https://t.me/CyHawk_Africa

MAY 2025

REPORT OF THE CYBER THREAT LANDSCAPE IN AFRICA

By

Hassanat Oladeji

Executive Summary

In May 2025, Africa faced a surge in cyberattacks, with Devman being the most active threat actor, responsible for eight incidents. South Africa was the most targeted country, while government and financial sectors bore the brunt of attacks.

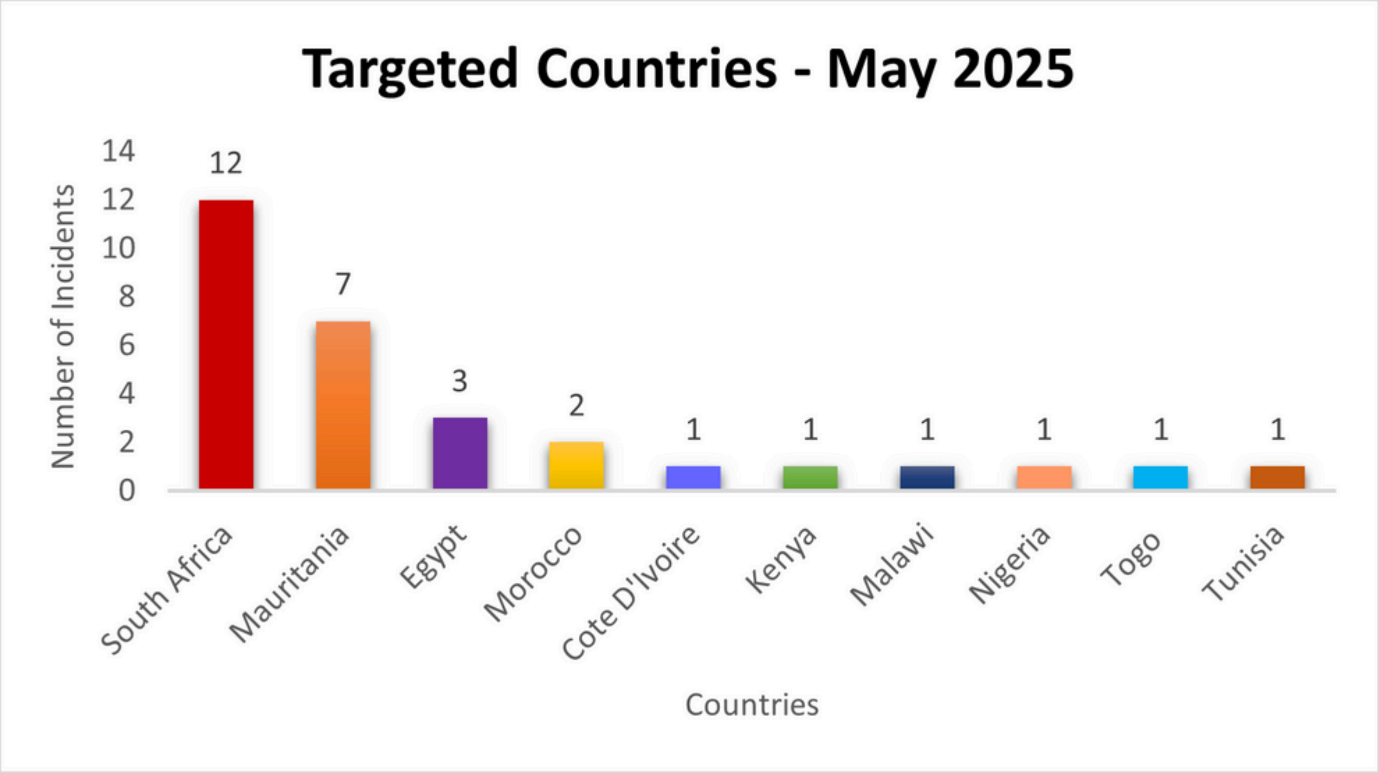
Database breaches (50%) and ransomware (34%) were the most common threats. The ransomware group Devman dominated the threat landscape, outpacing other groups like Nightspire and Incrasom.

This report highlights critical gaps in cybersecurity, especially in public infrastructure, and calls for urgent action to strengthen defenses across the region.

The analysis is based on a dataset of 30 cybersecurity incidents recorded between 1 May and 31 May 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)*

TARGETED COUNTRIES IN AFRICA



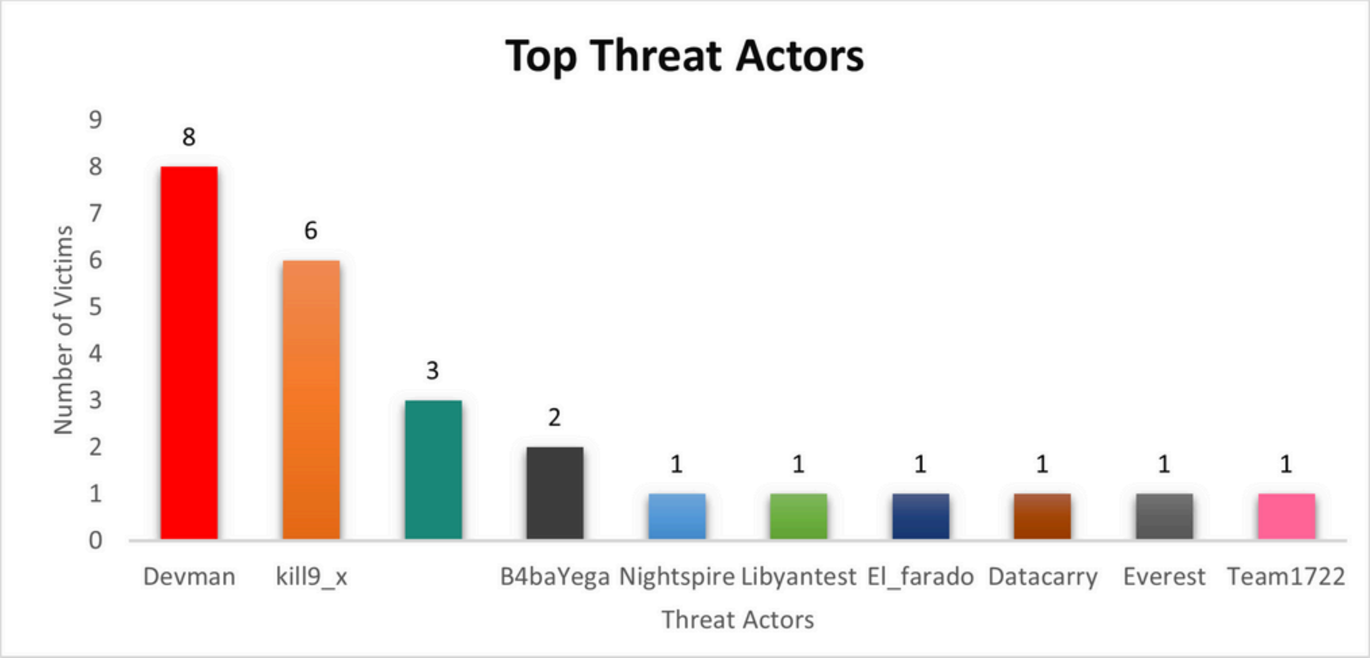
South Africa remained the top target with 12 reported incidents, driven largely by ransomware and defacement campaigns. The high frequency indicates sustained interest in South Africa's digital infrastructure, particularly in the government and technology sectors.

Other highly targeted countries include:

- Mauritania – 7 incidents
- Egypt – 3 incidents
- Morocco – 2 incidents

Additional countries like Côte d'Ivoire, Kenya, Malawi, Nigeria, Togo, and Tunisia were each hit once, signaling a broader regional threat distribution across Africa.

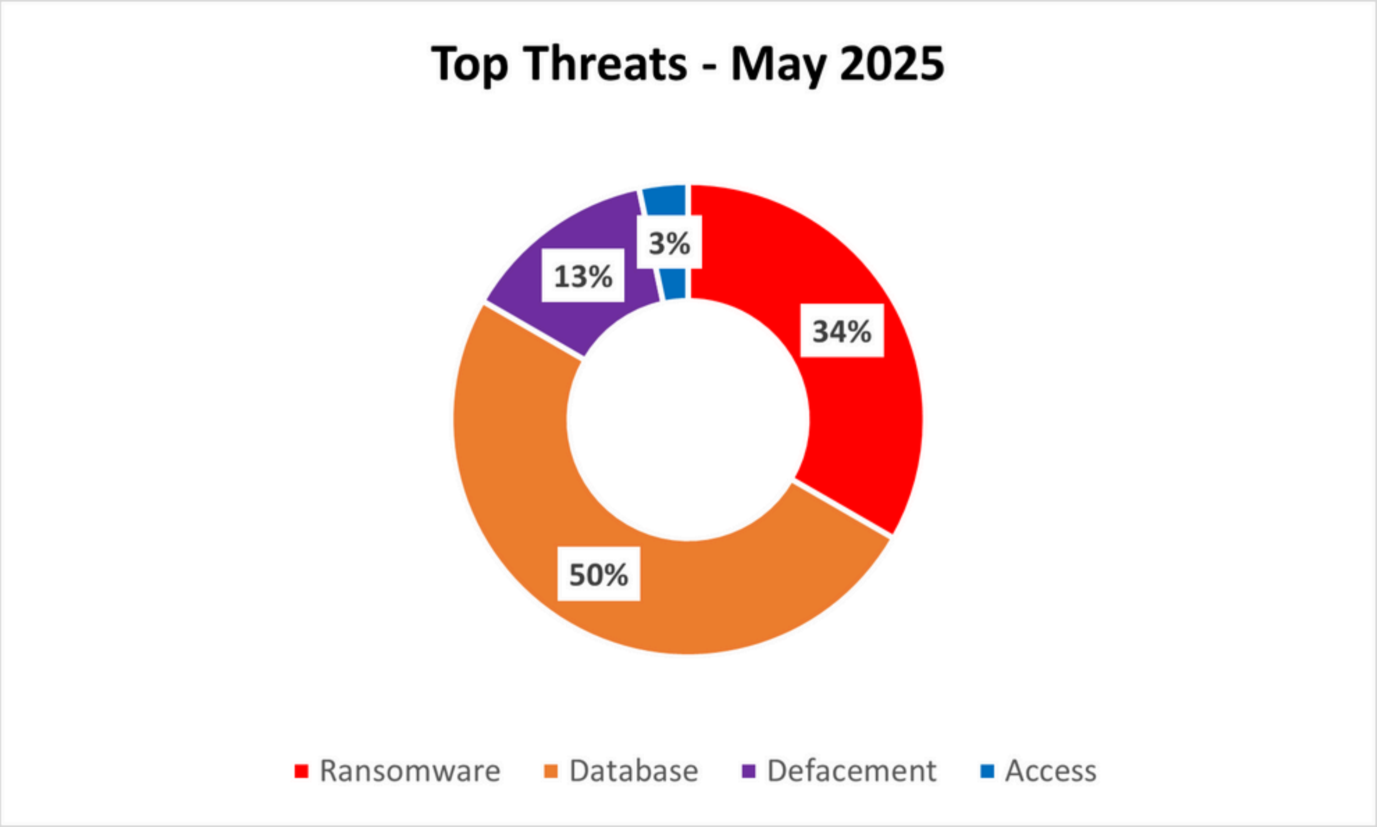
MOST ACTIVE THREAT ACTORS



The most active threat actor in May 2025 was Devman, responsible for 8 incidents, mostly involving ransomware. Devman's repeated targeting across sectors and geographies suggests a coordinated campaign with advanced capabilities. Following Devman:

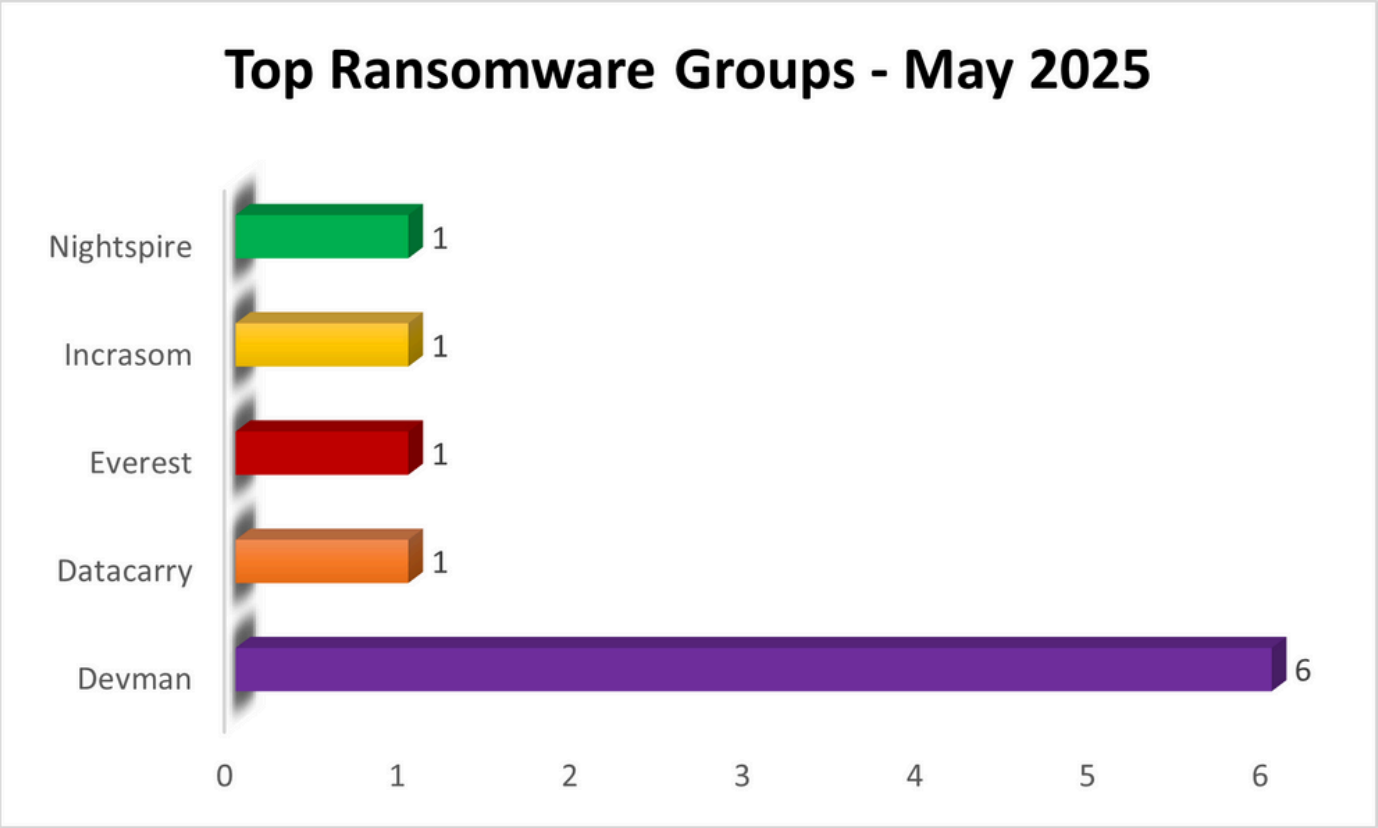
- kill9_x was involved in 6 attacks, mainly related to database leaks of 5 financial and 1 government institutions.
- B4baYega (3 incidents) and Nightspire (2 incidents) showed limited but specific targeting behavior.
- Other actors like Libyantest, El_farado, Datacarry, Everest, and Team1722 were linked to 1 incident each, indicating either isolated operations or early activity phases.

TOP THREATS



- Database compromises were the most prevalent at 50%, revealing widespread exposure of backend systems and poor data hygiene practices.
- Ransomware accounted for 34% of incidents, often deployed by Devman and other notable actors.
- Defacement campaigns stood at 13%, typically used for hacktivism or reputational damage.
- Access breaches (3%) were the least reported, possibly due to underdetection or covert intrusion.

TOP RANSOMWARE GROUPS



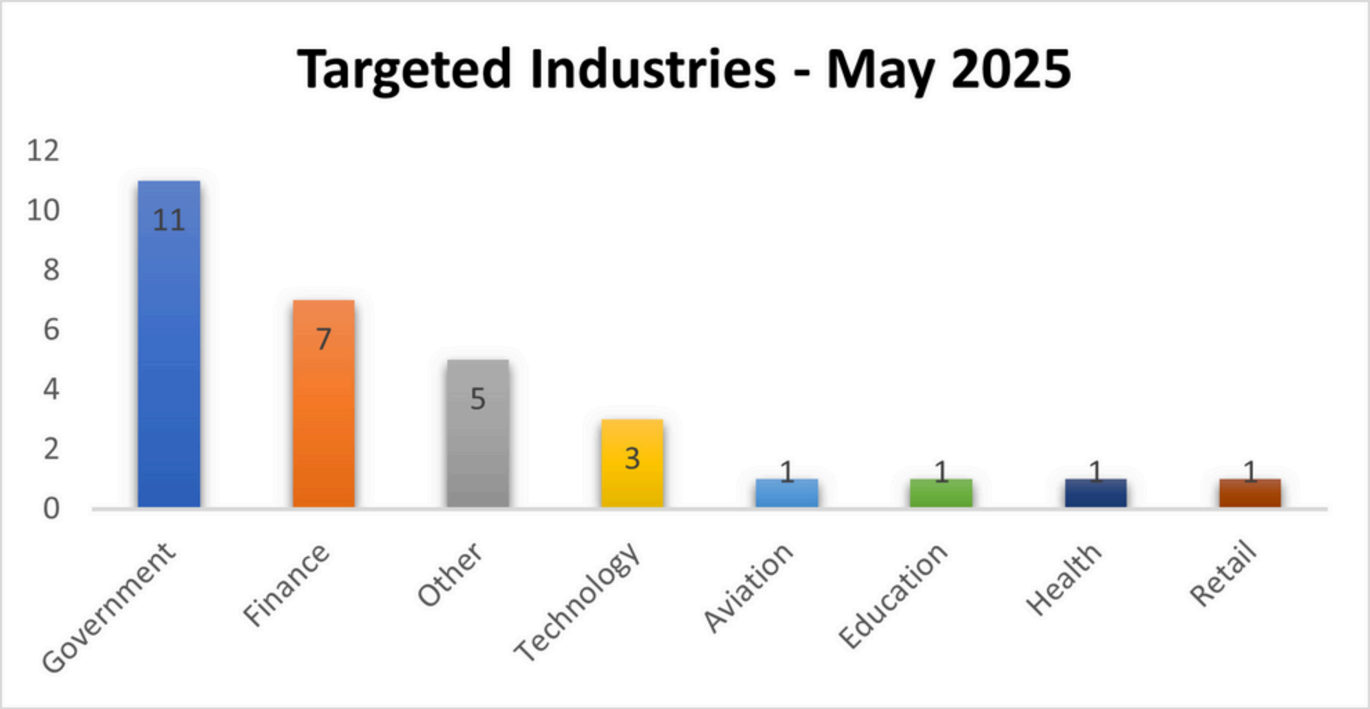
Devman led the ransomware threat landscape in May with 6 successful deployments across multiple countries and industries. This group's dominance aligns with a global increase in opportunistic and targeted ransomware campaigns.

Other active ransomware groups include:

- Nightspire
- Incrasom
- Everest
- Datacarry

Each group was responsible for one confirmed ransomware incident.

INDUSTRIES MOST TARGETED



The government sector was the most targeted in May 2025 with 11 incidents, continuing its trend as the primary focus for cyberattacks in Africa.

Following closely:

- Finance (7 incidents): Hit by ransomware and database leak.
- Other sectors (5), including NGOs and SMEs.
- Technology (3), Aviation, Education, Health, and Retail (1 each) round out the targeted list, highlighting cross-sector vulnerability.

CONCLUSION

The cybersecurity threat activity across Africa in May 2025 reflects an increasingly sophisticated and aggressive landscape. Threat actors are evolving their tactics, focusing not only on disruption but also on data exfiltration, extortion, and long-term infiltration. The continued dominance of ransomware and database compromises highlights systemic weaknesses in cyber hygiene, access management, and incident response across various sectors.

Devman's prominence as both a top threat actor and ransomware group is especially concerning. With operations spanning multiple industries and countries, this group demonstrates both scale and intent. The high number of incidents in South Africa suggests targeted campaigns against regions with relatively higher digital footprints and interconnected systems.

The government sector, as the most targeted, remains vulnerable due to legacy systems, limited cybersecurity funding, and inconsistent policy enforcement. Similarly, the financial sector continues to attract attackers due to the high-value data it holds and its critical role in economic stability.

Furthermore, the dominance of database-related breaches (50%) points to poor database configuration, lack of encryption, and insufficient monitoring. These lapses give threat actors easy entry points to steal, sell, or ransom sensitive information.

RECOMMENDATIONS

To effectively respond to the threats observed in May 2025, here are some 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 such as 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.

ABOUT US

CyHawk is Africa’s open-source cyber threat intelligence platform dedicated to tracking, documenting, and exposing digital threats targeting individuals, organizations, and key sectors across the continent.

We analyze real-time threat data—from ransomware and data breaches to defacements and dark web activity—focusing exclusively on incidents affecting Africa. Our mission is to bridge the intelligence gap by providing publicly accessible, evidence-based reports that empower defenders, raise awareness, and support policy efforts across the continent.

What We Offer

- Monthly threat reports highlighting emerging actors and trends
- Dark web monitoring for African-related leaks, sales, and chatter
- Blog posts & incident analyses breaking down complex attacks
- Awareness campaigns focused on education and resilience

We believe cybersecurity in Africa must be community-driven, transparent, and locally relevant.

Learn More
Visit us at www.cyhawk-africa.com
For collaborations, tips, or threat submissions:
info@cyhawk-africa.com