



SOUTH AFRICA

CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief, Week 40 | 20 September - 26 September 2026

THREAT LEVEL: HIGH

TLP: CLEAR

Report ID: SA-CTI-2026-W40 | Classification: TLP: CLEAR

Published Monday 28 September 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 (W40)
- 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, 23rd consecutive week (20 September - 26 September 2026)

Story 1. A second South African insurer appeared on The Gentlemen's leak site three weeks after the first. Guardrisk, the Sandton cell-captive insurer owned by Momentum Group, was indexed by the aggregator at 08:48 UTC on Saturday 26 September with an estimated attack date of 21 September; the listing carries no data volume, no sample and no deadline, and Guardrisk had published nothing by the close of the window.^{1,2,3} The W39 watch item asked whether the group would extort a second insurer from the MIP client set; a second insurer has been listed, and whether it is an MIP client is not known from any public source, so the item is half answered. The Gentlemen's index grew from 867 to 888 victims in seven days and it was the second most prolific group worldwide in NCC Group's August count.^{4,5} Rated CLAIMED. First indexed by the aggregator on 26 September 2026.

Story 2. The two regulators answered on the MIP breach, and the answer settles where the duty sits. The Information Regulator told TechCentral on 25 September that it has received only MIP's section 22 notification, that the obligation rests on the responsible party for the processing concerned, and that paying a ransom neither establishes nor resolves compliance with POPIA. The Prudential Authority said third-party providers are not required to report to it, that the insurers carry the 24-hour duty under Joint Standard 2 of 2024, and it declined to confirm MIP's account that the breach was found not to be systemic.⁶ In the same week Bidvest Bank's section 22 notice, dated 17 September and located this week, named RelyComply, named DireWolf and listed three regulators notified; it closes the last open question from W39 and is the subject of the correction below.⁷ First reported by TechCentral on 25 September 2026.

Story 3. Ten vulnerabilities entered the CISA catalogue between 21 and 25 September, against seven the week before and fourteen in W38, and seven were past their remediation date on Monday 28 September.⁸ Five sit on the network edge: two Check Point flaws, one in the management server exploited in a handful of targeted attacks since 23 July and one in VPN certificate handling exploited on Spark firewalls since 12 September; an F5 BIG-IP APM heap overflow that F5 says has been exploited; a second Arista VeloCloud Orchestrator flaw in two months; and the second half of the MikroTik chain on an appliance population of 5,252 exposed in South Africa.^{9,10,11,12,13,14} Three of the ten have a published South African exposure figure, against none of last week's seven, and the vendors published log checks for four of them; Section 9 carries every one.

W40 CORRECTION TO W39: the W39 edition stated, in Story 2, Section 3.3, the Section 11 watch list and the LinkedIn post, that Bidvest Bank had not named the provider behind its 12 September customer notice, and it left the Bidvest half of the shared-provider question open. That was wrong at the time of publication. Bidvest Bank published a Notification of a Security Compromise in terms of section 22 of POPIA on its website dated 17 September 2026, inside the W39 window, naming DataSeed (Pty) Ltd trading as RelyComply as the provider, describing the intruder as understood to be affiliated with the DireWolf group, and recording notification to the Information Regulator, the Financial Sector Conduct Authority and the Prudential Authority.⁷ The page is script-rendered and returned only metadata to the W39

collection. The W39 count of nine organisations confirming exposure in that window should have been ten. The corrections KPI row records it, and Section 3.5 carries the notice.

KPI Dashboard

Metric	Current (W40)	Prior (W39)	Change	Direction
Overall SA threat level	HIGH	HIGH	No change (23rd week)	FLAT
ransomware.live SA cumulative	132	128	+4	UP
SA claims discovered inside the window (ZA tag)	4	0	+4	UP
Window claims surviving the nationality check	3 of 4	0 of 0	n/a	n/a
SA organisations confirming a breach or supplier exposure in the window	1	9 (corrected to 10)	-9	DOWN
New CISA KEV additions	10	7	+3	UP
KEV adds already overdue at publication	7	4	+3	UP
KEV adds with a published VERIFIED SA exposure figure	3 of 10	0 of 7	+3	UP
Corrections issued to prior editions	1	1	0	FLAT
Weeks since last IR substantive publication	16	15	+1	UP

Three notes on the table. The four claims are the feed's ZA-tagged listings discovered between 20 and 26 September: Guardrisk, Apollo 21, ARCA Unlimited Architects and Morula IVF. Morula IVF is an Indonesian fertility network whose .co.id domain and the aggregator's generated description place it in Indonesia, so it fails the nationality check and three survive; the aggregator's country field has now invented a South African victim five times and hidden one.¹⁵ The confirmations row counts one organisation, Telkom, which disclosed an incident in a BCX legacy testing environment on 25 September; the developer of the Gauteng e-Panic app acknowledged and fixed its exposure by private email to the journalist who found it, which is not a public statement and is not counted, and the Bidvest notice belongs to the W39 window and is counted there by correction.^{16,17} The Information Regulator row moves to sixteen: its answers to TechCentral on 25 September are a position given to a publication, and the register and media-statements page carry nothing later than 10 June and 2 June.^{18,19} The W39 watch list said an answer of that kind would count as a publication; on reflection that would have contradicted the W37 rule that an announcement is not an instrument, and this edition applies the W37 rule. The row is retired from W41 unless the register moves.

W40 KEY FRAMING: the regulators have said that the insurer owes the notification whatever the supplier did, and this week's leak-site listing suggests the next test of that rule is already under way. A South African board reading the Information Regulator's words alongside Bidvest Bank's notice has, for the first time, both halves of the standard: the regulator says the duty is the responsible party's and that paying does not discharge it, and one bank has shown what a notice that meets the duty looks like, naming the provider, the actor and the three regulators told. On the technical side the week is the network edge

again, with Check Point joining Cisco, Citrix, Fortinet and MikroTik in the overdue column, and Check Point, F5, Arista and Cisco shipping a one-line compromise check that a South African SOC can run before Tuesday 29 September. The question for a CISO on Monday 28 September is whether anyone in the organisation owns the list of edge appliances against which those checks must be run, because nine appliance families from seven vendors have been added to it since 8 September.

1. ransomware.live, victim page for Guardrisk (The Gentlemen), discovered 26 September 2026 08:48 UTC, estimated attack date 21 September 2026, retrieved 27 September 2026; the same record is in the locally retrieved country feed.
<https://ransomware.live/id/R3VhcmRyaXNrQHROZWdibnRsZWl1bg==>
2. Guardrisk, About Guardrisk (subsidiary of Momentum Group Limited; licensed non-life, life and microinsurance insurers; offices in Johannesburg, Cape Town, Durban, Mauritius and Gibraltar), checked 27 September 2026. <https://guardrisk.co.za/about/>
3. Guardrisk, Newsroom, checked 27 September 2026 (newest item 17 September 2025; no statement on any cyber incident).
<https://guardrisk.co.za/newsroom/>
4. ransomware.live API, GET /groups, 402 groups with victim counts, retrieved 27 September 2026 and compared with the 20 September retrieval (feeds/r1_groups_2026-09-27.json). <https://api.ransomware.live/v2/groups>
5. Infosecurity Magazine, Ransomware attacks reach record high for 2026, reporting NCC Group's August 2026 threat intelligence report (23 September 2026). <https://www.infosecurity-magazine.com/news/ransomware-attacks-reach-record/>
6. TechCentral, Insurers carry the can for MIP breach, regulators say (25 September 2026).
<https://techcentral.co.za/insurers-mip-breach-regulators/286482/>
7. Bidvest Bank, Notification of a Security Compromise in terms of Section 22 of POPIA: RelyComply cyber incident (notice dated 17 September 2026; read through a browser on 27 September 2026 because the page is script-rendered, and stored as evidence/w40_bidvestbank_important_notice_2026-09-27.txt). <https://www.bidvestbank.co.za/important-notice>
8. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.09.25, released 25 September 2026 18:58 UTC, retrieved 27 September 2026 (feeds/kev_2026-09-27.json). <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
9. Check Point, sk1000171, CVE-2026-93616: directory traversal and file upload allows execution of arbitrary script on the Management Server (created 20 September 2026, last modified 22 September 2026; read through a browser).
<https://support.checkpoint.com/results/sk/sk1000171>
10. Check Point, sk1000117, CVE-2026-85102: authentication bypass and remote code execution in Remote Access and Site-to-Site VPN (created 7 September 2026, last modified 24 September 2026; read through a browser).
<https://support.checkpoint.com/results/sk/sk1000117>
11. F5, K000162605: BIG-IP APM vulnerability CVE-2026-94127 (published 22 September 2026, updated 23 September 2026; read through a browser). <https://my.f5.com/manage/s/article/K000162605>
12. Arista, Security Advisory 0183, CVE-2026-93952 in VeloCloud Orchestrator on-prem (published 22 September 2026, updated 23 September 2026). <https://www.arista.com/en/support/advisories-notices/security-advisory/24765-security-advisory-0183>
13. The Hacker News, MikroTik chain let attackers take over MikroTik routers without a password or SSH key (23 September 2026).
<https://thehackernews.com/2026/09/mikrotrick-chain-let-attackers-take.html>
14. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:02 UTC 27 September 2026 (feeds/shodan_zs_2026-09-27.json). <https://www.shodan.io/search?query=country%3AZA>
15. ransomware.live API, GET /v2/countryvictims/ZA, 132 records, za_records 132 against server_returned 132, filter purity 1.0, FREE v2 tier (delayed relative to PRO), retrieved 02:00 UTC 27 September 2026 and stored as feeds/ransomwarelive_zs_2026-09-27.json.
<https://api.ransomware.live/v2/countryvictims/ZA>
16. MyBroadband, Telkom discloses BCX cybersecurity incident which was limited to legacy testing environment (25 September 2026). <https://mybroadband.co.za/news/security/669235-telkom-discloses-bcx-cybersecurity-incident-which-was-limited-to-legacy-testing-environment.html>
17. GroundUp, How Gauteng's new panic app exposed your data (23 September 2026).
<https://groundup.org.za/article/gauteng-panic-app-exposes-crime-reports-users-locations/>
18. Information Regulator, Enforcement notices register, checked 27 September 2026 (newest 2026 entry dated 10 June 2026).
<https://infoeregulator.org.za/enforcement-notices/>
19. Information Regulator, Media statements page, checked 27 September 2026 (no statement dated later than 2 June 2026; the media invitation of 27 August 2026 recorded in W39 is an invitation, not a statement). <https://infoeregulator.org.za/media-statements/>

TOP 3 ACTIONS THIS WEEK

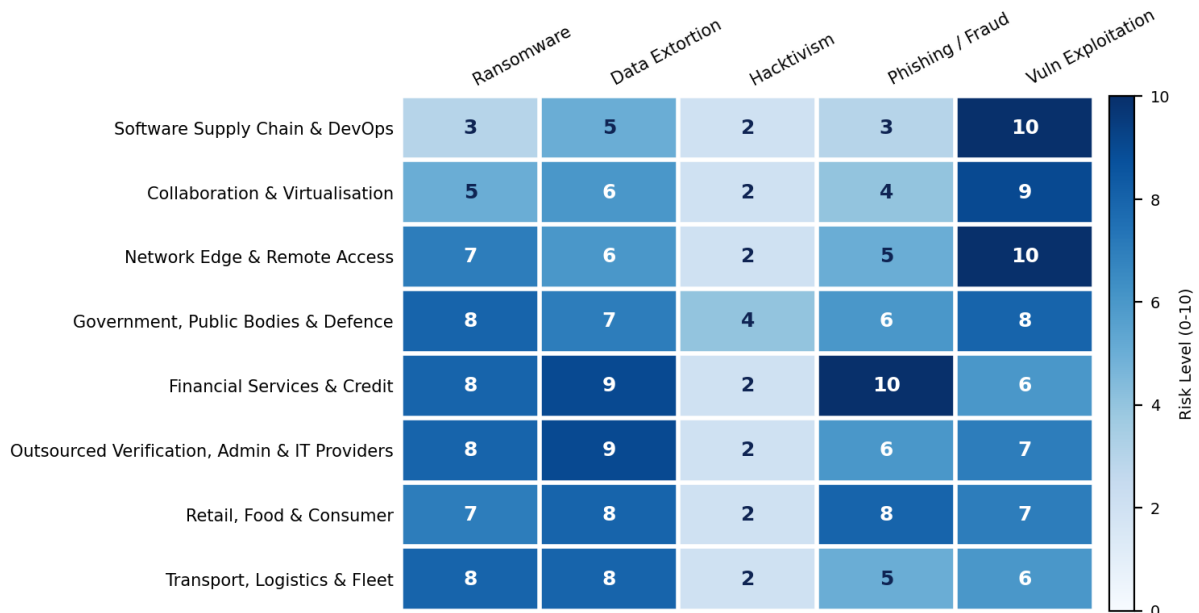
1. Run the Check Point and F5 compromise checks on Monday 28 September, before the patch and again after it. On every Security Management, Multi-Domain, Log and SmartEvent server, grep cpm.elg for a login request whose username exceeds 1,000 characters and for the ReflectionUtils error naming a path with ../ sequences; a hit with a matching FWM or MDS core dump is Check Point's own definition of an exploitation attempt. On every gateway and Spark firewall that allows certificate authentication for site-to-site or remote-access VPN, search Mobile Access logs after 12 September for certificate logins and inspect any subject reading CN=vpn, CN=vpn-user or CN=vpnuser. On any BIG-IP APM virtual server acting as an OAuth authorisation server, count repeated 01990004:3 invalid_token failures from one address in /var/log/apm, check tmctl global_oauth_stat for an unexplained rise in total_failed, and treat a TMM core file in the same window as a reason for human review. Restrict TCP/19009 and the management planes to trusted addresses while you patch.

2. If your organisation is an insurer, a policy administrator or a cell-captive participant, ask on Monday 28 September whether Guardrisk or MIP holds your customers' records, and prepare the section 22 notice before anyone asks you for it. The Information Regulator has now said in public that it received only MIP's notification for a breach that touched roughly 45 insurers, that the duty sits with the responsible party, and that an earlier notification is no blanket exemption from later obligations when the same data is published. Use Bidvest Bank's 17 September notice as the template: name the provider, name the actor as far as it is known, list the data classes, state which regulators were told, and give a contact channel. Where a cell captive or an underwriting manager sits between you and the insurer, agree in writing by Friday 2 October who issues the notice.

3. Finish the MikroTik and SharePoint work that the catalogue has now dated twice. South Africa exposes 5,252 RouterOS instances, 4,285 of them on the API port, and the second half of the MikroTrick chain fell due on Monday 28 September, fifteen days after the first half. Upgrade to 7.24.2, 7.23.4 or 6.49.21, check /user for an account named ops and the logs for a login attempt with the username -2, and close SSH and the API to the internet. On the 823 exposed SharePoint instances, confirm the August security update is installed (Subscription Edition 16.0.19725.20522, 2019 16.0.10417.20198, 2016 16.0.5565.1001) because Microsoft recorded reliable evidence of attacks on CVE-2026-65660 on 25 September, and it chains with the June authentication bypass.

2. THREAT LANDSCAPE HEATMAP

South African Sector Threat Levels, Week 40 (20 September – 26 September 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 that survives a 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. It is a forward-looking prioritisation aid rather than a measurement, and a sector with no observation this week carries its prior score rather than dropping to zero.

No row added or retired. The eight W39 rows stand. ARCA Unlimited Architects is a professional-services listing, and the Legal and Professional Services row was retired last week after one week on a single CLAIMED item; a second single CLAIMED item does not justify re-entering it, and the ARCA listing is scored in the narrative of Section 3.4 instead. The BCX incident sits under Outsourced Verification, Administration and IT Providers, where it holds the row's scores without raising them, because Telkom places it in a legacy testing environment with no customer impact found.¹⁶

Movements. Financial Services and Credit rises from 7 to 8 on ransomware: Guardrisk is the second South African insurer listed by The Gentlemen in three weeks, and Bidvest Bank's notice confirms a sixth customer in the RelyComply set and the first bank to name the provider.^{1,7} Transport, Logistics and Fleet rises from 7 to 8 on ransomware on the Apollo 21 listing by BlackLocks, the third transport or fleet name in five weeks after The Courier Guy and Cartrack.²⁰ Collaboration and Virtualisation rises from 8 to 9 on vulnerability exploitation: Microsoft recorded attacks on a SharePoint code-injection flaw on 25 September against 823 exposed South African instances.^{21,14} Retail, Food and Consumer rises from 6 to 7 on vulnerability exploitation on the Adobe Commerce and Magento authorisation flaw, exploited in the wild by Sansec's account and carrying the highest EPSS of the ten additions, and on the WordPress core flaw exploited within hours of its patch against a floor of 382 exposed South African sites.^{22,23} Network Edge and Remote Access holds at 10, which is the ceiling: Check Point, F5, Arista and MikroTik join the

overdue Cisco, Citrix and Fortinet entries. Government, Public Bodies and Defence holds: the Gauteng e-Panic exposure is a data-protection failure by a provincial contractor rather than an attack, and Rand Water produced nothing for a fourth week. Software Supply Chain and DevOps holds at 10 on vulnerability exploitation with WSO2 API Manager joining GitLab and Artifactory.

20. ransomware.live, group page for BlackLocks (new group, active; three victims, first discovered 5 September 2026), retrieved 27 September 2026. <https://www.ransomware.live/group/BlackLocks>

21. Microsoft MSRC, CVE-2026-65660, Microsoft SharePoint Server remote code execution vulnerability (released 11 August 2026, revision 1.2 of 25 September 2026; read through a browser). <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65660>

22. The Hacker News, WSO2 and Adobe Commerce flaws exploited in attacks, added to CISA KEV (25 September 2026). <https://thehackernews.com/2026/09/wso2-and-adobe-commerce-flaws-exploited.html>

23. The Hacker News, Attackers exploit WordPress CVE-2026-87902 within hours of disclosure (24 September 2026). <https://thehackernews.com/2026/09/attackers-exploit-wordpress-cve-2026.html>

3. TOP SA INCIDENTS (W40)

Five items. Two are leak-site claims from groups profiled in Section 4, one is a telecoms disclosure, one is a provincial app that exposed its users' locations, and one is a bank's notice that was published inside last week's window and located this week. Every rating follows the standing rule that a leak-site description is written by the attacker and cannot lift a rating on its own.

3.1 INC-2026-W40-01: Guardrisk Listed by The Gentlemen [CLAIMED]

Sector	Financial services and credit; cell-captive and specialist insurance
Organisation	Guardrisk Group, guardrisk.co.za, Sandton; subsidiary of Momentum Group Limited (JSE-listed); licensed non-life, life and microinsurance insurers
Listing	Indexed by ransomware.live at 08:48 UTC on Saturday 26 September 2026; the aggregator gives an estimated attack date of 21 September. No data volume, no sample, no deadline on the record. The description on the record is aggregator-compiled text about the company, which this report does not adopt
Confirmed	Nothing. Guardrisk's newsroom carried no statement at the close of the window and no South African publication had reported the listing
Context	Second South African insurer on the group's site in three weeks after Hollard (7 September), whose published data came from the MIP Holdings supplier breach. Whether Guardrisk is an MIP client is not stated by any public source and is not inferred
Confidence	CLAIMED. Threat-actor assertion only; no victim statement, no published data, no second source

The listing arrived in the last observed day of the window and is carried as a claim. Two things about it are known and one is not. It is known that the group has now listed two South African insurers in three weeks and that it published Hollard's data after Hollard refused a demand; it is known that the group's own leaked guidance to affiliates, as KELA read it in May, was to avoid India and Africa-style targets, which nine South African listings since January now contradict.^{1,24} It is not known whether the Guardrisk listing is a compromise of Guardrisk's own estate or a second downstream extortion from the MIP data set, and the two have different implications for every other insurer in the country. The distinguishing observations are

set out in Section 11. Guardrisk's cell-captive model means that the records at issue belong, in POPIA terms, to as many responsible parties as there are cells, which is the same structure that turned the MIP breach into 45 notifications.^{2,6} Detection relevance: TH-2026-W40-06 carries the group's file hashes and the backup-share exfiltration pattern documented in W39.

3.2 INC-2026-W40-02: Telkom Discloses BCX Incident in a Legacy Testing Environment [CONFIRMED]

Sector	Outsourced IT providers; telecommunications
Organisation	BCX, the IT services subsidiary of Telkom SA SOC Ltd
Disclosed	Telkom statement reported by MyBroadband on 25 September 2026: an incident identified within a limited area of a legacy testing environment, since contained and isolated from BCX's live production systems; no evidence to date that customer data was compromised; customer operations and services not affected; relevant customers notified as a precaution; specialist teams still investigating, with updates promised if verified findings materially change the position
Not disclosed	The date of the incident, the actor, any ransomware family, whether a demand was received, and whether any regulator was notified. No leak-site listing for BCX or Telkom in the feed since 2020
Confidence	CONFIRMED on the company's own statement. The scope statement is the company's and rests on an investigation it describes as continuing

BCX runs infrastructure and applications for a large share of South African corporate and public estates, so a testing environment at BCX is a supplier environment for its customers, and Telkom's decision to notify customers as a precaution follows the pattern the regulators described this week.¹⁶ The item is carried at the company's scope and will move if the position changes; the distinguishing observations are a leak-site listing naming BCX or a customer, or a further Telkom statement widening the environment. First reported by [MyBroadband](#) on 25 September 2026. Detection relevance: none specific; the standing supplier-integration review in Section 10 applies.

3.3 INC-2026-W40-03: Gauteng e-Panic Button App Exposed Users' Locations and Crime Reports [CONFIRMED]

Sector	Government and public bodies; provincial emergency services
Organisation	Gauteng Department of e-Government; app built and operated by Evolve Value Added Services of Midrand under a contract awarded 6 March 2024
Found	GroundUp's Joel Cedras reported on 23 September 2026 that the app's database could be reached without authentication: names, gender, age, phone numbers, email addresses, vehicle registrations, crime reports including domestic violence and assault, uploaded images, GPS coordinates and location histories back to the 2024 launch, and one-time PINs stored against cellphone numbers. GroundUp gave the department and Evolve 24 hours on 21 September; Evolve fixed the exposure on 22 September and described its actions in an email

Scale	More than 180,000 downloads since the 2024 launch by August 2026, of which only 15,000 came between October 2025 and August 2026; the Democratic Alliance put the total contract value at R269 million in the provincial legislature
Regulator	GroundUp's email to the Information Regulator drew an automated response directing it to the online portal. No department comment by publication
Confidence	CONFIRMED on the researcher's first-hand observation and the developer's acknowledgement and fix. The exposure is confirmed; whether anyone other than the researcher read the data is unknown

This is the second Gauteng provincial data exposure of 2026 and the first in a public-safety application whose whole value depends on users trusting it with their position. The stored OTPs are the technical detail that matters to a SOC: an unauthenticated read of a table holding live login codes and the numbers they belong to is account takeover without phishing. The R269 million figure and the download counts are the DA's, given in the legislature and reported by MyBroadband, and are carried as such.^{17,25,26} First reported by GroundUp on 23 September 2026. Detection relevance: none specific; Section 10 carries the API-authentication check for any public body running a citizen-facing app through a contractor.

3.4 INC-2026-W40-04: Apollo 21 and ARCA Unlimited Architects Listed by BlackLocks [CLAIMED]

Sector	Transport and fleet (truck, bus and trailer parts); professional services (architecture)
Organisations	Apollo 21, apollo21.co.za, head office Silvertondale, Pretoria, six branches nationally; ARCA Unlimited Architects, arcaunlimited.com, Pretoria, a multidisciplinary design firm
Listings	Both indexed by ransomware.live on 26 September 2026 (08:50 UTC and 17:07 UTC); the group's posts are dated 19 September and 22 September. Neither carries a data volume, sample or deadline; the listing text is a view counter
Group	BlackLocks, first seen by the aggregator on 5 September 2026 with a South Korean manufacturer; these are its second and third victims, and both are South African. Profiled in Section 4.2
Confirmed	Nothing. Neither company had published a statement and no South African publication had reported either listing at the close of the window
Confidence	CLAIMED for both. Threat-actor assertion only; the group has no track record against which to weigh it

Two Pretoria firms in one day from a group three weeks old is the week's tempo signal. The nationality check passes on the companies' own websites rather than on the aggregator's country field.^{20,27,28} Because the group is new, there are no encryptor samples, no ransom-note rule and no infrastructure indicators beyond two contact addresses in the aggregator's IOC feed, so the detection relevance is generic: TH-2026-W40-08 covers the valid-account entry through an SSL VPN that Kaspersky documents for another group this week and that fits an estate of this size.

3.5 INC-2026-W40-05: Bidvest Bank Names RelyComply and DireWolf in a Section 22 Notice [CONFIRMED]

Sector	Financial services and credit; banking
Organisation	Bidvest Bank Limited, bidvestbank.co.za
Notice	Notification of a Security Compromise in terms of section 22 of POPIA, dated 17 September 2026, on the bank's website under the page title RelyComply Cyber Incident, 8 September 2026. Names DataSeed (Pty) Ltd trading as RelyComply as a third-party provider used for anti-money-laundering transaction monitoring and sanctions screening; states the intruder is understood to be affiliated with the DireWolf group; states the bank's own systems and platform were unaffected
Data classes	Client name, contact details, identity or passport information, address, client-reference information and certain transaction information collected for regulatory purposes. The bank proceeds on the precautionary basis that the data may have been accessed or acquired; the forensic investigation had not established exfiltration at the date of the notice
Regulators	Information Regulator, Financial Sector Conduct Authority and Prudential Authority notified. Contact channel given: ccc@bidvestbank.co.za and 0860 11 11 77
Confidence	CONFIRMED on the bank's own notice. Attribution to DireWolf is the bank's characterisation and matches the aggregator's listing of RelyComply

The notice is carried for two reasons. It corrects W39, as Section 1 records, and it is the a complete section 22 notice: provider named, actor named as far as known, data classes listed, three regulators named, a contact channel given and a plain statement that the bank's own systems were not touched.⁷ With Bidvest named, the RelyComply set stands at EasyEquities, SA Home Loans, Peregrine Capital, Satrix, Alexforbes and Bidvest Bank confirmed, with Standard Bank investigating at last report. DireWolf's 14-day countdown from 9 September lapsed on or about 23 September; no publication of the RelyComply data was observed on the aggregator's record by the close of the window and RelyComply's notice has not been updated since 16 September, which with this group has previously meant a delay rather than a withdrawal.^{29,30} Detection relevance: TH-2026-W39-04 (integration credentials of a breached verification provider) stands as written and is not reprinted.

3.6 Carryovers

- MIP Holdings and Hollard, W39.** Developed. The two regulators' answers of 25 September are carried in Section 8.1; neither adds a fact about the intrusion itself. The Information Regulator has received only MIP's notification, which leaves open whether any of the roughly 45 insurers has notified in its own name.⁶ Both items stay CONFIRMED.
- RelyComply, W39.** The countdown lapsed with no observed publication; Bidvest Bank named the provider (Section 3.5). Stays CONFIRMED for the incident; DireWolf's 200 GB remains the actor's figure.
- Rand Water, W37.** No development for a fourth week. Nothing on the utility's website, no statement located, no attribution. The 3 October test set in W39 stands: silence a month after the SENS statement becomes the finding.³¹

Morula IVF, excluded. Listed by Everest on 25 September with a ZA tag. The company is an Indonesian fertility network: its domain is .co.id and the aggregator's generated description places every clinic in Indonesia. Excluded on the nationality check and not counted; Everest's only South African record remains Mediclinic Group in May 2025.¹⁵

Cell C Fibre, W39; Cartrack, W37; VSB Attorneys, W38; Rohloff Group, W36; The Courier Guy and Babcock Africa, W35; Furniture Bargaining Council, W36; Toyota South Africa's unnamed SMS provider, W34; Implats and Hungry Lion, W37. No development on any of them. All stay at their prior ratings and are carried without re-argument.

24. KELA, Inside The Gentlemen leak: how a new RaaS captured 10 per cent of 2026's global ransomware victims (14 May 2026).

<https://www.kelacyber.com/blog/the-gentlemen-ransomware-internal-chat-leak-analysis-2026/>

25. MyBroadband, South African emergency services app in the province with the most murders exposed the locations of users (23 September 2026). <https://mybroadband.co.za/news/security/668743-south-african-emergency-services-app-in-the-province-with-the-most-murders-exposed-the-locations-of-users.html>

26. MyBroadband, Gauteng spending R269 million for app downloaded 15,000 times in 10 months (25 September 2026). <https://mybroadband.co.za/news/gadgets/668550-gauteng-spending-r269-million-for-app-downloaded-15000-times-in-10-months.html>

27. Apollo 21, company website (head office 96 Siersteen Street, Silvertondale, Pretoria; six branches), checked 27 September 2026. <https://apollo21.co.za/>

28. ARCA Unlimited Architects, company website (Pretoria, South Africa; multidisciplinary design firm), checked 27 September 2026. <https://arcaunlimited.com/>

29. ransomware.live, victim page for RelyComply AML Platform (DireWolf, discovered 9 September 2026, country field GB, 200 GB claimed), re-read 27 September 2026. <https://ransomware.live/id/UmVseUNvbXBseSBBTUwgUGxhdGZvcmlAZGlyZXdvbGY=>

30. RelyComply, RelyComply cyber incident: what happened and what you can do, official notice (published 16 September 2026; re-read 27 September 2026, no later update on the page).

<https://relycomply.com/relycomply-cyber-incident-what-happened-and-what-you-can-do/>

31. Rand Water, corporate website, checked 27 September 2026 (no statement dated September 2026 on the incident). <https://www.randwater.co.za/>

4. THREAT ACTORS

Three profiles and a note. The Gentlemen, because it has now listed two South African insurers in three weeks; BlackLocks, because it is three weeks old and two of its three victims are South African; DireWolf, because its RelyComply countdown lapsed without a publication. A note on the PAYLOAD group closes the section.

4.1 The Gentlemen: Two Insurers in Three Weeks

The group's index rose from 867 to 888 between the 20 and 27 September retrievals, 21 listings in a week, after 30 the week before.⁴ NCC Group's August count, reported on 23 September, attributes 116 of August's record 1,073 attacks to it, second only to Qilin's 164 and ahead of Clop, DireWolf and INC Ransom; Africa was 2 per cent of the month's victims.⁵ Its South African record now stands at nine listings since January: Paltrack, Rola Motor Group and Witzenberg Municipality on 20 January, Intsika Yethu in February, Elundini in March, Sunspray Food in April, Babcock in August, Hollard on 7 September and Guardrisk on 26 September.¹⁵ The May leak of the operation's internal chats, as KELA analysed it, recorded a targeting preference for higher-income countries and Latin America and an instruction to avoid India and Africa-style targets, with negotiations run by affiliates on a 90/10 split; the South African record since then reads as an affiliate working against that guidance, or the guidance changing, and the two cannot be told apart from outside.²⁴ What can be said is that the Hollard case established the group will take a ransom

from a supplier and extort the supplier's customers afterwards, and that Guardrisk is the first insurer listed since. The aggregator's IOC feed carries 34 SHA-256 hashes, four SHA-1 and a set of MD5 values for the group's tooling, six Tox identifiers and one Session identifier; the ransom-note YARA rule matches the strings thegentlemen, THEGENTLEMEN and thegentlemen.onion. Every hash is exported to iocs_w40.csv with the endpoint it came from.^{32,33}

4.2 BlackLocks: Three Weeks Old, Two Thirds South African

BlackLocks appeared in the aggregator's index with a South Korean automotive-parts manufacturer discovered on 5 September, and its second and third listings, both on 26 September, are Apollo 21 and ARCA Unlimited Architects of Pretoria. The aggregator marks it as a new group and cautions that its claims should be treated with care until verified; the leak site is a single .onion host with a /leaks path and a view counter per post.²⁰ One vendor alert on the Korean listing calls the group Blacklocks, also known as BlackLock, which would tie it to the operation whose infrastructure Resecurity entered in early 2025; nothing on the aggregator's group record supports that link, the spelling differs, and this report does not assert it.³⁴ The IOC feed holds one Session and one Tox contact address for the group and nothing else; there is no YARA rule, no encryptor hash and no ransom-note name.³² Two South African SMEs in one day from an operation with no reputation to protect is either an affiliate with local access or a broker's inventory being worked through, and the distinguishing observation is whether the next listings are also South African.

4.3 DireWolf: The Countdown Lapsed

DireWolf's index held at 135 across the week.⁴ Its RelyComply listing of 9 September carried a 14-day countdown that ran out on or about 23 September; the aggregator's record still shows the listing screenshot and no data-published marker, RelyComply's notice is unchanged since 16 September, and no customer has reported published data.^{29,30} Bidvest Bank's notice is the first document from a RelyComply customer to name the group.⁷ The Cartrack listing of 2 September, also DireWolf, was confirmed by the company in W38 and W39; the group therefore holds two confirmed South African data sets and has published neither, which is the observation to weigh against its 43 attributions in NCC Group's August count.⁵

4.4 A Note on PAYLOAD

Kaspersky published on 21 September a case in which the PAYLOAD group achieved a ransomware outcome with no binary and no encryption: a valid account authenticated through a FortiGate SSL VPN, and two Group Policy Objects linked at the domain root pushed a ransom wallpaper, a logon banner, ransom-note files and the disabling of local administrator accounts to every domain-joined Windows host.³⁵ The group has one South African listing, CKR Consulting Engineers in July, and South Africa exposes 2,725 FortiGate instances, so the pattern is relevant here regardless of the group; TH-2026-W40-08 carries the GPO identifiers, file names and tool hashes from the report.^{15,14}

32. ransomware.live API, GET /iocs/{group} for the groups active against South Africa in the last 120 days, retrieved 27 September 2026 (feeds/rl_iocs_2026-09-27.json). <https://api.ransomware.live/v2/iocs/thegentlemen>

33. ransomware.live API, GET /yara/{group}, retrieved 27 September 2026 (feeds/rl_yara_2026-09-27.json). <https://api.ransomware.live/v2/yara/thegentlemen>

34. Brinztch, Blacklocks ransomware group lists South Korean firm Kwangmyung Industry as victim (6 September 2026). <https://www.brinztch.com/breach-alerts/brinztch-alert-blacklocks-ransomware-group-lists-south-korean-firm-kwangmyung-industry-as-victim>

35. Kaspersky Securelist, Group Policy hijacked: PAYLOAD ransomware weaponizes Active Directory GPO (21 September 2026). <https://securelist.com/tr/payload-ransomware-via-group-policy/121335/>

5. CRITICAL VULNERABILITIES & CISA KEV

Ten vulnerabilities entered the CISA catalogue of known exploited vulnerabilities between 21 and 25 September 2026, against seven the week before and fourteen in W38. Seven were past their remediation date on Monday 28 September, the day this report was published, and the remaining three fell due on that day.⁸ Every due date and overdue count in this section is arithmetic against the locally retrieved catalogue file, catalogVersion 2026.09.25, released at 18:58 UTC on Friday 25 September, so any addition made on Saturday 26 September is outside this edition; every CVSS score is from the NVD feed with its scoring source recorded.^{8,36} All ten carry knownRansomwareCampaignUse of Unknown, which is not the same as no. All ten received three-day deadlines under BOD 26-04. Four came with a vendor log check on the day of listing, the two Check Point entries, F5 and Arista; two came with the vendor's exploitation statement and no check, MikroTik and Microsoft; and for four, Zyxel, WSO2, Adobe and WordPress, the catalogue and third-party researchers are the record of exploitation, with Adobe's bulletin still stating that Adobe is not aware of exploits.³⁷

Check Point CVE-2026-93616 and CVE-2026-85102 arrived together on 22 September and are different problems. The first is a directory traversal and file upload in the Security Management Server web service that lets an unauthenticated attacker upload and run a script, scored 9.8; Check Point states it is exploited in the wild and that it is aware of a handful of customers who have been attacked, and The Hacker News dates the first targeted attacks to 23 July. It affects Security Management, Multi-Domain, Log and SmartEvent servers on R82.20 and on R82.10, R82 and R81.20 below Jumbo Takes 45, 127 and 170, and LivePatch Takes 28 and 29 do not fix it.^{9,38} The second is improper validation of certificate data during VPN negotiation on Security Gateways and Spark firewalls that allow certificate authentication, also 9.8; Check Point's update of 20 September states it has been actively exploited on Spark firewalls since 12 September, eleven days after the fix, with certificate subjects CN=vpn, CN=vpn-user and CN=vpnuser observed. Both advisories carry one-line checks, reproduced in TH-2026-W40-01.¹⁰ South Africa's Check Point population has no product label in the panel and no figure is published.

F5 BIG-IP APM CVE-2026-94127 is a heap overflow in the OAuth userinfo endpoint that gives an unauthenticated attacker code execution on any virtual server configured with an APM access policy and an OAuth authorisation-server profile; deployments using APM only as an OAuth client are not affected. F5 found it internally, published on 22 September with the sentence that it has learned the vulnerability has been exploited, and declined to say how widely; NVD carries 9.3 under CVSS 4.0 against F5's 9.8 under 3.1.^{11,39,36} watchTowr published the root cause on 23 September, an Authorization header copied into a 16,640-byte buffer without a length check, with a working exploit video; the fixes are engineering hotfixes for 21.1, 17.5 and 17.1 and an iRule available from support.⁴⁰ F5's advisory carries a three-part indicator set, repeated OAuth failures, suspicious commands and a TMM abort, that is the basis of TH-2026-W40-02.

Arista VeloCloud Orchestrator CVE-2026-93952 is the second on-prem VCO entry in two months. Arista states it was discovered externally and is known to be actively exploited; it needs certificate-based Edge authentication to be configured and the public part of an Edge certificate, and no tenant or operator credential. Fixes exist for the 5.2 and 6.4 trains and not yet for 6.1 or 7.0. Arista published file indicators, a

malicious MD5, two addresses and an nginx header, which TH-2026-W40-07 carries.^{12,41} The South African VeloCloud query returns zero by two methods and remains PROVISIONAL; under the evidence rules that zero is not published as an absence.

MikroTik RouterOS CVE-2026-67279 completes the MikroTrick chain that CERT Polska described: the SSH state-machine flaw lets an unauthenticated client open a session channel and send an exec request, and the September entry CVE-2026-86060 then reads the login program's identity from file descriptor 2 when the username is -2, giving full administrative access. Attack logs date to 2 September, a day before MikroTik shipped 7.24.2, 7.23.4 and 6.49.21; the observed attacker created an account named ops from 82.192.72.4, with attempts from 103.102.31.18.^{13,42} NVD scores this half 6.9 under CVSS 4.0, which is the lowest score in the table and the entry with the largest South African population: 5,252 RouterOS instances exposed, 4,285 of them on the API port 8728.^{36,14}

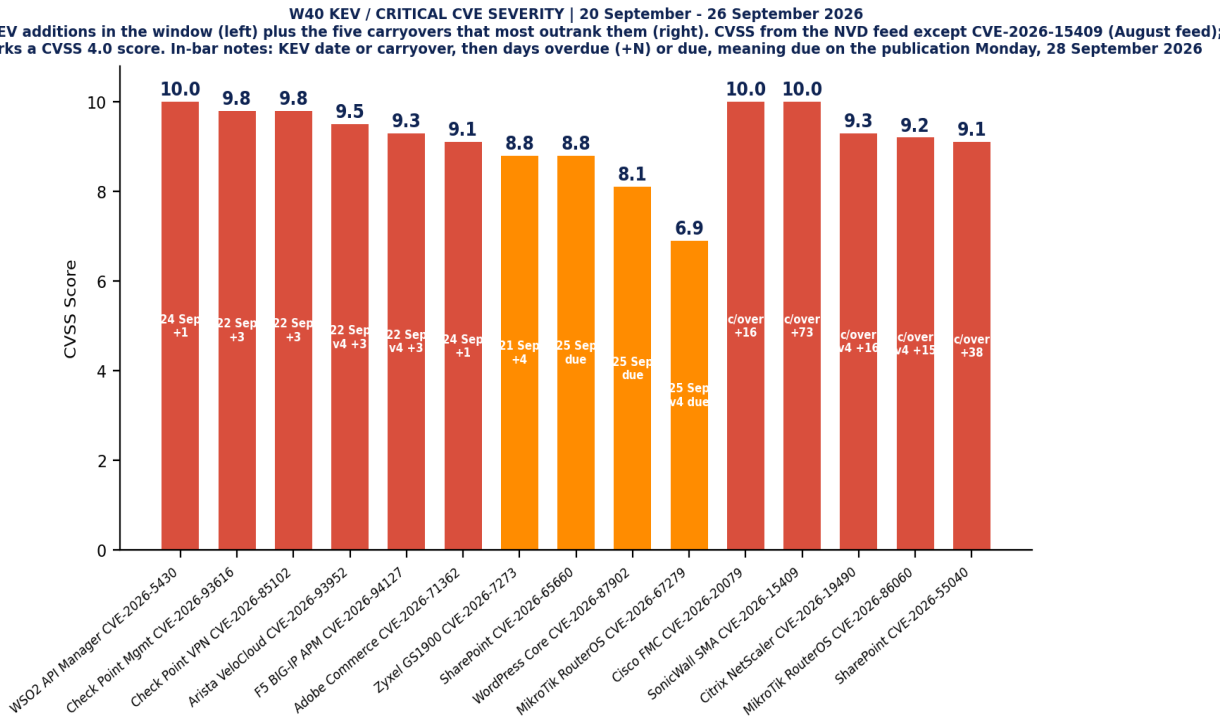
Microsoft SharePoint CVE-2026-65660 was patched on 11 August as a spoofing flaw scored 6.5, reclassified on 27 August as remote code execution at 8.8 for an authenticated low-privilege user, and revised again on 25 September with the sentence that Microsoft had reliable evidence of observed attacks. The researcher who found it notes it chains with the June authentication bypass for pre-authentication code execution.^{21,43} The W39 watch item on CVE-2026-69724 is resolved: that is a separate 8 September fix for a missing-authorisation flaw, also 8.8, marked not exploited and absent from the catalogue.⁴⁴ South Africa exposes 823 SharePoint instances.¹⁴

WordPress core CVE-2026-87902 is a remote file inclusion in page-template resolution that reaches code execution only where the active theme has a top-level directory beginning page- and a readable local .php target exists; the project scored it 9.2 and NVD's CISA-ADP record 8.1. Exploitation began at 11:49 UTC on 22 September, the day the 7.1.2 release and 24 back-ported branches shipped, using pearcmd.php as the target and staging web shells under /tmp and /var/tmp.^{45,23,36} The South African WordPress figure of 382 is a floor.¹⁴

WSO2 CVE-2026-5430 and Adobe Commerce CVE-2026-71362 entered on 24 September. The catalogue describes the WSO2 flaw as a path traversal leading to unrestricted file upload; the vendor advisory the catalogue links, WSO2-2026-5328 of 3 May, describes a JWT authentication bypass when a token is signed with an unsupported algorithm, and watchTowr's honeypots saw forged JWTs against it from 13 September. The two descriptions are recorded as they stand and the vendor's is followed for detection.^{8,46,22,47} The Adobe flaw is an incorrect authorisation in Commerce and Magento fixed in the August releases, exploited by Sansec's account and carrying the highest EPSS of the ten at 0.875, while Adobe's own bulletin still reads that it is not aware of exploits.^{37,48} **Zyxel GS1900 CVE-2026-7273**, the first addition of the week, is a LAN-side stack overflow in the switch CGI patched in June; it is adjacent-network only, and GreyNoise's Kapibala report of 21 September lists Zyxel switches among that actor's targets without naming the CVE.^{49,50}

Carryovers. The three Linux kernel entries fell due on 21 September; Red Hat has since acknowledged active exploitation and public exploits for all three without naming the activity, so they stay as patch items.⁵¹ Fortinet's advisory for CVE-2025-25249 was read this week: updated 23 February, it still prints Known Exploited: No and a vendor CVSS of 7.4 against NVD's 8.1 from the same PSIRT, which on publication Monday is nineteen days after the catalogue listed the flaw, and confirms the W38 finding.^{52,36} The Cisco email gateway and ISE entries reach +11 and +9, NetScaler, FMC and FortiOS +16, the MikroTik September pair +15, N-central and the August Adobe entry +17, ScreenConnect, GitLab and PaperCut +14, the SMA 1000 September pair +23, SharePoint CVE-2026-55040 +38, the July SMA pair with ransomware

use Known +73, Cisco FMC CVE-2026-20316 with ransomware use Known +58, the Pixel and Acronis entries +9, and LiteLLM CVE-2026-42271 +98.⁸



W40 CISA KEV / Critical CVE Tracking (ten additions 21 to 25 September plus active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-93616	Check Point Security Management, Multi-Domain, Log Server, SmartEvent	9.8	Path traversal, file upload (unauth)	25 Sept	KEV 22 Sept. OVERDUE +3. Vendor: exploited in the wild, a handful of customers attacked; THN dates first attacks 23 July. Fixed R82.20 hotfix, Jumbo Takes 45 / 127 / 170 / 192. LivePatch 28-29 do not fix. Check: cpm.elg username over 1,000 chars plus fwm/mds core; ReflectionUtils error with ../. No ZA product label. Ransomware: Unknown. EPSS 0.1965.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-85102	Check Point Security Gateway and Spark Firewall (VPN)	9.8	Improper cert validation (unauth RCE)	25 Sept	KEV 22 Sept. OVERDUE +3. Vendor: actively exploited on Spark firewalls since 12 Sept. Fixed LivePatch Take 26, Jumbo Takes 44 / 126 / 166 / 190, Spark R82.00.10 build 2325 and R81.10.17 build 4968. Check: Mobile Access certificate logins after 12 Sept; subjects CN=vpn, CN=vpn-user, CN=vpnuser. No ZA product label. Ransomware: Unknown. EPSS 0.0099.
CVE-2026-94127	F5 BIG-IP APM (OAuth authorisation server)	9.3 (v4.0)	Heap overflow (unauth RCE)	25 Sept	KEV 22 Sept. OVERDUE +3. Vendor: has learned it has been exploited; scale undisclosed. Engineering hotfixes 21.1.0.2.0.30.22 / 17.5.1.9.0.160.12 / 17.1.3.5.0.41.14; iRule from support. watchTower PoC 23 Sept. Check: repeated 01990004:3 invalid_token in /var/log/apm, tmctl global_oauth_stat, TMM core. No ZA product label (held). Ransomware: Unknown. EPSS 0.0223.
CVE-2026-93952	Arista VeloCloud Orchestrator on-prem	9.5 (v4.0)	Improper input validation	25 Sept	KEV 22 Sept. OVERDUE +3. Vendor: actively exploited; needs certificate-based Edge auth. Fixed 5.2.3.16 / 6.4.2.8; no fix yet for 6.1 or 7.0. IOCs: .vcnode.js, vc-sysmond (MD5 dc78e206...), vc-sysmon.service, x-vc-opt header, 142.93.149.77, 104.248.126.159. ZA query zero, PROVISIONAL. Ransomware: Unknown. EPSS 0.0090.
CVE-2026-7273	Zyxel GS1900 series switches	8.8	Stack overflow in CGI (LAN, unauth)	24 Sept	KEV 21 Sept. OVERDUE +4. Adjacent-network only. Patched June 2026, firmware 2.90(x.2)C0 per model. No vendor exploitation statement. No ZA product label (held). Ransomware: Unknown. EPSS 0.0250.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-5430	WSO2 API Manager, API Control Plane, Traffic Manager, Universal Gateway	10.0	Catalogue: path traversal; vendor: JWT auth bypass	27 Sept	KEV 24 Sept. OVERDUE +1. Advisory WSO2-2026-5328 of 3 May; watchTower honeypots saw forged JWTs from 13 Sept. Update levels per product; API Manager 4.1.0 to 4.6.0 affected. No ZA product label (held). Ransomware: Unknown. EPSS 0.0059.
CVE-2026-71362	Adobe Commerce and Magento Open Source	9.1	Incorrect authorisation (unauth)	27 Sept	KEV 24 Sept. OVERDUE +1. APSB26-92 of 11 Aug (fixed 2.4.9-aug to 2.4.4-aug) still states Adobe not aware of exploits; Sansec observed exploitation. Highest EPSS of the ten. No ZA product label (held). Ransomware: Unknown. EPSS 0.8751.
CVE-2026-67279	MikroTik RouterOS	6.9 (v4.0)	Workflow bypass (SSH, unauth)	28 Sept	KEV 25 Sept. Due on publication day. Second half of MikroTrick with CVE-2026-86060. Fixed 7.24.2 / 7.23.4 / 6.49.21. IOCs: username -2, account ops, 82.192.72.4, 103.102.31.18. 5,252 in ZA, 4,285 on port 8728. Ransomware: Unknown. EPSS 0.0103.
CVE-2026-65660	Microsoft SharePoint Server 2016, 2019, Subscription Edition	8.8	Code injection (authed RCE)	28 Sept	KEV 25 Sept. Due on publication day. Patched 11 Aug; reclassified RCE 27 Aug; Microsoft evidence of attacks 25 Sept. Builds 16.0.19725.20522 / 16.0.10417.20198 / 16.0.5565.1001. Chains with the June auth bypass. 823 in ZA. Ransomware: Unknown. EPSS 0.0210.
CVE-2026-87902	WordPress core 4.7.0 to 7.1.1	8.1	Remote file inclusion (unauth)	28 Sept	KEV 25 Sept. Due on publication day. Fixed 7.1.2 and 24 branches; project score 9.2. Exploited from 22 Sept 11:49 UTC; pearcmd.php target; shells in /tmp, /var/tmp. Seven attacker addresses in TH-05. 382 in ZA (floor). Ransomware: Unknown. EPSS 0.1817.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-76461	Cisco Secure Email Gateway (AsyncOS)	9.8	SQL injection (unauth, root)	17 Sept	Carryover. OVERDUE +11. ISE CVE-2026-76460 (10.0) reaches +9. Cisco log checks as in W39. No SA incident naming either appliance observed; no ZA product label, fingerprint still a collector task. EPSS now 0.2827 (was 0.0201), ISE 0.1403 (was 0.0078): EPSS lagging confirmed exploitation.
CVE-2026-19490	Citrix NetScaler ADC and Gateway	9.3 (v4.0)	Auth bypass (unauth)	12 Sept	Carryover. OVERDUE +16. FMC CVE-2026-20079 (10.0, EPSS 0.8818) and FortiOS CVE-2025-25249 (8.1; vendor page still Known Exploited: No) share the date. 111 in ZA; FortiGate 2,725. EPSS 0.0701.
CVE-2026-86060	MikroTik RouterOS	9.2 (v4.0)	Argument injection (SSH username -2)	13 Sept	Carryover. OVERDUE +15. CVE-2026-67277 shares the dates. First half of MikroTrick; see CVE-2026-67279 above. EPSS 0.0185.
CVE-2026-86218	N-able N-central	10.0 (v4.0)	Static code injection (pre-auth RCE)	11 Sept	Carryover. OVERDUE +17. Adobe Commerce CVE-2026-75650 (10.0) shares the date and the +17. Fixed 2026.3.1.14. No ZA product label. EPSS 0.1293.
CVE-2026-84869	ConnectWise ScreenConnect	9.9	Improper privilege management (client)	14 Sept	Carryover. OVERDUE +14. GitLab CVE-2026-85706 (10.0, EPSS 0.9143) and the PaperCut pair share the date and the +14. ZA figure omitted as an artefact, see 7.1. EPSS 0.0092.
CVE-2026-83548	SonicWall SMA 1000	10.0	SSRF (unauth)	5 Sept	Carryover. OVERDUE +23. CVE-2026-83549, Artifactory CVE-2026-82329, Kestra CVE-2026-49869 and Switchvox CVE-2026-9586 share the date and the +23. No SMA-specific ZA figure. EPSS 0.0876.
CVE-2026-55040	Microsoft SharePoint	9.1	Weak auth (JWT forgery)	21 Aug	Carryover. OVERDUE +38. 823 in ZA. Chains with CVE-2026-65660 above. EPSS 0.1754.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2025-39682	Linux kernel (TLS receive path)	9.8	Improper check (record handling)	21 Sept	Carryover. OVERDUE +7 with CVE-2026-53266 and CVE-2025-39964. Red Hat acknowledges active exploitation and public exploits; no activity named. Patch items, no hunt. No ZA product label.
CVE-2026-15409	SonicWall SMA 1000	10.0	SSRF (unauth)	17 Jul	Carryover. OVERDUE +73. CVE-2026-15410 shares the dates and the KNOWN ransomware flag; INC Ransom affiliate and UTA0533 attributed in July. LiteLLM CVE-2026-42271 at +98 is the deepest tracked. Rebuild rather than patch.

Pattern note: the week's ten divide by whether the vendor's page agrees with the catalogue. Check Point, F5, Arista and MikroTik say exploited and give you something to grep; Microsoft says exploited on a page that took six weeks and two revisions to describe the flaw correctly; WSO2's advisory describes a different vulnerability class from the one the catalogue lists under the same CVE; Adobe's bulletin and Fortinet's advisory still say no exploitation known for entries the catalogue has held for four and nineteen days respectively. A South African patch programme that gates on the vendor's exploitation flag would have skipped four of this week's ten, so gate on the catalogue. On EPSS, the two Cisco entries moved from 0.0201 and 0.0078 at listing to 0.2827 and 0.1403 two weeks later while nothing changed about their exploitation, which is EPSS lagging confirmed activity; Adobe's 0.875 is the one score this week that ran ahead of the catalogue and it is the entry whose vendor bulletin denies exploitation.⁴⁸ Three carryovers still outrank most of the additions: the July SonicWall pair at 73 days with ransomware use Known, SharePoint CVE-2026-55040 at 38 days against 823 exposed instances, and the MikroTik pair at 15 days against 5,252.^{8,14}

36. NIST NVD, CVE API 2.0, CVSS base scores with scoring source for the 61 catalogue entries added in the last 45 days, retrieved 27 September 2026 (feeds/nvd_cvss_2026-09-27.json). <https://services.nvd.nist.gov/rest/json/cves/2.0>

37. Adobe, Security update available for Adobe Commerce, APSB26-92 (11 August 2026). <https://helpx.adobe.com/security/products/magento/apsb26-92.html>

38. The Hacker News, Check Point warns of management server zero-day exploited in targeted attacks (22 September 2026). <https://thehackernews.com/2026/09/check-point-warns-of-management-server.html>

39. The Register, Someone's attacking a critical 0-day RCE in F5 BIG-IP APM (23 September 2026). <https://www.theregister.com/security/2026/09/23/someones-attacking-a-critical-0-day-rce-in-f5-big-ip-apm/5298659>

40. watchTowr Labs, Is this a joke? In the auth header? F5 BIG-IP unauthenticated heap overflow to RCE, CVE-2026-94127 (23 September 2026). <https://labs.watchtowr.com/is-this-a-joke-in-the-auth-header-f5-big-ip-unauth-heap-overflow-to-rce-cve-2026-94127/>

41. The Hacker News, New CVSS 10.0 VeloCloud Orchestrator flaw actively exploited in certificate-based setups (22 September 2026). <https://thehackernews.com/2026/09/new-cvss-100-velocloud-orchestrator.html>

42. MikroTik, September 2026 vulnerability notice (3 September 2026): fixed in RouterOS 7.24.2, 7.23.4, 6.49.21 and 7.25 beta 3. <https://mikrotik.com/supportsec/september-2026-vulnerability/>

43. The Hacker News, SharePoint flaw initially listed as spoofing by Microsoft enables authenticated RCE (22 September 2026). <https://thehackernews.com/2026/09/sharepoint-flaw-initially-listed-as.html>

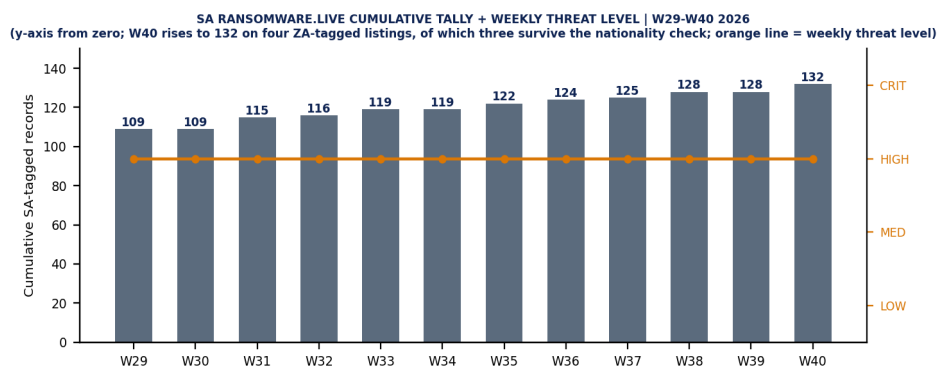
44. Microsoft MSRC, CVE-2026-69724, Microsoft Office SharePoint remote code execution vulnerability (released 8 September 2026, revision 1.1 of 17 September 2026; read through a browser). <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69724>

45. WordPress, security advisory GHSA-7hp8-65ch-5whp, CVE-2026-87902 (22 September 2026). <https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-7hp8-65ch-5whp>

46. WSO2, Security advisory WSO2-2026-5328, CVE-2026-5430 (published 3 May 2026). <https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2026-5328/>
47. BleepingComputer, CISA warns of SharePoint, WSO2, Adobe Commerce flaws exploited in attacks (25 September 2026). <https://www.bleepingcomputer.com/news/security/cisa-warns-of-sharepoint-wso2-adobe-commerce-flaws-exploited-in-attacks/>
48. FIRST, EPSS API, scores for the same 61 entries, retrieved 27 September 2026 (feeds/epss_2026-09-27.json). <https://api.first.org/data/v1/epss>
49. Zyxel, Security advisory for stack-based buffer overflow vulnerability in GS1900 series switches, CVE-2026-7273 (16 June 2026). <https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-stack-based-buffer-overflow-vulnerability-in-gs1900-series-switches-06-16-2026>
50. GreyNoise, Open season on Kapibala: attacker steals over 18,000 government records through WordPress exploitation (21 September 2026). <https://www.greynoise.io/blog/open-season-on-kapibala-attacker-steals-government-records-wordpress-exploitation>
51. Qualys, CISA BOD 26-04 timelines for three Linux kernel CVEs (23 September 2026). <https://blog.qualys.com/product-tech/2026/09/23/cisa-bod-26-04-timelines-for-three-linux-kernel-cves>
52. Fortinet PSIRT, FG-IR-25-084, heap-based buffer overflow in cw_acd daemon, CVE-2025-25249 (published 13 January 2026, updated 23 February 2026; read through a browser on 27 September 2026). <https://www.fortiguard.com/psirt/FG-IR-25-084>

6. RANSOMWARE LANDSCAPE

The South African victim feed held 132 records when retrieved at 02:00 UTC on 27 September 2026, four more than the week before. The collection is country-scoped by path, the written file records 132 South African records against 132 returned, the run log records filter purity 1.0 and a clean exit, and the tier is the delayed free v2.¹⁵ A set-difference against the 20 September file returns four additions and zero removals, all four discovered inside the window: Morula IVF (Everest, 25 September 16:28 UTC), Guardrisk (The Gentlemen, 26 September 08:48 UTC), Apollo 21 (BlackLocks, 26 September 08:50 UTC) and ARCA Unlimited Architects (BlackLocks, 26 September 17:07 UTC). Three survive the nationality check; Morula IVF is Indonesian. The derived South African count for the window is therefore three, and the feed total of 132 is reported as the aggregator publishes it. The aggregator's own country page, read as a cross-check, showed 131 with Apollo 21 and Guardrisk newest and without ARCA, consistent with a page cache older than the 17:07 UTC indexing.⁵³ The hand search of the world feed for South African victims under other country tags, the task recorded in W39 after RelyComply, was not run this week and remains a collector task.



Baseline at W39 close	128 records
New listings dated inside the window	4 with a ZA tag: Guardrisk (The Gentlemen), Apollo 21 and ARCA Unlimited Architects (BlackLocks), Morula IVF (Everest)
Surviving the nationality check	3. Morula IVF operates fertility clinics in Indonesia on a .co.id domain and is excluded; the aggregator's country field has invented a South African victim five times (Costa Rica twice, Philippines, India, Indonesia) and hidden one (RelyComply, GB)
Delistings or restorations	None. Set difference against the 20 September file returns four additions and zero removals
End count at W40 retrieval	132 records, filter purity 1.0 in the run log and 132 of 132 tagged ZA in the file
Groups active against SA, rolling 120 days	17 by discovery date, up from 15: BlackLocks and Everest enter on this week's listings. The rolling boundary moves each week, so this figure is not a trend
Threat-level drivers	A second insurer listed by The Gentlemen; a new group with two South African SMEs in a day; ten catalogue additions with seven overdue at publication; the regulators' answers on MIP

Group notes. The Gentlemen, BlackLocks and DireWolf are profiled in Section 4. Among the groups in the aggregator's index that have listed South African organisations this year, the week's movements were The Gentlemen from 867 to 888, Qilin from 2,298 to 2,315, INC Ransom from 941 to 949, Everest from 398 to 404, DragonForce from 651 to 657, LockBit 5.0 from 364 to 368, Krybit from 149 to 153 and BlackLocks from 1 to 3; DireWolf and Payload did not move, and two groups, cyberleek and imnotavillain, entered the index.⁴ NCC Group's August count, the record month of 2026 at 1,073 victims, put Africa at 2 per cent, which at the month's volume is roughly twenty organisations across the continent; the South African feed alone added eight in August.^{5,15}

Two intrusion patterns published this week that fit South African estates. Kaspersky's PAYLOAD case is the GPO-only ransomware described in Section 4.4. Huntress's INC Ransom timeline of 21 September describes a scheduled task named from random dictionary words running an obfuscated PowerShell implant from C:\ProgramData, a 17-day lull, then AnyDesk, a bring-your-own-vulnerable-driver step using a renamed Vicarius vRx binary and the driver HWAuidoOs2Ec.sys under a service named HwAudio, Impacket atexec for lateral movement, and two notes: INC-README.txt and, 53 minutes later, DATALEAK_PRESS_RELEASE.txt listing the paths searched and the files taken. INC Ransom has seven South African listings including Rohloff Group, confirmed in W38, and the two-note pattern is in iocs_w40.csv under the id SEC6-INC, separate from the hunt missions.^{54,15}

One measurement caution carried from prior editions and still binding. The victim feed is the free v2 tier and is delayed relative to the paid tier, so a listing dated inside this window may have been posted earlier, and one posted late on Saturday 26 September may not appear until next week's collection; the ARCA listing at 17:07 UTC on the Saturday shows how close the boundary sits. The window closes at the end of Saturday because an earlier edition ran to Sunday midnight and missed two South African victims in the unobserved hours.

53. ransomware.live, South Africa country page, cross-check only (showed 131 victims with Apollo 21 and Guardrisk newest when read on 27 September 2026, one short of the API file). <https://www.ransomware.live/country/ZA>

54. Huntress, The tale of two INC Ransom notes: a ransomware timeline (21 September 2026). <https://www.huntress.com/blog/two-inc-ransom-notes>

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 02:02 UTC on 27 September 2026, and none is a count of vulnerable systems; the version and vuln filters are not available on this plan, and rescan noise has moved single counts by more than 70 per cent inside a day, so week-on-week movement is not reported as a finding.¹⁴ Only queries whose product facet corroborates the fingerprint are published. This week's adds are served by three panel queries. MikroTik RouterOS: 5,252 instances, 4,285 on the API port 8728, 308 on 19999 and 215 on 8333. Microsoft SharePoint on-prem by http.component: 823, fingerprinted as IIS. WordPress by http.component: 382, a floor because component detection undercounts. The rest of the panel: FortiGate 2,725 (1,454 on 10443, 578 on 541); Citrix Netscaler 111 (109 on 443); Cisco ASA WebVPN 388 (348 on 443); Apache Tomcat 898; Remote Desktop on 3389, 8,222; services on port 445, 5,536, of which only 157 carry a Samba label; the SonicWall family 2,912 across five product strings, which cannot be narrowed to the SMA 1000 line; ownCloud 154; Metabase 130; MLflow 102; Langflow 75; Ray 71; Gitea 10; VMware vCenter 2; Artifactory 2.

Held and omitted. Four of this week's ten additions have no Shodan product label and were held by the discovery stage: WSO2, Adobe Commerce and Magento, F5 BIG-IP APM and Zyxel GS1900, each needing a hand-built http.html, component, favicon or port fingerprint before it can be measured. Check Point has no label in the panel either. VeloCloud returns zero by product match and by free text and stays PROVISIONAL, which under evidence rule 6 is not published as an absence. LiteLLM at 6,667 and ScreenConnect at 2,728 remain omitted as artefacts: their top five ports carry nine, eight, eight, seven and seven instances and three each respectively, against 4,285 on one port for MikroTik, and the collector's port-concentration test has still not been implemented, so both self-mark VERIFIED and are overridden by hand for a fourth week. Langflow, MLflow and Ray show the same scatter at totals of 75, 102 and 71; they are printed because the W38 test was written for populations too large for the product, and they carry this caveat until the collector applies the test to every auto-promoted query.¹⁴ The KPI row counts three of ten adds with a published figure.

7.2 Credential Exposure Around the Week's Victims

The aggregator's victim record for Guardrisk carries an infostealer panel: 495 passwords, 35 of them marked critical, three employees and one user with stealer-log records, four third-party employee credentials and three external attack-surface findings.¹ The RelyComply record carries six cookies and no critical passwords.²⁹ These are third-party stealer-log counts of unknown age, presented for the reader who runs an insurer's identity programme, and they do not say how either intrusion began. Set against them, the two supplier cases whose entry point is public both began with a credential: MIP's through a reused password on a personal laptop, and the PAYLOAD case in Section 4.4 through a valid account on an SSL VPN.^{6,35}

7.3 An Unauthenticated Citizen Database

The Gauteng e-Panic exposure in Section 3.3 was found without exploitation: the app's back-end could be read by anyone who looked, and it held live OTPs beside the numbers they were sent to. The check for any organisation with a contractor-built mobile app is the same one GroundUp ran: take the API endpoints from the app's own traffic and call them without a token.¹⁷

8. REGULATORY & POLICY

8.1 The Regulators Answer on MIP: Duty, Ransom and Systemic Risk

TechCentral published on 25 September the answers it was promised for 21 September. The Information Regulator confirmed it had received a section 22 notification from MIP only, said it was engaging MIP to establish the circumstances including the number of responsible parties and data subjects affected, and stated the principle that the obligation rests on the responsible party in respect of the processing concerned. On the ransom, it said payment should not be understood, in itself, as either establishing or resolving compliance with POPIA. On the Hollard publication, it said an earlier notification does not, as a general proposition, provide a blanket exemption from subsequent obligations. The Prudential Authority said third-party providers are not required to report to it, that supervised institutions must report material incidents within 24 hours under Joint Standard 2 of 2024, that a ransom payment does not conclude an incident or relieve an institution of its governance, notification and customer-protection responsibilities, and it declined to confirm MIP's account that the breach had been assessed as not systemic, saying it monitors incidents on factors including disruption and containment. Neither regulator would say which insurers had reported or when.⁶ Two readings follow. The first is that as of 25 September the regulator's only notification for a 45-insurer breach came from the operator, which either means the insurers have not filed or that the regulator counted MIP's consolidated filing; the distinguishing observation is in Section 11. The second is that the answers are given to a publication and not issued by the regulator, so the register and the media-statements page are unchanged and the KPI counter moves to sixteen weeks.^{18,19}

8.2 Bidvest Bank's Notice as the Working Standard

Section 3.5 sets out the notice. For a compliance officer its structure is the useful part: a section 22 heading and date; the provider named with its registered entity; the purpose for which the provider processed the data; the actor as far as known; a plain statement that the bank's own systems were unaffected; the data classes, qualified per person; the precautionary basis on which the bank proceeds while forensics continue; the three regulators notified; ten specific precautions for data subjects; and a contact channel. It reads as a notice drafted to the section rather than to a press cycle.⁷ Set beside the Information Regulator's statement that only MIP notified, it is also evidence that at least one institution in the RelyComply set filed in its own name.

8.3 Courts: FIC Information and Discovery Under POPIA

The Supreme Court of Appeal held on 23 September, in a unanimous judgment by Koen JA with Nedbank and Absa intervening, that information the Financial Intelligence Centre holds under FICA cannot be treated as ordinary litigation material: section 40(1)(e) confers no automatic right of access, a litigant must first establish an existing legal entitlement, relevance alone creates no right to receive, accountable institutions keep a confidentiality interest in what they submitted, and affected parties must be joined. For a bank's compliance function the judgment protects the suspicious-transaction reports it files from becoming discoverable by the party reported, which is the concern the interveners raised.⁵⁵ Werksmans' note of the same week on discovery and POPIA reads sections 10, 13, 12(2)(d)(iii), 15(3)(c)(iii) and 72 against Rule 35 and argues that a discovery request without a defined litigation purpose cannot satisfy minimality; it is the practical companion to the judgment for anyone producing customer records in litigation.⁵⁶

8.4 Provincial Accountability: The e-Panic Contract

The exposure in Section 3.3 sits inside a contract the Democratic Alliance put at R269 million in the Gauteng legislature, with R131.3 million paid over three financial years and 15,000 downloads in the ten months to August 2026. The department did not answer GroundUp before publication and the Information Regulator's mailbox returned an automated referral to its portal.^{26,17} Under POPIA the department is the responsible party and Evolve the operator; the section 22 duty is the department's, and no notice had been published by the close of the window.

8.5 Fraud Advisories and Who to Call

SARS issued no new scam alert in the window; the newest remains SARS-SCAM-400 of 2 September, the High Court summons lure, with the eFiling season running to 23 October.⁵⁷ GoTyme Bank warned on 26 September of discounted-flight advertisements on Facebook and Instagram that collect contact details, hand the victim to a WhatsApp consultant, and end in an app install that gives the fraudster control of the phone and its banking; the defence the bank gives is the standing one, never install an app on someone's instruction and never share a PIN, password or OTP.⁵⁸ No parliamentary committee meeting on cyber matters could be located for the week of Heritage Day.

Who to call. South Africa has six incident response teams in the FIRST directory, and a reader who has spent this series notifying the Information Regulator should also know them. The Cybersecurity Hub (cybersecurityhub.gov.za, kpillay@cybersecurityhub.gov.za) serves government and the private and public sectors; ECS-CSIRT at the State Security Agency (ecs-csirt@ssa.gov.za) serves government and the military; SA NREN CSIRT (csirt@sanren.ac.za) and UCT CSIRT (uctcsirt@uct.ac.za) serve research and education; Standard Bank Group CSIRT (csirt@standardbank.co.za) and Vodacom's Cyber Intelligence Centre (cisim@vodacom.co.za) serve their own constituencies and will take a report that touches them.⁵⁹ A ransomware event at a regulated financial institution has, from this week's regulators' answers, three clocks: 24 hours to the Prudential Authority under Joint Standard 2, 72 hours to SAPS under section 54 of the Cybercrimes Act, and as soon as reasonably possible to the Information Regulator under section 22.⁶

55. Moonstone, SCA draws the line on access to FIC information (25 September 2026), on the Supreme Court of Appeal judgment of 23 September 2026. <https://www.moonstone.co.za/sca-draws-the-line-on-access-to-fic-information/>

56. Werksmans, When discovery meets data privacy: navigating the tension between litigation obligations and data protection (23 September 2026). <https://werksmans.com/when-discovery-meets-data-privacy-navigating-the-tension-between-litigation-obligations-and-data-protection/>

57. SARS, Scams and phishing page, checked 27 September 2026 (newest alert SARS-SCAM-400, 2 September 2026). <https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>

58. MyBroadband, Cheap flight scams emptying bank accounts in South Africa (26 September 2026). <https://mybroadband.co.za/news/banking/668587-cheap-flight-scams-emptying-bank-accounts-in-south-africa.html>

59. ransomware.live API, GET /csirt/ZA, six South African CSIRTs from the FIRST directory, retrieved 27 September 2026 (feeds/ri_csirt_zs_2026-09-27.json). <https://api.ransomware.live/v2/csirt/ZA>

9. WEEKLY THREAT HUNT & IOCs

Eight missions. Three P1 cover edge appliances with confirmed exploitation this week: the two Check Point flaws and the F5 APM OAuth server, each with a vendor log check, and the completed MikroTik chain on the largest exposed population in the panel, whose indicators are CERT Polska's. Three P2 cover SharePoint, WordPress and The Gentlemen's tooling in the light of the Guardrisk listing. Two P3 cover the Arista orchestrator indicators and the GPO-only ransomware pattern that Kaspersky published. Indicators come from vendor advisories, named responder reporting and the aggregator's per-group feeds, and the atomic detail is exported to iocs_w40.csv rather than repeated in full here.³² No hunt is repeated from a prior week without new justification: the W39 Cisco, RelyComply-integration and reused-password missions stand as written and are not reprinted.

TH-2026-W40-01: Check Point: Management Server Traversal and VPN Certificate Bypass

P1 CRITICAL: both exploited in the wild per the vendor; overdue since 25 September

Hypothesis: An attacker has uploaded and executed a script on a Security Management, Multi-Domain, Log or SmartEvent server through the pre-authentication traversal in CVE-2026-93616, or has authenticated to a Security Gateway or Spark firewall over site-to-site or remote-access VPN with a forged certificate through CVE-2026-85102, and is now scanning internal services from the appliance.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1133 (External Remote Services), T1556 (Modify Authentication Process), T1046 (Network Service Discovery), T1078 (Valid Accounts).

IOCs: Management: a login request in cpm.elg whose username exceeds 1,000 characters, matched by the vendor's grep against \$MDS_FWDIR/log/cpm.elg*, with an fwm or mds core dump in /var/log/dump/usermode/ at the same time; an ERROR upgrade.base.ReflectionUtils Failed to load allResourceFiles map entry whose path contains ../ sequences. VPN: Mobile Access log-in events with a certificate after 12 September 2026; certificate subjects CN=vpn,OU=users,O=global, CN=vpn-user,OU=users,O=global, CN=vpnuser,OU=users,O=global (vendor list, not exhaustive).

Data Sources: cpm.elg on every management-plane server; /var/log/dump/usermode; SmartConsole or Spark Management Logs and Events view; gateway audit logs; netflow from the gateway toward internal segments.

Detection Guidance: Run both cpm.elg greps from Expert mode on every management server before patching and archive the output; a username hit with a matching core is the vendor's definition of an attempt. Query Mobile Access logs for product Mobile Access, action Log In and Certificate from 12 September, and inspect every event for a user, client or source you do not recognise; follow any confirmed unauthorised session into port scans and service enumeration from that source. Confirm the fix with cpinfo -y CPupdates (LivePatch Take 26) or the Jumbo Take, and note that LivePatch 28 and 29 do not fix the management flaw. Restrict TCP/19009 to trusted addresses and remove implied VPN rules for gateways that cannot be patched on Monday 28 September.

TH-2026-W40-02: F5 BIG-IP APM: OAuth Userinfo Heap Overflow**P1 CRITICAL:** vendor says exploited; public exploit video; overdue since 25 September

Hypothesis: An attacker has sent an oversized Authorization: Bearer header to /f5-oauth2/v1/userinfo on a BIG-IP APM virtual server configured as an OAuth authorisation server, crashed and re-entered TMM, and achieved code execution on the data plane through CVE-2026-94127.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1499.004 (Application or System Exploitation), T1059.004 (Unix Shell), T1543.002 (Systemd Service, via tmm.finish persistence as demonstrated by watchTower).

IOCs: Repeated /var/log/apm entries err tmm[.]: 01990004:3: : Request UserInfo from Source ID (null) IP failed. Error Code (invalid_token), ten or more in one log and especially from one address; an unexplained rise in total_failed from tmctl global_oauth_stat -s total_requests,total_userinfo_requests,total_failed; a TMM core file and SOD-issued SIGABRT in the same window; requests to /f5-oauth2/v1/userinfo with an Authorization header longer than 16,640 bytes (0x4100); modifications to /etc/bigstart/scripts/tmm.finish.

Data Sources: /var/log/apm, /var/log/audit, /var/log/ltm, tmctl statistics, core file directory, upstream proxy or IDS logs that see the request line and headers.

Detection Guidance: F5's own rule is three indicators close in time: OAuth failures, suspicious commands, TMM abort; treat the combination as a reason for human review and a single indicator as noise. Alert on the 01990004:3 string with a per-source threshold, and on any header over 16 KB to the userinfo path at the perimeter. Apply the engineering hotfix for your branch or obtain the iRule from F5 Support, and confirm with iHealth. Deployments using APM only as an OAuth client are out of scope; confirm which you are before closing the ticket.

TH-2026-W40-03: MikroTik: The Completed MikroTrick Chain on 5,252 Exposed Routers**P1 CRITICAL:** second half due 28 September; first half overdue +15; largest exposed population

Hypothesis: An unauthenticated client has opened an SSH session channel through CVE-2026-67279, sent an exec request with the username -2 to trigger CVE-2026-86060, obtained full administrative access to a RouterOS device, and created an account named ops for persistence.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1021.004 (SSH), T1136.001 (Create Account: Local), T1556 (Modify Authentication Process), T1090 (Proxy), T1071 (Application Layer Protocol).

IOCs: Login attempts with the username -2; a local account named ops not created by an administrator; source addresses 82.192.72.4 (successful attacks in CERT Polska's data) and 103.102.31.18 (attempts); the device reporting a Flagged status after upgrade; unexpected scripts, schedulers or user entries in the exported configuration. Fixed versions 7.24.2, 7.23.4, 6.49.21.

Data Sources: RouterOS system log and remote syslog, /user and /system script and scheduler exports, netflow from the router's WAN interface, Shodan or Censys for your own address space on 22, 8728, 8729 and Winbox.

Detection Guidance: Export /user, /system script, /system scheduler and /ip firewall from every device and diff against a known baseline; any ops account or unexplained script is an incident. Search logs for the -2 username and the two addresses. Upgrade, then re-check the Flagged status the vendor added, then close SSH and the API to the internet with an address list; 4,285 South African devices answer on port 8728 and none of them needs to. A device found compromised is netinstalled.

TH-2026-W40-04: SharePoint On-Prem: Code Injection After the JWT Bypass**P2 HIGH:** Microsoft evidence of attacks 25 September; 823 exposed in ZA; chains with June bypass

Hypothesis: An attacker holding low-privilege SharePoint credentials, or a session forged through the June authentication bypass CVE-2026-55040, has sent a crafted request that exploits CVE-2026-65660 to run code on the SharePoint front end.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1505.003 (Web Shell), T1059.001 (PowerShell), T1550.001 (Application Access Token).

IOCs: Farm builds below 16.0.19725.20522 (Subscription Edition), 16.0.10417.20198 (2019) or 16.0.5565.1001 (2016); w3wp.exe spawning cmd.exe or powershell.exe; new .aspx or .ashx files under LAYOUTS or in content databases; POST requests from external addresses to authenticated endpoints from accounts that have never used SharePoint; the July and August ToolShell indicators still apply to the same servers.

Data Sources: IIS logs, SharePoint ULS logs, Sysmon or EDR process creation on every web front end, file integrity on the 16 hive, Entra or AD sign-in logs for the service accounts.

Detection Guidance: Confirm the August update is installed on every front end and application server, because the September update guide revision changed the exploitation status of a patch many farms deferred as spoofing. Hunt w3wp child processes and any authenticated request path preceded by a session with no interactive logon. Where the farm is internet-facing and cannot be patched on Monday 28 September, put it behind pre-authentication at the proxy; 823 South African instances answer without it.

TH-2026-W40-05: WordPress Core: Page-Template Inclusion of pearcmd.php**P2 HIGH:** exploited from the day of disclosure; 382 exposed in ZA is a floor

Hypothesis: An attacker has requested a page template on a WordPress site whose active theme has a top-level directory beginning page-, caused get_page_template() to include /usr/local/lib/php/pearcmd.php, and used PEAR to write a web shell under /tmp or /var/tmp and fetch an uploader from GitHub.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1105 (Ingress Tool Transfer), T1036 (Masquerading).

IOCs: Requests resolving to /usr/local/lib/php/pearcmd.php; files named wp-pear-rce-flag.php, poc87902.php, luci_.php, zeta_.php; outbound fetches of raw.githubusercontent.com/MrG3P5/web-shell/refs/heads/main/uploader.php; attacker addresses 104.194.9.227, 43.250.53.42, 180.251.159.243, 195.178.110.247, 107.189.14.87, 45.61.184.170, 92.246.130.76 (Previdian and Patchstack, via The Hacker News). Fixed: 7.1.2, 7.0.6, 6.9.9, 6.8.10 and the back-ported branches to 4.7.37.

Data Sources: Web server access logs, PHP-FPM or mod_php error logs, file creation in /tmp and /var/tmp and the document root, egress proxy logs, WAF logs.

Detection Guidance: Inventory theme directories for a page- prefix first; sites without one are not exploitable by this path and can be patched in the normal cycle. On the rest, patch on Monday 28 September, then grep access logs for pearcmd and the seven addresses, list any .php written under /tmp since 22 September, and block the GitHub raw path at egress for web servers that have no reason to reach it.

TH-2026-W40-06: The Gentlemen: Tooling Hashes and Backup-Share Exfiltration Against Insurers**P2 HIGH:** second SA insurer listed in three weeks; 34 sourced hashes

Hypothesis: A Gentlemen affiliate with valid domain credentials inside an insurer or policy administrator is staging tooling whose hashes the aggregator's IOC feed records, mounting backup shares and opening virtual disks offline for the domain database, and exfiltrating with rclone before any listing.

MITRE ATT&CK: T1078 (Valid Accounts), T1021.002 (SMB/Windows Admin Shares), T1003.003 (NTDS), T1560.001 (Archive via Utility), T1567.002 (Exfiltration to Cloud Storage), T1486 (Data Encrypted for Impact).

IOCs: 34 SHA-256, 4 SHA-1 and 47 MD5 from the aggregator's /iocs/thegentlemen endpoint, unchanged since the W39 retrieval; twelve of the SHA-256 values were exported in W39 and the full set is exported to iocs_w40.csv (first three SHA-256: 025fc0976c548fb5a880c83ea3eb21a5f23c5d53c4e51e862bb893c11adf712a, 1334f0189a8e6dbc48456fa4b482c5726ab7609f7fa652fcc4c1a96f2334436f, 1af419b36a5edefef387409e2b3248c9223f7dc49a4f7b15ea095d371c3a70b2); the ransom-note YARA rule thegentlemen_Ransomnote matching thegentlemen, THEGENTLEMEN and thegentlemen.onion; the W39 Talos pattern of a CIFS mount under /mnt/Backup, VHDX under /mnt/vhdx, ntfs.txt and SAM.txt, zstd archives and rclone to Wasabi in 256 MiB chunks.

Data Sources: EDR file-hash telemetry, SMB audit on backup and file servers, Linux auth and mount logs on any jump host, egress logs for object-storage domains, DNS.

Detection Guidance: Load the 34 hashes into EDR and the YARA rule into mail and file scanning. Alert on any mount of a backup share from a host that is not the backup server, on libguestfs or qemu-nbd on a non-hypervisor, and on rclone or s5cmd binaries anywhere. Insurers and administrators should run this against the environments that hold policyholder identity numbers first, because that is what the group published for Hollard.

TH-2026-W40-07: Arista VeloCloud Orchestrator: Backdoor Daemon and Header Indicators**P3 MEDIUM:** exploited per the vendor; ZA population unmeasured (zero by two methods, held)

Hypothesis: An attacker holding the public part of an Edge authentication certificate has reached privileged functions on an on-prem VCO through CVE-2026-93952 and installed a Node.js backdoor as a systemd service.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1543.002 (Systemd Service), T1505 (Server Software Component), T1071.001 (Web Protocols).

IOCs: Files /usr/local/sbin/.vcnode.js, /usr/local/sbin/vc-sysmond (MD5 dc78e206eaeade59fc5801fe4556bd0), /etc/systemd/system/vc-sysmon.service; the HTTP header x-vc-opt in nginx logs; addresses 142.93.149.77 and 104.248.126.159. Fixed 5.2.3.16 and 6.4.2.8; 6.1 and 7.0 unfixed at 23 September.

Data Sources: VCO nginx access logs, systemd unit inventory, file integrity on /usr/local/sbin, egress netflow.

Detection Guidance: List systemd units and diff against a clean build; grep nginx logs for x-vc-opt and the two addresses; hash vc-sysmond if present. Restrict the VCO web interface to administrative networks regardless of version, because two trains have no fix. Priority is P3 only because the South African population is unmeasured; any organisation that runs on-prem VCO treats it as P1.

TH-2026-W40-08: GPO-Only Ransomware: PAYLOAD's Pattern Through an SSL VPN

P3 MEDIUM: one SA listing by the group; 2,725 FortiGate exposed; pattern generalises

Hypothesis: An attacker who authenticated with a valid account through an SSL VPN has obtained domain rights and linked malicious Group Policy Objects at the domain root that set a ransom wallpaper and logon banner, drop note files and disable local administrators, with no encryptor and no dropped binary on most hosts.

MITRE ATT&CK: T1078 (Valid Accounts), T1133 (External Remote Services), T1484.001 (Group Policy Modification), T1491.001 (Internal Defacement), T1531 (Account Access Removal).

IOCs: GPO GUIDs {C897F2C7-C2AC-4E6F-BF48-58036FF29E79} and {22099AD2-E062-4F56-B574-5099BBA4E7A6}; files payload.jpg, hello.txt and README-payload.txt in SYSVOL; killer.exe (MD5 0108656A3E1ADE6CA4F21B084F5E1208) and kill.exe (MD5 BEA5E267F24D7DA59F6821BFFDBFF293); addresses 37.19.210.12, 146.70.117.239, 149.102.229.154 (Kaspersky).

Data Sources: Domain controller security log events 5136, 5137 and 5141 (directory service changes), SYSVOL file integrity monitoring, SSL VPN authentication logs, GPO change auditing.

Detection Guidance: Alert on any new GPO linked at the domain root and on image, text or script files appearing in SYSVOL policy folders. Baseline the GPO set and diff daily. On the VPN, alert on a first-time source country or a first-time device for a privileged account, because the case began with a valid credential and no exploit.

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

- 1. Run the vendor and responder log checks on Monday 28 September and keep the output.** Check Point's two greps and its Mobile Access certificate query and F5's OAuth failure count and TMM core check are each the vendor's own definition of an attempt; the MikroTik ops-account and -2 username search is CERT Polska's. Each takes minutes. Archive the results with the patch ticket; a clean result dated before the patch is the evidence a regulator or an insurer will ask for later.
- 2. Treat the September SharePoint update guide revision as a new patch.** Farms that deferred an August fix labelled spoofing at 6.5 now carry an exploited 8.8 that chains with the June bypass. Confirm builds on every front end, and where a farm is internet-facing put pre-authentication in front of it by Friday 2 October.
- 3. Baseline Group Policy and alert on root-linked changes.** Kaspersky's PAYLOAD case reached every domain-joined host without an encryptor. Events 5136, 5137 and 5141 on the domain controllers and file integrity on SYSVOL are cheap to collect and almost never collected.
- 4. Check your own contractor-built apps the way GroundUp checked Gauteng's.** Take the endpoints from the app's traffic and call them without a token; look in particular for OTP tables, location histories and image stores. Do it before a researcher does.
- 5. Close SSH, the API and Winbox on every RouterOS device to the internet, then patch.** The chain is complete, the attacker's addresses are known, and 4,285 South African devices answer on port 8728. A compromised device is netinstalled.

Management (CISO / Board)

- 1. Adopt the Bidvest Bank notice as the organisation's section 22 template by Friday 2 October.** Provider named, actor named as far as known, data classes, regulators told, contact channel, and a plain line on whether your own systems were touched. The Information Regulator has now said in public that the duty is the responsible party's and that paying the ransom does not discharge it.
- 2. If you are an insurer or an administrator, decide on Monday 28 September who issues the notice when a cell captive or an underwriting manager is breached.** Guardrisk's model means that every cell is a responsible party. The MIP case produced 45 responsible parties and one notification; the regulator has noticed.
- 3. Put the edge-appliance inventory on the risk register as a named asset with an owner.** Nine appliance families from seven vendors (Citrix, Cisco, Fortinet, MikroTik, Check Point, F5 and Arista) have been added to the overdue column since 8 September, and six of them arrived with a compromise check that someone must be accountable for running. Ask for the list, the owner and the date each check was last run.
- 4. Ask what your suppliers' testing environments hold.** Telkom's BCX disclosure and MIP's decommissioned Jira instance are the same lesson from two directions: the data that leaks is in the environment nobody thought was production. Put legacy and test environments on the supplier questionnaire explicitly.
- 5. Read the exposure counts as counts of doors, not as a vulnerability score.** The 5,252 MikroTik and 823 SharePoint figures say how many South African instances exist, and the report has no way to say how many are patched. The board question is whether the organisation knows which of them are its own.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH, 23rd CONSECUTIVE WEEK

The South African cyber threat level remains HIGH for a twenty-third consecutive week (20 September to 26 September 2026). Escalation to CRITICAL was considered on the combination of a second insurer on The Gentlemen's site and ten catalogue additions with seven overdue, and rejected on the criterion applied since W35: no systemically important institution went out of service, no national-scale outage occurred, and the week's South African items are three claims with no confirmation, one confirmed incident that its owner places in a test environment, and one confirmed data exposure fixed the day after it was reported. De-escalation to MEDIUM was rejected on four network-edge vendors with five exploited flaws in one window, the regulators' confirmation that a 45-insurer breach produced one notification, and a new group opening its South African account with two victims in a day.

Rationale

Four network-edge vendors reported exploitation in one week. Check Point's management server and VPN certificate path, F5's APM OAuth server, Arista's orchestrator and the completed MikroTik chain, all with vendor-confirmed exploitation, joined Cisco, Citrix and Fortinet in the overdue column. South

Africa's measured populations are 5,252 MikroTik, 2,725 FortiGate, 823 SharePoint and 111 NetScaler; Check Point, F5 and VeloCloud are unmeasured.

The Gentlemen listed a second South African insurer. Guardrisk on 26 September, three weeks after Hollard, from a group whose leaked guidance said to avoid Africa and whose August count was second in the world. Whether this is a second downstream extortion from the MIP data set or a new intrusion is the week's open question.

The regulators said the duty is the insurer's and only the operator has notified. The Information Regulator's answer that it holds MIP's notification alone, for a breach touching roughly 45 insurers, is a direct statement of how far notification practice sits from the law, and Bidvest Bank's notice shows what compliance looks like.

A new group opened with two South African SMEs in a day. BlackLocks has no track record, no samples and no known access method, which is why its listings are CLAIMED and why the tempo matters.

Next-Week Watch (W41)

Guardrisk: own estate or MIP data. The distinguishing observations are a Guardrisk or Momentum Group statement, which would say whether its own systems were compromised; a statement from MIP that Guardrisk is or is not a client; or a published sample whose record format matches the Hollard set. A leak-site deadline appearing would suggest a live negotiation rather than a data set already in hand.

Whether the insurers have notified in their own names. The Information Regulator said on 25 September it had received only MIP's notification. The test is a second answer from the regulator, a statement from any of the 45 that it filed, or a section 22 notice on an insurer's website. Silence past Friday 9 October, four weeks after the Hollard listing, becomes a finding about practice rather than timing.

BlackLocks' next listings. If the next two are South African, the group has local access or a broker with South African inventory; if they are elsewhere, the two Pretoria firms were a coincidence of a young operation's first month. Either observation changes the Section 4 profile.

RelyComply's data. The countdown lapsed on or about 23 September with nothing observed. Publication would let the data classes be checked against the customers' notices, Bidvest's included; a further fortnight of silence would place DireWolf's South African behaviour, two confirmed sets and no publication, against its 43 August attributions.

BCX. Telkom's scope is a legacy testing environment with no customer impact found. A leak-site listing naming BCX or a BCX customer, or a widened Telkom statement, would move the item; silence leaves it at the company's scope.

Check Point, F5 and the two Cisco appliances in South Africa. None has a Shodan product label. No South African incident naming a Cisco email gateway or ISE as the entry point was observed in the window, so the W39 item is carried rather than closed. The collector task is a hand-built fingerprint for the Check Point management port, the APM OAuth path and the two Cisco appliances, so the P1 hunts can be sized; the observation to watch is a South African incident naming any of them as the entry point.

The Shodan port-concentration test. LiteLLM and ScreenConnect self-marked VERIFIED for a fourth week and were overridden by hand. The test is specified in W38; until the collector applies it, the panel's own flag is not sufficient for publication.

Rand Water at 3 October. A month after the SENS statement with no actor, no personal-information statement and no return from the disaster recovery site announced, silence becomes the finding and the item moves to the record.

Closed this week. The Bidvest provider question, resolved by the bank's own notice and corrected in Section 1; the regulators' answers, received on 25 September; CVE-2026-69724, resolved as a separate unexploited fix; the Fortinet Known Exploited field, confirmed still reading No on 27 September; the kernel trio, resolved as patch items on Red Hat's acknowledgement. Carried without re-argument: Cell C Fibre, Cartrack, VSB Attorneys, Rohloff, The Courier Guy, Babcock, the Furniture Bargaining Council claim, Toyota's SMS provider, Implats and Hungry Lion.

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 27 September 2026, with the exceptions this note records: the CISA catalogue URL is the public location of a file read locally; the two Check Point articles, the F5 advisory, the two Microsoft update guide entries, the Fortinet advisory and the Bidvest Bank notice are script-rendered or robot-gated and were read through a browser, with the Bidvest text stored under evidence/. **Collection notes.** The feed run completed at 02:07 UTC on 27 September 2026 and passed its integrity check with a clean exit. The victim feed returned 132 records, all tagged ZA; the run log records filter purity 1.0 and the written file records 132 South African records against 132 returned. The catalogue file is catalogVersion 2026.09.25, released on Friday 25 September at 18:58 UTC, so any Saturday addition falls to the next edition. The RSS sweep read 58 of 72 feeds; Daily Maverick, IOL, Engineering News, Polity, ITWeb's two feeds, News24 and INTERPOL failed at the source and were checked by hand where cited. The world-feed search for South African victims under other country tags could not be run because the aggregator's API is unreachable from the build environment; it remains a collector task. **Provenance of the machine-read feeds.** Every ransomware.live, NVD and EPSS figure in this report was retrieved from those services' APIs and the sources are cited as the endpoints actually called; the rendered ransomware.live pages used, the South African country page, the Guardrisk and RelyComply victim pages and the BlackLocks group page, are cited as cross-checks of records also present in the feed. **A correction.** This edition corrects W39's statement that Bidvest Bank had not named its provider: a section 22 notice dated 17 September 2026 on the bank's website names RelyComply and DireWolf. The correction is recorded in Section 1 and applied in Sections 3.5 and 8.2; the W39 confirmations count of nine is corrected to ten. **Figures withheld or resolved.** LiteLLM (6,667) and ScreenConnect (2,728) are omitted as port-scatter artefacts for a fourth week; VeloCloud's zero is PROVISIONAL and unpublished; WSO2, Adobe Commerce, F5 BIG-IP APM and Zyxel GS1900 have no product label and are held; no Check Point figure exists. **Description conflicts recorded.** The catalogue describes CVE-2026-5430 as a path traversal while the vendor advisory it links describes a JWT bypass; NVD carries 8.1 for CVE-2025-25249 from Fortinet's PSIRT while Fortinet's own page prints 7.4; WordPress scores CVE-2026-87902 at 9.2 and NVD's CISA-ADP record at 8.1. In each case both figures are printed and the NVD feed is carried in the table. **Attribution policy.** Where a story was broken by a publication this report names who broke it, links to them, and summarises only what the intelligence judgement requires. **Single-source disclosure.** The regulators' answers rest on TechCentral; the BCX disclosure and the flight-scam warning on MyBroadband; the e-Panic exposure on GroundUp's first-hand account with MyBroadband reporting the same researcher; the e-Panic contract figures on the DA via MyBroadband; the SCA judgment on Moonstone's

account; the PAYLOAD and INC Ransom patterns on Kaspersky and Huntress respectively; the KELA reading of The Gentlemen's leaked chats on KELA. **Claims deliberately excluded.** The Guardrisk, Apollo 21 and ARCA listings are carried as claims only. The aggregator's infostealer counts are third-party telemetry of unknown age. DireWolf's 200 GB is an attacker figure. The vendor alert's identification of BlackLocks with the 2025 BlackLock operation is not adopted. No actor or family is attributed to Rand Water or to BCX. MIP's ransom amount is undisclosed and no figure is implied.

1. ransomware.live, victim page for Guardrisk (The Gentlemen), discovered 26 September 2026 08:48 UTC, estimated attack date 21 September 2026, retrieved 27 September 2026; the same record is in the locally retrieved country feed. <https://ransomware.live/id/R3VhcmRyaXNrQHROZWdlbnRsZWlbg==>
2. Guardrisk, About Guardrisk (subsidiary of Momentum Group Limited; licensed non-life, life and microinsurance insurers; offices in Johannesburg, Cape Town, Durban, Mauritius and Gibraltar), checked 27 September 2026. <https://guardrisk.co.za/about/>
3. Guardrisk, Newsroom, checked 27 September 2026 (newest item 17 September 2025; no statement on any cyber incident). <https://guardrisk.co.za/newsroom/>
4. ransomware.live API, GET /groups, 402 groups with victim counts, retrieved 27 September 2026 and compared with the 20 September retrieval (feeds/r/_groups_2026-09-27.json). <https://api.ransomware.live/v2/groups>
5. Infosecurity Magazine, Ransomware attacks reach record high for 2026, reporting NCC Group's August 2026 threat intelligence report (23 September 2026). <https://www.infosecurity-magazine.com/news/ransomware-attacks-reach-record/>
6. TechCentral, Insurers carry the can for MIP breach, regulators say (25 September 2026). <https://techcentral.co.za/insurers-mip-breach-regulators/286482/>
7. Bidvest Bank, Notification of a Security Compromise in terms of Section 22 of POPIA: RelyComply cyber incident (notice dated 17 September 2026; read through a browser on 27 September 2026 because the page is script-rendered, and stored as evidence/w40_bidvestbank_important_notice_2026-09-27.txt). <https://www.bidvestbank.co.za/important-notice>
8. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.09.25, released 25 September 2026 18:58 UTC, retrieved 27 September 2026 (feeds/kev_2026-09-27.json). <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
9. Check Point, sk1000171, CVE-2026-93616: directory traversal and file upload allows execution of arbitrary script on the Management Server (created 20 September 2026, last modified 22 September 2026; read through a browser). <https://support.checkpoint.com/results/sk/sk1000171>
10. Check Point, sk1000117, CVE-2026-85102: authentication bypass and remote code execution in Remote Access and Site-to-Site VPN (created 7 September 2026, last modified 24 September 2026; read through a browser). <https://support.checkpoint.com/results/sk/sk1000117>
11. F5, K000162605: BIG-IP APM vulnerability CVE-2026-94127 (published 22 September 2026, updated 23 September 2026; read through a browser). <https://my.f5.com/manage/s/article/K000162605>
12. Arista, Security Advisory 0183, CVE-2026-93952 in VeloCloud Orchestrator on-prem (published 22 September 2026, updated 23 September 2026). <https://www.arista.com/en/support/advisories-notices/security-advisory/24765-security-advisory-0183>
13. The Hacker News, MikroTik chain let attackers take over MikroTik routers without a password or SSH key (23 September 2026). <https://thehackernews.com/2026/09/mikrotik-chain-let-attackers-take.html>
14. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:02 UTC 27 September 2026 (feeds/shodan_za_2026-09-27.json). <https://www.shodan.io/search?query=country%3AZA>
15. ransomware.live API, GET /v2/countryvictims/ZA, 132 records, za_records 132 against server_returned 132, filter purity 1.0, FREE v2 tier (delayed relative to PRO), retrieved 02:00 UTC 27 September 2026 and stored as feeds/ransomwarelive_za_2026-09-27.json. <https://api.ransomware.live/v2/countryvictims/ZA>
16. MyBroadband, Telkom discloses BCX cybersecurity incident which was limited to legacy testing environment (25 September 2026). <https://mybroadband.co.za/news/security/669235-telkom-discloses-bcx-cybersecurity-incident-which-was-limited-to-legacy-testing-environment.html>
17. GroundUp, How Gauteng's new panic app exposed your data (23 September 2026). <https://groundup.org.za/article/gauteng-panic-app-exposes-crime-reports-users-locations/>
18. Information Regulator, Enforcement notices register, checked 27 September 2026 (newest 2026 entry dated 10 June 2026). <https://infoeregulator.org.za/enforcement-notices/>
19. Information Regulator, Media statements page, checked 27 September 2026 (no statement dated later than 2 June 2026; the media invitation of 27 August 2026 recorded in W39 is an invitation, not a statement). <https://infoeregulator.org.za/media-statements/>
20. ransomware.live, group page for BlackLocks (new group, active; three victims, first discovered 5 September 2026), retrieved 27 September 2026. <https://www.ransomware.live/group/BlackLocks>
21. Microsoft MSRC, CVE-2026-65660, Microsoft SharePoint Server remote code execution vulnerability (released 11 August 2026, revision 1.2 of 25 September 2026; read through a browser). <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65660>
22. The Hacker News, WSO2 and Adobe Commerce flaws exploited in attacks, added to CISA KEV (25 September 2026). <https://thehackernews.com/2026/09/wso2-and-adobe-commerce-flaws-exploited.html>
23. The Hacker News, Attackers exploit WordPress CVE-2026-87902 within hours of disclosure (24 September 2026). <https://thehackernews.com/2026/09/attackers-exploit-wordpress-cve-2026.html>
24. KELA, Inside The Gentlemen leak: how a new RaaS captured 10 per cent of 2026's global ransomware victims (14 May 2026). <https://www.kelacyber.com/blog/the-gentlemen-ransomware-internal-chat-leak-analysis-2026/>
25. MyBroadband, South African emergency services app in the province with the most murders exposed the locations of users (23 September 2026). <https://mybroadband.co.za/news/security/668743-south-african-emergency-services-app-in-the-province-with-the-most-murders-exposed-the-locations-of-users.html>
26. MyBroadband, Gauteng spending R269 million for app downloaded 15,000 times in 10 months (25 September 2026). <https://mybroadband.co.za/news/gadgets/668550-gauteng-spending-r269-million-for-app-downloaded-15000-times-in-10-months.html>
27. Apollo 21, company website (head office 96 Siersteen Street, Silvertondale, Pretoria; six branches), checked 27 September 2026. <https://apollo21.co.za/>
28. ARCA Unlimited Architects, company website (Pretoria, South Africa; multidisciplinary design firm), checked 27 September 2026. <https://arcaunlimited.com/>
29. ransomware.live, victim page for RelyComply AML Platform (DireWolf, discovered 9 September 2026, country field GB, 200 GB claimed), re-read 27 September 2026. <https://ransomware.live/id/UmVseUNvbXBseSBBTUwGUGxhdGZvcmlAZGlyZXdvbGY=>

30. RelyComply, RelyComply cyber incident: what happened and what you can do, official notice (published 16 September 2026; re-read 27 September 2026, no later update on the page). <https://relycomply.com/relycomply-cyber-incident-what-happened-and-what-you-can-do/>
31. Rand Water, corporate website, checked 27 September 2026 (no statement dated September 2026 on the incident). <https://www.randwater.co.za/>
32. ransomware.live API, GET /iocs/{group} for the groups active against South Africa in the last 120 days, retrieved 27 September 2026 (feeds/rl_iocs_2026-09-27.json). <https://api.ransomware.live/v2/iocs/thegentlemen>
33. ransomware.live API, GET /yara/{group}, retrieved 27 September 2026 (feeds/rl_yara_2026-09-27.json). <https://api.ransomware.live/v2/yara/thegentlemen>
34. Brinztch, Blacklocks ransomware group lists South Korean firm Kwangmyung Industry as victim (6 September 2026). <https://www.brinztch.com/breach-alerts/brinztch-alert-blacklocks-ransomware-group-lists-south-korean-firm-kwangmyung-industry-as-victim>
35. Kaspersky Securelist, Group Policy hijacked: PAYLOAD ransomware weaponizes Active Directory GPO (21 September 2026). <https://securelist.com/tr/payload-ransomware-via-group-policy/121335/>
36. NIST NVD, CVE API 2.0, CVSS base scores with scoring source for the 61 catalogue entries added in the last 45 days, retrieved 27 September 2026 (feeds/nvd_cvss_2026-09-27.json). <https://services.nvd.nist.gov/rest/json/cves/2.0>
37. Adobe, Security update available for Adobe Commerce, APSB26-92 (11 August 2026). <https://helpx.adobe.com/security/products/magento/apsb26-92.html>
38. The Hacker News, Check Point warns of management server zero-day exploited in targeted attacks (22 September 2026). <https://thehackernews.com/2026/09/check-point-warns-of-management-server-zero-day-exploited-in-targeted-attacks>
39. The Register, Someone's attacking a critical 0-day RCE in F5 BIG-IP APM (23 September 2026). <https://www.theregister.com/security/2026/09/23/someones-attacking-a-critical-0-day-rce-in-f5-big-ip-apm/5298659>
40. watchTowr Labs, Is this a joke? In the auth header? F5 BIG-IP unauthenticated heap overflow to RCE, CVE-2026-94127 (23 September 2026). <https://labs.watchtowr.com/is-this-a-joke-in-the-auth-header-f5-big-ip-unauth-heap-overflow-to-rce-cve-2026-94127/>
41. The Hacker News, New CVSS 10.0 VeloCloud Orchestrator flaw actively exploited in certificate-based setups (22 September 2026). <https://thehackernews.com/2026/09/new-cvss-10-0-velocloud-orchestrator-flaw>
42. MikroTik, September 2026 vulnerability notice (3 September 2026): fixed in RouterOS 7.24.2, 7.23.4, 6.49.21 and 7.25 beta 3. <https://mikrotik.com/supportsec/september-2026-vulnerability/>
43. The Hacker News, SharePoint flaw initially listed as spoofing by Microsoft enables authenticated RCE (22 September 2026). <https://thehackernews.com/2026/09/sharepoint-flaw-initially-listed-as-spoofing-by-microsoft-enables-authenticated-rce>
44. Microsoft MSRC, CVE-2026-69724, Microsoft Office SharePoint remote code execution vulnerability (released 8 September 2026, revision 1.1 of 17 September 2026; read through a browser). <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69724>
45. WordPress, security advisory GHSA-7hp8-65ch-5whp, CVE-2026-87902 (22 September 2026). <https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-7hp8-65ch-5whp>
46. WSO2, Security advisory WSO2-2026-5328, CVE-2026-5430 (published 3 May 2026). <https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2026-5328/>
47. BleepingComputer, CISA warns of SharePoint, WSO2, Adobe Commerce flaws exploited in attacks (25 September 2026). <https://www.bleepingcomputer.com/news/security/cisa-warns-of-sharepoint-wso2-adobe-commerce-flaws-exploited-in-attacks/>
48. FIRST, EPSS API, scores for the same 61 entries, retrieved 27 September 2026 (feeds/epss_2026-09-27.json). <https://api.first.org/data/v1/epss>
49. Zyxel, Security advisory for stack-based buffer overflow vulnerability in GS1900 series switches, CVE-2026-7273 (16 June 2026). <https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-stack-based-buffer-overflow-vulnerability-in-gs1900-series-switches-06-16-2026>
50. GreyNoise, Open season on Kapibala: attacker steals over 18,000 government records through WordPress exploitation (21 September 2026). <https://www.greynoise.io/blog/open-season-on-kapibala-attacker-steals-government-records-wordpress-exploitation>
51. Qualys, CISA BOD 26-04 timelines for three Linux kernel CVEs (23 September 2026). <https://blog.qualys.com/product-tech/2026/09/23/cisa-bod-26-04-timelines-for-three-linux-kernel-cves>
52. Fortinet PSIRT, FG-IR-25-084, heap-based buffer overflow in cw_acd daemon, CVE-2025-25249 (published 13 January 2026, updated 23 February 2026; read through a browser on 27 September 2026). <https://www.fortiguards.com/psirt/FG-IR-25-084>
53. ransomware.live, South Africa country page, cross-check only (showed 131 victims with Apollo 21 and Guardrisk newest when read on 27 September 2026, one short of the API file). <https://www.ransomware.live/country/ZA>
54. Huntress, The tale of two INC Ransom notes: a ransomware timeline (21 September 2026). <https://www.huntress.com/blog/two-inc-ransom-notes>
55. Moonstone, SCA draws the line on access to FIC information (25 September 2026), on the Supreme Court of Appeal judgment of 23 September 2026. <https://www.moonstone.co.za/sca-draws-the-line-on-access-to-fic-information/>
56. Werksmans, When discovery meets data privacy: navigating the tension between litigation obligations and data protection (23 September 2026). <https://werksmans.com/when-discovery-meets-data-privacy-navigating-the-tension-between-litigation-obligations-and-data-protection/>
57. SARS, Scams and phishing page, checked 27 September 2026 (newest alert SARS-SCAM-400, 2 September 2026). <https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>
58. MyBroadband, Cheap flight scams emptying bank accounts in South Africa (26 September 2026). <https://mybroadband.co.za/news/banking/668587-cheap-flight-scams-emptying-bank-accounts-in-south-africa.html>
59. ransomware.live API, GET /csirt/ZA, six South African CSIRTs from the FIRST directory, retrieved 27 September 2026 (feeds/rl_csirt_za_2026-09-27.json). <https://api.ransomware.live/v2/csirt/ZA>

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.