SOUTH AFRICA
CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 13 | 16-22 March 2026

THREAT LEVEL: HIGH

Three new ransomware victims, Cisco FMC CVSS 10.0 zero-day exploited by Interlock, 9 CISA KEV entries, Gauteng XP95 root cause confirmed

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W13 | Classification: TLP:WHITE

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH — Sustained from the prior week. Three new ransomware victims (The Unlimited, Semenya Furumele, Elundini re-list), Cisco CVE-2026-20131 CVSS 10.0 now confirmed exploited by Interlock ransomware as zero-day since January 26, 9 new CISA KEV entries, Gauteng breach follow-up with XP95 root cause confirmed (unpatched scanner server, 70% of devices end-of-service), and SA banking fraud complaints nearly doubled YoY.[1]

KPI Dashboard

Metric	Current	Baseline	Change	Direction
SA org breach frequency	Every 3 hours	Every 5 hours (2025)	+40%	UP
Cyberattacks/week targeting SA	2,145/wk (Jan 2026)	1,575/wk (Jan 2025)	+36% YoY	UP
POPIA notifications (2024/25 FY)	2,374 (2024/25); ~2,500 proj.	1,500 (2023/24 est.)	+58%	UP
Avg SA breach cost	$2.37M / R49M	$2.78M (2024)	-15%	DOWN
SA ransomware victims tracked	94 total, 3 new this week	73 total same time 2025	+29%	UP
Digital banking fraud (NFO)	3,651 closed (2025), ~2x YoY	~1,900 (2024)	+92%	UP

ANOMALY FLAG: All metrics trending significantly above baseline except average breach cost. Breach frequency anomaly (every 3 hours vs. every 5 hours) is driven by identity-based attacks in approximately 90% of cases. Banking fraud complaints nearly doubled YoY.[2]

TOP 3 ACTIONS THIS WEEK

1. PATCH: Cisco FMC CVE-2026-20131 (CVSS 10.0) — exploited by Interlock ransomware since Jan 26. FCEB deadline PASSED. Treat unpatched as compromised. Patch Chrome to 146.0.7680.80+ (re-patched 16 March). Apply Oracle emergency patch CVE-2026-21992 (CVSS 9.8).

2. HUNT: Search for Interlock ransomware indicators on Cisco FMC environments. Hunt for MuddyWater CHAR backdoor IOCs (Telegram C2, Rust binary). Verify Quasar RAT .za.com C2 domains blocked (bkadbx.za.com, fqjbwh.za.com, vlitke.za.com).

3. COMPLY: POPIA monitoring exercise notices being issued — ensure Information Officer registered, PAIA manual current, incident response plan documented. R10M penalty for non-compliance. Information Regulator shifting from "education" to enforcement.

Key Findings:

- Gauteng Provincial Government breach (3.8 TB / XP95) — W13 follow-up confirmed root cause: unpatched internet-facing scanner server; 70% of network devices end-of-service.[3]
- The Unlimited listed by DragonForce ransomware on 20 March — same group that hit the National Credit Regulator in December 2025.[4]
- Semenya Furumele Consulting Engineers listed by Nightspire ransomware on 22 March — attack estimated 16 March.[5]
- Cisco CVE-2026-20131 (CVSS 10.0) confirmed exploited by Interlock ransomware as zero-day since 26 January 2026, over 5 weeks before public disclosure.[6]
- Nine new CISA KEV entries including 3 Apple DarkSword CVEs, Craft CMS (CVSS 10.0), and Laravel Livewire (MuddyWater).[7]
- SA banking fraud complaints at the National Financial Ombud nearly doubled YoY — 3,651 cases closed in 2025.[8]

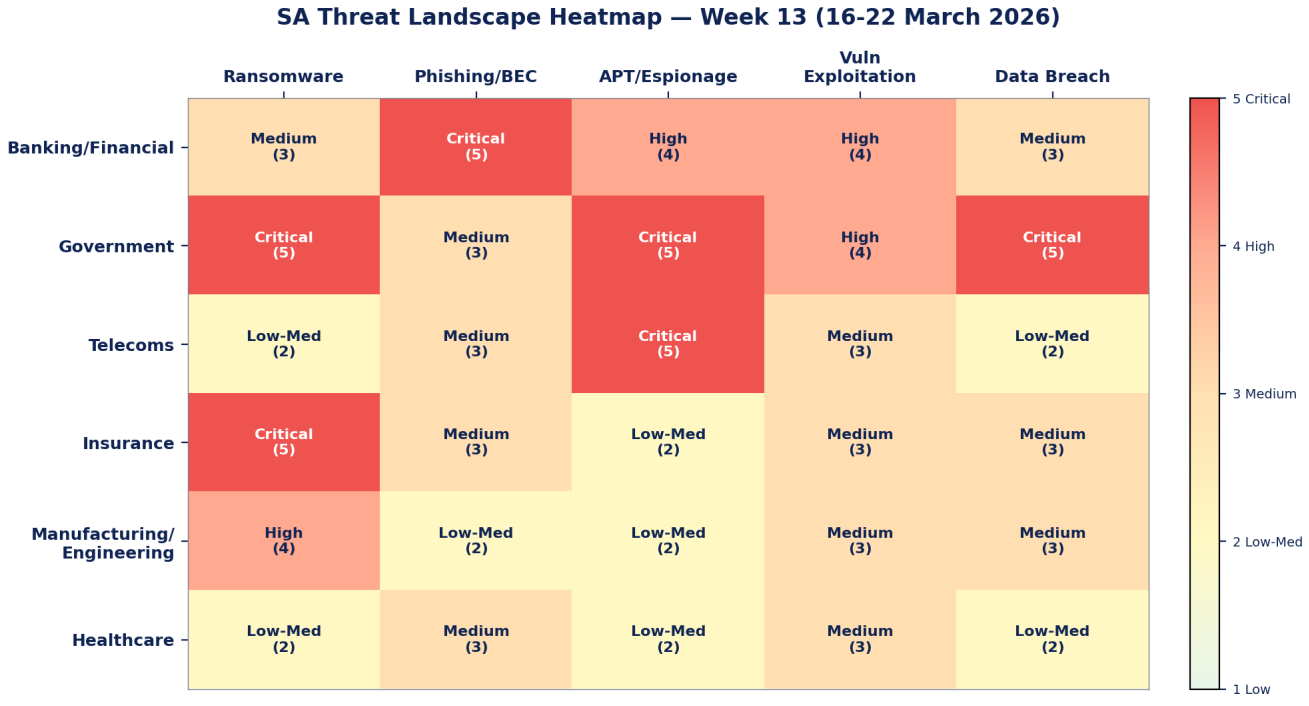
SECTOR SPOTLIGHT: INSURANCE (HIGH)

The insurance sector is this week's most at-risk sector. The Unlimited was listed by DragonForce ransomware on 20 March — the same group that hit the National Credit Regulator in December 2025.[4] Insurance companies are now in scope for POPIA Health Data Regulations (in force since 6 March 2026) AND FSCA Joint Standard 2/2024 (enforcement expected 2026).[9] The combination of active ransomware targeting + regulatory exposure creates compound risk. All SA insurers should verify DragonForce IOCs and conduct a gap analysis against new POPIA health data requirements.

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 — https://www.dailymaverick.co.za/article/2026-03-17-gauteng-was-lucky-with-latest-38tb-data-breach-but-the-luck-will-run-out/
4. Ransomware.live — DragonForce / The Unlimited — https://www.ransomware.live/id/dGhldW5saW1pdGVkLmNvLnphQGRyYWdvbmZvcmNl
5. Ransomware.live — Nightspire / Semenya Furumele — https://www.ransomware.live/id/U2VtZW55YSBGdXJ1bWVsZSBDb25zdWx0aW5nIEVuZ2luZWVyc0BuaWdodHNwaXJl
6. The Hacker News — Interlock exploiting Cisco FMC — https://thehackernews.com/2026/03/cisa-warns-of-zimbra-sharepoint-flaw.html
7. CISA KEV Catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
8. The Citizen — NFO fraud complaints double — https://www.citizen.co.za/business/fraud-complaints-at-the-banking-ombud-nearly-double-in-a-year-as-digital-scams-surge/
9. Moonstone — POPIA Health Data Regs — https://www.moonstone.co.za/new-popia-regulations-on-health-information-now-in-force/

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 13.



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

3. SA CYBER INCIDENTS & BREACHES

3.1 Gauteng Provincial Government — XP95 Data Breach (W13 Follow-up)

W13 Update: Daily Maverick analysis (17 March) confirmed the **3.8 TB** breach originated from an **internet-facing scanner server left unpatched**, not human error.[10] DA spokesperson Michael Waters issued a formal statement criticising systemic infrastructure neglect — **70% of Gauteng network devices (>1,734 units)** had reached end-of-service; core network infrastructure reached end-of-life in December 2024.[10] EngineerIT reported SA organisations are breached every three hours, with 90% preventable — citing the Gauteng breach as exemplary.[11] No ransom payment confirmed; no Information Regulator notification status confirmed in public reporting.

3.2 The Unlimited — DragonForce Ransomware (NEW)

DragonForce listed The Unlimited (theunlimited.co.za) on its leak site on **20 March 2026**.[4] The Unlimited offers health, auto, legal, and life insurance products. DragonForce is the same group that targeted the National Credit Regulator in December 2025 and Erwat in February 2024. No public statement from the organisation confirmed at time of research. Data exposure extent not yet disclosed.

3.3 Semenya Furumele Consulting Engineers — Nightspire Ransomware (NEW)

Nightspire listed Semenya Furumele Consulting Engineers (sfce.co.za) on **22 March 2026**, with an estimated attack date of 16 March.[5] Nightspire has previously claimed attacks on the Eastern Cape Department of Human Settlements (Nov 2025) and the Ingonyama Trust Board (Jun 2025). Data described as "not available now" — typical pre-negotiation posture.

3.4 Elundini Local Municipality — TheGentlemen Re-listing

TheGentlemen re-listed **Elundini Local Municipality** (elundini.gov.za) on **21 March 2026**.[12] The original attack dates to October 2025 and was first listed by LockBit5 in December 2025. Dual-listing indicates possible data re-selling or affiliate overlap between TheGentlemen and LockBit5. This is TheGentlemen's fifth SA victim in Q1 2026.

3.5 RE/MAX Southern Africa — Team Cyber Strike (Follow-up)

No new updates published during 16–22 March 2026.[13] Systems restored; full operations resumed as of 12 March 2026. Data-impact assessment ongoing. POPIA Section 22 notification filed.

3.6 Land Bank — Ransomware (Follow-up)

No new material developments during W13. Board-approved security improvement plan underway. Website remains down. CEO Themba Rikhotso resigned in February 2026.[14] The 5 BTC ransom demand was not paid.

3.7 SA Cybersecurity Statistics (W13 Publications)

- **ITWeb (20 March):** JSE-listed firms risk up to 30% share value loss after a cyberattack. SA organisations faced **2,145 cyberattacks/week** in Jan 2026 — 36% YoY increase.[1]
- **IOL (20 March):** SA organisations breached approximately every 3 hours; 90% deemed preventable; 60% rise in data breaches in H1 2025.[2]
- **Average SA breach cost:** $2.37M (down from $2.78M in 2024); SA orgs averaged 227 days to identify and

contain breaches (global avg: 258).[1]

10. Daily Maverick, 17 March 2026 — https://www.dailymaverick.co.za/article/2026-03-17-gauteng-was-lucky-with-latest-38tb-data-breach-but-the-luck-will-run-out/
11. EngineerIT, 18 March 2026 — https://www.engineerit.co.za/article/sa-organisations-are-breached-every-three-hours-90-could-be-prevented
12. Ransomware.live SA Map — https://www.ransomware.live/map/ZA
13. RE/MAX SA Incident Notice — https://www.remax.co.za/cyber-incident-notice
14. ITWeb, 9 March 2026 — Land Bank — https://www.itweb.co.za/article/land-bank-tightens-security-after-ransomware-attack/raYAyMorlOl7J38N

4. ACTIVE THREAT CAMPAIGNS

4.1 Salt Typhoon / RedMike (China) — SA Telco Still Compromised

Salt Typhoon (RedMike), attributed to China's Ministry of State Security, continues to compromise an unnamed **South African telecommunications provider** — one of only 7 globally confirmed compromised Cisco device networks.[15] The FBI stated the campaign is "still very much ongoing" as of February 2026.[16] The group targeted over 1,000 internet-facing Cisco network devices globally using CVE-2023-20198 and CVE-2023-20273. Key implants include **TernDoor**, **PeerTime**, and **BruteEntry**. GRE tunnels are used for persistent access and data exfiltration.

MITRE ATT&CK TTPs: T1190 (Exploit Public-Facing App), T1098 (Account Manipulation), T1572 (Protocol Tunneling), T1078.001 (Valid Accounts: Default), T1005 (Data from Local System)

4.2 MuddyWater — Operation Olalampo (Iran / MOIS)

Iran's MuddyWater (MOIS) deployed 4 new malware families in **Operation Olalampo** (activated 2 March 2026): **CHAR** (Rust-based backdoor using Telegram bots for C2), **GhostBackDoor**, **GhostFetch**, and **HTTP_VIP**.[17] C2 infrastructure was confirmed live on 16 March 2026, including IP **196.251.72.192** in the SA IP range. Historical targeting of financial institutions creates indirect risk for SA financial sector. Laravel Livewire CVE-2025-54068 (CVSS 9.8) is being exploited by MuddyWater targeting diplomatic, energy, and finance sectors.

MITRE ATT&CK TTPs: T1102 (Web Service — Telegram C2), T1059.007 (JavaScript), T1567 (Exfiltration to Cloud), T1566.001 (Spear-Phishing Attachment)

4.3 Void Manticore / Handala (Iran) — Stryker Corp 200K Systems Wiped

Iran's Void Manticore (MOIS) wiped **200,000+ systems** at US medical-tech giant Stryker Corporation on 11 March 2026 via Microsoft Intune MDM hijack — 50 TB exfiltrated; SEC 8-K filing confirmed.[18] FBI seized Handala websites during the week of 17-22 March. Stryker has significant SA healthcare market operations. The wiper tooling and MDM hijack technique (no malware binary deployed — uses legitimate management tools) is applicable against SA enterprise environments.

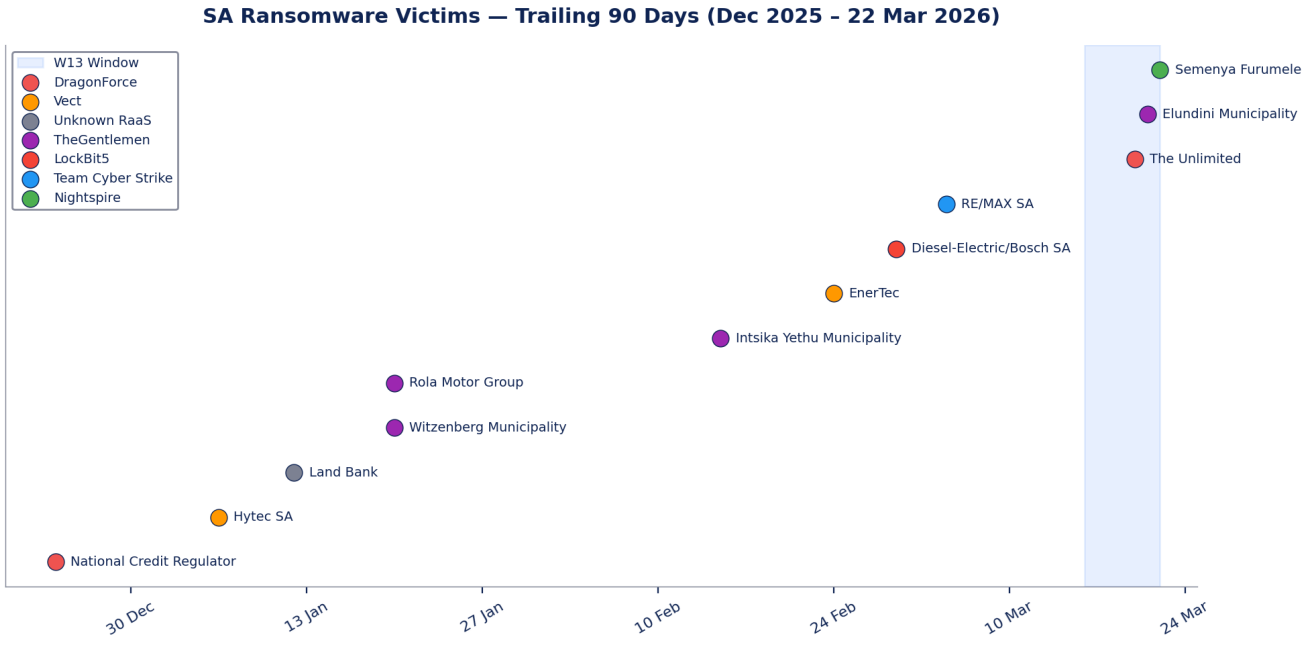
4.4 Interlock Ransomware — Exploiting Cisco FMC as Zero-Day

Amazon security research confirmed that the **Interlock ransomware group** has been exploiting **CVE-2026-20131** (Cisco FMC, CVSS 10.0) as a zero-day since **26 January 2026** — over 5 weeks before public disclosure on 4 March 2026.[6] Interlock targets education, healthcare, government, manufacturing, and infrastructure sectors. CISA added CVE-2026-20131 to KEV on 19 March with a 3-day patch deadline (22 March — now passed). All on-premise FMC deployments should be treated as potentially compromised if not yet patched.

15. TechCrunch — Salt Typhoon, 9 March 2026 — https://techcrunch.com/2026/03/09/salt-typhoon-china-who-has-been-hacked-global-telecom-giants/
16. CyberScoop — FBI: Salt Typhoon ongoing — https://cyberscoop.com/fbi-salt-typhoon-ongoing-threat-cybertalks-2026/

17. Red Piranha Threat Intelligence, March 2026 — https://redpiranha.net/news/threat-intelligence-report-march-10-march-16-2026
18. S-RM Cyber Intelligence Briefing, 20 March 2026 — https://www.s-rminform.com/en-us/cyber-intelligence-briefing/hackers-steal-one-million-gigabytes-of-data-cyber-intelligence-briefing-march-20-2026

5. RANSOMWARE ACTIVITY



South Africa recorded **94 total ransomware victims** tracked to date, with **3 new victims** in Week 13.[12] The ransomware landscape is dominated by **TheGentlemen** (5 SA victims Q1, including re-lists), **DragonForce** (2 SA victims since Dec 2025), and **Nightspire** (3 SA victims since Jun 2025). Active groups also include LockBit5, Qilin, INC Ransom, and Akira. A new MedusaLocker variant, **Zollo** (.zollo6 extension), was identified this week.[19]

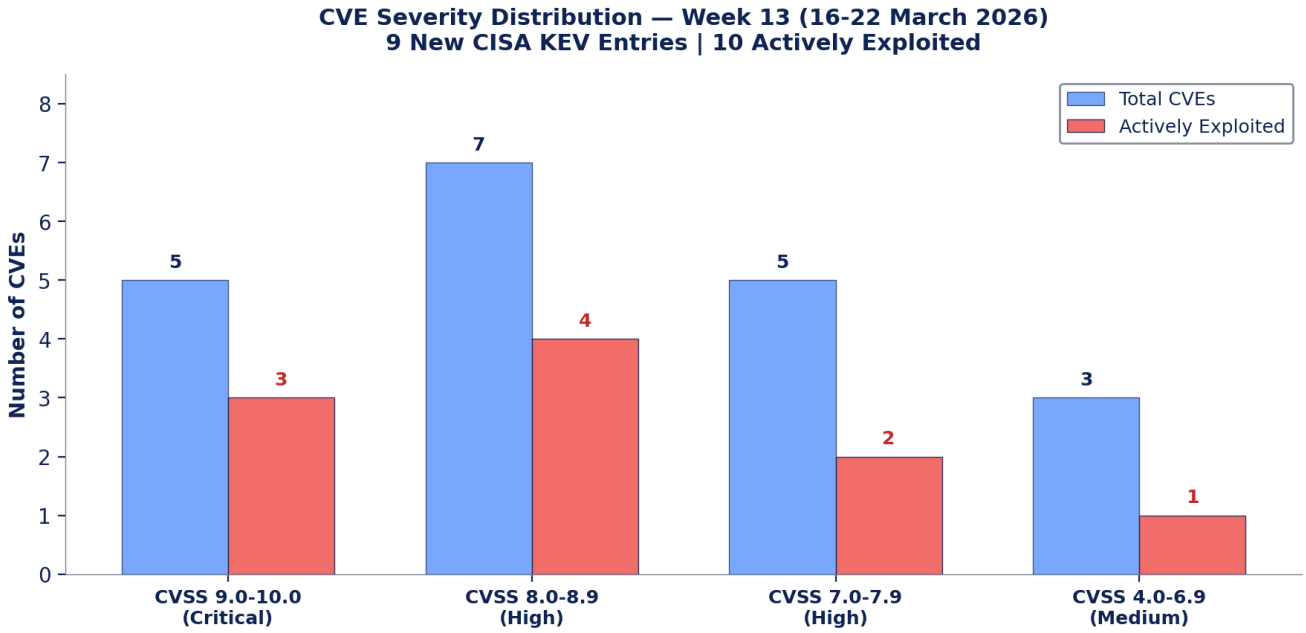
SA Ransomware Victims — Q1 2026

Date	Organisation	Sector	Group
24 Dec 2025	National Credit Regulator	Financial Reg	DragonForce
6 Jan	Hytec SA	Engineering	Vect
12 Jan	Land Bank	Financial	Unknown RaaS
20 Jan	Witzenberg Municipality	Government	TheGentlemen
20 Jan	Rola Motor Group	Automotive	TheGentlemen
15 Feb	Intsika Yethu Municipality	Government	TheGentlemen
24 Feb	EnerTec	Manufacturing	Vect
1 Mar	Diesel-Electric / Bosch SA	Automotive	LockBit5
5 Mar	RE/MAX SA	Real Estate	Team Cyber Strike
20 Mar	The Unlimited	Insurance	DragonForce
21 Mar	Elundini Municipality (re-list)	Government	TheGentlemen
22 Mar	Semenya Furumele	Engineering	Nightspire

Global Context: In W13, Qilin and LockBit5 each accounted for 13.75% of global ransomware hits, Akira 7.92%, Nightspire 6.67%, and TheGentlemen 6.25%.[17] Publicly disclosed ransomware increased 49% YoY in 2025 with 7,079 victims on leak sites — and 86% of all ransomware attacks are never publicly reported.

19. CYFIRMA Weekly Intelligence Report, 20 March 2026 — https://www.cyfirma.com/news/weekly-intelligence-report-20-march-2026/

6. CRITICAL VULNERABILITIES



This week saw **9 new CISA KEV entries**, including Cisco FMC CVSS 10.0 (exploited by Interlock since Jan 26), Craft CMS CVSS 10.0 (exploited since Feb 2025), and Oracle CVE-2026-21992 CVSS 9.8 (emergency out-of-band patch).[6] Chrome CVE-2026-3909 was re-patched on 16 March after the initial fix was found incomplete.[20]

Priority Vulnerability Matrix

CVE ID	Vendor/Product	CVSS	Exploited	Patch
CVE-2026-20131	Cisco Secure FMC + SCC	10.0	YES (Interlock)	Yes
CVE-2025-32432	Craft CMS	10.0	YES (Mimo)	Yes
CVE-2026-21992	Oracle Identity Manager	9.8	Not yet	Yes (OOB)
CVE-2025-54068	Laravel Livewire	9.8	YES (MuddyWater)	Yes
CVE-2026-24858	Fortinet FortiOS SSO	9.4	YES (ongoing)	Yes
CVE-2026-20079	Cisco Secure FMC	10.0	Not yet	Yes
CVE-2026-3909	Chrome / Skia	8.8	YES (re-patched)	Yes
CVE-2026-3910	Chrome / V8	8.8	YES (KEV)	Yes
CVE-2026-20963	MS SharePoint	8.8	YES (KEV)	Yes
CVE-2025-43520	Apple (DarkSword)	8.8	YES (KEV)	Yes
CVE-2025-31277	Apple Safari/iOS	8.8	YES (KEV)	Yes
CVE-2025-66376	Zimbra ZCS	7.2	YES (GhostMail)	Yes
CVE-2025-43510	Apple watchOS/iOS	7.8	YES (KEV)	Yes
CVE-2025-47813	Wing FTP Server	4.3	YES (KEV)	Yes

20. Malwarebytes — Chrome Zero-Days re-patched — https://www.malwarebytes.com/blog/news/2026/03/google-patches-two-chrome-zero-days-under-active-attack-update-now
21. Oracle Security Alert — CVE-2026-21992 — https://www.oracle.com/security-alerts/alert-cve-2026-21992.html

22. Arctic Wolf — Cisco FMC CVE-2026-20079/20131 — https://arcticwolf.com/resources/blog/cve-2026-20079-cve-2026-20131/

7. PHISHING & SOCIAL ENGINEERING

7.1 Standard Bank AI Spoofing Scams

An active AI-enhanced spoofing campaign targeted Standard Bank customers during W13. Fraudsters call victims posing as bank employees, using spoofed caller IDs and AI-generated voices, claiming to "upgrade" accounts. Victims are tricked into entering codes granting attacker access — multiple accounts drained, with one reported victim losing over **R600,000**.[23] Standard Bank deployed "Trusted Person" and "Trust Call" counter-measures.

7.2 R22M BEC Loss via WhatsApp CFO Impersonation

A South African company lost **R22 million** to a WhatsApp-based BEC attack where the attacker "perfectly" replicated the CFO's communication style.[24] This incident demonstrates the escalation from email-only BEC to multi-channel social engineering via messaging apps — SMS accounts for 66% and messaging apps 32% of BEC attack channels in 2025.

7.3 NFC Card-Relay Scam (SA-Specific)

ESET flagged an NFC card-relay attack particularly prevalent in South Africa. Fraudsters call victims posing as bank representatives, send a link to install a rogue app that reads the victim's physical card NFC chip, relaying data in real-time for ATM/POS use. Victims are asked to enter their PIN, believing they are verifying with the bank.[25]

7.4 NFO Fraud Complaints Nearly Doubled YoY

The National Financial Ombud closed **3,651 fraud-related cases** in 2025, with complaints nearly doubling YoY. Top categories: mobile banking fraud, phishing, vishing, push payment scams, card-not-present fraud, smishing, and smart device fraud.[8] Separately, Nedbank issued a deepfake investment scam alert involving AI-generated video advertisements.[26] ESET reports **phishing accounts for 46% of all SA cyber threats**.[25]

23. IOL — Standard Bank spoofing scams, 21 March 2026 — https://iol.co.za/news/2026-03-21-standard-bank-under-fire-customers-claim-data-exposure-led-to-scams/
24. LinkedIn — R22M WhatsApp BEC, 19 March 2026 — https://www.linkedin.com/posts/expert-advisory-consulting_cybersecurity-riskmanagement-businessstrategy-activity-7440223049829826560-pp0p
25. ESET / SABC — NFC card-relay and phishing stats — https://www.youtube.com/watch?v=qp7ExolLqZ0
26. IOL — Nedbank deepfake investment scam — https://iol.co.za/business-report/opinion/2026-02-01-nedbanks-deepfake-investment-scam-alert-is-just-the-start/

8. REGULATORY & COMPLIANCE

8.1 POPIA Enforcement Proceedings

Three enforcement actions confirmed during the period:[27]

- **Blouberg Municipality:** R500,000 fine — unlawful publication of financial disclosures; court proceedings initiated under section 109.
- **Lancet Laboratories:** R200,000 fine — failed to notify data subjects of security breaches (section 22 POPIA). Paid.
- **FT RAMS Consulting:** R200,000 fine — unlawful direct marketing. Court proceedings initiated.

8.2 POPIA Monitoring Exercise — Formal Notices Being Issued

The Information Regulator is issuing formal notices to selected organisations under section 40(1)(b)(i) requiring comprehensive POPIA compliance reports within **14 business days**.[28] Reports must cover lawful processing conditions, direct marketing, cross-border transfers, privacy policy, risk register, incident response plan, PAIA manual, training records, and security compromise log. Post-submission physical inspections are possible. Non-compliance escalates to Chapter 10 enforcement (**fines up to R10 million, civil liability, imprisonment**).

8.3 POPIA Health Data Regulations — In Force (No Grace Period)

Health information processing regulations came into force **6 March 2026 with no grace period** (Government Gazette No. 54268).[9] Eight categories of organisations in scope: insurance companies, medical schemes, administrators, managed healthcare organisations, pension funds, employers, and institutions acting on their behalf. The final regulations were simplified from the September 2025 draft — no dual-authorisation requirement, no mandatory LIAs, no mandatory written data subject agreements.

8.4 Information Regulator: "Education First" Era Ending

The Regulator outlined 2026 priorities: intensified investigations in high-risk sectors, targeted sectoral assessments, a "name and shame" approach, and the end of the "education first" leniency posture. Only **14% of SA companies** (~69,040 of ~490,000) have registered an Information Officer.[29] The Regulator is drafting POPIA amendments moving toward direct financial penalties for intentional non-compliance.

8.5 Cybercrimes Act: First Sustained Conviction Pattern

Three Western Cape convictions and two raids in February–March 2026 for digital piracy under sections 3(1), 4(2), and cyber fraud. Sentences ranged from 5-year to 8-year suspended terms with correctional supervision.[30] This represents the first sustained pattern of Cybercrimes Act convictions — signalling active enforcement capability.

8.6 FSCA Annual Industry Conference (18-19 March)

The FSCA held its Annual Industry Conference on 18-19 March 2026 with **AI governance** as a central theme. FSCA Joint Standard 2/2024 (effective June 2025) requires board-approved cybersecurity strategy, annual penetration testing, MFA, and 24-hour material incident reporting. Full enforcement expected in 2026.

Compliance Deadlines Summary

Deadline	Obligation	Regulator
Immediate (6 Mar 2026)	Health information processing safeguards	Information Regulator
Active (14 biz days)	POPIA monitoring exercise response	Information Regulator
Active (past due)	NPS cybersecurity compliance	SARB
Active (from Jun 2025)	Financial institution cybersecurity	FSCA / PA
2026 (enforcement)	Joint Standard 2/2024 compliance	FSCA

27. Bowmans — Data Protection Enforcement Trends, 17 March 2026 — https://bowmanslaw.com/insights/south-africa-data-protection-recent-developments-and-enforcement-trends/
28. Bowmans — POPIA Monitoring Exercise, 4 March 2026 — https://bowmanslaw.com/insights/south-africa-information-regulator-launches-popia-monitoring-exercise/
29. Mayet Law — POPIA Enforcement 2026, 20 March 2026 — https://mayet.law/popia-enforcement-in-south-africa-key-2026-developments-and-what-businesses-must-do-now/
30. TechCentral — Illegal streaming crackdown, 12 March 2026 — https://techcentral.co.za/illegal-streaming-crackdown-nets-arrests-convictions-in-cape-town/278890/

9. OSINT EXPOSURE

9.1 Gauteng Data on Dark Web

The Gauteng Provincial Government dataset (3.8 TB / 3,673,556 files) remains listed on a dark web forum and Telegram channel by XP95 for $25,000.[3] Contents include high-resolution copies of ID documents, passports, and CVs (likely from government job applicants). A 1.8 GB sample was dumped publicly as proof. The data creates industrialised risk of identity theft via National ID numbers, SARS eFiling fraud, and retail credit fraud.

9.2 Quasar RAT on .za.com Domains

Three **.za.com** domains were reported as Quasar RAT command-and-control infrastructure on ThreatFox (abuse.ch) on 22 March 2026:[31]

- bkadbx.za.com
- fqjbwh.za.com
- vlitke.za.com

Note: .za.com is a second-level domain hosted internationally (not co.za). These are likely attacker-registered domains using the "za" string. Defenders should block outbound DNS/TCP to these domains.

9.3 MuddyWater Infrastructure in SA IP Range

IP **196.251.72.192** appears in the Red Piranha consolidated IOC list under MuddyWater/Tsundere historical IPs. The 196.x.x.x range is a South African IP block. This may represent SA-based hosting used by threat actors rather than a SA-operated C2. Monitor outbound connections to this IP.[17]

9.4 HIBP Status

No new SA-specific organisations were added to the HIBP database during March 16-22, 2026. The Land Bank and Gauteng incidents are active but have not yet appeared in HIBP.

31. ThreatFox (abuse.ch) — https://threatfox.abuse.ch/browse/

10. WEEKLY THREAT HUNT & IOCs

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

10a. Hunt Missions

TH-2026-W13-01: Interlock Ransomware via Cisco FMC Exploitation — **P1 — CRITICAL**

Hypothesis: Interlock has been exploiting CVE-2026-20131 (CVSS 10.0) since Jan 26. Hunt for Java deserialization artefacts on FMC/SCC, anomalous root-level processes, unexpected outbound connections from FMC management interfaces.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1059.004 (Unix Shell)

IOCs: CVE-2026-20131 exploitation artefacts on Cisco FMC

Data Sources: FMC logs, EDR, Sysmon, firewall logs

TH-2026-W13-02: DragonForce / SA Insurance Sector — **P1 — CRITICAL**

Hypothesis: DragonForce listed The Unlimited (insurance) on 20 March. Hunt for Mimikatz credential dumping, lateral movement via RDP, DragonForce encryption markers in SA insurance environments.

MITRE ATT&CK: T1078 (Valid Accounts), T1003.001 (LSASS Memory), T1486 (Data Encrypted for Impact)

IOCs: IP 45.135.232.195 (DragonForce-linked)

Data Sources: EDR, Windows Event Logs, RDP logs

TH-2026-W13-03: MuddyWater CHAR Backdoor via Telegram C2 — **P2 — HIGH**

Hypothesis: Hunt for Rust-compiled binaries communicating with Telegram API endpoints, outbound connections to known MuddyWater infrastructure. CHAR backdoor uses Telegram bots for C2.

MITRE ATT&CK: T1102 (Web Service), T1059.007 (JavaScript), T1071.001 (Web Protocols)

IOCs: 185.236.25.119, 193.17.183.126, 194.11.246.101, 196.251.72.192 (SA range); domains: apro24docs.com, aproenvoid.com, worthscale.eu.com

Data Sources: Proxy, DNS, EDR, email gateway

TH-2026-W13-04: Quasar RAT C2 on .za.com Domains — **P2 — HIGH**

Hypothesis: Hunt for outbound DNS/TCP to .za.com domains associated with Quasar RAT, process injection behaviours consistent with Quasar RAT.

MITRE ATT&CK: T1071.001 (Application Layer Protocol), T1055 (Process Injection)

IOCs: bkadbx.za.com, fqjbwh.za.com, vlitke.za.com

Data Sources: DNS logs, proxy, EDR

TH-2026-W13-05: Chrome Zero-Day Exploit Chain (Skia + V8) — **P2 — HIGH**

Hypothesis: Verify Chrome 146.0.7680.80+ deployed across all endpoints. Hunt for anomalous renderer process behaviour indicating Skia OOB write or V8 exploitation.

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

IOCs: CVE-2026-3909/3910 — Chrome versions below 146.0.7680.80

Data Sources: EDR, browser version inventory

TH-2026-W13-06: Operation GhostMail — Zimbra Zero-Click XSS — **P3 — MEDIUM**

Hypothesis: Hunt for embedded JavaScript in email HTML bodies targeting Zimbra Classic UI. Anomalous DNS exfiltration from Zimbra servers. Zero-click exploitation — merely opening email triggers credential harvesting.

MITRE ATT&CK: T1189 (Drive-by Compromise), T1048 (Exfiltration Over Alternative Protocol)

IOCs: CVE-2025-66376 — Zimbra ZCS Classic UI

Data Sources: Email gateway, DNS logs, Zimbra access logs

10b. Hunt Checklist

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

Hunt ID	Hypothesis (short)	Priority	Data Sources	Status
TH-2026-W13-01	Interlock/Cisco FMC exploitation	P1	FMC, EDR, Sysmon, FW	Not Started
TH-2026-W13-02	DragonForce/SA insurance	P1	EDR, WinEvt, RDP	Not Started
TH-2026-W13-03	MuddyWater CHAR/Telegram C2	P2	Proxy, DNS, EDR, email	Not Started
TH-2026-W13-04	Quasar RAT .za.com C2	P2	DNS, proxy, EDR	Not Started
TH-2026-W13-05	Chrome zero-day deployment check	P2	EDR, browser inventory	Not Started

Hunt ID	Hypothesis (short)	Priority	Data Sources	Status
TH-2026-W13-06	GhostMail Zimbra zero-click	P3	Email GW, DNS, Zimbra	Not Started

10c. IOC Master Table

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

Indicator	Type	Attribution	Hunt ID
185.236.25.119	IPv4	MuddyWater C2	TH-W13-03
193.17.183.126	IPv4	MuddyWater C2	TH-W13-03
194.11.246.101	IPv4	MuddyWater C2	TH-W13-03
194.11.246.78	IPv4	MuddyWater C2	TH-W13-03
89.40.31.242	IPv4	MuddyWater C2	TH-W13-03
196.251.72.192	IPv4	MuddyWater (SA range)	TH-W13-03
185.178.208.137	IPv4	Void Manticore	N/A
31.192.237.207	IPv4	Void Manticore	N/A
146.185.219.235	IPv4	Void Manticore	N/A
45.135.232.195	IPv4	DragonForce	TH-W13-02
apro24docs.com	Domain	MuddyWater C2	TH-W13-03
aproenvoid.com	Domain	MuddyWater C2	TH-W13-03
worthscale.eu.com	Domain	MuddyWater C2	TH-W13-03
iaresult.us.com	Domain	MuddyWater C2	TH-W13-03
pushbeacon.org	Domain	MuddyWater C2	TH-W13-03
notifyblast.org	Domain	MuddyWater C2	TH-W13-03
bkadbx.za.com	Domain	Quasar RAT C2	TH-W13-04
fqjbwh.za.com	Domain	Quasar RAT C2	TH-W13-04
vlitke.za.com	Domain	Quasar RAT C2	TH-W13-04
cloudpub[.]ru	Domain	Raton RAT C2	N/A
www.dest-working.com	Domain	Camaro Dragon	N/A
202.59.10.106	IPv4	Camaro Dragon	N/A
login[.]citrixtv[.]com	Domain	Salt Typhoon	N/A
login[.]vmwaretv[.]com	Domain	Salt Typhoon	N/A
update[.]vmwaretv[.]com	Domain	Salt Typhoon	N/A
b15562c0771ce...362820	SHA256	Raton RAT	N/A
25b442da4774...abdab37	SHA256	Raton RAT	N/A
f5ef4a45e19d...eb9061	SHA256	MuddyViper	TH-W13-03
d5b7a5ae4156...9864c3	SHA256	MuddyViper	TH-W13-03
960e06362417...9bd0	SHA256	Camaro Dragon	N/A
*.zollo6	File Ext	Zollo Ransomware	N/A
READ_NOTE.html	Filename	Zollo Ransomware	N/A
cloud-noc@mail.io	Email	Fortinet CVE-24858	N/A
cloud-init@mail.io	Email	Fortinet CVE-24858	N/A

11. RECOMMENDATIONS

IMMEDIATE (This Week)

▪ **PATCH:** Upgrade Cisco FMC to latest fixed release — CVE-2026-20131 actively exploited by Interlock. Treat unpatched as compromised. Update Chrome to 146.0.7680.80+ (re-patched 16 March). Apply Oracle CVE-2026-21992 emergency patch. Deploy Microsoft March 2026 Patch Tuesday.

▪ **BLOCK:** Add all MuddyWater C2 IPs and domains from Section 10c to blocklists. Block Quasar RAT .za.com domains. Block DragonForce-linked IP 45.135.232.195.

▪ **HUNT:** Execute P1 hunt missions TH-W13-01 and TH-W13-02. Prioritise Interlock/Cisco FMC indicators and DragonForce indicators in insurance environments.

▪ **COMPLY:** If you receive a POPIA monitoring exercise notice, begin documentation assembly immediately (14 business day deadline). Ensure Information Officer is registered.

▪ **MONITOR:** Watch for DragonForce ransomware indicators in insurance sector. Verify Zimbra ZCS patched to 10.0.18+ (Operation GhostMail zero-click).

SHORT-TERM (This Quarter)

▪ Audit Information Officer registration status — 86% of SA companies non-compliant. Registration is a prerequisite to responding to monitoring exercise notices.

▪ Conduct a POPIA Health Data gap analysis for insurance companies, medical schemes, pension funds, and employers processing health information (Sec 8).

▪ Execute Salt Typhoon threat hunt on all Cisco IOS-XE routers — SA telco still compromised, FBI confirms "still ongoing" (Sec 4).

▪ Implement anti-phishing measures for AI-generated voice spoofing and NFC card-relay attacks — both SA-specific patterns (Sec 7).

▪ Review BEC detection rules for multi-channel attacks (WhatsApp CFO impersonation, SMS-based BEC). R22M loss in single incident (Sec 7).

▪ Verify all Apple devices on latest iOS/macOS to mitigate DarkSword exploit kit (3 KEV CVEs).

STRATEGIC (Next 6-12 Months)

▪ Prepare for POPIA amendment legislation moving toward direct financial penalties for intentional non-compliance (Sec 8).

▪ Deploy AI-powered threat detection and deepfake detection — banking fraud complaints nearly doubled YoY; AI spoofing scams escalating (Sec 7).

▪ Implement dark web monitoring as standard practice — Gauteng data selling for $25,000 illustrates the scale of exposure (Sec 9).

▪ Align cybersecurity programme with FSCA Joint Standard 2/2024 requirements — board-approved strategy, annual pentesting, MFA, 24-hour reporting (Sec 8).

▪ Address identity security as priority — 90% of SA breaches involve identity-based attacks; breach frequency at every 3 hours (Sec 1).

▪ Invest in government sector resilience — sustained multi-vector pressure from criminal and state-sponsored actors (Secs 2-4).

▪ Build incident response readiness — only 43% of SA organisations can restore in 24 hours (Sec 3).

12. OSINT SOURCES CONSULTED

#	Source	URL
1	Ransomware.live — SA Victims Map	https://www.ransomware.live/map/ZA
2	CISA KEV Catalog	https://www.cisa.gov/known-exploited-vulnerabilities-catalog
3	CYFIRMA Weekly Intel Report, 20 March 2026	https://www.cyfirma.com/news/weekly-intelligence-report-20-m...
4	Daily Maverick, 17 March 2026	https://www.dailymaverick.co.za/article/2026-03-17-gauteng-w...
5	The Citizen — Gauteng breach, 14 March 2026	https://www.citizen.co.za/news/panyaza-lesufi-responds-gaute...
6	ITWeb — Listed firms risk share plunge, 20 March 2026	https://www.itweb.co.za/article/listed-firms-risk-30-share-p...
7	IOL — Data breaches every 3 hours, 20 March 2026	https://iol.co.za/business-report/economy/2026-03-20-data-br...
8	EngineerIT, 18 March 2026	https://www.engineerit.co.za/article/sa-organisations-are-br...
9	RE/MAX SA Incident Notice	https://www.remax.co.za/cyber-incident-notice
10	ITWeb — Land Bank ransomware, 9 March 2026	https://www.itweb.co.za/article/land-bank-tightens-security-...
11	TechCrunch — Salt Typhoon, 9 March 2026	https://techcrunch.com/2026/03/09/salt-typhoon-china-who-has...
12	CyberScoop — FBI: Salt Typhoon ongoing	https://cyberscoop.com/fbi-salt-typhoon-ongoing-threat-cyber...
13	Red Piranha Threat Intelligence, March 2026	https://redpiranha.net/news/threat-intelligence-report-march...
14	S-RM Cyber Intelligence Briefing, 20 March 2026	https://www.s-rminform.com/en-us/cyber-intelligence-briefing...
15	The Hacker News — Cisco/SharePoint/Zimbra KEV	https://thehackernews.com/2026/03/cisa-warns-of-zimbra-share...
16	The Hacker News — Apple/Craft CMS/Laravel KEV	https://thehackernews.com/2026/03/cisa-flags-apple-craft-cms...
17	Malwarebytes — Chrome Zero-Days	https://www.malwarebytes.com/blog/news/2026/03/google-patche...
18	Oracle Security Alert — CVE-2026-21992	https://www.oracle.com/security-alerts/alert-cve-2026-21992....
19	Arctic Wolf — Cisco FMC CVEs	https://arcticwolf.com/resources/blog/cve-2026-20079-cve-202...
20	IOL — Standard Bank spoofing scams, 21 March 2026	https://iol.co.za/news/2026-03-21-standard-bank-under-fire-c...
21	The Citizen — NFO fraud complaints double	https://www.citizen.co.za/business/fraud-complaints-at-the-b...
22	Bowmans — Enforcement Trends, 17 March 2026	https://bowmanslaw.com/insights/south-africa-data-protection...
23	Bowmans — POPIA Monitoring Exercise	https://bowmanslaw.com/insights/south-africa-information-reg...
24	Moonstone — POPIA Health Regs	https://www.moonstone.co.za/new-popia-regulations-on-health-...
25	Mayet Law — POPIA Enforcement 2026	https://mayet.law/popia-enforcement-in-south-africa-key-2026...
26	ThreatFox (abuse.ch)	https://threatfox.abuse.ch/browse/
27	Recorded Future — RedMike/Salt Typhoon	https://www.recordedfuture.com/research/redmike-salt-typhoon...
28	RedPacket Security — Semenya Furumele / Nightspire	https://www.redpacketsecurity.com/nightspire-ransomware-vict...
29	RedPacket Security — The Unlimited / DragonForce	https://www.redpacketsecurity.com/dragonforce-ransomware-vic...
30	TechCentral — Piracy convictions, 12 March 2026	https://techcentral.co.za/illegal-streaming-crackdown-nets-a...
31	LinkedIn — R22M WhatsApp BEC	https://www.linkedin.com/posts/expert-advisory-consulting_cy...
32	ESET / SABC — NFC card-relay and phishing stats	https://www.youtube.com/watch?v=qp7ExolLqZ0
33	Fortinet PSIRT Advisories	https://www.fortiguard.com/psirt
34	SA CSIRT (State Security Agency)	https://www.ssa.gov.za/CSIRT
35	Cisco FMC Advisory	https://sec.cloudapps.cisco.com/security/center/content/Cisc...
36	SABRIC	https://www.sabric.co.za
37	Nova News — SA top African cyber target	https://novanews.co.za/south-africa-becomes-africas-top-cybe...