ethnos

The Cyber Threat Chronicles: Q1 2025

www.ethnoscyber.com

TABLE OF CONTENT

Overview & Methodology:

This section sets the stage by summarizing the quarter's most critical findings, such as shifts in overall threat levels and emerging patterns. It then explains the scope (geographies covered, sectors analyzed). Finally, it lists the primary research questions that framed the investigation, ensuring transparency around what drove our focus.

Executive Summary

This report provides a comprehensive analysis of the cyber threat landscape in Africa during the first quarter of 2025, spanning from January to March. The analysis draws upon various findings to identify the key trends, vulnerabilities, attack vectors, and significant incidents that shaped the threat environment across the continent. The findings reveal a persistent rise in cybercriminal activity targeting various sectors, including education, government, telecommunications, healthcare, financial services, manufacturing, and energy. Ransomware and social engineering attacks remain significant concerns, with the increasing use of artificial intelligence by threat actors to enhance the sophistication and scale of their operations.

The report highlights the exploitation of unpatched vulnerabilities, misconfigurations, and human error as primary weaknesses. It also underscores the growing risks associated with mobile devices, cloud environments, and third-party supply chains. This report aims to equip organizations operating in Africa with the knowledge necessary to strengthen their cybersecurity resilience and mitigate potential risks by detailing the prevalent threats and vulnerabilities.

Scope and Methodology

Overall Cyber Threat Trends:
Identifying prevalent cyber threats, vulnerabilities, and attack vectors targeting various sectors in Africa.

Insider Threats:
Assessing the prevalence and impact of insider threats in Africa, drawing on global data and regional surveys.

Top Vulnerabilities:
Identifying the primary vulnerabilities affecting organizations in Africa, including unpatched software, misconfigured cloud environments, human error, and third-party risks.

Top Attack Vectors:
Analyzing the most common attack vectors used by cybercriminals in Africa, including email phishing, social media, mobile devices, and applications.

Overall Cyber Country-Specific Insights:
Examining cyber-attack statistics and trends in specific African countries, with a focus on Nigeria, Angola, Kenya, and South Africa.

Sector-by-Sector Analysis:
Contains detailed examination of how cyber threats are affecting key sectors-including healthcare, finance, manufacturing, education, government, and telecommunications.

Key Cyber Incidents:
Detailing significant cyber incidents that occurred in Africa during Q1 2025, such as the cyber conflict between Algeria and Morocco, financial losses due to online fraud in Ghana, and attacks on critical infrastructure.

Main Research Questions Addressed in this Report:

01 What are the predominant cyber threats and attack vectors affecting Africa during the first quarter of 2025?

02 Which sectors and countries in Africa are most targeted by cybercriminals, and what trends are emerging in these regions?

03 What are the most significant vulnerabilities exploited by attackers in African organizations?

04 How prevalent and impactful are insider threats within African organizations during this period?

05 What are the notable cyber incidents that occurred in Africa in Q1 2025, and what were their consequences?

06 How are organizations in Africa responding to and mitigating these cyber threats and vulnerabilities?

Regional & Sectoral Threat Landscape

Here, we rank the top 12 African countries by overall cyber threat level, offering concise profiles that highlight each nation's risk drivers.

The sectoral analysis then drills into seven critical industries, Education, Government, Telecommunications, Manufacturing, Healthcare & Medical, Consumer Good & Services, and Financial Services, outlining their unique vulnerabilities, etc.

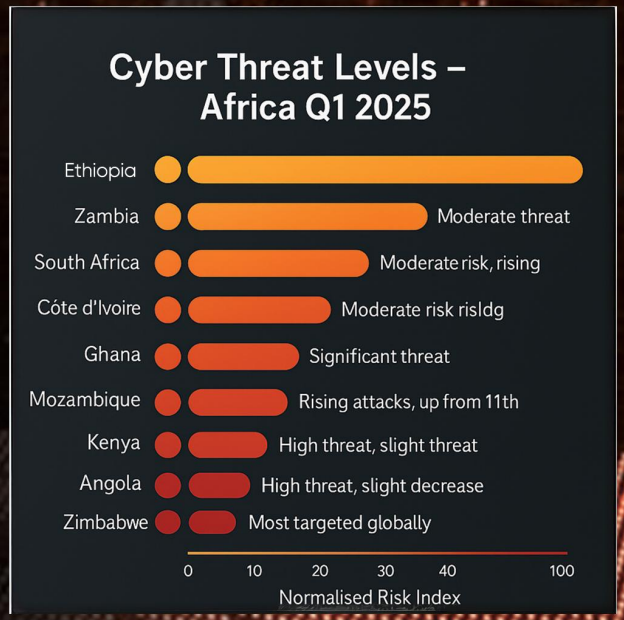
Together, these country and industrybreakdowns help stakeholders pinpoint where to concentrate defenses and allocate resources.

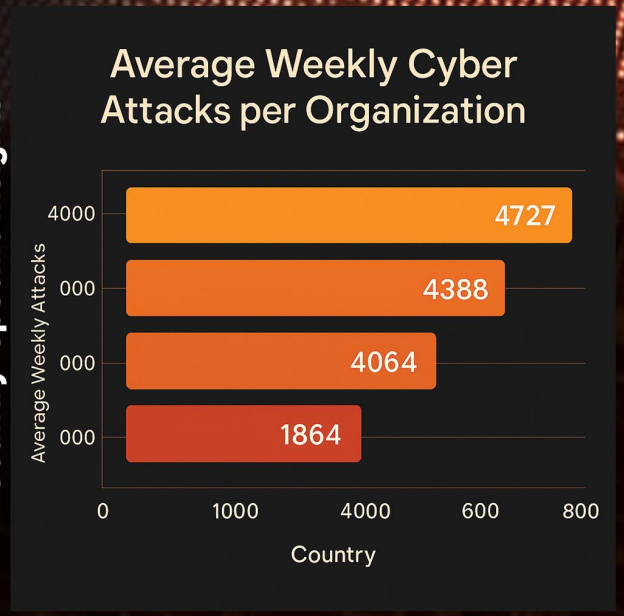
Top 12 African Countries by Cyber Threat Level Q1 2025

In Q1 2025, the cyber threat landscape across African countries revealed significant vulnerabilities, with Ethiopia leading globally as the most targeted nation, boasting a Normalized Risk Index (NRI) of 99.4, followed by Zimbabwe, Uganda, and Nigeria among the top 10 worldwide. The data, visualized through a striking polar bar chart and an annotated lollipop chart, underscores the intense concentration of cyber risks in East and Southern Africa, with countries like Kenya and Nigeria experienc

ing rising attacks, while South Africa and Egypt face moderate but escalating threats.

These visualizations, complemented by a detailed text table, provide a clear, multidimensional perspective on the varying threat levels, highlighting the urgent need for targeted cybersecurity measures in high-risk regions. This analysis sets the stage for a deeper exploration of sector-specific vulnerabilities and strategic responses to safeguard Africa's digital infrastructure.





Country-Specific Insights

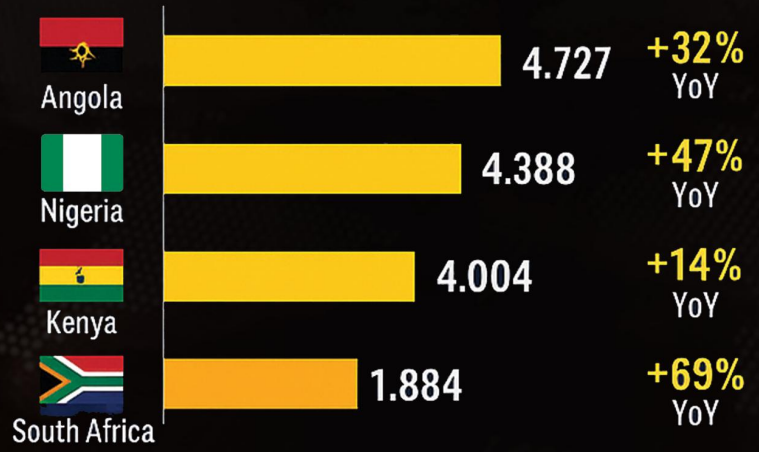
Top 12 African Countries by Cyber Threat Level Q1 2025

CYBER THREAT LANDSCAPE IN AFRICA: Q1 2025 Snapshot

Rising Cyber-Attacks and Law Enforcement Action Across the Continent

Weekly Cyber-Attacks per Organization (Q1 2025)

Source: Check Point Software Technologies



Insight South Africa had the highest growth rate despite the lowest attack volume

Cybercrime Crackdown:

Interpol's Operation Red Card

- Multiple arrests and digital evidence seizures

Emerging Threat: Mobile Application Attacks in Kenya

- Kenya is experiencing a notable surge in mobile app threats
- Attackers are increasingly targeting users through deceptive apps and phishing

Orgnizations and users in Kenya must be vigilant about mobile security practices

Key Takeaways

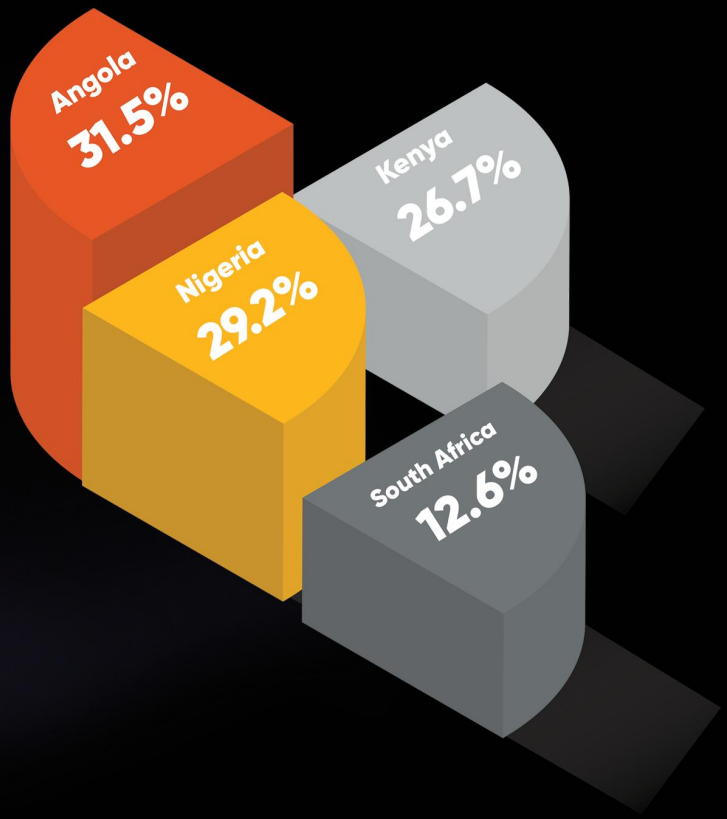
- Cyber-attacks are steadily rising across major Africon economies
- South Africa had the largest year-over-year increase in attack frequency

Protect Your Organization

- Implement mulit-layered security > Train employees on phishing and mobile safety • Monifor for emerging *threat*

These statistics reveal that the volume and growth rate of cyber-attacks varied considerably across different African nations during the first quarter of 2025. Angola and Nigeria experienced the highest average weekly attacks, suggesting a concentrated focus of cybercriminal activity on these countries. South Africa, while having a lower overall attack volume compared to Nigeria and Angola, witnessed the most substantial year-over-year increase, indicating a rapidly evolving threat landscape. These differences could be attributed to a multitude of factors, including the maturity of digital infrastructure, the level of cybersecurity awareness among users and organizations, the scale of economic activity,

Distribution of Average weekly Cyber attacks in Q1 2025



Sector-by-Sector Threat Analysis

This section breaks down the cyber threat environment across key African industries

- EDUCATION
- GOVERNMENT
- TELECOMMUNICATIONS
- HEALTHCARE & MEDICAL
- CONSUMER GOODS & SERVICES
- FINANCIAL SERVICES
- INDUSTRIAL MANUFACTURING

using Q1 2025 attack metrics and year-over-year trends. For each sector, we highlight the primary drivers of risk, including common vulnerability patterns, threat actor motivations, etc. These insights enable organizations to benchmark their exposure against peers and prioritize security investments where they are needed most.

Education Sector

The education sector emerged as the most heavily targeted industry across Africa during Q1 2025, experiencing an average of 4,484 weekly attacks per organization-a staggering 73%

increase from the previous year. This sector's vulnerability stems from several factors: typically, limited cybersecurity budgets, extensive networks serving diverse user populations, valuable research data, and increasingly digital learning environments. Educational institutions often maintain databases containing sensitive personal information of students and staff, making them attractive targets for identity theft and ransomware operations. African educational institutions face additional challenges due to rapid digitalization efforts that may outpace security implementations, creating exploitable gaps in their defensive postures. The sector's vulnerability is compounded by the often-open nature of academic networks designed

Government Sector

Government organizations across Africa experienced the second-highest attack volume, with 2,678 weekly attacks per organization-a 51% increase year-over-year. This sector holds enormous quantities of sensitive citizen data, critical infrastructure controls, and access to national resources, making it a prime target for cybercriminals and nation-state actors alike.

African government agencies increasingly implement digital services to improve efficiency and accessibility, but these initiatives often create new attack vectors when not adequately secured. The elevated threat level against government entities reflects the strategic value of compromising these organizations, whether for financial gain through ransomware, espionage, or disrupting essential services. The potential for socio-political impact from successful attacks on government systems makes this sector particularly vulnerable to sophisticated threat actors with diverse motivations.

Telecommunications Sector

The telecommunications sector experienced the most dramatic percentage increase in attacks, with a 94% year-over-year surge reaching 2,664 weekly attacks per organization.

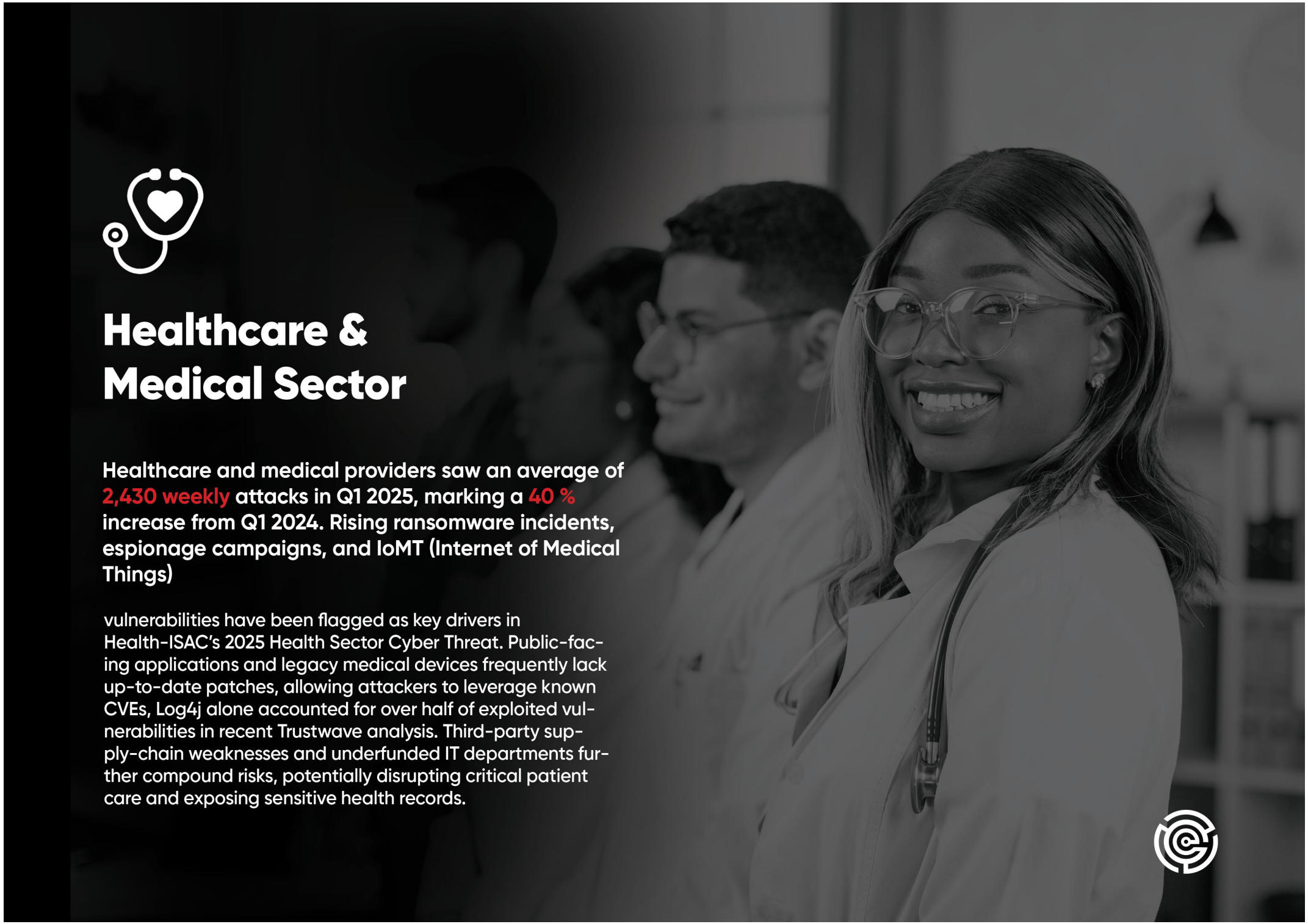
This sector forms the backbone of Africa's digital economy, making it both strategically valuable and potentially catastrophic if compromised. Telecommunications providers maintain critical infrastructure that facilitates communication, financial transactions, and data transmission across all other sectors. Telecommunications companies maintain vast networks with numerous potential entry points, handle enormous volumes of sensitive customer data, and provide essential services that impact virtually every other industry.

This rapid escalation is fueled by the continued operation of legacy network infrastructure alongside newly deployed 5G and IoT services, which often lack comprehensive security hardening. The widespread adoption of mobile-money platforms and cloud-based telecom services has expanded the attack surface, with threat actors exploiting misconfigurations and weak encryption protocols. Given their critical role in national communications and economic activity, telecom operators now represent high-value targets for both financially motivated cybercriminals and state-sponsored adversaries.

Industrial Manufacturing Sector

Industrial Manufacturing saw an average of 1,554 weekly attacks in Q1 2025, a 63 % year-over-year increase

The convergence of IT and operational-technology (OT) environments has introduced new attack vectors, with ransomware and supply-chain exploits often targeting unsegmented control networks. Aging machinery and ICS (Industrial Control System) components frequently run outdated firmware lacking vendor support, leaving them vulnerable to known remote-code-execution and denial-of-service exploits. As manufacturers push for greater automation and "Industry 4.0" integrations, insufficiently secured APIs and third-party modules have become prime intrusion points for attackers aiming to disrupt production or steal intellectual property.



Healthcare & Medical Sector

Healthcare and medical providers saw an average of 2,430 weekly attacks in Q1 2025, marking a 40 % increase from Q1 2024. Rising ransomware incidents, espionage campaigns, and IoMT (Internet of Medical Things)

vulnerabilities have been flagged as key drivers in Health-ISAC's 2025 Health Sector Cyber Threat. Public-facing applications and legacy medical devices frequently lack up-to-date patches, allowing attackers to leverage known CVEs, Log4j alone accounted for over half of exploited vulnerabilities in recent Trustwave analysis. Third-party supply-chain weaknesses and underfunded IT departments further compound risks, potentially disrupting critical patient care and exposing sensitive health records.

Consumer Goods & Services Sector

Consumer Goods & Services organizations recorded an average of 1,793 weekly attacks in Q1 2025, up 51 % year-over-year. The surge is largely due to a 126 percent spike in ransomware attacks targeting manufacturers and retailers, used as "testing grounds" before campaigns against larger western firms

E-commerce platforms and point-of-sale systems in this sector frequently rely on third-party payment processors and legacy web components, creating exploitable supply-chain and application-layer vulnerabilities. Additionally, consumer data, ranging from payment card information to personal profiles, is highly monetizable on underground markets, making these firms attractive ransomware and phishing targets.

Financial Services Sector

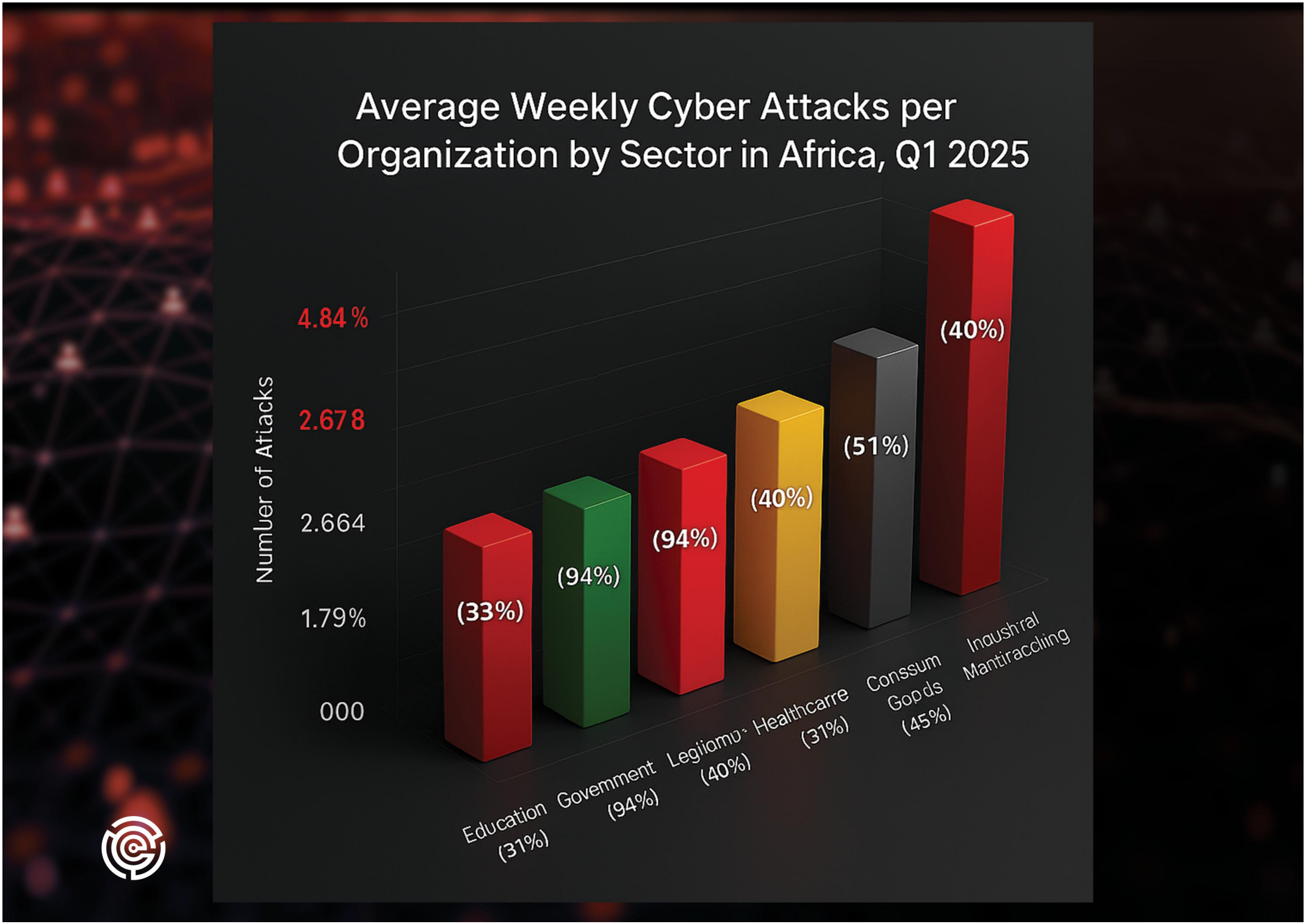
Financial Services entities experienced 1,747 weekly attacks in Q1 2025, representing a 45% increase versus Q1 2024. In Kenya alone, ransomware incidents rose 19% in 2024, while detected exploits climbed 55 %, underscoring a broader African trend of accelerated attacks on banks and fintech platforms.

Phishing campaigns targeting mobile-banking customers and business-email compromise (BEC) schemes remain prevalent, exploiting both human and technical gaps in authentication and fraud-detection controls. Regulatory fragmentation across jurisdictions further complicates coordinated incident response and threat-sharing efforts, allowing sophisticated groups to pivot between countries with relative impunity.

Spotlight Deep Dives

This module provides narrative-driven examinations of the quarter's standouts. It begins with insider threats, quantifying their prevalence and root causes, then moves to the top vulnerabilities exploited in Q1. We review a high-profile cyber conflict between Algeria and Morocco, catalog dominant attack vectors, profile key ransomware groups (with a focus on African-born FunkSec), and close with an in-depth look at Agent Tesla's operational mechanics and its strategic impact across the continent, accompanied by a mitigation framework recommended by Ethnos Cyber.

.


Average Weekly Cyber Attacks per Organization by Sector in Africa, Q1 2025
Number of Attacks
4.84%
2.678
2.664
1.79%
000
(33%)
(94%)
(94%)
(40%)
(51%)
(40%)
Education (31%)
Govemment (94%)
Legiiamu- (40%)
Healthcarre (31%)
Conssum Gop ds (45%)
Inaushiral Mantiraccling

Top Vulnerabilities Affecting Companies in Africa in Q1 2025

A primary vulnerability affecting companies in Africa during the first quarter of 2025 was the continued exploitation of unpatched vulnerabilities in various software and systems. Cybercriminals consistently leverage known weaknesses in outdated or unpatched software to gain unauthorized access to organizational networks and data. The alarming increase in the number of both disclosed and actively exploited vulnerabilities globally underscores the urgency for African organizations to prioritize timely patching and vulnerability management.

Misconfigurations and poor API security, particularly within cloud environments, also presented significant vulnerabilities. As more African companies migrate their operations and data to the cloud, inadequate security configurations and poorly secured Application Programming Interfaces (APIs) can inadvertently expose sensitive information and provide attackers with pathways to traverse systems undetected.

purposes further blurs the lines between personal and professional lives, potentially increasing the risk of accidental data exposure and susceptibility to social engineering schemes.

The presence of legacy systems and outdated defenses also contributed to the vulnerability landscape. In some sectors, particularly agriculture and construction, the reliance on older technologies that lack modern security features makes them easier targets for exploitation. These systems may contain known vulnerabilities that have not been addressed, providing readily accessible entry points for attackers.

Finally, third-party vendors and supply chain vul-

Key Cyber Incidents in Africa (Q1 2025)

1. Escalating Cyber Conflict Between Algeria and Morocco

In the first quarter of 2025, a significant escalation in cyber hostilities occurred between Algeria and Morocco,[9] [10] reflecting the broader geopolitical tensions between the two nations.

a. Breach of Morocco's Social Security Systems

In early April 2025, Moroccan authorities reported a major cyberattack [9] targeting the National Social Security Fund (CNSS) and the Ministry of Economic Inclusion, Small Business, Employment, and Skills. Hackers infiltrated these systems, leaking sensitive personal and financial data on Telegram. The leaked information reportedly included salary details of executives from state-owned companies, political parties,

b. Moroccan Hackers' Retaliatory Strike

In response, Moroccan hacker groups, operating under names such as "Phantom Atlas," "Phantom Morocco," and "Moroccan Cyber Forces," launched a counterattack on Algeria's Social Security Fund for Postal and Telecommunications Workers (MGPTT). They claimed responsibility for infiltrating the MGPTT's internal systems and leaking over 13 GB of sensitive data, including ID numbers, money transfer orders, and administrative documents. The hackers framed this action as a direct and calculated response to the CNSS breach, stating that any future provocation would be met with a "targeted and disproportionate response" .

Cybersecurity experts highlighted the ease with which the Moroccan hackers exploited vulnerabilities in Algeria's cybersecurity infrastructure, pointing to deep structural flaws and mismanagement within Algerian state institutions.

c. Historical Context and Ongoing Cyber Tensions

This cyber conflict is not unprecedented. In November 2021, the website of Morocco's General Confederation of Enterprises (CGEM) was defaced by attackers who replaced the homepage with the Algerian flag and a message stating "no peace between systems," an attack likely originating from Algeria . Conversely, Moroccan hacker groups have previously targeted Algerian government websites, including the Ministry of Finance, indicating a pattern of reciprocal cyberattacks between the two nations .

The recent cyber incidents underscore the escalating digital shadow war between Algeria and Morocco, where each offensive invites an equally forceful counter-offensive.

2. Financial Loss To Online Fraud In Ghana

The Cyber Security Authority (CSA) of Ghana reported that total financial losses from online fraud reached GH¢2,404,161 during the first quarter of 2024. Alarmingly, this figure nearly doubled to GH¢4,425,851 during the same period in 2025. These losses stemmed from 195 reported cases between January and March 2024, rising sharply to 305 cases over the corresponding months in 2025 [3].

Predominant forms of cybercrime in Ghana

The CSA further identified the leading categories of cybercrime impacting Ghana and the broader West African region. The most prevalent cyber-related incidents included [3]:

- Online Fraud: Investment scams, fraudulent online shopping schemes, and deceptive job recruitment offers.
- Unauthorized Access: Incidents such as WhatsApp account takeovers and phishing attacks targeting user credentials.
- Online Impersonation: Creation of fraudulent digital identities to deceive victims.
- Online Blackmail: Sextortion and the distribution of non-consensual intimate images.
- Cyberbullying: Harassment and intimidation conducted through digital platforms.
- Information Disclosure: Unauthorized exposure or theft of sensitive personal and corporate data.

Operation Red Card

A significant law enforcement operation, codenamed Operation Red Card, conducted between November 2024 and February 2025, resulted in the arrest of over 300 suspects across seven African countries and the seizure of 1,842 devices in seven African countries. This INTERPOL-led operation targeted cyber attacks and cyber-enabled scams, including those involving mobile banking, investment fraud, and messaging applications, affecting more than 5,000 victims. Countries involved included Benin, Côte d'Ivoire, Nigeria, Rwanda, South Africa, Togo, and Zambia [8].

Specifically, in Nigeria, authorities arrested 130 individuals, including 113 foreign nationals, who were involved in various cyber-enabled scams, including online casino fraud and investment scams[11].

The operation highlighted the prevalence of social engineering tactics, such as posing as telecom employees or impersonating family members, to extract sensitive information and gain access to victims' financial accounts.

4. South African Weather Service

In late January 2025, the South African Weather Service experienced a cyberattack that took its ICT systems offline, disrupting critical services, including aviation and marine forecasts, and shutting down its email system and website [14]. This incident underscored the vulnerability of critical infrastructure to cyber threats and the potential for significant disruptions to essential services.

5. Cell C Data Leak

South African mobile network operator Cell C confirmed a data leak in April 2025 following a cyberattack that occurred in the previous year. The hacker group, RansomHouse, claimed to have exfiltrated 2TB of the company's data, including sensitive customer information such as names, contact details, ID numbers, banking information, and medical records.

Top Attack Vectors in Africa in Q1 2025

- Email phishing consistently ranked as one of the most prevalent attack vectors in Africa during the first quarter of 2025. Cybercriminals continued to refine their phishing tactics, using increasingly sophisticated and deceptive emails to lure unsuspecting users into clicking malicious links, opening infected attachments, or divulging sensitive information.
- The use of social media and messaging applications, such as WhatsApp, as attack vectors also saw a rise. The widespread popularity and perceived trustworthiness of these platforms make them effective channels for social engineering attacks and the distribution of malware. Attackers often leverage these platforms to spread misinformation, conduct scams, and trick users into clicking on malicious links or downloading harmful files.
- The exploitation of mobile devices and applications emerged as a significant attack vector, particularly given the rapid growth of mobile financial services across Africa. Interpol's Operation Red Card brought to light the significant issue of mobile banking and investment application scams in Africa. The operation in Zambia revealed instances where attackers successfully compromised victims' mobile phones through SMS phishing links. These links led to the installation of malware that granted the attackers unauthorized access to the victims' banking applications.
- Furthermore, KnowBe4's report indicates a substantial 333% surge in mobile application threats detected in Kenya in the three months leading up to September 2024[7]. These threats were primarily aimed at stealing sensitive user information, such as login credentials. The increasing adoption of mobile financial services across Africa, reported by KnowBe4 at 85% of their respondent group[7], has expanded the attack surface for cybercriminals specifically targeting mobile devices.
- Malvertising the use of malicious advertisements displayed on legitimate websites or social media platforms, also served as an attack vector for distributing malware or redirecting users to phishing pages. This technique allows attackers to reach a broad audience by leveraging the trust associated with reputable online platforms.
- A concerning trend was the increasing utilization of AI-powered tools o enhance cyberattacks. Generative AI was increasingly used to create hyper-realistic fake documents, voices, and images, enabling more sophisticated and scalable social engineering attacks, including deep fakes, which can bypass traditional verification systems and manipulate victims more effectively.

Top Ransomware Groups

Based on data, Clop is the most prevalent ransomware group, responsible for 10% of the published attacks, followed by FunkSec with 8% and RansomHub with 7%.

Meanwhile, FunkSec continued its meteoric rise, carrying momentum from Q4 2024 into Q1 2025. Leveraging AI to develop malware, FunkSec named 152 victims this quarter—up from 82 last quarter, earning its place as the fourth most active ransomware groups in Q1 2025. This surge demonstrates how AI is enabling even inexperienced threat actors to launch sophisticated attacks across multiple sectors.

Ransomware Group to Watch out for in 2025 - FunkSec, an African Ransomware Group

FunkSec is a ransomware group that emerged publicly in late 2024 [12]. It quickly gained attention for the high number of victims it claimed in December 2024, surpassing many other ransomware groups during that period

Origin:

While definitive information about the individuals behind FunkSec is limited, research suggests a potential connection to Algeria. This is based on several clues:

- Parts of the FunkSec ransomware code and related tools have been uploaded to VirusTotal from sources in Algeria.
- The username "Abdellah," an Arabic name, appeared in the compilation path of the ransomware.
- Early versions of the ransom note referenced both "FunkSec" and "Ghost Algeria," a previously known hacktivist group with ties to Algeria [16].
- Analysis of online forum activity associated with early promoters of FunkSec also pointed to Algeria.

Activities and Characteristics:

- Ransomware and Data Leak Site (DLS): FunkSec operates a DLS on the Tor network where they list their victims and leak stolen data if the ransom is not paid. They employ double extortion tactics, encrypting files and exfiltrating data.
- AI Assistance: A notable characteristic of FunkSec is their apparent use of Artificial Intelligence (AI) in developing their ransomware and related tools. This may allow less experienced actors to create and refine sophisticated malware more quickly. Evidence of AI use has been found in code comments and the group's use of AI chatbots for operational support. [13]
- Ransomware-as-a-Service (RaaS): FunkSec appears to operate under a RaaS model, potentially selling their ransomware and tools to other, less sophisticated attackers.
- Low Ransom Demands: Unlike many major ransomware groups that demand millions, FunkSec has been known to ask for relatively low ransoms, sometimes around $10,000. This might be part of a "churn and burn" strategy to generate quicker revenue, possibly supplemented by selling stolen data on the dark web [13] .

- Hacktivist Ties: There are indications that FunkSec has connections to hacktivist activities. Some of their leaked datasets appear to be recycled from previous hacktivist campaigns. The group has also attempted to associate itself with defunct hacktivist groups like Ghost Algeria and Cyb3r Fl00d, possibly to enhance their credibility or mask their true motivations. They have also expressed political motivations, such as targeting the United States due to its support for Israel.
- Targeting: FunkSec has claimed victims across various sectors, including government and defense, technology, finance, and education. While a significant number of their claimed victims are in the United States and India, they have also listed victims in numerous other countries.
- Tools: Besides their custom ransomware (FunkLocker) [17], FunkSec has offered other tools, including a DDoS tool, a password generation and scraping tool ("funkgenerate"), and a remote desktop management tool.
- Evolving Operations: FunkSec has shown a pattern of continuous development of their ransomware and data leak site, with multiple versions of their encryptor being identified. They have also formed partnerships with other cybercriminal groups to expand their operations.
- Increased Victim Count: The number of victims claimed by FunkSec has continued to rise. By early 2025, they had claimed over 100 victims, and by the end of the first quarter, this number had reached 152.

Malware to Watch Out For: Agent Tesla, Africa's Rising Cyber Threat

Agent Tesla, a well-established Remote Access Trojan (RAT) and credential stealer, emerged as the most active malware across Africa in March 2025, disrupting both enterprise operations and individual users at scale.

Operational since 2014, Agent Tesla continues to dominate phishing campaigns, leveraging malicious attachments for credential theft, cyber espionage, and unauthorized system access. Its commercialization through a Malware-as-a-Service (MaaS) model ensures accessibility for a wide range of threat actors, driving its persistent relevance.

Operational since 2014, Agent Tesla continues to dominate phishing campaigns, leveraging malicious attachments for credential theft, cyber espionage, and unauthorized system access. Its commercialization through a Malware-as-a-Service (MaaS) model ensures accessibility for a wide range of threat actors, driving its persistent relevance.

According to Check Point's 2025 Cybersecurity Report, Agent Tesla ranked among the top 10 malware variants globally in 2024, compromising 6.3% of corporate networks. Its 22% year-over-year growth underscores its evolving capabilities and its effectiveness in evading traditional defenses.

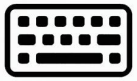
Strategic Impact Across Africa

Agent Tesla is increasingly destabilizing critical sectors across the continent, driving both financial and operational risk:

- Nigeria: Threat actors are systematically weaponizing Agent Tesla to harvest banking credentials, manipulate financial systems, and perpetrate fraud. Phishing vectors remain the preferred entry point, enabling cybercriminals to infiltrate financial institutions and monetize stolen data via underground markets.
- South Africa: Enterprises face elevated risk profiles as Agent Tesla targets cloud-based applications and corporate communication platforms. Credential harvesting has led to notable data breaches, intellectual property loss, and a surge in financially motivated cyberattacks.
- Kenya: Mobile platforms have become primary targets. Cybercriminals are exploiting mobile banking and payment systems, exfiltrating data from email clients, browsers, and clipboard applications. Advanced evasion tactics allow Agent Tesla to persist undetected, intensifying the risk for both individuals and SMEs.

Operational Mechanics of Agent Tesla

Agent Tesla is engineered for precision credential theft and remote system control. Core capabilities includ



Keylogging and screenshot capture

Credential theft across 50+ applications

Clipboard monitoring

Payload execution

Exfiltrated data is transmitted through multiple channels, HTTP, SMTP, FTP, and encrypted Telegram communications—maintaining persistent control over compromised environments.

It is primarily propagated through phishing emails containing malicious Office documents or disguised executables, exploiting known vulnerabilities such as CVE-2017-11882 and CVE-2018-0802 to execute remote code.

Agent Tesla's defense evasion tactics are sophisticated: it employs code obfuscation (Base64 encoding, XOR encryption, steganography), detects sandbox environments and debugging tools, and bypasses AMSI protections by injecting into legitimate Windows processes such as RegAsm.exe and RegSvcs.exe. Encrypted command-and-control (C2) channels further complicate detection and remediation.

Strategic Mitigation Framework (Recommendations by Ethnos Cyber)

Organizations must pivot to a proactive cybersecurity posture, integrating the following control measures:

- Patch Management: mmediate patching of vulnerabilities including CVE-2017-11882, CVE-2018-0802, and CVE-2024-3400 to eliminate high-risk attack vectors.
- Advanced Email Security: Implement AI-driven anti-phishing solutions with sandbox analysis to intercept and neutralize malicious payloads pre-delivery.
- Endpoint Protection: Deploy robust EDR platforms capable of detecting AMSI bypasses, process injections, and unauthorized credential access in real time.
- Multi-Factor Authentication (MFA): Enforce MFA across all access points to mitigate risks associated with compromised credentials.
- User Awareness Training: Deliver ongoing cybersecurity education initiatives tailored to Africa's most targeted sectors, focusing on phishing resistance and incident escalation protocols.

Final Thoughts

Agent Tesla's resurgence in Africa is not simply a technical threat, it is a strategic risk. Organizations must evolve from reactive defense to proactive threat management, combining real-time intelligence, layered security controls, and continuous user education to neutralize its impact and safeguard operational continuity.

Strategic Outlook & Recommendations

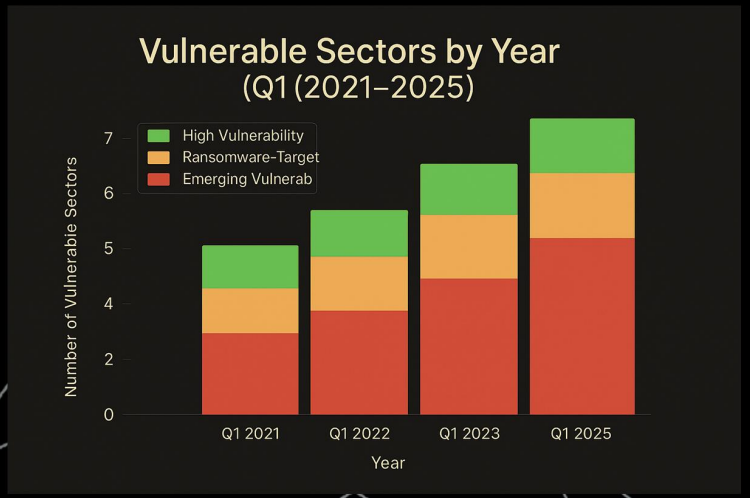
Building on the data and case studies, this final section tracks how vulnerability profiles are evolving across sectors and anticipates emerging risks for the next quarter. It distills our conclusions into forward-looking insights. A curated list of best practices and resilience measures provides a clear roadmap for strengthening defenses before the next reporting cycle.

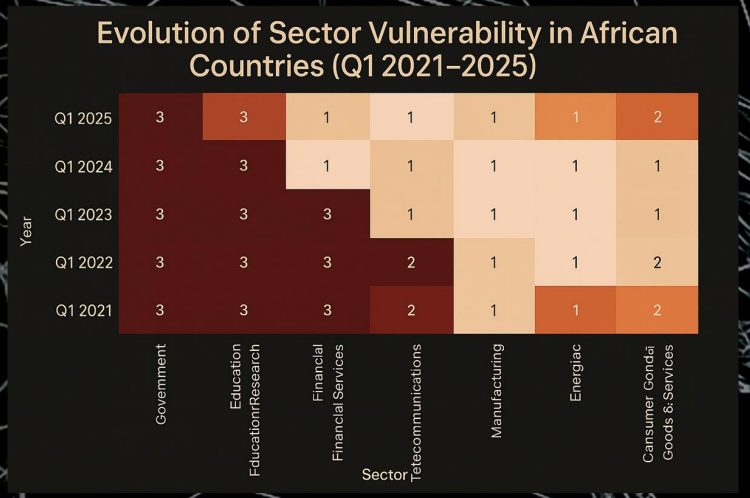
Evolution of Vulnerable Sectors

The most vulnerable sectors in African countries have shown some consistency over the period from Q1 2021 to Q1 2025, with certain sectors facing persistent threats while others have seen increased targeting. In Q1 2021, the government sector was identified as highly vulnerable to overall cyber-attacks, while the food-and-beverage and manufacturing sectors were specifically targeted by ransomware.

By Q1 2022, global trends suggested that the Education/Research sector was becoming increasingly vulnerable. This trend continued into Q1 2024 and Q1 2025, with the Education sector constantly appearing as one of the most attacked globally. The government and financial organizations remained primary targets throughout Q1 2023, and this trend extended into Q1 2024 and Q1 2025, with the telecommunications sector also showing significant vulnerability.

Notably, critical infrastructure, particularly energy and telecommunications, remained at risk throughout, and the Consumer Goods & Services sector emerged as a significant target for ransomware in Q1 2025. This evolution indicates a persistent threat to core government and financial services, a growing risk for the education sector, and an increasing focus on critical infrastructure and consumer-facing industries in later years.





Conclusion and Strategic Outlook

Africa's cyber threat landscape in Q1 2025 underscores an urgent reality: cyber risk is no longer peripheral, it is central to national security, economic growth, and societal trust. As threat actors grow more sophisticated, leveraging AI, RaaS platforms, and regional conflict dynamics, African nations and industries must adopt a fundamentally proactive, intelligence-driven cybersecurity model.

Recommendations for Regional Resilience

To achieve meaningful cybersecurity resilience, African organizations and governments must adopt a comprehensive, forward-thinking playbook:

- Strengthen Cybersecurity Governance: Elevate cybersecurity to a board-level and national security priority. Enforce cybersecurity regulations and frameworks aligned to global standards.
- Accelerate Zero Trust Adoption: Implement identity-centric security architectures across public and private sectors to mitigate insider and external threats.
- Invest in AI-Powered Defense Mechanisms: Deploy AI for threat detection, predictive analytics, anomaly identification, and rapid incident response.
- Enhance Critical Infrastructure Protection: Secure IT-OT convergence points, deploy industrial-grade cybersecurity measures, and harden legacy systems.
- Expand Regional Intelligence Sharing: Build real-time cross-border threat intelligence networks through public-private partnerships and regional CERT (Computer Emergency Response Team) collaborations.
- Prioritize Human Factor Mitigation: Launch aggressive, culturally tailored cybersecurity awareness programs targeting phishing, mobile threats, and insider risk behaviors.
- Strengthen Mobile Ecosystem Security: Apply end-to-end encryption, mobile application hardening, and mobile endpoint detection technologies.

REFERENCES

- https://www.globenewswire.com/news-release/2025/02/25/3032261/0/en/Ponemon-Cybersecurity-Report-Insider-Risk-Management-Enabling-Early-Breach-Detection-and-Mitigation.html
- https://ponemon.dtexsystems.com/
- https://ghana.dubawa.org/the-state-of-cybersecurity-and-crime-in-ghana/
- https://www.itedgenews.africa/check-point-software-q1-2025-global-cyber-attack-report-africa-most-targeted-region/
- https://businessday.ng/technology/article/nigerian-organisa-tions-recorded-4388-attacks-per-week-in-q1-check-point/
- https://techpoint.africa/news/african-countries-cyber-attacks/
- https://www.knowbe4.com/hubfs/Africa-Annual-Survey_Whitepaper_US_EN-F.pdf
- https://www.interpol.int/News-and-Events/News/2025/More-than-300-arrests-as-African-countries-clamp-down-on-cyber-threats#:~:text=The%20arrests%20were%20made%20as%20part%20of,cause%20significant%20harm%20to%20individuals%20and%20businesses.&text=%E2%80%9CThe%20success%20of%20Operation%20Red%20Card%20demonstrates,have%20devastating%20effects%20on%20individuals%20and%20communities.
- https://www.moroccoworldnews.com/2025/04/189655/algerian-hackers-target-moroccan-employment-ministrys-database/
- https://en.yabiladi.com/articles/details/163635/cyber-retaliation-moroccan-group-strikes.html
- https://arbiterz.com/nigeria-leads-africa-in-cybercrime-arrests-interpols-operation-red-card-busts-306-suspects/
- https://www.bitdefender.com/en-au/blog/businessinsights/funksec-an-ai-centric-and-affiliate-powered-ransomware-group
- https://www.scworld.com/news/funksec-ransomware-chases-notoriety-with-ai-assisted-code
- powered-by-ai/
- https://www.broadcom.com/support/security-center/protection-bulletin/funksec-ransomware
- https://fintechmagazine.africa/2025/02/17/nigeria-faces-rising-cybersecurity-threats-in-2025-csean-report-warns-of-crypto-scams-and-ai-powered-attacks/
- https://global.ptsecurity.com/analytics/cybersecurity-threatscape-for-african-countries-q1-2023-q3-2024
- https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2025-threat-report-ot-cyberattacks-with-physical-consequences/
- https://www.cm-alliance.com/cybersecurity-blog/january-2025-recent-cyber-attacks-data-breaches-ransomware-attacks
- https://www.rapid7.com/blog/post/2025/04/08/2025-ransomware-business-as-usual-business-is-booming/
- https://www.trendmicro.com/vinfo/us/security/news/-threat-landscape/trend-2025-cyber-risk-report
- https://www.checkpoint.com/security-report/
- https://techcentral.co.za/south-africa-business-cyber-risk-in-2025/258552/
- https://adf-magazine.com/2025/02/south-africa-faces-increased-cyberattacks-against-government-agencies/
- https://africacenter.org/programs/cyber/
- https://www.bankinfosecurity.com/whitepapers/2025-ransomware-report-what-q1-trends-reveal-about-year-ahead-w-14970
- https://www.dcvelocity.com/tech-infrastructure/technology/ransomware-attacks-by-hackers-jumped-in-q1
- South Africa's government-run weather service knocked offline by cyberattack, accessed April 16, 2025, https://therecord.media/south-african-weather-service-cyberattack
- https://sosransomware.com/en/cybersecurity/top-10-ransomware-groups-for-january-2025/
- https://www.zawya.com/en/economy/global/bfsi-security-summit-2025-to-address-rising-cybersecurity-threats-in-africas-financial-sector-reawenon
- https://www.zawya.com/en/press-release/africa-press-releas-

CONTACT US

Chat Us on Whatsapp

Enquiries: secure@ethnoscyber.com | **Sales:** bizdev@ethnoscyber.com

To learn more about our solutions and services, visit www.ethnoscyber.com