SOUTH AFRICA
CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 15 | 30 March - 5 April 2026

THREAT LEVEL: HIGH

XP95 claims Stats SA (154GB) and GCRA (147GB), DragonForce hits Singita, triple critical edge-device CVEs (F5/Citrix/Fortinet), SA victim count reaches 103, IR escalates Liberty investigation to CEO level

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W15 | Classification: TLP:WHITE

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH — Sustained and intensifying. XP95 ransomware group claimed two SA government targets in Week 15: Statistics South Africa (154 GB / 453,362 files) and the Gauteng City Region Academy (147 GB / 429,473 student records), both with a 20 April 2026 deadline. DragonForce claimed luxury safari operator Singita on 2 April, pushing SA's cumulative ransomware victim count to 103. Three simultaneous critical edge-device CVEs (F5 BIG-IP, Citrix NetScaler, Fortinet FortiClient EMS) are actively exploited — all dominant technologies in SA enterprise. The Information Regulator escalated the Liberty Group investigation to CEO level.[1]

KPI Dashboard

Metric	Current (W15)	Baseline / Prior	Change	Direction
SA cyberattacks/week	2,204	1,619 (W14 2025 avg)	+36% YoY	UP
SA ransomware victims (cumulative)	103	95-96 (W14 end)	+7 this week	UP
New SA victims (W15)	3 confirmed	5 (W14)	-2	DOWN
POPIA notifications YTD	2,898 (to 5 Mar 2026)	202 (2021/22)	+15x since 2021	UP
CISA KEV new entries W15	2	3 (W14)	-1	DOWN
Critical CVEs actively exploited	5	3 (W14 avg)	+2	UP
Latest SA ransom demand	$100K / R1.7M (XP95 vs Stats SA)	R5.4M (Land Bank, 5 BTC)	Smaller demand, diff actor	FLAT
SA avg recovery cost (excl. ransom)	R24M (Sophos 2025)	R19M (2024 Sophos)	+26% YoY	UP

ANOMALY FLAG: Cumulative SA victim count reached 103 — up 7-8 in a single week, the largest single-week increase since W12. Three simultaneous critical edge-device CVEs under active exploitation (F5, Citrix, Fortinet) present a compound perimeter-breach risk. The 20 April XP95 deadline creates a national PII crisis for 453,000+ job-seekers if government does not act.[2]

TOP 3 ACTIONS THIS WEEK

1. PATCH CITRIX AND F5 IMMEDIATELY (P1): CVE-2026-3055 (Citrix NetScaler, CVSS 9.3) and CVE-2025-53521 (F5 BIG-IP, CVSS 9.8) are both actively exploited with Metasploit modules publicly available. Every hour of delay increases breach probability. Check exposure via Shodan/Censys before patching to confirm whether appliances are internet-facing.

2. HUNT FOR XP95 INITIAL ACCESS INDICATORS: XP95 has three unresolved SA government targets with a 20 April deadline. Their TTPs indicate exploitation of internet-facing legacy HR systems and public-sector application portals. Run a threat hunt for unusual outbound data transfers (over 10GB), access to HR/student database tables outside business hours, and new scheduled tasks or admin accounts in government-adjacent environments.

3. BRIEF YOUR BOARD ON THE 20 APRIL DEADLINE: Stats SA and GCRA data will almost certainly be published or sold on 20 April if ransoms remain unpaid. Any organisation that shares employee data with Stats SA, or recruits from the GCRA bursary pool, has second-order PII exposure. Prepare breach notification templates now.

Critical Findings:

▪ XP95 ransomware group (emerged March 2026) has exclusively targeted SA government entities; two unresolved $100K deadlines converge 20 April — Stats SA (154GB/453K files) and GCRA (147GB/429K student records). Data publication near-certain unless deadline is extended or ransoms

paid.[3]

▪ DragonForce claimed luxury safari operator Singita (2 April); SA cumulative ransomware victim count rose to 103, up 7-8 from W14. DragonForce remains the most prolific group targeting SA, now with 5+ confirmed victims.[4]

▪ Standard Bank confirmed POPIA s22 notification and client alerts for a linked Liberty Group data exposure — ID numbers, names, email addresses. Information Regulator escalated investigation to CEO-level meeting.[5]

▪ Three simultaneous critical edge-device vulnerabilities actively exploited: F5 BIG-IP APM (CVSS 9.8, nation-state), Citrix NetScaler (CVSS 9.3, Metasploit-ready), Fortinet FortiClient EMS (CVSS 9.1, zero-day). All three are dominant technologies in SA enterprise.[6]

▪ Auditor-General SA: 64% of government entities have notable cybersecurity weaknesses; R5.5 billion in IT spending failed to drive meaningful modernisation. SABS still in recovery 15 months post-ransomware.[7]

SECTOR SPOTLIGHT: GOVERNMENT / PUBLIC SECTOR (CRITICAL)

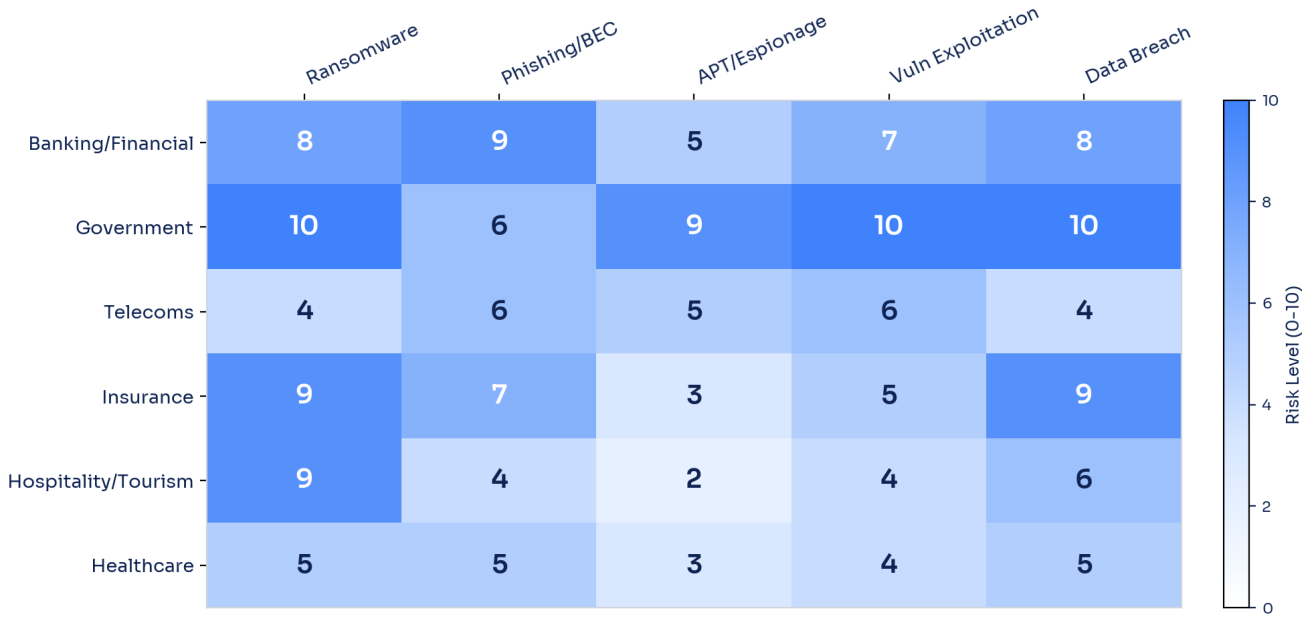
Government and public sector is the unambiguous high-risk sector for W15. Three government entities — Stats SA, GCRA, and the Gauteng Provincial Government — are confirmed XP95 victims with unresolved leak deadlines. The Auditor-General's April 2026 report confirmed that 64% of assessed government entities have notable cybersecurity weaknesses, and R5.5 billion in IT spending failed to drive meaningful modernisation. XP95's exclusive focus on SA public-sector targets — using pure data exfiltration rather than encryption — exploits the fact that government entities cannot legally pay ransoms under PFMA, making data publication near-certain once a government target is claimed.[7]

1. ITWeb SA — Cyber Threat Intelligence — https://www.itweb.co.za
2. Ransomware.live — SA Victims Map — https://www.ransomware.live/map/ZA
3. UpGuard — Stats SA Data Breach 2026 — https://www.upguard.com/news/statistics-south-africa-data-breach-2026-03-31
4. DeXpose.io — DragonForce targets Singita — https://www.dexpose.io/dragonforce-targets-luxury-safari-operator-singita/
5. EWN — Liberty data breach — https://www.ewn.co.za/2026/03/24/data-breach-at-liberty-insurance-and-investment-group-highlights-cyber-risk
6. CISA Known Exploited Vulnerabilities — 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 from Low to Critical based on active threat intelligence, confirmed incidents, and vulnerability exposure during Week 15. Government is rated MAXIMUM across ransomware, APT/espionage, vulnerability exploitation, and data breach — driven by three simultaneous XP95 victims with unresolved leak deadlines.

SA THREAT LANDSCAPE HEATMAP | W15 (30 Mar - 5 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 15 confirmed three new SA incidents and produced material developments on three W14 carry-overs. The SA cumulative ransomware victim count stands at **103** as of 5 April 2026.

3.1 Statistics South Africa — XP95 Data Extortion (W15 NEW)

Organisation	Statistics South Africa (statssa.gov.za)
Sector	Government / National Statistics
Threat Actor	XP95
Date	Exfiltration: est. February 2026; disclosed 29-30 March 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
Payment	Refused — PFMA prohibits ransom payment
Status	Active extortion. Sample posted on XP95 Telegram as proof-of-breach.
Sources	ITWeb, UpGuard, Breachsense, The Citizen, Pinsent Masons, BlackFog, CM Alliance

Stats SA is the national statistics authority holding sensitive demographic, economic, and census data. XP95 posted a sample of the stolen dataset on their Telegram channel as proof. Stats SA filed a POPIA s22 notification with the Information Regulator on 29 March. This is XP95's second SA government victim in one month after Gauteng Provincial Government (3.8 TB, 13 March). With PFMA prohibiting ransom

payment, data publication on 20 April is near-certain.[3]

3.2 Gauteng City Region Academy (GCRA) — XP95 Data Extortion (W15 NEW)

Organisation	Gauteng City Region Academy (gcrabursary.gauteng.gov.za)
Sector	Government / Education / Bursaries
Threat Actor	XP95
Date	Exfiltration: mid-March 2026; posted late March / W15 window
Data	147 GB / 429,473 files — scholarship and bursary applicant records (student PII, financial details, academic r
Demand	$100,000 USD (R1.7 million)
Deadline	20 April 2026 (same as Stats SA)
Payment	Unknown — GCRA issued no public statement as of 5 April
Status	Active extortion. No public response from GCRA.
Sources	ITWeb, BlackFog, social media

GCRA administers bursary and scholarship programmes for the Gauteng provincial government. The dataset contains student PII including financial and academic records for 429,473 individuals. The simultaneous 20 April deadline with Stats SA suggests a coordinated campaign targeting government entities that cannot legally pay ransoms under PFMA.[8]

3.3 Singita — DragonForce Ransomware (W15 NEW)

Organisation	Singita (singita.com) — luxury safari/conservation lodge operator
Sector	Hospitality / Tourism / Conservation
Threat Actor	DragonForce
Date	Claimed 2 April 2026
Data	Not yet published; DragonForce threatens imminent publication
Demand	Unknown
Payment	N/A
Status	Active extortion. No public statement from Singita.
SA significance	SA's 5th DragonForce victim (after The Unlimited, National Credit Regulator, ERWAT, affiliates)
Sources	DeXpose.io, ransomware.live

Singita is a high-profile conservation and safari hospitality operator with lodges across southern and east Africa. DragonForce's attack signals the group's expansion into the luxury travel and conservation sector — organisations that hold high-net-worth client data and are potentially less mature in cybersecurity than financial services targets. DragonForce's cartel affiliate model (80% affiliate payout) drives volume attacks across diverse sectors.[4]

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

Standard Bank sent client notification emails in the first days of April, confirming that names, surnames, ID numbers, and email addresses were compromised. The Information Regulator requested an urgent CEO-level meeting with Liberty Group around 25-29 March, and the matter escalated further into W15. Forensics remain ongoing; the full customer count and attack vector have not been disclosed publicly. Liberty's extortion attempt was declined.[59]

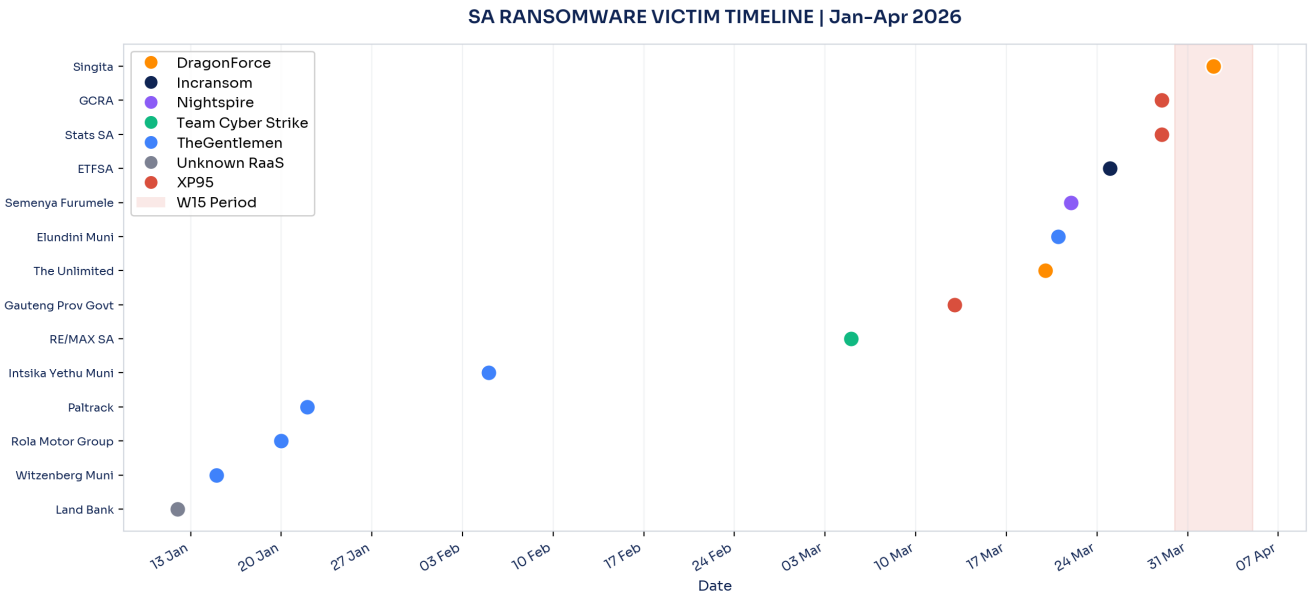
3.5 Virgin Active SA — IDOR Vulnerability (W14 Follow-On, Ongoing Coverage)

Originally reported 23-24 March (W14), an IDOR vulnerability in Virgin Active SA's payment systems potentially exposed bank account details of up to 631,000 members. No confirmed data exfiltration. No threat actor claimed it. Patch status not confirmed as of 5 April.[10]

3.6 ETFSA (Incransom) — W14 Follow-On, No New W15 Developments

Incransom listed ETFSA originally in W14 (26 March). No new public developments confirmed during the W15 reporting window. Full client dataset publication remains threatened. Incransom active in W15 globally.

SA Ransomware Victim Timeline — Jan-Apr 2026



8. BlackFog — State of Ransomware March 2026 — https://www.blackfog.com/the-state-of-ransomware-march-2026/
9. Priviso Live — Liberty breach, 29 March — https://www.youtube.com/watch?v=2MHBC9GizZc
10. MyBroadband — Virgin Active IDOR — https://mybroadband.co.za/news/security/635179-security-vulnerability-at-biggest-gym-chain-in-south-africa.html

4. ACTIVE THREAT CAMPAIGNS

4.1 Banking Fraud and BEC Surge

SABRIC data shows **R1.888 billion** in digital banking fraud losses in 2025, with **97,975 incidents (+86% YoY)**.[11] Absa, FNB, Nedbank, and Standard Bank issued a joint banking sector alert on a vishing and SIM-swap surge during W15. AI-powered fraud is 4.5x more profitable per INTERPOL's 2026 Financial Crime Report. No new W15-specific DDoS or defacement incidents were confirmed.

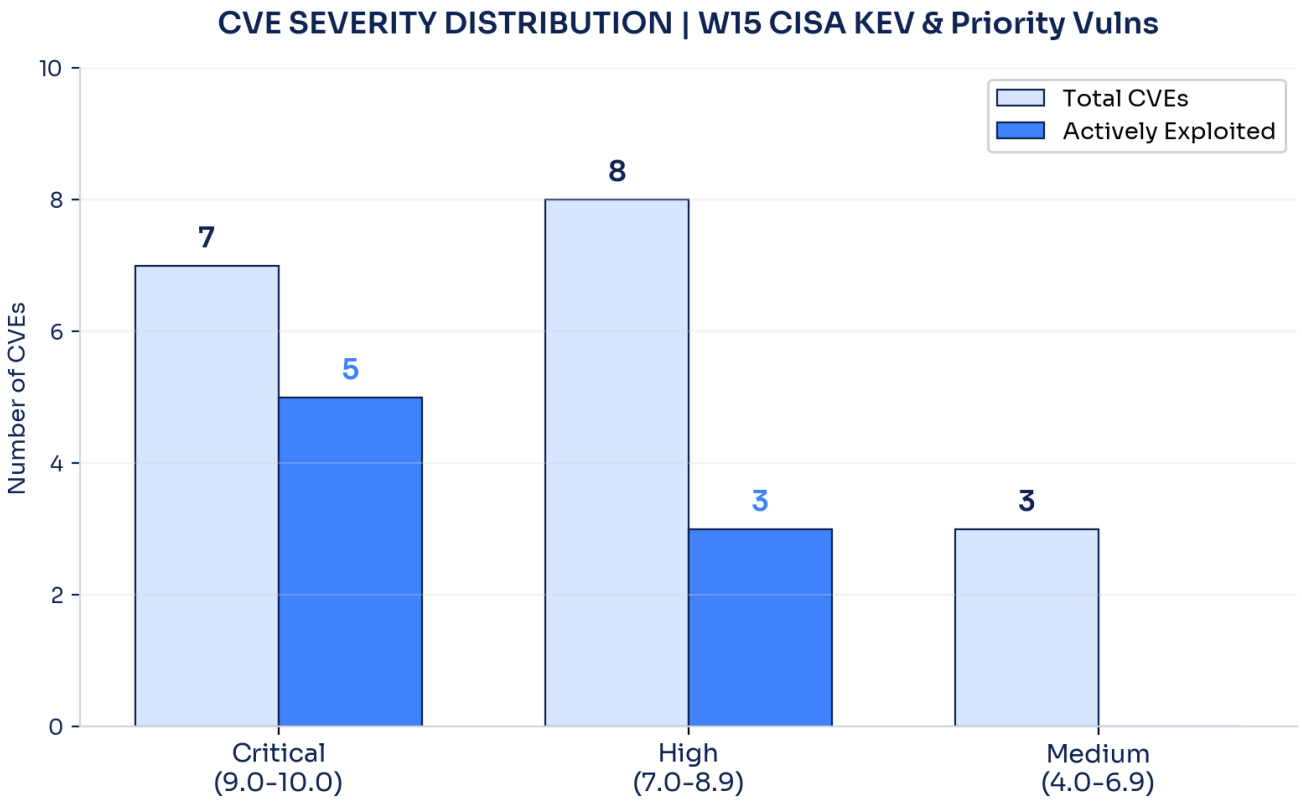
4.2 Lapsus$ Re-emergence

Lapsus$ claimed an AstraZeneca breach: **3 GB of source code and credentials** exfiltrated between 24-26 March, published 5 April 2026. Lapsus$ previously targeted **Vodacom and MTN** in 2022 — their historical SA nexus creates renewed relevance for SA telecoms and pharmaceutical sectors. The group also claimed the French Ministry of Agriculture and the University of Lille in this same re-emergence wave. SA telecoms

and pharma sector security teams should heighten monitoring.[12]

11. SABRIC Annual Crime Statistics 2024 — https://www.sabric.co.za/wp-content/uploads/2025/09/CRIME-STATISTICS-REPORT-2024.pdf
12. CM Alliance — Biggest cyber attacks March 2026 — https://www.cm-alliance.com/cybersecurity-blog/biggest-cyber-attacks-data-breaches-ransomware-attacks-of-march-2026

5. CRITICAL VULNERABILITIES



Week 15 saw **2 new CISA KEV entries**: CVE-2026-3055 (Citrix NetScaler, added 30 March) and CVE-2026-5281 (Google Chrome, added 1 April). Three simultaneous P1 critical edge-device vulnerabilities are actively exploited — F5 BIG-IP APM, Citrix NetScaler, and Fortinet FortiClient EMS — representing an unusually dangerous compound perimeter-breach risk for SA enterprises.[13]

CISA KEV Additions — W15

CVE ID	Product	CVSS	Date Added	Action Due
CVE-2026-3055	Citrix NetScaler ADC/Gateway	9.3	30 Mar 2026	2 Apr 2026
CVE-2026-5281	Google Chrome Dawn/WebGPU	High	1 Apr 2026	15 Apr 2026

Priority Vulnerability Matrix — W15

CVE ID	Vendor/Product	CVSS	Exploited?	SA Relevance
CVE-2025-53521	F5 BIG-IP APM	9.8	YES (UNC5221/China)	CRITICAL
CVE-2026-3055	Citrix NetScaler ADC/GW	9.3	YES (Metasploit)	CRITICAL
CVE-2026-35616	Fortinet FortiClient EMS	9.1	YES (zero-day)	CRITICAL
CVE-2026-21643	Fortinet FortiClient EMS	9.1	YES (SQL injection)	CRITICAL
CVE-2026-20093	Cisco IMC	9.8	Not yet; PoC imminent	HIGH

CVE ID	Vendor/Product	CVSS	Exploited?	SA Relevance
CVE-2026-5281	Google Chrome WebGPU	High	YES (KEV)	HIGH
CVE-2026-20160	Cisco SSM On-Prem	9.8	Not confirmed	HIGH
CVE-2026-27685	SAP NetWeaver Ent Portal	9.1	Not confirmed	HIGH
CVE-2019-17571	SAP FS-QUO (Log4j 1.2)	9.8	SAP Patch Day	HIGH

Top 5 CVE Detail — SA Priority

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

Pre-auth RCE; reclassified from CVSS 7.5 on 27 March after nation-state exploitation confirmed. Attributed to UNC5221 (China-nexus); Brickstorm backdoor deployed; memory webshells observed. 14,000+ instances still unpatched globally; SA scanning previously recorded (GreyNoise, Oct 2025). CISA KEV added 27 March; federal deadline 30 March. Patch: F5 advisory K000156741. **SA relevance:** F5 BIG-IP is primary SSO/VPN/ADC in SA banking and telco.[14]

CVE-2026-3055 — Citrix NetScaler ADC/Gateway — CVSS 9.3 — P1 CRITICAL

Memory leak via malformed SAML request; extracts authenticated admin session IDs. Metasploit module published — low skill barrier. Active exploitation from 27 March confirmed by watchTowr and Defused Cyber. 29,000 NetScaler + 2,250 Gateway instances exposed globally. Patch: 14.1-66.59, 13.1-62.23, 13.1-37.262. **SA relevance:** Dominant ADC/VPN in SA financial services, government, healthcare.[15]

CVE-2026-35616 — Fortinet FortiClient EMS — CVSS 9.1 — P1 HIGH

Zero-day; unauthenticated API command execution. Active exploitation from 31 March; out-of-band patches released 5 April. Companion CVE-2026-21643 (CVSS 9.1 SQL injection) also actively exploited since 26 March. Patch: FortiClient EMS 7.4.7 (hotfix). **SA relevance:** Fortinet dominant in SA mid-market and enterprise.[16]

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

Auth bypass; unauthenticated admin password reset on hardware management plane. No exploitation confirmed yet; PoC likely imminent. Affects UCS C/E/S series plus dozens of Cisco appliances. **SA relevance:** Cisco UCS widespread in SA enterprise data centres.[13]

CVE-2026-5281 — Google Chrome Dawn/WebGPU UAF — High — P2

4th actively exploited Chrome zero-day in 2026. All endpoints below Chrome 146.0.7680.178 at risk. CISA KEV added 1 April; due date 15 April. Universal SA endpoint risk.[13]

13. Cisco Security Advisories — https://sec.cloudapps.cisco.com/security/center/publicationListing.x
14. F5 Advisory K000156741 — https://my.f5.com/manage/s/article/K000156741
15. watchTowr — CVE-2026-3055 Advisory — https://labs.watchtowr.com/advisory-citrix-netscaler-cve-2026-3055/
16. Fortinet PSIRT — https://www.fortiguard.com/psirt

6. THREAT ACTOR PROFILES & RANSOMWARE ACTIVITY

South Africa's cumulative ransomware victim count stands at **103** as of 5 April 2026, up from 95-96 at the end of W14. This represents the largest single-week increase since W12 — 7 to 8 new victims in one week. DragonForce remains the most prolific group targeting SA, while XP95 is the most dangerous given its exclusive government focus and the structural impossibility of ransom payment under PFMA.[17]

Active Threat Actors Targeting SA — W15

Group	SA Victim(s)	Type	Key TTPs / CVEs	Status
DragonForce	Singita (W15); The Unlimited, NCR, ERWAT + affiliates	RaaS cartel (80% payout)	Ivanti CVE-2023-46805, SimpleHelp, Log4Shell, MEGA.nz exfil, BYOVD	PRIMARY THREAT
XP95	Stats SA, GCRA (W15); Gauteng (W14)	Data extortion (no encryption)	T1190 (internet-facing HR portals); Telegram C2; no ransom paid	EMERGING, CRITICAL

Group	SA Victim(s)	Type	Key TTPs / CVEs	Status
Nightspire	8 global W15 victims; Semenya Furumele (W14)	Closed RaaS	CVE-2024-55591 (FortiOS auth bypass)	ACTIVE
Incransom	ETFSA (W14 follow-on)	RaaS	CVE-2023-3519 (Citrix); financial sector focus	ACTIVE
Lapsus$	AstraZeneca (W15); historical: Vodacom, MTN (2022)	Data extortion	Credential theft; insider access; code exfil	RE-EMERGED
APT41	SA gov IT provider (confirmed Jul 2025)	Nation-state (China)	T1190; long-dwell supply chain	PERSISTENT
UNC5221	F5 BIG-IP global (incl. SA)	Nation-state (China-nexus)	CVE-2025-53521; Brickstorm backdoor	ACTIVE

DragonForce — PRIMARY SA Threat Actor

DragonForce operates as a RaaS cartel offering affiliates an 80% revenue share — a model that is driving volume attacks across diverse SA sectors. With 5+ confirmed SA victims, DragonForce is the most prolific group targeting South Africa. Their W15 target, Singita, represents a notable expansion into luxury hospitality and conservation. DragonForce's primary exfiltration channel is MEGA.nz (g.api.mega.co.nz), which should be blocked at the proxy/DNS layer in all SA enterprise environments.[4]

XP95 — EMERGING SA-Focused Data Extortion Group

XP95 emerged in March 2026 and has exclusively targeted SA government entities. In under 30 days, the group has claimed three SA victims: Gauteng Provincial Government (3.8 TB), Statistics South Africa (154 GB), and GCRA (147 GB). XP95 uses pure data exfiltration — no encryption — making traditional backup-based recovery irrelevant. Communications are exclusively via Telegram. The group's strategy of targeting entities prohibited from paying ransoms (PFMA constraint) virtually guarantees data publication. Their only confirmed international victim is Eholo Health (Spain, 165 GB, data released after failed negotiation).[3]

Nightspire — ACTIVE, Africa-Region Focus

Nightspire recorded 8 global victims in W15 (2-4 April). SA-linked victims include Semenya Furumele (W14), Eastern Cape DTHS (November 2025), and Ingonyama Trust Board. Primary vector is CVE-2024-55591 (FortiOS auth bypass).[17]

Nation-State Activity

APT41 (China) was confirmed active in southern Africa by Kaspersky MDR (July 2025 report, still operationally relevant). UNC5221 (China-nexus) actively exploiting F5 BIG-IP APM through W15. Volt Typhoon ("Voltzite") has documented African utilities targeting, but no new W15-specific disclosures for SA.[17]

Auditor-General SA — April 2026 Report

The Auditor-General confirmed: 64% of 70 assessed government entities have notable cybersecurity weaknesses; R5.5 billion in IT spending in 2024/25 failed to drive modernisation; multiple environments were breached during penetration testing. SABS remains in recovery 15 months after a November 2024 ransomware attack. This data validates XP95's targeting strategy: SA government is a soft target with structural underspend on security maturity.[7]

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

7. OSINT EXPOSURE & ATTACK SURFACE

7.1 Global Infrastructure Exposure with SA Impact

F5 BIG-IP (CVE-2025-53521): 14,000+ instances unpatched globally as of W15. SA scanning confirmed by GreyNoise in prior period (October 2025). SA banking and telco are primary F5 users.[14]
Citrix NetScaler (CVE-2026-3055): Approximately 29,000 NetScaler instances and 2,250 Gateway instances exposed globally. SA financial services sector is a heavy Citrix user. Metasploit module availability drastically lowers attacker skill threshold.[15]

7.2 POPIA Breach Notification Baseline

The Information Regulator received 2,898 POPIA s22 breach notifications in FY 2025/26 (to 5 March 2026) — representing a **15x increase** from the 2021/22 baseline of 202 notifications. Only 14% of the estimated 490,000 organisations required to register a POPIA information officer have done so. This systemic underinvestment across SA organisations creates broad attack surface and regulatory exposure simultaneously.[18]

7.3 XP95 Primary Attack Surface

XP95's confirmed attack pattern targets public-sector HR portals and citizen application portals. All three SA victims (Gauteng, Stats SA, GCRA) share this profile: internet-facing portals accepting public applications or CVs, with backend databases containing citizen PII. Any SA government entity with an internet-facing HR or application portal should treat itself as a likely XP95 target and run TH-2026-W15-01 immediately.[3]

7.4 No New SA-Specific Shodan/GreyNoise Data for W15

No new SA-specific infrastructure exposure data from Shodan or GreyNoise was published during the W15 reporting window beyond data from prior periods. The prior-period GreyNoise F5 BIG-IP SA scanning data remains operationally relevant.

18. ITLawCo — Information Regulator 2026/27 APP analysis — https://itlawco.com/information-regulator-2026-27-annual-performance-plan/

8. REGULATORY & COMPLIANCE

8.1 Information Regulator — W15 Escalations

Liberty Group: The Information Regulator requested an urgent CEO-level meeting with Liberty Group around 25-29 March. The investigation escalated further during W15. Full IR enforcement outcome pending.[5]
Stats SA: Stats SA filed a POPIA s22 notification on 29 March 2026. IR guidance on government sector XP95 response is pending. No public statement from IR on the GCRA breach as of 5 April.[3]

8.2 New Regulatory Publications

POPIA Health Data Regulations (GG 54268): In force from 6 March 2026. Covers insurers, medical schemes, pension funds, and employers processing employee health data. New data security safeguards and breach notification obligations.[18]
SARB/FSCA Joint Standard 2 of 2024 (effective June 2025): First enforcement cycle underway. Requirements include board-approved cybersecurity strategy, 24-hour material incident reporting, annual penetration testing, MFA, and third-party risk oversight.
PAIA Annual Report Deadline: 1 April – 30 June 2026 for all public and private bodies subject to PAIA.

Cumulative Information Regulator Enforcement Record

Organisation	Action	Status
Lancet Laboratories	R200,000 administrative fine	Paid
Department of Justice	R5,000,000 fine (highest to date)	Enforcement
Dis-Chem	Enforcement notice + corrective orders	Correcting
SAPS	Enforcement notice + apology + POPIA training	Closed
TransUnion	PIA ordered + access controls overhaul	Ongoing
JSE	PAIA notice (January 2026)	Ongoing
WhatsApp	Settlement (late 2025)	Settled
Liberty Group	Investigation escalated to CEO level	PENDING

Upcoming Regulatory Deadlines

Deadline	Obligation	Regulator / Body
20 April 2026	XP95 data publication deadline (Stats SA + GCRA)	XP95 / IR
30 June 2026	PAIA annual report submission	Information Regulator
July 2026	SARB/FSCA AI discussion paper expected	SARB / FSCA
October 2026	SA FATF/FSRB mutual evaluation	FATF

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 all three P1 missions for immediate execution given the current threat landscape.

9a. Hunt Missions

TH-2026-W15-01: XP95 Initial Access and Exfiltration — **P1 -- CRITICAL**

Hypothesis: XP95 may have compromised SA public-sector HR/application portals to exfiltrate citizen PII. Hunt for pre-compromise reconnaissance and data staging in government-adjacent environments.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1560 (Archive Collected Data), T1048 (Exfiltration Over Alt Protocol), T1567 (Exfiltration to Cloud Storage)

IOCs: XP95 Telegram comms (web.telegram.org, t.me, 149.154.160.0/20); zip/7z creation of HR database files; access to /careers, /jobs, /applications endpoints

Data Sources: Web application logs, EDR (bulk file access, archiving tools), Firewall/proxy (large outbound transfers over 1GB), DNS (Telegram-related domains)

TH-2026-W15-02: Citrix NetScaler SAML Session Hijack (CVE-2026-3055) — **P1 -- CRITICAL**

Hypothesis: Attackers may be exploiting CVE-2026-3055 to extract admin session IDs from SA-facing Citrix NetScaler appliances configured as SAML IDP. Metasploit module is public.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1078.004 (Cloud Accounts), T1550.004 (Web Session Cookie)

IOCs: POST to /saml/login or /wsfed/passive with missing AssertionConsumerServiceURL; probe traffic to /cgi/GetAuthMethods; session tokens from unexpected IPs

Data Sources: NetScaler Access Logs, NetScaler Management Logs, WAF Logs, SIEM

TH-2026-W15-03: F5 BIG-IP APM Nation-State Backdoor (CVE-2025-53521) **P1 -- CRITICAL**

Hypothesis: UNC5221/China-nexus actors may have deployed memory-resident webshells or Brickstorm backdoor on SA F5 BIG-IP APM appliances.

MITRE ATT&CK: T1190, T1505.003 (Web Shell), T1059 (Command and Scripting Interpreter), T1070.004 (File Deletion)

IOCs: Hash c05d5254 (malicious binary per F5 advisory K000156741); /mgmt/shared/identified-devices/config/device-info access from external IPs; SELinux disable events

Data Sources: F5 BIG-IP iHealth logs, BIG-IP REST API audit logs, SELinux audit logs, sys-eicheck integrity checker output

TH-2026-W15-04: DragonForce Lateral Movement Post-Singita **P2 -- HIGH**

Hypothesis: DragonForce may have established persistence in Singita's systems and could pivot to shared IT service providers or affiliate lodge networks.

MITRE ATT&CK: T1021.002 (SMB/Windows Admin Shares), T1078 (Valid Accounts), T1048.003 (Exfil via HTTPS to MEGA.nz)

IOCs: g.api.mega.co.nz uploads; PsExec from non-standard hosts; Mimikatz (sekurlsa::logonpasswords); LSASS access; RDP server-to-server

Data Sources: EDR, DNS/Proxy (MEGA.nz traffic), Active Directory (new local admin accounts)

9b. Hunt Checklist

Copy this table into your ticketing system to track hunt execution.

Hunt ID	Hypothesis (short)	Priority	Data Sources	Status
TH-2026-W15-01	XP95 HR portal exfiltration	P1	Web logs, EDR, FW, DNS	Not Started
TH-2026-W15-02	Citrix SAML session hijack	P1	NetScaler, WAF, SIEM	Not Started
TH-2026-W15-03	F5 BIG-IP nation-state backdoor	P1	F5 iHealth, REST, SELinux	Not Started
TH-2026-W15-04	DragonForce Singita pivot	P2	EDR, DNS, AD	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
c05d5254	File hash (F5 malicious binary)	UNC5221 / China-nexus	TH-2026-W15-03
web.telegram.org	Domain	XP95 C2 comms	TH-2026-W15-01
t.me	Domain	XP95 C2 comms	TH-2026-W15-01
149.154.160.0/20	IP range	Telegram / XP95 exfil channel	TH-2026-W15-01
g.api.mega.co.nz	Domain	DragonForce exfil	TH-2026-W15-04
mega.nz	Domain	DragonForce exfil	TH-2026-W15-04
/saml/login (malformed POST)	URL pattern	CVE-2026-3055 exploit	TH-2026-W15-02
/wsfed/passive (malformed POST)	URL pattern	CVE-2026-3055 exploit	TH-2026-W15-02
/cgi/GetAuthMethods	URL pattern	CVE-2026-3055 probe	TH-2026-W15-02
/mgmt/shared/identified-devices/...	URL pattern	F5 BIG-IP fingerprinting	TH-2026-W15-03
sekurlsa::logonpasswords	Command string	Mimikatz credential dumping	TH-2026-W15-04
CVE-2026-3055	CVE	Citrix NetScaler SAML exploit	TH-2026-W15-02
CVE-2025-53521	CVE	F5 BIG-IP nation-state	TH-2026-W15-03

Indicator	Type	Attribution	Hunt ID
CVE-2026-35616	CVE	Fortinet FortiClient EMS	N/A

10. RECOMMENDATIONS

IMMEDIATE (P1 — This Week)

- **Patch Citrix NetScaler** to 14.1-66.59 / 13.1-62.23 / 13.1-37.262 — CVE-2026-3055 (CVSS 9.3), SAML IDP configs at highest risk. Metasploit module publicly available. (Ref Sec 5)
- **Apply F5 BIG-IP APM patches** per advisory K000156741; check iHealth for IOC hash c05d5254. Nation-state exploitation confirmed (UNC5221). (Ref Sec 5)
- **Patch Fortinet FortiClient EMS** to 7.4.7; apply hotfix for CVE-2026-35616 and CVE-2026-21643. Both zero-days actively exploited. (Ref Sec 5)
- **Deploy Chrome 146.0.7680.178+** across all endpoints for CVE-2026-5281 (CISA KEV, due 15 April). (Ref Sec 5)
- **Run TH-2026-W15-01** XP95 hunt across government-adjacent or HR system environments. (Ref Sec 9)
- **Review Cisco IMC internet exposure** before CVE-2026-20093 PoC is weaponised. (Ref Sec 5)

SHORT-TERM (This Quarter)

- Audit POPIA s22 notification readiness — the 20 April XP95 deadline creates second-order breach risk for organisations holding Stats SA or GCRA-sourced data. (Ref Sec 8)
- Segment HR application portals from core network — XP95 exploits poorly segmented public-sector HR systems. (Ref Sec 4)
- Implement MEGA.nz domain blocking at proxy/DNS layer — primary DragonForce exfiltration channel. (Ref Sec 9)
- Validate backup integrity against DragonForce and Nightspire TTPs (both target backup infrastructure). (Ref Sec 6)
- Register POPIA information officers if not yet done — 14% national compliance rate. PAIA annual report due 1 April – 30 June. (Ref Sec 8)

STRATEGIC

- The XP95 20 April deadline creates a national PII crisis if unpaid. Organisations processing employee or citizen data from Stats SA or GCRA should prepare breach notification workflows and individual notification templates now.
- DragonForce's cartel model (80% affiliate payout) is driving volume attacks. A sector-wide defensive collaboration framework — similar to SABRIC for banking — is needed for hospitality and private conservation sectors newly in the crosshairs.
- The Auditor-General's finding (64% of government entities with notable weaknesses) validates the systemic nature of XP95's success. Government organisations should prioritise annual penetration testing and adopt the NIST CSF 2.0 governance tier model.

ANOMALY-DRIVEN FLAGS

Cumulative victim count hit 103 in one week: The largest single-week increase since W12. Three P1 critical CVEs exploited simultaneously. XP95 20 April deadline for two government entities. This is the highest compound risk week of 2026 for SA.

XP95's PFMA-exploitation model is working: By exclusively targeting entities legally prohibited from paying ransoms, XP95 makes data publication near-certain. This strategic innovation demands a policy response, not just a technical one.

Edge-device compound risk: Three simultaneous critical CVEs (F5, Citrix, Fortinet) are all in the perimeter/VPN category — the entry point that enables every subsequent kill-chain stage. Organisations not patching all three this week face an elevated breach probability.

11. OSINT SOURCES CONSULTED

#	Source	URL
1	ITWeb SA — Cyber Threat Intelligence	https://www.itweb.co.za
2	UpGuard — Statistics South Africa Data Breach 2026	https://www.upguard.com/news/statistics-south-africa-da...
3	Breachsense — Statistics South Africa Data Breach	https://www.breachsense.com/breaches/statistics-south-a...
4	Pinsent Masons — SA Data Breach Incident Response	https://www.pinsentmasons.com/out-law/news/south-africa...
5	DeXpose.io — DragonForce Targets Singita	https://www.dexpose.io/dragonforce-targets-luxury-safar...
6	BlackFog — State of Ransomware March 2026	https://www.blackfog.com/the-state-of-ransomware-march-...
7	CM Alliance — Biggest Cyber Attacks March 2026	https://www.cm-alliance.com/cybersecurity-blog/biggest-...
8	DataBreaches.net — XP95 SA Government Victims	https://databreaches.net/2026/03/30/south-african-gover...
9	The Citizen — Stats SA Hit By Cyberattack	https://www.citizen.co.za/lifestyle/technology/stats-sa...
10	Daily Maverick — Gauteng Data Breach	https://www.dailymaverick.co.za/article/2026-03-17-gaut...
11	Ransomware.live — SA Victims Map	https://www.ransomware.live/map/ZA
12	CISA Known Exploited Vulnerabilities	https://www.cisa.gov/known-exploited-vulnerabilities-ca...
13	watchTowr — CVE-2026-3055 Advisory (Citrix NetScaler)	https://labs.watchtowr.com/advisory-citrix-netscaler-cv...
14	F5 Advisory K000156741 (CVE-2025-53521)	https://my.f5.com/manage/s/article/K000156741
15	Fortinet PSIRT — FortiClient EMS Advisories	https://www.fortiguard.com/psirt
16	Cisco Security Advisories (CVE-2026-20093)	https://sec.cloudapps.cisco.com/security/center/publica...
17	ITLawCo — Information Regulator 2026/27 APP	https://itlawco.com/information-regulator-2026-27-annua...
18	Priviso Live — Liberty Breach Briefing (29 March)	https://www.youtube.com/watch?v=2MHBC9GizZc
19	IOL — Sophos SA Ransomware Recovery Costs 2025	https://iol.co.za/business-report/economy/2025-07-04-ra...
20	iAfrica — IBM Cost of Breach SA 2025	https://iafrica.com/ai-helps-cut-south-africas-data-bre...
21	TechCentral — AG Report on SA Government Cyber Defences	https://techcentral.co.za/gaping-holes-in-south-african...
22	EWN — Liberty Data Breach (24 March 2026)	https://www.ewn.co.za/2026/03/24/data-breach-at-liberty...
23	ITWeb — Liberty Data Breach Article	https://www.itweb.co.za/article/insurer-liberty-hit-by-...
24	SABRIC — Annual Crime Statistics 2024	https://www.sabric.co.za/wp-content/uploads/2025/09/CRI...
25	MyBroadband — Virgin Active IDOR Vulnerability	https://mybroadband.co.za/news/security/635179-security...
26	GreyNoise — 2026 State of the Edge Report	https://www.greynoise.io/press/greynoise-releases-2026-...
27	LEX Africa — SA Cybersecurity Shift 2026	https://lexafrica.com/2026/02/south-africas-cybersecuri...
28	Bowmans — Data Protection Enforcement Trends	https://bowmanslaw.com/insights/south-africa-data-prote...

#	Source	URL
29	IOL — SIM Card Crackdown SA (27 March 2026)	https://iol.co.za/news/2026-03-27-sim-card-crackdown-so...
30	INTERPOL — 2026 Global Financial Fraud Assessment	https://www.interpol.int/en/News-and-Events/News/2026/I...
31	BleepingComputer — Citrix NetScaler Exploitation	https://www.bleepingcomputer.com/news/security/
32	ThreatFox (abuse.ch) — IOC Database	https://threatfox.abuse.ch/browse/
33	SSA CSIRT — SA Computer Security Incident Response	https://www.ssa.gov.za/CSIRT
34	SABRIC — SA Banking Risk Intelligence	https://www.sabric.co.za
35	IOL — Data Breach Frequency (March 2026)	https://iol.co.za/business-report/economy/2026-03-20-da...