



SOUTH AFRICA

CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief, Week 44 | 18 October – 24 October 2026

THREAT LEVEL: HIGH

TLP: CLEAR

Report ID: SA-CTI-2026-W44 | Classification: TLP: CLEAR

Published Monday 26 October 2026

Compiled by Willem Steynberg – <https://www.linkedin.com/in/willem-steynberg-8a52234/>

Reviewed by Percy Kitso Sekate – <https://www.linkedin.com/in/percy-kitso-sekate/>

TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard
- 2. Threat Landscape Heatmap
- 3. Top SA Incidents (W44)
- 4. Threat Actors
- 5. Critical Vulnerabilities & CISA KEV
- 6. Ransomware Landscape
- 7. OSINT Exposure & Attack Surface
- 8. Regulatory & Policy
- 9. Weekly Threat Hunt & IOCs
- 10. Strategic Recommendations
- 11. Threat Level Assessment
- 12. OSINT Sources Consulted

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH, 27th consecutive week (18 October - 24 October 2026)

Story 1. Rand Mutual Assurance (RMA), the 1894-founded insurer that administers workplace injury and disease claims for the mining, iron and steel industries under COIDA, told MyBroadband and TechCentral on Friday 23 October that it "has received an alert about a data breach" and that investigations are under way.^{1,2} Behind the alert is an extortion listing: 366 GB, about 1.6 to 1.68 million claim records and 593,786 files, a demand of 95,000 to 98,000 US dollars and a deadline of 4 or 5 November. MyBroadband attributes it to the group Kazu and says it reviewed samples showing identity-document copies, claim forms, X-rays and medical certificates; TechCentral describes an unnamed hacker's forum post and had seen neither post nor sample. The aggregator this report relies on held no RMA record and showed Kazu unchanged at 20 victims, none South African.³ Rated PROBABLE: the company confirms an alert and a journalist has seen samples; the volumes are the actor's and are not adopted.

Story 2. Two PHP engine flaws leaked on Tuesday 20 October and patched on Wednesday 21 October, CVE-2026-109618 and CVE-2026-109619 (PHP2Shell, both 9.2 on CVSS 4.0), gave every internet-facing PHP server a window of unauthenticated code execution; Cloudflare counted millions of exploit attempts within a day and Amazon traced the first to Saturday 17 October.^{4,5,6} The Presidency took its website offline on Friday 23 October "as a precautionary measure in response to a global cybersecurity event", and TechCentral's test of more than 100 state websites found twelve of the seventeen that disclose a PHP version on an old release, eight of them on versions the PHP project no longer supports.⁷ Afrihost, Xneelo, 1-Grid and Absolute Hosting patched or mitigated their estates, and MyBroadband's Shodan search found more than 9,800 South African servers with a PHP banner; no South African compromise has been disclosed.⁸ The flaws were not in CISA's catalogue at its 23 October release; eight other entries were, led by a third exploited Arista VeloCloud Orchestrator flaw since July and a Plex Media Server chain against which 3,111 South African instances are exposed.^{9,10,11}

Story 3. The Information Regulator published three enforcement instruments on Friday 23 October with no statement. An enforcement notice under section 95 of POPIA against First National Bank records a security compromise FNB confirmed on 21 February 2022, in which the personal information of 88 data subjects was exposed to 696 unauthorised individuals and nine account numbers were accessed through a role-classification error; it finds five conditions contravened and gives FNB 90 days to report.^{12,13} A companion infringement notice fines FNB R1,000,000 under section 105(1), the account-number offence, for the nine; a third notice fines Central Johannesburg TVET College R500,000 for failing to comply with an earlier enforcement notice.^{14,15} The FNB fine is ten times what the regulator collected from the IEC and from Lancet Laboratories, and no coverage of it was located by Saturday 24 October.¹⁶ In the same week the IEC signed a disinformation partnership with Google, Meta, Microsoft, TikTok and Moxii Africa for the 4 November elections.¹⁷

W44 CORRECTION TO A PRIOR EDITION, one item. W43 did not carry The Foschini Group's investor notice of Tuesday 13 October, inside the W43 window, disclosing a cybersecurity incident identified on Sunday 11 October at TFG London, the group's United Kingdom business trading as Phase Eight, Hobbs and Whistles:

several IT systems unavailable while stores traded, UK authorities informed, customer-data impact not yet known, TFG Africa and TFG Australia on separate systems and unaffected.^{18,19} A JSE-listed South African group confirming an incident belongs in the incident list and the confirmations count, which for W43 should read three; it is rated CONFIRMED on the company's notice. The omission came from a media sweep that missed TechCentral's listing and is counted in the KPI row. No actor has claimed the incident and TFG had published no update by 24 October.

KPI Dashboard

Metric	Current (W44)	Prior (W43)	Change	Direction
Overall SA threat level	HIGH	HIGH	No change (27th week)	FLAT
ransomware.live SA cumulative	138	138	0	FLAT
SA claims discovered inside the window (ZA tag; passed the nationality check)	0	2	-2	DOWN
SA victims found under another country tag (hand search of active groups' pages)	0	0	0	FLAT
SA organisations confirming a breach or exposure in the window	0	3 (corrected from 2)	-3	DOWN
New CISA KEV additions	8	9	-1	DOWN
KEV adds already overdue at publication	3 of 8	7 of 9	-4	DOWN
KEV adds with a published VERIFIED SA exposure figure	4 of 8 (one product)	1 of 9	+3	UP
Corrections issued to prior editions	1	2	-1	DOWN

Five notes on the table. The victim feed returned the same 138 records on 25 October as on 18 October and the country page agreed; the RMA listing is a press-carried claim absent from the aggregator, so it falls in neither listing row and is counted in Section 3.^{20,21,3} The hand search read the 90 listings The Gentlemen, Krybit, Deadlock, Qilin and nOn indexed between 18 and 24 October and found nothing South African under any tag.^{22,23,24,25,26} The confirmations row reads zero because RMA has confirmed an alert, which is less than a breach, and the Presidency's outage was a precaution; the prior cell is corrected to three for TFG. Three of the eight catalogue additions were past their due date on Monday 26 October (SiteGuard and two Plex entries, due 23 October), two fell due on the publication day, and three carry 3 November dates.⁹ Four of the eight have a VERIFIED South African figure through one product, Plex Media Server at 3,111 (1,426 on port 32400), new to the panel this week; Arista, Collabora, SiteGuard and Siemens have no corroborated fingerprint.¹¹

W44 KEY FRAMING: the pressure this week came from outside the perimeter, with no new South African listing on the aggregator. A PHP engine flaw that touched most of the web was leaked before its patch, and the South African response was visible in two places: hosting companies mitigated before vendors published, and the Presidency switched its site off while its patch status was unverified. The wider state estate did not look like that; twelve of seventeen government sites that announce a PHP version announce an old one. For a board the question is whether the organisation can say, inside a day, which

internet-facing systems run which engine and who owns the patch. Rand Mutual Assurance is the other half of the week: an insurer holding a million mineworkers' claim files, with X-rays and identity documents in the sample a journalist saw, acknowledging an alert while an extortion clock runs to the first week of November. And the Information Regulator, whose media page carried nothing on Ampath, MIP or e-Panic when read on 25 October, published without a statement a R1 million fine and an enforcement notice against FNB for a security compromise confirmed in February 2022 and complained of in September 2022: the regulator does act on compromises, on a four-year clock, and the fine attached to the nine account numbers, an offence the Act singles out.

TOP 3 ACTIONS THIS WEEK

1. Close the PHP2Shell question by Tuesday 27 October and write the answer down. Inventory every internet-facing system that runs PHP, including appliances, control panels and vendor web interfaces; confirm 8.5.12, 8.4.27, 8.3.36 or 8.2.35, or the distribution's backported package by changelog; for anything on 8.1 or older, upgrade, take it offline, or put it behind a WAF with session.upload_progress.enabled set to 0, memory_limit set to -1 so applications cannot override it, and post_max_size kept low. Then hunt from 17 October, when exploitation began: PHP workers spawning shells or download tools, repeated HTTP 500 responses after oversized multipart requests, new files in web roots, new administrator accounts (TH-2026-W44-01). A server patched on 21 October may have been entered on the 20th.

2. If the organisation runs a GlobalProtect portal or a FortiGate, run the credential-market checks by Wednesday 28 October. Unit 42 has watched PAN-OS CVE-2026-0257 exploited since June and names Qilin and INC among the groups using it to open VPN sessions past MFA, and Group-IB ties a broker, k0t, to more than 70,000 credentials tied to network devices, harvested through that flaw, FortiWeb CVE-2025-64446 and brute force; both groups hold South African listings and 3,190 FortiGates answer the internet here. Search GlobalProtect logs for the nine Unit 42 addresses and the two spoofed host identifiers, disable Authentication Override cookies, confirm the FortiWeb and FortiGate builds, and reset every account whose credential has appeared in a stealer log (TH-2026-W44-02 and 03).

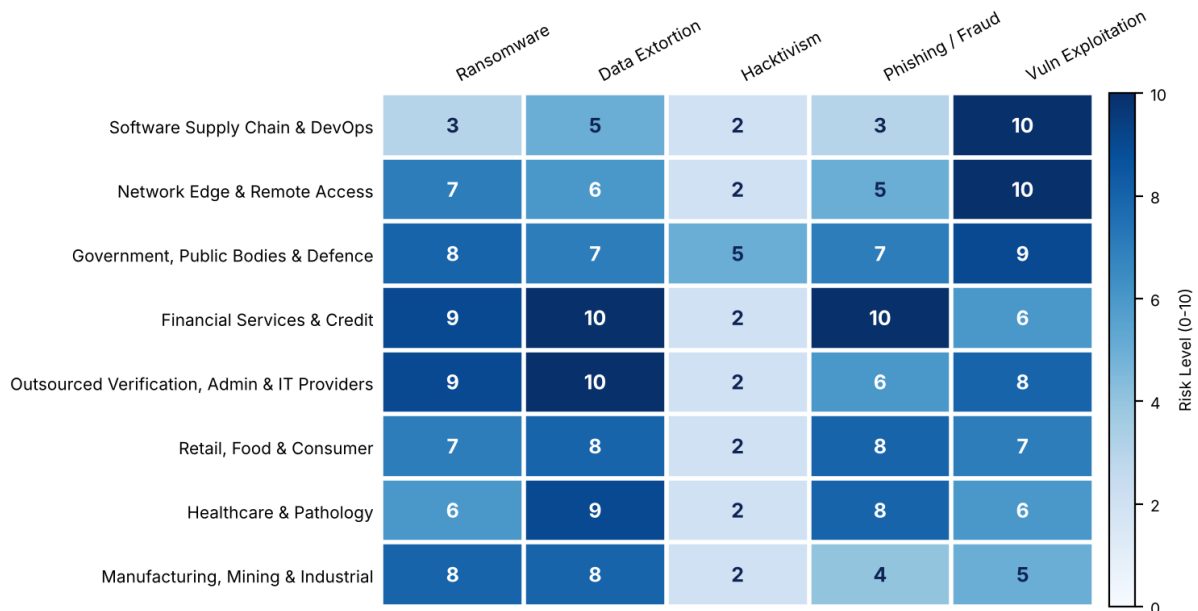
3. If the organisation administers claims, policies or scheme membership, re-run the first-48-hours plan against the RMA facts by Friday 30 October. The listing names the organisation, a volume, a price and a date; the sample a journalist sees decides the headline. The plan needs a holding statement that says more than "an alert was received", a decision on naming the actor, the Information Regulator record, the Prudential Authority or FSCA notification where Joint Standard 2 applies (24 hours from classifying the incident as material), and a call-centre briefing on claimants whose identity documents and medical records may now be in a third party's hands.

1. MyBroadband, 130-year-old financial provider that works with some of the biggest companies in South Africa hit by alleged 366GB cyberattack, by Luis Monzon (23 October 2026). <https://mybroadband.co.za/news/security/673772-130-year-old-financial-provider-that-works-with-some-of-the-biggest-companies-in-south-africa-hit-by-alleged-366gb-cyberattack.html>
2. TechCentral, Rand Mutual Assurance probes alleged theft of 1.68 million claim records, by Duncan McLeod (23 October 2026). <https://techcentral.co.za/rand-mutual-assurance-data-breach-claim/287621/>
3. ransomware.live, group page for Kazu, read 25 October 2026 (20 victims, 12 countries, none ZA; last discovery 7 September; uptime 15.4 per cent; RMA not listed). <https://www.ransomware.live/group/kazu>
4. The Hacker News, PHP issues emergency patches for two critical PHP2Shell RCE flaws as exploit attempts emerge, by Swati Khandelwal (21 October 2026). <https://thehackernews.com/2026/10/php-issues-emergency-patches-for-two.html>
5. BleepingComputer, Amazon says PHP2Shell exploitation began 4 days before patches, by Sergiu Gatian (22 October 2026). <https://www.bleepingcomputer.com/news/security/amazon-says-php2shell-exploitation-began-4-days-before-patches/>

6. The Hacker News, PHP2Shell exploit attempts hit millions as attackers try to deploy Mirai malware, by Ravie Lakshmanan (23 October 2026). <https://thehackernews.com/2026/10/php2shell-exploit-attempts-hit-millions.html>
7. TechCentral, Global PHP scramble reaches the Union Buildings, by Duncan McLeod (23 October 2026). <https://techcentral.co.za/presidency-website-offline-php-scramble/287614/>
8. MyBroadband, South African companies scrambled to protect customers from critical PHP security flaw, by Jan Vermeulen (22 October 2026). <https://mybroadband.co.za/news/cloud-hosting/673628-south-african-companies-scrambled-to-protect-customers-from-critical-php-security-flaw.html>
9. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.10.23, released 23 October 2026 19:30 UTC, retrieved 25 October (feeds/kev_2026-10-25.json). <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
10. Arista Networks, Security Advisory 0199, CVE-2026-114625, VeloCloud Orchestrator on-prem SQL injection (22 October 2026). <https://www.arista.com/en/support/advisories-notices/security-advisory/24838-security-advisory-0199>
11. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:00 UTC 25 October 2026 (feeds/shodan_za_2026-10-25.json). <https://www.shodan.io/search?query=country%3AZA>
12. Information Regulator, Enforcement notices register, checked 25 October 2026 (three entries dated 23 October 2026). <https://infoeregulator.org.za/enforcement-notices/>
13. Information Regulator, Enforcement Notice under section 95 of POPIA, First National Bank, signed 21 October 2026, published 23 October (security compromise confirmed 21 February 2022; 88 data subjects, 696 unauthorised individuals, nine account numbers; Conditions 1, 2, 3, 4 and 7; 90-day report). https://infoeregulator.org.za/wp-content/uploads/2026/10/FIRST-NATIONAL-BANK-ENFORCEMENT-NOTICE-211026_Redacted.pdf
14. Information Regulator, Infringement Notice under section 109(1) of POPIA, reference OIA-13-2023, First Rand Bank, known as First National Bank, signed 21 October 2026, published 23 October (fine R1,000,000 under section 105(1)). https://infoeregulator.org.za/wp-content/uploads/2026/10/FIRST-NATIONAL-BANK-INFRINGEMENT-NOTICE-211026_Redacted.pdf
15. Information Regulator, Infringement Notice under section 109(1) of POPIA, Central Johannesburg TVET College, signed 9 October 2026, published 23 October (fine R500,000). https://infoeregulator.org.za/wp-content/uploads/2026/10/INFRINGEMENT-NOTICE-CENTRAL-JOHANNESBURG-TVET-COLLEGE_Redacted.pdf
16. Michalsons, Information Regulator ramps up enforcement, by Tanika Upasani (2 September 2026). <https://www.michalsons.com/blog/information-regulator-ramps-up-enforcement/82825>
17. SANews, IEC enters into partnership to counter disinformation (20 October 2026). <https://www.sanews.gov.za/node/85074>
18. TechCentral, Fashion retailer TFG discloses cyberattack, Staff Reporter (13 October 2026). <https://techcentral.co.za/tfg-london-cyber-incident-phase-eight-hobbs-whistles/287214/>
19. BleepingComputer, TFG London cyberattack disrupts systems at Hobbs and Whistles retailers, by Bill Toulas (13 October 2026). <https://www.bleepingcomputer.com/news/security/tfg-london-cyberattack-disrupts-systems-at-hobbs-and-whistles-retailers/>
20. ransomware.live API, GET /v2/countryvictims/ZA, 138 records, za_records 138 against server_returned 138, filter purity 1.0, FREE v2 tier (delayed relative to PRO), retrieved 02:00 UTC 25 October 2026 (feeds/ransomwarelive_za_2026-10-25.json). <https://api.ransomware.live/v2/countryvictims/ZA>
21. ransomware.live, South Africa country page, cross-check only (138 victims, newest Europ Assistance South Africa 16 October; nothing discovered 18 to 25 October; read 25 October 2026). <https://www.ransomware.live/country/ZA>
22. ransomware.live, group page for The Gentlemen, read 25 October 2026 (1,007 victims; four listings 18 to 24 October, none South African; no published-data marker on the four SA records). <https://www.ransomware.live/group/thegentlemen>
23. ransomware.live, group page for Krybit, read 25 October 2026 (168 victims; six listings discovered 24 October, none South African). <https://www.ransomware.live/group/krybit>
24. ransomware.live, group page for Deadlock, read 25 October 2026 (109 victims; two listings 23 and 24 October, neither South African; Aeroklas Duys unchanged). <https://www.ransomware.live/group/deadlock>
25. ransomware.live, group page for Qilin, read 25 October 2026 (34 listings discovered 18 to 24 October, none South African by name or description). <https://www.ransomware.live/group/qilin>
26. ransomware.live, group page for nOn, read 25 October 2026 (44 listings 18 to 23 October; none South African). <https://www.ransomware.live/group/nOn>

2. THREAT LANDSCAPE HEATMAP

South African Sector Threat Levels, Week 44 (18 October – 24 October 2026)



Methodology: each cell is an analyst score from 0 to 10 for the coming week, set from what this edition observed: leak-site listings with a South African tag or a South African victim that passes the nationality check, incidents confirmed by the organisation affected, catalogue additions affecting software the sector runs, VERIFIED South African exposure counts for that software, and reported fraud activity. A sector with no observation keeps its prior score and a ceiling of 10 is held.

No rows changed. The matrix holds the eight rows W43 set, as that edition's review asked, and four cells move on observations. Financial Services and Credit rises from 8 to 9 on ransomware for the Rand Mutual Assurance listing, a press-carried double-extortion claim against a COIDA insurer rated PROBABLE on the company's own alert, with extortion and fraud already at the ceiling.¹ Government, Public Bodies and Defence rises from 8 to 9 on vulnerability exploitation, on the Presidency's precautionary outage and TechCentral's finding that twelve of seventeen state sites disclosing a PHP version run an old one, and from 6 to 7 on phishing and fraud, on the 190 to 200 domains impersonating AARTO, FinesSA and the RTIA.^{7,27} Its hacktivism score holds at 5: the elections fall nine days after publication, the IEC's platform partnership of 20 October is defensive, and no hostile activity was observed, so the score does not move again on the calendar.¹⁷ Outsourced Verification, Administration and IT Providers rises from 7 to 8 on exploitation: Storm-0940's use of the ConnectWise Cloud Backup compromise to attempt sign-ins to more than 2,250 downstream tenants is a managed-service supply-chain observation.²⁸ Network Edge and Remote Access holds at 10 on exploitation (a third VeloCloud Orchestrator zero-day, the kOt credential market, Qilin and INC on PAN-OS) and at 7 on ransomware, since no South African incident has yet named an edge appliance as its entry point.^{10,29,30} Software Supply Chain and DevOps holds at the ceiling with PHP2Shell, GitLab's 10.0 and Collabora. Healthcare, Retail and Manufacturing hold with no development on Ampath, Bootlegger, Aeroklas Duys or Tharisa.

27. MyBroadband, Motorists are under attack in South Africa, by Myles Illidge (23 October 2026).
<https://mybroadband.co.za/news/security/673383-motorists-are-under-attack-in-south-africa.html>

28. Microsoft Security Blog, AI-driven, large-scale nation-state campaign using ARTEX enables supply chain compromise (21 October 2026, updated 23 October). <https://www.microsoft.com/en-us/security/blog/2026/10/21/storm-0940-uses-artex-agentic-ai-connectwise-supply-chain-compromise/>

29. The Hacker News, Hackers breach enterprise firewalls and VPNs, exposing over 70,000 credentials, by Ravie Lakshmanan (23 October 2026; Group-IB and NyxLab research). <https://thehackernews.com/2026/10/hackers-breach-enterprise-firewalls-and.html>

30. Palo Alto Networks Unit 42, Active exploitation of May 2026 PAN-OS CVE-2026-0257 (20 October 2026, updated 23 October). <https://unit42.paloaltonetworks.com/active-exploitation-of-pan-os-cve-2026-0257/>

3. TOP SA INCIDENTS (W44)

Four items and a correction: an extortion claim against a COIDA insurer that the company has acknowledged as an alert, the Presidency's precautionary outage in the PHP2Shell week, a newly launched South African website entered through a password left in its page source, and a smishing campaign against motorists on about 200 lookalike domains. The TFG London incident W43 missed is added in 3.5. Ratings: CONFIRMED means the organisation affected, a regulator or two independent sources support the fact; PROBABLE means one credible source or strong technical evidence; CLAIMED means a threat-actor assertion only. A leak-site description is written by the attacker and cannot lift a rating on its own.

3.1 INC-2026-W44-01: Rand Mutual Assurance Acknowledges an Alert as Kazu Claims 366 GB of Claim Files [PROBABLE]

Sector	Financial services and credit (workers' compensation insurer licensed under COIDA; mining, iron, steel and related industries; more than one million covered workers by MyBroadband's account)
Organisation	Rand Mutual Assurance (RMA), founded 1894; clients named by MyBroadband include Anglo American, Sibanye-Stillwater, Impala Platinum and Harmony Gold
Claim	A leak-site listing attributed by MyBroadband to Kazu, first noticed on Friday 23 October: more than 366 GB, 1.6 million records including claim information, 593,786 other files, 98,000 US dollars (about R1.57 million) and a leak date of 4 November. TechCentral, from a Dark Web Intelligence post about an underground forum, gives 1.68 million claim records, 95,000 US dollars and 5 November, and names no group
Sample	MyBroadband says it reviewed sample data showing digital copies of identity cards, claim documents, X-rays, medical certificates and material from psychologists. TechCentral had seen neither the post nor a sample
Company account	Nduduzo Majozi, RMA chief information security officer, on 23 October, as MyBroadband quotes him: "Rand Mutual Assurance confirms it has received an alert about a data breach. Investigations are underway"; TechCentral carries the same statement; further communication once concluded. No intrusion date, data categories or regulator mention; no notice on the home page on 25 October
Aggregator	No RMA record on ransomware.live; Kazu unchanged at 20 victims in 12 countries since 7 September, none South African, leak-site uptime 15.4 per cent over 30 days
Confidence	PROBABLE. The company confirms an alert and a named journalist reports samples consistent with RMA's business; the volumes, price and date are the actor's. The actor's identity is PROBABLE on MyBroadband's screenshot of the Kazu site

Two things distinguish this from the insurance listings of September and October. The first is the data: a compensation claim file is an identity document, an employer, an injury or disease, a medical report and a bank account in one record, and the sample MyBroadband describes is special personal information under POPIA with no expiry date for the person concerned.^{1,2,31} The second is the actor. Kazu is a different kind of group from The Gentlemen: the aggregator records a group first seen in November 2025 with 20 listings, eleven of them healthcare, in the Americas, South Asia and the Gulf, a Nigerian insurer (Leadway Assurance, December 2025) as its only prior African name, a leak site reachable 15 per cent of the last month, and no listing since 7 September; SOCRadar gives RDP and unpatched web applications as its initial access and demands between 60,000 and 500,000 US dollars.^{3,32} A dormant brand with an unreliable site reappearing against a South African insurer at a price under 100,000 dollars fits an affiliate or a reseller using the name as well as it fits the group. The outlets' price and date differ by three thousand dollars and a day, and the listing itself was not read. The distinguishing observations are whether the aggregator indexes RMA under Kazu (the site's uptime makes a miss as likely as an absence), an RMA statement naming the actor and the data categories, an Information Regulator record, and what appears on the site after 4 or 5 November. First reported by MyBroadband and TechCentral on 23 October 2026. Detection relevance: TH-2026-W44-06.

3.2 INC-2026-W44-02: The Presidency Takes Its Website Offline in the PHP2Shell Week [CONFIRMED]

Sector	Government, public bodies and defence
Organisation	The Presidency of the Republic of South Africa (www.presidency.gov.za, a Drupal site by the Internet Archive's 18 October copy); SITA was asked for comment
Event	On Friday 23 October the Presidency announced that its website was temporarily unavailable "as a precautionary measure in response to a global cybersecurity event", apologised for the inconvenience, and named neither the event nor PHP. By Friday afternoon the server refused connections. The site was reachable and rendering normally when checked on Sunday 25 October
Context	PHP released fixes for CVE-2026-109618 and CVE-2026-109619 at 14:00 UTC on Wednesday 21 October after a leak on 20 October; Cert-EU advised organisations that could not patch to consider taking sites offline. TechCentral tested more than 100 state sites: the Presidency's was the only one deliberately taken down; of seventeen disclosing a PHP version, five ran a fixed release and twelve older ones, eight unsupported, the oldest PHP 5.4 (unsupported since 2015). The twelve were not named. The National Cybersecurity Hub's site has shown a maintenance notice since February
Hosting response	Afrihost and Axxess patched managed and shared servers; Xneelo applied mitigations before the patch, then updates, says its web application firewall blocked one published exploit, and warns that pre-patch compromise cannot be excluded; 1-Grid and Absolute Hosting applied mitigations and updates. MyBroadband's Shodan search returned more than 9,800 South African servers with a PHP banner
Confidence	CONFIRMED for the outage and its stated reason, on the Presidency's own statement as carried by TechCentral; the PHP link is TechCentral's inference from the platform and the Presidency has not confirmed it. No South African compromise through PHP2Shell has been disclosed

The outage and the survey around it describe the state's estate from two ends. A reported version is not proof of vulnerability, since distributions backport fixes under old version strings; but a site announcing PHP 5.4 announces that nobody has maintained its platform for a decade, and eight such sites among seventeen is a finding about ownership of the platforms.^{7,33} Afrihost says it acted on early reports before the vendors' advisories and Xneelo that it mitigated before the official patches, and Xneelo's caution that a server patched on 21 October may have been entered earlier applies to every estate, since Amazon's honeypots logged the first attempts on 17 October.^{8,5} Check Point's two per cent of South African organisations affected, against four for Africa and ten globally, is one vendor's telemetry share.³⁴ Detection relevance: TH-2026-W44-01.

3.3 INC-2026-W44-03: A Vibe-Coded South African Website Entered Through Its Own Page Source [PROBABLE]

Organisation	An unnamed client of Domains.co.za; account given by its chief executive, Wayne Diamond, in a LinkedIn post carried by MyBroadband on Sunday 18 October
What happened	The client built its own site with an AI coding tool instead of the registrar's builder. Six days after launch the site was gone. Diamond's account: the tool had left the administrator password in the site's code in plain text, readable with a browser's developer tools; no sophisticated attack, no zero-day; the attackers "just read the password and walked in through the front door"
Confidence	PROBABLE. A single credible source, the hosting company's chief executive, describing a client he does not name; the client has said nothing publicly and the data impact is not described

The item is small and belongs beside Bootlegger (W43), whose legacy dashboard delivered its data with its login page: two South African applications in two weeks that exposed their data to anyone who read the page.³⁵ The test is the same for both and takes a minute: view the source and the network calls of every internally built or generated application before it goes live. Detection relevance: the pre-launch check in Technical recommendation 4.

3.4 INC-2026-W44-04: About 200 AARTO and FinesSA Lookalike Domains in a Smishing Campaign Against Motorists [PROBABLE]

Targets	South African motorists; brands impersonated include AARTO, FinesSA, NATIS and forecourt brands such as Engen
Campaign	An industry source gave MyBroadband a spreadsheet of about 190 domains (the source speaks of 200-odd), some tied to smishing campaigns and some confirmed to target South Africans: misspellings such as aartd-finse.autos, aarta-finse.autos, aarto-finea.cfd, fineas.cfd and finesea.cc, plus .com, .co.za and .online variants; messages threatening licence and disc blocks, a R250 same-day discount, subject lines such as "Final Notice: Action Required to Avoid Additional Penalties", sent after hours and at weekends; fake password-protected PDF notices unlocked with the victim's ID or business registration number. The source attributes the campaign to the Smishing Triad using a platform called Ironroll

Agency response	The RTIA says it alone administers AARTO fines, that the only official site is online.aarto.gov.za , that payment needs only the 16-digit infringement notice number on a verified platform and no bank account details; it had not answered MyBroadband's questions about the list by publication
Confidence	PROBABLE. A single credible source with a reviewed domain list and the agency's standing warning; the attribution to a named smishing operation is the source's

Traffic-fine smishing is a fixture; this item earns its place on scale, since about 200 registered domains is infrastructure, and infrastructure is reused.²⁷ For a fleet operator or any employer that pays staff fines the control is procedural: one payment route, the 16-digit number, no links. Detection relevance: TH-2026-W44-07.

3.5 Added to the Record and Carryovers

TFG London (W43 window, added by correction). Incident identified Sunday 11 October; investor notice Tuesday 13 October; Phase Eight, Hobbs and Whistles systems affected, stores trading; UK authorities informed; customer-data impact under investigation; TFG Africa and TFG Australia unaffected. CONFIRMED on the company's notice as carried by TechCentral and BleepingComputer; no actor claim and no update by 24 October.^{18,19}

Ampath (ByteToBreach), W43. No sample, no count of individuals, no Information Regulator statement, and the section 22 notice is still not on the company's site, read 25 October; CONFIRMED, tests open.^{36,37}

Europ Assistance South Africa (The Gentlemen), W43. Record unchanged on 25 October: no timer, sample or published-data marker; no company statement. The group added four names in the window, none South African. CLAIMED.^{38,22} **Aeroklas Duys (Deadlock), W43.** Record unchanged; Deadlock added a German and an American name; the clearnet leak site still fails DNS. CLAIMED.²⁴

e-Panic Button, W40 and W43. No case number, departmental report or regulator statement located; CONFIRMED, tests stand. **Tharisa (UmBra), W42.** UmBra's page was served from an 18 October render; no new listing visible; on record, CLAIMED.³⁹ **LegalWise, Samwumed and Edcon, W41 and W42.** No published-data marker on any of the three on 25 October, a third week past the reported timers; CLAIMED.²²

Bootlegger, W43; BCX, Guardrisk and CoverCubed, W41; RelyComply, W39; ATNS, W41; BlackLocks, W40; Cell C Fibre, Cartrack, VSB Attorneys, Rohloff, The Courier Guy, Babcock, the Furniture Bargaining Council, Toyota's SMS provider, Implats, Hungry Lion and Rand Water. No development; carried at their prior ratings.

31. Rand Mutual Assurance, corporate website home page, checked 25 October 2026 (no incident notice readable). <https://www.randmutual.co.za/>

32. SOCRadar, Ransomware Intelligence group profile: Kazu (updated 22 October 2026). <https://socradar.io/free-tools/ransomware-intelligence/groups/kazu>

33. The Presidency, www.presidency.gov.za, checked 25 October 2026 (home page reachable and rendering normally). <https://www.presidency.gov.za/>

34. ITWeb, PHP2Shell alarm a major cyber security wake-up call, by Chris Tredger (23 October 2026). <https://www.itweb.co.za/article/php2shell-alarm-a-major-cyber-security-wake-up-call/WnpNgM2lVmP7VrGd>

35. MyBroadband, Vibe-coded South African website hacked just six days after launch, by Luis Monzon (18 October 2026). <https://mybroadband.co.za/news/security/672352-vibe-coded-south-african-website-hacked-just-six-days-after-launch.html>

36. Ampath Laboratories, website home page, read 25 October 2026 (no incident notice located). <https://www.ampath.co.za/>

37. Information Regulator, Media statements page, checked 25 October 2026 (newest item 21 September 2026). <https://infoeregulator.org.za/media-statements/>

38. ransomware.live, victim page for Europ Assistance South Africa (The Gentlemen), re-read 25 October 2026 (record unchanged, no marker). <https://www.ransomware.live/id/RXVyb3AgQXNzaXNOYW5jZSBtb3V0aCBBZnJpY2FAdGhIZ2VudGxlbWVu>

39. ransomware.live, group page for UmBra, read 25 October 2026 (served a render stamped 18 October 02:50 UTC; ten victims, none after 10 October). <https://www.ransomware.live/group/umbra>

4. THREAT ACTORS

Three profiles. Kazu, because it is the name on the Rand Mutual Assurance listing and is new to this series; the edge-credential market around k0t, Qilin and INC, because three reports in the window describe how groups with South African listings get in; and The Gentlemen's tempo, because the 33-name week was followed by a four-name week. The notes cover Storm-0940's managed-service supply chain and the groups that moved.

4.1 Kazu: A Dormant Double-Extortion Brand Reappears Against a South African Insurer

The aggregator's record is thin and specific. Kazu was first indexed on 11 November 2025; its 20 listings sit in twelve countries, eleven of them healthcare and the rest education, professional services and government; its page describes a double-extortion group active since September 2025 targeting government, healthcare and finance in South-East Asia, the Middle East and Latin America and claiming a 1.94 TB theft from Dubai's ports authority, a victim absent from its own list. Of five known onion addresses one was reachable at the 25 October check; 30-day uptime is 15.4 per cent; the last listing was 7 September, 48 days before.³ SOCRadar's profile, updated 22 October, gives initial access through exposed RDP and unpatched web applications with SmokeLoader as the first stage, data taken before encryption, demands from 60,000 to 500,000 US dollars, and South Africa among 38 affected countries without a named victim.³² The one prior African name is Leadway Assurance in Nigeria, listed 11 December 2025.³ The relevance is the pairing of a healthcare-heavy victim list with an insurer whose files are medical, which is what the sample MyBroadband describes.¹ Whether the listing is the group or someone using its name the record cannot say; Section 11 sets the test.

4.2 The Edge-Credential Market: k0t, Qilin, INC and The Gentlemen

Three reports describe one supply chain from different ends. Group-IB and NyxLab profile k0t (also CryptoFeel, Member19 and QazWsxShop), first seen 22 October 2025, who scanned for exposed appliances with FOFA and ZoomEye, exploited FortiGate and FortiWeb through CVE-2025-64446 and GlobalProtect, PAN-OS and Prisma Access through CVE-2026-0257, or brute-forced them, then built OpenConnect footholds, enumerated Active Directory and SMB, persisted with MeshCentral, Atera, Teramind, AnyDesk and AdaptixC2, and exfiltrated with Rclone to Wasabi and MEGA; they count more than 70,000 exposed credentials tied to network devices and LDAP dumps, a significant share of the compromises between February and June 2026, and assess links to Qilin and The Gentlemen as a broker or affiliate.²⁹ Unit 42's update of 20 October records exploitation of CVE-2026-0257 observed since June and names Qilin and INC among the ransomware operators using it to open GlobalProtect sessions past multifactor authentication, publishes nine addresses and the spoofed host identifiers the tooling uses, and records movement to vCenter, ESXi control changes and offline credential dumping from a domain controller's virtual disk; the catalogue has carried the flaw since 29 May with ransomware use marked

Known.^{30,9} Check Point's May profile of The Gentlemen lists exposed FortiGate and Cisco VPN appliances, brute force against web and VPN panels, and purchased broker access as initial access, with affiliates keeping 90 per cent of proceeds.⁴⁰ SOCRadar's exposed-infrastructure analysis of 23 October adds that INC and Gentlemen affiliates ran intrusions through an AI agent (OpenCode on commercial models) with a human approving each step, entered through FortiClient EMS, SimpleHelp, cPanel and VPN gateways, and had staged an exploit for SonicWall SMA 1000 CVE-2026-15409, the July carryover in this report's table.⁴¹ For South Africa: Qilin, INC and The Gentlemen hold ten of the 28 ZA-tagged listings discovered since 1 July, 3,190 FortiGates and an unmeasured GlobalProtect population answer the internet here, and a credential harvested in February may be used in November. No South African incident has yet named an edge appliance as its entry point, and this week's reporting describes how one would begin.

4.3 The Gentlemen's Tempo, Storm-0940, and the Groups That Moved

The Gentlemen's index rose from 1,002 to 1,006 between the 18 and 25 October retrievals, after movements of 21, 33, 39 and 42 in the four weeks before; the group page read 1,007 with four listings discovered 18 to 24 October, a Colorado school district and three other organisations.^{42,22} The 33-name Friday of 16 October was followed by a four-name week, consistent with Microsoft's hypothesis that the batch was posted for effect and equally with an affiliate intake now exhausted; the W43 test, how many of the 33 confirm by 16 November, runs. The indicator feed did not change for the group; the only change across the thirteen groups the feed covers is two Qilin addresses, 185.196.10.52 and 64.176.162.76, exported in TH-2026-W44-02.⁴³ Among the sixteen groups with a ZA-tagged listing since 1 July: Qilin 2,379 to 2,413, the largest mover with 34 listings and none South African; Krybit 162 to 167 with six listings on 24 October in Egypt, Malaysia, Mexico, Canada and India; Everest 416 to 421; LockBit 5.0 384 to 390; Deadlock 107 to 109; INC Ransom 977 to 979; Payload 76 to 78; the other eight unchanged.^{42,25,23,24} Outside that set, nOn went from 110 to 156 with 44 listings in six days, including Telecom Egypt and two Ethiopian organisations, none South African; the index grew to 412 groups on mimori and whitearmor.²⁶

Storm-0940. Microsoft describes a China-aligned actor using ARTEX, an open-source agentic penetration-testing framework, to turn access to ConnectWise's Cloud Backup application into sign-in attempts against more than 2,250 downstream Microsoft 365 tenants from September; the count is attempts, most unsuccessful, and no African victim is named.²⁸ ConnectWise sells to managed service providers, whose South African clients inherit the exposure; the three application identifiers, six addresses and five user agents Microsoft publishes are exported in iocs_w44.csv for tenants to check.

40. Check Point Research, Thus spoke The Gentlemen (13 May 2026). <https://research.checkpoint.com/2026/thus-spoke-the-gentlemen/>

41. The Hacker News, Exposed infrastructure reveals how ransomware affiliates used AI agents to execute intrusions, by Ravie Lakshmanan (23 October 2026; SOCRadar research). <https://thehackernews.com/2026/10/exposed-infrastructure-reveals-how.html>

42. ransomware.live API, GET /groups, 412 groups with victim counts, retrieved 25 October 2026 and compared with the 18 October retrieval (feeds/r1_groups_2026-10-25.json). <https://api.ransomware.live/v2/groups>

43. ransomware.live API, GET /iocs/{group} for groups active against South Africa, retrieved 25 October 2026 and diffed against 18 and 11 October (feeds/r1_iocs_2026-10-25.json; two Qilin addresses added). <https://api.ransomware.live/v2/iocs/qilin>

5. CRITICAL VULNERABILITIES & CISA KEV

CISA added eight vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue between Sunday 18 and Saturday 24 October 2026, six on Tuesday 20 October (EG Secure Solutions SiteGuard Server Edition CVE-2026-106931, the four Plex Media Server flaws CVE-2026-96652, CVE-2026-96654, CVE-2026-96655 and CVE-2026-96656, and Siemens Software Center CVE-2026-110936) and two on Friday 23 October (Arista VeloCloud Orchestrator CVE-2026-114625 and Collabora Online Built-in CODE Server CVE-2026-110447); none was added on Saturday 17 October, so W43's nine stand. The catalogue version is 2026.10.23, released 19:30 UTC on Friday 23 October, so any Saturday addition falls to W45.⁹ Deadlines under BOD 26-04, the directive binding US federal agencies that this report uses as a benchmark, are set per entry: three days for SiteGuard, two Plex entries and both Friday additions, fourteen days (3 November) for the two Plex SSRF entries and Siemens; three were overdue on Monday 26 October, two fell due that day, three are not yet due. CVSS is from the NVD feed and EPSS from the FIRST feed, under the standing rule that a low EPSS never deprioritises a catalogue entry; the highest of the eight is Collabora at 0.023, which says nothing about the web shells already found.^{44,45} Ransomware use reads Unknown for all eight; forensicTriage reads Yes for SiteGuard, the Plex file-write entry, Arista and Collabora and No for the other four. Two W43 questions close: NVD now carries Atlassian CVE-2026-21589 at 9.3 on version 4.0 with Atlassian as source; SonicWall SMA 1000 CVE-2026-102255 is still absent, a third week after the first recorded attempts.^{44,9}

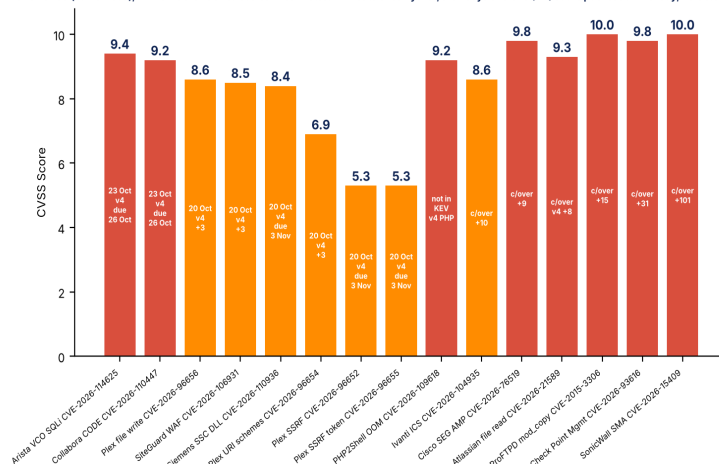
Arista VeloCloud Orchestrator CVE-2026-114625 is a SQL injection in on-premises VCO, 9.4 on version 4.0 (9.9 on 3.1 by Arista's own scoring; the feed carries the 4.0 figure), that lets any authenticated user with the lowest tenant role gain operator privileges and act as the local superuser operator; Arista detected the exploitation itself, says the interface is exposed by default with no configuration that prevents it, and publishes two attacking addresses, 74.82.197.86 and 38.54.50.151, and fixed releases 5.2.3.18, 6.1.3.10 and 6.4.2.12.^{10,44} It is the third exploited VCO flaw since July, after CVE-2026-16812 (27 July) and CVE-2026-93952 (22 September, 9.5 on version 4.0), in this report's carryover rows; the South African VCO population cannot be stated because the panel's query returns zero by two methods and stays PROVISIONAL (Section 7).¹¹ **Collabora Online Built-in CODE Server CVE-2026-110447**, 9.2 on version 4.0, is an OS command injection in the Nextcloud app richdocumentscode (26.4.302 and older; fixed 26.4.303 in September), reached through proxy.php when the built-in document server is not running; attackers planted web shells on Nextcloud servers and then searched for credential stores and cryptocurrency wallets; community members had been reporting the shells since 3 October, eleven days before the CVE was published.^{46,47} Nextcloud is a self-hosted file service and the panel has no fingerprint for it, so the South African population is unknown.

The Plex chain, CVE-2026-96652, 96654, 96655 and 96656 (5.3, 6.9, 5.3 and 8.6 on version 4.0), links two server-side request forgeries, loopback access to internal agent functions and an arbitrary file write to the Codecs directory into unauthenticated code execution as the Plex process. Plex says the flaws are actively and widely exploited against internet-facing servers older than 1.43.3.10861, with miners and proxy software installed, and gives the compromise checks: unrecognised processes started by the server, unfamiliar .so or .dll files in Codecs, connections to proxystream.st, high CPU with nothing playing; a public proof of concept appeared on 16 October.^{48,49} These four entries share the week's one product with a South African figure: 3,111 Plex Media Server instances exposed on 25 October, 1,426 on the default port 32400. Plex is a consumer media product, so most of that population will be home and small-office

servers: a compromised Plex host on a home connection is a proxy node inside a South African address range and, where the owner works from that network, a foothold beside a corporate laptop.¹¹ **SiteGuard Server Edition CVE-2026-106931**, 8.5 on version 4.0 (JPCERT), is a command injection in a Japanese host-based web application firewall, confirmed exploited by the vendor on 14 October and fixed in 8.00 Update 5; no South African footprint is visible.^{50,49} **Siemens Software Center CVE-2026-110936**, 8.4 on version 4.0, is a local DLL search-path flaw abused in ClickFix lures; it needs a user to run something.^{49,44}

Exploited and not in the catalogue. PHP CVE-2026-109618 and CVE-2026-109619, both 9.2 on version 4.0 by PHP, were disclosed on 21 October after a leak on 20 October and a mistakenly published proof-of-concept video; Chainguard published patched images six hours before PHP's 14:00 UTC release. The first is an out-of-memory path that leaves request data half-initialised, the second request state retained after its memory is freed, which a later request on the same worker can reach; together they give unauthenticated code execution on PHP-FPM, mod_php, php-cgi, FrankenPHP and LiteSpeed from 5.4 onward. Fixed in 8.5.12, 8.4.27, 8.3.36 and 8.2.35 with source backports for 7.4, 8.0 and 8.1; PHP's interim mitigations are memory_limit set to -1 so applications cannot override it, post_max_size kept low, RLIMIT_AS and RLIMIT_DATA unused, and session.upload_progress.enabled set to 0; Wiz demonstrated the attack against stock WordPress, Drupal and Joomla.^{4,51,52} Cloudflare saw millions of attempts by 22 October; Amazon's honeypots logged the first on 17 October; VulnCheck built a chain that bypasses ASLR; Previdian reports no successful code execution on its honeypots; a Mirai variant called Potassium was being dropped by 23 October; 32 UK government digital services were unavailable; a third, narrower flaw, CVE-2026-115560, goes to the regular release cycle.^{6,5,53} GitLab CVE-2026-110264, 10.0, is an integer overflow in the Onigmo regular-expression engine allowing unauthenticated code execution across every self-managed release since 7.0, fixed in 19.5.1, 19.4.3, 19.3.6, 19.2.9, 19.1.9, 19.0.10 and 18.11.13, no exploitation reported.⁵⁴ Ivanti's privilege-escalation flaw, the third link in the UTA0576 chain, still has no CVE and no fix located.⁵⁵ Oracle's October Critical Patch Update carried 1,295 patches and named no exploited flaw; its two out-of-band Java alerts of 21 and 24 October (CVE-2026-91403 and CVE-2026-114820, both 9.1) remove trust in eMudhra certificate authority certificates Oracle describes as impacted, a trust-store task with no exploitation claimed.^{56,57,58}

W44 KEV / CRITICAL CVE SEVERITY | 18 October - 24 October 2026
All eight KEV additions in the window (left), the PHP2Shell flaw that is exploited but not yet listed (centre), and six carryovers from the tracking table (right). CVSS from the NVD feed except PHP2Shell (PHP's own 4.0 score) and CVE-2026-15409 (earlier feed); v4 marks a CVSS 4.0 score. In-bar notes: KEV date or carryover, then days overdue (+N) at the publication Monday, 26 October 2026, or the due date



W44 CISA KEV / Critical CVE Tracking (eight additions 20 to 23 October plus active carryovers)

Column notes: KEV Due is the BOD 26-04 deadline for US federal agencies, used here as a benchmark; OVERDUE +N counts days past it at Monday 26 October; RW is the catalogue's ransomware-use field; Triage is the catalogue's forensicTriage flag; ZA figures are VERIFIED Shodan exposure counts of a product family, which do not measure vulnerability.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-114625	Arista VeloCloud Orchestrator (on-prem)	9.4 (v4.0)	SQL injection, privilege escalation (authenticated, lowest role)	26 Oct	KEV 23 Oct. Due on publication day. Third exploited VCO flaw since July. Fixed 5.2.3.18 / 6.1.3.10 / 6.4.2.12. IPs 74.82.197.86, 38.54.50.151. ZA query PROVISIONAL (zero). RW Unknown. Triage Yes. EPSS 0.0081.
CVE-2026-110447	Collabora Online Built-in CODE Server (Nextcloud)	9.2 (v4.0)	OS command injection via proxy.php (unauth)	26 Oct	KEV 23 Oct. Due on publication day. Web shells on Nextcloud servers since early Oct. Fixed richdocumentscode 26.4.303. No ZA label. RW Unknown. Triage Yes. EPSS 0.0228.
CVE-2026-96656	Plex Media Server (with CVE-2026-96652 5.3, 96654 6.9, 96655 5.3, all v4.0)	8.6 (v4.0)	File write to Codecs directory; chain to unauth RCE	23 Oct	KEV 20 Oct. OVERDUE +3. 96654 also due 23 Oct; 96652 and 96655 due 3 Nov. Widely exploited (miners, proxies). Fixed 1.43.3.10861. 3,111 in ZA (1,426 on 32400). RW Unknown. Triage Yes / No. EPSS 0.0082.
CVE-2026-106931	EG Secure Solutions SiteGuard Server Edition	8.5 (v4.0)	OS command injection (statistics feature)	23 Oct	KEV 20 Oct. OVERDUE +3. Vendor confirms exploitation 14 Oct. Fixed 8.00 Update 5. No ZA label. RW Unknown. Triage Yes. EPSS 0.0117.
CVE-2026-110936	Siemens Software Center	8.4 (v4.0)	DLL search path (local, authenticated)	3 Nov	KEV 20 Oct. Due 3 Nov. Abused in ClickFix lures per THN. No ZA label. RW Unknown. Triage No. EPSS 0.0024.
CVE-2026-104935	Ivanti Connect Secure	8.6	Auth bypass (unauth RCE)	16 Oct	Carryover. OVERDUE +10. Windows Shell 96951 +10; SEG 76519, PAN-OS 0322, Ahsay pair +9; Atlassian 21589 +8 (NVD now 9.3 v4); BeyondTrust, Fortinet 61624 +7. Priv-esc link unpatched. W43 missions stand.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-88779	Citrix NetScaler (SAML)	8.7 (v4.0)	Memory overflow, DoS	7 Oct	Carryover. OVERDUE +19. AA26-281A five +15 (172 ProFTPD in ZA); September NetScaler pair +26; SD-WAN +23; FortiMail +22; Zammad +21; Apple +13. 146 NetScaler in ZA.
CVE-2026-93616	Check Point Security Management	9.8	Path traversal, file upload	25 Sep	Carryover. OVERDUE +31. With 85102 and VCO 93952; MikroTik 67279, SharePoint 65660 +28; Adobe 71362 +29; NetScaler 19490, FMC 20079 +44; MikroTik 86060 +43 (see 7.1); ScreenConnect +42; SEG 76461 +39.
CVE-2026-0257	Palo Alto Networks PAN-OS GlobalProtect	Outside NVD feed window	Auth bypass, VPN session past MFA	1 Jun	Carryover, newly profiled. KEV 29 May. OVERDUE +147. RW KNOWN. Qilin and INC since June per Unit 42; kOt broker. GlobalProtect query BROKEN. TH-2026-W44-02.
CVE-2026-15409	SonicWall SMA 1000	10.0	SSRF (unauth)	17 Jul	Carryover. OVERDUE +101. With 15410, both RW KNOWN; exploit staged by INC and Gentlemen affiliates per SOCRadar. FMC 20316 (Known) +86; SharePoint 55040 +66; Zimbra +63; LiteLLM 42271 +126. CVE-2026-102255 not listed. SonicWall 1,214 in ZA.

Pattern note: the week's catalogue entries are consumer and niche software, and the week's exploitation story is a flaw the catalogue had not listed by Friday night. A defender working the catalogue alone would have spent the week on Plex and a Japanese WAF while PHP2Shell went unlisted; the catalogue is a lagging record of confirmed exploitation, and in a leak-before-patch week the trigger has to be the vendor advisory and the hosting provider's notice.^{9,6} The second pattern is older: Arista's third exploited VeloCloud Orchestrator flaw since July, on a web interface exposed by default; the control is the one W43 gave for every edge console: trusted networks only, and the compromise check before the upgrade.¹⁰

44. NIST NVD, CVE API 2.0, CVSS base scores with scoring source for the 53 catalogue entries added in the last 45 days, retrieved 25 October 2026 (feeds/nvd_cvss_2026-10-25.json). <https://services.nvd.nist.gov/rest/json/cves/2.0>

45. FIRST, EPSS API, scores for the same 53 entries, retrieved 25 October 2026 (feeds/epss_2026-10-25.json). <https://api.first.org/data/v1/epss>

46. The Hacker News, CISA flags two actively exploited critical flaws in Collabora Online and Arista VeloCloud, by Ravie Lakshmanan (24 October 2026). <https://thehackernews.com/2026/10/cisa-flags-two-actively-exploited.html>

47. Nextcloud community forum, To Collabora Built-in users: update ASAP (3 October 2026, updated 17 October; community-reported indicators without vendor confirmation). <https://help.nextcloud.com/t/to-collabora-built-in-user-update-asap/250516>

48. Plex, Important security update for Plex Media Server v1.43.2 and earlier, forum advisory (1 September 2026, updated 19 October 2026). <https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319>

49. The Hacker News, CISA orders federal agencies to patch exploited Plex2Shell, Siemens, and SiteGuard flaws, by Ravie Lakshmanan (21 October 2026). <https://thehackernews.com/2026/10/cisa-orders-federal-agencies-to-patch.html>

50. EG Secure Solutions, SiteGuard Server Edition security alert 202610-1, CVE-2026-106931 (14 October 2026; exploitation confirmed by the vendor). <https://www.eg-secure.co.jp/siteguard/news/alert-202610-1>

51. Huntress, Rapid Response: php2shell, leaked critical PHP vulnerabilities CVE-2026-109618 and CVE-2026-109619 (20 October 2026, updated 21 October). <https://www.huntress.com/blog/php2shell-leaked-critical-php-vulnerabilities>

52. Wiz Research, PHP2Shell: AI uncovers critical RCE vulnerabilities affecting 70 per cent of the Internet (21 October 2026). <https://www.wiz.io/blog/php2shell-php-rce>

53. The Hacker News, PHP warns of another unpatched RCE risk two days after emergency PHP2Shell patches, by Swati Khandelwal (23 October 2026; CVE-2026-115560). <https://thehackernews.com/2026/10/urgent-php-warns-of-another-unpatched.html>

54. The Hacker News, Critical GitLab flaw (CVSS 10.0) could allow unauthenticated RCE across 12 years of releases, by Swati Khandelwal (21 October 2026; CVE-2026-110264). <https://thehackernews.com/2026/10/critical-gitlab-flaw-cvss-100-could.html>

55. The Hacker News, Attacker chains three Ivanti Connect Secure zero-days for root access, only two patched so far, by Swati Khandelwal (13 October 2026). <https://thehackernews.com/2026/10/attacker-chains-three-ivanti-connect.html>

56. Oracle, Critical Patch Update Advisory, October 2026 (20 October 2026; 1,295 new security patches). <https://www.oracle.com/security-alerts/cpuoct2026.html>

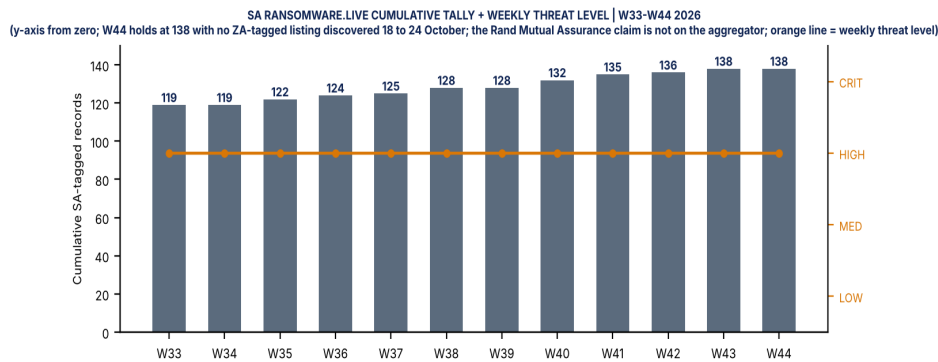
57. Oracle, Security Alert Advisory CVE-2026-91403, Java SE and GraalVM, distrust of eMudhra intermediate CA certificates (21 October 2026; CVSS 9.1). <https://www.oracle.com/security-alerts/alert-cve-2026-91403.html>

58. Oracle, Security Alert Advisory CVE-2026-114820, Java SE and GraalVM, removal of eMudhra root CA certificates (24 October 2026; CVSS 9.1). <https://www.oracle.com/security-alerts/alert-cve-2026-114820.html>

6. RANSOMWARE LANDSCAPE

The South African victim feed held 138 records when retrieved at 02:00 UTC on 25 October 2026, the same as the week before. The collection is country-scoped by path, the file records 138 South African records against 138 returned, and the tier is the delayed free v2.²⁰ A set-difference against the 18 October file returns no addition and no removal, a field-by-field comparison finds no shared record changed, and the country page showed 138 with Europ Assistance South Africa still newest.²¹ The hand search read the 90 listings that The Gentlemen (4), Krybit (6), Deadlock (2), Qilin (34) and nOn (44) indexed between 18 and 24 October and found none South African.^{22,23,24,25,26} The week's one South African extortion claim, Rand Mutual Assurance, is on none of these pages: Kazu is unchanged at 20 on the aggregator, which fits a site the crawler could not reach as well as a listing the press read elsewhere.³

Baseline at W43 close	138 records
New listings dated inside the window	0 with a ZA tag; 0 found under another tag for 18 to 24 October across 90 listings read by hand
Off-aggregator claims	1: Rand Mutual Assurance (Kazu per MyBroadband; unnamed forum post per TechCentral), 23 October, PROBABLE; not on ransomware.live at the 25 October retrieval
Delistings or restorations	None. Zero additions and zero removals against the 18 October file; no shared record changed
End count at W44 retrieval	138 records, filter purity 1.0 in the run log and 138 of 138 tagged ZA in the file
Groups active against SA, rolling 120 days	17 by discovery date, unchanged; 16 groups hold a ZA-tagged listing discovered since 1 July (28 listings). The boundary moves each week, so neither figure is a trend
Threat-level drivers	A PROBABLE extortion claim against a COIDA insurer with medical and identity records in the sample; a leaked-before-patch PHP engine flaw under mass exploitation against a South African PHP population MyBroadband's search puts above 9,800 and a state estate that announces old versions; three reports on how Qilin, INC and The Gentlemen enter through FortiGate and GlobalProtect credentials, against 3,190 FortiGates in South Africa



Group notes. Kazu and the edge-credential actors are profiled in Section 4 and the index movements are in 4.3.⁴² The sixteen groups with a ZA-tagged listing since 1 July are unchanged: The Gentlemen six, Krybit four, INC Ransom three, Deadlock and BlackLocks two each, and UmBra, Everest, LockBit 5.0, DireWolf, Qilin, MedusaLocker, Payload, m3rx, DragonForce, Arcus Media and RansomHouse one each.²⁰ A flat week after four weeks of additions is within the series' variation (W34 and W39 were also flat), and the RMA claim shows why the feed count is a floor: a listing on a site the aggregator reaches one day in seven is counted when the crawler gets through. The standing caution applies: the feed is the delayed free tier, and a listing posted late on Saturday 24 October may surface next week.

7. OSINT EXPOSURE & ATTACK SURFACE

7.1 The Panel: VERIFIED South African Exposure Counts

Every figure in this section is an exposure count of a product family in South Africa, retrieved at 02:00 UTC on 25 October 2026, and none is a count of vulnerable systems; the version and vuln filters are not available on this plan, rescan noise moves single counts by large fractions inside a day, and week-on-week movement is not reported as a finding.¹¹ Only queries whose product facet corroborates the fingerprint are published. The new figure is Plex Media Server, 3,111 instances with 1,426 on 32400, promoted at this run from the catalogue's 20 October entries with a facet of 100 per cent; it is the week's only catalogue product with a South African count. The edge population the week's actor reporting describes: Fortinet FortiGate 3,190 (1,566 on 10443, the SSL VPN port); the move from 2,801 is 14 per cent, inside the measured noise floor, and is not a finding. The rest of the panel: Citrix Netscaler 146 (100 on 443); Cisco ASA WebVPN 357; Microsoft SharePoint on-prem by http.component 769; WordPress by http.component 372, a floor; Apache Tomcat 951; Remote Desktop on 3389, 8,152; services on port 445, 5,681, of which 184 carry a Samba label; SonicWall by product string 1,214; ProFTPD 172, 135 on port 21; ownCloud 131; Metabase 129; MLflow 106; Ray 84; Langflow 81; Gitea 6; VMware vCenter 2; Artifactory 1.

MikroTik: a measurement change. The MikroTik RouterOS query returned 19,498 against 3,947 last week. The facet is still 100 per cent MikroTik labels, so the query measures what it claims, but its composition changed: 15,526 instances answer on port 1701, the L2TP port, where last week's result had no such population, while the API port 8728 reads 3,165 against 3,154. A fivefold move in seven days is a rescan that newly fingerprinted L2TP responders as RouterOS or a fingerprint change on Shodan's side, not 15,000 new routers; the comparable number for the catalogue's RouterOS entries is the API-port count, which is flat. Section 11 sets the test.¹¹

Held, missing and omitted. Arista VeloCloud Orchestrator, the week's most serious catalogue entry, has a query that returns zero by product match and by free text and stays PROVISIONAL; by evidence rule 6 a zero is not published as an absence, so the South African VCO population is unknown. Collabora, SiteGuard and Siemens Software Center have no Shodan product label. No query exists for PHP as an engine (MyBroadband's 9,800 is that publication's own search and is cited as such), for Nextcloud or for Ivanti Connect Secure, and the GlobalProtect title match remains BROKEN, so the PAN-OS population exposed to CVE-2026-0257 cannot be stated. LiteLLM at 6,559 and ScreenConnect at 2,700 are disclosed and not published for an eighth week as port-scatter artefacts; the SonicWall family sum (3,230) is withdrawn per W43. Check Point, F5 APM, WSO2, Adobe Commerce, Zyxel, Zammad, FortiMail, Catalyst SD-WAN Manager, BIND, Struts, ONLYOFFICE, BeyondTrust, AhsayCBS, Cisco Secure Email Gateway and the Atlassian products remain held.¹¹

7.2 Credentials: the Market and the Sample

Two credential stories meet in South Africa this week. The first is the market: more than 70,000 credentials tied to network devices and directory dumps, harvested by one broker through FortiWeb and GlobalProtect flaws and brute force, a significant share of them between February and June, and sold on to groups that hold South African listings, with the compromises concentrated in Asia-Pacific, Latin America, Europe and the Middle East and North Africa and no South African share stated.²⁹ The second is the sample: identity-card copies, X-rays and medical certificates from a workers' compensation insurer, seen by a journalist on an extortion site.¹ For the FortiGate population the W42 FortiBleed user-list audit and this week's stealer-log reset are the same control; for an insurer the exposure that matters now is the claimant's, and the fraud that follows a leaked claim file is a call quoting the claim number, the employer and the injury.

8. REGULATORY & POLICY

8.1 The Regulator's FNB Instruments: A 2022 Compromise, a 2026 Fine, No Statement

The Information Regulator's enforcement register acquired three entries dated Friday 23 October 2026, the first since 10 June. Two concern First Rand Bank, known as First National Bank, both signed at Johannesburg on 21 October by the Chairperson, Adv. Pansy Tlakula. The enforcement notice under section 95 sets out the facts: a complaint lodged on 27 September 2022 about a security compromise FNB had confirmed on 21 February 2022, in which the personal information of 88 data subjects was exposed to 696 unauthorised individuals and the contact details and account numbers of nine of them were accessed, because some individual account holders had been classified as employees and thereby given access to home-loan applicants' information; two customers had alerted the bank on 30 March and 3 May 2022 and the notice finds that the vulnerability was not fully addressed after either alert. It finds contraventions of Conditions 1, 2, 3, 4 and 7 (sections 8, 5, 12, 14, 15 and 19) and directs FNB to amend its privacy notice, justify collection from public sources, cut over-retained records with a destruction certificate, test its safeguards, tighten role-based access, train staff on incident reporting, and report with evidence within 90 days.^{12,13} The infringement notice, reference OIA-13-2023, records that FNB "has contravened the

provisions of section 8 in so far as the provisions relate to the processing of an account number of a data subject", finds the bank guilty of an offence under section 105(1), and imposes an administrative fine of R1,000,000, payable, arranged in instalments or contested in court within 30 days of service.¹⁴ The third fines Central Johannesburg TVET College R500,000 under section 103 for failing to comply with an enforcement notice on complaints CI462-22, CI491-22 and CI519-22, signed 9 October.¹⁵ The regulator issued no media statement (its newest remains 21 September) and no coverage of the matter was located by Saturday 24 October, with the sweep's gaps recorded in Section 12.³⁷ Three things in the instruments matter beyond FNB. The clock: a compromise confirmed in February 2022 and complained of in September 2022 produced its enforcement notice in October 2026, so the absence of an instrument on this year's compromises (MIP, Cartrack, RelyComply, e-Panic, Ampath) says nothing about whether one is coming. The fine: the fines the regulator had collected before this were R100,000 each from the IEC and Lancet Laboratories and a municipal fine a court cut to R250,000, and the R5 million imposed on the justice department after its 2021 ransomware incident is the larger instrument; the FNB amount attaches to the account-number offence in section 105(1), which the Act singles out; the 88 people exposed carry no separate fine.^{16,7} The scope: a compromise complaint became a review of the privacy notice, collection, retention and access control, the whole processing estate. The distinguishing observations are FNB's response within 30 days (payment, instalments, trial or an appeal under section 97), its 90-day report, and whether the regulator's media page catches up with its register.

8.2 The Election Fortnight, Clocks and Who to Call

The IEC signed a partnership on Tuesday 20 October with Google, Meta, Microsoft, TikTok and Moxii Africa to counter disinformation in the 4 November local government elections, built on the 2024 framework: a working group, awareness and training, platform action under their own policies, and Real411 as the complaints channel in all eleven official languages, with referral to the Electoral Court, the platform or a corrective statement as remedies; the code gazetted on 4 September binds parties and candidates.¹⁷ Chief Electoral Officer Sy Mamabolo's line, that a technically flawless election can still lose public trust to disinformation, is the frame for the fortnight: the risks are to trust and availability, and the Section 11 tests are unchanged and unmet. The Presidency's precautionary outage has a stated non-hostile cause and does not count toward them.⁷ The Acting Police Minister's reply to Dianne Kohler Barnard MP, reported 20 October, states that SAPS cybercrime capacity "is established in all 9 provinces and at Head Office", without numbers.⁵⁹ Discovery's integrated report for the year to 30 June 2026 moves cybercrime to the top of its ten risks from third, citing the speed AI gives attackers; it discloses no incident count.⁶⁰ For the Rand Mutual Assurance case and any like it, the clocks are: section 22 of POPIA, as soon as reasonably possible; section 54 of the Cybercrimes Act, a report to SAPS "without undue delay and, where feasible, not later than 72 hours" for electronic communications service providers and financial institutions, with a fine of up to R50,000 for non-compliance; and, for institutions under Joint Standards 1 of 2023 and 2 of 2024, an initial notification to the Prudential Authority (banks and insurers) or the FSCA within 24 ordinary hours of classifying an incident as material, with the impact section due in 14 days, under the template in force since 1 September 2026; outsourcing does not move the duty.^{61,62} Who to call is unchanged in the FIRST directory: the Cybersecurity Hub (kpillay@cybersecurityhub.gov.za) for government and the private sector, ECS-CSIRT at the State Security Agency (ecs-csirt@ssa.gov.za) for government and the military, SA NREN CSIRT and UCT CSIRT for research and education, and the Standard Bank and Vodacom teams for their constituencies.⁶³ SARS-SCAM-400 of 2 September remains SARS's newest alert; the AARTO campaign in 3.4 is the week's fraud advisory.⁶⁴

59. MyBroadband, South Africa's police force has cybercrime investigators in all 9 provinces, by Myles Illidge (20 October 2026). <https://mybroadband.co.za/news/security/672630-south-africas-police-force-has-cybercrime-investigators-in-all-9-provinces.html>
60. TechCentral, Discovery ranks cybercrime as its top risk, citing frontier AI, by Duncan McLeod (21 October 2026). <https://techcentral.co.za/discovery-cybercrime-top-risk-frontier-ai/287537/>
61. Cybercrimes Act 19 of 2020, section 54, Obligations of electronic communications service providers and financial institutions (acts.co.za consolidated text). https://source.acts.co.za/cybercrimes-act-2020/54__obligations_of_electronic_php
62. Moonstone, New IT and cyber incident reporting template now in effect (3 September 2026). <https://www.moonstone.co.za/new-it-and-cyber-incident-reporting-template-now-in-effect/>
63. ransomware.live API, GET /csirt/ZA, six South African CSIRTs from the FIRST directory, retrieved 25 October 2026 (feeds/r1_csirt_za_2026-10-25.json). <https://api.ransomware.live/v2/csirt/ZA>
64. SARS, Scams and phishing alerts page, checked 25 October 2026 (newest alert SARS-SCAM-400, 2 September 2026). <https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>

9. WEEKLY THREAT HUNT & IOCs

Seven missions. Three P1 cover the week's exploitation at scale: PHP2Shell with PHP's mitigations, Wiz's and Huntress's detection logic and the attacker infrastructure responders have published; the PAN-OS GlobalProtect bypass Unit 42 ties to Qilin and INC, with Unit 42's nine addresses and the two Qilin addresses the aggregator's feed added this week; and the FortiGate and FortiWeb harvesting behind the kOt inventory. Three P2 cover the Plex chain against 3,111 South African servers, the Collabora web shells on Nextcloud and the claims-administration pattern the RMA record describes; one P3 covers the AARTO smishing domains. The Arista VCO addresses and versions are exported from Section 5 to the CSV without a mission.⁴³ Every atomic indicator is exported to iocs_w44.csv with the URL that supports it; community-reported indicators are labelled. The W43 missions stand as written and are not reprinted.

TH-2026-W44-01: PHP2Shell: The Out-of-Memory Request, the Shell From the Worker, and the Known Attackers

P1 CRITICAL: exploited from 17 October, patched 21 October; not in KEV; Presidency offline as precaution

Hypothesis: An attacker has sent crafted multipart requests to a PHP server to trigger an out-of-memory condition (CVE-2026-109618) or reach freed session state on the same worker (CVE-2026-109619), executed code as the web worker and dropped a web shell, a miner or a Mirai loader; a server patched on or after 21 October may have been entered between 17 and 21 October.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1059.004 (Unix Shell), T1105 (Ingress Tool Transfer), T1496 (Resource Hijacking), T1136 (Create Account).

IOCs: Versions below 8.5.12, 8.4.27, 8.3.36 and 8.2.35, and any 8.1 or older build without a distribution backport. Request pattern (Wiz): unusual multipart requests followed by memory-limit fatal errors, repeated HTTP 500 responses, oversized or malformed PHPSESSID cookies, unexplained php-fpm worker restarts. Process pattern (Huntress): php-fpm, php-cgi, httpd or apache2 spawning sh, bash, python, perl, curl, wget, nc or certutil, or running whoami, id or uname. Attacker IPv4 addresses (Wordfence via The Hacker News; one IPv6 address in the source is omitted here): 87.121.84[.]174, 181.215.186[.]252, 185.196.220[.]132, 185.161.210[.]29, 152.233.51[.]69, 45.134.225[.]16, 107.189.14[.]87, 193.47.62[.]24, 103.147.220[.]17; SOCRadar exploitation server 206.188.197[.]105 port 9999; Mirai (Potassium) sources 85.11.167[.]243, 217.60.242[.]76, 45.198.224[.]169, loader 92.118.112[.]100, command server thunder.godofthunder.st at 134.199.154[.]64 port 50792 (Sophos).

Data Sources: Web server access and error logs; php-fpm logs; process-creation telemetry on web hosts; file-integrity monitoring on web roots; outbound connection logs from web servers; CMS administrator account audit.

Detection Guidance: On Monday 26 October confirm the running PHP build on every internet-facing host by changelog, and on anything that cannot be patched apply PHP's interim settings: memory_limit=-1 so applications cannot override it, post_max_size kept low, session.upload_progress.enabled=0 (on 8.5 also fatal_error_backtraces=0). Search since 17 October for the request and process patterns and the listed addresses; a web server process spawning a shell is an incident. On a hit, preserve logs, isolate, look for web shells, new web-root files, cron jobs and administrator accounts, and rebuild. Sources: The Hacker News 21 and 23 October, Huntress 20 to 21 October, Wiz 21 October, BleepingComputer 22 October.

TH-2026-W44-02: PAN-OS GlobalProtect
CVE-2026-0257: Nine Addresses, Two Spoofed Hosts, and
Qilin's New Feed Entries

P1 CRITICAL: exploited since June, Qilin and
INC named; KEV since 29 May, RW Known;
overdue +147; no ZA figure

Hypothesis: A ransomware affiliate has used the GlobalProtect authentication bypass CVE-2026-0257 to open a VPN session without satisfying multifactor authentication, moved from the gateway to vCenter and a domain controller, and is dumping credentials offline before encryption.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1556.006 (Multi-Factor Authentication bypass), T1133 (External Remote Services), T1003.003 (NTDS), T1562.001 (Impair Defenses), T1486 (Data Encrypted for Impact).

IOCs: Unit 42 addresses 23.128.228[.]6, 104.207.144[.]154, 146.19.216[.]119, 146.19.216[.]120, 146.19.216[.]125, 179.43.172[.]213, 185.195.232[.]139, 198.12.106[.]60, 202.144.192[.]47; spoofed host identifiers aa:bb:cc:dd:ee:ff and 00:11:22:33:44:55 and device names WINDOWS-LAPTOP-001, DESKTOP-GP01, GP-CLIENT; PoC client values endpoint_os_version "Microsoft Windows 10 Pro 64-bit" with an empty source_user_info.domain. Qilin addresses added to the aggregator's indicator feed on 25 October: 185.196.10[.]52 and 64.176.162[.]76 (role not stated).

Data Sources: GlobalProtect portal and gateway logs (gateway-connected events); PAN-OS authentication logs; vCenter and ESXi audit logs; domain controller 4624 and 4662 events; firewall and proxy logs for the eleven addresses.

Detection Guidance: On Wednesday 28 October search GlobalProtect logs since 1 June for successful gateway-connected events from the nine addresses, the spoofed host identifiers and the PoC client values; confirm the fixed PAN-OS build; generate a dedicated Authentication Override certificate or disable Authentication Override on portal and gateway; test the management interface from outside on 4443 and 3879. A successful connection from the list is an incident. Block and retro-hunt the two Qilin addresses for 30 days. Sources: Unit 42 (20 to 23 October), the catalogue entry, the aggregator's Qilin feed.

TH-2026-W44-03: The kOt Inventory: FortiWeb and
FortiGate Credential Harvesting and What Follows It

P1 CRITICAL: 70,000 credentials; FortiWeb
KEV since Nov 2025 (+339); 3,190 FortiGates in
ZA

Hypothesis: A broker has taken credentials from a FortiWeb or FortiGate through CVE-2025-64446 or brute force, and an affiliate who bought them has established an OpenConnect VPN foothold, enumerated Active Directory and SMB, installed a remote-access tool and is exfiltrating with Rclone to cloud storage before a ransomware deployment.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1110 (Brute Force), T1078 (Valid Accounts), T1087.002 (Domain Account Discovery), T1219 (Remote Access Software), T1567.002 (Exfiltration to Cloud Storage).

IOCs: FortiWeb builds affected by CVE-2025-64446 (path traversal); FortiGate administrator logins from unfamiliar addresses; MeshCentral, Atera, Teramind or AnyDesk installed outside change control; AdaptixC2 artefacts; OpenConnect connections to the organisation's VPN from new sources; Rclone processes or configurations naming Wasabi S3 buckets or MEGA (Group-IB and NyxLab via The Hacker News).

Data Sources: FortiGate and FortiWeb event logs and administrator audit; VPN authentication logs; EDR software inventory; DNS and proxy logs for Wasabi, MEGA and remote-access tool domains; domain controller enumeration events.

Detection Guidance: On Wednesday 28 October confirm every FortiWeb is on a build fixed for CVE-2025-64446 and every FortiGate on a FortiBleed-fixed build (W42); export the administrator and VPN user lists and reset any account whose credential appears in a stealer log or has not rotated since February; alert on the four remote-access tools and on Rclone wherever they are not approved; alert on outbound connections to object storage from servers that have no business there. A FortiGate administrator login from a hosting provider's range is an incident. Sources: The Hacker News 23 October (Group-IB and NyxLab), Check Point Research 13 May, the catalogue entry.

TH-2026-W44-04: Plex Media Server: The Codecs Folder, the Proxy Host and the Process That Should Not Be There

P2 HIGH: KEV 20 October, overdue +3; widely exploited; 3,111 exposed in ZA

Hypothesis: An attacker has chained the four Plex flaws against an internet-facing server older than 1.43.3.10861 to run code as the Plex process, written a shared library to the Codecs directory, and installed a miner or a residential proxy node on a South African home or small-business network.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1574 (Hijack Execution Flow), T1496 (Resource Hijacking), T1090 (Proxy), T1552 (Unsecured Credentials).

IOCs: Plex Media Server below 1.43.3.10861; unrecognised child processes of the server (Plex's examples: myawesomeproxy, mylovelyminer); unfamiliar .so or .dll files in the Codecs folder; transcoder options in Preferences.xml the owner did not set; outbound connections to proxystream.st; high CPU with nothing playing (Plex advisory); inbound exposure on port 32400.

Data Sources: Plex server logs; host process list and file timestamps in Codecs; router or firewall logs for port 32400 forwarding and for proxystream.st; EDR where present.

Detection Guidance: On Monday 26 October update to 1.43.3.10861 or later and disable Remote Access where not needed; check Codecs and Preferences.xml; on any finding rebuild from a clean installation, sign out all devices, change the Plex password and treat every share and credential the service account could reach as exposed. Corporate teams: ask staff who work from home whether they run Plex, since a compromised media server sits beside the work laptop. Sources: Plex advisory (updated 19 October), The Hacker News 21 October, the catalogue entries, the Shodan panel.

TH-2026-W44-05: Collabora Built-in CODE Server on Nextcloud: proxy.php, Nx_33143.php and the Shells Already Found

P2 HIGH: KEV 23 October, due on publication day; web shells reported from 3 October; no ZA figure

Hypothesis: An attacker has sent a crafted request to proxy.php on a Nextcloud server running richdocumentscode 26.4.302 or older while the built-in document server was not running, executed commands as the web server user, dropped a PHP web shell under the app directory, and is searching for credential stores, password-manager files and cryptocurrency wallets.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1552.001 (Credentials in Files), T1083 (File and Directory Discovery).

IOCs: richdocumentscode 26.4.302 and older; fixed 26.4.303. Community-reported on the Nextcloud forum without vendor confirmation: file apps/richdocumentscode/Nx_33143.php containing a system() call on a GET parameter, SHA-512 4b1c4012c882c512b1e4bb2938c554359f6a268f2a5d10471dbf6d08cce31c7b0e8cc24e5f709dc227fc3e2a34f685089219be2df4713f1a9933348ef4cbfe82; access-log requests for proxy.php?status; file names beginning shx or shrf. Exploitation condition: CODE server not running (The Hacker News).

Data Sources: Nextcloud web server access logs; the Nextcloud integrity check; file listings of the apps directory; web server user's outbound connections; credential-store and wallet file access audit.

Detection Guidance: On Monday 26 October update richdocumentscode to 26.4.303 or remove the app where Collabora runs in Docker or a distribution package; run the integrity check and list every PHP file under apps/richdocumentscode the package did not ship; search access logs since 1 October for proxy.php?status bursts from external addresses. On a hit, rotate every credential the web server user could read and rebuild. Sources: The Hacker News 24 October, the Nextcloud community thread (community indicators, labelled), the catalogue entry.

TH-2026-W44-06: Claims Administration Under Extortion: The RMA Pattern and Kazu's Published Methods

P2 HIGH: PROBABLE SA extortion claim;
medical and identity records in the sample;
deadline 4 or 5 November

Hypothesis: A double-extortion affiliate has entered a claims administrator through an exposed RDP service or an unpatched web application, staged a loader, exported claim files (identity documents, medical reports, bank details) and posted a listing with a deadline; a second actor is using the file contents to impersonate the administrator to claimants.

MITRE ATT&CK: T1133 (External Remote Services), T1190 (Exploit Public-Facing Application), T1110 (Brute Force), T1105 (Ingress Tool Transfer), T1048 (Exfiltration Over Alternative Protocol), T1486 (Data Encrypted for Impact), T1656 (Impersonation).

IOCs: No atomic indicator for the RMA intrusion is public and none is invented here. Kazu's published profile (SOCRadar): initial access through RDP and unpatched web applications, SmokeLoader as first stage, data taken before encryption, demands 60,000 to 500,000 US dollars. Listing attributes (MyBroadband): 366 GB, 1.6 million records, 593,786 files, deadline 4 November. Exposure baseline: 8,152 Remote Desktop services on 3389 in South Africa (Shodan panel).

Data Sources: RDP authentication logs and exposure inventory; web application logs; EDR for loader behaviour; database and file-server read volumes per account per day; egress volume per server; call-centre logs for callers quoting claim numbers; own-name monitoring under any country tag.

Detection Guidance: From Monday 26 October: confirm no RDP answers the internet without a gateway and multifactor authentication; hunt for file-server and database accounts whose daily read volume exceeds their 90-day median by an order of magnitude and for outbound transfers from file hosts to addresses outside the organisation's providers; brief call centres that a caller quoting a correct claim number, employer and injury is not thereby verified. Sources: MyBroadband and TechCentral 23 October, SOCRadar, the Shodan panel; the detection logic is the report's own.

TH-2026-W44-07: AARTO and FinesSA Smishing: Domain Patterns for Mail, SMS and DNS Filters

P3 MEDIUM: about 200 lookalike domains;
RTIA impersonation; consumer and fleet
exposure

Hypothesis: A smishing operation is sending traffic-fine notices by SMS and email from about 200 registered lookalike domains, directing victims to cloned payment portals and password-protected PDF lures unlocked with the victim's identity number, and collecting card and banking details.

MITRE ATT&CK: T1566.002 (Spearphishing Link), T1583.001 (Acquire Infrastructure: Domains), T1656 (Impersonation), T1204.001 (Malicious Link).

IOCs: Example domains from MyBroadband's reviewed list: aartd-finse.autos, aarta-finse.autos, aarto-finea.cfd, fineas.cfd, finesa.meichs.cfd, finesea.cc; patterns: misspellings of AARTO, FinesSA and NATIS on .autos, .cfd, .cc, .com, .co.za and .online; lure text "Final Notice: Action Required to Avoid Additional Penalties" and a R250 same-day discount; messages timed after hours and at weekends; password-protected PDF notices. The only legitimate portal per the RTIA is online.aarto.gov.za.

Data Sources: Secure email gateway and SMS filtering logs; DNS resolver logs for the listed TLD patterns; web proxy logs for the example domains; fleet and payroll fine-payment records.

Detection Guidance: On Monday 26 October add the six example domains to blocklists and a pattern for AARTO and FinesSA misspellings on the listed TLDs to the mail and DNS filters, with a review of hits; brief fleet administrators and staff that fines are paid only through online.aarto.gov.za quoting the 16-digit infringement number and that payment needs no bank account details. Source: MyBroadband 23 October (domain list and RTIA statement).

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

- 1. Finish the PHP inventory and the 17-to-21 October compromise hunt by Tuesday 27 October (Action 1), and keep the inventory.** The inventory outlives the flaw: every PHP runtime the organisation operates, who owns each, and the build it runs, checked by changelog, maintained after the week is over.
- 2. Run the GlobalProtect and FortiGate credential checks by Wednesday 28 October (Action 2; TH-2026-W44-02 and 03).** The broker's inventory was assembled between February and June and the credentials in it remain valid until rotated, so the reset of stealer-log accounts matters more than the patch date.
- 3. Treat every management plane the way Arista now tells VCO customers to treat theirs, by Friday 30 October.** Restrict the web interface to administrative networks, search the web log for encoded paths and the two advisory addresses, and apply 5.2.3.18, 6.1.3.10 or 6.4.2.12. The same control covers the Nextcloud and Plex entries, which are unauthenticated chains against anything that answers.
- 4. Add a view-source check to the release gate for every internally built or AI-generated web application, from Monday 26 October (carried from W43 Technical 2 with a second case).** Bootlegger delivered its data with the login page; the Domains.co.za client (3.3) shipped its administrator password in the page.
- 5. Export the week's indicators to blocklists on Monday 26 October and retro-hunt 30 days.** The two Qilin addresses from the aggregator's feed, the Unit 42 nine, the Arista two, the Wordfence and Sophos PHP2Shell sets, the Microsoft Storm-0940 addresses and the AARTO domain patterns are in iocs_w44.csv with their sources. The W43 sets stand.
- 6. If any Microsoft 365 tenant has had a ConnectWise application consented, check the three application identifiers in iocs_w44.csv against service-principal sign-ins since 1 October on Tuesday 27 October.** An hour per tenant; managed service providers run it for every client.

Management (CISO / Board)

- 1. Table the FNB instruments at the Monday 2 November risk committee, with two questions.** Which security compromises and complaints from 2022 to 2026 are still open with the Information Regulator, who owns each, and what would a 90-day report on them contain; and whether any customer, member or applicant data is reachable through a role classification error of the kind the notice describes, since the fine attached to account numbers reached by misclassified users and the number of people exposed carried none.
- 2. For an insurer, administrator, scheme or fund, re-run the first-48-hours plan against the RMA facts by Friday 30 October (Action 3; carried from W42 and W43 with one addition).** The addition is the regulated clock: where Joint Standard 2 applies, the Prudential Authority or FSCA notification is due within 24 ordinary hours of classifying the incident as material, and that classification decision needs an owner.

3. Ask the executive, for Monday 2 November, for the answer the Presidency could give and twelve of seventeen state sites announcing a PHP version could not: which internet-facing systems run which engine, who owns each, and how long a patch takes. The deliverable is a maintained inventory.

4. Decide the organisation's position on edge appliances as a class before the next zero-day, by Friday 30 October (carried from W43 Management 3 with this week's evidence). Four NetScaler, three Fortinet, two VeloCloud Orchestrator and two Secure Email Gateway exploited flaws have entered the catalogue since 1 September, and this week's reporting shows the groups with South African listings buying the resulting credentials. The policy question is whether management interfaces may face the internet at all, and under what exception; the inventory with the compromise-check column W43 asked for is the instrument.

5. Keep the election fortnight on the Monday 2 November agenda (carried from W43 Management 5) and add one item: who can say, within an hour, whether a site outage is hostile or housekeeping. The Presidency said "precautionary measure" on the day and avoided a week of speculation; a municipality, utility or media house whose site goes down on 4 November will need the same sentence ready, and the log evidence behind it.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH, 27th CONSECUTIVE WEEK

The South African cyber threat level remains HIGH for a twenty-seventh consecutive week (18 to 24 October 2026). Escalation to CRITICAL was considered on PHP2Shell and rejected: the exposure was universal and the exploitation real, but no South African compromise has been disclosed, the hosting layer mitigated before the patch, and the one state outage was precautionary and brief. De-escalation to MEDIUM was not in question: a flat week on the victim feed came with a PROBABLE extortion claim against a national insurer with medical records in the sample, mass exploitation of a flaw in the engine under most South African websites, three reports on how groups with South African listings buy their way through FortiGate and GlobalProtect, and an election nine days after publication.

Rationale

A COIDA insurer holding a million workers' claim files acknowledged an alert while an extortion clock runs. The sample a journalist saw holds identity documents, X-rays and medical certificates; the actor brand is new to South Africa, silent since 7 September and unreliable online; the volume is the actor's claim.

PHP2Shell was exploited before its patch and the state's estate announced old versions. Millions of attempts globally from 21 October, a Mirai operator by the 23rd, no catalogue entry by the 23rd, twelve of seventeen state sites disclosing a PHP version on an old one; the Presidency's precaution was the exception.

The edge-credential market now has names, dates and prices. k0t's 70,000 network-device credentials, Qilin and INC on CVE-2026-0257, The Gentlemen's edge preference, {fmt(FG)} FortiGates in South

Africa and no measurable GlobalProtect population.

The regulator fined a bank R1 million for a 2022 security compromise and said nothing. Eighty-eight people exposed, nine account numbers accessed, five conditions contravened, four years from confirmation to instrument; the year's compromises have no public instrument yet.

The victim feed was flat, the hand search found nothing, and the elections are on Wednesday 4 November. Zero ZA-tagged listings, zero under another tag across 90 names, four names from the group that posted 33 a week ago; no hostile election activity observed, the hacktivism score holds and the tests below are unmet.

Next-Week Watch (W45)

Rand Mutual Assurance. Whether the aggregator indexes RMA under Kazu in the 1 November retrieval (a miss would point to the site's uptime, an absence to a listing read from another source); an RMA statement naming the actor, the data categories and the regulator; an Information Regulator record; and what the site shows after 4 or 5 November. Reading the listing itself would settle the price and date.

PHP2Shell in South Africa. Whether CISA adds CVE-2026-109618 and 109619; whether any South African organisation discloses a compromise dated 17 to 21 October; whether the Presidency or SITA states what was done; whether TechCentral's twelve old-version state sites change. A disclosed compromise would move Government or Software Supply Chain scores; a catalogue entry would not.

The FNB instruments. Whether FNB pays, arranges instalments, elects trial or appeals under section 97 within 30 days of service; whether the regulator issues a statement or any outlet reports the matter; whether the 90-day report is made public.

The MikroTik measurement. Whether the 15,526 instances on port 1701 persist in the 1 November retrieval and whether the 8728 count stays near 3,165. Persistence with a flat API count would indicate a fingerprint change on Shodan's side; disappearance a rescan artefact; a rising API count would be the only reading that means more routers.

The election fortnight. Unchanged: an IEC or Real411 statement on volume or a specific operation; an outage of an IEC, municipal or media property attributed by the operator, as against a hacktivist channel's claim; any defacement or data claim against a municipality. A claim without an operator's confirmation stays CLAIMED; a precautionary outage with a stated cause, as on 23 October, does not count.

The catalogue. Whether SonicWall SMA 1000 CVE-2026-102255 is added, now three weeks after the first attempts; whether Ivanti publishes and names the privilege-escalation fix; whether GitLab CVE-2026-110264 acquires exploitation reporting; whether the Arista and Collabora entries, due 26 October, produce victim disclosures. The W43 edge missions stand.

The Gentlemen, Kazu and the 16 October batch. How many of the 33 names of 16 October confirm by 16 November (a third or more weighs against Microsoft's attention-seeking reading; fewer than five supports it); whether a four-name week is followed by another; whether Kazu lists anything else or stays dormant, which bears on whether the RMA listing is the group or a user of its name.

Carryovers. Ampath (sample, count, regulator, the notice itself); Europ Assistance (statement, marker); Aeroklas Duys (statement, a third South African Deadlock listing); e-Panic (case number, report); Bootlegger (section 22 record); TFG London (update, actor claim). The NetScaler fortnight for a South

African compromise closed on Sunday 25 October unobserved.

Collector tasks. Ivanti Connect Secure, PAN-OS GlobalProtect, Nextcloud and PHP-engine fingerprints for the panel; retire the SonicWall family sum; the port-concentration test, eight weeks outstanding; the name-keyed world-feed search; the Saturday-evening media sweep, to include TechCentral's category page; the Ampath notice and the FNB enforcement notice as evidence files.

Closed this week. The W42 NetScaler fortnight (unobserved). The Atlassian CVSS question (NVD 9.3 on version 4.0). The W43 SMA 1000 catalogue question (not added by 23 October; carried as a new question). Carried without re-argument: BCX, Guardrisk and CoverCubed, RelyComply, LegalWise, Samwumed and Edcon, Tharisa, ATNS, BlackLocks, Cell C Fibre, Cartrack, VSB Attorneys, Rohloff, The Courier Guy, Babcock, the Furniture Bargaining Council, Toyota's SMS provider, Implats, Hungry Lion and Rand Water.

12. OSINT SOURCES CONSULTED

All sources are TLP: CLEAR and publicly accessible, numbered in order of first citation. Every cited URL was retrieved and confirmed to contain the claim attributed to it, on 25 October 2026, with these exceptions: the CISA catalogue URL is the public location of a file read locally; MyBroadband's Presidency article could not be fetched and the item is cited through TechCentral; SonicWall's advisory page for CVE-2026-102255 returned an empty body and is not cited; the Microsoft Digital Defense Report (W43) was again not retrieved. **Collection notes.** The feed run completed at 02:05 UTC on 25 October 2026 and passed its integrity check: 1,756 catalogue entries at version 2026.10.23; 138 victim records with filter purity 1.0; 53 NVD and 53 EPSS entries; 28 Shodan results, one promoted (Plex) and two held (Collabora, SiteGuard). The RSS sweep read 57 of 72 feeds; the same fourteen failed for a third or later run (Daily Maverick, IOL, ITWeb's two feeds, News24, Polity, Engineering News, INTERPOL, Bishop Fox, Volexity, Cyble, Sansec, Blackpoint Cyber and Sophos) and Rapid7 failed on a parse error for a second run; no Daily Maverick or News24 item in the window was located. The UmBra group page served an 18 October render and is cited as such. **Correction to a prior edition.** W43 omitted The Foschini Group's 13 October investor notice on the TFG London incident; it is added in Section 1 and 3.5 and the W43 confirmations count is corrected from two to three. **Exposure panel notes.** The MikroTik RouterOS count moved from 3,947 to 19,498 on a change in composition (15,526 on port 1701) and is published with that caveat and the flat API-port count; the Arista VeloCloud zero stays PROVISIONAL and is not an absence; no query exists for PHP, Nextcloud, Ivanti Connect Secure or a working GlobalProtect fingerprint; LiteLLM (6,559) and ScreenConnect (2,700) are disclosed and not published for an eighth week; the SonicWall family sum (3,230) is withdrawn per W43. **Provenance.** Every ransomware.live, NVD, EPSS and Shodan figure was retrieved from those services' APIs; the rendered ransomware.live pages are cited as cross-checks and for the hand search. **Conflicts, single sources and exclusions.** MyBroadband's Kazu attribution and TechCentral's unnamed forum post, with their differing price and date, are both carried and neither adopted; Arista's CVSS 3.1 figure of 9.9 is noted beside the feed's 4.0 figure of 9.4; Unit 42 gives 13 May 2026 as the catalogue date for CVE-2026-0257 where the catalogue file reads 29 May, and the file is used. Absence claims about coverage rest on the RSS sweep and hand searches described above, in a week when the ITWeb, Daily Maverick, News24, IOL and Polity feeds were unreachable. Single-source: the RMA sample description, the Domains.co.za account and the AARTO domain list (MyBroadband); the state-site survey (TechCentral); the kOt research (Group-IB and NyxLab via The Hacker News); the Nextcloud web-shell indicators (community forum). Excluded: Kazu's volumes, price and date; the identity of the Domains.co.za client; the Smishing Triad attribution;

Microsoft's 2,250 figure as compromises (it counts attempts); any inference that a reported PHP version proves vulnerability.

1. MyBroadband, 130-year-old financial provider that works with some of the biggest companies in South Africa hit by alleged 366GB cyberattack, by Luis Monzon (23 October 2026). <https://mybroadband.co.za/news/security/673772-130-year-old-financial-provider-that-works-with-some-of-the-biggest-companies-in-south-africa-hit-by-alleged-366gb-cyberattack.html>
2. TechCentral, Rand Mutual Assurance probes alleged theft of 1.68 million claim records, by Duncan McLeod (23 October 2026). <https://techcentral.co.za/rand-mutual-assurance-data-breach-claim/287621/>
3. ransomware.live, group page for Kazu, read 25 October 2026 (20 victims, 12 countries, none ZA; last discovery 7 September; uptime 15.4 per cent; RMA not listed). <https://www.ransomware.live/group/kazu>
4. The Hacker News, PHP issues emergency patches for two critical PHP2Shell RCE flaws as exploit attempts emerge, by Swati Khandelwal (21 October 2026). <https://thehackernews.com/2026/10/php-issues-emergency-patches-for-two.html>
5. BleepingComputer, Amazon says PHP2Shell exploitation began 4 days before patches, by Sergiu Gatlan (22 October 2026). <https://www.bleepingcomputer.com/news/security/amazon-says-php2shell-exploitation-began-4-days-before-patches/>
6. The Hacker News, PHP2Shell exploit attempts hit millions as attackers try to deploy Mirai malware, by Ravie Lakshmanan (23 October 2026). <https://thehackernews.com/2026/10/php2shell-exploit-attempts-hit-millions.html>
7. TechCentral, Global PHP scramble reaches the Union Buildings, by Duncan McLeod (23 October 2026). <https://techcentral.co.za/presidency-website-offline-php-scramble/287614/>
8. MyBroadband, South African companies scrambled to protect customers from critical PHP security flaw, by Jan Vermeulen (22 October 2026). <https://mybroadband.co.za/news/cloud-hosting/673628-south-african-companies-scrambled-to-protect-customers-from-critical-php-security-flaw.html>
9. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.10.23, released 23 October 2026 19:30 UTC, retrieved 25 October (feeds/kev_2026-10-25.json). <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
10. Arista Networks, Security Advisory 0199, CVE-2026-114625, VeloCloud Orchestrator on-prem SQL injection (22 October 2026). <https://www.arista.com/en/support/advisories-notices/security-advisory/24838-security-advisory-0199>
11. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:00 UTC 25 October 2026 (feeds/shodan_za_2026-10-25.json). <https://www.shodan.io/search?query=country%3AZA>
12. Information Regulator, Enforcement notices register, checked 25 October 2026 (three entries dated 23 October 2026). <https://infoeregulator.org.za/enforcement-notices/>
13. Information Regulator, Enforcement Notice under section 95 of POPIA, First National Bank, signed 21 October 2026, published 23 October (security compromise confirmed 21 February 2022; 88 data subjects, 696 unauthorised individuals, nine account numbers; Conditions 1, 2, 3, 4 and 7; 90-day report). https://infoeregulator.org.za/wp-content/uploads/2026/10/FIRST-NATIONAL-BANK-ENFORCEMENT-NOTICE-211026_Redacted.pdf
14. Information Regulator, Infringement Notice under section 109(1) of POPIA, reference OIA-13-2023, First Rand Bank, known as First National Bank, signed 21 October 2026, published 23 October (fine R1,000,000 under section 105(1)). https://infoeregulator.org.za/wp-content/uploads/2026/10/FIRST-NATIONAL-BANK-INFRINGEMENT-NOTICE-211026_Redacted.pdf
15. Information Regulator, Infringement Notice under section 109(1) of POPIA, Central Johannesburg TVET College, signed 9 October 2026, published 23 October (fine R500,000). https://infoeregulator.org.za/wp-content/uploads/2026/10-INFRINGEMENT-NOTICE-CENTRAL-JOHANNESBURG-TVET-COLLEGE_Redacted.pdf
16. Michalsons, Information Regulator ramps up enforcement, by Tanika Upasani (2 September 2026). <https://www.michalsons.com/blog/information-regulator-ramps-up-enforcement/82825>
17. SANews, IEC enters into partnership to counter disinformation (20 October 2026). <https://www.sanews.gov.za/node/85074>
18. TechCentral, Fashion retailer TFG discloses cyberattack, Staff Reporter (13 October 2026). <https://techcentral.co.za/tfg-london-cyber-incident-phase-eight-hobbs-whistles/287214/>
19. BleepingComputer, TFG London cyberattack disrupts systems at Hobbs and Whistles retailers, by Bill Toulas (13 October 2026). <https://www.bleepingcomputer.com/news/security/tfg-london-cyberattack-disrupts-systems-at-hobbs-and-whistles-retailers/>
20. ransomware.live API, GET /v2/countryvictims/ZA, 138 records, za_records 138 against server_returned 138, filter purity 1.0, FREE v2 tier (delayed relative to PRO), retrieved 02:00 UTC 25 October 2026 (feeds/ransomwarelive_za_2026-10-25.json). <https://api.ransomware.live/v2/countryvictims/ZA>
21. ransomware.live, South Africa country page, cross-check only (138 victims, newest Europ Assistance South Africa 16 October; nothing discovered 18 to 25 October; read 25 October 2026). <https://www.ransomware.live/country/ZA>
22. ransomware.live, group page for The Gentlemen, read 25 October 2026 (1,007 victims; four listings 18 to 24 October, none South African; no published-data marker on the four SA records). <https://www.ransomware.live/group/thegentlemen>
23. ransomware.live, group page for Krybit, read 25 October 2026 (168 victims; six listings discovered 24 October, none South African). <https://www.ransomware.live/group/krybit>
24. ransomware.live, group page for Deadlock, read 25 October 2026 (109 victims; two listings 23 and 24 October, neither South African; Aeroklas Duys unchanged). <https://www.ransomware.live/group/deadlock>
25. ransomware.live, group page for Qilin, read 25 October 2026 (34 listings discovered 18 to 24 October, none South African by name or description). <https://www.ransomware.live/group/qilin>
26. ransomware.live, group page for nOn, read 25 October 2026 (44 listings 18 to 23 October; none South African). <https://www.ransomware.live/group/nOn>
27. MyBroadband, Motorists are under attack in South Africa, by Myles Illidge (23 October 2026). <https://mybroadband.co.za/news/security/673383-motorists-are-under-attack-in-south-africa.html>
28. Microsoft Security Blog, AI-driven, large-scale nation-state campaign using ARTEX enables supply chain compromise (21 October 2026, updated 23 October). <https://www.microsoft.com/en-us/security/blog/2026/10/21/storm-0940-uses-artex-agentic-ai-connectwise-supply-chain-compromise/>
29. The Hacker News, Hackers breach enterprise firewalls and VPNs, exposing over 70,000 credentials, by Ravie Lakshmanan (23 October 2026; Group-IB and NyxLab research). <https://thehackernews.com/2026/10/hackers-breach-enterprise-firewalls-and.html>
30. Palo Alto Networks Unit 42, Active exploitation of May 2026 PAN-OS CVE-2026-0257 (20 October 2026, updated 23 October). <https://unit42.paloaltonetworks.com/active-exploitation-of-pan-os-cve-2026-0257/>
31. Rand Mutual Assurance, corporate website home page, checked 25 October 2026 (no incident notice readable). <https://www.randmutual.co.za/>
32. SOCRadar, Ransomware Intelligence group profile: Kazu (updated 22 October 2026). <https://socradar.io/free-tools/ransomware-intelligence/groups/kazu>
33. The Presidency, www.presidency.gov.za, checked 25 October 2026 (home page reachable and rendering normally). <https://www.presidency.gov.za/>
34. ITWeb, PHP2Shell alarm a major cyber security wake-up call, by Chris Tredger (23 October 2026). <https://www.itweb.co.za/article/php2shell-alarm-a-major-cyber-security-wake-up-call/WnpNgM21VmP7VrGd>

35. MyBroadband, Vibe-coded South African website hacked just six days after launch, by Luis Monzon (18 October 2026). <https://mybroadband.co.za/news/security/672352-vibe-coded-south-african-website-hacked-just-six-days-after-launch.html>
36. Ampath Laboratories, website home page, read 25 October 2026 (no incident notice located). <https://www.ampath.co.za/>
37. Information Regulator, Media statements page, checked 25 October 2026 (newest item 21 September 2026). <https://infoeregulator.org.za/media-statements/>
38. ransomware.live, victim page for Europ Assistance South Africa (The Gentlemen), re-read 25 October 2026 (record unchanged, no marker). <https://www.ransomware.live/id/RXVyb3AgQXNzaXNOYW5jZSBtb3V0aCBBZnJpY2FAdGhlZ2VudGxlbWVu>
39. ransomware.live, group page for UmBra, read 25 October 2026 (served a render stamped 18 October 02:50 UTC; ten victims, none after 10 October). <https://www.ransomware.live/group/umbra>
40. Check Point Research, Thus spoke The Gentlemen (13 May 2026). <https://research.checkpoint.com/2026/thus-spoke-the-gentlemen/>
41. The Hacker News, Exposed infrastructure reveals how ransomware affiliates used AI agents to execute intrusions, by Ravie Lakshmanan (23 October 2026; SOCRadar research). <https://thehackernews.com/2026/10/exposed-infrastructure-reveals-how.html>
42. ransomware.live API, GET /groups, 412 groups with victim counts, retrieved 25 October 2026 and compared with the 18 October retrieval (feeds/r_l_groups_2026-10-25.json). <https://api.ransomware.live/v2/groups>
43. ransomware.live API, GET /iocs/[group] for groups active against South Africa, retrieved 25 October 2026 and diffed against 18 and 11 October (feeds/r_l_iocs_2026-10-25.json; two Qilin addresses added). <https://api.ransomware.live/v2/iocs/qilin>
44. NIST NVD, CVE API 2.0, CVSS base scores with scoring source for the 53 catalogue entries added in the last 45 days, retrieved 25 October 2026 (feeds/nvd_cvss_2026-10-25.json). <https://services.nvd.nist.gov/rest/json/cves/2.0>
45. FIRST, EPSS API, scores for the same 53 entries, retrieved 25 October 2026 (feeds/epss_2026-10-25.json). <https://api.first.org/data/v1/epss>
46. The Hacker News, CISA flags two actively exploited critical flaws in Collabora Online and Arista VeloCloud, by Ravie Lakshmanan (24 October 2026). <https://thehackernews.com/2026/10/cisa-flags-two-actively-exploited.html>
47. Nextcloud community forum, To Collabora Built-in users: update ASAP (3 October 2026, updated 17 October; community-reported indicators without vendor confirmation). <https://help.nextcloud.com/t/to-collabora-built-in-user-update-asap/250516>
48. Plex, Important security update for Plex Media Server v1.43.2 and earlier, forum advisory (1 September 2026, updated 19 October 2026). <https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319>
49. The Hacker News, CISA orders federal agencies to patch exploited Plex2Shell, Siemens, and SiteGuard flaws, by Ravie Lakshmanan (21 October 2026). <https://thehackernews.com/2026/10/cisa-orders-federal-agencies-to-patch.html>
50. EG Secure Solutions, SiteGuard Server Edition security alert 202610-1, CVE-2026-106931 (14 October 2026; exploitation confirmed by the vendor). <https://www.eg-secure.co.jp/siteguard/news/alert-202610-1>
51. Huntress, Rapid Response: php2shell, leaked critical PHP vulnerabilities CVE-2026-109618 and CVE-2026-109619 (20 October 2026, updated 21 October). <https://www.huntress.com/blog/php2shell-leaked-critical-php-vulnerabilities>
52. Wiz Research, PHP2Shell: AI uncovers critical RCE vulnerabilities affecting 70 per cent of the Internet (21 October 2026). <https://www.wiz.io/blog/php2shell-php-rce>
53. The Hacker News, PHP warns of another unpatched RCE risk two days after emergency PHP2Shell patches, by Swati Khandelwal (23 October 2026; CVE-2026-115560). <https://thehackernews.com/2026/10/urgent-php-warns-of-another-unpatched.html>
54. The Hacker News, Critical GitLab flaw (CVSS 10.0) could allow unauthenticated RCE across 12 years of releases, by Swati Khandelwal (21 October 2026; CVE-2026-110264). <https://thehackernews.com/2026/10/critical-gitlab-flaw-cvss-100-could.html>
55. The Hacker News, Attacker chains three Ivanti Connect Secure zero-days for root access, only two patched so far, by Swati Khandelwal (13 October 2026). <https://thehackernews.com/2026/10/attacker-chains-three-ivanti-connect.html>
56. Oracle, Critical Patch Update Advisory, October 2026 (20 October 2026; 1,295 new security patches). <https://www.oracle.com/security-alerts/cpuoct2026.html>
57. Oracle, Security Alert Advisory CVE-2026-91403, Java SE and GraalVM, distrust of eMudhra intermediate CA certificates (21 October 2026; CVSS 9.1). <https://www.oracle.com/security-alerts/alert-cve-2026-91403.html>
58. Oracle, Security Alert Advisory CVE-2026-114820, Java SE and GraalVM, removal of eMudhra root CA certificates (24 October 2026; CVSS 9.1). <https://www.oracle.com/security-alerts/alert-cve-2026-114820.html>
59. MyBroadband, South Africa's police force has cybercrime investigators in all 9 provinces, by Myles Illidge (20 October 2026). <https://mybroadband.co.za/news/security/672630-south-africas-police-force-has-cybercrime-investigators-in-all-9-provinces.html>
60. TechCentral, Discovery ranks cybercrime as its top risk, citing frontier AI, by Duncan McLeod (21 October 2026). <https://techcentral.co.za/discovery-cybercrime-top-risk-frontier-ai/287537/>
61. Cybercrimes Act 19 of 2020, section 54, Obligations of electronic communications service providers and financial institutions (acts.co.za consolidated text). https://source.acts.co.za/cybercrimes-act-2020/54__obligations_of_electronic_php
62. Moonstone, New IT and cyber incident reporting template now in effect (3 September 2026). <https://www.moonstone.co.za/new-it-and-cyber-incident-reporting-template-now-in-effect/>
63. ransomware.live API, GET /csirt/ZA, six South African CSIRTs from the FIRST directory, retrieved 25 October 2026 (feeds/r_l_csirt_za_2026-10-25.json). <https://api.ransomware.live/v2/csirt/ZA>
64. SARS, Scams and phishing alerts page, checked 25 October 2026 (newest alert SARS-SCAM-400, 2 September 2026). <https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>

TLP: CLEAR. Distributable without restriction. Compiled from open sources and from feeds retrieved under the compiler's own credentials, and identifies no South African organisation as running a specific exposed system.