



SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 20 | 3 May – 10 May 2026

THREAT LEVEL: HIGH

Standard Bank Group formally indexed on ransomware.live by PrinzEugen (ROOTBOY) on 4 May -- SA tally moves 107 to 108. City of Ekurhuleni R2 billion billing fraud disclosed at SCOPA 6 May (2023-24 Wi-Fi intrusion into billing/licensing systems). ShinyHunters Canvas/Instructure 12 May leak deadline directly impacts 5 SA institutions: Wits, Stadio, Milpark, Invictus, SPARK Schools. 4 new CISA KEV entries: PAN-OS (deadline 9 May), Ivanti EPMM (10 May), LiteLLM (11 May), Linux Kernel (15 May). Defender RedSun + UnDefend STILL UNPATCHED -- Patch Tuesday 12 May expected. APT28 SAMA financial-sector expansion flagged 7 May.

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W20 | 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: APT28 & Glowworm / APT41**
- 5. Active Threat Campaigns**
- 6. Critical Vulnerabilities & CISA KEV**
- 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 (unchanged from W19) — Week 20 (3–10 May 2026) delivered one new SA ransomware-tracker listing, a major new SCOPA disclosure, and escalating deadline pressure across multiple threat vectors. On **4 May**, Standard Bank Group was formally indexed on ransomware.live by **PrinzEugen (ROOTBOY)**, taking the SA cumulative tally from 107 to **108**. On **6 May**, the City of Ekurhuleni disclosed a **R2 billion billing fraud** at a Parliamentary SCOPA hearing — a Wi-Fi-enabled intrusion into licensing and billing systems spanning 2023–24. ShinyHunters set a **12 May leak deadline** for the Canvas/Instructure 275M-record dump, directly exposing five SA tertiary institutions: **Wits, Stadio, Milpark, Invictus, and SPARK Schools**. Four new CISA KEV additions hit in the window, with PAN-OS CVE-2026-0300 (state-sponsored since 16 April) topping the urgency list with a 9 May deadline. Microsoft Defender zero-days **RedSun and UnDefend remain unpatched**; Patch Tuesday 12 May is expected to address them. APT28 SAMA financial-sector expansion flagged by Fyntralink on 7 May broadens the nation-state watch horizon for SA banks.¹

KPI Dashboard

Metric	Current (W20)	Baseline / Prior	Change	Direction
SA threat level	HIGH	HIGH (W19)	Unchanged	FLAT
New SA ransomware.live victims (this week)	1 (Standard Bank/PrinzEugen)	1 (CGCSA/Stormous W19)	+1	UP
Cumulative SA ransomware.live victims	108	107	+1 net	UP
New CISA KEV entries (W20 scope)	4	2 (W19)	+4	UP
Active SA breach investigations	5	5	Unchanged	FLAT
Polmed scope (confirmed W20)	1.7M records / 68K SAPS officers / 214 GB	Prior: 100K+	Expanded	UP
SA avg recovery cost (excl. ransom)	R24M (Sophos 2025)	R24M	Unchanged	FLAT
SA POPIA breach notifications/month	~284/month (IR W20 data)	Q1 2026: 788 total	Elevated	UP
SA-relevant unpatched zero-days	2 (RedSun, UnDefend)	2 (W19)	Unchanged	FLAT
Canvas/Instructure leak deadline (SA)	12 May (5 SA institutions)	N/A	NEW W20	UP
Ekurhuleni R2bn SCOPA disclosure	6 May 2026 (NEW)	N/A	NEW W20	UP

W20 KEY FRAMING: Three compounding deadlines converge on 12 May: Microsoft Patch Tuesday (expected to patch RedSun/UnDefend), ShinyHunters Canvas leak deadline (5 SA institutions), and CISA KEV deadlines for ConnectWise ScreenConnect and Windows Shell NTLM. The Ekurhuleni SCOPA disclosure (6 May) is the first confirmed multi-year Wi-Fi-enabled municipal billing fraud at this scale in SA — a new threat model for the public sector. Standard Bank formal indexing (4 May) is a regulatory escalation signal: the IR now has ransomware.live as public evidence of the ROOTBOY operation.

TOP 3 ACTIONS THIS WEEK

- 1. PATCH PAN-OS CVE-2026-0300 IMMEDIATELY (deadline 9 May -- state-sponsored exploitation since 16 April):** Captive Portal RCE in Palo Alto PAN-OS (CVSS 9.3). State-sponsored actors have been exploiting this since 16 April. SA enterprises with PAN firewalls must restrict Captive Portal access to management-only and patch before 9 May. Hunt for unexpected `/api/?type=op&cmd=...` POSTs and outbound HTTPS from PAN-OS management-plane interfaces.
- 2. PRE-STAGE PATCH TUESDAY 12 MAY (Defender RedSun/UnDefend expected):** Microsoft Patch Tuesday on 12 May is expected to finally address RedSun and UnDefend -- the two unpatched Defender zero-days (6+ weeks unpatched). Pre-stage testing now. Also covers ConnectWise ScreenConnect KEV deadline and Windows Shell NTLM APT28 chain. Patch Tuesday is the single most important patching event of the W20 window.
- 3. RESET Canvas/Instructure API tokens for SA tertiaries ahead of 12 May ShinyHunters leak deadline:** Wits, Stadio, Milpark, Invictus, and SPARK Schools are confirmed in the Canvas/Instructure 3.65 TB / 275M record dump. Reset all Canvas admin and integration API tokens, rotate SSO secrets, audit OAuth refresh tokens and `/api/v1/users/*` access patterns. Prepare student data-subject communications ahead of the 12 May leak deadline.

Critical Findings:

- **Standard Bank / PrinzEugen FORMAL INDEXING (4 May):** ransomware.live formally indexed Standard Bank Group under the PrinzEugen / ROOTBOY listing on 4 May 2026. Volume: 1.2 TB, 154,333,668 SQL rows claimed. Daily dumps continuing; ransom (1 BTC) refused. SA tally 107 to 108. IR enforcement posture now has public indexing as evidence anchor.²
- **City of Ekurhuleni R2bn billing fraud SCOPA disclosure (6 May):** Parliamentary SCOPA hearing on 6 May revealed a Wi-Fi-based intrusion into Ekurhuleni licensing and billing systems spanning 2023–2024. Approximately R400M recovered; CIO suspended; SIU/Hawks investigating. First confirmed multi-year Wi-Fi-enabled municipal cyber-fraud at this scale in SA.³
- **ShinyHunters Canvas/Instructure 12 May deadline — 5 SA institutions confirmed:** ShinyHunters Canvas mega-breach (3.65 TB, 275M records, 8,809 institutions globally) carries a 12 May leak deadline. Five SA institutions are confirmed in the dump: **Wits, Stadio, Milpark, Invictus, SPARK Schools**. Reset API tokens and prepare breach communications immediately.⁴
- **Stormous CGCSA carry-over — no W20 movement:** CGCSA (listed 3 May by Stormous) had no data release during W20. Negotiation phase assessed. 151K+ documents, GS1 SharePoint, Sage 200 backups, Unilever/Nestlé/L'Oréal partner data remain in attacker hands.⁵
- **Polmed scope EXPANDED (W20):** Fuller breach scope circulated in IAB channels: 1.7M records, 68,000 active SAPS officers, 214 GB including undercover designations, PTSD codes, and home addresses. R67M emergency response underway. Data being weaponised/monetised.⁶
- **APT28 SAMA financial-sector expansion (7 May):** Fyntralink flagged APT28 expanding geographic targeting of financial institutions to broader geography including SA bank sector on 7 May. CVE-2026-32202 Windows Shell NTLM zero-click (KEV 12 May) is the primary weapon. SA banks to extend IOC coverage.⁷
- **cPanel CVE-2026-41940 SA hosting-provider wave (30 Apr – 4 May):** SA MSPs and hosting providers confirmed targeted with mass "Sorry" ransomware exploitation of cPanel vulnerability. SA-specific wave; patch immediately.⁸
- **IR APP 2025/26 scaling up:** Werksmans coverage (5 May) confirms proactive audit ramp-up, mandatory breach e-portal, cross-border Guidance Note imminent, Code of Conduct for gated-access in draft. IR litigating 4 enforcement matters in parallel. Blouberg R500K fine court action ongoing.⁹

W20 KEY INSIGHT: EKURHULENI MUNICIPAL CYBER-FRAUD MODEL

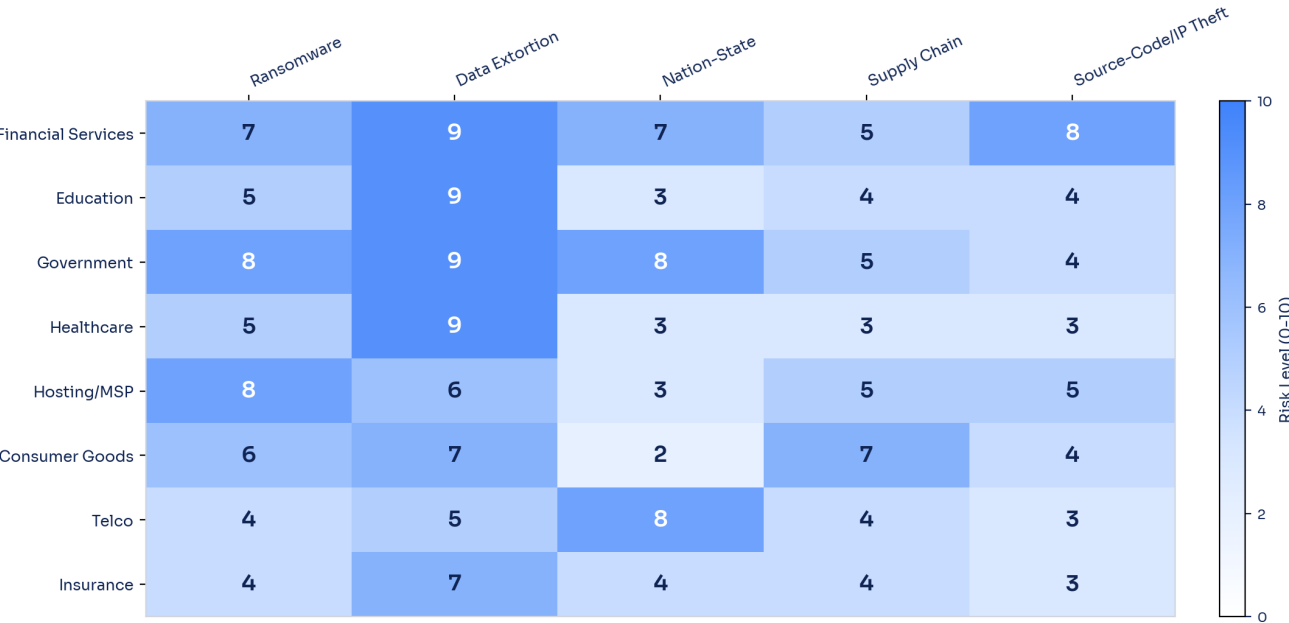
The Ekurhuleni R2 billion billing fraud (disclosed 6 May at SCOPA) represents a new threat model for SA municipalities: a patient, Wi-Fi-enabled intrusion into licensing and billing systems persisting undetected for 1–2 years. The attack vector -- SOHO/municipal Wi-Fi networks with routing to billing/revenue systems -- is reproduced across virtually every SA municipality. SALGA/SITA should initiate a sector-wide Wi-Fi segmentation audit. Any municipality with Wi-Fi access points that can route to billing, licensing, or revenue systems should treat this as a P1 architecture gap. Hunt mission TH-2026-W20-03 provides the detection playbook.³

1. Digital Progression — SA CTI Report W20 Compiled Briefing — <https://dpcyber.co.za>
2. ransomware.live — South Africa Recent Victims — <https://www.ransomware.live/recentvictims>
3. Parliament of South Africa — SCOPA Hearings — <https://www.parliament.gov.za/>
4. BlackFog — April 2026 Ransomware Report (ShinyHunters most active) — <https://www.blackfog.com/>
5. HookPhish — Stormous CGCSA — <https://www.hookphish.com/blog/ransomware-group-stormous-hits-cgcsa-co-za/>
6. ITWeb — Polmed/SAPS medical scheme breach coverage — <https://www.itweb.co.za/>
7. Fyntralink — Threat Intelligence (APT28 SAMA expansion 7 May) — <https://www.fyntralink.com/>
8. CISA KEV Catalog — W20 additions — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
9. Werksmans — IR APP 2025/26 coverage (5 May 2026) — <https://www.werksmans.com/>

2. THREAT LANDSCAPE HEATMAP

The heatmap below maps eight key South African sectors against five threat categories, rated 0–10 based on active threat intelligence, confirmed incidents, and vulnerability exposure during Week 20. **Financial Services** scores highest across multiple threat categories (Standard Bank formal indexing, APT28 SAMA expansion). **Education** spikes sharply on Data Extortion (9) driven by the Canvas/Instructure 12 May ShinyHunters deadline directly impacting five SA tertiary institutions. **Government** is elevated on Ransomware (8), Data Extortion (9), and Nation-State (8) driven by the Ekurhuleni R2bn disclosure and Glowworm/APT41 African government targeting. **Healthcare** remains critically high on Data Extortion (9) due to Polmed scope expansion (68K SAPS officers, undercover designations). **Hosting/MSP** spikes on Ransomware (8) due to the cPanel CVE-2026-41940 SA-specific wave.

SA THREAT LANDSCAPE HEATMAP | W20 (3 May - 10 May 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 20 brought one new SA ransomware-tracker listing: **Standard Bank Group formally indexed on ransomware.live by PrinzEugen (ROOTBOY) on 4 May 2026**, taking the SA cumulative tally from 107 to 108. A major new public disclosure emerged on 6 May: the City of Ekurhuleni R2 billion billing fraud at SCOPA. W20 incident reporting covers 5 active incidents (INC-2026-W20-01 through -05).²

3.1 INC-2026-W20-01 — Standard Bank Group / PrinzEugen (ROOTBOY) [CONFIRMED]

Organisation	Standard Bank Group (Johannesburg Stock Exchange: SBK)
Sector	Financial Services / Banking
Threat Actor	PrinzEugen (ROOTBOY operation)
Date	ransomware.live formal listing: 4 May 2026 (ongoing from 14 April)
Data	1.2 TB, 154,333,668 SQL rows claimed: PII, ID documents, passport/licence images, credit cards (no CVV), SAP records, SharePoint/OneDrive/Power Apps/Oracle SQL attacker movement
Demand	1 BTC (~R1.2M) -- refused
Deadline	Lapsed; daily dumps continuing since 14 April at escalating cadence: 5K to 25K to 50K to 100K rows/day
Payment	Not paid
Status	CONFIRMED ACTIVE -- W20 is when the listing became formally indexed on ransomware.live; daily ROOTBOY dumps continue
SA Significance	Highest-profile SA financial sector exposure of 2026. IR enforcement posture now has ransomware.live public indexing as evidence anchor. R10M POPIA fine and FSCA Joint Standard 2 24-hour notification obligations apply. Hunt: credential reuse from leaked records (TH-2026-W20-01).
Sources	ransomware.live; ITWeb; Daily Maverick; Standard Bank newsroom

The formal ransomware.live indexing on 4 May 2026 is a significant escalation: it moves the Standard Bank / ROOTBOY operation from a Tor-only attacker portal to a publicly indexed tracker visible to security researchers, insurers, regulators, and the media globally. Daily dumps have continued at escalating cadence since 14 April. The IR remains in fact-finding posture and has not yet converted its assessment into a formal POPIA investigation directive. FSCA Joint Standard 2 (24-hour rolling material-incident reporting) continues to apply. SA organisations with Standard Bank workforce relationships face elevated credential-stuffing, SIM-swap, and identity-fraud risk from the 154M+ row dataset. Hunt mission TH-2026-W20-01 provides the credential-reuse detection playbook.²

3.2 INC-2026-W20-02 — CGCSA / Stormous [REPORTED, no W20 update]

Organisation	Consumer Goods Council of South Africa (CGCSA) -- cgcsa.co.za
Sector	Industry Body / Retail Supply Chain / Consumer Goods
Threat Actor	Stormous (extortion / hacktivist-hybrid, STMX_GhostLocker RaaS partner)
Date	Listed on Stormous leak portal 3 May 2026; no W20 public data release
Data	151,000+ CRM documents; GS1 South Africa SharePoint (GDSN protocols + global FMCG partner data: Unilever, Nestlé, L'Oréal); Sage 200 Evolution SQL backups; vendor / corporate PII
Demand	Not publicly disclosed
Deadline	Not disclosed
Payment	Not disclosed
Status	W20 CARRY-OVER -- no data release, no CGCSA statement; assessed as negotiation phase
SA Significance	GS1 South Africa SharePoint exposure -- risk of supply-chain integrity compromise for SA retail. POPIA s.22 obligations apply. Partner data (Unilever/Nestlé/L'Oréal) creates third-party-trust blast radius.
Sources	HookPhish; RedPacket Security; Lyrie.ai; ransomware.live

No data release and no CGCSA public statement during W20. The negotiation phase assessment holds. CGCSA represents 9,000+ member companies across SA consumer goods, retail, and services. GS1 South Africa administers global product identification standards used by virtually every major SA retailer. SA retailers and FMCG manufacturers in CGCSA member networks should audit SharePoint document libraries and Sage 200 Evolution backup file integrity.⁵¹⁰

3.3 INC-2026-W20-03 — Polmed / ShinyHunters [CONFIRMED — scope EXPANDED]

Organisation	Police Medical Aid Scheme (Polmed)
Sector	Healthcare / Law Enforcement
Threat Actor	ShinyHunters (UNC6240 / Scattered LAPSUS\$ Hunters coalition)
Date	Notification 25 Mar; public 16–20 April (W18); W20: fuller scope circulated in IAB
Data	1.7M records, 68,000 active SAPS officers, 214 GB -- including undercover officer designations, PTSD codes, home addresses, command structure roles
Demand	Not publicly disclosed
Deadline	Not disclosed
Payment	Not paid
Status	CONFIRMED ACTIVE -- W20 saw expanded scope circulating in IAB channels; R67M emergency response underway; forensic probe ongoing
SA Significance	NATIONAL SECURITY -- undercover officer designations, PTSD codes, and home addresses create surveillance / targeting risk. Data being weaponised/monetised in IAB channels. First major test of SA Health Data Processing Regulations.
Sources	ITWeb; Cape Town ETC; Integrity360; allAfrica

W20 materially worsened the Polmed picture: the fuller breach scope (1.7M records, 68K active SAPS officers, 214 GB, including undercover designations) circulated in IAB channels during the week, and the data is actively being weaponised and monetised. R67M emergency response is underway. Three parallel

regulatory probes remain active (IR, SAPS, Council for Medical Schemes). Hunt mission TH-2026-W20-02 covers IAB monitoring for SAPS-adjacent identities.⁶

3.4 INC-2026-W20-04 — Adumo (Lesaka) — Unknown Seller
[REPORTED, no W20 update]

Organisation	Adumo (Lesaka Technologies subsidiary, Nasdaq: LSAK)
Sector	Fintech / Payments Processing
Threat Actor	Unknown dark web forum seller
Date	Surfaced ~17 Apr; W20 no movement
Data	14 GB, 15,546 files: InnerEDGE Docker images, C# POS source, EMV kernel source, PAX firmware, Mastercard/Visa cert artefacts, BIN EMV parameters
Demand	\$7,000 (R114,000) sale price
Deadline	N/A (sale listing)
Payment	N/A
Status	W20 UNRESOLVED -- no buyer confirmed, investigation ongoing; "no customer data" claim maintained
SA Significance	Adumo processes R100B+ across 29,000+ SA merchants. Patient adversary risk horizon: 6-18 months for EMV exploit research.
Sources	Techmoonshot; MEXC/Crypto.news; LaunchBase Africa

No W20 movement on the Adumo listing. No buyer confirmed, no investor 8-K, no POPIA s.22 notification confirmed. The patient-adversary risk horizon remains material from the leaked EMV kernel source and Mastercard/Visa certification artefacts.

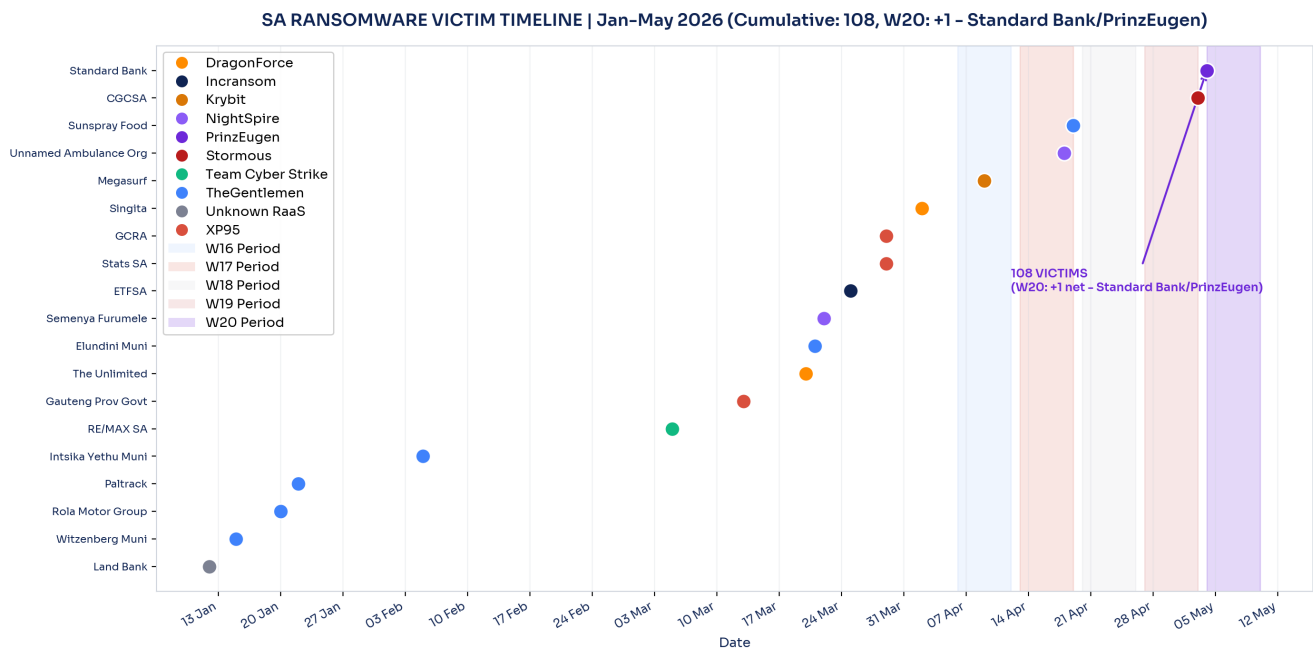
3.5 INC-2026-W20-05 — City of Ekurhuleni R2bn Billing Fraud
[CONFIRMED — NEW W20 disclosure]

Organisation	City of Ekurhuleni (Metropolitan Municipality, Gauteng)
Sector	Government / Municipal
Threat Actor	Unknown (Wi-Fi-based intrusion; suspected insider-assisted)
Date	Intrusion period: 2023–2024; disclosed at SCOPA hearing 6 May 2026
Data	Access to licensing and billing systems; approximately R2 billion in fraudulent billing manipulations
Demand	N/A (financial fraud, not extortion)
Deadline	N/A
Payment	N/A
Status	CONFIRMED NEW W20 DISCLOSURE -- CIO suspended; SIU/Hawks investigating; approximately R400M recovered to date
SA Significance	First confirmed multi-year Wi-Fi-enabled municipal cyber-fraud at this scale in SA. Attack vector (SOHO/municipal Wi-Fi with route to billing/revenue systems) is reproduced across SA municipalities. Sets precedent for sector-wide Wi-Fi segmentation audit. Hunt mission TH-2026-W20-03.
Sources	Parliament of South Africa SCOPA hearing 6 May 2026; ITWeb; MyBroadband

The Ekurhuleni disclosure at SCOPA on 6 May 2026 is the most operationally significant new W20 incident. A Wi-Fi-based intrusion into the City's licensing and billing systems remained undetected for

approximately 1–2 years (2023–2024), enabling approximately R2 billion in fraudulent billing manipulations. The CIO has been suspended and the SIU/Hawks are investigating. Approximately R400M has been recovered. The attack vector — municipal Wi-Fi networks with routing to billing and revenue systems — is a systemic architectural gap across SA municipalities. SALGA, SITA, and individual municipalities should treat this as a trigger for immediate Wi-Fi segmentation audits. Hunt mission TH-2026-W20-03 provides the detection playbook for this vector.³

SA Ransomware Victim Timeline — Jan–May 2026 (Cumulative: 108)



10. HookPhish — Stormous hits CGCSA (3 May 2026) —

<https://www.hookphish.com/blog/ransomware-group-stormous-hits-cgcsa-co-za/>

11. RedPacket Security — Stormous victim CGCSA (3 May 2026) —

<https://www.redpacketsecurity.com/stormous-ransomware-victim-cgcsa-co-za/>

12. Lyrie.ai — Stormous research (3 May 2026) — <https://lyrie.ai/research/research/2026-05-03-stormous-fanasa-mexican-supply-chain>

13. ITWeb — Adumo payment tech exposed (17 Apr) —

<https://www.itweb.co.za/article/adumo-payment-tech-exposed-hackers-offer-data-for-7-000/KWEBb7yLwdAvmRjO>

14. LaunchBase Africa — Adumo source code leak investigation (17 Apr) —

<https://launchbaseafrica.com/2026/04/17/south-african-fintech-adumo-investigates-alleged-source-code-leak/>

4. NATION-STATE: APT28 & GLOWWORM / APT41

W20 brings two nation-state escalations of direct SA relevance. **APT28 (Fancy Bear, Russia GRU)** was flagged by Fyntralink on 7 May as expanding geographic targeting to include the SA financial sector (SAMA-regulated institutions), using the CVE-2026-32202 Windows Shell NTLM zero-click zero-day (KEV deadline 12 May). **Glowworm / APT41-linked (China-nexus)** is confirmed compromising African government departments via ToolShell (CVE-2025-53770), with IOCs covering Zingdoor, ShadowPad, and KrustyLoader tooling. SA organisations with African government MOUs or data-sharing arrangements are at secondary risk.⁷¹⁵

APT28 — SAMA Financial Sector Expansion (7 May)

Attribution	APT28 (Fancy Bear) — Russia GRU Unit 26165 / 74455. Also tracked as Sofacy, STRONTIUM, UAC-0001.
SA Status	Fyntralink flagged SAMA bank-sector targeting expansion on 7 May 2026 -- broader geographic scope including South African financial institutions. No confirmed SA victim yet in W20.
Primary Weapon	CVE-2026-32202 — Windows Shell NTLM zero-click hash theft via LNK/library-ms files. CISA KEV deadline 12 May 2026. Predecessor CVE-2026-21510 used against Ukraine/EU since December 2025.
TTPs	Zero-click NTLM hash capture via malicious .lnk and .library-ms files delivered via email, SMB shares, or web share. Hash relay / Pass-the-Hash for lateral movement. No user interaction required.
Detection	Block outbound SMB (445/139) and WebDAV at perimeter; block .lnk and .library-ms email attachments at gateway; Sysmon EID 11 for .lnk files in user-writable paths with anomalous targets; outbound NTLM auth to non-corporate IPs.
SA Action	SA banks: extend APT28 IOC coverage via Fyntralink/CISA feeds. Apply April 2026 Patch Tuesday before 12 May. Hunt mission TH-2026-W20-07.

Glowworm / APT41-linked — African Government Departments Confirmed

Attribution	Glowworm (APT41-linked, China-nexus). Also tracked via MSTIC as Storm-0744.
SA Status	Confirmed compromising African government departments via ToolShell (CVE-2025-53770). SA government organisations with African MOU/data-share partners are at secondary risk.
Primary Weapon	ToolShell (CVE-2025-53770) — SharePoint-based web shell deployment.
Tooling	Zingdoor (C2 implant), ShadowPad (modular backdoor), KrustyLoader (staged loader). IOC hashes/domains/IPs documented in research_actors_w20.md.
TTPs	T1190 (Exploit Public-Facing App), T1505.003 (Web Shell), T1059 (Command Scripting).
SA Action	SA orgs with African government MOUs / data-share: run ToolShell IOC hunt. Hunt mission TH-2026-W20-08.

MuddyWater — Operation Olalampo (MENA, ongoing)

MuddyWater (Iran, Ministry of Intelligence) continues Operation Olalampo across MENA since January 2026. Full domain/IP/hash IOCs are documented. No confirmed SA target in W20; watch-list posture for SA organisations with MENA exposure. TTPs include spear-phishing, LOLBins, and custom C2 infrastructure.¹⁵

15. Fyntralink — Threat Intelligence (APT28/MuddyWater) — <https://www.fyntralink.com/>

16. CISA KEV Catalog — CVE-2026-32202 Windows Shell NTLM — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

5. ACTIVE THREAT CAMPAIGNS

5.1 ROOTBOY vs Standard Bank — Formal Indexing and Continued Daily Leaks

ROOTBOY's formal ransomware.live indexing on 4 May 2026 marks the transition from attacker-portal-only to globally visible public indexing. Daily leak cadence continues at 100,000 rows/day. The 1.2 TB / 154M+ row dataset includes PII, ID documents, passport/licence images, credit cards (no CVV), and SAP records. SA organisations processing Standard Bank-sourced data face second-order POPIA notification obligations. Credit card replacement operations, customer outreach, and IR fact-finding all continue.²

5.2 ShinyHunters Canvas/Instructure Mega-Breach — 12 May SA Deadline

ShinyHunters' Canvas/Instructure breach (3.65 TB, 275M records, 8,809 institutions globally) carries a 12 May 2026 public leak deadline. Five SA tertiary institutions are confirmed in the dump: **Wits University, Stadio, Milpark Education, Invictus Education Group, and SPARK Schools**. Canvas API tokens, OAuth refresh tokens, and SSO federation secrets must be rotated immediately. Student data-subject communications and breach notification planning are urgent. BlackFog named ShinyHunters the most active ransomware group in April 2026 with 15 confirmed incidents.⁴¹⁷

5.3 Stormous CGCSA — No W20 Data Release; Continued Watch

Stormous listed CGCSA on 3 May (final day of W19) and carried into W20 without a data release. The STMX_GhostLocker RaaS partnership is intact. Stormous also hit a UAE insurance firm (700 GB) and a Vietnamese architecture firm (5 TB, \$900K demand) in the same week, indicating an operational tempo spike. CGCSA negotiation phase is assessed; SA retailers in the CGCSA member network should use the W20 window to audit SharePoint and Sage 200 backup integrity.⁵¹⁰

5.4 cPanel CVE-2026-41940 — SA Hosting-Provider Wave (30 Apr – 4 May)

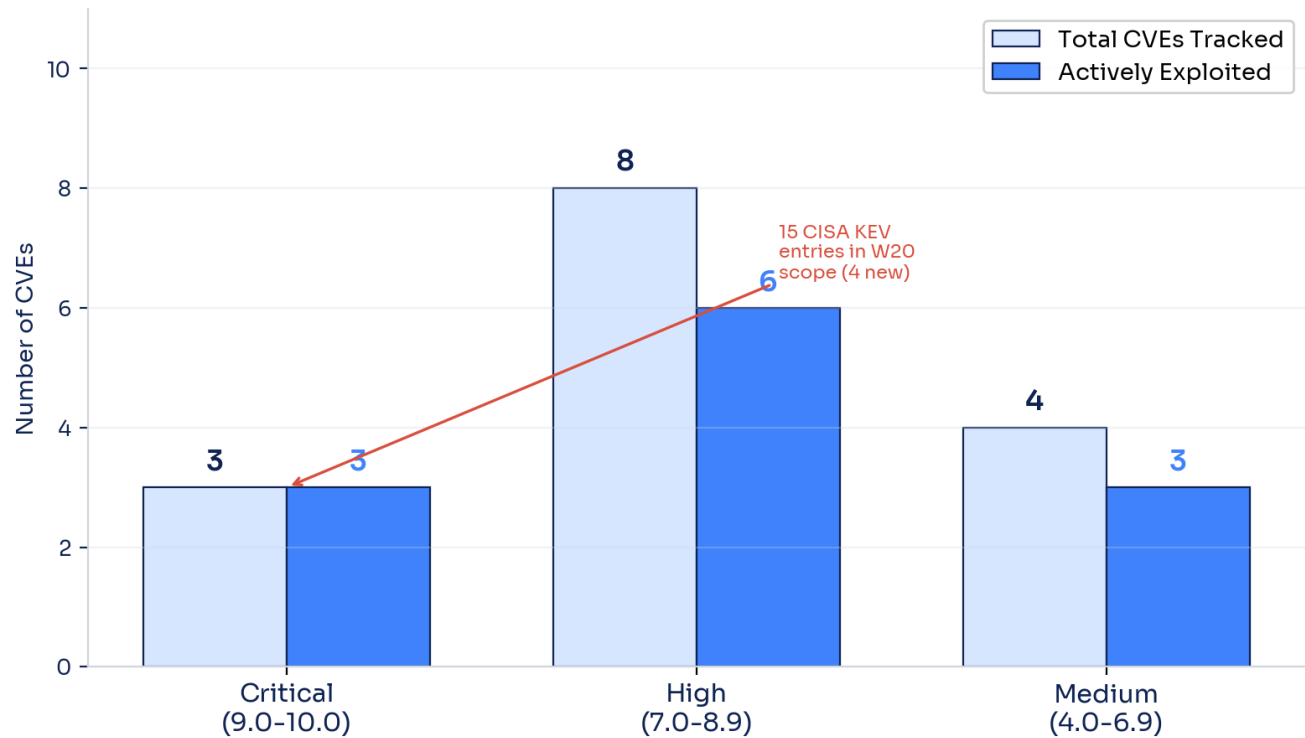
An unknown threat actor conducted a mass ransomware wave against SA MSPs and hosting providers using a cPanel vulnerability (CVE-2026-41940) between 30 April and 4 May. "Sorry" ransomware was deployed across shared-hosting volumes. SA hosting providers must patch cPanel immediately, audit new API tokens and SSH key additions, and scan for "Sorry" ransomware extension patterns. Hunt mission TH-2026-W20-06 provides the detection playbook.⁸

17. BlackFog — April 2026 Ransomware Report — <https://www.blackfog.com/>

18. ransomware.live — South Africa Recent Victims — <https://www.ransomware.live/recentvictims>

6. CRITICAL VULNERABILITIES & CISA KEV

CVE SEVERITY DISTRIBUTION | W20 Priority Vulns & CISA KEV



Week 20 brought **4 new CISA KEV additions** with aggressive deadlines clustered around the 12 May Patch Tuesday window. **CVE-2026-0300 (PAN-OS Captive Portal RCE, CVSS 9.3)** tops the urgency list with a 9 May deadline and confirmed state-sponsored exploitation since 16 April. **CVE-2026-41940 (cPanel)** is SA-specific with confirmed mass-ransomware targeting of SA hosting providers. Microsoft Defender **RedSun + UnDefend remain STILL UNPATCHED** 6+ weeks on -- Patch Tuesday 12 May is expected to address them. ConnectWise (CVE-2024-1708) and Windows Shell NTLM (CVE-2026-32202) carry over with 12 May KEV deadlines.⁸¹⁹

New CISA KEV Additions — W20 (3–10 May 2026)

CVE ID	Vendor/Product	CVSS	Class	Ransomware ?	KEV Deadline
CVE-2026-0300	Palo Alto PAN-OS (Captive Portal RCE)	9.3	RCE	Unknown	9 May 2026
CVE-2026-6973	Ivanti EPMM (Auth Bypass)	7.2	Auth Bypass	Unknown	10 May 2026
CVE-2026-42208	BerriAI LiteLLM (RCE)	9.3	RCE	Unknown	11 May 2026
CVE-2026-31431	Linux Kernel "Copy Fail" (LPE)	7.8	LPE	Unknown	15 May 2026

Carry-Over KEV Deadlines (12 May)

CVE ID	Vendor/Product	CVSS	Class	Ransomware ?	KEV Deadline
CVE-2024-1708	ConnectWise ScreenConnect	8.4	Path Traversal RCE	Medusa (Storm-1175)	12 May 2026
CVE-2026-32202	MS Windows Shell (NTLM zero-click)	4.3	NTLM Hash Leak	APT28-linked	12 May 2026

UNPATCHED ZERO-DAYS — Microsoft Defender RedSun + UnDefend: STILL UNPATCHED (6+ weeks): RedSun abuses Defender cloud rollback to disable signature updates. UnDefend denial-of-services Defender entirely. Both have NO patch available -- detection-only posture required until Patch Tuesday 12 May. Hunt for RedSun.exe / UnDefend.exe / FunnyApp.exe in user folders; Qualys QID 92382; alert on Defender service status anomalies and

signature update failures.

Top Priority CVE Details — W20

CVE-2026-0300 — Palo Alto PAN-OS Captive Portal RCE — CVSS 9.3 — P1 PATCH NOW (KEV 9 May)

Unauthenticated Remote Code Execution via the Captive Portal feature in PAN-OS. State-sponsored actors have been exploiting this since 16 April 2026 — over three weeks of active exploitation before the CISA KEV addition. SA enterprises with Palo Alto firewalls must: (1) restrict Captive Portal access to management-only immediately; (2) patch by 9 May. Detection: outbound HTTPS connections from PAN-OS management-plane interfaces; unexpected `/api/?type=op&cmd=...` POSTs; firewall config drift. MITRE: T1190, T1133. Hunt mission TH-2026-W20-04.⁸

CVE-2026-41940 — cPanel — SA HOSTING-PROVIDER MASS RANSOMWARE WAVE

A vulnerability in cPanel (already KEV-listed prior to W20) was weaponised in a targeted wave against SA MSPs and hosting providers between 30 April and 4 May 2026. "Sorry" ransomware deployed across shared-hosting volumes. Detection: `cpsrvd` / `whostmgrd` anomalous child processes; new cPanel API tokens; SSH key additions; "Sorry" ransomware extension scan on shared-hosting volumes. SA-specific wave confirmed. Patch immediately; audit all new API tokens and SSH keys added after 30 April. Hunt mission TH-2026-W20-06. MITRE: T1190, T1098, T1486.⁸

CVE-2026-6973 — Ivanti EPMM Auth Bypass — CVSS 7.2 — P1 PATCH NOW (KEV 10 May)

Authentication bypass in Ivanti Endpoint Manager Mobile (EPMM, formerly MobileIron). Allows unauthenticated attackers to gain administrative access to the MDM platform. SA enterprises managing mobile devices via Ivanti EPMM must patch by 10 May. Detection: MDM enrolment from anomalous IPs; sudden admin-role grants; unsigned profile pushes. Hunt mission TH-2026-W20-05. MITRE: T1190, T1078.004.⁸

CVE-2026-42208 — BerriAI LiteLLM RCE — CVSS 9.3 — P1 PATCH NOW (KEV 11 May)

Remote Code Execution in BerriAI LiteLLM, an open-source LLM proxy/gateway widely deployed in AI/ML workflows. SA organisations using LiteLLM in AI infrastructure must patch by 11 May. CVSS 9.3 with no user interaction required. Audit LiteLLM deployment exposure; restrict to internal/VPN-only access.⁸

CVE-2026-31431 — Linux Kernel "Copy Fail" LPE — CVSS 7.8 — P2 (KEV 15 May)

Local Privilege Escalation in the Linux Kernel. Public PoC available; no confirmed ITW exploitation yet in the W20 window. Vendor patches are rolling out. SA Linux server estates must apply kernel patches by 15 May. Dirty Frag (CVE-2026-43284 / CVE-2026-43500) is a related Linux Kernel LPE pair with public PoC -- patch those concurrently.⁸

CVE-2024-1708 — ConnectWise ScreenConnect — CVSS 8.4 — P1 PATCH NOW (KEV 12 May)

Path traversal-to-RCE in ConnectWise ScreenConnect (carry-over from W19). Active Medusa ransomware and Storm-1175 exploitation continues. ConnectWise is the most common RMM platform across SA MSP estates. Patch to 23.9.8+; audit technician sessions; rotate credentials. Federal patch deadline 12 May 2026. MITRE: T1190, T1219, T1486.⁸

RedSun + UnDefend — MS Defender — STILL UNPATCHED — P1 DETECTION ONLY

Two of the W17 Microsoft Defender zero-day trilogy remain unpatched 6+ weeks on. **RedSun** abuses Defender's cloud rollback mechanism to silently disable signature updates. **UnDefend** achieves a full denial-of-service against the Defender service. **Patch Tuesday 12 May is expected to address both.** Until then: Hunt for `RedSun.exe`, `UnDefend.exe`, `FunnyApp.exe` in user-writable directories. Use Qualys QID 92382. Alert on `mpcmdrun.exe -SignatureUpdate` failures. Apply BlueHammer (CVE-2026-33825) fix (4.18.26030.3011) if not already deployed.⁸

Remaining W20 Vulnerability Notes

- **Dirty Frag (CVE-2026-43284 / CVE-2026-43500) — Linux Kernel LPE:** Public PoC available; no confirmed ITW exploitation. Patch alongside CVE-2026-31431 (KEV 15 May).
- **Microsoft Patch Tuesday 12 May 2026:** Expected to patch RedSun, UnDefend (Defender zero-days); apply immediately across all Windows estates. Also covers ConnectWise and Windows Shell NTLM KEV deadlines.
- **Verizon DBIR 2026 SA commentary (ITWeb/IT-Online this week):** Credentials at R100/set on dark web; identity weaknesses in 90% of SA breaches; cybercrime costing R2.2bn/year. Webinar 19 May.
- **Standard Bank credential reuse risk (ongoing):** 154M+ row leak indexed publicly 4 May -- credential-stuffing and SIM-swap risk remains elevated for all SA organisations with Standard Bank workforce relationships.

19. CISA KEV Catalog — W20 Additions (4 entries, 3-10 May 2026) — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

20. Microsoft MSRC — Security Update Guide — <https://msrc.microsoft.com/update-guide/>

7. THREAT ACTOR PROFILES & RANSOMWARE ACTIVITY

SA Ransomware Victim Count: 108 as of end W20 (107 to 108, +1 net). One new SA ransomware.live listing in W20: **Standard Bank Group / PrinzEugen (ROOTBOY)**, formally indexed 4 May 2026. CGCSA (Stormous, 3 May W19) is a carry-over with no W20 data release. The Q1 2026 global landscape continues at the elevated 150–200 victims/week tempo. BlackFog named ShinyHunters the most active ransomware group in April 2026 with 15 incidents.¹⁷¹⁸

Active SA-Relevant Threat Actor Summary — W20

Actor	Type	SA Victims/Status	W20 Activity	Primary TTPs
Stormous	Extortion / hacktivist-hybrid (ST MX_GhostLocker)	CGCSA (W19, ongoing)	CARRY-OVER — no W20 data release; negotiation phase	CRM/SharePoint/Sage 200 access; supply chain
ShinyHunters	Data Extortion / EaaS	Polmed (214 GB expanded); Canvas 12 May SA deadline	CRITICAL — 12 May Canvas leak deadline (5 SA institutions)	Vishing to Okta FastPass; SaaS pivoting; T1528
PrinzEugen / ROOTBOY	Data Extortion (individual operator)	Standard Bank (formal indexing 4 May)	ACTIVE — 154M rows / 1.2TB; daily dumps 100K rows/day	SharePoint/OneDrive/Power Apps/Oracle SQL movement
LockBit 5.0	RaaS	No confirmed SA W20 victim	WATCH — 100+ DLS victims globally since Dec 2025	Process hollowing; anti-debug; ETW patching; 1/65 VT score
Storm-1175	Criminal (RaaS affiliate)	No confirmed SA target W20	ACTIVE — ScreenConnect CVE-2024-1708 exploitation	ConnectWise RMM abuse; Medusa ransomware deployment
APT28	Nation-State (Russia GRU)	SAMA financial-sector expansion flagged 7 May	ESCALATING — CVE-2026-32202 NTLM zero-click; SAMA watch	LNK/library-ms NTLM hash theft; Pass-the-Hash
Glowworm / APT41	Nation-State (China-nexus)	African govt depts (SA partners at risk)	ACTIVE — ToolShell CVE-2025-53770; Zingdoor/ShadowPad	Web shell; SharePoint exploitation; T1505.003
MuddyWater	Nation-State (Iran)	No confirmed SA target W20	ONGOING — Operation Olalampo MENA	Spear-phish; LOLBins; custom C2
Unknown (cPanel)	Criminal	SA hosting providers confirmed targeted	ACTIVE W20 — mass "Sorry" ransomware wave	cPanel CVE-2026-41940; mass-hosting ransomware
IAB market	Initial Access Broker	SA credential market flooded	ELEVATED — R100/set credentials; 69 SA servers listed	XSS[.jac; BreachForums fragments; RAMP premium

Stormous — CGCSA CARRY-OVER (no W20 release)

Stormous carries the CGCSA listing from W19 into W20 with no data release. The STMX_GhostLocker RaaS partnership remains intact. Stormous TTPs (spear-phish, Cobalt Strike, exfil, STMX_GhostLocker encryption) are documented. SA defenders should treat the absence of a W20 release as a negotiation window, not resolution. GS1 SharePoint and Sage 200 Evolution data remain in attacker hands.⁵¹²

ShinyHunters — CANVAS 12 MAY DEADLINE (5 SA INSTITUTIONS)

ShinyHunters' Canvas/Instructure mega-breach (3.65 TB, 275M records, 8,809 institutions) carries a 12 May 2026 public leak deadline. Five SA institutions confirmed in scope: Wits, Stadio, Milpark, Invictus, SPARK Schools. BlackFog named ShinyHunters the most active group in April 2026 with 15 incidents. Canvas API tokens, OAuth refresh tokens, SSO secrets must be reset. Prepare breach notifications for student data subjects. Polmed carry-over (214 GB, 1.7M records, 68K SAPS officers) also continues -- expanded scope confirms IAB monetisation.⁴¹⁷

PrinzEugen / ROOTBOY — STANDARD BANK FORMAL INDEXING (4 May)

PrinzEugen formally indexed Standard Bank on ransomware.live on 4 May, making the operation publicly visible globally. 154M rows, 1.2 TB. ROOTBOY operates as a focused single-target operator with no additional W20 victims. The daily dump cadence (100K rows/day) continues. The IR's parallel fact-finding now has public tracker evidence as an anchor.²

LockBit 5.0 — WATCH (no confirmed SA W20 victim)

LockBit 5.0 has claimed 100+ Data Leak Site victims globally since December 2025. No confirmed SA or Africa victim in W20. Technical maturity is high: process hollowing, anti-debug, geographic checks, ETW patching, 1/65 VirusTotal detection score. Watch-list posture for SA enterprises.

APT28 — SAMA FINANCIAL SECTOR EXPANSION (7 May)

APT28's expansion to SAMA-regulated financial institutions (flagged by Fyntralink 7 May) represents the most significant W20 nation-state escalation for SA. The CVE-2026-32202 Windows Shell NTLM zero-click chain (KEV 12 May) is the primary weapon. SA banks should extend APT28 IOC coverage and apply the April 2026 Patch Tuesday immediately. Hunt mission TH-2026-W20-07 provides the detection playbook.⁷¹⁵

Glowworm / APT41 — AFRICAN GOVERNMENT TARGETING (SA partners at risk)

Glowworm (APT41-linked) is confirmed compromising African government departments via ToolShell (CVE-2025-53770). Tooling includes Zingdoor, ShadowPad, and KrustyLoader. SA organisations with African government MOUs or data-sharing arrangements face secondary compromise risk. Hunt mission TH-2026-W20-08 covers SA-adjacent ToolShell hunting.¹⁵

IAB Market — SA CREDENTIAL MARKET FLOODED (R100/set)

The SA IAB market remains highly active: credentials available at R100/set, 69 SA server accesses bulk-listed in March 2026, Gauteng City Region Academy 147 GB sale identified. XSS migrated to xss[.]ac; BreachForums fragmented. RAMP remains the premium convergence point for higher-value SA access. Polmed data actively being monetised in IAB channels.

Q1 2026 Global Ransomware Landscape

Metric	Value
Q1 2026 victims (GuidePoint / ZeroFox)	2,622 / 2,059
Weekly tempo	150-200 (the new normal)
March 2026 monthly	808 victims, 65 active groups
US share of victims	51%
Africa share	Under 5%
Top 3 by Q1 victims	Qilin (361), Akira (197), TheGentlemen (192)
Most active April 2026 (BlackFog)	ShinyHunters (15 incidents)

21. Industrial Cyber — GuidePoint GRIT Q1 2026 Ransomware Report — <https://industrialcyber.co/reports/ransomware-reaches-elevated-new-normal-as-attack-volumes-hold-steady-into-2026-reshape-baseline-risk-expectations/>
22. BlackFog — April 2026 State of Ransomware — <https://www.blackfog.com/>

8. OSINT EXPOSURE & ATTACK SURFACE

Standard Bank / PrinzEugen — Formal ransomware.live indexing (4 May)

Standard Bank Group was formally indexed on ransomware.live by PrinzEugen (ROOTBOY) on 4 May 2026. The listing is publicly visible globally. 154,333,668 SQL rows, 1.2 TB. Daily dumps at 100K rows/day. SA organisations with Standard Bank workforce relationships: force credential rotation for any user matching the leaked dataset; maintain HIBP-style domain monitoring; alert on new-country logons. Hunt mission TH-2026-W20-01.²

City of Ekurhuleni R2bn billing fraud — SCOPA disclosure (6 May)

City of Ekurhuleni disclosed at SCOPA on 6 May that a Wi-Fi-based intrusion into licensing and billing systems spanning 2023-2024 caused approximately R2 billion in billing fraud. CIO suspended; SIU/Hawks investigating. SALGA/SITA: initiate sector-wide Wi-Fi segmentation audit immediately. Hunt mission TH-2026-W20-03 provides ARP/DHCP anomaly and long-duration RDP/SMB detection playbook.³

ShinyHunters Canvas/Instructure — 12 May deadline; 5 SA institutions confirmed

Three days from publication: ShinyHunters' Canvas/Instructure 3.65 TB / 275M record dump carries a 12 May 2026 leak deadline. Five SA tertiary institutions confirmed in scope: Wits, Stadio, Milpark, Invictus, SPARK Schools. Reset Canvas admin and integration API tokens NOW, rotate SSO secrets, review /api/v1/users/* access patterns for anomalies. Prepare student data-subject communications and breach notification packs. Hunt mission TH-2026-W20-02.⁴¹⁷

Stormous CGCSA — carry-over (no W20 data release)

No Stormous data release for CGCSA during W20. Negotiation phase assessed. 151K+ CRM documents, GS1 SharePoint, Sage 200 Evolution backups, Unilever/Nestlé/L'Oréal partner data remain in attacker hands. SA retailers in CGCSA member networks should audit SharePoint libraries and Sage 200 backup integrity as a precautionary measure.⁵¹⁰

APT28 NTLM zero-click campaign expansion to SA financial sector (7 May)

Fyntralink flagged APT28 expanding geographic targeting to SAMA-regulated SA financial institutions on 7 May. CVE-2026-32202 (KEV 12 May) is the primary weapon. SA banks: apply April 2026 Patch Tuesday before 12 May, block outbound 445/139, block .lnk/.library-ms email attachments. Hunt mission TH-2026-W20-07.⁷¹⁵

cPanel CVE-2026-41940 SA hosting-provider targeting wave (30 Apr – 4 May)

SA MSPs and hosting providers confirmed targeted with mass "Sorry" ransomware via cPanel CVE-2026-41940 between 30 April and 4 May. Patch cPanel immediately; audit new API tokens and SSH keys added after 30 April; scan shared-hosting volumes for "Sorry" ransomware extension patterns. Hunt mission TH-2026-W20-06.⁸

Polmed scope expansion in IAB channels (W20)

The fuller Polmed breach scope (1.7M records, 68K active SAPS officers, 214 GB, including undercover designations, PTSD codes, home addresses) circulated in IAB channels during W20. Data is being actively weaponised and monetised. Security organisations with SAPS-adjacent identities: force MFA reviews, monitor IAB chatter for SAPS officer email patterns. Hunt mission TH-2026-W20-02.⁶

Surfshark Q1 2026 SA data (reported 7–8 May by IT-Online/ITWeb)

Surfshark Q1 2026 SA data (reported by IT-Online and ITWeb on 7–8 May): 212,700 SA accounts leaked in Q1 2026; 70 in 100 South Africans historically affected; IR receives approximately 284 notifications per month. These figures contextualise the SA breach environment and underscore the credential-exposure baseline that attackers are exploiting via IAB markets at R100/set.²³²⁴

23. IT-Online — Surfshark Q1 SA data (7 May 2026) — <https://it-online.co.za/>

24. ITWeb — DBIR SA commentary (7–8 May 2026) — <https://www.itweb.co.za/>

9. REGULATORY & COMPLIANCE

Information Regulator — APP 2025/26 Activity (5 May Coverage)

IR Annual Performance Plan 2025/26 — Werksmans Coverage (5 May): The Information Regulator's APP signals a material operational scale-up: proactive audits are increasing; the mandatory breach e-portal is now live; a Cross-Border Data Transfer Guidance Note is imminent; a Code of Conduct for gated-access platforms is in draft. The IR is litigating 4 enforcement matters in parallel. The Blouberg R500K fine court application (filed 30 April) remains the active enforcement signal. Only approximately 14% of CIPC-registered companies have registered information officers.⁹²⁵

Surfshark Q1 2026 SA Data (IT-Online / ITWeb 7–8 May): 212,700 SA accounts leaked in Q1 2026; 70 in 100 South Africans historically affected by data leaks; IR receives approximately 284 breach notifications per month. The DBIR 2026 SA commentary (also published this week) puts credentials at R100/set on dark web and identity weaknesses in 90% of SA breaches, with cybercrime costing R2.2 billion per year.²³²⁴

SA Draft AI Policy Withdrawn: The DCDT's draft AI policy was withdrawn on 26 April after AI-hallucinated citations were identified. Wits published analysis on 4 May; The Common Sense published commentary on 9 May. The governance vacuum continues. SA organisations deploying AI systems should not rely on regulatory guidance for AI risk management until a new draft is published.²⁶²⁷

CPA Amendment Regulations 2026: The Opt-Out Registry is live (April 2026). NCC registration opens July 2026. Penalties up to R1M or 10% turnover. POPIA s.69 remains separately mandatory -- the CPA register does NOT substitute s.69 consent for direct marketing. SA marketers must maintain dual compliance.²⁵

Verizon DBIR 2026 SA Commentary (ITWeb/IT-Online this week): Credentials available at R100/set on dark web; identity weaknesses identified in 90% of SA breaches; cybercrime costing SA R2.2 billion per year; third-party involvement doubled to 30% of breaches globally. DBIR 2026 Webinar 19 May. Reference document for board-level briefings.²⁴²⁸

Global Regulatory with SA Impact

NIS2 first audit deadline 30 June 2026 (7 weeks away): SA organisations with EU operations are directly in scope. **EU AI Act full enforcement 2 August 2026** (high-risk AI systems, Annex III): SA AI/tech exporters to the EU must have compliance frameworks operational. **UK Cyber Resilience Bill** (penalties 4% worldwide turnover): SA MSPs with UK clients in scope. **Australia Cyber Security Act** full enforcement since 1 January 2026 (72-hour ransom-payment reporting): SA entities with Australian operations in scope.

Compliance Deadlines Table — W20 (Next 8 Weeks)

Deadline	Item	Jurisdiction
11 May 2026	KEV: BerriAI LiteLLM CVE-2026-42208	US federal (advisory globally)
12 May 2026	KEV: ConnectWise ScreenConnect (CVE-2024-1708)	US federal (advisory globally)
12 May 2026	KEV: Windows Shell NTLM CVE-2026-32202	US federal (advisory globally)
12 May 2026	ShinyHunters Canvas/Instructure leak deadline (5 SA institutions)	Global (SA impact)
12 May 2026	Microsoft Patch Tuesday (May 2026) -- RedSun/UnDefend expected	Global
15 May 2026	KEV: Linux Kernel CVE-2026-31431	US federal (advisory globally)
19 May 2026	Verizon DBIR 2026 SA Webinar	SA
30 June 2026	NIS2 first audit deadline	EU (SA orgs in scope)
July 2026	CPA Amendment: NCC registration opens	SA
2 August 2026	EU AI Act full enforcement (high-risk systems)	EU (SA orgs in scope)

25. Information Regulator South Africa — Media Statements — <https://infoeregulator.org.za/media-statements/>
26. Wits University — AI policy analysis (4 May 2026) — <https://www.wits.ac.za/>
27. The Common Sense — AI policy commentary (9 May 2026) — <https://thecommonsense.co.za/>
28. Verizon DBIR 2026 — Data Breach Investigations Report — <https://www.verizon.com/business/resources/reports/dbir/>

10. WEEKLY THREAT HUNT & IOCs

Eight hunt missions are active for W20. Four P1 missions address the Standard Bank credential-reuse hunt (TH-01), Canvas API token resets for 5 SA tertiaries ahead of 12 May deadline (TH-02), Ekurhuleni municipal Wi-Fi segmentation review (TH-03), and PAN-OS Captive Portal RCE state-sponsored exploitation (TH-04). Three P2 missions address Ivanti EPMM auth-bypass (TH-05), cPanel SA hosting-provider wave (TH-06), and APT28 NTLM zero-click (TH-07). One P3 mission covers Glowworm/APT41 ToolShell hunting for SA organisations with African government partners (TH-08).

TH-2026-W20-01 — Standard Bank Credential Reuse Hunt

P1 — CRITICAL: 154M+ rows indexed; credential reuse risk

Hypothesis: After the 4 May ransomware.live indexing of the Standard Bank 154M+ row dump, leaked credentials (.za / standardbank.* email domains) are being used for credential stuffing against corporate IdP, O365, and Azure AD. Any successful auth from a non-corporate IP using a leaked credential = high-confidence reuse incident.

MITRE ATT&CK: T1078 (Valid Accounts), T1110.004 (Credential Stuffing), T1589 (Gather Victim Identity Information).

IOCs: Standard Bank email domain patterns in IdP logs from non-corporate IPs; spike in failed auths; geolocation anomalies; SIM-swap requests for Standard Bank-registered numbers; phishing domains containing "standardbank", "liberty", "stanbic".

Data Sources: Azure AD / Okta sign-in logs (last 90 days), SIEM correlation, fraud-monitoring feeds, SIM-swap notifications, dark-web monitoring (HIBP, Flare, Recorded Future).

Detection Guidance: Pull all .za / standardbank.* email domains from leaked dataset; cross-reference IdP sign-in logs (last 90 days); alert on successful auth from non-corporate IP space using a leaked credential. HIBP-style domain monitoring. Alert on new-country logons within 7-day rolling window.

TH-2026-W20-02 — ShinyHunters Canvas 12 May Deadline Prep (SA Tertiary)**P1 — CRITICAL: 12 May leak deadline; 5 SA institutions**

Hypothesis: Wits, Stadio, Milpark, Invictus, and SPARK Schools are confirmed in the Canvas/Instructure dump. API tokens, OAuth refresh tokens, and SSO federation secrets are likely in the dataset and may already be in use by ShinyHunters or secondary actors. Anomalous access to Canvas /api/v1/users/* endpoints = pre-leak exploitation indicator.

MITRE ATT&CK: T1078.004 (Cloud Accounts), T1528 (Steal Application Access Token), T1552 (Unsecured Credentials).

IOCs: Anomalous Canvas API activity (/api/v1/users/*); unusual OAuth token grants; SSO federation anomalies; Canvas admin session from non-institutional IPs; bulk export of student records.

Data Sources: Canvas audit log, OAuth token grant log, SSO federation logs (last 180 days), IdP access logs, network perimeter (Canvas API endpoints).

Detection Guidance: Reset ALL Canvas admin and integration API tokens immediately. Rotate SSO secrets. Audit /api/v1/users/* access patterns for anomalies in last 180 days. Prepare breach notification packs for student data subjects ahead of 12 May deadline.

TH-2026-W20-03 — Municipal Wi-Fi Segmentation Review (Ekurhuleni model)**P1 — CRITICAL: Ekurhuleni model; SA municipal sector exposure**

Hypothesis: The Ekurhuleni R2bn fraud (2023-2024) used Wi-Fi network access with routing to billing/licensing/revenue systems. SA municipalities with similar architecture (SOHO/corporate Wi-Fi with route to billing) are exposed to the same multi-year fraud vector. ARP/DHCP anomalies and long-duration RDP/SMB from wireless subnets = active exploitation indicators.

MITRE ATT&CK: T1200 (Hardware Additions), T1078 (Valid Accounts), T1021 (Remote Services).

IOCs: ARP/DHCP anomalies on segments adjacent to billing; long-duration RDP/SMB sessions (>4 hours) originating from wireless subnets; anomalous billing-system write transactions; wireless client MAC addresses not in asset register.

Data Sources: Network switch ARP/DHCP logs, wireless controller session logs, billing-system audit log, SIEM correlation, Active Directory logon events from wireless-segment IPs.

Detection Guidance: Audit all wireless networks with routing to billing/licensing/revenue systems. Implement network segmentation to isolate billing systems from wireless. Alert on any new RDP/SMB session from a wireless subnet to billing systems. Review billing system audit logs for anomalous writes.

TH-2026-W20-04 — PAN-OS Captive Portal RCE (CVE-2026-0300)**P1 — CRITICAL: KEV 9 May; state-sponsored exploitation since 16 April**

Hypothesis: State-sponsored actors have been exploiting PAN-OS Captive Portal RCE (CVSS 9.3) since 16 April. SA enterprises with internet-facing PAN-OS Captive Portal are directly exposed. Outbound HTTPS from management-plane interfaces and unexpected API POST requests = active exploitation indicators.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1133 (External Remote Services).

IOCs: Outbound HTTPS connections from PAN-OS management-plane interfaces; unexpected /api/?type=op&cmd=... POSTs; firewall config drift; unexpected admin-tier accounts created; PAN-OS version below patched release.

Data Sources: PAN-OS system log, PAN-OS config audit log, perimeter NetFlow, EDR on management hosts, SIEM.

Detection Guidance: Restrict Captive Portal to management-only IMMEDIATELY. Patch PAN-OS by 9 May. Audit firewall config for drift. Review all admin-tier accounts created since 16 April.

TH-2026-W20-05 — Ivanti EPMM Auth Bypass (CVE-2026-6973)**P2 — HIGH: KEV 10 May;
MDM estate exposure**

Hypothesis: Unauthenticated attackers can gain administrative access to Ivanti EPMM (formerly MobileIron). SA enterprises managing mobile devices via Ivanti EPMM are exposed. Anomalous MDM enrolments and sudden admin-role grants = exploitation indicators.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1078.004 (Cloud Accounts).

IOCs: MDM enrolment events from anomalous IPs; sudden admin-role grants on EPMM; unsigned profile pushes; EPMM version below patched release.

Data Sources: Ivanti EPMM admin audit log, MDM enrolment log, IdP access logs, perimeter NetFlow.

Detection Guidance: Patch Ivanti EPMM by 10 May. Audit all admin-role grants on EPMM for the last 30 days. Restrict EPMM admin interface to VPN/OOB. Review unsigned profile pushes.

TH-2026-W20-06 — cPanel CVE-2026-41940 SA Hosting-Provider Wave**P2 — HIGH: SA-specific
confirmed targeting; "Sorry"
ransomware**

Hypothesis: SA MSPs and hosting providers were targeted with "Sorry" ransomware via cPanel CVE-2026-41940 between 30 April and 4 May. New cPanel API tokens, SSH key additions, and anomalous cpsrvd child processes = active exploitation indicators.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1098 (Account Manipulation), T1486 (Data Encrypted for Impact).

IOCs: cpsrvd / whostmgrd anomalous child processes; new cPanel API tokens created after 30 April; SSH key additions after 30 April; "Sorry" ransomware extension (.sorry / .srry) on shared-hosting volumes; unexpected cron jobs in /etc/cron.d/.

Data Sources: cPanel audit log (/var/cpanel/logs/), SSH auth log, shared-hosting volume file scan, cPanel API token audit, crontab review.

Detection Guidance: Patch cPanel immediately. Audit all API tokens and SSH keys added after 30 April -- revoke any unauthorised. Scan shared-hosting volumes for "Sorry" ransomware extension patterns. Review cron jobs for persistence.

TH-2026-W20-07 — APT28 NTLM Zero-Click (CVE-2026-32202)**P2 — HIGH: APT28 SAMA
expansion; KEV 12 May**

Hypothesis: APT28 is expanding to SA SAMA-regulated financial institutions (Fyntralink 7 May). CVE-2026-32202 allows NTLM hash capture when a user views a malicious .lnk or .library-ms file in Windows Explorer -- no click required. Outbound SMB/WebDAV and NTLM auth to non-corporate IPs = active exploitation indicators.

MITRE ATT&CK: T1187 (Forced Authentication), T1557 (Adversary-in-the-Middle), T1071 (Application Layer Protocol).

IOCs: Inbound .lnk / .library-ms files in email attachments or document-share repos; outbound SMB (445/139) or WebDAV to non-corporate IPs; Sysmon EID 11 for .lnk in user-writable paths with anomalous targets; unpatched Windows without April 2026 Patch Tuesday.

Data Sources: Email security gateway (attachment hashes), perimeter NetFlow (outbound 445/139), Sysmon EID 3 and 11, Windows Security log EID 4624/4625, EDR file-write telemetry.

Detection Guidance: Apply April 2026 Patch Tuesday by 12 May. Block outbound 445/139 at perimeter. Block .lnk and .library-ms email attachments at gateway. Hunt for outbound NTLM auth to non-corporate IPs.

TH-2026-W20-08 — Glowworm / APT41 ToolShell Hunt (SA gov-adjacent)

P3 — MONITOR: African gov-adjacent SA orgs at secondary risk

Hypothesis: Glowworm (APT41-linked) is confirmed compromising African government departments. SA organisations with African government MOUs or data-sharing arrangements are at secondary risk via trusted-network pivoting. ToolShell IOC indicators in SharePoint/IIS logs = active exploitation evidence.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1505.003 (Server Software Component: Web Shell), T1059 (Command Scripting).

IOCs: Zingdoor, ShadowPad, KrustyLoader hashes/domains/IPs (documented in research files); SharePoint CVE-2025-53770 exploit attempts; unexpected ASPX files under SharePoint web roots; outbound C2 to Glowworm-attributed infrastructure.

Data Sources: IIS logs on SharePoint servers, SharePoint ULS logs, EDR on SharePoint hosts, perimeter NetFlow, threat intel feeds (Glowworm IOC list).

Detection Guidance: Run Glowworm IOC list against all perimeter logs and EDR telemetry. Hunt for unexpected .aspx files under SharePoint web roots. Review outbound connections from SharePoint servers to unrecognised external IPs.

Hunt Mission Summary Checklist — W20

Hunt ID	Hypothesis (Short)	Priority	Key Data Sources	Status
TH-2026-W20-01	Standard Bank credential reuse hunt	P1 — CRITICAL	Azure AD/Okta, SIEM, dark web	Not Started
TH-2026-W20-02	Canvas API token reset (5 SA tertiary, 12 May)	P1 — CRITICAL	Canvas audit, OAuth, SSO federation	Not Started
TH-2026-W20-03	Municipal Wi-Fi segmentation review (Ekurhuleni)	P1 — CRITICAL	Network/wireless logs, billing audit	Not Started
TH-2026-W20-04	PAN-OS Captive Portal RCE (CVE-2026-0300)	P1 — CRITICAL	PAN-OS log, NetFlow, EDR	Not Started
TH-2026-W20-05	Ivanti EPMM auth bypass (CVE-2026-6973)	P2 — HIGH	EPMM audit log, MDM enrolments	Not Started
TH-2026-W20-06	cPanel SA hosting-provider wave (CVE-2026-41940)	P2 — HIGH	cPanel audit, SSH log, file scan	Not Started
TH-2026-W20-07	APT28 NTLM zero-click (CVE-2026-32202)	P2 — HIGH	Email gw, NetFlow 445/139, Sysmon	Not Started
TH-2026-W20-08	Glowworm / APT41 ToolShell (African gov-adjacent)	P3 — MONITOR	IIS/SharePoint logs, EDR, threat intel	Not Started

IOC Master Table — W20

Indicator	Type	Attribution	Hunt ID
Standard Bank .za / standardbank.* email domains (leaked)	Email pattern	PrinzEugen / ROOTBOY post-indexing credential reuse	TH-2026-W20-01
standardbank / liberty / stanbic lookalike domains	Domain pattern	Post-breach phishing (monitor only)	TH-2026-W20-01
Canvas /api/v1/users/* anomalous access	API endpoint	ShinyHunters Canvas mega-breach (12 May deadline)	TH-2026-W20-02
Canvas admin/integration API tokens (compromised)	Token	ShinyHunters Canvas; 5 SA institutions	TH-2026-W20-02
ARP/DHCP anomalies on billing-adjacent wireless segments	Network behaviour	Ekurhuleni-model Wi-Fi billing fraud	TH-2026-W20-03
CVE-2026-0300 (PAN-OS Captive Portal RCE)	CVE	State-sponsored; exploitation since 16 April	TH-2026-W20-04
Unexpected /api/?type=op&cmd;=... POSTs on PAN-OS	URI pattern	PAN-OS RCE exploitation indicator	TH-2026-W20-04
CVE-2026-6973 (Ivanti EPMM Auth Bypass)	CVE	Ivanti EPMM; KEV 10 May	TH-2026-W20-05
cPanel API tokens created after 30 April	Token anomaly	cPanel CVE-2026-41940 SA wave	TH-2026-W20-06
"Sorry" ransomware extension (.sorry/.srry) on hosting volumes	File extension	SA hosting-provider "Sorry" ransomware wave	TH-2026-W20-06
CVE-2026-32202 (Windows Shell NTLM zero-click)	CVE	APT28 SAMA expansion; KEV 12 May	TH-2026-W20-07
.lnk / .library-ms email attachments	File type	APT28 NTLM zero-click delivery vector	TH-2026-W20-07
Zingdoor / ShadowPad / KrustyLoader hashes (Glowworm)	File hash	Glowworm/APT41 ToolShell campaign	TH-2026-W20-08
UnDefend.exe / FunnyApp.exe / RedSun.exe	Filename	MS Defender zero-day chain (still unpatched)	N/A — Patch Tuesday 12 May
CVE-2026-42208 (LiteLLM RCE)	CVE	BerriAI LiteLLM; KEV 11 May	N/A — Patch

11. RECOMMENDATIONS

Immediate (This Week — Priority P1)

- **1. Patch PAN-OS CVE-2026-0300 (deadline today, 9 May):** Captive Portal RCE in Palo Alto PAN-OS (CVSS 9.3); state-sponsored exploitation confirmed since 16 April. Restrict Captive Portal to management-only IMMEDIATELY; patch by 9 May. Hunt for management-plane HTTPS egress and unexpected API POSTs.
- **2. Patch Ivanti EPMM CVE-2026-6973 (deadline 10 May):** Auth bypass in Ivanti EPMM (CVSS 7.2). Patch by 10 May. Audit all admin-role grants on EPMM for last 30 days. Restrict admin interface to VPN/OOB.
- **3. Microsoft Patch Tuesday 12 May — pre-stage testing NOW:** Expected to patch Defender RedSun + UnDefend (6+ weeks unpatched). Also covers ConnectWise ScreenConnect and Windows Shell NTLM KEV deadlines. Pre-stage testing across all Windows estates today.
- **4. Force credential rotation for any user matching Standard Bank dump:** PrinzEugen formally indexed Standard Bank on 4 May. Pull .za / standardbank.* email domains from leaked dataset; cross-reference IdP/O365 logs; force resets for any matching account. Alert on successful auth from non-corporate IP.
- **5. Reset Canvas/Instructure API tokens for Wits, Stadio, Milpark, Invictus, SPARK Schools:** ShinyHunters Canvas 12 May leak deadline. Reset ALL admin and integration API tokens. Rotate SSO

secrets. Audit /api/v1/users/* access patterns. Prepare student breach notification packs.

- **6. Restrict PAN-OS Captive Portal to management-only (architectural control):** Separate from patching — architectural isolation of Captive Portal access reduces exploit surface regardless of patch status.
- **7. Audit municipal Wi-Fi/billing segmentation (Ekurhuleni-style attack vector):** Any SA municipality with Wi-Fi networks routing to billing/licensing/revenue systems should treat this as a P1 architecture gap. Isolate billing systems from wireless networks.

Short-Term (Next 30 Days)

- Defender RedSun/UnDefend — post-Patch-Tuesday deployment: once Patch Tuesday 12 May ships the fix, deploy immediately across all Windows estates. Monitor for Patch Tuesday coverage confirmation. Deploy compensating EDR rules until patched.
- Verizon DBIR 2026 SA Webinar 19 May — schedule for SOC team: credentials at R100/set, 90% of SA breaches with identity weakness, 30% third-party involvement. Board-level framing tool.
- NIS2 first audit prep (deadline 30 June) for any SA org with EU operations: 7 weeks away. Gap assessment against NIS2 requirements for Essential and Important entities.
- SA tertiary-education sector data-breach communications playbook: 5 institutions confirmed in Canvas dump; develop student-data-subject notification templates and POPIA s.22 filing workflow for post-12 May disclosure.
- cPanel hardening across SA hosting estate; SOHO/Wi-Fi network segmentation audit: post-wave hardening for all SA MSPs and hosting providers. Ekurhuleni model triggers municipal-sector Wi-Fi review.
- Review IR enforcement-trajectory implications for own POPIA breach-notification readiness: IR APP scale-up, mandatory e-portal, 4 active enforcement matters, Blouberg High Court precedent.
- SAMA bank-sector APT28 watch: SA banks extend IOC coverage (Fyntralink feeds, CVE-2026-32202 indicators). Apply April 2026 Patch Tuesday by 12 May.

Strategic (Next Quarter)

- Identity-first defence — 90% of SA breaches now have an identity weakness (DBIR 2026). MFA maturity, IdP hardening, conditional access, and privileged-account management are the highest-leverage controls. Credential prices at R100/set on dark web make identity the attacker's cheapest entry point.
- Supply-chain and third-party risk programme — DBIR 2026 says third-party involvement doubled to 30% of breaches. The CGCSA/Stormous incident (GSI SharePoint, Unilever/Nestlé/L'Oréal partner data) and the Canvas/Instructure mega-breach (8,809 institutions) exemplify the supply-chain blast radius. Vendor risk programme review is urgent.
- Municipal-sector cyber-fraud architecture review — the Ekurhuleni model (multi-year Wi-Fi-enabled billing fraud) is a systemic gap. Engage SALGA/SITA for sector-wide architecture guidance. Billing/licensing systems must be isolated from wireless networks by design.
- EU AI Act readiness for SA AI/tech exporters (2 August 2026): Annex III high-risk AI systems must have full compliance frameworks operational. Start gap assessment now.

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. ransomware.live — South Africa Recent Victims — <https://www.ransomware.live/recentvictims>
2. Werksmans — IR Annual Performance Plan 2025/26 coverage (5 May 2026) — <https://www.werksmans.com/>

3. IT-Online — Surfshark Q1 SA data (7 May 2026) — <https://it-online.co.za/>
4. ITWeb — DBIR 2026 SA commentary — <https://www.itweb.co.za/>
5. Wits University — SA AI policy analysis (4 May 2026) — <https://www.wits.ac.za/>
6. The Common Sense — AI policy commentary (9 May 2026) — <https://thecommonsense.co.za/>
7. HookPhish — Stormous ransomware hits CGCSA (3 May 2026) — <https://www.hookphish.com/blog/ransomware-group-stormous-hits-cgcsa-co-za/>
8. RedPacket Security — Stormous victim CGCSA (3 May 2026) — <https://www.redpacketsecurity.com/stormous-ransomware-victim-cgcsa-co-za/>
9. Lyrie.ai — Stormous research (3 May 2026) — <https://lyrie.ai/research/research/2026-05-03-stormous-fanasa-mexican-supply-chain>
10. Parliament of South Africa — SCOPA hearing records — <https://www.parliament.gov.za/>
11. CISA — Known Exploited Vulnerabilities Catalog — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
12. Verizon DBIR 2026 — Data Breach Investigations Report — <https://www.verizon.com/business/resources/reports/dbir/>
13. Information Regulator South Africa — Media Statements — <https://inforegulator.org.za/media-statements/>
14. BlackFog — April 2026 State of Ransomware Report — <https://www.blackfog.com/>
15. Fyntralink — Threat Intelligence (APT28, MuddyWater) — <https://www.fyntralink.com/>
16. ITWeb — Standard Bank data breach coverage (W20) — <https://www.itweb.co.za/>
17. Daily Maverick — SA cyber landscape W20 — <https://www.dailymaverick.co.za/>
18. TechCentral — SA cyber incident coverage — <https://techcentral.co.za/>
19. ITWeb — SAPS medical aid scheme probe (17 Apr) — <https://www.itweb.co.za/article/saps-medical-aid-scheme-probes-potential-data-breach/P3gQ2MGA5VNvNRD1>
20. allAfrica — Polmed breach coverage — <https://allafrica.com/stories/202604160282.html>
21. ITWeb — Adumo payment tech exposed (17 Apr) — <https://www.itweb.co.za/article/adumo-payment-tech-exposed-hackers-offer-data-for-7-000/KWEBb7yLwdAvmRjO>
22. LaunchBase Africa — Adumo source code leak investigation — <https://launchbaseafrica.com/2026/04/17/south-african-fintech-adumo-investigates-alleged-source-code-leak/>
23. Microsoft MSRC — Security Update Guide — <https://msrc.microsoft.com/update-guide/>
24. Industrial Cyber — GuidePoint GRIT Q1 2026 Ransomware Report — <https://industrialcyber.co/reports/ransomware-reaches-elevated-new-normal-as-attack-volumes-hold-steady-into-2026-reshape-baseline-risk-expectations/>
25. Recorded Future — RedMike/Salt Typhoon SA telecom confirmed — <https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices>
26. TechCrunch — Salt Typhoon SA telecom confirmed (9 Mar 2026) — <https://techcrunch.com/2026/03/09/salt-typhoon-china-who-has-been-hacked-global-telecom-giants/>
27. BleepingComputer — Microsoft Defender RedSun / UnDefend — <https://www.bleepingcomputer.com/>
28. Mayet Law — POPIA enforcement 2026 developments — <https://mayet.law/popia-enforcement-in-south-africa-key-2026-developments-and-what-businesses-must-do-now/>
29. ITLawCo — Information Regulator 2026/27 Annual Performance Plan — <https://itlawco.com/information-regulator-2026-27-annual-performance-plan/>
30. Check Point Research — Q1 2026 attack volume baseline — <https://research.checkpoint.com/>
31. SABRIC — Annual Crime Statistics Report 2024 — <https://www.sabric.co.za/wp-content/uploads/2025/09/CRIME-STATISTICS-REPORT-2024.pdf>
32. 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/>
33. Standard Bank — Official data incident updates (newsroom) — <https://www.standardbank.co.za/southafrica/news-and-media/newsroom>
34. Inclusive Society Institute — SA Cybersecurity Blueprint — <https://www.inclusivesociety.org.za/post/securing-the-future-blueprint-for-solving-south-africa-s-cybersecurity-crisis-in-the-age-of-ai>
35. D3 Security — NIS2 SOC Audit Readiness 2026 — <https://d3security.com/blog/nis2-soc-audit-readiness-2026/>
36. Xcitium ThreatLabs — NightSpire Ransomware Profile — <https://threatlabsnews.xcitium.com/blog/nightspire-ransomware-emerging-double-extortion-threat/>
37. GuidePoint Security — GRIT Q1 2026 Ransomware Report — <https://www.guidepointsecurity.com/>
38. ZeroFox — ShinyHunters TTPs (Okta FastPass) — <https://www.zerofox.com/>
39. BleepingComputer — ConnectWise ScreenConnect Medusa/Storm-1175 — <https://www.bleepingcomputer.com/>
40. Techmoonshot — SA cyber intelligence coverage — <https://techmoonshot.com/>
41. Cape Town ETC — SA breach reporting W20 — <https://capetownetc.com/>
42. CentralNews — SA breach coverage W20 — <https://centralnews.co.za/>
43. UpGuard — SA Data Breach tracking 2026 — <https://www.upguard.com/>
44. DataBreaches.net — SA Government breach analysis — <https://databreaches.net/>
45. Censys — Salt Typhoon persistent threat tracking — <https://censys.com/blog/the-persistent-threat-of-salt-typhoon-tracking-exposures-of-potentially-targeted-devices/>

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-W20