



SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 22 | 17 May – 24 May 2026

THREAT LEVEL: HIGH

SA ISP/hosting ransom-DDoS wave (BlackMatter, attribution disputed) 18-20 May: 1-Grid, Xneelo, Network Platforms, Domains.co.za, Seacom -- peaks 676 Gbit/s / >1 Tbps in wider campaign. Microsoft Defender RedSun + UnDefend OOB patched 21 May after 7+ weeks. New CVSS 10.0 cPanel/LiteSpeed CVE-2026-48172. Cisco SD-WAN KEV deadline 17 May (NOW PAST). Exchange OWA KEV due 29 May (NO permanent patch). 11 CISA KEV additions including 5 legacy 2008-2010 CVEs re-weaponised. SA newly in Lazarus/CYFIRMA target geography.

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W22 | Classification: TLP:WHITE

© 2026 Digital Progression | dpcyber.co.za

TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard
- 2. Threat Landscape Heatmap
- 3. SA Cyber Incidents & Breaches
- 4. Global Incidents with SA Relevance
- 5. Threat Actors
- 6. Critical Vulnerabilities & CISA KEV
- 7. Ransomware Landscape
- 8. OSINT Exposure & Attack Surface
- 9. Regulatory & Compliance
- 10. Weekly Threat Hunt & IOCs
- 11. Recommendations
- 12. OSINT Sources Consulted

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH (unchanged from W21) — Week 22 (17–24 May 2026)

Story 1 — SA ISP/Hosting Ransom-DDoS (RDoS) Wave: A coordinated carpet-bombing RDoS campaign struck five South African internet infrastructure providers across 18–20 May: 1-Grid (>100 Gbit/s; 32,000 customers), Xneelo (KonsoleH disrupted), Network Platforms (>300 Gbit/s; ransom refused), Domains.co.za (impacted), and Seacom (downstream disruption). Extortion emails signed "BlackMatter" demanded ~R16,000 (2.5 XMR). Security experts dispute attribution: the ransom is inconsistent with BlackMatter's historical US\$80k–\$15M range; Dr Manny Corregedor (Telspace Africa) raised the nation-state reconnaissance theory. SSS neutralised a concurrent data-exfil attempt in 13 minutes and reported peaks exceeding 1 Tbps in the wider campaign.¹

Story 2 — Defender OOB Patch 21 May + New CVSS 10.0 cPanel Vuln: Microsoft released out-of-band patches on 21 May for **CVE-2026-41091** (Defender Engine RedSun, CVSS 7.8, priv-esc to SYSTEM) and **CVE-2026-45498** (Defender Platform UnDefend, CVSS 4.0, disables AV) after 7+ weeks unaddressed. Huntress confirmed live intrusions via FortiGate VPN entry then UnDefend/RedSun chain. Separately, new **CVE-2026-48172** (LiteSpeed cPanel plugin, CVSS 10.0) is in-the-wild and directly compounds the SA hosting wave. Patch Defender Engine 1.1.26040.8 and Platform 4.18.26040.7; update LiteSpeed cPanel plugin to 2.4.7.²

Story 3 — KEV Deadlines: Cisco SD-WAN PAST + Exchange OWA Approaching: The Cisco Catalyst SD-WAN **CVE-2026-20182** (CVSS 10.0) KEV deadline of **17 May has now passed**; UAT-8616 (Talos attribution) is actively exploiting unpatched controllers via SSH key injection and NETCONF modification. Exchange OWA **CVE-2026-42897** (CVSS 8.1) **still has no permanent patch** as of 24 May; EEMS Mitigation ID M2 is the only protection (KEV due 29 May). Additionally, CISA added 11 CVEs this week including 5 legacy 2008–2010 CVEs re-weaponised in 2026 campaigns.³

KPI Dashboard

Metric	Current (W22)	Prior (W21)	Change	Direction
SA threat level	HIGH	HIGH	Unchanged	FLAT
SA ransomware.live victims (total)	111	111	0 new W22	FLAT
New SA RW listings this week	0 confirmed	3 (W21)	-3	FLAT
SA ISPs/hosts hit by DDoS extortion	5+ (1-Grid, Xneelo, NP, Domains.co.za, Seacom)	N/A	NEW W22	UP
CISA KEV additions (W22)	11 (incl. 5 legacy 2008–2010)	3 (W21)	+8	UP
Microsoft OOB patches W22	1 (Defender RedSun/UnDefend)	0 (W21)	NEW	UP
Active hacktivist campaigns vs SA	1 (#OpSouthAfrica)	0	NEW W22	UP
Exchange OWA permanent patch	NO permanent patch (EEMS M2 only)	NO (W21)	UNCHANGED	FLAT
Cisco SD-WAN KEV deadline	17 May (NOW PAST)	Upcoming	DEADLINE PASSED	UP
Active KEV deadlines remaining	3 (Drupal 27 May, OWA 29 May, Ivanti 27 May)	N/A	URGENT	UP
POPIA breach notifications YTD	+40% YoY (IR APP figure)	Baseline	Accelerating	UP
SA in APT target geography (CYFIRMA)	YES -- 3 SA finance victims in 90 days	Not listed	NEW W22	UP

W22 KEY FRAMING: W22 was dominated by infrastructure-targeting activity, not ransomware encryption. The DDoS wave demonstrated operational capability to disrupt SA internet at >1 Tbps. Five providers declined to pay; the extortion failed commercially but demonstrated infrastructure dependency. The FLAT ransomware count (111) should not be read as reduced threat -- the threat actor mix is shifting toward DDoS extortion, hacktivism, and espionage-adjacent reconnaissance. CYFIRMA's addition of SA to the APT campaign target geography is a significant new signal.

TOP 3 ACTIONS THIS WEEK

1. DDoS READINESS CHECK: Validate scrubbing/CDN protection for all internet-facing infrastructure. Do not engage with extortion emails signed "BlackMatter" or any variant. Confirm Anycast routing, upstream cooperative mitigation (contact upstream ISP), and outage-comms templates. The campaign demonstrated >1 Tbps capability. SSS neutralised a concurrent attempt in 13 minutes -- review your IR timing. Ransom of R16,000 (2.5 XMR) must be refused.

2. PATCH DEFENDER OOB + LITESPEED CPANEL + VERIFY EXCHANGE OWA EEMS M2: Confirm Defender Engine 1.1.26040.8 and Platform 4.18.26040.7 (released 21 May, auto via Windows Update/WSUS) are deployed on every endpoint. Update LiteSpeed cPanel plugin to 2.4.7 (CVE-2026-48172, CVSS 10.0, ITW). Hunt cPanel IOCs: grep cpanel_jsonapi_func=redisAble in /var/cpanel/logs/; check for .sorry files, hasroot=1 sessions, root password 123Qwe123C. Verify Exchange Health Checker confirms Mitigation ID M2 on all Exchange servers (KEV due 29 May, no permanent patch).

3. HUNT SIDEWINDER + SHINYHUNTERS DOWNSTREAM + BLOCK IOCS: Block filenest[.]live, snagdrive[.]com, download-doc[.]net, adobeglobal[.]com, updates-installer[.]store at DNS/proxy (SideWinder delivery domains). Patch legacy Office CVE-2017-11882 / 2018-0802 / 0199 immediately. For Canvas-affected SA tertiaries (Wits, Stadio, Milpark, Invictus, SPARK): force credential resets and brief financial-aid / admin staff on spearphishing templates using stolen institutional data. Monitor for ClickOnce installs with zeroed publisher cert serial.

1. TechCentral -- Extortion fears as DDoS attacks hit SA internet infrastructure (19 May 2026) --

<https://techcentral.co.za/extortion-fears-as-ddos-attacks-hit-sa-internet-infrastructure/281499/>

2. BleepingComputer -- Microsoft warns of new Defender zero-days exploited in attacks (21 May 2026) --

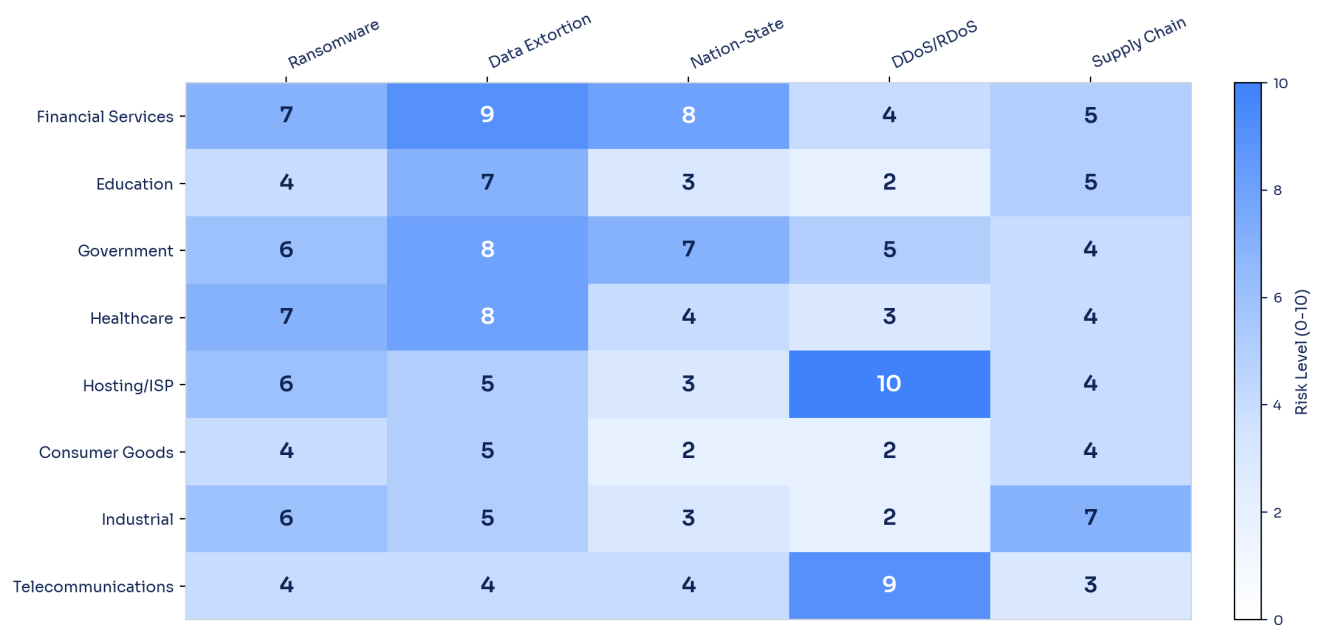
<https://www.bleepingcomputer.com/news/security/microsoft-warns-of-new-defender-zero-days-exploited-in-attacks/>

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

2. THREAT LANDSCAPE HEATMAP

The heatmap maps eight key South African sectors against five threat categories, rated 0–10 based on confirmed incidents, active threat actor campaigns, and vulnerability exposure during Week 22 (17–24 May 2026). **Hosting/ISP** spikes to 10 on DDoS/RDoS driven by the BlackMatter carpet-bombing wave. **Telecommunications** enters at 9 on DDoS from Seacom downstream impact and infrastructure dependency mapping. **Financial Services** rises to 8 on Nation-State following CYFIRMA's confirmation that SA newly entered APT campaign target geography (3 SA finance victims in 90 days). **Government** rises on Data Extortion and Nation-State following #OpSouthAfrica hacktivist wave.

SA THREAT LANDSCAPE HEATMAP | W22 (17 May - 24 May 2026)



Methodology: Risk levels are assessed using: (a) confirmed incidents in the reporting period, (b) active threat actor campaigns targeting the sector, (c) vulnerability exposure, and (d) regulatory scrutiny. **Critical (9-10)** = active exploitation or confirmed breach; **High (7-8)** = credible active threat; **Medium (4-6)** = elevated baseline risk; **Low (1-3)** = standard risk posture.

3. SA CYBER INCIDENTS & BREACHES

Week 22 (17-24 May 2026): Zero new ransomware.live listings (SA tally holds at 111). Dominant new story is the coordinated ransom-DDoS (RDoS) wave targeting SA internet infrastructure providers 18-20 May. Nigerian hacktivist group #OpSouthAfrica claims government breaches. Six prior-week incidents remain active or under investigation.⁴

3.1 INC-2026-W22-01 — SA ISP/Hosting Ransom-DDoS (RDoS) Wave [CONFIRMED -- Attribution Disputed]

Sector	Internet hosting / connectivity (telecommunications infrastructure)			
Dates	18-20 May 2026 (plus SSS concurrent attempt 22 May)			
Actor	Self-identified as "BlackMatter" in extortion emails; attribution disputed -- experts cite inconsistency with BlackMatter's demand range			
Ransom	~R16,000 (2.5 XMR) -- inconsistent with BlackMatter historical range of US\$80k-\$15M			
Ransom outcome	Network Platforms: REFUSED. SSS: REFUSED. Other providers: not disclosed. No payments confirmed.			
Peak traffic	676 Gbit/s (individual peaks); >1 Tbps in wider campaign (SSS measurement)			
Confidence	CONFIRMED -- all four named ISPs issued public status statements			

Date	Provider	Peak / Impact	Ransom	Source
18 May	1-Grid	>100 Gbit/s; 32,000 customers; 77,000 hosted sites	Not disclosed	ITWeb

Date	Provider	Peak / Impact	Ransom	Source
19 May	Xneelo	KonsoleH / hosting / email disrupted several hours	Not disclosed	TechCentral
19 May	Network Platforms	>300 Gbit/s; small-payload flood across IP ranges	REFUSED (2.5 XMR ~R16,000)	TechCentral
19-20 May	Seacom	Downstream disruption; DDoS-protected clients unaffected	No breach	ITWeb
19 May	Domains.co.za	Reported impacted	Not disclosed	TechCentral
22 May	SSS (Specialised Security Services)	Data-exfil attempt blocked in 13 minutes; >1 Tbps peaks noted	REFUSED	Mike Bolhuis/SSS

Attribution note: Dr Manny Corregedor (Telspace Africa) and Jayson O'Reilly (Private Protocol) suggest possible nation-state reconnaissance mapping SA network dependency trees or undersea-cable landing-station chokepoints. The scale (>1 Tbps) is consistent with either a large criminal botnet or nation-state operational capability. The R16,000 ransom is commercially implausible for an actor of that capability, supporting the false-flag or reconnaissance theory. SSS demonstrated effective 13-minute threat neutralisation as a defensive benchmark.¹⁴

3.2 INC-2026-W22-02 — #OpSouthAfrica Hactivist Wave [UNVERIFIED]

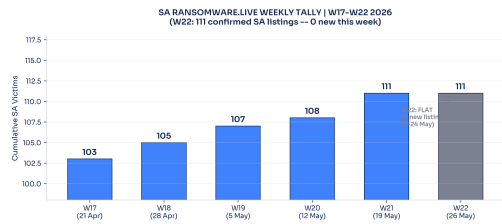
Actor	Nullsec Nigeria, Anonymous Nigeria, 404 Crew, Infernalis
Motivation	Retaliation for xenophobic violence against Nigerians in South Africa
Claimed targets	Dept. of Correctional Services, Ephraim Mogale Local Municipality, SACAA, SANSA, SASSA, DHS, NHFC
Data posted	~11 GB sample from Correctional Services / Ephraim Mogale (bid documents, financial statements, council resolutions)
Government response	NO SA government entity has confirmed the breach as of 24 May 2026
Method	Unconfirmed; DarkNotify cited likely phishing; mass defacement also observed
Confidence	UNVERIFIED -- no victim acknowledgement; no independent data verification; no POPIA notifications reported

Nigerian hactivist groups launched #OpSouthAfrica 18 May, claiming "full databases, PII, financial records, and internal employee data" from the listed government institutions. The assumption of phishing as an attack vector is consistent with group TTPs; no technical confirmation. All five government entity claims remain UNVERIFIED as of 24 May 2026. Monitor Nullsec Nigeria / 404 Crew / Infernalis Telegram channels and await POPIA notifications from the Information Regulator.⁵

3.3 SA Ransomware.live Tally (W22)

End W21 baseline	111 confirmed SA listings
New W22 listings (17-24 May)	0 confirmed
End W22 count	111 (FLAT)
Most recent listing	Standard Bank Group / PrinzEugen (4 May 2026)

No new ransomware.live entries with a discovered date of 17-24 May 2026 were detected for South Africa. The FLAT count should not be interpreted as reduced threat: the dominant SA threat vectors in W22 were DDoS extortion, hactivism, and IAB/credential monetisation.



3.4 Ongoing / Continuation Incidents (W22 Status)

Incident	W22 Status
Canvas/Instructure (5 SA tertiaries)	CLOSED -- Instructure ransom deal 11 May; FBI PSA 15 May warns of downstream spearphishing from Canvas data. Ongoing risk to Wits, Stadio, Milpark, Invictus, SPARK staff/students.
Polmed 1.7M / 214 GB (ShinyHunters)	DEVELOPING -- still no Polmed public statement; NOT covered by Canvas/Instructure ransom deal; forensic probe ongoing.
FlySafair chat-API exposure	CONFIRMED CLOSED -- Pinsent Masons POPIA analysis published 15 May. Reported to Information Regulator. No enforcement action confirmed.
ANC "Black Ax" (15 May claim)	STILL UNVERIFIED -- no ANC statement, no data publication as of 24 May 2026.
SANBS / KillSec (12 May claim)	STILL UNVERIFIED -- no SANBS statement, no KillSec data publication for SANBS.
Standard Bank / ROOTBOY (PrinzEugen)	DEVELOPING -- Information Regulator confirmed investigating; ITWeb 19 May reports public dumps continuing; 21 May new platform glitch raised additional concerns.

4. ITWeb -- 1-Grid DDoS attack (18 May 2026) — <https://www.itweb.co.za/article/large-scale-ddos-attack-hits-web-host-1-grid/o1Jr5MxPNN2MKdWL>
5. Daily Maverick -- #OpSouthAfrica hacktivist wave (18 May 2026) — <https://www.dailymaverick.co.za/article/2026-05-18-hacktivism-targ-et-sa-government-entities-in-cybercrime-wave-in-response-to-xenophobia/>

4. GLOBAL INCIDENTS WITH SA RELEVANCE

Foxconn / Nitrogen Ransomware (CONFIRMED, 18 May)

Nitrogen ransomware group confirmed 8 TB / 11M+ documents stolen from Foxconn North American factories, including Apple, Nvidia, Google, AMD, and Intel device schematics. SA importers and enterprises using affected product lines face potential supply-chain IP exposure risk.⁶

Checkmarx Supply Chain (Update 22 May)

Checkmarx investigation (with Mandiant) in final stages -- no evidence of customer data exfiltration as of 22 May. SA AppSec teams that used the malicious Jenkins AST plugin on 9–10 May must rotate credentials immediately. The malicious VS Code extension and Docker images also represent exposure windows.⁷

First VPN Takedown (21 May)

Europol/law enforcement seized 33 servers and arrested a Ukrainian admin, disrupting at least 25 ransomware gangs that used First VPN infrastructure. Intelligence sharing with 16 countries may yield SA-relevant leads on RaaS group persistence channels. Follow-on enforcement actions possible over coming weeks.⁸

Kimwolf Botnet (21 May -- arrest in Ottawa)

Jacob Butler arrested in Ottawa for allegedly operating Kimwolf botnet: 25,000+ DDoS attacks, 2M+ Android TV devices compromised. Temporal overlap with SA DDoS campaign noted by researchers; Kimwolf is one plausible DDoS-for-hire source for the SA ISP targeting. Arrest removes one capability node.⁸

INTERPOL Operation Ramz (18 May)

201 arrests across 13 MENA countries; Algeria PhaaS (Phishing-as-a-Service) dismantlement reduces SMS-spoofing capacity targeting SA banking consumers. SARS smishing and SA bank phishing kit operators may experience temporary disruption to infrastructure sourced from this supply chain.⁹

6. IANS Research -- Foxconn/Nitrogen ransomware (18 May 2026) — <https://www.iansresearch.com/resources/all-blogs/post/security-blog/2026/05/18/foxconn-confirms-cyberattack-by-nitrogen-ransomware-group>
7. Checkmarx -- Supply chain incident updates (22 May 2026) — <https://checkmarx.com/blog/ongoing-security-updates/>
8. CyberScoop -- Kimwolf botnet arrest (21 May 2026) — <https://cyberscoop.com/kimwolf-botnet-alleged-administrator-jacob-butler-arrested-canada/>
9. INTERPOL -- Operation Ramz MENA arrests (18 May 2026) — <https://www.interpol.int/en/News-and-Events/News/2026/201-arrests-in-first-of-its-kind-cybercrime-operation-in-MENA-region>

5. THREAT ACTORS

5.1 SideWinder (T-APT-04) — Africa Escalation, NCC CSIRT P1 Advisory 21 May

Nigeria's NCC CSIRT issued a Priority 1 advisory on 21 May warning of SideWinder's intensified espionage campaign targeting Africa and Asia, specifically naming government, military, maritime, logistics, telecoms, and finance sectors. Delivery chain: PDF + ClickOnce fake Adobe Reader update MagTek-signed (cert zeroed) "Adobe Compatibility Suite" DEVOBJ.dll sideloads StealerBot. Active exploitation of legacy Office CVEs: CVE-2017-11882, CVE-2018-0802, CVE-2017-0199. SA government, defence, and financial services organisations are explicitly in scope.¹⁰

Type	Indicator
PDF hash (SHA-256)	54ef2aaeeb850c07cf3e01754478da2b8947b7188e1aabc8dd7eb54c78b55bd1
ClickOnce hash (SHA-256)	e5cd4c5e6c35c07b7d1a078ed801a5676d529d41dcbecacd13f744b2c79fe46d
DEVOBJ.dll (SHA-256)	c1093860c1e5e04412d8509ce90568713fc56a0d5993bfdb7386d8dc5e2487b6
Domain	filenest[.]live, snagdrive[.]com, download-doc[.]net
Domain	adobeglobal[.]com, updates-installer[.]store
Domain	mofa-gov-bd[.]filenest[.]live, pmo-gov-pk[.]filenest[.]live
Domain	adobe[.]pdf-downlod[.]com
Indicator	ClickOnce with zeroed publisher cert serial (0000000000000000)

5.2 Lazarus / Kimsuky — Finance Sector Escalation; SA Newly in Target Geography

CYFIRMA Finance Q2 2026 (18 May): Lazarus appearances rose from 2 to 5 -- the largest growth of any group. North Korean actors (Lazarus/BlueNoroff) responsible for 18 of 28 attributed finance incidents (64%). **South Africa newly appears in CYFIRMA's APT campaign target geography** for the first time this quarter: 3 SA finance victims in the past 90 days. Kimsuky (APT43) is CYFIRMA's W22 "Threat Actor in Focus" -- expanded targeting including Belgium, Germany, France, Brazil, and NATO states. TTPs: .vbs/.hta/.ps1 scripts, schtasks /create persistence, exfiltration via docs.google.com/forms and Dropbox.¹¹

5.3 ShinyHunters — Post-Settlement Criminal Brand + FBI PSA Downstream Risk

Le Monde (20 May) confirmed ShinyHunters has evolved into a **criminal brand** rather than a cohesive group. Four French suspects in custody (Adel E./YuroSH, Ziad M./Hollow, Thibaut E./Noct, Yanis H./Depressed). BreachForums still operates under the Hollow alias. ShinyHunters directs **26% of all extortion victims to the finance sector**. The FBI PSA (15 May) warns SA universities (Wits, Stadio, Milpark, Invictus, SPARK) of ongoing downstream spearphishing from compromised Canvas data. Financial-aid and admin staff remain highest-risk targets.¹²

5.4 BravoX (Emerging RaaS) — TTPs Documented

BravoX surfaced January 2026 on RAMP. Full TTP chain documented by Red Piranha: SSL VPN exploitation (weak creds, no MFA) Tor hidden RDP + SOCKS5 SSH via dmw.exe to 45.61.136.225:22 BYOVD EDR kill (vulndriver.sys / wsftprm.sys + Killer.exe; terminates Defender + Sophos) Rclone exfiltration .bx-0000 extension; ransom note OO_Recovery_Notes.txt. Post-negotiation: mail bombing + LinkedIn direct contact to staff. C2 IPs: 91.222.174.96, 91.222.174.120, 64.94.85.76. DLS: bravoxxtrmqeeevhl7gdh2yzvrlrxajr66d33c7ozosrccx4cz7cepad[.]onion.¹³

5.5 SA-Specific Lure Activity (W22)

- **SARS smishing** active W22 -- alphanumeric sender ID spoofing appears inside legitimate SARS SMS threads. Frontline staff and public should validate all SARS payment links via sars.gov.za only.¹⁴
- **SA bank phishing kits** sold under R800 on forums. SIM-swap declining but number-porting/forwarding rising (now 58% of mobile banking fraud). Single-victim R187,000 loss documented.¹⁴
- **Sainbox RAT** (GhOstrAT variant) active via fake WPS Office / DeepSeek / Sougou landing pages. Relevant given WPS Office penetration in SA government endpoints.

5.6 RaaS Landscape Rankings (Red Piranha 12–18 May)

Rank	Group	Market Share	Notes
1	Qilin	17.93%	338 Q1 2026 victims; most active; highest finance sector count
2	The Gentlemen	9.66%	Emerging mid-2025; multiple SA victims YTD
3	Genesis	7.59%	
4	Akira	6.90%	Sustained tempo; cross-platform (Windows, Linux, ESXi)
5	Inc Ransom	6.21%	Active UAE/MENA; potential SA exposure
6	Lynx	5.52%	
7-8	Coinbase Cartel / Play	4.83%	
--	KillSec	1.38%	SANBS claim STILL UNVERIFIED
--	ShinyHunters	0.69%	Data-theft only; no encryption

10. NCC CSIRT -- SideWinder P1 advisory (21 May 2026) — <https://csirt.ncc.gov.ng/index.php/resources/security-advisories/310-escalation-of-sidewinder-apt-group-cyber-espionage-campaigns-targeting-critical-sectors-in-africa-and-asia>

11. CYFIRMA Finance Q2 2026 Industry Report (18 May 2026) — <https://www.cyfirma.com/research/finance-q2-2026-industry-report/>

12. Le Monde -- ShinyHunters the elusive hacking network (20 May 2026) — https://www.lemonde.fr/en/pixels/article/2026/05/20/shinyhunters-the-elusive-hacking-network-that-started-in-france_6753665_13.html

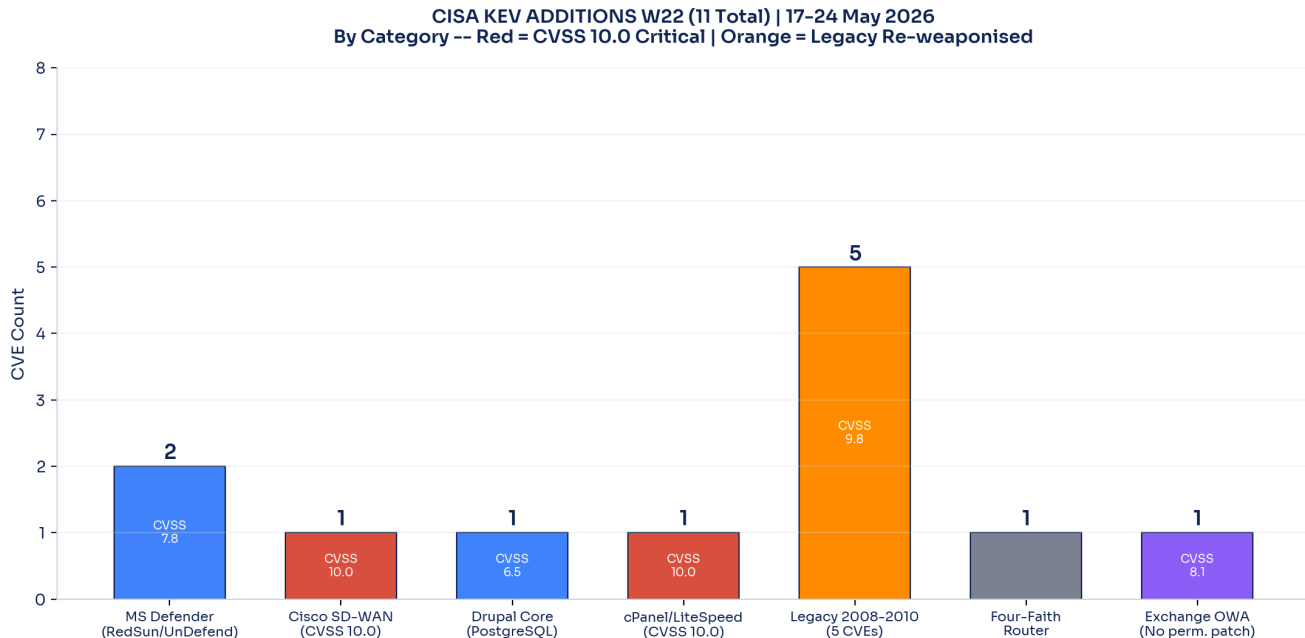
13. Red Piranha -- Threat Intelligence Report 12-18 May 2026 — <https://redpiranha.net/news/threat-intelligence-report-may-12-may-18-2026>

14. IOL -- SARS smishing SA inboxes (22 May 2026) — <https://iol.co.za/business/2026-05-22-the-new-sars-scam-flooding-sa-inboxes--what-you-need-to-know/>

6. CRITICAL VULNERABILITIES & CISA KEV

CISA added **11 CVEs** to the KEV catalog in W22, in two batches (20 May: 7 entries; 23 May: Drupal + others). A striking pattern: **5 of 11 are legacy CVEs from 2008–2010** -- MS08-067 (Conficker-era), DirectShow, Adobe Reader, and two Operation Aurora-era IE use-after-free vulnerabilities -- confirmed as actively re-weaponised in 2026 campaigns against unpatched legacy Windows.³

W22 CISA KEV Additions — Distribution by Category (11 Total)



W22 CISA KEV Additions (11 entries, 17–24 May 2026)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-20182	Cisco / Catalyst SD-WAN Controller & Manager	10.0	Auth bypass	17 May (now past)	UAT-8616 ITW; SSH key injection, NETCONF mod, root escalation
CVE-2026-42897	Microsoft / Exchange Server OWA (2016, 2019, SE)	8.1	XSS/Spoofing	29 May 2026	ITW; NO permanent patch; EEMS M2 only
CVE-2026-41091	Microsoft / Defender Engine (RedSun)	7.8	Privesc to SYSTEM	~10 Jun 2026	OOB patched 21 May; Engine 1.1.26040.8
CVE-2026-45498	Microsoft / Defender Platform (UnDefend)	4.0	DoS -- disables AV	~10 Jun 2026	OOB patched 21 May; Platform 4.18.26040.7
CVE-2026-9082	Drupal Core (PostgreSQL backends)	6.5	SQLi to RCE	27 May 2026	15,000+ attempts; ~6,000 sites; patch available
CVE-2026-48172	LiteSpeed cPanel Plugin	10.0	Privilege assignment	TBD	NEW W22; any tenant to root via lsws.redisAble; patch 2.4.7; ITW
CVE-2024-9643	Four-Faith F3x36 industrial router	N/A	Hard-coded creds	TBD	Active exploitation; internet-facing devices
CVE-2008-4250	Microsoft / Windows Server Service (MS08-067)	--	RCE via RPC	~10 Jun 2026	Conficker-era; re-weaponised 2026
CVE-2009-1537	Microsoft / DirectShow (DirectX QuickTime)	--	Null byte to RCE	~10 Jun 2026	Active 2026 campaigns
CVE-2009-3459	Adobe / Acrobat and Reader	--	Heap overflow to RCE	~10 Jun 2026	Malicious PDF payloads; active 2026
CVE-2010-0249	Microsoft / Internet Explorer	--	UAF to RCE	~10 Jun 2026	Operation Aurora-era; confirmed active re-exploitation
CVE-2010-0806	Microsoft / Internet Explorer	--	UAF to RCE	~10 Jun 2026	Operation Aurora-era; confirmed active re-exploitation

Pattern note: Five of the 11 KEV additions are CVEs from 2008–2010 (16+ years old), added following CISA's confirmation of active re-exploitation in 2026 threat campaigns. This confirms attackers are successfully targeting unpatched legacy Windows environments in operational use. SA organisations running Windows Server 2003/2008 vintage infrastructure or unpatched IE installations are materially exposed.

6.1 Prior KEV Status Updates

Cisco Catalyst SD-WAN CVE-2026-20182 (CVSS 10.0) — KEV deadline 17 May has now passed: UAT-8616 (Cisco Talos attribution) is actively exploiting unpatched controllers with post-compromise SSH key injection, NETCONF configuration modification, and root privilege escalation. The same actor previously exploited CVE-2026-20127. Rapid7 assessed this bug class as ideal for nation-state pre-positioning on critical infrastructure. No public CISA post-deadline compliance report. Any SA organisation running unpatched Cisco Catalyst SD-WAN must patch or implement compensating controls without further delay.¹⁵

Exchange OWA CVE-2026-42897 (CVSS 8.1) — KEV due 29 May 2026. NO permanent patch as of 24 May: Exchange OWA XSS/spoofing zero-day in active exploitation. EEMS Mitigation ID M2 is the only available protection (auto-deployed 14 May via EEMS; verify with Exchange Health Checker at aka.ms/ExchangeHealthChecker). Known breakage: OWA Print Calendar, inline images, OWA Light (?layout=light), IE-mode users remain unprotected. Air-gapped environments: use Exchange On-premises Mitigation Tool via elevated Exchange Management Shell.¹⁶

Ivanti EPMM CVE-2026-1281 (~CVSS 9.8) — KEV due approximately 27 May: Code injection / unauthenticated RCE in Ivanti EPMM. One Russian IP accounted for 83% of observed exploit attempts (DugganUSA). DugganUSA identified this CVE in threat feeds 57 days before CISA's listing. Patch available -- apply immediately. Related CVE-2026-1340 (also EPMM, also KEV) represents a second exploit chain.¹⁷

MICROSOFT DEFENDER OOB PATCH -- 21 MAY 2026 (ACTION REQUIRED)

CVE-2026-41091 (RedSun, CVSS 7.8): Improper link following in Malware Protection Engine (versions below 1.1.26040.8) allows SYSTEM privilege escalation. Patch: Engine 1.1.26040.8. Auto-deployed via Windows Update / WSUS / SCCM.

CVE-2026-45498 (UnDefend, CVSS 4.0): Antimalware Platform DoS silently disables Defender. Platform versions below 4.18.26040.7 are affected. Patch: Platform 4.18.26040.7.

Chain context: Third CVE BlueHammer (CVE-2026-33825) was patched 14 April 2026 PT. Attack sequence: (1) UnDefend disables Defender; (2) RedSun escalates to SYSTEM. Huntress confirmed live intrusions entering via compromised FortiGate VPN, then deploying the chain.

Confirmation steps: After Windows Update: Get-MpComputerStatus -- check AMEngineVersion (expect 1.1.26040.8+) and AMProductVersion (expect 4.18.26040.7+). For hosts where Defender silently stopped between mid-April and 21 May: investigate 4688 events for whoami /priv, cmdkey /list, net group from unexpected user contexts.

6.2 cPanel Hosting Wave — W22 Escalation (CVE-2026-48172)

CVE	CVSS	Type	Status	IOC
CVE-2026-41940	9.8	CRLF to WHM root	Mass-exploitation; PoC public; Mirai + "Sorry" ransomware payloads	.sorry files; root pwd 123Qwe123C; hasroot=1 sessions
CVE-2026-48172	10.0	LiteSpeed plugin privilege assignment	NEW W22; any tenant to root via lsws.redisAble; KEV-listed 23 May; ITW	cpanel_jsonapi_func=redisAble in /var/cpanel/logs/

Combined exposure: approximately 1.5M internet-facing cPanel instances, approximately 70M domains, 200–500 accounts per server. Both CVEs provide root access from a shared hosting tenant -- combined with the SA hosting DDoS wave, this represents a compounded infrastructure risk for SA shared-hosting providers.

6.3 FortiAuthenticator CVE-2026-44277 (CVSS 9.1) and New Zero-Days

FortiAuthenticator CVE-2026-44277: Unauthenticated RCE via improper access control. No confirmed ITW as of 24 May; not in KEV. Patches: 6.5.7 / 6.6.9 / 8.0.3. Cloud-hosted not affected. SA risk: dominant MFA/IdP stack -- pre-auth RCE on the authentication layer enables complete bypass of FortiGate-integrated MFA.¹⁸

Item	CVSS	Status
YellowKey (BitLocker bypass)	TBD	PoC public ~17 May (Chaotic Eclipse); UNPATCHED
GreenPlasma (any user to SYSTEM)	TBD	PoC public ~17 May; UNPATCHED
CVE-2026-42945 (NGINX Rift, heap overflow)	9.2	ITW from 16 May; ~5.7M exposed; patch 1.31.0/1.30.1
CVE-2026-34926 (TrendAI Apex One traversal)	Medium	ITW; patched 22 May
CVE-2026-20223 (Cisco Secure Workload)	10.0	Cross-tenant data theft via REST API; no exploitation; patched 22 May
CVE-2026-0300 (PAN-OS)	9.3/9.8	KEV 6 May; ITW since 9 April; remaining hotfixes due 28 May

Supply chain alerts W22: Laravel-Lang — 4 Composer packages compromised; ~700 malicious versions; PHP credential stealer. TeamPCP/Megalodon — 5,561 GitHub repos targeted; 5,718 malicious commits on 18 May; AWS/GCP/Azure/SSH/Vault/JWT exfil to 216.126.225[.]129:8443. Mini Shai-Hulud npm — TanStack, UiPath, Mistral AI, OpenSearch, and PyPI packages affected.¹⁹

¹⁵ Tenable -- Cisco SD-WAN UAT-8616 exploitation FAQ — <https://www.tenable.com/blog/faq-about-the-continued-exploitation-of-cisco-catalyst-sd-wan-vulnerabilities-uat-8616>

16. Tech Times -- Exchange OWA CVE-2026-42897 no permanent patch (19 May 2026) — <https://www.techtimes.com/articles/316860/20260519/exchange-server-owa-zero-day-cve-2026-42897-exploited-no-permanent-patch-new-mitigation-gaps.htm>
17. DugganUSA -- CISA Ivanti EPMM CVE-2026-1281 KEV (May 2026) — <https://www.dugganusa.com/post/cisa-added-ivanti-epmm-cve-2026-1281-to-kev-on-may-13-we-named-the-russian-ip-owning-83-of-exploit>
18. BleepingComputer -- Fortinet critical RCE FortiAuthenticator — <https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-rce-flaws-in-fortisandbox-and-fortiauthenticator/>
19. The Hacker News -- LiteSpeed cPanel CVE-2026-48172 (May 2026) — <https://thehackernews.com/2026/05/litespeed-cpanel-plugin-cve-2026-48172.html>

7. RANSOMWARE LANDSCAPE

2026 Verizon DBIR (19 May 2026): Ransomware appears in 48% of all breaches (up from 44%). Median ransom paid: less than US\$140,000. 31% of victims paid. Vulnerability exploitation overtook credential theft as the top breach vector (31% vs 13%) for the first time. Median patch time: 43 days (up from 32). Only 26% of CISA KEV entries are patched (down from 38%). Third-party breach involvement: 48% (up 60% year-on-year). Human-element breaches: 62%. Mobile phishing success rate: 40% higher than email phishing. Shadow AI on corporate devices: 67% of users.²⁰

SA Contextualisation: The SA ransomware.live count remains at 111 for W22 (FLAT). The DBIR median patch time of 43 days against CISA KEV patching rates of only 26% -- combined with SA's confirmed legacy Windows exposure (MS08-067 and Aurora-era CVEs now in KEV) -- paints a high-risk picture. ITWeb Security Summit Cape Town (25–26 May) will provide SA-specific contextualisation of DBIR 2026 findings.²⁰

20. Verizon DBIR 2026 -- Data Breach Investigations Report (19 May 2026) — <https://www.verizon.com/business/resources/reports/dbir/>

8. OSINT EXPOSURE & ATTACK SURFACE

SA ISP/Hosting RDoS -- 5 providers confirmed, nation-state recon theory raised

BlackMatter-signed extortion emails sent to multiple SA ISPs; all known recipients refused to pay. Security experts note R16,000 ransom is inconsistent with operational scale -- possible false-flag or nation-state mapping of SA undersea-cable dependency. SSS 13-minute neutralisation demonstrates IR timing benchmark. Any SA hosting-dependent organisation should review upstream DDoS protection and outage-comms plans.¹

#OpSouthAfrica -- 5 government entities claimed, ~11 GB posted

Nigerian hacktivist groups posted sample data from Dept. of Correctional Services and Ephraim Mogale Local Municipality. All five government entity claims remain UNVERIFIED as of 24 May 2026. SA government IT teams: monitor Telegram/dark-web leak boards for data verification; prepare POPIA notification capability.⁵

SideWinder domains active -- block immediately

SideWinder (T-APT-04) PDF+ClickOnce delivery chain active against Africa targets. Block filenest[.]live, snagdrive[.]com, download-doc[.]net, adobeglobal[.]com at DNS/proxy. Flag ClickOnce installs with zeroed publisher cert serial. Patch CVE-2017-11882, CVE-2018-0802, CVE-2017-0199 immediately.¹⁰

BravoX C2 infrastructure -- monitor and block

BravoX C2 IPs: 91.222.174.96, 91.222.174.120, 64.94.85.76. SSH exfil to 45.61.136.225:22. Alert on dmw.exe execution; presence of vulndriver.sys / wsftprm.sys; .bx-0000 file extension on endpoints.¹³

Standard Bank / ROOTBOY -- IR investigation confirmed, public dumps continuing

Information Regulator confirmed investigating. ITWeb 19 May: public dumps continuing. Credential-stuffing and identity-fraud risk elevated for organisations with Standard Bank workforce relationships. Review one-time PIN binding to device; audit sub-threshold transfer patterns.

SARS smishing + SA bank phishing kits -- ongoing W22

SARS smishing campaigns appear in legitimate SMS threads. Alert on outbound HTTP to non-sars.gov.za payment endpoints from SMS-clicked links. SA bank phishing kits available for under R800; number-porting/forwarding now 58% of mobile banking fraud.¹⁴

9. REGULATORY & COMPLIANCE

SARB Prudential Communication 10 of 2026 (20 May) — Significant for Non-Bank PSPs

The SARB Prudential Authority opened consultation on the **Payment Activities Authorisation Framework**. Covered activities: e-money, mobile money, payment initiation, TPPPs, money remittances. Key cyber implication: **cyber-attack and data-privacy breach are explicitly named regulated risks** with cybersecurity, operational resilience, and AML/CFT/CPF obligations extended to non-bank PSPs. SA fintech, mobile money, and payment-initiation providers must audit their cybersecurity posture against SARB's proposed framework.²¹

Abidjan Declaration (19 May) — Continental Data Governance Roadmap to 2030

The 9th RAPDP conference adopted the Abidjan Declaration, establishing Africa's continental data governance roadmap to 2030. Calls for harmonised AI, biometrics, and digital-finance frameworks across AU member states. The SA Information Regulator's forthcoming Cross-Border Transfer Guidance Note will reference AfCFTA Digital Trade Protocol and AU frameworks. SA organisations with pan-African data flows should track alignment with Abidjan Declaration principles.²²

Verizon DBIR 2026 (19 May) — Key Metrics for SA Context

Metric	Reading
Breaches via vulnerability exploitation	31% (overtook credential abuse 13% for first time)
Median patching time	43 days (up from 32)
CISA KEV patched within deadline	26% (down from 38%)
Ransomware in all breaches	48% (up from 44%)
Median ransom paid	Less than US\$140,000
Victims who paid ransom	31%
Third-party breach involvement	48% (up 60% year-on-year)
Human-element breaches	62%
Mobile phishing vs email phishing success	40% higher (mobile)
Shadow AI on corporate devices	67% of users

Other W22 Regulatory Developments

- **POPIA Health Data Regs (Webber Wentzel 24 May):** Guidance on "special personal information" framework for health data. No new IR enforcement action in W22. Compliance obligations: written confidentiality agreements; role-based access controls; documented secure disposal; cross-border transfer audit under s.72(1).²³
- **Cybercrimes Act SOPs (Webber Wentzel 17 May):** Detailed analysis of SAPS search/seizure powers under s.26 for cyber articles. SA organisations must understand evidentiary chain-of-custody requirements when engaging SAPS for cybercrime investigations.²³
- **SA Draft AI Policy:** Prof Benjamin Rosman's expert panel operational. Comment deadline 10 June 2026 (original; revised draft deadline pending). SA organisations deploying AI should engage the comment process.²⁴
- **FSCA actions (W22):** 20 May impersonation warnings (PWM Wealth Management, Prime Investments); 21 May regulatory action (Mr R F Linder / Equitos Group). Monitor FSCA notices for financial-services compliance.²⁵
- **EU AI Act Omnibus (7 May agreement):** HRAIS deadline moved to 2 December 2027; Art. 50 transparency obligations remain 2 August 2026 (unchanged); new "nudifier"/CSAM prohibition; SME threshold expanded to 750 staff / EUR150M.²⁶
- **GDPR enforcement context:** Yango Finland EUR100M (Russia transfers); Italian Garante EUR12.5M (banking-app device monitoring). Enforcement risk for SA organisations with EU data transfers continues to intensify.²⁶
- **NIS2 status:** Poland in force 2 April 2026; Italy security-measures deadline 1 October 2026.²⁷

Compliance Deadlines — W22 Forward View

Date	Item	Owner
27 May 2026	CISA KEV: Drupal CVE-2026-9082; Ivanti EPMM CVE-2026-1281	IT
28 May 2026	PAN-OS CVE-2026-0300 final hotfix ETA	IT
29 May 2026	CISA KEV: Exchange OWA CVE-2026-42897 (mitigation only; no permanent patch)	IT
25-26 May 2026	ITWeb Security Summit Cape Town	Leadership
10 June 2026	SA Draft AI Policy public comment (original deadline)	Compliance
30 June 2026	PAIA annual report (2024/25) via IR eServices	Privacy
2 August 2026	EU AI Act Art. 50 transparency obligations	Compliance
1 October 2026	Italy NIS2 security measures adoption	EU subsidiary
2 December 2026	EU AI Act watermarking; "nudifier" prohibition	Compliance
2 December 2027	EU AI Act HRAIS deadline (deferred)	Compliance

21. SARB Prudential Communication 10 of 2026 (20 May) — <https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-public-awareness/Communication/2026/prudential-communication-10-of-2026>

22. Financial Afrik -- Abidjan Declaration digital sovereignty (21 May 2026) — <https://www.financialafrik.com/en/2026/05/21/digital-africa-aims-to-make-data-governance-a-lever-for-sovereignty-and-attractiveness/>

23. Webber Wentzel -- POPIA health data compliance (24 May 2026) — <https://www.webberwentzel.com/News/Pages/popia-compliance-for-health-data-navigating-special-personal-information-requirements-in-healthcare.aspx>

24. Werksmans -- SA AI Policy expert panel and comment deadline — <https://werksmans.com/>

25. FSCA -- Financial Sector Conduct Authority media releases — <https://www.fsca.co.za/>

26. White and Case -- EU AI Act Digital Omnibus deal (7 May 2026) — <https://www.whitecase.com/insight-alert/eu-agrees-digital-omnibus-deal-simplify-ai-rules>

27. SecurityWeek -- Verizon DBIR 2026 vulnerability exploitation (19 May 2026) — <https://www.securityweek.com/verizon-dbir-2026-vulnerability-exploitation-overtakes-credential-theft-as-top-breach-vector/>

10. WEEKLY THREAT HUNT & IOCs

Nine hunt missions are active for W22. Four P1 missions address DDoS readiness, Exchange OWA EEMS verification, Defender OOB confirmation, and cPanel exploitation. Four P2 missions address SideWinder domain blocking, BravoX SSL VPN detection, Standard Bank/ROOTBOY exposure, and SARS smishing. One P3 mission provides Cisco SD-WAN post-compromise verification.

TH-2026-W22-01 — Cisco SD-WAN UAT-8616 Post-Compromise Verification

P1 — CRITICAL: KEV deadline 17 May (now past)

Hypothesis: On unpatched controllers (KEV deadline 17 May now past), UAT-8616 may have already established persistence via SSH key injection and NETCONF configuration modification.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1098.004 (SSH Authorized Keys), T1565.003 (Runtime Data Manipulation).

IOCs: Unexpected entries in `~/.ssh/authorized_keys` on controller; NETCONF config history showing unauthorized changes; root-shell access correlated with non-admin source IPs.

Data Sources: Cisco vManage audit logs, SD-WAN NETCONF configuration history, controller SSH auth log, NetFlow from controller management interfaces.

Detection Guidance: Check `~/.ssh/authorized_keys` for unexpected entries. Review NETCONF config history for non-admin changes. Correlate root-shell access events with source IP against allowed management IPs. Patch immediately if unpatched.

TH-2026-W22-02 — Exchange OWA EEMS M2 Verification and Exploitation Hunt

P1 — CRITICAL: ITW zero-day; KEV due 29 May; no permanent patch

Hypothesis: Organisations that have not confirmed EEMS Mitigation ID M2 are actively exposed to CVE-2026-42897 (XSS/spoofing, ITW). EEMS M2 is the only available protection.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1078 (Valid Accounts), T1059.007 (JavaScript).

IOCs: Anomalous OWA URL patterns with script payloads; unexpected OWA logon-cookie reuse from new IPs or geolocations; anomalous JavaScript execution in OWA context.

Data Sources: Exchange IIS logs (OWA paths), Exchange Health Checker output, Exchange audit log, Azure AD sign-in logs for Exchange-authenticated sessions.

Detection Guidance: Run Exchange Health Checker (aka.ms/ExchangeHealthChecker); confirm Mitigation ID M2 listed. Alert on OWA logon-cookie reuse from new geolocations. Review account takeover indicators (new forwarding rules, new delegates, anomalous mailbox access). Brief users on OWA Light and IE-mode limitations.

TH-2026-W22-03 — Defender RedSun/UnDefend OOB Verification

P1 — CRITICAL: ITW; OOB patched 21 May

Hypothesis: On hosts where Defender silently stopped between mid-April and 21 May 2026, an attacker may have already gained SYSTEM privileges via the UnDefend/RedSun chain following FortiGate VPN entry.

MITRE ATT&CK: T1562.001 (Impair Defenses: Disable or Modify Tools), T1548 (Abuse Elevation Control Mechanism).

IOCs: Defender Engine version below 1.1.26040.8; Platform version below 4.18.26040.7; 4688 events showing whoami /priv, cmdkey /list, net group from unexpected user contexts; compromised FortiGate VPN credentials.

Data Sources: Windows Security log (EID 4688), Windows Defender event log, Get-MpComputerStatus output via SCCM/Intune, FortiGate VPN authentication logs.

Detection Guidance: Get-MpComputerStatus: verify `AMEngineVersion >= 1.1.26040.8` and `AMProductVersion >= 4.18.26040.7`. Hunt 4688 events for whoami /priv, cmdkey /list, net group from non-admin contexts between 15 April and 21 May. Review FortiGate VPN login anomalies from that period.

P1 — CRITICAL:

CVE-2026-48172 CVSS 10.0;
ITW

TH-2026-W22-04 — cPanel CRLF + LiteSpeed Root-Escalation Hunt

Hypothesis: Both CVE-2026-41940 (CRLF to WHM root) and CVE-2026-48172 (LiteSpeed cPanel any tenant to root) are in-the-wild against SA hosting providers. Any unpatched cPanel instance should be treated as potentially compromised.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1098 (Account Manipulation), T1505.003 (Web Shell).

IOCs: grep -rE "cpanel_jsonapi_func=redisAble" in /var/cpanel/logs/ and /usr/local/cpanel/logs/; .sorry extension files on hosted volumes; hasroot=1 in /var/cpanel/sessions/raw/; root password 123Qwe123C; raw newlines in password field; tfa_verified=1 with no TFA origin.

Data Sources: cPanel audit log, SSH auth log, /var/cpanel/sessions/raw/ review, hosted volume file scan, cPanel API token audit.

Detection Guidance: Grep logs for cpanel_jsonapi_func=redisAble. Scan /var/cpanel/sessions/raw/ for hasroot=1. Check root password. Scan hosted volumes for .sorry files. Update LiteSpeed cPanel plugin to 2.4.7. Any hit = assume breach; escalate to IR.

P2 — HIGH: NCC CSIRT P1
advisory; Africa targeting
escalation

TH-2026-W22-05 — SideWinder PDF + ClickOnce Detection

Hypothesis: SideWinder T-APT-04 is targeting Africa-region government, military, maritime, and finance organisations using a PDF + ClickOnce delivery chain with zeroed publisher cert. NCC CSIRT P1 advisory 21 May.

MITRE ATT&CK: T1566.001 (Phishing: Spearphishing Attachment), T1204.002 (User Execution: Malicious File), T1574.002 (Hijack Execution Flow: DLL Side-Loading).

IOCs: filenest[.]live, snagdrive[.]com, download-doc[.]net, adobeglobal[.]com, updates-installer[.]store; ClickOnce publisher cert serial 0000000000000000; DEVOBJ.dll hash c1093860c...; PDF hash 54ef2aae...

Data Sources: DNS/proxy logs for listed domains, ClickOnce event logs, Windows Application event log (ClickOnce installs), endpoint file hash telemetry.

Detection Guidance: Block all SideWinder domains at DNS/proxy. Alert on ClickOnce installs from unrecognised publishers. Flag publisher cert serial 0000000000000000. Patch CVE-2017-11882 / CVE-2018-0802 / CVE-2017-0199 immediately.

P2 — HIGH: Emerging RaaS;
SA-relevant TTPs

TH-2026-W22-06 — BravoX RaaS SSL VPN Initial Access Detection

Hypothesis: BravoX targets SA organisations via SSL VPN exploitation (weak creds, no MFA). BYOVD EDR kill (vulndriver.sys/wsftprm.sys) disables Defender and Sophos before encryption.

MITRE ATT&CK: T1133 (External Remote Services), T1562.001 (Disable Security Tools), T1048 (Exfiltration Over Alternative Protocol).

IOCs: dmw.exe execution; SSH connections to 45.61.136.225:22; vulndriver.sys / wsftprm.sys file presence; .bx-0000 extension; 00_Recovery_Notes.txt; C2 IPs: 91.222.174.96, 91.222.174.120, 64.94.85.76.

Data Sources: SSL VPN authentication logs, EDR process tree, Windows file creation events, SIEM correlation for known C2 IPs.

Detection Guidance: Audit all SSL VPN endpoints for MFA enforcement. Alert on dmw.exe execution, SSH to 45.61.136.225:22, and presence of vulndriver.sys/wsftprm.sys. Block BravoX C2 IPs at perimeter. Require MFA on all SSL VPN.

TH-2026-W22-07 — DDoS Extortion Email Triage**P2 — HIGH: Active campaign targeting SA infrastructure**

Hypothesis: The "BlackMatter" RDoS campaign may send extortion emails to additional SA providers not yet publicly disclosed. Identifying and routing these emails without response is critical to avoiding inadvertent engagement.

MITRE ATT&CK: T1491 (Defacement/Disruption), T1566 (Phishing for extortion).

IOCs: "BlackMatter" sender pattern; Monero (XMR) wallet addresses in email body; extortion amounts near 2.5 XMR / R16,000; DDoS threat + payment deadline language.

Data Sources: Email security gateway, email abuse@/security@ inboxes, DNS/network telemetry for DDoS signature patterns.

Detection Guidance: Configure mail filters for "BlackMatter" sender patterns and Monero-address-bearing extortion bodies. Route to IR queue without response. Share IOCs with upstream ISP for cooperative mitigation. Do not pay; contact upstream ISP immediately on DDoS onset.

TH-2026-W22-08 — Standard Bank / ROOTBOY Exposure Monitoring**P2 — HIGH: IR investigation confirmed; dumps continuing**

Hypothesis: PrinzEugen/ROOTBOY public dumps continue. Customer-facing credential and identity data from Standard Bank is available for credential-stuffing and fraud against any organisation with Standard Bank workforce relationships.

MITRE ATT&CK: T1078 (Valid Accounts), T1110.004 (Credential Stuffing).

IOCs: Standard Bank customer PII on IAB markets; sub-threshold transfer patterns indicative of mule activity; Standard Bank email/ID combinations in credential-stuffing attack logs.

Data Sources: Authentication logs, transfer monitoring systems, dark web intelligence feeds, HudsonRock infostealer telemetry.

Detection Guidance: Revalidate one-time PIN binding to device. Review out-of-band login alerts. Audit for sub-threshold transfer patterns. Alert on Standard Bank-domain credentials appearing in credential-stuffing attempt logs.

TH-2026-W22-09 — SARS Smishing IOC Detection**P3 — MONITORING: Active campaign; staff awareness priority**

Hypothesis: SARS smishing campaigns use alphanumeric sender ID spoofing to appear within legitimate SARS SMS threads, directing victims to non-sars.gov.za payment endpoints.

MITRE ATT&CK: T1598.003 (Spearphishing via Service), T1566.004 (Phishing via SMS/Smishing).

IOCs: Outbound HTTP to non-sars.gov.za payment endpoints from SMS-clicked links; SARS-branded payment pages at non-.gov.za domains; alphanumeric sender IDs "SARS" in SMS metadata.

Data Sources: Mobile device management (MDM) URL logs, web proxy logs, email/SMS gateway telemetry, staff phishing reports.

Detection Guidance: Alert on outbound HTTP/HTTPS to non-sars.gov.za payment endpoints originating from SMS-clicked links. Brief frontline SARS-comms-handlers on sender-ID spoofing. Reinforce that SARS never requests payment via SMS link. Report smishing to SARS Fraud Hotline: 0800 00 7277.

IOC Master Table — W22

Indicator	Type	Attribution	Hunt ID
filenest[.]live, snagdrive[.]com, download-doc[.]net, adobeglobal[.]com	Domain	SideWinder (T-APT-04) delivery	TH-2026-W22-05
0000000000000000 (zeroed cert serial)	ClickOnce publisher cert	SideWinder fake Adobe update	TH-2026-W22-05
54ef2aaeeb850c07cf3e01754478da2b8947b7188e1aabc8dd7eb54c78b55bd1	SHA-256 (PDF)	SideWinder initial lure	TH-2026-W22-05
c1093860c1e5e04412d8509ce90568713fc56a0d5993bfdb7386d8dc5e2487b6	SHA-256 (DEVOBJ.dll)	SideWinder StealerBot sideload	TH-2026-W22-05
dmw.exe + SSH to 45.61.136.225:22	Process + network IOC	BravoX SOCKS5 tunnel	TH-2026-W22-06
91.222.174.96, 91.222.174.120, 64.94.85.76	IP (C2)	BravoX RaaS C2	TH-2026-W22-06
vulndriver.sys / wsftprm.sys + Killer.exe	File (BYOVD driver)	BravoX EDR kill chain	TH-2026-W22-06
216.126.225[.]129:8443	IP:Port (exfil)	TeamPCP/Megalodon supply chain exfil	Monitor
cpanel_jsonapi_func=redisAble	Log pattern	CVE-2026-48172 LiteSpeed cPanel exploitation	TH-2026-W22-04
hasroot=1 in /var/cpanel/sessions/raw/	File content	CVE-2026-41940 cPanel IOC	TH-2026-W22-04
root password 123Qwe123C	Credential IOC	CVE-2026-41940 post-exploitation	TH-2026-W22-04
.sorry extension on hosted volumes	File extension	cPanel/WHM "Sorry" ransomware payload	TH-2026-W22-04
CVE-2026-42897 (Exchange OWA)	CVE	ITW; KEV due 29 May; EEMS M2 only	TH-2026-W22-02
CVE-2026-20182 (Cisco SD-WAN)	CVE	UAT-8616 ITW; KEV 17 May (now past)	TH-2026-W22-01
CVE-2026-48172 (LiteSpeed cPanel)	CVE	CVSS 10.0; ITW; KEV 23 May	TH-2026-W22-04

11. RECOMMENDATIONS

Immediate (This Week — Priority P1)

- **1. DDoS readiness check -- validate scrubbing, anycast, comms templates:** After the 18-20 May RDoS wave hitting five SA ISPs at up to 1 Tbps: contact your upstream ISP about cooperative DDoS mitigation. Confirm CDN/scrubbing protection for all internet-facing infrastructure. Do not engage with extortion emails. Build or review outage-comms templates for rapid customer communication. Confirm IR timing target (SSS benchmark: 13 minutes).
- **2. Patch Defender OOB (21 May) -- confirm Engine 1.1.26040.8 and Platform 4.18.26040.7 on every endpoint:** Auto-deployed via Windows Update / WSUS / SCCM, but verify. For any host where Defender was silently inactive between mid-April and 21 May: treat as potentially compromised; hunt for whoami/priv, cmdkey/list, net group from unexpected user contexts.
- **3. Update LiteSpeed cPanel plugin to 2.4.7 (CVE-2026-48172, CVSS 10.0, KEV 23 May):** Any tenant can escalate to root via lsws.redisAble on unpatched versions. SA hosting providers are doubly exposed (DDoS wave + cPanel root-access path). Hunt IOC: grep cpanel_jsonapi_func=redisAble in /var/cpanel/logs/.
- **4. Verify Exchange OWA EEMS Mitigation ID M2 (KEV due 29 May, no permanent patch):** Run Exchange Health Checker (aka.ms/ExchangeHealthChecker). Confirm M2 deployed. Brief OWA users on calendar printing, inline images, OWA Light limitations until permanent patch.
- **5. Patch Drupal CVE-2026-9082 and Ivanti EPMM CVE-2026-1281 by 27 May (KEV deadline):** 15,000+ attacks against Drupal PostgreSQL backends. Ivanti EPMM code injection (approx CVSS 9.8):

one Russian IP accounts for 83% of observed attempts.

- **6. Block SideWinder domains at DNS/proxy (NCC CSIRT P1 advisory 21 May):** Block filenest[.]live, snagdrive[.]com, download-doc[.]net, adobeglobal[.]com, updates-installer[.]store. Patch CVE-2017-11882 / CVE-2018-0802 / CVE-2017-0199 on all Office installations.
- **7. Patch PAN-OS CVE-2026-0300 remaining hotfixes by 28 May:** KEV-listed 6 May; ITW since 9 April; final hotfixes due 28 May.
- **8. Canvas SA tertiaries -- force credential resets and brief admin/financial-aid staff:** Wits, Stadio, Milpark, Invictus, SPARK Schools remain exposed to ShinyHunters downstream spearphishing using stolen Canvas course and identity data. FBI PSA 15 May confirms ongoing campaigns.

Short-Term (Next 30 Days)

- Patch legacy Windows for MS08-067, DirectShow, Adobe Reader, IE UAF CVEs (all newly in KEV) -- these represent active re-exploitation in 2026 campaigns. Any unpatched Windows Server 2003/2008 vintage infrastructure must be isolated or upgraded.
- Attend ITWeb Security Summit Cape Town 25-26 May -- DBIR 2026 SA contextualisation and practical threat briefings.
- Review SARB PC10 (20 May) implications for any non-bank PSP: payment initiation, e-money, mobile money, money remittance operators must assess cyber obligations under the proposed Payment Activities Authorisation Framework.
- POPIA Health Data Regs compliance review for any SA organisation processing employee health data -- written confidentiality agreements, role-based access controls, and secure disposal documentation are mandatory.
- Submit comments on SA Draft AI Policy by 10 June 2026.
- PAIA annual report (2024/25) must be submitted via IR eServices by 30 June 2026.
- EU AI Act Art. 50 transparency obligations apply from 2 August 2026 -- assess AI-generated content disclosure requirements.

Strategic (Next Quarter)

- DDoS/RDoS resilience programme -- the W22 SA ISP wave demonstrated multi-vector capability at over 1 Tbps. Any SA organisation with internet-facing revenue infrastructure must have a formal DDoS response plan including upstream ISP cooperative mitigation, anycast capability, and pre-negotiated scrubbing.
- Infrastructure dependency mapping -- the nation-state reconnaissance theory raised by Dr Corregedor (Telspace Africa) suggests adversaries are mapping SA network dependency trees. SA critical infrastructure operators should conduct their own dependency analysis and engage NCPCC.
- APT programme readiness -- CYFIRMA's addition of SA to Lazarus/North Korean APT campaign target geography for the first time is a strategic indicator shift. SA financial services firms must elevate APT detection (lateral movement, long-dwell persistence) above perimeter-only defences.
- POPIA breach-notification readiness -- IR 2,374 notifications in 2024/25 (+40% YoY monthly rate) with faster enforcement. Incident-notification runbooks and IR eServices registration are non-negotiable.
- Third-party supply-chain risk -- Canvas/Instructure, Foxconn/Nitrogen, Checkmarx supply chain, and TeamPCP/Megalodon all affected SA organisations in W22. Extend vendor risk programme to cover SaaS platforms, AppSec tooling, and upstream hosting providers.

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. TechCentral -- Extortion fears as DDoS attacks hit SA internet infrastructure (19 May 2026) — <https://techcentral.co.za/extortion-fears-as-ddos-attacks-hit-sa-internet-infrastructure/281499/>
2. TechCentral -- DDoS extortionists carpet-bomb South African internet hosts — <https://techcentral.co.za/ddos-extortionists-carpet-bomb-south-african-internet-hosts/281504/>
3. TechCentral -- Troubling questions over SA internet infrastructure attacks — <https://techcentral.co.za/troubling-questions-over-south-african-internet-infrastructure-attacks/281524/>
4. ITWeb -- Large-scale DDoS attack hits 1-Grid (18 May 2026) — <https://www.itweb.co.za/article/large-scale-ddos-attack-hits-web-host-1-grid/o1Jr5MxPNN2MKdWL>
5. ITWeb -- DDoS-for-hire boom blamed for attacks on SA ISPs (20 May 2026) — <https://www.itweb.co.za/article/ddos-for-hire-boom-blamed-for-attacks-on-sas-isps/KjlyrvwBOQ3qk6am>
6. Mike Bolhuis/SSS -- SSS neutralises data breach and recovers critical infrastructure in 13 minutes — <https://www.mikebolhuis.co.za/post/success-project-sss-neutralises-data-breach-recovers-critical-infrastructure-within-13-minutes>
7. Daily Maverick -- #OpSouthAfrica hacktivist wave (18 May 2026) — <https://www.dailymaverick.co.za/article/2026-05-18-hacktivist-wave-targ-et-sa-government-entities-in-cybercrime-wave-in-response-to-xenophobia/>
8. TechnoMag -- Nigerian hackers claim breach of SA Correctional Services — <https://technomag.co.zw/nigerian-hackers-claim-breach-of-sa-correctional-services-demands-end-to-attacks-on-nigerians/>
9. ITWeb -- Standard Bank data breach video report (19 May 2026) — <https://www.itweb.co.za/videos/PmxVE7KER56qQY85>
10. IOL -- More Standard Bank clients come forward; fraud claims near R60m — <https://iol.co.za/news/south-africa/2026-05-06-more-standard-bank-clients-come-forward-as-fraud-claims-near-r60m-in-losses/>
11. Ransomware.live -- South Africa country map — <https://www.ransomware.live/map/ZA>
12. Pinsent Masons -- FlySafair data breach highlights POPIA reporting duties (15 May 2026) — <https://www.pinsentmasons.com/out-law/analysis/flysafair-data-breach-highlights-reporting-duties-south-africa>
13. IANS Research -- Foxconn confirms cyberattack by Nitrogen ransomware (18 May 2026) — <https://www.iansresearch.com/resources/all-blogs/post/security-blog/2026/05/18/foxconn-confirms-cyberattack-by-nitrogen-ransomware-group>
14. Checkmarx -- Supply chain incident security updates (22 May 2026) — <https://checkmarx.com/blog/ongoing-security-updates/>
15. CyberScoop -- Law enforcement shuts down First VPN service (21 May 2026) — <https://cyberscoop.com/europol-take-down-first-vpn-cybercrime/>
16. CyberScoop -- Kimwolf botnet administrator Jacob Butler arrested (21 May 2026) — <https://cyberscoop.com/kimwolf-botnet-alleged-administrator-jacob-butler-arrested-canada/>
17. INTERPOL -- Operation Ramz: 201 arrests across MENA region (18 May 2026) — <https://www.interpol.int/en/News-and-Events/News/2026/201-arrests-in-first-of-its-kind-cybercrime-operation-in-MENA-region>
18. CISA KEV Catalog -- Known Exploited Vulnerabilities — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
19. Windows Forum -- CISA KEV May 20 2026 legacy Windows bugs and Defender flaws — <https://windowsforum.com/threads/cisa-kev-may-20-2026-old-windows-bugs-and-defender-flaws-still-being-exploited.419101/>
20. The Hacker News -- Drupal Core SQL injection KEV (23 May 2026) — <https://thehackernews.com/2026/05/drupal-core-sql-injection-bug-actively.html>
21. Tenable -- Cisco SD-WAN UAT-8616 exploitation FAQ — <https://www.tenable.com/blog/faq-about-the-continued-exploitation-of-cisco-catalyst-sd-wan-vulnerabilities-uat-8616>
22. Tech Times -- Exchange OWA CVE-2026-42897 no permanent patch (19 May 2026) — <https://www.techtimes.com/articles/316860/20260519/exchange-server-owa-zero-day-cve-2026-42897-exploited-no-permanent-patch-new-mitigation-gaps.htm>
23. BleepingComputer -- Microsoft warns of new Defender zero-days exploited in attacks (21 May 2026) — <https://www.bleepingcomputer.com/news/security/microsoft-warns-of-new-defender-zero-days-exploited-in-attacks/>
24. DugganUSA -- Ivanti EPMM CVE-2026-1281 KEV and Russian IP exploit activity — <https://www.dugganusa.com/post/cisa-added-ivanti-epmm-cve-2026-1281-to-kev-on-may-13-we-named-the-russian-ip-owning-83-of-exploit>
25. The Hacker News -- LiteSpeed cPanel plugin CVE-2026-48172 (May 2026) — <https://thehackernews.com/2026/05/litespeed-cpanel-plugin-cve-2026-48172.html>
26. BleepingComputer -- Fortinet warns of critical RCE flaws in FortiAuthenticator (May 2026) — <https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-rce-flaws-in-fortisandbox-and-fortiauthenticator/>
27. Innovate Cybersecurity -- YellowKey and GreenPlasma Windows zero-days (May 2026) — <https://innovatecybersecurity.com/security-t-hreat-advisory/top-10-cybersecurity-news-may-18-2026-researcher-drops-yellowkey-and-greenplasma-windows-zero-days-exploits-microsoft-may-2026-patch-tuesday-microsoft-warns-of-active-zero-day-exchange-server-exp/>
28. Help Net Security -- NGINX vulnerability CVE-2026-42945 exploited (May 2026) — <https://www.helpnetsecurity.com/2026/05/18/nginx-vulnerability-exploited-cve-2026-42945/>
29. NCC CSIRT Nigeria -- SideWinder P1 advisory (21 May 2026) — <https://csirt.ncc.gov.ng/index.php/resources/security-advisories/310-escalation-of-sidewinder-apt-group-cyber-espionage-campaigns-targeting-critical-sectors-in-africa-and-asia>
30. Trellix -- SideWinder shifting sands ClickOnce for espionage — <https://www.trellix.com/blogs/research/sidewinders-shifting-sands-click-once-for-espionage/>
31. CYFIRMA -- Finance Q2 2026 Industry Report (18 May 2026) — <https://www.cyfirma.com/research/finance-q2-2026-industry-report/>
32. CYFIRMA -- Weekly Intelligence Report 22 May 2026 — <https://www.cyfirma.com/news/weekly-intelligence-report-22-may-2026/>
33. Le Monde -- ShinyHunters the elusive hacking network (20 May 2026) — https://www.lemonde.fr/en/pixels/article/2026/05/20/shinyhunters-the-elusive-hacking-network-that-started-in-france_6753665_13.html
34. Red Piranha -- Threat Intelligence Report 12-18 May 2026 — <https://redpiranha.net/news/threat-intelligence-report-may-12-may-18-2026>

35. IOL -- SARS smishing flooding SA inboxes (22 May 2026) — <https://iol.co.za/business/2026-05-22-the-new-sars-scam-flooding-sa-inboxes--what-you-need-to-know/>
36. Currency News -- How a perfectly faked SMS can empty your bank account — <https://currencynews.co.za/how-a-perfectly-faked-sms-can-empty-your-bank-account/>
37. SARB Prudential Communication 10 of 2026 -- Payment Activities Authorisation Framework — <https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-public-awareness/Communication/2026/prudential-communication-10-of-2026>
38. Financial Afrik -- Abidjan Declaration digital sovereignty (21 May 2026) — <https://www.financialafrik.com/en/2026/05/21/digital-africa-aims-to-make-data-governance-a-lever-for-sovereignty-and-attractiveness/>
39. Verizon DBIR 2026 -- Data Breach Investigations Report (19 May 2026) — <https://www.verizon.com/business/resources/reports/dbir/>
40. SecurityWeek -- Verizon DBIR 2026 vulnerability exploitation overtakes credential theft (19 May 2026) — <https://www.securityweek.com/verizon-dbir-2026-vulnerability-exploitation-overtakes-credential-theft-as-top-breach-vector/>
41. Webber Wentzel -- POPIA health data compliance guidance (24 May 2026) — <https://www.webberwentzel.com/News/Pages/popia-compliance-for-health-data-navigating-special-personal-information-requirements-in-healthcare.aspx>
42. Webber Wentzel -- Cybercrimes Act SOPs for search and seizure (17 May 2026) — <https://www.webberwentzel.com/News/Pages/New-standard-operating-procedures-for-the-investigation-search-access-or-seizure-of-cyber-articles.aspx>
43. White and Case -- EU AI Act Digital Omnibus deal (7 May 2026) — <https://www.whitecase.com/insight-alert/eu-agrees-digital-omnibus-deal-simplify-ai-rules>
44. Werksmans -- Information Regulator APP Portfolio Committee analysis (5 May 2026) — <https://werksmans.com/south-africas-information-regulator-what-the-2025-26-annual-performance-plan-means-for-business-as-presented-to-the-portfolio-committee-on-5-may-2026/>
45. ITWeb -- ITWeb Security Summit Cape Town (25-26 May 2026) — <https://www.itweb.co.za/article/cape-towns-cyber-security-leaders-set-to-gather-for-itweb-security-summit-this-month/Gb3BwMWa62dv2k6V>
46. IOL -- DDoS attacks hit South Africa everyday internet users (22 May 2026) — <https://iol.co.za/news/south-africa/2026-05-22-ddos-attacks-hit-south-africa-how-cybercrime-disrupted-everyday-internet-users/>

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-W22