



SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 23 | 24 May – 31 May 2026

THREAT LEVEL: HIGH

PAN-OS GlobalProtect CVE-2026-0257 (CVSS 9.3) moves to confirmed mass-exploit -- KEV 29 May, deadline 19 Jun. Pick n Pay/Bottles data breach CONFIRMED (POPIA s.22 triggered). Webworm China APT confirmed compromise of SA university. Exchange OWA KEV deadline 29 May PASSED with no permanent patch. Supply chain triple (DAEMON Tools/TanStack/Nx) KEV 27 May. Oracle ORDS CVSS 10.0 patched 28 May. SA ransomware count FLAT at 111; Oday Syndicate new leak site debuted with XL Africa Group.

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W23 | Classification: TLP:WHITE

Published Monday 1 June 2026

© 2026 Digital Progression | dpcyber.co.za

TABLE OF CONTENTS

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

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH (unchanged from W21-W22) — Week 23 (24–31 May 2026)

Story 1 — PAN-OS GlobalProtect CVE-2026-0257 Moves to Mass Exploitation: Palo Alto's authentication bypass vulnerability (CVSS 9.3) escalated from limited probing to confirmed mass exploitation across multiple SA-relevant managed-services customers. Rapid7 MDR documented two distinct attack waves originating from Vultr and Dromatics Systems hosting. CISA added to KEV on 29 May with a deadline of 19 June. Affected: PAN-OS 10.2, 11.0, 11.1, 11.2, 12.0, 12.1, and Prisma Access. Mitigation: patch to fixed versions immediately or disable auth override feature. SA relevance is CRITICAL -- PAN-OS is deployed across SA banking, telco, and public sector edge infrastructure.¹

Story 2 — Pick n Pay / Bottles Confirmed Breach + Webworm China APT at SA University: Pick n Pay confirmed on 27–28 May that 2022-vintage customer data from the decommissioned Bottles platform is being trafficked on dark-web markets -- POPIA section 22 notification triggered, Information Regulator and SAPS notified. Separately, ESET published evidence (29 May) confirming **Webworm (China-aligned)** infiltrated an unnamed South African university using Discord-based EchoCreep and Microsoft Graph-based GraphWorm backdoors with data exfiltration to compromised AWS S3 -- the first publicly documented China-APT compromise of a SA academic institution.²³

Story 3 — Exchange OWA KEV Deadline 29 May PASSED (No Permanent Patch) + Supply Chain Triple: Exchange OWA CVE-2026-42897 (CVSS 8.1) KEV deadline of 29 May passed with **no permanent patch available** -- only EEMS Mitigation ID M2 protects on-prem Exchange. Permanent fix expected at Patch Tuesday 9 June. On the same day, CISA added a supply chain triple (DAEMON Tools, @tanstack npm, Nx Console VS Marketplace) in a single batch on 27 May -- deadline 10 June. Oracle simultaneously released a CVSS 10.0 unauthenticated RCE in Oracle REST Data Services (CVE-2026-46840) in its inaugural monthly CSPU on 28 May.⁴⁵

KPI Dashboard

Metric	Current (W23)	Prior (W22)	Change	Direction
SA threat level	HIGH	HIGH	Unchanged	FLAT
SA ransomware.live victims (total)	111	111	0 new W23	FLAT
New SA RW listings this week (ransomware.live)	0 confirmed	0 (W22)	FLAT	FLAT
New RW-adjacent leak sites (SA victims)	1 (Oday Syndicate/XL Africa)	N/A	NEW W23	UP
CISA KEV additions (W23)	~8 (PAN-OS, Trend Micro, supply chain triple + others)	11 (W22)	-3 net	DOWN
Confirmed SA data breaches (new W23)	1 (Pick n Pay/Bottles CONFIRMED)	0 confirmed (W22)	NEW	UP
Confirmed APT compromise of SA institution	YES -- Webworm/SA university (ESET 29 May)	None confirmed	NEW W23	UP
Active hacktivist campaigns vs SA	1 (#OpSouthAfrica, 17+ targets)	1 (#OpSA)	Expanded	UP
Exchange OWA permanent patch	NO permanent patch (EEMS M2 only)	NO (W22)	UNCHANGED	FLAT
PAN-OS GlobalProtect KEV deadline	19 June 2026 (mass exploit NOW)	N/A	NEW W23	UP
POPIA breach notifications (Pick n Pay)	Triggered -- IR + SAPS notified 28 May	None W22	NEW	UP
Patch Tuesday next	9 June 2026	--	Exchange OWA perm patch expected	FLAT

W23 KEY FRAMING: W23 marks the first confirmed China-APT compromise of a SA academic institution (Webworm) and the first confirmed SA retail data disclosure of the period (Pick n Pay/Bottles). The FLAT ransomware count (111) again masks real threat escalation: a new RaaS group (Oday Syndicate) launched its leak site and immediately listed an SA HR/logistics firm (XL Africa Group). The dominant operational threat remains the PAN-OS GlobalProtect mass-exploit window -- every SA organisation with a PAN edge device must treat this as an active emergency.

TOP 3 ACTIONS THIS WEEK

1. PAN-OS GLOBALPROTECT EMERGENCY PATCH: Audit all PAN-OS edge devices running versions 10.2, 11.0, 11.1, 11.2, 12.0, 12.1, or Prisma Access. Identify any use of authentication override feature. Deploy fixed versions immediately (KEV deadline 19 June -- mass exploitation already confirmed from 17 May via Rapid7 MDR). Hunt indicators from Vultr and Dromatics Systems source IPs. This is the single highest-priority action for any SA organisation with PAN edge infrastructure.

2. EXCHANGE OWA: HOLD M2 MITIGATION AND PREPARE PATCH TUESDAY 9 JUNE: Validate EEMS Mitigation ID M2 is active on all on-prem Exchange 2016/2019/SE servers (run Exchange Health Checker at aka.ms/ExchangeHealthChecker). The 29 May KEV deadline has passed with no permanent patch. Document OWA Light, Print Calendar, and inline image breakage for users. Pre-stage the 9 June Patch Tuesday change window -- Exchange OWA permanent patch expected.

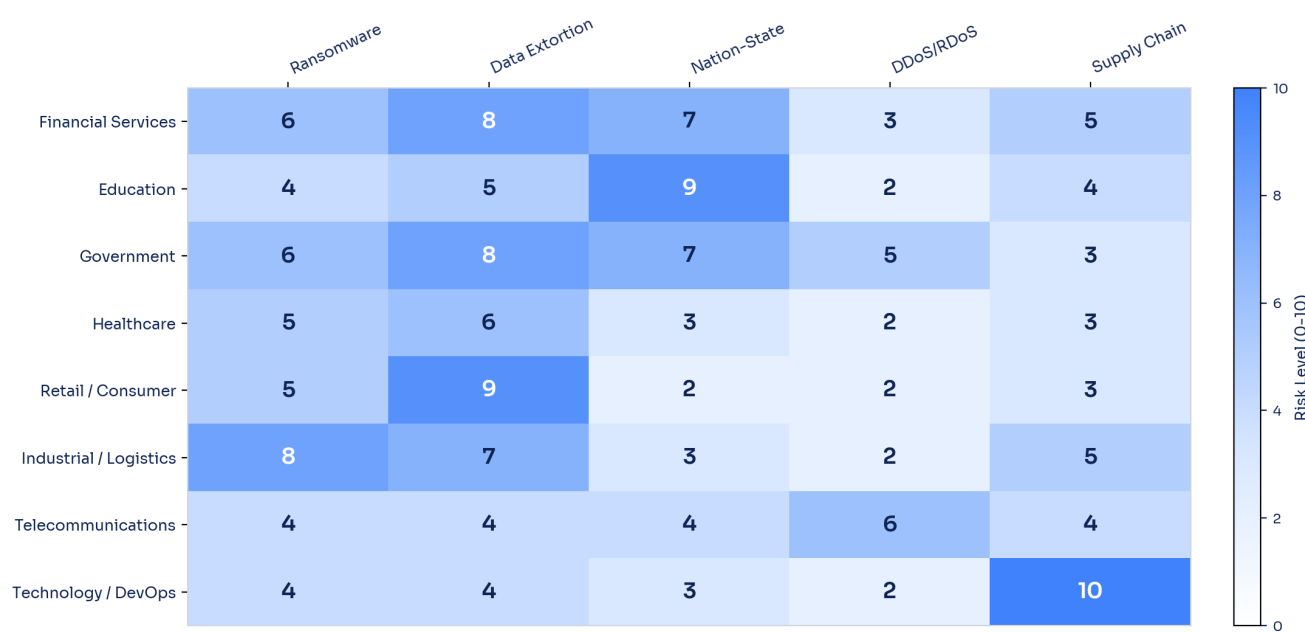
3. TREND MICRO APEX ONE OUT-OF-CYCLE PATCH (DEADLINE 4 JUNE): KEV-listed 26 May (CVSS 8.4). Directory traversal in on-prem Apex One server lets an admin-credentialed attacker poison the AV update channel -- endpoint protection becomes endpoint compromise. Patch management server immediately; verify update-channel signing integrity; audit recent agent updates for anomalies.

1. Rapid7 -- PAN-OS GlobalProtect auth bypass exploitation (CVE-2026-0257) — <https://www.rapid7.com/blog/post/etr-rapid7-observed-exploitation-of-pan-os-globalprotect-authentication-bypass-vulnerability-cve-2026-0257/>
2. MyBroadband -- Pick n Pay confirms Bottles data breach (27-28 May) — <https://mybroadband.co.za/news/security/>
3. ESET WeLiveSecurity -- Webworm Africa campaign (29 May 2026) — <https://www.welivesecurity.com/en/>
4. IntegSec -- Exchange OWA CVE-2026-42897 analysis — <https://integsec.com/blog/cve-2026-42897-exchange-owa-cross-site-scripting-spoofing-what-it-means-for-your-business-and-how-to-respond>
5. SecurityAffairs -- CISA KEV supply chain triple (27 May 2026) — <https://securityaffairs.com/192776/security/u-s-cisa-adds-daemon-tool-s-tanstack-and-nx-console-flaws-to-its-known-exploited-vulnerabilities-catalog.html>

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 23 (24–31 May 2026). **Technology/DevOps** spikes to 10 on Supply Chain following the DAEMON Tools / @tanstack / Nx Console KEV triple. **Education** rises to 9 on Nation-State following ESET's confirmed Webworm compromise of a SA university. **Retail/Consumer** spikes to 9 on Data Extortion following the Pick n Pay/Bottles confirmed disclosure. **Industrial/Logistics** rises on Ransomware following Oday Syndicate's listing of XL Africa Group and retrospective attribution of Sunspray Food Solutions to Storm-2697.

SA THREAT LANDSCAPE HEATMAP | W23 (24 May - 31 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 23 (24–31 May 2026): Zero new ransomware.live listings (SA tally holds at 111). Dominant stories: (1) Pick n Pay/Bottles confirmed data disclosure (first confirmed SA retail breach of the period); (2) Webworm China APT confirmed at SA university; (3) #OpSouthAfrica expands to 17+ targets; (4) Microsoft advisory on Storm-2697/The Gentlemen with retrospective SA victim attribution; (5) FSCA/SABRIC deepfake fraud warning; (6) Oday Syndicate new leak site with XL Africa.⁶

3.1 INC-2026-W23-01 — Pick n Pay / Bottles Platform Breach [CONFIRMED]

Sector	Retail / Consumer Goods
Dates	27–28 May 2026 (data disclosure confirmed; breach origin 2022)
Actor	Unknown dark-web sellers trafficking 2022-vintage Bottles app customer data
Data	Customer names, delivery addresses, partial card data, loyalty numbers (no full PANs, no CVVs per Pick n Pay)
Regulatory	POPIA s.22 notification trigger met; Information Regulator and SAPS notified 28 May
Company response	Forensic investigation under way; customer notification commenced
Confidence	CONFIRMED -- Pick n Pay issued public statement 28 May

Pick n Pay confirmed that data from its now-decommissioned Bottles on-demand alcohol ordering platform (operational 2019–2022) is being sold on dark-web markets. The Bottles platform was a separate mobile application with its own customer database -- Pick n Pay's core systems were not directly implicated. Data fields confirmed include customer names, delivery addresses, partial card data, and loyalty numbers. Pick n Pay confirmed no full PANs or CVVs are present. The Information Regulator and SAPS have been notified as required under POPIA. This is the first confirmed SA retail-side data disclosure of the W23 period.²

3.2 INC-2026-W23-02 — Webworm (China APT) -- SA University Compromise [CONFIRMED]

Actor	Webworm (China-aligned; overlaps with Space Pirates)
Sector	Higher Education / Academic Research
Target	Unnamed South African university (victim not disclosed by ESET)
Backdoors	EchoCreep (Discord-based C2); GraphWorm (Microsoft Graph API C2)
Exfiltration	Compromised AWS S3 bucket billed to victim organisation
Attribution basis	Infrastructure overlap with prior Webworm operations against Russia, Asia, Africa academic targets
Significance	First publicly documented China-APT compromise of a SA academic institution
Confidence	CONFIRMED (ESET vendor attribution, 29 May 2026); victim institution unnamed

ESET's WeLiveSecurity published the full technical breakdown on 29 May 2026. Webworm's dual-C2 architecture is operationally significant: EchoCreep uses Discord channels as command infrastructure (evading traditional domain-based blocking), while GraphWorm abuses legitimate Microsoft Graph API calls (blending with normal Office 365 traffic). Data exfiltration to a compromised AWS S3 bucket billed to the victim means forensic discovery is complicated by the absence of outbound traffic to attacker-controlled endpoints. All SA higher education institutions should hunt for Discord-to-host C2 traffic patterns and anomalous Microsoft Graph API call volumes.³

3.3 INC-2026-W23-03 — #OpSouthAfrica -- SARS / SITA Claims [DENIED]

Actor	Nullsec Nigeria (Anonymous Nigeria)
Claimed targets (W23)	SARS, SITA (posted Breached forum 23 May)
Sample data circulating	SARS taxpayer reference numbers; SITA configuration extracts
SARS response (25 May)	"These claims are false and unsubstantiated; no compromise of taxpayer data detected"
SITA response (25 May)	"Comprehensive investigation conducted; no anomalies detected in production systems"
Campaign scope	17+ claimed SA targets across 3 concurrent operations (data theft, DDoS extortion, ransomware)
Other confirmed circulating data	Stats SA 154 GB, ANC ~2M records, DCS 11 GB (data circulating; victim acknowledgement pending)
Confidence	UNVERIFIED (SARS and SITA actively denied)

The #OpSouthAfrica campaign continues to expand in scope. Black Matter-signed DDoS extortion infrastructure mapping is the most analytically concerning element -- it suggests the hacktivist wave may be providing target mapping for follow-on criminal operations. The SARS and SITA denials were formal and issued promptly. Unverified data continues to circulate for multiple other entities. The campaign should be tracked at Nullsec Nigeria / 404 Crew Telegram channels.⁷⁸

3.4 INC-2026-W23-04 — Storm-2697 / "The Gentlemen" RaaS -- Africa Campaign [CONFIRMED]

Actor	Storm-2697 / "The Gentlemen" (Go-based self-propagating RaaS)
Advisory	Microsoft Threat Intelligence, 28 May 2026
SA victim	Sunspray Food Solutions (March 2026 attack retrospectively attributed)
TTPs	Self-propagating Go-based RaaS; 21 lateral-movement techniques per host; file extension .umcl6h
Key risk	Self-propagation negates standard "isolate patient zero" containment playbooks
IOCs	3 SHA-256 hashes published by Microsoft
Target region	Africa explicitly listed in advisory
Confidence	CONFIRMED (Microsoft attribution, 28 May 2026)

The self-propagating capability of Storm-2697/The Gentlemen is the defining operational risk: once a single host is compromised, the malware traverses the network autonomously using 21 documented lateral-movement techniques, making traditional containment ("isolate patient zero") ineffective without comprehensive network segmentation. The retrospective attribution of the March 2026 Sunspray Food Solutions incident confirms Storm-2697's presence in SA. All SA organisations should validate network segmentation maturity as a defence against self-propagating ransomware.⁹

3.5 INC-2026-W23-05 — FSCA/SABRIC Deepfake Investment Fraud Warning [CONFIRMED]

The FSCA and SABRIC issued a joint formal warning on 29 May regarding deepfake-enabled impersonation of SA public figures for fraudulent investment platforms. Confirmed impersonations: President Ramaphosa, Patrice Motsepe, Deputy President Mashatile. Digital banking fraud rose 86% in 2024; app fraud losses exceeded R1.2B (SABRIC data). FSCA identified at least 14 active fraudulent platforms using deepfake video as the primary recruitment lure. Financial services firms should brief clients and implement deepfake-detection training in financial advisory workflows.¹⁰

3.6 INC-2026-W23-06 — Oday Syndicate New Leak Site -- XL Africa Group Listed [CLAIMED]

Actor	Oday Syndicate (new ransomware group; TTPs not yet publicly mapped)
Event	New leak site launched 28 May 2026
SA victim listed	XL Africa Group (HR / logistics / cash-management outsourcer; pan-African operations)
Time to first SA victim	Within 24 hours of site launch
Total W23 victims	5 (XL Africa highest-profile)
Confidence	CLAIMED (XL Africa not yet publicly acknowledged)

The rapid debut of a SA victim within 24 hours of the Oday Syndicate launch suggests the group either had pre-existing access to XL Africa's systems before launching its site, or specifically targeted a SA entity for high-visibility debut. XL Africa's role as an HR, logistics, and cash-management outsourcer with pan-African operations means the breach -- if confirmed -- could expose data from multiple downstream clients.¹¹

3.7 Ongoing / Continuation Incidents (W23 Status)

Incident	W23 Status
Standard Bank / ROOTBOY	DEVELOPING -- IR investigation continues; 1.2 TB cumulative public dumps; no new bank statement W23.
Polmed 1.7M / 214 GB (ShinyHunters)	STILL DEVELOPING -- no Polmed public statement W23; forensic probe ongoing.
Telkom SA (unidentified actor)	UNVERIFIED -- claimed ~28 May; Telkom denied; flag for W24 follow-up.
SA sports club 674K records (~28 May)	UNVERIFIED -- 674,000-record breach alleged per Data Breaches Digest; primary source unconfirmed; flag for W24.
SANBS / KillSec + ANC "Black Ax"	STILL UNVERIFIED -- carried from W21-W22; no victim acknowledgement.
Black Matter DDoS wave (W22)	Post-mortem phase -- no new attacks W23; CISO panel at ITWeb Cape Town referenced extensively.

6. Cyble -- Oday Syndicate emergence and XL Africa listing (29-30 May 2026) — <https://cyble.com/blog/>
7. Daily Maverick -- #OpSouthAfrica expanded targets — <https://www.dailymaverick.co.za/>
8. ITWeb -- SARS, SITA deny breach claims (25 May 2026) — <https://www.itweb.co.za/>
9. Microsoft Security Blog -- Storm-2697 / The Gentlemen advisory (28 May 2026) — <https://www.microsoft.com/security/blog/>
10. FSCA -- Public warning on deepfake investment fraud (29 May 2026) — <https://www.fsca.co.za/>
11. Cyble -- Oday Syndicate first SA victim XL Africa Group — <https://cyble.com/blog/>

4. GLOBAL INCIDENTS WITH SA RELEVANCE

Storm-2697 / "The Gentlemen" -- Africa in Scope (Microsoft, 28 May)

Full technical breakdown confirmed Africa-region targeting. Go-based self-propagating RaaS with 21 lateral-movement techniques per host. Sunspray Food Solutions (SA) retrospectively attributed. SA organisations should treat Storm-2697 as an active regional threat requiring network-segmentation maturity assessment.⁹

Lazarus (DPRK) -- axios npm library compromise (ESET retrospective)

ESET Q4 2025–Q1 2026 retrospective confirmed Lazarus' Operation DangerousPassword compromised the axios npm library (100M+ weekly downloads). Any SA fintech that used axios via npm during the exposure window may have been affected. Rotate API keys and credentials for any JavaScript project that consumed axios during the affected period.¹²

Multinational VPN Seizure for Ransomware Infrastructure (W23)

France, Netherlands, Ukraine, UK, Switzerland, and Luxembourg coordinated the first multinational VPN takedown targeting infrastructure used by 25+ ransomware groups including Avaddon. SA NPA reportedly briefed. Follow-on enforcement actions may disrupt C2 channels used by groups with SA victims.¹³

SideWinder -- African Nuclear and Maritime Escalation (WhoisXML, 27–29 May)

SideWinder (suspected India APT) escalated activity against African nuclear facilities and Djibouti/Egypt maritime infrastructure. NCC CSIRT P1 follow-up issued. SA nuclear and maritime operators should review SideWinder IOC blocks from W22 advisory. Discord C2 and Microsoft Graph C2 patterns (overlap with Webworm TTPs) require active hunting.¹⁴

Ghost CMS CVE-2026-26980 -- 700+ Compromised Sites, ClickFix Campaign

February 2026 SQLi (patched 3 months ago) now under mass exploitation by two competing threat clusters. Notable compromised hosts: Harvard, Oxford, DuckDuckGo. Visitors to compromised Ghost-hosted blogs are served ClickFix fake CAPTCHA leading to PowerShell C2 malware. SA users visiting any compromised Ghost-hosted blog are at risk regardless of internal stack.¹⁵

12. ESET -- Lazarus Operation DangerousPassword axios npm compromise (May 2026) — <https://www.welivesecurity.com/en/>

13. SecurityAffairs -- Multinational VPN infrastructure takedown (W23) — <https://securityaffairs.com/>

14. WhoisXML -- SideWinder African nuclear escalation (27–29 May 2026) — <https://main.whoisxmlapi.com/>

15. The Hacker News -- Ghost CMS CVE-2026-26980 ClickFix campaign — <https://thehackernews.com/2026/05/ghost-cms-cve-2026-26980-exploited-to.html>

5. THREAT ACTORS

5.1 Webworm (China APT) — SA University Compromise CONFIRMED (ESET 29 May)

Webworm (China-aligned; infrastructure overlaps with Space Pirates) confirmed compromise of an unnamed South African higher-education institution. TTPs: EchoCreep backdoor uses Discord channels as C2 (evades domain-based blocking); GraphWorm abuses Microsoft Graph API (blends with Office 365 traffic); data exfiltrated to compromised AWS S3 bucket billed to victim. ESET attribution based on overlapping infrastructure with prior Webworm operations against Russia, Asia, and Africa academic targets. This is the **first publicly documented China-APT compromise of a SA academic institution**. All SA HE institutions should hunt Discord C2 and Graph API anomalies.³

Type	Indicator
Backdoor	EchoCreep -- Discord-channel C2 (commands embedded in Discord messages)
Backdoor	GraphWorm -- Microsoft Graph API C2 (uses legitimate MS Graph calls for beaconing)

Type	Indicator
Exfil destination	Compromised AWS S3 bucket billed to victim (forensic obfuscation)
Hunting signal	Anomalous Discord traffic from server-side processes; unexpected MS Graph API volume from non-Office user contexts
Threat group	Webworm / Space Pirates overlap; China-aligned; prior Africa academic targeting documented

5.2 Storm-2697 / "The Gentlemen" — Self-Propagating RaaS; SA Victim Confirmed

Microsoft advisory (28 May): Storm-2697 is a self-propagating Go-based RaaS operator with 21 documented lateral-movement techniques per compromised host. File extension .umc16h. The self-propagation negates standard "isolate patient zero" containment -- the entire network must be treated as compromised once initial access is achieved. Sunspray Food Solutions (SA food manufacturer) confirmed as a March 2026 victim. Africa explicitly listed as target region. Three SHA-256 IOCs published.⁹

5.3 Oday Syndicate — New RaaS Group; XL Africa Group Listed W23

New ransomware leak site "Oday Syndicate" launched 28 May 2026. XL Africa Group (HR, logistics, cash-management outsourcer with pan-African operations) listed within 24 hours of debut. Five total victims posted in W23. Group TTPs not yet publicly mapped. The rapid debut of a SA victim suggests either pre-existing access or deliberate SA targeting for high-visibility launch. Monitor Oday Syndicate site for additional SA victims; track TTP documentation as group matures.⁶¹¹

5.4 Threat Actor Summary — W23

Actor	Type	Notable W23 Activity	Source
Webworm (China APT)	State espionage	Confirmed SA university compromise; EchoCreep (Discord C2) + GraphWorm (MS Graph C2); AWS S3 exfil	ESET 29 May
Storm-2697 / The Gentlemen	RaaS	Microsoft advisory; self-propagating Go-based; Sunspray SA victim; Africa region named	Microsoft 28 May
Oday Syndicate	New RaaS crew	Debut 28 May; XL Africa Group listed within 24h; 5 W23 victims	Cyble 29-30 May
Nullsec Nigeria (Anonymous Nigeria)	Hacktivist	SARS/SITA claims 23 May (denied 25 May); 17+ campaign targets across 3 concurrent operations	Breached forum, Daily Maverick
SideWinder (suspected India APT)	State espionage	Escalation against African nuclear plants + Djibouti/Egypt maritime; NCC CSIRT P1 follow-up	WhoisXML 27-29 May
Lazarus (DPRK)	State-aligned	ESET retrospective: Operation DangerousPassword compromised axios npm (100M+ weekly DL)	ESET May 2026
UAT-8616 (suspected China)	State-aligned	Continues Cisco Catalyst SD-WAN exploitation (CVE-2026-20182, CVSS 10.0); no workaround other than patch	Talos ongoing
ROOTBOY	Criminal	Standard Bank dumps continue; 1.2 TB cumulative public; no new disclosures W23	ITWeb tracking
GINES (Makop family)	Ransomware	CYFIRMA 29 May full TTP breakdown; Africa-aware targeting documented	CYFIRMA
NWH Stealer	Infostealer	14 SHA-256 IOCs published by CYFIRMA 29 May	CYFIRMA
Screening Serpens / UNC1549	Iran APT	New IOCs published W23; finance-sector targeting	CYFIRMA

5.5 Notable Law Enforcement Action (W23)

First multinational VPN seizure for ransomware infrastructure: France, Netherlands, Ukraine, UK, Switzerland, and Luxembourg coordinated a takedown of VPN infrastructure used by 25+ ransomware groups including Avaddon. Operation continues; SA NPA reportedly briefed. This represents the first coordinated international action specifically targeting ransomware group persistence channels rather than the ransomware operators themselves.¹³

12. ESET -- Lazarus Operation DangerousPassword npm compromise retrospective (May 2026) — <https://www.welivesecurity.com/en/>

13. SecurityAffairs -- VPN ransomware infrastructure takedown (W23) — <https://securityaffairs.com/>

14. WhoisXML -- SideWinder African nuclear + maritime escalation — <https://main.whoisxmlapi.com/>

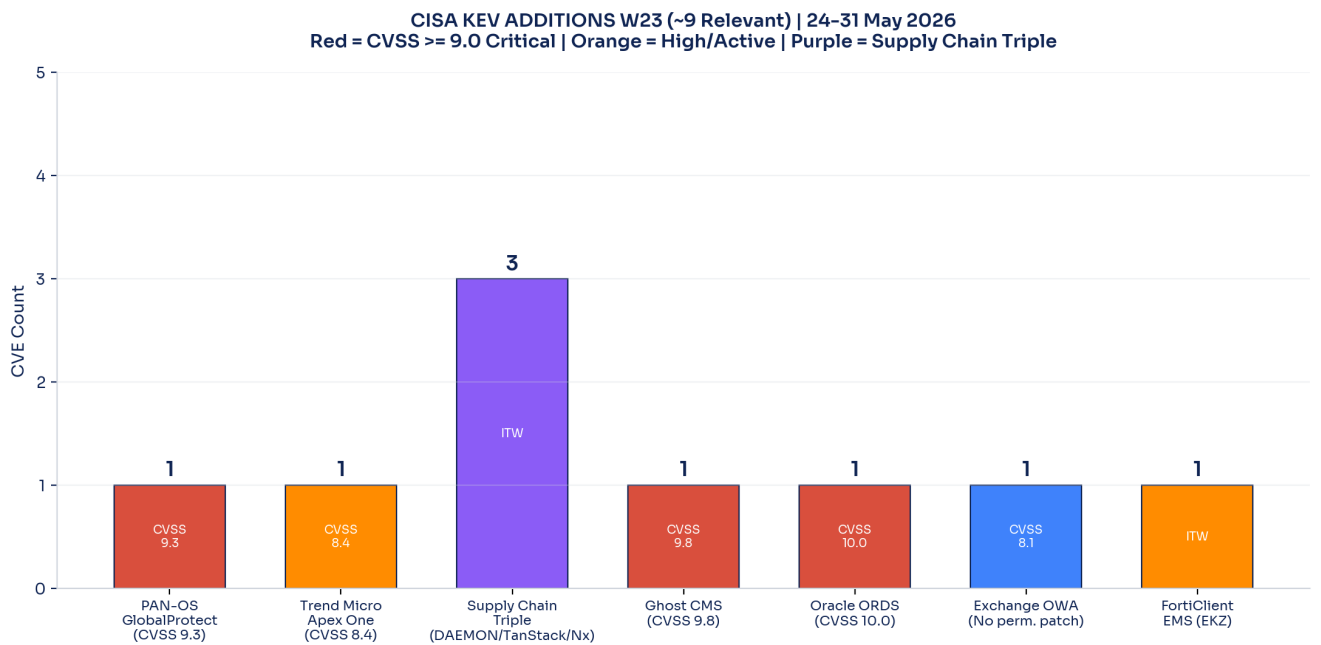
15. The Hacker News -- Ghost CMS ClickFix mass exploitation —

<https://thehackernews.com/2026/05/ghost-cms-cve-2026-26980-exploited-to.html>

6. CRITICAL VULNERABILITIES & CISA KEV

CISA added approximately **8 CVEs** to the KEV catalog in W23, headlined by PAN-OS GlobalProtect CVE-2026-0257 (29 May) and Trend Micro Apex One CVE-2026-34926 (26 May), plus a triple supply-chain entry on 27 May. The Exchange OWA CVE-2026-42897 KEV deadline of 29 May passed with no permanent patch. Oracle released a CVSS 10.0 unauthenticated RCE (CVE-2026-46840) in its inaugural monthly CSPU. Two Linux LPE PoC pairs with Metasploit modules were also published.⁴⁵

W23 CISA KEV Additions — Distribution by Category (~9 Total)



W23 CISA KEV / Critical CVE Tracking (24-31 May 2026)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-0257	Palo Alto / PAN-OS GlobalProtect	9.3	Auth bypass	19 Jun 2026	KEV 29 May; ITW mass-exploit from 17 May; Vultr + Dromatics source IPs
CVE-2026-42897	Microsoft / Exchange Server OWA (2016, 2019, SE)	8.1	XSS/Spoofing	29 May (PASSED)	NO permanent patch; EEMS M2 only; perm fix expected PT 9 Jun
CVE-2026-34926	Trend Micro / Apex One (on-prem)	8.4	Directory traversal	4 Jun 2026	KEV 26 May; AV update channel poisoning; endpoint compromise
CVE-2026-46840	Oracle / REST Data Services (ORDS)	10.0	Unauth RCE	Apply ASAP	Patched 28 May (CSPU); cascades to backend Oracle DB
CVE-2026-31431	Linux kernel / "Copy Fail"	7.8	LPE	Patch + reboot	Public PoC + Metasploit; Kubernetes container escape
CVE-2026-46333	Linux kernel / "ssh-keysign-pwn"	7.8	LPE	Patch + reboot	ptrace SSH key theft + /etc/shadow; public PoC + Metasploit
CVE-2026-26980	Ghost CMS	9.8	SQLi to RCE	Patched Feb 2026	Mass-exploit NOW; 700+ compromised sites; ClickFix campaign
DAEMON Tools supply chain	(multi-vendor)	n/a	Supply chain	10 Jun 2026	KEV 27 May; trojanized signed installer; legitimate cert abused
@tanstack npm packages	npm ecosystem	n/a	Supply chain	10 Jun 2026	KEV 27 May; 84 malicious versions (Query, Router, Form, Table)
Nx Console VS Marketplace	VS Marketplace	n/a	Supply chain	10 Jun 2026	KEV 27 May; malicious version live 36 min; audit exposure window
CVE-2026-35616	Fortinet / FortiClient EMS	High	EKZ Infostealer delivery	KEV Apr	W22-W23 exploit wave (Arctic Wolf); patches 7.4.5/7.4.6/7.4.7

Pattern note: W23 introduces a "weaponised update channel" pattern: both Trend Micro Apex One (AV poisoning) and FortiClient EMS (EKZ Infostealer via Fortinet patches) turn the endpoint security management plane into an attack delivery mechanism. Any organisation running these products must verify update-channel integrity as an incident response priority, not just as a patch action.

6.1 PAN-OS GlobalProtect CVE-2026-0257 (CVSS 9.3, KEV 29 May)

Authentication override cookie forgery vulnerability allows unauthenticated VPN access via GlobalProtect. Affected: PAN-OS 10.2, 11.0, 11.1, 11.2, 12.0, 12.1, and Prisma Access. Rapid7 MDR confirmed mass exploitation from 17 May across multiple customers, with two distinct attack waves from Vultr and Dromatics Systems hosting. SA relevance is CRITICAL -- PAN-OS is deployed across SA banking, telco, and public sector edge infrastructure. Patch immediately to fixed versions; or disable auth override feature as interim mitigation.¹

6.2 Prior KEV Status -- W22 Carryover Deadlines (W23 Status)

CVE	Status W23
Cisco SD-WAN CVE-2026-20182 (CVSS 10.0)	UAT-8616 still actively exploiting per Talos; SA telco patch state UNKNOWN -- treat as urgent P1
Ivanti EPMM CVE-2026-1281 (~9.8)	KEV deadline 27 May PASSED; exploitation continuing; patch immediately if not done
Drupal CVE-2026-9082	KEV deadline 27 May PASSED; 15K+ attempts/day baseline; patch or upgrade immediately
cPanel LiteSpeed CVE-2026-48172 (CVSS 10.0)	Patches 2.4.7 deployed by major SA hosts (Xneelo, 1-Grid confirmed); residual risk on smaller resellers

EXCHANGE OWA CVE-2026-42897 -- KEV DEADLINE 29 MAY PASSED (ACTION REQUIRED)

Status: KEV deadline 29 May 2026 has PASSED. No permanent patch as of 31 May. EEMS Mitigation ID M2 is the ONLY available protection.

Mitigation verification: Run Exchange Health Checker (aka.ms/ExchangeHealthChecker). Confirm Mitigation ID M2 listed as active. For air-gapped environments: use Exchange On-premises Mitigation Tool via elevated Exchange Management Shell.

Known M2 breakage: OWA Print Calendar, inline images in OWA, OWA Light (?layout=light), IE-mode users remain unprotected. Document these limitations with users pending permanent patch.

Permanent patch expected: Patch Tuesday 9 June 2026. Pre-stage change window now. Preview is expected to be light this week.

6.3 Supply Chain Triple KEV (27 May, Deadline 10 June)

- **DAEMON Tools (signed installer):** Legitimate code-signing certificate abused to distribute trojanized installers of the DAEMON Tools disk image utility. Any system where DAEMON Tools was installed in May 2026 should be treated as potentially compromised.⁵
- **@tanstack npm packages:** 84 malicious versions published across TanStack Query, Router, Form, and Table packages. The TanStack ecosystem is widely used in React and Vue applications. Audit package-lock.json files for affected version ranges; rotate developer credentials and API keys.⁵
- **Nx Console VS Marketplace extension:** A malicious version of the Nx Console VS Code extension was live in the VS Marketplace for 36 minutes. Download count not disclosed. Developers who updated the extension during the exposure window should rotate all credentials accessible from that development environment.⁵

4. IntegSec -- Exchange OWA CVE-2026-42897 no permanent patch — <https://integsec.com/blog/cve-2026-42897-exchange-owa-cross-site-scripting-spoofing-what-it-means-for-your-business-and-how-to-respond>

5. SecurityAffairs -- CISA KEV supply chain triple (27 May 2026) — <https://securityaffairs.com/192776/security/u-s-cisa-adds-daemon-tool-s-tanstack-and-nx-console-flaws-to-its-known-exploited-vulnerabilities-catalog.html>

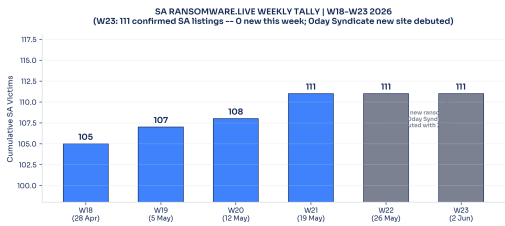
16. HelpNetSecurity -- Trend Micro Apex One CVE-2026-34926 actively exploited — <https://www.helpnetsecurity.com/2026/05/26/actively-exploited-trend-micro-apex-one-flaw-cve-2026-34926/>

- 17. Belgium CCB -- Oracle multi-product advisory (CVE-2026-46840) — <https://ccb.belgium.be/advisories/warning-multiple-vulnerabilities-oracle-products-patch-immediately-0>
- 18. CIQ -- CVE-2026-31431 Copy Fail Linux LPE — <https://ciq.com/blog/cve-2026-31431-copy-fail>
- 19. Bytelota -- CVE-2026-46333 Linux ssh-keysign-pwn — <https://byteiota.com/cve-2026-46333-linux-pttrace-ssh-keys/>
- 20. SecurityAffairs -- FortiClient EMS CVE-2026-35616 EKZ Infostealer — <https://securityaffairs.com/192817/malware/cve-2026-35616-forticlient-ems-flaw-actively-exploited-in-malware-attacks.html>

7. RANSOMWARE LANDSCAPE

SA ransomware.live victim count remains at **111 cumulative (FLAT)** for W23, with **zero new listings** on the ransomware.live tracker during 24–31 May 2026. However, this metric does not capture the debut of **Oday Syndicate** -- a new ransomware operator that launched its leak site on 28 May and immediately listed **XL Africa Group** (SA HR/logistics/cash-management outsourcer) within 24 hours. The FLAT official count again masks real-world threat activity.⁶

SA Contextualisation: The FLAT count is now a two-week streak (W22 and W23 both FLAT at 111). This should not be interpreted as a reduction in ransomware risk -- it reflects the absence of new ransomware.live listings rather than the absence of attacks. The Oday Syndicate debut with XL Africa confirms active interest in SA targets. The Storm-2697/The Gentlemen advisory (Microsoft, 28 May) demonstrates the SA landscape includes a self-propagating ransomware variant already responsible for at least one confirmed SA victim (Sunspray Food Solutions).⁹



End W22 baseline	111 confirmed SA listings
New W23 listings (24–31 May)	0 confirmed on ransomware.live
End W23 count	111 (FLAT)
New leak sites with SA victims (W23)	Oday Syndicate -- XL Africa Group (claimed, 28 May)
Most recent ransomware.live listing	Standard Bank Group / PrinzEugen (4 May 2026)

6. Cyble -- Oday Syndicate new leak site and XL Africa listing (29–30 May 2026) — <https://cyble.com/blog/>

8. OSINT EXPOSURE & ATTACK SURFACE

PAN-OS GlobalProtect mass exploit -- emergency hunting required

Two distinct attack waves observed from Vultr and Dromatics Systems source IPs (per Rapid7 MDR). Any SA organisation with PAN-OS 10.2/11.x/12.x edge devices should immediately verify auth override feature status and hunt for anomalous GlobalProtect session cookies. KEV deadline 19 June.¹

Pick n Pay / Bottles -- dark-web data circulating

2022-vintage Bottles customer data (names, delivery addresses, partial card data, loyalty numbers) is actively circulating on dark-web markets. Retailers and financial services firms with data-sharing arrangements with Pick n Pay should assess downstream exposure risk. Credential-stuffing attempts using email/partial card combinations are the primary downstream risk.²

Webworm Discord + MS Graph C2 -- active hunting required

Webworm confirmed to use Discord channels as C2 and Microsoft Graph API calls for beaconing. Standard perimeter blocks (domain-based) will not catch either vector. Hunt: anomalous Discord traffic from server-side processes; unexpected MS Graph API call volume from non-user contexts; AWS S3 bucket creation or access from server-side processes.³

Oday Syndicate -- XL Africa Group; pan-African supply chain exposure

XL Africa Group (HR, logistics, cash management) operates across multiple African countries. Breach of their systems could expose HR data, payroll data, and cash-management records for numerous downstream client organisations. Monitor for XL Africa Group data on dark-web markets; review any data-sharing agreements.⁶¹¹

Supply chain triple (DAEMON Tools / @tanstack / Nx Console) -- developer toolchain audit

All three KEV-listed supply chain CVEs from 27 May target developer and IT toolchains. Audit developer asset inventories for DAEMON Tools installations, @tanstack npm package consumption (check package-lock.json for affected version ranges), and Nx Console VS Code extension installations in May. Rotate all developer credentials and API keys where exposure is possible.⁵

Storm-2697 IOCs -- self-propagating detection

Three SHA-256 IOCs published by Microsoft (28 May). File extension .umcl6h is a detection signal. Network segmentation maturity is the primary defence against self-propagating ransomware. Map east-west movement controls; validate that endpoint isolation can be enforced at the host level without requiring network-side action.⁹

9. REGULATORY & COMPLIANCE

B15-2026 General Laws (AML/CFT) Amendment Bill — CIPC Fines Rise R1M to R10M (27 May)

The General Laws (AML/CFT) Amendment Bill (B15-2026) was tabled in the National Assembly on 27 May 2026. Key cyber and compliance implications: CIPC administrative fine ceiling rises from R1M to **R10M**; CIPC gains direct fine power (previously required court order); AML risk assessment required for new technologies; pre-FATF Mutual Evaluation mid-2026 positions SA for improved Financial Action Task Force standing. SA accountable institutions must expect board-level AML/CFT cyber posture reviews.²¹

Information Regulator -- IEC Voter-Data Warning (29 May)

The Information Regulator issued a public warning to the IEC and political parties on 29 May regarding voter-data protection ahead of 4 November 2026 local elections. POPIA obligations restated: purpose limitation, consent requirements, security measures, and breach notification. The IEC is to release a draft Misinformation Code. SA organisations that process voter data or work with election-technology vendors should conduct a POPIA compliance review.²²

DCDT AI Policy Crisis -- Comment Deadline Shifted to January 2027 (26-28 May)

Two DCDT officials were suspended after AI-hallucinated references were discovered in the draft SA AI Policy document. An expert panel (chaired by Prof. Benjamin Rosman) has been constituted to revise the document. The public comment deadline has shifted from June 2026 to **January 2027**; Cabinet approval target is November 2026. SA organisations deploying AI should continue their comment preparation but adjust the timeline.²³

SARB Stablecoin Warning + 25bps Repo Rate Hike to 7.00% (28-29 May)

SARB Governor Kganyago warned that stablecoins could "break apart" financial systems, signalling continued SARB caution on crypto integration. The SARB MPC hiked the repo rate 25bps to 7.00% on 29 May -- the first rate hike since 2023. Crypto capital-flow regulation comment deadline extended to 30 June 2026; crypto now treated on par with gold and foreign currency under exchange control.²⁴

Other W23 Regulatory Developments

- **ITWeb Security Summit Cape Town (25-26 May):** RSA ID Plus Sovereign Deployment (data sovereignty IAM), NETSCOUT AI-attack track, BDO board governance session completed. Johannesburg leg expected 2-4 June with SARB/SITA content.²⁵
- **ENISA NIS360 2026 (28 May):** Risk zone (high criticality, below-average maturity) sectors: health, railway, maritime, ICT management, space, public admin, water. High maturity sectors: banking, electricity, telecoms, trust services, FMIs, aviation. SA critical infrastructure operators should benchmark against ENISA maturity findings.²⁶
- **NIS2 standard incident reporting templates (27 May):** Adopted at 39th Plenary (Cyprus); EU Commission to make mandatory via implementing act. ENISA to build unified NIS2/GDPR/DORA/eIDAS/CER reporting portal (operational late 2027 - mid-2028).²⁶
- **EU AI Act Digital Omnibus (7 May, confirmed W23):** High-risk obligations for Annex III (recruitment/credit/law enforcement) deferred to 2 December 2027; Annex I to 2 August 2028; chatbot disclosure 2 August 2026 UNCHANGED; watermarking/deepfake marking deferred to 2 December 2026.²⁷
- **UK DUAA (active 19 June 2026):** ICO fined Energy Prices Direct GBP160,000 for unsolicited marketing; age-assurance warning issued to platforms.²⁷
- **ISO 19011:2026 (May 2026):** Updated audit guidelines effective immediately; applies to ISO 27001 / 27701 / 42001 audit programmes.²⁶
- **SSA restructure (W23):** GILAA proclamation progressing; SSA to split into SA Intelligence Agency (domestic) and SA Intelligence Service (foreign) in FY2026/27.²⁵

Compliance Deadlines — W23 Forward View

Date	Item	Owner
4 Jun 2026	CISA KEV: Trend Micro Apex One CVE-2026-34926 deadline	IT
9 Jun 2026	Patch Tuesday -- Exchange OWA permanent patch EXPECTED	IT
10 Jun 2026	CISA KEV: Supply chain triple (DAEMON/TanStack/Nx) deadline	IT
19 Jun 2026	CISA KEV: PAN-OS GlobalProtect CVE-2026-0257 deadline	IT
19 Jun 2026	UK DUAA complaints-handling statutory duty active	Compliance
30 Jun 2026	SARB crypto capital-flow regs comment deadline	Compliance
30 Jun 2026	PAIA annual report (2024/25) via IR eServices	Privacy
2 Aug 2026	EU AI Act Art. 50 transparency obligations (chatbot disclosure)	Compliance
4 Nov 2026	SA Local Government Elections (voter-data POPIA obligations active)	Privacy
Jan 2027	SA AI Policy public comment window (revised deadline)	Compliance
2 Dec 2027	EU AI Act HRAIS (Annex III) obligations	Compliance

21. National Assembly -- B15-2026 General Laws (AML/CFT) Amendment Bill (27 May 2026) — <https://pmg.org.za/>
22. SA Information Regulator -- IEC voter-data public warning (29 May 2026) — <https://inforegulator.org.za/>
23. DCDT -- AI Policy crisis; officials suspended; expert panel constituted (26-28 May 2026) — <https://www.dcdt.gov.za/>
24. SARB -- MPC statement 29 May 2026; repo rate 7.00% — <https://www.resbank.co.za/>
25. ITWeb Security Summit Cape Town programme (25-26 May 2026) — <https://securitysummit.co.za/>
26. ENISA -- NIS360 2026 report (28 May 2026) — <https://www.enisa.europa.eu/>
27. EU Digital Strategy -- AI Act Digital Omnibus — <https://digital-strategy.ec.europa.eu/>

10. WEEKLY THREAT HUNT & IOCs

Eight hunt missions are active for W23. Three P1 missions address PAN-OS GlobalProtect emergency hunting, Exchange OWA M2 verification, and Trend Micro Apex One update-channel integrity. Three P2 missions address Webworm Discord/MS Graph C2 detection, Storm-2697 self-propagating ransomware network segmentation validation, and developer toolchain supply chain audit. Two P3 missions address FSCA deepfake exposure monitoring and Oday Syndicate/XL Africa dark-web monitoring.

TH-2026-W23-01 — PAN-OS GlobalProtect Auth Bypass Active Compromise Hunt

P1 — CRITICAL: KEV 29 May; mass exploitation confirmed from 17 May

Hypothesis: CVE-2026-0257 is under confirmed mass exploitation from 17 May. Any SA organisation with unpatched PAN-OS 10.2/11.x/12.x or Prisma Access may have already been compromised via forged authentication override cookies.

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

IOCs: Source IPs from Vultr ASN and Dromatics Systems ASN in GlobalProtect authentication logs; anomalous GlobalProtect session cookies from non-MFA-enrolled sources; unexpected VPN sessions from Vultr/Dromatics hosting IPs.

Data Sources: PAN-OS GlobalProtect authentication logs, Panorama security event logs, SIEM correlation for Vultr/Dromatics ASN source IPs, endpoint telemetry for post-VPN lateral movement.

Detection Guidance: Immediately audit GlobalProtect logs for sessions originating from Vultr ASN (AS20473) and Dromatics Systems. Review authentication override feature status. Hunt for post-auth-bypass lateral movement: unexpected SMB, RDP, WMI from VPN-assigned IPs. Patch to fixed PAN-OS versions without delay.

TH-2026-W23-02 — Exchange OWA EEMS M2 Verification and Exploitation Hunt**P1 — CRITICAL: KEV deadline 29 May PASSED; no permanent patch; ITW exploitation**

Hypothesis: The 29 May KEV deadline for CVE-2026-42897 has passed with no permanent patch. Organisations that have not confirmed EEMS Mitigation ID M2 are in active exploitation window.

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). Pre-stage 9 June PT patch window.

TH-2026-W23-03 — Trend Micro Apex One Update-Channel Integrity (CVE-2026-34926)**P1 — CRITICAL: KEV 26 May; deadline 4 Jun; AV plane becomes attack plane**

Hypothesis: CVE-2026-34926 allows an admin-credentialed attacker to poison the Apex One AV update channel, converting endpoint security into an endpoint compromise delivery mechanism. KEV deadline 4 June.

MITRE ATT&CK: T1195.002 (Supply Chain: Compromise Software Supply Chain), T1072 (Software Deployment Tools), T1562.001 (Disable Security Tools).

IOCs: Unexpected executable payloads distributed via Apex One update channel; anomalous admin credential usage on Apex One management server; unexpected outbound connections from Apex One agents to non-Trend infrastructure.

Data Sources: Apex One management server logs, update-channel signing verification, endpoint telemetry for agent-side update execution events.

Detection Guidance: Patch Apex One management server immediately. Verify update-channel signing: check that all distributed updates carry valid Trend Micro certificates. Audit recent agent update events for anomalies. Review admin credential usage on management server (credential rotation if any anomaly detected).

TH-2026-W23-04 — Webworm Discord + MS Graph C2 Detection**P2 — HIGH: ESET confirmed SA university compromise 29 May**

Hypothesis: Webworm (China APT) confirmed compromise of a SA university using Discord and Microsoft Graph as C2 channels. These are legitimate services not blocked by standard perimeter controls -- any SA HE institution or research body may be targeted.

MITRE ATT&CK: T1102 (Web Service: C2 via legitimate web service), T1071.001 (Application Layer Protocol: Web Protocols), T1048 (Exfiltration over Alternative Protocol).

IOCs: EchoCreep: Discord API calls (discord.com/api) from server-side or non-interactive user processes; anomalous Discord message frequency from server processes. GraphWorm: Microsoft Graph API calls (graph.microsoft.com) from server-side processes with no corresponding user session.

Data Sources: Network proxy/firewall logs for Discord and Graph API traffic, endpoint process-to-network correlation, AWS S3 bucket creation/access logs, SIEM correlation.

Detection Guidance: Alert on discord.com/api traffic from server-side processes (not associated with a logged-in user session). Alert on graph.microsoft.com calls from processes running as SYSTEM or service accounts outside normal Office 365 traffic patterns. Review AWS S3 bucket access logs for any buckets created by server-side processes.

P2 — HIGH: Sunspray SA victim confirmed; self-propagating ransomware active

TH-2026-W23-05 — Storm-2697 Network Segmentation Validation

Hypothesis: Storm-2697 ("The Gentlemen") is self-propagating with 21 lateral-movement techniques. Standard "isolate patient zero" playbooks are ineffective. SA organisations must validate network segmentation maturity before experiencing an incident.

MITRE ATT&CK: T1570 (Lateral Tool Transfer), T1021 (Remote Services), T1018 (Remote System Discovery).

IOCs: .umc16h file extension on encrypted files; three SHA-256 IOCs published by Microsoft (28 May); anomalous east-west SMB, WMI, RDP, and scheduled task creation from unexpected source hosts.

Data Sources: Network flow data for east-west traffic, endpoint file creation events, SIEM east-west movement correlation, EDR process tree for lateral movement TTPs.

Detection Guidance: Alert on .umc16h file extension creation events. Validate network micro-segmentation: can an endpoint be isolated at the host level without requiring network-side ACL changes? Confirm east-west SMB is blocked between endpoint VLANs. Hunt for anomalous scheduled task creation from unexpected source hosts.

P2 — HIGH: KEV 27 May; developer credential compromise risk

TH-2026-W23-06 — Developer Toolchain Supply Chain Audit (DAEMON / @tanstack / Nx Console)

Hypothesis: Three developer toolchain components were KEV-listed 27 May (DAEMON Tools signed installer, @tanstack npm packages [84 malicious versions], Nx Console VS Code extension [36-min exposure]). Any developer or IT environment where these were installed in May 2026 may have credential exposure.

MITRE ATT&CK: T1195.002 (Compromise Software Supply Chain), T1078 (Valid Accounts via stolen dev credentials).

IOCs: DAEMON Tools installer hash mismatch; @tanstack package versions in compromised range (check package-lock.json); Nx Console extension version 0.x during exposure window.

Data Sources: Developer workstation asset inventory, npm package-lock.json files, VS Code extension install history, developer credential audit trail.

Detection Guidance: Query asset inventory for DAEMON Tools installations dated May 2026. Search all JavaScript project package-lock.json files for @tanstack package versions in the affected range. Check VS Code extension installation history for Nx Console updates during the 36-minute exposure window. If any exposure confirmed: rotate all developer credentials, API keys, cloud access tokens, and SSH keys immediately.

P3 — MONITORING: FSCA formal warning 29 May; 14 active platforms identified

TH-2026-W23-07 — FSCA Deepfake Investment Fraud -- Staff and Client Awareness

Hypothesis: FSCA/SABRIC identified 14 active fraudulent platforms using deepfake video of SA public figures. Financial services staff and clients may be recruited into fraudulent schemes via deepfake lures on social media.

MITRE ATT&CK: T1598 (Phishing for Information), T1566 (Phishing), T1534 (Internal Spearphishing).

IOCs: Social media videos using deepfaked images of President Ramaphosa, Patrice Motsepe, or Deputy President Mashatile promoting investment platforms; non-FSCA-licensed investment platform domains; WhatsApp/Telegram group recruitment messages referencing these figures.

Data Sources: Staff phishing reports, social media monitoring, dark-web intelligence feeds, FSCA warnings portal.

Detection Guidance: Brief all client-facing financial advisory staff on deepfake investment fraud patterns. Verify any investment platform against FSCA register (fsc.co.za). Alert on social media mentions of named public figures in investment contexts originating from new or low-follower accounts. Report to FSCA hotline.

TH-2026-W23-08 — Oday Syndicate / XL Africa Group Dark-Web Monitoring

P3 — MONITORING:
Claimed 28 May; XL Africa not yet acknowledged

Hypothesis: XL Africa Group (HR/logistics/cash-management) is listed on the Oday Syndicate leak site as of 28 May. If confirmed, data from downstream client organisations may follow. Any organisation with a data-sharing relationship with XL Africa should monitor dark-web markets.

MITRE ATT&CK: T1078 (Valid Accounts via stolen XL Africa credentials), T1110.004 (Credential Stuffing).

IOCs: XL Africa Group data appearing on Oday Syndicate leak site; XL Africa employee credentials in infostealer feeds; HR/payroll data from XL Africa clients on dark-web markets.

Data Sources: Dark web intelligence feeds, HudsonRock infostealer telemetry, Oday Syndicate leak site monitoring, SIEM credential-stuffing detection.

Detection Guidance: Subscribe to dark-web monitoring for XL Africa Group data. If your organisation has a HR, payroll, or logistics outsourcing relationship with XL Africa: review credential exposure for any shared system access. Monitor authentication logs for credential-stuffing patterns sourced from XL Africa-derived credentials.

IOC Master Table — W23

Indicator	Type	Attribution	Hunt ID
Vultr ASN (AS20473) + Dromatics Systems IPs	ASN / IP range	CVE-2026-0257 PAN-OS exploit source (Rapid7 MDR)	TH-2026-W23-01
discord.com/api from server-side processes	Network pattern	Webworm EchoCreep C2 channel	TH-2026-W23-04
graph.microsoft.com from service-account processes	Network pattern	Webworm GraphWorm C2 channel	TH-2026-W23-04
.umc16h file extension	File extension	Storm-2697 / The Gentlemen ransomware	TH-2026-W23-05
3 SHA-256 IOCs (Microsoft 28 May advisory)	SHA-256 hashes	Storm-2697 / The Gentlemen	TH-2026-W23-05
CVE-2026-0257 (PAN-OS GlobalProtect)	CVE	KEV 29 May; mass exploit confirmed; deadline 19 Jun	TH-2026-W23-01
CVE-2026-42897 (Exchange OWA)	CVE	KEV 29 May PASSED; no perm patch; EEMS M2 only	TH-2026-W23-02
CVE-2026-34926 (Trend Micro Apex One)	CVE	KEV 26 May; AV update channel poisoning; deadline 4 Jun	TH-2026-W23-03
@tanstack package-lock.json entries (affected range)	Supply chain	84 malicious npm versions; KEV 27 May	TH-2026-W23-06
DAEMON Tools installer hash mismatch (May 2026)	File hash	Trojanized signed installer; KEV 27 May	TH-2026-W23-06
Nx Console VS Code extension (36-min window)	VS Marketplace	Malicious version exposure; KEV 27 May	TH-2026-W23-06

11. RECOMMENDATIONS

Immediate (This Week — Priority P1)

- 1. PAN-OS GlobalProtect emergency patch programme (KEV deadline 19 June; mass exploit confirmed):** Audit all PAN-OS 10.2/11.x/12.x and Prisma Access deployments. Identify auth override usage. Deploy fixed versions immediately. Hunt for Vultr ASN (AS20473) and Dromatics Systems source IPs in GlobalProtect authentication logs. Any session from those ASNs since 17 May should be treated as a potential compromise indicator.

- **2. Exchange OWA: validate EEMS M2 active; pre-stage 9 June Patch Tuesday:** Run Exchange Health Checker (aka.ms/ExchangeHealthChecker). Confirm Mitigation ID M2 listed. Document OWA breakage (Print Calendar, inline images, OWA Light) with users. Pre-stage the 9 June Patch Tuesday change window for permanent patch.
- **3. Trend Micro Apex One out-of-cycle patch (KEV deadline 4 June):** Patch Apex One management server immediately. Verify update-channel signing integrity. Audit all recent agent updates for anomalous payload distribution. Any endpoint that received an unexpected update payload since 26 May should be investigated.
- **4. Developer toolchain audit -- DAEMON Tools / @tanstack / Nx Console (KEV deadline 10 June):** Query developer asset inventory for DAEMON Tools May 2026 installations. Search JavaScript project package-lock.json files for @tanstack affected version ranges. Check VS Code extension history for Nx Console during 36-minute exposure window. If any exposure found: rotate all developer credentials, API keys, and cloud access tokens immediately.
- **5. Pick n Pay / Bottles: downstream credential and POPIA assessment:** Any organisation with data-sharing arrangements with Pick n Pay / Bottles should assess downstream exposure. Monitor dark-web markets for Bottles customer data being used for credential-stuffing against shared systems. Review any POPIA data-processing agreements with Pick n Pay.
- **6. Webworm / China APT SA university: sector-wide academic hunt:** All SA higher-education institutions and research organisations should hunt for Webworm IOCs. Block or alert on discord.com/api traffic from server-side processes; flag anomalous Microsoft Graph API call volumes from service accounts. Review AWS S3 bucket creation and access by server-side processes.
- **7. POPIA elections briefing (Information Regulator 29 May notice):** For clients with political-party data processing or election-technology relationships: conduct POPIA compliance review covering purpose limitation, consent, security measures, and breach notification readiness ahead of 4 November 2026 elections.

Short-Term (Next 30 Days)

- Patch Trend Micro Apex One by 4 June KEV deadline; patch supply chain triple (DAEMON/TanStack/Nx) by 10 June; patch PAN-OS by 19 June. Treat all three as emergency out-of-cycle actions.
- FATF Mutual Evaluation mid-2026: SA accountable institutions should expect CIPC fine ceiling escalation (R1M to R10M, B15-2026) to drive board-level AML/CFT cyber posture review. Begin gap assessment now.
- Prepare for ITWeb Security Summit Johannesburg leg (2-4 June): expect formal payment-system cyber circulars from SARB. Engage SARB crypto exchange-control comment process by 30 June deadline.
- Storm-2697 network segmentation maturity test: validate east-west movement controls; confirm endpoint isolation can be enforced at host level. Self-propagating ransomware requires a fundamentally different containment strategy.
- China APT (Webworm) sector-wide sweep: extend Discord C2 and MS Graph C2 hunting beyond the confirmed SA university to all SA academic and government research institutions.
- PAIA annual report (2024/25) due via IR eServices by 30 June 2026.
- SARB crypto capital-flow regulations comment deadline 30 June 2026.

Strategic (Next Quarter)

- China APT academic programme: Webworm's confirmed compromise of a SA university represents a new threat tier for SA higher education. Academic institutions hold sensitive research data, government partnerships, and student PII. A sector-wide IR capability programme for SA HE is warranted.

- Deepfake investment fraud: FSCA/SABRIC's identification of 14 active fraudulent platforms using deepfaked SA public figures signals that deepfake-enabled fraud is operational at scale. Financial services firms should invest in deepfake detection tooling for client-facing channels and conduct regular client awareness campaigns.
- Self-propagating ransomware readiness: Storm-2697's 21 lateral-movement techniques per host requires network segmentation maturity beyond simple VLAN segregation. Zero-trust micro-segmentation with host-level isolation capabilities is the strategic defence.
- POPIA breach notification readiness: the Pick n Pay/Bottles disclosure confirms that legacy data from decommissioned systems remains a POPIA liability. Organisations must maintain data inventories for decommissioned apps and ensure retention/deletion schedules are enforced.
- Supply chain trustworthiness programme: three separate supply chain vectors were KEV-listed in a single day (27 May). Developer toolchain integrity must be treated as a board-level risk: code signing verification, npm audit automation, and VS Marketplace extension allowlisting should be standard controls.

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. Rapid7 -- PAN-OS GlobalProtect CVE-2026-0257 exploitation (ETR) — <https://www.rapid7.com/blog/post/etr-rapid7-observed-exploitation-of-pan-os-globalprotect-authentication-bypass-vulnerability-cve-2026-0257/>
2. MyBroadband -- Pick n Pay confirms Bottles data breach (27-28 May 2026) — <https://mybroadband.co.za/news/security/>
3. ESET WeLiveSecurity -- Webworm Africa campaign (29 May 2026) — <https://www.welivesecurity.com/en/>
4. IntegSec -- Exchange OWA CVE-2026-42897 analysis and mitigation — <https://integsec.com/blog/cve-2026-42897-exchange-owa-cr-oss-site-scripting-spoofing-what-it-means-for-your-business-and-how-to-respond>
5. SecurityAffairs -- CISA KEV supply chain triple DAEMON Tools / TanStack / Nx Console (27 May 2026) — <https://securityaffairs.com/192776/security/u-s-cisa-adds-daemon-tools-tanstack-and-nx-console-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
6. Cyble -- Oday Syndicate new leak site emergence (29-30 May 2026) — <https://cyble.com/blog/>
7. Daily Maverick -- #OpSouthAfrica expanded targets (W23) — <https://www.dailymaverick.co.za/>
8. ITWeb -- SARS, SITA deny breach claims (25 May 2026) — <https://www.itweb.co.za/>
9. Microsoft Security Blog -- Storm-2697 / The Gentlemen technical advisory (28 May 2026) — <https://www.microsoft.com/security/blog/>
10. FSCA -- Public warning on deepfake investment fraud (29 May 2026) — <https://www.fsca.co.za/>
11. Cyble -- Oday Syndicate XL Africa Group listing (29-30 May 2026) — <https://cyble.com/blog/>
12. ESET -- Lazarus Operation DangerousPassword axios npm compromise retrospective (May 2026) — <https://www.welivesecurity.com/en/>
13. SecurityAffairs -- Multinational VPN ransomware infrastructure takedown (W23) — <https://securityaffairs.com/>
14. WhoisXML -- SideWinder Africa nuclear and maritime escalation (27-29 May 2026) — <https://main.whoisxmlapi.com/>
15. The Hacker News -- Ghost CMS CVE-2026-26980 ClickFix mass exploitation — <https://thehackernews.com/2026/05/ghost-cms-cve-2026-26980-exploited-to.html>
16. HelpNetSecurity -- Trend Micro Apex One CVE-2026-34926 actively exploited (26 May 2026) — <https://www.helpnetsecurity.com/2026/05/26/actively-exploited-trend-micro-apex-one-flaw-cve-2026-34926/>
17. Belgium CCB -- Oracle multi-product advisory CVE-2026-46840 (28 May 2026) — <https://ccb.belgium.be/advisories/warning-multiple-vulnerabilities-oracle-products-patch-immediately-0>
18. CIQ -- CVE-2026-31431 Linux Copy Fail LPE analysis — <https://ciq.com/blog/cve-2026-31431-copy-fail>
19. Bytelota -- CVE-2026-46333 Linux ssh-keysign-pwn ptrace analysis — <https://byteiota.com/cve-2026-46333-linux-pttrace-ssh-keys/>
20. SecurityAffairs -- FortiClient EMS CVE-2026-35616 EKZ Infostealer delivery — <https://securityaffairs.com/192817/malware/cve-2026-35616-forticlient-ems-flaw-actively-exploited-in-malware-attacks.html>
21. Parliament -- B15-2026 General Laws (AML/CFT) Amendment Bill (27 May 2026) — <https://pmg.org.za/>
22. SA Information Regulator -- IEC voter-data POPIA warning (29 May 2026) — <https://infoeregulator.org.za/>
23. DCDT -- AI Policy crisis: officials suspended; expert panel constituted (26-28 May 2026) — <https://www.dcdt.gov.za/>
24. SARB -- MPC statement: 25bps hike to 7.00% (29 May 2026) — <https://www.resbank.co.za/>
25. ITWeb Security Summit -- Cape Town 25-26 May 2026 programme — <https://securitysummit.co.za/>
26. ENISA -- NIS360 2026 sector maturity report (28 May 2026) — <https://www.enisa.europa.eu/>
27. EU Digital Strategy -- AI Act Digital Omnibus (confirmed W23) — <https://digital-strategy.ec.europa.eu/>
28. CISA KEV Catalog -- Known Exploited Vulnerabilities — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
29. Ransomware.live -- South Africa country map — <https://www.ransomware.live/map/ZA>
30. CYFIRMA -- Weekly Intelligence Report 29 May 2026 (GINES, NWH Stealer, Screening Serpens) — <https://www.cyfirma.com/news/>
31. SABRIC -- Digital banking fraud statistics 2024 (deepfake context) — <https://www.sabric.co.za/>
32. FSCA notices portal -- Financial Sector Conduct Authority — <https://www.fsca.co.za/>

-
33. Data Breaches Digest -- SA breach aggregator (W23) — <https://databreaches.net/>
34. ITWeb -- SA cybersecurity statistics 2026: 1,947 compromises +40% YoY — <https://www.itweb.co.za/>
35. ENISA -- NIS2 incident reporting templates adopted at 39th Plenary (27 May 2026) — <https://www.enisa.europa.eu/>
36. Tenable -- Cisco SD-WAN UAT-8616 ongoing exploitation FAQ — <https://www.tenable.com/blog/faq-about-the-continued-exploitation-of-cisco-catalyst-sd-wan-vulnerabilities-uat-8616>
-

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-W23 | Published Monday 1 June 2026