



SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief -- Week 28 | 28 June - 5 July 2026

THREAT LEVEL: HIGH

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W28 | Classification: TLP:WHITE

Published Monday 6 July 2026

(c) 2026 Digital Progression | dpcyber.co.za

TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard
- 2. Threat Landscape Heatmap
- 3. Top SA Incidents (W28)
- 4. Threat Actors
- 5. Critical Vulnerabilities & CISA KEV
- 6. Ransomware Landscape
- 7. OSINT Exposure & Attack Surface
- 8. Regulatory & Policy
- 9. Weekly Threat Hunt & IOCs
- 10. Strategic Recommendations
- 11. Threat Level Assessment
- 12. OSINT Sources Consulted

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH (unchanged, 8th consecutive week) -- Week 28 (28 June - 5 July 2026)

Story 1 -- Pick n Pay Breach Escalates Into Banking-Sector Remediation as Capitec Orders Card Replacements: On 2 July Capitec began notifying a subset of clients that their card details were exposed in the breach of Pick n Pay's legacy Bottles / Asap! delivery platform, advising card replacement.¹ Pick n Pay has confirmed the 2022-era database held names, emails, phone numbers, delivery addresses, encrypted passwords, card type, last-four digits and expiry dates; the retailer states full card numbers and valid CVVs were not stored, disputing the seller's Breach Forums claim.³⁴ Reported Capitec specifics -- waived replacement fees and dataset pricing of ~R37,600 (R163,500 exclusive) -- rest on a single outlet.¹² Expect card-not-present fraud against affected customers through July. CONFIRMED (core); PROBABLE (pricing/fee detail).

Story 2 -- Mystery Medical-Aid Breach Identified: Profmed via PPS Healthcare Administrators, With a Five-Scheme Exposure Surface: The unnamed ~200,000-member medical aid breach flagged in W27 is Profmed, administered by PPSHA.⁵⁶ Members were notified on 25 June that an unauthorised party used compromised credentials to access third-party service-provider systems, potentially removing names, ID numbers, contact details, membership numbers and scheme options; PPSHA says its own systems were unaffected and the Information Regulator is being notified under POPIA s.22.⁵ PPSHA's own client listing confirms five administered schemes -- Profmed, KeyHealth, SEDMED, De Beers Benefit Society and the SANDF Regular Force Medical Continuation Fund -- so scope expansion is credible, with the defence-adjacent RFMCF the most sensitive extension.⁷ Separately, hotel-PMS provider Hospitality Technology International (NebulaPMS) lost ~2 million guest records in a March intrusion.⁸ PROBABLE (breach detail); CONFIRMED (administrator surface).

Story 3 -- Patch Pressure Rotates: Two Short-Fuse KEV Adds, BlueHammer Goes Ransomware, and Oracle EBS Exploited Pre-KEV: CISA added SimpleHelp RMM CVE-2026-48558 (KEV 29 June, due 7 July, exploited to chain the TaskWeaver loader into Djinn Stealer through MSP deployments, with instructed forensic triage)¹⁴ and SharePoint CVE-2026-45659 (KEV 1 July, deserialization RCE, CVSS 8.8, deadline 4 July -- a three-day fuse, now lapsed).¹³ CISA's 29 June update flagged Defender LPE CVE-2026-33825 (BlueHammer) as ransomware-exploited.¹⁵ The most dangerous item is NOT in the KEV: Oracle EBS Payments CVE-2026-46817 (CVSS 9.8, unauthenticated) exploited since 27 June,¹⁶ ~950 exposed instances per Shadowserver,¹⁷ while Nissan's 29 June disclosure confirmed hundreds of companies may have lost personnel records via PeopleSoft CVE-2026-35273.¹⁸ SA ransomware.live moved to 109 -- a restored listing, not a new victim.¹² FICA cross-border cash conveyance went live 1 July (R100,000 threshold).²³ CONFIRMED.

KPI Dashboard

Metric	Current (W28)	Prior (W27)	Change	Direction
SA threat level	HIGH	HIGH	Unchanged (8th consecutive week)	FLAT
SA ransomware.live victims (total)	109 (verified 5 Jul)	108	Net +1 (restored listing; no new SA postings)	UP
New SA RW listings this week (ransomware.live)	0 confirmed	0 (W26)	FLAT	FLAT
#OpSouthAfrica hacktivism (Nullsec / Anonymous Nigeria)	30 Jun flashpoint passed; no cyber escalation observed in open sources	DCS + Ephraim Mogale breached; 30 Jun flashpoint	DE-ESCALATING (open-source view)	DOWN
Pick n Pay Asap!/Bottles breach -- banking impact	Capitec card replacements from 2 Jul; CVV claim disputed	N/A	NEW W28	UP
SA medical-aid breach attribution	Profmed via PPSHA third party; five schemes administered incl. SANDF RFMCF	Unnamed, ~200,000 members claimed	IDENTIFIED	UP
Prinz Eugen / ROOTBOY -- Standard Bank leak	No new public development 28 Jun - 5 Jul; listing unchanged	Publicly attributed; 100,000 rows/day claimed	MONITORING	FLAT
New CISA KEV additions (28 Jun - 5 Jul)	2 (SimpleHelp due 7 Jul; SharePoint deadline lapsed 4 Jul) + BlueHammer ransomware flag	6 (W27)	FEWER ADDS, SHORTER FUSES	DOWN
Oracle EBS Payments CVE-2026-46817	Exploited ITW since 27 Jun; ~950 exposed instances; NOT yet in KEV	N/A	NEW W28	UP
IR s.59 notices -- TransUnion SA + Experian SA (per W27)	Responses due ~6 Jul; no public development this week	Served 26 Jun	PENDING	FLAT
FICA cross-border cash regime (CCR) via SARS	LIVE 1 Jul; R100,000 threshold; no first-week seizures reported	Go-live pending	LIVE	UP
AVBOB Mutual Assurance (carryover)	~5 weeks post-incident; no leak-site claim or attribution	Partial-manual mode 20+ days	UNDETERMINED	FLAT

W28 KEY FRAMING: W28 is a consolidation week: the hacktivist flashpoint passed without observed escalation and no new SA victim appeared on leak sites, but the week's real signal is downstream impact -- a bank replacing cards because of a retailer's legacy app, a medical-aid breach resolving to a third-party administrator with a five-scheme blast radius, and Oracle telling Nissan that hundreds of

companies may have lost personnel data. The dominant operational drivers are two short-fuse KEV deadlines (SharePoint lapsed 4 July, SimpleHelp due 7 July), active pre-KEV exploitation of Oracle EBS Payments, and the FICA cash-conveyance regime now live at the borders.

TOP 3 ACTIONS THIS WEEK

1. CLEAR THE TWO SHORT-FUSE KEVs -- SHAREPOINT CVE-2026-45659 (DEADLINE LAPSED 4 JUL) + SIMPLEHELP CVE-2026-48558 (DUE 7 JUL):

Apply Microsoft's May 2026 SharePoint fix immediately if not already done -- any authenticated user with Site Member permissions can achieve RCE, and the CISA deadline has already passed. For SimpleHelp, patch AND perform forensic triage per CISA's instruction: the flaw has been exploited since ~29 June to deploy the TaskWeaver loader and Djinn Stealer, and stolen cloud/SCM/SSH/AI-assistant tokens remain valid after patching. MSPs and their customers must rotate credentials issued through SimpleHelp-managed environments.¹³¹⁴

2. TREAT INTERNET-FACING ORACLE E-BUSINESS SUITE AS UNDER ATTACK: CVE-2026-46817 (CVSS

9.8, unauthenticated file read via the /OA_HTML/ibytransmit Payments endpoint, reaching DB credentials and payment API keys) has been exploited in the wild since 27 June and was still not KEV-listed as of 5 July -- do not wait for the catalog. Apply the May 2026 CPU, hunt for POST requests to /OA_HTML/ibytransmit, and if unpatched and exposed, treat as potentially compromised. PeopleSoft CVE-2026-35273 remediation is now 20 days overdue, with Nissan the first named large victim.¹⁶¹⁷¹⁸

3. CARD-FRAUD AND CREDENTIAL-EXPOSURE RESPONSE -- PICK N PAY / CAPITEC AND PPSHA-ADMINISTERED SCHEMES:

Banks and issuers should tighten card-not-present fraud rules for customers flagged in the Pick n Pay dataset; affected consumers should replace cards and reset any reused passwords. Members of the five PPSHA-administered schemes (Profmed, KeyHealth, SEDMED, De Beers Benefit Society, SANDF RFMCF) should be treated as at elevated phishing and identity-fraud risk; scheme principals should demand written scope confirmation from PPSHA. Brief staff on tax-season fake-eFiling lures now circulating.¹⁵⁷¹⁰

1. MyBroadband -- Capitec tells specific customers to replace bank cards following Pick n Pay data breach (2 July 2026) -- <https://mybroadband.co.za/news/security/656369-capitec-tells-specific-customers-to-replace-bank-cards-following-pick-n-pay-data-breach.html>
2. Data Breaches Digest -- Week 27 2026, covering 29 June - 5 July (fetched 5 July 2026) -- <https://www.dbdigest.com/2026/06/data-breaches-digest-week-27-2026.html>
3. News24 -- Used Pick n Pay's old delivery service? Your address and card info may have been leaked (28 May 2026) -- <https://www.news24.com/business/consumer-lookout/used-pick-n-pays-old-delivery-service-your-address-and-card-info-may-have-been-leaked-20260528-0993>
4. TechCabal -- Pick n Pay breach puts South Africa's retail cybersecurity under scrutiny (1 June 2026) -- <https://techcabal.com/2026/06/01/pick-n-pay-cyberbreach/>
5. MyBroadband -- Top medical aid in South Africa with 200,000 clients hit by data breach (25 June 2026) -- <https://mybroadband.co.za/news/security/655653-top-medical-aid-in-south-africa-with-200000-clients-hit-by-data-breach.html>
6. Data Breaches Digest -- Week 26 2026 (fetched 5 July 2026) -- <https://www.dbdigest.com/2026/06/data-breaches-digest-week-26-2026.html>
7. PPS Healthcare Administrators -- Our Clients (fetched 5 July 2026) -- <https://ppsha.co.za/our-clients/>
8. Cybernews -- Claude AI exploited to breach hotel booking platforms (23 June 2026) -- <https://cybernews.com/security/claude-ai-exploited-breach-hotel-booking-platforms/>
10. Everywhere VC -- Orca Fraud warns of SARS scam surge (1 June 2026) -- <https://ideas.everywhere.vc/p/orca-fraud-warns-of-sars-scam-surge>
12. Ransomware.live -- South Africa country tracking and map (verified 5 July 2026; 109 cumulative) -- <https://ransomware.live/map/ZA>
13. The Hacker News -- SharePoint RCE CVE-2026-45659 Added to CISA KEV After Active Exploitation (2 July 2026) -- <https://thehackernews.com/2026/07/sharepoint-rce-cve-2026-45659-added-to.html>

14. Help Net Security -- SimpleHelp vulnerability exploited, CVE-2026-48558 (30 June 2026) -- <https://www.helpnetsecurity.com/2026/06/30/simplehelp-vulnerability-exploited-cve-2026-48558/>

15. BleepingComputer -- CISA: Windows BlueHammer flaw now exploited by ransomware gangs (30 June 2026) -- <https://www.bleepingcomputer.com/news/security/cisa-windows-bluehammer-flaw-now-exploited-by-ransomware-gangs/>

16. Help Net Security -- Oracle Payments CVE-2026-46817 exploitation observed (30 June 2026) -- <https://www.helpnetsecurity.com/2026/06/30/oracle-payments-cve-2026-46817-exploitation/>

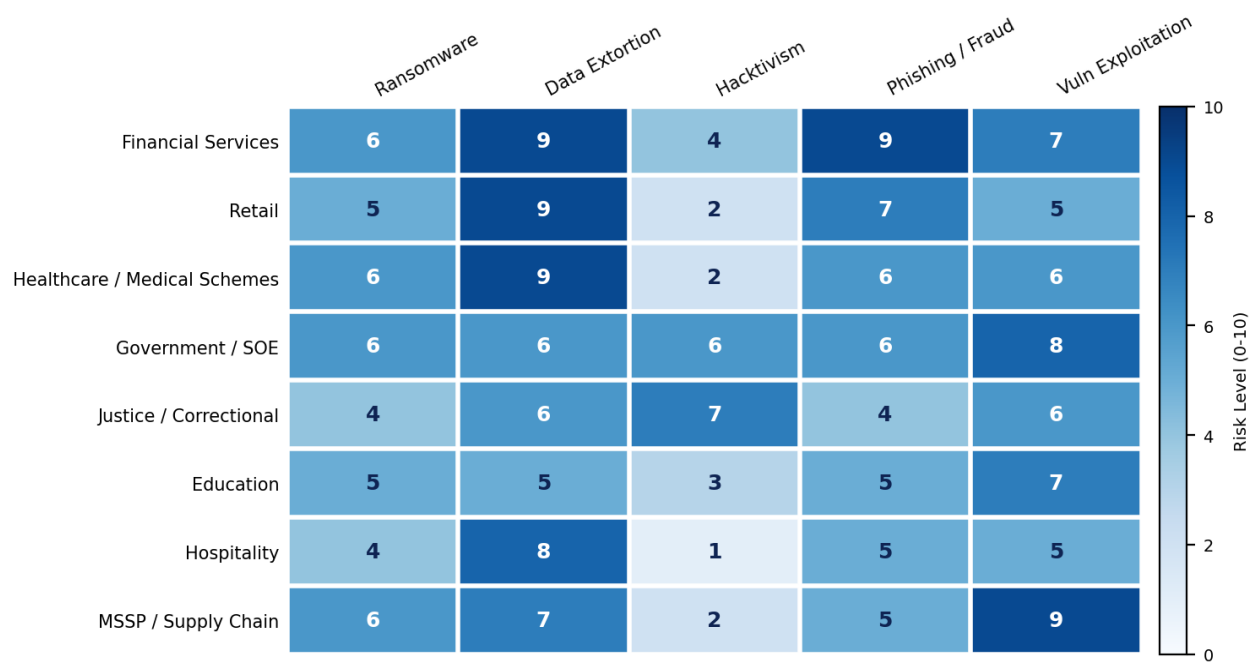
17. BleepingComputer -- Over 900 Oracle E-Business instances exposed to ongoing attacks (1 July 2026) -- <https://www.bleepingcomputer.com/news/security/over-900-oracle-e-business-instances-exposed-to-ongoing-attacks/>

18. BleepingComputer -- Nissan discloses employee data breach linked to Oracle zero-day attacks (29 June 2026) -- <https://www.bleepingcomputer.com/news/security/nissan-discloses-employee-data-breach-linked-to-oracle-zero-day-attacks/>

23. Engineering News -- Domestic, foreign travellers must now declare cash of more than R100 000: FIC (1 July 2026) -- <https://www.engineeringnews.co.za/article/domestic-foreign-travellers-must-now-declare-cash-of-more-than-r100-000-fic-2026-07-01>

2. THREAT LANDSCAPE HEATMAP

SA THREAT LANDSCAPE HEATMAP | W28 (28 June - 5 July 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.

Financial Services holds 9 on Data Extortion (the unresolved Standard Bank / Liberty leak, the credit-bureau enforcement matter and Pick n Pay card exposure) and 9 on Phishing/Fraud (Capitec card replacements, the R1.07m vishing sentencing at Mthatha and the tax-season fake-eFiling wave).¹⁹¹⁰ **Healthcare/Medical Schemes** sits at 9 on Data Extortion following the Profmed / PPSHA identification with its five-scheme exposure surface.⁵⁷ **Retail** registers 9 on Data Extortion (Pick n Pay dataset actively marketed).¹ **MSSP/Supply Chain** peaks at 9 on Vulnerability Exploitation (SimpleHelp RMM KEV with Djinn Stealer targeting MSP deployments).¹⁴ **Government/SOE** and **Justice/Correctional** ease from last week's hacktivism peaks (10 and 9) to 6 and 7 respectively: the 30 June flashpoint passed without observed

escalation, but the campaign has not been renounced and DCS breach data remains in actor hands. **Education** carries 7 on Vulnerability Exploitation (the PeopleSoft campaign primarily hit education-sector organisations).¹⁸ **Hospitality** holds 8 on Data Extortion (NebulaPMS ~2M guest records).⁸

9. NovaNews / PE Express -- Two sentenced in R1.07m Standard Bank impersonation fraud case (2 July 2026) -- <https://novanews.co.za/peexpress/two-sentenced-in-r1-07m-standard-bank-impersonation-fraud-case/>

29. GroundUp -- Here's how insecure government's websites are (11 June 2026; standing SA exposure baseline) -- <https://groundup.org.za/article/heres-how-insecure-governments-websites/>

3. TOP SA INCIDENTS (W28)

Week 28 (28 June – 5 July 2026): the SA ransomware.live tally moved to 109 (net +1 versus W27 from a restored listing; no new SA leak-site postings in the window; verified 5 July).¹² The week's incident picture is dominated by downstream consequences of earlier breaches rather than fresh compromises. Each incident carries a confidence rating: CONFIRMED (victim/regulator acknowledgment or two independent sources), PROBABLE (single credible source), CLAIMED (threat-actor assertion only).

3.1 INC-2026-W28-01 -- Pick n Pay Asap!/Bottles Breach: Capitec Card Replacements [CONFIRMED core; PROBABLE detail]

Sector	Retail / Financial Services (downstream banking remediation)
Date	Capitec notifications from 2 July 2026; PnP customer notifications began 30 May
Confirmed	2022-era Bottles/Asap! database: names, emails, phone numbers, delivery addresses, encrypted passwords, card type, last-four digits, expiry dates; Information Regulator notified; retailer disputes the seller's CVV claim
Reported (single outlet)	Capitec fee waiver; dataset offered for ~R37,600 or R163,500 exclusive on Breach Forums
Significance	Clearest recent example of a retail-app compromise propagating into bank-side remediation
Confidence	CONFIRMED (core incident); PROBABLE (pricing and fee-waiver detail)

Capitec notified a subset of clients on 2 July that card details were exposed in the breach of Pick n Pay's legacy Bottles/Asap! delivery platform and advised replacement.¹ The underlying breach is well corroborated: Pick n Pay began notifying users of the discontinued delivery service on 30 May, confirmed the exposed field set, stated that full card numbers and CVVs were not stored, and notified the Information Regulator.³⁴ The Capitec notification specifics trace to a single outlet, indexed in the Data Breaches Digest under 2 July.¹² Expect card-not-present fraud attempts and convincing PnP/Capitec-branded phishing against affected customers through July.

3.2 INC-2026-W28-02 -- Profmed / PPS Healthcare Administrators Breach Identified [PROBABLE detail; CONFIRMED surface]

Sector	Healthcare / Medical schemes (third-party administrator ecosystem)
--------	--

Date	Member notification 25 June 2026; identified in coverage during W28
Vector	Compromised login credentials used against third-party service-provider systems; PPSHA core systems reported unaffected
Data at risk	Names, ID numbers, contact details, membership numbers, scheme options (~200,000 members claimed)
Administrator surface	PPSHA administers five schemes: Profmed, KeyHealth, SEDMED, De Beers Benefit Society, SANDF Regular Force Medical Continuation Fund
Confidence	PROBABLE (breach specifics, single fetchable source chain); CONFIRMED (administrator relationships, PPSHA's own client listing)

The W27 unnamed SA medical aid item resolves to Profmed, whose administrator PPSHA notified members on 25 June that an unauthorised party used compromised credentials to access third-party service-provider systems; the Information Regulator is being notified under POPIA s.22.⁵⁶ What is independently confirmed from PPSHA's own client listing is the five-scheme administration surface -- Profmed (South Africa's largest restricted scheme for graduate professionals), KeyHealth, SEDMED, the De Beers Benefit Society and the defence-adjacent SANDF RFMCF -- making scope expansion the primary watch item.⁷

3.3 INC-2026-W28-03 -- Hospitality Technology International / NebulaPMS: ~2M Hotel Guest Records [CONFIRMED]

Sector	Hospitality / Travel technology
Date	March 2026 intrusion; actor server found 16 April; SA media disclosure 26 June
Scale	~2 million guest records (names, emails, phone numbers, check-in/out dates, hotel names); ~2.1M unique emails across four victim booking platforms
Vector	Russian-speaking actor driving the HexStrike AI offensive framework with a mainstream AI assistant whose guardrails were bypassed under a penetration-testing pretext
Confidence	CONFIRMED (primary research; discovery via the actor's own exposed server)

The South African hotel property-management provider's NebulaPMS platform lost approximately two million guest records in a March 2026 intrusion. The theft was discovered via the actor's own exposed server, and the research identified three further victim booking platforms.⁸ Disclosure reached SA media on 26 June, at the edge of the W27 window; SA hotel groups using NebulaPMS should assume guest PII exposure and prepare guest notifications.

3.4 INC-2026-W28-04 -- Information Regulator Enforcement Notice: Central Johannesburg TVET College [CONFIRMED]

Sector	Education / Public sector (POPIA enforcement)
Date	Enforcement notice analysed in coverage published 29 June 2026
Findings	POPIA s.22 security compromise (credential-verification reports forwarded to unauthorised internal staff); s.8 (no information officer registered); s.19 (inadequate safeguards); s.15 (incompatible further processing)

Precedent	A misdirected internal email can constitute a reportable breach
Confidence	CONFIRMED

An enforcement notice against Central Johannesburg TVET College holds that employees' credential-verification reports forwarded to unauthorised internal staff constituted a POPIA s.22 security compromise, alongside findings under s.8, s.19 and s.15.¹¹ Information officers should update incident-classification playbooks accordingly: internal misdirection is now squarely within reportable-compromise territory.

3.5 INC-2026-W28-05 -- Vishing Prosecution: R1.07m Theft via Standard Bank Impersonation [CONFIRMED]

Sector	Financial Services / Consumer fraud (prosecution)
Date	Sentenced 1 July 2026, Mthatha Specialised Commercial Crimes Court
Amount	R1,070,749.85 stolen; R797,312 recovered via Hawks financial tracing
Outcome	Sibusiso Mabaso (34) and Lethulwazi Wandile Mnguni (33): five years' imprisonment wholly suspended for five years, plus compensation orders
Confidence	CONFIRMED (Hawks statement via fetched coverage)

The pair posed as Standard Bank fraud staff, extracted OTPs, instructed the victim to power off his phone for around two hours, stole R1,070,749.85 and laundered it through Hollywoodbets accounts.⁹ Note that the sentences were wholly suspended -- headlines saying the pair were jailed are inaccurate. A clean case study for consumer-awareness material: the bank will never ask for an OTP or for the phone to be switched off.

3.6 INC-2026-W28-06 -- Tax-Season Fraud Wave: Fake SARS eFiling Refund Sites [PROBABLE]

Sector	Consumer / SME finance
Date	Orca public warnings since 1 June 2026; further reporting dated 4 July
Method	Fake eFiling links via SMS and email -- penalty-threat, auto-assessment and refund-lure variants -- harvesting credentials and cloning cards through fake checkout pages
Unverified detail	Automated burst attacks cycling batches of stolen cards; fraud spiking before card expiry (single source)
Confidence	PROBABLE (single-source vendor telemetry; no SARS statement or named victim)

Anti-fraud firm Orca has been publicly warning since the start of tax season that criminals are exploiting it with fake SARS eFiling lures.¹⁰ Further reporting dated 4 July described automated card-testing bursts; those specifics could not be independently verified in the window. Finance teams should verify any SARS communication via the official app or portal, never SMS links.

Carryover Status (checked, no development as of 5 July)

#OpSouthAfrica (Nullsec Nigeria / Anonymous Nigeria): the 30 June flashpoint passed without observed cyber escalation; no new leaks, defacements or claims dated on or after 30 June were found in open sources through 5 July. Caveat: Telegram and dark-web channels were not directly observable, so absence of reporting is not proof of inactivity. **Standard Bank / Liberty (Prinz Eugen / ROOTBOY):** no new public development in the window; the ransomware.live listing is unchanged.¹² **AVBOB Mutual Assurance:** ~5 weeks post-incident, restoration presumed ongoing, still no leak-site claim or attribution. **SAPS Western Cape POPIA breach (3,000 officers' medical records):** no Information Regulator statement or investigation outcome published; the Regulator's media-statements page, checked 5 July, shows nothing newer than 2 June.³⁰ The Data Breaches Digest edition covering 29 June – 5 July lists exactly one SA item -- the Capitec/Pick n Pay story under 2 July -- corroborating a quiet week for new SA postings.²

11. DataBreaches.net -- ZA: Copying the wrong person on an email could be considered a data breach in South Africa (29 June 2026) --

<https://databreaches.net/2026/06/29/za-copying-the-wrong-person-on-an-email-could-be-considered-a-data-breach-in-south-africa/>

30. Information Regulator (South Africa) -- Media statements (checked 5 July 2026; most recent statement dated 2 June 2026) --

<https://inforegulator.org.za/media-statements>

4. THREAT ACTORS

4.1 Prinz Eugen / ROOTBOY -- Solo Data-Extortion Operator [CONFIRMED profile; CLAIMED leak cadence]

Go-based ransomware using ChaCha20-Poly1305 with Argon2id/HKDF key derivation; prioritises recently modified files; drops no ransom note on disk; persists via RemotePC RMM and a backdoor admin account; initial access via stolen RDP credentials. Standard Bank refused a 1 BTC demand; the leak site lists three victims with at least five known.²² The ROOTBOY operator attribution (aliases avtokz, GERMANIA) was established in Malwarebytes ThreatDown research carried in DP-CTI-2026-W27. Claims of escalating daily Standard Bank dumps (up to 50,000+ SQL rows/day from a ~1.2 TB dataset) circulate only in sources that could not be independently verified and remain CLAIMED. No new in-window development.

4.2 Nullsec Nigeria / Anonymous Nigeria (#OpSouthAfrica) [CONFIRMED campaign; de-escalating]

The xenophobia-motivated campaign that breached the Department of Correctional Services (~11 GB claimed) and Ephraim Mogale Local Municipality did not visibly escalate through its own 30 June deadline, and no new activity was indexed through 5 July. Exfiltrated DCS data remains in actor hands and the campaign has not been renounced; .gov.za and SOE defenders should treat this as dormant, not resolved.

4.3 ShinyHunters [CONFIRMED -- PeopleSoft campaign fallout]

Nissan Americas disclosed on 29 June that current and former employee data (including SSNs, banking and tax data across the US, Canada, Mexico and Brazil) was taken in the Oracle PeopleSoft CVE-2026-35273 zero-day campaign; Oracle told Nissan the campaign may have hit personnel records of hundreds of companies. ShinyHunters claims 300+ compromised PeopleSoft instances across 100+ organisations; Mandiant confirmed zero-day exploitation between 27 May and 9 June, primarily impacting education-sector organisations.¹⁸ No SA victims named yet -- SA universities and provincial governments running PeopleSoft remain the key exposure.

4.4 Storm-2603 / Warlock [PROBABLE context]

The SharePoint CVE-2026-45659 KEV addition is contextually linked in reporting to ongoing SharePoint-focused intrusion activity, including Microsoft's 22 June incident-response account of two unrelated intruders operating in parallel in a single network -- one attributed to Storm-2603, which deploys Warlock ransomware via on-premises SharePoint.¹³ Actor and goals for the KEV-listed exploitation remain officially unattributed.

4.5 Scattered Spider [CONFIRMED -- law enforcement]

Peter Stokes, 19, a dual US/Estonian citizen arrested in Finland in April, was extradited to the US in late June (DoJ complaint unsealed 30 June) over an \$8m extortion attempt against a luxury jewellery retailer; the DoJ ties the group to 100+ intrusions and over \$100m in ransom payments.²⁰ Continued pressure on the anglophone social-engineering ecosystem whose techniques (helpdesk impersonation, MFA fatigue) are regularly copied against SA targets.

4.6 Interpol-Impersonation Ransomware Crew [CONFIRMED research]

Bitdefender documented phishing from a fake Interpol Cybercrime Investigation Unit delivering simple ransomware via password-protected Proton Drive links with Tox-based negotiation, targeting small businesses across Europe, Asia, the Middle East and North America.²¹ SA is not named, but law-enforcement brand abuse translates directly to the SA SME threat model.

4.7 Black X [CONFIRMED -- carryover]

The 2 June ransomware.live listing of the African National Congress (attack estimated August 2025) remains the most recent new SA leak-site entry.¹² No in-window activity.

20. Infosecurity Magazine -- Scattered Spider member extradited to US (2 July 2026) --

<https://www.infosecurity-magazine.com/news/scattered-spider-member-extradited/>

21. Infosecurity Magazine -- Cybercriminals pose as Interpol to deliver ransomware (2 July 2026; Bitdefender research 1 July) --

<https://www.infosecurity-magazine.com/news/cybercriminals-pose-interpol/>

22. BleepingComputer -- New Prinz Eugen ransomware prioritizes recent files for encryption (20 June 2026; carryover technical profile) --

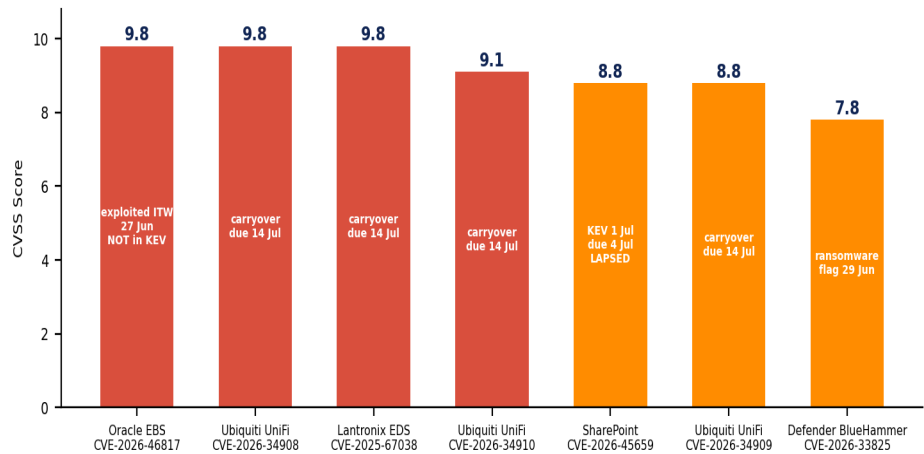
<https://www.bleepingcomputer.com/news/security/new-prinz-eugen-ransomware-prioritizes-recent-files-for-encryption/>

5. CRITICAL VULNERABILITIES & CISA KEV

Two new KEV entries landed in the window, both with unusually short remediation fuses, and CISA's 29 June update flagged an April entry as now exploited by ransomware operators.¹⁵ No further KEV additions were published between 2 and 5 July. The week's most dangerous item is arguably NOT in the KEV: Oracle E-Business Suite Payments CVE-2026-46817 (CVSS 9.8, unauthenticated file read reaching database credentials and payment API keys via /OA_HTML/ibytransmit, affecting EBS 12.2.3-12.2.15) has been exploited in the wild since 27 June against internet-facing instances,¹⁶ with Shadowserver tracking roughly 950 exposed EBS deployments globally as of 1 July.¹⁷ Note: CISA KEV facts this week are anchored to multiple independent fetched secondary sources quoting the CISA alerts; cisa.gov blocks direct automated retrieval from our fetch environment.¹³¹⁴

W28 KEV / Critical CVE Severity Overview -- (2 New KEV Adds 28 Jun - 5 Jul + Pre-KEV Oracle EBS + Carryovers)

W28 KEV / CRITICAL CVE SEVERITY | 28 June - 5 July 2026
2 new KEV entries (SimpleHelp CVE-2026-48558 unrated + SharePoint 8.8) + BlueHammer ransomware flag; Oracle EBS 9.8 exploited pre-KEV; SimpleHelp not charted (no CVSS assigned)



W28 CISA KEV / Critical CVE Tracking (new adds 28 June - 5 July + active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-48558	SimpleHelp RMM	n/r	Auth bypass (OIDC)	7 Jul 2026	KEV 29 Jun; exploited since ~29 Jun; TaskWeaver loader to Djinn Stealer via MSPs; CISA instructed forensic triage; stolen tokens survive patching
CVE-2026-45659	Microsoft SharePoint Server (SE, 2019, 2016)	8.8	Deserial RCE	4 Jul 2026 (LAPSED)	KEV 1 Jul; exploited ITW; Site Member is enough; apply May 2026 patch; hunt w3wp child processes
CVE-2026-33825	Microsoft Defender (BlueHammer)	7.8	LPE via SAM	7 May 2026 (LAPSED)	Flagged ransomware-exploited 29 Jun; public PoC since April; verify April patch fleet-wide
CVE-2026-46817	Oracle EBS Payments	9.8	Unauth file read	NOT IN KEV (5 Jul)	Exploited ITW since 27 Jun; ~950 exposed instances; /OA_HTML/ibytransmit; apply May 2026 CPU; treat exposed unpatched EBS as compromised

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-12569	PTC Windchill / FlexPLM	Critical	Unauth RCE	28 Jun 2026 (OV ERDUE +7)	KEV 25 Jun; JSP webshells actively deployed per PTC advisory IOCs; review /Windchill/servlet/; SA aerospace/mining/defence exposure
CVE-2026-20230	Cisco Unified Communications Manager	8.6	SSRF to RCE	28 Jun 2026 (OV ERDUE +7)	No new in-window reporting; apply hotfix; restrict WebDialer to internal
CVE-2026-35273	Oracle PeopleSoft	Critical	Zero-day RCE	15 Jun 2026 (OV ERDUE +20)	ShinyHunters campaign; Nissan disclosed 29 Jun; hundreds of companies may be affected; SA universities/provincial govts priority
CVE-2026-34908 /-09/-10	Ubiquiti UniFi OS (trio)	9.8 / 8.8 / 9.1	Auth bypass / priv esc / cmd inject	14 Jul 2026	Added 23 Jun; internet-exposed consoles; fix UniFi OS 4.0.6 (UI-SA-2026-349); botnet exploitation reported [CLAIMED]
CVE-2025-67038	Lantronix EDS5000	9.8	RCE	14 Jul 2026	Public PoC; botnet weaponization [CLAIMED]; fix firmware 6.12.0.4; check OT/ICS estates

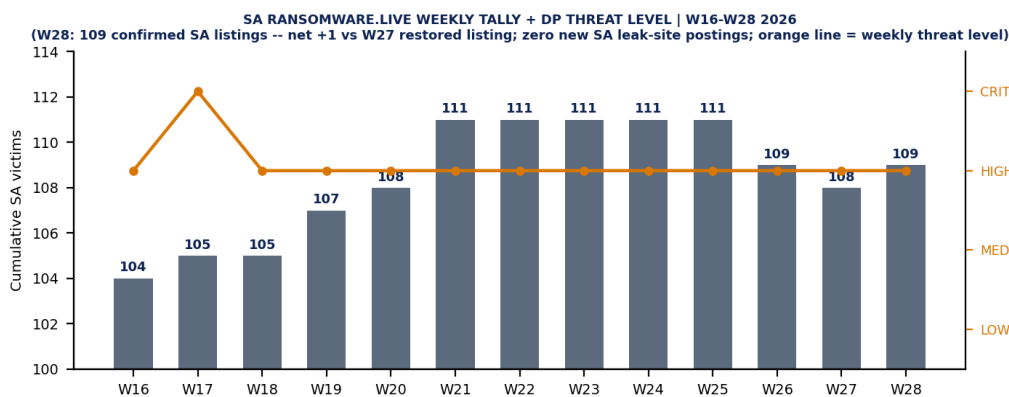
Pattern note: W28 rotates the pressure from volume to speed -- only two new KEV entries, but with three-day and eight-day fuses, one of which (SharePoint) has already lapsed, plus a CISA-instructed forensic triage on SimpleHelp because stolen credentials survive patching. Meanwhile the most severe item (Oracle EBS Payments 9.8) is being exploited ahead of any KEV listing, and the OVERDUE backlog (Windchill +7, Cisco UCM +7, PeopleSoft +20) keeps compounding. SA estates should treat SimpleHelp triage, SharePoint patching and the Oracle EBS sweep as a single high-priority change event before the 14 July Patch Tuesday adds the Ubiquiti and Lantronix deadlines.

FortiBleed: no new analysis, victim reporting or revised device counts published in the window (73,932-86,644 compromised FortiGates remains the range carried in DP-CTI-2026-W27, with named SA banks, municipalities, universities and healthcare entities in the dataset). Organisations that have not yet completed credential rotation, MFA enforcement and FortiOS upgrades should treat the W27 guidance as still current. **Microsoft KB5094126:** the Recycle Bin fix remains slated for the 14 July Patch Tuesday; BitLocker recovery lockouts (HP EliteBook/ProBook, Dell Precision), OneDrive-on-domain failures and Office OLE breakage remained unacknowledged or unfixed as of 5 July, with no out-of-band release in the window. **SharePoint deadline aftermath:** no public reporting of post-deadline exploitation had appeared by 5 July; coverage clusters on the 1-2 July KEV addition.

19. Help Net Security -- PTC Windchill CVE-2026-12569 exploited (29 June 2026) -- <https://www.helpnetsecurity.com/2026/06/29/ptc-windchill-cve-2026-12569-exploited/>

6. RANSOMWARE LANDSCAPE

The SA ransomware.live cumulative count is 109, verified 5 July via the country map.¹² Movement is net +1 versus W27's 108, but no new SA victim was posted in the window: the three most recent discovery dates in the entire ZA dataset remain 2 June (African National Congress -- Black X), 4 May (Standard Bank Group -- Prinz Eugen) and 3 May (Consumer Goods Council of SA -- Stormous). The +1 is therefore a restored or backfilled listing -- most plausibly the reversal of W27's single delisting -- not fresh victim activity. This is now a fifth week without a confirmed new SA leak-site posting since the ANC entry surfaced on 2 June, while actual SA-relevant threat activity continues to surface through breach disclosures, regulatory channels and fraud prosecutions instead.



End W27 baseline	108 confirmed SA listings
New W28 listings (28 Jun - 5 Jul)	0 confirmed on ransomware.live
Restorations (W28)	1 (restored/backfilled listing -- most plausibly reversal of W27's delisting; NOT a new SA victim)
End W28 count	109 (net +1 vs W27; verified 5 July via country map)
Most recent SA discovery dates	2 Jun (ANC -- Black X); 4 May (Standard Bank Group -- Prinz Eugen); 3 May (CGCSA -- Stormous)
Threat-level drivers (n on-ransomware.live)	Capitec card replacements (Pick n Pay); Profmed/PPSHA five-scheme surface; SimpleHelp MSP supply chain; Oracle EBS pre-KEV exploitation; tax-season fraud wave

Group notes: **Prinz Eugen** -- no leak-site movement verifiable this week (see Section 4). **The Gentlemen / GentleKiller** -- no new SA activity; the group retains three historical SA victims (Elundini and Intsika Yethu municipalities, Sunspray Food). **DragonForce** -- no development beyond the mid-June Symantec research into its Microsoft Teams C2 tradecraft. **KillSec, BlackSuit, Nightspire, Interlock, XP95 and Stormous** -- checked, no in-window SA or Africa developments. **Law enforcement:** the Scattered Spider extradition (complaint unsealed 30 June) is the window's main action;²⁰ Operation Endgame's StealIC/Amadey takedown (approximately 200 C2 servers, 27M stolen credentials, EUR 41m frozen) landed 24 June, just before the window -- SA organisations should still check the associated credential-notification channels. **Monthly statistics:** BlackFog's June 2026 State of Ransomware page would not render for verification and

its figures are deliberately excluded this week.

7. OSINT EXPOSURE & ATTACK SURFACE

Oracle EBS -- internet-exposed ERP attack surface

Shadowserver tracks ~950 internet-exposed Oracle E-Business Suite instances globally (reported 1 July, with improved fingerprinting) amid active CVE-2026-46817 exploitation; there is no public data on how many are patched. SA organisations running EBS should establish their exposure immediately and sweep for /OA_HTML/ibytransmit POSTs from 27 June.¹⁷

SA government web estate -- standing baseline (pre-window)

GroundUp's June investigation remains the freshest public SA attack-surface dataset: a Shodan scan of non-SITA .gov.za infrastructure found 1,089 exposed service records across 516 hosts, with 106 hosts (one in five) vulnerable and 4,466 total CVEs including 726 critical; SITA's own network separately showed 1,112 IPs with 5,014 CVEs (575 critical). Named exposures included Amathole District Municipality (353 CVEs, 94 critical), Witzenberg Municipality (347), Thaba Chweu Local Municipality mail (268), DALRRD/ARC, the National Development Agency and Midvaal Municipality, plus an Integrated Justice System server with exposed RDP vulnerable to SMBGhost (CVE-2020-0796) and insecure PPTP VPNs at Joe Gqabi, Bojanala Platinum and the KZN Nerve Centre among others.²⁹ With the #OpSouthAfrica campaign dormant rather than resolved, this baseline is the most likely target surface if hacktivism resumes.

Credential exposure -- RMM supply chain and infostealer takedown fallout

SimpleHelp-managed MSP environments must assume token theft (Section 5); the stealer chain harvests cloud, SCM, package-registry, AI-assistant, browser, SSH and cryptocurrency credentials, and stolen tokens survive patching.¹⁴ Operation Endgame's 27M recovered credentials warrant a check of haveibeenpwned-style notification services for corporate domains.

8. REGULATORY & POLICY

FICA cross-border cash conveyance regime LIVE [CONFIRMED]

The regime commenced 1 July as scheduled. The FIC confirmed that travellers crossing any SA air, land or sea border with cash or bearer negotiable instruments above R100,000 must declare via the SARS Customs traveller management system, piloted at various ports before go-live; the new reporting stream is designated cash conveyance reporting (CCR). FIC director Thabiso Thiti framed the system as years of SARS/FIC collaboration, explicitly tied to FATF Recommendation 32 -- one of SA's two remaining partially-compliant recommendations.²³ The commencement proclamation (5 June) brought ss.30, 54, 55 and 70 into force: wilful failure to report is a criminal offence and s.70 provides for search, seizure and mandatory forfeiture on conviction. Note a legal nuance: FICA s.30 creates an on-demand reporting duty triggered by an authorised official's demand, while the FIC's go-live framing describes proactive declaration; counsel should reconcile traveller policies against both readings.²⁴ No first-week seizures or operational reporting had been published by 5 July.

FICA 2026 RCR -- first-batch deadline passed, no tally yet [CONFIRMED framework; PROBABLE figure]

The 30 June 17:00 deadline for the first cohort has passed with no final filing rate published by 5 July; the FIC's RCR page was unchanged at the time of checking. The last published figure was 655 of 5,614 entities (11.66%) as at 17 June,²⁴ implying either a heavy late surge or a large non-compliant population now exposed to Directive 11 administrative sanctions under FICA s.62E. PCC 60 (final version of Draft PCC 125) governs submission mechanics.²⁵ The second-batch deadline (legal practitioners, estate agents, high-value goods dealers, non-casino gambling) is 31 July -- expect FIC enforcement messaging within weeks. Backdrop: the General Laws (AML/CTF) Amendment Bill is on an urgent July-November parliamentary timetable tied to the FATF mutual evaluation, whose first key reports are due in July and October 2026, with the on-site visit in March 2027.²⁷

Information Regulator -- TVET enforcement precedent and pending matters [CONFIRMED]

The Central Johannesburg TVET College enforcement notice (Section 3.4) is the week's substantive POPIA development: a misdirected internal email now sits squarely within s.22 reportable-compromise territory, alongside findings on s.8 (information officer registration), s.19 (safeguards) and s.15 (further processing).¹¹

TransUnion SA / Experian SA: responses to the s.59 notices reported in W27 are due approximately 6 July; no statement or coverage surfaced this week, and open-source confirmation of the notices themselves remains thin -- W29's primary regulatory watch item. **Tembisa Hospital / Gauteng Health:** the Regulator's 10-day window for Gauteng Health to hand over the Tembisa records (per the mid-June enforcement notice, on pain of criminal prosecution of the information officer) lapsed in late June; no compliance or prosecution decision had been published by 5 July. **IR capacity:** no Presidency proclamation yet formalising the Mtshontshi/Tilley appointments endorsed by the National Assembly on 23 June; the Regulator's media-statements page showed nothing newer than 2 June when checked on 5 July.³⁰

EU AI Act Digital Omnibus adopted [CONFIRMED adoption; PROBABLE deadline detail]

The Council of the EU gave final approval on 29 June, concluding the legislative process after Parliament's 16 June plenary vote.²⁸ Reported effect (pending Official Journal publication): high-risk AI obligations deferred to December 2027 / August 2028, with AI-generated-content transparency due December 2026 -- these substantive dates come from wider reporting on the agreed text rather than the tracker itself. SA businesses selling AI-enabled products or services into the EU gain breathing room on high-risk conformity but face the content-transparency deadline first; the parallel GDPR/ePrivacy/NIS2 omnibus remains in committee.

24. Moonstone -- FICA cross-border cash provisions take effect on 1 July (18 June 2026) -- <https://www.moonstone.co.za/fica-cross-border-cash-provisions-take-effect-on-1-july/>

25. Moonstone -- FIC finalises guidance on how to complete the 2026 RCR (18 June 2026) -- <https://www.moonstone.co.za/fic-finalises-guidance-on-how-to-complete-the-2026-rcr/>

26. Moonstone -- RCR compliance falls short as June deadline looms (18 June 2026) -- <https://www.moonstone.co.za/rcr-compliance-falls-short-as-june-deadline-looms/>

27. Moonstone -- Latest FATF review puts South Africa under a harsher spotlight (11 June 2026) -- <https://www.moonstone.co.za/latest-fatf-review-puts-south-africa-under-a-harsher-spotlight/>

28. MediaLaws -- Digital Omnibus Legislative Tracker (updated 30 June 2026; Council adoption 29 June) -- <https://www.medialaws.eu/digital-omnibus-legislative-tracker/>

9. WEEKLY THREAT HUNT & IOCs

Eight hunt missions are active for W28. Three P1 missions address the two short-fuse KEV entries (SharePoint deadline lapsed 4 July, SimpleHelp due 7 July) and the pre-KEV Oracle EBS Payments exploitation. Three P2 missions cover BlueHammer ransomware exploitation, the continuing PTC Windchill webshell campaign (overdue +7, per PTC advisory IOCs)¹⁹ and PeopleSoft mass-compromise fallout (overdue +20, Nissan named). Two P3 missions address SA fraud campaigns: Pick n Pay-derived card fraud and brand phishing, and tax-season fake-eFiling infrastructure. A machine-readable indicator export accompanies this report (iocs_w28.csv).

TH-2026-W28-01 -- SharePoint CVE-2026-45659 Deserialization RCE Hunt

P1 -- CRITICAL: CVSS 8.8; KEV due 4 Jul
(3-day fuse, LAPSED); exploited ITW

Hypothesis: An authenticated attacker with Site Member permissions exploits deserialization of untrusted data in SharePoint Server (Subscription Edition, 2019, 2016) for RCE. Patched May 2026 but rated Exploitation Less Likely, so many estates deferred; contextually linked to ongoing SharePoint intrusion activity including Storm-2603/Warlock reporting.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1078 (Valid Accounts), T1505.003 (Web Shell), T1059 (Command and Scripting Interpreter).

IOCs: Anomalous child processes of w3wp.exe (cmd.exe, powershell.exe); serialized-object payloads in SharePoint ULS logs; new .aspx/.ashx files under SharePoint LAYOUTS or content web roots; unexpected use of low-privilege Site Member accounts followed by server-side execution.

Data Sources: SharePoint ULS logs, IIS logs, EDR process-creation telemetry, file-integrity monitoring on SharePoint web roots, Entra ID / AD authentication logs.

Detection Guidance: Apply the May 2026 security update immediately -- the CISA deadline lapsed on 4 July. Audit which accounts hold Site Member or higher on internet-reachable sites. Hunt from 1 May onward for w3wp.exe spawning shells.

TH-2026-W28-02 -- SimpleHelp RMM CVE-2026-48558 to TaskWeaver / Djinn Stealer Hunt**P1 -- CRITICAL:** auth bypass; exploited since ~29 Jun; MSP supply chain; KEV due 7 Jul + instructed triage

Hypothesis: An OIDC authentication bypass (token signature not verified) in SimpleHelp RMM is exploited to deploy the TaskWeaver loader (obfuscated Node.js masquerading as jquery.js) and Djinn Stealer, harvesting cloud, SCM, package-registry, AI-assistant, browser, SSH and cryptocurrency credentials -- primarily through MSP-managed deployments. Stolen tokens remain valid after patching, so patch-only response is insufficient.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1199 (Trusted Relationship), T1555 (Credentials from Password Stores), T1552.001 (Credentials in Files), T1105 (Ingress Tool Transfer).

IOCs: Unrecognised SimpleHelp technician sessions or OIDC logins; TaskWeaver loader artefacts (jquery.js-named Node.js payloads); unexpected processes spawned by SimpleHelp service binaries; bulk reads of browser credential stores, .ssh, cloud CLI config and AI-assistant token files; anomalous outbound transfers from RMM hosts.

Data Sources: SimpleHelp server/audit logs, IdP/OIDC logs, EDR telemetry on RMM servers and managed endpoints, egress netflow, secrets-manager access logs.

Detection Guidance: Patch to the fixed SimpleHelp release before 7 July, then perform forensic triage per CISA's instruction. Rotate ALL credentials and tokens reachable from SimpleHelp-managed environments. MSP customers: demand attestation of both patch and triage from providers.

TH-2026-W28-03 -- Oracle EBS Payments CVE-2026-46817 Pre-KEV Exploitation Hunt**P1 -- CRITICAL:** CVSS 9.8 unauth; exploited ITW since 27 Jun; ~950 exposed; NOT in KEV as of 5 Jul

Hypothesis: Unauthenticated file read via the /OA_HTML/ibytransmit endpoint in Oracle Payments File Transmission (EBS 12.2.3-12.2.15) yields database credentials and payment API keys. First in-the-wild exploitation observed 27 June on honeypots using a targeted private exploit -- attackers are ahead of the public tooling curve.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1552 (Unsecured Credentials), T1078.004 (Cloud/Service Accounts), T1005 (Data from Local System).

IOCs: POST requests to /OA_HTML/ibytransmit (any occurrence on unpatched instances is suspect); anomalous file reads by the EBS application account; new database sessions from the EBS app tier using DBA-equivalent credentials; payment API calls from unfamiliar sources.

Data Sources: EBS Apache/OA framework access logs, database audit logs, WAF logs, payment-gateway API logs, egress netflow from EBS tiers.

Detection Guidance: Apply the May 2026 CPU. Sweep access logs back to at least 27 June for ibytransmit POSTs. If exposed and unpatched, treat as potentially compromised: rotate DB credentials and payment API keys.

TH-2026-W28-04 -- BlueHammer CVE-2026-33825 Ransomware Exploitation Hunt	P2 -- HIGH: Defender LPE; KEV due date lapsed 7 May; flagged ransomware-exploited 29 Jun
Hypothesis: Ransomware operators use the BlueHammer Microsoft Defender LPE (public PoC since April, leaked by Nightmare Eclipse) for SAM-hive access and SYSTEM escalation during post-compromise lateral movement, in estates that missed the April patch cycle. MITRE ATT&CK: T1068 (Exploitation for Privilege Escalation), T1003.002 (SAM Credential Dumping), T1486 (Data Encrypted for Impact). IOCs: SAM registry-hive access originating from Defender-related processes; unexpected SYSTEM-level process creation following Defender service activity; PoC artefacts referencing the April Nightmare Eclipse release. Data Sources: EDR telemetry, Windows Security/Sysmon registry-access events, Defender operational logs. Detection Guidance: Confirm the April 2026 Defender/Windows updates are deployed fleet-wide. Alert on SAM-hive reads by non-standard processes. Include in ransomware-readiness purple-team scenarios.	
TH-2026-W28-05 -- PTC Windchill / FlexPLM JSP Webshell Hunt (OVERDUE +7)	P2 -- HIGH: critical unauth RCE; KEV due 28 Jun lapsed; webshell deployment continuing
Hypothesis: Attackers continue dropping JSP webshells on unpatched Windchill/FlexPLM PLM servers; PTC's advisory keeps being updated with fresh IOCs. SA aerospace, mining engineering and defence contractors remain the exposed population. MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1505.003 (Web Shell), T1213 (Data from Information Repositories). IOCs: JSP files under /Windchill/servlet/; anomalous deserialization payloads to PLM web services; unexpected child processes of the Windchill service; bulk export of design/engineering data; outbound connections from PLM tiers to unfamiliar IPs. Data Sources: Windchill web/application logs, file-integrity monitoring on the web root, EDR telemetry, egress netflow from PLM tiers. Detection Guidance: Apply the PTC patch and re-check against the advisory's latest IOC revision. Review /Windchill/servlet/ for webshells. Segment PLM from the internet.	

TH-2026-W28-06 -- Oracle PeopleSoft CVE-2026-35273
Mass-Compromise Fallout Hunt (OVERDUE +20)

P2 -- HIGH: zero-day campaign 27 May-9 Jun; Nissan named 29 Jun; education sector primary

Hypothesis: ShinyHunters exploited PeopleSoft as a zero-day to exfiltrate HR/payroll records from 100+ organisations; Oracle privately told victims hundreds of companies may be affected. SA universities and provincial governments running PeopleSoft may be unnamed victims.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1213 (Data from Information Repositories), T1567 (Exfiltration Over Web Service).

IOCs: Anomalous PeopleSoft web-service requests during 27 May-9 June; bulk HR/payroll table reads; unfamiliar outbound transfers from PeopleSoft tiers in that window.

Data Sources: PeopleSoft web/app logs, database audit logs, netflow archives for May-June, HR-system access reviews.

Detection Guidance: Patch (20 days overdue). Run a retrospective compromise assessment across the 27 May-9 June window even if no notification has been received; Oracle's victim notifications have lagged public disclosure.

TH-2026-W28-07 -- Pick n Pay Dataset Monetisation: Card Fraud + Brand Phishing Hunt

P3 -- MEDIUM: dataset actively marketed; Capitec remediation live since 2 Jul

Hypothesis: Buyers of the Pick n Pay Asap!/Bottles dataset weaponise names, contact details and partial card data for card-not-present fraud and convincing PnP/Capitec-branded smishing/phishing against affected customers.

MITRE ATT&CK: T1566 (Phishing), T1598 (Phishing for Information), T1657 (Financial Theft).

IOCs: Spikes in CNP declines on cards with matching last-four/expiry combinations; newly registered domains mimicking Pick n Pay, Asap! or Capitec; SMS lures referencing card replacement or refunds.

Data Sources: Issuer fraud telemetry, domain-registration feeds, SMS-gateway abuse reports, customer-complaint channels.

Detection Guidance: Issuers: raise CNP scrutiny for flagged customers. Brand owners: monitor and take down lookalike domains. Communicate that genuine card-replacement contact will never request OTPs (reinforce with the Mthatha vishing case).

TH-2026-W28-08 -- Tax-Season Fake-eFiling Infrastructure Hunt

P3 -- MEDIUM: Orca public warnings since 1 Jun; burst-attack detail PROBABLE (single source)

Hypothesis: Fraud crews exploit the open tax season with fake SARS eFiling refund/penalty/auto-assessment SMS and email lures harvesting credentials and card data through fake checkout pages, then run automated card-testing bursts (burst-attack specifics rest on a single source).

MITRE ATT&CK: T1566.002 (Spearphishing Link), T1056 (Input Capture), T1657 (Financial Theft).

IOCs: Newly registered SARS/eFiling-lookalike domains; SMS lures with refund or penalty themes; card-testing bursts of sequential authorisations; credential-harvesting pages mimicking eFiling login.

Data Sources: Domain-registration feeds, SMS abuse reports, issuer authorisation telemetry, web-proxy logs.

Detection Guidance: Block lookalike domains at DNS/proxy. Finance teams: verify any SARS communication via the official app or portal, never SMS links. Issuers: tune burst-attack velocity rules.

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

- 1. Clear both short-fuse KEVs and go beyond the patch on SimpleHelp:** SharePoint CVE-2026-45659 immediately (the 4 July deadline has lapsed); SimpleHelp CVE-2026-48558 by 7 July including CISA's instructed forensic triage and full token rotation -- patch-only response leaves stolen credentials live. MSP customers should demand written attestation of both steps.
- 2. Sweep Oracle estates now:** hunt /OA_HTML/ibytransmit POSTs (EBS, from 27 June) and run the PeopleSoft 27 May - 9 June retrospective compromise assessment regardless of notification status. Both campaigns demonstrate exploitation running ahead of KEV listing and vendor victim notification.
- 3. Tune fraud detection for the week's SA-specific campaigns:** CNP velocity rules for Pick n Pay-flagged cards, card-testing burst detection, SARS/eFiling and Capitec lookalike-domain monitoring, and OTP-harvesting vishing playbooks referencing the Mthatha case.
- 4. Keep hacktivist hardening in place at reduced tempo:** the #OpSouthAfrica campaign is dormant, not resolved -- retain WAF rules and OWASP Top 10 monitoring on .gov.za/SOE estates, and use the GroundUp exposure baseline to prioritise remediation of the named municipal and justice-system systems.

Management (CISO / Board)

- 1. Third-party administrator risk is this week's board lesson:** PPSHA (five schemes, one breach via a third-party provider) and Pick n Pay (legacy app, bank-side remediation) both show impact landing outside the breached entity. Demand current attestations from scheme administrators, payment processors and legacy-platform custodians, and map which of your services could force a partner into customer remediation.
- 2. Update breach-classification thresholds after the TVET precedent:** a misdirected internal email can now constitute a reportable POPIA s.22 compromise. Information officers should refresh incident-classification playbooks and confirm s.8 registration and s.19 safeguards documentation.
- 3. Prepare for the credit-bureau outcome:** TransUnion SA and Experian SA responses to the Information Regulator are due approximately 6 July per W27 reporting. Organisations consuming bureau data should pre-draft customer-facing language and confirm contractual breach-notification rights before the outcome lands.
- 4. Operationalise FICA changes:** travel policies must reflect the R100,000 CCR declaration threshold (criminal offences apply from commencement); accountable institutions in the second RCR batch have a hard 31 July deadline with s.62E sanctions in active use.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH -- 8th CONSECUTIVE WEEK

The South African cyber threat level remains **HIGH** for an eighth consecutive week (28 June - 5 July 2026). The level is held rather than raised or lowered: headline hacktivist risk de-escalated when the 30 June flashpoint passed quietly, but the week added confirmed banking-sector remediation from a retail breach, a five-scheme medical-administrator exposure surface, two short-fuse KEV deadlines and active pre-KEV exploitation of a CVSS 9.8 Oracle EBS flaw. The drivers are sustained and material, not newly escalating.

Rationale

- **Downstream breach impact is compounding:** Capitec card replacements (Pick n Pay dataset) and the Profmed/PPSHA identification -- with five administered schemes including the SANDF RFMCF -- both expand real consumer exposure this week without any new intrusion.
- **Two KEV deadlines inside seven days:** SharePoint CVE-2026-45659 (deadline 4 July, three-day fuse, now lapsed) and SimpleHelp CVE-2026-48558 (due 7 July with instructed forensic triage and MSP supply-chain reach).
- **Active exploitation ahead of the KEV:** Oracle EBS Payments CVE-2026-46817 (CVSS 9.8, unauthenticated, ~950 exposed instances) exploited since 27 June; PeopleSoft fallout confirmed via Nissan's disclosure that hundreds of companies may be affected.
- **Hacktivism dormant, not resolved:** no observed escalation through 5 July, but exfiltrated DCS data remains in actor hands, the campaign is unrenounced, and Telegram/dark-web channels were not directly observable.
- **Standard Bank leak and credit-bureau enforcement unresolved:** no new public development, with IR responses due approximately 6 July -- outcome pending, not risk retired.
- **A fifth week without a new SA leak-site victim:** the 109 count reflects a restored listing; threat activity continues to surface through disclosures, regulation and fraud channels instead.

Next-Week Watch (W29)

- TransUnion SA / Experian SA responses to the Information Regulator (due approximately 6 July) and any IR statement.
- SimpleHelp KEV deadline (7 July) aftermath and first post-deadline exploitation reporting for SharePoint CVE-2026-45659.
- Patch Tuesday 14 July: KB5094126 Recycle Bin fix, BitLocker lockout acknowledgment, plus the Ubiquiti UniFi and Lantronix KEV due dates the same day.
- Possible KEV listing of Oracle EBS Payments CVE-2026-46817 and identification of victims.

- PPSHA breach scope: confirmation or exclusion of the other four administered schemes, especially the SANDF Regular Force Medical Continuation Fund.
- FIC: final 2026 RCR first-batch filing tally and enforcement posture ahead of the 31 July second batch; first CCR operational reporting from the borders.
- ransomware.live: identity of the restored SA listing; any new SA victims ending the five-week quiet streak.
- #OpSouthAfrica residual monitoring: any delayed release of DCS or municipal data.
- Tembisa Hospital information-officer prosecution decision following the lapsed hand-over window.

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. Numbers 1-30 correspond to the inline footnote citations used throughout this report; each unique source appears exactly once. All cited URLs were retrieved and verified on 5 July 2026, with two exceptions: items 1 and 5 (MyBroadband) are blocked from direct automated retrieval in our fetch environment; their existence, headlines and dates were verified via the fetched Data Breaches Digest editions (items 2 and 6) and their substantive claims are corroborated by items 3, 4 and 7 as indicated in the text.

1. MyBroadband -- Capitec tells specific customers to replace bank cards following Pick n Pay data breach (2 July 2026) -- <https://mybroadband.co.za/news/security/656369-capitec-tells-specific-customers-to-replace-bank-cards-following-pick-n-pay-data-breach.html>
2. Data Breaches Digest -- Week 27 2026, covering 29 June - 5 July (fetched 5 July 2026) -- <https://www.dbdigest.com/2026/06/data-breaches-digest-week-27-2026.html>
3. News24 -- Used Pick n Pay's old delivery service? Your address and card info may have been leaked (28 May 2026) -- <https://www.news24.com/business/consumer-lookout/used-pick-n-pays-old-delivery-service-your-address-and-card-info-may-have-been-leaked-20260528-0993>
4. TechCabal -- Pick n Pay breach puts South Africa's retail cybersecurity under scrutiny (1 June 2026) -- <https://techcabal.com/2026/06/01/pick-n-pay-cyberbreach/>
5. MyBroadband -- Top medical aid in South Africa with 200,000 clients hit by data breach (25 June 2026) -- <https://mybroadband.co.za/news/security/655653-top-medical-aid-in-south-africa-with-200000-clients-hit-by-data-breach.html>
6. Data Breaches Digest -- Week 26 2026 (fetched 5 July 2026) -- <https://www.dbdigest.com/2026/06/data-breaches-digest-week-26-2026.html>
7. PPS Healthcare Administrators -- Our Clients (fetched 5 July 2026) -- <https://ppsha.co.za/our-clients/>
8. Cybernews -- Claude AI exploited to breach hotel booking platforms (23 June 2026) -- <https://cybernews.com/security/claude-ai-exploited-breach-hotel-booking-platforms/>
9. NovaNews / PE Express -- Two sentenced in R1.07m Standard Bank impersonation fraud case (2 July 2026) -- <https://novanews.co.za/peexpress/two-sentenced-in-r1-07m-standard-bank-impersonation-fraud-case/>
10. Everywhere VC -- Orca Fraud warns of SARS scam surge (1 June 2026) -- <https://ideas.everywhere.vc/p/orca-fraud-warns-of-sars-scam-surge>
11. DataBreaches.net -- ZA: Copying the wrong person on an email could be considered a data breach in South Africa (29 June 2026) -- <https://databreaches.net/2026/06/29/za-copying-the-wrong-person-on-an-email-could-be-considered-a-data-breach-in-south-africa/>
12. Ransomware.live -- South Africa country tracking and map (verified 5 July 2026; 109 cumulative) -- <https://ransomware.live/map/ZA>

13. The Hacker News -- SharePoint RCE CVE-2026-45659 Added to CISA KEV After Active Exploitation (2 July 2026) -- <https://thehackernews.com/2026/07/sharepoint-rce-cve-2026-45659-added-to.html>
14. Help Net Security -- SimpleHelp vulnerability exploited, CVE-2026-48558 (30 June 2026) -- <https://www.helpnetsecurity.com/2026/06/30/simplehelp-vulnerability-exploited-cve-2026-48558/>
15. BleepingComputer -- CISA: Windows BlueHammer flaw now exploited by ransomware gangs (30 June 2026) -- <https://www.bleepingcomputer.com/news/security/cisa-windows-bluehammer-flaw-now-exploited-by-ransomware-gangs/>
16. Help Net Security -- Oracle Payments CVE-2026-46817 exploitation observed (30 June 2026) -- <https://www.helpnetsecurity.com/2026/06/30/oracle-payments-cve-2026-46817-exploitation/>
17. BleepingComputer -- Over 900 Oracle E-Business instances exposed to ongoing attacks (1 July 2026) -- <https://www.bleepingcomputer.com/news/security/over-900-oracle-e-business-instances-exposed-to-ongoing-attacks/>
18. BleepingComputer -- Nissan discloses employee data breach linked to Oracle zero-day attacks (29 June 2026) -- <https://www.bleepingcomputer.com/news/security/nissan-discloses-employee-data-breach-linked-to-oracle-zero-day-attacks/>
19. Help Net Security -- PTC Windchill CVE-2026-12569 exploited (29 June 2026) -- <https://www.helpnetsecurity.com/2026/06/29/ptc-windchill-cve-2026-12569-exploited/>
20. Infosecurity Magazine -- Scattered Spider member extradited to US (2 July 2026) -- <https://www.infosecurity-magazine.com/news/scattered-spider-member-extradited/>
21. Infosecurity Magazine -- Cybercriminals pose as Interpol to deliver ransomware (2 July 2026; Bitdefender research 1 July) -- <https://www.infosecurity-magazine.com/news/cybercriminals-pose-interpol/>
22. BleepingComputer -- New Prinz Eugen ransomware prioritizes recent files for encryption (20 June 2026; carryover technical profile) -- <https://www.bleepingcomputer.com/news/security/new-prinz-eugen-ransomware-prioritizes-recent-files-for-encryption/>
23. Engineering News -- Domestic, foreign travellers must now declare cash of more than R100 000: FIC (1 July 2026) -- <https://www.engineeringnews.co.za/article/domestic-foreign-travellers-must-now-declare-cash-of-more-than-r100-000-fic-2026-07-01>
24. Moonstone -- FICA cross-border cash provisions take effect on 1 July (18 June 2026) -- <https://www.moonstone.co.za/fica-cross-border-cash-provisions-take-effect-on-1-july/>
25. Moonstone -- FIC finalises guidance on how to complete the 2026 RCR (18 June 2026) -- <https://www.moonstone.co.za/fic-finalises-guidance-on-how-to-complete-the-2026-rcr/>
26. Moonstone -- RCR compliance falls short as June deadline looms (18 June 2026) -- <https://www.moonstone.co.za/rcr-compliance-falls-short-as-june-deadline-looms/>
27. Moonstone -- Latest FATF review puts South Africa under a harsher spotlight (11 June 2026) -- <https://www.moonstone.co.za/latest-fatf-review-puts-south-africa-under-a-harsher-spotlight/>
28. MediaLaws -- Digital Omnibus Legislative Tracker (updated 30 June 2026; Council adoption 29 June) -- <https://www.medialaws.eu/digital-omnibus-legislative-tracker/>
29. GroundUp -- Here's how insecure government's websites are (11 June 2026; standing SA exposure baseline) -- <https://groundup.org.za/article/heres-how-insecure-governments-websites/>
30. Information Regulator (South Africa) -- Media statements (checked 5 July 2026; most recent statement dated 2 June 2026) -- <https://infoforegulator.org.za/media-statements>

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. Where a claim rests on a single source or a threat-actor assertion, it is explicitly rated PROBABLE or CLAIMED in the text. Prepared by Digital Progression | dpcyber.co.za | DP-CTI-2026-W28 | Published Monday 6 July 2026