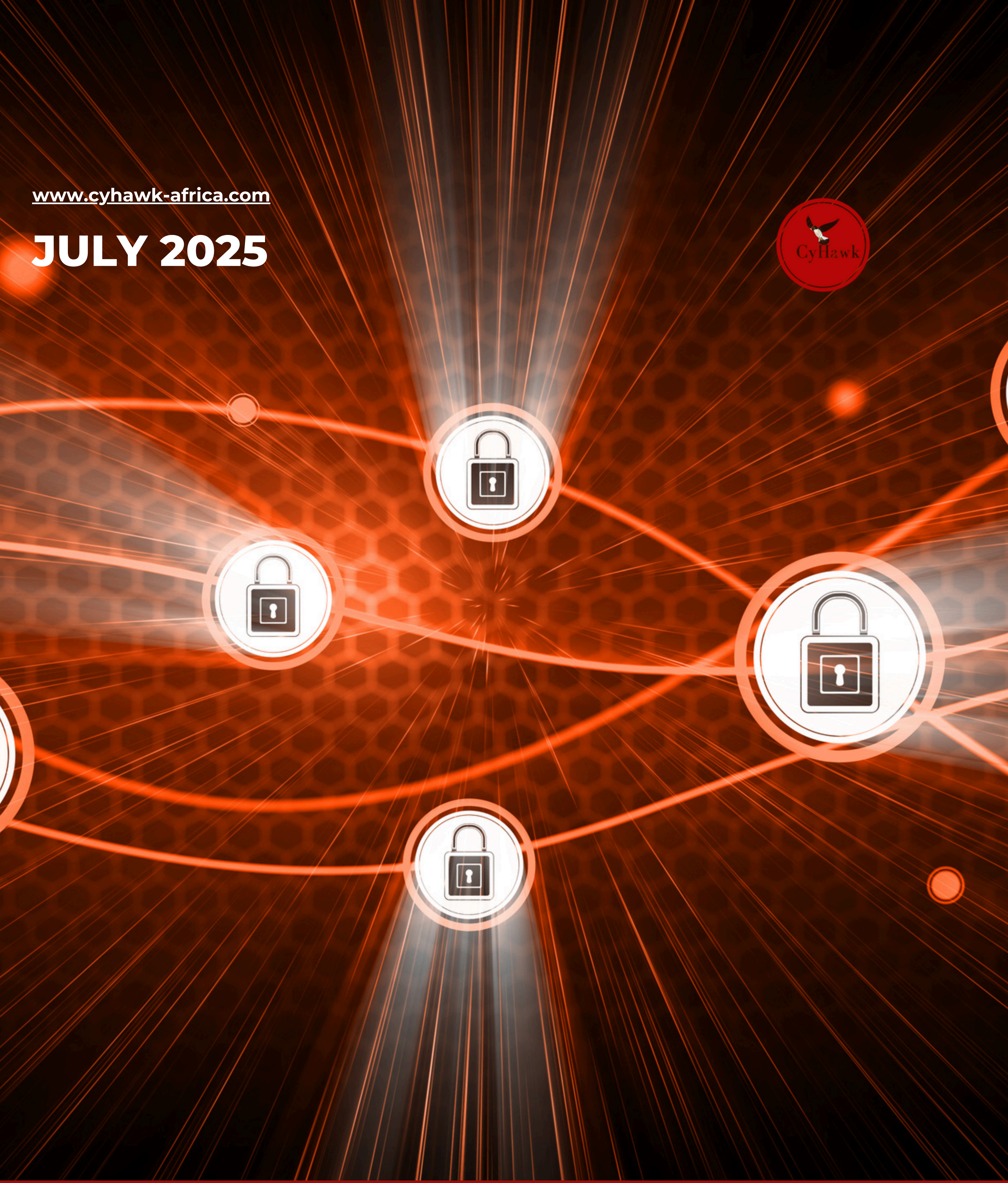
www.cyhawk-africa.com

JULY 2025



REPORT OF THE CYBER THREAT LANDSCAPE IN AFRICA

By

Hassanat Oladeji

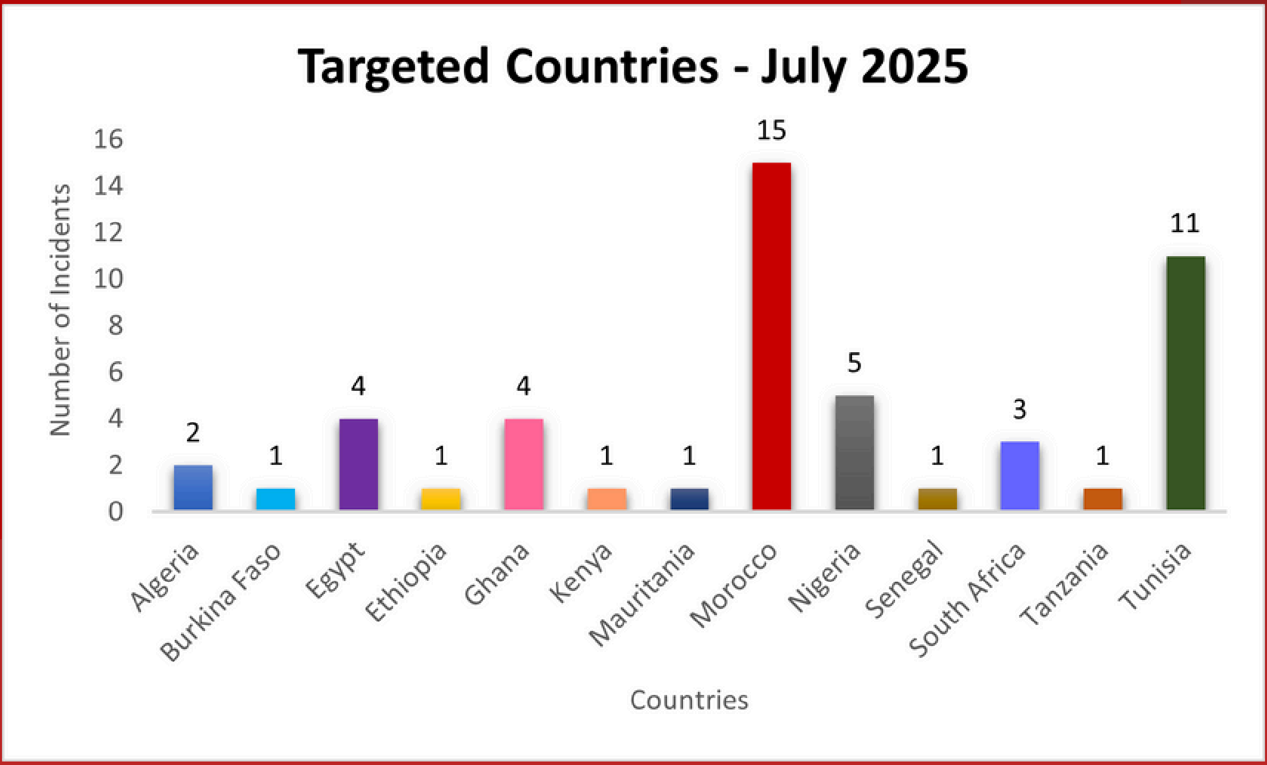
Executive Summary

July 2025 witnessed a notable surge in cyber threat activities across the African continent, particularly the Northern Africa. CyHawk Africa recorded 50 distinct cyber incidents that spanned 13 countries and with 25 unique threat actors. The overwhelming majority of attacks focused on unauthorized database access and data breaches. Financial institutions, government agencies, telecommunications, providers, education and healthcare sectors continued to be primary targets. This month's data further emphasizes the growing professionalism and operational tempo of both known and emerging threat actor groups.

The analysis is based on a dataset of 50 cybersecurity incidents recorded between 1 July and 30 July 2025. The dataset includes the following fields:

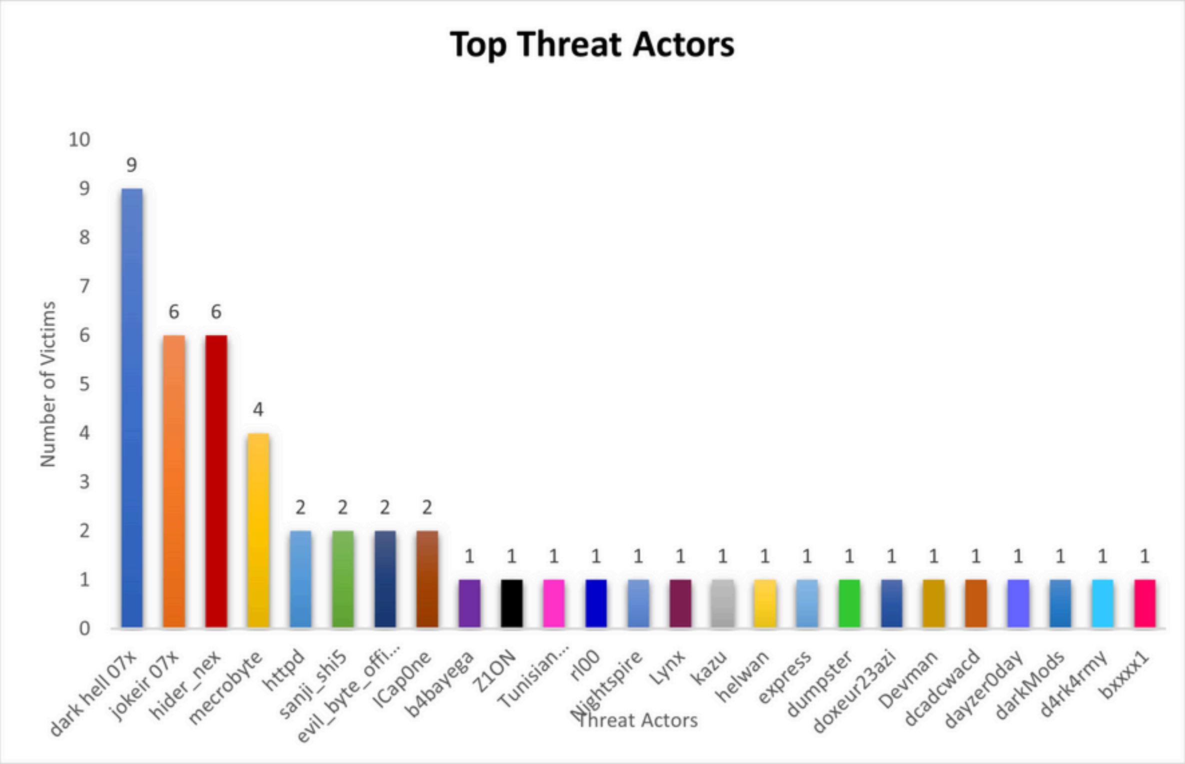
- *S/No: Incident identifier*
- *Date: Date of the incident*
- *Threat Actor: Group or individual responsible*
- *Country: Targeted country*
- *Threat Type: Nature of the attack (e.g., database breach, defacement, ransomware)*
- *Industry: Sector targeted (e.g., government, education, telecommunications)*

TARGETED COUNTRIES IN AFRICA



Morocco recorded the highest incident count in July with 15 incidents, primarily targeting government, financial, and telecommunications sectors. Tunisia followed with 11 incidents, impacting government, technology, and education institutions. Nigeria ranked third with 5 incidents, aimed at financial services and telecommunications. Egypt and Ghana each recorded 4 incidents, while South Africa saw 3 incidents. Other countries affected included Algeria (2), Burkina Faso (1), Ethiopia (1), Kenya (1), Mauritania (1), Senegal (1), and Tanzania (1). The spread highlights a broad geographic distribution of threat activity across North, West, East, and Southern Africa.

MOST ACTIVE THREAT ACTORS



dark hell 07x, the most prolific group, was responsible for 9 incidents, primarily targeting West African financial institutions and public-sector organizations.

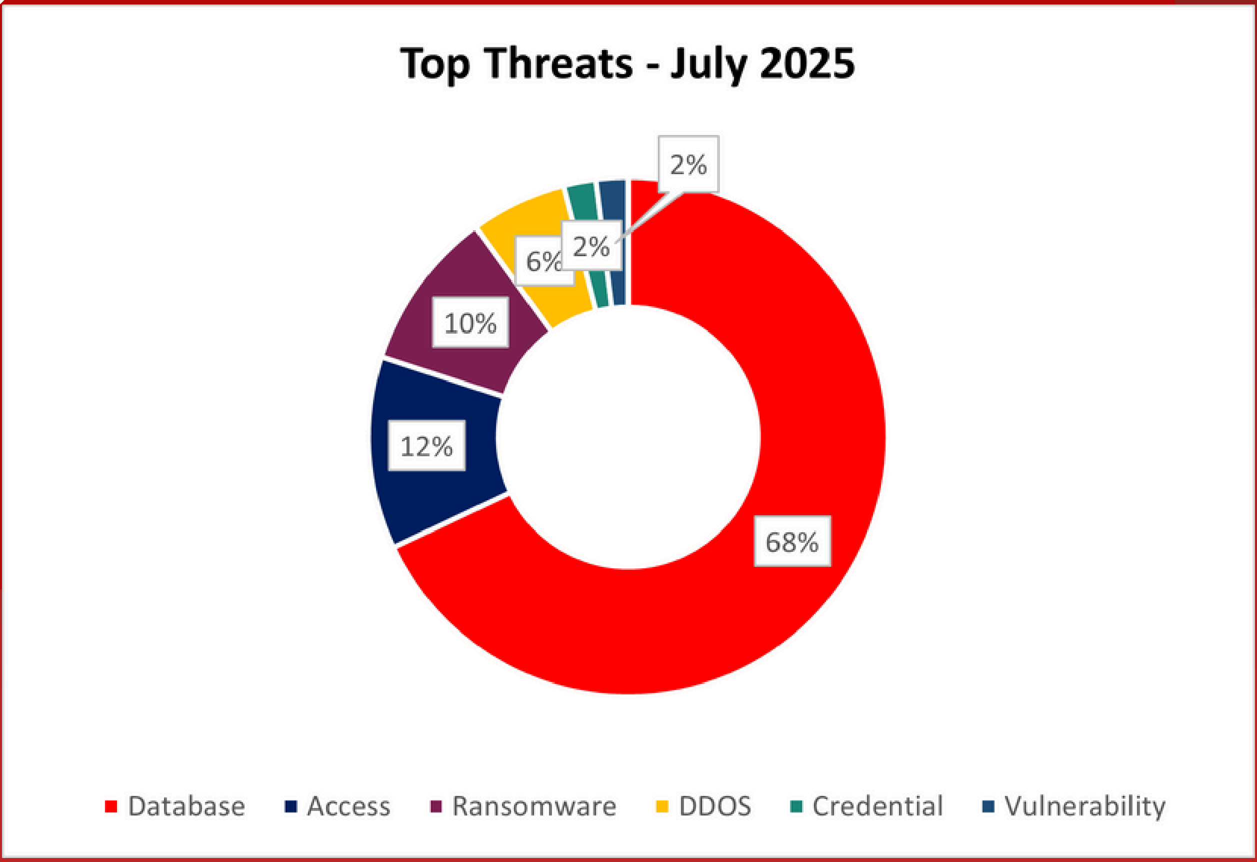
Hider_nex, with 6 incidents, targeted educational and healthcare institutions in North Africa, often compromising internal networks to steal research data and patient records for resale or strategic use.

Jokeir 07x and server_dump maintained a steady presence, employing a mix of access intrusions and data theft aimed at telecommunications, technology, and government entities. Their activity patterns suggest both opportunistic targeting and long-term infiltration strategies.

Mecrobyte was observed in multiple incidents across Tunisia, focusing on both government and technology sectors, potentially as part of coordinated regional espionage or politically motivated campaigns.

These top actors' motives ranged from financially driven campaigns to politically influenced cyber-espionage, while sharing common tactics such as credential harvesting, SQL injection, and exploitation of unpatched vulnerabilities.

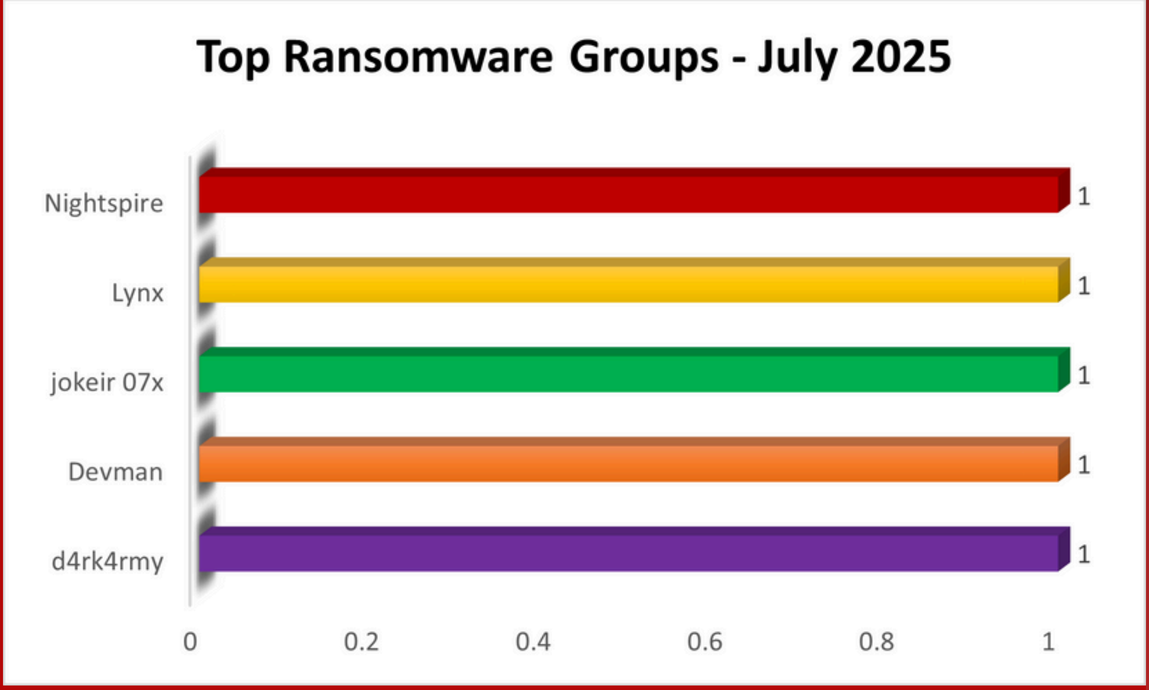
TOP THREATS



Database breaches accounted for approximately 68% of the total incidents, underscoring the high market value of sensitive datasets, such as personal identifiable information (PII), government records, and financial data. Access attacks comprised 12% of activity, often leveraging stolen credentials or exploiting insecure endpoints.

While ransomware, vulnerability, and doxing incidents were less frequent, they still posed significant operational and reputational risks.

TOP RANSOMWARE GROUPS



- d4rk4rmy (South Africa): This group targeted the mining sector in South Africa. Theirr ransomware campaign focused on operational disruption and data encryption, with ransom demands designed to halt extraction activities until payment was received. The attack underscores the rising trend of targeting resource-based economies for high-value extortion.

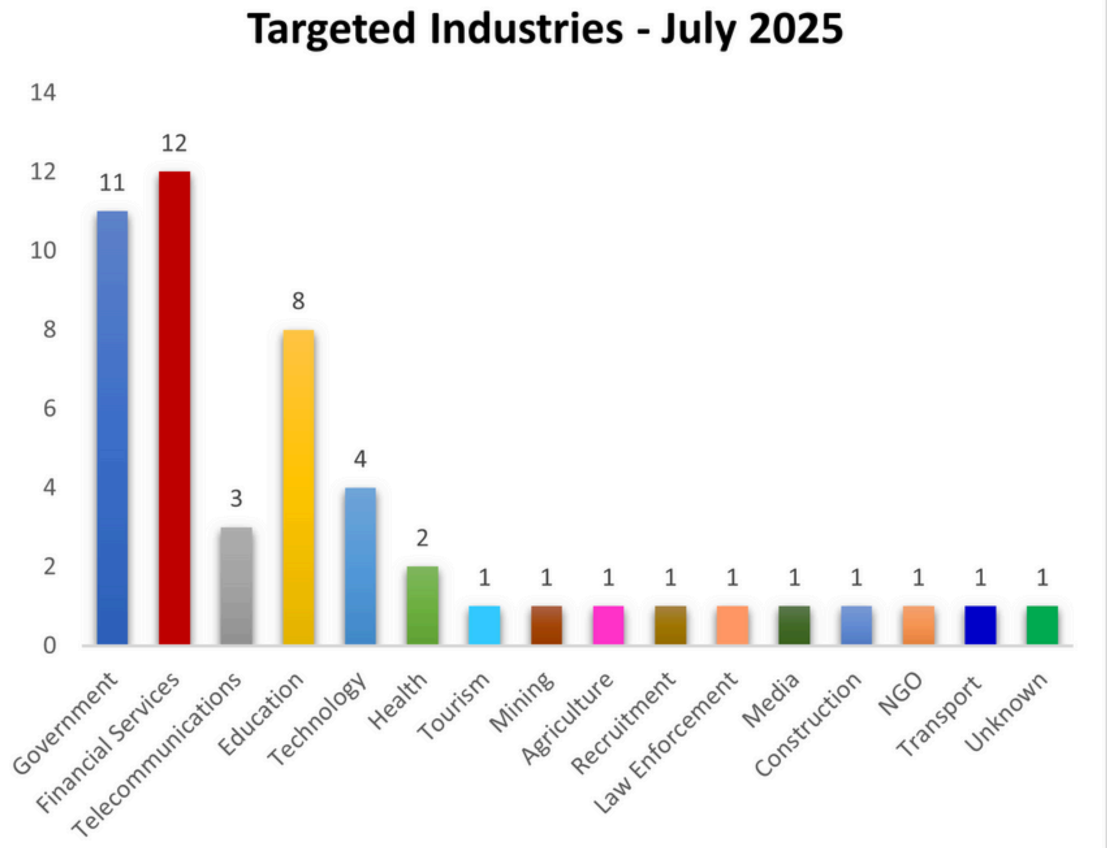
- Devman (Egypt): Devman's ransomware was deployed against an Egyptian public sector system, likely aiming to disrupt service delivery or compromise sensitive internal records.

- Nightspire (Tanzania): Focused on an NGO in Tanzania, this group leveraged ransomware to extract data and cripple administrative functions. Their targeting of a non-profit organization is particularly concerning, as it impacts humanitarian and development efforts and may be driven by ideological or financially opportunistic motives.

- Lynx (Kenya): Lynx focused on the technology sector in Kenya, encrypting systems and exfiltrating codebases or intellectual property. The group's goal appears to blend data theft with disruption, creating pressure for payment while retaining valuable data for future exploitation or sale.

- jokeir 07x (Tunisia): Operating across multiple sectors, jokeir 07x executed a ransomware campaign in the Tunisian tech landscape. jokeir 07x is a hacktivist group "protecting the Moroccan cyber landscape"

INDUSTRIES MOST TARGETED



Financial Services were the most targeted for the direct monetary gains possible through customer data, account information, and internal financial records theft. Many attacks involved database breaches aimed at acquiring credentials for fraudulent transactions or resale on underground markets.

Government Ministries and Agencies were targeted for both political and strategic purposes, with intrusions often seeking to exfiltrate sensitive policy documents, citizen records, or classified information that could be weaponized in geopolitical contexts.

Telecommunications providers were attacked primarily for large-scale customer data access, which can be leveraged for identity theft, surveillance, or as a pivot point for further targeting of subscribers.

Education institutions, particularly universities and research centers, were compromised for theft of intellectual property and personal details of staff and students.

Healthcare facilities saw targeted campaigns to obtain patient medical records, which are increasingly valuable for both financial fraud and targeted social engineering attacks.

THE THREAT LANDSCAPE OF NORTH AFRICA

North Africa experienced a high volume of cyber threat activity in July, with Morocco, Tunisia, Egypt, and Algeria collectively accounting for over 60% of the total incidents reported across the continent. Morocco was the hardest hit, recording 15 incidents, primarily database breaches, targeting government agencies, telecommunications providers, and financial institutions. Tunisia followed closely with 11 incidents, many of which involved initial access attacks and data theft from government, education, and technology sectors. Egypt recorded 4 incidents, affecting government and energy-related infrastructure, while Algeria experienced 2 incidents linked to politically motivated campaigns and opportunistic data breaches.

The region's strategic geopolitical position, combined with its concentration of government and financial infrastructure, continues to make it an attractive target for both financially motivated threat actors and politically driven groups. North African threat activity in July was marked by the presence of well-known actors such as mecrobyte, hider_nex, and server_dump, whose campaigns leveraged phishing, credential theft, and exploitation of unpatched vulnerabilities. Several of these attacks appeared to have cross-border implications, indicating collaboration or coordination between actors targeting multiple North African states.

CONCLUSION

The July 2025 threat landscape across Africa, and particularly in North Africa, reflects an increasingly complex and aggressive cyber environment. The dominance of database breaches highlights the persistent market for sensitive data, while the activity of both financially motivated and politically aligned actors demonstrates the convergence of crime and geopolitics in cyberspace. The prominence of actors like dark hell 07x and server_dump shows that certain groups have the resources, skills, and persistence to sustain long-term campaigns across borders. The diverse targeting of industries—from finance to healthcare—signals that no sector is immune, and that both public and private organizations must adopt proactive, intelligence-driven security strategies. Collaboration, rapid information sharing, and investment in detection and response capabilities remain critical for mitigating the evolving cyber threats facing the African continent.

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 ongoing cybersecurity training so employees can recognize phishing and social engineering attempts, since many attacks start there.
- 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.

RECOMMENDATIONS (CONT’D)

- 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