SOUTH AFRICA
CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 26 | 14 June – 21 June 2026

THREAT LEVEL: HIGH

FortiBleed: ~74,000 internet-facing Fortinet firewalls (~50% of global FortiGate) have valid plaintext credentials on the dark web; CISA emergency alert 18 June; significant SA exposure. Splunk Enterprise CVE-2026-20253 (9.8) pre-auth RCE actively exploited, KEV due 21 June. Google and Palo Alto attribute the 2026 GitHub/npm supply-chain campaign (~3,800 repos stolen in 11 minutes) to TeamPCP/ResoluteXBF, a single operator based in South Africa. AVBOB remains in partial restoration with no leak-site claim. SA ransomware count FLAT at 109 (6th consecutive week; corrected vs live screenshot 21 Jun).

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W26 | Classification: TLP:WHITE

Published Monday 22 June 2026

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH (unchanged, 6th consecutive week) — Week 26 (14–21 June 2026)

Story 1 — FortiBleed: ~74,000 Fortinet Firewalls With Plaintext Credentials Leaked: Roughly 74,000 internet-facing Fortinet FortiGate firewalls — about 50% of all internet-exposed FortiGate devices globally, spanning 21,632 domains across 194 countries — have valid usernames and plaintext passwords circulating on an attacker-controlled server. CISA issued an emergency alert on 18 June. SA exposure is significant across government, banking, retail, and ISPs. Organisations must check their domain at hudsonrock.com/fortinet, rotate all VPN and admin credentials, enable phishing-resistant MFA, and upgrade to FortiOS 7.2.11 / 7.4.8 / 7.6.1+.[1][2]

Story 2 — Splunk Enterprise CVE-2026-20253 (CVSS 9.8) Pre-Auth RCE, KEV Due Today: A pre-authentication RCE via an unauthenticated PostgreSQL sidecar endpoint affects Splunk Enterprise, with a CISA KEV deadline of 21 June. Splunk PSIRT confirmed limited in-the-wild exploitation on 18 June; watchTowr Labs published the full exploit chain on 12 June. Splunk is the SIEM of record across SA banks and telcos — a compromised Splunk blinds the SOC. Patch to 10.0.7 or 10.2.4; if unable to patch, disable the PostgreSQL sidecar and restrict management-interface access. Splunk Cloud Platform is not affected.[3]

Story 3 — TeamPCP / ResoluteXBF Supply-Chain Campaign Attributed to a South African Operator: Google and Palo Alto Networks publicly attributed the most damaging open-source software supply-chain campaign of 2026 — compromising Trivy, Bitwarden CLI, TanStack, SAP and Red Hat npm packages and ultimately stealing ~3,800 internal GitHub repositories in 11 minutes — to a single operator based in South Africa (handle ResoluteXBF, also TeamPCP). CISA, SANS and multiple global vendors are now tracking the operator. This is a law-enforcement-relevant SA development; SA DevSecOps teams should audit dependency provenance and rotate any tokens that touched compromised registries. AVBOB remains in partial restoration with no leak-site claim or attribution as of 21 June, and the SA ransomware.live count holds FLAT at 109.[4][5]

KPI Dashboard

Metric	Current (W26)	Prior (W25)	Change	Direction
SA threat level	HIGH	HIGH	Unchanged (6th consecutive week)	FLAT
SA ransomware.live victims (total)	109	109 (corrected)	0 new W26 (6th week FLAT)	FLAT
New SA RW listings this week (ransomware.live)	0 confirmed	0 (W25)	FLAT	FLAT
FortiBleed Fortinet credential exposure	~74,000 FortiGate firewalls (plaintext creds); CISA alert 18 Jun	N/A	NEW W26	UP
Splunk Enterprise CVE-2026-20253 (9.8)	Pre-auth RCE; ITW confirmed 18 Jun; KEV due 21 Jun	N/A	NEW W26	UP
TeamPCP / ResoluteXBF SA attribution	Google + Palo Alto attribute 2026 npm/GitHub campaign to SA operator	N/A	NEW W26	UP
New CISA KEV additions (14-21 Jun)	5 (Joomla 10.0, Splunk 9.8, LiteSpeed 8.5, Serv-U 7.5, Cisco SD-WAN 7.2)	multiple (W25)	ELEVATED	UP
AVBOB Mutual Assurance (360 branches)	Partial restoration; no leak-site claim/attribution (5+ weeks)	OFFLINE (W25)	IMPROVING	DOWN
ShinyHunters/C10p PeopleSoft escalation	Council of Europe (297GB/429k files); C10p now also exploiting CVE-2026-35273	ITW mass-compromise (W25)	ESCALATING	UP
Cannabis Club "CannaLeaks" SA exposure	~88,000 SA identities in ~985,000-record global leak (GDPR primary)	N/A	NEW W26	UP
SAPS Western Cape POPIA breach	Independent senior SAPS officer appointed to lead investigation	2,978 records leaked (W25)	INVESTIGATION	FLAT
IR Tembisa PAIA enforcement (16 Jun)	Gauteng Health: 10-day comply-or-prosecute order	N/A	NEW W26	UP

W26 KEY FRAMING: W26 was moderate-to-quiet on fresh SA-originating ransomware claims but operationally heavy on global exposure events that hit South African infrastructure directly. Three structural exposures dominate: FortiBleed (~74,000 FortiGate firewalls with plaintext credentials), the actively-exploited Splunk Enterprise pre-auth RCE (CVE-2026-20253, KEV due 21 June), and the public attribution of the 2026 npm/GitHub supply-chain campaign to a South Africa-based operator (TeamPCP/ResoluteXBF). The FLAT ransomware count (109, now corrected against a live 21 June screenshot and at its longest plateau of 2026) again masks real threat activity. The dominant operational drivers this week are the FortiBleed credential rotation, the Splunk patch deadline, and the overdue Joomla JCE (CVE-2026-48907, 10.0) and Splunk KEV items.

TOP 3 ACTIONS THIS WEEK

1. FORTIBLEED TRIAGE (CISA ALERT 18 JUNE): Check your organisation domain at hudsonrock.com/fortinet; force-rotate ALL FortiGate VPN and admin credentials; enable phishing-resistant MFA on admin interfaces; upgrade FortiOS to 7.2.11 / 7.4.8 / 7.6.1+ (which triggers PBKDF2 re-hash on next admin login); remove management interfaces from the public internet; and review logs for unexpected successful admin logins. SA exposure spans government, banking, retail, and ISPs.

2. SPLUNK ENTERPRISE CVE-2026-20253 (9.8, KEV DUE 21 JUN): Patch Splunk Enterprise to 10.0.7 or 10.2.4 immediately — the pre-auth RCE via the unauthenticated PostgreSQL sidecar (/v1/postgres/recovery/backup and /restore) is confirmed exploited in the wild. If patching is not immediately possible, disable the PostgreSQL sidecar and restrict network access to the management interface. Splunk Cloud Platform is not affected. A compromised SIEM blinds the SOC.

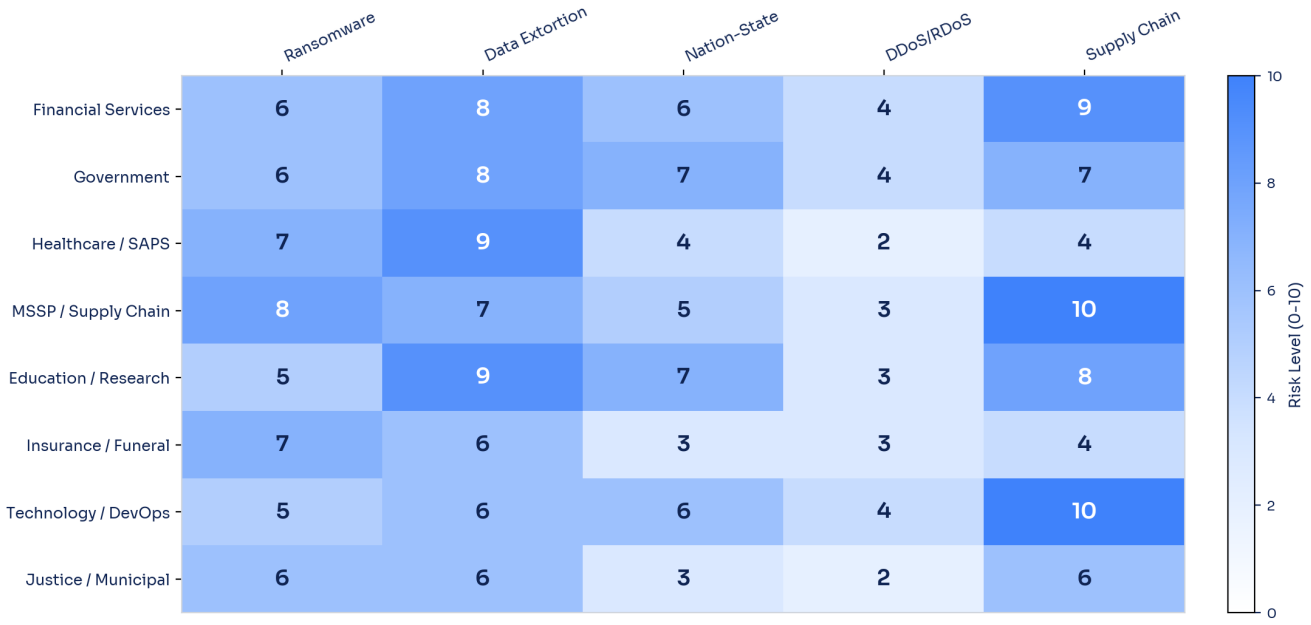
3. OVERDUE KEV (JOOMLA JCE 10.0 + LITESPEED 8.5) + EXCHANGE OWA + PEOPLESOFT: Joomla JCE CVE-2026-48907 (10.0) is OVERDUE and under automated mass exploitation since 9 June — verify version, review the #__wf_profiles table and images/, media/, tmp/ for rogue PHP. Apply LiteSpeed cPanel CVE-2026-54420 (8.5, OVERDUE). Deploy Exchange OWA permanent fix KB5094139 (CVE-2026-42897, actively exploited). For any internet-accessible PeopleSoft 8.61/8.62, apply Oracle June CPU and review logs from 27 May onward.

1. Security Affairs -- CISA warns of active exploitation following FortiBleed leak — https://securityaffairs.com/193902/hacking/cisa-warns-of-active-exploitation-following-fortibleed-leak.html
2. Bitsight -- Security alert: FortiBleed Fortinet VPN credentials / firewall exposed — https://www.bitsight.com/blog/security-alert-fortibleed-fortinet-vpn-credentials-firewall-exposed
3. BleepingComputer -- CISA: Splunk Enterprise flaw actively exploited, patch by Sunday — https://www.bleepingcomputer.com/news/security/cisa-splunk-enterprise-flaw-actively-exploited-patch-by-sunday/
4. The Register -- Council of Europe hacked in ShinyHunters PeopleSoft heist — https://www.theregister.com/cyber-crime/2026/06/15/council-of-europe-hacked-in-shinyhunters-peoplesoft-heist/5255757
5. ITWeb -- Malicious actors take down AVBOB's digital platforms — https://www.itweb.co.za/article/malicious-actors-take-down-avbobs-digital-platforms/5yONP7Erd6QMXWrb

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 26 (14–21 June 2026). **Technology/DevOps** and **MSSP/Supply Chain** peak at 10 on Supply Chain following the public attribution of the 2026 npm/GitHub supply-chain campaign to a South Africa-based operator (TeamPCP/ResoluteXBF) and the SuppCenter (Xcitium/Comodo) M3RX listing. **Government**, **Financial Services**, and **Healthcare/SAPS** sit at 8–9 on Data Extortion (IR Tembisa PAIA enforcement against Gauteng Health; FortiBleed exposure across banking and government; SAPS Western Cape POPIA breach now under an independent senior SAPS investigator). **Education/Research** remains at 9 on Data Extortion (SA universities running PeopleSoft, with ShinyHunters and now C10p both exploiting CVE-2026-35273; Nottingham 455,000+ records). **Insurance/Funeral** holds at 7 on Ransomware as AVBOB continues partial restoration with no leak-site claim five-plus weeks post-attack.

SA THREAT LANDSCAPE HEATMAP | W26 (14 - 21 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 26 (14–21 June 2026): Zero new ransomware.live SA listings (SA tally holds at 109, 6th consecutive week FLAT). Dominant stories: (1) AVBOB Mutual Assurance — partial restoration, still unattributed with no leak-site claim; (2) SAPS Western Cape — independent senior SAPS officer appointed to lead the 2,978-record POPIA breach investigation; (3) Cannabis Club Systems "CannaLeaks" — ~88,000 SA identities in a ~985,000-record global leak (GDPR primary); (4) NPA Asset Forfeiture — R21.5m frozen in an online banking scam (15 June); (5) TikTok 2.4bn-record leak claim — likely aggregated infostealer data, UNVERIFIED; (6) GroundUp Part 2 — non-SITA gov.za attack surface (4,466 CVEs); (7) SuppCenter Global/SA MSSP M3RX listing. Africa-region leak-site activity: LockBit 5.0 Botswana Vaccine Institute (20 June); Krybit Cour des Comptes du Sénégal (17 June); NightSpire Sheraton El Gouna, Egypt (15 June).[6]

3.1 INC-2026-W26-01 — AVBOB Mutual Assurance -- Partial Restoration, Unattributed [CONFIRMED]

Sector	Insurance / Funeral Services (private)
Date	Original attack 30 May 2026; W26 partial restoration
Actor	"External malicious actors" -- NO ransomware group has claimed AVBOB on any public leak site as of 21 Jun
Scale	SA's largest funeral insurer; 360 branches reverted to manual operations
W26 update	AVBOB published a "Progress on System Restoration" PDF; several systems restored; eNCA confirmed ongoing recovery 18 Jun
Regulatory	POPIA s.22 investigation continuing; claims via myclaim@avbob.co.za; premiums via PayAt
Confidence	CONFIRMED (operational impact); attribution UNKNOWN

AVBOB Mutual Assurance, struck by "external malicious actors" on 30 May, remained in partial restoration during W26. The insurer published a "Progress on System Restoration" PDF confirming several systems restored (with claims routed via myclaim@avbob.co.za and premiums via PayAt), and eNCA confirmed ongoing recovery on 18 June. Critically, no ransomware group has claimed AVBOB on any public leak site as of 21 June — the attack is still described only as the work of external malicious actors, and the POPIA s.22 investigation continues. With AVBOB now more than five weeks post-attack and still undetermined, SA insurance and funeral-services peers should continue independent risk reviews on shared access pathways and broker portals.[78]

3.2 INC-2026-W26-02 — SAPS Western Cape POPIA Breach -- Independent Investigator Appointed [CONFIRMED]

Sector	Government / Law Enforcement (SAPS Western Cape)
Original report	9 June 2026 -- 2,978 officers' medical records (PTSD, bipolar, depression, alcoholism, cancer) via HR email attachment
W26 update	Standing Committee on Police Oversight engaged SAPS management; refresher training mandated; independent senior SAPS officer from outside Western Cape appointed to lead investigation
Labour response	POPCRU threatened legal/labour/regulatory action
Regulatory	No Information Regulator enforcement notice tied to this specific incident as of 21 Jun; no disciplinary outcomes published
Confidence	CONFIRMED

The SAPS Western Cape POPIA breach — 2,978 officers' diagnostic medical records leaked via an HR email attachment (reported 9 June) — escalated in W26. The Standing Committee on Police Oversight discussed the matter with SAPS management, refresher training was mandated, and an independent senior SAPS officer from outside the Western Cape was appointed to lead the investigation. POPCRU threatened legal, labour, and regulatory action. No Information Regulator enforcement notice tied to this specific incident has been issued as of 21 June, and no disciplinary outcomes have been published. The Werksmans analysis of internal misdirected-email breaches (see Section 9) applies directly here. SA HR functions and special-category data processors should continue to treat internal disclosure of sensitive records as a notifiable POPIA compromise.[9]

3.3 INC-2026-W26-03 — Cannabis Club Systems "CannaLeaks" -- ~88,000 SA Identities [CONFIRMED, GDPR primary]

Sector	Consumer platform (cannabis club management, global; Irish controller Nefos Solutions)
Exposure	~985,000 identity documents exposed globally via unauthenticated URLs on the CCS/PuffPal platform
SA scale	~88,000 individuals linked to SA cannabis dispensaries and clubs
Data	Passport/ID images, names, contact details, dates of birth, facial images
Branding	High Times investigation (17 Jun) branded it "CannaLeaks"
Jurisdiction	GDPR applies primarily (Irish controller); POPIA cross-border provisions likely triggered; no IR notification confirmed
Confidence	CONFIRMED

A High Times investigation on 17 June branded the Cannabis Club Systems exposure "CannaLeaks": roughly 985,000 identity documents were exposed globally via unauthenticated URLs on the CCS/PuffPal platform, operated by Irish data controller Nefos Solutions. About 88,000 of the affected individuals are linked to SA cannabis dispensaries and clubs, with passport/ID images, names, contact details, dates of birth, and facial images exposed. GDPR applies primarily given the Irish controller, but POPIA cross-border provisions are likely triggered; no POPIA notification to the Information Regulator has been confirmed. Affected SA individuals should treat exposed ID/passport and biometric data as compromised and monitor for downstream identity-fraud abuse.[10]

3.4 INC-2026-W26-04 — NPA Asset Forfeiture: R21.5m Frozen in Online Banking Scam [CONFIRMED]

Sector	Financial / Law Enforcement (NPA Asset Forfeiture Unit)
Date	15 June 2026
Action	AFU obtained a court order freezing R21.5m linked to cyber-enabled banking fraud
Significance	Confirms continued active fraud volume against SA banking customers
Confidence	CONFIRMED

On 15 June the NPA's Asset Forfeiture Unit obtained a court order freezing R21.5m linked to a cyber-enabled online banking scam. The action confirms continued active fraud volume against SA banking customers and aligns with the FortiBleed and credential-theft exposure themes elsewhere in this report. SA banks should reinforce transaction-monitoring and customer fraud-awareness messaging, particularly given the FortiBleed credential exposure affecting the financial sector.[11]

3.5 INC-2026-W26-05 — TikTok 2.4 Billion Record Leak Claim -- SA Exposure [UNVERIFIED]

Sector	Consumer / social media (global)
Date	11–12 June 2026 (hacker-forum claim)
Claim	2.4 billion TikTok-linked records (emails, phone numbers, DOBs, usernames)
Researcher assessment	Likely aggregated from infostealer malware, NOT a direct TikTok breach
SA relevance	EWN flagged SA children's account-takeover risk
Status	UNVERIFIED -- TikTok has not confirmed a system compromise

On 11–12 June a threat actor on a hacker forum claimed 2.4 billion TikTok-linked records (emails, phone numbers, dates of birth, usernames). Researchers assess the dataset as likely aggregated from infostealer

malware rather than a direct TikTok system breach. EWN flagged the account-takeover risk for SA children specifically. The claim remains UNVERIFIED — TikTok has not confirmed a system compromise. SA users, parents, and schools should treat the claim as an infostealer-aggregation reminder: enforce unique passwords and MFA, and run infostealer-exposure checks rather than assume a fresh TikTok breach.[12]

3.6 GroundUp Part 2 + SuppCenter / M3RX + Ongoing / Carryover Incidents (W26 Status)

GroundUp Part 2 (non-SITA gov.za): No government remediation response in W26. The investigation documented 4,466 CVEs across 516 hosts — Amathole District Municipality 353 CVEs (94 critical on one server), Witzenberg 347 CVEs, and Apache 2.4.7 on Ubuntu 14.04 (unsupported since April 2019). **SuppCenter Global/SA (M3RX):** Posted on the M3RX leak site 11 June; SuppCenter is an MSSP implementing Xcitium/Comodo Zero Trust for large SA enterprise and public-sector clients (downstream client risk). No follow-up data release or negotiation update in W26.[13][14]

W25/Prior Item	W26 Update
Dept of Employment & Labour	Official suspended (9-11 Jun) after job-seekers data-leak probe; no further disciplinary outcome or IR notification in W26.
GroundUp Part 2 non-SITA gov.za	No government remediation response in W26; 4,466 CVEs / 516 hosts; Amathole 353 CVEs; Witzenberg 347; Apache 2.4.7 on Ubuntu 14.04.
SuppCenter Global/SA (M3RX)	Listed 11 Jun; Xcitium/Comodo Zero Trust MSSP; no follow-up data release or negotiation update in W26.
AVBOB Mutual Assurance	Partial restoration; eNCA confirmed recovery 18 Jun; NO leak-site claim or attribution as of 21 Jun; POPIA s.22 ongoing.
SAPS Western Cape POPIA breach	Independent senior SAPS officer from outside WC appointed; POPCRU threatened action; no IR notice tied to incident yet.
No new SA ransomware.live postings	ZA cumulative remains at 109 (verified live screenshot 21 Jun 10:14 SAST); no fresh SA-named victim 14-21 Jun.

6. Ransomware.live -- South Africa country map (W26) — https://www.ransomware.live/map/ZA
7. AVBOB -- Progress on System Restoration (W26 PDF) — https://www.avbob.co.za/media/pdf/system-restoration-progress.pdf
8. eNCA -- AVBOB confirms ongoing recovery (18 June 2026) — https://www.facebook.com/eNCAnews/posts/avbob-confirms-that-the-recent-disruption-to-certain-of-its-digital-platforms-an/1326555792960733/
9. 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/
10. High Times -- CannaLeaks: nearly one million cannabis club users' data exposed (17 June 2026) — https://hightimes.com/news/cannaleaks-nearly-one-million-cannabis-club-users-data-was-exposed/
11. IOL -- NPA Asset Forfeiture Unit freezes R21.5m linked to online banking scam (15 June 2026) — https://iol.co.za/news/crime-and-courts/2026-06-15-npa-asset-forfeiture-unit-secures-court-order-to-freeze-r215million-linked-to-online-banking-scam/
12. EWN -- TikTok breach sparks fresh concerns over children's online safety (12 June 2026) — https://www.ewn.co.za/2026/06/12/tiktok-breach-sparks-fresh-concerns-over-children-s-online-safety
13. GroundUp -- Here's how insecure governments' websites are (Part 2) — https://groundup.org.za/article/heres-how-insecure-governments-websites/
14. Ransomware.live -- SuppCenter Global / SA listing (M3RX, 11 June 2026) — https://www.ransomware.live/id/c3VwcGNlbnRlci5nbG9iYWwgLyBzdXBwY2VudGVyc2EuY29tQG0zcng

4. GLOBAL INCIDENTS WITH SA RELEVANCE

TeamPCP / ResoluteXBF -- 2026 npm/GitHub Supply-Chain Campaign Attributed to a SINGLE SOUTH AFRICAN Operator

Google and Palo Alto Networks publicly attributed the most damaging open-source software supply-chain campaign of 2026 to a single operator based in South Africa (handle ResoluteXBF, also tracked as TeamPCP). The campaign compromised Trivy, Bitwarden CLI, TanStack, SAP npm packages, and Red Hat packages, and ultimately reached GitHub itself, stealing approximately 3,800 internal GitHub repositories in 11 minutes. CISA, SANS, and multiple global vendors are now actively tracking the operator. This is a law-enforcement-relevant SA development. SA DevSecOps teams should audit dependency provenance, review published IOCs, and rotate any tokens that touched the compromised registries.[15]

Oracle PeopleSoft CVE-2026-35273 -- ShinyHunters/UNC6240 Data Dumps Begin; Cl0p Now Also Exploiting

Extortion deadlines expired during W26 and ShinyHunters/UNC6240 began publishing PeopleSoft victim data: Council of Europe (297 GB / 429,000 files), Kodak (2.2M records), Madison Square Garden (45 GB / 26M records including facial-recognition data), Glendale Community College, Moody Bible Institute, Illinois Central College, Houston Community College, Deep Well Services, JCPenney, American Tower, and Ralph Lauren. The University of Nottingham confirmed 455,000+ student records leaked. Critically, Cl0p is now confirmed exploiting the same flaw -- a second ransomware group on CVE-2026-35273. UNC6240 deployed persistent backdoors that survive patching, so log review from 27 May onward is mandatory. SA universities (HESA) and provincial governments commonly run PeopleSoft and must assume compromise where instances were internet-facing.[1617]

The Gentlemen / Storm-2697 / LARVA-368 -- Administrator Unmasked; 517 Victims

KrebsOnSecurity unmasked the administrator of "The Gentlemen" (Storm-2697 / LARVA-368) as Alexander Andreevich Yapaev (36, of Izhevsk, Russia; aliases hastalamuerte and Zeta88). ESET published "Killing Me Gently", a full analysis of the group's GentleKiller EDR-killer framework (8 variants targeting 400+ security processes). The global victim count reached 517 during W26, with 15 new victims posted on 15 June alone. The group's primary initial-access vectors are CVE-2026-50751 (Check Point IKEv1 VPN bypass) and CVE-2026-20131 (Cisco FMC). SA was confirmed as a targeted nation in W24 by PRODAFT; no new SA victim was posted in W26, but the group remains actively listed.[18]

Africa-Region Ransomware Leak-Site Activity (W26)

Three African organisations were posted to ransomware leak sites during W26: LockBit 5.0 listed the Botswana Vaccine Institute (20 June), a SADC critical-infrastructure target in animal pharma and vaccine supply; Krybit listed the Cour des Comptes du Senegal (17 June, 20 GB, 5-day countdown) with the Senegal government confirming a "major technical incident"; and NightSpire listed the Sheraton Miramar Resort El Gouna, Egypt (15 June). No new SA-named leak-site victim was posted in W26, leaving the ransomware.live ZA cumulative FLAT at 109.[6]

CISA BOD 26-04 -- 9 August 2026 Vulnerability-Management Policy Deadline

CISA's Binding Operational Directive 26-04 sets a 9 August 2026 deadline for US federal civilian agencies to stand up a risk-based vulnerability-management process. While SA organisations are not bound by the directive, it continues to set an international benchmark for KEV-driven patch governance. SA SOCs should treat risk-based vulnerability management as the baseline expectation, particularly given the OVERDUE Splunk, Joomla, PeopleSoft, Check Point, and Ivanti Sentry items below.[19]

Other Notable Global Research (W26)

Dragos' Industrial Ransomware Q1 2026 report logged 19 OT incidents in the Africa region. Broadcom/Symantec documented DragonForce's Backdoor.Turn, which abuses Microsoft Teams as a C2 evasion channel. The Hacker News profiled INC Ransomware (830+ victims), and CYFIRMA's Threat Actor in Focus again covered UNC5221 / Silk Typhoon. AhnLab's May 2026 APT Trends confirmed Webworm targeting an SA university. SA defenders should fold these IOC sets into ongoing hunt and detection work.[20]

15. KrebsOnSecurity / CyberScoop -- TeamPCP / ResoluteXBF SA attribution (W26 coverage) — https://krebsonsecurity.com/
16. The Register -- Council of Europe hacked in ShinyHunters PeopleSoft heist — https://www.theregister.com/cyber-crime/2026/06/15/council-of-europe-hacked-in-shinyhunters-peoplesoft-heist/5255757
17. Tenable -- Oracle June 2026 Critical Patch Update (CVE-2026-35273) — https://www.tenable.com/blog/oracle-june-2026-critical-security-patch-update-addresses-243-cves-cve-2026-35273
18. ESET / KrebsOnSecurity -- "Killing Me Gently": GentleKiller framework / The Gentlemen admin unmasked — https://www.welivesecurity.com/
19. CISA -- Binding Operational Directive 26-04 — https://www.cisa.gov/news-events/directives
20. Dragos / Broadcom-Symantec / CYFIRMA / The Hacker News -- W26 threat research — https://www.dragos.com/blog/

5. THREAT ACTORS

5.1 TeamPCP / ResoluteXBF — SA-Attributed npm/GitHub Supply-Chain Operator (HIGHEST SA RELEVANCE)

TeamPCP / ResoluteXBF is the defining W26 actor for South Africa. Google and Palo Alto Networks attributed the most damaging open-source supply-chain campaign of 2026 to a single operator based in SA. The campaign poisoned Trivy, Bitwarden CLI, TanStack, SAP, and Red Hat packages and reached GitHub itself, exfiltrating roughly 3,800 internal repositories in 11 minutes. CISA and SANS are tracking the operator, and KrebsOnSecurity has covered the attribution. The SA nexus makes this directly law-enforcement-relevant. SA DevSecOps teams should audit dependency provenance across npm, PyPI, and GitHub, rotate any tokens that touched compromised registries, and subscribe to vendor advisories for the affected Trivy, Bitwarden CLI, TanStack, SAP, and Red Hat releases.[15]

5.2 The Gentlemen / Storm-2697 / LARVA-368 — Admin Unmasked, 517 Victims, SA Targeted

KrebsOnSecurity unmasked the administrator of "The Gentlemen" (Storm-2697 / LARVA-368) as Alexander Andreevich Yapaev (36, Izhevsk, Russia; aliases hastalamuerte, Zeta88). ESET's "Killing Me Gently" detailed the group's GentleKiller EDR-killer framework (8 variants, 400+ targeted security processes). The global victim total reached 517 in W26, with 15 victims posted on 15 June alone. Initial access relies on CVE-2026-50751 (Check Point IKEv1 bypass) and CVE-2026-20131 (Cisco FMC). SA was confirmed targeted in W24 by PRODAFT; no new SA victim appeared in W26, but SA enterprises should validate EDR-tamper protections and patch the named initial-access CVEs.[18]

5.3 ShinyHunters / UNC6240 — PeopleSoft Data Dumps Begin; Cl0p Joins (CVE-2026-35273)

ShinyHunters/UNC6240 began publishing PeopleSoft victim data in W26 as extortion deadlines expired: Council of Europe (297 GB / 429,000 files), Kodak (2.2M), Madison Square Garden (45 GB / 26M incl. facial recognition), and several US colleges, with Nottingham confirming 455,000+ records. Cl0p is now confirmed exploiting the same CVE-2026-35273 -- a second ransomware group on the flaw. UNC6240 backdoors survive patching, so SA universities and provincial governments running PeopleSoft (PeopleTools 8.61/8.62) must apply the Oracle June CPU and review logs from 27 May onward, treating any previously internet-facing instance as compromised.[16][17]

5.4 Threat Actor Summary — W26

Actor	Type	Notable W26 Activity	Source
TeamPCP / ResoluteXBF	Supply-chain / criminal	Google + Palo Alto attribute 2026 npm/GitHub campaign to single SA operator; ~3,800 repos in 11 min; CISA/SANS tracking	Krebs, CyberScoop
The Gentlemen / Storm-2697 / LARVA-368	Ransomware	Admin unmasked (A. Yapaev); ESET GentleKiller framework; 517 victims; CVE-2026-50751 + CVE-2026-20131 access; SA targeted (W24)	Krebs, ESET
ShinyHunters / UNC6240	Criminal / data theft	PeopleSoft CVE-2026-35273 dumps begin: Council of Europe, Kodak, MSG, Nottingham 455k; persistent backdoors survive patching	The Register, Tenable
C1Op	Ransomware / extortion	Confirmed as SECOND group exploiting PeopleSoft CVE-2026-35273	The Register
Qilin	Ransomware	Confirmed exploiting Check Point IKEv1 CVE-2026-50751 (OVERDUE +10)	CISA KEV
LockBit 5.0	Ransomware	Botswana Vaccine Institute (20 Jun) -- SADC critical infrastructure	Ransomware.live
Krybit	Ransomware	Cour des Comptes du Senegal (17 Jun); 20 GB; 5-day countdown	Ransomware.live
NightSpire	Ransomware	Sheraton El Gouna, Egypt (15 Jun); hospitality	Ransomware.live
DragonForce	Ransomware	Backdoor.Turn using Microsoft Teams as C2 (Broadcom/Symantec)	Symantec
UNC5221 / Silk Typhoon	China APT	CYFIRMA profile; edge-appliance/VPN espionage; relevant to Ivanti Sentry KEV	CYFIRMA
Webworm (China APT)	State espionage	AhnLab May 2026 APT Trends: SA university targeting confirmed	AhnLab
INC Ransomware	Ransomware	The Hacker News profile: 830+ cumulative victims	The Hacker News
M3RX / SuppCenter	Extortion portal	SuppCenter Global/SA (Xcitium/Comodo MSSP) listed 11 Jun; no follow-up in W26	Ransomware.live

5.5 Notable Industry Intelligence Actions (W26)

SA supply-chain attribution (Google + Palo Alto): The public attribution of the 2026 npm/GitHub campaign to an SA-based operator is the most consequential SA-nexus intelligence event of the cycle and should drive an immediate dependency-provenance and token-rotation programme across SA DevSecOps teams.[15]

ESET "Killing Me Gently": The GentleKiller EDR-killer framework analysis (8 variants, 400+ targeted processes) is the authoritative dataset for hardening EDR-tamper protections against The Gentlemen / LARVA-368, a group with a confirmed SA targeting history.[18]

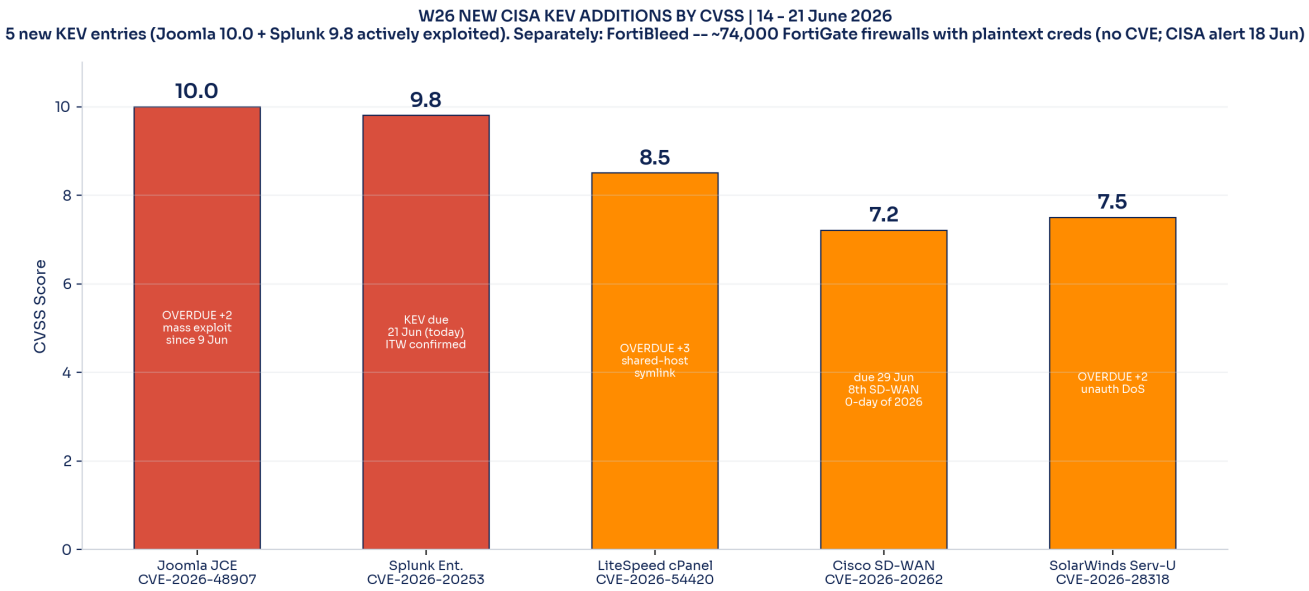
15. KrebsOnSecurity / CyberScoop -- TeamPCP / ResoluteXBF SA attribution (W26 coverage) — https://krebsonsecurity.com/
16. The Register -- Council of Europe hacked in ShinyHunters PeopleSoft heist — https://www.theregister.com/cyber-crime/2026/06/15/council-of-europe-hacked-in-shinyhunters-peoplesoft-heist/5255757
17. Tenable -- Oracle June 2026 Critical Patch Update (CVE-2026-35273) — https://www.tenable.com/blog/oracle-june-2026-critical-security-patch-update-addresses-243-cves-cve-2026-35273
18. ESET / KrebsOnSecurity -- "Killing Me Gently": GentleKiller framework / The Gentlemen admin unmasked — https://www.welivesecurity.com/

6. CRITICAL VULNERABILITIES & CISA KEV

W26 was defined by two actively exploited OVERDUE/due-today KEV items and a major credential-exposure event. **Splunk Enterprise CVE-2026-20253** (CVSS 9.8) is a pre-auth RCE via an unauthenticated PostgreSQL sidecar endpoint, KEV-due **21 June (today)**, with ITW exploitation confirmed

by Splunk PSIRT on 18 June and a watchTowr PoC public since 12 June. **Joomla JCE CVE-2026-48907** (CVSS 10.0) is a pre-auth PHP RCE under automated mass-exploitation since 9 June, now **OVERDUE +2**. Separately, **FortiBleed** (no CVE; CISA alert 18 June) exposed valid plaintext credentials for ~74,000 internet-facing FortiGate firewalls. Five new KEV entries landed in the 14-21 June window, and the OVERDUE PeopleSoft (CVE-2026-35273), Check Point IKEv1 (CVE-2026-50751), and Ivanti Sentry (CVE-2026-10520) carryovers all remain actively exploited.[1321]

W26 KEV / Critical CVE Severity Overview — (5 New KEV Adds 14-21 Jun + FortiBleed + Active Carryovers)



W26 CISA KEV / Critical CVE Tracking (new adds 14-21 June + active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-20253	Splunk Enterprise (PostgreSQL sidecar)	9.8	Pre-auth RCE	21 Jun (today)	ITW confirmed by Splunk PSIRT 18 Jun; watchTowr PoC since 12 Jun; patch 10.0.7 / 10.2.4; Cloud not affected
CVE-2026-48907	Joomla Content Editor (JCE)	10.0	Pre-auth RCE	19 Jun	OVERDUE +2; automated mass exploitation since 9 Jun; check #__wf_profiles + images/media/tmp for PHP
CVE-2026-54420	LiteSpeed cPanel Plugin	8.5	Symlink follow	18 Jun	OVERDUE +3; UNIX symlink follow -> cross-tenant; shared-hosting risk
CVE-2026-20262	Cisco Catalyst SD-WAN Manager	7.2	Path traversal -> root	29 Jun	Patched ~16 Jun via malicious .war; 8th SD-WAN 0-day of 2026
CVE-2026-28318	SolarWinds Serv-U	7.5	Unauth DoS	19 Jun	OVERDUE +2; DoS only per Bishop Fox analysis
CVE-2026-35273	Oracle / PeopleSoft	9.8	Unauth RCE	15 Jun	OVERDUE +6; ShinyHunters + C10p both exploiting; persistent backdoors survive patching; log review from 27 May
CVE-2026-50751	Check Point Security Gateway (IKEv1)	9.3	Auth bypass	11 Jun	OVERDUE +10; Qilin ransomware exploiting; exploitation since ~7 May; disable IKEv1 if not required
CVE-2026-10520	Ivanti / Sentry	10.0	Unauth RCE	14 Jun	OVERDUE +7; weaponised <24h after patch; UNC5221 edge-appliance focus
CVE-2026-11645	Google / Chrome V8	n/a	Type confusion	23 Jun	Exploited ITW; 2 days; push browser update + restart estate-wide
CVE-2026-20245	Cisco / SD-WAN	n/a	0-day RCE	23 Jun	2 days; PATCH NOW AVAILABLE; 7th SD-WAN 0-day of 2026
CVE-2026-7473	Arista EOS (tunnel decap)	5.8	Tunnel decap	23 Jun	Arista DECLINED to patch; implement filtering workaround
CVE-2026-42897	Microsoft / Exchange OWA	8.1	XSS/Spoofing	Apply NOW	Permanent fix KB5094139 ACTIVELY EXPLOITED since May 2026; replaces W22 EEMS interim mitigation

Pattern note: W26 is a "structural exposure" week rather than a fresh-victim week. Two actively exploited KEV items reached or passed their deadlines with confirmed in-the-wild exploitation (Splunk CVE-2026-20253 due today; Joomla JCE CVE-2026-48907 OVERDUE +2), while three high-severity carryovers (PeopleSoft, Check Point IKEv1, Ivanti Sentry) remain OVERDUE and under active exploitation by ShinyHunters/C10p and Qilin. FortiBleed compounds the picture with ~74,000 firewalls exposing crackable credentials. SA estates should treat credential rotation, Splunk patching, and Joomla web-shell hunting as a single high-priority change event.

6.1 FortiBleed (no CVE, CISA alert 18 June) -- ~74,000 FortiGate Firewalls Expose Plaintext Credentials

FortiBleed is a credential-exposure event affecting approximately 74,000 internet-facing Fortinet FortiGate firewalls and VPN gateways -- roughly 50% of all internet-exposed FortiGate devices globally, spanning 21,632 unique domains across 194 countries. Valid usernames and plaintext-recoverable passwords were found on an attacker-controlled server. The root cause: FortiOS SHA-256 admin hashes migrated to PBKDF2 in early 2025 only re-hash on a manual admin login after upgrade -- so even patched devices that no admin had logged into still stored crackable hashes. Discovery is credited to Bob Diachenko with Kevin Beaumont confirmation; named victims include Samsung, Siemens, Oracle, PwC, Accenture, and NATO defence contractors. SA exposure is significant across government, banking, retail, and ISPs. Check the organisation domain at hudsonrock.com/fortinet, rotate ALL VPN and admin credentials, enable phishing-resistant MFA, upgrade to FortiOS 7.2.11 / 7.4.8 / 7.6.1+, and remove management interfaces from the public internet.[121]

6.2 Splunk Enterprise CVE-2026-20253 (CVSS 9.8, KEV due TODAY) -- Pre-Auth RCE via PostgreSQL Sidecar

CVE-2026-20253 (CVSS 9.8) is a missing-authentication flaw in Splunk Enterprise's PostgreSQL sidecar endpoints (/v1/postgres/recovery/backup and /restore) allowing pre-auth arbitrary file write and RCE via lo_export. watchTowr Labs published a full exploit chain on 12 June, and Splunk PSIRT confirmed limited ITW exploitation on 18 June. The KEV deadline is today, 21 June. SA relevance is HIGH: Splunk is the SIEM of record across SA banks and telcos, and a compromised Splunk blinds the SOC. Patch to 10.0.7 or 10.2.4 immediately; Splunk Cloud Platform is not affected. If patching is not immediately possible, disable the PostgreSQL sidecar and restrict management-interface network access.[322]

6.3 Oracle PeopleSoft CVE-2026-35273 (OVERDUE +6) + Carryover Deadlines (W26 Status)

Oracle PeopleSoft CVE-2026-35273 (CVSS 9.8) is now OVERDUE +6 against the 15 June KEV deadline and is being exploited by BOTH ShinyHunters/UNC6240 and C10p. UNC6240 has deployed persistent backdoors that survive patching, so applying the Oracle June 2026 CPU (245 patches, 122 critical, full PeopleTools 8.61/8.62 remediation) is necessary but not sufficient -- a mandatory log review from 27 May onward is required, and any instance for which log review is impossible should be treated as compromised. SA universities (HESA) and provincial governments commonly run PeopleSoft and are squarely in scope.[1617]

CVE / Item	Status W26
Oracle PeopleSoft CVE-2026-35273 (9.8)	OVERDUE +6; ShinyHunters + C10p both exploiting; backdoors survive patching; apply June CPU + review logs from 27 May
Check Point IKEv1 CVE-2026-50751 (9.3)	OVERDUE +10; Qilin ransomware exploiting; exploitation since ~7 May; disable IKEv1 where not required; apply 8 Jun hotfixes
Ivanti Sentry CVE-2026-10520 (10.0)	OVERDUE +7; weaponised <24h after patch; UNC5221 edge focus; patch + assume-breach hunt
Chrome V8 CVE-2026-11645	KEV 23 Jun (2 days); exploited ITW; push browser update + restart estate-wide
Cisco SD-WAN CVE-2026-20245 (0-day)	KEV 23 Jun (2 days); PATCH NOW AVAILABLE; confirm patched build; 7th SD-WAN 0-day of 2026
Cisco Catalyst SD-WAN Manager CVE-2026-20262 (7.2)	KEV 29 Jun; patched ~16 Jun; path traversal -> root via .war; 8th SD-WAN 0-day of 2026
Arista EOS CVE-2026-7473 (5.8)	KEV 23 Jun; Arista DECLINED to patch; implement tunnel-decap filtering workaround
SAP CVE-2026-44748 (9.9) + CVE-2026-27671 (9.8)	SAML XML wrapping + unauth RFC memory corruption; SA mining/retail/gov ERP risk; patch June SAP notes
PAN-OS GlobalProtect CVE-2026-0257	Arctic Wolf 15 Jun confirms ongoing exploitation; Rapid7 MDR: 8 of 10 clients hit; complete patch

CVE / Item	Status W26
Atlassian AV26-608 (16 Jun)	Crowd DC HTTP request smuggling (CVE-2026-42581 9.8 / -42584 9.1); Syracom 2FA bypass (CVE-2026-12225)
Apple iOS 26.3 / macOS Tahoe 26.3 (~17 Jun)	CVE-2026-20700 dyld zero-day exploited ITW; update estate
GitLab security release (~20 Jun)	CVE-2026-10087 XSS in EE + others; self-hosted SA DevSecOps teams must update

EXCHANGE OWA CVE-2026-42897 -- PERMANENT FIX KB5094139 -- ACTIVELY EXPLOITED, APPLY NOW

Status: ACTIVELY EXPLOITED since May 2026. The permanent patch KB5094139 replaces the W22 EEMS interim mitigation. Any estate that has not yet applied KB5094139 remains exposed to active exploitation.

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 healthy.

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

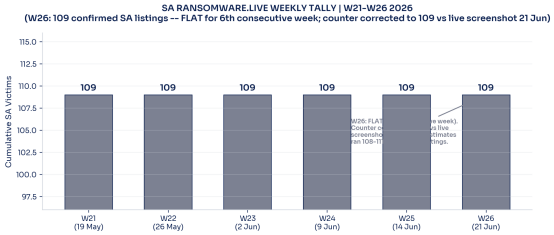
June PT caution: KB5094126 (June PT package) is confirmed by Microsoft (18 Jun) to cause system freezes and BitLocker recovery loops with no fix yet; KB5085516 (~18 Jun) is a sign-in fix, NOT security. Stage June rollups carefully but do not defer KB5094139.

1. Security Affairs -- CISA warns of active exploitation following FortiBleed leak — https://securityaffairs.com/193902/hacking/cisa-warns-of-active-exploitation-following-fortibleed-leak.html
3. BleepingComputer -- CISA: Splunk Enterprise flaw actively exploited, patch by Sunday — https://www.bleepingcomputer.com/news/security/cisa-splunk-enterprise-flaw-actively-exploited-patch-by-sunday/
16. The Register -- Council of Europe hacked in ShinyHunters PeopleSoft heist — https://www.theregister.com/cyber-crime/2026/06/15/council-of-europe-hacked-in-shinyhunters-peoplesoft-heist/5255757
17. Tenable -- Oracle June 2026 Critical Patch Update (CVE-2026-35273) — https://www.tenable.com/blog/oracle-june-2026-critical-security-patch-update-addresses-243-cves-cve-2026-35273
21. Bitsight -- Security alert: FortiBleed Fortinet VPN credentials / firewall exposed — https://www.bitsight.com/blog/security-alert-fortibleed-fortinet-vpn-credentials-firewall-exposed
22. Deepwatch -- CA-26-022: Splunk Enterprise CVE-2026-20253 (PostgreSQL sidecar) — https://www.deepwatch.com/labs/ca-26-022-unauthenticated-arbitrary-file-creation-and-truncation-in-splunk-enterprise-via-postgresql-sidecar-cve-2026-20253/
23. Brinqa / CrowdStrike -- June 2026 Patch Tuesday analysis (record 208 CVEs; KB5094126 issues; Exchange OWA) — https://www.brinqa.com/blog/june-2026-patch-tuesday-analysis

7. RANSOMWARE LANDSCAPE

SA ransomware.live victim count remains at **109 cumulative (FLAT)** for W26, with **zero new SA-named listings** on the ransomware.live tracker during 14–21 June 2026 (verified by live screenshot 21 June 10:14 SAST). The count is now unchanged for a **sixth consecutive week FLAT at 109** — the longest plateau of 2026. Africa-region activity continued elsewhere: LockBit 5.0 listed the Botswana Vaccine Institute (20 Jun), Krybit listed the Cour des Comptes du Senegal (17 Jun, 20 GB), and NightSpire listed the Sheraton El Gouna in Egypt (15 Jun).[6]

SA Contextualisation: The FLAT count is now a six-week streak and should not be read as a reduction in ransomware risk. W26 was a "structural exposure" week: FortiBleed (~74,000 firewalls), the Splunk pre-auth RCE, and the SA-attributed TeamPCP/ResoluteXBF supply-chain campaign each carry downstream consequences well beyond the immediate window. AVBOB remains undetermined more than five weeks post-attack with no leak-site claim, while ShinyHunters/UNC6240 and C10p continue dumping PeopleSoft victim data globally. SA exposure increasingly surfaces through credential leaks, supply-chain attribution, and regulatory channels rather than the ransomware.live tracker alone.[14]



End W25 baseline	109 confirmed SA listings
New W26 listings (14 - 21 Jun)	0 confirmed on ransomware.live
End W26 count	109 (FLAT -- 6th consecutive week; longest plateau of 2026)
Africa-region W26 listings	LockBit 5.0 -> Botswana Vaccine Institute; Krybit -> Cour des Comptes du Senegal; NightSpire -> Sheraton El Gouna (Egypt)
Global PeopleSoft extortion	ShinyHunters/UNC6240 + C10p dumping CVE-2026-35273 victim data (Council of Europe, Kodak, MSG, Nottingham 455k)
Threat-level drivers (non-ransomware.live)	FortiBleed credential exposure; Splunk RCE; TeamPCP/ResoluteXBF SA supply-chain attribution; AVBOB undetermined

6. Ransomware.live -- South Africa country map (W26) — https://www.ransomware.live/map/ZA
14. Ransomware.live -- SuppCenter Global / SA listing (M3RX, 11 June 2026) — https://www.ransomware.live/id/c3VwcGNlbnRlci5nbG9iYWwgLyBzdXBwY2VudGVyc2EuY29tQG0zcng

8. OSINT EXPOSURE & ATTACK SURFACE

FortiBleed -- SA FortiGate firewall and VPN credential exposure

With ~74,000 internet-facing FortiGate devices (~50% of all exposed FortiGate globally) leaking valid plaintext credentials across 21,632 domains in 194 countries, every SA FortiGate deployment is a priority attack-surface item. SA government, banking, retail, and ISP estates should check their domains at hudsonrock.com/fortinet, rotate all VPN and admin credentials, enable phishing-resistant MFA, upgrade FortiOS to 7.2.11/7.4.8/7.6.1+, and remove management interfaces from the public internet.[121]

Splunk Enterprise CVE-2026-20253 -- SIEM-of-record attack surface

Because Splunk is the SIEM of record across SA banks and telcos, an unpatched internet-reachable Splunk Enterprise with the PostgreSQL sidecar exposed is a high-value pre-auth RCE target -- and a compromised Splunk blinds the SOC. Identify all Splunk Enterprise instances, patch to 10.0.7/10.2.4 ahead of today's KEV deadline, or disable the PostgreSQL sidecar and restrict management-interface access.[3]

TeamPCP / ResoluteXBF -- software supply-chain provenance exposure

The SA-attributed npm/GitHub campaign that poisoned Trivy, Bitwarden CLI, TanStack, SAP, and Red Hat packages means dependency provenance is now an active SA attack-surface concern. SA DevSecOps teams should audit npm/PyPI/GitHub dependencies, rotate any tokens that touched the compromised registries, and subscribe to advisories for the affected vendor releases.[15]

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

With ShinyHunters/UNC6240 and Cl0p both exploiting CVE-2026-35273 and deploying backdoors that survive patching, every internet-facing PeopleSoft (PeopleTools 8.61/8.62) deployment in SA universities and provincial governments is a priority item. Apply the Oracle June CPU, review logs from 27 May onward, and treat any instance where log review is impossible as compromised.[1617]

Joomla JCE CVE-2026-48907 -- SA web-estate exposure

The pre-auth Joomla Content Editor RCE (CVSS 10.0) is under automated mass-exploitation since 9 June and is OVERDUE +2. SA Joomla sites across government, NGO, and SME estates are at high risk. Verify JCE version, and inspect the #__wf_profiles table and the images/, media/, and tmp/ directories for rogue profiles and dropped PHP web shells.[13]

CannaLeaks -- ~88,000 SA identities exposed via unauthenticated URLs

The High Times "CannaLeaks" investigation found ~985,000 identity documents exposed globally via unauthenticated URLs on the CCS/PuffPal platform (Irish controller Nefos Solutions), including ~88,000 SA individuals linked to cannabis dispensaries and clubs -- passport/ID images, names, contact details, DOBs, and facial images. SA organisations operating special-category data platforms should audit for unauthenticated direct-object references and confirm POPIA cross-border notification obligations.[10]

9. REGULATORY & COMPLIANCE

Information Regulator: Tembisa PAIA Enforcement Notice (16 June)

IR Chair Adv. Pansy Tlakula issued a scathing PAIA enforcement notice on 16 June ordering the Gauteng Department of Health to disclose Tembisa Hospital R2.3bn graft-payment records to News24 within 10 days, or face criminal prosecution (up to three years' imprisonment for the Information Officer). The notice confirms the IR will use binding enforcement powers against government departments even in politically sensitive matters. SA Information Officers should treat PAIA access requests as enforceable obligations with personal criminal liability, not discretionary administrative matters.[24]

Parliament Fills Two IR Vacancies (18 June)

The Portfolio Committee on Justice recommended Alison Tilley (part-time) and Nomagcina Mtshontshi (full-time, five-year term) to the Information Regulator on 18 June, with National Assembly and Presidential appointment pending under POPIA s.40. The appointments rebuild IR capacity at a time of escalating POPIA and PAIA enforcement activity. SA privacy officers should anticipate sustained or increased regulatory throughput.[25]

Werksmans: Misdirected Internal Email = POPIA Breach (18 June)

A Werksmans analysis (18 June) of the IR's 22 May Central JHB TVET College enforcement notice confirms that accidental, purely internal disclosures to unauthorised staff constitute a "security compromise" under POPIA, triggering s.22 notification obligations. Three POPIA violations were cited (ss.8, 15, 19), with penalties of up to a R10m fine plus 10 years' imprisonment. This applies directly to the SAPS Western Cape HR email incident. SA organisations should treat misdirected emails containing personal information as notifiable security compromises.[26]

IR Sibanye-Stillwater PAIA Precedent Confirmed (15 June)

ENS Africa and Moonstone analysis (15 June) of the IR's 22 May enforcement notice confirms that vague "commercial harm" claims under PAIA, made without supporting evidence, will be overridden. The listed-company implication is that PAIA enforcement is a real litigation risk. SA companies relying on blanket commercial-harm refusals should re-baseline their PAIA response posture against an evidence standard.[27]

Other W26 Regulatory Developments

- **FICA dual crunch (30 June / 1 July):** The FICA 2026 Risk and Compliance Return (RCR) deadline for the first batch (CASPs, credit providers, casinos, TCSPs) is 30 June, with only ~12% filed as of 18 June per the FIC. FICA ss.30/54/55/70 (mandatory cross-border cash and bearer-instrument reporting, criminal penalties, forfeiture-on-conviction) activate 1 July per Proclamation Notice 317 (GG 54783). The SARB Capital Flow Management Regulations comment window also closes 30 June.
- **DCDT AI Policy retracted (12 June, GG 3880):** DCDT formally retracted the draft National AI Policy via Government Gazette. A revised draft goes to Cabinet in November 2026 with public comment in January 2027, leaving a policy vacuum in the interim.
- **EU AI Act Digital Omnibus passes EP (16 June, 423/57/174):** High-risk obligations are postponed (Annex III standalone to 2 Dec 2027; Annex I embedded systems to 2 Aug 2028), with a new prohibition on nudifier AI apps and CSAM-generating systems from 2 Dec 2026. Council formal adoption is still required; until Official Journal publication, the original 2 August 2026 deadline remains live law, and SA AI companies with EU operations still need Article 50 user-disclosure compliance from 2 August.
- **UK DUAA s.164A complaints duty LIVE (19 June):** All controllers processing UK personal data must operate a formal complaints process (acknowledge within 30 days, investigate without undue delay, communicate outcomes) with no grace period. The same day, UK Information Commissioner John Edwards resigned following a workplace-conduct investigation, leaving a UK ICO leadership vacuum. SA businesses with UK customers, employees, or users must update privacy notices and ensure complaints routing exists.
- **US CISA BOD 26-04:** A 9 August 2026 deadline applies for US federal civilian agencies to update vulnerability-management policy to a risk-based process; SA SOCs should adopt the standard as a benchmark.
- **FATF June plenary -- Namibia delisted (~20 June):** The delisting reduces SA-Namibia correspondent-banking friction.

Compliance Deadlines — W26 Forward View

Date	Item	Owner
21 Jun 2026	CISA KEV: Splunk Enterprise CVE-2026-20253 deadline (TODAY)	IT
23 Jun 2026	CISA KEV: Chrome V8 CVE-2026-11645, Cisco SD-WAN CVE-2026-20245, Arista EOS CVE-2026-7473	IT
26 Jun 2026	Tembisa PAIA: Gauteng Dept of Health 10-day comply-or-prosecute order (issued 16 Jun)	Legal/Compliance
29 Jun 2026	CISA KEV: Cisco Catalyst SD-WAN Manager CVE-2026-20262 deadline	IT
30 Jun 2026	FICA 2026 RCR deadline (CASPs, credit providers, casinos, TCSPs); ~12% filed	Compliance
30 Jun 2026	SARB Capital Flow Management Regulations comment window closes	Finance/Legal
1 Jul 2026	FICA ss.30/54/55/70 activate (cross-border cash / bearer-instrument reporting)	Finance/Legal
2 Aug 2026	EU AI Act Art. 50 user-disclosure (live until Omnibus enters Official Journal)	Compliance
9 Aug 2026	US CISA BOD 26-04 vulnerability-management policy deadline (benchmark)	IT/Compliance
Nov 2026	SA National AI Policy revised draft to Cabinet (DCDT)	Compliance
2 Dec 2026	EU AI Act: nudifier/CSAM prohibition + Art. 50 watermarking deferral	Compliance

24. Medical Brief / News24 -- Gauteng Health ordered to hand over Tembisa files to News24 (17 June 2026) — https://www.medicalbrief.co.za/gauteng-health-ordered-to-hand-over-tembisa-files-to-news24/

25. Parliament -- Justice Committee recommends two candidates for Information Regulator (18 June 2026) — https://www.parliament.gov.za/press-releases/media-statement-justice-committee-recommends-two-candidates-information-regulator

26. Werksmans -- When a misdirected email becomes a data breach (18 June 2026) — https://werksmans.com/when-a-misdirected-email-becomes-a-data-breach-the-information-regulator-issues-an-enforcement-notice-on-internal-and-accidental-security-compromises/

27. Moonstone -- Enforcement notice may signal tougher PAIA scrutiny for companies (15 June 2026) — https://www.moonstone.co.za/enforcement-notice-may-signal-tougher-paia-scrutiny-for-companies/

10. WEEKLY THREAT HUNT & IOCs

Eight hunt missions are active for W26. Two P1 missions address the FortiBleed FortiGate credential exposure and the Splunk Enterprise pre-auth RCE (CVE-2026-20253) with its KEV deadline today. Two further P1/P2 missions address the Oracle PeopleSoft mass-compromise (now exploited by both ShinyHunters/UNC6240 and C1Op) and the SA-attributed TeamPCP/ResoluteXBF supply-chain campaign. Two P2 missions address the Joomla JCE pre-auth RCE and the Check Point IKEv1 / The Gentlemen initial-access vectors. Two P3 missions address the CannaLeaks unauthenticated-URL exposure and the AVBOB undetermined-incident impact assessment.

TH-2026-W26-01 — FortiBleed FortiGate Credential Exposure -- Rotate-and-Hunt

P1 — CRITICAL: ~74,000 firewalls; plaintext creds ITW; CISA alert 18 Jun; significant SA exposure

Hypothesis: Approximately 74,000 internet-facing FortiGate devices (~50% globally) have valid plaintext credentials circulating. SA government, banking, retail, and ISP estates are significantly exposed; any FortiGate that did not have an admin manually log in after the early-2025 PBKDF2 migration still stored crackable hashes.

MITRE ATT&CK: T1078 (Valid Accounts), T1133 (External Remote Services), T1556 (Modify Authentication Process), T1110 (Brute Force / Credential Cracking).

IOCs: Unexpected successful admin or VPN logins on FortiGate; logins from unfamiliar geolocations/ASNs; config changes outside change windows; presence of the organisation domain in the hudsonrock.com/fortinet dataset.

Data Sources: FortiGate admin/VPN authentication logs, FortiOS event logs, perimeter netflow, hudsonrock.com/fortinet exposure check, MFA/identity-provider logs.

Detection Guidance: Check the organisation domain at hudsonrock.com/fortinet. Force-rotate ALL FortiGate VPN and admin credentials. Enable phishing-resistant MFA on admin interfaces. Upgrade FortiOS to 7.2.11/7.4.8/7.6.1+ (triggers PBKDF2 re-hash on next admin login). Remove management interfaces from the public internet and review logs for unexpected successful admin logins.

TH-2026-W26-02 — Splunk Enterprise CVE-2026-20253 (KEV due TODAY) -- Pre-Auth RCE Hunt

P1 — CRITICAL: CVSS 9.8 pre-auth RCE; ITW confirmed; KEV due today; SIEM-of-record impact

Hypothesis: Splunk Enterprise PostgreSQL sidecar endpoints (/v1/postgres/recovery/backup and /restore) allow pre-auth arbitrary file write -> RCE via lo_export. Splunk PSIRT confirmed limited ITW exploitation 18 Jun; a compromised Splunk blinds the SOC across SA banks and telcos.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1059 (Command and Scripting Interpreter), T1505 (Server Software Component), T1562.001 (Impair Defenses).

IOCs: Unauthenticated POST requests to /v1/postgres/recovery/backup or /restore; unexpected files written by the Splunk service account; lo_export activity in PostgreSQL logs; new processes spawned by Splunk daemons; anomalous egress from Splunk hosts.

Data Sources: Splunk web-access logs, Splunk internal/PostgreSQL logs, host EDR process-creation telemetry, perimeter logs for the Splunk management interface, egress netflow.

Detection Guidance: Inventory all Splunk Enterprise instances and patch to 10.0.7/10.2.4 ahead of the 21 June KEV deadline. If patching is not immediately possible, disable the PostgreSQL sidecar and restrict management-interface network access. Hunt for unauthenticated requests to the sidecar endpoints and Splunk-service-account file writes. Splunk Cloud Platform is not affected.

TH-2026-W26-03 — Oracle PeopleSoft CVE-2026-35273 (OVERDUE +6) -- ShinyHunters + Cl0p Backdoor Hunt

P1 — CRITICAL: OVERDUE +6; two ransomware groups; backdoors survive patching

Hypothesis: Both ShinyHunters/UNC6240 and Cl0p are exploiting CVE-2026-35273, and UNC6240 backdoors survive patching. Any SA PeopleSoft instance (PeopleTools 8.61/8.62) that was internet-facing before patching should be assumed compromised regardless of patch status.

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

IOCs: Web shells in PeopleSoft PIA web directories; persistence artefacts surviving patch; anomalous PS service-account authentication; bulk record exports; outbound connections to unfamiliar IPs from PeopleSoft tiers.

Data Sources: PeopleSoft PIA web-server logs, application-server logs, database audit logs, file-integrity monitoring, egress netflow, logs retained from 27 May onward.

Detection Guidance: Apply the Oracle June 2026 CPU AND review logs from 27 May onward (mandatory). Hunt for persistent backdoors that survive patching, web shells, and bulk data egress. Treat any instance where 27 May log review is impossible as compromised. Prioritise SA universities (HESA) and provincial governments.

TH-2026-W26-04 — TeamPCP / ResoluteXBF (SA-Attributed) -- Dependency-Provenance and Token Hunt

P2 — HIGH: SA-attributed; law-enforcement-relevant; software supply-chain provenance risk

Hypothesis: A single SA-based operator poisoned Trivy, Bitwarden CLI, TanStack, SAP, and Red Hat packages and exfiltrated ~3,800 GitHub repositories in 11 minutes. SA DevSecOps environments that consumed affected releases may have leaked tokens or ingested malicious dependencies.

MITRE ATT&CK: T1195.002 (Compromise Software Supply Chain), T1199 (Trusted Relationship), T1552 (Unsecured Credentials), T1528 (Steal Application Access Token).

IOCs: Affected versions of Trivy / Bitwarden CLI / TanStack / SAP / Red Hat packages in build manifests; anomalous outbound traffic from CI/CD runners; unexpected use of GitHub/npm tokens; new or unfamiliar repository clones/exfiltration patterns.

Data Sources: CI/CD pipeline logs, npm/PyPI/GitHub audit logs, SBOM / dependency manifests, secrets-scanning output, GitHub token and repository access logs.

Detection Guidance: Audit npm/PyPI/GitHub dependency provenance against the affected releases. Rotate any tokens that touched the compromised registries. Subscribe to vendor advisories for Trivy, Bitwarden CLI, TanStack, SAP, and Red Hat. Review CI/CD egress and GitHub repository access for anomalies.

TH-2026-W26-05 — Joomla JCE CVE-2026-48907 (OVERDUE +2) -- Web-Shell Hunt

P2 — HIGH: CVSS 10.0; OVERDUE +2; mass-automated exploitation since 9 Jun

Hypothesis: The pre-auth Joomla Content Editor RCE (CVSS 10.0) is under automated mass-exploitation since 9 June. SA Joomla sites across government, NGO, and SME estates may already have dropped web shells.

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

IOCs: Rogue rows in the #__wf_profiles table; unexpected PHP files in images/, media/, and tmp/ directories; anomalous POST requests to JCE endpoints; web-server processes spawning shells.

Data Sources: Joomla/CMS web-server access logs, file-integrity monitoring on the web root, database audit logs for #__wf_profiles, WAF logs.

Detection Guidance: Verify JCE version (>= 2.9.99.5). Review the #__wf_profiles table and the images/, media/, and tmp/ directories for rogue profiles and PHP files. Patch immediately given the OVERDUE +2 KEV status, and hunt for post-exploitation web shells on all SA Joomla estates.

TH-2026-W26-06 — Check Point IKEv1 CVE-2026-50751 (OVERDUE +10) -- Qilin / The Gentlemen Access Hunt

P2 — HIGH: CVSS 9.3; OVERDUE +10; Qilin + The Gentlemen initial access

Hypothesis: Check Point IKEv1 CVE-2026-50751 (CVSS 9.3) is OVERDUE +10 and exploited by Qilin and used as an initial-access vector by The Gentlemen / LARVA-368. Exploitation began as early as 7 May; any active IKEv1 gateway is at risk.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1133 (External Remote Services), T1078 (Valid Accounts).

IOCs: Anomalous IKEv1 VPN session establishment; management-plane access from unfamiliar IPs; configuration changes outside change windows; post-exploitation lateral movement following VPN access.

Data Sources: Check Point gateway/VPN logs, management-plane audit logs, perimeter netflow, internal east-west telemetry.

Detection Guidance: Disable IKEv1 where not required and apply the 8 June hotfixes. Treat any active VPN session anomalies prior to the fix as potentially compromised. Hunt for Qilin and The Gentlemen post-access activity, and validate that CVE-2026-20131 (Cisco FMC) is also remediated.

TH-2026-W26-07 — CannaLeaks Unauthenticated-URL Exposure -- SA Special-Category Data

P3 — MONITORING: ~88,000 SA identities; unauthenticated-URL exposure; POPIA cross-border

Hypothesis: The CCS/PuffPal platform exposed ~985,000 identity documents (incl. ~88,000 SA individuals) via unauthenticated URLs. SA organisations operating similar special-category data platforms may have equivalent insecure-direct-object-reference exposure.

MITRE ATT&CK: Not applicable (web exposure / IDOR governance hunt).

IOCs: Unauthenticated direct-object-reference URLs serving ID/passport/facial images; absent access controls on document endpoints; bulk sequential-ID enumeration in web logs.

Data Sources: Web-application access logs, external attack-surface scans, application authorisation configuration, POPIA processing records.

Detection Guidance: Audit special-category data platforms for unauthenticated direct-object references and missing authorisation checks. Confirm POPIA cross-border notification obligations are assessed (Irish controller; GDPR primary, POPIA cross-border likely triggered). Monitor for bulk enumeration of document endpoints.

TH-2026-W26-08 — AVBOB Undetermined Incident -- Supplier/Partner Impact Assessment

P3 — MONITORING: undetermined 5+ weeks; no claim/attribution; sector supply-chain risk

Hypothesis: AVBOB remains in partial restoration more than five weeks after the 30 May attack with no leak-site claim or attribution as of 21 June. Suppliers, partners, and affiliates sharing access pathways may face correlated exposure while the incident status is undetermined.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1486 (Data Encrypted for Impact), T1657 (Financial Theft), T1199 (Trusted Relationship).

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

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

Detection Guidance: If you are an AVBOB supplier, partner, or affiliate, conduct an independent risk review of shared access pathways given AVBOB's undetermined status. Monitor indexed leak sites for any AVBOB claim. Review partner-integration access logs for anomalies during and after the incident window. Verify POPIA s.22 readiness.

IOC Master Table — W26

Indicator	Type	Attribution	Hunt ID
FortiGate plaintext creds (hudsonrock.com/fortinet)	Cred leak	FortiBleed; ~74,000 firewalls; CISA alert 18 Jun; rotate all VPN/admin creds	TH-2026-W26-01
CVE-2026-20253 (Splunk /v1/postgres/recovery endpoints)	CVE	Pre-auth RCE CVSS 9.8; ITW (Splunk PSIRT 18 Jun); KEV 21 Jun; patch 10.0.7/10.2.4	TH-2026-W26-02
CVE-2026-35273 (PeopleSoft web shells / backdoors)	CVE/0-day	ShinyHunters/UNC6240 + Cl0p; OVERDUE +6; backdoors survive patching	TH-2026-W26-03
Trivy / Bitwarden CLI / TanStack / SAP / Red Hat poisoned pkgs	Supply chain	TeamPCP / ResoluteXBF (SA-attributed); ~3,800 GitHub repos in 11 min	TH-2026-W26-04
CVE-2026-48907 (Joomla JCE; #__wf_profiles; images/media/tmp PHP)	CVE	Pre-auth RCE CVSS 10.0; OVERDUE +2; mass-automated since 9 Jun	TH-2026-W26-05
CVE-2026-50751 (Check Point IKEv1)	CVE	OVERDUE +10; Qilin + The Gentlemen initial access; since ~7 May	TH-2026-W26-06
CVE-2026-20131 (Cisco FMC)	CVE	The Gentlemen / LARVA-368 secondary initial-access vector	TH-2026-W26-06
GentleKiller EDR-killer framework (8 variants, 400+ processes)	Malware	The Gentlemen / Storm-2697 / LARVA-368 (ESET "Killing Me Gently")	TH-2026-W26-06
Unauthenticated CCS/PuffPal document URLs	Web exposure	CannaLeaks; ~88,000 SA identities; IDOR; POPIA cross-border	TH-2026-W26-07
CVE-2026-11645 (Chrome V8) / CVE-2026-20245 (Cisco SD-WAN) / CVE-2026-7473 (Arista)	CVE	KEV deadlines 23 Jun; patch / filtering workaround	N/A (carryover)

11. RECOMMENDATIONS

Immediate (Next 72 Hours — Priority P1)

- **1. FortiBleed triage:** Check the organisation domain at hudsonrock.com/fortinet; force-rotate ALL FortiGate VPN and admin credentials; enable phishing-resistant MFA on admin interfaces; upgrade FortiOS to 7.2.11/7.4.8/7.6.1+; remove management interfaces from the public internet; and review logs for unexpected successful admin logins. ~74,000 firewalls are exposed globally with significant SA presence.
- **2. Splunk Enterprise CVE-2026-20253 (KEV due TODAY):** Patch to 10.0.7 or 10.2.4 immediately. If patching is not immediately possible, disable the PostgreSQL sidecar and restrict network access to the management interface. Splunk Cloud Platform is not affected. A compromised Splunk blinds the SOC.
- **3. Joomla JCE CVE-2026-48907 (OVERDUE +2):** Verify the JCE version (>= 2.9.99.5); review the #__wf_profiles table and the images/, media/, and tmp/ directories for rogue profiles and PHP web shells. Mass-automated exploitation has been ongoing since 9 June.
- **4. Exchange OWA CVE-2026-42897 -- apply KB5094139:** If not yet applied, deploy KB5094139 (the permanent fix that replaces the W22 EEMS interim mitigation). The flaw is actively exploited; run Exchange Health Checker to confirm a healthy state before removing EEMS M2.
- **5. Oracle PeopleSoft CVE-2026-35273 (OVERDUE +6):** For any internet-accessible 8.61/8.62 endpoint, apply the Oracle June CPU AND review logs from 27 May onward. Treat the instance as compromised if log review is impossible -- UNC6240 backdoors survive patching, and Cl0p is now also exploiting the flaw.

This Week

- AVBOB suppliers, partners, and affiliates: conduct an independent risk review of shared access pathways given AVBOB's undetermined status more than five weeks post-attack.
- Check Point Security Gateway IKEv1 (CVE-2026-50751, OVERDUE +10): disable IKEv1 where not required; apply the 8 June hotfixes; treat any active VPN session anomalies prior to the fix as potentially compromised (Qilin + The Gentlemen exploitation).
- Cisco SD-WAN: confirm patched builds for CVE-2026-20245 (KEV 23 Jun, patch now available) and CVE-2026-20262 (Catalyst SD-WAN Manager, KEV 29 Jun).
- SA universities and provincial governments running PeopleSoft: apply the Oracle June CPU and review logs from 27 May onward (see immediate item 5).
- POPIA internal-email controls: given the Werksmans/IR clarification, audit shared-mailbox handling, group sends, and attachment policies. Treat misdirected emails containing personal information as notifiable security compromises (directly applicable to the SAPS WC incident).
- Chrome V8 (CVE-2026-11645) and Arista EOS (CVE-2026-7473): push the estate-wide browser update and implement the Arista tunnel-decap filtering workaround ahead of the 23 June KEV deadlines.

Strategic (Next Quarter)

- FICA filings: first-batch institutions (CASPs, credit providers, casinos, TCSPs) must file the 2026 RCR by 30 June -- only ~12% had filed as of 18 June.
- Cross-border cash reporting: ensure operational readiness for FICA ss.30/54/55/70 effective 1 July (criminal penalties and forfeiture-on-conviction powers).
- UK customer/employee touchpoints: implement the DUAA s.164A complaints process now (effective 19 June, no grace period; UK ICO leadership vacuum following the Commissioner's resignation).
- Software supply-chain provenance: given the TeamPCP/ResoluteXBF SA attribution, stand up a dependency-provenance programme -- audit npm/PyPI/GitHub dependencies, rotate tokens that touched compromised registries, and subscribe to vendor advisories for the affected Trivy, Bitwarden CLI, TanStack, SAP, and Red Hat releases.
- Edge-appliance and SIEM resilience programme: the FortiBleed exposure, the Ivanti Sentry OVERDUE KEV, and the Splunk pre-auth RCE collectively warrant a structured edge/SIEM lifecycle programme -- rapid patch SLAs, credential rotation discipline, MFA, and reduced internet exposure for all management interfaces.

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. Security Affairs -- CISA warns of active exploitation following FortiBleed leak — https://securityaffairs.com/193902/hacking/cisa-warns-of-active-exploitation-following-fortibleed-leak.html
2. Bitsight -- Security alert: FortiBleed Fortinet VPN credentials / firewall exposed — https://www.bitsight.com/blog/security-alert-fortibleed-fortinet-vpn-credentials-firewall-exposed
3. BleepingComputer -- CISA: Splunk Enterprise flaw actively exploited, patch by Sunday — https://www.bleepingcomputer.com/news/security/cisa-splunk-enterprise-flaw-actively-exploited-patch-by-sunday/
4. Deepwatch -- CA-26-022: Splunk Enterprise CVE-2026-20253 (PostgreSQL sidecar) — https://www.deepwatch.com/labs/ca-26-022-unauthenticated-arbitrary-file-creation-and-truncation-in-splunk-enterprise-via-postgresql-sidecar-cve-2026-20253/
5. The Register -- Council of Europe hacked in ShinyHunters PeopleSoft heist (15 June 2026) — https://www.theregister.com/cyber-crime/2026/06/15/council-of-europe-hacked-in-shinyhunters-peoplesoft-heist/5255757
6. Tenable -- Oracle June 2026 Critical Patch Update (CVE-2026-35273) — https://www.tenable.com/blog/oracle-june-2026-critical-security-patch-update-addresses-243-cves-cve-2026-35273
7. KrebsOnSecurity -- TeamPCP / ResoluteXBF SA supply-chain attribution (June 2026) — https://krebsonsecurity.com/
8. ESET WeLiveSecurity -- "Killing Me Gently": GentleKiller / The Gentlemen analysis — https://www.welivesecurity.com/

9. ITWeb -- Malicious actors take down AVBOB's digital platforms — https://www.itweb.co.za/article/malicious-actors-take-down-avbobs-digital-platforms/5yONP7Erd6QMXWrb
10. AVBOB -- Progress on System Restoration (W26 PDF) — https://www.avbob.co.za/media/pdf/system-restoration-progress.pdf
11. eNCA -- AVBOB confirms ongoing recovery (18 June 2026) — https://www.facebook.com/eNCAnews/posts/avbob-confirms-that-the-recent-disruption-to-certain-of-its-digital-platforms-an/1326555792960733/
12. 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/
13. High Times -- CannaLeaks: nearly one million cannabis club users' data exposed (17 June 2026) — https://hightimes.com/news/cannaleaks-nearly-one-million-cannabis-club-users-data-was-exposed/
14. IOL -- NPA Asset Forfeiture Unit freezes R21.5m linked to online banking scam (15 June 2026) — https://iol.co.za/news/crime-and-courts/2026-06-15-npa-asset-forfeiture-unit-secures-court-order-to-freeze-r215million-linked-to-online-banking-scam/
15. EWN -- TikTok breach sparks fresh concerns over children's online safety (12 June 2026) — https://www.ewn.co.za/2026/06/12/tiktok-breach-sparks-fresh-concerns-over-children-s-online-safety
16. GroundUp -- Here's how insecure governments' websites are (Part 2) — https://groundup.org.za/article/heres-how-insecure-governments-websites/
17. Ransomware.live -- South Africa country map / SuppCenter M3RX listing — https://www.ransomware.live/map/ZA
18. CrowdStrike / Brinqa -- June 2026 Patch Tuesday analysis (record 208 CVEs; Exchange OWA) — https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-june-2026/
19. Dragos / Broadcom-Symantec / CYFIRMA / The Hacker News / AhnLab -- W26 threat research — https://www.dragos.com/blog/
20. CISA -- Binding Operational Directive 26-04 / KEV Catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
21. Medical Brief / News24 -- Gauteng Health ordered to hand over Tembisa files (17 June 2026) — https://www.medicalbrief.co.za/gauteng-health-ordered-to-hand-over-tembisa-files-to-news24/
22. Parliament of South Africa -- Justice Committee recommends two IR candidates (18 June 2026) — https://www.parliament.gov.za/press-releases/media-statement-justice-committee-recommends-two-candidates-information-regulator
23. Werksmans -- When a misdirected email becomes a data breach (18 June 2026) — https://werksmans.com/when-a-misdirected-email-becomes-a-data-breach-the-information-regulator-issues-an-enforcement-notice-on-internal-and-accidental-security-compromises/
24. Moonstone -- Enforcement notice may signal tougher PAIA scrutiny for companies (15 June 2026) — https://www.moonstone.co.za/enforcement-notice-may-signal-tougher-paia-scrutiny-for-companies/
25. The Verge -- Passports data breach: Cannabis Club Systems / Nefos / PuffPal (10 June 2026) — https://www.theverge.com/tech/947157/passports-data-breach-cannabis-club-systems-nefos-puffpal

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-W26 | Published Monday 22 June 2026