SOUTH AFRICA
CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 14 | 23-29 March 2026

THREAT LEVEL: HIGH

XP95 hits Stats SA (154GB stolen), Liberty 3.2M-customer breach, DragonForce 316GB confirmed, F5 BIG-IP RCE nation-state exploitation, AI-powered banking fraud surges +86% YoY

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W14 | Classification: TLP:WHITE

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH — Sustained from the prior week. XP95 claimed its second SA government victim (Statistics South Africa, 29 March — 154 GB / 453,362 files stolen). Liberty Group SA disclosed a breach affecting up to 3.2M customers (names, ID numbers). DragonForce data volume on The Unlimited confirmed at 316.63 GB. F5 BIG-IP APM CVE-2025-53521 (CVSS 9.8) reclassified from DoS to RCE with Chinese nation-state exploitation confirmed. AI-powered digital banking fraud surged 86% YoY with R1.888B in losses.[1]

KPI Dashboard

Metric	Current (W14)	Baseline / Prior	Change	Direction
SA breach frequency	Every 3 hours	Every 4.2 hrs (2025 avg)	-28% interval	UP (worse)
Cyberattacks/week per org	2,145	1,577 (Jan 2025)	+36% YoY	UP
POPIA notifications YTD	2,898 (FY 2025/26)	2,374 (full FY 2024/25)	Exceeded prior FY	UP
Ransomware recovery cost avg	R5.4M (Land Bank)	R3.2M (2025 avg)	+69%	UP
SA ransomware victims total	96 (95 + Stats SA)	94 (end W13)	+2 new W14	UP

ANOMALY FLAG: All five KPI metrics trending above baseline. POPIA breach notifications in FY 2025/26 have already exceeded the entire prior financial year total of 2,374. Government sector under unprecedented multi-vector pressure with three entities under simultaneous active extortion.[2]

TOP 3 ACTIONS THIS WEEK

1. PATCH F5 BIG-IP APM IMMEDIATELY: CVE-2025-53521 (CVSS 9.8) reclassified from DoS to RCE; Chinese nation-state exploitation confirmed; Brickstorm backdoor link; CISA deadline 30 March (TODAY). Check for /run/bigtlog.pipe and /run/bigstart.ltm indicators.

2. HUNT FOR XP95 IOCs IN GOVERNMENT NETWORKS: XP95 hit Stats SA (29 March) after Gauteng Provincial Government; second government target in one month; pure data extortion via unpatched internet-facing servers. Audit all internet-facing assets.

3. VERIFY LIBERTY BREACH EXPOSURE: If your organisation uses Liberty insurance products, assume your client data (names, ID numbers) may be compromised; enable enhanced fraud monitoring for identity theft. Review POPIA s22 notification obligations.

Critical Findings:

- Statistics South Africa (Stats SA) claimed by XP95 on 29 March — 154 GB / 453,362 files stolen; deadline 20 April 2026. Second SA government target by XP95 after Gauteng (3.8 TB).[3]
- Liberty Group SA disclosed a breach (23-24 March) potentially affecting 3.2M customers; names and ID numbers compromised; extortion attempted and refused; repeat breach (2018). Major POPIA test case.[4]
- DragonForce data volume on The Unlimited confirmed at 316.63 GB (Breachsense, 23 March); leak imminent if ransom not paid.[5]
- F5 BIG-IP APM CVE-2025-53521 (CVSS 9.8) reclassified to RCE; Chinese nation-state exploitation confirmed; Brickstorm backdoor deployed; CISA KEV added 27 March with 30 March deadline.[6]
- Digital banking fraud surged 86% YoY to 97,975 incidents with R1.888B in losses; banking apps account for 65.3% of fraud; AI-powered fraud 4.5x more profitable (INTERPOL).[7]

SECTOR SPOTLIGHT: GOVERNMENT / PUBLIC SECTOR (CRITICAL)

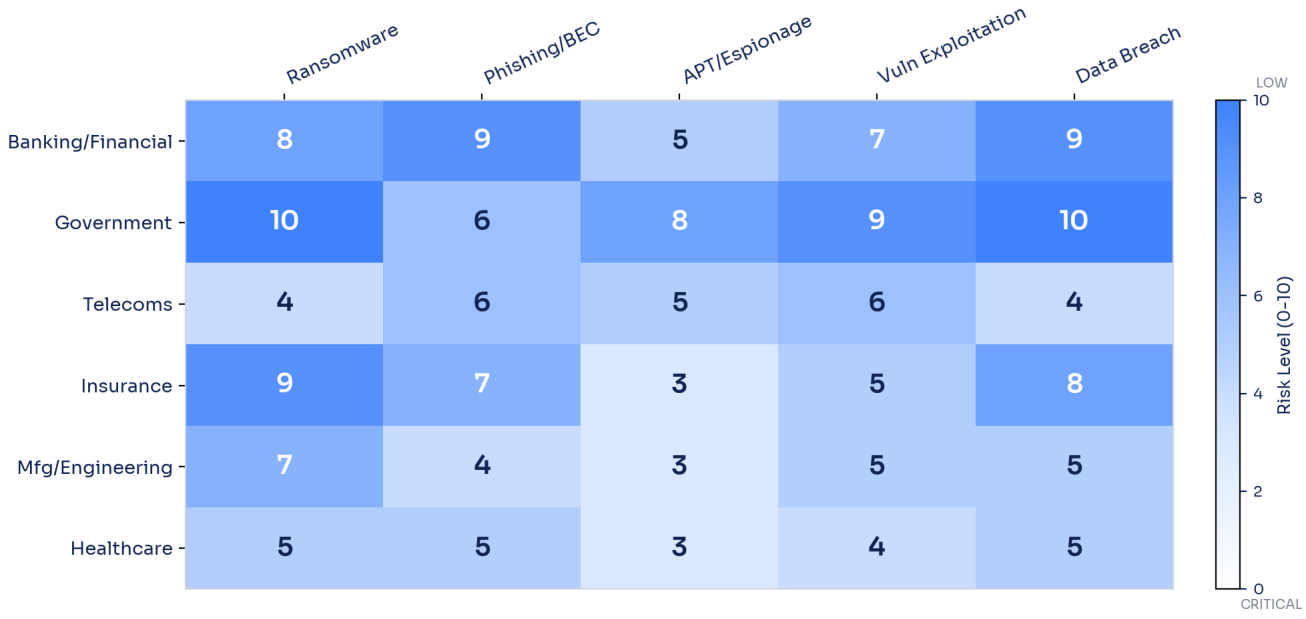
Government is the most at-risk sector this week. XP95 claimed its SECOND South African government victim in one month (Stats SA, 29 March — 154 GB / 453,362 files stolen). TheGentlemen re-listed Elundini Municipality. Combined with the ongoing Gauteng 3.8 TB breach, **three government entities are under active extortion simultaneously**. Root cause across all: unpatched, internet-facing servers with end-of-life infrastructure. 70% of Gauteng's network devices were past end-of-service. This is systemic, not isolated.[3]

1. ITWeb, 20 March 2026 — Listed firms risk 30% share plunge — https://www.itweb.co.za/article/listed-firms-risk-30-share-plunge-amid-rising-cyber-attacks/Olx4z7kawaQq56km
2. IOL, 20 March 2026 — Data breaches every 3 hours — https://iol.co.za/business-report/economy/2026-03-20-data-breaches-in-south-africa-occur-every-three-hours-with-90-deemed-preventable/
3. Daily Maverick, 17 March 2026 — Gauteng breach — https://www.dailymaverick.co.za/article/2026-03-17-gauteng-was-lucky-with-latest-38tb-data-breach-but-the-luck-will-run-out/
4. ITWeb, 24 March 2026 — Liberty data breach — https://www.itweb.co.za/article/insurer-liberty-hit-by-data-breach/o1Jr5MxPwrdMKdWL
5. Breachsense, 23 March 2026 — The Unlimited — https://www.breachsense.com/breaches/the-unlimited-group-data-breach/
6. Help Net Security, 28 March 2026 — F5 BIG-IP exploitation — https://www.helpnetsecurity.com/2026/03/28/big-ip-apm-vulnerability-cve-2025-53521-exploited/
7. SABRIC Annual Crime Statistics 2024 — https://www.sabric.co.za/wp-content/uploads/2025/09/CRIME-STATISTICS-REPORT-2024.pdf

2. THREAT LANDSCAPE HEATMAP

The heatmap below maps six 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 14.

SA THREAT LANDSCAPE HEATMAP | W14 (23-29 Mar 2026)



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 (9-10)** = active exploitation or confirmed breach; **High (7-8)** = credible active threat; **Medium (4-6)** = elevated baseline risk; **Low (1-3)** = standard risk posture.

3. SA CYBER INCIDENTS & BREACHES

3.1 Statistics South Africa — XP95 Data Extortion (NEW — BREAKING)

XP95 claimed Statistics South Africa (statssa.gov.za) on **29 March 2026** — **154 GB / 453,362 files** stolen.[3] This is XP95's second SA government target after Gauteng Provincial Government (3.8 TB, March 13). Deadline for payment set at 20 April 2026. Attack vector consistent with XP95's MO: exploitation of unpatched internet-facing servers for mass data exfiltration without encryption (pure data extortion). Stats SA holds sensitive national demographic, economic, and census data. This represents a critical escalation of government-targeting activity.

3.2 Liberty Group SA — Customer Data Breach (NEW)

Liberty Group (liberty.co.za, Standard Bank subsidiary) disclosed unauthorised access to data systems on **23-24 March 2026**.[4] Customer names, ID numbers, and email data confirmed compromised. Liberty has approximately 3.2M customers continent-wide. Extortion was attempted; Liberty refused to pay. IOL (25 March) clarified the breach specifically impacted email systems.[8] This is Liberty's second major breach after the 2018 email repository exfiltration. The breach is a significant POPIA test case given the involvement of ID numbers, repeat offender status, and the Information Regulator's stated priority to enforce against financial services entities.

3.3 ETFSA — Incransom Ransomware (NEW)

Incransom listed ETFSA (etfsa.co.za) on its leak site on **26 March 2026**. ETFSA is a financial services ETF platform. The CEO was named in the leak post. Data leak threatened. Incransom operates as a RaaS group with historical exploitation of CVE-2023-3519 (Citrix NetScaler) for initial access.

3.4 Virgin Active SA — IDOR / Payment Vulnerability (NEW)

An Insecure Direct Object Reference (IDOR) vulnerability was disclosed at **Virgin Active SA** on **24 March 2026** by ethical hacker Bruce Malaudzi via MyBroadband.[9] The flaw exposed member PII (names, email addresses, amounts owed, gym branch) for 631,000 members and enabled payment manipulation (R1,425 reduced to R1). Backend auth tokens were exposed in plaintext. Virgin Active disabled affected payment links; security review conducted.

3.5 The Unlimited — DragonForce (UPDATE: 316.63 GB Confirmed)

Breachsense confirmed on 23 March 2026 that DragonForce's data volume on The Unlimited stands at **316.63 GB**.[5] The Unlimited offers health, auto, legal, and life insurance products. No public response from the organisation. DragonForce is actively operating as a RaaS cartel allowing affiliates to create sub-brands. Leak publication imminent if ransom not paid.

3.6 Carry-Over Incidents

- **Semenya Furumele Consulting Engineers (Nightspire):** Still in negotiation phase. NightSpire leak site shows "Data is not available now" consistent with active negotiations.[10]
- **Elundini Local Municipality (TheGentlemen):** Re-listing remains active; full leak threatened. Long breach-to-disclosure gap (Oct 2025 to Mar 2026).[11]
- **Gauteng Provincial Government (XP95):** 3.8 TB / 3,673,556 files. No resolution; DA parliamentary inquiry ongoing. No ransom payment confirmed.[3]
- **RE/MAX SA (Team Cyber Strike):** Operationally recovered; data impact assessment still in progress. POPIA notification filed.[12]

8. IOL, 25 March 2026 — Liberty email systems — https://iol.co.za/business/2026-03-25-liberty-confirms-data-breach-email-systems-compromised-but-client-assets-secure/

9. MyBroadband, 24 March 2026 — Virgin Active IDOR — https://mybroadband.co.za/news/security/635179-security-vulnerability-at-biggest-gym-chain-in-south-africa.html
10. DeXpose, 23 March 2026 — Nightspire / Semenya Furumele — https://www.dexpose.io/nightspire-targets-semenya-furumele-consulting-engineers/
11. DeXpose, 21 March 2026 — TheGentlemen / Elundini — https://www.dexpose.io/thegentlemen-ransomware-strikes-elundini-local-municipality/
12. RE/MAX SA Incident Notice — https://www.remax.co.za/cyber-incident-notice

4. ACTIVE THREAT CAMPAIGNS

4.1 AI-Powered Banking Fraud Surge

Digital banking fraud exploded to **97,975 incidents** in 2024 (**+86% YoY**), with gross losses of **R1.888 billion** (+74%).[7] Banking apps account for 65.3% of all fraud incidents. INTERPOL's 2026 Global Financial Fraud Assessment (16 March) warns that AI-enhanced fraud is **4.5x more profitable** than traditional methods, with "agentic AI" systems autonomously executing complete fraud campaigns.[13] Capitec stopped 64,000+ mule accounts in 15 months, indicating the scale of organised crime infrastructure. Discovery Bank claims zero card fraud via counter-vishing controls (blocking payments during active phone calls).[14]

4.2 Tycoon2FA PhaaS with .za.com Domains

The CrowdStrike-documented Tycoon2FA phishing-as-a-service platform, disrupted by Europol on 4 March 2026 (330 domains seized), continued operating post-disruption. .za.com domains identified in active MFA-bypass campaigns:[15]

- 811inboard.aeroprimelink.za.com — threat actor-controlled, first observed 6 March 2026
- pass.aeroprimelink.za.com — compromised third-party domain

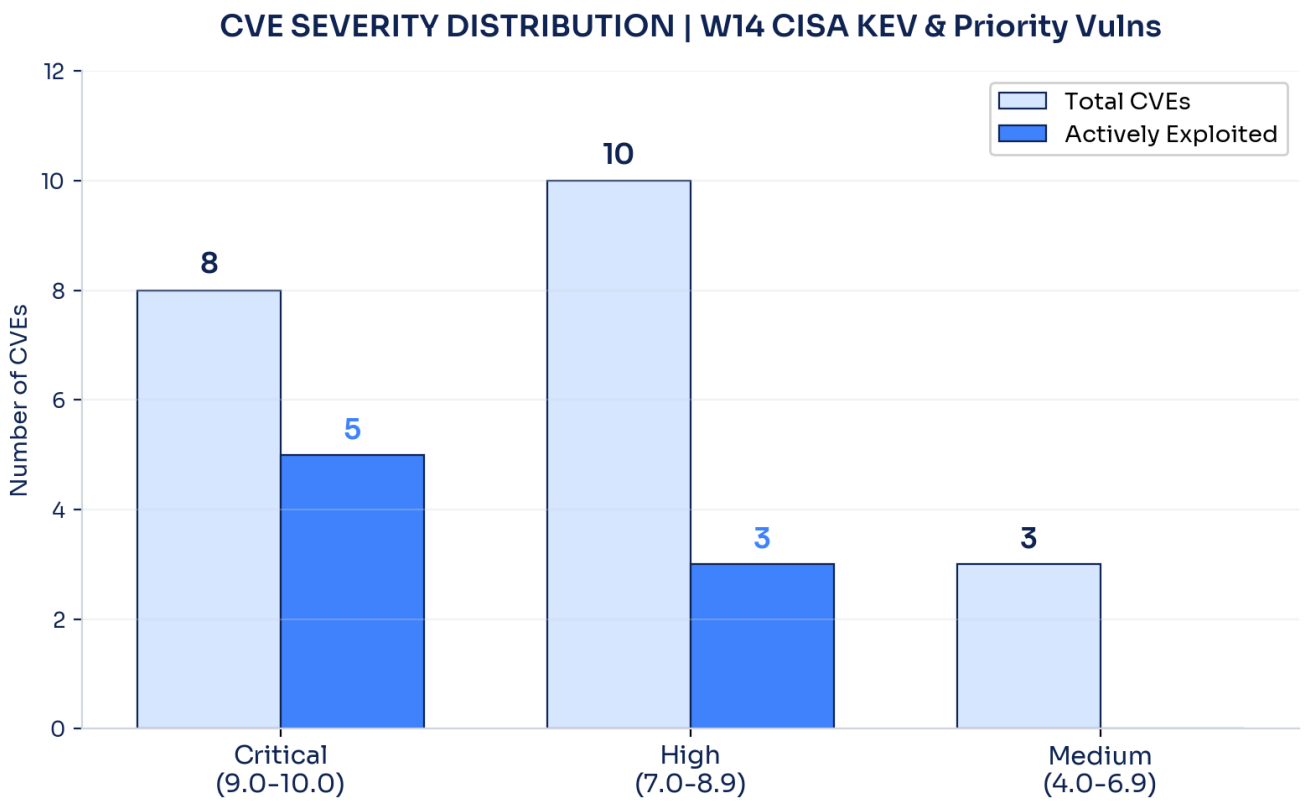
Post-disruption campaigns include BEC phishing, email thread hijacking, cloud account takeover, and SharePoint compromise.

4.3 Business Email Compromise Trends

BEC attack losses remain significant. The National Financial Ombud (NFO) finds in favour of banks in 79% of banking fraud cases, placing the burden of proof on customers.[14] Standard Bank customers reported accounts wiped by fraudsters following vishing attacks (March 2026). SMS accounts for 66% and messaging apps 32% of BEC attack channels in 2025. SABRIC confirms 100% of digital fraud cases involved compromised customer credentials through social engineering.[7]

13. INTERPOL — 2026 Global Financial Fraud Threat Assessment — https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat
14. Daily Maverick, 26 March 2026 — SA bank with zero fraud — https://www.dailymaverick.co.za/article/2026-03-26-the-sa-bank-with-zero-fraud-in-an-industry-risking-complacency-with-the-crime/
15. CrowdStrike — Tycoon2FA Persistence — https://www.crowdstrike.com/en-us/blog/tycoon2fa-phishing-as-a-service-platform-persists-following-takedown/

5. CRITICAL VULNERABILITIES



Week 14 saw **3 new CISA KEV entries** (Langflow, Trivy, F5 BIG-IP APM) with continued fallout from Cisco FMC (CVSS 10.0) Interlock ransomware campaign. F5 BIG-IP APM CVE-2025-53521 was reclassified from DoS to RCE with Chinese nation-state exploitation confirmed. Citrix NetScaler CVE-2026-3055 (CVSS 9.3) under active reconnaissance — similar to CitrixBleed.[6]

CISA KEV Additions — W14

CVE ID	Product	CVSS	Date Added	Action Due
CVE-2026-33017	Langflow (AI platform)	9.3	25 Mar 2026	8 Apr 2026
CVE-2026-33634	Aquasecurity Trivy	9.4	26 Mar 2026	9 Apr 2026
CVE-2025-53521	F5 BIG-IP APM	9.8	27 Mar 2026	30 Mar 2026

Priority Vulnerability Matrix

CVE ID	Vendor/Product	CVSS	Exploited	SA Relevance
CVE-2025-53521	F5 BIG-IP APM	9.8	YES (China)	CRITICAL
CVE-2026-20131	Cisco FMC (ongoing)	10.0	YES (Interlock)	CRITICAL
CVE-2026-3055	Citrix NetScaler	9.3	Active recon	CRITICAL
CVE-2026-33634	Trivy (supply chain)	9.4	YES (TeamPCP)	HIGH
CVE-2026-33017	Langflow	9.3	YES (24hr)	HIGH
CVE-2026-21992	Oracle Identity Mgr	9.8	Not yet	HIGH
CVE-2026-24858	FortiOS SSO	9.4	YES (ongoing)	CRITICAL
CVE-2026-3909	Chrome / Skia	8.8	YES (re-patched)	HIGH
CVE-2026-3910	Chrome / V8	8.8	YES (KEV)	HIGH
CVE-2026-22719	VMware Aria Ops	8.1	Reports	HIGH
CVE-2026-20963	MS SharePoint	8.8	YES (KEV)	HIGH

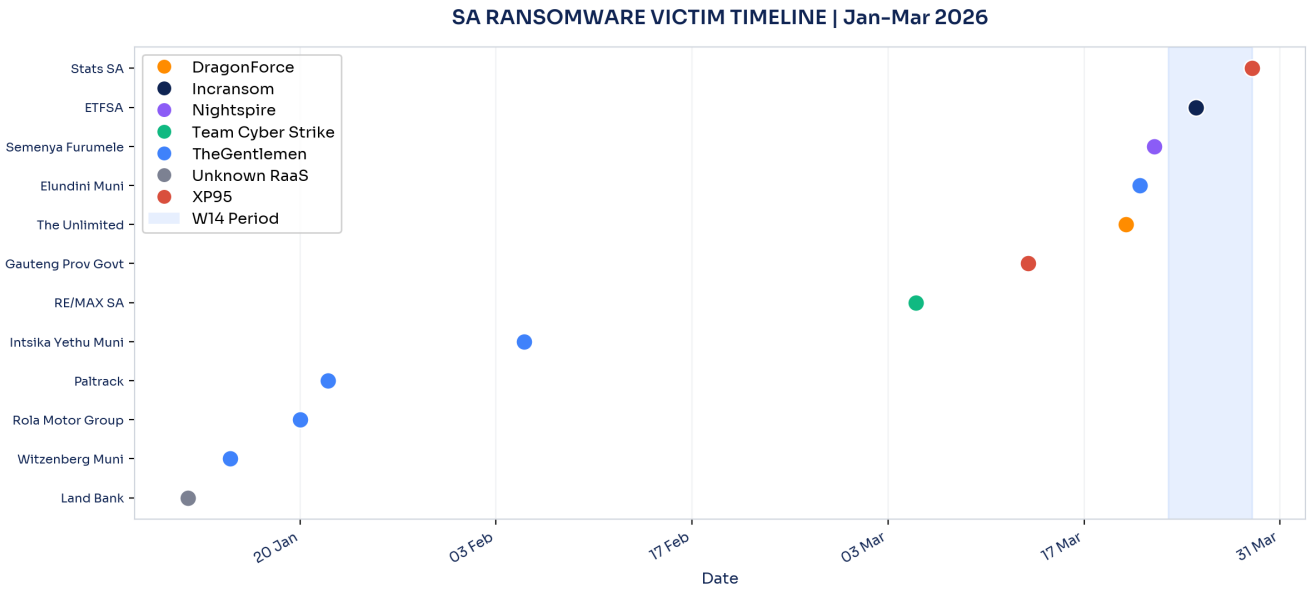
16. BleepingComputer — Langflow KEV — https://www.bleepingcomputer.com/news/security/cisa-new-langflow-flaw-actively-exploited-to-hijack-ai-workflows/
17. GitHub Advisory — Trivy GHSA-69fq-xp46-6x23 — https://github.com/aquasecurity/trivy/security/advisories/GHSA-69fq-xp46-6x23
18. The Hacker News — Citrix NetScaler active recon — https://thehackernews.com/2026/03/citrix-netscaler-under-active-recon-for.html

6. THREAT ACTOR PROFILES & RANSOMWARE ACTIVITY

Active Threat Actors Targeting SA — W14

Group	SA Victim(s)	Type	Key TTPs / CVEs
XP95	Stats SA, Gauteng	Data extortion	T1190 (unpatched servers)
Incransom	ETFSA	RaaS	CVE-2023-3519 (Citrix)
DragonForce	The Unlimited (316.63GB)	RaaS cartel	CVE-2021-44228, Ivanti
Nightspire	Semenya Furumele	Closed RaaS	CVE-2024-55591 (FortiOS)
TheGentlemen	Elundini Municipality	RaaS (Qilin)	FortiGate exploitation
APT41	SA gov IT provider	State (China)	T1190
Interlock	Global (Cisco FMC)	Ransomware	CVE-2026-20131

SA Ransomware Victim Timeline — Jan-Mar 2026



South Africa has recorded **96 total ransomware victims** (95 indexed + Stats SA pending indexing), with **2 new confirmed additions** in Week 14.[19] The ransomware landscape is dominated by **TheGentlemen** (5+ SA victims Q1), **XP95** (2 government targets in 1 month), and **DragonForce** (2 SA victims since Dec 2025). XP95's pure data extortion model (no encryption) represents an evolution in the threat, making traditional ransomware defences (backups, endpoint protection) insufficient against data theft.

19. Ransomware.live — SA Victims Map — https://www.ransomware.live/map/ZA

7. OSINT EXPOSURE & ATTACK SURFACE

7.1 SA Breach Rate Metrics

SA organisations are being breached approximately **every 3 hours**, with 90% deemed preventable (Unit 42/The Citizen).[2] 2,898 security compromises reported to the Information Regulator in FY 2025/26 — already exceeding the full prior year of 2,374. Identity-related weaknesses found in ~90% of investigated breaches. Mean time to data theft has dropped to **72 minutes** (down from 285 minutes in 2024, Unit 42).[20]

7.2 GreyNoise / Shodan Findings

GreyNoise reported elevated scanning activity targeting F5 BIG-IP infrastructure in South Africa (October 2025 baseline, still relevant). The 2026 State of the Edge report documented a credential-spraying botnet growing from 2,000 to 300,000 IPs in 72 days targeting RDP, 91,403 sessions targeting Ollama LLM inference servers (emerging AI attack surface), and 84,142 sessions targeting SonicWall VPN infrastructure.[21] Defused Cyber and watchTowr confirmed acute scanning following the F5 BIG-IP CISA KEV listing on 27 March.

7.3 Tycoon2FA PhaaS on .za.com Domains

Two .za.com domains confirmed in Tycoon2FA MFA-bypass phishing campaigns (811inboard.aeroprimelink.za.com, pass.aeroprimelink.za.com). The .za.com TLD (distinct from .co.za) is being exploited as a spoofing vector targeting Microsoft 365 and Google accounts.[15]

7.4 XP95 Data Exposure

The Gauteng Provincial Government dataset (3.8 TB / 3,673,556 files) and now Stats SA (154 GB / 453,362 files) remain listed on XP95's TOR site and BreachForums. Combined, these represent the largest known SA government data exposure event. Contents include ID documents, passports, CVs, and census/demographic data. A 1.8 GB Gauteng sample was dumped publicly as proof.

20. The Citizen, 13 March 2026 — SA breach exposure — https://www.citizen.co.za/news/sa-exposed-to-cyber-security-threats-amid-conflict-in-iran/
21. GreyNoise 2026 State of the Edge Report — https://www.greynoise.io/press/greynoise-releases-2026-state-of-the-edge-report

8. REGULATORY & COMPLIANCE

8.1 POPIA Enforcement Actions

Three enforcement actions disclosed at the Information Regulator's 5 March 2026 stakeholder engagement:[22]

- **Lancet Laboratories:** R200,000 fine — failed to comply with breach reporting obligations. Paid.
- **Blouberg Municipality:** R500,000 fine — unlawful publication of financial disclosures; refused to pay; court proceedings initiated under s109 POPIA.
- **FT RAMS Consulting:** R200,000 fine — unlawful direct marketing; refused to pay; court proceedings initiated.

8.2 Liberty as POPIA Test Case

The Liberty breach is the highest-profile financial sector breach since the 2023 TransUnion exposure.[4] It triggers multiple regulatory obligations simultaneously: **POPIA s22** (mandatory IR notification), **Joint Standard 2** (24-hour FSCA/PA incident reporting), and potential **GDPR exposure** (EU-resident Standard Bank Group clients). Liberty is a repeat offender (2018 breach) — aggravating circumstances. The Information Regulator has specifically flagged financial services as a priority enforcement sector for 2026/27.

8.3 Joint Standard 2 — Enforcement Phase

The FSCA/Prudential Authority Joint Standard on Cybersecurity and Cyber Resilience Requirements (effective 1 June 2025) is now in active enforcement.[23] Key requirements: board-approved cybersecurity strategy, **24-hour material incident reporting**, mandatory annual penetration testing, MFA, continuous monitoring, and third-party risk oversight. LEX Africa notes significant fines may be issued for non-compliance, similar to FICA fines (tens of millions).

8.4 SIM Card Crackdown

Minister of Justice Mmamoloko Kubayi announced a major SIM card registration crackdown beginning **1 July 2026**, supported by SAPS and NPA.[24] RICA amendment draft legislative proposals to be finalised by June 2026. Industry engagements with ICASA within 6 weeks from 27 March. Context: SA's FATF/FSRB mutual evaluation is scheduled for October 2026 — SIM card compliance is part of that preparation.

Compliance Deadlines Summary

Deadline	Obligation	Regulator
Immediate (6 Mar 2026)	Health information processing safeguards	Information Regulator
Active (enforcement)	Joint Standard 2 compliance	FSCA / PA
By June 2026	RICA amendment draft legislation	DoJ
1 July 2026	SIM card registration crackdown	SAPS / NPA
2 August 2026	EU AI Act full enforcement (high-risk)	EU
October 2026	SA FATF/FSRB mutual evaluation	FATF

22. Bowmans — Data Protection Enforcement Trends, 17 March 2026 — https://bowmanslaw.com/insights/south-africa-data-protection-recent-developments-and-enforcement-trends/
23. LEX Africa — Cybersecurity Shift 2026 — https://lexafrica.com/2026/02/south-africas-cybersecurity-shift-2026/
24. IOL — SIM Card Crackdown, 27 March 2026 — https://iol.co.za/news/2026-03-27-sim-card-crackdown-south-africas-strategic-assault-on-organised-crime/

9. 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.

9a. Hunt Missions

TH-2026-W14-01: XP95 Government Data Extortion — **P1 -- CRITICAL**

Hypothesis: XP95 exploits unpatched internet-facing servers for mass data exfiltration without encryption. Hunt for large outbound data transfers (>10GB), scanner/printer server anomalies, and unauthorised access to file shares.

MITRE ATT&CK: T1190, T1039, T1567

IOCs: XP95 TOR site (371fmt...onion), BreachForums account, Keybase, Session ID (05d3d75e...)

Data Sources: Firewall logs, NetFlow, file server audit logs, DNS logs

TH-2026-W14-02: DragonForce Double Extortion via Ivanti/Log4j — **P1 -- CRITICAL**

Hypothesis: DragonForce affiliates exploit CVE-2021-44228/CVE-2023-46805 for initial access, deploy Cobalt Strike, exfiltrate via MEGA/rclone. Hunt for MEGA uploads, SystemBC backdoor, PingCastle/AdFind recon, BYOVD (RogueKiller driver).

MITRE ATT&CK: T1190, T1566, T1059.001, T1003.001, T1486, T1567.002

IOCs: MEGA/rclone exfil patterns; SystemBC backdoor; PingCastle/AdFind; RogueKiller BYOVD driver

Data Sources: EDR, proxy logs, Sysmon, Windows Event Logs, RDP logs

TH-2026-W14-03: F5 BIG-IP APM Exploitation / Brickstorm Backdoor — **P1 -- CRITICAL**

Hypothesis: Chinese nation-state actor exploiting CVE-2025-53521 to deploy Brickstorm backdoor on BIG-IP APM. Hunt for /run/bigtlog.pipe, /run/bigstart.ltm, file hash mismatches in /usr/bin/umount and /usr/sbin/httpd, HTTP 201 with CSS content-type, SELinux disabled.

MITRE ATT&CK: T1190, T1059, T1562

IOCs: /run/bigtlog.pipe, /run/bigstart.ltm, file hash mismatches, SELinux disable entries in /var/log/auditd/

Data Sources: F5 device integrity checks, file system auditing, SELinux status, web logs

TH-2026-W14-04: Nightspire via FortiOS Auth Bypass — **P2 -- HIGH**

Hypothesis: Nightspire uses CVE-2024-55591 (FortiOS auth bypass) for initial access to SA engineering/construction firms. Hunt for .nspire file extension, FortiGate auth bypass indicators, unauthorised admin accounts.

MITRE ATT&CK: T1190, T1133, T1486, T1041

IOCs: .nspire file extension; CVE-2024-55591 exploitation artifacts

Data Sources: FortiGate logs, EDR, file extension monitoring

TH-2026-W14-05: Incransom via Citrix NetScaler — **P2 -- HIGH**

Hypothesis: Incransom exploits CVE-2023-3519 (Citrix NetScaler) targeting SA financial services. Hunt for NetScaler webshells, unusual RDP/SMB lateral movement, Incransom leak site references.

MITRE ATT&CK: T1190, T1078, T1021, T1550.002, T1486, T1567.002

IOCs: incblog6qu4y4mm...onion (Incransom leak site); Tycoon2FA domains: 811inboard.aeroprimelink.za.com, pass.aeroprimelink.za.com

Data Sources: NetScaler appliance integrity, web shell detection, RDP/SMB logs

9b. 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-W14-01	XP95 Gov data extortion	P1	FW, NetFlow, file srv	Not Started
TH-2026-W14-02	DragonForce Ivanti/Log4j	P1	EDR, proxy, Sysmon	Not Started
TH-2026-W14-03	F5 BIG-IP Brickstorm	P1	F5 integrity, logs	Not Started
TH-2026-W14-04	Nightspire FortiOS bypass	P2	FortiGate, EDR	Not Started
TH-2026-W14-05	Incransom Citrix NetScaler	P2	NetScaler, RDP/SMB	Not Started

9c. IOC Master Table

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

Indicator	Type	Attribution	Hunt ID
37lfmtakhknzx5t6k57ie...onion	TOR URL	XP95	TH-W14-01

Indicator	Type	Attribution	Hunt ID
breachforums.as/User-XP95	URL	XP95	TH-W14-01
keybase.io/XP95	URL	XP95	TH-W14-01
05d3d75e8370cfc72c7a...c934	Session ID	XP95	TH-W14-01
browser-updater[.]com	Domain	Interlock (Cisco FMC)	TH-W14-03
os-update-server[.]com	Domain	Interlock (Cisco FMC)	TH-W14-03
os-update-server[.]org	Domain	Interlock (Cisco FMC)	TH-W14-03
os-update-server[.]live	Domain	Interlock (Cisco FMC)	TH-W14-03
os-update-server[.]top	Domain	Interlock (Cisco FMC)	TH-W14-03
/run/bigtlog.pipe	File Path	F5 BIG-IP exploit	TH-W14-03
/run/bigstart.ltm	File Path	F5 BIG-IP exploit	TH-W14-03
811inboard.aeroprimelink.za.com	Domain	Tycoon2FA PhaaS	TH-W14-05
pass.aeroprimelink.za.com	Domain	Tycoon2FA PhaaS	TH-W14-05
c07b712a984a506042ea2cf6e193f20c	MD5	Gunra Ransomware	N/A
incblog6qu4y4mm4zvw...onion	TOR URL	Incransom	TH-W14-05
.nspire	File Ext	Nightspire ransomware	TH-W14-04
CVE-2024-55591	CVE	Nightspire (FortiOS)	TH-W14-04
CVE-2023-3519	CVE	Incransom (Citrix)	TH-W14-05

10. RECOMMENDATIONS

IMMEDIATE (P1 — This Week)

▪ **PATCH:** F5 BIG-IP APM CVE-2025-53521 (CVSS 9.8) — CISA deadline 30 March (TODAY). Check for /run/bigtlog.pipe and /run/bigstart.ltm IoCs. Verify Cisco FMC patched (CVE-2026-20131, CVSS 10.0 — Interlock active). Patch Citrix NetScaler CVE-2026-3055 immediately (active recon underway).

▪ **HUNT:** Execute P1 hunt missions TH-W14-01, TH-W14-02, TH-W14-03. Government entities: audit all internet-facing assets for XP95 indicators. Insurance sector: hunt for DragonForce indicators.

▪ **VERIFY:** Check Trivy CI/CD pipelines — if any pipeline ran Trivy v0.69.4 or referenced mutable trivy-action tags on 19-20 March, treat as fully compromised and rotate all secrets immediately.

▪ **MONITOR:** Liberty breach: if your organisation uses Liberty products, enable enhanced fraud monitoring. Watch for identity theft patterns using stolen ID numbers.

▪ **BLOCK:** Add all IOCs from Section 9c to blocklists. Block Tycoon2FA domains. Block Interlock C2 domains.

SHORT-TERM (P2 — This Quarter)

▪ Conduct government sector infrastructure audit — the Gauteng root cause (70% end-of-service devices) is systemic across SA government. Identify and remediate end-of-life hardware on internet-facing perimeters.

▪ Implement BEC detection for multi-channel attacks — banking fraud at 97,975 incidents (+86% YoY) with R1.888B losses demands enhanced vishing/smishing controls.

▪ Review POPIA s22 notification procedures — 2,898 compromises reported in FY 2025/26 (already exceeding prior full year). Ensure 72-hour notification window is achievable.

▪ Verify Langflow instances are upgraded to v1.9.0+ and not exposed to the internet (CVE-2026-33017 — exploited within 24 hours).

▪ Execute FortiOS audit — CVE-2024-55591 and CVE-2026-24858 actively exploited. FortiGate is SA's most widely deployed enterprise firewall.

STRATEGIC (Next 6-12 Months)

▪ Prepare for POPIA amendment legislation removing the remedy period — direct sanctions without cure window. Align with GDPR-style enforcement posture.

▪ Deploy data loss prevention (DLP) as priority — XP95's pure data extortion model (no encryption) bypasses traditional ransomware defences. DLP and outbound traffic monitoring are the critical controls.

▪ Address identity security — 90% of SA breaches involve identity-based attacks; breach frequency at every 3 hours. Implement robust MFA, privileged access management, and conditional access policies.

▪ Align with FSCA Joint Standard 2/2024 requirements — board-approved strategy, annual pentesting, MFA, 24-hour reporting. Enforcement fines expected similar to FICA (tens of millions).

▪ Prepare for FATF/FSRB mutual evaluation (October 2026) — SIM card/RICA compliance and cybercrime enforcement capacity will be evaluated.

▪ Invest in AI-powered threat detection — AI-powered fraud is 4.5x more profitable (INTERPOL). Counter with AI-powered defence, deepfake detection, and real-time transaction monitoring.

▪ Build government sector resilience — three entities under simultaneous extortion this week; systemic infrastructure rot demands coordinated national response.

ANOMALY-DRIVEN FLAGS

Government sector under unprecedented multi-vector pressure: Three entities (Gauteng, Stats SA, Elundini) under simultaneous active extortion by different groups (XP95, TheGentlemen). Root cause is systemic: unpatched, end-of-life infrastructure.

Data extortion without encryption is the new norm: XP95 does not encrypt systems — it exfiltrates and extorts. Traditional ransomware-focused defences (backups, endpoint protection) are insufficient. DLP, network segmentation, and outbound traffic monitoring are critical.

Financial sector regulatory convergence: Liberty breach simultaneously triggers POPIA, Joint Standard 2, and potential GDPR obligations. SA financial institutions face triple regulatory exposure as the new baseline.

11. 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-ca...
3	Daily Maverick, 17 March 2026	https://www.dailymaverick.co.za/article/2026-03-17-gaut...
4	ITWeb, 24 March 2026 — Liberty breach	https://www.itweb.co.za/article/insurer-liberty-hit-by-...
5	Breachsense, 23 March 2026 — The Unlimited	https://www.breachsense.com/breaches/the-unlimited-grou...
6	Help Net Security, 28 March 2026 — F5 BIG-IP	https://www.helpnetsecurity.com/2026/03/28/big-ip-apm-v...
7	SABRIC Annual Crime Statistics 2024	https://www.sabric.co.za/wp-content/uploads/2025/09/CRI...
8	IOL, 25 March 2026 — Liberty email systems	https://iol.co.za/business/2026-03-25-liberty-confirms-...
9	MyBroadband, 24 March 2026 — Virgin Active IDOR	https://mybroadband.co.za/news/security/635179-security...
10	DeXpose, 23 March 2026 — Nightspire	https://www.dexpose.io/nightspire-targets-semenya-furum...
11	DeXpose, 21 March 2026 — TheGentlemen / Elundini	https://www.dexpose.io/thegentlemen-ransomware-strikes-...

#	Source	URL
12	RE/MAX SA Incident Notice	https://www.remax.co.za/cyber-incident-notice
13	INTERPOL — Financial Fraud 2026	https://www.interpol.int/en/News-and-Events/News/2026/I...
14	Daily Maverick, 26 March 2026 — Zero fraud bank	https://www.dailymaverick.co.za/article/2026-03-26-the-...
15	CrowdStrike — Tycoon2FA Persistence	https://www.crowdstrike.com/en-us/blog/tycoon2fa-phishi...
16	BleepingComputer — Langflow KEV	https://www.bleepingcomputer.com/news/security/cisa-new...
17	GitHub — Trivy Advisory	https://github.com/aquasecurity/trivy/security/advisori...
18	The Hacker News — Citrix NetScaler	https://thehackernews.com/2026/03/citrix-netscaler-unde...
19	Ransomware.live — SA Map	https://www.ransomware.live/map/ZA
20	The Citizen, 13 March 2026	https://www.citizen.co.za/news/sa-exposed-to-cyber-secu...
21	GreyNoise — State of the Edge 2026	https://www.greynoise.io/press/greynoise-releases-2026-...
22	Bowmans — Enforcement Trends	https://bowmanslaw.com/insights/south-africa-data-prote...
23	LEX Africa — Cybersecurity Shift 2026	https://lexafrica.com/2026/02/south-africas-cybersecuri...
24	IOL — SIM Card Crackdown	https://iol.co.za/news/2026-03-27-sim-card-crackdown-so...
25	IOL, 20 March 2026 — Breach frequency	https://iol.co.za/business-report/economy/2026-03-20-da...
26	Bowmans — POPIA Monitoring Exercise	https://bowmanslaw.com/insights/south-africa-informatio...
27	EWN, 24 March 2026 — Liberty	https://www.ewn.co.za/2026/03/24/data-breach-at-liberty...
28	UpGuard, 26 March 2026 — Liberty	https://www.upguard.com/news/liberty-group-sa-data-brea...
29	Vox Telecom, 26 March 2026	https://www.vox.co.za/content-hub/article/cybersecurity...
30	Amazon AWS — Interlock Ransomware	https://aws.amazon.com/blogs/security/amazon-threat-int...
31	ThreatFox (abuse.ch)	https://threatfox.abuse.ch/browse/
32	SSA CSIRT	https://www.ssa.gov.za/CSIRT
33	SABRIC	https://www.sabric.co.za