DARKTRACE

# ANNUAL THREAT REPORT 2026: AFRICA REGIONAL OUTLOOK

The global cyber threat landscape in 2025 was increasingly defined not by uniform trends, but by regional threat economies shaped by maturity, geopolitics, the speed of digitization, and attacker objectives. This regional breakdown provides a focused analysis of the key threat trends, notable threat actors, and outlook for Africa.

Africa's digital ecosystem is growing rapidly, but cyber threats are rising just as quickly, **with network-based attacks accounting for 76% of compromises detected** and ransomware increasing 60% year-over-year, likely due to Ransomware-as-a-Service (RaaS) operations [1].


Phishing remains the leading entry point at 43%, while the Finance (27%) and Energy (10%) sectors are the most targeted. Data exfiltration is also on the rise, observed in 25% of the cases Darktrace detected in the region.


Connectivity fragility, including recent subsea cable outages, further increases the impact of attacks during disruptions [1]. Cybercrime now accounts for over 30% of reported crime in some regions, with **scam activity rising by as much as 3,000%** in certain Afrian countries and causing significant economic losses, including USD 500m in Nigeria in 2022 and USD 83m in in 2023 [1, 2].

Many nations still lack fully operational Computer Security Incident Response Teams (CSIRTs), though initiatives such as ITU-INTERPOL cyberdrills aim to strengthen response capabilities [3], while generative AI is accelerating threat sophistication through automated and highly tailored phishing and reconnaissance.

## REGIONAL TRENDS AND STATISTICS

76% of compromises seen among Darktrace customers in Africa were network-based. 50% of those network-based attacks were ransomware-related, with around 60% year-on-year growth in ransomware between June 2024 and June 2025 compared with the same period in each of the prior three years.

Ransomware-related activity accounted for 39% of all incidents observed by Darktrace in Africa, with BlackCat (ALPHV) and RansomHub being the most active ransomware groups in the region. Finance and Energy were the most affected sectors, making up 27% and 10% of incidents respectively, while repeated targeting of Manufacturing and Education was also observed.

## NOTABLE THREAT ACTORS

| Actor | Motivation & Targets | Key Tactics |
|---|---|---|
| **BlackCat (Russian RaaS)** | Financially motivated; RaaS that targets large enterprises across sectors such as Healthcare, Manufacturing, and critical infrastructure. | **Defense Evasion** (TA0005)<br>**Lateral Movement** (TA0008) |
| **RansomHub (Russian RaaS)** | Financially motivated; RaaS that largely targets US-based organizations within the Manufacturing and Healthcare sectors. | **Initial Access** (TA0001),<br>**Execution** (TA0002<br>**Defense Evasion** (TA0005)<br>**Credential Access** (TA0006)<br>**Impact** (TA0040) |

**CASE STUDY: Vo1d botnet**

First seen in September 2024 by Darktrace [4], Vo1d began as a backdoor for sideloading apps on smart TVs and low-cost Android TV boxes, and later evolved into a multi-function threat for payload deployment, proxy services, and advertisement fraud. It uses XXTEA/RSA encryption [5] and a Domain Generation Algorithm (DGA) to sustain command-and-control (C2) servers even after takedowns [4].

**Whilst the botnet is global, spread across more than 200 countries and sustaining over 800,000 IPs daily [6], South Africa was heavily impacted in particular, with Darktrace detecting a high level of activity linked to Vo1d among South African customers.**

South Africa ranks among the hardest-hit regions, hosting 8.3% of affected IPs [7] and recording a 13.6% infection rate in early 2025. Victims spanned critical sectors such as Energy, Retail, Manufacturing, and Public Administration, highlighting the broad impact of this campaign.

External researchers believe infections stem from uncertified Android TV devices often sold on popular marketplaces or malicious apps disguised as legitimate tools. Google confirmed that affected devices were not Play Protect certified [8, 9], meaning they lacked security and compatibility checks.

This case highlights the importance of using certified hardware and software, enforcing regular patching, and taking measures to prevent exploitation of outdated or uncertified technology in critical environments. Additional steps such as network segmentation and egress controls (block unused high ports, monitoring DNS traffic for DGAs) and device controls such as, app allow listing/disabling sideloading, and isolation.

**CASE STUDY: React2Shell**

Darktrace observed multiple organizations across the African region affected by attackers exploiting CVE-2025-55812, known as React2Shell. This vulnerability in React server components enables an unauthenticated attacker to achieve remote code execution with a single request. Africa accounted for approximately one-third of all React2Shell-related activity detected globally by Darktrace, with impacted customers located in countries including Kenya and South Africa.

## GOVERNMENT & REGULATORY OVERVIEW

Africa's governments are advancing cybersecurity and data protection while preparing for AI regulation. South Africa enforces the Protection of Personal Information Act of 2013 (POPIA), which governs data privacy and breach notifications, and the Cybercrimes Act of 2020, and also introduced the National AI Policy Framework in 2024, expected to be implemented in stages over the next few years.

**Kenya** combines the Computer Misuse & Cybercrimes Act of 2018 and Data Protection Act of 2019 with its National Cybersecurity Strategy (2022–2027), and plans revisions to address AI misuse and critical infrastructure risks.

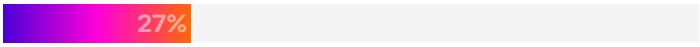
**Nigeria** mandates breach reporting under the Cybercrimes Act and strengthened privacy through the Data Protection Act (2023), with new sector-specific cybersecurity rules in development. Mauritius leads with General Data Protection Regulation (GDPR)-aligned-aligned data laws and the Cybersecurity & Cybercrime Act of 2021, and its proposed Blueprint for Mauritius 2025–2029 strategy  plans to update AI and cyber regulations and create an AI Office and a national cyber resilience agency.

## INSIGHTS & OUTLOOK

Phishing emails remain the leading cause of compromise in Africa, with 67% of Software-as-a-Service (SaaS) incidents originating from phishing, making up 16% of all initial access vectors observed by Darktrace in the region.

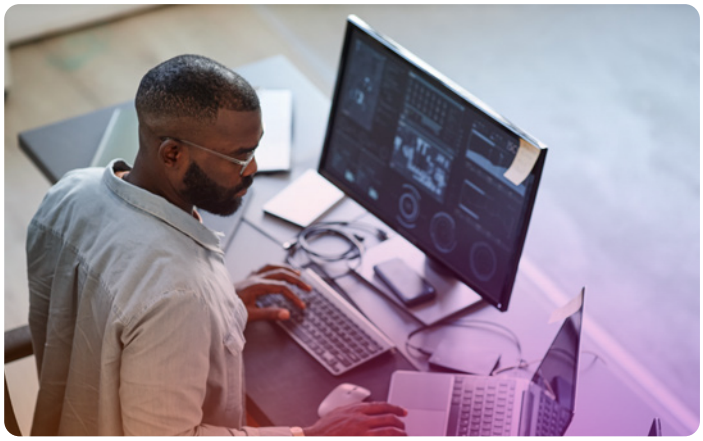

This trend is reinforced globally by the widespread availability of generative AI, which makes writing more convincing phishing emails much faster and more accessible.

VPNs and exposed internet-facing systems are also major attack vectors. One-third of known network-based intrusions involved VPN access, while 27% stemmed from exploited Common Vulnerabilities and Exposures (CVEs) and exposed services.




About 57% of identified ransomware strains were RaaS, representing half of all ransomware cases; the comparatively lower observed RaaS use in Africa may suggest more targeted, goal-driven intrusions rather than purely financial campaigns.


**Data exfiltration has also risen over the last three years, potentially reflecting pre-ransomware activity detected earlier in the kill chain.**



### REGIONAL ANALYSIS METHODOLOGY:

It is important to note that while the analysis is relevant and broadly representative of wider global trends, it is also influenced by the geographic distribution of Darktrace's customer base. For example, within the Americas (AMS) region, the US represents the largest share of Darktrace customers, meaning insights in this section may be weighted more heavily toward US-based activity.


[1] [Online]. Available: https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa.

[2] [Online]. Available: https://www.uneca.org/cybersecurity-for-development-in-the-fourth-industrial-revolution-research-report.

[3] [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Africa_GCIv2_report.pdf.

[4] [Online]. Available: https://www.darktrace.com/blog/unmasking-vo1d-inside-darktraces-botnet-detection .

[5] [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/23779497.2025.2532556?src=#d1e121 .

[6] [Online]. Available: https://thehackernews.com/2025/03/vo1d-botnets-peak-surpasses-159m.html .

[7] [Online]. Available: https://www.virusbulletin.com/uploads/pdf/conference/vb2025/papers/Vo1d-rising-inside-the-botnet-controlling-168M-Android-TVs-worldwide.pdf .

[8] [Online]. Available: https://mybroadband.co.za/news/broadcasting/596007-warning-for-south-africans-using-specific-types-of-tv-sticks.html.

[9] [Online]. Available: https://www.securityweek.com/vo1d-botnet-evolves-as-it-ensnares-1-6-million-android-tv-boxes/ .