastructure.

Observed Fraud Typologies

– Social engineering leading to voluntary OTP disclosure
– SIM swap operations — both socially engineered and potentially insider-facilitated
– Account takeover following credential harvesting
– Agent-assisted fraud schemes
– QR-code manipulation in merchant payment contexts

Structural Risk Factors

– Heavy reliance on SMS-based OTP authentication as the primary security layer
– Variable maturity in transaction anomaly monitoring across platforms
– Inconsistent public awareness of SIM swap fraud risks and defensive practices
– Insider access control weaknesses assessed as a potential enabling factor

Assessment

Observed fraud patterns are consistent with strong localisation capability and operational familiarity with Ghana's mobile financial ecosystem. The convergence of SMS-based authentication reliance, variable monitoring maturity, and effective social engineering is assessed as representing a sustained structural exposure condition rather than a temporary or isolated occurrence.

Outlook

Mobile money fraud is assessed as persistent and adaptive. Observed patterns suggest that social engineering over technical exploitation is likely to remain the primary operational approach, given the assessed continued effectiveness of non-technical methods against current defensive configurations.

CONFIDENCE ASSESSMENT: MODERATE TO HIGH

Based on structured OSINT monitoring, regional pattern comparison, and public reporting review.

SECTION 04

Mobile Banking Threat Landscape

Application targeting, credential compromise, and authentication exposure

04

SECTION 04

Mobile Banking Threat Landscape

Mobile banking applications represent a distinct threat surface from mobile money platforms. Observed campaign activity suggests continued targeting of banking users through credential compromise and authentication interception, with campaigns demonstrating increasing optimisation for the mobile context.

Observations

– Mobile-optimised phishing pages mimicking retail banking portals

– OTP interception attempts via social engineering

– Account takeover activity following phishing-based credential compromise

– Distribution of malicious APK files through unofficial application channels

– Fake banking application update lures delivered via SMS

Assessment

Reliance on SMS-based authentication mechanisms is assessed as increasing institutional and individual exposure to interception-based fraud. Users installing unofficial applications carry assessed exposure to malware-assisted account compromise. The mobile-optimised nature of observed phishing infrastructure is consistent with adversary adaptation to the predominant access pattern of Ghanaian banking users.

Outlook

Mobile banking compromise attempts are assessed as likely to continue. Observed patterns suggest the potential for increasing integration of AI-assisted content generation to improve phishing personalisation and perceived legitimacy. Institutions without application-level anomaly detection or out-of-band authentication carry elevated assessed exposure in the near term.

CONFIDENCE ASSESSMENT: MODERATE TO HIGH

Based on structured OSINT monitoring, regional pattern comparison, and public reporting review.

SECTION 05

Ransomware and Regional Exposure

Operator activity, sector exposure conditions, and precursor indicators

05

SECTION 05

Ransomware and Regional Exposure

Ransomware operators active in the West Africa region are assessed as maintaining operational capability relevant to Ghanaian institutional environments. No publicly confirmed large-scale critical infrastructure incidents were recorded in Q1 2026. However, structural exposure conditions assessed as consistent with ransomware precursor patterns remain present across several institutional sectors.

Regional Patterns Relevant to Ghana

– Exploitation of exposed RDP and VPN services as observed primary initial access vectors in regional incidents

– Credential harvesting preceding ransomware deployment — consistent dwell periods observed in regional reporting

– Affiliate-based Ransomware-as-a-Service (RaaS) models assessed as lowering barriers to regional operation

– Data exfiltration prior to encryption — a pattern observed in regional incidents, assessed as increasing victim leverage

Sector Exposure Assessment

Sector	Exposure Level	Primary Risk Factor	Key Defensive Gap
Healthcare institutions	Elevated	Patient data assessed as high-value target category regionally	Unvalidated offline backup integrity
Government agencies	Elevated	Exposed remote access services	Remote access audit and hardening
SMEs	Moderate to High	Limited segmentation and endpoint monitoring	Network segmentation; EDR deployment
Financial services	Moderate	Credential theft assessed as precursor pathway	Credential monitoring; MFA enforcement
Telecoms	Moderate	Upstream exposure from supply chain	Third-party access controls

Outlook

A moderate probability environment for targeted ransomware incidents affecting the SME or healthcare sector is assessed within the 6–12 month horizon, contingent on current exposure conditions persisting without remediation. The primary assessed precursor indicators — exposed remote access services and unvalidated backup configurations — are amenable to near-term remediation without significant operational investment.

CONFIDENCE ASSESSMENT: MODERATE

Based on regional pattern analysis. No confirmed Ghana-specific incidents observed during the reporting period.

SECTION 06

Investment Fraud and Financial Deception

Campaign typology and citizen-level impact

06

SECTION 06

Investment Fraud and Financial Deception

Fraudulent investment schemes targeting Ghanaian citizens and diaspora communities remain active across social media and messaging platforms. Observed campaigns frequently employ fabricated regulatory endorsements and impersonation of recognised financial institutions as the primary credibility mechanism.

Observed Scheme Typologies

– **Crypto trading impersonation:** false brokerage platforms with fabricated performance records
– **Forex signal fraud:** subscription-based schemes promising guaranteed returns
– **Government bond impersonation:** communications purporting to originate from regulatory bodies
– **High-yield Ponzi-style promotions:** short-horizon schemes distributed primarily through messaging groups

Assessment

Primary assessed impact from investment fraud operations remains at the citizen-level financial loss category. Systemic institutional compromise is not assessed as the primary objective in this threat category. Fabricated regulatory endorsements and institutional impersonation are assessed as the principal credibility mechanisms employed, based on observed campaign characteristics.

Outlook

Investment fraud operations are assessed as likely to persist, with observed patterns suggesting potential expansion across available messaging platforms. Paid social media advertising as a distribution mechanism remains an observed operational characteristic.

CONFIDENCE ASSESSMENT: HIGH

Based on structured OSINT monitoring, regional pattern comparison, and public reporting review.

SECTION 07

Underground Ecosystem Observations

OSINT-derived observations on adversary infrastructure and intent

07

SECTION 07

Underground Ecosystem Observations

COLLECTION SCOPE AND LEGAL BASIS

All observations in this section are derived exclusively from lawful open-source intelligence (OSINT) monitoring of publicly accessible sources. No classified, proprietary, or unauthorised access sources are used in the production of this intelligence product. No claims of confirmed institutional breach are made unless separately verified through publicly available reporting. No interaction with, purchase from, or operational engagement with underground actors, services, or infrastructure occurred at any stage of collection. All monitoring activity was passive and lawful. All collection is conducted within professionally and legally bounded methodologies.

Structured OSINT monitoring of underground forums, marketplace infrastructure, and messaging channel activity during Q1 2026 identified patterns consistent with sustained adversary interest in Ghana's financial ecosystem. All observations are derived exclusively from publicly accessible sources.

Observed Themes

– Underground references to Ghana-linked financial account access
– SIM swap service advertisements targeting West African telecom subscribers
– Credential marketplace listings referencing Ghanaian email domains and banking platforms
– Recruitment activity seeking money mule account access

Assessment

Observed patterns are assessed as consistent with sustained adversary interest in Ghana's financial ecosystem rather than isolated or opportunistic activity. The observed availability of underground services — including SIM swap execution services and credential listings is assessed as lowering the operational barrier for actors without direct technical capability, potentially broadening the range of actors able to conduct financially motivated activity. No confirmed institutional breaches are claimed or implied.

CONFIDENCE ASSESSMENT: MODERATE

Based on lawful OSINT monitoring only. Volume and attribution are limited; patterns assessed from publicly accessible sources.

SECTION 08

Cross-Cutting Intelligence Themes

Three dominant characteristics persist across all threat categories observed in Q1 2026 and reinforce a consistent strategic picture.

Theme	Implication
Social engineering is assessed as the primary observed attack pathway — not technical exploitation	Defensive investment should prioritise human-layer controls, awareness programmes, and detection of social engineering indicators alongside technical controls.
Financial motivation drives rational, cost-optimised adversary behaviour	Observed adversary activity patterns are consistent with rational, economically optimised decision-making. Controls that raise operational cost or reduce the yield of financially motivated attacks are assessed as producing measurable deterrence value.
Detection absence is a greater risk amplifier than patch absence	The primary assessed risk amplifier in Ghana's Q1 landscape is not the absence of patches but the absence of detection. Intelligence-led detection engineering is assessed as addressing the actual exposure surface more directly than vulnerability management alone.

SECTION 09

Q2 2026 Risk Outlook

The following outlook assessments are derived from Q1 intelligence observations and regional trend analysis. Probability and impact assessments are structured analytical judgements and should be interpreted accordingly — not as predictive certainties.

PROBABILITY	IMPACT	SCENARIO
HIGH	MODERATE	Continued phishing and mobile fraud operations with improved lure localisation
HIGH	HIGH	Mobile banking credential compromise via smishing and OTP interception
MODERATE	HIGH	Ransomware exposure environment persisting for SME and healthcare sectors
MODERATE	MODERATE	Investment fraud operations expanding across new messaging platforms
EMERGING	MODERATE	AI-assisted phishing content increasing campaign personalisation
EMERGING	MODERATE	Cross-border fraud coordination within West African networks

CONFIDENCE ASSESSMENT: MODERATE

Based on Q1 intelligence observations, regional trajectory analysis, and structured OSINT monitoring.

SECTION 10

Intelligence-Derived Defensive Priorities

The following defensive priorities are derived directly from Q1 2026 intelligence observations. They are sector-specific and ordered by assessed urgency relative to the threat environment characterised in this brief.

Priorities are structured by implementation timeline. Immediate actions address active exposure conditions identified in Q1 2026. Near-Term and Sustained actions address structural gaps and ongoing posture maintenance.

Financial Institutions

Timeline	Priority Action
Immediate (0–30 days)	Strengthen behavioural transaction monitoring to detect anomalous account activity patterns. This directly addresses the primary fraud vector observed in Q1 2026. Harden SIM swap verification controls in alignment with Bank of Ghana guidance — this is the most exploited credential pathway observed in Q1 2026.
Near-Term (30–90 days)	Improve phishing detection and email gateway integration for BEC-pattern lures. Deploy DNS-layer blocking for identified phishing infrastructure categories.
Sustained (Quarterly / Continuous)	Conduct structured intelligence-led phishing simulation for corporate finance staff. Maintain intelligence-driven review of transaction anomaly thresholds.

Government Ministries and Agencies

Timeline	Priority Action
Immediate (0–30 days)	Audit and reduce exposed remote access services immediately. This is the assessed primary ransomware initial access vector identified in Q1 2026.
Near-Term (30–90 days)	Conduct ransomware preparedness tabletop exercise with IT leadership and senior management. Establish structured intelligence sharing channels with the National Cybersecurity Authority.
Sustained (Quarterly / Continuous)	Deploy and maintain structured phishing awareness programme for government staff.

Healthcare Institutions

Timeline	Priority Action
Immediate (0–30 days)	Validate offline backup integrity and conduct a full restoration test. Restrict and audit RDP and VPN exposure — assessed primary ransomware initial access pathway in Q1 2026 regional reporting.
Near-Term (30–90 days)	Implement network segmentation between clinical, administrative, and public-facing systems.
Sustained (Quarterly / Continuous)	Maintain scheduled backup validation and recovery testing cycles.

SMEs and Growth-Stage Enterprises

Timeline	Priority Action
Immediate (0–30 days)	Enforce multi-factor authentication across all critical business systems. MFA directly addresses the credential compromise pathway that underpins the majority of financially motivated activity observed in Q1 2026.
Near-Term (30–90 days)	Conduct structured phishing awareness programme — social engineering is the primary assessed risk vector for this sector. Review and document incident response procedures for ransomware and fraud scenarios.
Sustained (Quarterly / Continuous)	Maintain phishing simulation cycles and IR procedure review on a quarterly basis.

SECTION 11

Methodology and Scope

This Public Release edition is produced using the following intelligence collection and analytical methodologies.

Method	Description
Structured OSINT Monitoring	Systematic monitoring of publicly accessible sources for indicators of adversary activity, infrastructure, and targeting relevant to Ghana and the West African region.
Underground Forum Observation	Lawful monitoring of underground marketplace and forum activity for references to Ghanaian targets, credentials, and service offerings.
Regional Campaign Correlation	Comparison of observed Q1 activity patterns against regional and global intelligence reporting to assess threat actor context and campaign scope.
Public Incident Reporting Review	Analysis of publicly confirmed incidents and disclosures across the region to calibrate exposure assessments.
Analytical Confidence Assessment	Structured application of confidence ratings (Low / Moderate / Moderate to High / High) to all principal analytical assessments in accordance with AfriWealth methodology.

No classified, restricted, or proprietary source data is included in this edition. All intelligence collection activity is conducted within lawful and professionally bounded methodologies. This edition contains no confirmed breach data or attribution claims.

AfriWealth Threat Assessment Model (ATAM)

To ensure consistency across all assessments, AfriWealth applies a structured analytical model to derive risk ratings and confidence levels.

AfriWealth's structured intelligence assessments are produced in accordance with the AfriWealth Threat Assessment Model — an internal analytical framework governing the derivation of risk ratings, confidence assessments, and analytical judgements across all intelligence products in this series.

Component	Definition
Observed Adversary Activity	Frequency and consistency of campaign activity directed at the assessed sector, derived from structured OSINT monitoring and public incident reporting.
Structural Exposure Conditions	Persistent configuration, architectural, or operational characteristics of the sector that create sustained adversary-accessible risk, independent of specific targeting activity.
Impact Potential	Assessed consequence of successful adversary activity, considering operational disruption, financial loss, data exposure, and service continuity impact.

Risk ratings represent the assessed intersection of all three components. A sector with low observed targeting but high structural exposure will not automatically receive a high rating. All ratings carry inherent analytical uncertainty arising

from the public-source nature of this edition's collection base. Ratings should be interpreted as structured analytical benchmarks, not quantitative risk scores.

SECTION 12

Subscriber Edition Notice

This Public Release edition provides structured national-level assessment without the technical intelligence content available to AfriWealth institutional subscribers.

Content Category	Public Release	Subscriber Edition
Structured threat assessment	Included	Included
Sector risk summary	Included	Included
Defensive priority guidance	Included	Included
Technical Indicators of Compromise (IOCs)	Excluded	Included
Detailed infrastructure mapping	Excluded	Included
Actor-specific attribution analysis	Excluded	Included
Detection engineering artefacts (Sigma, YARA, KQL)	Excluded	Included
TLP-restricted intelligence notes	Excluded	Included
Quarterly institutional intelligence calls	Excluded	Included

SUBSCRIPTION ENQUIRIES

For institutional subscription enquiries, please contact: intelligence@afriwealthintel.com · contact@afriwealthintel.com Subscriber editions are available to financial institutions, government agencies, healthcare organisations, and enterprise security teams.

REFERENCES

Selected Open-Source References

SOURCE BASIS

Publicly available sources consulted for contextual validation and regional trend alignment. This list is non-exhaustive and reflects open-source materials only.

– Cyber Security Authority (CSA), Ghana — CERT-GH Alerts & Advisories
Selected public alerts and guidance.

– Bank of Ghana — Cyber & Information Security Directive
Regulatory directive and associated publications.

– Bank of Ghana — Publication of Banks, SDIs and PSPs 2024 Fraud Report
Financial-sector fraud context and patterns.

– INTERPOL / AFRIPOL — African Cyberthreat Assessment Report 2024
Regional cybercrime and threat trends.

– ENISA — ENISA Threat Landscape (ETL) 2024
Global threat categories and evolving tactics.

– Microsoft — Microsoft Digital Defense Report 2025
Identity threats, cybercrime economy, ransomware and initial access trends.

– Verizon — 2025 Data Breach Investigations Report (DBIR)
Attack patterns, social engineering prevalence, breach trends.

– GSMA — Mobile Money Fraud Typologies and Mitigation Strategies
Mobile money fraud typologies and mitigation concepts.

Note: This Public Release edition does not include restricted distribution sources, proprietary feeds, or any classified material.

SECTION 13

About AfriWealth Cyber Intelligence

AfriWealth Cyber Intelligence is a Ghana-based firm specialising in Cyber Threat Intelligence (CTI) and Blue Team advisory. The firm is structured around a CTI-First operating model: one in which adversary understanding informs detection strategy, defensive architecture, and security decision-making.

Through disciplined intelligence production and analytical rigour, AfriWealth is positioned to contribute to Ghana's structured cyber threat analysis ecosystem — providing the institutional and enterprise communities of Ghana and West Africa with intelligence products grounded in adversary behaviour rather than vendor prescription.

Attribute	Detail
Legal Entity	AfriWealth Cyber Intelligence
Headquarters	Accra, Ghana
Practice Areas	Cyber Threat Intelligence | Blue Team Operations
Regional Scope	Ghana and West Africa
Client Sectors	Government · Financial Services · Healthcare · Enterprise
Intelligence Series	AfriWealth National Intelligence Brief Series

AfriWealth Cyber Intelligence welcomes dialogue with government agencies, financial institutions, international development partners, and aligned organisations engaged in strengthening the security and resilience of Africa's digital infrastructure.

AfriWealth Cyber Intelligence

Built for Defense. Driven by Intelligence.

Accra, Ghana · West Africa

Cyber Threat Intelligence | Blue Team Operations