Report of the Cyber Threat Landscape in Africa

August 2025

Prepared by :
Hassanat Oladeji

www.cyhawk-africa.com

Executive Summary

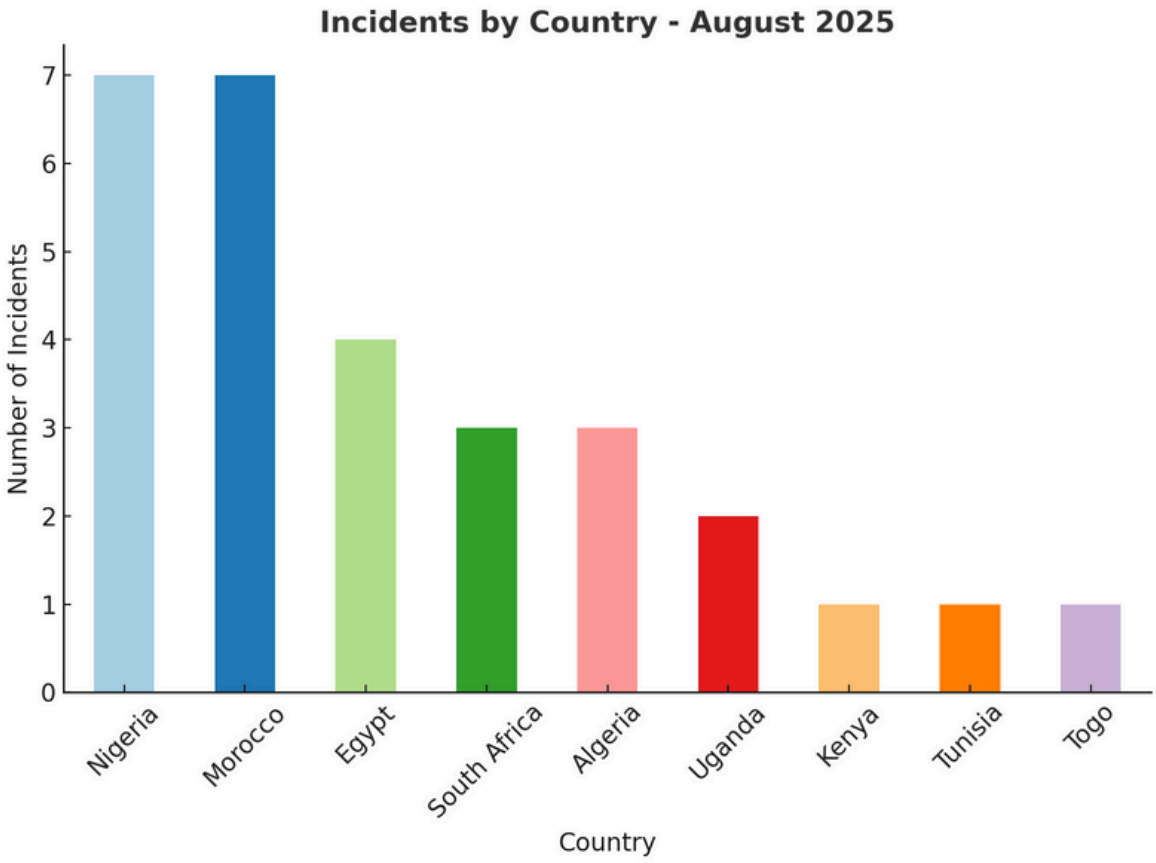
August 2025 witnessed 29 reported cyber incidents across Africa, reinforcing the continent's rising exposure to both global and local threat actors. The month's activity showed a mix of ransomware attacks on critical infrastructure, persistent database leaks affecting education and financial services, and renewed denial-of-service (DOS) campaigns targeting e-commerce platforms.

The most targeted countries were Nigeria, Morocco, and Egypt, highlighting the concentration of attacks on financial hubs, large government institutions, and education systems. A notable trend was the focus on the power sector, where ransomware groups such as Qilin launched disruptive attacks against Kenya and Uganda. Meanwhile, repeat offenders such as hider_nex, N1KA, and oursec continued their campaigns, solidifying their presence in the African cyber threat ecosystem.

The analysis is based on a dataset of 50 cybersecurity incidents recorded between 1 August and 31 August 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)*

REGIONAL THREAT LANDSCAPE



West Africa

- Nigeria remained the most impacted, recording incidents that spanned vulnerabilities, database breaches, and access operations. Education and financial services institutions were repeatedly targeted, with actors such as N1KA and 888 compromising customer data.
- Togo also appeared in the dataset, where bigbrother gained access to government systems, emphasizing the expansion of access broker activity in West Africa.

REGIONAL THREAT LANDSCAPE

North Africa

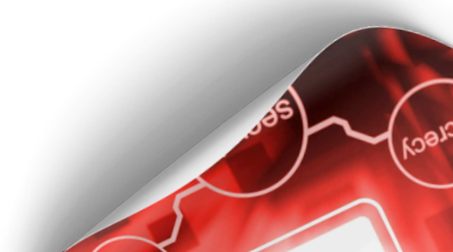
- Morocco recorded a high number of database-related incidents, especially within government, education, and e-commerce sectors. Actors like oursec and chucky_bf led campaigns that included DOS operations.
- Algeria saw both ransomware (Akira) and government database compromises. This suggests a dual threat landscape; financially motivated ransomware alongside politically or criminally motivated leaks.
- Tunisia experienced an attack on the entertainment sector, which may indicate experimentation by threat actors in diversifying their targets.

East Africa

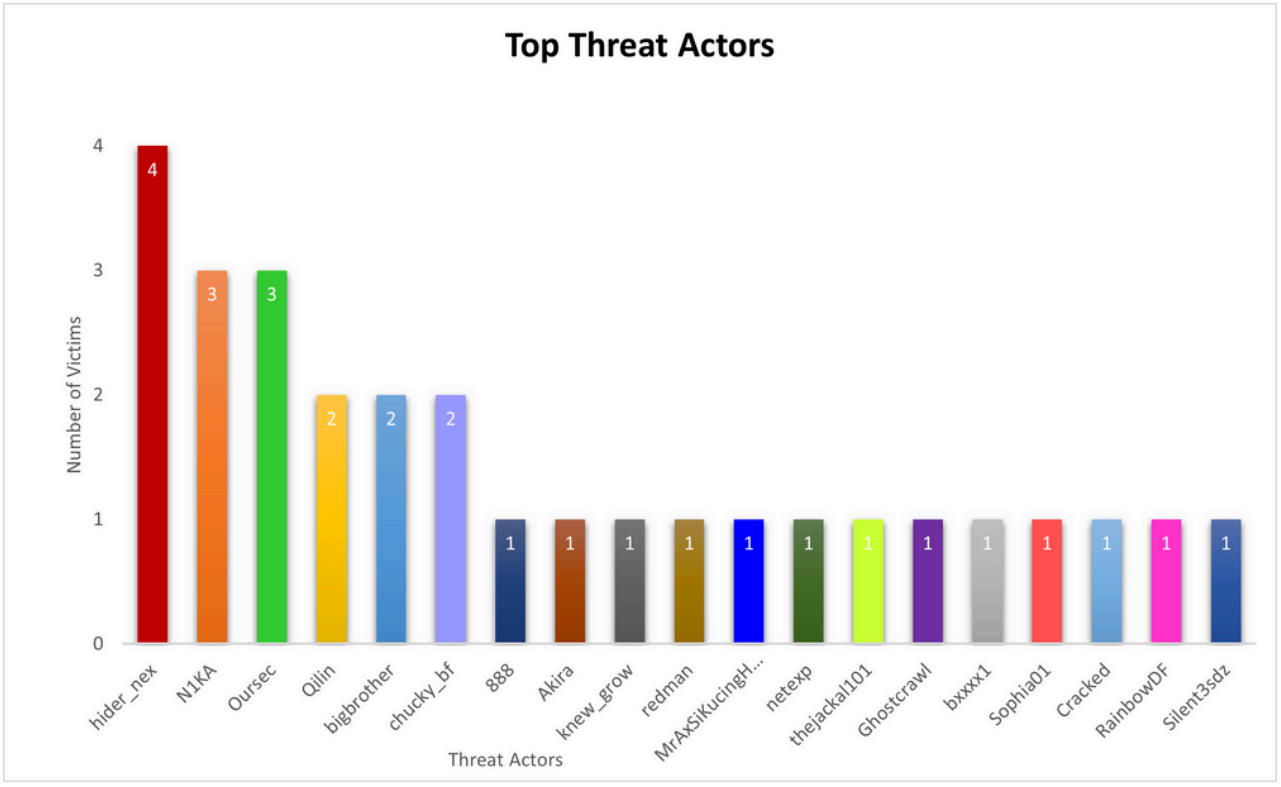
- Kenya and Uganda were specifically targeted by Qilin ransomware, both attacks aimed at the power sector. This is a worrying development, as energy infrastructure attacks carry high operational and national security risks.

Southern Africa

- South Africa saw incidents targeting e-commerce and general database systems. N1KA and Sophia01 were active in this region.
- Egypt recorded the highest number of incidents in the south, with DOS, ransomware, and database compromises across education, government, and technology.

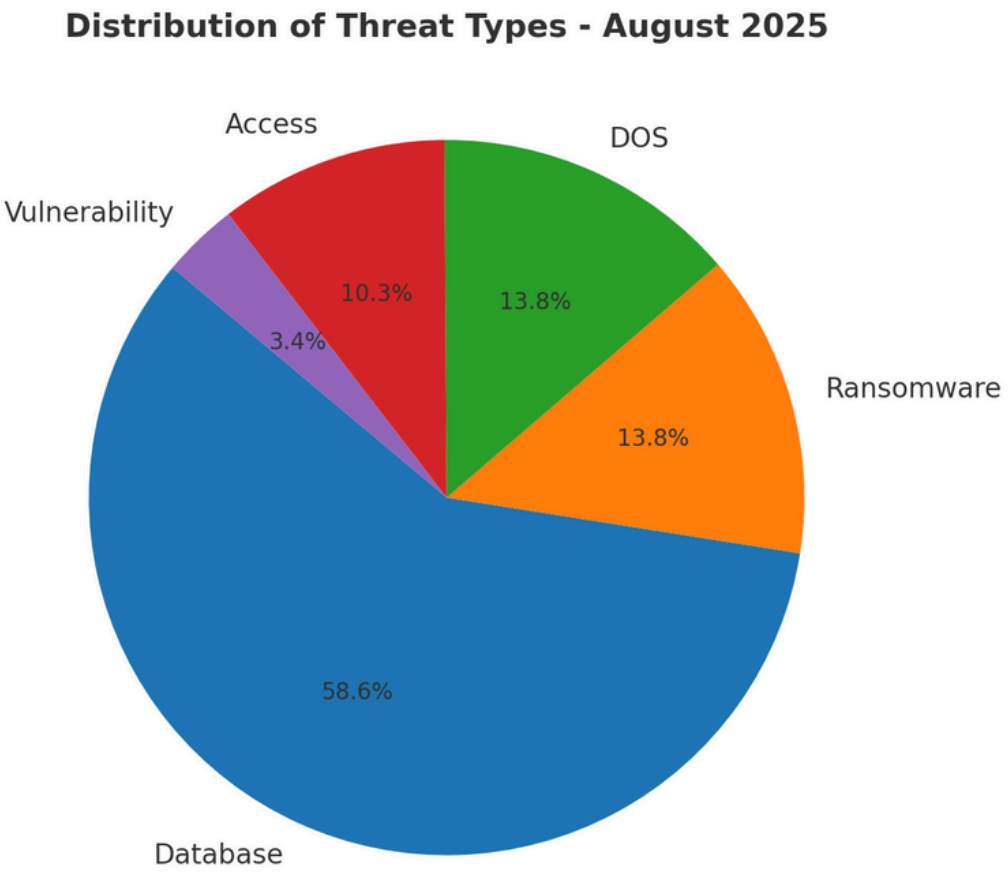


MOST ACTIVE THREAT ACTORS



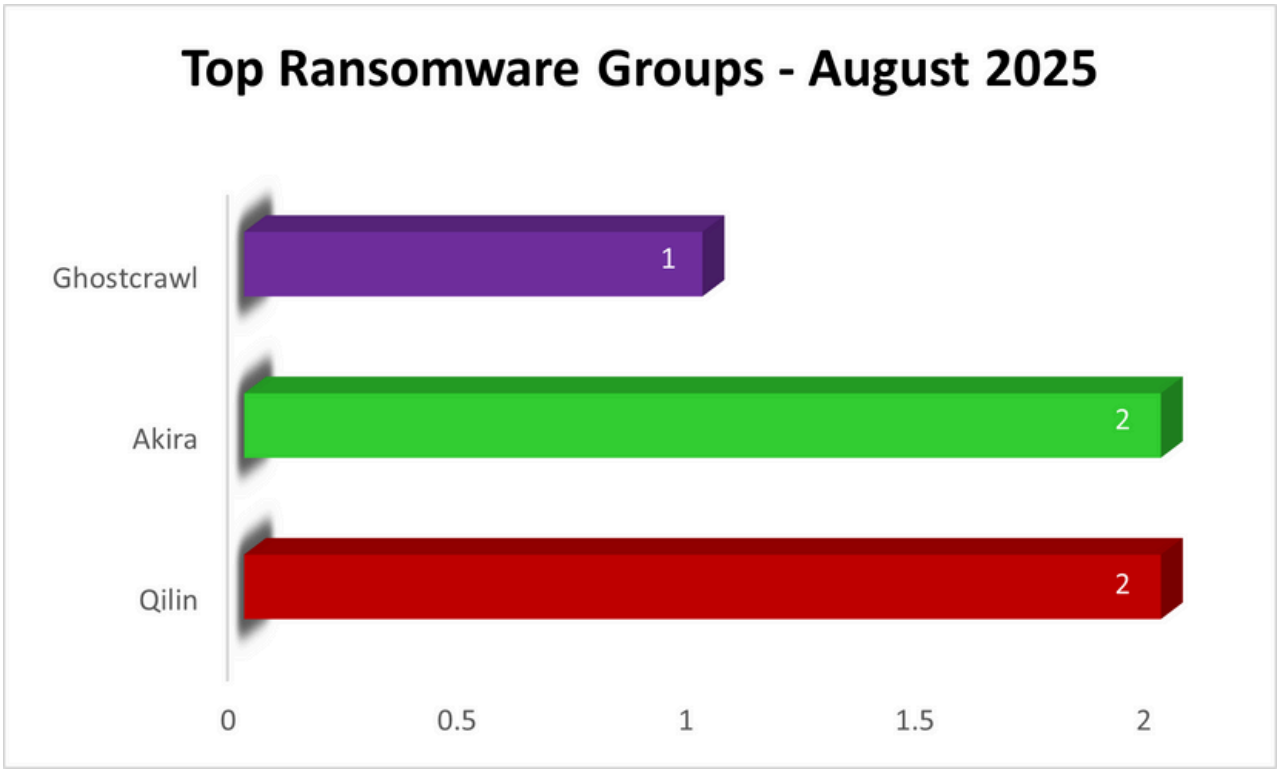
- **hider_nex**: Targeted four countries (Nigeria, Uganda, Egypt, Morocco). Responsible for vulnerabilities, DOS attacks, and database compromises, showing a wide operational capability.
- **N1KA**: Targeted both Nigeria and South Africa. Notably breached financial services and agriculture in Nigeria, expanding beyond generic leaks.
- **Oursec**: Concentrated in Morocco, launching DOS and database attacks toward the end of August, suggesting coordinated campaigns.
- **Qilin**: A prolific ransomware group targeted critical infrastructure (power) in Kenya and Uganda.
- **bigbrother**: Functioning as an access broker, compromised government systems in Togo and Egypt.

TOP THREATS



- **Database Compromises:** The most common threat (~60%) that affected education, government, financial services, and telecoms. Actors like N1KA, oursec, and chucky_bf drove widespread leaks, fueling fraud and dark web sales.
- **Ransomware Attacks:** High-severity cases by Qilin, Akira, and Ghostcrawl disrupted power (Kenya, Uganda), tech (Egypt), and other sectors. Qilin's focus on critical infrastructure is a major concern.
- **Denial-of-Service (DOS):** hider_nex and oursec launched attacks against Moroccan e-commerce and education, causing temporary outages.
- **Access Brokers:** bigbrother and thejackal101 sold government access in Egypt, Togo, and Nigeria, creating risks of future ransomware or espionage.
- **Vulnerability Exploitation:** hider_nex exploited weaknesses in Nigerian government systems, highlighting poor patch management.

TOP RANSOMWARE GROUPS



Qilin

- **Regions affected**: Kenya, Uganda
- **Industry focus**: Power (critical infrastructure)
- **Analysis**: Qilin launched two coordinated attacks on East Africa's energy sector, marking a dangerous escalation. By targeting power utilities, the group demonstrated a focus on high-value, high-impact victims where disruption could pressure governments and operators into ransom payments.

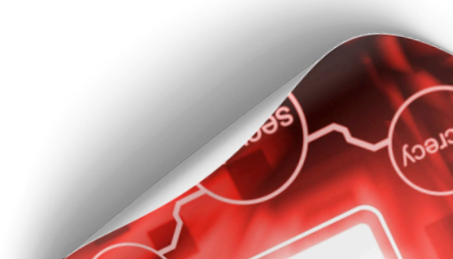
TOP RANSOMWARE GROUPS

Akira

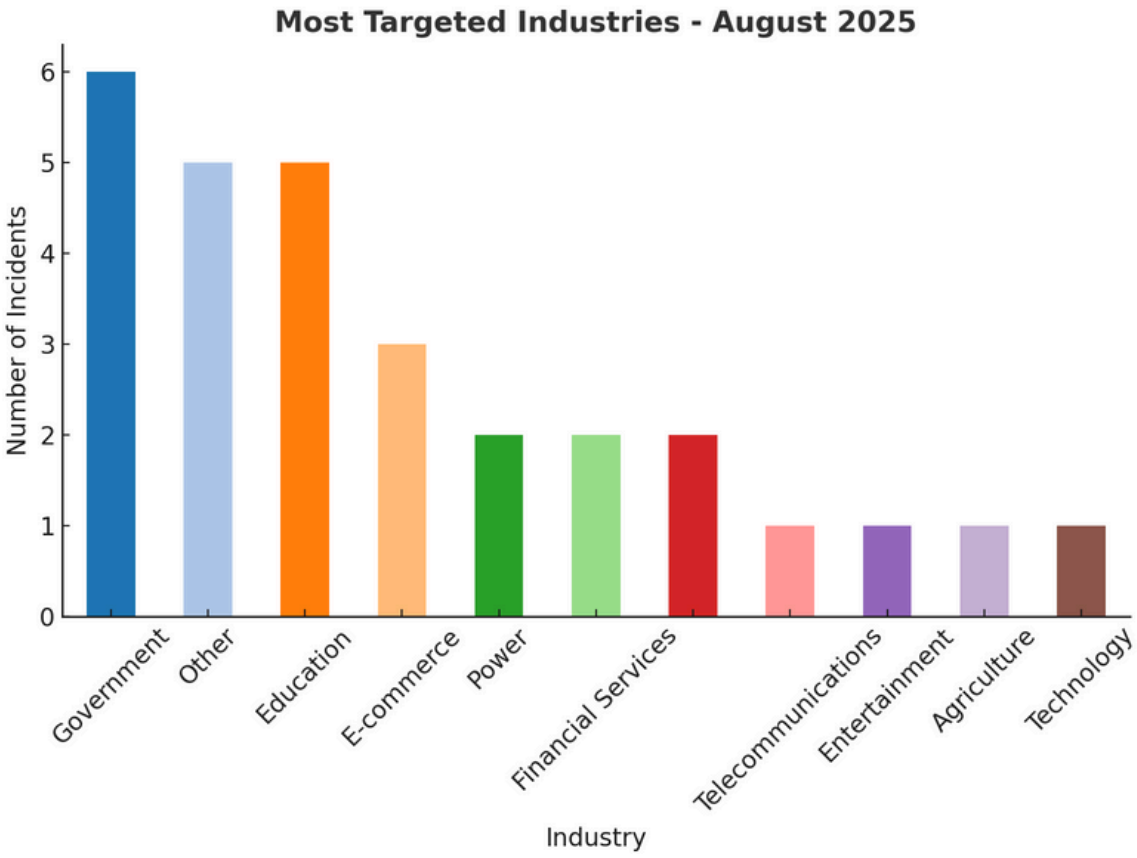
- **Region affected**: Algeria
- **Industry focus**: Miscellaneous/Other
- **Analysis**: Akira resurfaced in North Africa with a ransomware campaign in Algeria. While the incident was not in a critical sector, the group's global track record suggests Africa is now within its operational scope. This increases the likelihood of future campaigns across higher-value industries.

Ghostcrawl

- **Region affected**: Egypt
- **Industry focus**: Technology
- **Analysis**: Ghostcrawl attacked Egypt's technology sector, reflecting the trend of ransomware groups diversifying into industries handling intellectual property and digital infrastructure. Such targeting threatens both service providers and downstream clients.



MOST TARGETED INDUSTRIES



Government (6 incidents)

- The government sector was the most targeted, impacted by vulnerabilities, database leaks, DOS attacks, and access intrusions. This reflects the high value of state systems for espionage, disruption, and criminal resale markets.

Education (5 incidents)

- Education ranked second, showing repeated database compromises across Nigeria, Algeria, Egypt, and Morocco. Weak security funding and reliance on online systems continue to make this sector a soft target.

MOST TARGETED INDUSTRIES

Other / Miscellaneous (5 incidents)

- Actors like Cracked and Akira carried out attacks in undefined "Other" industries, which may include smaller businesses and organizations with less visibility but equally weak defenses.

E-commerce (3 incidents)

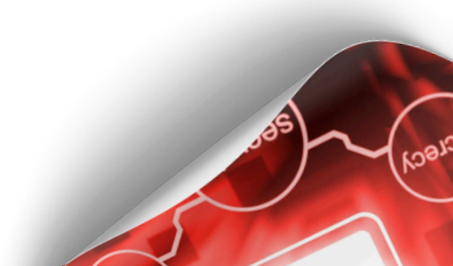
- Online platforms in South Africa and Morocco were hit with both database breaches and DOS campaigns, showing how threat actors are exploiting Africa's growing digital retail sector.

Power & Financial Services (2 incidents each)

- The power sector saw high-severity ransomware attacks by Qilin in Kenya and Uganda, raising national security concerns. Meanwhile, financial services in Nigeria were breached by N1KA and 888, exposing sensitive customer data.

Telecommunications, Technology, Agriculture, Entertainment (1 incident each)

- These industries saw lower attack volumes but still highlight the breadth of targeting across Africa. For example, telecoms in Morocco and tech in Egypt were both compromised, pointing to expanding threat actor interest.



CONCLUSION

The cyber threat landscape in Africa during August 2025 highlighted both persistent and evolving risks. Database compromises remained the most dominant threat, with widespread impact across education, government, and financial services. Meanwhile, ransomware actors such as Qilin, Akira, and Ghostcrawl extended their reach into critical infrastructure and technology sectors, raising the stakes for organizations across the continent.

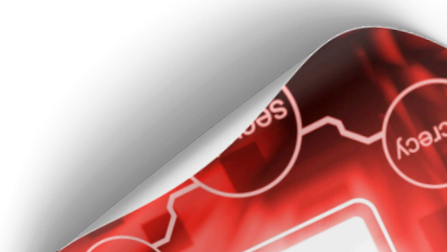
The targeting of government agencies and education institutions underscores the vulnerability of sectors with vast data repositories but limited security budgets. At the same time, Qilin's ransomware campaign against East Africa's power sector demonstrated that global threat actors now view Africa's critical infrastructure as a viable target, posing risks that go beyond data loss to affect national stability and public safety.

August also revealed the growing role of access brokers and denial-of-service campaigns, showing that Africa faces a full spectrum of threats, from disruptive operations to those that enable future ransomware attacks.

Overall, the findings reinforce the urgent need for:

- Stronger cybersecurity investments in education, government, and financial services.
- Cross-border intelligence sharing to track recurring actors like hider_nex, N1KA, and oursec.
- Critical infrastructure hardening against ransomware, particularly in the energy sector.

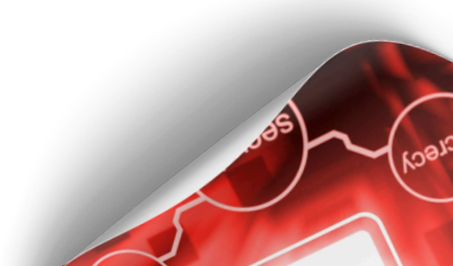
Africa's cyber threat environment is no longer peripheral, it is firmly integrated into the global threat landscape. Proactive defense, intelligence-driven strategies, and regional collaboration will be essential to protect organizations, governments, and citizens from the growing threats of cyber risks.



RECOMMENDATIONS

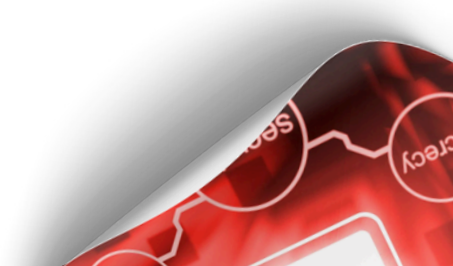
CyHawk Africa urges both organizations and individuals to adopt the following measures to strengthen their cybersecurity posture and resilience:

- Encrypt all sensitive data, both at rest and in transit.
- Regularly audit databases for misconfigurations and eliminate unnecessary public access.
- Apply strict access controls and ensure users only have permissions essential to their roles.
- Enforce multi-factor authentication (MFA) across all critical systems, with special attention to administrator accounts.
- Monitor login patterns for suspicious activity, like unusual locations or failed login bursts, and set up alerts.
- Adopt strong password policies and require regular password changes to reduce credential theft risks.
- Maintain a rigorous patching cycle, especially for public-facing applications and legacy systems that attackers frequently exploit.
- Use security tools to scan regularly for vulnerabilities and address them without delay.
- Deploy detection systems that can spot abnormal behaviors such as unexpected large data transfers or odd working-hour logins.
- Develop and routinely test incident response plans so teams know exactly how to react when breaches occur.
- Conduct regular cybersecurity training so employees can recognize phishing and social engineering attempts, since many attacks start this way.



RECOMMENDATIONS

- Extend security awareness efforts to contractors and third parties who may have access to your systems.
- Keep secure, offline backups of critical data and test restoration processes to prepare for ransomware scenarios.
- Have a communication and legal plan ready in case of ransomware or extortion demands.
- Given the cross-border nature of threats, especially highlighted by activity in North Africa, build cooperative relationships with neighboring countries to share intelligence and coordinate defenses.
- Participate in regional or sector-specific threat intelligence networks to gain early insights into campaigns that could affect your organization.



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 defacement 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