AFRICA

Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

Executive Summary

Top Takeaways

- **Public sector and finance are key targets:** Dark web and phishing data show that government bodies and financial services remain top priorities for attackers due to sensitive information and monetary gain.

- **South Africa leads in exposure:** It records the highest share of both ransomware and phishing attacks, showing its position as the main cybercrime hub in Africa.

- **Data and access drive the dark web economy:** Nearly 70% of dark web threats involve stolen databases, and over 20% involve system access, showing a strong supply chain for large-scale attacks.

- **Ransomware landscape is fragmented:** Smaller groups dominate activity, with few established names like RansomHub or FunkSec standing out. This suggests experimentation rather than control by big global syndicates.

- **Phishing campaigns are professionalizing:** Over 80% of phishing sites now use HTTPS, making them harder to distinguish from legitimate platforms. Attackers also mix generic lures with targeted hooks like crypto wallets or messaging apps.

- **Regional concentration of phishing:** South Africa, Morocco, and Mauritius together account for over 80% of phishing incidents, highlighting their digital and financial importance.

- **Hybrid attacker motives:** Selling dominates dark web threats, but sharing also makes up nearly 40%, showing that reputation-building and community collaboration remain important in cybercriminal ecosystems.

Technical Details

This report based on data collected between September 2024 and September 2025

In the following chapters, you will be reading about the various aspects of the cyber threat landscape around the Africa region.

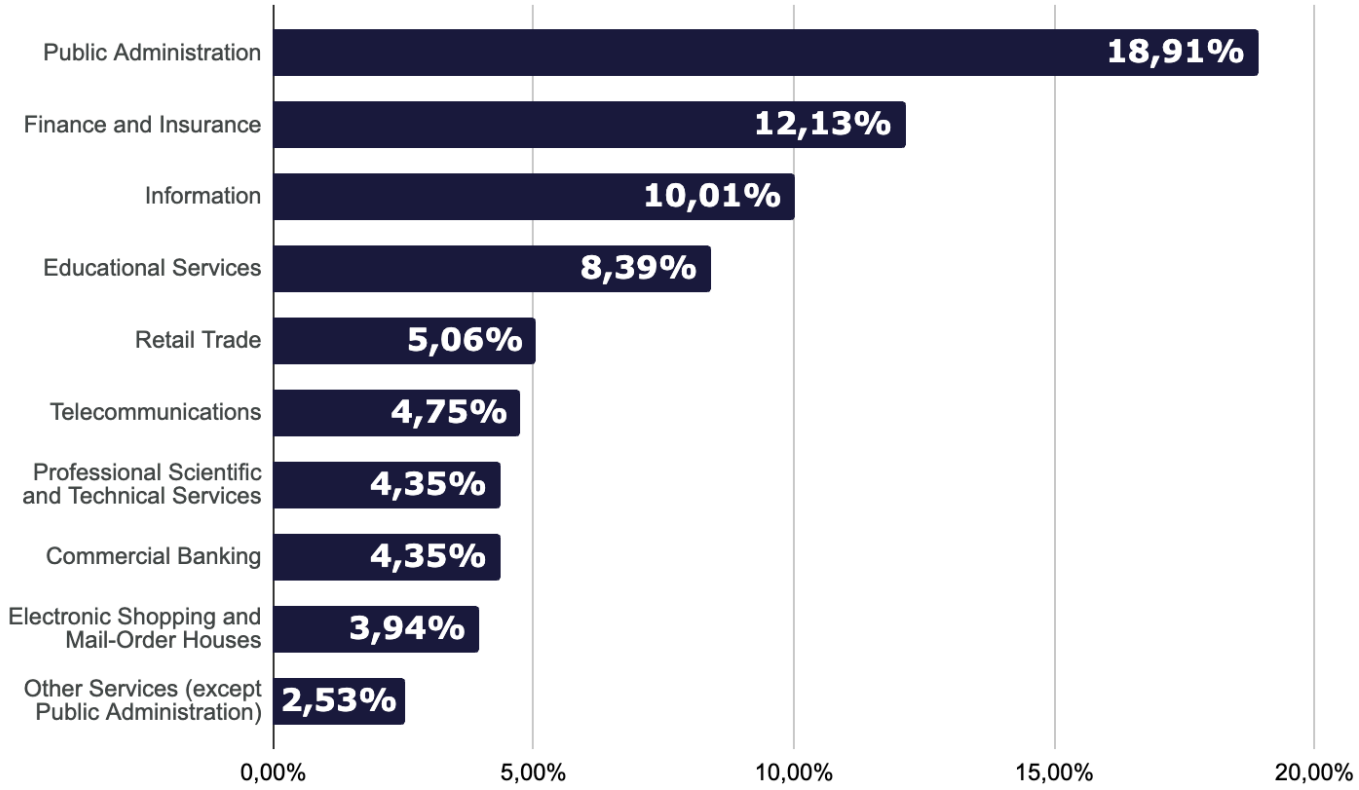
In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups and so on. These are areas where threat actors with various skill sets come together, discuss, share tools and publish their alleged cyber attacks.

In the Ransomware Threats chapter you will find detailed information about ransomware actors targeting the Africa region, their detailed profiles and the necessary data that summarizes the ransomware activities.

The Phishing Threats chapter will show you how threat actors target various organizations with fake websites. By examining the data here, you can take the necessary steps to prevent your employees from falling into threat actors' traps.

Dark Web Threats Targeting the Africa Region

Distribution of Dark Web Threats by Industry

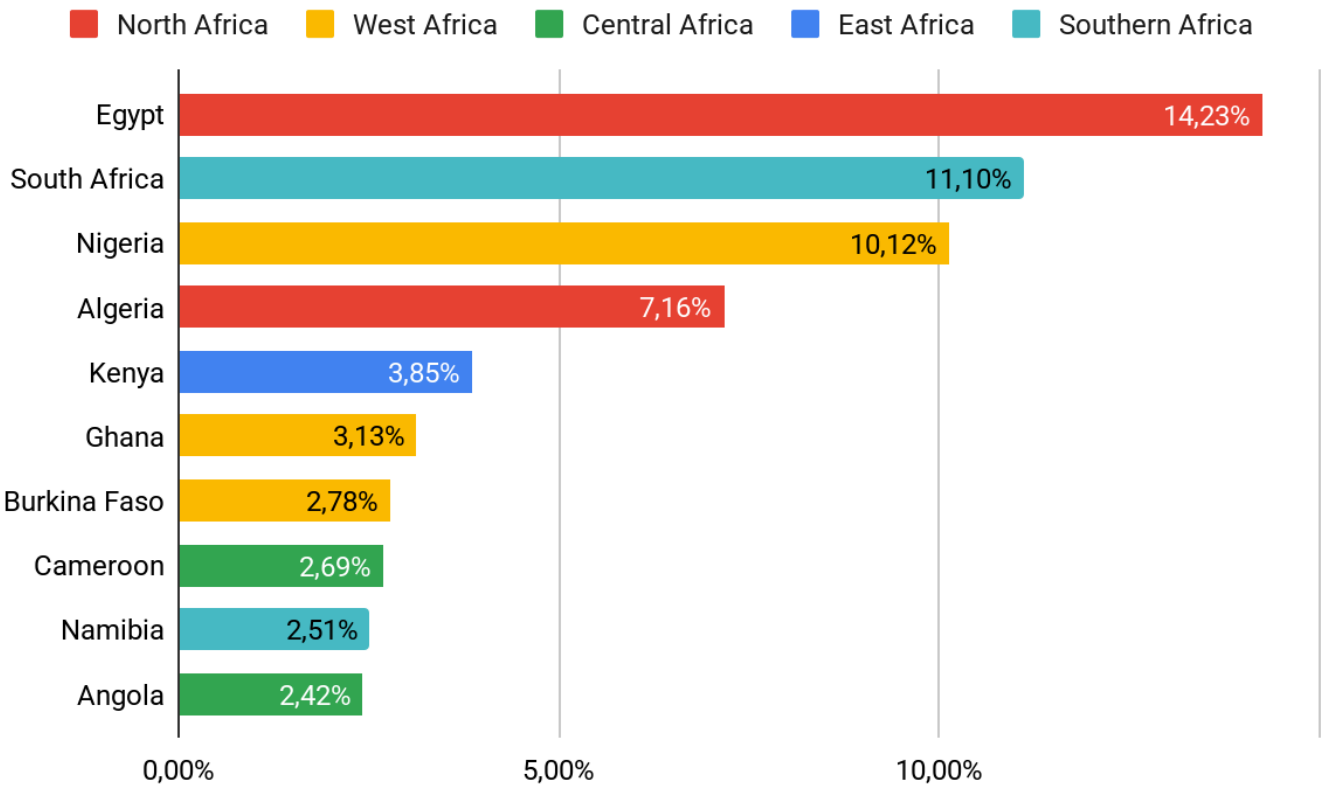


Public administration leads with almost 19% of observed dark web threats. This dominance shows how government bodies remain a primary target, likely due to the sensitive data they store and their role in critical infrastructure.

Finance and insurance follow at 12%, with commercial banking adding another 4%. Together, financial services account for a significant share, underlining the ongoing interest of cybercriminals in monetary gain and personal financial records.

The information sector holds 10%, reflecting the value of intellectual property and data-driven businesses.

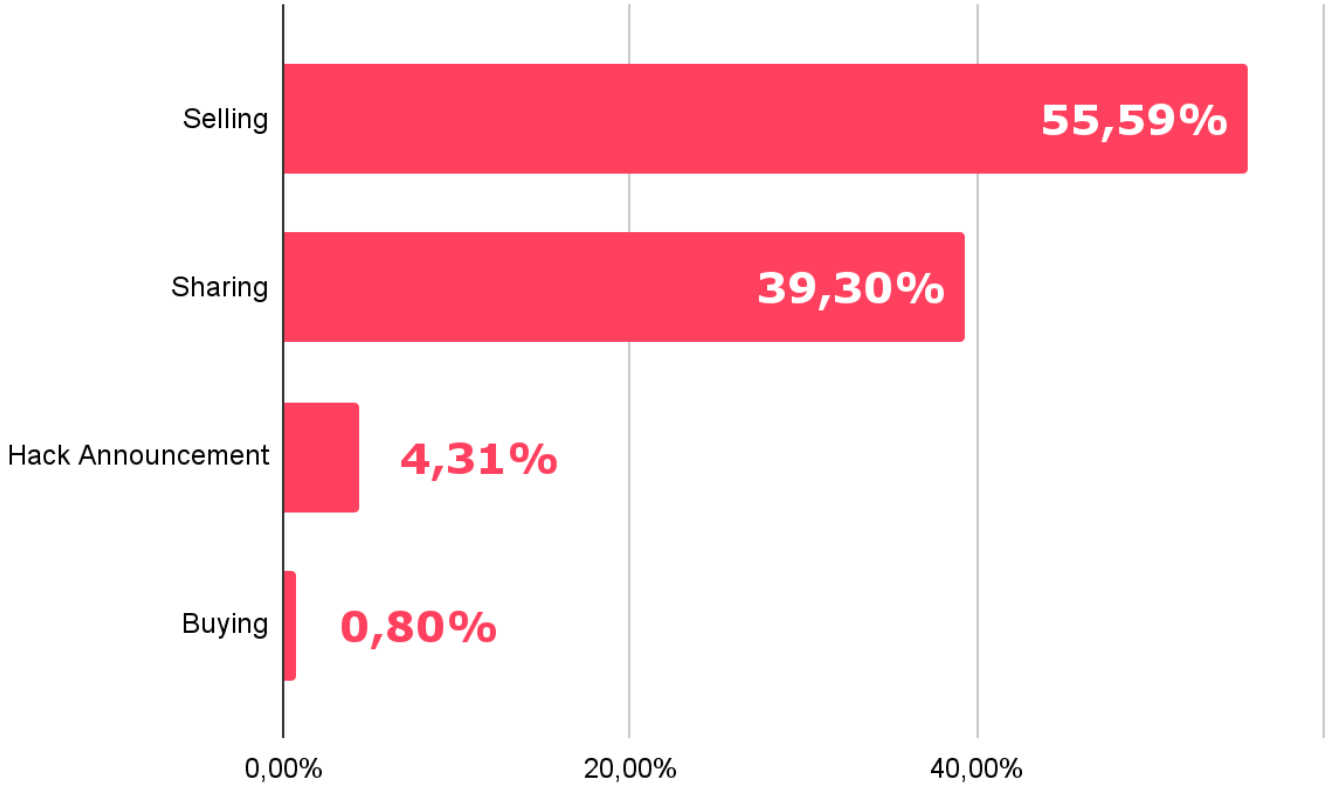
Distribution of Dark Web Threats by Target Country



Egypt ranks first with over 14% of reported dark web threats, making it the most exposed country in the region. South Africa (11%) and Nigeria (10%) follow closely, together forming a strong concentration of threat activity. These three countries stand out as primary targets, likely due to their larger economies, higher internet penetration, and more developed financial systems.

The data highlights that North, West, and Southern Africa face the highest levels of dark web threats, driven by economic hubs and population centers. Attackers appear to focus on countries with stronger digital infrastructure and higher-value targets, while smaller nations still face risks, even if at reduced volumes.

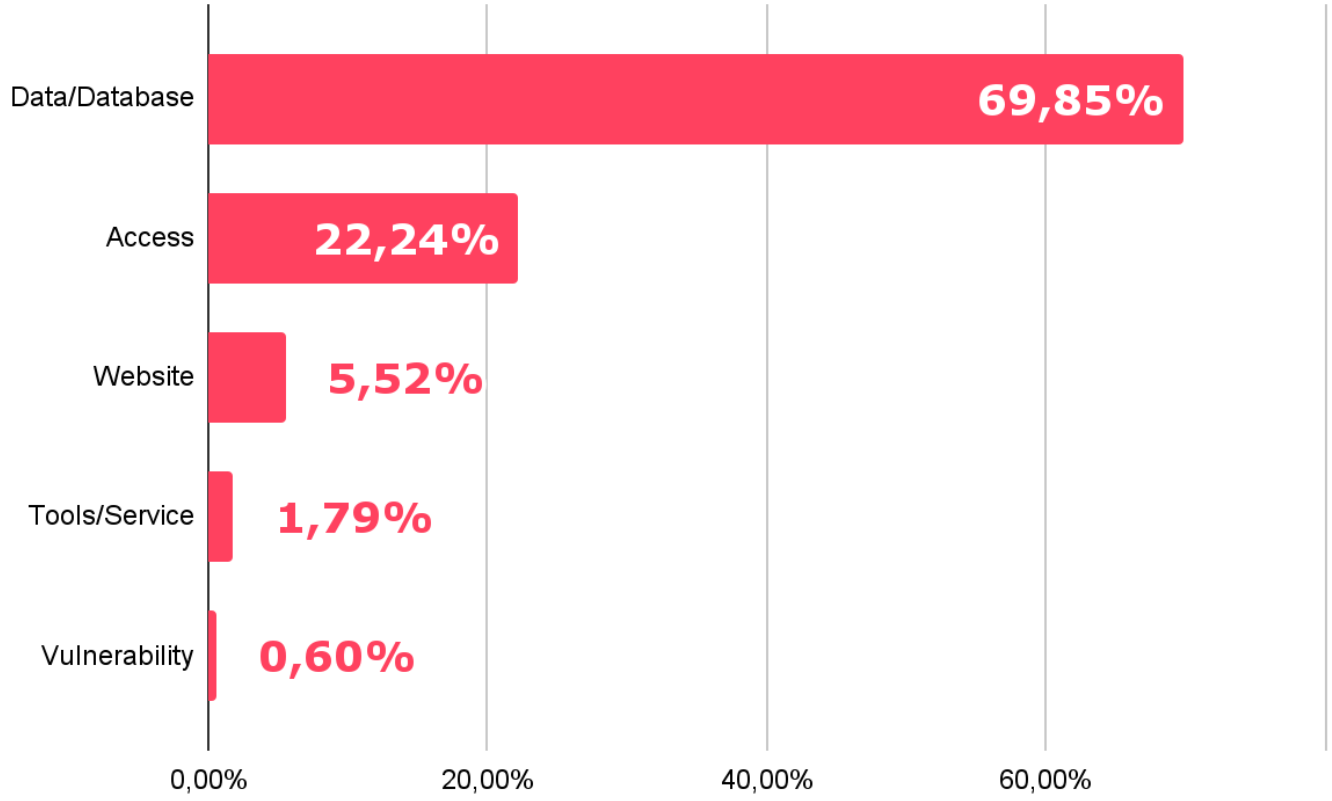
Distribution of Dark Web Threats by Threat Categories



Selling dominates the landscape with more than half of all activity (56%). This shows that dark web forums remain heavily driven by profit, with stolen data, credentials, and tools being traded. Sharing follows at 39%, which signals that threat actors still exchange information and resources freely, either to build reputation or to strengthen criminal communities.

The data suggests the dark web economy is supply-heavy, with actors focusing on monetization and influence through sales and information exchange. The balance between selling and sharing also points to a hybrid model where both profit and reputation fuel threat activity.

Distribution of Dark Web Threats by Threat Type



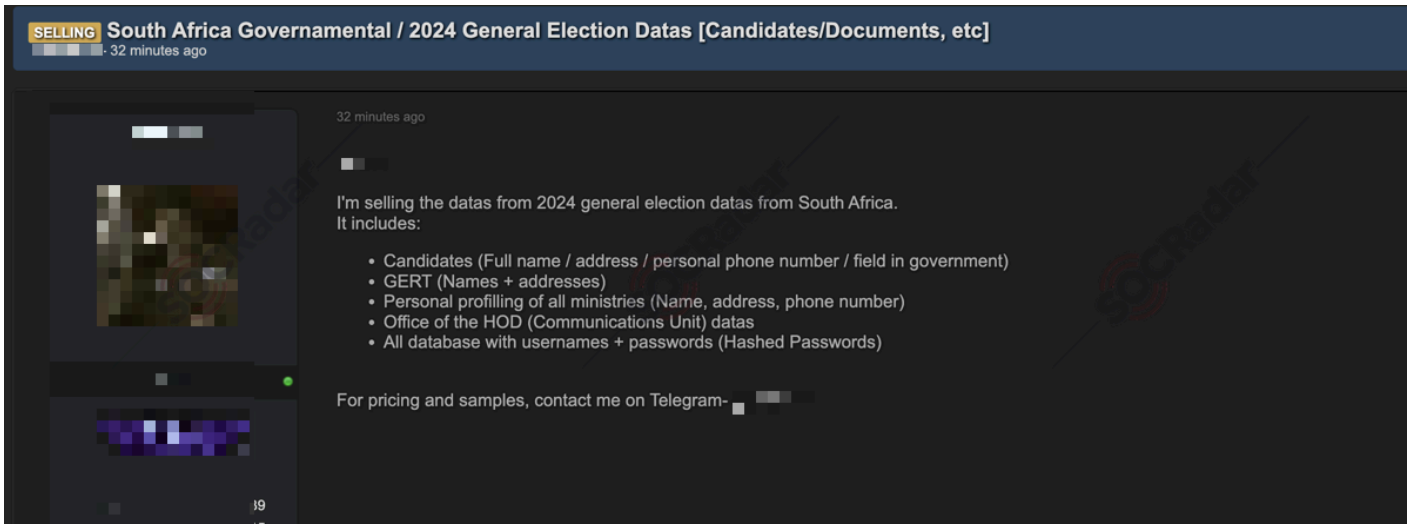
Data and databases dominate with nearly 70% of all threats, showing that stolen information is the main commodity on the dark web. This highlights the strong demand for personal, financial, and corporate records, which can fuel identity theft, fraud, or larger cyber operations.

Access comes next at 22%, pointing to a large market for direct entry into systems and networks. Selling access is often more valuable than single data leaks, as it gives attackers the ability to launch further intrusions or ransomware campaigns.

The figures show that the dark web threat landscape is primarily about exploiting stolen data and selling system access, both of which directly enable large-scale cybercrime.

Recent Dark Web Activities Targeting Entities in the Africa Region

Alleged South Africa 2024 Election Data Offered for Sale on a Dark Web Forum



A post on a Dark Web forum monitored by SOCRadar claims to be offering comprehensive data from South Africa's 2024 general election, including personal information.

The seller's listing states it includes: full names, home addresses and personal phone numbers for candidates and ministry staff; lists for GERT and communications units; profiling of ministries and offices of HOD (Communications Unit); and an "all database" of usernames and hashed passwords. The post invites interested buyers to request samples and pricing via Telegram.

Moroccan Accommodation Site Admin Access Offered for Sale on a Dark Web Forum

SOCRadar detected a forum post offering unauthorized admin panel and shell access to a Moroccan camp-glamping website.

The seller claims the site processes 1,135+ orders, mainly from cardholders in France, Morocco, and the UK, with payments handled via Payzone. The listing advertises access starting at 300, with a "blitz" price of 650 (24h).

In the context of underground forum auctions, a "blitz price" refers to a fixed buy-it-now amount. Instead of participating in incremental bidding (e.g., starting at 300 with steps of 50), an interested party can immediately secure the listing by paying the blitz price (in this case, 650).

Alleged Unauthorized VPN Access for Zimbabwean Power Company Detected

SOCRadar has observed a forum listing advertising alleged unauthorized VPN access to a Zimbabwean power company.

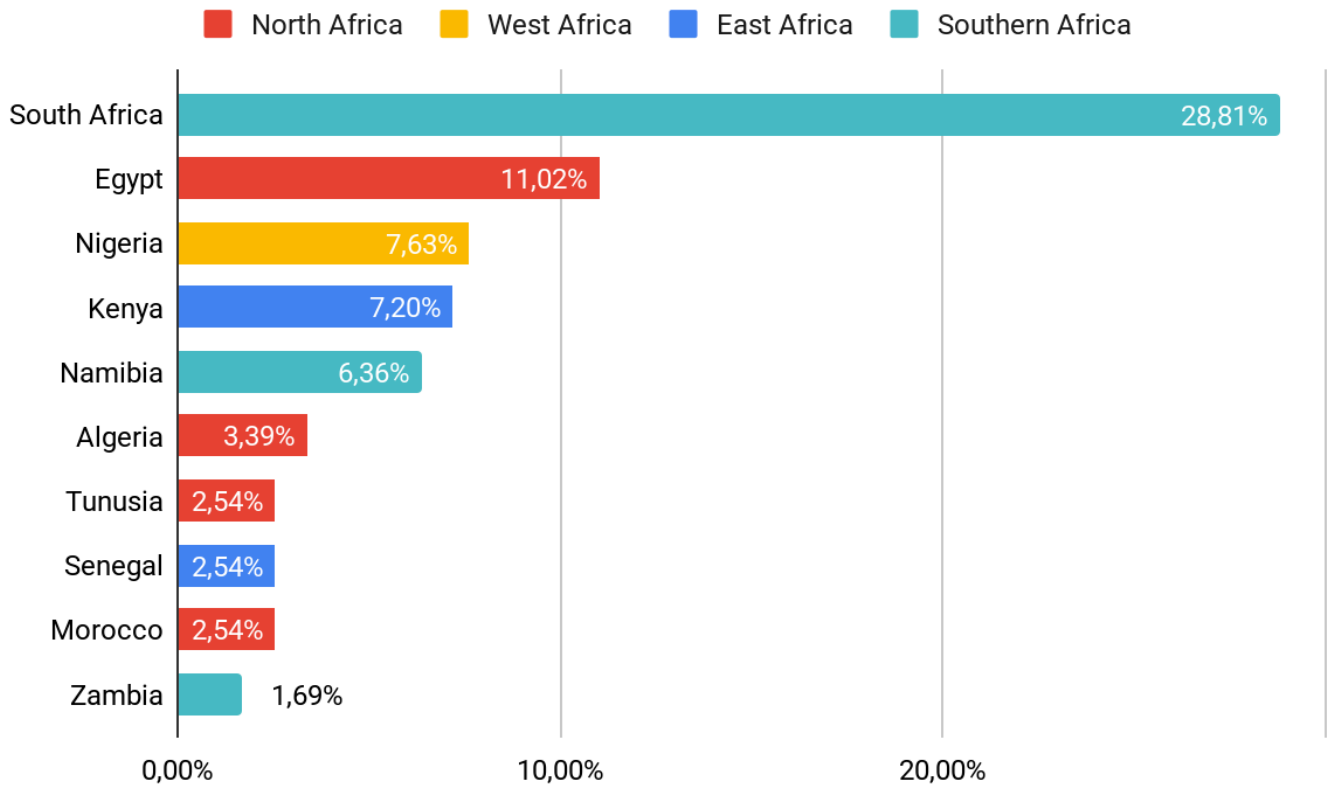
According to the post, the access includes:

- VPN (Sophos) credentials
- Exchange server (LA)
- Approximately 2,450 domain computers
- Offered at a price of $2,000, with room for negotiation.

Such access could enable threat actors to infiltrate core infrastructure systems, exposing both operational technology and corporate networks to significant risk.

Ransomware Threats Targeting the Africa Region

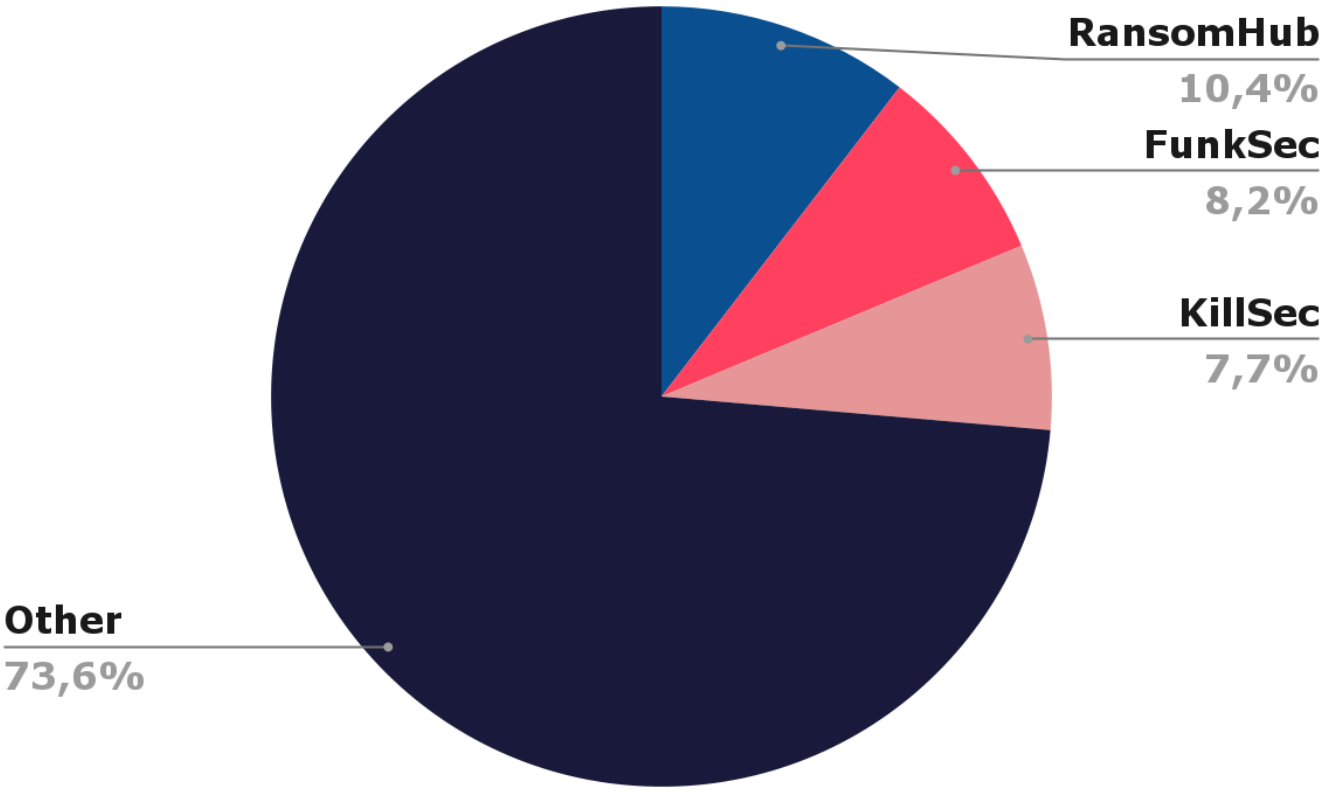
Distribution of Ransomware Attacks by Primary Target Country



South Africa stands out as the top ransomware target, with almost 29% of all recorded attacks. This dominance shows how its advanced economy and broad digital adoption make it an attractive focus for cybercriminals. Egypt follows at 11%, while Nigeria and Kenya record around 7% each, together representing other key hubs in the region.

The data shows that ransomware actors focus on regional leaders with stronger digital infrastructure, but they do not ignore smaller countries. The spread across North, West, East, and Southern Africa highlights that ransomware has become a continent-wide problem, though the highest risks remain concentrated in economic powerhouses like South Africa and Egypt.

Top Ransomware Groups Targeting the Africa Region



The data shows a very fragmented ransomware landscape in Africa. The “Other” category dominates with almost 74% of activity, suggesting that many smaller or short-lived groups operate in the region. This fragmentation makes it harder to track campaigns and highlights the diverse range of actors testing opportunities across African markets.

Among named groups, RansomHub leads with just over 10% of attacks. FunkSec follows at 8%, and KillSec at nearly 8% as well. While their share is smaller compared to the overall threat volume, these groups stand out for sustained operations and recognizable branding. Their presence points to a mix of both established and emerging players.

A Closer Look into The Top 3 Ransomware Groups

RansomHub

As stated on the group's About page, RansomHub is comprised of hackers from various locations united by a common goal of financial gain. The gang explicitly mentions prohibiting attacks on specific countries and non-profit organizations. In February 2024, RansomHub posted its first victim, the Brazilian company YKP.

The gang's website states that they refrain from targeting CIS, Cuba, North Korea, and China. While they suggest a global hacker community, their operations notably resemble a traditional Russian ransomware setup. Their stance on Russian-affiliated nations and the overlap in targeted companies with other Russian ransomware groups are also worth noting.

You can visit our ***blog post*** for more detailed information about RansomHub.

FunkSec

FunkSec, a new ransomware group, emerged in December 2024 and claimed responsibility for attacks on multiple victims. By the time of writing the number of victims reached 129. The group appears to be involved in both hacktivism and ransomware, with members likely inexperienced and seeking recognition.

Researchers suggest that the file-encrypting malware, written in Rust, was likely developed by an inexperienced malware creator from Algeria with the assistance of AI. The developer also uploaded parts of the ransomware's source code online. Operating under the Ransomware-as-a-Service (RaaS) model, FunkSec engages in double extortion, threatening to release stolen data to coerce victims into paying the ransom.

You can visit our ***blog post*** to read the rest of the threat actor profile.

KillSec

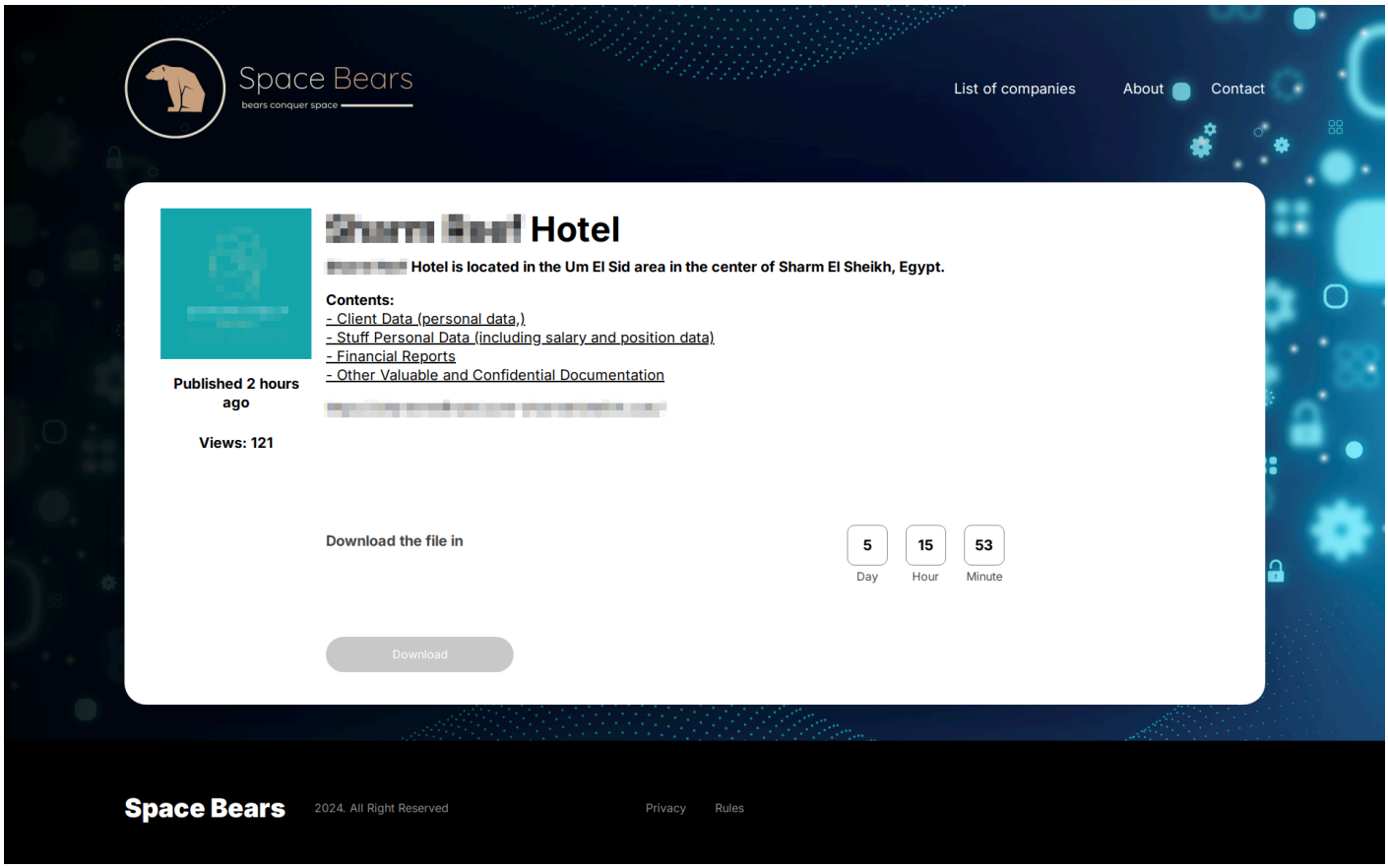
KillSec is a highly active entity known for its involvement in ransomware attacks and data breaches. First identified in October 2023, this actor has steadily increased its presence by targeting organizations across sectors.

KillSec exhibits a strong focus on India, with 29.55% of its alleged attacks targeting organizations in the country. Regarding industries, KillSec has shown a distinct focus on targeting key sectors, with healthcare being its primary target, comprising 20.45% of its alleged attacks.

You can visit our ***blog post*** for more detailed information about KillSec.

Recent Ransomware Attacks Targeting Entities in Africa Region

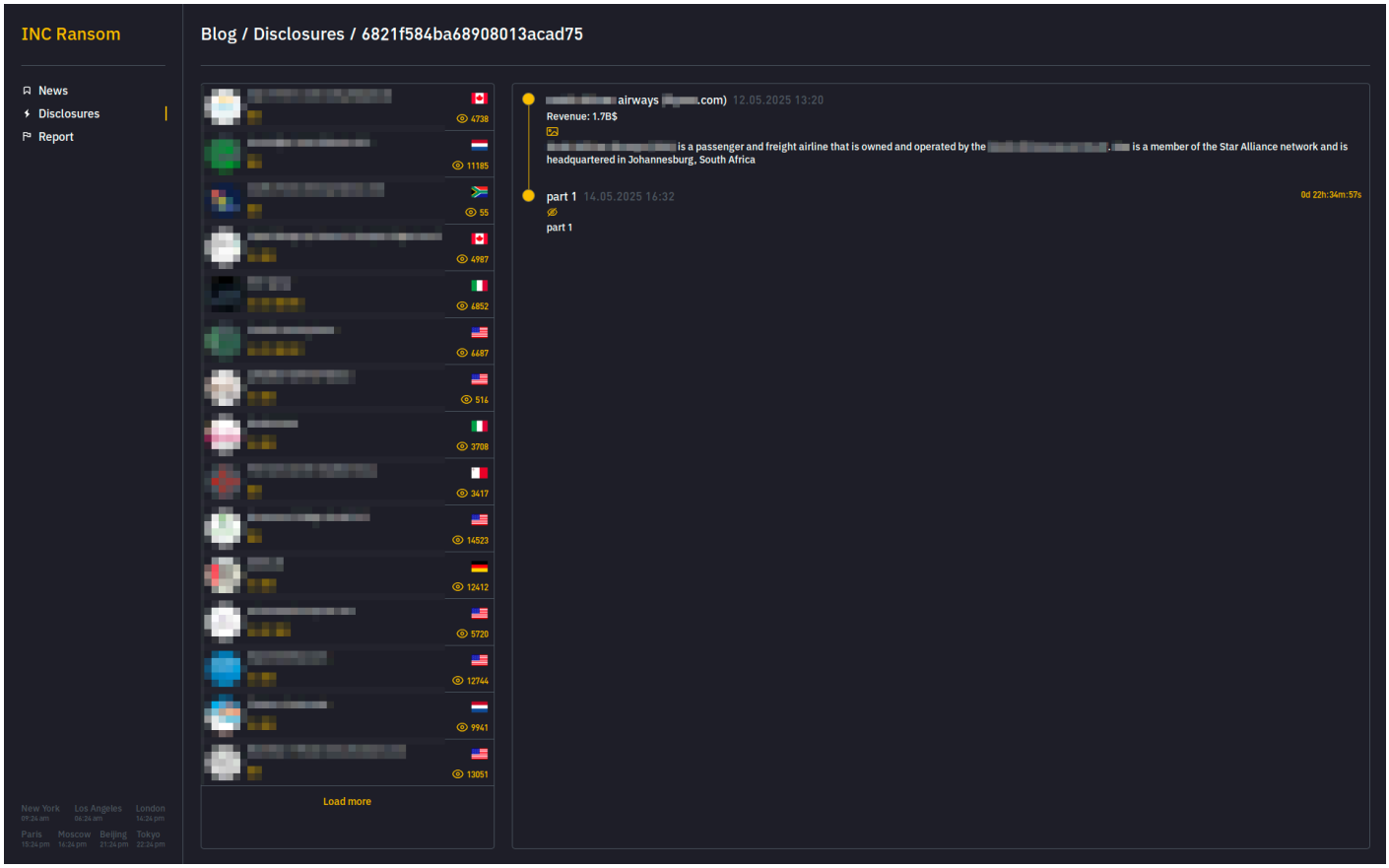
Ransomware Group Claims New Victim in Egyptian Hospitality Sector



SOCRadar has detected a new post on the Space Bears ransomware group's website, reporting an alleged attack on a hotel located in Sharm El Sheikh, Egypt.

The victim operates in the hospitality sector and reportedly manages sensitive data, including guest information, staff records, financial reports, and other confidential documentation.

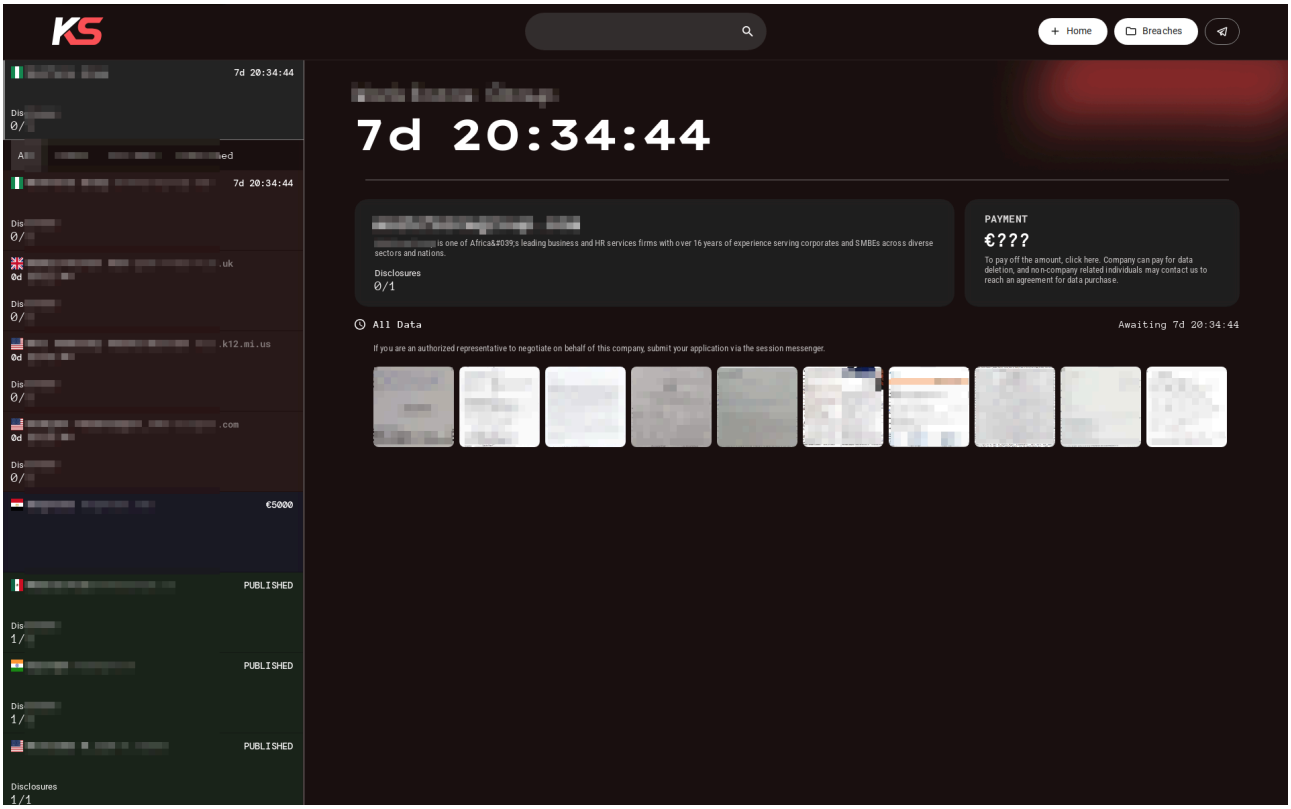
Ransomware Group Lists New Victim in African Aviation Sector



SOCRadar has observed a new post on the INC Ransom ransomware group's website, naming an alleged victim in the aviation industry.

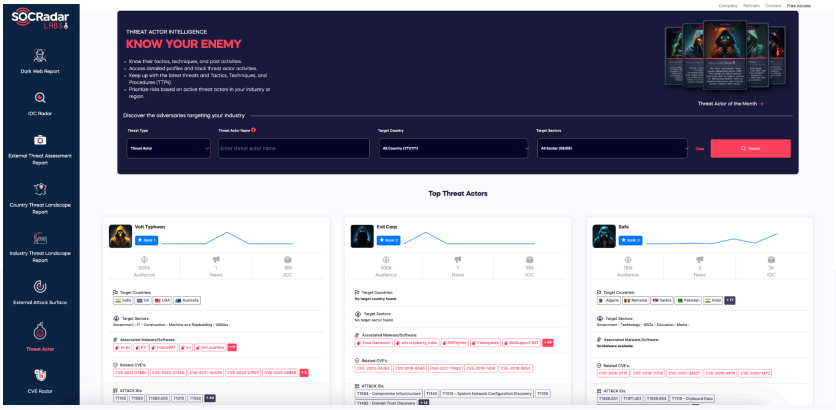
The targeted entity is a government-owned airline, operating both passenger and freight services and serving as a member of the Star Alliance network.

Ransomware Group Claims New Victim in African HR and Business Services Sector



SOCRadar has identified a new post on the KillSec ransomware group's website, announcing an alleged attack against a prominent African firm in the business and human resources services sector.

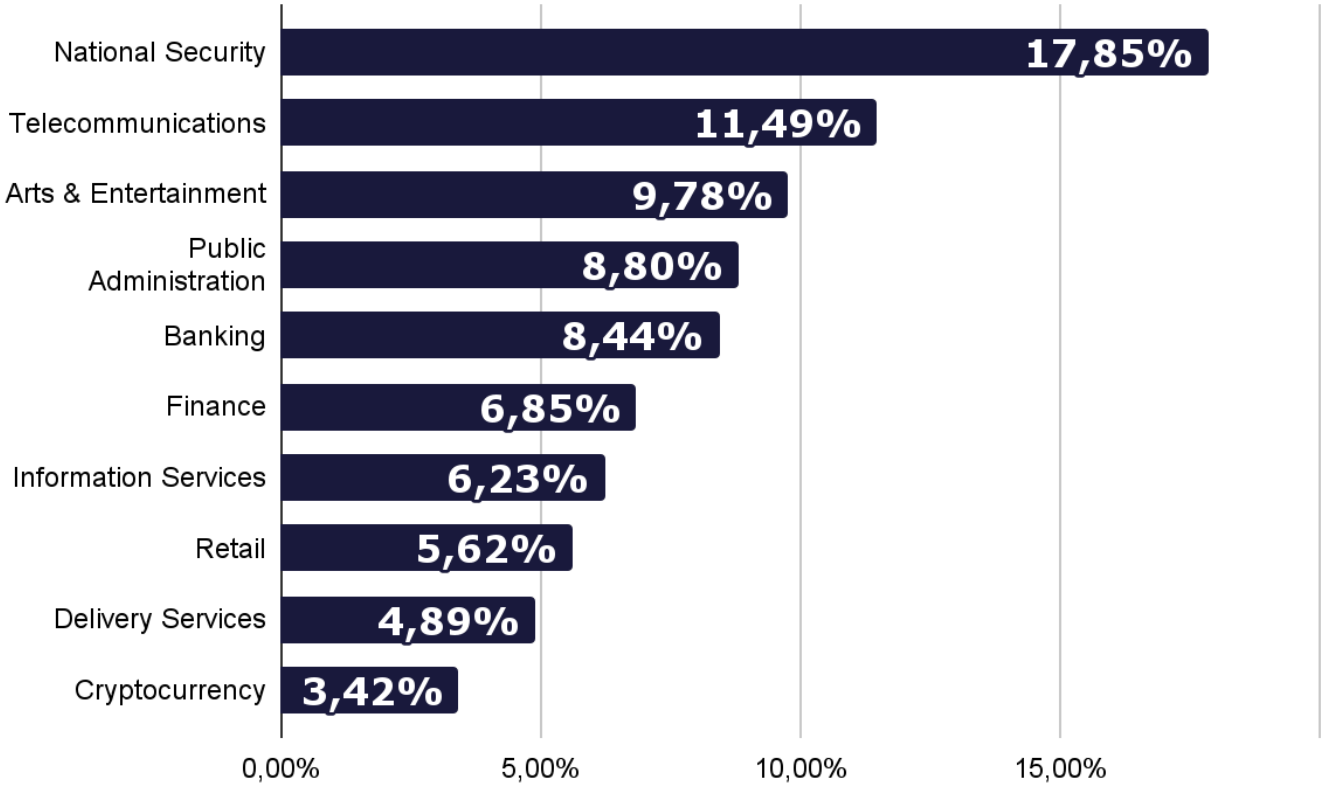
The targeted organization is described as a leading provider with more than 16 years of experience supporting both large corporations and small to medium-sized enterprises across multiple industries and countries.



*SOCRadar enhances cybersecurity measures with its **Threat Actor Intelligence Module**, which features advanced Threat Actor Tracking capabilities for organizations that want to stay ahead of cyber threats in real time.*

Phishing Threats Targeting Africa

Phishing Attacks - Distribution by Industry



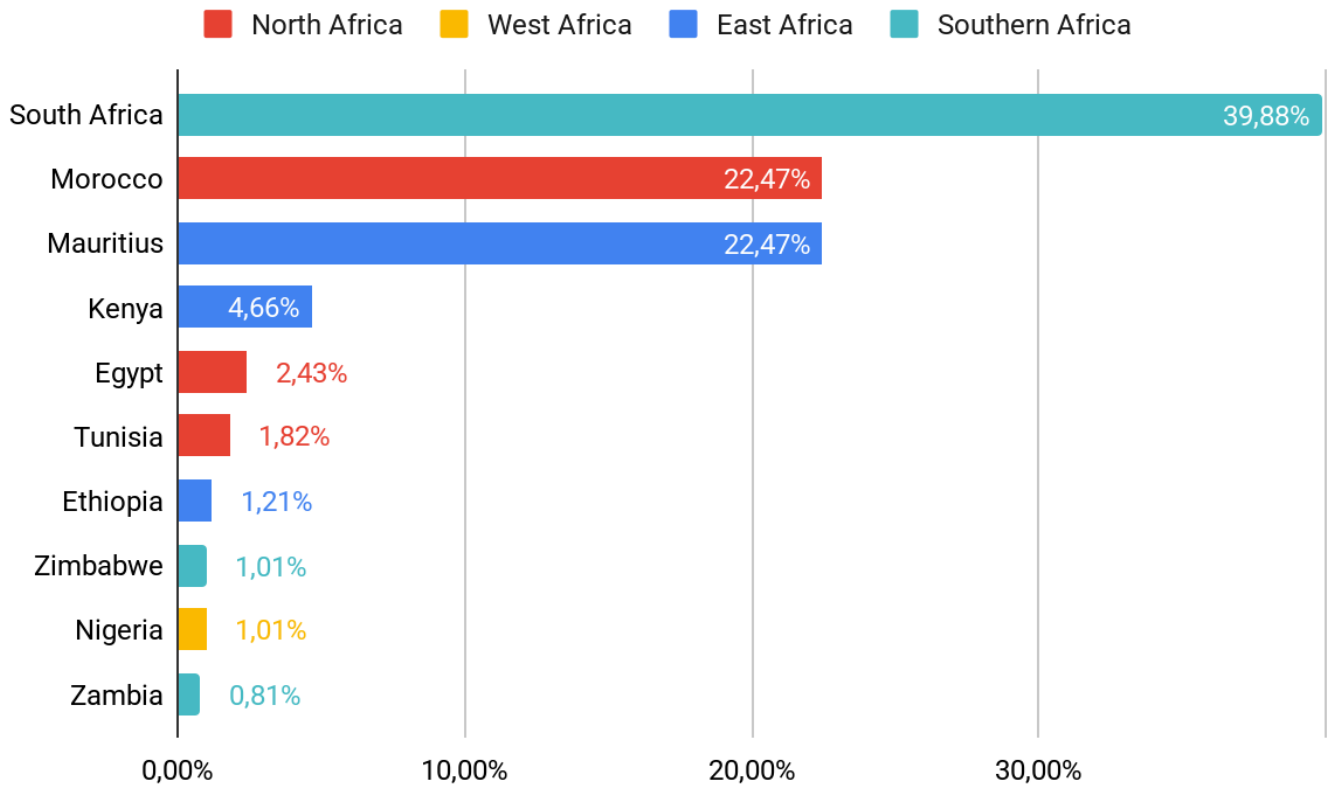
National security and international affairs lead with almost 18% of phishing activity. This shows how attackers seek to exploit sensitive government and defense-related organizations, aiming for intelligence or disruption. Telecommunications follows at 11%, reflecting the critical role of mobile and internet providers, which can serve as entry points to wider networks.

Banking and Finance combined results around 15% which can take the second spot.

Finance and information services together go up to 13%, showing that phishing actors continue to chase both monetary and data-driven rewards. Retail and delivery services (about 10% combined) highlight the risk tied to online shopping and logistics, often exploited during peak demand periods.

Overall, phishing in Africa targets both high-value government sectors and fast-growing digital industries.

Phishing Attacks - Distribution by Target Country

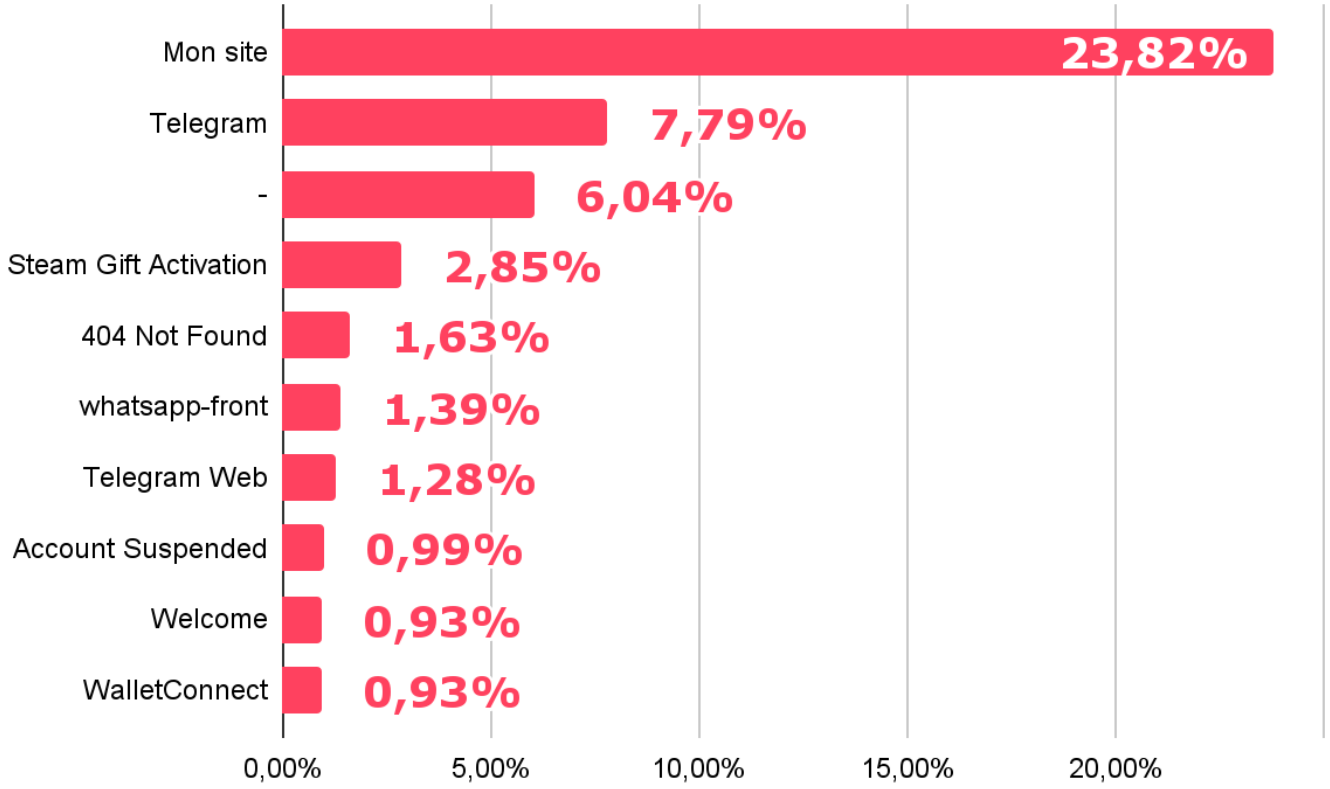


South Africa dominates with nearly 40% of phishing attacks, making it the clear hotspot in the region. Its advanced digital economy, large user base, and strong financial sector likely make it attractive to phishing actors.

Morocco and Mauritius follow at 22% each, which shows that North Africa and the Indian Ocean region also face heavy targeting. The equal share for Mauritius is notable, as it suggests attackers see value in the island's role as a financial and business hub.

The data shows that phishing is highly concentrated in a few countries, with South Africa, Morocco, and Mauritius together making up over 80% of activity. Attackers appear to prioritize nations with stronger financial systems and international connectivity, while other regions remain secondary but not immune.

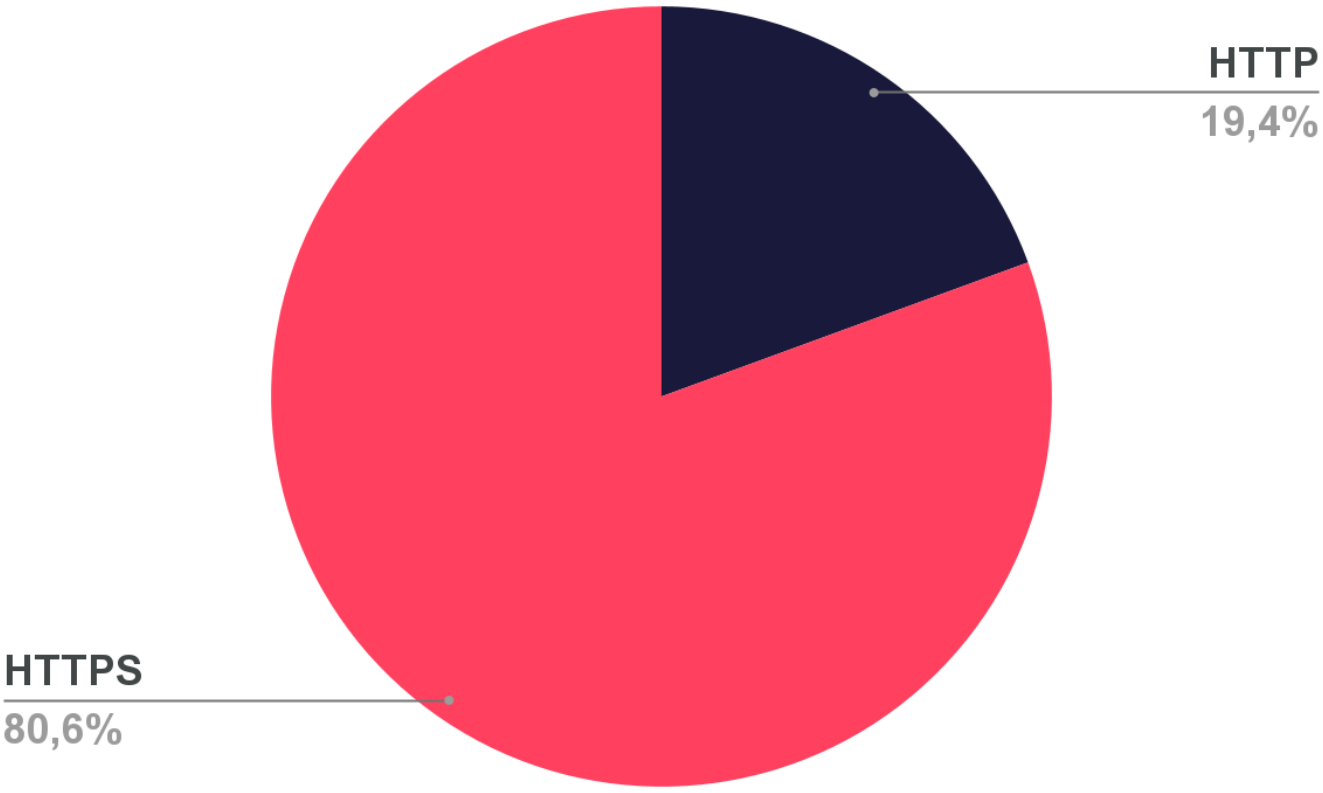
Phishing Attacks - Distribution by Phishing Page Title



The most common phishing page title is “Mon site”, accounting for almost 24% of all cases. This generic label suggests the use of mass-produced or poorly customized phishing kits, which can still be effective due to volume. Telegram-related pages appear next, making up more than 9% when combined (Telegram and Telegram Web). This highlights how attackers exploit popular messaging platforms to trick users into giving up credentials or personal data.

Although the majority of titles are generic, the presence of platform-specific and financial hooks shows that attackers mix mass campaigns with more targeted efforts. This blend helps them reach both broad audiences and high-value users in digital finance and communication platforms.

Phishing Attacks - Distribution by SSL/TLS Protocol



Most phishing pages now use HTTPS, with more than 80% adopting encrypted connections. This shows how attackers take advantage of free or low-cost SSL certificates to make their fake sites look legitimate. For many users, the presence of a padlock icon still signals trust, which increases the success rate of these scams. Only 19% of phishing sites remain on plain HTTP. While these are easier to detect as unsafe, their presence shows that some attackers still rely on speed and volume rather than credibility.

The data highlights a clear shift: encryption is no longer a sign of safety but a standard feature in phishing campaigns. This trend raises the bar for detection, as users and even some security tools may be misled by the appearance of a “secure” connection.

Strategic Recommendations

- **Enhance Endpoint Security:** Implement advanced anti-malware, regular device audits, and employee training on safe browsing practices.
- **Strengthen Phishing Defense:** Invest in phishing detection systems, web filtering tools, and employee training on recognizing phishing attempts.
- **Enforce Multi-Factor Authentication (MFA):** Apply MFA across critical systems to protect against stolen credentials.
- **Fortify Ransomware Defenses:** Regularly back up data, segment networks, and develop incident response plans for ransomware attacks.
- **Monitor Dark Web Activity:** Use dark web monitoring to detect exposed company data early and respond quickly to breaches.
- **Collaborate on Cyber Threat Intelligence:** Share insights with industry peers and stay informed about emerging threats and new attack vectors.
- **Secure Communications and Data:** Ensure encryption for sensitive communications and transactions, and train employees on secure data handling.
- **Proactive Vulnerability Management:** Regularly apply patches and conduct penetration testing to address potential system vulnerabilities.
- **Build a Cybersecurity Culture:** Foster ongoing employee training, phishing simulations, and establish clear security policies to ensure a security-first mindset across the organization.

Who is SOCRadar?

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by
21.000+ companies
in 150+ countries

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.