



SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 25 | 7 June – 14 June 2026

THREAT LEVEL: HIGH

AVBOB, SA's largest funeral insurer (350+ branches), knocked offline by external malicious actors 7-8 June. Microsoft June Patch Tuesday breaks records at 208 CVEs (38 Critical); CVE-2026-45657 wormable Windows kernel TCP/IP RCE (9.8) is the top priority. SAPS Western Cape POPIA breach exposes 2,978 officers' medical records. Oracle PeopleSoft CVE-2026-35273 0-day mass-compromise by ShinyHunters (300+ instances). Ivanti Sentry CVE-2026-10520 (10.0) weaponised in under 24h. GroundUp Part 2: non-SITA gov.za shows 4,466 CVEs. SA ransomware count FLAT at 111 (5th consecutive week); SuppCenter MSSP listed on M3RX.

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W25 | Classification: TLP:WHITE

Published Monday 15 June 2026

© 2026 Digital Progression | dpcyber.co.za

TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard
- 2. Threat Landscape Heatmap
- 3. SA Cyber Incidents & Breaches
- 4. Global Incidents with SA Relevance
- 5. Threat Actors
- 6. Critical Vulnerabilities & CISA KEV
- 7. Ransomware Landscape
- 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 W21-W24, 5th consecutive week) — Week 25 (7-14 June 2026)

Story 1 — AVBOB Cyberattack Knocks SA's Largest Funeral Insurer Offline: AVBOB Mutual Assurance, South Africa's largest funeral insurer with 350+ branches, was struck by external malicious actors on or around 7-8 June. Digital platforms went offline, branches reverted to manual operations, and the Information Regulator was notified. As of 14 June no group has claimed credit on indexed leak sites; ransomware versus extortion-only remains unconfirmed; the forensic audit is in progress. This is the highest-profile SA private-sector disruption since the current cycle began.¹²

Story 2 — Record 208-CVE Patch Tuesday + Wormable Kernel RCE: The 9 June Patch Tuesday was the largest in Microsoft's program history at 208 CVEs (38 Critical). The standout fixes are **CVE-2026-42897** — the Exchange OWA permanent patch finally shipped via KB5094139 (closing the four-week patchless window since the W22 KEV deadline) — and **CVE-2026-45657**, a wormable Windows kernel TCP/IP RCE at CVSS 9.8 that should be every SA estate's #1 June patch. The companion OpenSSL advisory shipped 18 CVEs including CVE-2026-45447, a critical heap UAF in PKCS7_verify().³

Story 3 — SAPS Western Cape POPIA Breach + Oracle PeopleSoft Mass-Compromise: SAPS Western Cape confirmed a POPIA breach affecting **2,978 officers** when an HR email circulated an attachment exposing diagnostic medical records (PTSD, bipolar disorder, alcoholism, cancer). Separately, **Oracle PeopleSoft CVE-2026-35273 (CVSS 9.8)** was exploited as a zero-day by ShinyHunters/UNC6240 from 27 May; 300+ instances compromised across 100+ organisations including the University of Nottingham (454,600 records); CISA KEV deadline 15 June. Ivanti Sentry CVE-2026-10520 (10.0) was weaponised within 24 hours of patch release.⁴⁵

KPI Dashboard

Metric	Current (W25)	Prior (W24)	Change	Direction
SA threat level	HIGH	HIGH	Unchanged (5th consecutive week)	FLAT
SA ransomware.live victims (total)	111	111	0 new W25 (5th week FLAT)	FLAT
New SA RW listings this week (ransomware.live)	0 confirmed	0 (W24)	FLAT	FLAT
AVBOB Mutual Assurance (350+ branches)	OFFLINE -- external malicious actors 7-8 Jun; IR notified	N/A	NEW W25	UP
Microsoft Patch Tuesday volume	208 CVEs (record; 38 Critical) -- 9 Jun	~70-90 typical	RECORD HIGH	UP
SAPS Western Cape POPIA breach	2,978 officers medical records leaked (HR email)	No comparable	NEW W25	UP
Oracle PeopleSoft CVE-2026-35273 (9.8)	0-day mass-compromise; 300+ instances/100+ orgs; KEV 15 Jun	N/A	NEW W25	UP
Ivanti Sentry CVE-2026-10520 (10.0)	Weaponised <24h of patch; KEV 14 Jun	N/A	NEW W25	UP
Exchange OWA permanent patch	SHIPPED via KB5094139 (9 Jun) -- closes W22 gap	NO perm patch (W24)	RESOLVED	DOWN
Cisco SD-WAN 0-days (2026 total)	7 (CVE-2026-20245 -- STILL NO patch); KEV 9 Jun	7 (W24)	PERSISTING	FLAT
GroundUp gov.za attack surface (non-SITA)	4,466 CVEs; 1-in-5 hosts vulnerable (Part 2, 11 Jun)	SITA 5,014 CVEs (W24 Part 1)	EXPANDED	UP
SuppCenter MSSP (Xcitium/Comodo)	Listed on M3RX 11 Jun -- supply-chain risk to SA pub-sec	N/A	NEW W25	UP

W25 KEY FRAMING: W25 is defined by a live private-sector incident (AVBOB, SA's largest funeral insurer, 350+ branches offline), a record-breaking 208-CVE Patch Tuesday led by a wormable kernel RCE, and a cluster of high-severity actively-exploited vulnerabilities (PeopleSoft 0-day mass-compromise, Ivanti Sentry 10.0, Chrome V8 0-day). The FLAT ransomware count (111, now 5th consecutive week) again masks real threat activity outside the ransomware.live tracker. The dominant operational driver is the 9 June Patch Tuesday — CVE-2026-45657 (wormable kernel) plus the PeopleSoft and Ivanti emergency responses must be the primary change-window focus for every SA organisation this week.

TOP 3 ACTIONS THIS WEEK

1. PATCH THE WORMABLE KERNEL RCE FIRST (CVE-2026-45657): Deploy the full Windows June security rollup as the #1 priority. CVE-2026-45657 (wormable Windows kernel TCP/IP RCE, CVSS 9.8) plus companion HTTP.sys CVE-2026-47291 (9.8) are the standout fixes. Apply the Exchange OWA permanent patch (KB5094139, CVE-2026-42897) in the same change window; Exchange 2016/2019 estates require ESU enrolment. Rebuild container images and restart TLS services for the OpenSSL PKCS7 fix (CVE-2026-45447).

2. ORACLE PEOPLESOFT EMERGENCY RESPONSE (CVE-2026-35273, KEV 15 JUN):

ShinyHunters/UNC6240 mass-exploited this 9.8 0-day from 27 May (300+ instances across 100+ orgs). Disable PSEMHUB; block /PSEMHUB/hub at the perimeter; audit web-server logs from 27 May onward. SA relevance is HIGH — PeopleSoft is present in SA universities, public-sector HCM, and large enterprise.

3. IVANTI SENTRY (10.0, KEV 14 JUN) + CHECK POINT GATEWAY (KEV 11 JUN, 3-DAY) + CHROME V8 0-DAY: Patch Ivanti Sentry CVE-2026-10520 (10.0) and companion CVE-2026-10523 (9.9) to R10.5.2/R10.6.2/R10.7.1 — exploits deployed within 24h of release. Remediate Check Point Security Gateway CVE-2026-50751 (IKEv1 auth bypass) within the 3-day window. Force-update all Chromium browsers for V8 CVE-2026-11645 (actively exploited).

1. ITWeb -- Malicious actors take down AVBOB's digital platforms -- <https://www.itweb.co.za/article/malicious-actors-take-down-avbobs-digital-platforms/5yONP7Erd6QMXWrb>

2. The Bulrushes -- Cyber attack disrupts AVBOB funeral services digital platforms (8 June 2026) — <https://thebulrushes.com/2026/06/08/cyber-attack-disrupts-avbob-funeral-services-digital-platforms/>

3. PDQ -- Patch Tuesday June 2026 (record 208 CVEs) — <https://www.pdq.com/blog/patch-tuesday-june-2026/>

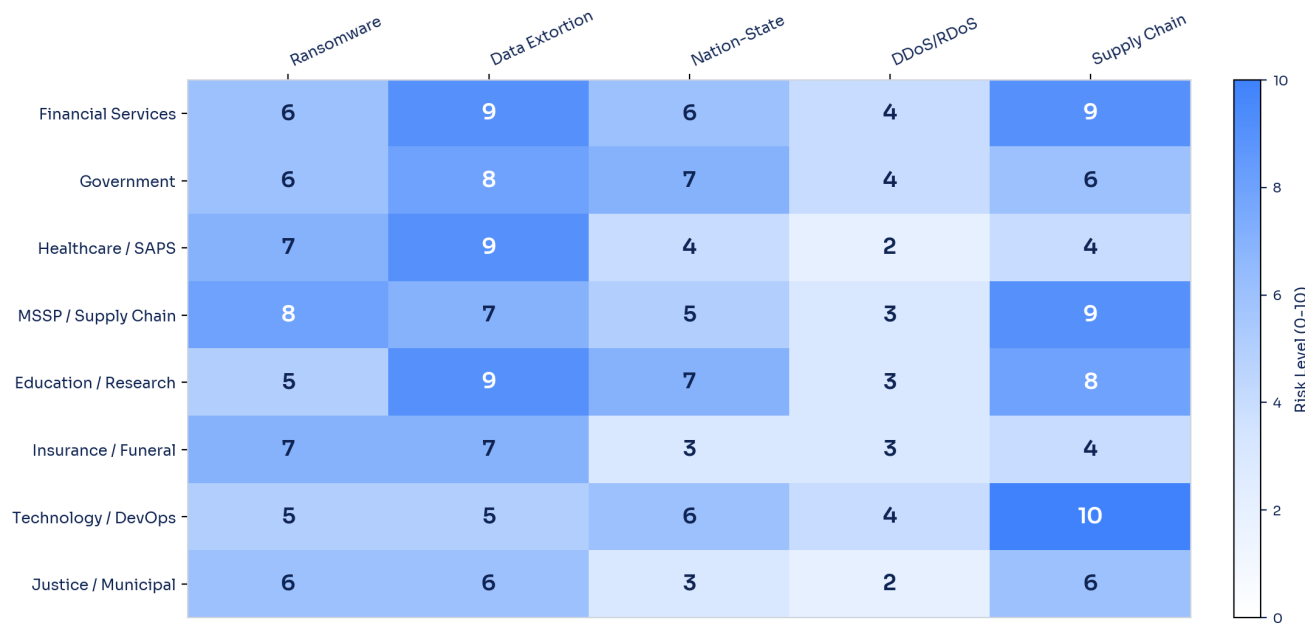
4. Cape Argus -- Confidential medical records of 3,000 SAPS officers leaked (9 June 2026) — <https://capeargus.co.za/news/2026-06-09-shock-as-confidential-medical-records-of-3-000-saps-officers-leaked/>

5. The Hacker News -- Weekly recap (PeopleSoft 0-day, ShinyHunters/UNC6240) — <https://thehackernews.com/2026/06/weekly-recap-instagram-account-hacks.html?m=1>

2. THREAT LANDSCAPE HEATMAP

The heatmap maps eight South African sectors against five threat categories, rated 0–10 based on confirmed incidents, active threat actor campaigns, and vulnerability exposure during Week 25 (7–14 June 2026). **Technology/DevOps** peaks at 10 on Supply Chain following the record 208-CVE Patch Tuesday, the Ivanti Sentry 10.0 weaponisation, the Chrome V8 0-day, and the persisting Cisco SD-WAN 0-day. **Financial Services, Healthcare/SAPS, and Education/Research** rise to 9 on Data Extortion (SAPS WC 2,978-officer medical-records breach; Oracle PeopleSoft mass-compromise affecting universities and HCM; Nottingham 454,600 records). **MSSP/Supply Chain** rises to 8 on Ransomware and 9 on Supply Chain following the SuppCenter (Xcitium/Comodo) M3RX listing. **Insurance/Funeral** elevates to 7 on Ransomware on the AVBOB live incident.

SA THREAT LANDSCAPE HEATMAP | W25 (7 - 14 June 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 25 (7–14 June 2026): Zero new ransomware.live listings (SA tally holds at 111, 5th consecutive week FLAT). Dominant stories: (1) AVBOB Mutual Assurance — SA’s largest funeral insurer, 350+ branches offline (7–8 June); (2) SAPS Western Cape — 2,978 officers’ medical records leaked via HR email (POPIA breach, 9 June); (3) Cannabis Club Systems — ~88,000 South Africans in a global 1.08M-record API leak

(GDPR-governed); (4) Dept of Employment & Labour — official suspended over reckless disposal of job-seekers' data (11 June); (5) GroundUp Part 2 — non-SITA gov.za attack surface, 4,466 CVEs (11 June); (6) SuppCenter Global/SA MSSP listed on M3RX (11 June); (7) NightSpire EC Human Settlements + Ingonyama Trust breaches tabled in Portfolio Committee (11 June).⁶

3.1 INC-2026-W25-01 — AVBOB Mutual Assurance Cyberattack [CONFIRMED]

Sector	Insurance / Funeral Services (private)
Date	7–8 June 2026 (digital platforms taken offline)
Actor	"External malicious actors" -- no attribution; no leak-site claim as of 14 Jun
Scale	SA's largest funeral insurer; 350+ branches forced to manual operations
Regulatory	Information Regulator notified; POPIA s.22 obligations active given customer-data scope
Ransomware?	Ransomware vs extortion-only UNCONFIRMED; forensic audit in progress
Confidence	CONFIRMED (operational impact); attribution UNKNOWN

AVBOB Mutual Assurance, South Africa's largest funeral insurer with 350+ branches, was struck by "external malicious actors" on or around 7–8 June. Digital platforms were taken offline and branches reverted to manual operations. The Information Regulator has been notified and a forensic audit is in progress. As of 14 June no group has claimed credit on indexed leak sites and the ransomware-versus-extortion-only question remains unconfirmed. This is the highest-profile SA private-sector disruption of the current cycle. SA insurance and funeral-services peers should review dependence on shared infrastructure and broker portals, and verify POPIA s.22 notification readiness.¹²

3.2 INC-2026-W25-02 — SAPS Western Cape -- 2,978 Officers' Medical Records Leaked [CONFIRMED POPIA BREACH]

Sector	Government / Law Enforcement (SAPS Western Cape)
Date	9 June 2026
Cause	HR email circulated an attachment ("leave subcategory") exposing diagnostic medical records
Records exposed	2,978 officers; PTSD, bipolar disorder, alcoholism, cancer diagnoses
Acknowledgement	Lt Gen Patekile acknowledged POPIA-reportable breach; independent investigation under way
Material	Mirrors W24 Central JHB TVET precedent at far greater scale -- internal HR disclosure = notifiable POPIA compromise
Confidence	CONFIRMED

An SAPS Western Cape HR email circulated an attachment that exposed the diagnostic medical records of 2,978 officers — including PTSD, bipolar disorder, alcoholism, and cancer diagnoses. Lt Gen Patekile acknowledged a POPIA-reportable breach and an independent investigation is under way. The incident mirrors the W24 Central JHB TVET precedent at far greater scale: inadvertent internal HR disclosure of special personal information is treated as a notifiable security compromise under POPIA. Every SA HR function and special-category data processor should re-examine internal data-sharing workflows, attachment-handling controls, and Information Officer registration status.⁴

3.3 INC-2026-W25-03 — Cannabis Club Systems -- ~88,000 South Africans Exposed [CONFIRMED, GDPR-governed]

Sector	Consumer platform (cannabis club management, global)
Exposure	Global API left 1.08 million records publicly accessible; 40+ countries affected
SA scale	~88,000 South Africans -- SA second-most affected country (after Spain)
Data	SA ID numbers, passports, cannabis-use records
Disclosure timeline	Researcher discovered in April; vendor ignored notification for 26 days before fix
Jurisdiction	Platform GDPR-governed -- outside POPIA reach despite SA victim scale
Boundary case	SA citizens with no SA legal remedy
Confidence	CONFIRMED

A global API exposure at Cannabis Club Systems left 1.08 million records publicly accessible across 40+ countries, with South Africa the second-most affected country after Spain at roughly 88,000 records (SA IDs, passports, cannabis-use data). A researcher discovered the exposure in April; the vendor reportedly ignored notification for 26 days before remediating. Because the platform is GDPR-governed and outside POPIA's reach, this is a notable boundary case: SA citizens are materially affected yet have no SA legal recourse. SA users should treat exposed ID/passport data as compromised and monitor for downstream identity-fraud abuse.⁷

3.4 INC-2026-W25-04 — Dept of Employment & Labour -- Job-Seekers Data Breach [CONFIRMED]

Sector	Government (Department of Employment & Labour)
Date	11 June 2026
Cause	Reckless physical disposal of job-applicant personal information
Action	Official placed on precautionary suspension; internal probe under way
Regulatory	POPIA ss.19/22 assessment under way; IR notification not yet confirmed as filed
Confidence	CONFIRMED

The Department of Employment & Labour suspended an official on 11 June over the reckless physical disposal of job-applicants' personal information. A POPIA ss.19/22 assessment is under way and Information Regulator notification has not yet been confirmed as filed. The incident underscores that POPIA security-safeguard obligations extend to physical-media disposal, not only digital exfiltration. SA organisations should verify secure-destruction procedures for paper records containing personal information.⁸

3.5 INC-2026-W25-05 — GroundUp Part 2: Non-SITA gov.za Attack Surface [CONFIRMED, investigative]

Source	GroundUp -- Part 2 investigation, 11 June 2026 (Shodan analysis of 516 non-SITA gov.za hosts)
Headline finding	1,089 exposed service records; 4,466 CVEs; 1-in-5 hosts vulnerable (worse than SITA's own rate)
Amathole District Municipality	353 CVEs; 94 critical on a single server
Integrated Justice System (IJS)	RDP exposed to internet + unpatched SMBGhost (courts/NPA/prisons)
VPN exposure	17 public-sector PPTP VPNs still operational (crackable in minutes); Ekurhuleni VPN compromise confirmed by acting city manager
EOL software	Multiple municipalities running Ubuntu 14.04 (EOL 2019)
Governance gap	No single body has the mandate to fix it
Confidence	CONFIRMED (investigative reporting)

GroundUp's Part 2 investigation analysed 516 SA government internet-facing hosts outside SITA's network and documented 4,466 CVEs with 1-in-5 hosts vulnerable — a worse rate than SITA's own (W24 Part 1). Amathole District Municipality alone showed 353 CVEs (94 critical on a single server); the Integrated Justice System runs RDP exposed to the internet with unpatched SMBGhost; 17 public-sector PPTP VPNs remain operational; and the Ekurhuleni VPN compromise was confirmed by the acting city manager. The defining problem is governance: no single body has the mandate to remediate the non-SITA estate. SA SOCs serving public-sector clients should treat the GroundUp inventory as a remediation-prioritisation baseline.⁹

3.6 INC-2026-W25-06 — SuppCenter Global/SA -- M3RX Ransomware Listing [CLAIMED]

Entity	SuppCenter Global/SA -- Xcitium/Comodo MSSP with SA-linked operations
Listing	Listed on M3RX dark-web portal 11 June 2026
Risk	Supply-chain risk to SA public-sector clients that use the operator
Status	CLAIMED (vendor not yet acknowledged)

SuppCenter Global/SA, a Xcitium/Comodo MSSP with SA-linked operations, was listed on the M3RX dark-web portal on 11 June. The primary concern is supply-chain exposure: any SA public-sector or enterprise client that relies on the operator for managed security services inherits downstream risk if the listing proves valid. The vendor has not yet acknowledged the claim, so it is tracked as CLAIMED. SA organisations using Xcitium/Comodo-managed services should request a breach-status attestation and review third-party access pathways.¹⁰

3.7 NightSpire -- Parliamentary Record (11 June) + Ongoing / Carryover Incidents (W25 Status)

NightSpire (parliamentary record): The EC Department of Human Settlements attack (Nov 2025) and the Ingonyama Trust breach were tabled in the Portfolio Committee record on 11 June — both incidents are now formally on parliamentary record. **TA4922 (China-linked):** Proofpoint confirmed W25 SA-targeted tax/payroll/HR lures delivering Atlas RAT, RomulusLoader, and Winos 4.0 (intelligence; no named SA victim).⁵

W24 Item	W25 Update
Standard Bank / ROOTBOY	IR formally scrutinising POPIA compliance; Belgian court ruling 3 Jun shifts fraud burden-of-proof debate with SA resonance; Standard Bank issued tax-season fraud advisory; no new W25 data dump.
SABS / Lynx	Forensic investigation tabled 12 Jun confirms Nov 2024 attack enabled by 2-year failure to act on AGSA recommendations; exec disciplinary hearings start late June.
SARS / SITA Nullsec claims	FORMALLY CLOSED as UNVERIFIED -- 25 May denials stand; W25 Check Point recycled-claim reference noted.
CSIR / CHPC Lengau	No public attribution W25; no exfiltration confirmation.
Central JHB TVET	No further IR statement W25.
Polmed 1.7M / 214 GB	STILL DEVELOPING -- no statement.
Webworm @ SA university	No new W25 victims.
Oday Syndicate / XL Africa	No new W25 listings.
SANBS / KillSec	STILL UNVERIFIED.
ANC "Black Ax" (W21) / Black X (W24)	STILL UNVERIFIED.

6. GroundUp -- Here's how insecure government's websites are (11 June 2026) —

<https://groundup.org.za/article/heres-how-insecure-governments-websites/>

7. MyBroadband / researcher Instagram thread -- Cannabis Club Systems API leak — <https://www.instagram.com/p/DZfCySwjukr/>

8. Sunday World -- Official suspended as Labour Department probes job-seekers data breach —

<https://sundayworld.co.za/business/official-suspended-as-labour-department-probes-job-seekers-data-breach/>

9. GroundUp -- Non-SITA gov.za attack surface investigation Part 2 (11 June 2026) —

<https://groundup.org.za/article/heres-how-insecure-governments-websites/>

10. Ransomware.live -- SuppCenter Global/SA listing (M3RX, 11 June 2026) —

<https://www.ransomware.live/id/c3VwcGNlbnRlci5nbG9iYWwgLyBzdXBwY2VudGVyc2EuY29tQG0zong>

4. GLOBAL INCIDENTS WITH SA RELEVANCE

TA4922 (China-linked) Tax/Payroll/HR Lures Target SA -- Atlas RAT / RomulusLoader / Winos 4.0

The Hacker News weekly recap confirmed that financially motivated China-linked actor TA4922 expanded SA-targeted phishing in W25, using tax, payroll, and HR-themed lures to deliver Atlas RAT, RomulusLoader, and the Winos 4.0 toolkit. The campaign is crimeware-motivated rather than espionage. No named SA victim has been confirmed, but the SA-specific lure themes mark a deliberate localisation. SA financial services, payroll bureaus, and HR functions should hunt for Atlas RAT / RomulusLoader / Winos 4.0 IOCs in inbound phishing.⁵

Oracle PeopleSoft CVE-2026-35273 Mass-Compromise -- ShinyHunters / UNC6240 (Global)

ShinyHunters / UNC6240 exploited Oracle PeopleSoft CVE-2026-35273 (CVSS 9.8) as a zero-day from 27 May, compromising 300+ internet-facing instances across 100+ organisations worldwide. The University of Nottingham disclosed 454,600 records affected. CISA added the CVE to KEV with a 15 June federal deadline. SA universities, government departments, and large enterprises running PeopleSoft HCM/ERP should assume compromise where the instance was internet-facing before patching, and hunt for UNC6240 web-shell and credential-theft activity.¹³¹⁶

PRODAFT "The Gentlemen" / LARVA-368 / Phantom Mantis -- 478-483 Victims, SA Confirmed

PRODAFT profiled the ransomware operation tracked as "The Gentlemen" / LARVA-368 / Phantom Mantis, documenting 478-483 total victims with South African organisations confirmed among them. The group uses self-propagating Go-based payloads and an extensive lateral-movement arsenal. The confirmed SA footprint elevates this from monitoring to active concern. SA enterprises should review LARVA-368 TTPs and validate east-west segmentation and lateral-movement detection.¹⁷

CYFIRMA: UNC5221 / Silk Typhoon (China APT) -- Edge-Device Espionage

CYFIRMA's "Threat Actor in Focus" profiled UNC5221 / Silk Typhoon (China-aligned), continuing edge-appliance and VPN-gateway exploitation for espionage. No confirmed SA targets at time of publication, but the actor's focus on Ivanti and other edge appliances is directly relevant given the W25 Ivanti Sentry KEV additions. SA organisations operating Ivanti and similar edge devices should review UNC5221 IOCs and prioritise the Ivanti Sentry patches.¹⁴

CISA BOD 26-04 (10 June) -- 3-Day Remediation Mandate for KEV

CISA issued Binding Operational Directive 26-04 on 10 June, compressing the remediation window for actively exploited KEV entries to three days for US federal civilian agencies. While SA organisations are not bound by the directive, it sets a de-facto international benchmark for KEV-driven patch urgency. SA SOCs should treat the 3-day standard as the new baseline expectation for actively exploited vulnerabilities, particularly the PeopleSoft, Ivanti Sentry, and Check Point gateway items below.²⁵

G7 Cybersecurity Declaration (8 June)

G7 leaders issued a Cybersecurity Declaration on 8 June reaffirming collective commitments on ransomware disruption, critical-infrastructure resilience, and secure-by-design software. The declaration signals continued multilateral pressure on ransomware ecosystems and supply-chain security expectations that increasingly flow to vendors serving SA organisations. SA technology suppliers exporting to G7 markets should track resulting procurement and disclosure expectations.²³

5. The Hacker News -- Weekly recap (TA4922 SA lures; PeopleSoft 0-day) —

<https://thehackernews.com/2026/06/weekly-recap-instagram-account-hacks.html?m=1>

13. Oracle -- June 2026 Critical Patch Update (PeopleSoft CVE-2026-35273) — <https://www.oracle.com/security-alerts/>

14. CYFIRMA -- UNC5221 / Silk Typhoon threat actor profile — <https://www.cyfirma.com/news/>

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

17. PRODAFT -- The Gentlemen / LARVA-368 / Phantom Mantis ransomware report — <https://www.prodaft.com/resources>

23. European Council / G7 -- TTE Council and G7 Cybersecurity Declaration (8-9 June 2026) — <https://www.consilium.europa.eu/>

25. CISA -- Binding Operational Directive 26-04 (10 June 2026) — <https://www.cisa.gov/>

5. THREAT ACTORS

5.1 ShinyHunters / UNC6240 — Oracle PeopleSoft Mass-Compromise (CVE-2026-35273)

ShinyHunters / UNC6240 is the dominant W25 actor, exploiting Oracle PeopleSoft CVE-2026-35273 (CVSS 9.8) as a zero-day from 27 May. The campaign compromised 300+ internet-facing instances across 100+ organisations, with the University of Nottingham disclosing 454,600 affected records. CISA added the CVE to KEV with a 15 June federal deadline. SA universities, government HCM/ERP deployments, and large enterprises running PeopleSoft should assume compromise where instances were internet-facing prior to patching and hunt for UNC6240 web-shell and credential-theft indicators.⁵¹³

5.2 The Gentlemen / LARVA-368 / Phantom Mantis — 478-483 Victims, SA Confirmed (PRODAFT)

PRODAFT's report on the ransomware operation tracked as "The Gentlemen" / LARVA-368 / Phantom Mantis documented 478-483 total victims, with South African organisations confirmed among them. The group deploys self-propagating Go-based payloads with an extensive lateral-movement arsenal. The confirmed SA footprint moves this group from regional monitoring to an active SA concern. SA enterprises should review LARVA-368 TTPs and validate east-west segmentation, privileged-access controls, and lateral-movement detection.¹⁷

5.3 Lynx Ransomware — SABS Attribution Tabled in Parliament (12 June)

The Lynx ransomware attribution to the November 2024 SABS attack was formally tabled in the parliamentary record on 12 June, with the SABS executive accountability proceedings referencing failure to implement prior SSA and Auditor-General cybersecurity recommendations. This remains the leading SA precedent for tying C-suite accountability to documented governance failures. Every SA board and executive holding unactioned AGSA cybersecurity findings should treat this as a direct governance-risk precedent.²²

5.4 Threat Actor Summary — W25

Actor	Type	Notable W25 Activity	Source
ShinyHunters / UNC6240	Criminal / data theft	PeopleSoft CVE-2026-35273 0-day from 27 May; 300+ instances / 100+ orgs; Nottingham 454,600 records; KEV 15 Jun	Oracle, THN, CISA
The Gentlemen / LARVA-368 / Phantom Mantis	Ransomware	PRODAFT: 478-483 victims; SA organisations confirmed; self-propagating Go payloads	PRODAFT
UNC5221 / Silk Typhoon	China APT	CYFIRMA profile; edge-appliance/VPN espionage; relevant to W25 Ivanti Sentry KEV	CYFIRMA
TA4922 (China-linked)	Fin. crimeware	W25 SA tax/payroll/HR lures -> Atlas RAT / RomulusLoader / Winos 4.0; no named SA victim	The Hacker News
ROOTBOY	Criminal	Standard Bank 1.2 TB dataset remains in open domain (W24); continued IR/fraud scrutiny	ITWeb, EWN
NightSpire	Ransomware	EC Human Settlements (Nov 2025) + Ingonyama Trust breaches tabled in Portfolio Committee 11 Jun	Parliament record
M3RX / SuppCenter	Extortion portal	SuppCenter Global/SA (Xcitium/Comodo MSSP) listed on M3RX 11 Jun; CLAIMED, unacknowledged	Ransomware.live
Lynx	Ransomware	SABS Nov 2024 attribution tabled in parliamentary record 12 Jun; C-suite accountability precedent	Parliament record
Nullsec / 404 Crew / Infernalis	Hacktivist	#OpSouthAfrica reaffirmed claims; no new verified SA victim acknowledgements	Multiple
Webworm (China APT)	State espionage	No new Africa victims W25; prior SA university compromise stands	ESET
Oday Syndicate	Ransomware	Continued global listings; no new confirmed Africa victims W25	Cyble
Black X	Ransomware	ANC claim (W24) STILL UNVERIFIED; HudsonRock telemetry showed only 3 compromised users	Black X leak site
SideWinder (suspected India)	APT	Africa nuclear + maritime targeting continuing from prior weeks	WhoisXML

5.5 Notable Industry Intelligence Actions (W25)

CISA BOD 26-04 (10 June): CISA compressed the KEV remediation window to three days for actively exploited vulnerabilities affecting US federal civilian agencies. SA SOCs should adopt the 3-day standard as the de-facto international benchmark for the PeopleSoft, Ivanti Sentry, Chrome V8, and Check Point gateway items now in KEV.²⁵

PRODAFT The Gentlemen / LARVA-368 report: The 478-483-victim profile with confirmed SA organisations is the most authoritative dataset to date on this operation's SA exposure and validates lateral-movement detection as the priority control.¹⁷

5. The Hacker News -- Weekly recap (PeopleSoft 0-day; TA4922 SA lures) —

<https://thehackernews.com/2026/06/weekly-recap-instagram-account-hacks.html?m=1>

13. Oracle -- June 2026 Critical Patch Update (PeopleSoft CVE-2026-35273) — <https://www.oracle.com/security-alerts/>

17. PRODAFT -- The Gentlemen / LARVA-368 / Phantom Mantis ransomware report — <https://www.prodaft.com/resources>

22. Parliament -- Portfolio Committee record (NightSpire, SABS/Lynx tabling, 10-12 June 2026) — <https://www.parliament.gov.za/>

25. CISA -- Binding Operational Directive 26-04 (10 June 2026) — <https://www.cisa.gov/>

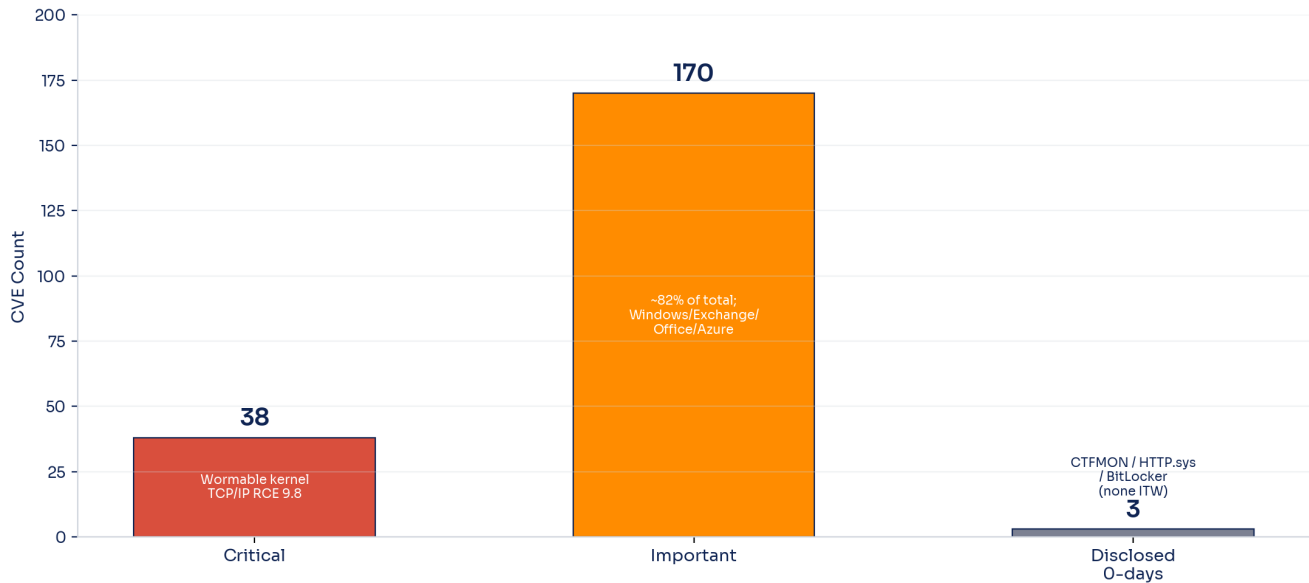
6. CRITICAL VULNERABILITIES & CISA KEV

W25 was dominated by the record-setting 9 June Patch Tuesday and a dense wave of KEV additions.

Microsoft shipped 208 CVEs (38 Critical, 3 disclosed zero-days, none exploited in the wild) — the largest Patch Tuesday in program history. The standout fix is **CVE-2026-45657**, a wormable Windows kernel TCP/IP RCE at CVSS 9.8 that should be every SA estate's #1 June patch; the Exchange OWA permanent patch **CVE-2026-42897** also finally shipped via **KB5094139**. Newly KEV-listed and SA-relevant items include **Oracle PeopleSoft CVE-2026-35273** (KEV 15 Jun), **Ivanti Sentry CVE-2026-10520 / -10523** (KEV 14 Jun), **Chrome V8 CVE-2026-11645** (ITW, KEV 23 Jun), and **Check Point Gateway CVE-2026-50751** (KEV 11 Jun, 3-day deadline). **Cisco SD-WAN CVE-2026-20245** remains its seventh exploited zero-day of 2026 with still no patch.¹¹¹⁶¹⁸

W25 Patch Tuesday Severity Overview — (Record 208 CVEs, 38 Critical, 3 Zero-Days, 9 June)

MICROSOFT JUNE 2026 PATCH TUESDAY BY SEVERITY | 9 June 2026
Record 208 CVEs (largest in program history) -- 38 Critical / ~170 Important / 3 disclosed 0-days (none exploited at release)



W25 CISA KEV / Critical CVE Tracking (9 June Patch Tuesday + KEV additions)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-45657	Microsoft / Windows Kernel TCP/IP	9.8	Wormable RCE	9 Jun PT	TOP PRIORITY June patch; wormable network-stack RCE; deploy full June rollout estate-wide
CVE-2026-35273	Oracle / PeopleSoft	9.8	0-day RCE	15 Jun 2026	ShinyHunters/UNC6240 ITW since 27 May; 300+ instances / 100+ orgs; Nottingham 454,600 records
CVE-2026-10520	Ivanti / Sentry	10.0	Unauth RCE	14 Jun 2026	Weaponised <24h after patch; paired with CVE-2026-10523 (9.9); edge-appliance espionage (UNC5221)
CVE-2026-50751	Check Point / Security Gateway (IKEv1)	n/a	Exploited	11 Jun (3-day)	KEV 11 Jun with 3-day deadline; IKEv1 VPN gateway; patch immediately if IKEv1 enabled
CVE-2026-47291	Microsoft / HTTP.sys	9.8	Unauth RCE	9 Jun PT	Network-facing IIS/HTTP.sys RCE; prioritise on all internet-exposed Windows web servers
CVE-2026-42897	Microsoft / Exchange OWA (2016, 2019, SE)	8.1	XSS/Spoofing	RESOLVED	PERMANENT patch shipped 9 Jun via KB5094139; remove EEMS M2 after Health Checker confirms healthy
CVE-2026-11645	Google / Chrome V8	n/a	Type confusion	23 Jun 2026	Exploited in the wild; KEV 23 Jun; push browser update + restart estate-wide
CVE-2026-45447	OpenSSL (PKCS7_verify)	CRITICAL	Heap UAF	9 Jun advisory	18-CVE OpenSSL advisory; inventory containerised + statically linked deployments; rebuild and redeploy
CVE-2026-44748	SAP / NetWeaver (SAML)	9.9	Auth bypass	Patch NOW	Paired with CVE-2026-27671 ABAP (9.8); patch SAP June 2026 security notes immediately
CVE-2026-20245	Cisco / SD-WAN (all editions)	n/a	0-day RCE	NO PATCH	7th SD-WAN 0-day 2026 PERSISTING; KEV 9 Jun; Mandiant ITW; collect admin-tech logs, no patch yet
CVE-2026-0257	Palo Alto / PAN-OS GlobalProtect	9.3	Auth bypass	19 Jun 2026	W23 carryover; ITW continuing; complete patch programme ahead of federal deadline

Pattern note: The 9 June Patch Tuesday is the largest in Microsoft's program history at 208 CVEs (38 Critical, 3 disclosed zero-days, none exploited in the wild). The wormable Windows Kernel TCP/IP RCE (CVE-2026-45657, CVSS 9.8) is the single most important June patch for SA estates. Cisco SD-WAN's seventh exploited zero-day of 2026 (CVE-2026-20245) PERSISTS with no patch — a continuation of the W24 pattern, not a new development. SA organisations should treat the full June rollout as a single high-priority change event.

6.1 Oracle PeopleSoft CVE-2026-35273 (0-day, KEV 15 June) -- ShinyHunters/UNC6240 Mass-Compromise

CVE-2026-35273 (CVSS 9.8) is an unauthenticated RCE in Oracle PeopleSoft exploited as a zero-day by ShinyHunters/UNC6240 from 27 May, before the June Critical Patch Update. 300+ internet-facing instances across 100+ organisations were compromised, including the University of Nottingham (454,600 records). CISA added the CVE to KEV with a 15 June federal deadline. SA relevance is HIGH: PeopleSoft underpins HCM/ERP at SA universities, government departments, and large enterprises. Any instance that was internet-facing before patching should be treated as compromised; hunt for web shells, anomalous service-account activity, and bulk data egress.¹³¹⁶

6.2 Cisco SD-WAN CVE-2026-20245 (PERSISTING 0-day) + Carryover Deadlines (W25 Status)

Cisco SD-WAN CVE-2026-20245 remains the seventh exploited SD-WAN zero-day of 2026 — PERSISTING from W24 with no patch and no workaround. Mandiant continues to observe exploitation resulting in configuration changes pushed to edge devices. SA telcos/ISPs and enterprise WAN edges should keep collecting admin-tech logs, restrict netadmin access to out-of-band management, and monitor for configuration drift pending a Cisco fix.¹⁸

CVE	Status W25
Cisco SD-WAN CVE-2026-20245 (0-day)	PERSISTING from W24; KEV 9 Jun; STILL NO patch; 7th SD-WAN 0-day of 2026; collect admin-tech logs
PAN-OS GlobalProtect CVE-2026-0257 (CVSS 9.3)	W23 carryover; KEV deadline 19 Jun UPCOMING; ITW continuing; complete patch programme
SolarWinds Serv-U CVE-2026-28318 (7.5)	KEV deadline 19 Jun UPCOMING; patch 15.5.4 HF1; audit external Serv-U exposure
Citrix NetScaler CVE-2026-3055 (9.8)	Carryover; mass exploitation continuing against SAML IDP; patch 13.1-62.23 / 14.1-60.58
Windows Netlogon CVE-2026-41089 (9.8)	Carryover; ensure 12 May PT applied across all DCs; rotate krbtgt if any DC was exposed
SAP NetWeaver CVE-2026-44748 (9.9) + CVE-2026-27671 (9.8)	New June SAP notes; SAML auth bypass + ABAP RCE; patch immediately
Chrome V8 CVE-2026-11645	Exploited ITW; KEV 23 Jun; push browser update + restart estate-wide
Ivanti Sentry CVE-2026-10520 (10.0) + CVE-2026-10523 (9.9)	KEV 14 Jun; weaponised <24h after patch; UNC5221 edge-appliance focus; patch now

EXCHANGE OWA CVE-2026-42897 -- PERMANENT PATCH SHIPPED 9 JUNE (KB5094139) -- RESOLVED

Status: RESOLVED. The permanent patch shipped on 9 June Patch Tuesday via KB5094139, closing the four-week patchless window that ran from the W22 KEV deadline (29 May) through the EEMS M2 interim mitigation period.

Action now: Apply KB5094139 across all Exchange 2016, 2019, and Subscription Edition servers. Run Exchange Health Checker (aka.ms/ExchangeHealthChecker) to confirm the patch is applied and the server reports a healthy state.

Remove M2: Remove the EEMS Mitigation ID M2 interim mitigation ONLY after KB5094139 is confirmed applied and Health Checker shows healthy. Removing M2 restores OWA Print Calendar, inline images, and OWA Light functionality broken under M2.

Verification: Confirm no residual EEMS M2 entries remain after patch validation; document the change in the June rollout change record.

6.3 Ivanti Sentry CVE-2026-10520 (CVSS 10.0) + CVE-2026-10523 (9.9) -- KEV 14 June

Ivanti Sentry CVE-2026-10520 (CVSS 10.0) is an unauthenticated RCE that was weaponised within 24 hours of patch release, paired with CVE-2026-10523 (9.9). CISA added both to KEV with a 14 June deadline. The vulnerabilities align with UNC5221 / Silk Typhoon's documented focus on edge appliances. SA relevance is HIGH: Ivanti Sentry sits at the network edge in SA enterprise and public-sector mobility stacks. Patch immediately, audit for post-exploitation web shells, and treat any internet-facing Sentry as a priority assume-breach target.¹⁴¹⁶

11. PDQ -- Patch Tuesday June 2026 (record 208 CVEs, 38 Critical, 3 zero-days) — <https://www.pdq.com/blog/patch-tuesday-june-2026/>

13. Oracle -- June 2026 Critical Patch Update (PeopleSoft CVE-2026-35273) — <https://www.oracle.com/security-alerts/>

14. Ivanti -- Sentry Security Advisory (CVE-2026-10520 / CVE-2026-10523) — <https://www.ivanti.com/blog/topics/security-advisory>

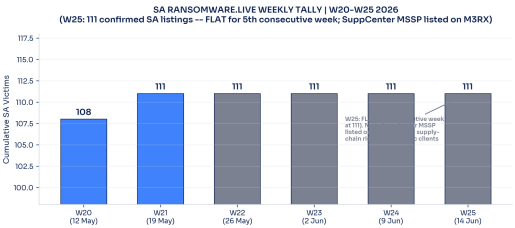
15. Google -- Chrome Releases (V8 CVE-2026-11645 exploited in the wild) — <https://chromereleases.googleblog.com/>

16. CISA KEV Catalog -- Known Exploited Vulnerabilities — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
18. Help Net Security -- June 2026 Patch Tuesday / Cisco SD-WAN CVE-2026-20245 — <https://www.helpnetsecurity.com/2026/06/05/june-2026-patch-tuesday-forecast/>
19. OpenSSL -- Security Advisory (18-CVE advisory incl. CVE-2026-45447 PKCS7 heap UAF) — <https://www.openssl.org/news/secadv/>

7. RANSOMWARE LANDSCAPE

SA ransomware.live victim count remains at **111 cumulative (FLAT)** for W25, with **zero new listings** on the ransomware.live tracker during 7–14 June 2026. The count is now unchanged from W21 through W24 — a **fifth consecutive week FLAT at 111**. The only notable new development is the SuppCenter Global/SA listing on the M3RX dark-web portal (11 June), which is tracked as CLAIMED and not yet reflected as a confirmed ransomware.live country-map increment.²⁰

SA Contextualisation: The FLAT count is now a five-week streak (W21, W22, W23, W24, and W25 all FLAT at 111). This should not be interpreted as a reduction in ransomware risk. The W25 AVBOB disruption, the SAPS Western Cape POPIA breach, the Cannabis Club Systems API leak, and the SuppCenter/M3RX MSSP listing all demonstrate that the criminal ecosystem remains active and is increasingly active against SA targets outside the ransomware.live tracking mechanism. The PRODAFT The Gentlemen / LARVA-368 profile (478–483 victims, SA confirmed) and the parliamentary tabling of NightSpire and SABS/Lynx incidents show that ransomware consequences continue to surface through regulatory and governance channels.¹⁰



End W24 baseline	111 confirmed SA listings
New W25 listings (7 - 14 Jun)	0 confirmed on ransomware.live
End W25 count	111 (FLAT -- 5th consecutive week, unchanged from W21-W24)
New W25 development	SuppCenter Global/SA (Xcitium/Comodo MSSP) listed on M3RX 11 Jun -- CLAIMED
SA-confirmed external profile	PRODAFT The Gentlemen / LARVA-368: 478-483 victims, SA orgs confirmed
Threat level drivers (non-ransomware.live)	AVBOB disruption; SAPS WC POPIA breach; Cannabis Club Systems API leak

10. Ransomware.live -- SuppCenter Global/SA listing (M3RX, 11 June 2026) — <https://www.ransomware.live/id/c3VwcGNlbnRlci5nbG9iYWwgLyBzdXBwY2VudGVyc2EuY29tQG0zcng>
20. Ransomware.live -- South Africa country map (W25) — <https://www.ransomware.live/map/ZA>

8. OSINT EXPOSURE & ATTACK SURFACE

AVBOB platform disruption -- insurance/funeral-services supply-chain exposure review

AVBOB's 350+ branches reverting to manual operations after the 7-8 June disruption highlights the operational fragility of consolidated digital platforms in the insurance and funeral-services sector. SA insurers and funeral-services peers should map dependence on shared infrastructure, broker portals, and payment service providers; segment third-party exposure; and verify POPIA s.22 notification readiness in case the forensic audit confirms data exfiltration.¹²

SAPS Western Cape POPIA breach -- internal HR disclosure of special personal information

The leak of 2,978 SAPS officers' diagnostic medical records via an HR email attachment shows that inadvertent internal disclosure of special personal information is a notifiable POPIA compromise. SA HR functions and special-category data processors should audit internal data-sharing workflows, restrict attachment distribution of sensitive records, and confirm Information Officer registration and breach-notification triggers cover internal disclosure events.⁴

Oracle PeopleSoft CVE-2026-35273 -- SA HCM/ERP attack surface

With 300+ PeopleSoft instances compromised globally by ShinyHunters/UNC6240, every internet-facing PeopleSoft deployment in SA universities, government, and large enterprises is a priority attack-surface item. Identify all PeopleSoft instances, patch ahead of the 15 June KEV deadline, and treat any instance that was internet-facing before patching as compromised — hunt for web shells, anomalous service-account use, and bulk data egress.⁵¹³

GroundUp Part 2 -- non-SITA gov.za attack surface (4,466 CVEs)

GroundUp's Part 2 inventory of 516 non-SITA government hosts documented 4,466 CVEs with 1-in-5 hosts vulnerable, including Amathole's 353 CVEs, an internet-exposed IJS RDP with unpatched SMBGhost, 17 operational PPTP VPNs, and a confirmed Ekurhuleni VPN compromise. SA SOCs serving public-sector clients should treat the GroundUp inventory as a remediation-prioritisation baseline and escalate RDP/PPTP/SMBGhost exposures first.⁶⁹

Ivanti Sentry CVE-2026-10520 / -10523 -- edge-appliance exposure

The Ivanti Sentry CVSS 10.0 / 9.9 pair, weaponised within 24 hours of patch and aligned with UNC5221 / Silk Typhoon edge-appliance targeting, makes every internet-facing Sentry an immediate exposure. Identify all Sentry instances, patch ahead of the 14 June KEV deadline, audit for post-exploitation web shells, and place edge appliances on an assume-breach footing.¹⁴¹⁶

POPIA enforcement expansion -- physical-media disposal and internal disclosure now notifiable

The Department of Employment & Labour suspension over reckless physical disposal of job-seekers' data, combined with the SAPS WC internal-disclosure breach, confirms that POPIA security-safeguard obligations extend to physical-media destruction and internal sharing, not only digital exfiltration. SA organisations should verify secure-destruction procedures for paper records and confirm internal disclosure events trigger POPIA breach assessment.⁸

9. REGULATORY & COMPLIANCE

IR Loses Leave to Appeal Matric-Results Judgment

The Information Regulator lost its application for leave to appeal in the matric-results publication matter, leaving the December 2025 Full Bench judgment in control. That judgment's "without diligence and without more" test now governs the standard for assessing POPIA processing-condition compliance. SA Information Officers and privacy counsel should re-read internal POPIA assessment frameworks against the Full Bench standard, which raises the bar for demonstrating diligent processing.²⁴

SARB Financial Stability Review (10 June) + NPS Authorisation Framework Comment Deadline (15 June)

SARB published its June 2026 Financial Stability Review on 10 June, raising the countercyclical capital buffer (CCyB) to 1% and confirming the digital-rand programme is paused. Separately, the comment deadline for the SARB NPS Activity-Based Authorisation Framework closes 15 June, and the Capital Flow Management Regulations comment window was extended to 30 June. SA banks, PSPs, and fintechs should file NPS framework comments before 15 June and brief treasury teams on the CCyB increase.²¹

B15/2026 AML/CFT Bill to Standing Committee (10 June)

The B15/2026 AML/CFT Bill advanced to the Standing Committee on 10 June, continuing SA's post-FATF-greylisting legislative programme. The Bill tightens beneficial-ownership, reporting, and supervisory provisions across accountable institutions. SA accountable institutions should brief finance and legal teams on the anticipated obligations and track the Standing Committee timeline alongside existing FICA and exchange-control compliance work.²²

SA National AI Policy -- Rosman Panel, November 2026 Target

The revised SA National AI Policy is now being developed by an expert panel under Prof. Benjamin Rosman (Wits MIND), with a Cabinet-approval target of November 2026. SA organisations deploying AI should continue comment preparation aligned to the November 2026 target. EU AI Act Article 4 literacy obligations for 2 August 2026 remain unaffected by SA timelines — EU-operating SA organisations remain in scope.²³

Other W25 Regulatory Developments

- **EU CSA2 / NIS2 (9 June TTE Council):** The Cyber Solidarity Act 2 / NIS2 package was EXAMINED but NOT adopted at the Transport, Telecommunications and Energy Council on 9 June; negotiations continue. SA technology exporters to the EU should keep tracking high-risk ICT supplier designation criteria.²³
- **EU AI Act Omnibus -- European Parliament vote 16 June:** The European Parliament is scheduled to vote on the AI Act Digital Omnibus on 16 June. Article 4 AI-literacy obligations remain due 2 August 2026 regardless of Omnibus deferrals; all EU-operating SA organisations are in scope.²³
- **UK DUAA s.164A live 19 June 2026:** The Data (Use and Access) Act complaints-handling duty under s.164A goes live on 19 June — within 5 days of this report. Internal data-protection complaints processes become mandatory with defined acknowledgement timelines.²⁴
- **CISA BOD 26-04 (10 June):** Binding Operational Directive 26-04 mandates 3-day remediation of actively exploited KEV vulnerabilities for US federal civilian agencies; SA SOCs should adopt the standard as a benchmark.²⁵
- **G7 Cybersecurity Declaration (8 June):** G7 leaders reaffirmed collective commitments on ransomware disruption, critical-infrastructure resilience, and secure-by-design software, signalling continued supply-chain security expectations for vendors serving SA organisations.²³

Compliance Deadlines — W25 Forward View

Date	Item	Owner
14 Jun 2026	CISA KEV: Ivanti Sentry CVE-2026-10520 / -10523 deadline	IT
15 Jun 2026	CISA KEV: Oracle PeopleSoft CVE-2026-35273 federal deadline	IT
15 Jun 2026	SARB NPS Activity-Based Authorisation Framework comment deadline	Compliance
16 Jun 2026	EU AI Act Digital Omnibus -- European Parliament vote	Compliance
19 Jun 2026	UK DUAA s.164A complaints-handling duty live	Compliance
19 Jun 2026	CISA KEV: PAN-OS GlobalProtect CVE-2026-0257 + SolarWinds Serv-U deadlines	IT
23 Jun 2026	CISA KEV: Chrome V8 CVE-2026-11645 deadline	IT
30 Jun 2026	SARB Capital Flow Management Regulations comment window (extended)	Finance/Legal
2 Aug 2026	EU AI Act Art. 4 literacy obligations (unchanged)	Compliance
Nov 2026	SA National AI Policy Cabinet approval target (Rosman panel)	Compliance
2 Dec 2026	EU AI Act watermarking/deepfake marking	Compliance

21. SARB -- Financial Stability Review June 2026 + NPS Activity-Based Authorisation Framework — <https://www.resbank.co.za/>
22. Parliament -- Standing Committee record (B15/2026 AML/CFT Bill, 10 June 2026) — <https://www.parliament.gov.za/>
23. European Council -- TTE Council 9 June + EU AI Act Omnibus / G7 Declaration — <https://www.consilium.europa.eu/>
24. UK ICO -- DUAA s.164A complaints-handling guidance (live 19 June 2026) — <https://ico.org.uk/>
25. CISA -- Binding Operational Directive 26-04 (10 June 2026) — <https://www.cisa.gov/>

10. WEEKLY THREAT HUNT & IOCs

Eight hunt missions are active for W25. Two P1 missions address the Oracle PeopleSoft CVE-2026-35273 mass-compromise and the wormable Windows Kernel TCP/IP RCE (CVE-2026-45657) from the record 9 June Patch Tuesday. Two P2 missions address the Ivanti Sentry edge-appliance KEV pair and the TA4922 SA tax/payroll/HR lure campaign delivering Atlas RAT / RomulusLoader / Winos 4.0. Two P2 missions address the AVBOB incident impact assessment and the SAPS Western Cape internal HR disclosure. Two P3 missions address the SuppCenter/M3RX MSSP supply-chain claim and the GroundUp non-SITA gov.za attack-surface baseline.

TH-2026-W25-01 — Oracle PeopleSoft CVE-2026-35273 (0-day, KEV 15 Jun) -- Mass-Compromise Hunt

Hypothesis: ShinyHunters/UNC6240 exploited PeopleSoft CVE-2026-35273 as a 0-day from 27 May, compromising 300+ instances across 100+ organisations. Any SA PeopleSoft instance that was internet-facing before patching should be assumed compromised.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1505.003 (Web Shell), T1078 (Valid Accounts), T1567 (Exfiltration Over Web Service).

IOCs: Unexpected files / web shells in PeopleSoft PIA web directories; anomalous PS service-account authentication; bulk record exports; outbound connections to unfamiliar IPs from PeopleSoft app/web tiers.

Data Sources: PeopleSoft PIA web-server logs, application-server logs, database audit logs, web-tier file-integrity monitoring, egress netflow.

Detection Guidance: Inventory all PeopleSoft instances and confirm internet exposure history. Patch ahead of the 15 June KEV deadline. For any previously internet-facing instance: hunt for web shells via file-integrity baselines, review PS service-account auth, and alert on bulk data export and anomalous egress. Treat pre-patch internet-facing instances as assume-breach.

P1 — CRITICAL: 0-day ITW since 27 May; KEV 15 Jun; 300+ instances / 100+ orgs

TH-2026-W25-02 — Windows Kernel TCP/IP CVE-2026-45657 (Wormable RCE) + Full June Rollup**P1 — CRITICAL: wormable kernel RCE CVSS 9.8; record 208-CVE Patch Tuesday**

Hypothesis: The record 9 June Patch Tuesday (208 CVEs) includes CVE-2026-45657, a wormable Windows kernel TCP/IP RCE at CVSS 9.8. Unpatched estates face self-propagating network-stack exploitation; this is the single most important June patch.

MITRE ATT&CK: T1210 (Exploitation of Remote Services), T1190 (Exploit Public-Facing App), T1570 (Lateral Tool Transfer).

IOCs: Unexpected SMB/TCP-stack crashes or restarts; anomalous east-west network-stack traffic; new services or scheduled tasks created post-exploitation; lateral connection bursts from a single host.

Data Sources: Windows System / Security event logs, EDR network telemetry, internal netflow, patch-management compliance reports.

Detection Guidance: Deploy the full June security rollup estate-wide, prioritising CVE-2026-45657 and the HTTP.sys RCE CVE-2026-47291. Confirm patch compliance across all Windows hosts. Until fully patched, alert on anomalous network-stack crashes and lateral connection bursts. Treat the June rollup as a single high-priority change event.

TH-2026-W25-03 — Ivanti Sentry CVE-2026-10520 / -10523 (KEV 14 Jun) -- Edge-Appliance Hunt**P2 — HIGH: CVSS 10.0 / 9.9; KEV 14 Jun; weaponised <24h; UNC5221 edge focus**

Hypothesis: Ivanti Sentry CVE-2026-10520 (CVSS 10.0) and CVE-2026-10523 (9.9) were weaponised within 24 hours of patch and align with UNC5221 / Silk Typhoon edge-appliance targeting. Any internet-facing Sentry is at immediate risk.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1505.003 (Web Shell), T1133 (External Remote Services).

IOCs: Unexpected files / web shells on Sentry appliances; anomalous management-plane access; outbound connections from Sentry to unfamiliar IPs; configuration changes outside change windows.

Data Sources: Ivanti Sentry system/access logs, perimeter/WAF logs for Sentry endpoints, egress netflow, management-plane audit logs.

Detection Guidance: Identify all Sentry instances and patch ahead of the 14 June KEV deadline. Audit appliances for post-exploitation web shells and configuration tampering. Review UNC5221 IOCs. Place internet-facing Sentry on an assume-breach footing pending forensic validation.

TH-2026-W25-04 — TA4922 SA Tax/Payroll/HR Lures -- Atlas RAT / RomulusLoader / Winos 4.0**P2 — HIGH: confirmed W25 SA-targeted China-linked campaign; finance/payroll/HR focus**

Hypothesis: China-linked TA4922 expanded SA-targeted phishing in W25 using tax, payroll, and HR-themed lures delivering Atlas RAT, RomulusLoader, and Winos 4.0. SA financial services, payroll bureaus, and HR functions are the primary targets.

MITRE ATT&CK: T1566.001 (Spearphishing Attachment), T1204.002 (Malicious File), T1055 (Process Injection), T1071 (Application Layer Protocol C2).

IOCs: Tax/payroll/HR-themed phishing with malicious attachments or links; Atlas RAT / RomulusLoader / Winos 4.0 loader artefacts; anomalous process injection; C2 beacons to unfamiliar infrastructure from finance/HR endpoints.

Data Sources: Email gateway logs, EDR process-creation/injection telemetry, proxy/DNS logs, sandbox detonation results for inbound attachments.

Detection Guidance: Tune email-gateway detection for SA tax/payroll/HR lure themes. Hunt EDR for Atlas RAT / RomulusLoader / Winos 4.0 loader behaviour and process injection. Alert on C2 beaconing from finance and HR endpoints. Brief payroll and HR staff on the localised lure themes.

TH-2026-W25-05 — AVBOB Incident Impact -- Insurance/Funeral-Services Supply-Chain Assessment

P2 — HIGH: highest-profile SA private-sector disruption of the cycle; sector supply-chain risk

Hypothesis: AVBOB's 7-8 June disruption took 350+ branches to manual operations. Peers sharing infrastructure, broker portals, or payment service providers may face correlated exposure; the ransomware-versus-extortion-only question remains open pending forensics.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1486 (Data Encrypted for Impact), T1657 (Financial Theft).

IOCs: Service disruption or anomalous activity on shared insurance/funeral-services platforms; broker-portal authentication anomalies; AVBOB-related data appearing on leak sites; PSP-linked anomalies.

Data Sources: Broker-portal and PSP access logs, leak-site monitoring, shared-platform availability telemetry, SIEM for partner-integration anomalies.

Detection Guidance: Map dependence on shared infrastructure, broker portals, and PSPs. Segment third-party exposure. Verify POPIA s.22 notification readiness. Monitor indexed leak sites for any AVBOB claim. Review partner-integration access logs for anomalies during the incident window.

TH-2026-W25-06 — SAPS Western Cape Internal HR Disclosure -- POPIA Special-Category Data

P2 — HIGH: 2,978 records of special personal information; notifiable POPIA compromise

Hypothesis: An SAPS WC HR email exposed 2,978 officers' diagnostic medical records. Inadvertent internal disclosure of special personal information is a notifiable POPIA compromise; organisations with weak internal data-sharing controls face the same risk.

MITRE ATT&CK: Not applicable (governance/internal-disclosure hunt).

IOCs: Internal emails or shares circulating special-category staff data; attachments containing bulk sensitive records; absent or stale Information Officer registration; missing internal-disclosure breach triggers.

Data Sources: Email DLP logs, internal file-share audit logs, Information Officer registration records, internal incident register.

Detection Guidance: Audit internal data-sharing workflows for special personal information (health, vetting, HR). Implement DLP controls on bulk sensitive-record attachments. Confirm Information Officer registration and that breach-notification triggers cover internal disclosure, not only external exfiltration.

TH-2026-W25-07 — SuppCenter / M3RX MSSP Supply-Chain Claim -- Attestation and Access Review

P3 — MONITORING: CLAIMED, unacknowledged; MSSP supply-chain downstream risk

Hypothesis: SuppCenter Global/SA (Xcitium/Comodo MSSP) was listed on the M3RX dark-web portal on 11 June. The claim is unacknowledged (CLAIMED). Clients relying on the operator for managed security inherit downstream risk if the listing is valid.

MITRE ATT&CK: T1199 (Trusted Relationship), T1078 (Valid Accounts), T1190 (Exploit Public-Facing App).

IOCs: SuppCenter/Xcitium/Comodo-managed data appearing on M3RX; anomalous MSSP-originated access into client environments; unexpected use of MSSP service accounts or remote-access tooling.

Data Sources: M3RX leak-site monitoring, MSSP remote-access and service-account logs, client-side privileged-access audit logs.

Detection Guidance: Request a breach-status attestation from the MSSP. Review and constrain all MSSP third-party access pathways and service-account privileges. Monitor M3RX for data publication. Alert on anomalous MSSP-originated access into client environments.

TH-2026-W25-08 — GroundUp Non-SITA gov.za Attack Surface -- Remediation-Prioritisation Baseline

P3 — MONITORING: 4,466 CVEs; 1-in-5 hosts vulnerable; governance gap on non-SITA estate

Hypothesis: GroundUp Part 2 documented 4,466 CVEs across 516 non-SITA gov.za hosts (1-in-5 vulnerable), including internet-exposed IJS RDP with SMBGghost, 17 PPTP VPNs, and a confirmed Ekurhuleni VPN compromise. SOCs serving public-sector clients should baseline against this inventory.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1133 (External Remote Services), T1210 (Exploitation of Remote Services).

IOCs: Internet-exposed RDP (3389) on government hosts; operational PPTP VPN endpoints; unpatched SMBGghost (CVE-2020-0796) signatures; VPN compromise indicators (Ekurhuleni precedent).

Data Sources: External attack-surface scans, perimeter firewall/VPN logs, government-host vulnerability inventories, GroundUp Part 2 dataset.

Detection Guidance: Use the GroundUp Part 2 inventory as a remediation-prioritisation baseline for public-sector clients. Escalate internet-exposed RDP, PPTP VPNs, and SMBGghost first. Validate VPN configurations against the Ekurhuleni compromise pattern. Track Amathole's 353-CVE host cluster as a priority.

IOC Master Table — W25

Indicator	Type	Attribution	Hunt ID
CVE-2026-35273 (Oracle PeopleSoft web shells)	CVE/0-day	ShinyHunters/UNC6240 ITW since 27 May; KEV 15 Jun; 300+ instances	TH-2026-W25-01
CVE-2026-45657 (Windows Kernel TCP/IP)	CVE	Wormable RCE CVSS 9.8; 9 Jun Patch Tuesday; top June priority	TH-2026-W25-02
CVE-2026-47291 (Windows HTTP.sys)	CVE	Unauth RCE CVSS 9.8; 9 Jun Patch Tuesday	TH-2026-W25-02
CVE-2026-10520 / -10523 (Ivanti Sentry)	CVE	CVSS 10.0 / 9.9; KEV 14 Jun; weaponised <24h; UNC5221 edge focus	TH-2026-W25-03
Atlas RAT / RomulusLoader / Winos 4.0 loaders	Malware	TA4922 (China-linked) SA tax/payroll/HR lures (W25)	TH-2026-W25-04
CVE-2026-11645 (Chrome V8 type confusion)	CVE	Exploited ITW; KEV 23 Jun; estate-wide browser update	TH-2026-W25-02
CVE-2026-45447 (OpenSSL PKCS7_verify heap UAF)	CVE	Critical; 18-CVE OpenSSL advisory 9 Jun; rebuild static/container	TH-2026-W25-02
CVE-2026-50751 (Check Point Gateway IKEv1)	CVE	Exploited; KEV 11 Jun; 3-day deadline; IKEv1 VPN gateways	TH-2026-W25-03
SuppCenter / Xcitium / Comodo data on M3RX	Leak-site	SuppCenter Global/SA MSSP listed 11 Jun; CLAIMED	TH-2026-W25-07
CVE-2026-20245 (Cisco SD-WAN admin-tech logs)	CVE/0-day	7th SD-WAN 0-day 2026 PERSISTING; KEV 9 Jun; STILL no patch	N/A (carryover)

11. RECOMMENDATIONS

Immediate (This Week — Priority P1)

- **1. Oracle PeopleSoft CVE-2026-35273 (0-day, KEV 15 June):** Inventory all PeopleSoft instances and patch ahead of the 15 June KEV deadline. Treat any instance that was internet-facing before patching as compromised — hunt for web shells in PIA web directories, review service-account authentication, and alert on bulk data export and anomalous egress. This is the dominant W25 mass-compromise.

- **2. Windows June rollup (record 208 CVEs) -- wormable kernel RCE is the #1 priority:** Deploy the full 9 June security rollup estate-wide, prioritising CVE-2026-45657 (wormable Windows Kernel TCP/IP RCE, CVSS 9.8) and CVE-2026-47291 (HTTP.sys RCE, CVSS 9.8). Confirm patch compliance across all Windows hosts and treat the rollup as a single high-priority change event.
- **3. Exchange OWA CVE-2026-42897 -- apply permanent patch KB5094139 (RESOLVED):** Apply KB5094139 across all Exchange 2016/2019/SE servers. Run Exchange Health Checker to confirm the patch is applied and healthy. Remove the EEMS M2 interim mitigation only after the permanent patch is confirmed.
- **4. Ivanti Sentry CVE-2026-10520 / -10523 (KEV 14 June):** Identify all Sentry instances and patch ahead of the 14 June deadline. Audit edge appliances for post-exploitation web shells and configuration tampering. Place internet-facing Sentry on an assume-breach footing; review UNC5221 IOCs.
- **5. Check Point Gateway CVE-2026-50751 (KEV 11 June, 3-day deadline):** If IKEv1 is enabled on any Check Point Security Gateway, patch immediately and review VPN access logs for exploitation indicators.
- **6. OpenSSL 18-CVE advisory incl. CVE-2026-45447 (critical PKCS7 heap UAF):** Inventory all OpenSSL deployments including containerised and statically linked builds; rebuild and redeploy affected artefacts.
- **7. TA4922 SA tax/payroll/HR lures (Atlas RAT / RomulusLoader / Winos 4.0):** Tune email-gateway detection for SA tax/payroll/HR lure themes; hunt EDR for the loader families and process injection; alert on C2 beaconing from finance and HR endpoints; brief payroll and HR staff.
- **8. POPIA internal-disclosure readiness (SAPS WC + Labour precedents):** Audit internal data-sharing workflows for special personal information; apply DLP controls on bulk sensitive attachments; verify secure-destruction procedures for paper records; confirm Information Officer registration and that breach triggers cover internal disclosure.

Short-Term (Next 30 Days)

- AVBOB incident impact: insurance/funeral-services peers to map dependence on shared infrastructure, broker portals, and PSPs; segment third-party exposure; verify POPIA s.22 notification readiness pending forensic outcome.
- GroundUp Part 2 non-SITA gov.za baseline: SA SOCs serving public-sector clients to use the 4,466-CVE inventory as a remediation-prioritisation baseline; escalate internet-exposed RDP, PPTP VPNs, and SMBGhosts first; track Amathole's 353-CVE host cluster.
- SARB NPS Activity-Based Authorisation Framework: file comments before the 15 June deadline; brief treasury on the CCyB increase to 1%; track the Capital Flow Management Regulations window to 30 June.
- PAN-OS GlobalProtect CVE-2026-0257 + SolarWinds Serv-U CVE-2026-28318 (KEV deadlines 19 June): complete patch programmes; Chrome V8 CVE-2026-11645 estate-wide browser update ahead of 23 June.
- Cisco SD-WAN CVE-2026-20245 (PERSISTING 0-day, no patch): keep collecting admin-tech logs, restrict netadmin to out-of-band, monitor configuration drift, and prepare an emergency patch window for when Cisco ships a fix.
- UK DUAA s.164A (live 19 June): EU/UK-operating SA organisations to stand up the mandatory complaints-handling process with defined acknowledgement timelines.
- B15/2026 AML/CFT Bill: brief finance and legal teams on anticipated beneficial-ownership and reporting obligations; track the Standing Committee timeline.

Strategic (Next Quarter)

- PeopleSoft / ERP exposure programme: treat the ShinyHunters/UNC6240 mass-compromise as a wake-up for internet-facing ERP/HCM. Establish an assume-breach validation cycle and remove unnecessary internet exposure for PeopleSoft and similar platforms across SA universities, government, and enterprise.
- Edge-appliance security programme: the Ivanti Sentry CVSS 10.0 pair (weaponised <24h) and UNC5221 / Silk Typhoon edge focus warrant a structured edge-appliance lifecycle programme — rapid patch SLAs, assume-breach monitoring, and reduced internet exposure for all edge/VPN gateways.
- Cisco SD-WAN zero-day programme: seven exploited zero-days in a single product line in one calendar year (PERSISTING) remains analytically unprecedented. SA organisations dependent on Cisco SD-WAN should continue formal architecture reviews for zero-day exposure reduction, including air-gapped management plane options and vendor diversification planning.
- POPIA enforcement trajectory: the SAPS WC internal-disclosure breach, the Labour Department physical-disposal suspension, and the IR's lost leave-to-appeal (Full Bench "without diligence and without more" test now controlling) collectively raise the diligence bar. SA privacy officers should re-baseline internal POPIA assessment frameworks accordingly.
- SA National AI Policy (Rosman panel, Nov 2026 target): prepare for the revised public-comment cycle; align internal AI-governance work with the EU AI Act Article 4 literacy obligations due 2 August 2026 for cross-border-operating SA organisations.

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. ITWeb -- Malicious actors take down AVBOB's digital platforms (8 June 2026) — <https://www.itweb.co.za/article/malicious-actors-take-down-avbobs-digital-platforms/5yONP7Erd6QMXWrb>
2. The Bulrushes -- Cyber attack disrupts AVBOB funeral services digital platforms (8 June 2026) — <https://thebulrushes.com/2026/06/08/cyber-attack-disrupts-avbob-funeral-services-digital-platforms/>
3. PDQ -- Patch Tuesday June 2026 analysis (208 CVEs) — <https://www.pdq.com/blog/patch-tuesday-june-2026/>
4. Cape Argus -- Confidential medical records of SAPS officers leaked (9 June 2026) — <https://capeargus.co.za/news/2026-06-09-shock-as-confidential-medical-records-of-3-000-saps-officers-leaked/>
5. The Hacker News -- Weekly recap: PeopleSoft 0-day, TA4922 SA lures (June 2026) — <https://thehackernews.com/2026/06/weekly-recap-instagram-account-hacks.html>
6. GroundUp -- Here's how insecure governments' websites are (11 June 2026) — <https://groundup.org.za/article/heres-how-insecure-governments-websites/>
7. Cybersecurity researcher disclosure -- Cannabis Club Systems API leak (June 2026) — <https://www.instagram.com/p/DZfCySwjukr/>
8. Sunday World -- Official suspended as Labour Department probes job-seekers data breach (11 June 2026) — <https://sundayworld.co.za/business/official-suspended-as-labour-department-probes-job-seekers-data-breach/>
9. GroundUp -- Insecure government websites investigation, Part 2 (11 June 2026) — <https://groundup.org.za/article/heres-how-insecure-governments-websites/>
10. Ransomware.live -- SuppCenter Global / SA listing on M3RX portal (11 June 2026) — <https://www.ransomware.live/>
11. Help Net Security -- June 2026 Patch Tuesday forecast / Cisco SD-WAN — <https://www.helpnetsecurity.com/2026/06/05/june-2026-patch-tuesday-forecast/>
13. Oracle -- Critical Patch Update, June 2026 (PeopleSoft CVE-2026-35273) — <https://www.oracle.com/security-alerts/>
14. CYFIRMA -- Ivanti Sentry / UNC5221 threat actor profile (June 2026) — <https://www.cyfirma.com/news/>
16. CISA KEV Catalog -- Known Exploited Vulnerabilities — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
17. PRODAFT -- The Gentlemen / LARVA-368 / Phantom Mantis threat profile (June 2026) — <https://www.prodaft.com/resources>
18. Help Net Security -- Cisco SD-WAN CVE-2026-20245 zero-day exploited — <https://www.helpnetsecurity.com/2026/06/05/june-2026-patch-tuesday-forecast/>
20. Ransomware.live -- South Africa country map — <https://www.ransomware.live/map/ZA>
21. SARB -- Financial Stability Review June 2026 / NPS Activity-Based Authorisation Framework — <https://www.resbank.co.za/>
22. Parliament of South Africa -- Portfolio / Standing Committee record (June 2026) — <https://www.parliament.gov.za/>
23. European Council -- TTE Council 9 June 2026 / EU AI Act Omnibus / G7 Cybersecurity Declaration — <https://www.consilium.europa.eu/>
24. UK ICO -- Data (Use and Access) Act s.164A complaints guidance (live 19 June 2026) — <https://ico.org.uk/>
25. CISA -- Binding Operational Directive 26-04 (10 June 2026) — <https://www.cisa.gov/>

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-W25 | Published Monday 15 June 2026