DIGITAL PROGRESSION

# SOUTH AFRICA
# CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 12 | 9-15 March 2026

**THREAT LEVEL: HIGH**

Escalated from ELEVATED — Gauteng 3.8 TB breach, Salt Typhoon SA telco targeting, multiple ransomware victims

**TLP:WHITE**

**Prepared by Digital Progression | dpcyber.co.za**

Report ID: DP-CTI-2026-W12 | Classification: TLP:WHITE

# TABLE OF CONTENTS

# 1. EXECUTIVE SUMMARY

**Overall Threat Level: HIGH** — Escalated from the prior week's ELEVATED rating due to the Gauteng Provincial Government massive data breach (3.8 TB exfiltrated by XP95)[1], confirmed Salt Typhoon targeting of SA telecoms[2], and three new ransomware victims in the reporting period.[3]

## KPI Dashboard

| Metric | Current | Baseline | Change | Direction |
|---|---|---|---|---|
| SA org breach frequency | Every 3 hours | Every 5 hours (2025) | +40% | UP |
| Cyberattacks/week targeting SA | 2,204/wk (Feb 2026) | 1,806/wk (Feb 2025) | +22% YoY | UP |
| POPIA breach notifications (YTD) | 2,898 (to 5 Mar 2026) | ~1,900 (same period 2025) | +53% | UP |
| Avg ransomware recovery cost | R24M (2025) | R17M (2024) | +41% | UP |
| SA ransomware victims tracked | 91 total, 3 new this week | 73 total same time 2025 | +25% | UP |
| Digital banking fraud cases | 98,000 (2024) | 52,000 (2023) | +88% | UP |

ANOMALY FLAG: All metrics trending significantly above baseline. Breach frequency anomaly (every 3 hours vs. every 5 hours) is driven by identity-based attacks in approximately 90% of cases.[4]

### TOP 3 ACTIONS THIS WEEK

**1. PATCH:** Update Chrome to 146.0.7680.75+ (2 zero-days in CISA KEV, active exploitation). Patch Cisco FMC (CVSS 10.0 x2). Apply Microsoft March 2026 Patch Tuesday.

**2. HUNT:** Search for Salt Typhoon indicators on Cisco IOS-XE routers and telco infrastructure — SA telecoms confirmed targeted. Hunt for XP95 indicators following Gauteng data theft.

**3. COMPLY:** Immediate POPIA health data regulation compliance review — in force since 6 March 2026, R10M penalty for non-compliance. No grace period.

### Key Findings:

- Gauteng Provincial Government suffered a 3.8 TB data exfiltration by threat actor XP95 — healthcare, education, housing, and employment records of millions of citizens exposed, now for sale at $25,000 on dark web.[1]
- RE/MAX Southern Africa: 291 GB database stolen via brute-force + SQL injection by Team Cyber Strike; POPIA Section 22 notification filed.[5]
- Salt Typhoon (China MSS) confirmed targeting SA telecoms with TernDoor, PeerTime, and BruteEntry malware — campaign affecting 200+ telcos globally.[2]
- Land Bank ransomware attack fully disclosed to Parliament — 5 BTC (R5.67M) demanded, not paid; multi-regulator notification completed.[6]
- Six new CISA KEV entries this week including Chrome zero-days (CVE-2026-3909, CVE-2026-3910), n8n RCE, and SolarWinds Web Help Desk deserialization.[7]

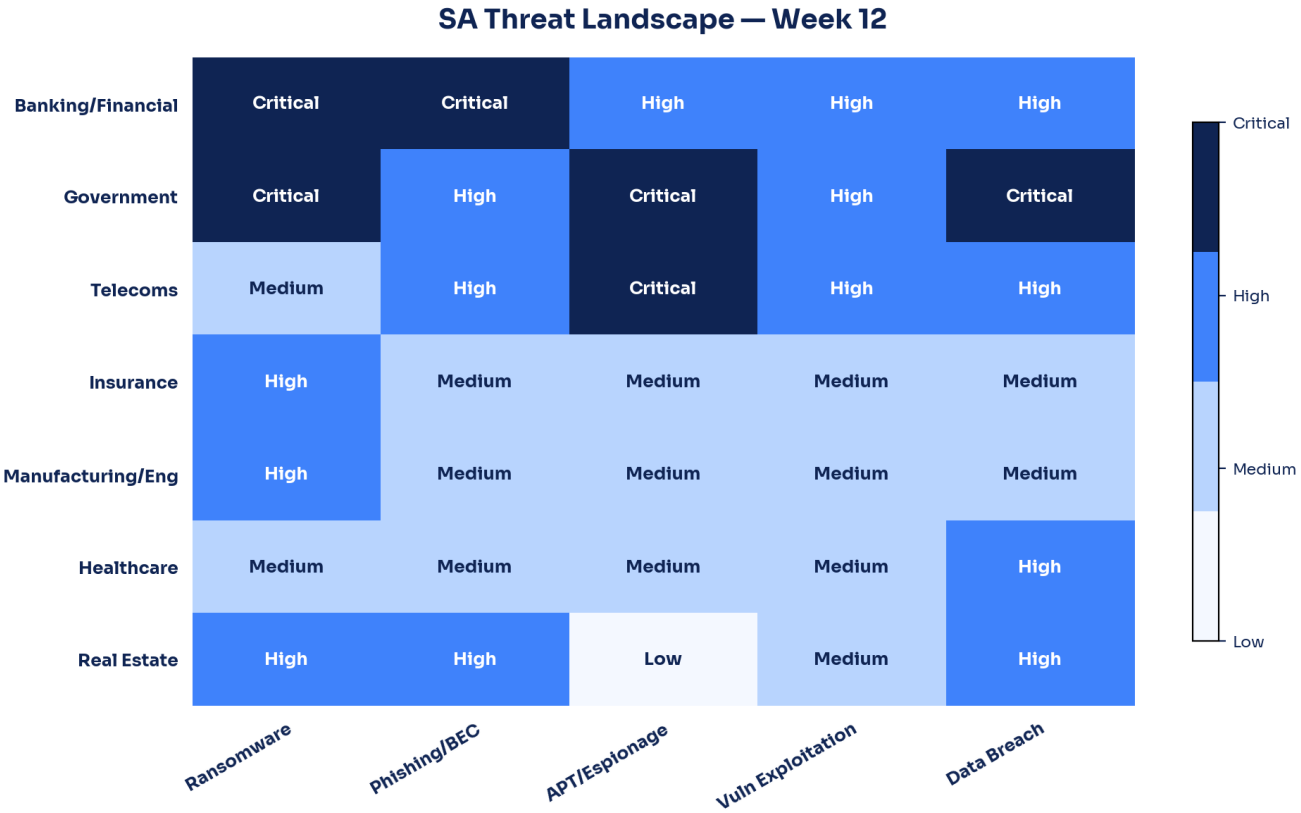
### SECTOR SPOTLIGHT: GOVERNMENT (CRITICAL)

The government sector is this week's highest-risk sector. The Gauteng Provincial Government suffered a massive 3.8 TB data exfiltration by threat actor XP95, exposing healthcare, education, housing and employment records of millions of citizens.[1] This follows The Gentlemen ransomware group's ongoing targeting of SA municipalities (Witzenberg, Intsika Yethu).[8] Combined with Salt Typhoon's confirmed targeting of SA telecom infrastructure[2] and nation-state actors pre-positioning in SA critical infrastructure[4], the government sector is under sustained multi-vector pressure from both criminal and state-sponsored actors.

1. The Citizen, 14 March 2026 — https://www.citizen.co.za/news/panyaza-lesufi-responds-gauteng-government-data-breach-claims/
2. CYFIRMA Weekly Intelligence Report, 13 March 2026 — https://www.cyfirma.com/news/weekly-intelligence-report-13-march-2026/
3. Ransomware.live SA Map — https://www.ransomware.live/map/ZA
4. The Citizen / Unit 42, 13 March 2026 — https://www.citizen.co.za/news/sa-exposed-to-cyber-security-threats-amid-conflict-in-iran/
5. RE/MAX SA Cyber Security Incident Notice, 12 March 2026 — https://www.remax.co.za/cyber-incident-notice
6. ITWeb, 9 March 2026 — https://www.itweb.co.za/article/land-bank-tightens-security-after-ransomware-attack/raYAyMorlOl7J38N
7. CISA KEV Catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
8. DeXpose — The Gentlemen Intsika Yethu — https://www.dexpose.io/the-gentlemen-ransomware-attack-on-intsika-yethu-municipality/

## 2. THREAT LANDSCAPE HEATMAP

The heatmap below maps seven key South African sectors against five threat categories, rated from Low to Critical based on active threat intelligence, confirmed incidents, and vulnerability exposure during Week 12.




| | Ransomware | Phishing/BEC | APT/Espionage | Vuln Exploitation | Data Breach |
|---|---|---|---|---|---|
| Banking/Financial | Critical | Critical | High | High | High |
| Government | Critical | High | Critical | High | Critical |
| Telecoms | Medium | High | Critical | High | High |
| Insurance | High | Medium | Medium | Medium | Medium |
| Manufacturing/Eng | High | Medium | Medium | Medium | Medium |
| Healthcare | Medium | Medium | Medium | Medium | High |
| Real Estate | High | High | Low | Medium | High |

**Methodology:** Risk levels are assessed using a combination of: (a) confirmed incidents in the reporting period, (b) active threat actor campaigns targeting the sector, (c) vulnerability exposure, and (d) regulatory scrutiny. **Critical** = active exploitation or confirmed breach; **High** = credible active threat; **Medium** = elevated baseline risk; **Low** = standard risk posture.

# 3. SA CYBER INCIDENTS & BREACHES

## 3.1 Gauteng Provincial Government — Data Breach (CRITICAL)

Threat actor **XP95** exfiltrated **3.8 TB** (3,673,556 files) from Gauteng provincial systems, including healthcare records, education data (student/teacher PII), housing title deeds, and economic development programme files.[9] The dataset was listed on a dark web forum and Telegram channel for **$25,000 (approx. R460,000)**.[10] Premier Panyaza Lesufi confirmed the investigation on 14 March 2026.[9] The November 2025 Microsoft licensing crisis (R344 million unpaid) likely left systems unpatched, contributing to the compromise.

## 3.2 RE/MAX Southern Africa — Cyberattack & Data Breach

**Team Cyber Strike** breached RE/MAX Southern Africa via brute-force + SQL injection against a public-facing website on 5 March 2026, gaining access to AWS infrastructure including an S3 bucket.[11] The attacker exfiltrated a **291 GB** complete database backup containing client PII (ID numbers, emails, phone numbers, addresses), transactional data, OTPs, and commission records. RE/MAX rejected the extortion demand, restored from backups, and filed a POPIA Section 22 notification.[12]

## 3.3 Land Bank — Ransomware (Parliamentary Disclosure)

Finance Minister Enoch Godongwana disclosed to Parliament on 9 March 2026 that the Land Bank suffered a ransomware attack on 12 January 2026.[13] Attackers exploited a vulnerability on an internet-facing server, encrypted non-SAP servers and laptops, and demanded **5 BTC (R5.4–5.67M)**. The ransom was not paid. Board and governance documents, HR records were exfiltrated from the file server. Critical ERP, core banking, and CRM systems (on separate SAP infrastructure) were not compromised. The Land Bank notified SAPS, the Information Regulator, the Prudential Authority, and the State Security Agency.[14]

## 3.4 Kimwolf/Aisuru Android Botnet — DDoS Threat Advisory

A threat advisory published 10 March 2026 warned of the **Kimwolf botnet** (Mirai variant linked to the Aisuru ecosystem) which has amassed ~2 million compromised Android devices.[15] South Africa consistently appears among the top infected geographies due to high rates of no-name Android TV box usage. The botnet is capable of direct-path DDoS floods exceeding 20 Tbps.

## 3.5 SA Cybersecurity Statistics Published This Week

- **Check Point Research (Feb 2026):** SA organisations faced 2,204 cyberattacks per week — a 22% YoY increase, the steepest of any African country surveyed.[16]
- **Tanosec 2026 Report:** 60% surge in data breaches YoY; SA confirmed as the most targeted economy on the African continent.[17]
- **Mimecast Human Risk Report:** 46% of SA organisations report rising malicious insider incidents; 56% report increased account takeovers (15 points above global average).[18]

9. The Citizen, 14 March 2026 — https://www.citizen.co.za/news/panyaza-lesufi-responds-gauteng-government-data-breach-claims/
10. Brinztech Threat Alert, 13 March 2026 — https://www.brinztech.com/breach-alerts/brinztech-alert-3-8-tb-database-of-gauteng-provincial-government-for-sale-25000/
11. IOL Business Report, 12 March 2026 — https://iol.co.za/business-report/companies/2026-03-12-how-the-remax-cyberattack-exposed-customer-data-and-what-it-means-for-you/
12. RE/MAX SA Incident Notice, 12 March 2026 — https://www.remax.co.za/cyber-incident-notice
13. ITWeb, 9 March 2026 — https://www.itweb.co.za/article/land-bank-tightens-security-after-ransomware-attack/raYAyMorlOl7J38N
14. Tech4Law, 9 March 2026 — https://www.tech4law.co.za/news-in-brief/security-news-in-brief/hackers-demanded-r5-7-million-after-bringing-important-south-african-bank-to-its-knees/
15. ITWeb, 10 March 2026 — https://www.itweb.co.za/article/kimwolf-at-the-door-why-sa-africa-are-prime-targets-for-the-next-gen-android-botnet/KA3WwMdzdGnvrydZ
16. TechTrends Africa, 11 March 2026 — https://techtrends.africa/global-cyber-attacks-stay-near-record-highs-in-february-2026-even-as-ransomware-dips/

17. Tanosec 2026 Report via MyCityBFN, 6 March 2026 — https://www.facebook.com/mycitybfn/posts/tanosecs-2026-annual-threat-intelligence-report-documents-a-60-surge-in-data-bre/924917166912595/
18. TechCentral, 5 March 2026 — https://techcentral.co.za/malicious-insider-threats-surging-in-south-africa-new-study-finds/278598/

# 4. ACTIVE THREAT CAMPAIGNS

## 4.1 Salt Typhoon (UAT-9244) — China-Linked Telecom Espionage

Salt Typhoon (UAT-9244), attributed to China's Ministry of State Security, has **explicitly listed South Africa as a target geography** in the CYFIRMA W12 2026 report.[19] The group has been confirmed targeting at least 200 telecommunications companies globally, including an identified SA telecom provider.[20] Key malware implants include **TernDoor** (backdoor), **PeerTime** (P2P backdoor), and **BruteEntry** (brute-force scanner). The campaign targets Cisco IOS-XE routers to gain persistent access to telco infrastructure for intelligence collection.

**MITRE ATT&CK TTPs:** T1190 (Exploit Public-Facing App), T1557 (Adversary-in-the-Middle), T1040 (Network Sniffing), T1098.004 (SSH Authorized Keys), T1572 (Protocol Tunneling), T1048.003 (Exfiltration Over Unencrypted Non-C2 Protocol)

## 4.2 APT28 (Fancy Bear / GRU) — CVE-2026-21509 Campaign

Russia's GRU-affiliated APT28 is actively weaponizing **CVE-2026-21509** (Microsoft Office security feature bypass) within 24 hours of disclosure.[21] The campaign deploys **NotDoor** (Outlook VBA backdoor) and **CovenantGrunt** (modified Covenant C2 implant) via spear-phishing documents, abusing legitimate cloud storage (filen.io) as C2. Primary targets include European defence and diplomatic entities, with UAE listed as a target — creating spillover risk for SA-based organisations with Gulf partnerships.

**MITRE ATT&CK TTPs:** T1566.001 (Spearphishing Attachment), T1204.002 (User Execution: Malicious File), T1059.001 (PowerShell), T1567 (Exfiltration to Cloud Storage)

## 4.3 MuddyWater (Iran MOIS) — Dindoor & Fakeset Backdoors

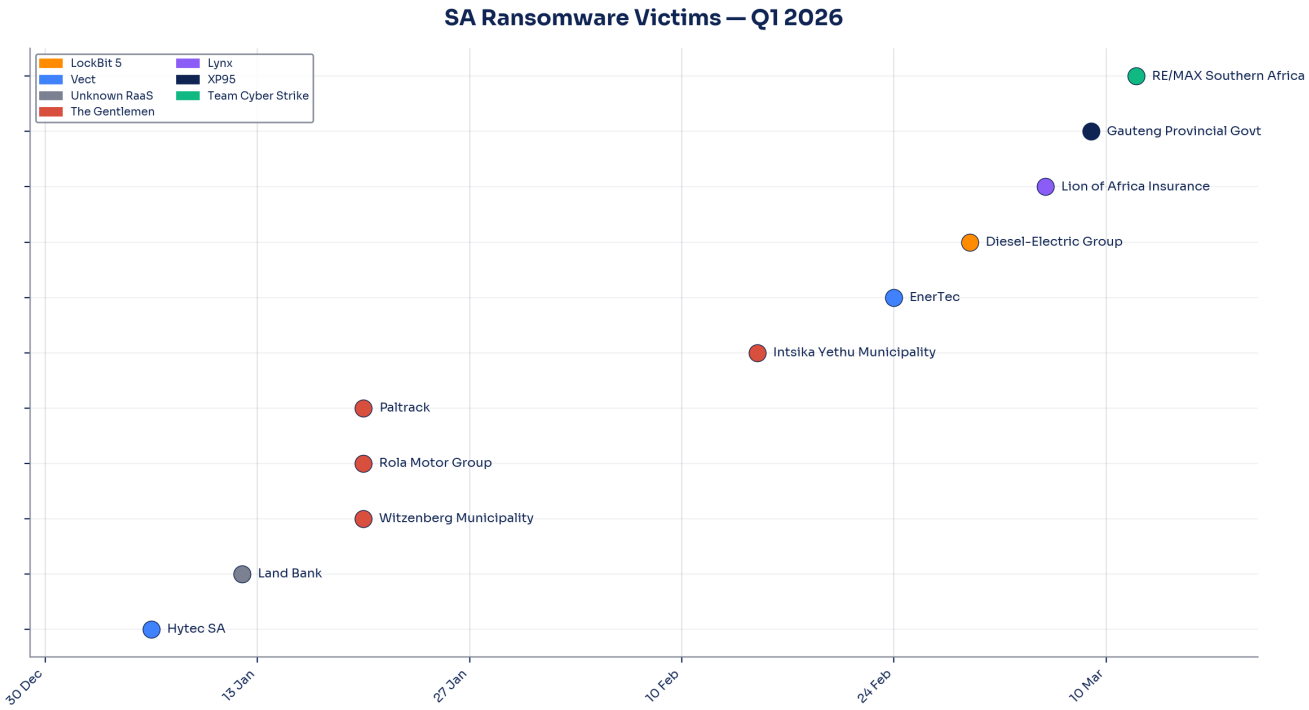
Iran's MuddyWater (MOIS) deployed new **Dindoor** and **Fakeset** (Python) backdoors in early February 2026 campaigns targeting US and Israeli entities.[22] Unit 42 notes SA organisations are "particularly exposed" to Iran-linked hacktivist and espionage spillover following Operation Epic Fury (Feb 28, 2026). Post-operation, 149 DDoS attacks hit 110 organisations across 16 countries.[23]

## 4.4 Chip Ransomware — New MedusaLocker Variant

CYFIRMA identified **Chip Ransomware**, a new MedusaLocker family variant using AES + RSA encryption.[19] File extension: .chip1; ransom note: Recovery_README.html. Targets manufacturing, healthcare, education, government, and financial sectors globally. Uses parent PID spoofing (T1134.004), sandbox evasion (T1497.001), and keylogging (T1056.001).

19. CYFIRMA Weekly Intelligence Report, 13 March 2026 — https://www.cyfirma.com/news/weekly-intelligence-report-13-march-2026/
20. TechCrunch, 9 March 2026 — https://techcrunch.com/2026/03/09/salt-typhoon-china-who-has-been-hacked-global-telecom-giants/
21. Trellix — APT28 CVE-2026-21509 Campaign — https://www.trellix.com/blogs/research/apt28-stealthy-campaign-leveraging-cve-2026-21509-cloud-c2/
22. Unit 42 — Iranian Cyberattacks 2026 — https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
23. The Hacker News, March 2026 — https://thehackernews.com/2026/03/149-hacktivist-ddos-attacks-hit-110.html

# 5. RANSOMWARE ACTIVITY




South Africa recorded **91 total ransomware victims** tracked to date in 2026, with **3 new victims** in Week 12.[24] The ransomware landscape is dominated by **The Gentlemen** (4 SA victims Q1), **Vect** (2 victims), and **LockBit 5** (latest iteration of the LockBit operation, now operating as part of a formal cartel with Qilin and DragonForce).[25]

## SA Ransomware Victims — Q1 2026

| Date | Organisation | Sector | Group |
|---|---|---|---|
| 6 Jan | Hytec SA | Engineering | Vect |
| 12 Jan | Land Bank | Financial | Unknown RaaS |
| 20 Jan | Witzenberg Municipality | Government | The Gentlemen |
| 20 Jan | Rola Motor Group | Automotive | The Gentlemen |
| 20 Jan | Paltrack | Logistics | The Gentlemen |
| 15 Feb | Intsika Yethu Municipality | Government | The Gentlemen |
| 24 Feb | EnerTec | Manufacturing | Vect |
| 1 Mar | Diesel-Electric Group | Automotive | LockBit 5 |
| 6 Mar | Lion of Africa Insurance | Insurance | Lynx |
| 9 Mar | Gauteng Provincial Govt | Government | XP95 (data theft) |
| 12 Mar | RE/MAX Southern Africa | Real Estate | Team Cyber Strike |

**Global Context:** BlackFog reported 82 publicly disclosed ransomware incidents globally in February 2026, with healthcare accounting for 31% of attacks.[26] Publicly disclosed ransomware increased 49% YoY in 2025 with 7,079 victims announced on dark web leak sites — and 86% of all ransomware attacks are never publicly reported.[27]

24. Ransomware.live SA Map — https://www.ransomware.live/map/ZA
25. Dark Reading — Extortion Gangs Join Forces — https://www.darkreading.com/cyberattacks-data-breaches/extortion-gangs-join-forces-ransomware-cartel
26. BlackFog State of Ransomware 2026 — https://www.blackfog.com/the-state-of-ransomware-2026/

27. BlackFog 2025 Annual Report, Feb 2026 — https://www.blackfog.com/2025-state-of-ransomware-report-released/

# 6. CRITICAL VULNERABILITIES


This week saw **6 new CISA KEV entries** and **94 Microsoft patches** (March Patch Tuesday).[28] Two Cisco FMC vulnerabilities scored **CVSS 10.0**.[29] Two Chrome zero-days were actively exploited in the wild.[30]

## Priority Vulnerability Matrix

| CVE ID | Vendor/Product | CVSS | Exploited | Patch |
|---|---|---|---|---|
| CVE-2026-20079 | Cisco Secure FMC | 10.0 | No (yet) | Yes |
| CVE-2026-20131 | Cisco Secure FMC | 10.0 | No (yet) | Yes |
| CVE-2019-17571 | SAP FS-QUO (Log4j) | 9.8 | No | Yes |
| CVE-2026-24858 | Fortinet FortiOS SSO | 9.4 | YES (KEV) | Yes |
| CVE-2026-27685 | SAP NetWeaver EP | 9.1 | No | Yes |
| CVE-2026-3909 | Chrome/Skia OOB Write | 8.8 | YES (KEV) | Yes |
| CVE-2026-3910 | Chrome/V8 | 8.8 | YES (KEV) | Yes |
| CVE-2026-21262 | MS SQL Server EoP | 8.8 | No (public) | Yes |
| CVE-2026-26110 | MS Office RCE | 8.4 | No | Yes |
| CVE-2026-26113 | MS Office RCE | 8.4 | No | Yes |
| CVE-2026-22719 | VMware Aria Ops | 8.1 | YES (KEV) | Yes |
| CVE-2025-68613 | n8n RCE | High | YES (KEV) | Yes |
| CVE-2025-26399 | SolarWinds WHD | High | YES (KEV) | Yes |
| CVE-2026-1603 | Ivanti EPM | High | YES (KEV) | Yes |
| CVE-2021-22054 | VMware Workspace ONE | High | YES (KEV) | Yes |

28. Microsoft March 2026 Security Update Guide — https://msrc.microsoft.com/update-guide/releaseNote/2026-Mar
29. Cisco Security Advisory — FMC Auth Bypass — https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2
30. The Hacker News — Chrome Zero-Days — https://thehackernews.com/2026/03/google-fixes-two-chrome-zero-days.html

# 7. PHISHING & SOCIAL ENGINEERING

## 7.1 FACEBK Card Fraud Campaign

An active card fraud campaign using the **"FACEBK" merchant descriptor** is affecting customers of all major SA banks — FNB, Standard Bank, Absa, Nedbank, and Capitec.[31] Stolen card details are used to purchase Facebook advertising credits, bypassing 3D Secure protections. Reported transaction amounts range from R941.67 to R9,262.06. FNB is reimbursing impacted customers and has introduced virtual cards with dynamic CVV.

## 7.2 SABRIC Digital Banking Fraud Statistics

SABRIC reported **98,000 digital banking fraud incidents** in 2024, up 88% from 52,000 in 2023.[32] Digital banking now accounts for 65.3% of all reported banking fraud. AI-generated **deepfake scams surged 1,200%** in SA, with a notable deepfake video impersonating SARB Governor Letsetja Kganyago promoting fake investment opportunities. Card-not-present fraud accounts for 85.6% of gross credit card losses.

## 7.3 BEC & SIM Swap Trends

Business Email Compromise attacks increased 15% in 2025 globally, with $2.7 billion in FBI-reported losses.[33] SA organisations are particularly exposed: identity-related weaknesses are found in ~90% of investigated breaches.[4] BEC tactics now include AI-generated contextually-aware emails via FraudGPT variants, "Request for Contact" dual-channel attacks, and executive impersonation.

## 7.4 Scam Signal SA Launch

South Africa became the **second country after the UK** to deploy Scam Signal, an API-based real-time intelligence system to detect Authorised Push Payment (APP) fraud during live transactions.[34] The initiative involves MTN Chenosis, FICO, GSMA, major SA banks, and SABRIC.

31. StormWarning — FACEBK Card Fraud — https://stormwarning.co.za/index.php/cybersecurity-news/fraudulent-facebk-transactions-hit-major-banks-cards-in-sa
32. iAfrica — SABRIC AI Fraud Warning — https://iafrica.com/sabric-warns-of-rising-ai-powered-fraud-in-south-africa-despite-overall-drop-in-financial-crime/
33. LevelBlue — BEC Trends 2025 — https://www.levelblue.com/blogs/spiderlabs-blog/bec-email-trends-attacks-up-15-in-2025/
34. GSMA — Scam Signal SA Launch — https://www.gsma.com/newsroom/article/scam-signal-launches-in-south-africa-to-tackle-app-fraud-and-combat-financial-crime/

# 8. REGULATORY & COMPLIANCE

## 8.1 POPIA Health Data Regulations — NOW IN FORCE

New POPIA health information processing regulations (Government Gazette No. 54268) came into force on **6 March 2026 with no grace period**.[35] Eight categories of organisations are in scope: insurance companies, medical schemes, medical scheme administrators, managed healthcare organisations, administrative bodies, pension funds, employers, and institutions acting on their behalf. Non-compliance carries a maximum administrative fine of **R10,000,000**.

## 8.2 Information Regulator Performance Data

The Information Regulator disclosed at its 2026/27 Annual Performance Plan session that it had received **2,898 security compromise notifications** to date — a 15x increase from 202 in 2021/22.[36] Only **14% of CIPC-active companies (~69,040 of ~490,000)** have registered information officers. The Regulator is drafting POPIA amendments moving toward direct financial penalties for intentional non-compliance.

## 8.3 Land Bank Triple-Reporting Obligation

The Land Bank ransomware incident illustrates the multi-regulator reporting obligation: SAPS (Cybercrimes Act, 17 Jan), Information Regulator (POPIA Section 22, 16 Jan), Prudential Authority (29 Jan + updates), and State Security Agency (9 Feb).[37] This demonstrates the compliance complexity for regulated financial institutions in South Africa.

## 8.4 SARB Directive 01 of 2024 / FSCA Joint Standard

The SARB Directive on Cybersecurity within the National Payment System (issued May 2024) is in active enforcement.[38] Key requirements: 24-hour incident reporting, quarterly resilience testing, 2-hour recovery for critical systems. The FSCA/PA Joint Standard 2 of 2024 (effective June 2025) requires board-approved cybersecurity strategy, annual penetration testing, MFA, and 24-hour material incident reporting.[39]

### Compliance Deadlines Summary

| Deadline | Obligation | Regulator |
|---|---|---|
| Immediate (6 Mar 2026) | Health information processing safeguards | Information Regulator |
| Active (past due) | NPS cybersecurity compliance | SARB |
| Active (from Jun 2025) | Financial institution cybersecurity | FSCA / PA |
| June 2026 | Regulation S-P cybersecurity (US) | SEC |
| March 2026 (expected) | SA Draft AI Policy public comment | DCDT |

35. Moonstone, 12 March 2026 — https://www.moonstone.co.za/new-popia-regulations-on-health-information-now-in-force/
36. ITLawCo, 6 March 2026 — https://itlawco.com/information-regulator-2026-27-annual-performance-plan/
37. Tech4Law, 9 March 2026 — https://www.tech4law.co.za/news-in-brief/security-news-in-brief/hackers-demanded-r5-7-million-after-bringing-important-south-african-bank-to-its-knees/
38. Michalsons — SARB Directive — https://www.michalsons.com/blog/sarb-cybersecurity-and-cyber-resilience-directive/78268
39. LEX Africa, 26 February 2026 — https://lexafrica.com/2026/02/south-africas-cybersecurity-shift-2026/

# 9. OSINT EXPOSURE

## 9.1 Gauteng Data on Dark Web Marketplace

The Gauteng Provincial Government dataset (3.8 TB / 3,673,556 files) was listed on a dark web forum and Telegram channel by threat actor XP95 for $25,000.[10] The data includes provincial healthcare records, education PII, housing title deeds, and employment application records — creating industrialised risk of identity theft via National ID numbers, SARS eFiling fraud, and retail credit fraud.

## 9.2 SA-Hosted Malware Infrastructure

URLhaus identified **10 South African IP addresses** actively hosting malware payloads (primarily Mirai/botnet loader scripts).[40] Key IPs include:

| IP Address | Payload | Range |
|---|---|---|
| 154.9.241.34 | Mirai variants (x86, MIPS, MPSL) | AFRINIC |
| 105.225.239.100 | Botnet loader / shell script | SA ISP (105.x) |

| IP Address | Payload | Range |
|---|---|---|
| 196.189.9.27 | Botnet loader | 196.x Africa range |
| 196.189.96.59 | Botnet loader / shell script | 196.x Africa range |
| 196.190.1.39 | Botnet loader | 196.x Africa range |

### 9.3 HIBP Status

No new SA-specific organisations were added to the HIBP database during March 9–15, 2026.[41] The Land Bank and Gauteng incidents are active but have not yet appeared in HIBP. The absence of entries does not indicate absence of breach data — it means datasets have not been catalogued by HIBP.

40. URLhaus Recent Malware URLs — https://urlhaus.abuse.ch/downloads/text_recent/
41. HIBP API v3 — Breaches — https://haveibeenpwned.com/api/v3/breaches

## 10. WEEKLY THREAT HUNT & IOCs

This section provides structured hunt missions for SOC analysts and threat hunters. Each mission includes a hypothesis, MITRE ATT&CK mapping, indicators of compromise, and recommended data sources. Prioritise P1 missions for immediate execution.

### 10a. Hunt Missions

**TH-2026-W12-01: Gauteng/XP95 Data Exfiltration** — **P1 — CRITICAL**

**Hypothesis:** XP95 may have maintained persistent access to Gauteng provincial systems. Hunt for unusual large data transfers (3.8 TB exfil indicates sustained access), unauthorized remote access tools, and lateral movement from internet-facing servers.

**MITRE ATT&CK:** T1071 (App Layer Protocol), T1048 (Exfiltration Over Alternative Protocol), T1078 (Valid Accounts), T1005 (Data from Local System)

**IOCs:** XP95 threat actor indicators (check dark web marketplace listings)

**Data Sources:** Firewall logs (large outbound transfers), proxy logs, DLP alerts, Active Directory audit logs

**TH-2026-W12-02: Salt Typhoon Telecom Espionage** — **P1 — CRITICAL**

**Hypothesis:** Salt Typhoon has confirmed SA telecom targeting. Hunt for compromise of Cisco IOS-XE routers, lawful intercept system access, and passive network intelligence collection.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing App), T1557 (Adversary-in-the-Middle), T1040 (Network Sniffing)

**IOCs:** C2 domains: login[.]citrixtv[.]com, login[.]vmwaretv[.]com, update[.]vmwaretv[.]com, api[.]citrixtv[.]com, cdn[.]citrixtv[.]com. IPs: 45.77.46.118, 45.32.162.37, 108.61.214.194, 149.28.68.101, 207.148.14.48. Malware: TernDoor, PeerTime, BruteEntry.

**Data Sources:** Router logs, NetFlow, DNS logs, EDR

**TH-2026-W12-03: Chrome Zero-Day Exploitation** — **P1 — CRITICAL**

**Hypothesis:** Chrome zero-days CVE-2026-3909 (Skia OOB write) and CVE-2026-3910 (V8) are actively exploited. Hunt for exploitation indicators in browser telemetry.

**MITRE ATT&CK:** T1189 (Drive-by Compromise), T1203 (Exploitation for Client Execution)

**IOCs:** Chrome versions below 146.0.7680.75

**Data Sources:** Software inventory, EDR browser process monitoring, web proxy logs

**TH-2026-W12-04: RE/MAX / Team Cyber Strike SQL Injection** — **P2 — HIGH**

**Hypothesis:** Team Cyber Strike used brute-force + SQL injection against RE/MAX. Similar attacks may target other SA real estate/property firms.

**MITRE ATT&CK:** T1110 (Brute Force), T1190 (Exploit Public-Facing App), T1505.001 (SQL Stored Procedures)

**IOCs:** N/A — hunt for SQL injection patterns

**Data Sources:** WAF logs, database audit logs, IDS/IPS alerts for SQL injection signatures

### TH-2026-W12-05: FACEBK Card Fraud Campaign — P2 — HIGH

**Hypothesis:** Active card fraud campaign bypassing 3D Secure across all major SA banks. Hunt for FACEBK merchant descriptor in transaction logs.

**MITRE ATT&CK:** T1656 (Impersonation), T1078 (Valid Accounts)

**IOCs:** "FACEBK" merchant descriptor in card-not-present transactions

**Data Sources:** Transaction monitoring, fraud detection systems, card issuer alerts

### TH-2026-W12-06: Lynx Ransomware — P2 — HIGH

**Hypothesis:** Lynx (INC Ransomware rebrand) hit Lion of Africa Insurance on ~6 March. Hunt for .LYNX file extension, README.txt ransom notes, and Restic exfiltration tool usage.

**MITRE ATT&CK:** T1486 (Data Encrypted for Impact), T1489 (Service Stop), T1041 (Exfiltration)

**IOCs:** .LYNX file extension, README.txt ransom note, Restic.exe, SoftPerfect NetScan

**Data Sources:** EDR (process creation for Restic.exe, SoftPerfect NetScan), file system monitoring, Sysmon Event ID 1

### TH-2026-W12-07: SA-Hosted Malware Infrastructure — P3 — MEDIUM

**Hypothesis:** SA IP addresses are actively serving IoT botnet payloads. Monitor and block.

**MITRE ATT&CK:** N/A — infrastructure monitoring

**IOCs:** 154.9.241.34, 105.225.239.100, 196.189.9.27, 196.189.96.59, 196.190.1.39

**Data Sources:** Firewall logs, DNS sinkholes, threat feed integration

### TH-2026-W12-08: Cisco FMC CVSS 10.0 Pre-Positioning — P2 — HIGH

**Hypothesis:** Two CVSS 10.0 Cisco FMC vulnerabilities (CVE-2026-20079, CVE-2026-20131) have no workarounds. Hunt for unauthorized access to Cisco FMC management interfaces.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing App), T1068 (Exploitation for Privilege Escalation)

**IOCs:** CVE-2026-20079, CVE-2026-20131

**Data Sources:** Cisco FMC audit logs, network access to management interfaces, vulnerability scans

## 10b. Hunt Checklist

Print or copy this table into your ticketing system to track hunt execution.

| Hunt ID | Hypothesis (short) | Priority | Data Sources | Status |
|---|---|---|---|---|
| TH-2026-W12-01 | Gauteng/XP95 persistent access | P1 | FW, Proxy, DLP, AD | Not Started |
| TH-2026-W12-02 | Salt Typhoon telecom compromise | P1 | Router, NetFlow, DNS, EDR | Not Started |
| TH-2026-W12-03 | Chrome zero-day exploitation | P1 | Software inv, EDR, Proxy | Not Started |
| TH-2026-W12-04 | SQL injection (RE/MAX pattern) | P2 | WAF, DB audit, IDS/IPS | Not Started |
| TH-2026-W12-05 | FACEBK card fraud campaign | P2 | Txn monitoring, Fraud sys | Not Started |
| TH-2026-W12-06 | Lynx ransomware indicators | P2 | EDR, File mon, Sysmon | Not Started |
| TH-2026-W12-07 | SA malware infrastructure IPs | P3 | FW, DNS sinkhole, TI feeds | Not Started |
| TH-2026-W12-08 | Cisco FMC CVSS 10.0 pre-posn | P2 | FMC logs, Vuln scans | Not Started |

## 10c. IOC Master Table

Consolidated indicators of compromise for SIEM/EDR ingestion. Validate in organisational context before blocking.

| Indicator | Type | Attribution | Hunt ID |
|---|---|---|---|
| login[.]citrixtv[.]com | Domain | Salt Typhoon | TH-W12-02 |
| login[.]vmwaretv[.]com | Domain | Salt Typhoon | TH-W12-02 |
| update[.]vmwaretv[.]com | Domain | Salt Typhoon | TH-W12-02 |
| api[.]citrixtv[.]com | Domain | Salt Typhoon | TH-W12-02 |
| cdn[.]citrixtv[.]com | Domain | Salt Typhoon | TH-W12-02 |
| updata.mgil01.workers.dev | Domain | Salt Typhoon | TH-W12-02 |
| service.oneipsoft.com | Domain | Salt Typhoon | TH-W12-02 |
| myoffice.techralsolution.com | Domain | Salt Typhoon | TH-W12-02 |
| 45.77.46.118 | IPv4 | Salt Typhoon | TH-W12-02 |
| 45.32.162.37 | IPv4 | Salt Typhoon | TH-W12-02 |
| 108.61.214.194 | IPv4 | Salt Typhoon | TH-W12-02 |
| 149.28.68.101 | IPv4 | Salt Typhoon | TH-W12-02 |
| 207.148.14.48 | IPv4 | Salt Typhoon | TH-W12-02 |
| 13.89.97.154 | IPv4 | Salt Typhoon | TH-W12-02 |
| 114.119.158.36 | IPv4 | Salt Typhoon | TH-W12-02 |
| 34.234.200.207 | IPv4 | Salt Typhoon | TH-W12-02 |
| 54.225.199.17 | IPv4 | Salt Typhoon | TH-W12-02 |
| 23.23.103.31 | IPv4 | Salt Typhoon | TH-W12-02 |
| 154.9.241.34 | IPv4 | Mirai Botnet | TH-W12-07 |
| 105.225.239.100 | IPv4 | Mirai Botnet | TH-W12-07 |
| 196.189.9.27 | IPv4 | Botnet Loader | TH-W12-07 |
| 196.189.96.59 | IPv4 | Botnet Loader | TH-W12-07 |
| 196.190.1.39 | IPv4 | Botnet Loader | TH-W12-07 |
| filen.io (C2 usage) | Domain | APT28 | N/A |
| BULLETEN_H.doc | Filename | APT28 | N/A |
| Courses.doc | Filename | APT28 | N/A |
| OperInformativ_163.doc | Filename | APT28 | N/A |
| ps1u_ex200822.ps1 | Filename | Salt Typhoon | TH-W12-02 |
| win32.exe / win32.dll | Filename | Salt Typhoon | TH-W12-02 |
| 7896a1429d79...f7108 | SHA256 | AMOS Stealer | N/A |
| 5efe3d6ff690...72a62 | SHA256 | AMOS Stealer | N/A |
| ClearI_AI.dmg | Filename | AMOS Stealer | N/A |
| *.chip1 | File Ext | Chip Ransomware | N/A |
| Recovery_README.html | Filename | Chip Ransomware | N/A |
| FACEBK (merchant desc) | Indicator | Card Fraud | TH-W12-05 |
| .LYNX | File Ext | Lynx Ransomware | TH-W12-06 |
| Restic.exe | Tool | Lynx Ransomware | TH-W12-06 |
| cloud-noc@mail.io | Email | Fortinet CVE-24858 | N/A |
| cloud-init@mail.io | Email | Fortinet CVE-24858 | N/A |

# 11. RECOMMENDATIONS

## IMMEDIATE (This Week)

- **PATCH:** Update Chrome to 146.0.7680.75+ across all endpoints (Sec 6). Apply Cisco FMC patches for CVE-2026-20079 and CVE-2026-20131 (CVSS 10.0). Deploy Microsoft March 2026 Patch Tuesday updates.
- **BLOCK:** Add all Salt Typhoon C2 domains and IPs from Section 10c to blocklists. Block SA-hosted malware IPs (154.9.241.34, 105.225.239.100 etc).
- **HUNT:** Execute P1 hunt missions TH-W12-01 through TH-W12-03 (Sec 10a). Prioritise XP95/Gauteng indicators and Salt Typhoon on Cisco routers.
- **COMPLY:** Initiate POPIA health data compliance review — regulations effective 6 March, no grace period, R10M penalty (Sec 8).
- **MONITOR:** Watch for FACEBK merchant descriptor in card transaction logs (Sec 7). Review VMware Aria Operations patch status before March 24 KEV deadline.

## SHORT-TERM (This Quarter)

- Conduct phishing simulation focused on AI-generated BEC emails and FACEBK-style fraud (Sec 7).
- Audit Information Officer registration status — 86% of SA companies non-compliant (Sec 8).
- Implement BEC detection rules for dual-channel "Request for Contact" attacks and FraudGPT-generated emails.
- Execute Salt Typhoon threat hunt on all Cisco IOS-XE routers and telco infrastructure (Sec 10a, TH-W12-02).
- Review and strengthen SQL injection WAF rules — Team Cyber Strike attack vector on RE/MAX (Sec 3, TH-W12-04).
- Implement Scam Signal API or equivalent real-time fraud detection for payment systems (Sec 7).

## STRATEGIC (Next 6-12 Months)

- Prepare for POPIA amendment legislation moving toward direct financial penalties for intentional non-compliance (Sec 8).
- Deploy AI-powered threat detection and deepfake detection for voice/video authentication — deepfakes up 1,200% (Sec 7).
- Implement external risk scoring and dark web monitoring as standard practice — Gauteng data selling for $25,000 illustrates the risk (Sec 9).
- Align cybersecurity programme with NIST CSF 2.0 / ISO 27001 as required by SARB Directive and FSCA Joint Standard (Sec 8).
- Establish board-level cyber risk reporting — cyber risk is a governance failure, not a technical problem (Wits/Interpol).
- Invest in government sector resilience — the sector is under sustained multi-vector pressure from criminal and state-sponsored actors (Sec 2).
- Initiate post-quantum cryptography readiness assessment aligned with EU NIS2 2030 timeline (Sec 8).

# 12. OSINT SOURCES CONSULTED

| # | Source | URL |
|---|---|---|
| 1 | Ransomware.live — SA Victims Map | https://www.ransomware.live/map/ZA |
| 2 | CISA KEV Catalog | https://www.cisa.gov/known-exploited-vulnerabilities-catalog |
| 3 | CYFIRMA Weekly Intel Report, 13 March 2026 | https://www.cyfirma.com/news/weekly-intelligence-report-13-m... |
| 4 | The Citizen, 14 March 2026 | https://www.citizen.co.za/news/panyaza-lesufi-responds-gaute... |
| 5 | Brinztech Threat Alert, 13 March 2026 | https://www.brinztech.com/breach-alerts/brinztech-alert-3-8-... |
| 6 | RE/MAX SA Incident Notice | https://www.remax.co.za/cyber-incident-notice |
| 7 | IOL Business Report, 12 March 2026 | https://iol.co.za/business-report/companies/2026-03-12-how-t... |
| 8 | ITWeb, 9 March 2026 — Land Bank | https://www.itweb.co.za/article/land-bank-tightens-security-... |
| 9 | Tech4Law, 9 March 2026 | https://www.tech4law.co.za/news-in-brief/security-news-in-br... |
| 10 | BlackFog State of Ransomware 2026 | https://www.blackfog.com/the-state-of-ransomware-2026/ |
| 11 | TechTrends Africa, 11 March 2026 | https://techtrends.africa/global-cyber-attacks-stay-near-rec... |
| 12 | TechCentral, 5 March 2026 — Insider Threats | https://techcentral.co.za/malicious-insider-threats-surging-... |
| 13 | CrowdStrike 2026 Global Threat Report | https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-glob... |
| 14 | Recorded Future 2026 State of Security | https://www.recordedfuture.com/research/state-of-security |
| 15 | TechCrunch — Salt Typhoon, 9 March 2026 | https://techcrunch.com/2026/03/09/salt-typhoon-china-who-has... |
| 16 | Trellix — APT28 Campaign | https://www.trellix.com/blogs/research/apt28-stealthy-campai... |
| 17 | Unit 42 — Iranian Cyberattacks 2026 | https://unit42.paloaltonetworks.com/iranian-cyberattacks-202... |
| 18 | The Hacker News — Hacktivist DDoS | https://thehackernews.com/2026/03/149-hacktivist-ddos-attack... |
| 19 | Microsoft March 2026 Security Update | https://msrc.microsoft.com/update-guide/releaseNote/2026-Mar |
| 20 | Cisco FMC Advisory | https://sec.cloudapps.cisco.com/security/center/content/Cisc... |
| 21 | StormWarning — FACEBK Fraud | https://stormwarning.co.za/index.php/cybersecurity-news/frau... |
| 22 | SABRIC via iAfrica | https://iafrica.com/sabric-warns-of-rising-ai-powered-fraud-... |
| 23 | GSMA — Scam Signal SA | https://www.gsma.com/newsroom/article/scam-signal-launches-i... |
| 24 | LevelBlue — BEC Trends | https://www.levelblue.com/blogs/spiderlabs-blog/bec-email-tr... |
| 25 | Moonstone — POPIA Health Regs | https://www.moonstone.co.za/new-popia-regulations-on-health-... |
| 26 | ITLawCo — Information Regulator | https://itlawco.com/information-regulator-2026-27-annual-per... |
| 27 | Michalsons — SARB Directive | https://www.michalsons.com/blog/sarb-cybersecurity-and-cyber... |
| 28 | LEX Africa — Cybersecurity 2026 | https://lexafrica.com/2026/02/south-africas-cybersecurity-sh... |
| 29 | URLhaus Malware URLs | https://urlhaus.abuse.ch/downloads/text_recent/ |
| 30 | HIBP API | https://haveibeenpwned.com/api/v3/breaches |
| 31 | Dark Reading — Ransomware Cartel | https://www.darkreading.com/cyberattacks-data-breaches/extor... |
| 32 | DeXpose — The Gentlemen | https://www.dexpose.io/the-gentlemen-ransomware-attack-on-in... |
| 33 | ITWeb — Kimwolf Botnet | https://www.itweb.co.za/article/kimwolf-at-the-door-why-sa-a... |
| 34 | Wits University — Cyber Risk | https://www.wits.ac.za/news/latest-news/opinion/2026/2026-03... |
| 35 | Fortinet PSIRT Advisories | https://www.fortiguard.com/psirt |
| 36 | Broadcom VMSA-2026-0001 | https://support.broadcom.com/web/ecx/support-content-notific... |
| 37 | SAP March 2026 Patch Day | https://support.sap.com/en/my-support/knowledge-base/securit... |