Africa Cyberthreat Landscape Report

2025

kaspersky bring on the future

kaspersky.com

Contents

Intro

Africa's rapid digital expansion has brought significant opportunities, but it has also exposed the continent to a growing array of cyberthreats. Recent incidents, affecting critical sectors across multiple countries, highlight the challenges facing the region's cybersecurity landscape.

- In June 2023 BGFIBank Gabon was targeted by the Bianlian ransomware group[1]. The attackers stole sensitive commercial data, showcasing the threat to Africa's financial sector. This breach disrupted banking services and raised concerns about data security in Central Africa.
- In December 2024, the National Bureau of Statistics (NBS) in Nigeria was attacked[2]. The agency's website was compromised and displayed a blank page with the message "Page Hacked." NBS confirmed the attack and assured the public that efforts were underway to restore the website and secure it.
- In South Africa, a media personality and actress Shashi Naidoo recently fell victim to a mugging, resulting in the loss of a cellphone and more than R500 000. Maher Yamout, lead security researcher at Kaspersky, suggested that the attackers were most likely able to find out the smartphone's passcode using various methods[3].
- Another example is Kenya's e-citizen portal getting crippled by a distributed denial-of-service (DDoS) attack in 2023, halting access to public services[4]. This incident affected government operations and citizens' daily lives, marking it as a notable assault on national infrastructure.

These and other cases reflect the diverse and severe cyberthreats targeting Africa's financial, governmental, and telecom sectors, driven by both local and international actors exploiting the region's rapid digital growth.

In this report we will take a closer look at the situation with the cybersecurity landscape in Africa.

Kaspersky data shows that for businesses on the African continent the number of web threat detections increased from 2023 to 2024. Apart from that, there was a 14% growth in spyware attack detections on businesses in the African region in 2024 compared to 2023. Most often corporate users from organizations in the spheres of manufacturing, finance, agriculture, education and government organizations were targeted.

[1] Cyberattaque contre la BGFIBank : la liste des fichiers volés désormais en accès sur internet (https://cybersecuritymag.africa/cyberattaque-bgfibank-liste-fichiers-voles-internet)

[2] Major Cyber Attacks in Africa's Top organizations in 2024 (https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024/)

[3] Inside Shashi Naidoo's costly mugging nightmare: Phone stolen, bank accounts drained of over R500k (https://www.news24.com/life/lifestyle-trends/inside-shashi-naidoos-costly-mugging-nightmare-phone-stolen-bank-accounts-drained-of-over-r500k-20241101)

[4] Anonymous Sudan DDoS cyberattacks cripple Kenya's new e-Citizen digital infrastructure (https://www.techmonitor.ai/technology/cybersecurity/anonymous-sudan-kenya-ddos-cyberattack-ecitizen)

A snapshot of general cyberattack vectors

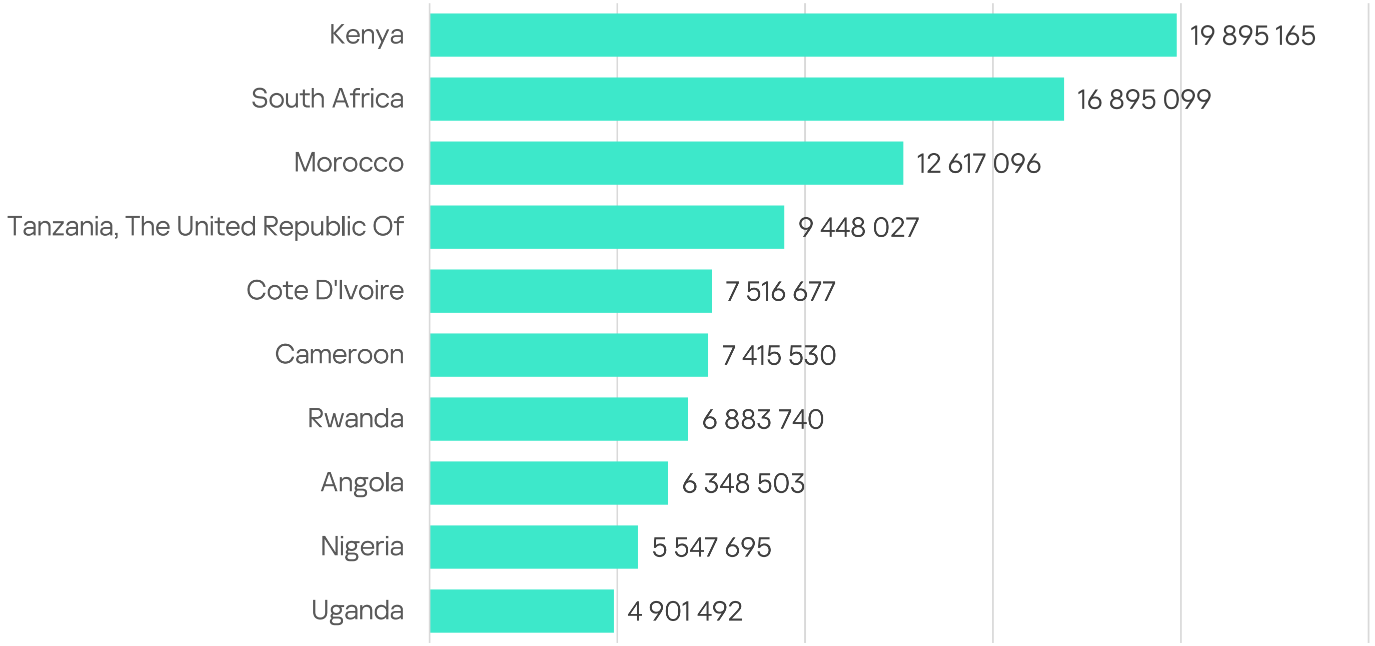
According to Kaspersky data, there were 131 580 587 web threats detected in 2024 in the African region for both corporate and individual users.

This data comes from Kaspersky Security Network (KSN)[9]. It is designed to receive and process complex global cyberthreat data, transforming it into the actionable threat intelligence.

Web threats

Web-based threats, or online threats, are a category of cybersecurity risks that may cause an undesirable event or action via the internet. Web threats are not limited to online activity but ultimately involve the internet at some stage for inflicted harm.

- As of January 2024, Nigeria led with over 103 million internet users[5], followed by South Africa with 45.34 million[6], and Kenya with 22.71 million[7], according to DataReportal. Forecasts suggest a 51.79% increase in Africa's internet users from 2024 to 2029, reaching 1.1 billion by 2029[8], implying an annual growth rate of roughly 10-11%. Applying this to 2025, the continent's total could rise from approximately 646 million in 2024 to around 710-720 million.



Web threat detections in Africa (per country), 2024
(Data from Kaspersky Security Network)

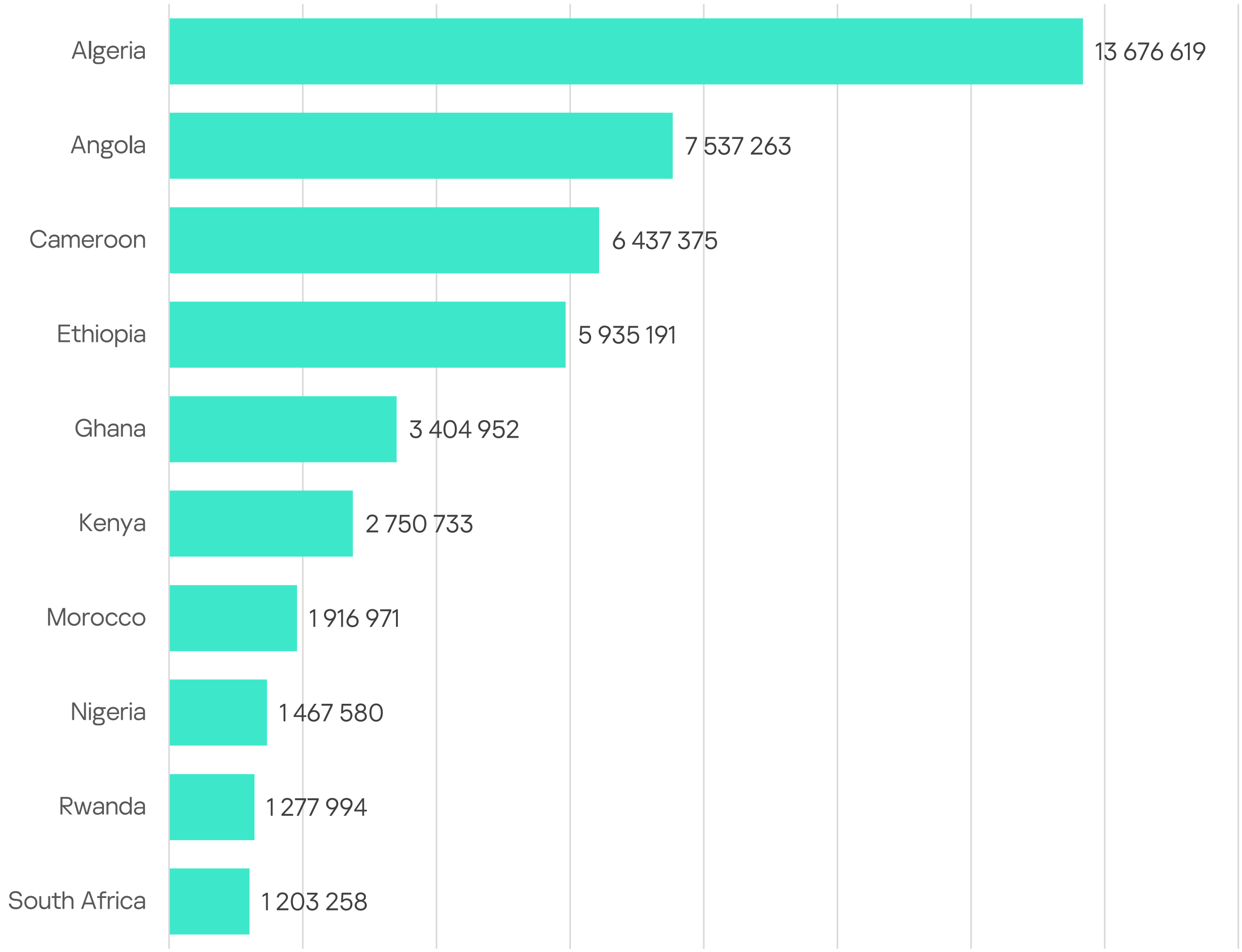
South Africa and Kenya, with their substantial internet user bases and advanced digital ecosystems, face frequent attacks, while Cameroon and Rwanda, though smaller in user numbers, experience rising threats due to increasing connectivity, making them attractive targets for cybercriminals exploiting rapid digitalization.

[5] Digital 2024: Nigeria (https://datareportal.com/reports/digital-2024-nigeria)
[6] Digital 2024: South Africa (https://datareportal.com/reports/digital-2024-south-africa)
[7] Digital 2024: Kenya (https://datareportal.com/reports/digital-2024-kenya)
[8] Number of internet users in Africa as of January 2024, by country (https://www.statista.com/statistics/505883/number-of-internet-users-in-african-countries/)
[9] Learn more about KSN here: https://www.kaspersky.com/ksn

Phishing

Phishing is a type of Internet fraud that seeks to acquire a user's credentials by deception. It includes theft of passwords, credit card numbers, bank account details and other confidential information.

According to Kaspersky telemetry, there were over **66 million** phishing link clicks in the African region in 2024.



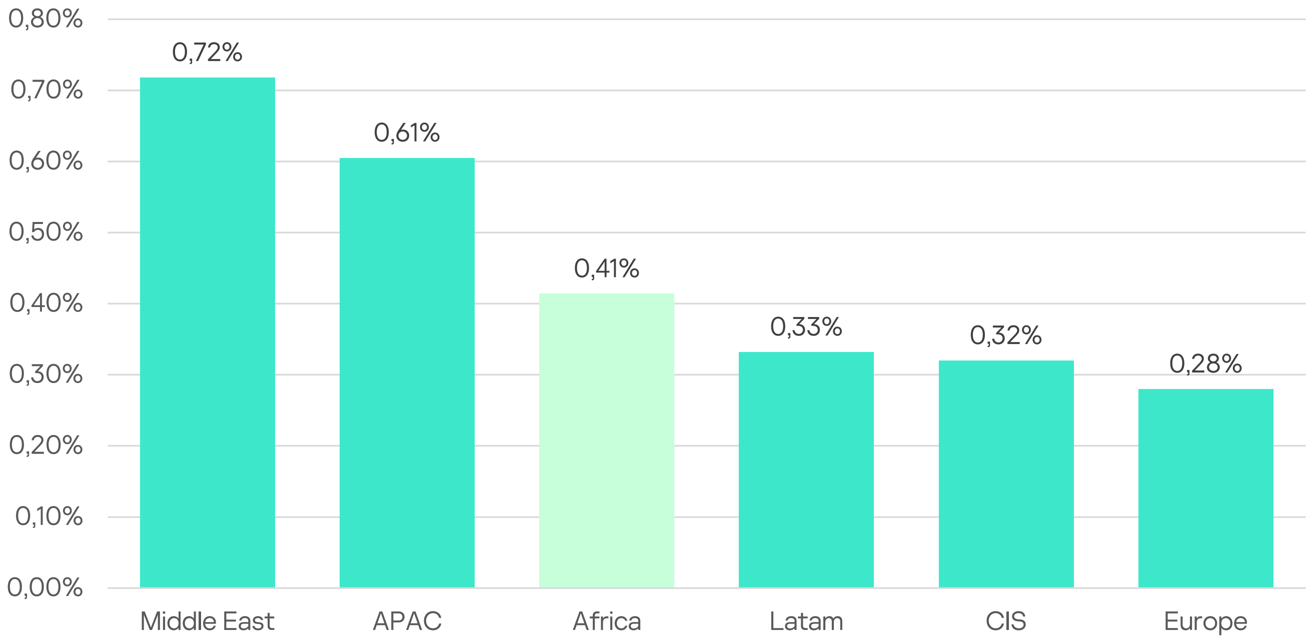
Phishing link clicks in Africa (per country), 2024
Data from Kaspersky Security Network

Ransomware

Ransomware is extortion software that can lock a user's computer and then demand a ransom for its release.

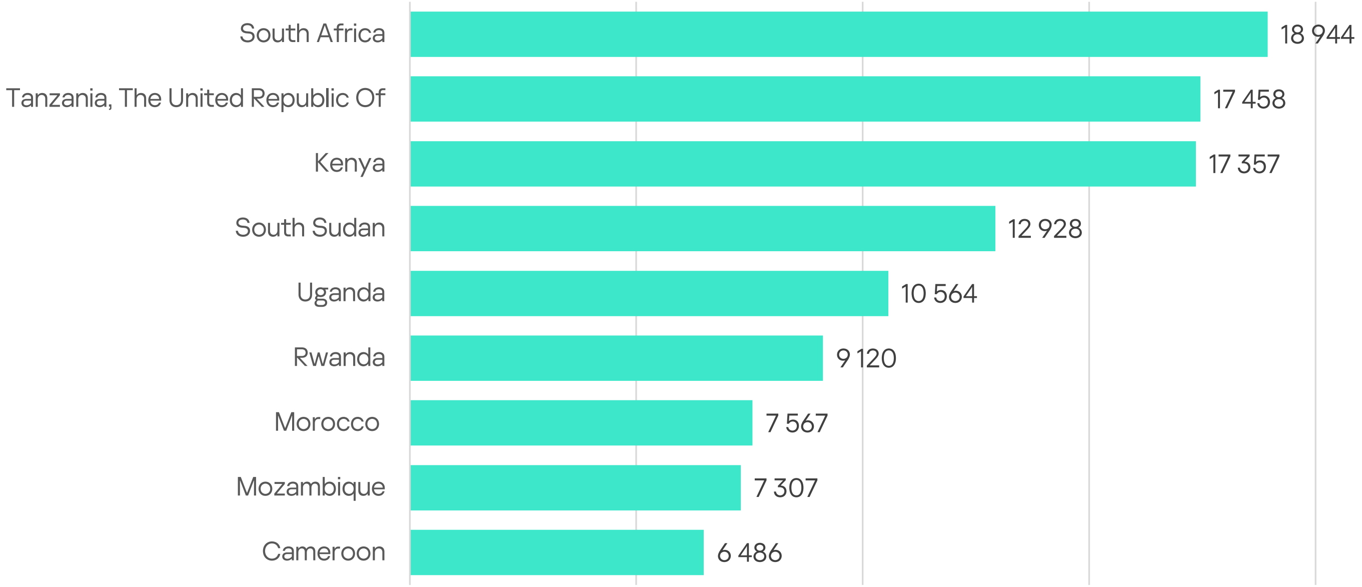
In Africa, ransomware emerged as one of the most serious and widespread types of cyberthreats, targeting infrastructure, financial institutions, and manufacturing facilities, among others.

Africa ranks 3rd among the world regions in terms of the share of users attacked with crypto-ransomware.



Share (%) of users attacked with ransomware, per world regions
Data from Kaspersky Security Network

Most often users in Africa were attacked by such specific crypto-ransomware families (not necessarily directly related to Ransomware-as-a-Service groups) as WannaCry, Stop/Djvu, PolyRansom/VirLock, Lockbit.

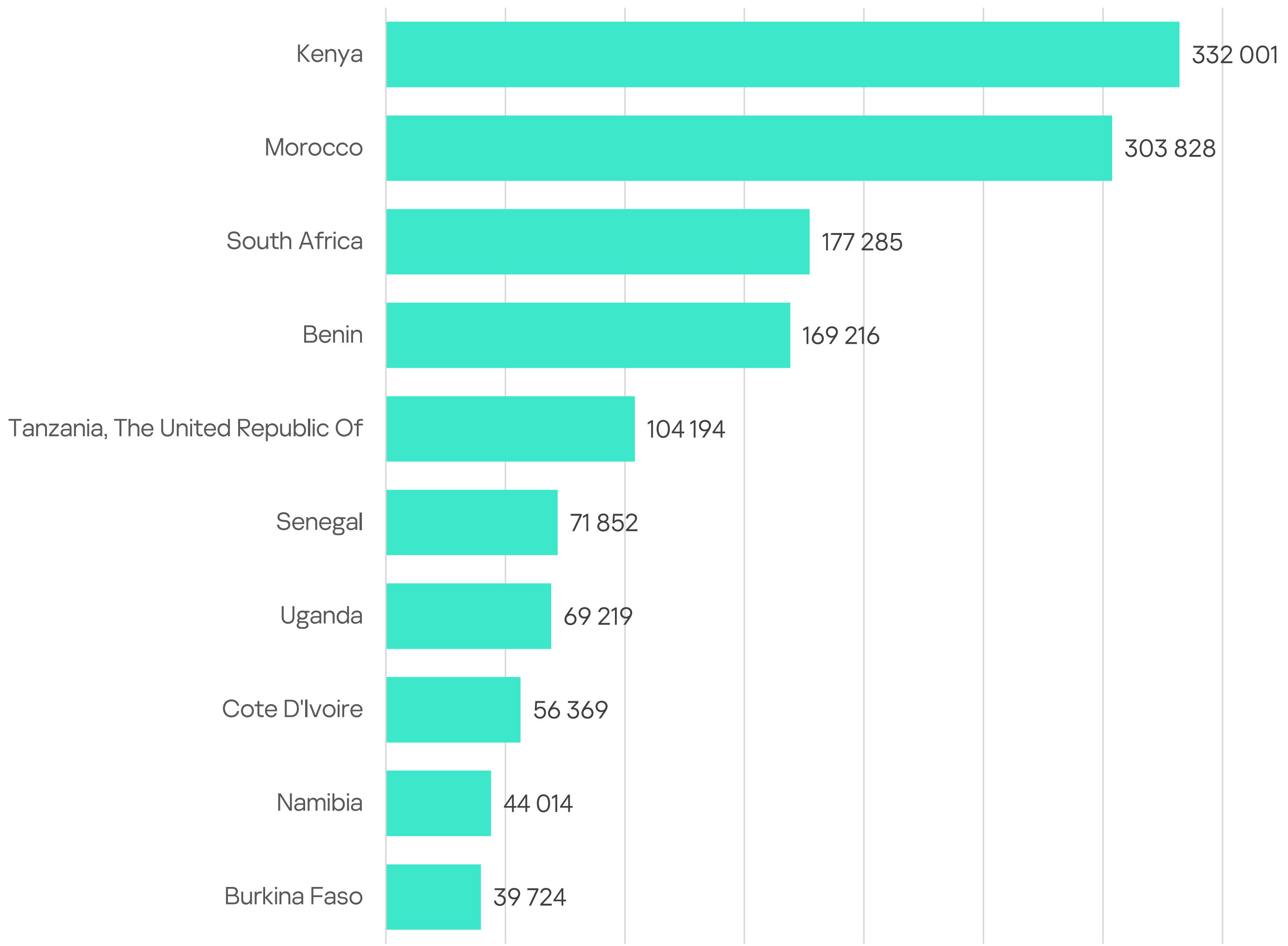


Ransomware detections in Africa (per country), 2024
Data from Kaspersky Security Network

Password stealers

Password stealers, a type of malware designed to harvest login credentials and other sensitive data, are a growing problem in the African region, where increasing internet adoption meets uneven cybersecurity defenses.

According to Kaspersky's telemetry, there were **1 424 291** password stealer detections in the African region in 2024, a 26% increase compared to 2023.

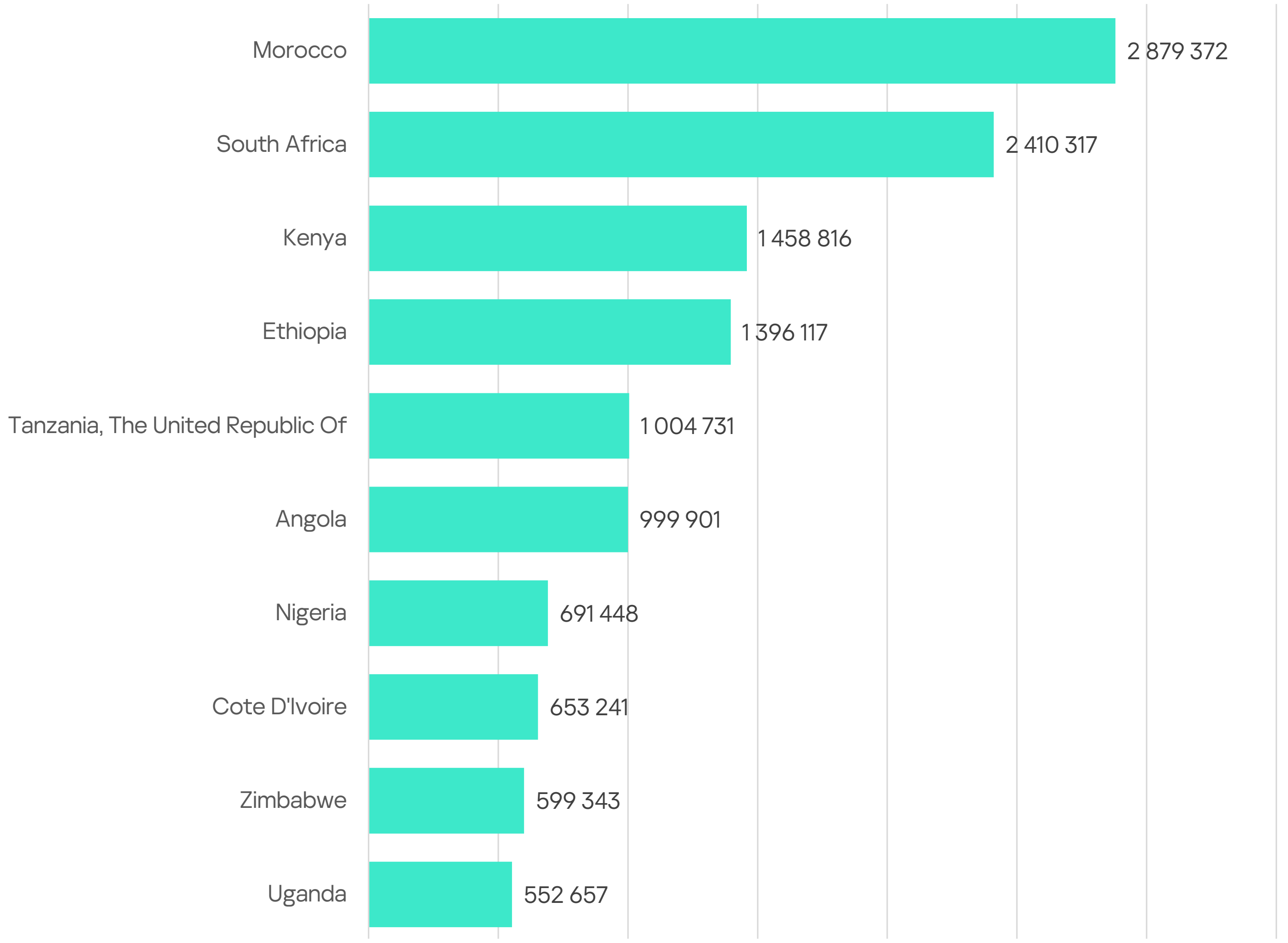


Password stealer detections in Africa (per country), 2024
Data from Kaspersky Security Network

How businesses in Africa were attacked

Web threats

According to Kaspersky data, businesses got targeted by web threats more often in 2024 than in 2023, with web threats detections increased by 1.2%. Rwanda, Zambia and Tanzania saw the largest increase in web threats year-on-year.

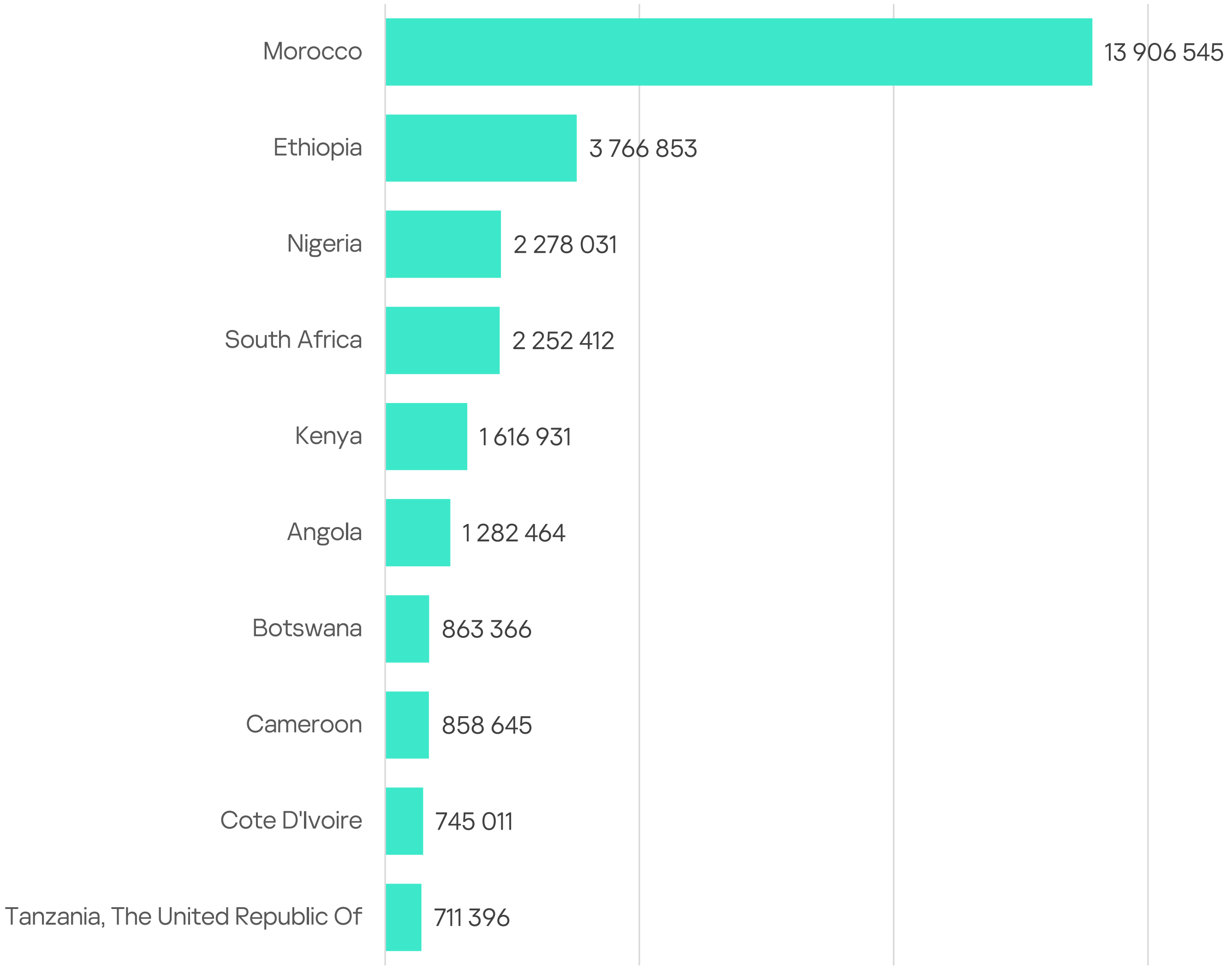


Web threat detections for businesses in Africa (per country), 2024
Data from Kaspersky Security Network

Local (on device) threats

Local threats include malware that is spread via removable USB drives, CDs and DVDs, or that initially makes way onto the computer in non-open form (for example, programs in complex installers, encrypted files, etc.).

According to Kaspersky telemetry, local (on device) threat detections in organizations in the African region in 2024 increased by 4% compared to 2023. Morocco, Nigeria, South Africa and Ethiopia were among the countries that saw the highest growth in local threats.

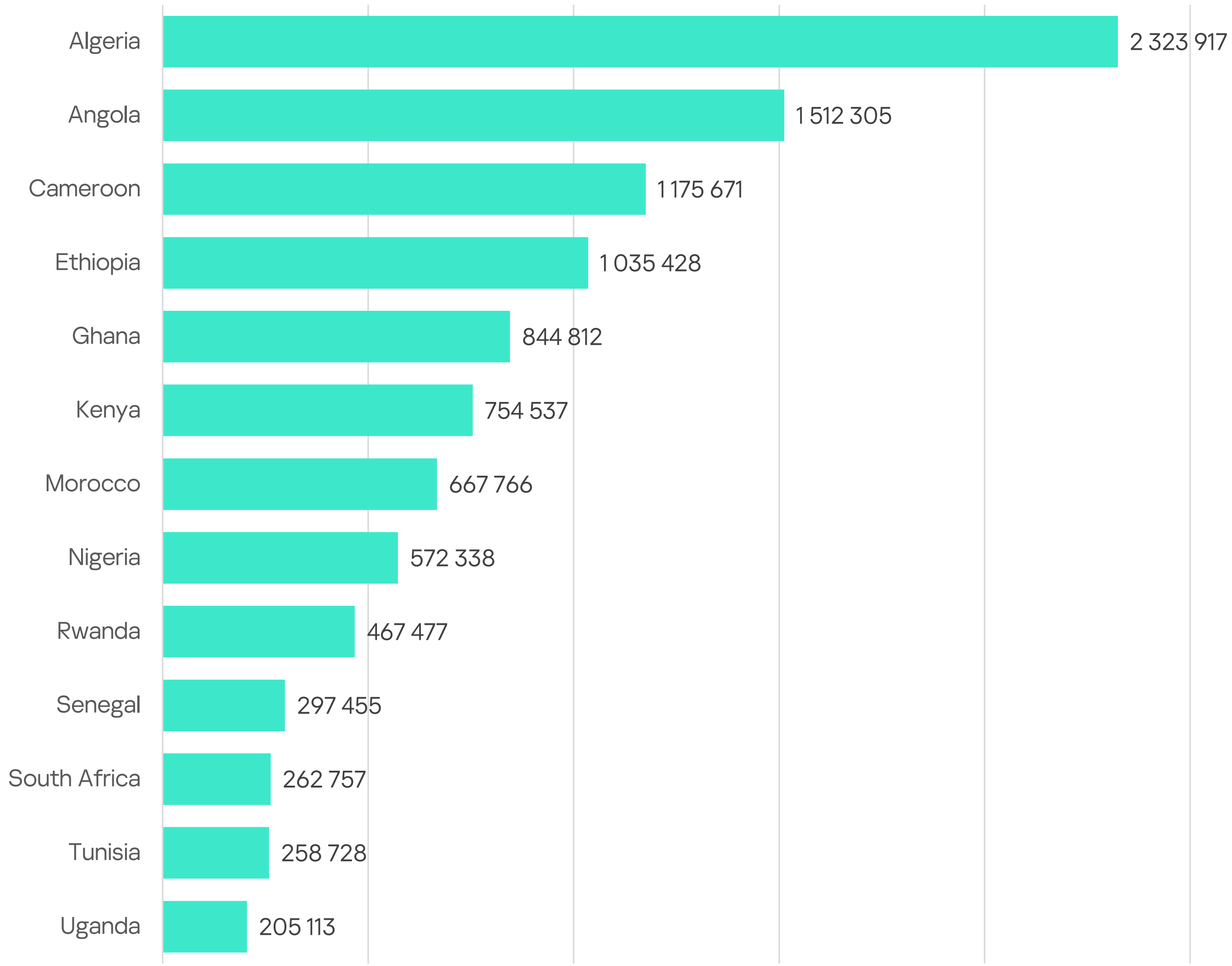


Local (on device) threat detections for businesses in Africa (per country), 2024
Data from Kaspersky Security Network

According to Kaspersky telemetry, there were over 14.8 million phishing link clicks by corporate users in the business sector in the African region in 2024.

Phishing

African countries are particularly susceptible to digital extortion, phishing and other online scams, such as business email compromise (BEC). A cyberattack method targeting both businesses and individuals by exploiting trusted relationships, BEC is on the rise across the continent and poses a significant threat to the financial sector. Although prior to 2023 these attacks were characterized by poor grammar and style, criminals now send far more convincing emails to potential victims in their native languages.



Phishing link clicks by corporate users in Africa (per country), 2024
Data from Kaspersky Security Network

Advanced Persistent Threats in the African region

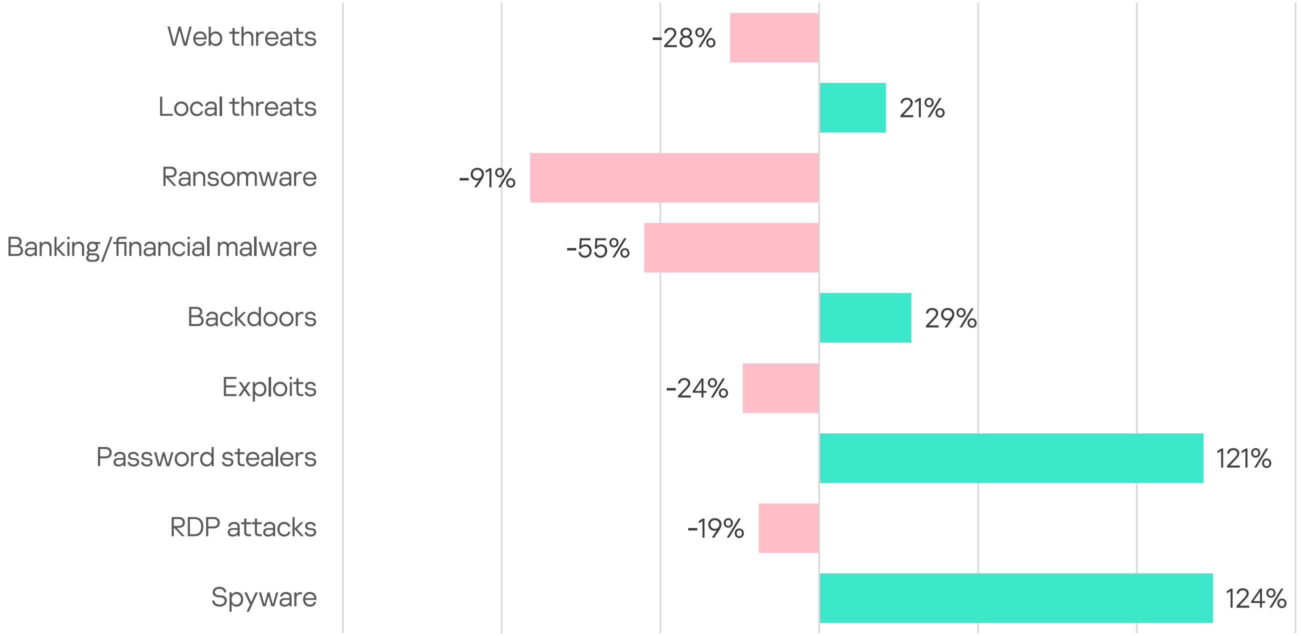
Advanced Persistent Threats (APTs) are sophisticated, long-term cyberattacks typically orchestrated by well-resourced groups, often state-sponsored or linked to large criminal organizations. Unlike traditional cyberattacks that aim for quick gains, APTs focus on stealthily infiltrating a network, remaining undetected for extended periods, and pursuing specific objectives such as espionage, data theft, or system sabotage. These attacks involve advanced techniques like custom malware, social engineering, and supply-chain exploitation, requiring significant planning and expertise to target high-value entities such as governments, corporations, and critical infrastructure.

In the African region, APT activity has been increasingly notable, with groups targeting sectors like government, energy, and telecommunications. There are several active APT actors in Africa as of 2024, with prominent groups such as MuddyWater, FruityArmor, and Sidewinder driving these efforts[10]. These actors employ diverse tactics, including spear-phishing, modular malware like DeadGlyph and StealerBot, and the weaponization of legitimate tools and cloud platforms to penetrate networks. The motivations often align with espionage, sabotage or financial gain, reflecting the continent's growing geopolitical and economic significance, which makes it an attractive target for such persistent threats.

[10] Kaspersky Intelligence on APT groups targeting Africa (https://www.kaspersky.co.za/about/press-releases/kaspersky-intelligence-shows-government-energy-and-telecommunication-institutions-as-main-targets-for-apt-groups-in-africa)

Trends for 2025

Africa's cyberthreat landscape in the first quarter of 2025 has shown a marked escalation compared to the same period in 2024, reflecting the region's deepening integration into the global digital economy and the corresponding rise in cybercriminal activity. In the business-to-business (B2B) sector, on-device (local) threat detections have surged by 21%, backdoor detections have risen by 29%, and password stealer detections have more than doubled. Spyware detections in this sector have also seen a near twofold increase. These shifts indicate a growing sophistication among attackers, who are increasingly trying to exploit unpatched systems, insider vulnerabilities, and the proliferation of remote work infrastructure across African organizations. The rapid adoption of cloud services and mobile devices in countries like South Africa and Nigeria, often without commensurate security upgrades, has widened the attack surface, enabling cybercriminals to deploy stealthier and more persistent threats.



Attack dynamics for businesses in the African region, Q1 2024 vs Q1 2025
Data from Kaspersky Security Network

The changes driving these increases are multifaceted. In the B2B sector, the shift toward hybrid work models and the rush to digitize operations—often outpacing cybersecurity investments—have left African businesses exposed to advanced persistent threats. In the B2C space, the explosion of digital financial services, coupled with low digital literacy rates, has made individuals prime targets for opportunistic attacks. Across both sectors, the use of artificial intelligence by cybercriminals to craft convincing phishing lures and automate malware deployment may amplify the scale and success of these campaigns. As Africa continues its digital transformation, these trends underscore the urgent need for enhanced security measures, from endpoint protection in businesses to public awareness campaigns for consumers, to counter a threat landscape that is evolving faster than the region's defenses.

Recommendations for protection

Cyber Awareness.

Boosting digital literacy is key to narrowing Africa's tech divide, especially with over 60% of its people under 25. Education campaigns must reach everyone but should zero in on the youth, weaving cyber hygiene into school and university curriculums. The private sector can pitch in by creating accessible training resources and running awareness drives. Equipping people with the know-how to spot and dodge online risks builds a stronger, safer digital culture across the region.

Skill Development.

Africa's digital boom has outpaced its supply of skilled defenders, leaving IT systems vulnerable to attacks from within and beyond the continent. To close this gap, there's a pressing need for robust training in cybersecurity, ethical hacking, and digital forensics. Governments and businesses could team up to boost law enforcement's expertise, offering hands-on programs like Kaspersky Expert Training. Expanding these efforts ensures a growing pool of pros ready to safeguard critical systems and outsmart evolving threats.

Strengthened Collaboration.

Effective teamwork among African stakeholders—policymakers, private companies, academics, and more—sets the stage for dismantling cybercriminal networks and stopping attacks in their tracks. This cooperation shines through in efforts like the African Cyber Surge II operation, launched in April 2023 and spanning four months across 25 countries. Kaspersky contributed by sharing critical data—indicators of compromise, malicious server details, fake IPs, and phishing links—with INTERPOL, while other law enforcement partners helped nab 14 suspects and expose the criminals' infrastructure. These wins highlight the power of unified action and could spark even deeper partnerships to tackle cybercrime head-on.

Africa's rising cyberthreats hit hard, undermining financial security for millions, yet they also open doors for progress. By rallying around shared goals — collaboration, skills, and awareness — the region can turn risks into momentum. A united front against cybercrime not only curbs losses but also paves the way for a more resilient digital future, driven by dialogue and action.

kaspersky

www.kaspersky.com