Report of the Cyber Threat Landscape in Africa

September 2025

www.cyhawk-africa.com

Executive Summary

September 2025 recorded 179 reported cyber incidents across Africa, marking a sharp rise in activity. The month was overwhelmingly dominated by Keymous Plus, which was responsible for 113 incidents (63.5% of the total). Their campaigns primarily involved distributed denial-of-service (DDoS) attacks (95 incidents), alongside 16 database breaches and 1 unauthorized access intrusion, reflecting a diverse yet disruptive threat profile.

The most impacted country was Morocco, which accounted for 145 incidents (81% of all cases), highlighting its heightened exposure to coordinated campaigns against government and public-sector infrastructure. Other affected nations included Nigeria, Algeria, Egypt, Tunisia, Kenya, South Africa, and Mali, though at significantly lower volumes. The Government sector was the most targeted industry, with 59 confirmed incidents, underscoring adversaries' strategic focus on critical state assets and public-facing systems.

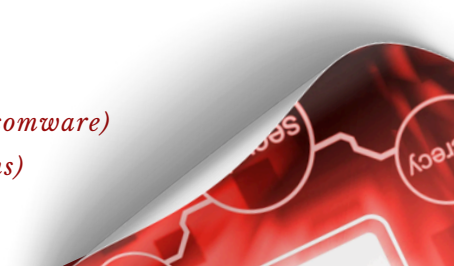
A notable trend in September was the concentration of attacks under a single actor, with Keymous Plus displacing the multi-actor threat activity observed in previous months. This shift signals a centralized threat landscape, where one group is capable of shaping the continent's exposure at scale.

In addition to hacktivist-led campaigns, September also witnessed the reemergence of a global cybercrime group, Shinyhunters, that carried out a large-scale data breach against an African financial organization, resulting in the exfiltration of a substantial volume of sensitive corporate data.

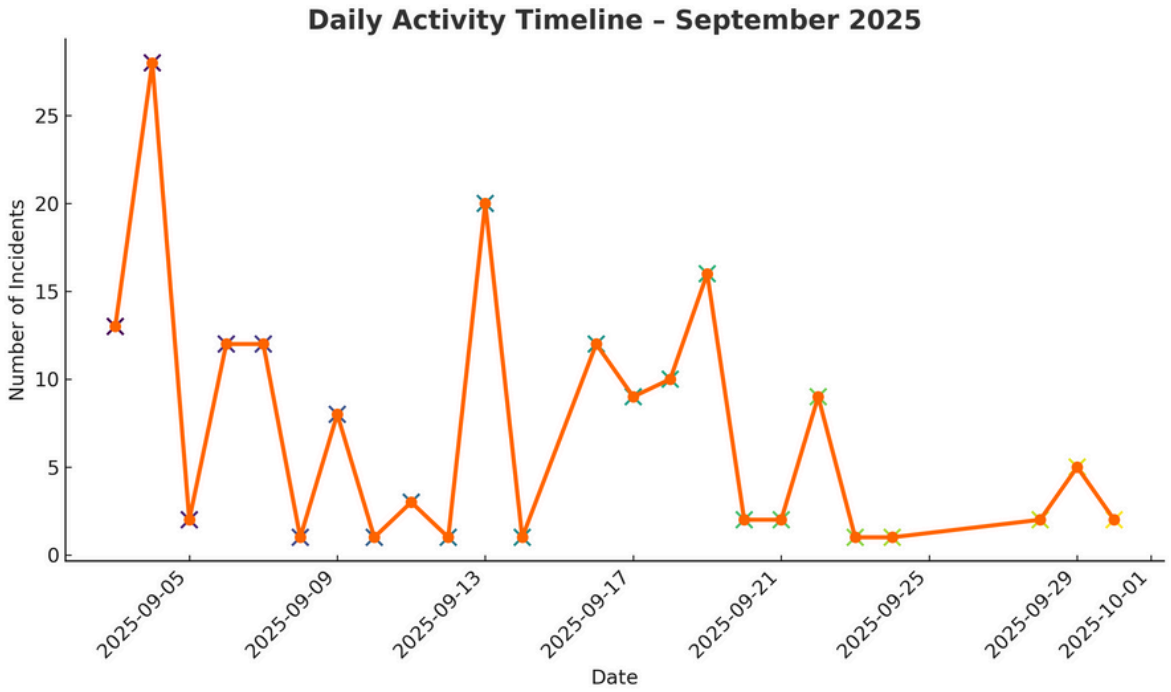
The month also showed high disclosure patterns, with a peak on September 4th, when 28 victims were published in a single day.

The analysis is based on a dataset of 179 cybersecurity incidents recorded between 1 September and 30 September 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)*



DAILY ACTIVITY TIMELINE

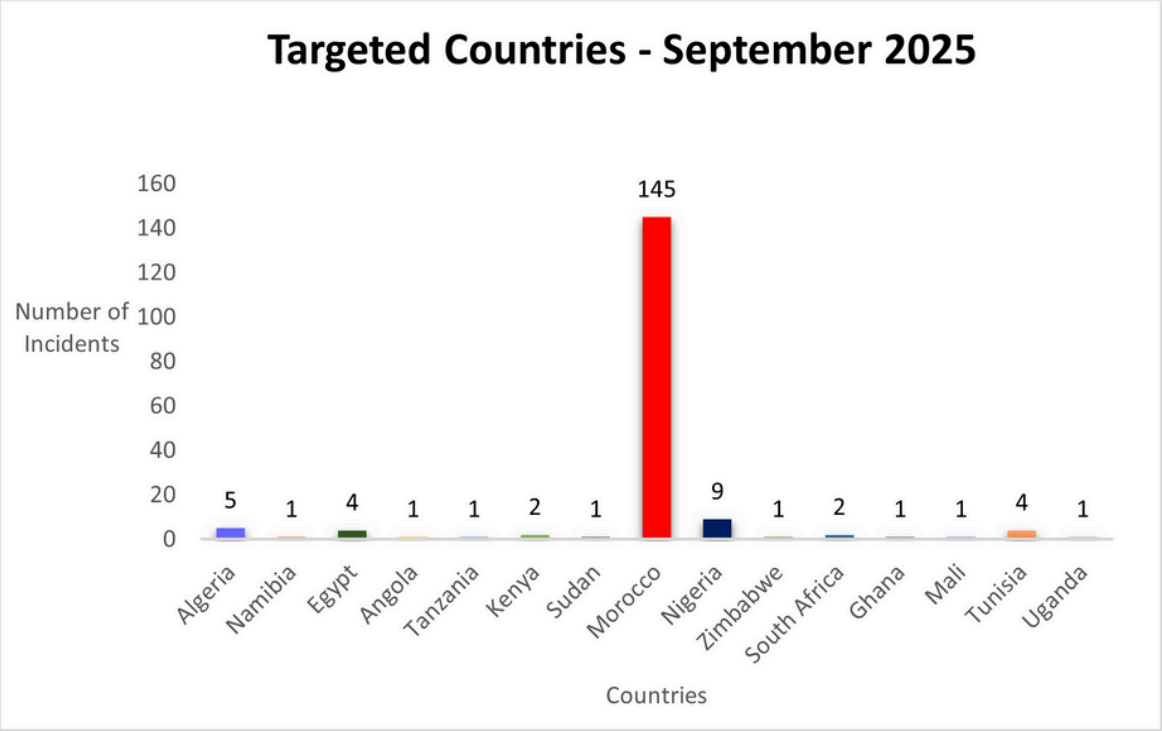


September 2025 recorded frequent bursts of cyber activity, with major spikes between September 3rd and 19th driven by Keymous Plus. The group's campaign against Moroccan government infrastructure dominated the timeline, peaking on September 3rd, 4th, 13th, and 19th, where dozens of victims were targeted in coordinated attacks.

The early-month surge (Sept 3–7) marked the start of Keymous Plus' retaliatory operations targeting Morocco, while mid-month activity (Sept 13–19) saw overlapping campaigns involving OurSec, Privilege, and Fire Wire. Privilege notably targeted Nigeria's financial sector and Angola's government, adding a multi-regional dimension to the month's incidents.

By late September, activity slowed, with attacks by BigBrother, KaruHunters, and r3i, signaling the wind-down of large-scale campaigns. Overall, the timeline reflects a high-intensity, actor-concentrated month dominated by hacktivist and financially motivated operations across North Africa.

TARGETED COUNTRIES



This data shows an overwhelming concentration of cyber incidents in Morocco, which recorded 145 attacks out of 179 across Africa. This figure dwarfs activity in other countries such as Nigeria (9), Algeria (5), Egypt (4), Tunisia (4), South Africa (2), Mali (1), Ghana (1), and Uganda (1).

The disproportionate targeting of Morocco is attributed to the hacktivist group Keymous Plus, which launched a sustained campaign as part of a retaliatory response against Algerian infrastructure operations. This reflects the spillover of geopolitical tensions into cyberspace, where hacktivist groups exploit national rivalries to conduct high-volume denial-of-service, website defacement, and database breach attacks.

AFRICAN THREAT LANDSCAPE

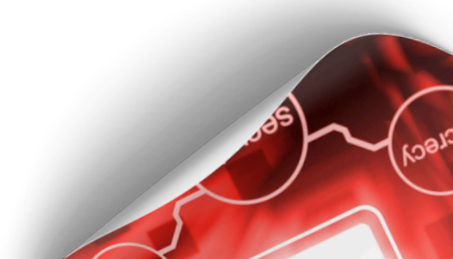
The African cyber threat landscape in September 2025 reflected a complex interplay between hacktivism, financially motivated crime, and geopolitical cyber tensions. While global threat actors maintained selective interest in high-value African targets, the majority of incidents observed during the month originated from regional and locally coordinated campaigns, underscoring the continent's evolving internal threat ecosystem.

Hacktivism and Geopolitical Tension

The North African region remained the epicenter of activity, driven primarily by the retaliatory campaigns of Keymous Plus against Moroccan infrastructures. This campaign, initially triggered by alleged Algerian cyber actions, evolved into a sustained DDoS and data breach operation targeting Moroccan government systems, public services, and digital infrastructure. The attacks highlight how political and territorial disputes are increasingly spilling into cyberspace, transforming digital operations into instruments of state influence and protest.

Financially Motivated Operations

Beyond hacktivism, financially motivated threat actors continued to exploit weaknesses in data protection and access controls. Groups such as Privilege and Fire Wire launched targeted attacks on financial institutions in Nigeria and other key economic centers, seeking to exfiltrate sensitive databases and credentials for resale or extortion. This shift reflects a maturing cybercriminal economy within the region, where smaller actors leverage exposed assets and weak authentication practices to generate illicit profit.



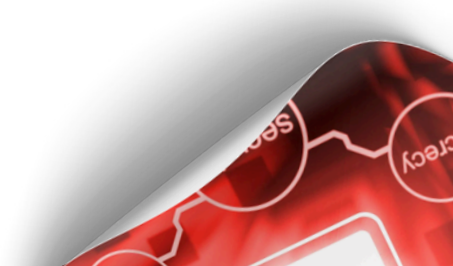
AFRICAN THREAT LANDSCAPE CONT'D

A significant development during the month was the reemergence of a global Advanced Persistent Group, Shinyhunters, which conducted a major data exfiltration operation targeting an African financial organization. The incident highlights a growing trend of international actors expanding their operations into Africa's financial sector, reflecting the continent's increasing integration into the global data exploitation economy.

This progression signals a maturing cybercriminal ecosystem, where both regional and global groups now view Africa not merely as a target of opportunity but as a strategically valuable environment for data monetization, intelligence gathering, and influence operations.

Expanding Attack Surface

As Africa's digital transformation accelerates, the attack surface has broadened significantly, encompassing education, telecommunications, technology, and healthcare sectors. Many of these industries lack adequate defensive maturity or incident response planning, making them ideal targets for opportunistic and low-complexity attacks. The growing adoption of cloud services and remote access tools has further introduced vulnerabilities that adversaries continue to exploit for persistence and lateral movement.



NORTH AFRICA THREAT LANDSCAPE

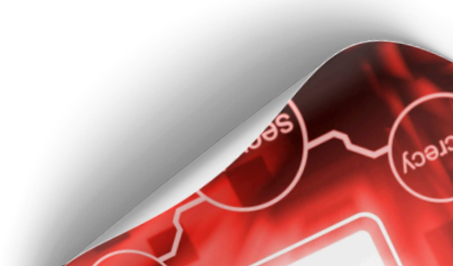
The North African region continues to emerge as a critical hotspot for cyber conflict, driven by longstanding political and territorial disputes. Hacktivist groups, rather than financially motivated ransomware operators, are increasingly shaping the regional threat picture. September's surge in attacks against Morocco highlights several trends.

Geopolitical Retaliation: Keymous Plus framed its operations as a direct response to Algeria, weaponizing cyber tools as a means of political signaling.

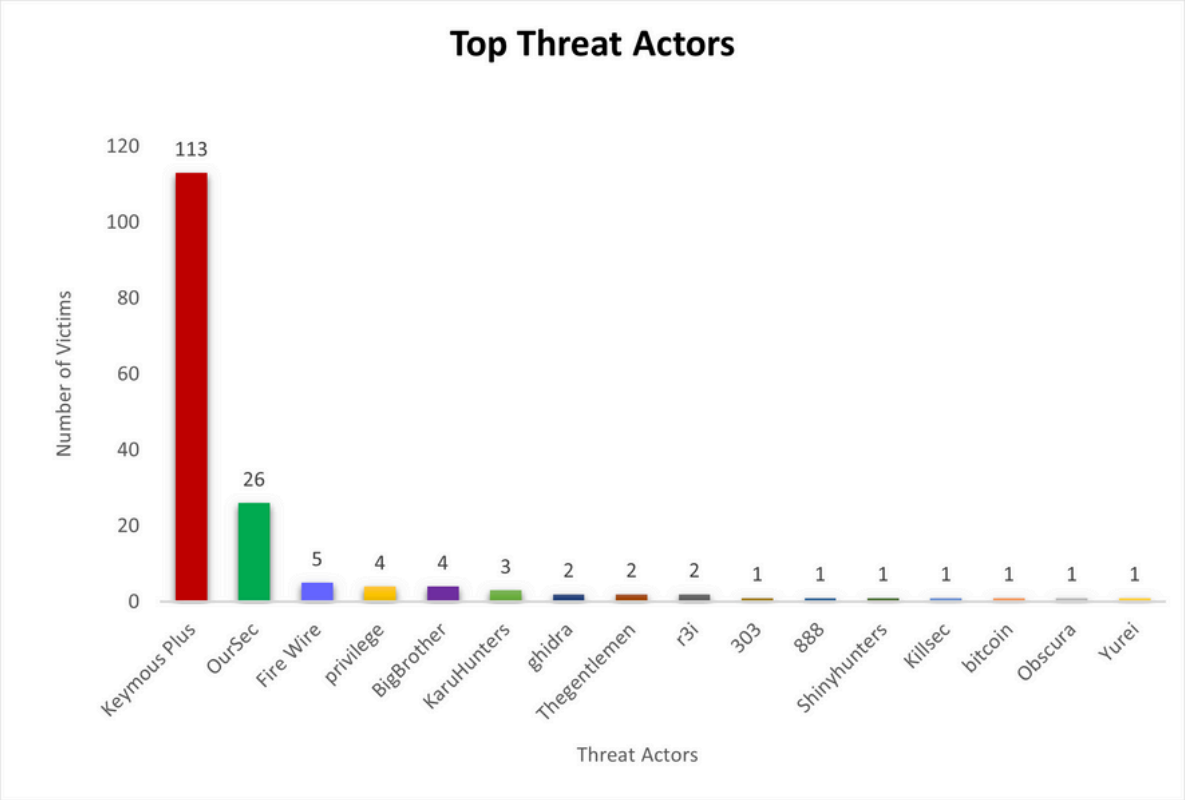
Government and State Infrastructure Focus: The majority of incidents in Morocco targeted government-linked assets, consistent with hacktivist goals of undermining state authority and disrupting public trust.

Regional Escalation Risk: With Algeria already impacted (5 incidents), and Tunisia and Egypt also recording cases, the threat landscape in North Africa is interconnected. Campaigns initiated in one country are increasingly spilling into neighboring countries.

Hacktivism as a Strategic Tool: Unlike ransomware-driven extortion seen in Sub-Saharan Africa, North Africa's threat ecosystem is tilting toward hacktivism and politically motivated cyber operations, creating volatility that aligns with regional disputes rather than global criminal markets.



MOST ACTIVE THREAT ACTORS



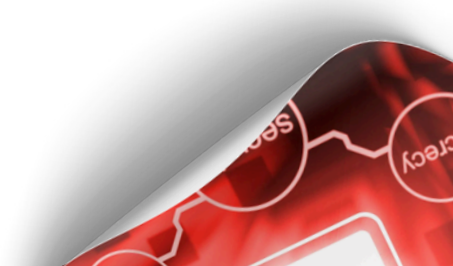
The threat actor landscape was overwhelmingly shaped by Keymous Plus, which accounted for 113 incidents (63.5% of all activity). Their operations included large-scale DDoS campaigns, database breaches, and access breach, primarily targeting Moroccan government infrastructure. This dominance highlights how a single hacktivist group can significantly alter the regional threat landscape.

The second most active group was OurSec, linked to 26 incidents, continuing their persistent campaigns in Morocco. Though significantly smaller in scale compared to Keymous Plus, OurSec's steady operations highlight their role as one of the continent's consistent hacktivist groups.

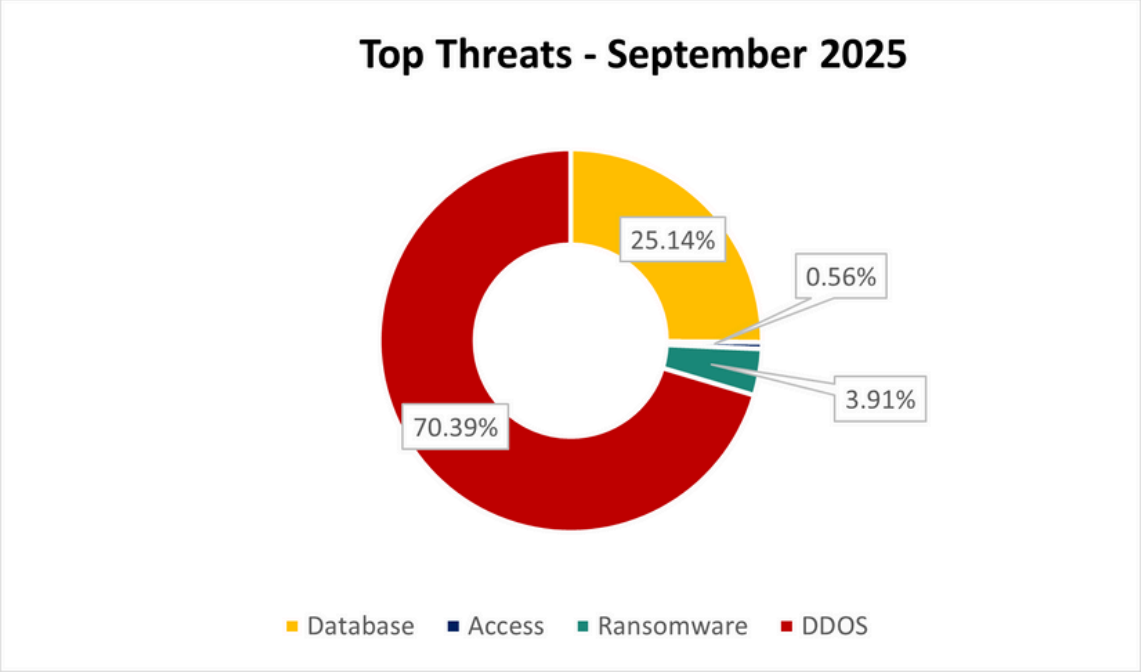
MOST ACTIVE THREAT ACTORS

A particularly notable actor this month was Privilege, responsible for 4 incidents. Within a short period, Privilege targeted financial services in Nigeria, launching disruptive database attacks, and extended its activity to the government sector in Angola.

Other groups, such as Fire Wire (5 incidents) and BigBrother (4 incidents) also registered activity, while smaller actors like KaruHunters, Ghidra, Thegentlemen, and r3i recorded 2–3 incidents each. Single-case actors (303, 888, Bitcoin, Obscura, Shinyhunters) contributed to the long tail of September's threat ecosystem.



TOP THREATS

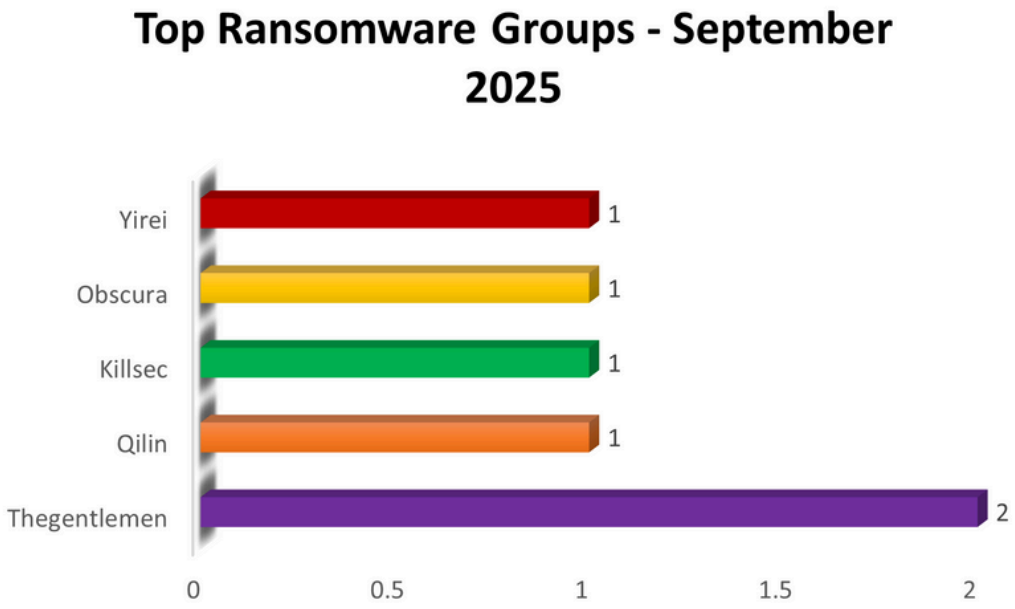


The overall threat distribution for September 2025 was heavily skewed towards Distributed Denial-of-Service (DDoS) attacks, which accounted for 70.39% of all recorded incidents. This dominance was primarily driven by Keymous Plus, whose large-scale DDoS campaigns against the Moroccan government and public service infrastructure shaped the continent's threat profile for the month.

Database breaches followed at 25.14%, underscoring continued exploitation of misconfigured and unprotected data assets, particularly in financial services, education, and technology sectors. These breaches were frequently tied to actors like Privilege and Fire Wire, Shinyhunters who focused on leaking exposed records for monetary and/or reputational gain.

Access intrusions made up 0.56% of incidents, indicating limited but concerning attempts to gain unauthorized entry into sensitive systems. Meanwhile, ransomware activity constituted 3.91%, led by groups such as Thegentlemen and Qilin, which focused on opportunistic targeting rather than large-scale campaigns.

TOP RANSOMWARE GROUPS



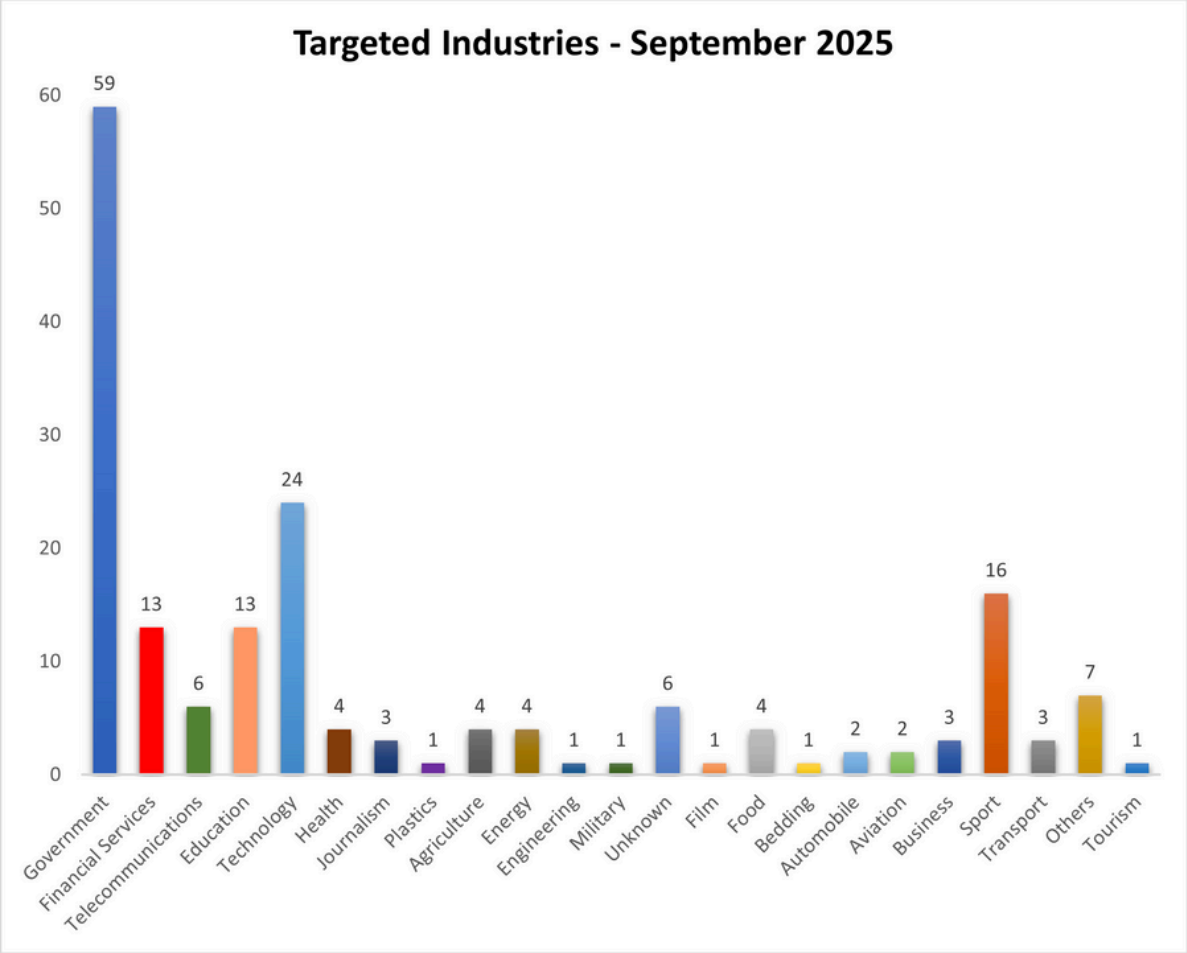
Ransomware activity across Africa in September 2025 remained moderate but diverse, with six distinct ransomware groups observed. The landscape was led by Thegentlemen, which recorded two confirmed victims, while Radar, Yirei, Obscura, Killsec, and Qilin each recorded one incident.

Although the overall number of ransomware cases was lower than the hacktivist-driven campaigns that dominated the month, the diversity of groups indicates continued interest in African targets by multiple ransomware operations, both emerging and established.

Thegentlemen showed the most notable presence, expanding its operations into African-based organizations following previous activity in Europe and South America. Their attacks were characterized by targeted data encryption and subsequent publication threats on leak sites, indicating a hybrid extortion model that blends both data theft and service disruption.

Qilin maintained a steady footprint with a single case observed in September, continuing its known pattern of opportunistic targeting across multiple regions. Meanwhile, lesser-known groups such as Radar, Yirei, Obscura, and Killsec each made isolated appearances, likely testing or re-emerging in the regional landscape.

MOST TARGETED INDUSTRIES



The government sector emerged as the most targeted, recording 59 incidents. This consistent trend highlights how state institutions remain prime targets for both hacktivist and other threat groups, particularly in campaigns seeking to disrupt national operations or expose sensitive administrative data.

The technology sector followed with 24 incidents, reflecting attackers' growing focus on digital service providers, hosting companies, and critical software platforms. This aligns with broader campaigns observed across the continent targeting IT infrastructure as an access point into downstream clients.

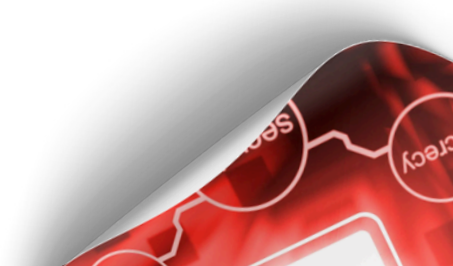
MOST TARGETED INDUSTRIES

The Education sector recorded 13 incidents, indicating continued exploitation of undersecured learning platforms and academic networks, often leveraged for credential harvesting or data exposure. Similarly, Financial Services (13 incidents) and Telecommunications (6 incidents) retained their positions among the most targeted industries, underscoring adversaries' sustained interest in monetizable data and communication networks.

Meanwhile, sectors such as Transport (16 incidents), Health (4 incidents), and Tourism (1 incident) recorded lower but significant activity, showing that attackers continue to probe organizations broadly for opportunistic gains.

Assessment

- **Government Exposure**: The high volume of incidents in the public sector stems largely from hacktivist-led campaigns, particularly by Keymous Plus, which focused on Moroccan government infrastructure throughout the month.
- **Technology as a Gateway**: Threat actors are increasingly exploiting technology service providers to pivot into client environments, signaling the need for stronger supply-chain monitoring.
- **Sectoral Consistency**: Compared to August, targeting patterns remained largely stable, but the intensity of government-focused attacks increased, reflecting the spillover of geopolitical cyber conflicts in North Africa.
- **Expanding Scope**: The inclusion of industries such as transport and business services demonstrates a widening operational scope, indicating that adversaries are pursuing both symbolic and financially motivated objectives.



CONCLUSION

September 2025 saw a significant rise in Africa's cyber threat landscape, driven by hacktivist-led operations and retaliatory campaigns across North Africa. The overwhelming dominance of Keymous Plus, responsible for more than 60% of recorded incidents, reflects a shift from financially motivated attacks to politically charged cyber conflicts that leverage DDoS and database breaches as tools of disruption.

The persistent targeting of government, technology, and financial sectors demonstrates adversaries' intent to undermine public trust, disrupt essential services, and expose critical data. Meanwhile, emerging groups such as Privilege, which attacked financial institutions in Nigeria and government entities in Angola, illustrate how cyber threats are becoming increasingly regional and multi-dimensional.

A notable development during the month was the large-scale data breach of an African investment organization, attributed to a global cybercrime group. This incident signifies a strategic expansion of international threat actors into Africa's financial and development ecosystems, marking a shift from regional hacktivism to global data exploitation. The breach highlights the growing economic and intelligence value of African corporate data, especially within sectors that manage investments, impact funding, and Environmental, Social and Governance (ESG) portfolios.

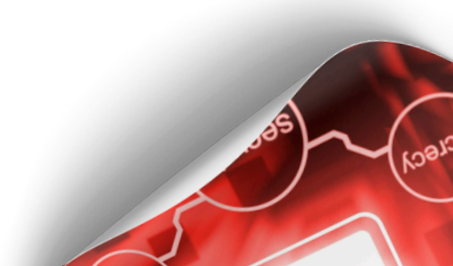
Moving forward, Africa's cybersecurity trajectory will depend on its ability to foster cross-border collaboration, enhance data protection standards, and strengthen national CERT coordination. Without unified regional defense strategies and continuous sharing of threat intelligence, the continent risks deeper exposure to both external and locally initiated cyber campaigns.

Africa's cyber threats are no longer sporadic incidents but sustained, campaign-driven operations that mirror global threat patterns. The continent's digital future will therefore hinge on the readiness of its governments and institutions to anticipate, detect, and disrupt these evolving adversaries.

RECOMMENDATIONS

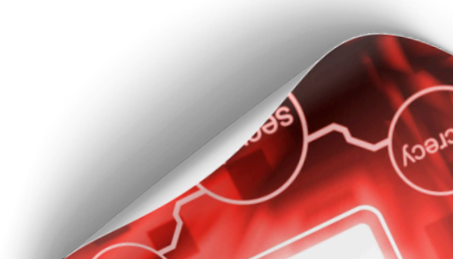
CyHawk Africa urges both organizations and individuals to adopt the following measures to strengthen their cybersecurity posture and resilience:

- 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