



SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 16 | 6-12 April 2026

THREAT LEVEL: HIGH

XP95 20-April deadline 7 days away (Stats SA + GCRA), Salt Typhoon confirms first SA telecom breach, Krybit claims Megasurf ISP, IR demands Liberty/Standard Bank transparency, victim count 104

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W16 | Classification: TLP:WHITE

© 2026 Digital Progression | dpcyber.co.za

TABLE OF CONTENTS

- 1. Executive Summary
- 2. Threat Landscape Heatmap
- 3. SA Cyber Incidents & Breaches
- 4. Nation-State: Salt Typhoon SA Telecom Confirmed
- 5. Active Threat Campaigns
- 6. Critical Vulnerabilities
- 7. Threat Actor Profiles & Ransomware Activity
- 8. OSINT Exposure & Attack Surface
- 9. Regulatory & Compliance
- 10. Weekly Threat Hunt & IOCs
- 11. Recommendations
- 12. OSINT Sources Consulted

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH — W16 is the final full week before the XP95 20 April data publication deadline. Neither Statistics South Africa (154 GB / 453,362 files) nor the Gauteng City Region Academy (147 GB / 429,473 student records) has paid. XP95 posted 6 new global victims in a single 24-hour window on 9 April, demonstrating active operational tempo at the worst possible moment. Salt Typhoon (China-nexus) confirmed targeting a South African telecom provider via compromised Cisco IOS-XE routers — the first publicly confirmed nation-state telecom breach in SA. The Information Regulator publicly demanded coordinated transparency from both Liberty Group and Standard Bank, marking the first time the IR has compelled dual-entity coordinated disclosure.¹

KPI Dashboard

Metric	Current (W16)	Baseline / Prior	Change	Direction
SA cyberattacks/week	2,204	1,619 (2025 avg)	+36% YoY	UP
SA ransomware victims total	104	103 (W15 end)	+1 this week	UP
New SA victims (W16)	1 confirmed (Megasurf)	3 (W15)	-2	DOWN
POPIA notifications YTD	2,898+ (to 5 Mar 2026)	202 (2021/22)	+15x since 2021	UP
CISA KEV new entries W16	2	2 (W15)	FLAT	FLAT
Critical CVEs actively exploited	4	5 (W15)	-1	DOWN
Latest SA ransom demand	\$100K / R1.7M (XP95)	\$100K / R1.7M (W15)	Unchanged	FLAT
SA avg recovery cost (excl. ransom)	R24M (Sophos 2025)	R19M (2024 Sophos)	+26% YoY	UP

ANOMALY FLAG: XP95 20 April deadline is 7 days away — data release from Stats SA (154GB) and GCRA (147GB) is now operationally expected in W17. Salt Typhoon confirmed an SA telecom provider as its latest global victim. XP95 posted 6 new global victims in a single 24-hour window on 9 April, demonstrating active operational tempo at the worst possible moment.

TOP 3 ACTIONS THIS WEEK

- 1. ACTIVATE POPIA BREACH NOTIFICATION READINESS NOW (P1 — URGENT):** The 20 April XP95 deadline is 7 days away. Draft s22 notifications, individual notification templates, and a public statement now. Legal review should begin this week — not after 20 April.
- 2. AUDIT CISCO ROUTERS FOR SALT TYPHOON INDICATORS (P1):** Salt Typhoon confirmed an SA telecom victim. Run the Cisco TAC Salt Typhoon detection playbook. Check for anomalous GRE tunnels, SNMP polling from unexpected hosts, and unauthorised interface config changes on all IOS-XE edge devices.
- 3. PATCH FORTINET AND IVANTI BEFORE WEDNESDAY (P1):** CVE-2026-35616 (FortiClient EMS, CVSS 9.8, CISA KEV 6 April, deadline 9 April) and CVE-2026-1340 (Ivanti EPMM, CVSS 9.8, CISA KEV 8 April, deadline 11 April) — both federal deadlines have already passed. Patch now.

Critical Findings:

- XP95 20 April deadline now 7 days away. Stats SA (154GB/453K files) confirmed non-payment under PFMA; GCRA silent. XP95 posted 6 new global victims in 24 hours on 9 April — data release is operationally expected in W17.²
- Salt Typhoon (China-nexus telecom espionage group) confirmed targeting an unnamed South African telecom provider via Cisco IOS-XE router compromise — SA’s first publicly confirmed nation-state telecom breach.³

- Krybit ransomware claimed Megasurf ISP/data centre (9 April) — an emerging group with potential downstream hosted-client exposure risk.⁴
- Information Regulator publicly demanded coordinated transparency from both Liberty Group and Standard Bank (10-11 April) — first IR compelled dual-entity disclosure. Standard Bank confirmed names, ID numbers, account details exposed.⁵
- Two new CISA KEV entries with 3-4 day federal deadlines: Fortinet FortiClient EMS (CVSS 9.8) and Ivanti EPMM (CVSS 9.8) — both already past federal due date; unpatched SA systems are actively at risk.⁶

SECTOR SPOTLIGHT: GOVERNMENT — 7-DAY COUNTDOWN TO CRISIS

The 20 April XP95 deadline represents the most significant pre-planned national cybersecurity event in South Africa's history. Three government entities — Stats SA, GCRA, and the Gauteng Provincial Government — face near-certain data publication within 7 days. The Auditor-General's expanded April 2026 report confirms that 45 of 70 government departments are vulnerable to cyberattack, with R12.1 billion in IT system failures recorded. The structural reality is unambiguous: SA government cannot legally pay ransoms (PFMA), cannot technically prevent data publication once XP95 releases, and cannot retroactively prevent the identity fraud that will follow. The only actionable response this week is proactive communication to affected data subjects.⁷

1. ITWeb — SA Cyber Threat Intelligence W16 — <https://www.itweb.co.za>

2. UpGuard — Stats SA Data Breach 2026 — <https://www.upguard.com/news/statistics-south-africa-data-breach-2026-03-31>

3. TechCrunch — Salt Typhoon SA Telecom Confirmed —

<https://techcrunch.com/2026/03/09/salt-typhoon-china-who-has-been-hacked-global-telecom-giants/>

4. Breachsense — ransomware.live ZA — <https://www.ransomware.live/map/ZA>

5. ITWeb — Liberty IR Escalation — <https://www.itweb.co.za/article/insurer-liberty-hit-by-data-breach/o1Jr5MxPwrdMKdWL>

6. CISA Known Exploited Vulnerabilities Catalog — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

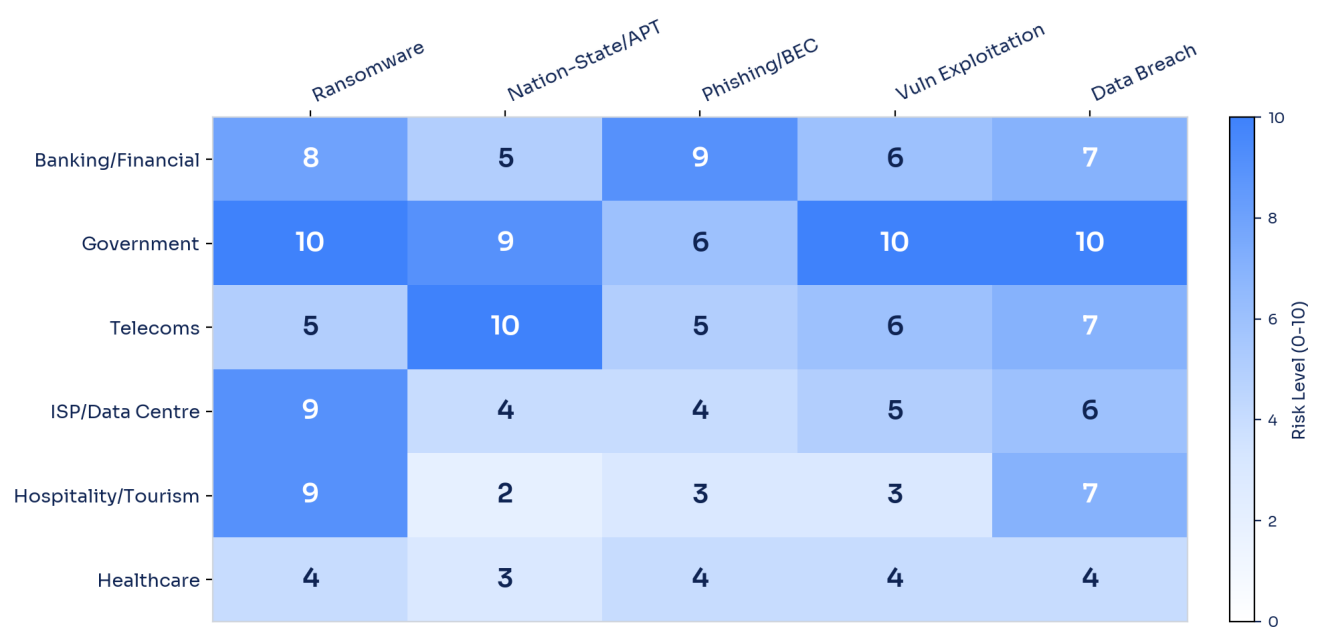
7. TechCentral — AG Report on Government Cyber Defences —

<https://techcentral.co.za/gaping-holes-in-south-african-government-cyber-defences/279769/>

2. THREAT LANDSCAPE HEATMAP

The heatmap below maps six key South African sectors against five threat categories, rated 0-10 based on active threat intelligence, confirmed incidents, and vulnerability exposure during Week 16. Government remains at MAXIMUM across ransomware, vulnerability exploitation, and data breach — driven by the XP95 7-day deadline. Telecoms is elevated to MAXIMUM for Nation-State/APT following Salt Typhoon's confirmed SA victim. ISP/Data Centre is elevated due to the Krybit/Megasurf compromise.

SA THREAT LANDSCAPE HEATMAP | W16 (6-12 Apr 2026)



Methodology: Risk levels are assessed using: (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

Week 16 added one new confirmed SA ransomware victim (Megasurf/Krybit) and produced critical developments on five W14/W15 carry-over incidents. The SA cumulative ransomware victim count stands at **104** as of 12 April 2026. The XP95 20 April deadline is the defining event of this reporting period.⁴

3.1 XP95 / Statistics South Africa — W15 Follow-On (CRITICAL — 7 Days to Deadline)

Organisation	Statistics South Africa (statssa.gov.za) — National statistics authority
Sector	Government / National Statistics
Threat Actor	XP95
Date	Exfiltration: est. February 2026; disclosed 29-30 March 2026; deadline 20 April 2026
Data	154 GB / 453,362 files — HR job-seeker portal (names, CVs, ID numbers, contact details)
Demand	\$100,000 USD (R1.7 million)
Deadline	20 April 2026 (7 days from end of W16)
Payment	Refused — PFMA prohibits ransom payment; confirmed non-payment as of W16
Status	Active extortion. POPIA s22 filed 29 March. No IR advisory to data subjects as of 12 April.
SA Significance	453,362 job-seekers’ PII imminent publication; second-order exposure for employers
Sources	UpGuard, Breachsense, DataBreaches.net, The Citizen, ITWeb, Pinsent Masons

Stats SA confirmed non-payment under PFMA in the W16 period. The 20 April deadline is 7 days away. Data publication will expose 453,362 job-seekers' PII including names, CVs, ID numbers, and contact details. The IR has not yet issued public guidance to affected data subjects — a gap that creates significant regulatory liability for Stats SA. XP95's pattern with prior victims (Eholo Health, Spain) is to release data promptly after deadline expiry. Any SA organisation that submitted employee data via the Stats SA portal faces second-order breach notification obligations under POPIA.²

3.2 XP95 / Gauteng City Region Academy — W15 Follow-On (CRITICAL — 7 Days to Deadline)

Organisation	Gauteng City Region Academy (gcrabursary.gauteng.gov.za)
Sector	Government / Education / Bursaries
Threat Actor	XP95
Date	Exfiltration: mid-March 2026; deadline 20 April 2026
Data	147 GB / 429,473 files — bursary/scholarship applicant records (student PII, financial details, academic records)
Demand	\$100,000 USD (R1.7 million)
Deadline	20 April 2026
Payment	Unknown — GCRA has issued no public statement as of 12 April
Status	Active extortion. No POPIA s22 notification confirmed. Breachsense re-indexed 10 April.
SA Significance	429,473 students' financial and academic records at imminent publication risk
Sources	Breachsense, DataBreaches.net, BlackFog, social media

GCRA administers bursary and scholarship programmes for the Gauteng provincial government. It has issued no public response. No POPIA s22 notification has been confirmed. Breachsense re-indexed the GCRA breach listing on 10 April — indicating XP95 refreshed its claim. The 429,473 student records include financial details and academic information that are highly valuable for identity fraud targeting young professionals.⁸

3.3 DragonForce / Singita — W15 Follow-On (ACTIVE EXTORTION)

Organisation	Singita (singita.com) — luxury safari/conservation lodge operator
Sector	Hospitality / Tourism / Conservation
Threat Actor	DragonForce
Date	Claimed 2 April 2026; Breachsense indexed 7 April 2026
Data	43.74 GB confirmed (Breachsense indexed 7 April). Data not yet published as of 12 April.
Demand	Unknown
Deadline	Unknown — publication imminent per threat actor pattern
Payment	None confirmed. No Singita public statement.
Status	Active extortion. No data published. Publication assessed as imminent.
SA Significance	High-net-worth client PII: passport copies, payment details, medical/dietary requirements
Sources	Breachsense, DeXpose.io, ransomware.live

Data volume confirmed at 43.74 GB (Breachsense indexed 7 April). No data published as of 12 April. No public statement from Singita. Data likely includes high-net-worth client PII: passport copies, payment details, medical/dietary requirements. Luxury hospitality operators hold unusually sensitive client profiles.

Imminent publication is expected given DragonForce's operational pattern post-deadline.⁹

3.4 Liberty Group SA / Standard Bank — W14 Follow-On (IR ESCALATION)

Organisation	Liberty Group SA (liberty.co.za) and Standard Bank (standardbank.co.za)
Sector	Financial Services / Insurance / Banking
Threat Actor	Unknown — attack vector not publicly disclosed
Date	Standard Bank client notifications ~7 April 2026; IR demand 10–11 April 2026
Data	Names, ID numbers, company registration numbers, account details (Standard Bank business clients)
Demand	N/A
Deadline	N/A
Payment	N/A
Status	IR transparency demand stage. Formal Enforcement Notice not yet published as of 12 April.
SA Significance	First IR compelled dual-entity coordinated disclosure; W17 enforcement action expected
Sources	ITWeb, IR public statements, EWN

Standard Bank notified business clients approximately 7 April: names, ID numbers, company registration numbers, account details exposed. The Information Regulator publicly demanded greater transparency from both Standard Bank and Liberty on 10–11 April — the first time the IR has compelled coordinated dual-entity disclosure. No formal Enforcement Notice has been published on the IR site as of 12 April — this is the transparency demand stage, a precursor to formal enforcement expected in W17.⁵

3.5 Megasurf (ISP/Data Centre) — Krybit Ransomware (W16 NEW)

Organisation	Megasurf — SA ISP and data centre operator
Sector	ISP / Data Centre / Telecommunications
Threat Actor	Krybit (emerging group, 9 known global victims total)
Date	9 April 2026
Data	Volume and types unknown; listed on Krybit dark web leak site
Demand	Unknown
Deadline	Unknown
Payment	Unknown — no Megasurf public response
Status	Active extortion. Listed on Krybit dark web leak site.
SA Significance	ISP/DC compromise creates downstream hosted-client supply-chain risk
Sources	Breachsense, ransomware.live

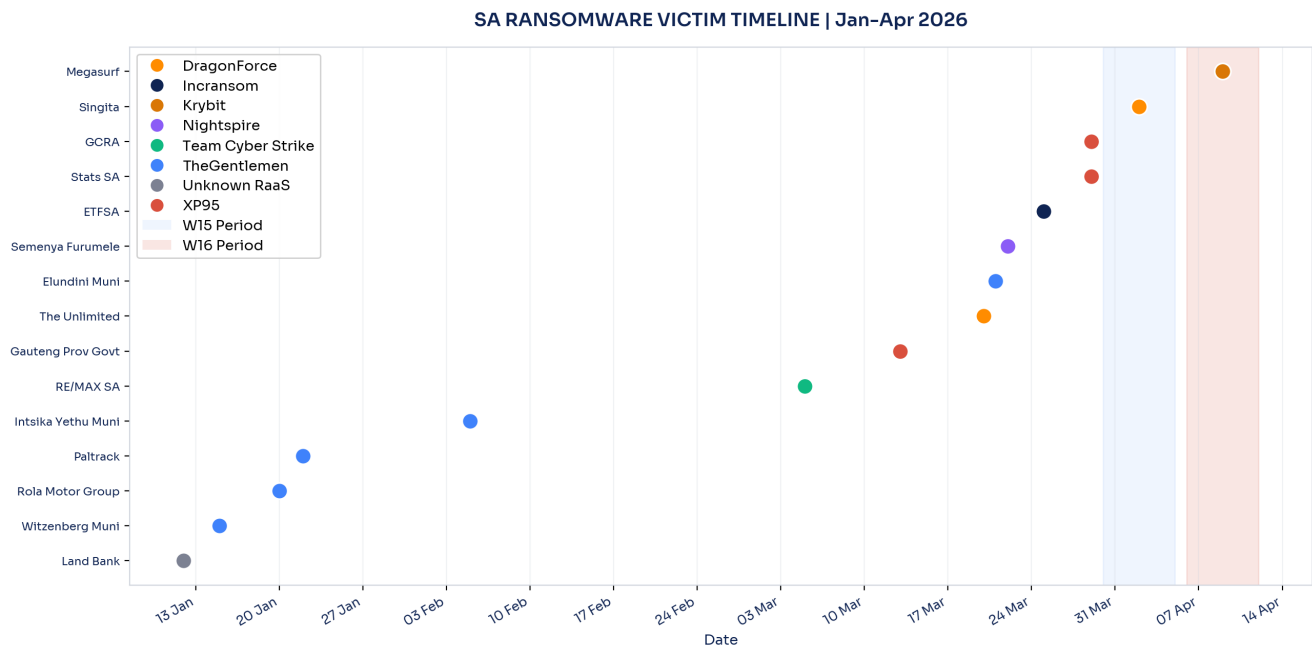
Krybit is a newly emerged ransomware group with 9 known global victims. Megasurf is its first confirmed South African victim. The significance extends beyond Megasurf itself: as an ISP and data centre operator, a compromise of its management infrastructure could provide lateral access to hosted client environments. Organisations co-located at Megasurf or using Megasurf connectivity services should treat this as a potential supply-chain event and review their network ingress controls accordingly.⁴

3.6 ETFSA (Incransom) — W14 Follow-On (No New Developments)

Organisation	ETFSA (Exchange Traded Funds SA)
Sector	Financial Services
Threat Actor	Incransom
Date	Originally listed W14 (26 March 2026)
Data	Full client dataset threatened
Status	No data publication or new Incransom statements in W16. Threat remains live.
Sources	ransomware.live, Incransom dark web

No data publication or new Incransom statements detected in W16. The threat remains live; full client dataset still threatened. Incransom remains active globally in W16.

SA Ransomware Victim Timeline — Jan-Apr 2026



8. Breachsense — GCRA Breach — <https://www.breachsense.com/breaches/gauteng-city-region-academy/>
9. Breachsense — Singita Breach — <https://www.breachsense.com/breaches/singita/>
10. DeXpose.io — DragonForce Singita — <https://www.dexpose.io/dragonforce-targets-luxury-safari-operator-singita/>

4. NATION-STATE: SALT TYPHOON SA TELECOM CONFIRMED

The confirmation of a South African telecom provider as a Salt Typhoon victim represents a significant strategic escalation. This is SA’s first publicly confirmed nation-state telecom infrastructure breach. Salt Typhoon is a China-nexus advanced persistent threat group also tracked as **Earth Estries**, **GhostEmperor**, and **RedMike**.³¹¹

Attribution	Salt Typhoon (China-nexus) — also tracked as Earth Estries / GhostEmperor / RedMike
Victim	Unnamed South African telecom provider (identity protected per Recorded Future/TechCrunch)
Confirmed by	Recorded Future / TechCrunch investigation (published W16)
Method	Cisco IOS-XE router exploitation; GRE tunnel implantation; passive traffic interception; SNMP abuse
Global scale	AT&T, Verizon, T-Mobile, 9+ US carriers, EU/Asian telcos, now SA
SA implications	Telecom infra serves government comms, banking networks, and national critical infrastructure
Detection	Cisco TAC Salt Typhoon detection playbook — GRE tunnels, SNMP anomalies, interface config changes
Sources	Recorded Future, TechCrunch, Cisco TAC advisory

What This Means for South Africa

Telecom infrastructure in SA serves government communications, banking networks, and national critical infrastructure. Persistent router-level access enables passive interception of all traffic traversing that infrastructure. This is a long-term intelligence collection capability, not a one-time breach. Unlike ransomware, the goal is sustained, silent access — Salt Typhoon was active inside US carrier infrastructure for 18+ months before detection.³

Salt Typhoon’s attack chain typically begins with exploitation of legacy IOS-XE vulnerabilities (CVE-2023-20198, CVE-2023-20273). Once inside, they implant GRE tunnels for persistent exfiltration and use SNMP to enumerate the network topology. The attacker’s objective is passive collection of metadata and content from traffic traversing the carrier infrastructure — meaning enterprise customers of the compromised SA telco may have had their traffic passively intercepted.

Recommended Detection Actions

- Run Cisco TAC Salt Typhoon detection script on all IOS-XE edge routers
- Execute "show ip tunnel" and look for undocumented GRE tunnel entries
- Compare running-config to known-good baseline; any delta is suspicious
- Review SNMP poll logs: Salt Typhoon uses SNMP from unexpected external IPs to enumerate topology
- Check for new admin accounts or "ip route" entries to unexpected /32 destinations
- Review interface config change history vs. change management records

11. Recorded Future — Salt Typhoon Global Telecom Espionage — <https://www.recordedfuture.com/research/salt-typhoon-global-telecom-espionage>
12. Cisco TAC — Salt Typhoon Detection Advisory — https://sec.cloudapps.cisco.com/security/center/resources/salt_typhoon_detection.html

5. ACTIVE THREAT CAMPAIGNS

5.1 Banking Fraud Surge

Four major SA banks — Absa, FNB, Nedbank, and Standard Bank — issued a joint fraud alert on 2 April on a surging vishing and SIM-swap combination targeting customers. SA telecom fraud costs R5.3 billion annually per SABRIC. AI-powered fraud is 4.5x more profitable per the INTERPOL 2026 Financial Crime Report — lowering the technical barrier for threat actors. The Standard Bank compromise (Section 3.4) may be related to this broader fraud surge.¹³¹⁴

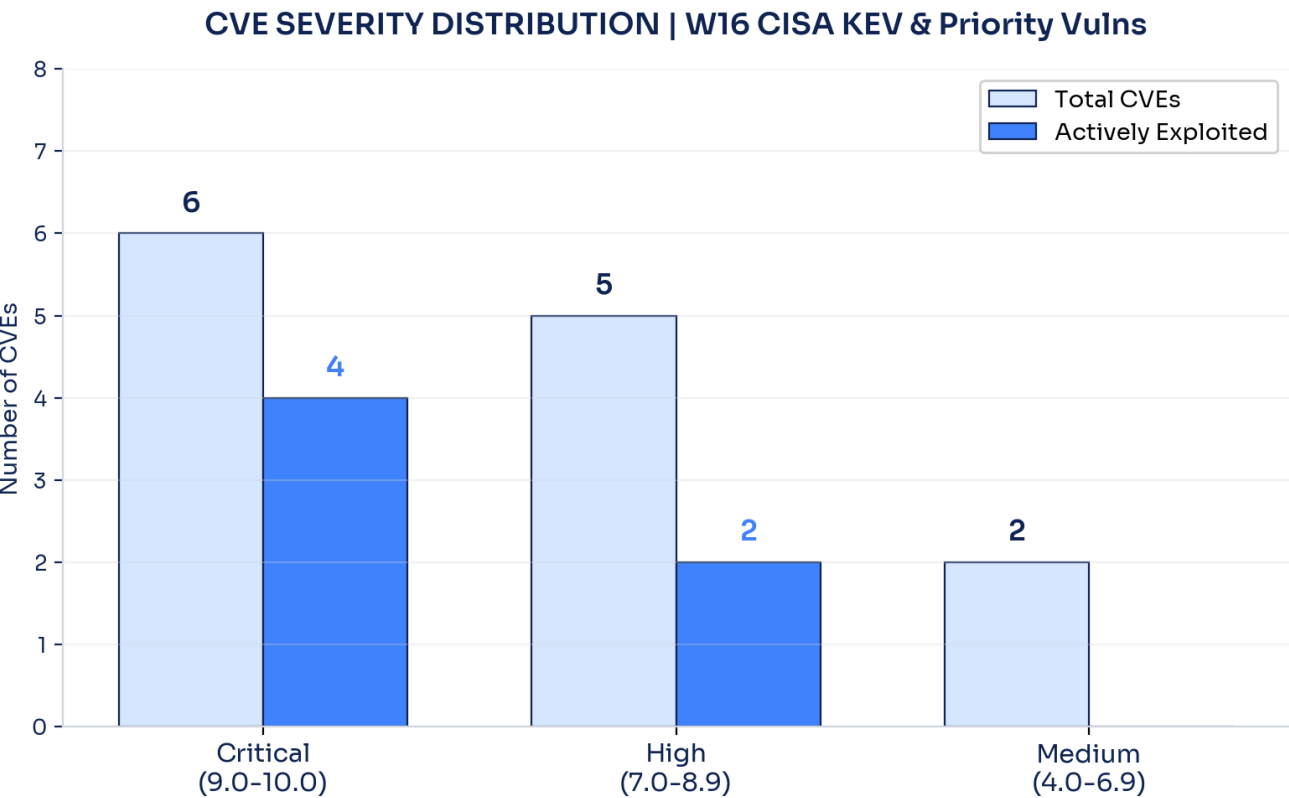
5.2 Supply Chain Threats

North Korean Contagious Interview campaign: 1,700+ malicious packages published across npm, PyPI, and three other package ecosystems since 1 March 2026. The campaign targets developers with fake interview tasks delivering BeaverTail and InvisibleFerret info-stealers. SA developers active in AI, data science, and financial technology sectors are at direct risk. Audit all npm/PyPI packages installed since 1 March 2026 from unknown authors.¹⁵

Smart Slider 3 Pro (WordPress/Joomla plugin): Unauthenticated backdoor discovered and patched within a 6-hour window on 7 April 2026. During that window, 1M+ sites were exposed globally. SA WordPress/Joomla sites using this plugin should update immediately and review server logs for 7 April access anomalies.¹⁶

13. EWN — SA Banks SIM-Swap Vishing Warning — <https://www.ebnewsdaily.co.za/2026/04/02/south-africa-banks-warn-sim-swap-voice-phishing-fraud-2026/>
14. INTERPOL 2026 Financial Crime Report — <https://www.interpol.int/en/News-and-Events/News/2026/I...>
15. BleepingComputer — Contagious Interview 1,700 Packages — <https://www.bleepingcomputer.com/news/security/north-korean-hackers-contagious-interview-1700-packages/>
16. BleepingComputer — Smart Slider 3 Pro Backdoor — <https://www.bleepingcomputer.com/news/security/smart-slider-3-pro-backdoor/>

6. CRITICAL VULNERABILITIES



Week 16 adds **2 new CISA KEV entries** with unusually short federal deadlines (3-4 working days). Both have already passed the federal due date, meaning any unpatched SA system is actively at risk. Microsoft April Patch Tuesday falls on 14 April (W17) — a critical Kerberos RC4 enforcement update requires pre-action this week.⁶

CISA KEV Additions — W16

CVE ID	Product	CVSS	Date Added (KEV)	Federal Due Date
CVE-2026-35616	Fortinet FortiClient EMS	9.8	6 April 2026	9 April 2026 (PASSED)
CVE-2026-1340	Ivanti EPMM (MobileIron)	9.8	8 April 2026	11 April 2026 (PASSED)

CRITICAL PRE-ACTION — Microsoft Patch Tuesday 14 April: The April 2026 Patch Tuesday (W17) enforces AES-SHA1 on domain controllers and will break legacy systems using RC4 Kerberos authentication. Audit RC4 dependencies on all domain controllers NOW — before the update deploys on 14 April. Systems still using RC4 will fail authentication after the update.

Priority Vulnerability Matrix — W16

CVE ID	Vendor/Product	CVSS	Exploited?	SA Relevance
CVE-2026-35616	Fortinet FortiClient EMS	9.8	YES (KEV — zero-day)	CRITICAL — dominant SA mid-market
CVE-2026-1340	Ivanti EPMM (MobileIron)	9.8	YES (KEV — API bypass)	CRITICAL — SA enterprise MDM
CVE-2026-39987	Marimo Python Notebook	9.3	YES (9h 41m post-disclosure)	HIGH — SA AI/data science sector
CVE-2025-53521	F5 BIG-IP APM	9.8	YES (UNC5221/China-nexus)	CRITICAL — SA banking/telco
CVE-2026-20093	Cisco IMC	9.8	No PoC yet; trivial to exploit	HIGH — SA enterprise data centres
CVE-2026-21643	Fortinet FortiClient EMS	9.1	YES (SQL injection)	CRITICAL — companion to KEV entry

Top 5 CVE Detail — SA Priority

CVE-2026-35616 — Fortinet FortiClient EMS — CVSS 9.8 — P1 CRITICAL

Unauthenticated RCE exploited as a zero-day since 31 March before advisory publication. Hotfix only available (7.4.7); no full patch released as of W16. CISA KEV added 6 April with a 3-day federal deadline (9 April — now passed). Companion vulnerability CVE-2026-21643 (CVSS 9.1, SQL injection, same product) is also actively exploited. Fortinet is dominant in SA mid-market and enterprise — this is the single highest-urgency patch action this week. Patch to 7.4.7 immediately.¹⁷

CVE-2026-1340 — Ivanti EPMM (MobileIron) — CVSS 9.8 — P1 CRITICAL

Unauthenticated RCE via improper authentication in API endpoints. CISA gave only 4 working days (8-11 April) to patch — reflecting confirmed active exploitation. Upgrade to Ivanti EPMM 12.8 or later. SA enterprise MDM environments using Ivanti/MobileIron are directly at risk.¹⁸

CVE-2026-39987 — Marimo Python Notebook — CVSS 9.3 — P1 HIGH

Exploited within 9 hours 41 minutes of disclosure — no public PoC existed at time of exploitation, suggesting a sophisticated threat actor with access to the advisory before public release. Impacts data science and AI/ML infrastructure running Marimo notebooks. Upgrade to Marimo 0.23.0. SA AI/data science sector and financial sector analytics teams are at risk.¹⁹

CVE-2025-53521 — F5 BIG-IP APM — CVSS 9.8 — P1 CRITICAL (ONGOING)

Nation-state exploitation (UNC5221/China-nexus) ongoing through W16. 17,000+ exposed IPs globally. IOC review mandatory even for patched systems — Brickstorm backdoor may persist post-patch. SA banking and telecom are primary F5 users.²⁰

CVE-2026-20093 — Cisco IMC — CVSS 9.8 — P2 HIGH

Auth bypass enabling unauthenticated admin password reset on the hardware management plane. No PoC confirmed yet but single HTTP request attack vector makes weaponisation trivial. Patch and isolate IMC interfaces from internet immediately. Cisco UCS is widespread in SA enterprise data centres.²¹

17. Fortinet PSIRT — CVE-2026-35616 Advisory — <https://www.fortiguard.com/psirt/FG-IR-26-35616>

18. Ivanti — CVE-2026-1340 Security Advisory — <https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-EPMM-CVE-2026-1340>
19. Marimo — CVE-2026-39987 Security Advisory — <https://github.com/marimo-team/marimo/security/advisories/>
20. CISA — Known Exploited Vulnerabilities Catalog — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
21. Cisco PSIRT — IMC CVE-2026-20093 — <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-auth-bypass>

7. THREAT ACTOR PROFILES & RANSOMWARE ACTIVITY

SA Ransomware Victim Count: 104 as of end W16 (up from 103 at end W15). Net new W16: +1 (Megasurf/Krybit). The lower weekly count (1 vs 3 in W15) does not reflect reduced threat; rather, XP95’s looming 20 April deadline dominates the risk landscape.⁴

Active SA-Relevant Threat Actor Summary

Actor	Type	SA Victims	Status	Primary TTPs
XP95	Data Extortion	Stats SA, GCRA, Gauteng Prov Govt	CRITICAL — 7 days to deadline	Data exfiltration only; Telegram C2; targets PFMA entities
DragonForce	RaaS	Singita + 4 prior SA victims	ACTIVE — publication imminent	80% affiliate model; multi-sector; data + encryption
Krybit	Ransomware	Megasurf (W16 NEW)	EMERGING — monitor	New group; 9 global victims; ISP/DC targeting
Nightspire	Ransomware	Semenya Furumele, E Cape DTHS, Ingonyama Trust	ACTIVE	CVE-2024-55591 (FortiOS auth bypass)
Lapsus\$	Data Extortion	AstraZeneca W15; Vodacom/MTN 2022	ACTIVE	Social engineering; insider access; pharma/telco
Incransom	Ransomware	ETFSA	LIVE THREAT	Financial sector focus; multi-platform

XP95 — CRITICAL ESCALATION

Emerged March 2026 with an exclusive focus on SA government entities. SA victims: Stats SA (154GB), GCRA (147GB), Gauteng Provincial Government (3.8TB). Pure data extortion model — no encryption, Telegram-only C2. Posted 6 new global victims in a 24-hour window on 9 April, demonstrating active operational tempo. The 20 April deadline is 7 days away and data release is near-certain. International confirmed victim: Eholo Health Spain (data released after non-payment — the operational precedent).²

DragonForce — PRIMARY SA THREAT ACTOR

DragonForce remains the most prolific ransomware group targeting SA with 5+ confirmed SA victims. Singita data confirmed at 43.74 GB (Breachesense indexed 7 April). Publication is imminent per the group’s pattern. DragonForce operates an 80% affiliate payout model (highest in the RaaS market), which drives volume attacks across diverse sectors. The group has shown willingness to attack high-profile SA organisations including conservation and luxury hospitality.⁹

Krybit — EMERGING GROUP

Krybit is a newly emerged ransomware group with 9 known global victims as of W16. Megasurf (9 April) is their first confirmed South African victim and their first confirmed ISP/data centre target. Their operational capability is unproven but their selection of an ISP target suggests some sophistication in understanding downstream exposure potential. Monitor for escalation and further SA targeting.⁴

Nightspire — ACTIVE

Two redacted-victim claims from Nightspire were observed on 3-6 April; countries of origin unknown. Nightspire’s prior confirmed SA victims include Semenya Furumele, Eastern Cape Department of Transport and Human Settlements, and the Ingonyama Trust Board. Primary attack vector: CVE-2024-55591 (FortiOS authentication bypass). Any SA organisation using FortiOS should verify this patch is applied.²²

Lapsus\$ — ACTIVE

Lapsus\$ confirmed an AstraZeneca breach (5 April): 3 GB of source code, credentials, and employee database. Lapsus\$ has a documented historical SA nexus: Vodacom and MTN were targets in 2022. SA pharmaceutical and telecom sector security teams should heighten monitoring. The group’s re-emergence wave in April 2026 represents renewed SA risk.²³

Nation-State Activity

Actor	SA Status	TTPs	Notes
Salt Typhoon (China-nexus)	CONFIRMED SA TELECOM	IOS-XE router exploitation, GRE tunnels, passive interception	See Section 4 for full analysis
APT41 (China-nexus)	ACTIVE in southern Africa	Government IT provider targeting	Kaspersky MDR July 2025 — operationally relevant
UNC5221 (China-nexus)	F5 BIG-IP active	CVE-2025-53521 exploitation	Brickstorm backdoor; ongoing W16

22. Nightspire — ransomware.live — <https://www.ransomware.live/map/ZA>
23. CM Alliance — Biggest Cyber Attacks March-April 2026 — <https://www.cm-alliance.com/cybersecurity-blog/biggest-cyber-attacks-data-breaches-ransomware-attacks-of-march-2026>

8. OSINT EXPOSURE & ATTACK SURFACE

F5 BIG-IP Global Exposure

17,000+ F5 BIG-IP instances unpatched globally; SA banking and telco are primary F5 users. SA-specific Shodan/Censys scanning has been previously confirmed. CVE-2025-53521 nation-state exploitation (UNC5221) is ongoing through W16.²⁰

Salt Typhoon Lateral Reach

Salt Typhoon’s confirmed SA telecom compromise via GRE tunnel implants may provide lateral access to downstream enterprise customers via peering and transit relationships. Any organisation whose traffic transits the affected SA telco’s infrastructure should assume potential passive interception.³

Krybit/Megasurf Hosted Client Risk

Megasurf operates as both an ISP and data centre operator. A compromise of its management infrastructure creates a downstream supply-chain risk for all hosted clients. Organisations co-located or interconnected with Megasurf should audit their network ingress controls and review for any anomalous connectivity from Megasurf IP ranges.⁴

Smart Slider 3 Pro Backdoor Window

Any SA WordPress or Joomla site using Smart Slider 3 Pro was at risk during a 6-hour window on 7 April 2026. Check update logs for that date. If the plugin was not updated on 7 April, assume compromise and audit server logs for web shells or unauthorised admin account creation.¹⁶

Contagious Interview Package Exposure

1,700+ malicious npm/PyPI packages are in the wild from the North Korean Contagious Interview campaign (since 1 March 2026). SA developers active in AI, data science, and fintech should audit all packages installed from unknown authors since 1 March 2026. Check for BeaverTail and InvisibleFerret malware hashes.¹⁵

9. REGULATORY & COMPLIANCE

Information Regulator — W16 Escalations

Liberty Group / Standard Bank: The IR publicly demanded greater transparency from both entities on 10-11 April — the first time the IR has compelled coordinated dual-entity disclosure. No formal Enforcement Notice has been published on the IR website as of 12 April. The transparency demand is a precursor stage; W17 formal enforcement action is expected.⁵

Stats SA / XP95: The IR has issued no public advisory to data subjects (453,000+ affected) as of 12 April. The s22 notification was filed by Stats SA on 29 March, but no IR guidance has been issued to other government entities about XP95. A critical gap exists: 453,000 job-seekers have not been notified that their data is 7 days from publication.²

GCRA / XP95: No POPIA s22 filing confirmed by GCRA. Breachsense re-indexed the breach on 10 April — confirming threat actor activity. 429,473 students have not been notified. GCRA's silence represents the most significant regulatory gap in W16.⁸

Auditor-General — Expanded April 2026 Finding

The Auditor-General's expanded April 2026 report confirms that **45 of 70 government departments** are vulnerable to cyberattack, with **R12.1 billion** in IT system failures recorded. SABS remains in recovery 15 months post-ransomware. The structural vulnerability of SA government to cyber threats — combined with the PFMA prohibition on ransom payment — creates a structural policy gap that the XP95 crisis has exposed. This requires legislative consideration.⁷

New Regulatory Developments

SARB / PA Joint Communication 2 (7 April)

OTC derivatives clearing only — no new cyber directive issued

Parliament IR Capacity Discussion (8 April)

Portfolio Committee on Justice discussed IR vacancies; member cited cybercrime urgency. Capacity constraint acknowledged.

EU DORA (First Register of Information)

First filing period closed end of March 2026. SA subsidiaries of EU financial institutions must comply. NIS2 audit deadline 30 June 2026.

FSCA Joint Standard 2

No new enforcement actions in W16. Monitoring continues.

Information Regulator — Cumulative Enforcement Actions

Organisation	Incident	IR Action	Status (W16)
Liberty Group / Standard Bank	Data breach via Liberty affiliate	Public transparency demand (dual-entity)	ESCALATED — W17 enforcement expected
Mediosa / CABS	Patient data breach	Enforcement Notice issued	Closed / Remediation
Stats SA	XP95 extortion (154GB)	s22 received; no advisory issued	ACTIVE — gap in data subject notification
GCRA	XP95 extortion (147GB)	No s22 confirmed; no IR action	ACTIVE — critical gap
Land Bank	RaaS attack Jan 2026	s22 filed; remediation monitored	Remediation ongoing (target Sep 2026)
Transnet	Prior ransomware	Previous enforcement	Completed

Upcoming Regulatory Deadlines

Deadline	Obligation	Body
14 April 2026 (IMMEDIATE)	Microsoft Patch Tuesday — Kerberos RC4 enforcement pre-audit	Microsoft / Internal
20 April 2026	XP95 data publication deadline (Stats SA + GCRA)	XP95 / IR / Stats SA / GCRA
30 June 2026	PAIA annual report submission	Information Regulator
30 June 2026	EU NIS2 audit deadline (SA subsidiaries of EU companies)	EU / ENISA
July 2026	SARB/FSCA AI discussion paper	SARB / FSCA
September 2026	Land Bank remediation plan target	Land Bank / IR
October 2026	SA FATF/FSRB mutual evaluation	FATF

10. WEEKLY THREAT HUNT & IOCs

Four hunt missions are active for W16. Two P1 missions address nation-state and near-certain data publication events. Two P2 missions address supply-chain and developer ecosystem risks.

TH-2026-W16-01 — Salt Typhoon Cisco Router Implant Detection

Hypothesis: Salt Typhoon may have implanted GRE tunnels or persistent backdoors on SA enterprise Cisco IOS-XE edge routers, particularly in telco, ISP, and financial services environments, leveraging the confirmed SA telecom compromise as a pivot point.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1572 (Protocol Tunneling / GRE), T1046 (Network Service Scanning), T1020 (Automated Exfiltration)

IOCs: Anomalous GRE tunnel creation on IOS-XE; SNMP polling from unexpected external IPs; interface config changes not matching change records; new admin users on network devices; traffic to Chinese CDN exit nodes from router management interfaces

Data Sources: Network device syslog (SNMP traps, interface config), TACACS+/RADIUS logs, NetFlow/IPFIX for GRE traffic, Cisco IOS-XE audit logs, AAA server logs

P1 — CRITICAL:
Nation-state; confirmed SA victim

TH-2026-W16-02 — XP95 Pre-Publication Data Validation

P1 — CRITICAL: 7-day countdown; publication near-certain

Hypothesis: With 7 days to the XP95 publication deadline, XP95 may be re-accessing or re-validating exfiltrated SA government data. Secondary: any SA government-adjacent environment may have undetected XP95 access.

MITRE ATT&CK: T1083 (File and Directory Discovery), T1530 (Data from Cloud Storage), T1048 (Exfiltration Over Alt Protocol), T1567 (Exfiltration to Cloud Storage — Telegram)

IOCs: Telegram API traffic (api.telegram.org, 149.154.160.0/20) from government infrastructure; bulk ZIP/RAR archive creation of PII datasets; access to HR/recruitment database tables from non-admin accounts; cloud storage upload to non-standard destinations

Data Sources: Firewall/proxy logs (outbound to Telegram IPs), EDR (archiving tool execution, bulk file reads), SIEM (after-hours database access), DNS

TH-2026-W16-03 — Krybit ISP Lateral Risk

P2 — HIGH: Active extortion; downstream risk unconfirmed but plausible

Hypothesis: Krybit’s compromise of Megasurf (ISP/data centre) may have exposed hosted client environments to lateral access via shared network infrastructure or management plane compromise.

MITRE ATT&CK: T1199 (Trusted Relationship), T1078 (Valid Accounts), T1021.001 (Remote Desktop Protocol)

IOCs: Unexpected RDP or SSH sessions from Megasurf IP ranges (check ASN); new admin accounts on hosted servers; anomalous traffic from data centre management VLANs

Data Sources: Firewall logs (ingress from Megasurf ASN), EDR (new account creation, RDP from DC ranges), hosted server authentication logs

TH-2026-W16-04 — Contagious Interview Supply Chain

P2 — HIGH: 1,700+ malicious packages in the wild

Hypothesis: North Korean Contagious Interview actors may have delivered malicious npm/PyPI packages to SA developers or data science teams, installing info-stealers or credential harvesters.

MITRE ATT&CK: T1195.001 (Compromise Software Dependencies), T1566.001 (Spearphishing Attachment — fake interview task), T1059.007 (JavaScript/Node.js execution)

IOCs: npm packages from unknown authors published after 1 March 2026; Python packages matching Contagious Interview naming patterns; outbound connections to Korean/Russian IPs from developer workstations; BeaverTail or InvisibleFerret malware hashes (CISA advisory)

Data Sources: EDR (npm/node/python process trees), developer workstation proxy logs, SIEM (after-hours package install events), endpoint AV/XDR telemetry

Hunt Checklist

Hunt ID	Hypothesis (Short)	Priority	Data Sources	Status
TH-2026-W16-01	Salt Typhoon Cisco router implant	P1 — CRITICAL	Syslog, NetFlow, AAA, IOS-XE	Not Started
TH-2026-W16-02	XP95 pre-publication data validation	P1 — CRITICAL	Firewall, EDR, SIEM, DNS	Not Started
TH-2026-W16-03	Krybit ISP lateral risk	P2 — HIGH	Firewall, EDR, Auth logs	Not Started
TH-2026-W16-04	Contagious Interview supply chain	P2 — HIGH	EDR, Proxy, SIEM, AV/XDR	Not Started

IOC Master Table — W16

Indicator	Type	Attribution	Hunt ID
api.telegram.org	Domain	XP95 C2 / exfiltration	TH-2026-W16-02
149.154.160.0/20	IP Range	Telegram / XP95	TH-2026-W16-02
GRE tunnel (unexpected)	Network artefact	Salt Typhoon	TH-2026-W16-01

Indicator	Type	Attribution	Hunt ID
SNMP poll from external IP	Network artefact	Salt Typhoon	TH-2026-W16-01
BeaverTail malware	Malware family	Contagious Interview (DPRK)	TH-2026-W16-04
InvisibleFerret malware	Malware family	Contagious Interview (DPRK)	TH-2026-W16-04
CVE-2026-35616	CVE	Fortinet exploit (unattributed)	N/A — Patch
CVE-2026-1340	CVE	Ivanti exploit (unattributed)	N/A — Patch
CVE-2026-39987	CVE	Marimo exploit (unattributed)	N/A — Patch
c05d5254	File hash	UNC5221 / F5 BIG-IP	Carry-forward from W15

11. RECOMMENDATIONS

Immediate (This Week — Before 20 April)

- **1. Activate POPIA s22 notification readiness:** Draft individual notification templates and public statement for Stats SA / GCRA data subjects. Legal review required. If your organisation employed Stats SA job-seekers or recruited GCRA bursary holders, draft your own POPIA s22. Deadline: this week.
- **2. Run Salt Typhoon detection playbook** on all Cisco IOS-XE edge routers — especially telco, ISP, and financial services environments. Run "show ip tunnel" and compare running-config to baseline. Any unexplained delta is a P1 incident.
- **3. Patch FortiClient EMS to 7.4.7** (CVE-2026-35616) and **Ivanti EPMM to 12.8** (CVE-2026-1340) — both CISA KEV with federal deadlines already passed. Unauthenticated RCE is actively exploited.
- **4. Audit Kerberos RC4 dependencies** before 14 April Microsoft Patch Tuesday — the update enforces AES-SHA1 on DCs and will break legacy RC4 systems. Inventory now.
- **5. Run TH-2026-W16-02** (XP95 pre-publication hunt) on government-adjacent HR portal environments to detect any residual XP95 access.

Short-Term (This Quarter)

- Implement network segmentation between data centre management VLANs and client-hosted environments — Krybit/Megasurf compromise illustrates ISP supply-chain risk.
- Audit npm/PyPI packages installed since 1 March 2026 on developer workstations — Contagious Interview campaign delivered 1,700+ malicious packages. Scan with BeaverTail/InvisibleFerret hashes.
- Update WordPress/Joomla Smart Slider 3 Pro plugin on all SA-hosted sites. Audit server logs for 7 April access anomalies if not updated on that date.
- Conduct a full Cisco IOS-XE device inventory and verify firmware versions against Cisco PSIRT advisories. All edge devices should be inventoried and current.
- Assess DORA Register of Information requirements if operating as SA subsidiary of EU financial institution — first filing period closed March 2026; NIS2 audit deadline 30 June 2026.

Strategic

- The XP95 PFMA constraint reveals a structural policy gap: SA government entities cannot pay ransoms but also lack compensating controls (air-gapped backups, encrypted HR databases, rapid data classification). A formal PFMA policy exemption or national incident response fund needs legislative consideration.
- Salt Typhoon's confirmed SA telecom targeting requires a national-level response. ICASA and SARB should coordinate to mandate Salt Typhoon detection scanning across all licensed SA telecom

operators.

- The IR's capacity constraint (1,320 open matters; 14% IO registration rate) versus the incoming 20 April PII crisis suggests the IR needs emergency resource allocation from the Department of Justice. The current staffing level cannot process a 453,000+ data subject notification event.

12. OSINT SOURCES CONSULTED

The following open-source intelligence sources were consulted in the preparation of this report. All sources are TLP:WHITE and publicly accessible.

1. UpGuard — Statistics South Africa Data Breach 2026 — <https://www.upguard.com/news/statistics-south-africa-data-breach-2026-03-31>
2. Breachsense — GCRA Breach Listing — <https://www.breachsense.com/breaches/gauteng-city-region-academy/>
3. Breachsense — Singita Breach Listing — <https://www.breachsense.com/breaches/singita/>
4. Ransomware.live — South Africa Victim Map — <https://www.ransomware.live/map/ZA>
5. TechCrunch — Salt Typhoon SA Telecom Confirmed — <https://techcrunch.com/2026/03/09/salt-typhoon-china-who-has-been-hacked-global-telecom-giants/>
6. Recorded Future — Salt Typhoon Global Telecom Espionage — <https://www.recordedfuture.com/research/salt-typhoon-global-telecom-espionage>
7. DataBreaches.net — XP95 SA Government Victims — <https://databreaches.net/2026/03/30/south-african-government-agency-and-spamish-psychological-software-provider-victims-of-cyberattacks-by-xp95/>
8. ITWeb — Liberty IR Escalation — <https://www.itweb.co.za/article/insurer-liberty-hit-by-data-breach/o1Jr5MxPwrdMKdWL>
9. EWN — SA Banks SIM-Swap and Vishing Warning April 2026 — <https://www.ebnewsdaily.co.za/2026/04/02/south-africa-banks-warn-sim-swap-voice-phishing-fraud-2026/>
10. CISA — Known Exploited Vulnerabilities Catalog — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
11. Fortinet PSIRT — CVE-2026-35616 Advisory — <https://www.fortiguard.com/psirt/FG-IR-26-35616>
12. Ivanti — CVE-2026-1340 Security Advisory — <https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-EPMM-CVE-2026-1340>
13. Cisco TAC — Salt Typhoon Detection Advisory — https://sec.cloudapps.cisco.com/security/center/resources/salt_typhoon_detection.html
14. BleepingComputer — Contagious Interview 1,700 Packages — <https://www.bleepingcomputer.com/news/security/north-korean-hackers-contagious-interview-1700-packages/>
15. TechCentral — AG Report on Government Cyber Defences — <https://techcentral.co.za/gaping-holes-in-south-african-government-cyber-defences/279769/>
16. IOL / Sophos — SA Ransomware Recovery Costs R24M — <https://iol.co.za/business-report/economy/2025-07-04-ransomware-recovery-costs-south-african-businesses-r24-million-on-average-report-finds/>
17. iAfrica — IBM Breach Cost AI 2025 — <https://iafrica.com/ai-helps-cut-south-africas-data-breach-costs-by-17-in-2025-ibm-report/>
18. INTERPOL — 2026 Financial Crime Report — <https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-Financial-Crime-Report-2026>
19. ITLawCo — IR Annual Performance Plan 2026-27 — <https://itlawco.com/information-regulator-2026-27-annual-performance-plan/>
20. SABRIC — Annual Crime Statistics Report 2024 — <https://www.sabric.co.za/wp-content/uploads/2025/09/CRIME-STATISTICS-REPORT-2024.pdf>
21. Kaspersky — APT41 Targets Southern Africa — <https://www.kaspersky.com/about/press-releases/kaspersky-apt41-targets-southern-african-organization-in-espionage-attack>
22. DeXpose.io — DragonForce Targets Singita — <https://www.dexpose.io/dragonforce-targets-luxury-safari-operator-singita/>
23. Marimo — CVE-2026-39987 Security Advisory — <https://github.com/marimo-team/marimo/security/advisories/>
24. BleepingComputer — Smart Slider 3 Pro Backdoor — <https://www.bleepingcomputer.com/news/security/smart-slider-3-pro-backdoor/>
25. Pinsent Masons — SA Data Breach Incident Response — <https://www.pinsentmasons.com/out-law/news/south-african-data-breach-highlights-need-incident-response>
26. BlackFog — State of Ransomware March 2026 — <https://www.blackfog.com/the-state-of-ransomware-march-2026/>
27. CM Alliance — Biggest Cyber Attacks March-April 2026 — <https://www.cm-alliance.com/cybersecurity-blog/biggest-cyber-attacks-data-breaches-ransomware-attacks-of-march-2026>
28. SABRIC — Digital Banking Fraud Statistics 2025 — <https://www.sabric.co.za/wp-content/uploads/2025/09/CRIME-STATISTICS-REPORT-2024.pdf>
29. ITWeb — SA Cyber Intelligence W16 — <https://www.itweb.co.za>
30. Cisco PSIRT — IMC CVE-2026-20093 Advisory — <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-auth-bypass>

This report is classified TLP:WHITE. It may be distributed without restriction. Information sourced from publicly available OSINT. No classified or restricted sources were used. Prepared by Digital Progression | dpcyber.co.za | DP-CTI-2026-W16