https://t.me/CyHawk_Africa

APRIL 2025

REPORT OF THE CYBER THREAT LANDSCAPE IN AFRICA

By

Hassanat Oladeji

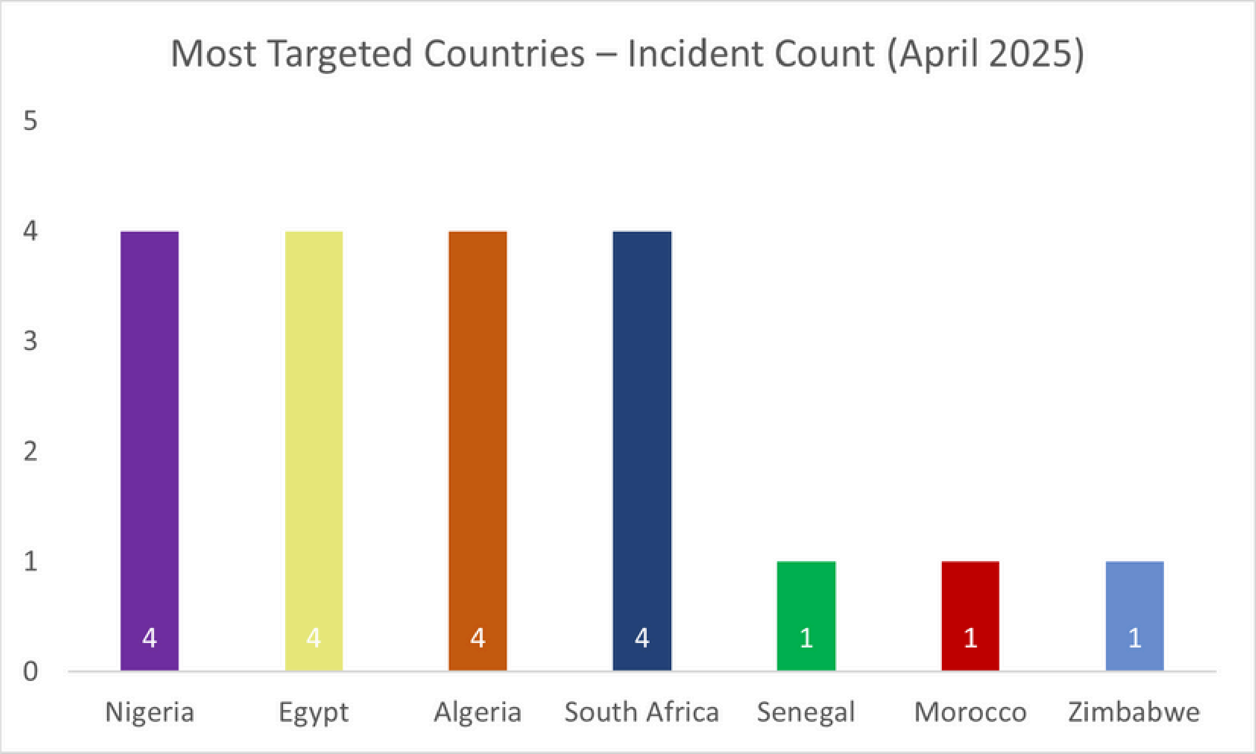
Executive Summary

In April 2025, a total of 19 cyber incidents were tracked across several African countries. This report provides a comprehensive analysis of the threat actors involved, targeted industries, geolocations, and the types of cyber threats observed. The data highlights a persistent focus on government entities and telecommunications infrastructure, with threat actors exploiting access vectors and databases, while ransomware incidents, though fewer, pose a critical risk to public and private sector organizations.

The analysis is based on a dataset of 19 cybersecurity incidents recorded between 1 April and 30 April 2025. The dataset includes the following fields:

- *S/No: Incident identifier*
- *Date: Date of the incident*
- *Threat Actor: Group or individual responsible*
- *Country: Targeted country*
- *Threat Type: Nature of the attack (e.g., database breach, defacement, ransomware)*
- *Industry: Sector targeted (e.g., government, education, telecommunications)*

TOP TARGETED COUNTRIES IN AFRICA



The geographic distribution of incidents reveals a significant concentration in four major African economies:

- Nigeria: 4 incidents (21%)
- South Africa: 4 incidents (21%)
- Egypt: 4 incidents (21%)
- Algeria: 4 incidents (21%)
- Senegal: 1 incident (5%)
- Morocco: 1 incident (5%)
- Zimbabwe: 1 incident (5%)

Egypt

Egypt experienced four significant cyber incidents, marking it as one of the most targeted countries in April. The threats were diverse, including:

- Database breaches (KILLUAX) aimed at telecommunication systems, potentially to gather sensitive communications metadata.
- Ransomware deployments by DragonForce, Crypto24, and Gunra, impacting various sectors including health.

This suggests both nation-state and financially motivated actors are active in the region. Egypt's role as a technological hub in North Africa and its complex geopolitical landscape make it a prime target.

Nigeria

Nigeria faced four incidents primarily aimed at government systems:

- Ghudra, responsible for two access intrusions, appears to be focused on gaining and maintaining unauthorized access.
- Sythe and MisterSam expanded their attacks to the education sector and public institutions.

Algeria

PhantomAtlas led the charge in Algeria with two incidents, mainly database breaches targeting government and telecom infrastructures. 0xraul and v1rusno1r targeted the “other” sector and government infrastructure, respectively. Algeria’s growing digital transformation and international relations might be drawing attention from adversarial cyber groups.

South Africa

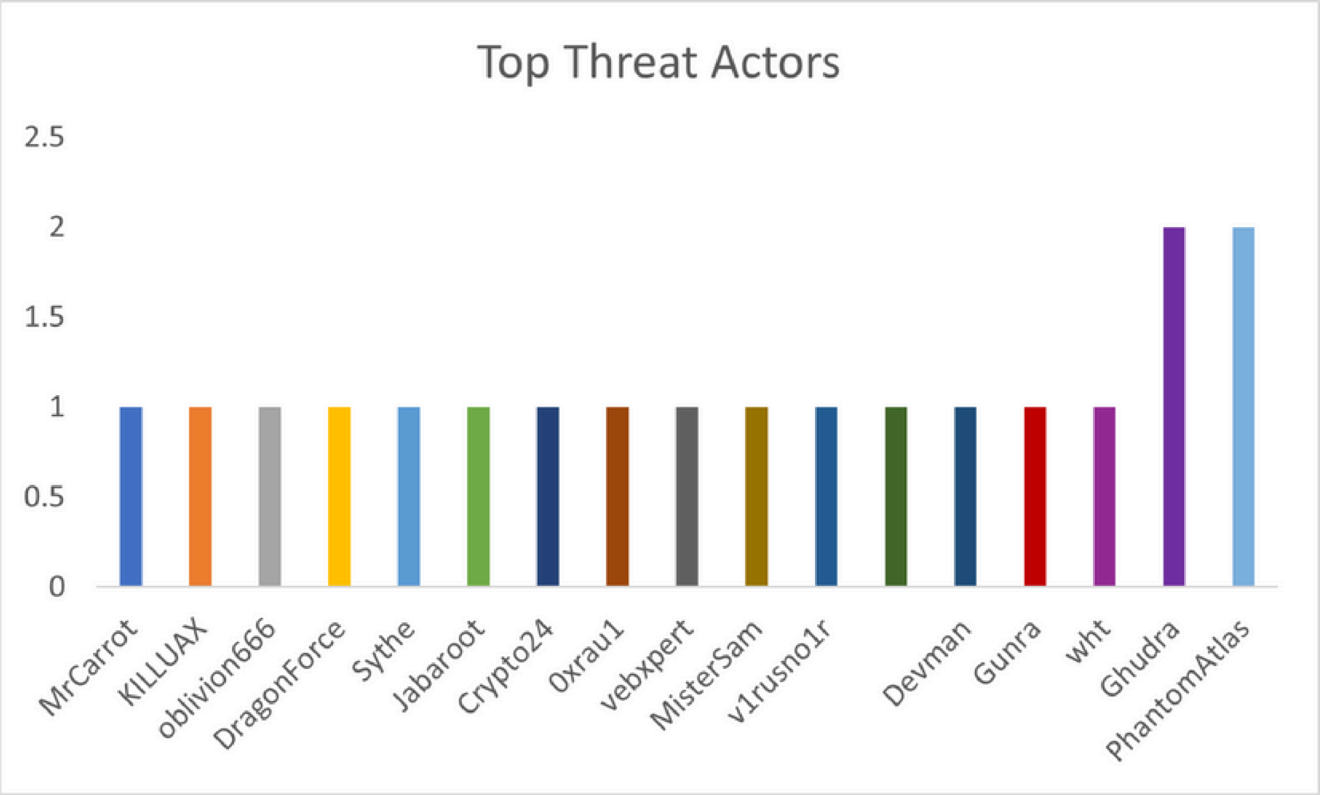
South Africa saw a range of attack types:

- Access threats from actors like MrCarrot and vebxpert.
- A ransomware attack by Devman.

The four countries with the highest incident counts collectively accounted for 84% of all recorded events. This concentration in major African economies suggests targeted campaigns based on economic or strategic significance rather than opportunistic attacks.

The distribution pattern indicates a deliberate focus on countries with more developed digital infrastructure and economic importance, potentially indicating strategic targeting rather than random attacks.

MOST ACTIVE THREAT ACTORS



The analysis identified several distinct threat actors responsible for the recorded incidents:

- Ghudra: 2 incidents (11%)
- PhantomAtlas: 2 incidents (11%)

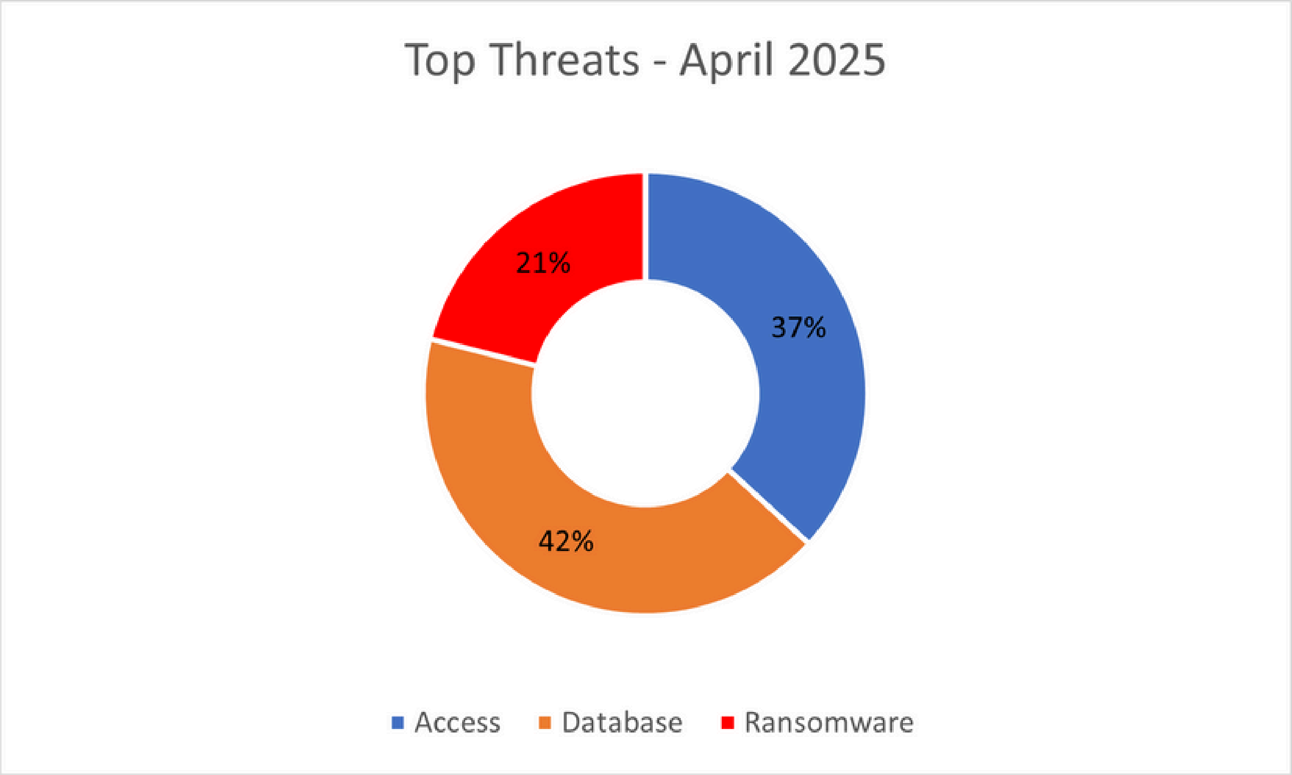
Ghudra and PhantomAtlas were the most active threat actors, with each responsible for 2 incidents each during the reporting period. The remaining incidents were attributed to various actors, each responsible for a single incident.

Notable patterns in threat actor behavior include:

- Ghudra: Exclusively targeted government institutions in Nigeria
- PhantomAtlas: Conducted both attacks in Algeria
- Other notable actors: MrCarrot, KILLUAX, oblivion666, DragonForce, Sythe, Jabaroot, Crypto24, and 0xraul.
- Crypto24, DragonForce, Devman and Gunra – Involved in ransomware deployments, often targeting non-specific sectors, indicating a financially motivated campaign.

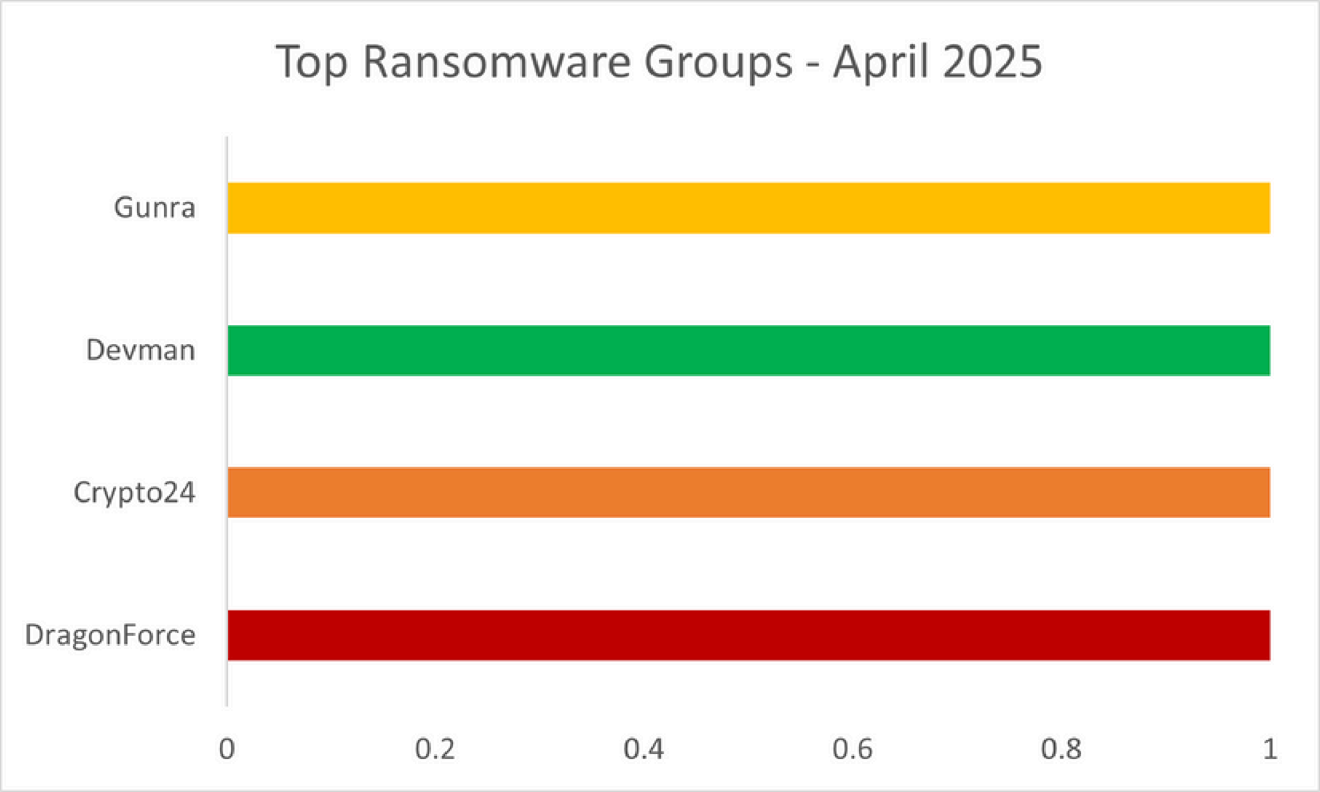
The diversity of threat actors suggests a complex threat landscape with multiple independent or loosely affiliated groups operating across the region.

TOP THREATS



- **Database Attacks**: The most common threat type, targeting data exfiltration, sale, or exposure. This indicates a high demand for sensitive information, possibly for espionage or monetization.
- **Access-based Intrusions**: Suggest preliminary compromise efforts such as credential harvesting or exploiting remote access services.
- **Ransomware Attacks**: Though less frequent, these attacks cause significant disruption and financial damage, especially when targeting critical infrastructure.

TOP RANSOMWARE GROUPS



DragonForce

- Target Country: Egypt
- Target Sector: Miscellaneous/Other

DragonForce deployed ransomware on unspecified entities, suggesting opportunistic targeting for financial extortion.

TOP RANSOMWARE GROUPS

Crypto24

- Target Country: Egypt
- Target Sector: Miscellaneous/Other

Operating a RaaS (Ransomware-as-a-Service) model, Crypto24 primarily focuses on rapid encryption of critical files followed by extortion threats. They are known for using double extortion (data exfiltration + encryption) and leveraging Telegram for ransom negotiations.

Gunra

- Target Country: Egypt
- Target Sector: Healthcare

Gunra is a recently emerged ransomware group that was first observed in April 2025. The group primarily targets Windows systems and has already claimed multiple victims across different sectors including healthcare, manufacturing, and real estate.

Devman

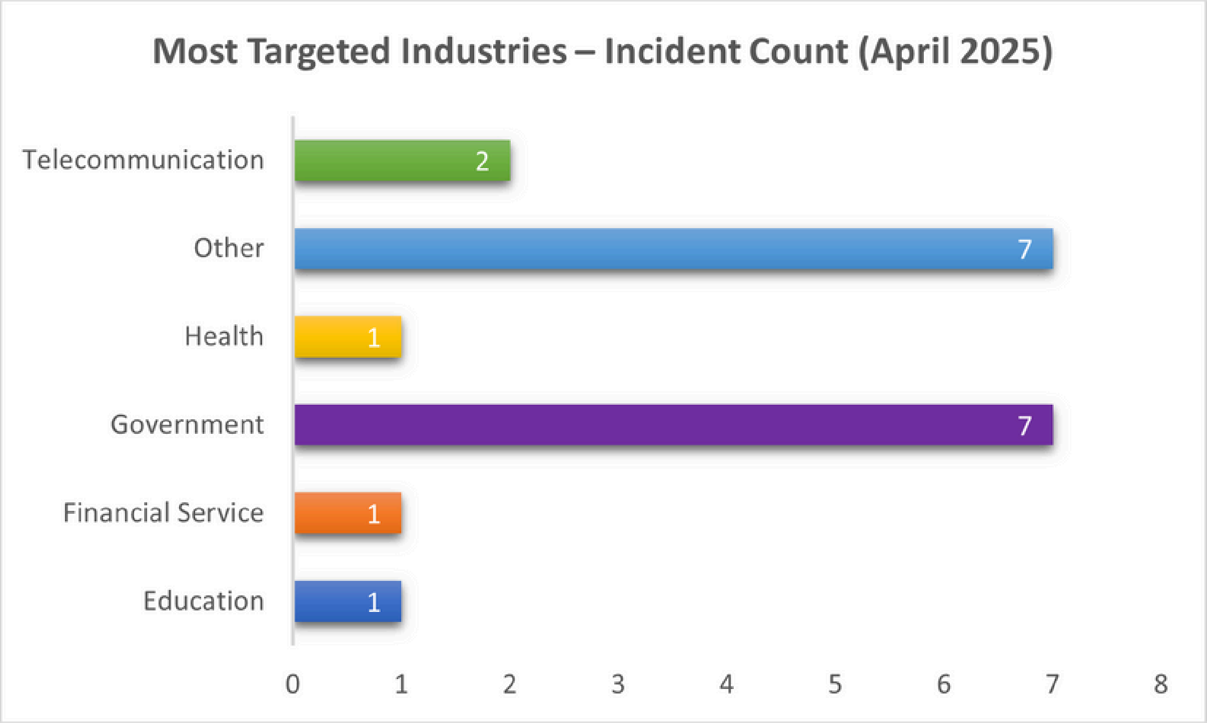
- Target Country: South Africa
- Target Sector: Other

DevMan is a relatively new ransomware group that emerged in early 2025. The group has been actively targeting organizations across various sectors and geographical locations.

DragonForce

DragonForce ransomware employs a double extortion strategy, both encrypting victims' data and threatening to leak stolen information if ransom demands aren't met. With 149 claimed victims since November 2023, the group has quickly established itself as a significant threat in the ransomware landscape. The group targeted Egypt in April 2025.

INDUSTRIES MOST TARGETED



Government – (7 incidents)
The government sector accounted for the highest number of attacks (7), underscoring its status as a high-value target. Attacks in this category primarily involved access-based intrusions and database breaches. These activities indicate attempts to gather intelligence, disrupt governance, or access classified or politically sensitive data. Repeated attacks by actors such as Ghudra and PhantomAtlas suggest a coordinated or sustained campaign against public sector infrastructures in countries like Nigeria, Algeria, and Morocco.

Telecommunications (2 incidents)

With 2 significant database-related incidents, the telecommunications sector remains a high-stakes target. Attacks on this sector—such as those carried out by KILLUAX and PhantomAtlas—highlight the risk of surveillance, call metadata harvesting, and even manipulation of national communication channels. These threats may be linked to both espionage and competitive disruption motives.

Education (1 incident)

A single but notable database attack by Sythe targeted the education sector in Nigeria. Although representing a small portion of total incidents, attacks on educational institutions are concerning due to the sensitive personal data they hold, including records of students and staff, and potential intellectual property theft.

Health (1 incident)

Gunra's ransomware deployment against a healthcare institution in Egypt brings to light the vulnerability of critical health infrastructure. Such incidents can have life-threatening consequences and are often designed to exploit the urgency and low tolerance for downtime in the medical sector.

Financial Services (1 incident)

The attack on a financial service provider in Zimbabwe, involving database compromise, poses severe risks including customer identity theft, financial fraud, and regulatory non-compliance. As financial entities digitize operations, they become increasingly susceptible to sophisticated cyber threats.

Other (7 incidents)

Seven incidents fell under "Other," encompassing private companies, small enterprises, and undefined organizations. Actors like DragonForce, MrCarrot, and Devman primarily targeted these entities with access attempts and ransomware, potentially aiming for quick financial gain or as part of a broader campaign testing vulnerabilities across less-defended environments.

CONCLUSION

The April 2025 cybersecurity landscape across major African economies shows a pattern of targeted, strategic attacks focused on data theft and access violations, with government institutions being particularly vulnerable.

The diversity of threat actors and the observed specialization in targeting specific countries and sectors create a complex threat landscape that requires sophisticated and coordinated defense strategies.

Organizations across all sectors should implement enhanced security measures, with particular attention to database security and access management.

Regional cooperation is essential for addressing these transnational threats effectively. Policymakers should prioritize information sharing, joint response capabilities, and harmonized legal frameworks to combat cybercrime across borders.

By understanding the patterns and strategies of threat actors operating in the region, organizations and governments can develop more effective defenses and reduce their vulnerability to future attacks.

RECOMMENDATIONS

To effectively respond to the threats observed in April 2025, here are a few practical steps organizations across Africa should take:

1. **Strengthen Access Control Measures**
Organizations should enforce the use of multi-factor authentication (MFA) and routinely review user access rights—especially in sectors like government and education where we’ve seen repeated targeting.

2. **Keep Systems Up to Date**
It's important to regularly patch systems and applications. Automating this process where possible can help ensure vulnerabilities are closed before attackers exploit them.

3. **Leverage Localized Threat Intelligence**
Tapping into up-to-date and localized cyber threat intelligence can help security teams stay ahead of attackers. Engaging with threat intel communities also enhances our ability to anticipate threats.

4. **Educate Employees About Cyber Risks**
Staff awareness is critical. Everyone—especially those in high-risk industries like health and finance—should be trained to recognize phishing attempts, suspicious links, and other social engineering tactics.

RECOMMENDATIONS

5. **Improve Network Segmentation and Endpoint Visibility**
Critical infrastructure should be separated from general-use networks. Having good endpoint detection and response (EDR) tools helps detect and respond to suspicious behavior more quickly.

6. **Test Your Incident Response Plan**
It’s not enough to have a plan—organizations need to test it regularly. Tabletop exercises and internal simulations help identify gaps before a real incident occurs.

7. **Track Data Leaks and Exposed Credentials**
Given the rising exposure of African data on dark web forums, tools that monitor for leaked credentials and brand impersonation can help detect threats early and reduce the damage.

Taking these steps will go a long way in helping African organizations build resilience and respond more effectively to future cyber attacks.