



# **SOUTH AFRICA**

# **CYBER THREAT INTELLIGENCE REPORT**

Weekly OSINT Brief, Week 41 | 27 September – 3 October 2026

**THREAT LEVEL: HIGH**

**TLP: CLEAR**

Report ID: SA-CTI-2026-W41 | Classification: TLP: CLEAR

**Published Monday 5 October 2026**

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

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

# TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard
- 2. Threat Landscape Heatmap
- 3. Top SA Incidents (W41)
- 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, 24th consecutive week (27 September – 3 October 2026)

**Story 1.** The state-owned air navigation operator found ransomware-linked malware in an airport operational technology network and disclosed it through a procurement document. Air Traffic and Navigation Services issued a request for quotation on 18 September for forensic investigators, stating that preliminary investigation had identified malware commonly associated with the early stages of ransomware attacks in the operational technology environment supporting weather services at Chief Dawid Stuurman International Airport in Gqeberha, that network monitoring indicated possible data exfiltration to external addresses located in China, and that internal teams had contained and removed it; a second workstream covers alleged insider access to personal information. ATNS's spokesperson told the Sunday Times it cannot comment on compromised data until the forensic work is done.<sup>1,2,3</sup> No actor is named; the China reference is a destination for traffic. Rated CONFIRMED on the spokesperson's statement and on the RFQ as read by three publications. The item fell inside the W40 window and W40 did not capture it; the correction below records that. First reported by [Sunday Times](#) on 26 September 2026.

**Story 2.** INC Ransom listed BCX four days after Telkom disclosed an incident in a BCX legacy testing environment, and The Gentlemen's insurer thread resolved and widened in the same week. The BCX listing was indexed at 12:32 UTC on 29 September and claims 500 GB in 4,224,088 files, described by the actor as source code and technical documentation for six business applications and more than fifteen integration libraries; neither Telkom nor BCX had responded to the listing by the close of the window and the claim is CLAIMED, with the W40 incident it appears to follow still CONFIRMED at the company's scope.<sup>4,5,6</sup> Guardrisk answered the W40 question on 28 and 30 September: by its account the data on The Gentlemen's site appears to be linked to the June MIP incident through a binder holder, CoverCubed, covering about 6,000 funeral policies, and not to any compromise of Guardrisk's own systems; CoverCubed, Guardrisk says, has notified the Information Regulator and its clients.<sup>7,8</sup> The group then listed LegalWise, the legal-expenses insurer, and Edcon, the retail group in business rescue since 2020, both indexed at 03:40 UTC on 30 September and both CLAIMED.<sup>9,10</sup>

**Story 3.** Citrix disclosed two NetScaler zero-days on Sunday 27 September that were already being exploited, one of them a pre-authentication command injection in the default configuration, and the catalogue took seven entries in the window against ten the week before.<sup>11</sup> Mandiant and Google describe a campaign running since at least early September that leaves a PHP web shell and a Python tunneller on the appliance and sets the SUID bit on /bin/sh, against government, financial, technology, education and legal targets in North America and Europe; Rapid7 saw the first attempt on 20 September and two compromises in which the attacker archived the configuration directory that holds the certificates and private keys.<sup>12,13,14</sup> South Africa exposes 122 NetScaler instances, and the responders' advice is to examine the appliance before patching it.<sup>15</sup> Cisco's SD-WAN Manager, Fortinet's FortiMail, Apple's CoreGraphics and a Zammad helpdesk pair used against a Dutch vulnerability-disclosure institute make up the rest; five of the seven were past their remediation date on Monday 5 October.<sup>16,17,18,19</sup>

W41 CORRECTION TO W40: the W40 edition, covering 20 to 26 September, did not carry the ATNS incident. The Sunday Times published it on Saturday 26 September, the last day of that window, with the operator's spokesperson on record, and the request for quotation that discloses it is dated 18 September.<sup>1</sup> W40's KPI row counted one South African organisation confirming a breach in its window, Telkom; it should have counted two, and the Government and Transport rows of the W40 heatmap were scored without it. The item is written up in Section 3.1 of this edition, the corrections KPI row records it, and the W40 threat-level reasoning, which turned on no systemically important institution going out of service, is unchanged by it because ATNS reports containment and no service disruption.

KPI Dashboard

| Metric                                                                  | Current (W41) | Prior (W40)          | Change                | Direction |
|-------------------------------------------------------------------------|---------------|----------------------|-----------------------|-----------|
| Overall SA threat level                                                 | HIGH          | HIGH                 | No change (24th week) | FLAT      |
| ransomware.live SA cumulative                                           | 135           | 132                  | +3                    | UP        |
| SA claims discovered inside the window (ZA tag)                         | 3             | 4                    | -1                    | DOWN      |
| Window claims surviving the nationality check                           | 3 of 3        | 3 of 4               | n/a                   | n/a       |
| SA organisations confirming a breach or supplier exposure in the window | 1             | 2 (corrected from 1) | -1                    | DOWN      |
| New CISA KEV additions                                                  | 7             | 10                   | -3                    | DOWN      |
| KEV adds already overdue at publication                                 | 5             | 7                    | -2                    | DOWN      |
| KEV adds with a published VERIFIED SA exposure figure                   | 2 of 7        | 3 of 10              | -1                    | DOWN      |
| Corrections issued to prior editions                                    | 1             | 1                    | 0                     | FLAT      |

Three notes on the table. The three claims are the feed's ZA-tagged listings discovered between 27 September and 3 October: bcx.co.za, Edcon and LegalWise, each South African on its own domain, so all three survive the nationality check.<sup>20</sup> The confirmations row counts one organisation, Guardrisk, whose statements of 28 and 30 September deny a compromise of its own systems and report that policy data held by its binder holder appears to sit in the MIP breach; ATNS's disclosure is dated to the W40 window and is counted there by correction, on the rule W40 applied to the Bidvest notice, and CoverCubed's notification is reported by Guardrisk rather than published by CoverCubed and is not counted separately.<sup>7,8</sup> The Information Regulator row is retired, as W40 said it would be unless the register moved: the register's newest entry is still 10 June and the media-statements page's newest item 2 June, which on Monday 5 October is seventeen weeks, and the figure returns to the table only if an instrument is published.<sup>21,22</sup>

**W41 KEY FRAMING:** two South African organisations that run other organisations' systems were the week's victims, and in both cases the public learned of it from a document that was not written as a disclosure. ATNS told the market through a tender; BCX's customers learned the actor's version from a leak site four days after Telkom's statement placed the incident in a test environment. The MIP data

reached a second insurer this week through a binder holder, which means an insurer can be on a leak site for data it never held. For a board the three cases ask the same question in different words: for each supplier that builds, hosts or administers on your behalf, does the contract say who tells you, within what time, and in what form, when their environment is breached. On the technical side, the NetScaler pair gives pre-authentication remote code execution on a default configuration, 122 instances are exposed in South Africa, and the responder guidance is to look for the web shell before the patch removes the evidence of it.

## TOP 3 ACTIONS THIS WEEK

**1. On Monday 5 October, examine every NetScaler ADC and Gateway for compromise before you upgrade it, then rotate what the appliance held.** Mandiant's order is check first, patch second, because the exploit leaves evidence the upgrade may remove; TH-2026-W41-01 lists the five checks, which take minutes on each appliance. Then upgrade to 14.1-73.37 or 13.1-64.23. Because Rapid7 watched an attacker archive the configuration directory, which holds the administrator and directory bind credentials, the TLS private keys and the SSH host keys, rotate all of them on every appliance that was internet-facing while unpatched, whether or not the checks found anything, and have the owner of the appliance list report by Friday 9 October which appliances were examined before they were patched.

**2. If BCX, or any provider, builds or hosts applications for you, ask on Monday 5 October whether your source code, integration libraries or embedded credentials sat in the environment, and treat the answer as a secrets-rotation list.** The actor's listing names application and connector libraries and says vulnerabilities were found in them; whether that is true is unknown, and what you can control is whether any database connection string, API key or service account in that code still works. The same question goes to every binder holder and underwriting manager an insurer uses: CoverCubed's data, by Guardrisk's account, reached The Gentlemen through MIP, and Guardrisk was named on a leak site before any notice reached it. Put the question in writing by Friday 9 October and keep the replies.

**3. Run the two vendor log checks for the week's other edge entries on Monday 5 October, and push the Apple builds.** On Catalyst SD-WAN Manager, grep `/var/log/nms/containers/service-proxy/serviceproxy-access.log` and `/var/log/nms/vmanage-server.log` for POST requests to `j_security_check` that carry percent-encoded characters such as `%6a`, from any address you do not recognise, then move to 20.9.10.1, 20.12.8.2, 20.15.6.1, 20.18.4.1, 26.1.2.1 or 26.2.1. On FortiMail, search for archive-account configuration changes from 79.141.169.187 and any POST carrying `./` to an `/ibe` path, disable IBE if you do not use it, and move to 8.0.2, 7.6.7 or 7.4.9. On the fleet, push iOS 26.7.1, iPadOS 26.7.1, macOS 26.7.1 or 15.8.1 through MDM and report compliance by Friday 9 October.

1. Sunday Times (TimesLIVE), Air traffic agency probes cyberattack, by Kabelo Khumalo (26 September 2026; premium article, the opening text and the ATNS spokesperson's statement were readable to this collection).

<https://www.sundaytimes.timeslive.co.za/business/news/2026-09-26-air-traffic-agency-probes-cyberattack/>

2. MyBroadband, China-linked hackers attacked South Africa's air traffic control system, by Luis Monzon (2 October 2026).

<https://mybroadband.co.za/news/security/670359-china-linked-hackers-attacked-south-africas-air-traffic-control-system.html>

3. Dark Reading, South Africa seeks help after cyberattack targets air traffic control, by Robert Lemos (30 September 2026).

<https://www.darkreading.com/cyberattacks-data-breaches/south-africa-help-cyberattack-air-traffic-control>

4. ransomware.live, victim page for bcx.co.za (INC Ransom), discovered 29 September 2026 12:32 UTC, post dated 29 September 2026, 500 GB claimed, retrieved 4 October 2026; the same record is in the locally retrieved country feed; the infostealer panel figures of the three victim pages are stored as evidence/w41\_ransomwarelive\_victim\_panels\_2026-10-04.md.

<https://ransomware.live/id/YmN4LmNvLnphQGluY3JhbnNvbQ==>

5. MyBroadband, Telkom discloses BCX cybersecurity incident which was limited to legacy testing environment (25 September 2026). <https://mybroadband.co.za/news/security/669235-telkom-discloses-bcx-cybersecurity-incident-which-was-limited-to-legacy-testing-envi>

ronment.html

6. BCX, corporate website, checked 4 October 2026 (no notice, banner or statement on any incident; the /news/ path returns 404).  
<https://www.bcx.co.za/>

7. ITWeb, Guardrisk distances itself from MIP cyber breach, by Admire Moyo (28 September 2026).  
<https://www.itweb.co.za/article/guardrisk-distances-itself-from-mip-cyber-breach/DZQ58MV8B1pvzXy2>

8. MyBroadband, Momentum Group company responds to data breach claims, by Luis Monzon (30 September 2026).  
<https://mybroadband.co.za/news/security/669576-momentum-group-company-responds-to-data-breach-claims.html>

9. ransomware.live, victim page for LegalWise (The Gentlemen), discovered 30 September 2026 03:40 UTC, estimated attack date 29 September 2026, retrieved 4 October 2026. <https://ransomware.live/id/TGVnYWwXaXNIQHROZWdlbnRsZWl1bg==>

10. ransomware.live, victim page for Edcon (The Gentlemen), discovered 30 September 2026 03:40 UTC, estimated attack date 29 September 2026, retrieved 4 October 2026. <https://ransomware.live/id/RWRjb25AdGhlZ2VudGxlbWVu>

11. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.10.02, released 2 October 2026 15:19 UTC, retrieved 4 October 2026 (feeds/kev\_2026-10-04.json). <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

12. Google Threat Intelligence Group and Mandiant, Defending against active exploitation of Citrix NetScaler ADC and Gateway appliances (29 September 2026). <https://cloud.google.com/blog/topics/threat-intelligence/defending-against-active-exploitation-of-citrix-netscaler-adc-and-gateway-appliances/>

13. Rapid7, Zero-day exploitation of Citrix NetScaler ADC and Gateway: CVE-2026-88771 and CVE-2026-88772 (28 September 2026, updated 30 September 2026). <https://www.rapid7.com/blog/post/etr-zero-day-exploitation-of-citrix-netscaler-adc-and-gateway-cve-2026-88771-and-cve-2026-88772>

14. The Register, Custom malware used in Citrix 0-day attacks targeting govt, banks, professional services, by Jessica Lyons (29 September 2026). <https://www.theregister.com/security/2026/09/29/custom-malware-used-in-citrix-0-day-attacks-targeting-govt-banks-professional-services/5299867>

15. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:01 UTC 4 October 2026 (feeds/shodan\_za\_2026-10-04.json).  
<https://www.shodan.io/search?query=country%3AZA>

16. Cisco, Security advisory cisco-sa-sdwan-webauth-xr8beuuU, Cisco Catalyst SD-WAN Manager API authentication bypass vulnerability, CVE-2026-76504 (published 30 September 2026, updated 2 October 2026).  
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU>

17. Fortinet PSIRT, FG-IR-26-175, FortiMail path traversal and null-byte handling, CVE-2026-104286 (published 1 October 2026).  
<https://fortiguard.fortinet.com/psirt/FG-IR-26-175>

18. The Hacker News, Apple patches CoreGraphics flaw possibly exploited in targeted attacks, CVE-2026-86950 (28 September 2026).  
<https://thehackernews.com/2026/09/apple-patches-coregraphics-flaw.html>

19. Infosecurity Magazine, Two zero-days exploited in attack on Dutch Institute for Vulnerability Disclosure (2 October 2026).  
<https://www.infosecurity-magazine.com/news/zerodays-dutch-institute/>

20. ransomware.live API, GET /v2/countryvictims/ZA, 135 records, za\_records 135 against server\_returned 135, filter purity 1.0, FREE v2 tier (delayed relative to PRO), retrieved 02:00 UTC 4 October 2026 and stored as feeds/ransomwarelive\_za\_2026-10-04.json.  
<https://api.ransomware.live/v2/countryvictims/ZA>

21. Information Regulator, Enforcement notices register, checked 4 October 2026 (newest entry Gauteng Department of Health, 10 June 2026). <https://infoeregulator.org.za/enforcement-notice/>

22. Information Regulator, Media statements page, checked 4 October 2026 (2026 tab rendered; newest statement 2 June 2026; the media invitation of 27 August 2026 recorded in W39 is an invitation and did not render on this read).  
<https://infoeregulator.org.za/media-statements/>

## 2. THREAT LANDSCAPE HEATMAP

South African Sector Threat Levels, Week 41 (27 September – 3 October 2026)



**Methodology:** each cell is an analyst score from 0 to 10 for the coming week, set from what this edition observed: leak-site listings with a South African tag 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. A sector with no observation this week carries its prior score rather than dropping to zero, and a ceiling score of 10 is held.

**No row added or retired.** The eight rows stand. ATNS is scored under Transport, Logistics and Fleet because the compromised environment is airport operational technology, and it is noted under Government because ATNS is a state-owned company; the observation is counted once. LegalWise is an insurer and is scored under Financial Services; Edcon's listing is scored under Retail in the narrative only, because what estate a group in business rescue still operates is not known.<sup>23</sup>

**Movements.** Outsourced Verification, Administration and IT Providers rises from 8 to 9 on ransomware and from 9 to 10 on data extortion: a 500 GB claim against the IT services subsidiary of Telkom, posted on the actor's disclosures page, moves the row whatever its truth.<sup>4</sup> Transport, Logistics and Fleet rises from 8 to 9 on ransomware on ATNS's own statement that ransomware-linked malware sat in an airport operational technology network.<sup>1</sup> Financial Services and Credit rises from 9 to 10 on data extortion: the MIP data has now produced leak-site listings or published data for Hollard, Guardrisk's binder holder and, if the group's listing is what it appears to be, a legal-expenses insurer, and the group's affiliates are evidently working the sector.<sup>8,9</sup> Network Edge and Remote Access holds at 10 on vulnerability exploitation with the NetScaler pair, SD-WAN Manager and FortiMail joining nine overdue families; its ransomware score holds at 7 because no South African incident has yet named an edge appliance as the entry point this quarter. Collaboration and Virtualisation holds at 9: Symantec's Warlock cases reached water, telecoms and government bodies in Portuguese- and Spanish-speaking countries through SharePoint, and South Africa exposes 826 instances.<sup>24,15</sup> Government, Retail and Software Supply Chain hold their W40 scores.

The hacktivism column has not moved since W37 because nothing has been observed in it; it stays in the matrix so that an observation has somewhere to land.

23. The Citizen, Edcon files for voluntary business rescue (29 April 2020; business rescue practitioners Piers Marsden and Lance Schapiro). <https://www.citizen.co.za/business/edcon-files-for-voluntary-business-rescue/>

24. The Record, Warlock ransomware used in attacks on critical infrastructure in Portuguese, Spanish-speaking countries, on Symantec Threat Hunter Team reporting (2 October 2026). <https://therecord.media/warlock-ransomware-used-in-critical-infrastructure-attacks>

### 3. TOP SA INCIDENTS (W41)

Four items. One is a state-owned operator's disclosure through a tender, one is a leak-site claim that follows a confirmed incident at the same company, one is the resolution of last week's insurer question, and one is a pair of claims from the same group. Every rating follows the standing rule that a leak-site description is written by the attacker and cannot lift a rating on its own.

#### 3.1 INC-2026-W41-01: ATNS Finds Ransomware-Linked Malware in Airport OT and Tenders for Forensics [CONFIRMED]

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sector        | Transport (civil aviation; air navigation services); state-owned company under the Department of Transport                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Organisation  | Air Traffic and Navigation Services SOC Ltd (ATNS), which manages South African airspace and serves 21 aerodromes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Disclosed     | Request for quotation issued 18 September 2026 for cyber-forensic services, reported by the Sunday Times on 26 September and by Dark Reading and MyBroadband on 30 September and 2 October. The RFQ states that preliminary investigations identified malware commonly associated with the early stages of ransomware attacks in the operational technology environment supporting weather services and the associated IT infrastructure at Chief Dawid Stuurman International Airport (Gqeberha), that network monitoring indicated possible data exfiltration to external IP addresses located in China, and that internal teams implemented containment and malware removal. The investigator is to establish root cause and extent, analyse the malware, and certify whether exfiltration occurred and what was taken |
| Second matter | A separate forensic workstream into reports that employees may have unlawfully accessed and exfiltrated personal information; initial internal investigation could not substantiate it. MyBroadband places it at Mahikeng Airport; Dark Reading reads the same RFQ code as Maputo, which this report does not adopt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Statement     | Spokesperson Khulu Phasiwe to the Sunday Times: ATNS cannot comment on the nature or extent of any potentially compromised data until the forensic investigation has concluded. No date of detection, no actor, no family and no regulator named; no service disruption reported                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Confidence    | CONFIRMED on the spokesperson's on-record statement and on the RFQ text as read by the Sunday Times, Dark Reading and MyBroadband; the ATNS tenders page was not readable to this collection. The China reference is the operator's description of traffic destinations and names no actor; MyBroadband's headline goes further than the document                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

The system at issue carries weather data to controllers, and the Sunday Times notes that its loss could have affected flight planning, visibility data and the link between meteorological systems and the tower; ATNS's

own account is that the malware was found, contained and removed, and nothing in the public record says a service stopped.<sup>1,3</sup> Two things make it the week's lead. It is operational technology at a national air navigation provider, confirmed by the operator. And the disclosure route was a tender with a budget ceiling below R50 million, which means the first public account of a national-infrastructure cyber incident was written by a procurement office for bidders, and a journalist found it.<sup>2</sup> The insider workstream concerns personal information; the RFQ says the internal investigation could not substantiate the reports, so the section 22 question is open rather than answered. The timing of detection is given only as the current financial year. Detection relevance: none specific to ATNS; the OT segmentation and egress questions in Section 10 apply to every operator with a weather, SCADA or building-management network reachable from the corporate side.

### 3.2 INC-2026-W41-02: BCX Listed by INC Ransom With a 500 GB Source-Code Claim [CLAIMED]

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sector       | Outsourced IT providers; telecommunications                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Organisation | BCX, the IT services subsidiary of Telkom SA SOC Ltd; listed as bcx.co.za                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Listing      | Indexed by ransomware.live at 12:32 UTC on Tuesday 29 September 2026 from INC Ransom's blog, on the group's disclosures path, post dated 29 September. The actor's text claims 500 GB, 4,224,088 files and 596,613 folders, described as source code, technical documentation and other confidential information: six business applications named by the actor (a cemetery-management system, an mSCOA posting-level creator, a receipting module, a portal single sign-on, a reporting tool and a change-request manager), more than fifteen integration libraries and connectors, and test and utility projects, with the sentence that numerous vulnerabilities have been found in current versions |
| Prior record | Telkom's statement of 25 September (W40, Section 3.2) placed an incident in a limited area of a BCX legacy testing environment, contained and isolated from production, with no evidence to date of customer data compromised and customers notified as a precaution. No leak-site record for BCX before this one; Telkom's own records are from 2017 and 2020                                                                                                                                                                                                                                                                                                                                         |
| Confirmed    | Nothing about the listing. BCX's website carried no notice and no statement responding to the listing was located by the close of the window; no South African publication had reported it                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Confidence   | CLAIMED for the listing and its contents. The underlying incident is CONFIRMED by Telkom at the scope Telkom gave. The two are not joined by any public statement and this report does not join them                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

The claim is carried as the actor's. What can be said without adopting it is that the names on the listing read as municipal and local-government line-of-business systems, that source code and integration libraries are what one would expect to find in a testing environment, and that the actor's description is therefore consistent with Telkom's scope statement rather than in tension with it, and consistency confirms nothing.<sup>4,5</sup> For a BCX customer the practical exposure, if the claim is true, is secrets embedded in code and connectors rather than customer records, which is why the second action in Section 1 is a rotation list. INC Ransom's South African record stands at seven listings once an Ivorian airline tagged ZA is excluded on its domain, among them South African Airways in May 2025 and Rohloff Group, confirmed in W38; the group's cadence against South African targets is profiled in Section 4.2 below.<sup>20</sup> The distinguishing observations are a Telkom or BCX statement on the listing, a data-published marker or sample on the actor's page, and whether any named application corresponds to a product BCX sells to

municipalities. First reported by [ransomware.live](#) on 29 September 2026. Detection relevance: TH-2026-W41-04 carries the group's sourced hashes, addresses and YARA rule.

### 3.3 INC-2026-W41-03: Guardrisk Denies a Breach and Points to MIP Data Held by a Binder Holder [CONFIRMED]

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sector        | Financial services and credit; cell-captive insurance and intermediaries                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Organisations | Guardrisk Group (Momentum Group), the insurer named on The Gentlemen's site on 26 September; CoverCubed, a Johannesburg health-insurance and medical-scheme intermediary that acts as a binder holder for Guardrisk                                                                                                                                                                                                                                                                                                                                                                             |
| Statement     | Guardrisk to ITWeb on 28 September and MyBroadband on 30 September: the information appears to be linked to the June 2026 cybersecurity incident involving MIP and not to any breach or compromise of Guardrisk's systems; there is no indication that its systems or client data have been compromised; approximately 6,000 funeral policies administered by an affected binder holder are involved; the binder holder has notified the Information Regulator under section 22 and its affected clients. Guardrisk's position is that accountability for the data rests with the binder holder |
| The listing   | Still on the group's site with a leak timer per MyBroadband; no volume, sample or published data observed on the aggregator's record by the close of the window. The group's own-system claim against Guardrisk stays CLAIMED and is denied by the company                                                                                                                                                                                                                                                                                                                                      |
| Confidence    | CONFIRMED for Guardrisk's denial that its own systems were compromised, on its statement to two publications. The MIP origin (which Guardrisk words as appears to be linked) and the binder holder's section 22 filing are Guardrisk's account of a third party; CoverCubed has published nothing that this collection could locate, so both are carried as Guardrisk's account                                                                                                                                                                                                                 |

The W40 watch item asked whether the Guardrisk listing was the insurer's own estate or a second downstream extortion from the MIP set; the company's answer, hedged as it is, points to the second, by way of a binder holder rather than the insurer as MIP's client; the aggregator's record still shows no volume, sample or published data.<sup>7,8,25</sup> That matters for every insurer in the country because it means the MIP cascade reaches names that never contracted with MIP, and that an insurer can appear on a leak site, and be extorted, for data its intermediary processed. MyBroadband's longer piece of 3 October sets the Hollard, Guardrisk and MIP accounts side by side, with MIP's position that Jira is an Atlassian platform rather than an MIP system and that the breach was limited to it and certain third-party file-transfer sites.<sup>26</sup> Under POPIA the question of whether the binder holder or the insurer is the responsible party for a given record is a question of who determines the purpose and means, and it is not settled by either party's statement; what Guardrisk reports is that notification has been made in the binder holder's name, which would make CoverCubed the second institution after Bidvest Bank to file in its own name in the two supplier cascades.<sup>27</sup> Detection relevance: TH-2026-W40-06 (The Gentlemen's tooling hashes and backup-share exfiltration) stands as written and is not reprinted.

### 3.4 INC-2026-W41-04: LegalWise and Edcon Listed by The Gentlemen [CLAIMED]

|        |                                                                                  |
|--------|----------------------------------------------------------------------------------|
| Sector | Financial services (legal-expenses insurance); retail (group in business rescue) |
|--------|----------------------------------------------------------------------------------|

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Organisations</b> | LegalWise South Africa (RF) (Pty) Ltd, legalwise.co.za, Johannesburg, a legal-expenses insurance provider whose cover is underwritten by Legal Expenses Insurance Southern Africa Limited (LEZA); both sit in Legal Expenses Group Africa, in which Sithega holds 62 per cent and Hollard 38 per cent. Edcon, edcon.co.za, the former owner of Edgars, Jet and CNA, in voluntary business rescue since April 2020 |
| <b>Listings</b>      | Both indexed by ransomware.live at 03:40 UTC on Wednesday 30 September 2026, posts dated 29 September, estimated attack date 29 September. Neither carries a data volume, sample or deadline on the aggregator's record. The descriptions on the records are aggregator-compiled company text, which this report does not adopt                                                                                   |
| <b>Confirmed</b>     | Nothing. LegalWise's website carried no notice and no South African publication had reported either listing by the close of the window; edcon.co.za could not be read because its certificate does not match the hostname                                                                                                                                                                                         |
| <b>Confidence</b>    | CLAIMED for both. Threat-actor assertion only. Whether LegalWise is an MIP client, and what systems Edcon's business-rescue estate still operates, are both unknown and neither is inferred                                                                                                                                                                                                                       |

Two listings in one minute from the group that has now named four South African organisations since 7 September, three of them insurance-linked.<sup>9,10,28,29</sup> LegalWise is the item to watch: it is an insurer by licence, it is partly owned by Hollard, and the Hollard case resolved to the MIP data set and the Guardrisk case, on the insurer's account, appears to. None of that makes LegalWise an MIP client, and the distinguishing observations are a LegalWise statement, an MIP statement, or a published sample whose record format matches the Hollard set. Edcon is a different kind of record: the company's trading businesses were sold in 2020 and the domain now serves the business-rescue process, so if the group holds anything it is legacy data from a wound-up retailer with four million store-card accounts in its past, which is personal information whether or not the responsible party still trades; the business rescue practitioners named in 2020 were Piers Marsden and Lance Schapiro.<sup>23</sup> The Gentlemen's index rose by 33 in the week to 921, the largest move of any group in the aggregator's table.<sup>30</sup> Detection relevance: TH-2026-W40-O6 stands.

### 3.5 Carryovers

**Rand Water, W37. Closed at the 3 October test.** A month after the SENS statement there is no actor, no personal-information statement and no announcement of a return from the disaster recovery site; the utility's website carries nothing on the incident.<sup>31</sup> As W39 and W40 set out, silence at this point is the finding, and the item moves to the record at CONFIRMED for the incident and unresolved for everything else.

**RelyComply, W39.** A second fortnight of silence. The notice still reads last updated 16 September; no publication of the data was observed; DireWolf's index did not move.<sup>32,30</sup> Stays CONFIRMED for the incident; the 200 GB remains the actor's figure.

**MIP Holdings and Hollard, W39.** Developed through 3.3 and 3.4: the MIP set has produced a second insurer-linked listing, this one by way of a binder holder. The Information Regulator's position of 25 September, that it had received only MIP's notification, now has one further filing against it, CoverCubed's, reported by Guardrisk.<sup>33,8</sup> Both items stay CONFIRMED. The W40 test of whether insurers have notified in their own names runs to Friday 9 October and is carried in Section 11.

**Telkom and BCX, W40.** Developed into Section 3.2. The company's scope statement stands; the listing is the actor's.

**BlackLocks (Apollo 21 and ARCA Unlimited Architects), W40.** No development on either company and no new listing by the group in the window, so neither branch of the W40 tempo test was observed; carried one more week at CLAIMED.

**Gauteng e-Panic Button, W40; Cell C Fibre, W39; Cartrack, W37; VSB Attorneys, W38; Rohloff Group, W36; The Courier Guy and Babcock Africa, W35; Furniture Bargaining Council, W36; Toyota South Africa's unnamed SMS provider, W34; Implats and Hungry Lion, W37.** No development on any of them. All stay at their prior ratings and are carried without re-argument.

25. ransomware.live, victim page for Guardrisk (The Gentlemen), discovered 26 September 2026 08:48 UTC, re-read 4 October 2026. <https://ransomware.live/id/R3VhcmRyaXNrQHRoZWdlbnRsZWlbg==>

26. MyBroadband, Insurance industry in South Africa under attack and customers are the victims, by Luis Monzon (3 October 2026). <https://mybroadband.co.za/news/security/669782-insurance-industry-in-south-africa-under-attack-and-customers-are-the-victims.html>

27. Bidvest Bank, Notification of a Security Compromise in terms of Section 22 of POPIA: RelyComply cyber incident (notice dated 17 September 2026; text stored in W40 as evidence/w40\_bidvestbank\_important\_notice\_2026-09-27.txt). <https://www.bidvestbank.co.za/important-notice>

28. LegalWise, corporate website, checked 4 October 2026 (no notice or statement on any incident; names LegalWise South Africa (RF) (Pty) Ltd and the insurer Legal Expenses Insurance Southern Africa Limited, LEZA). <https://www.legalwise.co.za/>

29. Investec, Sithega transaction page (Sithega acquired 62 per cent of Legal Expenses Group Africa, LEGA, with Hollard retaining 38 per cent; 2023), checked 4 October 2026. [https://www.investec.com/en\\_za/investec-for-corporates/transactions/sithega-2023.html](https://www.investec.com/en_za/investec-for-corporates/transactions/sithega-2023.html)

30. ransomware.live API, GET /groups, 403 groups with victim counts, retrieved 4 October 2026 and compared with the 27 September retrieval (feeds/r1\_groups\_2026-10-04.json). <https://api.ransomware.live/v2/groups>

31. Rand Water, corporate website, checked 4 October 2026 (no statement on the incident; consumption data, tariff consultations and a hotline only). <https://www.randwater.co.za/>

32. RelyComply, RelyComply cyber incident: what happened and what you can do, official notice (published 16 September 2026; re-read 4 October 2026, page still reads last updated 16 September 2026). <https://relycomply.com/relycomply-cyber-incident-what-happened-and-what-you-can-do/>

33. TechCentral, Insurers carry the can for MIP breach, regulators say (25 September 2026). <https://techcentral.co.za/insurers-mip-breach-regulators/286482/>

## 4. THREAT ACTORS

Three profiles and three notes. The Gentlemen, because it listed two more South African names and one of last week's appears, on the insurer's account, to resolve to its MIP data; INC Ransom, because it listed BCX; and the unattributed NetScaler intrusion set, because its tooling is documented and 122 South African appliances are in scope. Notes on Warlock and on the groups that did not move close the section.

### 4.1 The Gentlemen: Eleven South African Listings, Three of Them Insurance-Linked

The group's index rose from 888 to 921 between the 27 September and 4 October retrievals, 33 listings in a week after 21 and 30 in the two before, the largest movement in the aggregator's table this week.<sup>30</sup> Its South African record stands at eleven ZA-tagged listings since January: Paltrack, Rola Motor Group and Witzenberg Municipality on 20 January, Intsika Yethu in February, Elundini in March, Sunspray Food in April, Babcock in August, Hollard on 7 September, Guardrisk on 26 September, and Edcon and LegalWise on 30 September.<sup>20</sup> What changed this week is the shape of the insurance thread. Hollard's published records came from MIP; Guardrisk's listing, by the insurer's account, is MIP data held by a binder holder; the

group has not said where the LegalWise material came from, and the company has not said anything.<sup>8,9</sup> An affiliate holding the MIP data set, which MIP says covered about 45 insurers' customers, has an inventory of extortion targets that does not require a single further intrusion, and the leaked May guidance to avoid Africa-style targets, as KELA read it, is plainly not what this affiliate is doing.<sup>26,34</sup> The aggregator's IOC feed for the group is byte-identical to the 27 September retrieval: 34 SHA-256, four SHA-1 and 47 MD5 hashes, six Tox and one Session identifier, two email addresses, and the ransom-note YARA rule matching thegentlemen, THEGENTLEMEN and thegentlemen.onion; all were exported in iocs\_w40.csv and are not re-exported.<sup>35,36</sup>

## 4.2 INC Ransom: BCX, and a Record That Includes an Airline

INC Ransom's index rose from 949 to 959 in the week.<sup>30</sup> The feed holds eight ZA-tagged records for the group, one of which, aircotedivoire.com in February 2026, is Ivorian by its own domain and is excluded here; prior editions' count of seven included it, which makes this week's South African count seven rather than eight. The seven are South African Airways (May 2025), Netstar (August 2025), Climatron (October 2025), ETFSA (March 2026), Reatile (July 2026), Rohloff Group (27 August 2026, confirmed by the company in W38) and now BCX.<sup>20</sup> The cadence against South African targets since July is roughly one listing every five to six weeks, and the two most recent are a KFC franchisee and the country's largest IT services company, a spread that reads as access brokerage rather than sector targeting. The aggregator's IOC feed carries two SHA-256 hashes and two addresses for the group, and its YARA set carries rivitna's Inc rule, which matches the Windows encryptor on byte patterns and on the command-line switches lhd, ens and sup, each written with a double hyphen in the binary, and the shadow-copy deletion string; Huntress's W40 timeline supplies the two-note pattern (INC-README.txt followed by DATALEAK\_PRESS\_RELEASE.txt), the HwAudio driver service and the dictionary-word scheduled task. All of it is in TH-2026-W41-04 and iocs\_w41.csv.<sup>35,36,37</sup> The BCX listing sits on the group's disclosures path rather than a countdown page, which with this group has meant the negotiation is over; that is an inference from the page structure and is recorded as such.

## 4.3 The NetScaler Intrusion Set: WHIPSHOT, SLAPSHOT and a Patch That Destroys Evidence

Mandiant and Google Threat Intelligence Group published on 29 September the tooling of a campaign that has exploited the two NetScaler zero-days since at least early September, without naming an actor or a state; the Register's account of the same report records that no attribution has been made public.<sup>12,14</sup> The chain is a DTLS record over UDP/443 that corrupts the packet engine's heap and runs shellcode as root, or the command injection through the log-processing script, followed by an installer that edits /etc/httpd.conf so that .deb or .sig files in the VPN scripts directory execute as PHP, sets the SUID bit on /bin/sh, scrubs its own path from /etc/crontab, and restarts the web server or reboots the appliance. WHIPSHOT is the PHP web shell, which takes Base64 commands from the HTTP\_NSC\_LDAP, HTTP\_NSC\_CLIENTTYPE or HTTP\_X\_UX headers and answers with a 404 while tunnelling in the body; SLAPSHOT is a Python daemon bound to a port it writes to /tmp.uxdport, with a JSON wire protocol of open, push, pull, exch, close and ping verbs, which gives the operator a bridge into the internal network from the appliance. Victims are in government, financial services, technology, education and legal and professional services in North America and Europe; addresses 143.198.7.94 and 157.254.167.12 are published as scanning and installation infrastructure.<sup>12</sup> Rapid7 saw the first exploitation attempt at 14:28

UTC on 20 September, a week before disclosure, and two compromises: one in which the command injection archived `/flash/nsconfig` to a web-served path, and one with a web shell at `/var/netScaler/logon/LogonPoint/custom/.ctxs.receiver` on 24 September.<sup>13</sup> watchTower traced the command injection to `ns_monupload_err.pl`, which builds a filename from logged text and passes it to a shell; anything the appliance logs, including the login field of a failed authentication, can carry the payload.<sup>38</sup> No South African victim is named by any of the three; the set is profiled because the hunt in TH-2026-W41-01 is sized at 122 exposed instances and because the responder guidance, examine before you patch, is the opposite of most patch programmes.

## 4.4 Notes: Warlock, BlackLocks, DireWolf

**Warlock.** Symantec's Threat Hunter Team, as reported by The Record and Industrial Cyber on 2 October, describes a China-based group, which Microsoft has not tied to a known state actor, using the 2025 ToolShell SharePoint chain and newer SharePoint flaws against a water utility, a telecoms provider, a university and a regional government in Portuguese- and Spanish-speaking countries across Europe, Africa and Latin America over the past two months, with a tool that disabled security software on at least 40 hosts in about two hours, Visual Studio Code's tunnel feature installed as a service, and ransomware staged through SYSVOL.<sup>24,39</sup> No country in Africa is named. It is noted here because the same SharePoint population, 826 exposed in South Africa, carries two overdue catalogue entries, and TH-2026-W41-06 takes the tunnel service and SYSVOL staging as indicators.<sup>15</sup> **BlackLocks** did not list anything in the week; the group holds at three victims, two of them the Pretoria firms of W40, and the tempo question stays open.<sup>30</sup> **DireWolf** held at 135 for a third week, with two confirmed South African data sets (Cartrack and RelyComply) and no publication; its listing of RelyComply is now four weeks old.<sup>30,32</sup>

34. KELA, Inside The Gentlemen leak: how a new RaaS captured 10 per cent of 2026's global ransomware victims (14 May 2026). <https://www.kelacyber.com/blog/the-gentlemen-ransomware-internal-chat-leak-analysis-2026/>

35. ransomware.live API, GET /iocs/{group} for the groups active against South Africa in the last 120 days, retrieved 4 October 2026 (feeds/rl\_iocs\_2026-10-04.json). <https://api.ransomware.live/v2/iocs/incransom>

36. ransomware.live API, GET /yara/{group}, retrieved 4 October 2026 (feeds/rl\_yara\_2026-10-04.json; the INC rule is rivitna's Inc.yar). <https://api.ransomware.live/v2/yara/incransom>

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

38. watchTower Labs, Oh look, the foot gun went off again: Citrix NetScaler pre-auth command injection CVE-2026-88771 (28 September 2026). <https://labs.watchtower.com/oh-look-the-foot-gun-went-off-again-citrix-netScaler-preauth-command-injection-cve-2026-88771/>

39. Industrial Cyber, report on Symantec Threat Hunter Team's Warlock findings: water, telecom and government targets reached through SharePoint flaws (2 October 2026). <https://industrialcyber.co/ransomware/symantec-reports-warlock-ransomware-group-targets-water-telecom-government-organizations-through-sharepoint-flaws/>

## 5. CRITICAL VULNERABILITIES & CISA KEV

Seven vulnerabilities entered the CISA catalogue of known exploited vulnerabilities between Sunday 27 September and Friday 2 October 2026, against ten the week before. Five were past their remediation date on Monday 5 October, the day this report was published, and the Zammad pair fell due on that day.<sup>11</sup> Every due date and overdue count in this section is arithmetic against the locally retrieved catalogue file, catalogVersion 2026.10.02, released at 15:19 UTC on Friday 2 October, so any addition made on Saturday 3 October is outside this edition; every CVSS score is from the NVD feed with its scoring source recorded,

except the two carryovers older than its 45-day window, CVE-2026-15409 and CVE-2026-55040, which carry the scores recorded when they entered.<sup>11,40</sup> All seven carry knownRansomwareCampaignUse of Unknown, which is not the same as no. All seven received three-day deadlines under BOD 26-04. Four came with vendor indicators on the day of listing: Citrix through its IOC scanner and the Mandiant report, Cisco with two log paths, Fortinet with two addresses and three log patterns; Apple published a fix and a sentence; Zammad's record is a community thread and the victim's own account.<sup>12,16,17,18,19</sup>

**Citrix NetScaler CVE-2026-88771 and CVE-2026-88772** were added on Sunday 27 September, the day of the vendor bulletin, with a due date of 30 September. The first is an input-validation flaw that gives remote code execution in a default configuration with low attack complexity, which Citrix itself glosses as reliable RCE against any vulnerable appliance regardless of configuration; the second is a memory overflow in DTLS handling that needs DTLS enabled and is harder to exploit. Both are 9.5 under CVSS 4.0 from the vendor CNA. Fixed builds are 14.1-73.37, 13.1-64.23, 14.1-FIPS 14.1-73.37 and 13.1-FIPS and NDcPP 13.1.37.279; six further CVEs in the same bulletin, CVE-2026-88773 to 88778, are not reported exploited.<sup>13,40,11</sup> The intrusion tooling is in Section 4.3 and TH-2026-W41-01. South Africa exposes 122 NetScaler instances, 107 of them on 443; the September authentication bypass CVE-2026-19490 on the same population reaches +23 on Monday 5 October.<sup>15,11</sup>

**Apple CVE-2026-86950** is an out-of-bounds write in CoreGraphics reachable from a crafted file, fixed in iOS and iPadOS 26.7.1, macOS 26.7.1 and macOS 15.8.1 on 28 September and reported by Meta Product Security; Apple's note is that it may have been exploited in an extremely sophisticated attack against specific targeted individuals on older iOS versions, which is the vendor's standard form of words for a commercial-spyware chain. NVD's CISA-ADP record scores it 8.8 under CVSS 3.1.<sup>18,40</sup> It was added on 29 September, due 2 October, and reaches +3; for a South African estate it is a mobile device management compliance report.<sup>11</sup>

**Cisco Catalyst SD-WAN Manager CVE-2026-76504** is an authentication bypass through improper handling of URI encoding: a percent-encoded request to an endpoint whose access rule matches on the literal path reaches the API with admin privileges. Cisco published on 30 September with the sentence that in September the PSIRT became aware of active exploitation, scored it 9.8, gave no workaround, and published two log checks: POST requests to `_security_check` with encoded characters in the service-proxy access log and the `vmanage` server log.<sup>16,40</sup> Fixed releases are 20.9.10.1, 20.12.8.2, 20.15.6.1, 20.18.4.1, 26.1.2.1 and 26.2.1. Added 30 September, due 3 October, +2. The discovery stage found no Shodan product label for the manager and held it.<sup>11</sup>

**Fortinet FortiMail CVE-2026-104286** is a path traversal with null-byte handling in the identity-based encryption (IBE) web path that lets an unauthenticated attacker write arbitrary files through crafted HTTP requests. Fortinet published FG-IR-26-175 on 1 October, credited its own product security team with the discovery, stated that it has been reported to be exploited in the wild, scored it 9.8, and published two addresses, 79.141.169.187 and 45.129.0.192, and three log signatures: archive-account configuration changes from the first address, decryption failures with invalid Base64, and administrator logout events without a user-interface context. Fixed in 8.0.2, 7.6.7 and 7.4.9; 7.2 is to be upgraded. Workarounds are to disable IBE, restrict the webmail interface and block POST requests carrying `../` to `/ibe` paths.<sup>17,40</sup> Added 1 October, due 4 October, +1. The discovery stage found no product label for FortiMail and held it; the panel's FortiGate count does not describe the mail appliance.<sup>11</sup>

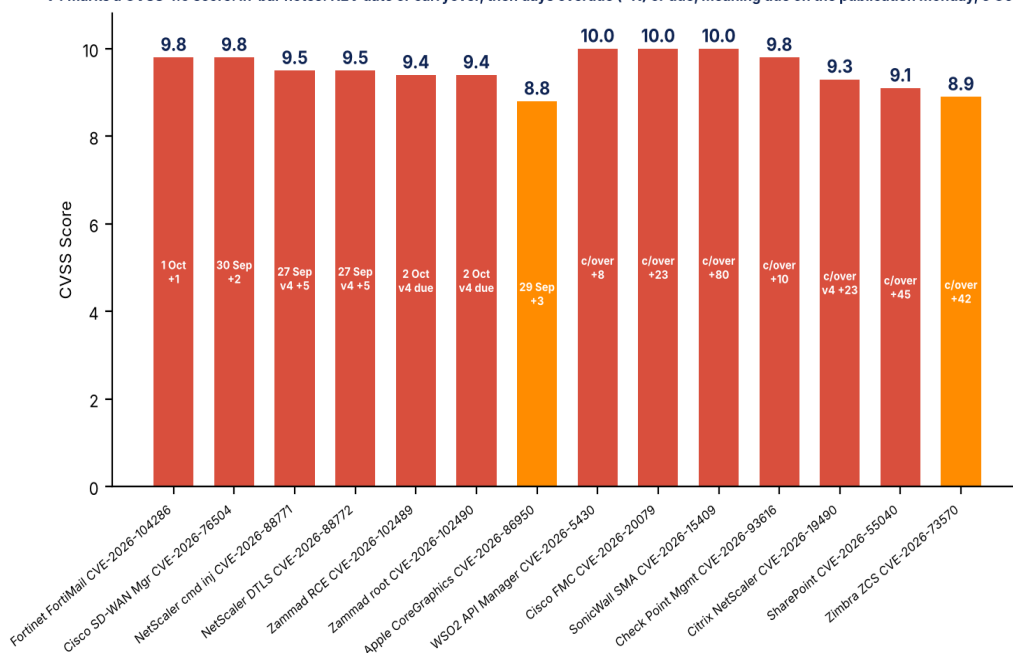
**Zammad CVE-2026-102489 and CVE-2026-102490** are a session fixation that leads to code execution as the zammad service user and a privilege escalation from that user to root, chained; both are 9.4 under

CVSS 4.0 and the scoring source is the Dutch Institute for Vulnerability Disclosure, because DIVD was the victim. DIVD detected the attack on its own Zammad helpdesk on 24 September and disclosed on 30 September that volunteer email addresses and possibly contact details were taken, that the two flaws were chained in seconds, and that the attacker's scripts contained notes in which an agent justified its own actions, which DIVD reads as an autonomous AI-driven intrusion; the fix is version 7 of Zammad.<sup>19,40</sup> Added 2 October, due 5 October, on publication day. Zammad is an open-source helpdesk of the kind managed service providers run; it has no Shodan product label and the discovery stage held it.<sup>11</sup>

**Carryovers.** Microsoft published on 30 September its tracking of the Zimbra CVE-2026-73570 command injection, +42 on Monday 5 October: reconnaissance from 28 July, exploitation between the 20 July patch and the 13 August disclosure, JSP web shells in the Jetty and mailboxd directories, escalation through the zmmailboxdmgr sudo path, credential theft through zmlocalconfig, mailbox staging to /opt/zimbra/final.tar.gz and exfiltration with AzCopy, and a systemd unit named zimlog.service; the flaw needs the optional SNMP package.<sup>41,11</sup> The EPSS feed moved two carryovers sharply upward while nothing changed about their exploitation status: WordPress CVE-2026-87902 from 0.1817 to 0.4550 and NetScaler CVE-2026-19490 from 0.0701 to 0.2316, which is the lag the methodology note describes.<sup>42</sup> The overdue counts for every tracked carryover are in the table; the ones not given their own row are Zyxel CVE-2026-7273 +11, the kernel trio led by CVE-2025-39682 +14, Cisco ISE CVE-2026-76460 +16, and ScreenConnect CVE-2026-84869 and GitLab CVE-2026-85706 +21.<sup>11</sup> The SharePoint builds that carry the August fix are unchanged from W40 and are repeated in TH-2026-W41-06.<sup>43</sup>

W41 KEV / CRITICAL CVE SEVERITY | 27 September - 3 October 2026

All seven KEV additions in the window (left) plus the seven carryovers that most outrank them (right). CVSS from the NVD feed except CVE-2026-15409 and CVE-2026-55040 (earlier feeds); v4 marks a CVSS 4.0 score. In-bar notes: KEV date or carryover, then days overdue (+N) or due, meaning due on the publication Monday, 5 October 2026



## W41 CISA KEV / Critical CVE Tracking (seven additions 27 September to 2 October plus active carryovers)

| CVE             | Vendor / Product                        | CVSS       | Type                                             | KEV Due | Notes                                                                                                                                                                                                                                                                  |
|-----------------|-----------------------------------------|------------|--------------------------------------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-88771  | Citrix NetScaler ADC and Gateway        | 9.5 (v4.0) | Input validation, pre-auth RCE (default config)  | 30 Sept | KEV 27 Sept. OVERDUE +5. Exploited before disclosure; Rapid7 first attempt 20 Sept, two compromises. Root cause ns_monupload_err.pl. Fixed 14.1-73.37 / 13.1-64.23. Checks in TH-01. 122 in ZA. Ransomware: Unknown. EPSS 0.0106.                                      |
| CVE-2026-88772  | Citrix NetScaler ADC and Gateway        | 9.5 (v4.0) | Memory overflow, DTLS (pre-auth RCE)             | 30 Sept | KEV 27 Sept. OVERDUE +5. Needs DTLS; UDP/443; heap corruption to root shellcode (GTIG). Log: DTLSv1.0 handshake failure, Internal Error; NSPPE not restarted. Block UDP/443 if unpatched. 122 in ZA. Ransomware: Unknown. EPSS 0.0130.                                 |
| CVE-2026-86950  | Apple iOS, iPadOS, macOS (CoreGraphics) | 8.8        | Out-of-bounds write (crafted file)               | 2 Oct   | KEV 29 Sept. OVERDUE +3. Apple: may have been exploited against specific targeted individuals. Fixed iOS/iPadOS 26.7.1, macOS 26.7.1 and 15.8.1. MDM item. Ransomware: Unknown. EPSS 0.0124.                                                                           |
| CVE-2026-76504  | Cisco Catalyst SD-WAN Manager           | 9.8        | Auth bypass via URI encoding (unauth, admin API) | 3 Oct   | KEV 30 Sept. OVERDUE +2. PSIRT aware of active exploitation; no workaround. Fixed 20.9.10.1 / 20.12.8.2 / 20.15.6.1 / 20.18.4.1 / 26.1.2.1 / 26.2.1. Check j_security_check with %-encoding in two logs (TH-02). No ZA label (held). Ransomware: Unknown. EPSS 0.0158. |
| CVE-2026-104286 | Fortinet FortiMail (IBE web path)       | 9.8        | Path traversal, null byte (unauth file write)    | 4 Oct   | KEV 1 Oct. OVERDUE +1. FG-IR-26-175: reported exploited in the wild. Fixed 8.0.2 / 7.6.7 / 7.4.9; 7.2 upgrade. IOCs 79.141.169.187, 45.129.0.192 (TH-03). Disable IBE. No ZA label (held). Ransomware: Unknown. EPSS 0.0220.                                           |

| CVE             | Vendor / Product                                    | CVSS       | Type                                          | KEV Due | Notes                                                                                                                                                                                                                                            |
|-----------------|-----------------------------------------------------|------------|-----------------------------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-102489 | Zammad helpdesk                                     | 9.4 (v4.0) | Session fixation (RCE as zammad user)         | 5 Oct   | KEV 2 Oct. Due on publication day. Chained with CVE-2026-102490 (9.4 v4, zammad to root, also due 5 Oct) against DIVD on 24 Sept. Fixed Zammad 7. Scoring source DIVD. No ZA label (held). Ransomware: Unknown. EPSS 0.0140 and 0.0063.          |
| CVE-2026-93616  | Check Point Security Management and related servers | 9.8        | Path traversal, file upload (unauth)          | 25 Sept | Carryover. OVERDUE +10 with CVE-2026-85102, F5 APM CVE-2026-94127 (9.3 v4) and Arista VCO CVE-2026-93952 (9.5 v4). W40 checks stand. No ZA label for any of the four. EPSS 0.1965.                                                               |
| CVE-2026-5430   | WSO2 API Manager and related products               | 10.0       | Catalogue: path traversal; vendor: JWT bypass | 27 Sept | Carryover. OVERDUE +8 with Adobe Commerce CVE-2026-71362 (9.1, EPSS 0.8751). Description conflict stands. No ZA label (held). EPSS 0.0059.                                                                                                       |
| CVE-2026-67279  | MikroTik RouterOS                                   | 6.9 (v4.0) | Workflow bypass (SSH, unauth)                 | 28 Sept | Carryover. OVERDUE +7 with SharePoint CVE-2026-65660 (8.8) and WordPress CVE-2026-87902 (8.1; EPSS 0.1817 to 0.4550). First half CVE-2026-86060 at +22. 4,938 in ZA, 4,007 on 8728; SharePoint 826; WordPress 402 floor. EPSS 0.0103.            |
| CVE-2026-73570  | Synacor Zimbra Collaboration Suite                  | 8.9        | OS command injection, SNMP trap path (unauth) | 24 Aug  | Carryover, newly profiled. OVERDUE +42. Microsoft 30 Sept: multiple compromises; JSP shells, zimlog.service, AzCopy exfiltration; needs zimbra-snmp. Fixed 10.1.20. TH-05. No ZA label. EPSS 0.1174.                                             |
| CVE-2026-76461  | Cisco Secure Email Gateway (AsyncOS)                | 9.8        | SQL injection (unauth, root)                  | 17 Sept | Carryover. OVERDUE +18; ISE CVE-2026-76460 (10.0), Pixel and Acronis +16; N-central CVE-2026-86218 (10.0 v4) and Adobe CVE-2026-75650 +24; ScreenConnect, GitLab (EPSS 0.9296) and PaperCut +21. No SA incident naming any of them. EPSS 0.2827. |

| CVE            | Vendor / Product                 | CVSS       | Type                    | KEV Due | Notes                                                                                                                                                                                                             |
|----------------|----------------------------------|------------|-------------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-19490 | Citrix NetScaler ADC and Gateway | 9.3 (v4.0) | Auth bypass (unauth)    | 12 Sept | Carryover. OVERDUE +23 with Cisco FMC CVE-2026-20079 (10.0, EPSS 0.8818) and FortiOS CVE-2025-25249 (8.1). Same 122 instances as the new pair. EPSS 0.0701 to 0.2316 in a week.                                   |
| CVE-2026-83548 | SonicWall SMA 1000               | 10.0       | SSRF (unauth)           | 5 Sept  | Carryover. OVERDUE +30 with CVE-2026-83549, Artifactory CVE-2026-82329, Kestra CVE-2026-49869 and Switchvox CVE-2026-9586. SonicWall family 2,960 in ZA, not narrowable to SMA 1000. EPSS 0.0876.                 |
| CVE-2026-55040 | Microsoft SharePoint             | 9.1        | Weak auth (JWT forgery) | 21 Aug  | Carryover. OVERDUE +45. 826 in ZA. Chains with CVE-2026-65660. Warlock used ToolShell and newer SharePoint flaws (Symantec via The Record). TH-06.                                                                |
| CVE-2026-15409 | SonicWall SMA 1000               | 10.0       | SSRF (unauth)           | 17 Jul  | Carryover. OVERDUE +80. CVE-2026-15410 shares the dates and the KNOWN ransomware flag; Cisco FMC CVE-2026-20316 (Known) at +65; LiteLLM CVE-2026-42271 at +105 is the deepest tracked. Rebuild rather than patch. |

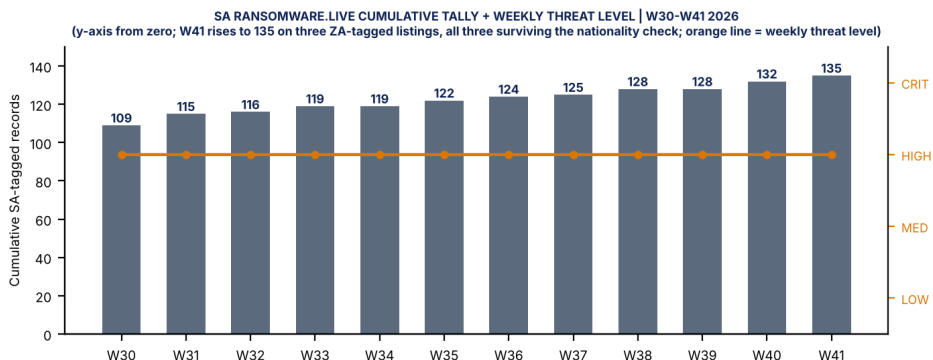
Pattern note: the week's seven divide by who found the flaw. Fortinet and F5 before it found theirs internally and still had exploitation in the wild by the time the advisory shipped; Citrix disclosed a week after Rapid7's first observed attempt; DIVD learned of the Zammad pair by being attacked through it. The common thread is that the catalogue entry arrived after the exploitation started in every case, and that for four of the seven the vendor shipped a log check with the fix, which is the only thing in the week that a South African SOC can act on inside the three-day deadline. The NetScaler pair also inverts the normal order of work: Mandiant's advice is to examine the appliance before upgrading it, because the upgrade can remove the artefacts, and Rapid7's observation that the attacker took the configuration directory means the patch does not end the incident even where it removes the shell. On EPSS, WordPress CVE-2026-87902 moved from 0.1817 to 0.4550 and NetScaler CVE-2026-19490 from 0.0701 to 0.2316 in one week, nine and 25 days respectively after the catalogue listed them; the score is following the catalogue, which is the reason it must not be used to rank catalogue entries.<sup>42</sup> Three carryovers still outrank most of the additions: the July SonicWall pair at 80 days with ransomware use Known, SharePoint CVE-2026-55040 at 45 days against 826 exposed instances, and the MikroTik pair at 22 and seven days against 4,938.<sup>11,15</sup>

40. NIST NVD, CVE API 2.0, CVSS base scores with scoring source for the 62 catalogue entries added in the last 45 days, retrieved 4 October 2026 (feeds/nvd\_cvss\_2026-10-04.json). <https://services.nvd.nist.gov/rest/json/cves/2.0>

41. Microsoft Threat Intelligence, Unauthenticated command injection on internet-facing mail servers: tracking CVE-2026-73570 (30 September 2026). <https://www.microsoft.com/en-us/security/blog/2026/09/30/unauthenticated-command-injection-on-internet-facing-mail-servers-tracking-cve-2026-73570/>
42. FIRST, EPSS API, scores for the same 62 entries, retrieved 4 October 2026 (feeds/epss\_2026-10-04.json). <https://api.first.org/data/v1/epss>
43. Microsoft MSRC, CVE-2026-65660, Microsoft SharePoint Server remote code execution vulnerability (released 11 August 2026, revision 1.2 of 25 September 2026; the fixed builds cited in TH-06 and iocs\_w41.csv). <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65660>

## 6. RANSOMWARE LANDSCAPE

The South African victim feed held 135 records when retrieved at 02:00 UTC on 4 October 2026, three more than the week before. The collection is country-scoped by path, the written file records 135 South African records against 135 returned, the run log records filter purity 1.0 and a clean exit, and the tier is the delayed free v2.<sup>20</sup> A set-difference against the 27 September file returns three additions and zero removals, all three discovered inside the window: bcx.co.za (INC Ransom, 29 September 12:32 UTC), Edcon (The Gentlemen, 30 September 03:40 UTC) and LegalWise (The Gentlemen, 30 September 03:40 UTC). All three are South African on their own domains and survive the nationality check, so the derived count equals the feed count. The aggregator's country page, read as a cross-check, showed 135 with the same three newest.<sup>44</sup> The hand search of the world feed for South African victims under other country tags was not run this week either and remains a collector task; the Ivorian airline found under the ZA tag in Section 4.2 is the reverse case and was found by reading the group's records rather than by a search.



|                                                   |                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Baseline at W40 close</b>                      | 132 records                                                                                                                                                                                                                                                                                                                                                         |
| <b>New listings dated inside the window</b>       | 3 with a ZA tag: bcx.co.za (INC Ransom), Edcon and LegalWise (The Gentlemen)                                                                                                                                                                                                                                                                                        |
| <b>Surviving the nationality check</b>            | 3. Each is South African on its own domain. The aggregator's country field has invented a South African victim five times in the series (Costa Rica twice, Philippines, India, Indonesia) and hidden one (RelyComply, GB); a sixth invention, aircotedivoire.com tagged ZA in February, predates the check and is excluded from the INC Ransom count in Section 4.2 |
| <b>Delistings or restorations</b>                 | None. Set difference against the 27 September file returns three additions and zero removals                                                                                                                                                                                                                                                                        |
| <b>End count at W41 retrieval</b>                 | 135 records, filter purity 1.0 in the run log and 135 of 135 tagged ZA in the file                                                                                                                                                                                                                                                                                  |
| <b>Groups active against SA, rolling 120 days</b> | 16 by discovery date, down from 17 as the rolling boundary moved past a June listing. The boundary moves each week, so this figure is not a trend                                                                                                                                                                                                                   |
| <b>Threat-level drivers</b>                       | Operator-confirmed malware in airport operational technology; a 500 GB claim against the country's largest IT services company; the MIP data reaching a second insurer through a binder holder, on that insurer's account; a default-configuration NetScaler zero-day with 122 instances exposed                                                                    |

**Group notes.** The Gentlemen, INC Ransom and the NetScaler set 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 888 to 921, Qilin from 2,315 to 2,328, INC Ransom from 949 to 959, Krybit from 153 to 159, m3rx from 38 to 44, MedusaLocker from 97 to 101, RansomHouse from 209 to 212, LockBit 5.0 from 368 to 370, Payload from 74 to 75 and Arcus Media from 114 to 115; DireWolf, Everest, DragonForce and BlackLocks did not move. The index grew from 402 to 403 groups on one entry with a non-Latin name and no victims.<sup>30</sup> Fifteen groups hold a ZA-tagged listing discovered since 1 July 2026; the four profiled or noted in Section 4 are those whose listings this month were South African by domain and current, and the other eleven are carried through the IOC export rather than the narrative.<sup>20</sup>

**Two patterns from the week for South African estates.** The first is the one Section 3 is built on: two of the four items concern data held by a supplier or a binder holder, and in one of them the organisation named on the leak site is not the organisation whose systems held the data. The second is in the KEV table: the NetScaler command injection is reachable by anything the appliance logs, and the responder sequence is examine, patch, rotate, in that order, because the attacker took the configuration directory in at least one observed case.<sup>13</sup>

The standing measurement caution applies. 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 3 October 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.

44. ransomware.live, South Africa country page, cross-check only (showed 135 victims with LegalWise, Edcon and bcx.co.za newest when read on 4 October 2026, agreeing with the API file). <https://www.ransomware.live/country/ZA>

## 7. OSINT EXPOSURE & ATTACK SURFACE

### 7.1 The Panel: VERIFIED South African Exposure Counts

Every figure in this section is an exposure count of a product family in South Africa, retrieved at 02:01 UTC on 4 October 2026, and none is a count of vulnerable systems; the version and vuln filters are not available on this plan, and rescan noise has moved single counts by more than 70 per cent inside a day, so week-on-week movement is not reported as a finding.<sup>15</sup> Only queries whose product facet corroborates the fingerprint are published. This week's additions are served by one panel query. Citrix Netscaler, by product match with the lowercase s that Shodan uses: 122 instances, 107 of them on 443, which is the population for both zero-days and for the September authentication bypass. The rest of the panel: MikroTik RouterOS 4,938 (4,007 on the API port 8728, 300 on 19999, 206 on 8333); FortiGate 2,700 (1,442 on 10443, 560 on 541); Cisco ASA WebVPN 382 (337 on 443); Microsoft SharePoint on-prem by http.component 826; WordPress by http.component 402, a floor; Apache Tomcat 869; Remote Desktop on 3389, 8,228; services on port 445, 5,537, of which only 167 carry a Samba label in the product facet; the SonicWall family 2,960 across five product strings, which cannot be narrowed to the SMA 1000 line; ownCloud 158; Metabase 125; MLflow 100; Ray 76; Langflow 69; Gitea 9; VMware vCenter 2; Artifactory 2.

**Held and omitted.** Four of this week's seven additions have no Shodan product label and were held by the discovery stage: Zammad, FortiMail, Catalyst SD-WAN Manager and Apple's operating systems, the last of which is an endpoint rather than a measurable service. The collector's free-text probes return hits for the other three but no product facet corroborates them, so under evidence rule 2 none is published. Check Point, F5 APM, WSO2, Adobe Commerce and Zyxel remain held from prior weeks; VeloCloud returns zero by two methods and stays PROVISIONAL. LiteLLM at 6,891 and ScreenConnect at 2,652 are again not published as exposure figures, being artefacts for a fifth week: their top five ports carry eight, seven, seven, six and six instances and three, three, two, two and two respectively, against 4,007 on one port for MikroTik; the collector's port-concentration test is still not implemented. Langflow, MLflow and Ray are printed with the W40 caveat that they show the same scatter at small totals.<sup>15</sup> The KPI row counts two of seven adds with a published figure, the NetScaler pair.

### 7.2 Credential Exposure Around the Week's Victims

The aggregator's infostealer panels for the week's three listings are, in order of size: bcx.co.za, 20,242 passwords of which 1,983 are marked critical, 152 employees and 61 users with stealer-log records, 268 third-party employee credentials and 89 external attack-surface findings; Edcon, 8,271 passwords (311 critical), five employees, 24 users and thirteen third-party credentials; LegalWise, 162 passwords (two critical), three users and one third-party credential.<sup>4,10,9</sup> These are third-party stealer-log counts of unknown age and they do not say how any intrusion began. The BCX figure is presented for one reason: an IT services company with 152 staff credentials in stealer logs is a company whose customers' administrative sessions are in those logs too, and a customer that has not rotated the credentials BCX staff use into its environment this quarter should.

## 7.3 What a NetScaler Compromise Exposes

The 122 South African NetScaler instances are a count of exposure. What the week's reporting adds is what an attacker gets from one: Rapid7 watched the command injection archive /flash/nsconfig, which holds ns.conf with the encrypted administrator and LDAP, RADIUS and TACACS bind passwords, the TLS certificates and private keys, the SSH host keys and the high-availability settings; GTIG's SLAPSHOT daemon then uses the appliance as a bridge into the network behind it.<sup>13,12</sup> The appliance is, by design, the thing that authenticates users and terminates TLS for the organisation, which is why the rotation list in Section 1 is longer than the patch.

## 8. REGULATORY & POLICY

### 8.1 The Binder Holder Files: Where the MIP Cascade Reached This Week

Guardrisk's statements of 28 and 30 September add one reported filing to the notification record of the MIP breach: a section 22 notification by CoverCubed, the binder holder, to the Information Regulator, with notice to the roughly 6,000 affected policyholders, as Guardrisk describes it.<sup>7,8</sup> Set against the regulator's 25 September position that it had received only MIP's notification for a breach touching about 45 insurers, the record now holds MIP's filing, Bidvest Bank's in the RelyComply case and CoverCubed's in this one.<sup>33,27</sup> Guardrisk's further position, that accountability rests with the binder holder, is the insurer's reading of the binder agreement and of POPIA's responsible-party test; a binder holder that collects and administers policy data under its own licence can be the responsible party for that data, and the point is that the duty followed the data to the party that processed it, which is the outcome the regulator's September statement described. For a compliance officer at any insurer the practical reading is that every binder agreement and every outsourcing agreement should say, in a clause, which party notifies under section 22 for which processing, because the MIP cascade has now reached an insurer through an intermediary rather than through the insurer's own contract with MIP.

### 8.2 Procurement as Disclosure: The ATNS Request for Quotation

ATNS disclosed the operational technology compromise in a tender document, with a spokesperson's confirmation after a newspaper found it, and the insider workstream concerns personal information.<sup>1,2</sup> Two regulatory threads follow. The first is section 22 of POPIA, which puts a duty on the responsible party to notify the regulator and the data subjects where there are reasonable grounds to believe personal information has been accessed; the RFQ's own words are that the internal investigation could not substantiate the allegations, and no notice has been located, so the question stays open rather than answered. The second is the absence of any sector obligation on an air navigation provider to disclose a cyber incident publicly: the Cybercrimes Act's section 54 duty runs to SAPS, the Critical Infrastructure Protection Act runs to the minister, and neither reaches the travelling public, which is why the first account was written for bidders. A board that runs infrastructure should assume that its procurement documents will be read as disclosures and draft them accordingly.

## 8.3 The Opt-Out Registry: NCC Draft Guidelines

The National Consumer Commission gazetted draft guidelines for the national consumer opt-out registry under section 11 of the Consumer Protection Act, with fifteen days for comment from publication, as reported by BusinessTech on 2 October and MyBroadband on 3 October. The draft requires every direct marketer, which it defines to include insurers, financial institutions, retailers, telemarketing firms and call centres, to register before marketing and to renew annually; to cleanse its databases against the registry's pre-emptive blocks at R0.12 per name, with a cleansed list valid for 30 days; and it provides for compliance notices, referral to the National Consumer Tribunal, administrative penalties of up to R1 million or ten per cent of annual turnover, and on conviction a fine or imprisonment of up to twelve months. Consumers may block calls, messages, email, post or all of them. The Commission's own figure is 17.5 billion spam calls in the first half of 2026, about two-thirds of them sales calls. Fundraising calls count as direct marketing and so fall under the registry; soliciting votes does not.<sup>45,46</sup> The registry is not yet live. For an organisation that markets by telephone the consequence is a new third party that will receive a copy of its marketing database every 30 days, which is processing under POPIA and needs an operator agreement. The comment window closes in the week of 16 October.

## 8.4 Identity Documents: The Green ID Book's End Date and a Digital ID Demonstration

Home Affairs announced on 1 October that production of the green barcoded ID book ends on 31 March 2027 and that the book ceases to be valid on 31 March 2028, with the minister describing it as one of the most defrauded documents on the continent.<sup>47</sup> The same day the minister demonstrated a digital ID prototype in the MyMzansi app, a remote verification tool tied to biometrics in which the holder chooses which fields to share and can see every access; the department's plan puts hosting infrastructure at 31 March 2027 and citizen issuance in the 2027/28 financial year, and adoption will be voluntary.<sup>48</sup> For KYC and FICA functions two dates matter: a green book presented after 31 March 2028 is not an identity document, so onboarding systems that accept a photographed green book need a retirement plan before then; and the digital ID, when it arrives, is a verification query against the population register rather than a document image, a copy of which is what the MIP and RelyComply breaches yielded.

## 8.5 Fraud Advisories, the Regulator's Record and Who to Call

SARS issued no new scam alert in the window; the newest remains SARS-SCAM-400 of 2 September, the High Court summons lure.<sup>49</sup> Kaspersky warned, as MyBroadband reported on 2 October, of fraudulent iPhone 18 Pro pre-order and discount sites in several languages that collect names, phone numbers, WhatsApp details and card data against a recommended price of R28,799 for the 256 GB model; the defence is the standing one, buy from the named official channels and use a virtual card.<sup>50</sup> The Information Regulator's enforcement register and media-statements page were checked on 4 October and carry nothing later than 10 June and 2 June; the KPI row is retired as W40 said, and the MIP, RelyComply and Gauteng e-Panic matters, and on Guardrisk's account CoverCubed's, are all before the regulator with no public instrument on any of them.<sup>21,22</sup> No parliamentary committee meeting on cyber matters was located for the week by this collection.

**Who to call.** The six South African incident response teams in the FIRST directory are unchanged in the feed: the Cybersecurity Hub (kpillay@cybersecurityhub.gov.za) for government and the private and public sectors, ECS-CSIRT at the State Security Agency (ecs-csirt@ssa.gov.za) for government and the military, SA NREN CSIRT and UCT CSIRT for research and education, and the Standard Bank Group and Vodacom teams for their own constituencies.<sup>51</sup> For a state-owned operator in ATNS's position the Cybersecurity Hub and ECS-CSIRT are the two national teams, and the three clocks set out in W40 for regulated financial institutions (24 hours to the Prudential Authority under Joint Standard 2, 72 hours to SAPS under section 54, as soon as reasonably possible to the Information Regulator under section 22) apply to LegalWise and LEZA if the listing proves true.<sup>33</sup>

45. BusinessTech, End of an era for spam calls in South Africa, with a big catch for political parties and charities (2 October 2026). <https://businessstech.co.za/news/government/877986/say-goodbye-to-spam-calls-in-south-africa-with-a-big-catch-for-political-parties-and-charities/>

46. MyBroadband, One year in prison for people who will not stop spam calling in South Africa, by Myles Illidge (3 October 2026). <https://mybroadband.co.za/news/cellular/670370-one-year-in-prison-for-serial-spam-callers-in-south-africa.html>

47. TechCentral, Home affairs pulls the plug on the green ID book, by Duncan McLeod (1 October 2026). <https://techcentral.co.za/home-affairs-green-id-book-phase-out/286748/>

48. TechCentral, South Africa's digital ID is here, but you can't have it yet, by Fanie van Rooyen (1 October 2026). <https://techcentral.co.za/south-africa-digital-id-schreiber-demo/286764/>

49. SARS, Scams and phishing page, checked 4 October 2026 (newest alert SARS-SCAM-400, 2 September 2026). <https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>

50. MyBroadband, iPhone 18 Pro scammers are trying to steal people's bank details, by Hanno Labuschagne, on Kaspersky's warning (2 October 2026). <https://mybroadband.co.za/news/security/669482-iphone-18-pro-scammers-are-trying-to-steal-peoples-bank-details.html>

51. ransomware.live API, GET /csirt/ZA, six South African CSIRTs from the FIRST directory, retrieved 4 October 2026 (feeds/r1\_csirt\_zs\_2026-10-04.json). <https://api.ransomware.live/v2/csirt/ZA>

## 9. WEEKLY THREAT HUNT & IOCs

Eight missions. Three P1 cover the week's edge entries with vendor or responder indicators: the NetScaler pair with Mandiant's, Rapid7's and watchTowr's artefacts, the Catalyst SD-WAN Manager with Cisco's two log paths, and FortiMail with Fortinet's addresses and log patterns. Three P2 cover INC Ransom in the light of the BCX listing, the Zimbra command injection that Microsoft documented, and the SharePoint population in the light of Warlock. Two P3 cover the Zammad chain and the Apple fleet. Indicators come from vendor advisories, named responder reporting and the aggregator's per-group feeds, and the atomic detail is exported to iocs\_w41.csv rather than repeated in full here.<sup>35</sup> The Gentlemen's hashes are unchanged since W39 and TH-2026-W40-06 stands as written; the W40 Check Point, F5, MikroTik and PAYLOAD missions likewise stand and are not reprinted.

## TH-2026-W41-01: NetScaler: WHIPSHOT Web Shell, SLAPSHOT Tunnel and the Configuration Theft

P1 CRITICAL: both exploited before disclosure;  
122 exposed in ZA; overdue since 30  
September

**Hypothesis:** An attacker has executed code as root on a NetScaler ADC or Gateway through the default-configuration command injection CVE-2026-88771 or the DTLS overflow CVE-2026-88772, installed a PHP web shell under the VPN scripts directory with an httpd.conf handler for .deb or .sig files, started a Python tunnelling daemon bound to localhost, set the SUID bit on /bin/sh, and archived /flash/nsconfig for its keys and bind credentials.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1548.001 (Setuid and Setgid), T1070.004 (File Deletion / log scrubbing), T1090.001 (Internal Proxy), T1005 (Data from Local System), T1552.004 (Private Keys).

**IOCs:** httpd.conf directives AddHandler application/x-httpd-php .deb or .sig, php\_flag engine on, AliasMatch ^/vpn/media/(.+).ico\$ to /var/netscaler/gui/vpn/scripts/linux/\$1.sig; files nsginstaller[0-9].deb, nsginstaller[0-9].sig, e6ee7c85.sig in /var/netscaler/gui/vpn/scripts/linux/; request headers HTTP\_NSC\_LDAP, HTTP\_NSC\_CLIENTTYPE, HTTP\_X\_UX and HTTP\_X\_UX\_[0-9]+; URI /vpn/media/\*.ico returning 404 with a body over 5,000 bytes; /tmp/.uxdport and /tmp/.uxdlock; /bin/sh with mode -rwsr-xr-x; /netscaler/nsshutdown -R and /bin/httpd -k restart in /var/log/sh.log; ns.log SSL\_HANDSHAKE\_FAILURE with ClientVersion DTLSv1.0 and Reason Handshake failure-Internal Error; /var/log/messages NSPPE exit with orphan rings and pitboss NOT restarting NSPPE; addresses 143.198.7.94 (scanning and staging) and 157.254.167.12 (installation) (GTIG). Command tar czf /var/netscaler/gui/vpn/c -C /flash nsconfig; web shell /var/netscaler/logon/LogonPoint/custom/.ctxs.receiver, SHA-256 ed082f744f035035900f67edf438f2f7d0528ac501234f63d476d65273cdb9a1 (Rapid7). Log strings AAAD API: sending login req to aaad for and process\_kernel\_socket: call to authenticate user carrying shell metacharacters (watchTower). Fixed 14.1-73.37, 13.1-64.23, 13.1-FIPS 13.1.37.279.

**Data Sources:** Appliance shell (Expert mode) for /etc/httpd.conf, the four script directories, /tmp and /bin/sh; ns.log and /var/log/messages via syslog; /var/log/httpaccess.log and httperror; /var/log/sh.log; netflow from NSIP and SNIP; upstream firewall logs for UDP/443; the Citrix IOC scanner.

**Detection Guidance:** Run the five GTIG greps on Monday 5 October before any upgrade and preserve a VM snapshot: grep -En -i application/x-httpd-php|php\_flag|AliasMatch /etc/httpd.conf; file the scripts/linux, vista and mac directories and the vpn/media directory and look for ASCII text or PHP script; grep -rIE for <?php, eval(, base64\_decode( or shell\_exec( under /var/netscaler/gui/ and /netscaler/ns\_gui/; ls -la /tmp/.uxd\*; ls -l /bin/sh; ps aux for python with .uxd or base64. Any hit is an incident and the appliance is isolated, HA sync disabled, and the keys and bind accounts rotated. Then upgrade. Where DTLS is not needed, disable it or block UDP/443 upstream. Load the four GTIG YARA rules (WHIPSHOT, SLAPSHOT, NetScaler PHP config, C2 headers) into file scanning. Treat the nsconfig archive as the worst case: rotate administrator, LDAP, RADIUS, TACACS, SNMP and NITRO credentials and reissue TLS and SSH keys on every appliance that was internet-facing and unpatched between 20 September and the day you patched.

**TH-2026-W41-02: Catalyst SD-WAN Manager: Encoded Requests to j\_security\_check****P1 CRITICAL:** vendor-confirmed active exploitation; no workaround; overdue since 3 October

**Hypothesis:** An unauthenticated attacker has sent an HTTP request with percent-encoded characters in the URI to a Catalyst SD-WAN Manager so that the authentication rule protecting a specific API endpoint did not match, and has reached the API with the privileges of the admin user through CVE-2026-76504.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1078.004 (Valid Accounts: Cloud or application admin), T1562 (Impair Defenses, through fabric policy changes), T1602 (Data from Configuration Repository).

**IOCs:** POST requests to j\_security\_check whose path or parameters carry percent-encoding such as %6a, in /var/log/nms/containers/service-proxy/serviceproxy-access.log and /var/log/nms/vmanage-server.log, from addresses outside the administrative allow-list; administrative API calls that follow such a request with no interactive login; configuration pushes, template changes or new users not tied to a change ticket. Fixed 20.9.10.1, 20.12.8.2, 20.15.6.1, 20.18.4.1, 26.1.2.1, 26.2.1 (Cisco).

**Data Sources:** The two Cisco log paths on the manager; manager audit log; the fabric's configuration change history; reverse proxy or firewall logs in front of the manager; netflow from the manager's management interface.

**Detection Guidance:** Grep both logs for j\_security\_check and filter for any percent sign in the request line, then join the source addresses against your administrators' known networks; a hit from anywhere else is an incident and the fabric's device templates and credentials are reviewed for changes since 1 September. Cisco offers no workaround: if the manager is reachable from the internet, put it behind a firewall rule limited to administrative addresses on Monday 5 October and upgrade in the same change. No South African population figure exists for this product; any organisation running it treats the hunt as P1.

**TH-2026-W41-03: FortiMail: Arbitrary File Write Through the IBE Path****P1 CRITICAL:** vendor says exploited in the wild; overdue since 4 October

**Hypothesis:** An unauthenticated attacker has sent crafted HTTP or HTTPS requests to a FortiMail appliance's identity-based encryption path, used path traversal with a null byte to write files outside the intended directory through CVE-2026-104286, and used the write to alter configuration or gain execution.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1505 (Server Software Component), T1565.001 (Stored Data Manipulation), T1114.002 (Remote Email Collection).

**IOCs:** Addresses 79.141.169.187 and 45.129.0.192; archive-account configuration changes logged with remote-ip 79.141.169.187; decryption failures citing invalid Base64 encoding; administrator logout events with no user-interface context; POST requests carrying ../ to any /ibe path (Fortinet FG-IR-26-175). Affected 8.0.0 to 8.0.1, 7.6.0 to 7.6.6, 7.4.0 to 7.4.8, all 7.2; fixed 8.0.2, 7.6.7, 7.4.9.

**Data Sources:** FortiMail event and admin logs, web access logs for the IBE and webmail interfaces, upstream WAF or reverse proxy logs, mail-flow logs for archive and forwarding rule changes.

**Detection Guidance:** Search the admin log for any archive-account change since 1 September and for logouts without a UI session; search the web logs for the two addresses and for ../ in POST bodies to /ibe. A hit means the appliance's archive and forwarding configuration is audited line by line, because an attacker who can write files on a mail gateway can copy mail. Disable IBE on Monday 5 October if the organisation does not use it, restrict webmail to trusted networks, and upgrade. No South African FortiMail figure exists; the FortiGate count does not describe this product.

**TH-2026-W41-04: INC Ransom: Encryptor Rule, Two Notes and the Service Provider Path****P2 HIGH:** BCX listed 29 September; seven SA listings; sourced hashes and YARA

**Hypothesis:** An INC Ransom affiliate with access to a South African IT services provider or one of its customers is running a scheduled task that launches an obfuscated PowerShell implant from C:\ProgramData, has returned after a lull with AnyDesk and a renamed driver-loading binary, is moving laterally with Impacket atexec, and will drop INC-README.txt followed by DATALEAK\_PRESS\_RELEASE.txt listing what was taken.

**MITRE ATT&CK:** T1053.005 (Scheduled Task), T1059.001 (PowerShell), T1219 (Remote Access Software), T1068 (Exploitation for Privilege Escalation, BYOVD), T1021.002 (SMB/Windows Admin Shares), T1490 (Inhibit System Recovery), T1486 (Data Encrypted for Impact).

**IOCs:** SHA-256 ef394149c8da3af730c37d550027df8639a3aaa6feacce60112461ae6955829 and 753207ad5e72ddc6b13889132e5de18836b1a2acf954443655fea82b430e4c99; addresses 213.176.114.6 and 178.20.41.208 (aggregator IOC feed). YARA rule Inc (rivitna) matching the encryptor's byte patterns and the double-hyphen switches lhd, ens and sup, and the strings delete shadow copies from, [+] Start encryption of and background-image.jpg (aggregator YARA feed). Scheduled task named from random dictionary words; driver HWAuidoOs2Ec.sys under a service named HwAudio; renamed Vicarius vRx binary; notes INC-README.txt and DATALEAK\_PRESS\_RELEASE.txt 53 minutes apart (Huntress, 21 September).

**Data Sources:** EDR file-hash and process telemetry, scheduled task creation events (4698) and service installs (7045), driver load events, AnyDesk installation and connection logs, SMB session logs on servers, egress to the two addresses.

**Detection Guidance:** Load the two hashes and the YARA rule into EDR and file scanning. Alert on any new scheduled task whose name is two or three English words with no vendor prefix, on a service named HwAudio or a driver with that file name, and on AnyDesk appearing on a host that has no remote-support role. Service providers should run this across the customer tenants they administer, and customers should ask their providers on Monday 5 October whether they have. The BCX listing is the actor's claim; the hunt stands on the group's record of seven South African listings in seventeen months.

## TH-2026-W41-05: Zimbra: SNMP-Path Command Injection and the zimlog Persistence Unit

P2 HIGH: Microsoft tracked multiple compromises; overdue +42; SA mail estates run Zimbra

**Hypothesis:** An attacker has sent a crafted SMTP request to a Zimbra server with the optional SNMP package enabled, injected a command through the swatchdog-to-snmpttrap path as the zimbra user (CVE-2026-73570), dropped JSP web shells, escalated through zmmailboxdmgr and PAM changes, harvested the preauth and auth-token keys, and staged mailboxes for exfiltration.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1548.003 (Sudo and Sudo Caching), T1552.001 (Credentials in Files), T1543.002 (Systemd Service), T1114.002 (Remote Email Collection), T1567.002 (Exfiltration to Cloud Storage).

**IOCs:** C2 domains transzimbra.linkpc.net and psklzim.abrdns.com; addresses 117.107.25.243, 192.255.193.111, 45.32.30.235, 193.42.40.135, 3.209.137.175; SHA-256  
 dee5af1c0f76b45d28bafd6e60c07bb8e391d98addf81ef8f13d073acdb3c48a (de.sh),  
 bf28f38122bf20d5fac969cc414daa6a890cdea872d389ca93d2092b6b7773cf (zimdown2),  
 b594a42b8f1c6f090327bb9a3361c2d3515537fb7ac8da6b9061b9a3f330e159 (zimclient2);  
 /etc/systemd/system/zimlog.service; /opt/zimbra/final.tar.gz; zmlocalconfig -s invocations; JSP files under the Jetty and mailboxd web roots; perl-spawned shells whose command line contains snmpttrap and shell metacharacters; AzCopy to Azure Blob Storage (Microsoft, 30 September). Fixed 10.1.20.

**Data Sources:** Zimbra mailbox and audit logs, process creation on the mail servers, systemd unit inventory, file integrity on the web roots and /opt/zimbra, DNS and egress logs, LDAP query logs.

**Detection Guidance:** Confirm whether zimbra-snmpt is installed; if it is and the server is below 10.1.20, treat it as possibly compromised and hunt before patching. Grep for snmpttrap in process histories, list JSP files modified since 20 July, diff systemd units against a clean build, look for final.tar.gz and for memfd execution. Rotate zimbraPreAuthKey and zimbraAuthTokenKey on any server that was exposed, because a copied key forges sessions after the patch. Block the two domains and five addresses at egress.

## TH-2026-W41-06: SharePoint On-Prem: Warlock's Tunnel Service and SYSVOL Staging

P2 HIGH: two overdue catalogue entries; 826 exposed in ZA; Warlock active in Portuguese-speaking countries, none named

**Hypothesis:** An attacker has entered through an unpatched on-prem SharePoint server (the 2025 ToolShell chain or CVE-2026-55040 with CVE-2026-65660), installed Visual Studio Code's tunnel as a service for command and control, run a tool that disables security software across dozens of hosts, and staged a ransomware payload in the domain's SYSVOL share.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1219 (Remote Access Software), T1562.001 (Disable or Modify Tools), T1574.002 (DLL Side-Loading), T1570 (Lateral Tool Transfer, via SYSVOL), T1486 (Data Encrypted for Impact).

**IOCs:** code-insiders.exe or code.exe installed as a Windows service or running a tunnel on a server; a burst of security-agent service stops across many hosts inside two hours; executables or scripts appearing under the domain SYSVOL policies folders; DLL side-loading from user-writable paths on domain controllers and servers (Symantec Threat Hunter Team, via The Record and Industrial Cyber, 2 October). Farm builds below 16.0.19725.20522, 16.0.10417.20198 or 16.0.5565.1001; the July and August ToolShell indicators still apply.

**Data Sources:** Service installation events (7045) and process creation on SharePoint front ends and domain controllers, EDR tamper and service-stop telemetry, SYSVOL file integrity, IIS and ULS logs, egress to the VS Code tunnel endpoints.

**Detection Guidance:** Alert on any VS Code binary installed as a service or spawning a tunnel on a server, which has no administrative use. Alert on more than a handful of security-agent service stops in one hour across the estate. Watch SYSVOL for any new executable. Confirm the August SharePoint builds on every front end and put internet-facing farms behind pre-authentication; 826 South African instances answer without it. Priority is P2 because no South African victim is named; a Mozambican or Angolan subsidiary raises it.

TH-2026-W41-07: Zammad: Session Fixation to Root in Seconds

P3 MEDIUM: exploited against DIVD; due on publication day; no SA population figure

**Hypothesis:** An attacker has fixed a session on an internet-facing Zammad helpdesk (CVE-2026-102489), executed code as the zammad user, escalated to root through CVE-2026-102490, and read the ticket store, which in a service provider holds customers' credentials, network diagrams and incident histories.

**MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1563 (Remote Service Session Hijacking), T1068 (Exploitation for Privilege Escalation), T1213 (Data from Information Repositories).

**IOCs:** Zammad versions below 7; shells, scripts or interpreters spawned by the zammad service user; sudo or setuid activity by that user; session identifiers reused across source addresses; outbound connections from the Zammad host that are not to mail or identity providers; scripted request sequences whose timing is machine-paced, which is how DIVD characterised the attacker (Infosecurity Magazine, 2 October).

**Data Sources:** Zammad application and web server logs, Linux auditd on the host, process creation, egress netflow.

**Detection Guidance:** If the helpdesk is below 7 and reachable from the internet, take it offline on Monday 5 October until it is upgraded, which is DIVD's own advice. Audit the zammad user's process history and sudo log for the period since 24 September. Treat the ticket database as sensitive data for section 22 purposes: a service provider's helpdesk holds its customers' secrets, and it is a supplier system that is rarely on the customer's asset list.

TH-2026-W41-08: Apple CoreGraphics: Fleet Compliance Against a Targeted Exploit

P3 MEDIUM: may have been exploited in targeted attacks per Apple; overdue +3; compliance item

**Hypothesis:** A targeted individual in the organisation, typically an executive, a journalist or a lawyer, has received a crafted file that exploits CVE-2026-86950 on an iPhone, iPad or Mac below the 28 September builds, giving the attacker code execution on the device.

**MITRE ATT&CK:** T1203 (Exploitation for Client Execution), T1566.001 (Spearphishing Attachment), T1430 (Location Tracking, mobile), T1636 (Protected User Data, mobile).

**IOCs:** Devices below iOS 26.7.1, iPadOS 26.7.1, macOS 26.7.1 or macOS 15.8.1; devices on unsupported older iOS trains, which Apple names as the exploited population; unexpected crash logs in CoreGraphics or image-rendering processes (The Hacker News on Apple's advisory, 28 September). No file hashes or infrastructure are public.

**Data Sources:** MDM inventory and compliance reports, Apple crash and diagnostic logs where collected, mail gateway attachment logs for the executive population.

**Detection Guidance:** Push the four builds through MDM on Monday 5 October and set a compliance deadline of Friday 9 October; report the exceptions by name. For the executive and legal population, enable Lockdown Mode where the role tolerates it, and treat any unexplained device crash in that group as a reason to image the device. This is a hygiene mission; it is in the list because the catalogue entry is overdue and because the exploited population is specifically the people whose devices hold the organisation's most sensitive conversations.

# 10. STRATEGIC RECOMMENDATIONS

## Technical (SOC / IR)

**1. Reverse the order of work on NetScaler: examine, patch, rotate.** The GTIG greps, the SUID check and the DTLS handshake log search take minutes and must precede the upgrade because the upgrade can remove the evidence; the rotation list follows because the attacker was seen taking the configuration directory.

Archive the pre-patch output with the change ticket.

**2. Run the SD-WAN Manager and FortiMail log checks on Monday 5 October and keep the output.** Cisco's two paths and Fortinet's two addresses and three log signatures are each the vendor's own definition of an attempt. A clean result dated before the patch is the evidence a regulator or an insurer will ask for later.

**3. Put the OT network's egress on the same monitoring as the corporate network's.** ATNS found the weather system's malware through network monitoring that saw traffic to foreign addresses. Any operator with a SCADA, weather, building-management or laboratory segment should be able to answer, for that segment, which external addresses it talked to in the past 90 days.

**4. Treat supplier helpdesks, ticketing and testing environments as in scope for your own detection.** The week's two supplier cases (BCX's test environment, DIVD's Zammad) and the W39 MIP Jira case are the same system class: the place where the supplier keeps your secrets and does not count as production. Ask for the supplier's log retention and alerting on those systems as well as on the ones that serve you.

**5. Rotate credentials that a service provider's staff use into your environment.** The BCX infostealer panel is third-party data of unknown age, and 152 employee credentials in stealer logs is reason enough to rotate every provider account, VPN certificate and jump-host credential issued to that provider this quarter, whether or not the listing is true.

## Management (CISO / Board)

**1. Decide this week how the organisation would disclose a cyber incident before a tender, a leak site or a journalist does it.** ATNS's first public account was a procurement document; BCX's customers read the actor's version before the company's. A one-page disclosure protocol, who signs, what it says, which regulators and customers are told and in what order, costs nothing and was missing in both cases.

**2. Map every binder holder, underwriting manager, administrator and intermediary that holds your customers' data, and ask each whether it was an MIP or RelyComply client, by Friday 9 October.** Guardrisk says a binder holder's 6,000 policies appear to sit in the MIP set, and the insurer's name was on a leak site before that was known. The regulator has said the duty follows the responsible party; the board's question is whether the organisation knows who that is for each book of business.

**3. Put a clause in every outsourcing and binder agreement that names the notifying party, the time limit and the form of notice for a supplier breach.** POPIA's section 22 says the operator notifies the responsible party immediately; the MIP, RelyComply, CoverCubed and BCX cases show that without a contractual clock and a named recipient the word carries no operational meaning.

**4. Keep the edge-appliance inventory on the risk register and add a column for the last compromise check.** The NetScaler pair joins the edge families added to the overdue column since 8 September, and Citrix's own description is reliable remote code execution against any vulnerable appliance regardless of configuration. The owner of the list should report by Friday 9 October which appliances were examined before they were patched.

**5. Plan the retirement of green ID book acceptance in onboarding and the response to the opt-out registry's comment window now.** The book ceases to be valid on 31 March 2028; the registry guidelines close for comment in the week of 16 October and will create a new 30-day data transfer for every organisation that markets by telephone. Both are data-protection decisions that will be made by default if

nobody is assigned to them.

## 11. THREAT LEVEL ASSESSMENT

### THREAT LEVEL: HIGH, 24th CONSECUTIVE WEEK

The South African cyber threat level remains HIGH for a twenty-fourth consecutive week (27 September to 3 October 2026). Escalation to CRITICAL was considered on the combination of operator-confirmed ransomware-linked malware in national air navigation operational technology, a default-configuration zero-day on an appliance class with 122 South African instances, and a 500 GB claim against the country's largest IT services company. It was rejected on the criterion applied since W35: ATNS reports containment and removal and no service disruption has been reported, no national-scale outage occurred, the BCX claim is unconfirmed, and no South African organisation has reported a NetScaler compromise. De-escalation to MEDIUM was not considered.

### Rationale

**Operational technology at a national infrastructure operator was compromised, by the operator's own account.** ATNS's RFQ describes ransomware-linked malware in an airport weather system with possible exfiltration abroad, and it was disclosed by a tender.

**Two of the week's named victims are supplier cases.** BCX is a supplier, and Guardrisk was named for data its binder holder held, which multiplies the number of South African responsible parties with a notification question this week beyond the number of names on the leak sites.

**A pre-authentication, default-configuration zero-day on NetScaler with documented post-exploitation tooling.** Exploited from 20 September, disclosed 27 September, overdue since 30 September, with 122 instances exposed in South Africa and vendor guidance to examine before patching.

**The Gentlemen's South African tempo did not slow.** Two further listings, both financial-sector names by licence or history, and, on Guardrisk's account, a second route for the MIP data into the sector.

### Next-Week Watch (W42)

**ATNS: scope, actor and the personal-information question.** The distinguishing observations are the award of the forensic contract, a Department of Transport or ATNS statement giving a detection date or naming a family, a leak-site listing for ATNS, and any section 22 notice arising from the insider workstream. Silence on all four by Friday 16 October leaves the item at the RFQ's scope.

**BCX: whether Telkom answers the listing.** A Telkom or BCX statement on the INC claim, a sample or data-published marker on the actor's page, or a municipal customer reporting that a named application is one it runs would each move the item. The applications named by the actor are the test: if they are products BCX sells, the claim and the test-environment scope can both be true.

**LegalWise and Edcon.** A LegalWise or LEZA statement, an MIP statement on whether LegalWise is a client, or a published sample in the Hollard record format would resolve the first; any statement from the Edcon business rescue practitioners would resolve the second. A leak timer appearing on either suggests a live negotiation.

**Whether the insurers have notified in their own names.** The W40 test stands: a second answer from the regulator, a statement from any of the roughly 45 that it filed, or a section 22 notice on an insurer's or binder holder's website. CoverCubed's filing, reported by Guardrisk, is the first such observation. Silence from the rest past Friday 9 October becomes a finding about practice.

**A South African NetScaler compromise.** The observation is a South African organisation reporting a NetScaler intrusion, or a leak-site listing whose victim is known to run one, in the fortnight after disclosure; its absence is not evidence, because the responder reports place victims only in North America and Europe so far.

**BlackLocks.** Carried one more week. If the group lists nothing further by Friday 16 October the W40 tempo question closes as unanswered; a fourth listing anywhere reopens it.

**Collector tasks.** The port-concentration test for auto-promoted Shodan queries, now five weeks outstanding; hand-built fingerprints for Check Point management, F5 APM, the two Cisco appliances, FortiMail, Catalyst SD-WAN Manager and Zammad; and the world-feed search for South African victims under other country tags, which this week's Ivorian record under the ZA tag shows is needed in both directions.

**Closed this week.** Rand Water, at the 3 October test, moves to the record. Guardrisk's own-estate question, answered by the company. The W40 Cisco email gateway and ISE item is carried in the KEV table without a separate watch line. Carried without re-argument: Cell C Fibre, Cartrack, VSB Attorneys, Rohloff, The Courier Guy, Babcock, the Furniture Bargaining Council claim, Toyota's SMS provider, Implats, Hungry Lion and the Gauteng e-Panic exposure.

## 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 4 October 2026, with the exceptions this note records: the CISA catalogue URL is the public location of a file read locally; the Sunday Times article is a premium article of which the opening text and the spokesperson's statement were readable; the Citrix security bulletin for CVE-2026-88771 to CVE-2026-88778 returned an access error to this collection and is not cited, its contents being taken from Rapid7's and GTIG's accounts of it; CISA's own alert pages for the week returned 403 and the catalogue file is cited instead; the ATNS tenders page returned 403 and the RFQ is cited through the three publications that read it; edcon.co.za could not be read because its certificate does not match the hostname. **Collection notes.** The feed run completed at 02:05 UTC on 4 October 2026 and passed its integrity check with exit status 0; the victim feed and catalogue figures it produced are stated in Sections 5 and 6. The RSS sweep read 57 of 72 feeds; the run log names fourteen failing three or more runs in succession: Daily Maverick, IOL, ITWeb's two feeds, News24, Polity, Engineering News, INTERPOL, Bishop Fox, Volexity, Cyble, Sansec, Blackpoint Cyber and Sophos; ITWeb was read by hand where cited. The world-feed search for South African victims under other country tags was not run; it remains a collector task. **Provenance of the machine-read feeds.** Every ransomware.live, NVD and EPSS figure in this report was retrieved from those services' APIs and the sources are cited as the

endpoints actually called; the rendered ransomware.live pages used, the South African country page and the four victim pages, are cited as cross-checks of records also present in the feed. **A correction.** This edition corrects W40's omission of the ATNS incident, which the Sunday Times reported on 26 September inside the W40 window; W40's count of one confirming organisation is corrected to two. The correction is recorded in Section 1 and the item is written up in Section 3.1. **A count revised.** INC Ransom's South African record is given as seven rather than the eight ZA-tagged records in the feed, because aircotedivoire.com is Ivorian by its own domain; prior editions' count of seven included it without noting that the domain is Ivorian. **Figures withheld or resolved.** LiteLLM (6,891) and ScreenConnect (2,652) are disclosed here but not published as exposure figures, being port-scatter artefacts for a fifth week; VeloCloud's zero is PROVISIONAL and unpublished; Zammad, FortiMail, Catalyst SD-WAN Manager, Check Point, F5 BIG-IP APM, WSO2, Adobe Commerce and Zyxel have no product label and are held, and Apple's operating systems are endpoints with no service to count. **Description conflicts recorded.** MyBroadband's headline on ATNS attributes the attack to China-linked hackers; the RFQ says possible exfiltration to addresses in China and names no actor, and the report follows the document. Dark Reading reads one RFQ airport code as Maputo where MyBroadband reads Mahikeng; the report follows MyBroadband and notes the difference. The catalogue's description of WSO2 CVE-2026-5430 still differs from the vendor's. **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; the compiler of this report is quoted in MyBroadband's 3 October article and that article is cited for its reporting of the companies' statements only. **Single-source disclosure.** The ATNS RFQ text rests on three publications reading the same document; the Guardrisk statement on ITWeb and MyBroadband; the Zammad attack on Infosecurity Magazine's account of DIVD's disclosure; the Warlock cases on The Record's and Industrial Cyber's accounts of Symantec; the opt-out registry on BusinessTech and MyBroadband; the Zimbra tracking on Microsoft alone; the NetScaler first-attempt date and nsconfig theft on Rapid7 alone. **Claims deliberately excluded.** The BCX, LegalWise and Edcon listings are carried as claims only. The aggregator's infostealer counts are third-party telemetry of unknown age. INC Ransom's 500 GB and DireWolf's 200 GB are attacker figures. No actor is attributed to ATNS. The agentic-AI characterisation of the Zammad attack is DIVD's reading of the attacker's scripts and is reported as such. The inference that INC's disclosures path means a concluded negotiation is marked as an inference.

1. Sunday Times (TimesLIVE), Air traffic agency probes cyberattack, by Kabelo Khumalo (26 September 2026; premium article, the opening text and the ATNS spokesperson's statement were readable to this collection). <https://www.sundaytimes.livestock.co.za/business/news/2026-09-26-air-traffic-agency-probes-cyberattack/>
2. MyBroadband, China-linked hackers attacked South Africa's air traffic control system, by Luis Monzon (2 October 2026). <https://mybroadband.co.za/news/security/670359-china-linked-hackers-attacked-south-africas-air-traffic-control-system.html>
3. Dark Reading, South Africa seeks help after cyberattack targets air traffic control, by Robert Lemos (30 September 2026). <https://www.darkreading.com/cyberattacks-data-breaches/south-africa-help-cyberattack-air-traffic-control>
4. ransomware.live, victim page for bcx.co.za (INC Ransom), discovered 29 September 2026 12:32 UTC, post dated 29 September 2026, 500 GB claimed, retrieved 4 October 2026; the same record is in the locally retrieved country feed; the infostealer panel figures of the three victim pages are stored as evidence/w41\_ransomwarelive\_victim\_panels\_2026-10-04.md. <https://ransomware.live/id/YmN4LmNvLnphQGluY3JhbnNvbQ==>
5. MyBroadband, Telkom discloses BCX cybersecurity incident which was limited to legacy testing environment (25 September 2026). <https://mybroadband.co.za/news/security/669235-telkom-discloses-bcx-cybersecurity-incident-which-was-limited-to-legacy-testing-environment.html>
6. BCX, corporate website, checked 4 October 2026 (no notice, banner or statement on any incident; the /news/ path returns 404). <https://www.bcx.co.za/>
7. ITWeb, Guardrisk distances itself from MIP cyber breach, by Admire Moyo (28 September 2026). <https://www.itweb.co.za/article/guardrisk-distances-itself-from-mip-cyber-breach/DZQ58MV8B1pvzXy2>
8. MyBroadband, Momentum Group company responds to data breach claims, by Luis Monzon (30 September 2026). <https://mybroadband.co.za/news/security/669576-momentum-group-company-responds-to-data-breach-claims.html>
9. ransomware.live, victim page for LegalWise (The Gentlemen), discovered 30 September 2026 03:40 UTC, estimated attack date 29 September 2026, retrieved 4 October 2026. <https://ransomware.live/id/TGVnYWxXaXNIQHROZWdlbnRsZWl1bG==>
10. ransomware.live, victim page for Edcon (The Gentlemen), discovered 30 September 2026 03:40 UTC, estimated attack date 29 September 2026, retrieved 4 October 2026. <https://ransomware.live/id/RWRjb25AdGh1Z2VudGxlbWVv>
11. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.10.02, released 2 October 2026 15:19 UTC, retrieved 4 October 2026 (feeds/kev\_2026-10-04.json). <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

12. Google Threat Intelligence Group and Mandiant, Defending against active exploitation of Citrix NetScaler ADC and Gateway appliances (29 September 2026). <https://cloud.google.com/blog/topics/threat-intelligence/defending-against-active-exploitation-of-citrix-netscaler-adc-and-gateway-appliances/>
13. Rapid7, Zero-day exploitation of Citrix NetScaler ADC and Gateway: CVE-2026-88771 and CVE-2026-88772 (28 September 2026, updated 30 September 2026). <https://www.rapid7.com/blog/post/etr-zero-day-exploitation-of-citrix-netscaler-adc-and-gateway-cve-2026-88771-and-cve-2026-88772>
14. The Register, Custom malware used in Citrix 0-day attacks targeting govt, banks, professional services, by Jessica Lyons (29 September 2026). <https://www.theregister.com/security/2026/09/29/custom-malware-used-in-citrix-0-day-attacks-targeting-govt-banks-professional-services/5299867>
15. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:01 UTC 4 October 2026 (feeds/shodan\_za\_2026-10-04.json). <https://www.shodan.io/search?query=country%3AZA>
16. Cisco, Security advisory cisco-sa-sdwan-webauth-xr8beuuU, Cisco Catalyst SD-WAN Manager API authentication bypass vulnerability, CVE-2026-76504 (published 30 September 2026, updated 2 October 2026). <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU>
17. Fortinet PSIRT, FG-IR-26-175, FortiMail path traversal and null-byte handling, CVE-2026-104286 (published 1 October 2026). <https://fortiguard.fortinet.com/psirt/FG-IR-26-175>
18. The Hacker News, Apple patches CoreGraphics flaw possibly exploited in targeted attacks, CVE-2026-86950 (28 September 2026). <https://thehackernews.com/2026/09/apple-patches-coregraphics-flaw.html>
19. Infosecurity Magazine, Two zero-days exploited in attack on Dutch Institute for Vulnerability Disclosure (2 October 2026). <https://www.infosecurity-magazine.com/news/zerodays-dutch-institute/>
20. ransomware.live API, GET /v2/countryvictims/ZA, 135 records, za\_records 135 against server\_returned 135, filter purity 1.0, FREE v2 tier (delayed relative to PRO), retrieved 02:00 UTC 4 October 2026 and stored as feeds/ransomwarelive\_za\_2026-10-04.json. <https://api.ransomware.live/v2/countryvictims/ZA>
21. Information Regulator, Enforcement notices register, checked 4 October 2026 (newest entry Gauteng Department of Health, 10 June 2026). <https://infoeregulator.org.za/enforcement-notices/>
22. Information Regulator, Media statements page, checked 4 October 2026 (2026 tab rendered; newest statement 2 June 2026; the media invitation of 27 August 2026 recorded in W39 is an invitation and did not render on this read). <https://infoeregulator.org.za/media-statements/>
23. The Citizen, Edcon files for voluntary business rescue (29 April 2020; business rescue practitioners Piers Marsden and Lance Schapiro). <https://www.citizen.co.za/business/edcon-files-for-voluntary-business-rescue/>
24. The Record, Warlock ransomware used in attacks on critical infrastructure in Portuguese, Spanish-speaking countries, on Symantec Threat Hunter Team reporting (2 October 2026). <https://therecord.media/warlock-ransomware-used-in-critical-infrastructure-attacks>
25. ransomware.live, victim page for Guardrisk (The Gentlemen), discovered 26 September 2026 08:48 UTC, re-read 4 October 2026. <https://ransomware.live/id/R3VhcmRyaXNrQHRoZWdlbnRsZWllbg==>
26. MyBroadband, Insurance industry in South Africa under attack and customers are the victims, by Luis Monzon (3 October 2026). <https://mybroadband.co.za/news/security/669782-insurance-industry-in-south-africa-under-attack-and-customers-are-the-victims.html>
27. Bidvest Bank, Notification of a Security Compromise in terms of Section 22 of POPIA: RelyComply cyber incident (notice dated 17 September 2026; text stored in W40 as evidence/w40\_bidvestbank\_important\_notice\_2026-09-27.txt). <https://www.bidvestbank.co.za/important-notice>
28. LegalWise, corporate website, checked 4 October 2026 (no notice or statement on any incident; names LegalWise South Africa (RF) (Pty) Ltd and the insurer Legal Expenses Insurance Southern Africa Limited, LEZA). <https://www.legalwise.co.za/>
29. Investec, Sithega transaction page (Sithega acquired 62 per cent of Legal Expenses Group Africa, LEGA, with Hollard retaining 38 per cent; 2023), checked 4 October 2026. [https://www.investec.com/en\\_za/investec-for-corporates/transactions/sithega-2023.html](https://www.investec.com/en_za/investec-for-corporates/transactions/sithega-2023.html)
30. ransomware.live API, GET /groups, 403 groups with victim counts, retrieved 4 October 2026 and compared with the 27 September retrieval (feeds/r1\_groups\_2026-10-04.json). <https://api.ransomware.live/v2/groups>
31. Rand Water, corporate website, checked 4 October 2026 (no statement on the incident; consumption data, tariff consultations and a hotline only). <https://www.randwater.co.za/>
32. RelyComply, RelyComply cyber incident: what happened and what you can do, official notice (published 16 September 2026; re-read 4 October 2026, page still reads last updated 16 September 2026). <https://relycomply.com/relycomply-cyber-incident-what-happened-and-what-you-can-do/>
33. TechCentral, Insurers carry the can for MIP breach, regulators say (25 September 2026). <https://techcentral.co.za/insurers-mip-breach-regulators/286482/>
34. KELA, Inside The Gentlemen leak: how a new RaaS captured 10 per cent of 2026's global ransomware victims (14 May 2026). <https://www.kelacyber.com/blog/the-gentlemen-ransomware-internal-chat-leak-analysis-2026/>
35. ransomware.live API, GET /iocs/[group] for the groups active against South Africa in the last 120 days, retrieved 4 October 2026 (feeds/r1\_iocs\_2026-10-04.json). <https://api.ransomware.live/v2/iocs/incransom>
36. ransomware.live API, GET /yara/[group], retrieved 4 October 2026 (feeds/r1\_yara\_2026-10-04.json; the INC rule is rivitna's Inc.yar). <https://api.ransomware.live/v2/yara/incransom>
37. Huntress, The tale of two INC Ransom notes: a ransomware timeline (21 September 2026). <https://www.huntress.com/blog/two-inc-ransom-notes>
38. watchTowr Labs, Oh look, the foot gun went off again: Citrix NetScaler pre-auth command injection CVE-2026-88771 (28 September 2026). <https://labs.watchtowr.com/oh-look-the-foot-gun-went-off-again-citrix-netscaler-preauth-command-injection-cve-2026-88771/>
39. Industrial Cyber, report on Symantec Threat Hunter Team's Warlock findings: water, telecom and government targets reached through SharePoint flaws (2 October 2026). <https://industrialcyber.co/ransomware/symantec-reports-warlock-ransomware-group-targets-water-telecom-government-organizations-through-sharepoint-flaws/>
40. NIST NVD, CVE API 2.0, CVSS base scores with scoring source for the 62 catalogue entries added in the last 45 days, retrieved 4 October 2026 (feeds/nvd\_cvss\_2026-10-04.json). <https://services.nvd.nist.gov/rest/json/cves/2.0>
41. Microsoft Threat Intelligence, Unauthenticated command injection on internet-facing mail servers: tracking CVE-2026-73570 (30 September 2026). <https://www.microsoft.com/en-us/security/blog/2026/09/30/unauthenticated-command-injection-on-internet-facing-mail-servers-tracking-cve-2026-73570/>
42. FIRST, EPSS API, scores for the same 62 entries, retrieved 4 October 2026 (feeds/epss\_2026-10-04.json). <https://api.first.org/data/v1/epss>
43. Microsoft MSRC, CVE-2026-65660, Microsoft SharePoint Server remote code execution vulnerability (released 11 August 2026, revision 1.2 of 25 September 2026; the fixed builds cited in TH-06 and iocs\_w41.csv). <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65660>

44. ransomware.live, South Africa country page, cross-check only (showed 135 victims with LegalWise, Edcon and bcx.co.za newest when read on 4 October 2026, agreeing with the API file). <https://www.ransomware.live/country/ZA>
45. BusinessTech, End of an era for spam calls in South Africa, with a big catch for political parties and charities (2 October 2026). <https://business.tech.co.za/news/government/877986/say-goodbye-to-spam-calls-in-south-africa-with-a-big-catch-for-political-parties-and-charities/>
46. MyBroadband, One year in prison for people who will not stop spam calling in South Africa, by Myles Illidge (3 October 2026). <https://mybroadband.co.za/news/cellular/670370-one-year-in-prison-for-serial-spam-callers-in-south-africa.html>
47. TechCentral, Home affairs pulls the plug on the green ID book, by Duncan McLeod (1 October 2026). <https://techcentral.co.za/home-affairs-green-id-book-phase-out/286748/>
48. TechCentral, South Africa's digital ID is here, but you can't have it yet, by Fanie van Rooyen (1 October 2026). <https://techcentral.co.za/south-africa-digital-id-schreiber-demo/286764/>
49. SARS, Scams and phishing page, checked 4 October 2026 (newest alert SARS-SCAM-400, 2 September 2026). <https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>
50. MyBroadband, iPhone 18 Pro scammers are trying to steal people's bank details, by Hanno Labuschagne, on Kaspersky's warning (2 October 2026). <https://mybroadband.co.za/news/security/669482-iphone-18-pro-scammers-are-trying-to-steal-peoples-bank-details.html>
51. ransomware.live API, GET /csirt/ZA, six South African CSIRTs from the FIRST directory, retrieved 4 October 2026 (feeds/r1\_csirt\_za\_2026-10-04.json). <https://api.ransomware.live/v2/csirt/ZA>

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