https://t.me/CyHawk_Africa

MARCH 2025

REPORT OF THE CYBER THREAT LANDSCAPE IN AFRICA

By
Hassanat Oladeji

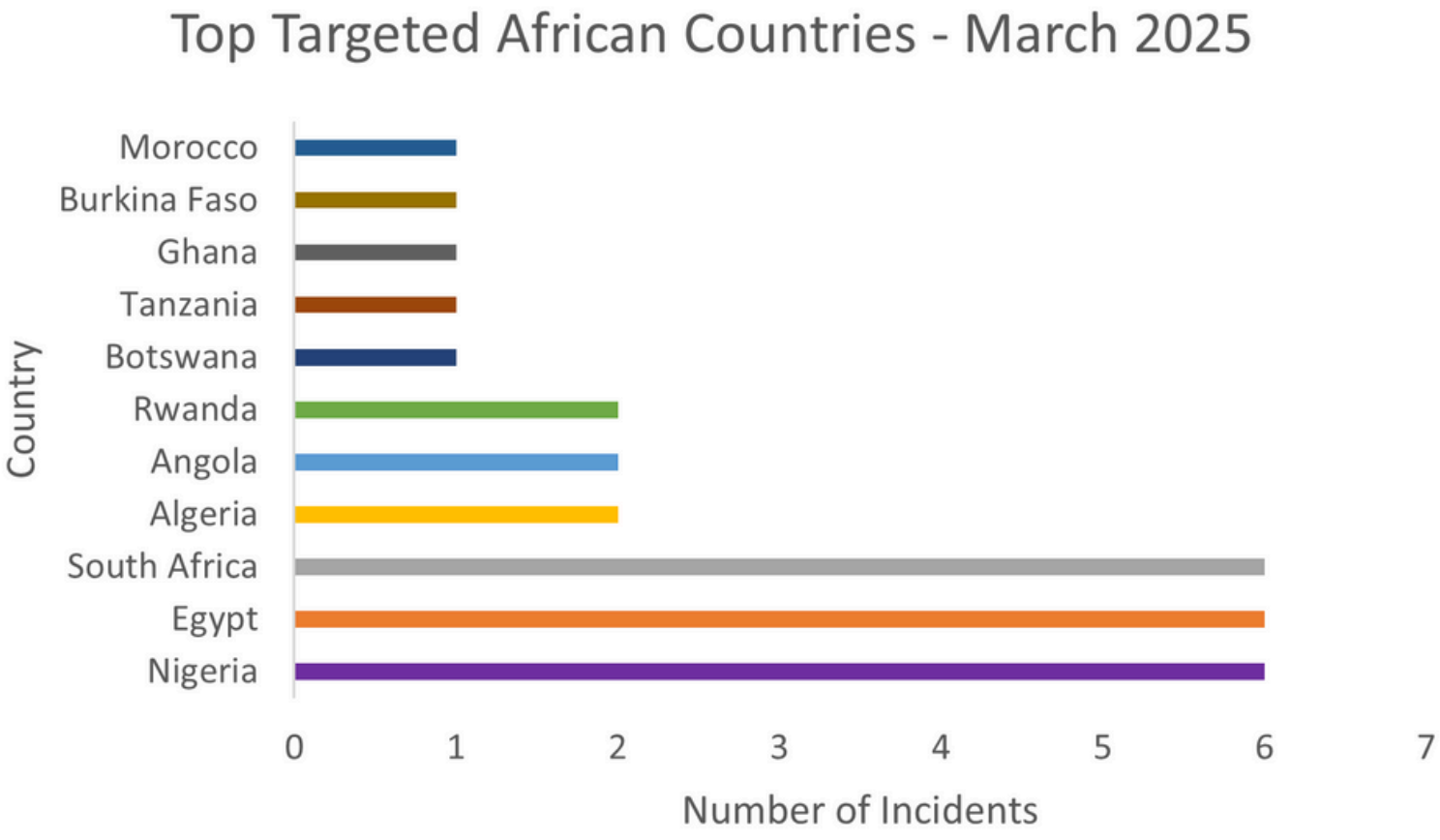
Executive Summary

In March 2025, CyHawk observed a surge in cyber threats targeting African digital infrastructure. Government, education, and technology sectors faced persistent access breaches, ransomware incidents, and database exfiltration. Notable threat actors such as DataSec and Ghudra were actively involved in these campaigns. Nigeria, Egypt, and South Africa remained the most targeted nations during this period. This report provides a comprehensive breakdown of the incidents observed, including threat actor activity and targeted sectors.

The analysis is based on a dataset of 29 cybersecurity incidents recorded between 1 March and 31 March 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



🇳🇬 Nigeria – 6 Incidents

- Nigeria remains the most targeted nation this month, driven largely by ransomware, access attacks, and defacements. Threat actors targeted government platforms, financial services, and technology firms. Its leading fintech ecosystem and growing digital adoption continue to attract attention from cybercriminals.

🇪🇬 Egypt – 6 Incidents

- Egypt matched Nigeria in attack volume, with a mix of access, ransomware, database breaches, and even a DDoS incident. The education and government sectors were frequent targets, indicating vulnerabilities in public sector digital infrastructure.

🇿🇦 South Africa – 6 Incidents

- South Africa faced a range of threats, including ransomware and database leaks, targeting e-commerce, government, and other sectors. Its status as a regional tech hub makes it a prime target for financially motivated actors.

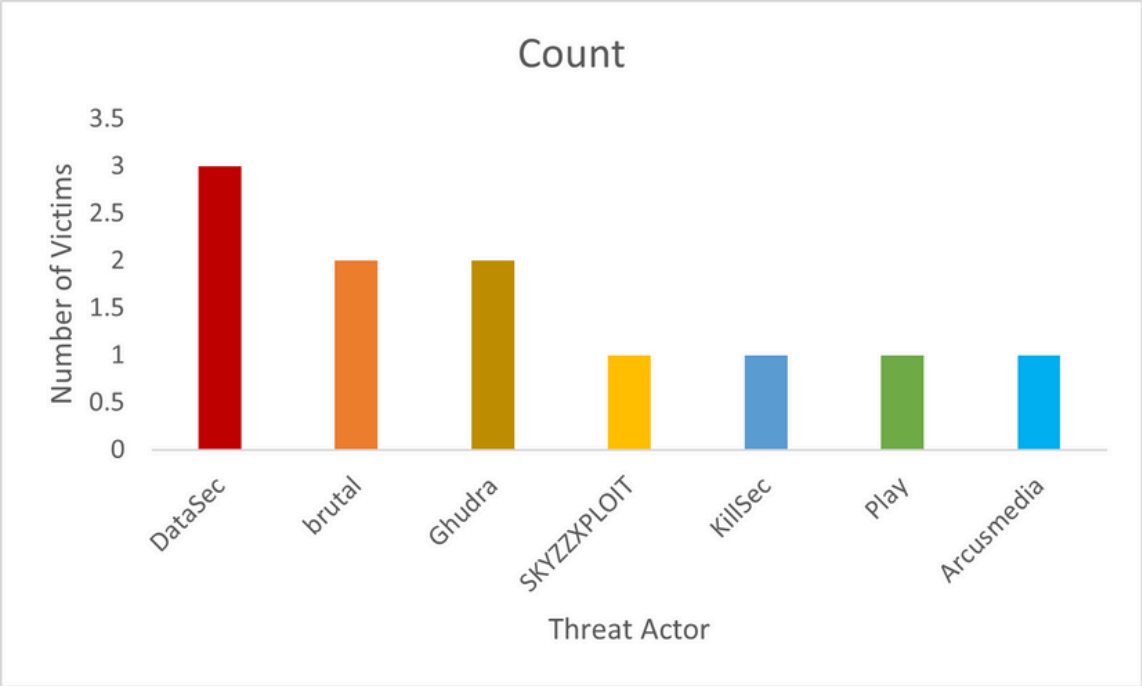
🇩🇿 Algeria – 2 Incidents

- Algeria experienced access-related incidents aimed at government and other critical sectors. These could indicate probing behavior by threat actors scouting for vulnerabilities.

🇦🇴 Angola – 2 Incidents

- Angola saw two access-based attacks targeting government institutions, likely indicating attempts to infiltrate sensitive systems or exfiltrate data.

MOST ACTIVE THREAT ACTORS



🕵️ **DataSec**

- Country Targets: Algeria, Egypt, Tanzania
- Industry Focus: Primarily Government
- Threat Type: Unauthorized Access

Summary: DataSec was the most active threat actor in March 2025, targeting government agencies across North and East Africa. Their attacks focused on gaining unauthorized access, likely for espionage, data theft, or initial footholds for further exploitation.

🕵️ **Ghudra**

- Country Targets: Rwanda, Burkina Faso
- Industry Focus: Government
- Threat Type: Database compromises and Access

Summary: Ghudra focused on West and East Africa, breaching government systems through database leaks and access intrusions. This suggests a persistent effort to expose or exploit state-held data.

🕵️ **brutal**

- Country Targets: Angola, South Africa
- Industry Focus: Government
- Threat Type: Access

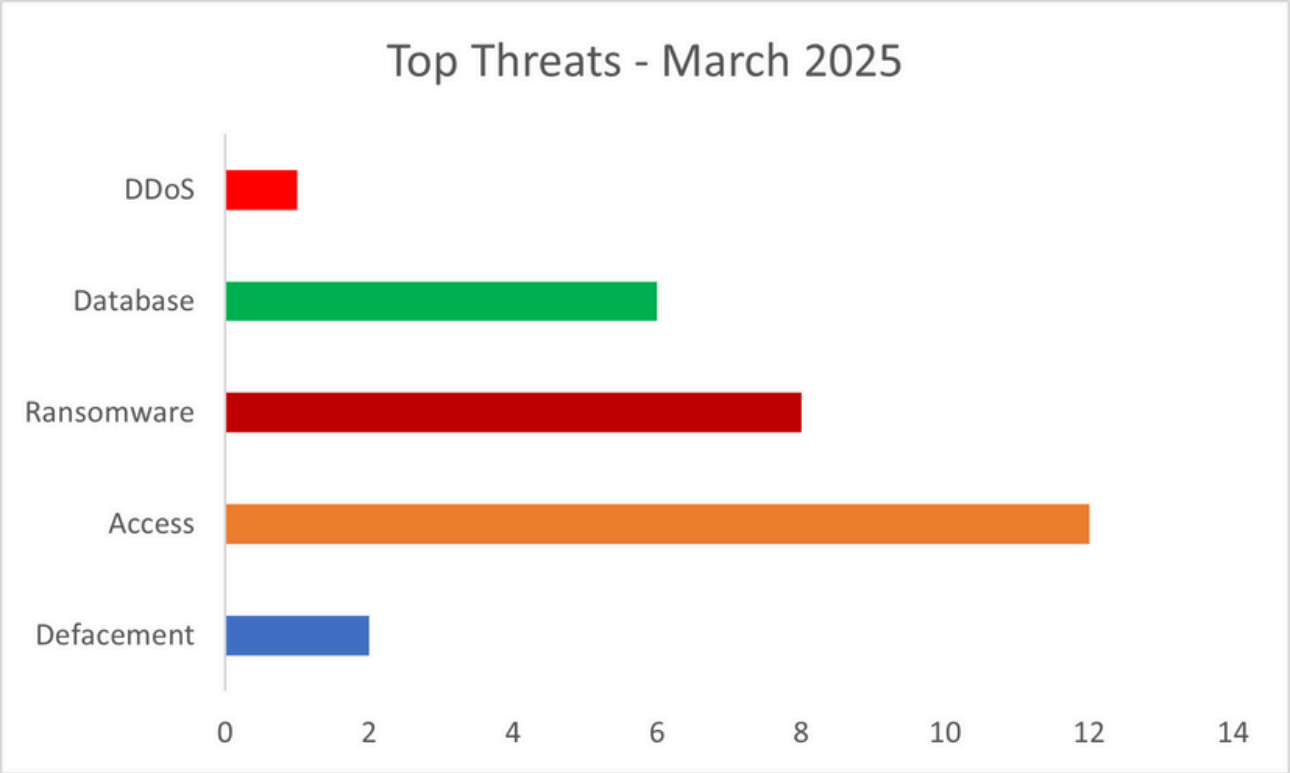
Summary: Operating with a focus on government institutions, brutal's campaigns were centered on unauthorized access. The dual targeting of Southern African nations hints at regionally coordinated efforts or interests.

🕵️ **Arcusmedia & Lynx**

- Country Targeted: South Africa
- Industry Focus: Other (likely private sector or SMEs)
- Threat Type: Ransomware

Summary: These actors deployed ransomware in South Africa, signaling rising ransomware activity in the region against non-government sectors.

TOP THREATS



In March 2025, Access attacks were the most common threat type, accounting for a significant portion of incidents. These attacks typically aim to gain unauthorized entry into systems, often targeting government entities across multiple countries.

TOP THREATS

- 🔓 **Access** (41%)

This was the most dominant threat, accounting for the highest number of incidents across multiple regions in Africa. Threat actors like **DataSec**, **brutal**, and **Ghudra** consistently gained unauthorized access into systems, primarily targeting government entities. These intrusions are often used to establish footholds for espionage, data theft, or future attacks such as ransomware.

- Most Targeted Countries: Egypt, Nigeria, South Africa, Angola
- Industries Affected: Government, Education, Other

💥 **Ransomware Attacks** (28%)

Ransomware remains a severe and financially motivated threat. Actors like KillSec, Arcusmedia, Play, Funksec, and Babuk launched encryption-based attacks, demanding ransoms from victims to restore access to systems or sensitive data.

- Most Targeted Countries: South Africa, Nigeria, Egypt, Rwanda
- Industries Affected: Technology, Health, Education, Other

🗄️ **Database Compromises** (21%)

Multiple actors, including **bib0rn**, **Jumbojet**, **Kobal**, and **Ghudra**, were involved in breaches where large volumes of data were exposed or exfiltrated from vulnerable databases. These often affect sectors that store vast user data sets, including education and financial services.

- Most Targeted Countries: Egypt, Ghana, South Africa
- Industries Affected: Education, E-Commerce, Financial Services

TOP THREATS

🏜️ **Website Defacements** (7%)

Defacements are typically politically or ideologically motivated, meant to embarrass targets or spread a message. Actors like SKYZZXPLOIT and 0x focused on altering websites in Nigeria, primarily targeting technology and government sectors.

- Most Targeted Country: Nigeria
- Industries Affected: Government, Technology

🌐 **DDoS Attacks** (3%)

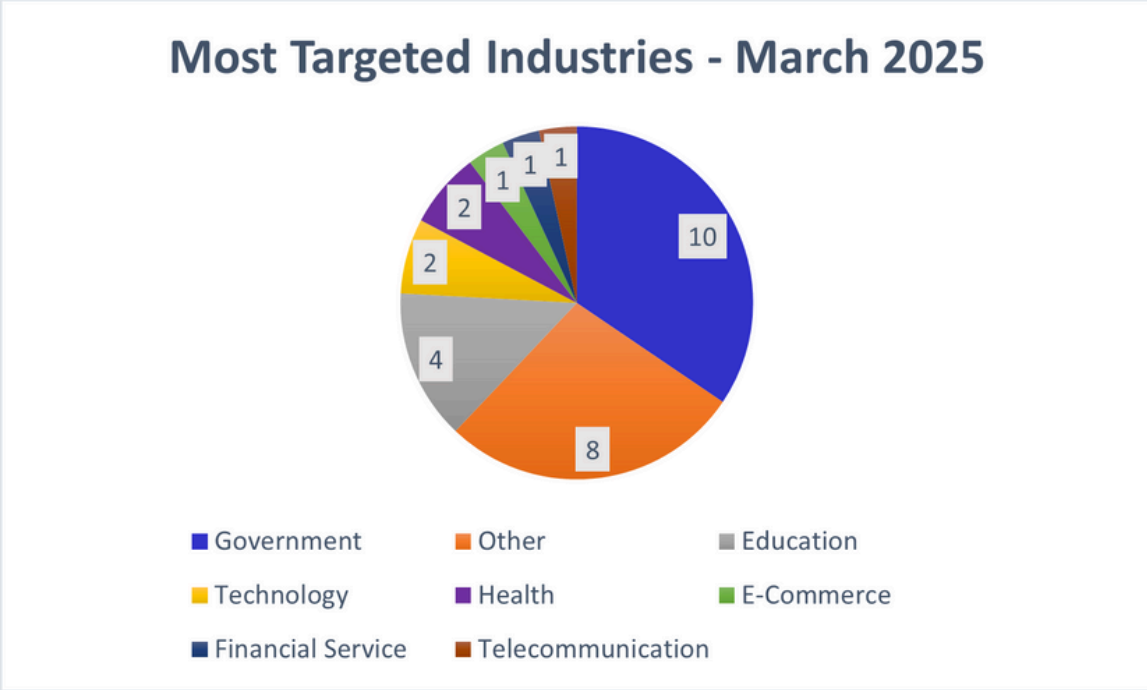
- Description: Only one notable DDoS campaign was observed, orchestrated by DieNet, targeting the telecommunication sector in Egypt. Although not widespread, this highlights the vulnerability of critical communication infrastructure.
- Most Targeted Country: Egypt
- Industries Affected: Telecommunications

TOP RANSOMWARE GROUPS

Ransomware remained one of the most dominant threats in Africa during March 2025, with several APT groups actively targeting critical sectors. These actors focused on industries such as healthcare, technology, and education, leveraging encryption and extortion tactics to pressure victims. Below are the top ransomware groups observed:

1. **KillSec** – Targeted a victim in Nigeria.
2. **Play** – Hit Botswana's tech sector using double extortion tactics.
3. **Arcusmedia** – Operated in South Africa, targeting miscellaneous sectors.
4. **Lynx** – Focused on a victim in South Africa.
5. **Funksec** – Attacked Egypt's education sector.
6. **Sarcoma** – Targeted a victim in South Africa.
7. **NightSpire** – Targeted a victim in Egypt's healthcare sector.
8. **Babuk** – Hit a victim in Rwanda's health sector.

INDUSTRIES MOST TARGETED



🏛️ Government – (10 incidents)

The government sector was the most targeted industry across multiple countries, accounting for nearly half of all reported incidents.

- Common Threats: Access intrusions, defacements, ransomware
- Countries Impacted: Egypt, Nigeria, Angola, Algeria, Burkina Faso, South Africa, Tanzania
- This trend highlights government systems as lucrative targets for cybercriminals seeking to disrupt critical services or steal sensitive information.

🎓 Education – Soft Target for Data Breaches (4 incidents)
Educational institutions faced database leaks and ransomware, mostly in Egypt, Ghana, and Morocco.

- Common Threats: Database exposure, ransomware, access
- The education sector often suffers from outdated infrastructure and limited cybersecurity resources, making it a recurring target.

💻 Other / Miscellaneous – Ransomware-Focused (8 incidents)

- Several attacks were directed at unidentified or uncategorized "Other" organizations, many of which were hit by ransomware.
- This category's diversity suggests that small businesses and miscellaneous service providers remain highly vulnerable.

🛒 E-Commerce – Targeted for Databases (1 incident)

- Threat Type: Database breach
- E-commerce platforms face a growing threat due to the value of customer data stored in online systems.

🏥 Health – Ransomware & Database (2 incidents)

- Rwanda's health sector experienced ransomware, while Egypt's health sector experienced database compromise.
- This emphasizes an alarming rise in healthcare-related cybercrime, which can have life-threatening consequences.

CONCLUSION

The cyber threat landscape in Africa for March 2025 reveals a clear pattern of targeted, persistent, and financially motivated attacks, with a strong focus on government institutions, critical infrastructure, and data-sensitive sectors such as education, health, and technology. The prominence of Access and Ransomware attacks reflects attackers' efforts to gain footholds in high-value environments, disrupt services, and extract financial gain.

As threat actors grow increasingly organized and regionally focused, it is crucial for organizations across Africa to strengthen their cyber defense strategies, improve incident response capabilities, and prioritize threat intelligence to stay ahead of evolving threats. Collaboration, information sharing, and proactive monitoring will remain essential in building resilience against future attacks.

CyHawk will continue to monitor, analyze, and report on emerging threats to help organizations across Africa stay informed and protected.

RECOMMENDATIONS

To effectively respond to the threats observed in March 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.