tanosec

MARCH
2026

ANNUAL THREAT INTELLIGENCE REPORT

THE DIGITAL WILD WEST

South Africa's 2026 Cyber Landscape

Fact-based intelligence on the threats reshaping South African business, government, and civil society — with no jargon, no filler, and no sugarcoating.

1,607	R2.2BN	60%	17,849	#1
Breaches Reported April–Sept 2025	Annual Cybercrime Cost to SA	YoY Increase in Data Breaches	Ransomware Incidents Highest in Africa	SARanked Most Attackedin Africa

CONTENTS

What's Inside

EXECUTIVE SUMMARY

The State of Play

Let's be blunt. If your business is still treating cybersecurity as an IT afterthought — something you'll 'get around to' — 2026 is going to be a very expensive year. South Africa is no longer a soft target at the edge of the global threat map. We are the target. Africa's most digitally integrated economy has become Africa's most attacked economy.

> ***"The numbers don't care about your budget constraints or your "never been hacked" track record. They only care about your vulnerabilities." — Tanosec***

KEY FINDINGS FOR 2026

01 AI has industrialised the attacker's toolkit — autonomous recon, tailored attacks, machine-speed exploitation

02 MFA bypass through session hijacking now accounts for a growing share of the 54% identity-based breaches

03 Banking trojans surged 136%, spyware grew 3.6x, backdoors increased 123% — perimeter defence is dead

04 38% of breaches involved peripheral devices: your printer, router, ATM and POS are active attack vectors

05 Quantum 'harvest now, decrypt later' attacks are already underway — infrastructure decisions matter today

06 POPIA enforcement intensifies; FSCA Joint Cybersecurity Standard in effect June 2025 — compliance is liability

BOTTOM LINE

The threat landscape has never been more sophisticated. But neither have the tools available to defend against it. Knowledge is your first line of defence.

THE NUMBERS

What the Data Actually Says

Real statistics from SABRIC, Kaspersky, Accenture, INTERPOL and the Information Regulator of South Africa.

1,607
Data Breaches
Reported Apr–Sep 2025. A 60% surge on 2024.

R2.2BN
Annual Cost
Total estimated cybercrime cost to the SA economy annually (SABRIC).

17,849
Ransomware Hits
SA recorded the highest ransomware detections on the African continent.

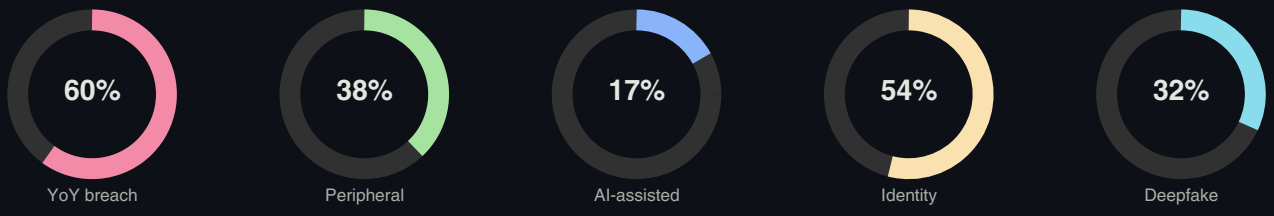
10.3M
Malware Incidents
H1 2025 malware-related incidents (Kaspersky)

6M+
Online Attacks
Attack attempts targeting SA users in H1 2025 (Kaspersky)

R2.5M+
Avg Recovery
Average ransomware recovery cost per SA business

54%
Identity Breaches
SA breaches involving compromised identities (Accenture 2025)

BREACH CHARACTERISTICS — H1 2025



THREAT ESCALATION TIMELINE

2022
SA enters top 10 most attacked globally

2023
POPIA enforcement begins; breach reporting rises

2024
Ransomware peaks at 17,849 — highest in Africa

2025
AI attacks surge 17%; breach reports up 60% in 6 months

2026
Quantum threats emerge; FSCA Joint Standard begins

AI ON THE WRONG SIDE

How Cybercriminals Industrialised with Artificial Intelligence

INTERPOL reported a 17%rise in AI-assisted cyber crime across Africa in 2025,with South Africa among the most affected nations. This is not about better phishing emails. This is industrialisation.

THE AI-POWERED ATTACK CHAIN

01 RECON
AI agents map your network, employees, vendors & suppliers autonomously

02 TARGET
Machine learning identifies the weakest human and technical entry points

03 CRAFT
Deepfakes, synthetic voice & personalised lures generated at scale

04 EXECUTE
Automated exploitation — no human operator needed after initial setup

05 PERSIST
AI-driven lateral movement & data exfiltration while evading detection

DEEPFAKE THREAT

32%

Annual Growth in AI Fraud Damage

Synthetic voice cloning can replicateyour CEO accurately enough to authorise wire transfers. Video deepfakes have cleared facial recognition in documented SA banking incidents. On track to exceed $40bn in global losses by 2027.

AI IN YOUR DEFENCE

The same technology works both ways.

- Behavioural AI detects anomalous activity signature-based tools miss entirely
- AI-driven threat hunting identifies lateral movement before exfiltration occurs
- Automated response compresses mean-time-to-contain from hours to minutes
- NLP models flag social engineering attempts in real time across email & messaging

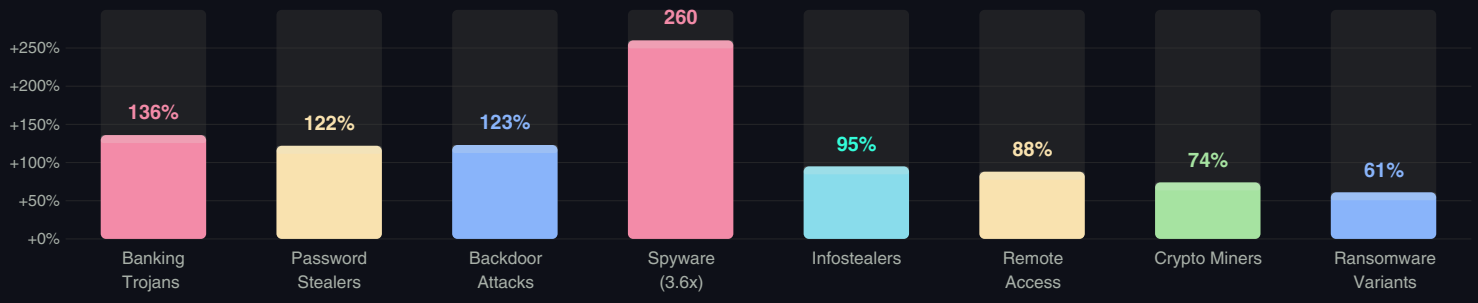
> ***"The attacker of 2026 doesn't sleep, doesn't take lunch breaks, and doesn't need a VPN to find your backdoor. But your AI-assisted defence can work exactly the same way." — Tanosec***

MALWARE SURGE

The Categories Exploding in 2025–26

Backdoor attacks increased 123%. Banking trojans surged 136%. Spyware grew 3.6x. These are not isolated anomalies — they represent a deliberate shift in attacker investment.

MALWARE CATEGORY GROWTH (2024 → H1 2025)



THREAT SEVERITY INDEX — SOUTH AFRICA 2026

SPOTLIGHT: SparkCat & The Official App Store Problem

Info stealers like SparkCat have been documented spreading through legitimate app stores. Users following all the 'right' advice can still be compromised. Perimeter thinking is dead.

THE IDENTITY CRISIS

MFA Is Not Dead. But Attackers Found the Emergency Exit.

54%of South African data breaches in 2025 involved compromised user identities (Accenture). Not brute-forced passwords. Not guessed PINs. Stolen identities — and stolen session tokens that render MFA entirely irrelevant.

HOW SESSION HIJACKING BYPASSES MFA

01 USER LOGS IN
Employee authenticates normally. MFA code entered. Session token issued by server.

02 COOKIE STOLEN
Malware or browser extension extracts the session token from browser storage.

03 TOKEN REPLAYED
Attacker injects stolen token. Server sees a valid, authenticated session.

04 MFA IRRELEVANT
No password needed. No MFA prompt triggered. Attacker is inside as a trusted user.

THE IDENTITY THREAT LANDSCAPE | KEY VECTORS

Credential Stuffing
Automated use of leaked username/password combinations from breach databases against SA banking & government portals.

SIM Swap Fraud
Fraudulent porting of mobile numbers to attacker-controlled SIMs — a documented SA telecoms vulnerability.

Adversarial AI Login Attacks
AI models trained to solve CAPTCHAs, bypass bot detection, and generate convincing login behaviour patterns.

Insider Threats
Credential misuse by employees remains a persistent and under-reported source of identity compromise in SA.

ZERO TRUST IS NOT A BUZZWORD ANYMORE
Zero Trust Architecture assumes every request — internal or external — is potentially compromised. Continuous verification, least-privilege access, and micro-segmentation are now baseline requirements for any South African organisation handling customer data or financial transactions.

THE BLINDSPOT

The Devices Nobody Thought Were Dangerous

SABRIC's 2025 data shows 38% of breaches involved compromised peripheral devices — the same devices your IT policy probably hasn't touched in three years.

PRINTERS — CRITICAL

Often run outdated firmware. Can store print jobs in unencrypted flash memory. Frequently forgotten in security audits.

ATMs — CRITICAL

Physical skimming and firmware attacks. SA has one of Africa's highest ATM fraud rates. Remote management interfaces often exposed.

OFFICE ROUTERS — HIGH

Default credentials active in 40%+ of SA SME deployments. Primary entry point for network-level intrusion.

POS SYSTEMS — HIGH

Payment terminal malware is a growing threat in SA retail. EMV alone does not protect back-end systems and databases.

IP CAMERAS — MEDIUM

Typically lowest-priority patching cadence. Provide attackers with reconnaissance capability from inside your perimeter.

IoT SENSORS — MEDIUM

Building management, HVAC and industrial IoT running flat networks with no segmentation. Lateral movement goldmine.

SOUTH AFRICA'S SPECIFIC EXPOSURE

SA's distributed hardware across branches,warehouses, hospitals, mining operations and municipal offices creates an attack surface that is uniquely large, uniquely dispersed, and uniquely under-managed.

PERIPHERAL AUDIT CHECKLIST — WHERE TO START

- Inventory every network-connected device — including those outside the IT department's primary scope
- Audit firmware versions against manufacturer releases — patch where available, replace where not
- Change all default credentials immediately — especially on routers, cameras and industrial controllers
- Segment IoT and peripheral devices onto isolated VLANs away from core business systems
- Schedule periodic physical security inspections for ATMs, POS terminals and access control hardware

QUANTUM & THE FUTURE

This Sounds Futuristic. It Isn't.

NIST formalized quantum-safe cryptography standards in 2024.'Harvest-now, decrypt-later' attacks are already underway. The question isn't if — it's when decryption becomes possible. Infrastructure decisions made today will still have consequences then.

QUANTUM TIMELINE — WHAT'S HAPPENING NOW

NOW
Adversaries collecting & archiving encrypted comms, financial records and state secrets

2026–28
IBM and Google targeting 1M+ qubit systems. Error correction maturing rapidly.

2028–30
Cryptanalytically relevant quantum computers within projected reach of nation-states

ACT NOW
Infrastructure procured today will still be operational when this threshold is crossed

NIST POST-QUANTUM CRYPTOGRAPHY STANDARDS (FIPS 203, 204, 205)

- **CRYSTALS-Kyber (ML-KEM)**
  Primary standard for key encapsulation. Lattice-based. Recommended for immediate adoption.
- **CRYSTALS-Dilithium (ML-DSA)**
  Digital signature algorithm. Lattice-based. Drop-in replacement roadmap now available.
- **SPHINCS+ (SLH-DSA)**
  Hash-based signatures. Conservative choice for highest-security applications.

WHAT TO DO RIGHT NOW

Start the quantum conversation with your infrastructure vendors. Any hardware or software procured today should have a documented roadmap to quantum-resilient cryptographic standards. For financial services and government: this is now a procurement requirement, not a future project.

POPIA & COMPLIANCE

POPIA Has Teeth Now.

Compliance isn't a cybersecurity strategy. But non-compliance in 2026 is a guaranteed liability.

POPIA AMENDMENTS

Effective April 2025

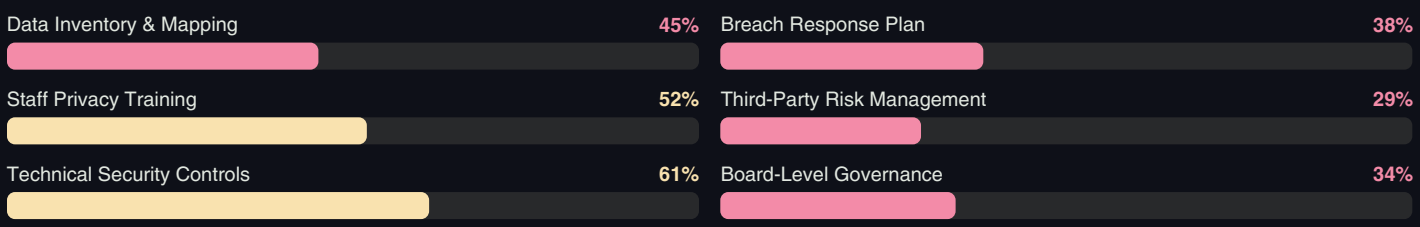
- Mandatory written consent for direct marketing now strictly enforced
- Information Regulator launched mandatory online breach reporting portal
- Breach notification timelines tightened — 72 hours to notify the Regulator
- Enforcement focus for 2026 is data breach response readiness
- Penalty exposure: up to R10M or 10 years imprisonment for wilful violations

FSCA JOINT STANDARD

In EffectJune 2025

- Applies to banks, insurers, fund administrators and financial market infrastructures
- Mandatory cyber risk governance frameworks at board level
- Annual independent cybersecurity assessments now required
- Incident response plans must be documented, tested and current
- Third-party and vendor cyber risk management now a formal obligation

COMPLIANCE READINESS — TYPICAL SA ORGANISATION



* Based on aggregate assessment data from Tanosec engagements and industry research. Indicative only.

BOTTOM LINE

POPIA compliance is not a tick-box exercise — it's a framework for understanding what data you hold, where it lives, who can access it, and what happens when things go wrong. That understanding has direct commercial value.

ACTION PLAN

What To Actually Do in 2026

Not generic advice. Specific, practical, South African context.

01 ASSUME BREACH — NOW

IMMEDIATE

Redesign systems and response plans on the assumption an attacker has already found a way in. Detection speed and containment now matter more than perfect prevention. No incident response plan? That's your first deliverable.

02 AUDIT YOUR PERIPHERALS

THIS WEEK

ATMs, printers, routers, POS terminals and IoT are your softest targets. Firmware, default credentials and patch cycles need active management — not periodic audits. Start today.

03 TEST YOUR PEOPLE

QUARTERLY

Phishing simulations are the most cost-effective security investment per rand. Staff are simultaneously your greatest vulnerability and — when trained — your first line of defence.

04 GET YOUR DIGITAL FOOTPRINT ASSESSED

URGENT

You likely have more exposed data than you know — dark web credentials, exposed APIs, misconfigured cloud assets. An OSINT-based assessment shows what attackers see before they act.

05 START THE QUANTUM CONVERSATION

STRATEGIC

Vendors should articulate a roadmap to NIST-standardised quantum-resilient cryptography. This is now a procurement question, not a future IT project.

06 REVIEW YOUR POPIA OBLIGATIONS

COMPLIANCE

Understand what data you hold, where it lives, who has access, and what your breach response looks like. The Information Regulator's 2026 enforcement priority is breach response readiness.

"Knowledge is your first line of defence. Action is your second."

— Tanosec Cybersecurity | 2026 SA Cyber Landscape Report

ABOUT TANOSEC

tanosec

Comprehensive Cybersecurity Solutions for Modern Threats

Tanosec is a South African cybersecurity firm based in Bloemfontein, built for organisations navigating a threat landscape that evolves faster than most security policies get reviewed.

PENETRATION TESTING
Full-scope network and application penetration testing. We find your weaknesses before attackers

DIGITAL FOOTPRINT AUDIT
OSINT-based assessment — dark web credential leaks, exposed infrastructure and third-party risk.

MANAGED SECURITY
Continuous monitoring, threat detection and incident response for organisations without in-house SOC.

SECURITY AWARENESS
Human-focused training and phishing simulations that turn staff from a vulnerability into an asset.

VULNERABILITY ASSESSMENTS
Comprehensive vulnerability assessments identifying exploitable weaknesses across your network,

THREAT INTELLIGENCE
SA-specific intelligence feeds and sector advisory. Know what's targeting you before it arrives.

Ready to find out what attackers see when they look at your business?

Start with a Digital Footprint Assessment or Penetration Test.

www.tanosec.co.za

Bloemfontein, South Africa

info@tanosec.co.za

linkedin.com/company/tanosec-cybersecurity

2025 WINNER Cybersecurity

PROUD MEMBER COMPANY MSPAlliance International Association of Cloud and Managed Service Providers

Statistics sourced from SABRIC, Kaspersky, Accenture, INTERPOL, the Information Regulator of South Africa, Deloitte and NIST. Tanosec makes no warranty as to completeness or accuracy of third-party data.