January 2025

APT Attacks in Africa

Authored by

Hassanat Oladeji

Executive Summary

This report provides an analysis of Advanced Persistent Threat (APT) activities targeting various industries across African countries in January 2025. The data highlights threat actors, targeted industries, and attack trends, offering actionable intelligence to cybersecurity professionals, government agencies, and private sector organizations.

In January 2025, Africa witnessed a surge in cyber threats, particularly from Advanced Persistent Threat (APT) groups employing ransomware and initial access techniques. A total of 10 APT groups were observed targeting critical sectors, including government, finance, and education. Among these, Funksec, Gdlockersec, and Anonymous Sudan emerged as the most active and disruptive ransomware groups.

The rise of these threats underscores the importance of proactive threat intelligence, robust cybersecurity defences, and collaborative efforts among organizations to mitigate risks.

ATTACK TRENDS

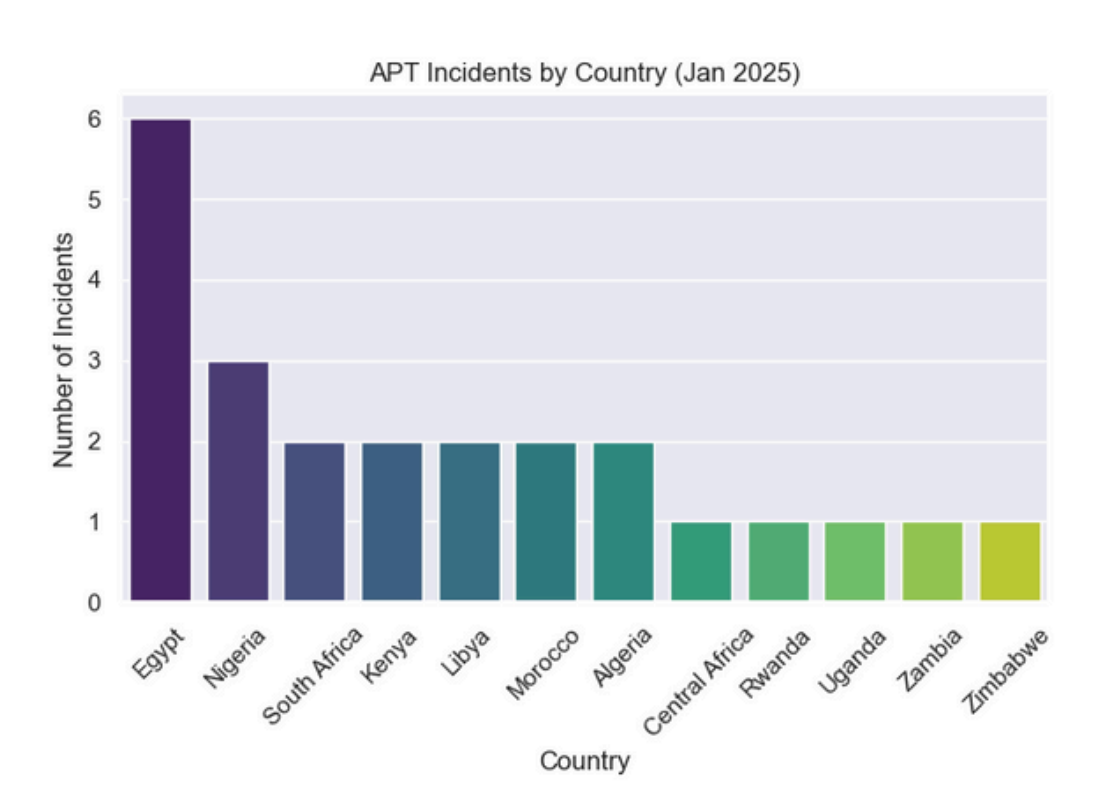

Figure 1: Countries Most Targeted by APT Activities

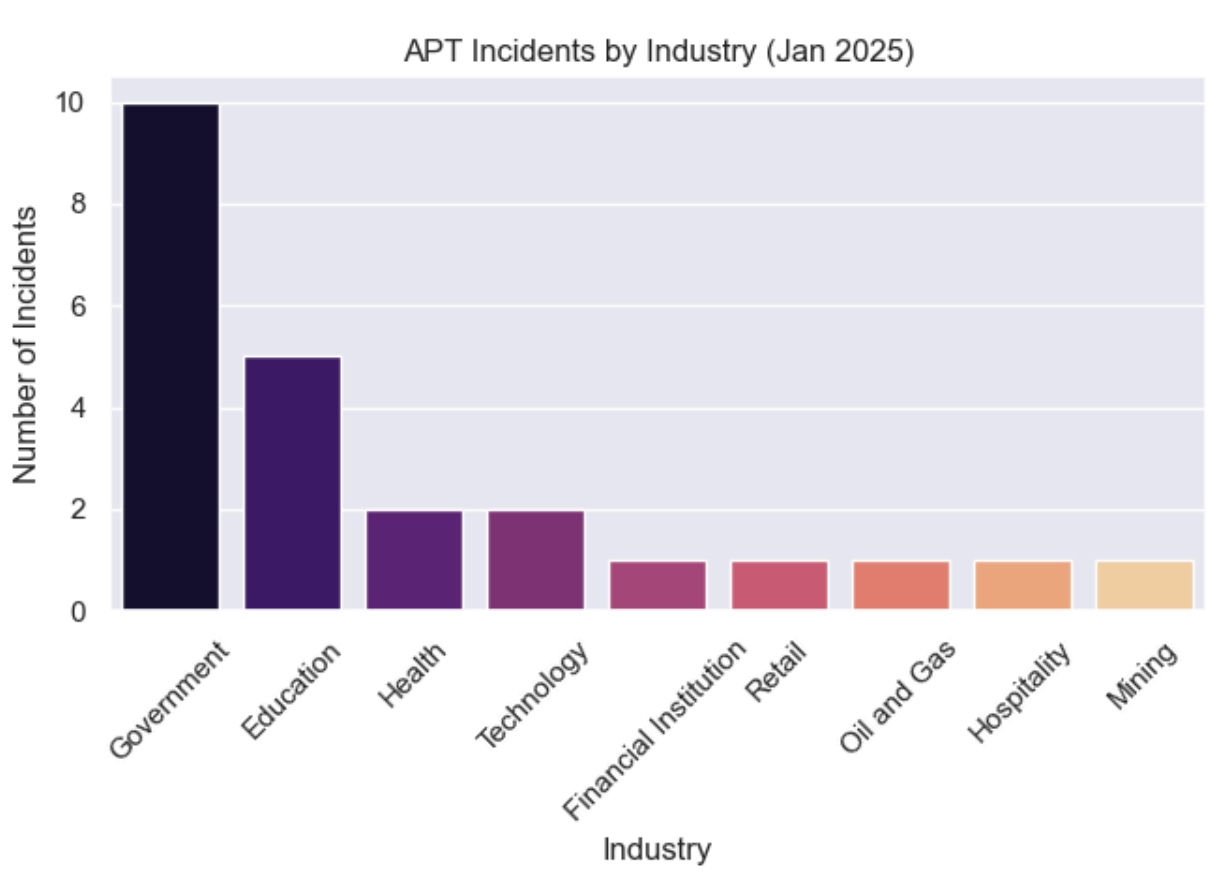

Figure 2: Industries Most Targeted by APT Activities

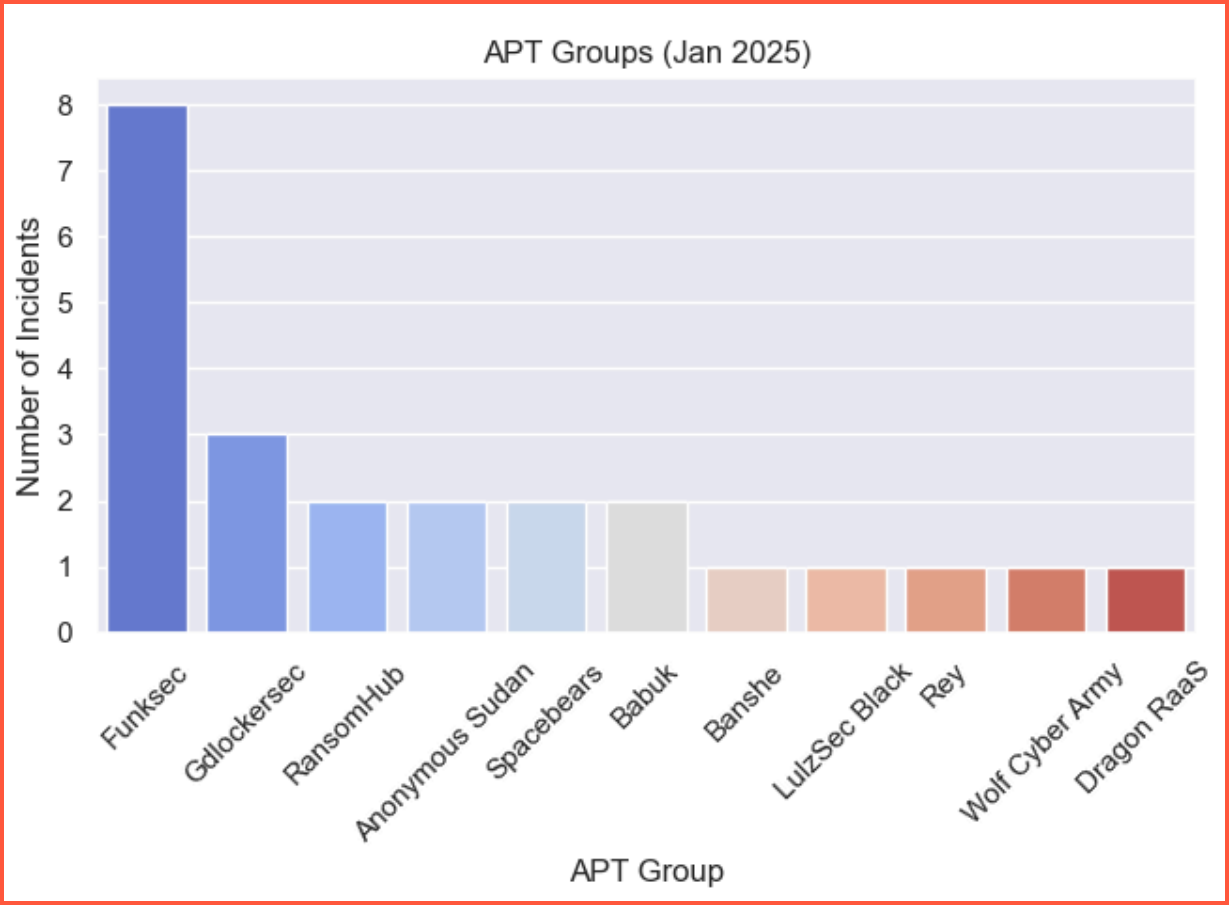

Figure 3: Top APT Groups by Number of Incidents

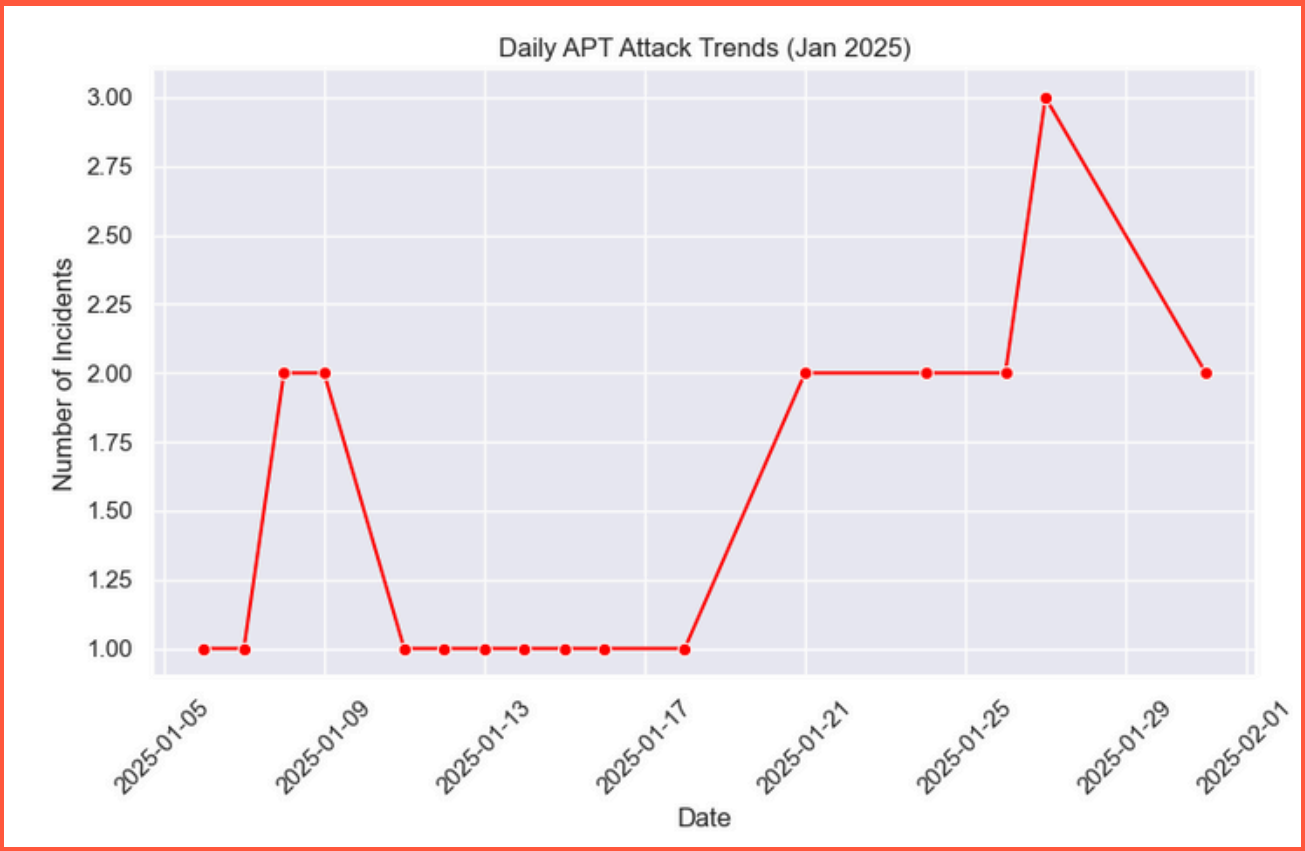

Figure 4: Trend of Attacks of APT Groups in January 2025

TOP APT Groups

In January 2025, we detected 10 APT groups target Africa via ransomware and initial access. The top 3 ransomware groups are:

Funksec

Funksec has demonstrated a high level of sophistication, executing ransomware campaigns against several industries in the world since its emergence. In Africa, in Jan 2025, they targeted government institutions in Egypt and Algeria, technology and education institutions in Morocco and Nigeria respectively.

Targeted Industries

- Government institutions (5)
- Technology (2)
- Education (1)

Targeted Countries

- Egypt (4)
- Nigeria (1)
- Morocco (1)
- Algeria (1)
- Uganda (1)

Gdlockersec

This new ransomware group emerged in January 2025. The group targeted two education institutions in Morocco and Egypt, and one government institution in Nigeria.

Targeted Industries

- Government institutions (1)
- Education (2)

Targeted Countries

- Egypt (1)
- Nigeria (1)
- Morocco (1)

Anonymous Sudan

Anonymous Sudan, a hacktivist collective, carries out politically motivated cyberattacks, primarily using Distributed Denial-of-Service (DDoS) attacks against its victims. In Africa, they targeted the Bank of Central African States and one government institution in Libya.

Their primary objectives are to disrupt critical national infrastructure and spread political propaganda.

Targeted Industries

- Government institutions (1)
- Financial Institution (1)

Targeted Countries

- Central Africa (1)
- Libya (1)

Conclusion

APT groups continue to evolve, leveraging advanced tactics to infiltrate organizations in Africa. Governments and private enterprises must continue to improve their security measures, share intelligence, and adopt proactive defense strategies to mitigate cyber risks.

Join our channel to get updates on cyber threats in Africa.

Telegram: CyHawk Africa