https://t.me/CyHawk_Africa

FEBRUARY 2025

REPORT OF THE CYBER THREAT LANDSCAPE IN AFRICA

Executive Summary

The African cyber threat landscape in February 2025 saw significant developments, with a shift in attack patterns, emerging threat actors, and evolving attack techniques. This report provides an in-depth analysis of cyber threats affecting Africa during this period, including attack distribution by country, key threat actors, industries most targeted, and observed trends. Additionally, a brief comparative analysis of January and February 2025 is included to highlight key changes. This document serves as a valuable resource for cybersecurity professionals, businesses, and policymakers seeking to enhance their defenses against evolving cyber threats.

The analysis is based on a dataset of 43 cybersecurity incidents recorded between 1 February and 28 February 2025. The dataset includes the following fields:

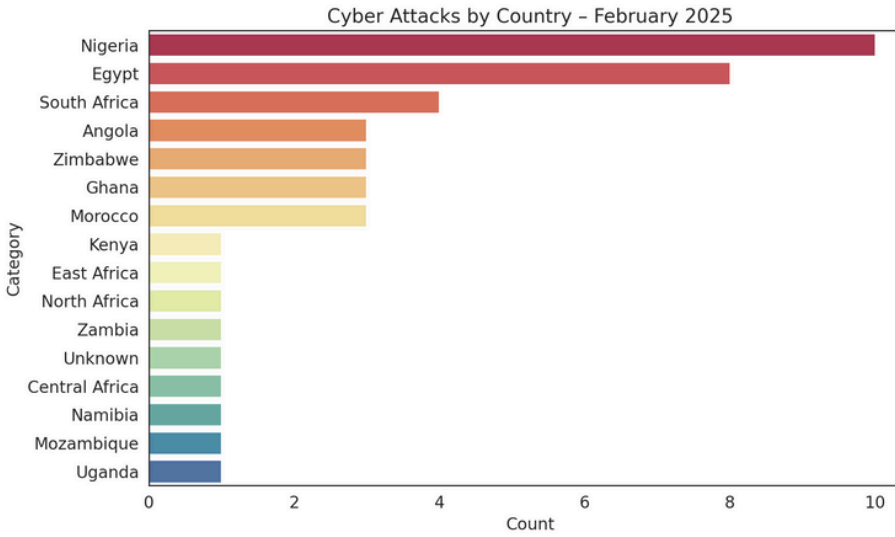
- *S/No: Incident identifier*
- *Date: Date of the incident*
- *Threat Actor: Group or individual responsible*
- *Country: Targeted country*
- *Threat Type: Nature of the attack (e.g., database breach, defacement, ransomware)*
- *Industry: Sector targeted (e.g., government, education, telecommunications)*

FREQUENCY OF ATTACKS BY COUNTRY

In February 2025, cyberattacks targeted various African nations, with some countries witnessing an increase in incidents compared to previous month.

27.9%

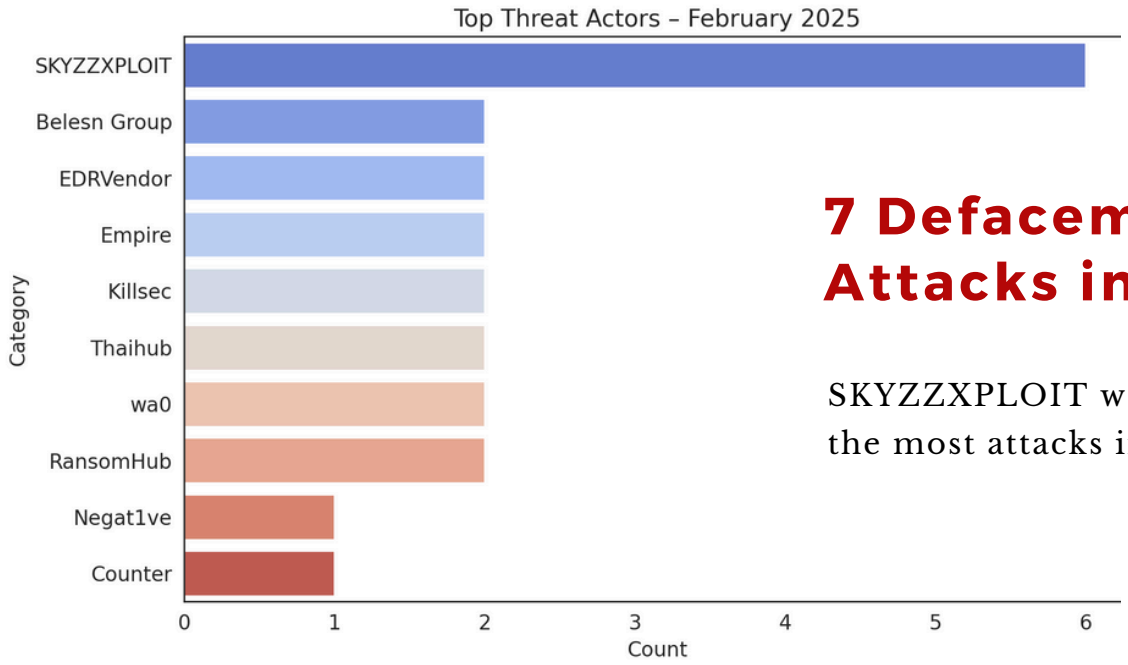
Nigeria has the most number of victims in February 2025



- Countries such as Angola, Zimbabwe, Nigeria, and South Africa recorded a noticeable rise in cyber threats, marking a shift in attacker focus.
- Kenya, Egypt, and Ghana continued to experience persistent threats, with new attack methods emerging.

MOST ACTIVE THREAT ACTORS

A diverse range of threat actors were responsible for cyber incidents in February 2025, including both Advanced Persistent Threat (APT) groups and independent threat actors.



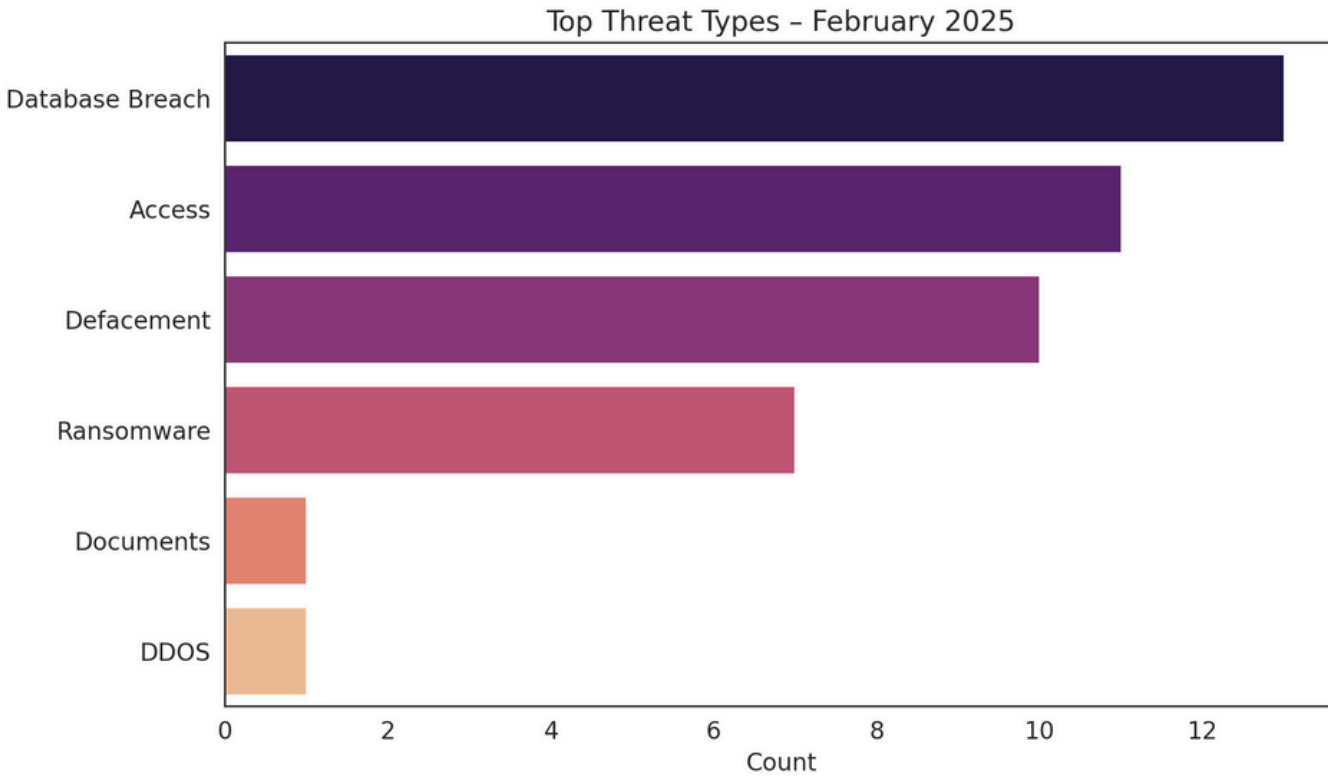
7 Defacement Attacks in Nigeria

SKYZZXPLOIT was responsible for the most attacks in Africa.

- Groups such as CYBER TEAM, Fog, wa0, and Pylades were prominent in launching attacks, engaging in activities such as website defacements, unauthorized access, and data breaches.
- Compared to January, the threat actor landscape diversified, with more actors engaging in disruptive rather than financially motivated attacks.

TOP THREATS

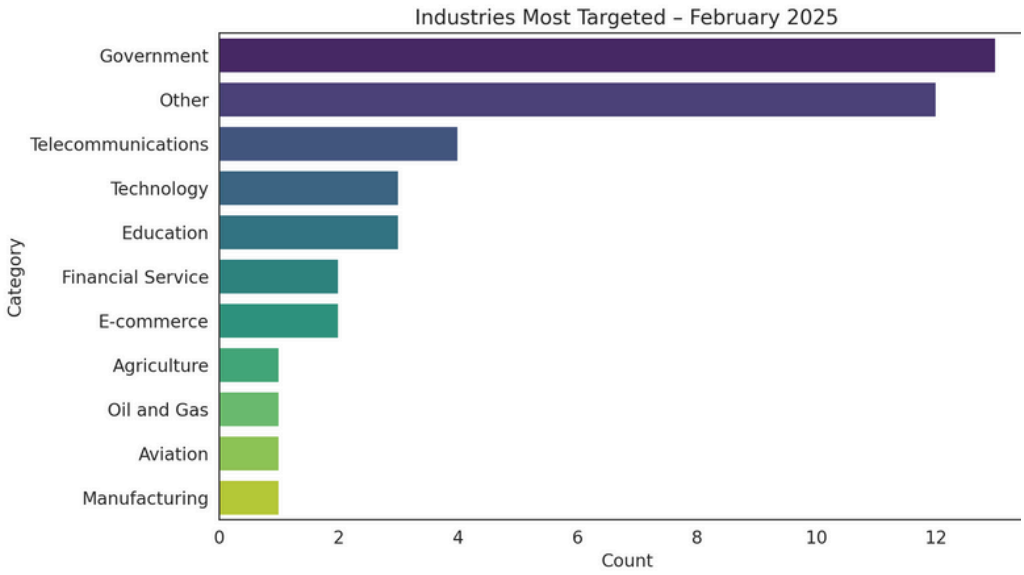
The nature of cyber threats in February saw an evolution in attack methods.



- Website defacements and unauthorized access incidents increased, particularly targeting government and telecommunications sectors.
- Ransomware attacks, phishing campaigns, and cyber espionage remained prevalent, but the tactics appeared more targeted and sophisticated.
- Database breaches surged, with attackers exfiltrating and exposing sensitive data from financial and technology firms.

INDUSTRIES MOST TARGETED

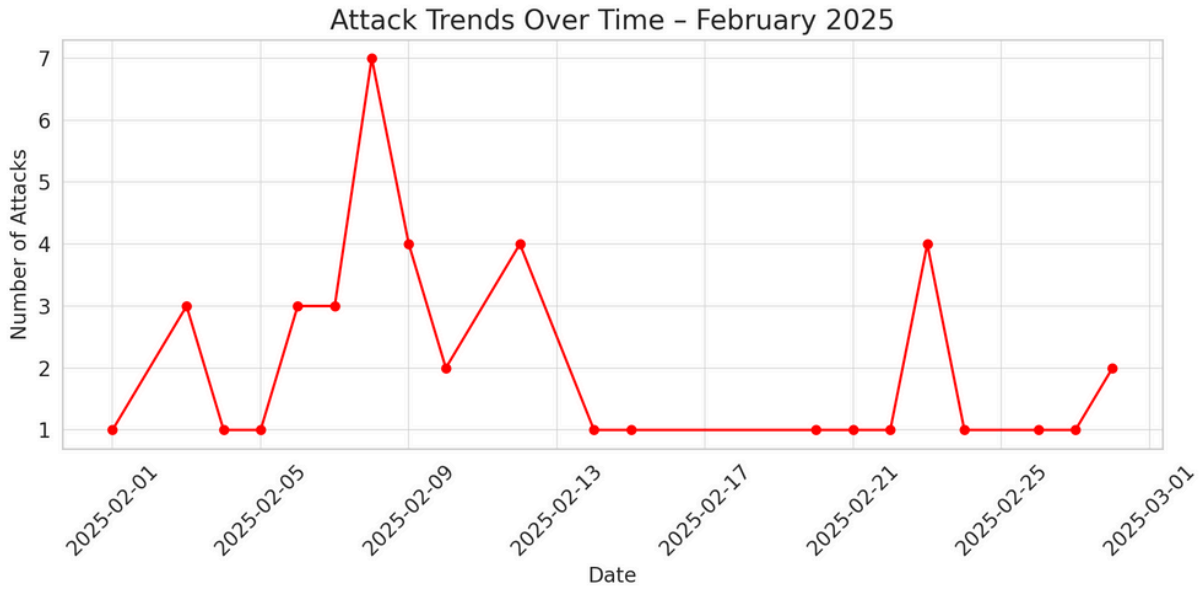
Sectoral analysis of the attacks in February 2025 reveals key industries facing heightened cyber threats.



- Telecommunications and technology firms emerged as primary targets, indicating increased interest in digital infrastructure disruption.
- Financial services and government institutions continued to experience cyber threats, largely driven by ransomware and cyber espionage activities.
- Healthcare remained a critical target, though at a slightly lower frequency than in January.

TREND

An analysis of cyberattacks throughout February 2025 provides insights into the varying frequency of incidents, with noticeable increases at specific periods, likely driven by coordinated threat campaigns or newly exploited vulnerabilities.



- 8 February 2025 recorded the highest number of incidents (6), all attributed to SKYZZXPLOIT in Nigeria.
- Attack frequency varied significantly, with spikes occurring mid-month and towards the end of February.
- These surges may be attributed to coordinated campaigns by threat actors, possibly linked to geopolitical events or cybersecurity vulnerabilities discovered during the month.

COMPARATIVE SUMMARY: JANUARY VS FEBRUARY 2025

A high-level comparison of cyber threats between January and February 2025 reveals important trends.

- **Countries Targeted**: While activities in January focused heavily on Kenya and Egypt, February saw increased activity in Angola and Zimbabwe.
- **Threat Actor Diversity**: January was largely dominated by APT groups, while February saw a mix of APT groups and independent cybercriminals engaging in disruptive activities.
- **Attack Methods**: January's primary threats were ransomware and phishing, whereas February introduced more defacements, unauthorized access incidents, and database breaches.
- **Industry Impact**: Government and healthcare were the main targets in January, while telecommunications and technology sectors took precedence in February.

This comparative insight underscores the rapidly evolving cyber threat landscape in Africa, requiring continuous adaptation and enhanced security measures.

CONCLUSION

The findings from February 2025 indicate an increasingly complex cyber threat environment in Africa.

The geographic expansion of threats, diversification of threat actors, and evolution of attack techniques emphasize the need for organizations to stay vigilant and proactive in their cybersecurity strategies.

Key Points:

- Cyber threats expanded to new regions, with Angola and Zimbabwe experiencing heightened attacks.
- A shift from financially motivated cybercrime to more disruptive attacks was observed.
- The telecommunications and technology sectors faced increased cyber threats compared to January.
- The attack frequency fluctuated throughout February, possibly influenced by external factors such as geopolitical events.

RECOMMENDATIONS

- Threat Intelligence Monitoring: Organizations should continuously monitor and analyze cyber threats to anticipate emerging attack trends.
- Website administrators should deploy web application firewalls (WAFs) and monitor for unauthorized changes to prevent defacement.
- Implement zero-trust architectures to limit unauthorized access.
- Prioritize data protection and cybersecurity awareness.
- Improved Cyber Resilience: Businesses must enhance their security frameworks to protect against evolving attack methods.
- Implement advanced security tools such as endpoint protection, and MFA.
- Conduct regular security audits and employee training programs.
- Collaborative Cybersecurity Efforts: Increased public-private partnerships can enhance collective defense against cyber threats.