



SOUTH AFRICA

CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief, Week 39 | 13 September – 19 September 2026

THREAT LEVEL: HIGH

TLP: CLEAR

Report ID: SA-CTI-2026-W39 | Classification: TLP: CLEAR

Published Monday 21 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/>



TRAIN LIKE AN ATTACKER. LEVEL UP.

Live, virtual, instructor-led hacking courses — **attend online from anywhere.**

Two days per course · 09:00–17:00 (GMT+2) · Taught live by SensePost hackers



0xCD: Web Application Hacking

Sharpen your web app testing skills against real-world style targets.

6–7 OCT
2026

- » Individual lab access for each person joining the training
- » Taught by ethical hackers with current field experience
- » Practical-driven learning through guided tasks, hands-on labs, and real-world style challenges
- » Content grounded in real methodologies and client work



BOOK YOUR SEAT

training+sept@orange cyberdefense.com

R20 500

PER COURSE



TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard
- 2. Threat Landscape Heatmap
- 3. Top SA Incidents (W39)
- 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, 22nd consecutive week (13 September - 19 September 2026)

Story 1. The Hollard claim resolved, and the answer was a supplier. MIP Holdings, which supplies policy administration software to insurers, medical schemes and lenders, told TechCentral on 15 September that intruders spent about three weeks from late May inside a Jira support platform it was decommissioning, took roughly 400,000 records belonging to the customers of about 45 insurers, and that MIP paid The Gentlemen a substantial ransom for an undertaking to destroy the data.¹ The undertaking did not hold. The group listed Hollard on 7 September, demanded a ransom Hollard refused, and published records this week that MyBroadband counted at more than 100,000 Hollard funeral policyholders, with identity numbers, dates of birth and the names of children and beneficiaries.^{2,3} Hollard's statement of 16 September says the data came from the June MIP incident and that forensic work has found no compromise of its own environment.⁴ The publication and its supplier origin are CONFIRMED; the group's claim to have breached Hollard itself stays CLAIMED. First reported by [TechCentral](#) on 15 September 2026.

Story 2. The provider behind the EasyEquities notice of 12 September has a name, and it serves much of the financial sector. RelyComply, the Johannesburg and Cape Town compliance platform that runs FICA identity verification and screening for banks, brokers and lenders, published a notice on 16 September: an unauthorised party exploited a zero-day in a third-party application, reached systems holding customer data, and the incident is reported to the Information Regulator under reference SC20263150.⁵ DireWolf listed it on 9 September claiming 200 GB from production databases and Amazon S3 storage, and the aggregator tagged the record GB, which is why it did not appear in W38's South African count.^{6,7} EasyEquities, SA Home Loans, Peregrine Capital, Satrix and Alexforbes have each confirmed that customer records sat in the breached environment; Standard Bank is investigating; Bidvest Bank has still not named its provider, so its notice of the same evening is not attributed to this event.^{7,8,9,10,11} First reported by [MyBroadband](#) on 13 September 2026.

Story 3. Seven vulnerabilities entered the CISA catalogue between 14 and 18 September, half last week's count, and two of them are Cisco zero-days that Cisco found while working support cases: a 9.8 SQL injection in Secure Email Gateway that reaches root from a crafted email, and a 10.0 authentication bypass in Identity Services Engine, the product that decides who joins a corporate network.^{12,13,14} Four of the seven were past their remediation date on Monday 21 September and the three Linux kernel entries fell due that day.¹² Cisco published a one-line compromise check for each of its two, and Section 9 carries both. No South African exposure figure exists for any of the seven: Shodan has no product label for the Cisco appliances or the kernel, and the Pixel and Acronis queries returned zero, which under this report's rules is not published as an absence.¹⁵

W39 CORRECTION TO W38: the W38 edition put the derived South African listing count for its window (6 to 12 September) at two, VSB Attorneys and Hollard. It was three. DireWolf listed RelyComply AML Platform on 9 September 2026, inside that window, and the aggregator recorded the country as GB; the country-scoped feed this report reads therefore never returned it, and the W38 collection could not have seen it. RelyComply lists Johannesburg and Cape Town offices alongside London and reported the

incident to the South African Information Regulator, so it is a South African victim for this report's purposes. The W38 statement that no source connected the Bidvest Bank and EasyEquities notices was correct when written; the confirmations in Section 3.3 attach the EasyEquities notice to RelyComply, while Bidvest Bank's remains unattributed. Every previous aggregator country-field error in this series invented a South African victim; this one hid one. The corrections KPI row records it.^{6,16,5}

KPI Dashboard

Metric	Current (W39)	Prior (W38)	Change	Direction
Overall SA threat level	HIGH	HIGH	No change (22nd week)	FLAT
ransomware.live SA cumulative	128	128	0	FLAT
SA claims dated inside the window (ZA tag)	0	3	-3	DOWN
Window claims surviving the nationality check	0 of 0	2 of 3	n/a	n/a
SA organisations confirming a breach or supplier exposure in the window	9	4	+5	UP
New CISA KEV additions	7	14	-7	DOWN
KEV adds already overdue at publication	4	7	-3	DOWN
KEV adds with a published VERIFIED SA exposure figure	0 of 7	6 of 14	-6	DOWN
Corrections issued to prior editions	1	1	0	FLAT
Weeks since last IR substantive publication	15	14	+1	UP

Three notes on the table. The zero in the claims row is a zero in the ZA-tagged feed, confirmed by the aggregator's own country page and by its 100 most recent listings worldwide, none of which is South African; it is not a claim that no South African organisation was listed, because the RelyComply case shows the tag itself can hide one. The confirmations row counts organisations that made a new public statement inside the window that their own systems or their customers' data in a supplier were affected: MIP Holdings, Hollard, RelyComply, EasyEquities, SA Home Loans, Peregrine Capital, Satrix, Alexforbes and Cell C Fibre; Cartrack's second customer notice and Standard Bank's investigation are not counted because neither adds a new confirmation of impact. The exposure row is zero because none of the seven catalogue additions has a Shodan product label with a South African population that passes the collection's rules, as Section 7 sets out.

W39 KEY FRAMING: this week South Africa learned what its supplier breaches contained, and who else was in them. One policy-administration vendor held identity numbers for the customers of roughly 45 insurers in support tickets that were supposed to be scrubbed; one compliance platform held the FICA verification records of at least six regulated institutions in a single environment. In both cases the institutions whose names appear on the policies and accounts did nothing wrong in their own estates

and still owe the notification, because POPIA puts the duty on the responsible party and the Prudential Authority has already asked whether one unregulated software supplier serving a large share of a sector is a systemic risk. MIP's experience settles one board question: it paid, ran anti-money laundering checks on the wallet first, received an undertaking to destroy the data, and the data was published anyway. For a CISO the question to put to the executive on Monday 21 September is which operators hold identity numbers on the organisation's behalf, in what environment, and whether the contract says who tells the customers.

1. TechCentral, Customers of 45 insurers exposed in South African cyber breach (15 September 2026, updated 16 September). <https://techcentral.co.za/customers-45-insurers-exposed-cyber-breach/286139/>
2. TechCentral, Hollard client data dumped on the dark web (18 September 2026). <https://techcentral.co.za/hackers-extort-insurers-mip-ransom-hollard/286251/>
3. MyBroadband, Hollard customer data leaked on the dark web (19 September 2026). <https://mybroadband.co.za/news/security/668276-hollard-customer-data-leaked-on-the-dark-web.html>
4. Hollard, Hollard statement regarding reported cyber threat claims, media centre (published 16 September 2026). <https://www.hollard.co.za/media-centre/press-releases/hollard-statement-regarding-reported-cyber-threat-claims>
5. RelyComply, RelyComply cyber incident: what happened and what you can do, official notice (published 16 September 2026, updated 17 September 2026). <https://relycomply.com/relycomply-cyber-incident-what-happened-and-what-you-can-do/>
6. ransomware.live API, victim record via GET /v2/searchvictims/relycomply: RelyComply AML Platform, DireWolf, discovered 9 September 2026 13:28 UTC, country field GB, retrieved 20 September 2026 and stored as evidence/w39_ransomwarelive_searchvictims_relycomply_2026-09-20.json (public page: ransomware.live/id/UmVseUNvbXBseSBBTUwgUGxhdGZvcmlAZGlyZXdvbGY=). <https://api.ransomware.live/v2/searchvictims/relycomply>
7. MyBroadband, EasyEquities data at third-party hacked and customer information compromised (16 September 2026). <https://mybroadband.co.za/news/security/667868-easyequities-data-at-third-party-hacked-and-customer-information-compromised.html>
8. MyBroadband, South African home loans giant affected by data breach, customer records potentially exposed (17 September 2026). <https://mybroadband.co.za/news/security/667893-south-african-home-loans-giant-affected-by-data-breach-customer-records-potentially-exposed.html>
9. Moneyweb, EasyEquities, Satrix hit by data breach (14 September 2026). <https://www.moneyweb.co.za/news/companies-and-deals/easyequities-satrix-hit-by-data-breach/>
10. ITWeb, Third-party cyber breaches rock SA firms (17 September 2026). <https://www.itweb.co.za/article/third-party-cyber-breaches-rock-sa-firms/KWEBb7yLe1NvmRjO>
11. MyBroadband, Standard Bank investigates 200GB data breach (18 September 2026). <https://mybroadband.co.za/news/security/668048-standard-bank-investigates-200gb-data-breach.html>
12. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.09.18, released 18 September 2026, retrieved 20 September 2026. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
13. Cisco, Security advisory cisco-sa-esa-inj-2bLVGmhX, Cisco Secure Email Gateway SQL injection vulnerability, version 1.1 (published 14 September 2026, updated 17 September 2026). <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX>
14. Cisco, Security advisory cisco-sa-ISE-ABP-VNSW7Tn5, Cisco Identity Services Engine authentication bypass vulnerability, version 1.0 (16 September 2026). <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>
15. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:01 UTC 20 September 2026. <https://www.shodan.io/search?query=country%3AZA>
16. RelyComply, Contact us page listing Johannesburg (Sandton), Cape Town (Newlands) and London offices, checked 20 September 2026. <https://relycomply.com/contact-us/>

TOP 3 ACTIONS THIS WEEK

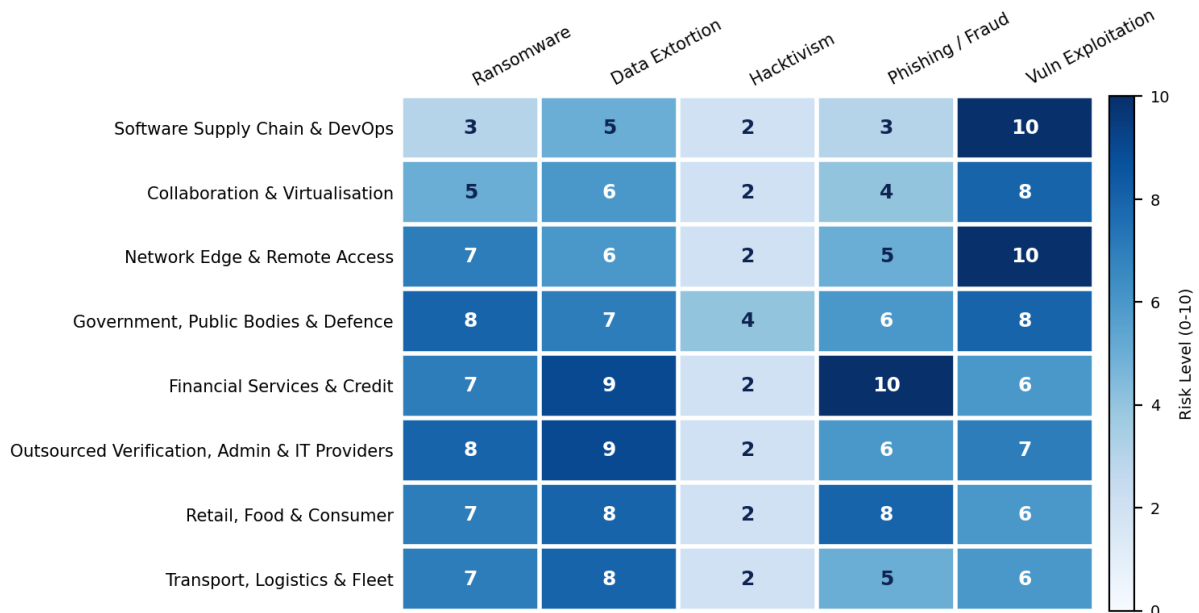
1. Patch Cisco Secure Email Gateway and Identity Services Engine on Monday 21 September and run both vendor compromise checks before trusting the appliance again. CVE-2026-76461 was due on 17 September and CVE-2026-76460 on 19 September; Cisco confirms active exploitation of both and found each while resolving a support case. On the email gateway the check is `grep -i for COPY.*TO PROGRAM` across `mail_logs` on every cluster member, because a compromised member exposes the SSH keys the cluster shares; a virtual appliance with a hit is rebuilt on 16.5.0-780; cleaning it in place is not enough. On ISE the check is `show logging application ise-kong/access.log` piped to `dummyuser` on every node, and a hit means re-image from a configuration backup. Restrict management-plane reachability with infrastructure ACLs while you patch.

2. If your organisation uses RelyComply, or any FICA verification provider, rotate the API tokens and the single sign-on federation this week, and read the provider's logs for your integration. RelyComply's notice asks customers to rotate tokens and refresh identity-provider configurations, and SA Home Loans and Alexforbes both report doing so before reinstating the service. Treat every verification record the provider held for you as exposed for phishing purposes: full name, identity number, date of birth, contact details and, for some clients, bank account details. Send the customer notice on that basis rather than waiting for the forensic result, as EasyEquities and SA Home Loans did, and register affected customers' interest in the Southern African Fraud Prevention Service.

3. Find the identity numbers sitting in your suppliers' support tickets. MIP's intruders took 400,000 records from Jira tickets in which insurers' staff had pasted screenshots and reports with identity numbers in the clear, on a platform reached through one employee's reused password. Ask each operator that administers policies, claims, payroll or loans on your behalf which ticketing and collaboration platforms hold your data, whether the tickets are scrubbed, and whether the platform enforces single sign-on with multi-factor authentication and managed devices. Where the answer is a personal laptop and a reused password, the responsible party under POPIA is still you.

2. THREAT LANDSCAPE HEATMAP

South African Sector Threat Levels, Week 39 (13 September – 19 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.

One row retired, one row added. Legal and Professional Services, which entered in W38 on the LockBit 5.0 listing of VSB Attorneys, is retired after one week: nothing touching the sector was observed in this window and the VSB item moves to the carryovers in Section 3.7. In its place, Outsourced Verification, Administration and IT Providers enters at 8 for ransomware, 9 for data extortion, 2 for hacktivism, 6 for phishing and fraud and 7 for vulnerability exploitation. It enters rather than rises. The basis is two providers breached by two ransomware operations whose customer bases between them cover roughly 45 insurers and at least six regulated financial institutions, one entered through a reused employee password and one through a zero-day in a third-party application, plus a third, unnamed provider behind the Cell C Fibre notice.^{1,5,17}

Movements among the retained rows. Financial Services and Credit rises from 8 to 9 on data extortion, because the Hollard records are now published and because the RelyComply environment held verification data for at least six named institutions, five of which have confirmed; its ransomware score holds at 7 and its phishing and fraud score stays at the ceiling, now with identity numbers for hundreds of thousands of policyholders and account holders in circulation.^{3,8} Network Edge and Remote Access holds at 10 on vulnerability exploitation: two Cisco zero-days join NetScaler, FMC, FortiOS and MikroTik, all still overdue, and the Arctic Wolf credential waves against Fortinet VPNs land on the largest appliance population in the panel.^{13,14,18} Transport, Logistics and Fleet holds at 8 on data extortion with Cartrack now

confirming that bank account information may have been taken.¹⁹ Government, Public Bodies and Defence holds; Rand Water produced nothing in the window and the hacktivism placeholder stays. Retail, Food and Consumer holds at 8 on phishing and fraud on Capitec's Black Friday warning and the SARS eFiling lures ahead of the 23 October filing deadline.^{20,21} Software Supply Chain and DevOps and Collaboration and Virtualisation hold; the week's kernel, Pixel and Acronis entries are endpoint and hosting problems and are scored under the sectors that run them.

17. MyBroadband, Cell C warns fibre customers about possible data breach (13 September 2026).
<https://mybroadband.co.za/news/security/667360-cell-c-warns-fibre-customers-about-possible-data-breach.html>

18. The Hacker News, Cisco Secure Email Gateway flaw exploited in the wild, enables root command execution, including Arctic Wolf's Fortinet VPN credential-attack findings (15 September 2026).
<https://thehackernews.com/2026/09/cisco-secure-email-gateway-flaw.html>

19. MyBroadband, Cartrack warning after hackers access sensitive data (14 September 2026).
<https://mybroadband.co.za/news/security/667519-cartrack-warning-after-hackers-access-sensitive-data.html>

20. MyBroadband, Capitec warns of fake Takealot and Game websites on Black Friday (16 September 2026).
<https://mybroadband.co.za/news/banking/667781-capitec-warns-of-fake-takealot-and-game-websites-on-black-friday.html>

21. MyBroadband, Hyper-realistic SARS eFiling scams hit South Africa (19 September 2026).
<https://mybroadband.co.za/news/security/667861-hyper-realistic-sars-efiling-scams-hit-south-africa.html>

3. TOP SA INCIDENTS (W39)

Six incidents. The first three are one story told from three positions: the software supplier that was breached in June and spoke this week, the insurer whose customers' records were published, and the compliance platform whose breach explains the notices of the previous weekend. Every rating follows the standing rule that a leak-site description is written by the attacker and cannot lift a rating on its own; this week the confirmations came from the organisations themselves.

3.1 INC-2026-W39-01: MIP Holdings, Supplier Breach Behind the Hollard Listing [CONFIRMED]

Sector	Outsourced administration and IT providers; policy administration and CRM software for insurers, medical schemes, lenders and pension administrators
Organisation	MIP Holdings, mip.co.za, Johannesburg. CEO Richard Firth on the record to TechCentral
Timeline	Intruders inside from about 25 May 2026; discovered on a Sunday in mid-June; disclosed by MIP to TechCentral on 15 September 2026
Confirmed	In the region of 400,000 records taken from an Atlassian Jira support platform being decommissioned: email addresses, cellphone numbers, policy numbers with identity numbers attached, a small number of residential addresses; one file held roughly 200,000 cellphone numbers assembled for an SMS campaign. About 45 client organisations affected, just under half of MIP's client base, almost all life insurers. Core administration systems untouched. Entry through an employee's personal laptop using credentials reused on an unrelated breached service. Some data encrypted. MIP paid the extortionists a sum it describes as substantial after anti-money laundering checks on the accounts, in exchange for an undertaking to destroy the data. Reported to the Information Regulator and the Prudential Authority

Regulator	Information Regulator case open; Prudential Authority convened a meeting on systemic risk and concluded, per Firth, that it was not one. Neither regulator had commented publicly by the close of the window; TechCentral reports both undertook to answer by Monday 21 September
Confidence	CONFIRMED on the company's own on-record account. The record count and the ransom amount are MIP's figures and are not independently verified

The point of this item is what the tickets contained. MIP's clients logged support requests on a Jira service that was supposed to hold obfuscated data; in practice their staff pasted the error message, the screenshot or the complained-about report, and the underlying customer record came with it, identity numbers in the clear.¹ The intruders did not touch MIP's perimeter. They used a password the employee had reused on an unrelated service that had itself been breached, identified the MIP mailbox, and found the Atlassian instance from the personal laptop. Three weeks of slow exfiltration followed. MIP built a messaging platform so each insurer could notify its own customers, which is the correct reading of POPIA: the responsible party is the insurer, and the operator's breach is the insurer's notification.¹ The payment is the second lesson. MIP paid a group whose undertaking to destroy the data lasted until it found a downstream victim with a bigger name, and Section 4.1 sets out why that was predictable. First reported by [TechCentral](#) on 15 September 2026. Detection relevance: TH-2026-W39-05 covers reused credentials against SaaS support platforms and the stealer-log telemetry that precedes them.

3.2 INC-2026-W39-02: Hollard Insurance Group, Policyholder Records Published by The Gentlemen [CONFIRMED]

Sector	Financial services and credit; life and funeral insurance
Organisation	Hollard Insurance Group, hollard.co.za , Johannesburg; listed by The Gentlemen on 7 September 2026 (W38, then CLAIMED)
Development	Data published on the group's leak site after its deadline lapsed; reported by TechCentral on 18 September and MyBroadband on 19 September. TechCentral reports that Hollard received a ransom demand and refused
Confirmed	Hollard, 16 September: the published information is linked to the June 2026 MIP incident, appears isolated to individual funeral policyholders, customers affected by the June incident have already been notified, the company is engaging the regulators, and forensic work to date shows no compromise of the Hollard environment. MIP identified markers in the published material linking it to the data taken in June
Published data	MyBroadband counted more than 100,000 records marked as Hollard funeral policies: full names, identity numbers, dates of birth, email addresses, phone numbers, contract numbers and types, and in some cases the details of partners, children and beneficiaries. TechCentral reviewed material with policyholder names, children's names, identity numbers and email addresses
Confidence	CONFIRMED for the publication and for its origin in the MIP breach, on Hollard's and MIP's statements and two publications' review of the material. The group's assertion that it breached Hollard's own systems is contradicted by Hollard and stays CLAIMED

The W38 watch item asked which of two observations would move Hollard from CLAIMED: a Hollard acknowledgement or a published dataset. Both arrived, and they point in different directions. The dataset is real and the exposure to the individuals is real; the compromise is a supplier's, disclosed in June, and

Hollard says the affected customers were notified then.^{4,2,3} Funeral policies are the product class in which dependants, including minors, are routinely listed, so the published set carries the identity numbers of children. TechCentral's reading is the one to carry: identity numbers do not change, and paired with a name and an email address they are the raw material for account opening and targeted phishing for years.² MyBroadband's count of more than 100,000 Hollard records is one publication's count of a subset and may not be all the compromised data; it is carried as that.³ First reported by TechCentral on 18 September 2026. Detection relevance: TH-2026-W39-01 carries The Gentlemen's exfiltration tradecraft from Talos and the aggregator's hash set; for the 44 other MIP clients the immediate task is the customer notice before any hunt.

3.3 INC-2026-W39-03: RelyComply, FICA Verification Platform, DireWolf [CONFIRMED]

Sector	Outsourced verification providers; KYC, FICA screening and anti-money laundering platform for banks, brokers, lenders and insurers
Organisation	RelyComply, relycomply.com; offices in Sandton, Newlands and London; ICO-registered in the United Kingdom; reported to the South African Information Regulator under reference SC20263150
Timeline	Unauthorised access from 2 September 2026 (per SA Home Loans, citing RelyComply); RelyComply became aware on 8 September; DireWolf listing indexed 9 September 13:28 UTC carrying a 14-day countdown from listing, still running when checked on 16 September; RelyComply notice published 16 September, updated 17 September
Confirmed	RelyComply: an unauthorised third party appears to have exploited a zero-day in a third-party application to reach systems holding customer data; affected systems taken offline and the environment fully reset and rebuilt; all credentials rotated; customers asked to rotate API tokens and refresh single sign-on identity-provider configurations; the zero-day patched; no evidence of movement into any customer's own network; the attackers cannot be identified
Customers confirming	EasyEquities (16 September: full names, identity information, date of birth, gender, nationality, country of residence, account number; integration disabled 11 September); SA Home Loans (16 September: name, identity or passport number, gender, date of birth, email, cellphone, loan property address, PEP flag, employer details; credentials to the RelyComply application replaced); Peregrine Capital (name, identity, passport or company registration number, date of birth, contact details, residential address, bank account details); Satrix via SatrixNOW; Alexforbes (identity-related client information; service suspended and reinstated after forensic sign-off). Standard Bank is investigating with the provider. Bidvest Bank has not named its provider
Actor claim	200 GB comprising 3.57 billion rows from production databases and Amazon S3 storage: identity verification, transaction monitoring, compliance screening and credential management data. Volume and content are the attacker's and are not adopted
Confidence	CONFIRMED on the provider's own notice and five customers' notifications. The initial-access vector is the provider's characterisation; the third-party application is not named

This settles half of the W38 watch item. EasyEquities' provider is RelyComply, and the blast radius is wider than one notice suggested: five institutions have confirmed their data sat in the RelyComply environment, the largest bank in the country is investigating, and the provider's home page carries testimonials from

Standard Bank and SnapScan.^{7,8,9,10,11,22} The other half stays open: Bidvest Bank has not named its provider, MyBroadband's reading that the two notices belong together is an inference, and this report does not adopt it.²³ Two features of the notice matter to a peer organisation. The vector is a zero-day in a third-party application inside the provider's environment, which is the pattern of the Cisco, GitLab and Artifactory entries in Section 5 rather than the reused-password pattern at MIP; and the remediation the provider asked of its customers, token rotation and identity-provider refresh, is the same step Artifactory customers were told to take in W38, because an integration credential survives the provider's rebuild unless the customer revokes it.⁵ What RelyComply held is the FICA file: the identity document, the proof of address, the politically exposed person screening and the employer, which is the data set a fraudster needs to pass another institution's onboarding. First reported by [MyBroadband](#) on 13 September 2026. Detection relevance: TH-2026-W39-04 covers the integration-credential and provider-side hunts for any institution using a verification platform.

3.4 INC-2026-W39-04: Cartrack, Bank Account Data Confirmed in the DireWolf Breach [CONFIRMED]

Sector	Transport, logistics and fleet; vehicle telematics
Organisation	Cartrack, cartrack.co.za, wholly owned by Karooooo Limited; over 2.2 million subscribers at 31 May 2026
Development	Second customer notice reported by MyBroadband on 14 September; Cartrack statement to TimesLIVE on 15 September
Confirmed	Cartrack's own words to TimesLIVE: on 26 August at about 02:00 it identified an incident involving ransomware affecting certain systems; the platform was fully operational by 07:00; the Information Regulator was notified on 26 August and a public notice issued on 28 August. Customer email: attackers accessed the customer database; data that may relate to customers includes personal contact information, bank account information and certain vehicle and driving-related data. Investigation continuing to establish what was exfiltrated. Cartrack believes the attack was carried out by DireWolf
Actor claim	500 GB including financial documents, source code, customer profile data, NDAs and backups; sample folders published across two pages, much of the reviewed material relating to United States customers
Confidence	CONFIRMED. The ransomware characterisation, carried in W38 as MyBroadband's, is now Cartrack's own; the bank account category is Cartrack's own; the volume remains the attacker's

Two things moved. Cartrack now uses the word ransomware itself and gives the discovery time, the regulator notification date and the attribution, all of which W38 had to carry as a publication's characterisation.²⁴ And the data categories now include bank account information, which for a subscription telematics company means the debit-order details of a customer base above 2.2 million.¹⁹ Cartrack's warning is specific about the consequence: calls, emails and SMS from someone claiming to be Cartrack, the customer's bank or another trusted organisation. DireWolf has now taken two South African data sets in one month, a telematics customer base and a FICA verification store, and Section 4.2 profiles it on that basis. First reported by [MyBroadband](#) on 14 September 2026. Detection relevance: the DireWolf hunt ran as TH-2026-W37-01; TH-2026-W39-04 carries the group's ransom-note name from the aggregator feed alongside the provider-side hunts.

3.5 INC-2026-W39-05: Cell C Fibre, Third-Party Provider Credential Compromise [CONFIRMED]

Sector	Telecommunications; fixed broadband
Organisation	Cell C Fibre; customer notice reported by MyBroadband on 13 September 2026
Confirmed	On 9 September a third-party service provider supporting parts of the Cell C Fibre customer environment reported a cybersecurity incident; the provider identified that its access credentials were compromised, resulting in certain customer records being accessed. Data limited to customer names, email addresses, mobile numbers and Cell C account numbers. Cell C told ITWeb the access was by an associated party via a platform used by that provider
Not stated	The provider's name and the number of customers affected
Relationship to RelyComply	None. Cell C confirmed to MyBroadband and to ITWeb that its provider is a separate entity and the incident is not connected
Confidence	CONFIRMED on Cell C's notice and statements to two publications

This item is carried at short length for one reason: it is the third distinct supplier behind a South African customer notice in a fortnight, and the vector is again a credential, this time the provider's own.^{17,23,10} The data set is contact data rather than identity data, which places it below the MIP and RelyComply sets for fraud value and above them for immediate use in smishing against a fibre customer base. First reported by [MyBroadband](#) on 13 September 2026. Detection relevance: none in Cell C's own estate is described; the item belongs to supplier assurance in Section 10.

3.6 INC-2026-W39-06: Unnamed Manufacturer, R50 Million Ransomware Loss [PROBABLE]

Sector	Manufacturing; components for the mining industry
Organisation	Not named. A company of about 500 people operating for 20 years, described by Neels Pretorius, cybersecurity solutions business executive at iOCO, as a recent client
Reported	MyBroadband, 17 September 2026. Attack earlier in 2026; ransomware encrypted every networked device including historical backups and financial reports; the only clean backup found was six months old; no email, ERP or invoicing; return to manual processes; losses of up to R50 million against monthly revenue of R3 million to R4 million. iOCO says it has helped three clients in the same position in six months and that recovery typically takes six to nine months
Confidence	PROBABLE. Single credible source, the responder, with the victim unnamed and no leak-site record to match

The item is carried because it is the only South African account in the window of what a ransomware event costs when the backups go with it, and because it lands in the same week as Sophos's South African survey, in which only 40 per cent of organisations recovered within a week, the lowest of any country surveyed.^{25,26} A six-month-old backup leaves six months of business to rebuild by hand; Section 10 returns to this. First reported by [MyBroadband](#) on 17 September 2026.

3.7 Carryovers

Rand Water, W37. No development in the window. No SENS statement, parliamentary question, attribution or statement about personal information could be located, and the parliamentary committee listing for 15 to 19 September carries nothing on it. The most recent item found remains ITWeb's of 4 September.^{27,28} Stays CONFIRMED for the intrusion with the three W37 tests open.

Black Axe extradition, W38. Resolved. W38 carried the Hawks' handover of six Nigerian nationals to the FBI and the United States Secret Service as a stated plan. MyBroadband reports the six were handed over on 11 September and that alleged leaders appeared before a United States federal court on Monday 14 September; five are charged as leaders of the Cape Town zone with wire fraud and aggravated identity theft over romance scams run from 2011 to 2021, with the Hawks estimating R100 million taken from victims.²⁹

USB Attorneys, LockBit 5.0, W38. No development. No firm statement, no Legal Practice Council comment and no data published. Stays CLAIMED; the Legal and Professional Services heatmap row is retired.

Rohloff Group, W36; The Courier Guy, W35; 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.

22. RelyComply, home page carrying client testimonials from Standard Bank and SnapScan, checked 20 September 2026. <https://relycomply.com/>

23. MyBroadband, Why EasyEquities, Cell C and a bank announced potential data breaches on the same weekend in South Africa (13 September 2026). <https://mybroadband.co.za/news/security/667365-why-easyequities-cell-c-and-a-bank-announced-potential-data-breaches-on-the-same-weekend-in-south-africa.html>

24. TimesLIVE, Cyberattacks put South Africans' personal data in the spotlight (15 September 2026). <https://www.timeslive.co.za/news/sci-tech/2026-09-15-cyberattacks-put-south-africans-personal-data-in-the-spotlight/>

25. MyBroadband, South African company which generated R4 million per month lost R50 million after a cyberattack (17 September 2026). <https://mybroadband.co.za/news/security/667352-south-african-company-which-generated-r4-million-per-month-lost-r50-million-after-a-cyberattack.html>

26. IT-Online, Defences improve, but ransomware still threatens SA businesses, reporting the Sophos State of Ransomware in South Africa 2026 survey (18 September 2026). <https://it-online.co.za/2026/09/18/defences-improve-but-ransomware-still-threatens-sa-businesses/>

27. ITWeb, Hackers breach Rand Water's defences (4 September 2026), the most recent Rand Water item located; nothing dated 13 to 19 September 2026 was found. <https://www.itweb.co.za/article/hackers-breach-rand-waters-defences/Gb3BwMWaO4ov2k6V>

28. Parliamentary Monitoring Group, committee meetings index, listing for 15 to 19 September 2026, checked 20 September 2026. <https://pmg.org.za/committee-meetings/?page=1>

29. MyBroadband, Nigerian crimelords operating in South Africa busted after 10 years and R100 million (16 September 2026). <https://mybroadband.co.za/news/security/667816-nigerian-crimelords-operating-in-south-africa-busted-after-10-years-and-r100-million.html>

4. THREAT ACTORS

Two profiles. The Gentlemen, because it took a ransom from a South African supplier and published the data anyway, and DireWolf, because it has now taken two South African data sets in a month. A note on ShinyHunters closes the section.

4.1 The Gentlemen: Paid, Published, and Now Extorting Downstream

The group's South African record now reads as a chain rather than a list. MIP Holdings was breached from late May, paid in June for an undertaking to destroy the data, and the same data surfaced on the group's leak site under Hollard's name on 7 September with a fresh demand to the insurer, refused, followed by publication.^{1,2} The remaining 44 MIP clients, almost all life insurers, hold data in the same set. MyBroadband names LegalWise and JustMoney among them.³ The group's tempo supports the reading that this is a business model rather than a lapse: the aggregator's index moved from 837 to 867 victims between 13 and 20 September, thirty listings in a week, and it now carries the Microsoft alias Storm-2697.³⁰ Black Kite counts 142 of its listings between January and July, second only to Qilin's 178, with manufacturing at 23 per cent of the group's own listings.³¹

Talos published the first open look at the group's infrastructure on 17 September, from an exposed directory tied to its Japanese intrusions, and the tooling is what a South African hunter should expect: RustHound and BloodHound for Active Directory mapping, NetExec, Impacket and Responder for credential work, Ligolo-ng and chisel for tunnelling, AnyDesk for persistence, nmap and masscan for scanning, sqlmap and exploit code for a GLPI SQL injection, a cPanel and WHM scanner, traces of Zerologon and MS17-010, and AdaptixC2 as the command framework.³² The exfiltration routine is precise enough to write a detection from. A backup share is mounted over CIFS at /mnt/Backup; virtual disk images are opened with libguestfs and nbd-client under /mnt/vhdx; ntfs.dit, SAM and SYSTEM are copied out and the secretsdump output saved as ntfs.txt and SAM.txt; the images are compressed with zstd and pushed to Wasabi cloud storage with rclone in 256 MiB chunks, sixteen uploads at a time; and the dumps and scan results are deleted afterwards.³² Talos also recovered a bash history with commands typed on a Russian keyboard layout and assesses the operators as Russia-based. Initial access in its cases came through VPN, remote access and network device weaknesses and through stolen credentials, which matches the MIP entry point. The aggregator holds 85 sample hashes and six Tox identifiers for the group; a subset is in iocs_w39.csv and the kernel-driver and GPO behaviours documented in W38 are unchanged.³³

4.2 DireWolf: Two South African Data Sets in a Month

DireWolf listed Cartrack on 2 September and RelyComply on 9 September, a telematics customer base and a FICA verification store, and both organisations have since confirmed the intrusions in their own words.^{24,5} The group's index stood at 135 victims on both 13 and 20 September, so it added nothing worldwide in the week it was preparing to publish RelyComply, and its 14-day countdown from the 9 September listing runs out on or about 23 September.^{30,7} DireWolf uses the double-extortion model: encryption at Cartrack, where the platform was restored within hours, and a data claim at RelyComply, where the provider rebuilt the environment. The aggregator carries no atomic indicators for the group, only a ransom-note name, HowToRecoveryFiles, and a generic YARA rule matching the group's own name; the W37 hunt indicators stand and the RelyComply case adds nothing technical because the third-party application and the zero-day are not named.^{33,5} What distinguishes the group's South African month is target selection: both victims are aggregators of other organisations' customer data, which is where a listing produces the most downstream notices per intrusion.

4.3 Note: ShinyHunters Against Clop

On the evening of Friday 18 September ShinyHunters defaced Clop's leak site through what it says was an unauthenticated file-upload flaw in the site's Grav CMS, claimed the site's source code and Tor private keys, and said it would extort the ransomware group. BleepingComputer confirmed the defacement and did not verify the wider claims.³⁴ It is carried as a one-line observation: Clop has no South African listing in the aggregator's 2026 record and the incident changes nothing for a South African defender beyond the reminder that leak-site infrastructure is itself contested.

30. ransomware.live API PRO, group index GET /groups, 400 groups, retrieved 13 and 20 September 2026 (public pages: ransomware.live/group/thegentlemen, /direwolf, /lockbit5). <https://api-pro.ransomware.live/groups>

31. Infosecurity Magazine, Manufacturing accounts for 22% of all ransomware victims, reporting Black Kite (18 September 2026). <https://www.infosecurity-magazine.com/news/manufacturing-22-ransomware-victims/>

32. Cisco Talos, Ransomware incidents in Japan in the first half of 2026: investigation of The Gentlemen's infrastructure and evidence of Qilin's AI use (17 September 2026). <https://blog.talosintelligence.com/ransomware-incidents-in-japan-in-the-first-half-of-2026/>

33. ransomware.live API PRO, per-group endpoints GET /iocs/{group}, /yara/{group} and /ransomnotes/{group}, retrieved 20 September 2026 (key required; the public group pages carry the same sets). <https://api-pro.ransomware.live/iocs/thegentlemen>

34. BleepingComputer, ShinyHunters hacks Clop leak site, threatens to extort ransomware gang (19 September 2026). <https://www.bleepingcomputer.com/news/security/shinyhunters-hacks-clop-leak-site-threatens-to-extort-ransomware-gang/>

5. CRITICAL VULNERABILITIES & CISA KEV

Seven vulnerabilities entered the CISA catalogue of known exploited vulnerabilities between 14 and 18 September 2026, against fourteen the week before. Four were past their remediation date on Monday 21 September, the day this report was published, and the three Linux kernel entries fell due on that day.¹² Every due date and overdue count in this section is arithmetic against the locally retrieved catalogue file, catalogVersion 2026.09.18, released at 19:00 UTC on Friday 18 September, so any addition made on Saturday 19 September is outside this edition; every CVSS score is from the NVD feed with its scoring source recorded.^{12,35} All seven carry knownRansomwareCampaignUse of Unknown, which is not the same as no. All seven received a three-day deadline under BOD 26-04, the catalogue's signal that the exploitation evidence was strong at listing. The week's shape differs from W38 in one respect that matters to a defender: four of the seven, the two Cisco entries, Pixel and Acronis, came with the vendor's own exploitation statement on the day of listing, and the two Cisco entries came with a one-line log check; the three kernel entries came with no vendor statement at all.

Cisco Secure Email Gateway CVE-2026-76461 is a SQL injection in AsyncOS that lets an unauthenticated remote attacker run commands as root on the gateway's operating system, scored 9.8 and affecting every physical and virtual appliance regardless of configuration; the Secure Email and Web Manager and the Secure Web Appliance are not affected.^{13,35} Cisco published on 14 September, the same day the catalogue listed it, stating that its PSIRT became aware of active exploitation in September through a TAC support case; Rapid7 reads the same-day listing as exploitation before disclosure and notes that the attacker needs no administrative interface, because a crafted email through a vulnerable gateway is enough.^{13,36} Fixed releases are 15.5.5-014 for 15.5 and earlier, 16.0.4-302 and 16.5.0-780, with Cisco recommending migration to 16.5.0-780 and reporting that every Secure Email Cloud device is already there; customers whose cloud devices showed indicators have been contacted directly.¹³ There is no workaround. The compromise check is a single grep for COPY.*TO PROGRAM across mail_logs, and the 17 September revision adds the detail that changes the recovery scope: cluster members authenticate to each other with

SSH key pairs that a compromised appliance exposes, so every member of a cluster containing one compromised appliance must be restored to a secure configuration.¹³ Cisco also warns that a root-level attacker may remove the log evidence and asks administrators to cross-check firewall logs for unexpected uploads from the gateway. No Shodan product label exists for the appliance and no South African figure is published.¹⁵

Cisco Identity Services Engine CVE-2026-76460 is the 10.0 of the week: an incorrect use of privileged APIs that lets an unauthenticated remote attacker bypass the web-based management interface of ISE and the ISE Passive Identity Connector, regardless of configuration.^{14,35} Cisco published on 16 September with the statement that its PSIRT is aware of active exploitation, again found through a TAC case; fixed releases are 3.1 Patch 12, 3.2 Patch 11, 3.3 Patch 12, 3.4 Patch 7 and 3.5 Patch 4, and release 3.0 has reached end of software maintenance with no fix.¹⁴ There is no workaround, but there is a mitigation: infrastructure access control lists that admit only required management and control-plane traffic to the appliance. The compromise check is show logging application ise-kong/access.log piped to dummyuser, run on every node of a distributed deployment; a hit means re-image the node and restore from a configuration backup.¹⁴ Cisco has not disclosed the endpoint, the request format or the scale of the attacks, no public proof of concept was identified by SOCRadar at the close of the window, and no actor is attributed.^{37,38} The same day's Cisco publication run carried 77 CVEs, 41 of them in ISE and 28 across the Secure Firewall line, including a 9.9 sftunnel root execution flaw in FMC, none of which is listed as exploited; the FMC static-credential advisory for CVE-2026-20316, exploited since July, was revised on 16 September to replace its hot fixes with fixed releases 7.0.10, 7.2.12, 7.4.8, 7.6.6, 7.7.13, 10.0.2 and 10.1.0.^{37,39} ISE is the network access control layer of a corporate estate, so a bypass of its management interface is a bypass of the policy that decides which devices join the network. No Shodan product label exists and no South African figure is published.¹⁵

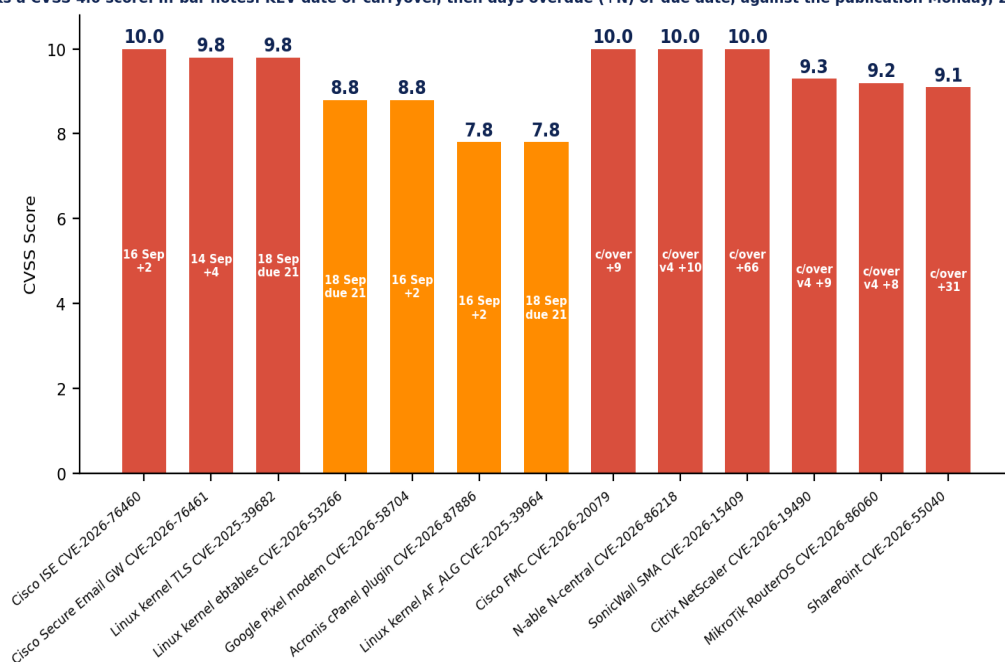
Google Pixel CVE-2026-58704 is an improper authorisation flaw in the cellular modem in which a logic error lets an attacker bypass permission checks and escalate privileges. Google's Pixel bulletin of 15 September says there are indications it may be under limited, targeted exploitation and gives no further detail; The Register and The Hacker News describe it as exploitable without user interaction, and the NVD vector, adjacent network with no interaction required, is consistent with that, although the bulletin itself says nothing about how it is triggered.^{40,35,41} Security patch level 2026-09-05 or later closes it along with 109 other Pixel flaws, 46 of them rated critical.^{40,41} The Hacker News prints a CVSS of 8.0 for this entry; the NVD feed read for this report gives 8.8 from the CISA-ADP source, and the feed figure is carried.³⁵ **Acronis CVE-2026-87886** is a local privilege escalation from insecure default file permissions in the Acronis Backup plugin for cPanel and WHM, the extension for Plesk and the plugin for DirectAdmin, scored 7.8. Acronis states that exploitation has been detected in the wild in limited, targeted attacks against cPanel and WHM deployments and, separately, that it sees no signs of exploitation on Plesk; fixed builds are 1.9.3.1021 for cPanel and WHM, 1.8.11.638 for Plesk and 1.2.3.238 for DirectAdmin, and the vendor has published nothing about the attacks.^{42,43} The affected product is a hosting control-panel add-on, which places the exposure with South African web hosts and the shared servers their customers rent; the Shodan discovery query for the product label returned zero in South Africa and is held rather than published.¹⁵

The three Linux kernel entries arrived together on 18 September with almost no public detail. CVE-2025-39682 is an improper check in the TLS receive path that lets a zero-length record bypass record-type handling, scored 9.8; CVE-2026-53266 is an out-of-bounds write in the ebttables SNAT target, scored 8.8, on a component the catalogue notes may be end of life; and CVE-2025-39964 is a race condition in AF_ALG sockets, scored 7.8.^{12,35,44} No one has published how any of the three is being

exploited or whether they form a chain; Red Hat updated its advisories at 02:00 UTC on 19 September to acknowledge active exploitation and public exploits.⁴⁴ They land in the same week as a separate set of four local root exploits from researcher Asim Manizada, DirtyAH6, TUNderflow, PPPoEject and DiagSpill, published on 18 September with fixed stable kernels 5.10.270, 5.15.221, 6.1.188, 6.6.157, 6.12.109, 6.18.50 and 7.2.4 and no reports of use in the wild; three of the four need unprivileged user namespaces, which a hardened host can disable.⁴⁵ The practical reading for a South African estate is that a local privilege escalation on Linux is a second-stage tool, and the first stage this week is already in the catalogue: a hosting control panel plugin, an email gateway that runs on Linux and a network access control appliance that does too.

Carryovers. Nothing in the W38 set was closed. NetScaler CVE-2026-19490, Cisco FMC CVE-2026-20079 and FortiOS CVE-2025-25249 are nine days overdue, the MikroTik pair CVE-2026-86060 and CVE-2026-67277 eight, N-central and Adobe Commerce ten, ScreenConnect and GitLab seven; the PaperCut pair fell due on 14 September and is seven days overdue; the SonicWall SMA 1000 September pair, Artifactory CVE-2026-82329, Kestra and Switchvox are sixteen; SharePoint CVE-2026-55040 is 31 days overdue against 830 exposed South African instances; the July SonicWall pair is 66 days overdue with ransomware use recorded as Known; and LiteLLM CVE-2026-42271 is 91 days overdue, the deepest tracked; and the Cisco FMC static-credential flaw CVE-2026-20316, 51 days overdue with ransomware use recorded as Known, is the other carryover besides the July SonicWall pair to carry that flag.^{12,15} Citrix's bulletin still carries only its 19 August initial publication and no mention of exploitation when checked on 20 September; Fortinet's advisory page could not be read this week behind a bot check, so the W38 finding that it read Known Exploited: No is neither confirmed nor withdrawn.⁴⁶ Horizon3 adds one calibration to the N-central entry: NIST scores CVE-2026-86218 at 9.8 under CVSS 3.1 against N-able's 10.0 under 4.0, and public intrusion reporting involves other recent N-central flaws, so not every compromise is attributable to this one.⁴⁷ The two Windows zero-days fell due on 22 September, the day after publication, and Chromium V8 CVE-2026-87491 on 23 September; Volexity's published GRIMWEDGE detail for the chain is in TH-2026-W39-07.^{12,48}

W39 KEV / CRITICAL CVE SEVERITY | 13 September - 19 September 2026
All seven KEV additions in the window (left) plus the six carryovers that most outrank them (right). CVSS from the NVD feed except CVE-2026-15409 (August feed); v4 marks a CVSS 4.0 score. In-bar notes: KEV date or carryover, then days overdue (+N) or due date, against the publication Monday, 21 September 2026



W39 CISA KEV / Critical CVE Tracking (seven additions 14 to 18 September plus active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-76461	Cisco Secure Email Gateway (AsyncOS)	9.8	SQL injection (unauth, root)	17 Sept	KEV 14 Sept. OVERDUE +4. Vendor confirms active exploitation, found via TAC case; crafted email is enough. Fixed 15.5.5-014 / 16.0.4-302 / 16.5.0-780; no workaround. Check: grep -i COPY.*TO PROGRAM in mail_logs on every cluster member; cluster SSH keys exposed. No ZA product label. Ransomware: Unknown. EPSS 0.0201.
CVE-2026-76460	Cisco Identity Services Engine and ISE-PIC	10.0	Privileged API misuse (unauth mgmt bypass)	19 Sept	KEV 16 Sept. OVERDUE +2. Vendor confirms active exploitation, found via TAC case; endpoint and scale undisclosed; no PoC located. Fixed 3.1 P12 / 3.2 P11 / 3.3 P12 / 3.4 P7 / 3.5 P4; 3.0 unsupported. Mitigation: iACLs. Check: ise-kong/access.log for dummyuser on every node; re-image on a hit. No ZA product label. Ransomware: Unknown. EPSS 0.0078.
CVE-2026-58704	Google Pixel (cellular modem)	8.8	Improper authorisation (adjacent EoP)	19 Sept	KEV 16 Sept. OVERDUE +2. Google: indications of limited, targeted exploitation; no trigger detail. Patch level 2026-09-05. THN prints 8.0; NVD feed 8.8 carried. ZA query zero, held. Ransomware: Unknown. EPSS 0.0021.
CVE-2026-87886	Acronis Backup plugin for cPanel and WHM, Plesk, DirectAdmin	7.8 (v3.0)	Incorrect default permissions (local EoP)	19 Sept	KEV 16 Sept. OVERDUE +2. Acronis: exploited in limited, targeted attacks on cPanel and WHM; no signs on Plesk. Fixed 1.9.3.1021 / 1.8.11.638 / 1.2.3.238. Hosting-provider estate. ZA query zero, held. Ransomware: Unknown. EPSS 0.0025.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2025-39682	Linux kernel (TLS receive path)	9.8	Improper check (record handling)	21 Sept	KEV 18 Sept. Due on publication day. No public exploitation detail; Red Hat acknowledges active exploitation and public exploits 19 Sept. No ZA product label. Ransomware: Unknown. EPSS 0.0120.
CVE-2026-53266	Linux kernel (ebtables SNAT)	8.8	Out-of-bounds write (local)	21 Sept	KEV 18 Sept. Due on publication day. Catalogue notes the component may be end of life. No public exploitation detail. Ransomware: Unknown. EPSS 0.0028.
CVE-2025-39964	Linux kernel (AF_ALG)	7.8	Race condition (local)	21 Sept	KEV 18 Sept. Due on publication day. Concurrent writes to one AF_ALG socket; crash or corrupted crypto results. No public exploitation detail. Ransomware: Unknown. EPSS 0.0079.
CVE-2026-19490	Citrix NetScaler ADC and Gateway	9.3 (v4.0)	Authentication bypass (unauth)	12 Sept	Carryover. OVERDUE +9. Bulletin unrevised since 19 Aug, still silent on exploitation. Fixed 14.1-73.32 / 13.1-63.21 / 13.1-37.277 FIPS; 12.1 and 13.0 EOL. Sessions as user anonymous. 110 in ZA. EPSS 0.0560.
CVE-2026-20079	Cisco Secure FMC and SCC Firewall Management	10.0	Authentication bypass (unauth, root)	12 Sept	Carryover. OVERDUE +9. Talos clusters UAT-12197, UAT-11823, UAT-11988. Static-credential companion CVE-2026-20316 now has fixed releases 7.0.10 to 10.1.0 (advisory v1.6, 16 Sept). Check: <code>zgrep package_info.*license /var/log/messages*</code> . No ZA product label. EPSS 0.7575.
CVE-2025-25249	Fortinet FortiOS, FortiSwitchManager	8.1	Heap overflow (CAPWAP, unauth)	12 Sept	Carryover. OVERDUE +9. PivotC2 campaign (SOCRadar). Fixed 7.6.4 / 7.4.9 / 7.2.12 / 7.0.18. Vendor page unreadable this week behind a bot check. FortiGate 2,791 in ZA. EPSS 0.0240.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-86060	MikroTik RouterOS	9.2 (v4.0)	Argument injection (SSH username)	13 Sept	Carryover. OVERDUE +8. CVE-2026-67277 shares the dates. CERT Polska chain; user ops; 82.192.72.4. Fixed 7.24.2 / 7.23.4 / 6.49.21. 5,585 in ZA, 4,561 on API port 8728. EPSS 0.0106.
CVE-2026-86218	N-able N-central	10.0 (v4.0)	Static code injection (pre-auth RCE)	11 Sept	Carryover. OVERDUE +10. Horizon3: NIST 9.8 under v3.1; not every N-central intrusion attributable to this CVE. Fixed 2026.3.1.14. No ZA product label. EPSS 0.0749.
CVE-2026-75650	Adobe Commerce and Magento Open Source	10.0	Template injection (unauth RCE)	11 Sept	Carryover. OVERDUE +10. StyleSmuggler; hotfix plus key rotation. No ZA product label. EPSS 0.0215.
CVE-2026-84869	ConnectWise ScreenConnect	9.9	Improper privilege management (client)	14 Sept	Carryover. OVERDUE +7. Fixed 26.6.5. GitLab CVE-2026-85706 (10.0, fixed 19.3.2 / 19.2.6 / 19.1.8) shares the date and the +7. ZA figure omitted as an artefact, see 7.2. EPSS 0.0069.
CVE-2026-82078	PaperCut NG/MF	9.4 (v4.0)	Unsafe reflection	14 Sept	Carryover. OVERDUE +7. CVE-2026-81578 shares the row. Maintenance releases 26.0.5 / 25.0.13 / 24.1.10. No ZA product label. EPSS 0.0357.
CVE-2026-83548	SonicWall SMA 1000	10.0	SSRF (unauth)	5 Sept	Carryover. OVERDUE +16. CVE-2026-83549 shares the dates; Artifactory CVE-2026-82329, Kestra CVE-2026-49869 and Switchvox CVE-2026-9586 share the due date and the +16. No SMA-specific ZA figure. EPSS 0.0467.
CVE-2026-55040	Microsoft SharePoint	9.1	Weak authentication (JWT forgery)	21 Aug	Carryover. OVERDUE +31. 830 in ZA. EPSS 0.5059, the highest among the carryovers after FMC.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-59822	BerriAI LiteLLM	8.8 (v4.0)	Improper authentication (MCP)	16 Sept	Carryover. OVERDUE +5. Starlette CVE-2026-48710 shares the date. Fixed 1.84.0, which also clears CVE-2026-42271 (due 22 Jun, OVERDUE +91, the deepest tracked). ZA figure omitted as an artefact, see 7.2. EPSS 0.0087.
CVE-2026-15409	SonicWall SMA 1000	10.0	SSRF (unauth)	17 Jul	Carryover. OVERDUE +66. CVE-2026-15410 shares the dates and the KNOWN ransomware flag; INC Ransom affiliate and UTA0533 attributed in July. Rebuild rather than patch.

Pattern note: the week's seven divide by how much the vendor told you. Cisco told you the most, twice: an active-exploitation statement, a fixed build and a one-line log check on the day of listing, which is the disclosure standard the W38 pattern note asked for and did not get from Citrix, Fortinet or N-able. Google and Acronis told you that exploitation exists and nothing about it. The kernel maintainers told you nothing at all, and the catalogue is the only public record that the three flaws are exploited. Prioritise by that gradient: the two Cisco entries can be verified in minutes on the appliance, the Pixel and Acronis entries are patch-and-move-on for the fleets that run them, and the kernel trio is a reason to check hosting and appliance patch levels rather than a hunt. On EPSS, ISE at 0.0078 and the email gateway at 0.0201 sit far below FMC at 0.7575 while all three are confirmed exploited by the same vendor; EPSS predicts the next thirty days and lags confirmed activity, so it ranks items not yet in the catalogue and must never deprioritise one that is.⁴⁹ Two carryovers still outrank most of the additions: the July SonicWall pair at 66 days with ransomware use Known, and SharePoint at 31 days against 830 exposed South African instances.^{12,15}

35. NVD API, CVSS base scores with scoring source, GET /rest/json/cves/2.0?cveId=, 55 CVEs resolved, retrieved 20 September 2026. <https://services.nvd.nist.gov/rest/json/cves/2.0>

36. Rapid7, CVE-2026-76461: Critical Cisco Secure Email Gateway vulnerability exploited in the wild (15 September 2026). <https://www.rapid7.com/blog/post/etr-cve-2026-76461-critical-cisco-secure-email-gateway-vulnerability-exploited-in-the-wild>

37. The Hacker News, Cisco warns of new zero-day ISE auth bypass (CVSS 10.0) exploited in active attacks (17 September 2026). <https://thehackernews.com/2026/09/cisco-warns-of-new-zero-day-ise-auth.html>

38. SOCRadar, CVE-2026-76460: Cisco ISE flaw actively exploited (17 September 2026). <https://socradar.io/blog/cve-2026-76460-cisco-ise-flaw/>

39. Cisco, Security advisory cisco-sa-fmc-static-cred-BET3Cjh, Secure Firewall Management Center static credential vulnerability, version 1.6 (updated 16 September 2026). <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh>

40. Google, Pixel Update Bulletin September 2026 (published 15 September 2026). <https://source.android.com/docs/security/bulletin/pixel/2026/2026-09-01>

41. The Hacker News, Google patches Pixel modem flaw amid signs of limited targeted exploitation (16 September 2026). <https://thehackernews.com/2026/09/google-patches-pixel-modem-flaw-amid.html>

42. Acronis, Security advisory SEC-10986, local privilege escalation due to insecure file permissions, CVE-2026-87886 (read through a browser, 20 September 2026). <https://security-advisory.acronis.com/advisories/SEC-10986>

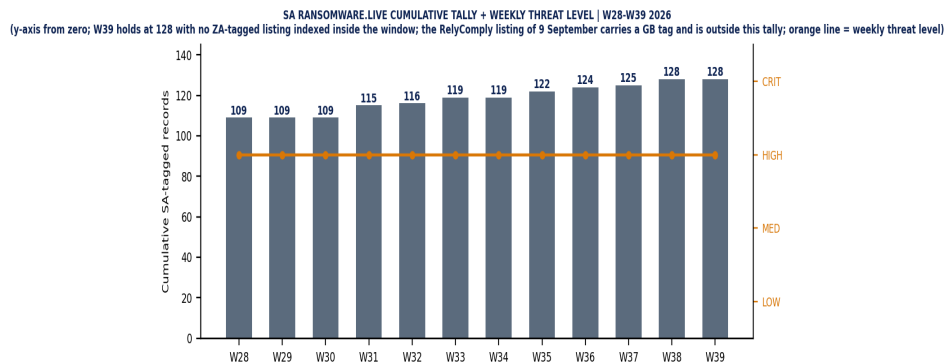
43. Help Net Security, Acronis Backup plugin vulnerability exploited in the wild (CVE-2026-87886) (16 September 2026). <https://www.helpnetsecurity.com/2026/09/16/acronis-backup-plugin-vulnerability-exploited-cve-2026-87886/>

44. The Hacker News, CISA flags three Linux kernel vulnerabilities exploited in the wild (19 September 2026). <https://thehackernews.com/2026/09/cisa-flags-three-linux-kernel.html>

45. The Hacker News, Public exploits released for four Linux kernel flaws that enable local root (18 September 2026). <https://thehackernews.com/2026/09/public-exploits-released-for-four-linux.html>
46. Citrix, NetScaler ADC and NetScaler Gateway security bulletin for CVE-2026-19489 and CVE-2026-19490, CTX696939, change log still showing only the 19 August 2026 initial publication when checked 20 September 2026. <https://support.citrix.com/external/article/CTX696939/netscaler-adc-and-netscaler-gateway-secu.html>
47. Horizon3.ai, CVE-2026-86218: N-able N-central pre-authentication remote code execution vulnerability (16 September 2026). <https://horizon3.ai/attack-research/vulnerabilities/cve-2026-86218/>
48. The Hacker News, China-linked hackers exploit Chrome-Windows zero-day chain to deploy GRIMWEDGE, reporting Volexity (15 September 2026). <https://thehackernews.com/2026/09/china-linked-hackers-exploit-chrome.html>
49. FIRST EPSS API, GET /data/v1/epss?cve=, 55 CVEs scored, retrieved 20 September 2026. <https://api.first.org/data/v1/epss>

6. RANSOMWARE LANDSCAPE

The South African victim feed held 128 records when retrieved at 02:00 UTC on 20 September 2026, unchanged on the previous week. The collection is country-scoped by path, the written file records 128 South African records against 128 returned, the run log records filter purity 1.0 and a clean exit, and the country filter that failed on 5 August is not in use.⁵⁰ A set-difference against the 13 September file returns zero additions and zero removals. Under this report's rule that a zero is usually a broken query, the absence was tested two further ways: the aggregator's own South African country page shows 128 victims with capricornlogistics.com as the newest, and its 100 most recent listings worldwide, covering 16 to 18 September, contain no ZA tag.^{51,52} The zero is therefore a zero in the aggregator's ZA tag, and South African victims can still sit outside it: the RelyComply listing of 9 September carries a GB tag, sits outside every ZA-scoped query, and was found only because five South African institutions named the company. The feed total of 128 is reported as the aggregator publishes it, and the derived South African count for the W38 window is corrected from two to three in Section 1; for this window it is zero by the tag and zero by hand search, with the caveat that the hand search finds only what a customer discloses.⁶



Baseline at W38 close	128 records
New listings dated inside the window	0 with a ZA tag. Zero confirmed by the aggregator's country page and by its 100 most recent listings worldwide
Back-filled South African victim	1: RelyComply AML Platform, DireWolf, discovered 9 September 2026 13:28 UTC, tagged GB by the aggregator, belonging to the W38 window. Not added to the 128, which is the aggregator's figure
Delistings or restorations	None. Set difference against the 13 September file returns zero additions and zero removals
End count at W39 retrieval	128 records, filter purity 1.0 in the run log and 128 of 128 tagged ZA in the file
Groups active against SA, rolling 120 days	15 by discovery date, unchanged; DireWolf would appear twice if the RelyComply record carried a ZA tag. The rolling boundary moves each week, so this figure is not a trend
Threat-level drivers	Two supplier breaches whose downstream victims number roughly 45 insurers and at least six financial institutions, one data set published after a ransom was paid, a second on a countdown to 23 September, and two Cisco zero-days on the network edge

Group notes. The Gentlemen 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 837 to 867, INC Ransom from 936 to 941, LockBit 5.0 from 359 to 364, Krybit from 146 to 149 and Qilin from 2,269 to 2,298; DireWolf, Deadlock, MedusaLocker and Payload did not move.³⁰ None of those additions carries a ZA tag. Of the last ten ZA-tagged listings in the feed, two are not South African and, of the remaining eight, three have been confirmed by the organisation named, Cartrack, Rohloff Group and the Furniture Bargaining Council, and one, Hollard, has been confirmed as a supplier's data published under the insurer's name.⁵⁰

The South African survey. Sophos's State of Ransomware in South Africa 2026 survey, reported on 18 September, draws on 135 South African IT and security leaders whose organisations were hit in the previous twelve months, and the figures give a national ransomware baseline to set beside the SABRIC fraud statistics. Data was encrypted in 63 per cent of incidents, above the 56 per cent global figure and up from 60 per cent in the 2025 survey. The median ransom demand fell 57 per cent to R6.8 million and the median payment 28 per cent to about R5 million, with those who paid handing over 71 per cent of the original demand; the recovery cost excluding any ransom was put at over R17 million, down from R21 million. The root causes were compromised credentials at 27 per cent, exploited vulnerabilities at 25 per cent and malicious email at 22 per cent, and 47 per cent of respondents cited a lack of adequate protection, the highest proportion in any country surveyed. Backups were used to recover data in 54 per cent of cases, up from 35 per cent, and payment fell from 71 to 58 per cent. Only 40 per cent recovered within a week, the lowest rate of any country surveyed and down from 47 per cent.²⁶ ITWeb's account of the same release prints the median demand as R6.9 million; IT-Online's R6.8 million is carried as the figure that matches the stated dollar value.⁵³ Read alongside the R50 million manufacturing case in Section 3.6 and the MIP payment in Section 3.1, the survey describes a market in which demands are falling and recovery is still the slowest measured.

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 19 September may not appear until next week's collection. 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. A second caution is new this week: the aggregator's country tag has now failed in both directions, and a South African victim tagged to another country is invisible to every ZA-scoped method this report uses until a customer names it.

50. ransomware.live API, SA victim records, GET /v2/countryvictims/ZA, 128 records all tagged ZA, retrieved 02:00 UTC 20 September 2026. <https://api.ransomware.live/v2/countryvictims/ZA>

51. ransomware.live, country page for South Africa, showing 128 victims with capricornlogistics.com as the newest, checked 20 September 2026. <https://www.ransomware.live/country/ZA>

52. ransomware.live API, GET /v2/recentvictims, the 100 most recent listings worldwide (16 to 18 September 2026), none tagged ZA, retrieved 20 September 2026. <https://api.ransomware.live/v2/recentvictims>

53. ITWeb, SA organisations under pressure to protect against ransomware onslaught (18 September 2026). <https://www.itweb.co.za/article/sa-organisations-under-pressure-to-protect-against-ransomware-onslaught/Pero37Z36dyMQb6m>

7. OSINT EXPOSURE & ATTACK SURFACE

7.1 What the Panel Publishes, and What It Cannot

Every figure in this section is an exposure count: how many instances of a product Shodan sees on the South African internet, not a count of vulnerable systems. The vuln: filter is unavailable on this collection's plan, so no figure here should be read as the number of South African systems affected by a given CVE. Only results the collection marks VERIFIED are published. This week the discovery stage examined all five vendor and product pairs added to the catalogue and promoted none: Shodan has no product label for the Linux kernel, Cisco Identity Services Engine or Cisco Secure Email Gateway, so those are held for manual fingerprinting, and the Pixel and Acronis Backup labels returned zero South African hits, which are held under the rule that a zero from one method is not evidence of absence.¹⁵ The Palo Alto GlobalProtect title match and the Arista VeloCloud zero remain unpublishable. No organisation is named anywhere in this section.

7.2 Two Withheld Figures, Now Resolved as Artefacts

W38 withheld the LiteLLM and ScreenConnect counts on a port-concentration test and set the observation that would settle them: a third collection either finding a genuine port cluster or confirming the scatter. The third collection confirms the scatter. LiteLLM returned 6,410 South African instances, up from 5,171, with its five most common ports carrying twelve, nine, seven, six and six hosts; ScreenConnect returned 2,942, with its five most common ports carrying four, four, three, three and three.¹⁵ A population of thousands spread across hundreds of ports at a handful apiece, none of them the product's defaults, on three successive collections, is a fingerprint matching something other than the product or a deception network answering with the product's banner, and either way it is not a count of proxies or clients. Both figures are marked artefact and will be omitted from the panel until the collector's port-concentration test is implemented and the queries re-derived; the W38 watch item closes on that basis. The remaining promoted queries pass the same test comfortably: of 5,585 MikroTik instances, 4,561 sit on the API port 8728; of 922 Tomcat instances, 276 sit on 8080; of 2,791 FortiGate instances, 1,474 sit on 10443.¹⁵

7.3 The Standing Exposure Panel

MikroTik RouterOS	5,585; 4,561 on the API port 8728 and 1,024 carrying the sshd product label. The largest population in the panel, against a chain eight days overdue with a named attacker address
Fortinet FortiGate	2,791. Facet resolves cleanly across model variants. The product family behind CVE-2025-25249 and the target of Arctic Wolf's late-August credential waves; a family count that says nothing about patch level
Citrix Netscaler	110, noting Shodan's lowercase spelling. The population sitting against CVE-2026-19490, nine days overdue with a public exploit
Microsoft SharePoint on-prem	830. Component match. The population sitting against CVE-2026-55040, 31 days overdue
SonicWall, all products	2,885, summing five product strings; 10 on the SSL-VPN proxy string. It CANNOT be narrowed to the SMA 1000 line that carries four catalogue entries
Apache Tomcat / Cisco ASA WebVPN	922 across the Tomcat and Coyote labels; 385 ASA WebVPN on the /+CSCOE+/ path
Exposed RDP and port 445	8,168 services on port 3389; 5,279 on port 445, mostly unfingerprinted, so read the second as services on that port rather than identified SMB servers
WordPress / Langflow / Metabase	387, a floor because component detection undercounts; 77; 136
MLflow / Ray / vCenter	92, 67 and 3, carried. The vCenter figure is an external count of a normally internal system
ownCloud / Gitea / Artifactory	144, 10 and 2, carried. Artifactory sits against four catalogue entries
LiteLLM / ScreenConnect	ARTEFACT, 6,410 and 2,942 returned and not published. See 7.2
This week's seven additions	No figure. No product label for Cisco SEG, Cisco ISE or the Linux kernel; Pixel and Acronis Backup returned zero and are held

These are point-in-time magnitudes. The collection records that Shodan rescan artefacts have moved individual counts by as much as 73 per cent inside twenty-four hours, so week-on-week movement in these figures is not a finding and none is drawn here.¹⁵ The right use of them is the absolute size of an exposed population sitting against an actively exploited flaw, which this week is 5,585 RouterOS instances, 110 NetScaler instances and 830 SharePoint instances, all against entries that are overdue.

7.4 Credentials: The Access Route of the Month

Two of the week's South African incidents began with a credential. MIP's intruders used a password an employee had reused on an unrelated breached service, and Cell C Fibre's provider reports its own access credentials compromised.^{1,17} The Hollard record in the aggregator shows what that route looks like from the outside: third-party stealer-log telemetry for the insurer's domain of 22 employee and 200 user credential records across Raccoon, RedLine and Vidar logs, the most recent employee compromise dated 1 May 2026, stored with this edition's evidence; it describes an available route and does not show it was used.⁵⁴ Arctic Wolf adds the edge-appliance version: two waves of credential attacks against

internet-facing Fortinet VPN appliances from 26 to 28 August generated tens of millions of authentication failures using organisation-specific usernames, corporate email addresses and common administrative identities, and in one environment a successful login from 158.94.211.14 was followed by malicious activity.¹⁸ FortiGate is the largest appliance population in this panel at 2,791. The Sophos survey's 27 per cent for compromised credentials as the root cause is the national figure for the same pattern.²⁶

54. ransomware.live API, victim record via GET /v2/searchvictims/hollard: Hollard Insurance Group, The Gentlemen, discovered 7 September 2026 21:56 UTC, retrieved 20 September 2026 and stored as evidence/w39_ransomwarelive_searchvictims_hollard_2026-09-20.json (public page: ransomware.live/id/SG9sbGFyZCBJbnN1cmFuY2UgR3JvdXBAdGhIZ2VudGxlbWVu). <https://api.ransomware.live/v2/searchvictims/hollard>

8. REGULATORY & POLICY

8.1 The Regulator, the Register and Two Open Cases

The enforcement-notices register still carries nothing later than the Gauteng Department of Health notice listed on 10 June, and the media statements index nothing later than the briefing invitation of 27 August; the SABS notice described at the 31 August briefing has not appeared in three weeks, and the KPI moves to fifteen weeks.^{55,56} The week did, however, produce two cases that will test the Regulator in public. MIP reported its June breach to the Regulator and the Prudential Authority and says the Regulator's case remains open; RelyComply reported under reference SC20263150, and EasyEquities and Alexforbes report their own notifications.^{1,5,10} TechCentral put questions to the Regulator and to the Reserve Bank on 18 September, including how many notifications the MIP incident has produced, whether the investigation extends to the insurers that used MIP as an operator, and whether the Regulator takes a view on operators paying ransoms; both undertook to answer by Monday 21 September, which is publication day for this edition and a watch item in Section 11.² Neither regulator had said anything in public by the close of the window, and the Prudential Authority's systemic-risk meeting with MIP is known only from MIP's account.¹

8.2 Responsible Party, Operator, and Three Clocks

The MIP and RelyComply cases turn on one section of POPIA. The obligation to notify the Regulator and the data subjects under section 22 rests with the responsible party, the insurer or the bank, rather than with the operator processing on its behalf; MIP's response, building a messaging platform so each insurer could notify its own customers, is the practical expression of that rule, and Hollard's statement that it notified affected customers after the June incident is the insurer performing it.^{1,4} Werksmans' two-part survey of African cybercrime law, published on 17 September, adds the second clock: section 54 of the Cybercrimes Act requires electronic communications service providers and financial institutions to report cyber offences to the South African Police Service within 72 hours of becoming aware of them, with a fine of up to R50,000 for non-compliance, and the authors' point is that one incident triggers parallel reports to different authorities under different statutes with different thresholds.⁵⁷ The third clock is the FSCA and Prudential Authority 24-hour notification under Joint Communication 5 of 2026, covered in W38, which runs from the institution's own classification of materiality. The survey also records that only 20 of 55 African Union states have ratified the Malabo Convention and that the UN Convention Against Cybercrime, opened for signature in Hanoi on 25 October 2025, enters into force 90 days after the fortieth ratification; Nigeria's 72-hour reporting duty to its national CERT carries a N2 million fine.^{57,58} For a South

African group with regional subsidiaries the RelyComply pattern, one provider and many institutions, is the case in which all three clocks start at once.

8.3 Fraud: The Tax Season, the Fake Fine and the Forged Card

Kaspersky reports a working replica of the SARS eFiling login page that harvests usernames, passwords and phone numbers, a second lure built as an Adobe PDF sign-in screen that takes email credentials, and attachments named in the pattern Tax Returns Of RXX,XXX.XXX and Final_Assessment_Notification-2026-0X-0X.pdf carried in emails using the phrases Refund due and SARS Letter of demand, all timed to the 23 October filing deadline for non-provisional taxpayers.^{21,59} SARS itself published no new alert in the window; the most recent remains SARS-SCAM-400 of 2 September.⁶⁰ The Road Traffic Infringement Agency warned of cloned AARTO payment portals and messages using the subject lines Final Notice: Action Required to Avoid Additional Penalties and Final Demand: Enforcement Notices, sent after hours and at month-end, offering a R250 discounted settlement; the only official site is online.aarto.gov.za and genuine notices arrive as password-protected PDFs opened with the recipient's identity number.⁶¹ Capitec expects impersonation of Takealot, Game and Incredible ahead of Black Friday and reports blocking over 131,000 suspicious beneficiary accounts, 64,000 of them mule accounts, and protecting clients from over R699 million in losses between July 2025 and June 2026.²⁰ Police arrested a man in Hillbrow on 10 September with six completed smart identity cards, 22 blank cards and a card printer, alongside forged bank statements and payslips, which is the supply side of the identity-number market the MIP and RelyComply sets feed.⁶² Investec's head of fraud risk told the Morningstar conference on 10 September that phishing is the entry point in 99 per cent of business email compromise cases, that the fidelity fund does not cover cyber losses, and that the banking regulator's stance is that a bank which did not materially contribute to the fraud generally bears no liability, with the Supreme Court of Appeal's 2024 Hawarden ruling as the illustration.⁶³ The Black Axe extradition is recorded in Section 3.7.

8.4 Public Bodies and the Quiet Regulators

Airports Company South Africa's annual report rates cyber threats as highly likely with significant consequence, four and three on a five-point scale, lowered its residual rating from Priority I to Priority II on the strength of a dedicated cybersecurity operations centre and cloud identity protection, and records that IT capital spend of R266 million ran below a R464 million budget; its only disclosed incident remains the compromise of 50 email accounts in January 2019.⁶⁴ Parliament's committee listing for 15 to 19 September carries nothing on cybersecurity, Rand Water, SITA or the Information Regulator.²⁸ ISPA's advisory on .za domain fraud sets out the remedies a South African organisation has when its name is used in a fraudulent domain: the ISPA take-down notice for locally hosted sites, the ZA Registry Consortium abuse process for .za names without a local host, the .za alternative dispute resolution process for impersonation, and a report to the National Cybersecurity Hub.⁶⁵ The FIC, ICASA, the NCR and SABRIC could not be read in this environment and are recorded as unchecked rather than as silent.

8.5 Who to Call

Six South African teams are registered with FIRST and remain current in this week's collection: the Cybersecurity Hub for private and public sector organisations, ECS-CSIRT at the State Security Agency for government and military, SA NREN CSIRT for research and education, and the UCT, Standard Bank Group

and Vodacom Group teams.⁶⁶ An insurer, a bank or a software supplier in the position of this week's named organisations has the Cybersecurity Hub as its constituency match. Notifying a CSIRT is not the same as notifying the Information Regulator under POPIA section 22, the Police under Cybercrimes Act section 54 or the FSCA and Prudential Authority under Joint Communication 5; a regulated financial institution whose supplier has lost personal information owes all four, and the provider's own notice, as RelyComply's did, should say which of them it has made.

55. Information Regulator of South Africa, enforcement notices register; the 2026 tab carries three instruments dated 20 May, 2 June and 10 June 2026 and nothing later, checked 20 September 2026. <https://infoeregulator.org.za/enforcement-notice/>

56. Information Regulator of South Africa, media statements index, most recent entry the media invitation of 27 August 2026, checked 20 September 2026. <https://infoeregulator.org.za/media-statements/>

57. Werksmans Attorneys, Cybercrime across borders: navigating Africa's fragmented legislative landscape, Part 1 (17 September 2026). <https://werksmans.com/cybercrime-across-borders-navigating-africas-fragmented-legislative-landscape-part-1/>

58. Werksmans Attorneys, Cybercrime across borders: navigating Africa's fragmented legislative landscape, Part 2 (17 September 2026). <https://werksmans.com/cybercrime-across-borders-navigating-africas-fragmented-legislative-landscape-part-2/>

59. IT-Online, Tax deadline rush gives scammers an opening (18 September 2026). <https://it-online.co.za/2026/09/18/tax-deadline-rush-gives-scammers-an-opening/>

60. SARS, Scams and phishing index, most recent entry SARS-SCAM-400 (2 September 2026), checked 20 September 2026. <https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>

61. MyBroadband, AARTO scam targets South African motorists with fake fines and threatens to block licences (16 September 2026). <https://mybroadband.co.za/news/motoring/667800-aarto-scam-targets-south-african-motorists-with-fake-fines-and-threatens-to-block-licences.html>

62. MyBroadband, South Africa's fraud-resistant smart IDs are being forged (15 September 2026). <https://mybroadband.co.za/news/government/667581-south-africas-fraud-resistant-smart-ids-are-being-forged.html>

63. Moonstone, Your client's email is hacked. You make the payment. Who pays? (17 September 2026). <https://www.moonstone.co.za/your-clients-email-is-hacked-you-make-the-payment-who-pays/>

64. MyBroadband, Biggest airports in South Africa highly likely to be hacked with significant consequences (15 September 2026). <https://mybroadband.co.za/news/security/667686-biggest-airports-in-south-africa-highly-likely-to-be-hacked-with-significant-consequences.html>

65. IT-Online, There are remedies for .za domain name fraud, reporting ISPA (18 September 2026). <https://it-online.co.za/2026/09/18/there-are-remedies-for-za-domain-name-fraud/>

66. FIRST member teams. SA CSIRT records retrieved via the ransomware.live /csirt/ZA endpoint, 20 September 2026, six teams. <https://www.first.org/members/teams/>

9. WEEKLY THREAT HUNT & IOCs

Eight missions. Three P1 cover the week's confirmed exploitation on the network edge, the two Cisco zero-days and The Gentlemen's exfiltration routine as Talos documented it, each with the vendor's or the responder's own indicators. Three P2 cover the supplier pattern that produced nine South African confirmations: the integration credential a breached verification provider leaves behind, the reused password against a SaaS support platform, and the hosting-estate privilege escalations that the Acronis and kernel entries describe. Two P3 cover the endpoint chain behind the Pixel and Chromium entries and the seasonal phishing lures. Indicators come from vendor advisories, named responder reporting and the aggregator's per-group feeds, and the atomic detail is exported to iocs_w39.csv rather than repeated in full here.³³ No hunt is repeated from a prior week without new justification: the W38 NetScaler, FMC, MikroTik and management-plane missions stand as written and are not reprinted, and the DireWolf indicators from W37 are unchanged.

TH-2026-W39-01: The Gentlemen: Backup-Share Mounting and Rclone Exfiltration to Wasabi

P1 CRITICAL: SA supplier paid and was published anyway; 44 MIP clients hold the same data set

Hypothesis: A Gentlemen operator with domain credentials has mounted a backup share, opened virtual disk images offline to lift the domain database and registry hives, dumped credentials with Impacket, and is staging the images to Wasabi cloud storage with rclone in parallel chunks before any encryption or listing, so the extortion holds whether or not the ransom is paid.

MITRE ATT&CK: T1078 (Valid Accounts), T1021.002 (SMB/Windows Admin Shares), T1003.003 (OS Credential Dumping: NTDS), T1003.002 (Security Account Manager), T1005 (Data from Local System), T1560.001 (Archive via Utility), T1567.002 (Exfiltration to Cloud Storage), T1070.004 (File Deletion), T1219 (Remote Access Software).

IOCs: Per Talos: a backup share mounted over CIFS at /mnt/Backup; VHDX images opened with libguestfs-tools, qemu-utils and nbd-client under /mnt/vhdx; ntds.dit, SAM and SYSTEM copied out; secretsdump output saved as ntds.txt and SAM.txt; zstd compression; rclone to Wasabi in 256 MiB chunks with 16 concurrent uploads; tooling RustHound, BloodHound, NetExec, Impacket,Responder, Ligo-ng, chisel, AnyDesk, nmap, masscan, sqlmap and AdaptixC2; scripts and dumps deleted after use. From the aggregator feed: 85 sample hashes, six Tox identifiers and two contact addresses, elsignore@onionmail.org and thegentlemen88@atomicmail.io; a subset is in iocs_w39.csv. Talos Snort 2 coverage 1:67111.

Data Sources: SMB session and file-share audit logs on backup servers and NAS devices, Linux auditd for mount, nbd-client and guestmount, EDR process telemetry for secretsdump and rclone, egress netflow and proxy logs to Wasabi and other object-storage endpoints, and AnyDesk service installations.

Detection Guidance: Alert on any Linux host in the estate mounting a Windows backup share and then loading nbd or guestfs modules, because the pair has no legitimate use outside a restore exercise. Alert on rclone or any process opening dozens of parallel HTTPS sessions to object-storage domains from a server that does not back up to the cloud. Treat a copy of ntds.dit outside a domain controller's own backup chain as an incident. For the 44 MIP insurers and any organisation whose supplier has paid a Gentlemen ransom, assume the data will be published and issue the customer notice on that basis.

TH-2026-W39-02: Cisco Secure Email Gateway: SQL Injection to Root From a Crafted Email**P1 CRITICAL:** zero-day, active exploitation confirmed by Cisco, due 17 September, OVERDUE +4

Hypothesis: An attacker has sent a crafted email through an internet-facing Cisco Secure Email Gateway and used CVE-2026-76461 to execute commands as root, then harvested the cluster's SSH key material and staged data outward through the gateway, removing the mail_logs evidence afterwards.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), T1552.004 (Unsecured Credentials: Private Keys), T1021.004 (Remote Services: SSH), T1048 (Exfiltration Over Alternative Protocol), T1070 (Indicator Removal).

IOCs: Cisco's check: `grep -i "COPY.*TO PROGRAM" mail_logs` on the appliance, run on every cluster member; any entry may indicate malicious activity. Affected: every physical and virtual Secure Email Gateway regardless of configuration; not affected: Secure Email and Web Manager, Secure Web Appliance. Fixed AsyncOS 15.5.5-014, 16.0.4-302, 16.5.0-780. Cluster SSH key pairs exposed by one compromised member. Snort 67109 and 67110. No attacker addresses or hashes published by Cisco or Rapid7.

Data Sources: Appliance mail_logs and system logs, cluster membership records, perimeter firewall and netflow for connections initiated by the gateway to external addresses, and change records for appliance credentials and certificates.

Detection Guidance: Run the grep on every member before and after patching, because the hit is in the log the attacker may have cleaned; where the log is empty but the appliance is old, cross-check firewall logs for uploads initiated from the gateway's address. Rebuild a virtual appliance on 16.5.0-780 from a fresh image and reimport configuration rather than patching in place, renew every credential and cryptographic secret the gateway held, and restore every member of a cluster containing one compromised member. For a physical appliance open a TAC case and enable remote access for Cisco. Cisco Secure Email Cloud customers with indicators have been contacted; an appliance Cisco has not called about still needs the check.

TH-2026-W39-03: Cisco ISE: Management-Interface Bypass on the Network Access Control Plane**P1 CRITICAL:** CVSS 10.0 zero-day, active exploitation confirmed by Cisco, due 19 September, OVERDUE +2

Hypothesis: An attacker has reached the ISE or ISE-PIC web management interface from an untrusted network, used CVE-2026-76460 to bypass authentication through a privileged API on the node that decides which devices and users are admitted to the network, with the root command execution Cisco warns may follow, with the aim of changing authorisation policy or harvesting the identities ISE holds.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1556 (Modify Authentication Process), T1098 (Account Manipulation), T1552 (Unsecured Credentials), T1562 (Impair Defenses), T1059 (Command and Scripting Interpreter).

IOCs: Cisco's check: show logging application ise-kong/access.log | include dummyuser, on every node of a distributed deployment; additional logs in a support bundle at ./ise/logs/apigateway/access.log.gz. Any entry may indicate malicious activity. Fixed 3.1 Patch 12, 3.2 Patch 11, 3.3 Patch 12, 3.4 Patch 7, 3.5 Patch 4; release 3.0 is unsupported. Mitigation: infrastructure ACLs on the management and control plane. Companion FMC check for CVE-2026-20316: zgrep "package_info.*license" /var/log/messages* with a hit referencing /var/tmp/license.tmp; fixed releases 7.0.10 to 10.1.0.

Data Sources: ISE application access logs on every node, administrative audit logs, policy-set change history, RADIUS and TACACS authorisation records for unexpected permits, and perimeter logs for management traffic to ISE from outside the management ranges.

Detection Guidance: Run the dummyuser check on every node, because a distributed deployment logs locally; a hit means re-image the node and restore from configuration backup rather than patch. Put an infrastructure ACL in front of the management interface on Monday 21 September whether or not the patch is applied, since no exploit detail is public and the bypass is unauthenticated. Review every policy-set and authorisation-profile change since 1 September against change records, and treat an unexplained permit rule as the objective of the intrusion. Apply the same discipline to FMC, where the static-credential flaw is still exploited and the new fixed releases replace the July hot fixes.

TH-2026-W39-04: Breached Verification Provider: Integration Credentials and the DireWolf Countdown

P2 HIGH: one KYC platform, at least six institutions; provider countdown runs to about 23 September

Hypothesis: An attacker who held a compliance provider's environment for six days before detection has copied the API tokens, single sign-on federation metadata and stored customer verification records, and may use the tokens against the institutions' own integrations, or the records to pass another institution's onboarding, after the provider's rebuild.

MITRE ATT&CK: T1199 (Trusted Relationship), T1528 (Steal Application Access Token), T1550.001 (Use Alternate Authentication Material: Application Access Token), T1078.004 (Valid Accounts: Cloud Accounts), T1530 (Data from Cloud Storage), T1486 (Data Encrypted for Impact).

IOCs: From RelyComply's notice: unauthorised access through a zero-day in an unnamed third-party application; customers asked to rotate RelyComply API tokens and refresh identity-provider configurations; incident reference SC20263150. From the aggregator feed for DireWolf: ransom note HowToRecoveryFiles; a name-match YARA rule; no atomic indicators published for the group. Data classes held per SA Home Loans and Peregrine: identity or passport number, date of birth, contact details, residential address, employer, PEP status and, for some clients, bank account details.

Data Sources: Your own integration logs for the provider's API, identity-provider sign-in and token-issuance logs for the federation used with the provider, outbound calls from your systems to the provider's endpoints, and onboarding-fraud telemetry for applications that pass verification with data matching the exposed classes.

Detection Guidance: Rotate the provider API tokens and the SSO federation now and again after the provider's forensic sign-off, as SA Home Loans and Alexforbes did, because a credential minted before the rebuild survives it. Alert on any call to the provider's API from a source address outside your own integration ranges, and on token use after rotation. Raise the manual-review threshold on new-account onboarding where the applicant's identity number appears in your own exposure set, since the FICA file is exactly what synthetic-identity fraud needs. Prepare the section 22 and Joint Communication 5 notifications before the countdown lapses rather than after.

TH-2026-W39-05: Reused Passwords Against SaaS Support Platforms and the Stealer-Log Signal**P2 HIGH:** one reused password on a personal laptop opened a Jira instance holding 400,000 records

Hypothesis: An employee's password, reused on an unrelated service that was breached or captured by an infostealer, has been used from an unmanaged device to sign in to a SaaS ticketing or collaboration platform that holds customer data pasted into tickets, and data is being read out slowly enough to stay under volume alerts.

MITRE ATT&CK: T1078 (Valid Accounts), T1586.002 (Compromise Accounts: Email Accounts), T1133 (External Remote Services), T1213 (Data from Information Repositories), T1530 (Data from Cloud Storage), T1020 (Automated Exfiltration).

IOCs: From TechCentral on MIP: credentials reused on an unrelated breached service, an employee's personal laptop, an Atlassian Jira service under decommissioning, about three weeks of slow exfiltration from 25 May, identity numbers pasted into tickets in the clear. From the aggregator record for Hollard: third-party stealer-log telemetry of 22 employee and 200 user credential records across Raccoon, RedLine and Vidar. From Arctic Wolf via The Hacker News: Fortinet VPN credential waves 26 to 28 August using organisation-specific usernames and administrative identities, with 158.94.211.14 as the address behind one successful login.

Data Sources: SaaS platform audit logs (Atlassian, ServiceNow, Zendesk, Freshdesk) for sign-ins by device, location and API token, identity-provider conditional-access logs, stealer-log monitoring for your own domain, and VPN authentication logs for failure storms against named accounts.

Detection Guidance: Enforce single sign-on with multi-factor authentication and a device-compliance condition on every SaaS platform that holds tickets, because a support ticket is a customer record. Alert on sign-ins from unmanaged devices and on bulk issue exports or API reads outside working hours. Search your ticket stores for identity-number patterns and scrub them; MIP's tickets were supposed to be obfuscated and were not. Subscribe to stealer-log monitoring for your domain and reset any account that appears, and treat tens of thousands of VPN failures against named accounts as a credential attack rather than noise.

TH-2026-W39-06: Hosting Estates: cPanel Backup Plugin and Kernel Privilege Escalation**P2 HIGH:** Acronis plugin exploited in targeted attacks; three kernel flaws in the catalogue with no detail

Hypothesis: An attacker holding a single hosting account or a low-privileged shell on a shared Linux server has used the Acronis Backup plugin's default permissions, or one of the kernel flaws now in the catalogue, to reach root and every other tenant's data on the host.

MITRE ATT&CK: T1068 (Exploitation for Privilege Escalation), T1548 (Abuse Elevation Control Mechanism), T1222.002 (File and Directory Permissions Modification: Linux), T1078.003 (Valid Accounts: Local Accounts).

IOCs: Acronis: cPanel and WHM plugin before build 1.9.3.1021, Plesk extension before 1.8.11.638, DirectAdmin plugin before 1.2.3.238; exploitation confirmed on cPanel and WHM only. Kernel: CVE-2025-39682 (TLS receive path), CVE-2026-53266 (eatables SNAT), CVE-2025-39964 (AF_ALG); no public indicators. Separate public local-root exploits DirtyAH6 CVE-2026-80844, TUNderflow CVE-2026-81000, PPPoEject CVE-2026-68121 and DiagSpill CVE-2026-74469, fixed in stable kernels 5.10.270, 5.15.221, 6.1.188, 6.6.157, 6.12.109, 6.18.50 and 7.2.4; three of the four need unprivileged user namespaces.

Data Sources: cPanel and WHM access and error logs, auditd for setuid and capability changes, kernel logs for oops and warning storms, process telemetry for user-namespace creation by tenant accounts, and file integrity monitoring on the plugin's directories.

Detection Guidance: Update the Acronis plugins first on cPanel hosts, where exploitation is confirmed, then patch kernels to a fixed stable release and reboot. Disable unprivileged user namespaces where no workload needs them, which removes three of the four public exploits, and unload AH6, TUN/TAP, PPPoE and SCTP where unused. Alert on any tenant process creating a user namespace or writing under the plugin's paths. A South African hosting provider whose customers include the organisations in Section 3 should treat this as the week's patch priority.

TH-2026-W39-07: Endpoint Chain: Pixel Modem Zero-Click and the GRIMWEDGE Browser Implant

P3 MEDIUM: limited, targeted exploitation; espionage clusters; September patches close both

Hypothesis: A targeted individual's Pixel handset has been compromised through the cellular modem without interaction, or a Windows workstation has been compromised through the Chrome and ALPC chain via a spear-phishing link, and a lightweight implant is reading files and credentials for a state-aligned operator.

MITRE ATT&CK: T1203 (Exploitation for Client Execution), T1068 (Exploitation for Privilege Escalation), T1574.002 (DLL Side-Loading), T1176 (Browser Extensions), T1056.001 (Keylogging), T1539 (Steal Web Session Cookie), T1041 (Exfiltration Over C2 Channel).

IOCs: Pixel: CVE-2026-58704, security patch level 2026-09-05 or later; no indicators published by Google. GRIMWEDGE per Volatility via The Hacker News: loader msgbox.exe side-loading wsc.dll, JavaScript payload variables p1, p2 and pp, C2 domain ocr.opusaccel[.]top polled over HTTP with commands executed through eval, an MSI installer carrying an obfuscated JavaScript backdoor; LONGTALE Chrome extension masquerading as Google Gemini, extension ID ckiknalbep1pcpofpnabcnhjcecgckfei; actors UTA0560 and JungleBamboo (APT31); delivery through a reflected XSS on a United States university site filtering for Chrome on Windows.

Data Sources: Mobile device management patch-level reporting, Chrome extension inventory from browser management, DNS and proxy logs for the C2 domain, process creation for msgbox.exe with a sideloaded wsc.dll, and MSI installation events with custom actions on user endpoints.

Detection Guidance: Confirm every managed Pixel is on patch level 2026-09-05 and restart every Chrome and Edge fleet to 153.0.8010.36 or later with the September Windows update applied. Block the C2 domain and alert on the extension ID, which will not appear in a legitimate Gemini deployment. The chain's target set is non-governmental organisations, aerospace and manufacturing; a South African organisation in those sectors with executives on Pixel handsets is inside it.

TH-2026-W39-08: Seasonal Lures: SARS eFiling, AARTO Fines and Black Friday Storefronts

P3 MEDIUM: 23 October filing deadline; cloned AARTO portals; identity numbers newly in circulation

Hypothesis: A phishing operator is using the tax deadline, a fake traffic fine or a cloned retailer to harvest eFiling, email or card credentials from South African staff and customers, and the identity numbers published or exposed this month make the lures personalised.

MITRE ATT&CK: T1566.001 (Spearphishing Attachment), T1566.002 (Spearphishing Link), T1598 (Phishing for Information), T1656 (Impersonation), T1583.001 (Acquire Infrastructure: Domains).

IOCs: Kaspersky via MyBroadband and IT-Online: a working replica of the SARS eFiling login page requesting username, password and phone number; an Adobe PDF sign-in lure for email credentials; attachment names in the pattern Tax Returns Of RXX,XXX.XXX and Final_Assessment_Notification-2026-0X-0X.pdf; email phrases Refund due and SARS Letter of demand. RTIA via MyBroadband: subject lines Final Notice: Action Required to Avoid Additional Penalties and Final Demand: Enforcement Notices; a R250 settlement lure; the only official site is online.aarto.gov.za and any .com, .co.za or .online AARTO domain is fraudulent. SARS: it never asks for passwords, OTPs or eFiling credentials by email, SMS or phone, and does not send .htm or .html attachments.

Data Sources: Mail gateway attachment and subject logs, web proxy logs for lookalike eFiling and AARTO domains, helpdesk reports, and card-fraud telemetry on the retail side.

Detection Guidance: Quarantine inbound mail carrying the two attachment-name patterns and the four subject lines, and block any AARTO-branded domain other than online.aarto.gov.za. Brief finance and payroll staff before the 23 October deadline that SARS communicates through eFiling and the MobiApp and never requests credentials. For customer-facing teams at the institutions in Section 3, expect callers who quote the customer's correct identity number and policy number and script the verification accordingly.

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

1. Work the two Cisco zero-days on Monday 21 September and treat the log checks as part of the patch.

The email gateway was due on 17 September and ISE on 19 September. Run `grep -i COPY.*TO PROGRAM` on every gateway cluster member and the dummyuser check on every ISE node before and after the update; a hit on either means rebuild or re-image; cleaning in place is not an option. Put infrastructure ACLs in front of the ISE management plane regardless, and use the new FMC fixed releases to retire the July hot fixes at the same time.

2. Revoke every integration credential a breached provider ever held. RelyComply asked its customers to rotate API tokens and refresh SSO federation; Artifactory customers were told the same in W38. Inventory the tokens, service accounts and federation trusts you have issued to every verification, administration and support provider, rotate the ones touched by an incident, and alert on use of the old ones, because the provider's rebuild does not invalidate what the attacker copied.

3. Scrub the tickets. Search every SaaS support and collaboration store for identity-number patterns, screenshots and report exports, and remove them; require single sign-on with multi-factor authentication and a managed-device condition on those platforms; and alert on sign-ins from personal devices and on bulk exports. MIP's 400,000 records were in tickets that were meant to be obfuscated.

4. Write the Gentlemen exfiltration detections while the tradecraft is fresh. Talos gives the sequence: CIFS mount of a backup share, VHDX opened with nbd and guestfs, ntfs.dit copied, rclone to Wasabi in 256 MiB chunks. Each step has a log source and none has a legitimate use on a production host outside a restore exercise. Add the AnyDesk-as-a-service and GPO-deployment rules from W38 if they are not already live.

5. Test a restore this month, and measure the time. The R50 million manufacturer had one clean backup and it was six months old; the Sophos survey puts South African one-week recovery at 40 per cent, the lowest measured. Restore a domain controller and a line-of-business server from immutable or offline media on Friday 25 September and record how long it took; that number is the recovery capability, whatever the backup job's status page says.

Management (CISO / Board)

1. Decide the ransom question before the call comes, and decide it knowing that MIP paid and was published anyway. MIP paid a substantial sum after anti-money laundering checks, received an undertaking to destroy the data, and watched the same data appear under Hollard's name three months later with a fresh demand to the insurer. A payment buys the attacker's word and nothing else. Record the board's position in writing, with the legal, sanctions and FIC considerations, and make sure your suppliers know what you expect of them.

2. Map the operators that hold identity numbers on your behalf and ask each one where. One policy-administration vendor held the customers of 45 insurers in support tickets; one compliance

platform held the FICA files of at least six institutions in one environment; a third provider's credentials exposed Cell C Fibre's customer list. The Prudential Authority has already asked whether one unregulated supplier serving a sector is a systemic risk. Ask the same question of your own supplier list, and price concentration accordingly.

3. Own the notification, whoever was breached. POPIA puts the section 22 duty on the responsible party, and this week's insurers and brokers performed it for breaches in someone else's estate, with the Cybercrimes Act's 72-hour Police report and the FSCA's 24-hour clock running alongside. Put the three clocks, the trigger for each and the person who starts them in one page of the incident plan, and rehearse the supplier-breach scenario rather than the ransomware one.

4. Treat published identity numbers as a permanent condition for your customers. The Hollard set carries children's identity numbers; the RelyComply set carries the full FICA file. Neither can be reissued. Fund the customer-side response: a standing SAFPS protective-registration offer, call-centre scripts that assume the caller knows the customer's identity number, and onboarding controls that do not treat a correct identity number as proof of anything.

5. Read the one improving number in context. Sophos records South African ransom demands down 57 per cent and payment rates down from 71 to 58 per cent, and those are real. The same survey records 47 per cent of respondents citing inadequate protection, the highest of any country, and the slowest recovery measured. A falling demand leaves the loss where it was, as the unnamed manufacturer's R50 million shows.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH, 22nd CONSECUTIVE WEEK

The South African cyber threat level remains HIGH for a twenty-second consecutive week (13 September to 19 September 2026). Escalation to CRITICAL was considered on the breadth of the supplier breaches, roughly 45 insurers through MIP and at least six financial institutions through RelyComply, with one data set published and a second on a countdown, and rejected on the criterion applied since W35: no systemically important institution went out of service and no national-scale outage occurred, and both incidents are data exposures at operators rather than compromises of the institutions' own estates. De-escalation to MEDIUM was rejected on two Cisco zero-days on the network edge with confirmed exploitation, seven catalogue additions of which four were overdue at publication, and a South African month in which nine organisations confirmed exposure.

Rationale

The supplier breaches now have names, numbers and a published data set. MIP Holdings, 400,000 records, 45 insurers, paid and published; RelyComply, the FICA files of at least five confirmed institutions, a countdown to about 23 September; Cell C Fibre's provider, a credential. Nine South African organisations confirmed exposure in one window, and none of them was breached in its own estate.

Two Cisco zero-days with confirmed exploitation landed on the network edge in one week. A 9.8 in the email gateway reachable by a crafted message and a 10.0 in the network access control plane, both found through support cases, both with vendor log checks. They join NetScaler, FMC, FortiOS and MikroTik, all still overdue, on an edge whose South African populations are measured in thousands.

The aggregator's country tag hid a South African victim for the first time. RelyComply was listed on 9 September under a GB tag, was invisible to every ZA-scoped method this report uses, and was found because its customers named it. The W38 count is corrected, and this week's zero ZA-tagged listings is carried as the tag's zero.

The one improving number is real and does not offset the rest. Sophos records South African ransom demands down 57 per cent and payment rates falling, alongside the lowest one-week recovery rate of any country surveyed and 47 per cent of respondents citing inadequate protection; the unnamed manufacturer's R50 million loss is the same survey from the inside.

Next-Week Watch (W40)

The RelyComply countdown, on or about 23 September. The distinguishing observations are DireWolf publishing the set, which would let the data classes be verified against the customers' notices, or silence past the date, which with this group has meant a delay rather than a withdrawal. A published set that contains bank account details would move Peregrine's and Cartrack's data-class statements from the provider's word to observation.

The regulators' answers to TechCentral, promised for Monday 21 September. Two observations matter: whether the Information Regulator states how many section 22 notifications the MIP incident produced, which would show whether all 45 insurers notified, and whether the Prudential Authority confirms the systemic-risk assessment MIP describes. A statement of either kind would be the Regulator's first substantive publication in fifteen weeks; silence extends the count to sixteen.

Whether The Gentlemen extorts the other MIP clients. The test is a second insurer from the MIP set appearing on the leak site or issuing a statement about a demand. One would confirm the downstream-extortion model this edition describes; none by 3 October would suggest Hollard was chosen for its name and the rest of the set is being held.

Bidvest Bank and its provider. Every other institution in the RelyComply set has named it. Bidvest naming RelyComply would complete the set; naming a different provider would mean a fourth supplier breach in a fortnight, which is the more important observation and the reason the item stays open rather than being inferred.

Whether the Cisco zero-days reach South African victims. Both flaws have confirmed exploitation abroad and no South African exposure figure, because Shodan has no product label for either appliance. The observation to watch is a South African leak-site listing or incident naming an email gateway or network access control compromise as the entry point, and the collector task is a hand-built fingerprint for both products so the panel can measure them.

The Linux kernel trio. No exploitation detail exists for any of the three. The distinguishing observation is a vendor or responder publication naming the exploiting activity; if none appears by the catalogue's next kernel addition, the entries stay in the table as patch items without a hunt.

Rand Water, with no development in three weeks. The three W37 tests remain: a named actor or family, a statement about personal information, or a return from the Centurion disaster recovery site. Silence

past 3 October, a month from the SENS statement, becomes the finding.

Closed this week. Hollard, resolved as a supplier's data published; the EasyEquities half of the shared-provider question, resolved as RelyComply, with the Bidvest half kept open above; the LiteLLM and ScreenConnect figures, resolved as artefacts on a third collection; the Black Axe handover, confirmed. Carryovers held without re-argument: VSB Attorneys, Rohloff, The Courier Guy, Babcock, the Furniture Bargaining Council exfiltration 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 20 September 2026, with the exceptions this note records: the CISA catalogue URL is the public location of a file read locally, the Acronis advisory was read through a browser, and the Fortinet and Microsoft pages named below could not be read.

Collection notes. The feed run completed at 02:05 UTC on 20 September 2026 and passed its integrity check with a clean exit. The victim feed returned 128 records, all tagged ZA; the run log records filter purity 1.0 and the written file records 128 South African records against 128 returned. The catalogue file is catalogVersion 2026.09.18, released on Friday 18 September, so any Saturday addition falls to the next edition. The RSS sweep read 58 of 72 feeds; Daily Maverick, IOL, Engineering News, ITWeb's two feeds and News24 failed at the source and were checked by hand where cited. **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 one rendered ransomware.live page used, the South African country page, is cited as a cross-check only. **A correction.** This edition corrects the W38 derived South African listing count for 6 to 12 September from two to three: RelyComply AML Platform was listed by DireWolf on 9 September under a GB country tag and was outside the ZA-scoped feed. The correction is recorded in Section 1 and applied in Section 6; the W38 feed total of 128 stands as the aggregator's figure. The two searchvictims records relied on are stored under evidence/ with this edition.

Two figures resolved as artefacts. The Shodan collection returned 6,410 LiteLLM and 2,942 ScreenConnect instances in South Africa; a third collection confirms port scatter and both are omitted, as Section 7.2 sets out. None of the seven catalogue additions has a published South African figure: no product label exists for Cisco Secure Email Gateway, Cisco ISE or the Linux kernel, and the Pixel and Acronis Backup queries returned zero and are held. **Environment limitations.** cisa.gov returns an empty body here, so every catalogue date and due date comes from the locally retrieved file. The Acronis advisory and the Sophos survey figures were read through a browser and through named secondary reporting; Fortinet's PSIRT page sat behind a bot check and could not be re-read, so the W38 finding about its Known Exploited field is neither confirmed nor withdrawn; Microsoft's update guide entry for CVE-2026-69724 rendered as an empty shell and is not used. **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 MIP account rests on TechCentral's interview with its CEO and is corroborated only by Hollard's and MyBroadband's references to the June incident; the Cell C Fibre, iOCO, AARTO, smart ID and ACSA items each rest on MyBroadband; the Sophos figures on IT-Online with ITWeb as a second account; the cross-border legal analysis on Werksmans; the BEC liability material on Moonstone. **Claims deliberately excluded.** The Gentlemen's assertion that it breached Hollard's own systems is contradicted by the insurer and is not carried as fact. DireWolf's 200 GB and 3.57 billion rows and Cartrack's 500 GB are attacker figures and are not adopted. Bidvest Bank is not linked to RelyComply

on any statement of its own. MIP's ransom amount is undisclosed and no figure is implied. The ShinyHunters claims against Clop beyond the confirmed defacement are not carried. No actor or family is attributed to Rand Water.

1. TechCentral, Customers of 45 insurers exposed in South African cyber breach (15 September 2026, updated 16 September). <https://techcentral.co.za/customers-45-insurers-exposed-cyber-breach/286139/>
2. TechCentral, Hollard client data dumped on the dark web (18 September 2026). <https://techcentral.co.za/hackers-extort-insurers-mip-ransom-hollard/286251/>
3. MyBroadband, Hollard customer data leaked on the dark web (19 September 2026). <https://mybroadband.co.za/news/security/668276-hollard-customer-data-leaked-on-the-dark-web.html>
4. Hollard, Hollard statement regarding reported cyber threat claims, media centre (published 16 September 2026). <https://www.hollard.co.za/media-centre/press-releases/hollard-statement-regarding-reported-cyber-threat-claims>
5. RelyComply, RelyComply cyber incident: what happened and what you can do, official notice (published 16 September 2026, updated 17 September 2026). <https://relycomply.com/relycomply-cyber-incident-what-happened-and-what-you-can-do/>
6. ransomware.live API, victim record via GET /v2/searchvictims/relycomply: RelyComply AML Platform, DireWolf, discovered 9 September 2026 13:28 UTC, country field GB, retrieved 20 September 2026 and stored as evidence/w39_ransomwarelive_searchvictims_relycomply_2026-09-20.json (public page: <https://api.ransomware.live/v2/searchvictims/relycomply>)
7. MyBroadband, EasyEquities data at third-party hacked and customer information compromised (16 September 2026). <https://mybroadband.co.za/news/security/667868-easyequities-data-at-third-party-hacked-and-customer-information-compromised.html>
8. MyBroadband, South African home loans giant affected by data breach, customer records potentially exposed (17 September 2026). <https://mybroadband.co.za/news/security/667893-south-african-home-loans-giant-affected-by-data-breach-customer-records-potentially-exposed.html>
9. Moneyweb, EasyEquities, Satrix hit by data breach (14 September 2026). <https://www.moneyweb.co.za/news/companies-and-deals/easyequities-satrix-hit-by-data-breach/>
10. ITWeb, Third-party cyber breaches rock SA firms (17 September 2026). <https://www.itweb.co.za/article/third-party-cyber-breaches-rock-sa-firms/KWEBb7yLeINvmRjO>
11. MyBroadband, Standard Bank investigates 200GB data breach (18 September 2026). <https://mybroadband.co.za/news/security/668048-standard-bank-investigates-200gb-data-breach.html>
12. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.09.18, released 18 September 2026, retrieved 20 September 2026. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
13. Cisco, Security advisory cisco-sa-esa-inj-2bLVGmhX, Cisco Secure Email Gateway SQL injection vulnerability, version 1.1 (published 14 September 2026, updated 17 September 2026). <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX>
14. Cisco, Security advisory cisco-sa-ISE-ABP-VNSW7Tn5, Cisco Identity Services Engine authentication bypass vulnerability, version 1.0 (16 September 2026). <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>
15. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:01 UTC 20 September 2026. <https://www.shodan.io/search?query=country%3AZA>
16. RelyComply, Contact us page listing Johannesburg (Sandton), Cape Town (Newlands) and London offices, checked 20 September 2026. <https://relycomply.com/contact-us/>
17. MyBroadband, Cell C warns fibre customers about possible data breach (13 September 2026). <https://mybroadband.co.za/news/security/667360-cell-c-warns-fibre-customers-about-possible-data-breach.html>
18. The Hacker News, Cisco Secure Email Gateway flaw exploited in the wild, enables root command execution, including Arctic Wolf's Fortinet VPN credential-attack findings (15 September 2026). <https://thehackernews.com/2026/09/cisco-secure-email-gateway-flaw.html>
19. MyBroadband, Cartrack warning after hackers access sensitive data (14 September 2026). <https://mybroadband.co.za/news/security/667519-cartrack-warning-after-hackers-access-sensitive-data.html>
20. MyBroadband, Capitec warns of fake Takealot and Game websites on Black Friday (16 September 2026). <https://mybroadband.co.za/news/banking/667781-capitec-warns-of-fake-takealot-and-game-websites-on-black-friday.html>
21. MyBroadband, Hyper-realistic SARS eFiling scams hit South Africa (19 September 2026). <https://mybroadband.co.za/news/security/667861-hyper-realistic-sars-efiling-scams-hit-south-africa.html>
22. RelyComply, home page carrying client testimonials from Standard Bank and SnapScan, checked 20 September 2026. <https://relycomply.com/>
23. MyBroadband, Why EasyEquities, Cell C and a bank announced potential data breaches on the same weekend in South Africa (13 September 2026). <https://mybroadband.co.za/news/security/667365-why-easyequities-cell-c-and-a-bank-announced-potential-data-breaches-on-the-same-weekend-in-south-africa.html>
24. TimesLIVE, Cyberattacks put South Africans' personal data in the spotlight (15 September 2026). <https://www.timeslive.co.za/news/sci-tech/2026-09-15-cyberattacks-put-south-africans-personal-data-in-the-spotlight/>
25. MyBroadband, South African company which generated R4 million per month lost R50 million after a cyberattack (17 September 2026). <https://mybroadband.co.za/news/security/667352-south-african-company-which-generated-r4-million-per-month-lost-r50-million-after-a-cyberattack.html>
26. IT-Online, Defences improve, but ransomware still threatens SA businesses, reporting the Sophos State of Ransomware in South Africa 2026 survey (18 September 2026). <https://it-online.co.za/2026/09/18/defences-improve-but-ransomware-still-threatens-sa-businesses/>
27. ITWeb, Hackers breach Rand Water's defences (4 September 2026), the most recent Rand Water item located; nothing dated 13 to 19 September 2026 was found. <https://www.itweb.co.za/article/hackers-breach-rand-waters-defences/Gb3BwMWaO4ov2k6V>
28. Parliamentary Monitoring Group, committee meetings index, listing for 15 to 19 September 2026, checked 20 September 2026. <https://pmg.org.za/committee-meetings/?page=1>
29. MyBroadband, Nigerian crimelords operating in South Africa busted after 10 years and R100 million (16 September 2026). <https://mybroadband.co.za/news/security/667816-nigerian-crimelords-operating-in-south-africa-busted-after-10-years-and-r100-million.html>
30. ransomware.live API PRO, group index GET /groups, 400 groups, retrieved 13 and 20 September 2026 (public pages: <https://api-pro.ransomware.live/groups>)
31. Infosecurity Magazine, Manufacturing accounts for 22% of all ransomware victims, reporting Black Kite (18 September 2026). <https://www.infosecurity-magazine.com/news/manufacturing-22-ransomware-victims/>
32. Cisco Talos, Ransomware incidents in Japan in the first half of 2026: investigation of The Gentlemen's infrastructure and evidence of Qilin's AI use (17 September 2026). <https://blog.talosintelligence.com/ransomware-incidents-in-japan-in-the-first-half-of-2026/>

33. ransomware.live API PRO, per-group endpoints GET /iocs/{group}, /yara/{group} and /ransomnotes/{group}, retrieved 20 September 2026 (key required; the public group pages carry the same sets). <https://api-pro.ransomware.live/iocs/thegentlemen>
34. BleepingComputer, ShinyHunters hacks Clop leak site, threatens to extort ransomware gang (19 September 2026). <https://www.bleepingcomputer.com/news/security/shinyhunters-hacks-clop-leak-site-threatens-to-extort-ransomware-gang/>
35. NVD API, CVSS base scores with scoring source, GET /rest/json/cves/2.0?cveId=, 55 CVEs resolved, retrieved 20 September 2026. <https://services.nvd.nist.gov/rest/json/cves/2.0>
36. Rapid7, CVE-2026-76461: Critical Cisco Secure Email Gateway vulnerability exploited in the wild (15 September 2026). <https://www.rapid7.com/blog/post/etr-cve-2026-76461-critical-cisco-secure-email-gateway-vulnerability-exploited-in-the-wild>
37. The Hacker News, Cisco warns of new zero-day ISE auth bypass (CVSS 10.0) exploited in active attacks (17 September 2026). <https://thehackernews.com/2026/09/cisco-warns-of-new-zero-day-ise-auth.html>
38. SOCRadar, CVE-2026-76460: Cisco ISE flaw actively exploited (17 September 2026). <https://socradar.io/blog/cve-2026-76460-cisco-ise-flaw/>
39. Cisco, Security advisory cisco-sa-fmc-static-cred-BET3Cjh, Secure Firewall Management Center static credential vulnerability, version 1.6 (updated 16 September 2026). <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh>
40. Google, Pixel Update Bulletin September 2026 (published 15 September 2026). <https://source.android.com/docs/security/bulletin/pixel/2026/2026-09-01>
41. The Hacker News, Google patches Pixel modem flaw amid signs of limited targeted exploitation (16 September 2026). <https://thehackernews.com/2026/09/google-patches-pixel-modem-flaw-amid.html>
42. Acronis, Security advisory SEC-10986, local privilege escalation due to insecure file permissions, CVE-2026-87886 (read through a browser, 20 September 2026). <https://security-advisory.acronis.com/advisories/SEC-10986>
43. Help Net Security, Acronis Backup plugin vulnerability exploited in the wild (CVE-2026-87886) (16 September 2026). <https://www.helpnetsecurity.com/2026/09/16/acronis-backup-plugin-vulnerability-exploited-cve-2026-87886/>
44. The Hacker News, CISA flags three Linux kernel vulnerabilities exploited in the wild (19 September 2026). <https://thehackernews.com/2026/09/cisa-flags-three-linux-kernel.html>
45. The Hacker News, Public exploits released for four Linux kernel flaws that enable local root (18 September 2026). <https://thehackernews.com/2026/09/public-exploits-released-for-four-linux.html>
46. Citrix, NetScaler ADC and NetScaler Gateway security bulletin for CVE-2026-19489 and CVE-2026-19490, CTX696939, change log still showing only the 19 August 2026 initial publication when checked 20 September 2026. <https://support.citrix.com/external/article/CTX696939/netscaler-adc-and-netscaler-gateway-secu.html>
47. Horizon3.ai, CVE-2026-86218: N-able N-central pre-authentication remote code execution vulnerability (16 September 2026). <https://horizon3.ai/attack-research/vulnerabilities/cve-2026-86218/>
48. The Hacker News, China-linked hackers exploit Chrome-Windows zero-day chain to deploy GRIMWEDGE, reporting Volexity (15 September 2026). <https://thehackernews.com/2026/09/china-linked-hackers-exploit-chrome.html>
49. FIRST EPSS API, GET /data/v1/epss?cve=, 55 CVEs scored, retrieved 20 September 2026. <https://api.first.org/data/v1/epss>
50. ransomware.live API, SA victim records, GET /v2/countryvictims/ZA, 128 records all tagged ZA, retrieved 02:00 UTC 20 September 2026. <https://api.ransomware.live/v2/countryvictims/ZA>
51. ransomware.live, country page for South Africa, showing 128 victims with capricornlogistics.com as the newest, checked 20 September 2026. <https://www.ransomware.live/country/ZA>
52. ransomware.live API, GET /v2/recentvictims, the 100 most recent listings worldwide (16 to 18 September 2026), none tagged ZA, retrieved 20 September 2026. <https://api.ransomware.live/v2/recentvictims>
53. ITWeb, SA organisations under pressure to protect against ransomware onslaught (18 September 2026). <https://www.itweb.co.za/article/sa-organisations-under-pressure-to-protect-against-ransomware-onslaught/Pero37Z36dyMQb6m>
54. ransomware.live API, victim record via GET /v2/searchvictims/hollard: Hollard Insurance Group, The Gentlemen, discovered 7 September 2026 21:56 UTC, retrieved 20 September 2026 and stored as evidence/w39_ransomwarelive_searchvictims_hollard_2026-09-20.json (public page: <https://api.ransomware.live/v2/searchvictims/hollard>)
55. Information Regulator of South Africa, enforcement notices register; the 2026 tab carries three instruments dated 20 May, 2 June and 10 June 2026 and nothing later, checked 20 September 2026. <https://infoforegulator.org.za/enforcement-notice/>
56. Information Regulator of South Africa, media statements index, most recent entry the media invitation of 27 August 2026, checked 20 September 2026. <https://infoforegulator.org.za/media-statements/>
57. Werksmans Attorneys, Cybercrime across borders: navigating Africa's fragmented legislative landscape, Part 1 (17 September 2026). <https://werksmans.com/cybercrime-across-borders-navigating-africas-fragmented-legislative-landscape-part-1/>
58. Werksmans Attorneys, Cybercrime across borders: navigating Africa's fragmented legislative landscape, Part 2 (17 September 2026). <https://werksmans.com/cybercrime-across-borders-navigating-africas-fragmented-legislative-landscape-part-2/>
59. IT-Online, Tax deadline rush gives scammers an opening (18 September 2026). <https://it-online.co.za/2026/09/18/tax-deadline-rush-gives-scammers-an-opening/>
60. SARS, Scams and phishing index, most recent entry SARS-SCAM-400 (2 September 2026), checked 20 September 2026. <https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>
61. MyBroadband, AARTO scam targets South African motorists with fake fines and threatens to block licences (16 September 2026). <https://mybroadband.co.za/news/motoring/667800-aarto-scam-targets-south-african-motorists-with-fake-fines-and-threatens-to-block-licences.html>
62. MyBroadband, South Africa's fraud-resistant smart IDs are being forged (15 September 2026). <https://mybroadband.co.za/news/government/667581-south-africas-fraud-resistant-smart-ids-are-being-forged.html>
63. Moonstone, Your client's email is hacked. You make the payment. Who pays? (17 September 2026). <https://www.moonstone.co.za/your-clients-email-is-hacked-you-make-the-payment-who-pays/>
64. MyBroadband, Biggest airports in South Africa highly likely to be hacked with significant consequences (15 September 2026). <https://mybroadband.co.za/news/security/667686-biggest-airports-in-south-africa-highly-likely-to-be-hacked-with-significant-consequences.html>
65. IT-Online, There are remedies for .za domain name fraud, reporting ISPA (18 September 2026). <https://it-online.co.za/2026/09/18/there-are-remedies-for-za-domain-name-fraud/>
66. FIRST member teams. SA CSIRT records retrieved via the ransomware.live /csirt/ZA endpoint, 20 September 2026, six teams. <https://www.first.org/members/teams/>

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.