DIGITAL PROGRESSION

SOUTH AFRICA
CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 27 | 21 June – 28 June 2026

THREAT LEVEL: HIGH

#OpSouthAfrica hacktivism (Nullsec Nigeria / Anonymous Nigeria) breaches the Department of Correctional Services and Ephraim Mogale Local Municipality, with threats against SARS, SITA and ProWellness running into a 30 June flashpoint. The Information Regulator served 10-day notices on TransUnion SA and Experian SA (26 June) over an alleged W27 credit-bureau breach. Prinz Eugen / ROOTBOY is now publicly attributed for the ongoing Standard Bank Group leak (~1.2 TB / 154M rows, 100,000 rows/day). An unnamed SA medical aid (~200,000 members) breach is claimed; FortiBleed confirms SA banks, municipalities and universities in the dataset. SA ransomware count is 108 (net -1 vs W26 from a single delisting; 7th consecutive week HIGH).

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W27 | Classification: TLP:WHITE

Published Monday 29 June 2026

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH (unchanged, 7th consecutive week) — Week 27 (21–28 June 2026)

Story 1 — #OpSouthAfrica Hacktivism Breaches Two State Entities Into a 30 June Flashpoint: Week 27 is the first week in months where SA-targeted hacktivism is the dominant story. Two crews — Nullsec Nigeria and Anonymous Nigeria — breached the Department of Correctional Services (~11 GB claimed, document evidence posted) and Ephraim Mogale Local Municipality in retaliation for xenophobic violence against Nigerians in SA. Further claims against SARS, SITA and ProWellness remain unverified (SARS denies). The 30 June anti-immigration deadline creates a sustained high-risk window running into W28. Anyone with .gov.za, .ac.za or SOE infrastructure should brief their SOC, tighten WAF rules, monitor for OWASP Top 10 probing and validate IR retainer contacts.[1]

Story 2 — Information Regulator Serves 10-Day Notices on TransUnion SA and Experian SA: Both credit bureaus were served 10-day notices on 26 June over an alleged new W27 breach, with responses due by approximately 6 July. This is the first invocation since 2024 of the IR's POPIA enforcement-notice power against the credit-bureau sector, and it echoes the 2024 enforcement against TransUnion for the 2022 N4ughtySecTU incident affecting 3M+ SA consumers. The IR is also now confirmed at full strength after the National Assembly endorsed Mtshontshi (full-time) and Tilley (part-time) on 23 June. TransUnion / Experian customers should request written breach-status confirmation and monitor for out-of-cycle credit reports.[2]

Story 3 — Prinz Eugen / ROOTBOY Publicly Attributed for the Ongoing Standard Bank Group Leak: Malwarebytes ThreatDown published full attribution and IOC analysis on 22 June: a newly attributed solo operator (handles ROOTBOY / avtokz / GERMANIA) running Go-based Prinz Eugen ransomware exfiltrated ~1.2 TB / 154 million SQL rows in a February 2026 breach. After Standard Bank refused a 1 BTC ransom (~$107,000), the operator escalated to publishing 100,000 rows/day on a dedicated dark-web portal; Liberty Insurance (a Standard Bank subsidiary) is also listed. Separately, an unnamed SA medical aid (~200,000 members) appeared on Data Breaches Digest 25 June with no attribution, and FortiBleed is now confirmed at 73,932–86,644 compromised FortiGates with named SA banks, municipalities and universities in the dataset. Two more "due today" KEVs — Cisco UCM CVE-2026-20230 (8.6) and PTC Windchill CVE-2026-12569 (9.3) — demand same-day patching, and the FICA cross-border cash regime goes live 1 July with no grace period. SA ransomware.live holds at 108 (net -1 vs W26 from a single delisting).[3][4][5]

KPI Dashboard

Metric	Current (W27)	Prior (W26)	Change	Direction
SA threat level	HIGH	HIGH	Unchanged (7th consecutive week)	FLAT
SA ransomware.live victims (total)	108	109	Net -1 (single delisting; no new SA listings)	DOWN
New SA RW listings this week (ransomware.live)	0 confirmed	0 (W26)	FLAT	FLAT
#OpSouthAfrica hacktivism (Nullsec / Anonymous Nigeria)	DCS (~11 GB) + Ephraim Mogale breached; SARS/SITA/ProWellness threats; 30 Jun flashpoint	N/A	NEW W27	UP
IR 10-day notices to TransUnion SA + Experian SA	Served 26 Jun over alleged W27 credit-bureau breach; response due ~6 Jul	N/A	NEW W27	UP
Prinz Eugen / ROOTBOY -- Standard Bank leak	Publicly attributed 22 Jun; 1.2 TB / 154M rows; 100,000 rows/day; Liberty listed	Unattributed (prior)	ESCALATING	UP
Unnamed SA medical aid breach	~200,000 members claimed (Data Breaches Digest 25 Jun); no attribution	N/A	NEW W27	UP
FortiBleed confirmed SA exposure	73,932-86,644 FortiGates; SA banks/munis/universities/healthcare in dataset	~74,000 (CISA alert W26)	CONFIRMED	UP
New CISA KEV additions (21-28 Jun)	6 (Cisco UCM 8.6 + PTC Windchill 9.3 due TODAY; Ubiquiti UniFi x3; Lantronix 9.8)	5 (W26)	ELEVATED	UP
AVBOB Mutual Assurance (carryover)	Partial-manual mode persists 20+ days; still no leak-site claim/attribution	Partial restoration (W26)	UNDETERMINED	FLAT
SAPS Western Cape POPIA breach (carryover)	Investigation continues; no IR enforcement notice as of 28 Jun	Independent investigator (W26)	INVESTIGATION	FLAT
FICA cross-border cash regime	ss.30/54/55/70 LIVE 1 July; no grace period; criminal penalties	N/A	NEW W27	UP

W27 KEY FRAMING: W27 is the first week in months where SA-targeted hacktivism becomes the dominant story rather than a footnote. Three threads drive the week: the #OpSouthAfrica campaign (Nullsec Nigeria / Anonymous Nigeria) breaching two state entities into a 30 June flashpoint; the Information Regulator escalating against TransUnion SA and Experian SA with 10-day notices; and the public attribution of the ongoing Standard Bank Group data-leak to Prinz Eugen / ROOTBOY (now publishing 100,000 rows/day). The ransomware.live count edged down to 108 (net -1 vs W26 from a single delisting, NOT a new SA victim), masking real threat activity that increasingly surfaces through hacktivism, regulatory channels, and active data-leak portals. The dominant operational drivers are two "due today" KEVs (Cisco UCM CVE-2026-20230 and PTC Windchill CVE-2026-12569), hacktivist hardening through 30 June, and the FICA cross-border cash regime going live 1 July.

TOP 3 ACTIONS THIS WEEK

1. TWO KEV "DUE TODAY" (28 JUN) -- CISCO UCM CVE-2026-20230 (8.6) + PTC WINDCHILL CVE-2026-12569 (9.3): Treat any internet-exposed Cisco UCM with WebDialer enabled as compromised until proven clean (SSRF escalates to RCE; Tor-routed automated sweeps since 22 Jun); review /platform-services/axis2-web/ for unexpected .jsp files and apply Cisco's hotfix. For PTC Windchill / FlexPLM, apply PTC advisory CS473270 and review /Windchill/servlet/ for JSP webshells — this is the first-ever PTC entry in the CISA KEV catalog, with SA exposure across aerospace, mining engineering and defence contractors.

2. HACKTIVIST HARDENING (NEXT 72 HOURS THROUGH 30 JUNE): The #OpSouthAfrica campaign has already breached the Department of Correctional Services (~11 GB) and Ephraim Mogale Local Municipality, with threats against SARS, SITA and ProWellness. Anyone with .gov.za, .ac.za or SOE infrastructure must brief their SOC, tighten WAF rules, monitor for OWASP Top 10 probing, review API exposure and pre-stage IR retainer escalation. Communications and finance ministries are the highest priority into the 30 June flashpoint and W28.

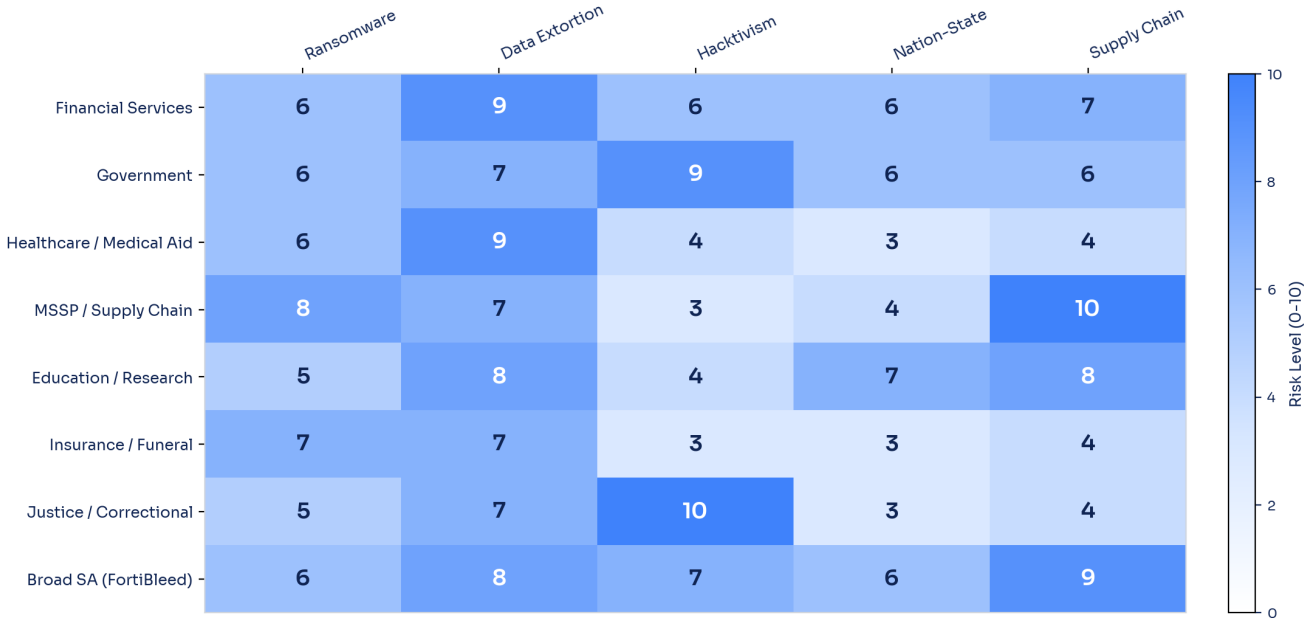
3. FORTIBLEED FINAL TRIAGE + STANDARD BANK / CREDIT-BUREAU EXPOSURE: FortiBleed is confirmed at 73,932-86,644 FortiGates with named SA banks, municipalities and universities in the dataset — last call to rotate ALL FortiGate VPN and admin credentials, enforce phishing-resistant MFA, upgrade FortiOS to 7.2.11/7.4.8/7.6.1+, and remove management interfaces from the public internet. Standard Bank suppliers should review shared access pathways and rotate any integration tokens; TransUnion / Experian customers should request written breach-status confirmation given the IR notices.

1. Nigeria Communications Week -- Xenophobic attacks: Anonymous Nigeria threatens to leak South African stolen data (27 June 2026) — https://www.nigeriacommunicationsweek.com.ng/xenophobic-attacks-anonymous-nigeria-threatens-to-leak-south-african-stolen-data/
2. ITWeb -- Information Regulator serves notices on TransUnion and Experian (26 June 2026) — https://www.itweb.co.za/categories/oJKjlyr7wO7k6amV
3. Malwarebytes ThreatDown -- Prinz Eugen ransomware / ROOTBOY attribution (22 June 2026) — https://www.malwarebytes.com/blog/threat-intelligence/2026/06/prinz-eugen-ransomware-rootboy
4. Data Breaches Digest -- Unnamed SA medical aid breach (25 June 2026) — https://www.dbdigest.com
5. Recorded Future -- Critical FortiBleed campaign — https://www.recordedfuture.com/blog/critical-fortibleed-campaign

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 27 (21–28 June 2026). **Justice/Correctional** peaks at 10 on Hacktivism following the #OpSouthAfrica breaches of the Department of Correctional Services (~11 GB) and Ephraim Mogale Local Municipality, while **Government** sits at 9 on Hacktivism given the sustained Nullsec Nigeria / Anonymous Nigeria campaign and threats against SARS, SITA and ProWellness. **Financial Services** and **Healthcare/Medical Aid** sit at 9 on Data Extortion (the publicly attributed Standard Bank / Liberty leak by Prinz Eugen / ROOTBOY plus the TransUnion / Experian IR notices; the unnamed ~200,000-member medical aid breach). **MSSP/Supply Chain** peaks at 10 on Supply Chain (SuppCenter M3RX carryover plus the TeamPCP / ResoluteXBF SANS white paper), and **Broad SA (FortiBleed)** registers 9 on Supply Chain reflecting named SA banks, municipalities, universities and healthcare entities in the confirmed 73,932–86,644-device dataset.

SA THREAT LANDSCAPE HEATMAP | W27 (21 - 28 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. TOP SA INCIDENTS (W27)

Week 27 (21–28 June 2026): the SA ransomware.live tally edged to 108 (net -1 vs W26 from a single delisting; no new SA leak-site postings in the window). Hacktivism dominates: (1) the #OpSouthAfrica campaign breaching the Department of Correctional Services and Ephraim Mogale Local Municipality; (2) Information Regulator 10-day notices to TransUnion SA and Experian SA over an alleged W27 credit-bureau breach; (3) the publicly attributed Prinz Eugen / ROOTBOY data-leak against Standard Bank Group (1.2 TB / 154M rows, 100,000 rows/day; Liberty also listed); (4) an unnamed SA medical aid (~200,000 members) breach claimed; (5) AVBOB still partial and unattributed at 20+ days; (6) SAPS Western Cape investigation continuing; (7) FortiBleed confirmed SA exposure; (8) SuppCenter Global/SA still on M3RX. Africa-region W27 activity: Nova DOSAB (SA industrial, claimed); NightSpire still holding EC Human Settlements + Ingonyama Trust.[6]

3.1 INC-2026-W27-01 — #OpSouthAfrica: Nullsec Nigeria / Anonymous Nigeria Hacktivist Campaign [CONFIRMED partial release]

Sector	Government / State entities (Correctional Services; municipal)
Trigger	Xenophobic violence against Nigerians in SA (20+ reported killed, hundreds evacuated); 30 June 2026 anti-immigration deadline
Confirmed	Department of Correctional Services -- ~11 GB claimed by Nullsec Nigeria; document evidence posted publicly. Ephraim Mogale Local Municipality -- separate Nullsec Nigeria release
Claimed (unverified)	SARS, SITA, ProWellness -- additional claims by Anonymous Nigeria; SARS denies; sustained threats of further dumps
Significance	Most prolific state-sector hacktivist escalation against SA in years; operational risk extends through W28
Confidence	CONFIRMED (DCS + Ephraim Mogale); UNVERIFIED (SARS/SITA/ProWellness)

Two distinct hacktivist crews — Nullsec Nigeria and Anonymous Nigeria — were active during W27 in retaliation for xenophobic violence against Nigerians in South Africa. Confirmed compromises include the Department of Correctional Services (~11 GB claimed by Nullsec Nigeria, with document evidence posted publicly) and Ephraim Mogale Local Municipality. Additional claims against SARS, SITA and ProWellness remain unverified — SARS denies a breach — but the crews continue to threaten further dumps. The 30 June 2026 anti-immigration deadline creates a sustained high-risk window running into W28. SA defenders with .gov.za, .ac.za or SOE infrastructure should harden public-facing web infrastructure, tighten WAF rules, review API exposure and pre-stage IR retainer escalation.[6]

3.2 INC-2026-W27-02 — Information Regulator 10-Day Notice to TransUnion SA & Experian SA [CONFIRMED]

Sector	Financial Services / Credit bureaus (regulatory action)
Date	26 June 2026
Action	IR demanded details within 10 days from both credit bureaus over an alleged new breach during W27
Precedent	Echoes 2024 enforcement against TransUnion for the 2022 N4ughtySecTU breach affecting 3M+ SA consumers and 6M businesses
Deadline	Bureaus must respond by ~6 July; failure triggers an infringement notice and potential administrative fine
Confidence	CONFIRMED (regulatory action); underlying breach UNVERIFIED

On 26 June the Information Regulator served 10-day notices on both TransUnion SA and Experian SA, demanding details over an alleged new credit-bureau breach during W27. This is the first invocation since 2024 of the IR's POPIA enforcement-notice power against the credit-bureau sector, echoing the 2024 enforcement against TransUnion for the 2022 N4ughtySecTU incident that affected 3M+ SA consumers and 6M businesses. The bureaus must respond by approximately 6 July; failure would trigger an infringement notice and a potential administrative fine. TransUnion / Experian customers should request written breach-status confirmation from their account contacts and monitor for any out-of-cycle credit reports.[7]

3.3 INC-2026-W27-03 — Prinz Eugen / ROOTBOY: Standard Bank Group Active Data-Leak [CONFIRMED attribution]

Sector	Financial Services (Standard Bank Group; Liberty Insurance subsidiary)
Actor	Newly attributed solo operator -- handles ROOTBOY / avtokz / GERMANIA; Go-based Prinz Eugen ransomware
Scale	~1.2 TB / 154 million SQL rows exfiltrated in a February 2026 breach (W18 attack)
Escalation	After Standard Bank refused a 1 BTC ransom (~$107,000), the operator escalated to 100,000 rows/day on a dedicated dark-web portal
Related	Liberty Insurance (Standard Bank subsidiary) also listed; Standard Bank status page shows no incident
Confidence	CONFIRMED (Malwarebytes ThreatDown attribution + IOC analysis, 22 Jun)

Malwarebytes ThreatDown published full attribution and IOC analysis on 22 June, naming a solo operator (handles ROOTBOY / avtokz / GERMANIA) running Go-based Prinz Eugen ransomware as responsible for the ongoing Standard Bank Group data-leak. Approximately 1.2 TB / 154 million SQL rows were exfiltrated in a February 2026 breach (the W18 attack). After Standard Bank refused the 1 BTC ransom (~$107,000), the operator escalated to publishing 100,000 rows/day on a dedicated dark-web portal; Liberty Insurance, a Standard Bank subsidiary, is also listed. The Standard Bank status page shows no incident, consistent with the bank's continued silence. This is direct SA bank intelligence — defenders should run YARA and IOC sweeps across all RDP-exposed assets, and Standard Bank suppliers should review shared access pathways and rotate integration tokens.[8]

3.4 INC-2026-W27-04 — Unnamed SA Medical Aid: ~200,000 Members Affected [CLAIMED]

Sector	Healthcare / Medical aid scheme (SA)
Date	25 June 2026 (Data Breaches Digest listing)
Scale	~200,000 members
Attribution	No threat actor, scheme identity, or POPIA notification public
Intelligence gap	Scheme identification is the primary intelligence gap for W28
Confidence	CLAIMED (unverified)

On 25 June, Data Breaches Digest listed an unnamed SA medical aid as breached, affecting approximately 200,000 members. No threat actor, scheme identity, or POPIA notification is public, and scheme identification is the primary intelligence gap heading into W28. SA medical schemes and their administrators should proactively verify their own breach posture, review access logs for member-data exfiltration, and prepare POPIA s.22 notification readiness in case they are the unnamed entity.[9]

3.5 INC-2026-W27-05 — FortiBleed: Confirmed SA Exposure (Recorded Future 24 June) [CONFIRMED]

Sector	Broad SA (banks, municipalities, universities, healthcare)
Final count	73,932-86,644 FortiGate devices compromised across 194 countries
Credentials	110M+ credentials harvested via custom Golang sniffer across 24 protocols
Attribution	Russian-speaking IAB "SantaAd"; campaign still active 28 Jun
SA exposure	SA banks, municipalities, universities and healthcare entities in the dataset (SA security analyst confirmation); CRAN Namibia warned 13 regional organisations
Confidence	CONFIRMED

Recorded Future confirmed the final FortiBleed compromise count on 24 June at 73,932–86,644 FortiGate devices across 194 countries, with 110M+ credentials harvested via a custom Golang sniffer across 24 protocols. The campaign remains active as of 28 June under the Russian-speaking initial-access broker "SantaAd". Critically, SA banks, municipalities, universities and healthcare entities are confirmed in the dataset by an SA security analyst, and CRAN Namibia warned 13 regional organisations about the spillover. SA estates should treat this as a final-triage call: rotate ALL FortiGate VPN and admin credentials, enforce phishing-resistant MFA, upgrade FortiOS to 7.2.11/7.4.8/7.6.1+, and remove management interfaces from the public internet.[5][10]

3.6 AVBOB + SAPS WC + SuppCenter + Africa-Region Carryover (W27 Status)

AVBOB Mutual Assurance: 20+ days post-attack (30 May origin); several systems restored but partial-manual mode persists. No ransomware group has claimed AVBOB on any monitored leak site as of 28 June; no ransom note, data sample, or group name is public, and no POPIA s.22 notification has been published. **SAPS Western Cape POPIA breach:** an independent senior SAPS officer from outside the Western Cape is confirmed in role; no IR enforcement notice as of 28 June; POPCRU cited POPIA violations but has filed no court action. **SuppCenter Global/SA (M3RX):** listed 11 June, no follow-up data release in W26 or W27 — MSSP downstream client risk remains.[11][12]

Prior Item	W27 Update
AVBOB Mutual Assurance	20+ days post-attack; partial-manual mode persists; NO leak-site claim or attribution as of 28 Jun; no POPIA s.22 notification.
SAPS Western Cape POPIA breach	Independent senior SAPS officer (outside WC) confirmed; no IR enforcement notice as of 28 Jun; POPCRU cited violations, no court action.
SuppCenter Global/SA (M3RX)	Listed 11 Jun; no follow-up data release in W26 or W27; MSSP downstream client risk remains.
ransomware.live ZA cumulative	108 (verified live screenshot 28 Jun); net -1 vs W26 from a single operator-side delisting; no new SA leak-site postings in W27.
Africa-region leak-site activity	Nova -> DOSAB (SA industrial, CLAIMED, details limited); NightSpire still holding EC Human Settlements + Ingonyama Trust.

6. Nigeria Communications Week -- Anonymous Nigeria threatens to leak South African stolen data (27 June 2026) — https://www.nigeriacommunicationsweek.com.ng/xenophobic-attacks-anonymous-nigeria-threatens-to-leak-south-african-stolen-data/
7. ITWeb -- Information Regulator serves notices on TransUnion and Experian (26 June 2026) — https://www.itweb.co.za/categories/oJKjlyr7wO7k6amV
8. Malwarebytes ThreatDown -- Prinz Eugen ransomware / ROOTBOY attribution (22 June 2026) — https://www.malwarebytes.com/blog/threat-intelligence/2026/06/prinz-eugen-ransomware-rootboy
9. Data Breaches Digest -- Unnamed SA medical aid breach (25 June 2026) — https://www.dbdigest.com
10. Security Affairs -- CISA warns of active exploitation following FortiBleed leak — https://securityaffairs.com/193902/hacking/cisa-warns-of-active-exploitation-following-fortibleed-leak.html
11. ITWeb -- Malicious actors take down AVBOB's digital platforms — https://www.itweb.co.za/article/malicious-actors-take-down-avbobs-digital-platforms/5yONP7Erd6QMXWrb
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/

4. THREAT ACTORS

4.1 Prinz Eugen / ROOTBOY — SA Solo Operator Publicly Attributed (HIGHEST SA RELEVANCE)

Malwarebytes ThreatDown released full attribution and IOC analysis on 22 June, naming a solo operator (handles ROOTBOY / avtokz / GERMANIA) running the Go-based Prinz Eugen ransomware family. The Standard Bank breach (W18, February 2026) exfiltrated ~1.2 TB / 154M SQL rows; after the bank refused a 1 BTC ransom (~$107,000), the operator escalated to a daily 100,000-row leak, with Liberty Insurance (a Standard Bank subsidiary) also on the leak portal. This is direct SA bank intelligence — defenders must run YARA and IOC sweeps across all RDP-exposed assets, validate the published indicators, and review for the Prinz Eugen Go-based payload across the estate.[8]

4.2 #OpSouthAfrica — Nullsec Nigeria / Anonymous Nigeria (HACKTIVISM)

Two distinct hacktivist crews were active during W27 in retaliation for SA xenophobic violence. Confirmed compromises: the Department of Correctional Services (~11 GB) and Ephraim Mogale Local Municipality. Claimed but unverified: SARS, SITA and ProWellness — SARS denies. The operational window is sustained through the 30 June 2026 anti-immigration deadline and into July. Defender priorities: harden public-facing government web infrastructure, tighten WAF rules, review API exposure, and pre-stage IR retainer escalation — communications and finance ministries are the highest priority.[6]

4.3 The Gentlemen / Storm-2697 — Global Victim Count Growth

The group continues operations after Krebs unmasked admin Alexander Andreevich Yapaev (W26). ESET's "Killing Me Gently" GentleKiller framework analysis remains the reference document (8 BYOVD variants, 400+ targeted processes). Initial-access vectors are unchanged: CVE-2026-50751 (Check Point IKEv1) plus CVE-2026-20131 (Cisco FMC). No new SA-named victim appeared in W27, but SA enterprises should validate EDR-tamper protections and confirm the named initial-access CVEs are remediated.[13]

4.4 ShinyHunters / UNC6240 + C10p — PeopleSoft Data Dumps Continue

Council of Europe, Kodak, MSG and Nottingham data dumps remain published; no new high-profile victims were posted in W27. SA universities (HESA) and provincial governments running PeopleTools 8.61/8.62 remain at risk, with the CISA KEV deadline for CVE-2026-35273 (15 June) now 13 days overdue. Apply the Oracle June CPU and review logs from 27 May onward, treating any previously internet-facing instance as compromised.[14]

4.5 Threat Actor Summary — W27

Actor	Type	Notable W27 Activity	Source
Prinz Eugen / ROOTBOY (avtokz / GERMANIA)	Ransomware / solo operator	Publicly attributed 22 Jun for Standard Bank leak; 1.2 TB / 154M rows; 100,000 rows/day; Liberty also listed	Malwarebytes
Nullsec Nigeria	Hacktivism	#OpSouthAfrica: DCS (~11 GB) + Ephraim Mogale Local Municipality breached	Nigeria Comms Week
Anonymous Nigeria	Hacktivism	#OpSouthAfrica: SARS / SITA / ProWellness claims (unverified; SARS denies); threats of further dumps	Nigeria Comms Week
The Gentlemen / Storm-2697	Ransomware	Operations continue post-Krebs unmasking; GentleKiller framework; CVE-2026-50751 + CVE-2026-20131 access; no new SA victim	Krebs, ESET
ShinyHunters / UNC6240	Criminal / data theft	PeopleSoft CVE-2026-35273 dumps continue (Council of Europe, Kodak, MSG, Nottingham); no new W27 victims	The Register
Cl0p	Ransomware / extortion	Second group exploiting PeopleSoft CVE-2026-35273 (15 Jun KEV now +13 OVERDUE)	CISA KEV
TeamPCP / ResoluteXBF	Supply-chain / SA operator	SANS "When the Security Scanner Became the Weapon" white paper (25-26 Jun); no arrest/indictment in W27	SANS Institute
Nova	Ransomware	DOSAB (SA industrial) -- CLAIMED, details limited	Ransomware.live
NightSpire	Ransomware	Still holding EC Human Settlements + Ingonyama Trust on leak site	Ransomware.live
SantaAd	Initial-access broker	FortiBleed: 73,932-86,644 FortiGates; 110M+ creds; campaign active 28 Jun	Recorded Future
DragonForce	Ransomware	Backdoor.Turn Microsoft Teams C2 analysis (Symantec / Carbon Black)	Symantec
Operation Endgame (LE action)	Law enforcement	StealC + Amadey takedown 24 Jun: 326 servers, 142 domains, EUR41M frozen, 27M creds recovered	Europol / partners

4.6 Other Notable Threat Intelligence Published W27

Operation Endgame — StealC + Amadey takedown (24 June): An international law-enforcement operation seized 326 servers and 142 domains, froze EUR41M and recovered 27 million credentials. StealC and Amadey infostealers are commonly used in SA-targeted phishing as ransomware pre-staging, so SA defenders should refresh credential rotation and infostealer-IOC sweeps.[15]

Barracuda Networks — Africa evolving cyberthreat landscape: A 24% surge in detected activity over March–May 2026, with rising initial-access activity primarily targeting financial services and manufacturing. **Symantec / Carbon Black** published a DragonForce Backdoor.Turn analysis (Microsoft Teams used as a C2 evasion channel) — refresh detection on Microsoft Teams API anomalies.[16]

8. Malwarebytes ThreatDown -- Prinz Eugen ransomware / ROOTBOY attribution (22 June 2026) — https://www.malwarebytes.com/blog/threat-intelligence/2026/06/prinz-eugen-ransomware-rootboy

13. ESET WeLiveSecurity / KrebsOnSecurity -- "Killing Me Gently": GentleKiller framework / The Gentlemen — https://www.welivesecurity.com/

14. 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

15. Europol -- Operation Endgame StealC + Amadey takedown (24 June 2026) — https://www.europol.europa.eu/operation-endgame

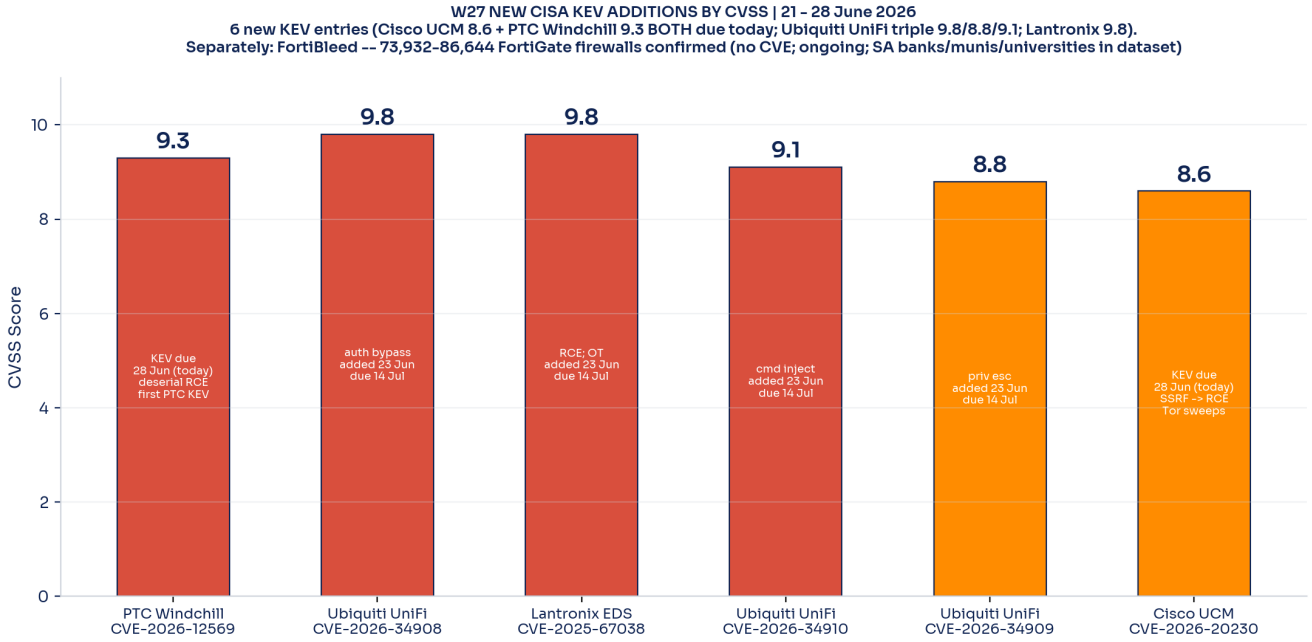
16. Barracuda Networks -- Africa evolving cyberthreat landscape (Mar-May 2026) — https://blog.barracuda.com/

5. CRITICAL VULNERABILITIES & CISA KEV

W27 is defined by two actively exploited "due today" KEV items and a confirmed credential-exposure event. **Cisco UCM CVE-2026-20230** (CVSS 8.6) is an SSRF in WebDialer that escalates to RCE via a crafted

SOAP message to an internal axis2 endpoint, KEV-due **28 June (today)**, with Tor-routed automated webshell sweeps confirmed since 22 June and the full chain public from SSD Secure Disclosure. **PTC Windchill / FlexPLM CVE-2026-12569** (CVSS 9.3) is an insecure Java deserialization in the PLM web service yielding unauth RCE, also KEV-due **28 June (today)** — the first-ever PTC entry in the CISA KEV catalog, with JSP webshells actively deployed. Four further KEV adds landed 23 June (Ubiquiti UniFi triple 9.8/8.8/9.1; Lantronix EDS5000 9.8, due 14 Jul). Separately, **FortiBleed** (no CVE) is now confirmed at 73,932–86,644 FortiGates with named SA banks, municipalities and universities in the dataset, and multiple OVERDUE carryovers (Splunk, Joomla JCE, PeopleSoft, Check Point IKEv1, Ivanti Sentry) remain actively exploited.[517]

W27 KEV / Critical CVE Severity Overview — (6 New KEV Adds 21-28 Jun + FortiBleed + Active Carryovers)



W27 CISA KEV / Critical CVE Tracking (new adds 21-28 June + active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-20230	Cisco UCM (WebDialer / axis2)	8.6	SSRF -> RCE	28 Jun (today)	Tor-routed automated sweeps since 22 Jun; SSD full chain public; treat exposed UCM with WebDialer as compromised; apply Cisco hotfix
CVE-2026-12569	PTC Windchill / FlexPLM	9.3	Deserial RCE	28 Jun (today)	JSP webshells in the wild; FIRST-EVER PTC KEV entry; advisory CS473270; review /Windchill/servlet/
CVE-2026-34908	Ubiquiti UniFi OS	9.8	Auth bypass	14 Jul	Added 23 Jun; SOHO + SMB exposure across SA
CVE-2026-34909	Ubiquiti UniFi OS	8.8	Priv escalation	14 Jul	Added 23 Jun; UniFi triple
CVE-2026-34910	Ubiquiti UniFi OS	9.1	Command injection	14 Jul	Added 23 Jun; UniFi triple
CVE-2025-67038	Lantronix EDS5000	9.8	RCE	14 Jul	Added 23 Jun; industrial serial-to-Ethernet; SA mining/utility OT
CVE-2026-20253	Splunk Enterprise 9.8	n/a	Pre-auth RCE	21 Jun	OVERDUE +7; patch 10.0.7 / 10.2.4 still mandatory
CVE-2026-48907	Joomla JCE 10.0	n/a	Pre-auth RCE	19 Jun	OVERDUE +9; automated PHP webshell mass-exploit
CVE-2026-54420	LiteSpeed cPanel 8.5	n/a	Symlink follow	18 Jun	OVERDUE +10
CVE-2026-28318	SolarWinds Serv-U 7.5	n/a	Unauth DoS	19 Jun	OVERDUE +9 (DoS only)
CVE-2026-35273	Oracle PeopleSoft 9.8	n/a	Unauth RCE	15 Jun	OVERDUE +13; ShinyHunters + C10p exploiting
CVE-2026-10520	Ivanti Sentry 10.0	n/a	Unauth RCE	14 Jun	OVERDUE +14
CVE-2026-50751	Check Point IKEv1 9.3	n/a	Auth bypass	11 Jun	OVERDUE +17; Qilin exploiting
CVE-2026-11645	Chrome V8 (ITW)	n/a	Type confusion	23 Jun	OVERDUE +5
CVE-2026-20245	Cisco SD-WAN 9.2	n/a	0-day RCE	23 Jun	OVERDUE +5 (patch available)
CVE-2026-7473	Arista EOS 5.8	n/a	Tunnel decap	23 Jun	OVERDUE +5 (Arista declined to patch)
CVE-2026-20262	Cisco SD-WAN Manager 7.2	n/a	Path traversal -> root	29 Jun	1 day; patch before deadline

Pattern note: W27 stacks two "due today" KEV items with confirmed in-the-wild exploitation (Cisco UCM CVE-2026-20230 and PTC Windchill CVE-2026-12569 — the latter the first-ever PTC KEV entry) on top of a long tail of OVERDUE carryovers (Splunk +7, Joomla +9, LiteSpeed +10, PeopleSoft +13, Ivanti Sentry +14, Check Point IKEv1 +17). FortiBleed compounds the picture with 73,932-86,644 firewalls confirmed exposed and named SA entities in the dataset. SA estates should treat same-day UCM/Windchill patching, FortiBleed credential rotation, and clearing the OVERDUE backlog as a single high-priority change event, while the Cisco SD-WAN Manager CVE-2026-20262 deadline falls 29 June.

5.1 Cisco UCM CVE-2026-20230 (CVSS 8.6, KEV due TODAY) -- SSRF Escalating to RCE

CVE-2026-20230 (CVSS 8.6) is an SSRF in Cisco Unified Communications Manager's WebDialer that escalates to RCE via a crafted SOAP message to the internal axis2 endpoint. Defused confirmed automated Tor-routed webshell sweeps since 22 June, and the full exploit chain is public from SSD Secure Disclosure. The KEV deadline is today, 28 June. Immediate action: treat any internet-exposed Cisco UCM with WebDialer enabled as compromised until proven clean; review /platform-services/axis2-web/ for unexpected .jsp files; apply Cisco's hotfix; and restrict WebDialer to the internal network only.[17]

5.2 PTC Windchill / FlexPLM CVE-2026-12569 (CVSS 9.3, KEV due TODAY) -- Deserialization RCE

CVE-2026-12569 (CVSS 9.3) is an insecure Java deserialization in the PLM web service yielding unauthenticated RCE. JSP webshells are actively deployed on industrial PLM servers across manufacturing, aerospace and defence, and this is the first-ever PTC entry in the CISA KEV catalog. SA exposure spans aerospace (Denel, Paramount), mining engineering (Sasol, Sibanye) and defence contractors. Action: apply PTC advisory CS473270 and review /Windchill/servlet/ for webshells; the KEV deadline is today, 28 June.[17]

5.3 FortiBleed Status Update + Microsoft KB5094126 + Exchange CVE-2026-45502 + Carryover Deadlines (W27)

FortiBleed (no CVE): final compromise count 73,932–86,644 FortiGate devices across 194 countries; 110M+ credentials harvested over 24 protocols by a custom Golang sniffer; attributed to the Russian-speaking IAB "SantaAd". Required actions: rotate ALL admin and VPN credentials; enforce phishing-resistant MFA; upgrade FortiOS to 7.2.11/7.4.8/7.6.1+; remove management interfaces from the public internet; and confirm domain involvement via the SOCRadar FortiBleed Checker. **Microsoft June Patch Tuesday — KB5094126 still broken:** no out-of-band fix for the system-freeze and BitLocker recovery-loop bugs was released this week; Microsoft is targeting the 14 July Patch Tuesday. Pre-stage BitLocker recovery keys on HP and Dell enterprise laptops before applying the June update. CVE-2026-45657 (wormable kernel TCP/IP RCE 9.8) still has no confirmed ITW. **Exchange CVE-2026-45502:** a new PoC dropped 24 June — apply the full June Exchange Security Update bundle (KB5094139/40/42/44) immediately if not already deployed; it pairs with the W22 carryover CVE-2026-42897 (permanent fix already in KB5094139).[518]

CVE / Item	Status W27
Cisco UCM CVE-2026-20230 (8.6)	KEV due TODAY 28 Jun; SSRF -> RCE; Tor-routed sweeps since 22 Jun; SSD full chain public; restrict WebDialer to internal
PTC Windchill / FlexPLM CVE-2026-12569 (9.3)	KEV due TODAY 28 Jun; deserialization RCE; JSP webshells ITW; FIRST PTC KEV; advisory CS473270
Ubiquiti UniFi OS CVE-2026-34908/09/10 (9.8/8.8/9.1)	Added 23 Jun; due 14 Jul; SOHO + SMB SA exposure; auth bypass / priv esc / command injection
Lantronix EDS5000 CVE-2025-67038 (9.8)	Added 23 Jun; due 14 Jul; industrial serial-to-Ethernet; SA mining/utility OT environments
Oracle PeopleSoft CVE-2026-35273 (9.8)	OVERDUE +13; ShinyHunters + Cl0p exploiting; apply Oracle June CPU + review logs from 27 May
Check Point IKEv1 CVE-2026-50751 (9.3)	OVERDUE +17; Qilin exploiting; disable IKEv1 where not required
Ivanti Sentry CVE-2026-10520 (10.0)	OVERDUE +14; patch + assume-breach hunt
Splunk Enterprise CVE-2026-20253 (9.8)	OVERDUE +7; patch 10.0.7 / 10.2.4 still mandatory
Joomla JCE CVE-2026-48907 (10.0)	OVERDUE +9; automated PHP webshell mass-exploit; check #__wf_profiles + images/media/tmp
Cisco SD-WAN Manager CVE-2026-20262 (7.2)	KEV 29 Jun (1 day); path traversal -> root; patch before deadline

CVE / Item	Status W27
Microsoft KB5094126 (June PT)	Still broken; system-freeze + BitLocker recovery-loop; no OOB fix; Microsoft targeting 14 Jul; pre-stage recovery keys
Exchange CVE-2026-45502	PoC dropped 24 Jun; apply full June Exchange SU bundle KB5094139/40/42/44; pairs with W22 CVE-2026-42897

MICROSOFT KB5094126 STILL BROKEN -- PRE-STAGE BITLOCKER RECOVERY KEYS BEFORE APPLYING JUNE UPDATE

Status: No out-of-band fix for the KB5094126 system-freeze and BitLocker recovery-loop bugs was released this week. Microsoft is targeting the 14 July Patch Tuesday.

Action now: Pre-stage BitLocker recovery keys on HP and Dell enterprise laptops before applying the June update. Confirm key escrow in your identity provider / MDM before any estate-wide rollout.

Exchange: A new PoC for CVE-2026-45502 dropped 24 June — apply the full June Exchange Security Update bundle (KB5094139/40/42/44) immediately if not already deployed. It pairs with the W22 carryover CVE-2026-42897 (permanent fix already in KB5094139).

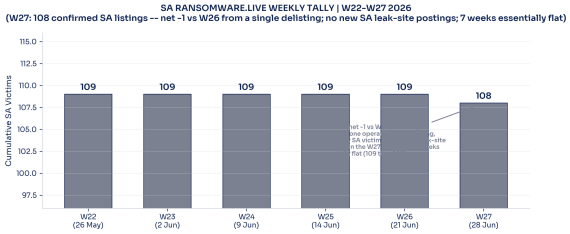
Kernel watch: CVE-2026-45657 (wormable kernel TCP/IP RCE, CVSS 9.8) still has no confirmed in-the-wild exploitation; patch diffs are being actively analysed — prioritise the June rollup where BitLocker key escrow is confirmed.

5. Recorded Future -- Critical FortiBleed campaign — https://www.recordedfuture.com/blog/critical-fortibleed-campaign
17. CISA -- Known Exploited Vulnerabilities Catalog (Cisco UCM CVE-2026-20230; PTC Windchill CVE-2026-12569) — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
18. SOCRadar -- FortiBleed Checker (free tool) — https://socradar.io/free-tools/fortibleed

6. RANSOMWARE LANDSCAPE

SA ransomware.live victim count stands at **108 cumulative** for W27 (verified by live screenshot 28 June), a **net -1 from W26's 109** that reflects a single operator-side delisting (data hygiene) rather than any new SA victim. There were **zero new SA leak-site postings** in the W27 window, leaving the tally **essentially flat across seven consecutive weeks** (109 then 108) — the longest plateau of 2026. Africa-region activity continued elsewhere: Nova listed DOSAB (SA industrial — CLAIMED, details limited), and NightSpire is still holding EC Human Settlements and Ingonyama Trust on its leak site. No fresh Botswana / Senegal / Namibia / Egypt postings appeared beyond W26 continuation.[6]

SA Contextualisation: The essentially-flat count is now a seven-week pattern and should not be read as a reduction in ransomware risk. W27's most consequential developments surface outside the ransomware.live tracker: the publicly attributed Standard Bank / Liberty leak by Prinz Eugen / ROOTBOY (100,000 rows/day), the #OpSouthAfrica hacktivist breaches of two state entities, the IR notices to TransUnion and Experian, and the unnamed ~200,000-member medical aid breach. AVBOB also remains undetermined at 20+ days with no leak-site claim. SA exposure increasingly surfaces through hacktivism, active data-leak portals, credential leaks and regulatory channels rather than the ransomware.live tracker alone.[8]



End W26 baseline	109 confirmed SA listings
New W27 listings (21 - 28 Jun)	0 confirmed on ransomware.live
Delistings (W27)	1 (operator-side data hygiene; NOT a new SA victim)
End W27 count	108 (net -1 vs W26; 7 weeks essentially flat at 109 then 108)
Africa-region W27 listings	Nova -> DOSAB (SA industrial, CLAIMED); NightSpire still holding EC Human Settlements + Ingonyama Trust
Threat-level drivers (non-ransomware.live)	Prinz Eugen / ROOTBOY Standard Bank leak (100,000 rows/day); #OpSouthAfrica hacktivism; IR TransUnion/Experian notices; unnamed medical aid; FortiBleed

6. Ransomware.live -- South Africa country map (W27) — https://www.ransomware.live/map/ZA
8. Malwarebytes ThreatDown -- Prinz Eugen ransomware / ROOTBOY attribution (22 June 2026) — https://www.malwarebytes.com/blog/threat-intelligence/2026/06/prinz-eugen-ransomware-rootboy

7. OSINT EXPOSURE & ATTACK SURFACE

Cisco UCM CVE-2026-20230 -- internet-exposed UC attack surface

Any internet-exposed Cisco Unified Communications Manager with WebDialer enabled is a high-value SSRF-to-RCE target, with Tor-routed automated sweeps confirmed since 22 June and a public SSD exploit chain. Treat exposed UCM as compromised pending investigation; review /platform-services/axis2-web/ for unexpected .jsp files; apply Cisco's hotfix; and restrict WebDialer to the internal network ahead of today's KEV deadline.[17]

PTC Windchill / FlexPLM CVE-2026-12569 -- SA industrial PLM attack surface

The first-ever PTC KEV entry (CVSS 9.3 deserialization RCE) has JSP webshells deployed in the wild on industrial PLM servers. SA exposure spans aerospace (Denel, Paramount), mining engineering (Sasol, Sibanye) and defence contractors. Apply PTC advisory CS473270 and review /Windchill/servlet/ for webshells ahead of today's KEV deadline.[17]

FortiBleed -- confirmed SA FortiGate credential exposure

With 73,932-86,644 FortiGate devices compromised across 194 countries and named SA banks, municipalities, universities and healthcare entities in the dataset, every SA FortiGate deployment is a priority attack-surface item. Confirm domain involvement via the SOCRadar FortiBleed Checker, rotate all VPN and admin credentials, enforce phishing-resistant MFA, upgrade FortiOS to 7.2.11/7.4.8/7.6.1+, and remove management interfaces from the public internet.[518]

Hacktivist attack surface (#OpSouthAfrica) -- .gov.za / .ac.za / SOE web infrastructure

With the Department of Correctional Services and Ephraim Mogale Local Municipality already breached and threats outstanding against SARS, SITA and ProWellness, public-facing government web infrastructure is an active attack surface into the 30 June flashpoint. Harden public-facing web apps, tighten WAF rules, monitor for OWASP Top 10 probing, review API exposure, and pre-stage IR retainer escalation — communications and finance ministries highest priority.[6]

Standard Bank / Liberty + TransUnion / Experian -- financial-sector data exposure

The publicly attributed Prinz Eugen / ROOTBOY leak (1.2 TB / 154M rows, 100,000 rows/day) and the IR 10-day notices to TransUnion SA and Experian SA make financial-sector data provenance an active concern. Standard Bank suppliers should review shared access pathways and rotate integration tokens; TransUnion / Experian customers should request written breach-status confirmation and monitor for out-of-cycle credit reports.[78]

Ubiquiti UniFi + Lantronix EDS5000 -- SA SMB and OT attack surface

The Ubiquiti UniFi OS triple (CVE-2026-34908/09/10, due 14 Jul) exposes many SA small businesses running UniFi to auth bypass, privilege escalation and command injection, while Lantronix EDS5000 (CVE-2025-67038, 9.8) is an industrial serial-to-Ethernet device used in SA mining and utility OT environments. Inventory UniFi and Lantronix assets, restrict management exposure, and schedule patching ahead of the 14 July KEV deadline.[17]

8. REGULATORY & POLICY

SA: National Assembly Confirms IR Appointments (23 June)

The National Assembly formally confirmed Nomagcina Mtshontshi (full-time, five-year term) and Alison Tilley (part-time, five-year term) to the Information Regulator on 23 June, with presidential/ministerial ratification the remaining step. The IR returns to full strength after a months-long capacity gap, just as POPIA and PAIA enforcement activity escalates. SA privacy officers should anticipate sustained or increased regulatory throughput.[19]

SA: IR 10-Day Notice to TransUnion + Experian (26 June)

See Section 3.2 for the underlying facts. Regulatory-side significance: this is the first invocation since 2024 of the IR's POPIA s.59 enforcement-notice power against the credit-bureau sector, with a response deadline of approximately 6 July. Any failure to respond triggers an infringement notice and a potential administrative fine.[7]

SA: Tembisa PAIA Enforcement Window Expired (~26 June)

The 10-day compliance window from the IR's 16 June order against the Gauteng Department of Health expired around 26 June. There is no confirmed compliance or prosecution outcome as of 28 June, so the IR must now decide between commencing criminal prosecution of the Information Officer (up to three years' imprisonment) or accepting late compliance. This is a key watchpoint for W28.

SA: FICA Dual Deadline Cluster (30 June / 1 July)

30 June (Tuesday): the FICA 2026 RCR first batch (CASPs, TCSPs, casinos, credit providers) faces a 17:00 hard close; Capital Flow Management Regulations public comment closes; ICASA satellite spectrum comment closes; and the PAIA Annual Report 2025/26 is due. **1 July (Wednesday):** FICA ss.30/54/55/70 cross-border cash regime goes LIVE — mandatory cross-border cash and bearer-instrument reporting, criminal penalties and forfeiture-on-conviction powers, with NO grace period. Also 1 July, the EU MiCA transitional period ENDS, so SA CASPs serving EU clients must be fully MiCA-compliant. First-batch institutions should confirm RCR submission now and run a 1 July operational-readiness check across cashiers, treasury and payments teams.[20]

Other W27 Regulatory & Policy Developments

- **EU AI Act Digital Omnibus Council adoption expected 29 June:** following the EP vote on 16 June (423/57/174), Council formal adoption is expected tomorrow, 29 June, with OJEU publication anticipated 18–25 July. Once published, Annex III high-risk obligations shift from 2 August 2026 to 2 December 2027, Annex I embedded systems to 2 August 2028, and watermarking (Art. 50(2)) plus the new nudifier/CSAM ban apply from 2 December 2026. Until publication, the original 2 August 2026 deadline remains live law, and Article 50(1)/(3)/(4) general transparency obligations remain live 2 August 2026 regardless.
- **FATF June 2026 plenary (17–19 June):** Namibia and Algeria were removed from the grey list; Bosnia and Herzegovina and Iraq were added (grey list now 22 jurisdictions); Recommendation 6 was amended for humanitarian exemptions; UK Presidency priorities were set; and the 7th VASP targeted update was approved. SA relevance: reduced friction in SA-Namibia and SA-Algeria correspondent-banking and trade-finance corridors.
- **UK DUAA s.164A early enforcement (carryover):** live since 19 June with no grace period; no major enforcement actions confirmed in W27. UK ICO Commissioner John Edwards resigned (19 Jun) and an interim appointment is still pending. SA businesses with UK customers, employees or users must confirm the DUAA s.164A complaints process is operational.
- **SA SARB & Treasury upcoming:** 17 July — SARB NPSD cross-border payment facilitators directive comment close; 31 July — FICA 2026 RCR second batch (legal practitioners, estate agents, HVGDs).
- **SA DCDT AI Policy (carryover):** retracted 12 Jun (GG 3880); revised draft to Cabinet November 2026, public comment January 2027 — the policy vacuum continues.
- **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.

Compliance Deadlines — W27 Forward View

Date	Item	Owner
28 Jun 2026	CISA KEV: Cisco UCM CVE-2026-20230 + PTC Windchill CVE-2026-12569 deadlines (TODAY)	IT
29 Jun 2026	CISA KEV: Cisco SD-WAN Manager CVE-2026-20262 deadline	IT
29 Jun 2026	EU AI Act Digital Omnibus Council formal adoption expected	Compliance
30 Jun 2026	FICA 2026 RCR first batch (CASPs, TCSPs, casinos, credit providers) -- 17:00 hard close	Compliance
30 Jun 2026	Capital Flow Management Regulations comment close; ICASA satellite spectrum comment; PAIA Annual Report 2025/26	Finance/Legal
1 Jul 2026	FICA ss.30/54/55/70 cross-border cash regime LIVE (no grace period); EU MiCA transitional period ENDS	Finance/Legal
~6 Jul 2026	TransUnion SA + Experian SA response to IR 10-day notices due	Legal/Compliance
14 Jul 2026	CISA KEV: Ubiquiti UniFi x3 + Lantronix EDS5000 deadlines	IT
14 Jul 2026	Microsoft targeting KB5094126 fix at July Patch Tuesday	IT
17 Jul 2026	SARB NPSD cross-border payment facilitators directive comment close	Finance/Legal
31 Jul 2026	FICA 2026 RCR second batch (legal practitioners, estate agents, HVGDs)	Compliance
2 Aug 2026	EU AI Act Art. 50 transparency (live until Omnibus enters Official Journal)	Compliance
9 Aug 2026	US CISA BOD 26-04 vulnerability-management policy deadline (benchmark)	IT/Compliance

19. Parliament of South Africa -- National Assembly approves reports filling vacancies (23 June 2026) — https://www.parliament.gov.za/press-releases/media-statement-national-assembly-approves-reports-filling-vacancies-democratic-institutions-and-government-entities

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

9. WEEKLY THREAT HUNT & IOCs

Eight hunt missions are active for W27. Two P1 missions address the two CISA KEV entries with deadlines today: Cisco UCM CVE-2026-20230 (SSRF chained to RCE) and PTC Windchill / FlexPLM CVE-2026-12569 (deserialization RCE, the first-ever PTC KEV entry). Two further P1 missions address the #OpSouthAfrica hacktivist campaign building into the 30 June flashpoint and the publicly attributed Prinz Eugen / ROOTBOY Standard Bank data leak. Two P2 missions address the FortiBleed FortiGate credential exposure (final triage) and the Oracle PeopleSoft mass-compromise (now OVERDUE +13). Two P3 missions address the unattributed SA medical-aid breach (intelligence gap) and the AVBOB undetermined-incident impact assessment.

TH-2026-W27-01 — Cisco UCM CVE-2026-20230 (KEV due TODAY) -- SSRF-to-RCE Webshell Hunt

P1 — CRITICAL: CVSS 8.6 SSRF-to-RCE; KEV due TODAY; Tor sweeps since 22 Jun; full chain public

Hypothesis: A WebDialer SSRF in Cisco Unified Communications Manager escalates to RCE via a crafted SOAP message to the internal axis2 endpoint. Automated Tor-routed webshell sweeps have been confirmed since 22 June and the full exploit chain is public from SSD Secure Disclosure. Any internet-exposed UCM with WebDialer enabled should be treated as compromised until proven clean.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1090.003 (Multi-hop Proxy / Tor), T1505.003 (Web Shell), T1059 (Command and Scripting Interpreter).

IOCs: Unexpected .jsp files under /platform-services/axis2-web/; crafted SOAP requests to the internal axis2 endpoint; WebDialer SSRF callbacks to internal hosts; inbound exploitation from Tor exit nodes since 22 June; new processes spawned by the UCM service account.

Data Sources: UCM web/access logs, axis2 servlet logs, host EDR process-creation telemetry, perimeter netflow for the UCM management interface, Tor exit-node threat feeds.

Detection Guidance: Treat any internet-exposed UCM with WebDialer enabled as compromised pending investigation. Review /platform-services/axis2-web/ for unexpected .jsp files. Apply Cisco's hotfix and restrict WebDialer to the internal network only. Hunt for Tor-sourced exploitation attempts from 22 June onward.

TH-2026-W27-02 — PTC Windchill / FlexPLM CVE-2026-12569 (KEV due TODAY) -- Deserialization RCE Hunt

P1 — CRITICAL: CVSS 9.3 unauth RCE; KEV due TODAY; first-ever PTC KEV; JSP webshells ITW

Hypothesis: Insecure Java deserialization in the PTC PLM web service allows unauthenticated RCE, and JSP webshells are being actively deployed on industrial PLM servers. This is the first-ever PTC entry in the CISA KEV catalog. SA aerospace (Denel, Paramount), mining engineering (Sasol, Sibanye), and defence contractors are exposed.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1059 (Command and Scripting Interpreter), T1505.003 (Web Shell), T1213 (Data from Information Repositories).

IOCs: JSP webshells under /Windchill/servlet/; anomalous deserialization payloads to the PLM web service; unexpected child processes spawned by the Windchill service; outbound connections from PLM tiers to unfamiliar IPs; bulk export of design/engineering data.

Data Sources: Windchill / FlexPLM web-server logs, application-server logs, file-integrity monitoring on the web root, host EDR telemetry, egress netflow from PLM tiers.

Detection Guidance: Apply PTC advisory CS473270 immediately. Review /Windchill/servlet/ for JSP webshells. Restrict and segment internet exposure of PLM servers. Prioritise SA aerospace, mining-engineering, and defence-contractor estates given the targeting profile.

TH-2026-W27-03 — #OpSouthAfrica Hacktivism -- Public-Facing Government Infrastructure Hunt

P1 — CRITICAL: first sustained anti-SA hacktivist campaign in years; 30 Jun flashpoint; 2 state entities confirmed

Hypothesis: Nullsec Nigeria and Anonymous Nigeria are running a sustained #OpSouthAfrica campaign in retaliation for SA xenophobic violence, with a flashpoint through the 30 June anti-immigration deadline and into July. Confirmed compromises of DCS (~11 GB) and Ephraim Mogale Local Municipality; SARS, SITA, and ProWellness are claimed but unverified (SARS denies). Any .gov.za, .ac.za, or SOE web estate is a potential target.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1595 (Active Scanning), T1498 (Network Denial of Service), T1567 (Exfiltration Over Web Service).

IOCs: OWASP Top 10 probing of public-facing government/SOE web apps; anomalous API enumeration; defacement attempts; bulk data egress; activity spikes coinciding with the 30 June deadline; references to #OpSouthAfrica / Nullsec Nigeria / Anonymous Nigeria on hacktivist channels.

Data Sources: WAF logs, web-application access logs, API gateway logs, perimeter netflow, external attack-surface monitoring, leak-site and hacktivist-channel monitoring.

Detection Guidance: For any .gov.za, .ac.za, or SOE infrastructure: brief the SOC, tighten the WAF, monitor for OWASP Top 10 probing, review API exposure, and validate IR retainer contacts. Communications and finance ministries are the highest priority. Pre-stage IR retainer escalation through the 30 June flashpoint.

TH-2026-W27-04 — Prinz Eugen / ROOTBOY -- Standard Bank Leak & RDP Credential Hunt

P1 — CRITICAL: SA bank active leak; publicly attributed; 100,000 rows/day; direct SA targeting

Hypothesis: SA solo operator Prinz Eugen / ROOTBOY (handles avtokz / GERMANIA), running a Go-based ransomware family, has been publicly attributed by Malwarebytes ThreatDown. After a refused 1 BTC ransom, the operator is publishing Standard Bank data (~1.2 TB / 154M SQL rows) at 100,000 rows/day; Liberty Insurance is also on the leak portal. SA banks should assume direct targeting and sweep RDP-exposed assets.

MITRE ATT&CK: T1133 (External Remote Services / RDP), T1078 (Valid Accounts), T1486 (Data Encrypted for Impact), T1567 (Exfiltration Over Web Service), T1657 (Financial Theft).

IOCs: Go-based Prinz Eugen ransomware artefacts; anomalous RDP authentication from unfamiliar geolocations/ASNs; Standard Bank / Liberty data appearing on the leak portal; references to ROOTBOY / avtokz / GERMANIA; bulk SQL-row exfiltration patterns.

Data Sources: RDP/remote-access authentication logs, host EDR telemetry, leak-portal monitoring, database audit logs, egress netflow, Malwarebytes ThreatDown IOC feed.

Detection Guidance: Run a YARA + IOC sweep across all RDP-exposed assets using the Malwarebytes ThreatDown IOC set. Disable or MFA-gate internet-facing RDP. Standard Bank suppliers and partners should review shared access pathways and rotate any integration tokens. Monitor the leak portal for the daily 100,000-row escalation.

TH-2026-W27-05 — FortiBleed FortiGate Credential Exposure -- Final Rotate-and-Hunt

P2 — HIGH: 73,932-86,644 firewalls; 110M+ creds; campaign still active; confirmed SA exposure

Hypothesis: Recorded Future's 24 June final analysis confirms 73,932-86,644 FortiGate devices compromised across 194 countries, with 110M+ credentials harvested via a custom Golang sniffer over 24 protocols, still active under Russian-speaking IAB "SantaAd." SA banks, municipalities, universities, and healthcare entities are confirmed in the dataset; CRAN Namibia warned 13 regional organisations.

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; the organisation domain appearing in the SOCRadar FortiBleed Checker dataset.

Data Sources: FortiGate admin/VPN authentication logs, FortiOS event logs, perimeter netflow, SOCRadar FortiBleed Checker, MFA/identity-provider logs.

Detection Guidance: Last call: check the organisation domain at the SOCRadar FortiBleed Checker. Force-rotate ALL FortiGate VPN and admin credentials. Enforce 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.

TH-2026-W27-06 — Oracle PeopleSoft CVE-2026-35273 (OVERDUE +13) -- ShinyHunters + C1Op Backdoor Hunt

P2 — HIGH: OVERDUE +13; two ransomware groups; backdoors survive patching

Hypothesis: Both ShinyHunters/UNC6240 and C1Op continue to exploit CVE-2026-35273, and UNC6240 backdoors survive patching. The KEV deadline (15 June) is now 13 days overdue. Any SA PeopleSoft instance (PeopleTools 8.61/8.62) that was internet-facing before patching should be assumed compromised regardless of patch status. SA universities (HESA) and provincial governments remain the priority estates.

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-W27-07 — Unattributed SA Medical-Aid Breach (~200,000 members) -- Intelligence-Gap Hunt

P3 — MONITORING: ~200,000 members; unattributed; primary intelligence gap; special-category data

Hypothesis: Data Breaches Digest reported (25 June) an unnamed SA medical aid with approximately 200,000 affected members. No attribution, vector, or named entity is confirmed, making this a primary intelligence gap. SA medical schemes and their administrators should proactively assess for equivalent special-category data exposure.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1078 (Valid Accounts), T1567 (Exfiltration Over Web Service); vector undetermined.

IOCs: Special-category (medical) member data appearing on breach/leak sites; anomalous bulk member-record exports; unauthenticated access to member portals; absent authorisation checks on document/member endpoints.

Data Sources: Member-portal access logs, database audit logs, external attack-surface scans, leak-site and breach-aggregator monitoring (Data Breaches Digest), POPIA processing records.

Detection Guidance: SA medical schemes and administrators: proactively review member portals and claims platforms for unauthenticated access and bulk-export anomalies. Confirm POPIA s.22 breach-notification readiness for special-category data. Monitor breach aggregators for any named attribution and assess whether your scheme is the unnamed entity.

TH-2026-W27-08 — AVBOB Undetermined Incident -- Supplier/Partner Impact Assessment

P3 — MONITORING: undetermined 4+ weeks; no claim/attribution; sector supply-chain risk

Hypothesis: AVBOB remains in partial-manual operation more than four weeks after the original attack, with no leak-site claim or attribution as of 28 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 — W27

Indicator	Type	Attribution	Hunt ID
CVE-2026-20230 (Cisco UCM /platform-services/axis2-web/ .jsp)	CVE	SSRF-to-RCE CVSS 8.6; KEV due 28 Jun; Tor sweeps since 22 Jun; SSD chain public	TH-2026-W27-01
CVE-2026-12569 (PTC Windchill /Windchill/servlet/ JSP webshells)	CVE	Deserialization RCE CVSS 9.3; KEV due 28 Jun; first-ever PTC KEV; advisory CS473270	TH-2026-W27-02
#OpSouthAfrica probing of .gov.za / .ac.za / SOE web apps	Hacktivism	Nullsec Nigeria + Anonymous Nigeria; DCS (~11 GB) + Ephraim Mogale confirmed; 30 Jun flashpoint	TH-2026-W27-03
Go-based Prinz Eugen ransomware; anomalous RDP auth	Malware/Cred	ROOTBOY / avtokz / GERMANIA; Standard Bank 1.2 TB / 154M rows; 100,000 rows/day; Liberty also listed	TH-2026-W27-04
FortiGate plaintext creds (SOCRadar FortiBleed Checker)	Cred leak	FortiBleed; 73,932-86,644 firewalls; IAB "SantaAd"; confirmed SA exposure	TH-2026-W27-05
CVE-2026-35273 (PeopleSoft web shells / backdoors)	CVE	ShinyHunters/UNC6240 + Cl0p; OVERDUE +13; backdoors survive patching	TH-2026-W27-06
Unattributed SA medical-aid member data (~200,000 members)	Data breach	Unnamed SA medical aid (Data Breaches Digest, 25 Jun); vector undetermined; special-category data	TH-2026-W27-07
AVBOB shared-platform / broker-portal anomalies	Incident	AVBOB undetermined 4+ weeks; no leak-site claim/attribution; supply-chain risk	TH-2026-W27-08
StealC / Amadey infostealer IOCs (Operation Endgame, 24 Jun)	Malware	LE takedown: 326 servers, 142 domains, 27M creds recovered; refresh SA phishing-pre-stage sweeps	N/A (advisory)
CVE-2026-45502 (Exchange) PoC + CVE-2026-20262 (Cisco SD-WAN Mgr)	CVE	Exchange PoC dropped 24 Jun (apply KB5094139/40/42/44); SD-WAN Mgr KEV 29 Jun	N/A (carryover)

17. CISA -- Known Exploited Vulnerabilities Catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
18. SOCRadar -- FortiBleed Checker (free tool) — https://socradar.io/free-tools/fortibleed
15. Europol -- Operation Endgame (StealC + Amadey takedown, 24 June 2026) — https://www.europol.europa.eu/operation-endgame

10. STRATEGIC RECOMMENDATIONS

Immediate (Next 24-48 Hours — Priority P1)

- **1. Cisco UCM CVE-2026-20230 (KEV due TODAY):** If you run internet-exposed Unified Communications Manager with WebDialer, treat it as compromised pending investigation. Apply Cisco's hotfix, restrict WebDialer to the internal network only, and review /platform-services/axis2-web/ for unexpected .jsp files. Tor-routed automated sweeps have been active since 22 June and the full SSD exploit chain is public.[17]
- **2. PTC Windchill / FlexPLM CVE-2026-12569 (KEV due TODAY):** Apply PTC advisory CS473270 and review /Windchill/servlet/ for JSP webshells. This is the first-ever PTC KEV entry, with deserialization RCE actively exploited against industrial PLM servers — SA aerospace, mining-engineering, and defence-contractor estates are the priority.[17]
- **3. Hacktivist hardening (next 72 hours through 30 June):** Anyone with .gov.za, .ac.za, or SOE infrastructure must brief the SOC, tighten the WAF, monitor for OWASP Top 10 probing, review API exposure, and validate IR retainer contacts. Communications and finance ministries are the highest priority through the 30 June #OpSouthAfrica flashpoint.
- **4. TransUnion / Experian customers:** Request written breach-status confirmation from your credit-bureau account contact and monitor for any out-of-cycle credit reports, given the IR's 26 June 10-day notices.
- **5. Standard Bank suppliers / partners:** Review shared access pathways; if you hold Standard Bank API tokens or integration accounts, rotate them now. Run a YARA + IOC sweep across all RDP-exposed assets using the Malwarebytes ThreatDown Prinz Eugen / ROOTBOY IOC set.[3]

This Week

- **FortiBleed final triage:** Last call to rotate ALL FortiGate VPN and admin credentials; upgrade to FortiOS 7.2.11/7.4.8/7.6.1+; remove management interfaces from the public internet; and check your domain at the SOCRadar FortiBleed Checker. The campaign remains active under IAB "SantaAd" with confirmed SA exposure.[18]
- **Microsoft June Patch Tuesday pre-staging:** Pre-stage BitLocker recovery keys on HP and Dell enterprise laptops before applying KB5094126. No out-of-band fix for the system-freeze and BitLocker recovery-loop bugs is expected before the 14 July Patch Tuesday.
- **Exchange CVE-2026-45502:** Apply the full June Exchange Security Update bundle (KB5094139/40/42/44) immediately if not already deployed; a new PoC dropped on 24 June and it pairs with the W22 carryover CVE-2026-42897.
- **Cisco SD-WAN Manager CVE-2026-20262:** Patch before the 29 June KEV deadline (Catalyst SD-WAN Manager).

Strategic (Next Quarter)

- **FICA 30 June filing crunch:** First-batch institutions (CASPs, TCSPs, casinos, credit providers) must file the 2026 RCR by 17:00 on Tuesday 30 June — confirm submission status now.[20]
- **FICA 1 July cross-border cash regime:** Run an operational-readiness check across cashiers, treasury, and payments teams; update SAR templates; and review correspondent-banking documentation. The ss.30/54/55/70 regime goes live with criminal penalties and forfeiture-on-conviction powers and NO grace period.
- **EU MiCA 1 July:** SA CASPs serving EU clients must be fully MiCA-compliant from tomorrow as the transitional period ends.
- **UK customer/employee touchpoints:** Confirm the DUAA s.164A complaints process is operational and document the acknowledgement and investigation workflow (live since 19 June, no grace period; UK ICO leadership vacuum continues).

- **POPIA internal-email controls:** Given the Werksmans/IR clarification, audit shared-mailbox handling, group sends, and attachment policies, and treat misdirected internal emails containing personal information as notifiable security compromises.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH — 7th CONSECUTIVE WEEK

The South African cyber threat level remains **HIGH** for a seventh consecutive week (21–28 June 2026). The level is held — not raised — because the elevated drivers are sustained rather than newly escalating, but the convergence of a live hacktivist campaign, an active SA-bank data leak, a fresh regulatory-enforcement escalation, and two same-day KEV deadlines keeps the assessment firmly elevated.

Rationale

- **First sustained hacktivist campaign against SA in years:** Nullsec Nigeria and Anonymous Nigeria #OpSouthAfrica are running into the 30 June flashpoint, with confirmed compromises of two state entities (DCS, Ephraim Mogale Local Municipality) and threats against five more (SARS, SITA, ProWellness among them).
- **First post-2024 IR enforcement escalation against credit bureaus:** The Information Regulator served 10-day POPIA s.59 notices on TransUnion SA and Experian SA on 26 June.
- **Standard Bank active data-leak now publicly attributed:** Prinz Eugen / ROOTBOY is publishing approximately 100,000 rows per day from the ~1.2 TB / 154M-row dataset.
- **Unattributed SA medical-aid breach (~200,000 members):** reported 25 June — a primary intelligence gap with no confirmed entity, vector, or attribution.
- **Two more "due today" KEV entries:** Cisco UCM CVE-2026-20230 and PTC Windchill CVE-2026-12569, both with in-the-wild exploitation confirmed.
- **AVBOB still undetermined at 4+ weeks:** partial-manual operation continues with no leak-site claim or attribution.

Next-Week Watch (W28)

- Hacktivist activity escalation through 30 June and into July.
- TransUnion / Experian formal IR response (~6 July).
- Tembisa prosecution decision (criminal prosecution of the Information Officer vs. accepting late compliance).
- FICA 2026 RCR first-batch filing-rate final tally (30 June 17:00 close).
- FICA cross-border cash regime first-week operational issues (live 1 July, no grace period).
- EU AI Act Digital Omnibus Council adoption result (expected 29 June).
- Council of Europe / Madison Square Garden PeopleSoft fallout if SA universities or provincial governments appear next.
- KB5094126 fix availability (likely deferred to the 14 July Patch Tuesday).

12. OSINT SOURCES CONSULTED

The following open-source intelligence sources were consulted in the preparation of this report. All sources are TLP:WHITE and publicly accessible. Numbers 1–20 correspond to the inline footnote citations

used throughout this report.

1. Nigeria Communications Week -- Xenophobic attacks: Anonymous Nigeria threatens to leak South African stolen data (27 June 2026) — https://www.nigeriacommunicationsweek.com.ng/xenophobic-attacks-anonymous-nigeria-threatens-to-leak-south-african-stolen-data/

2. ITWeb -- Information Regulator category coverage (TransUnion / Experian notices, 26 June 2026) — https://www.itweb.co.za/categories/oJKjlyr7wO7k6amV

3. Malwarebytes ThreatDown -- Prinz Eugen ransomware / ROOTBOY attribution and IOC analysis (22 June 2026) — https://www.malwarebytes.com/blog/threat-intelligence/2026/06/prinz-eugen-ransomware-rootboy

4. Data Breaches Digest -- Unnamed SA medical aid breach (~200,000 members, 25 June 2026) — https://www.dbdigest.com

5. Recorded Future -- Critical FortiBleed campaign analysis (24 June 2026) — https://www.recordedfuture.com/blog/critical-fortibleed-campaign

6. Ransomware.live -- South Africa country map / leak-site tracking (W27, 108 cumulative) — https://www.ransomware.live/map/ZA

7. ITWeb -- Information Regulator serves notices on TransUnion and Experian (26 June 2026) — https://www.itweb.co.za/categories/oJKjlyr7wO7k6amV

8. Malwarebytes ThreatDown -- Prinz Eugen / ROOTBOY threat-intelligence write-up (22 June 2026) — https://www.malwarebytes.com/blog/threat-intelligence/2026/06/prinz-eugen-ransomware-rootboy

9. Data Breaches Digest -- breach aggregation and SA medical-aid disclosure (25 June 2026) — https://www.dbdigest.com

10. Security Affairs -- CISA warns of active exploitation following FortiBleed leak — https://securityaffairs.com/193902/hacking/cisa-warns-of-active-exploitation-following-fortibleed-leak.html

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

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. ESET WeLiveSecurity -- "Killing Me Gently": GentleKiller / The Gentlemen analysis — https://www.welivesecurity.com/

14. 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

15. Europol -- Operation Endgame (StealC + Amadey takedown, 24 June 2026) — https://www.europol.europa.eu/operation-endgame

16. Barracuda Networks -- Africa evolving cyberthreat landscape (24% surge Mar-May 2026) — https://blog.barracuda.com/

17. CISA -- Known Exploited Vulnerabilities Catalog (Cisco UCM CVE-2026-20230; PTC Windchill CVE-2026-12569) — https://www.cisa.gov/known-exploited-vulnerabilities-catalog

18. SOCRadar -- FortiBleed Checker (free tool) — https://socradar.io/free-tools/fortibleed

19. Parliament of South Africa -- National Assembly approves reports filling vacancies (23 June 2026) — https://www.parliament.gov.za/press-releases/media-statement-national-assembly-approves-reports-filling-vacancies-democratic-institutions-and-government-entities

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

21. SANS Institute -- "When the Security Scanner Became the Weapon" (TeamPCP / ResoluteXBF white paper, 25-26 June 2026) — https://www.sans.org/white-papers/

22. Symantec / Carbon Black Threat Hunter Team -- DragonForce Backdoor.Turn Microsoft Teams C2 analysis — https://www.security.com/threat-intelligence

23. Standard Bank Group -- Service status page (Standard Bank / Liberty leak monitoring) — https://statuspage.standardbank.co.za

24. PTC -- Security Advisory CS473270 (Windchill / FlexPLM CVE-2026-12569) — https://www.ptc.com/en/support/security

25. Cisco -- Security Advisories (Unified Communications Manager CVE-2026-20230; Catalyst SD-WAN Manager CVE-2026-20262) — https://sec.cloudapps.cisco.com/security/center/publicationListing.x

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-W27 | Published Monday 29 June 2026