



SOUTH AFRICA

CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief, Week 43 | 11 October – 17 October 2026

THREAT LEVEL: HIGH

TLP: CLEAR

Report ID: SA-CTI-2026-W43 | Classification: TLP: CLEAR

Published Monday 19 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 (W43)
- 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, 26th consecutive week (11 October - 17 October 2026)

Story 1. Ampath, one of the country's largest pathology laboratory groups, confirmed a cyber incident it detected on Friday 2 October and issued a notice under section 22 of POPIA on Tuesday 13 October, naming the criminal actor ByteToBreach and listing names, identity numbers, dates of birth, contact details, medical scheme names and membership numbers and payment records as the data that may have been taken.^{1,2} The actor's forum post of 13 October claims ten of about 375 databases and an admissions table of more than 80 million rows; Ampath's answer of 14 October is that the figure counts database records, that one patient generates many over years, and that it has found no evidence that test results, diagnoses or banking details were taken.^{3,4} Rated CONFIRMED for the incident on the company's own notice; the 80 million figure and the database count are the actor's and are not adopted. Ampath has not given a count of individuals.

Story 2. The Gentlemen listed Europ Assistance South Africa, which the aggregator describes as a Roodepoort emergency-assistance and insurance-administration company, at 09:31 UTC on Friday 16 October, one of 33 organisations the group indexed that day in a batch that also carried MoneyGram, KFC and Confluent; its index rose by 42 in the week to 1,002.^{5,6,7} Microsoft's Digital Defense Report, published in the same week, counts seventeen South African ransomware cases in the year to June against seven the year before, places The Gentlemen fourth on leak-site volume with six per cent of postings, and cautions that the group's leak-site activity may be pushed to attract attention because it is a far smaller share of Microsoft's own telemetry.⁸ Deadlock, a group with 107 listings since June, took its second South African name on Monday 12 October: Aeroklas Duys, an automotive accessories manufacturer that the aggregator describes as a joint venture of the Duys Engineering Group and Thailand's Aeroklas.^{9,10} Both listings are CLAIMED; neither company has published anything and no South African outlet had carried either by Saturday 17 October.

Story 3. CISA added nine vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue between Tuesday 13 and Friday 16 October, and seven were past their three-day deadline on Monday 19 October.¹¹ Four sit on the network edge. Two were exploited before a fix existed and a third has exploitation the vendor has observed: Ivanti Connect Secure CVE-2026-104935, an authentication bypass Volexity saw a criminal actor chain to root from 3 October, with an integrity checker that CISA says may not detect it; Cisco Secure Email Gateway CVE-2026-76519, a root file write triggered by an email attachment and the second Secure Email Gateway entry in five weeks; and PAN-OS CVE-2026-0322, code execution by an authenticated user of the management interface.^{12,13,14} The fourth, a Fortinet CLI path traversal, needs an administrator session. The other five are a Windows Mark of the Web bypass from Microsoft's record 1,411-fix patch day, an Atlassian file-read flaw across eight Data Center products, a BeyondTrust Remote Support bypass and an AhsayCBS backup-console pair being used to mine cryptocurrency.^{15,16,17} The SonicWall SMA 1000 flaw flagged in W42 is still absent from the catalogue after 135 recorded exploitation attempts.¹⁸

W43 CORRECTIONS TO PRIOR EDITIONS, two items. **First**, W40, W41 and W42 printed a SonicWall family exposure figure for South Africa of 2,912, 2,960 and 2,965, described as the sum of five Shodan product

strings. The sum was wrong in two ways that this week's facet data makes plain. The generic string, product:SonicWall, already contains the Dell SonicWALL, SSL-VPN and firewall-config strings in its own facet, so adding them counted those appliances twice; and the string SonicWALL, Inc., which contributed 1,808 to W42's sum and reads 1,974 this week, resolves in its facet to Juniper, Fortinet, Alcatel-Lucent and Aruba devices alongside SonicWall ones, with 741 of them answering on the SNMP port 161. It is a vendor banner, not a product fingerprint, and it fails the corroboration test the evidence rules require.¹⁹ The family figure is withdrawn. The SonicWall exposure figure this edition carries is the product:SonicWall count alone, 1,206 instances on 18 October, whose facet is 99 per cent SonicWall strings; the prior family figures should be read as overstated by roughly a factor of two and a half. No conclusion in those editions rested on the family total. **Second**, W42 stated that The Gentlemen's indicator feed was byte-identical to the 27 September retrieval. It was not: the 11 October retrieval carried seven addresses and a second Session identifier that appear in no retrieval from 6 September to 4 October, so the statement was wrong at publication and the W40 hunt mission built on the feed, TH-2026-W40-06, lacked those rows. They are exported this week in TH-2026-W43-06 and iocs_w43.csv.²⁰ Both corrections are counted in the KPI row and recorded in Section 12.

KPI Dashboard

Metric	Current (W43)	Prior (W42)	Change	Direction
Overall SA threat level	HIGH	HIGH	No change (26th week)	FLAT
ransomware.live SA cumulative	138	136	+2	UP
SA claims discovered inside the window (ZA tag; all passed the nationality check)	2	1	+1	UP
SA victims found under another country tag (hand search of active groups' pages)	0	0	0	FLAT
SA organisations confirming a breach or exposure in the window	2	0	+2	UP
New CISA KEV additions	9	6	+3	UP
KEV adds already overdue at publication	7 of 9	6 of 6	+1	UP
KEV adds with a published VERIFIED SA exposure figure	1 of 9	2 of 6	-1	DOWN
Corrections issued to prior editions	2	2	0	FLAT

Five notes on the table. The two claims are Aeroklas Duys (Deadlock, 12 October 17:50 UTC) and Europ Assistance South Africa (The Gentlemen, 16 October 09:31 UTC), both with .co.za domains and South African operations, so both pass the nationality check (the report's test of whether a victim the aggregator tags ZA is in fact South African).²¹ The separate row that counted survivors has been folded into this one because it had read n of n for four editions. The hand-search row stays at zero after a read of every listing The Gentlemen indexed from 11 to 17 October and of Deadlock's six October listings, looking for a South African location or domain under any country tag.^{6,10} The confirmations row counts Ampath's section 22 notice and Bootlegger's statement on its exposed franchise dashboard; the Gauteng Department of e-Government's SMS to residents that it is investigating a cybersecurity incident in the e-Panic Button

app is a development of the W40 confirmation and is not counted again.^{1,22,23} Seven of the nine KEV catalogue additions were past their due date on Monday 19 October (Ivanti and Windows by three days, the four of 14 October by two, Atlassian by one); the BeyondTrust and Fortinet entries fell due on the publication day itself.¹¹ One of the nine has a VERIFIED South African exposure figure: the Fortinet entry, through the FortiGate count of 2,801, with the qualification that the flaw needs an administrator session; the Ivanti, PAN-OS, Cisco, Atlassian, BeyondTrust and Ahsay products have no corroborated fingerprint in the panel.¹⁹

W43 KEY FRAMING: two South African organisations answered a disclosure question this week and gave opposite answers. Ampath detected an intrusion on 2 October, notified the regulator, published a section 22 notice on the eleventh day naming the actor and the data categories, and when the actor claimed 80 million records it explained within a day why a row count is not a patient count. The Gauteng Department of e-Government, three weeks after a student showed GroundUp that its R269 million panic-button app served its database to anyone, has by his account not answered him, has sent residents an SMS about a cybersecurity incident, and says it has approached SAPS about a criminal case, which its MEC describes as standard practice. The question for a board is which of those two it would be: whether it has, written down, the answer it would give to a claimed record count within 24 hours, and whether its first instinct on a disclosed flaw is the fix or the charge sheet. On the technical side, four exploited edge-appliance flaws entered the catalogue in one week, two of them used before a patch existed, against a South African FortiGate population of 2,801 and no measurable count for the Ivanti, Cisco and Palo Alto populations; and The Gentlemen, now fourth by leak-site postings in Microsoft's count, put a South African assistance and claims-administration company (by the aggregator's description) in a 33-name batch on a Friday morning.

TOP 3 ACTIONS THIS WEEK

1. Treat the three exploited edge flaws as one incident-response task, closed by Wednesday 21 October, with a written result to the CISO by Friday 23 October. Ivanti Connect Secure: upgrade to 22.8R2.5, 25.1.1.2, 25.1.3.0 or 25.1.3.1, then search gateway logs since 1 October for requests carrying the X-DSCGI-PATH header and for the four addresses in TH-2026-W43-01; CISA says the Integrity Checker Tool may not detect this one because the attacker's commands run in memory, so treat a clean checker result as no information, and any hit means factory reset, rebuild, and rotation of every credential, certificate and API key the appliance held. Cisco Secure Email Gateway: run `grep "System Security" system_logs` on every appliance and cluster member, upgrade Content Scanner Tools to 25.3.0.5525 or later, and treat a suspected-compromise line as an incident. PAN-OS: take the management interface off the internet if it is still there, patch to the fixed release for the branch, and search for the three advisory addresses.

2. If the organisation holds patient, member or policyholder records, prepare the Ampath answer by Friday 23 October. Write down, in advance, how the organisation would respond within 24 hours to a claimed record count: which tables hold one row per person and which hold one per event, so that records and people can be separated in a statement; the section 22 notice template with the data categories pre-mapped; and the call-centre briefing that a caller quoting a correct medical-scheme or policy number is not thereby verified. For an insurer, administrator or scheme the W42 action stands: a watch on the organisation's own name on leak sites under any country tag, because the group that listed Europ Assistance listed 33 names in one morning.

3. Run a decommissioning and management-plane inventory by Friday 23 October. Bootlegger's exposure was a legacy dashboard nobody had switched off; the AhsayCBS chain is being used against backup consoles left reachable from the internet with no working patch; Atlassian's own advice for CVE-2026-21589 is to take internet-exposed Data Center instances offline until patched. List every application the organisation migrated away from this year and confirm the old one is down; restrict every backup, remote-support and firewall management console to trusted addresses; and for managed service providers, do it for every client tenant, since the Ahsay victims so far are the providers' customers.

1. TechCentral, Ampath finds no evidence that test results were taken in breach, by Fanie van Rooyen (14 October 2026; quotes the 13 October notice and the 14 October statement). <https://techcentral.co.za/ampath-breach-no-evidence-test-results-taken/287314/>
2. ITWeb, Ampath downplays data breach claims, by Admire Moyo (15 October 2026; detection date 2 October, containment steps). <https://www.itweb.co.za/article/ampath-downplays-data-breach-claims/8OKdWqDXOjmqbznQ>
3. MyBroadband, Attackers claim to have stolen 80 million South African patient records in massive Ampath Laboratories data breach, by Luis Monzon (13 October 2026). <https://mybroadband.co.za/news/security/672153-attackers-claim-to-have-stolen-80-million-south-african-patient-records-in-massive-ampath-laboratories-data-breach.html>
4. Bizcommunity, Ampath says data breach claims of 80 million patient records are overstated (14 October 2026; carries the 14 October statement). <https://www.bizcommunity.com/article/ampath-says-data-breach-claims-of-80-million-patient-records-are-overstated-303808a>
5. ransomware.live, victim page for Europ Assistance South Africa (The Gentlemen), discovered 16 October 2026 09:31 UTC, estimated attack date 14 October; no data size, deadline, sample or published-data marker; infostealer panel 78 users, 6 employees, 1,470 passwords (60 critical); read 18 October 2026. <https://www.ransomware.live/id/RXVyb3AgQXNzaXN0YW5jZSBTb3V0aCBBZnJpY2FAdGhIZ2VudGxlbWVu>
6. ransomware.live, group page for The Gentlemen, read 18 October 2026 (999 victims, 91 countries; 38 listings 11 to 17 October, 33 on 16 October; LegalWise, Samwumed and Edcon unchanged). <https://www.ransomware.live/group/thegentlemen>
7. ransomware.live API, GET /groups, 410 groups with victim counts, retrieved 18 October 2026 and compared with the 11 October retrieval (feeds/r1_groups_2026-10-18.json). <https://api.ransomware.live/v2/groups>

8. TechCentral, MIP attackers rank fourth on ransomware leak sites, says Microsoft, by Fanie van Rooyen, on the Microsoft Digital Defense Report 2026 (14 October 2026). <https://techcentral.co.za/microsoft-ransomware-south-africa-digital-defense-report-2026/287306/>
9. ransomware.live, victim page for Aeroklas Duys / Duys Engineering Group (Deadlock), discovered 12 October 2026 17:50 UTC, website aeroklasduys.co.za, no data size, deadline or published-data marker; infostealer panel 1 employee, 12 passwords; read 18 October 2026. <https://www.ransomware.live/id/QWVyb2tsYXMgRHV5cyAvIER1eXMgRW5naW5lZXJpbmcgR3JvdXBARGVhZGxvY2s=>
10. ransomware.live, group page for Deadlock, read 18 October 2026 (107 victims, 42 countries; first discovery 15 June 2026; six listings in October). <https://www.ransomware.live/group/deadlock>
11. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.10.16, released 16 October 2026 17:15 UTC, retrieved 18 October (feeds/kev_2026-10-18.json). <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
12. BleepingComputer, CISA warns admins to immediately fix Ivanti flaw exploited as zero-day, by Sergiu Gatlan (14 October 2026). <https://www.bleepingcomputer.com/news/security/cisa-warns-admins-to-immediately-fix-ivanti-flaw-exploited-as-zero-day/>
13. Cisco, Security Advisory cisco-sa-esa-afw-zqYJkxp, Cisco Secure Email Gateway Advanced Malware Protection arbitrary file write vulnerability (14 October 2026). <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkxp>
14. Palo Alto Networks, Security Advisory CVE-2026-0322, PAN-OS: authenticated remote code execution in the management interface (14 October 2026, updated 15 October). <https://security.paloaltonetworks.com/CVE-2026-0322>
15. BleepingComputer, Microsoft October 2026 Patch Tuesday fixes 1,411 flaws, 3 zero-days, by Lawrence Abrams (13 October 2026). <https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2026-patch-tuesday-fixes-1-411-flaws-3-zero-days/>
16. Atlassian, CVE-2026-21589: arbitrary file access vulnerability impacts multiple products, security advisory (5 October 2026). <https://confluence.atlassian.com/security/cve-2026-21589-arbitrary-file-access-vulnerability-impacts-multiple-products-1870495748.html>
17. BleepingComputer, Unpatched AhsayCBS flaws exploited to deploy webshells, mine crypto, by Bill Toulas (9 October 2026). <https://www.bleepingcomputer.com/news/security/unpatched-ahsaycbs-flaws-exploited-to-deploy-webshells-mine-crypto/>
18. The Hacker News, Critical SonicWall SMA 1000 flaw targeted in 135 exploitation attempts after patch, by Ravie Lakshmanan (12 October 2026). <https://thehackernews.com/2026/10/critical-sonicwall-sma-1000-flaw.html>
19. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:01 UTC 18 October 2026 (feeds/shodan_za_2026-10-18.json). <https://www.shodan.io/search?query=country%3AZA>
20. ransomware.live API, GET /iocs/{group} for groups active against South Africa in the last 120 days, retrieved 18 October 2026 (feeds/r1_iocs_2026-10-18.json; The Gentlemen gained one address and one MD5 since 11 October; no Deadlock record). <https://api.ransomware.live/v2/iocs/thegentlemen>
21. ransomware.live API, GET /v2/countryvictims/ZA, 138 records, za_records 138 against server_returned 138, filter purity 1.0, FREE v2 tier (delayed relative to PRO), retrieved 02:00 UTC 18 October 2026 (feeds/ransomwarelive_za_2026-10-18.json). <https://api.ransomware.live/v2/countryvictims/ZA>
22. MyBroadband, CEO of top South African coffee franchise responds after vibe-coded web application exposed sensitive data, by Jan Vermeulen (16 October 2026). <https://mybroadband.co.za/news/security/672647-ceo-of-top-south-african-coffee-franchise-responds-after-vibe-coded-web-application-exposed-sensitive-data.html>
23. MyBroadband, Gauteng's plan to charge student who discovered a security flaw in R269-million app is absurd, by Luis Monzon (16 October 2026). <https://mybroadband.co.za/news/government/672623-gautengs-plan-to-charge-student-who-discovered-a-security-flaw-in-r269-million-app-is-absurd.html>

2. THREAT LANDSCAPE HEATMAP

South African Sector Threat Levels, Week 43 (11 October - 17 October 2026)



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

Two rows retired, two rows entered. Healthcare and Pathology enters at ransomware 6, data extortion 9, hacktivism 2, phishing and fraud 8 and vulnerability exploitation 6, on Ampath: a confirmed intrusion through what the company calls a vulnerability in application functionality, an actor whose business is selling and leaking databases without encrypting anything, and a data set of identity numbers and medical-scheme membership numbers that is built for impersonation of the laboratory, the scheme or a bank.^{1,24} Manufacturing, Mining and Industrial enters at 8, 8, 2, 4 and 5, replacing the Mining and Resources row that entered last week at 7, 8, 2, 4 and 5: it carries Tharisa, silent through its 13 October production report, and Aeroklas Duys, listed by Deadlock, an encrypting group whose leak-site record is mostly manufacturing and engineering firms, which is the reason the ransomware score enters one point higher.^{25,9,26} To make room, Collaboration and Virtualisation is retired: its observations were the SharePoint, Zimbra and vCenter carryovers, which stay in the KEV table, and the Atlassian entry this week is scored under Software Supply Chain and DevOps, where Bitbucket and Bamboo sit. Mining and Resources is retired as a row because its single observation has had no development; the wider row inherits it.

Movements. Government, Public Bodies and Defence moves from 4 to 5 on hacktivism, the first movement in that column since W37: the local government elections are on Wednesday 4 November, the IEC's disinformation code has been in force since 4 September, and the Information Regulator's 2024 statement on a security compromise at the IEC is the precedent for the coming fortnight; the score is a forward-looking one and says nothing about an observed campaign.^{27,28} Its other scores hold on the

e-Panic development.²³ Network Edge and Remote Access holds at 10 on exploitation with four catalogue entries in a week and the SMA 1000 flaw still outside it; its ransomware score holds at 7 because no South African incident has named an edge appliance as the entry point this quarter. Financial Services and Credit holds at the ceiling on extortion and fraud: Europ Assistance South Africa is an assistance and claims-administration company by the aggregator's description, and the BioCatch figures BusinessTech carries, 85 per cent of banking leaders reporting more fraud attempts, add nothing a ceiling can show.^{5,29} Outsourced Verification, Administration and IT Providers holds at 9 and 10: Europ Assistance also runs white-label claims administration for underwriters by the aggregator's description, and the Ahsay victims are managed service providers' customers.¹⁷ Retail, Food and Consumer holds; Bootlegger's exposure was franchise and manager data, with no customer data on the platform by the company's account.²² Software Supply Chain and DevOps holds at 10 on Atlassian, Ahsay and BeyondTrust.

24. KELA, ByteToBreach: a deep dive into a persistent data leak operator (17 November 2025, updated 17 July 2026). <https://www.kelacyber.com/blog/bytetobreach-a-deep-dive-into-a-persistent-data-leak-operator/>

25. Tharisa plc, SENS and RNS announcements page, read 18 October 2026 (Q4 and full-year production report, 13 October; Valterra offtake announcement, 15 October; neither mentions a cyber incident). <https://www.tharisa.com/sens-rns-announcements.php>

26. ZeroFox Intelligence, Flash report: DeadLock's ransomware leak site lists over 80 victims (29 June 2026). <https://www.zerofox.com/intelligence/flash-report-deadlocks-ransomware-leak-site-lists-over-80-victims/>

27. SANews, IEC gazettes code to tackle disinformation ahead of local elections (8 September 2026; code promulgated 4 September; elections 4 November 2026). <https://www.sanews.gov.za/node/84131>

28. Information Regulator, Media statements page, checked 18 October 2026 (newest item 21 September 2026; newest enforcement statement 2 June; nothing on Ampath, MIP or e-Panic). <https://infoeregulator.org.za/media-statements/>

29. BusinessTech, Warning for people using WhatsApp in South Africa, by Caitlyn Hilliard-Lomas (17 October 2026). <https://businesstech.co.za/news/telecommunications/880136/warning-for-people-using-whatsapp-in-south-africa/>

3. TOP SA INCIDENTS (W43)

Five items. One is a pathology group's confirmed intrusion with a disputed record count, two are leak-site claims against Europ Assistance South Africa and a parts manufacturer, one is a provincial department's response to a disclosed flaw, and one is a franchise group's exposed dashboard. Ratings: CONFIRMED means the organisation affected, a regulator or two independent sources support the fact; PROBABLE means one credible source or strong technical evidence; CLAIMED means a threat-actor assertion only. A leak-site description is written by the attacker and cannot lift a rating on its own.

3.1 INC-2026-W43-01: Ampath Confirms an Intrusion; ByteToBreach Claims 80 Million Rows [CONFIRMED]

Sector	Healthcare and pathology
Organisation	Amphat Laboratories, private pathology group with laboratories and depots across South Africa
Timeline	Detected Friday 2 October 2026 and incident response activated; section 22 notice issued Tuesday 13 October, the day the actor posted; website replaced by a holding page on the afternoon of 13 October with functions returning that evening; follow-up statement Wednesday 14 October

Company account	The notice names ByteToBreach as a criminal threat actor and says data may have been accessed and exfiltrated without authorisation. Categories listed: names, identity numbers, dates of birth, age, sex, language, physical and email addresses and mobile numbers; medical scheme name, membership number and plan option; payer names, payment amounts and transaction dates and times; not all records contain all fields. No indication that health, diagnostic or clinical information was in the affected data; on 14 October, no evidence that patient records, diagnoses, test results or banking information were compromised. Containment: malicious addresses blocked, unauthorised files removed, compromised accounts disabled, a vulnerability in application functionality fixed, the affected web server restored from a clean backup. Information Regulator notified; external forensic specialists and legal advisers engaged; laboratories and patient services operational; no evidence of continuing access
Actor claim	Posted on a criminal forum on 13 October with screenshots and download links: ten of about 375 databases copied in full, covering HR, patient, finance, LDAP and provider data from the mid-2000s to the present; an admissions table of more than 80 million records; negotiations with Ampath described as short, with no amount given. MyBroadband reports that a scan of one download showed malware. TechCentral had not seen the post
Company on the figure	The publicly cited number appears to refer to database records or entries rather than unique individuals; one patient generates many records over years; the figure materially overstates the number of people affected. No count of individuals has been given
Confidence	CONFIRMED for the incident, on the company's own notice as carried by four publications; the notice itself was not located on the Ampath home or news pages on 18 October. The database count, the record count and the data span are CLAIMED by the actor and are not adopted

Three things in the record are worth separating. The first is the sequence: detection on 2 October, regulator notified, notice on 13 October with the actor named and the data categories listed, and a second statement within a day of the actor's claim.^{1,2,4} The second is what the containment list says: a fixed application vulnerability, a web server restored from backup and unauthorised files removed describe an internet-facing application compromise, which matches the actor's method as KELA profiles it.²⁴ The third is the figure. An admissions table records visits, and the company's point that rows are not people is sound; the categories it lists, identity number with scheme membership number and payment history, are nonetheless the fields a fraudster needs to impersonate the laboratory, the scheme or a bank, and the notice says so. The distinguishing observations are a published sample on the forum, an Ampath count of individuals, and any Information Regulator statement; the regulator's pages carried nothing on 18 October.²⁸ First reported by MyBroadband on 13 October 2026. Detection relevance: TH-2026-W43-04 carries the application-compromise pattern and the patient-facing fraud that follows.

3.2 INC-2026-W43-02: Europ Assistance South Africa Listed by The Gentlemen in a 33-Name Batch [CLAIMED]

Sector	Financial services and credit; outsourced administration (emergency assistance, claims administration and white-label BPO for underwriters, by the aggregator's description)
Organisation	Europ Assistance South Africa, Roodepoort, domain europassistance.co.za. The aggregator's generated description says the company completed a management buyout from its French parent in 2023 and rebranded in October 2025; that is the aggregator's text and was not confirmed from the company, whose website returned only its title to this collection ³⁰

Listing	Indexed by ransomware.live at 09:31 UTC on Friday 16 October 2026 from The Gentlemen's site, estimated attack date 14 October. No data size, sample, deadline or published-data marker on the record on 18 October. One of 33 organisations in at least 15 countries the group indexed on 16 October, alongside MoneyGram, KFC, Confluent and Ecuador's national police
Infostealer panel	78 users, six employees and eleven third-party employees with stealer-log records; 1,470 passwords for the domain in exposure data, 60 marked critical; 19 external attack-surface findings. Third-party telemetry of unknown age
Statement	None located. No South African publication had carried the listing by Saturday 17 October
Confidence	CLAIMED. Threat-actor assertion only. A mass posting argues against South Africa being singled out and says nothing about whether the group holds the company's data

The listing is the group's thirteenth South African name since January and its fifth in the insurance and administration cluster after Hollard, Guardrisk, LegalWise and Samwumed, four names the MIP cascade accounts for; whether Europ Assistance has any connection to MIP is unknown and is not inferred.^{5,6} What distinguishes it from the September listings is the batch. The three 30 September names, two of them MIP-linked, went up in one minute with timers; Europ Assistance went up in a 33-name global dump that moved the index by more in a day than the group managed in the whole of the W40 week (21), and that is the pattern Microsoft's report describes when it says the group's leak-site activity may be pushed to attract attention.⁸ The distinguishing observations are a company statement, a sample, and whether the record acquires the timer and directory-profile features TechCentral described on the September three. First observed on the aggregator; no publication credit. Detection relevance: TH-2026-W43-06 carries the one new address and one new hash on the group's indicator feed this week.

3.3 INC-2026-W43-03: Gauteng Approaches SAPS Over the e-Panic Button Disclosure [CONFIRMED]

Sector	Government, public bodies and defence
Organisation	Gauteng Department of e-Government; developer Evolve Value Added Services (R269 million five-year contract, R131.3 million paid); backend previously Aura, reportedly replaced by Trigger Systems ²³
Background	W40 carried GroundUp's finding of 23 September that the app's database of names, contact details, vehicle registrations, crime reports, images, location histories and live one-time PINs could be read without authentication; the student researcher Joel Cedras alerted the developers on 21 September and Evolve fixed it the next day

Development	The department has described the disclosure as a security compromise, contacted SAPS about a criminal case (SAPS reportedly advised that Evolve, as custodian, should open it), and sent residents an SMS stating that it is investigating a cybersecurity incident affecting the app and urging them to stay alert to suspicious communications. MEC Bonginkosi Dhlamini: opening police cases when security breaches are recorded is standard practice; the matter remains under investigation; a report will be made public at the right time. Cedras to EWN: static analysis, no hacking, no law broken; the department never answered his emails; he believes the case is meant to intimidate. The DA's Michael Waters called the plan absurd and asked the MEC to state the basis for charges, whether a case is registered, how long the data was exposed and whether anyone else accessed it
Confidence	CONFIRMED on the MEC's statements and the department's SMS as reported by MyBroadband and EWN; whether a case has in fact been registered, and against whom, is unconfirmed

The W40 exposure needed no further confirmation; what is new is the department's position, and it matters beyond Gauteng. South Africa has no safe-harbour provision for security research: section 2 of the Cybercrimes Act makes unlawful access an offence without a research exception, and the only protection a researcher has is the prosecutor's discretion.^{23,31} A department that says it treats a disclosure as the incident, three weeks after the developer fixed it, tells the next person who finds a provincial database open to say nothing. The SMS is the other half: it is the first notice residents have received from the department, it came after the fix, it names no data category and no date, and it is not a section 22 notice to data subjects in the form the regulator's guidance describes. The distinguishing observations are a registered case number, a departmental report with an exposure period and an access log analysis, and any Information Regulator action. Detection relevance: none; the relevance is in Section 8 and in Management recommendation 2.

3.4 INC-2026-W43-04: Bootlegger's Legacy Dashboard Served Franchise Data to Anyone With the Link [CONFIRMED]

Sector	Retail, food and consumer (coffee franchise, 132 locations)
Organisation	Bootlegger Coffee Company; chief executive Ricky Ruthenberg
Exposure	An internal operations dashboard (BOS) hosted on Railway sat behind a login screen but sent its data with the login page, readable in the page source by anyone with the URL. Exposed: names and contact details for 132 locations (verified by MyBroadband), franchisee and operator names and email addresses, general managers' names and mobile numbers, performance and pipeline data. Found by an anonymous poster on the MyBroadband forums and Reddit after staff posted screen photographs on Instagram; the poster attributed the app to the CEO's publicised vibe-coding
Company account	Bootlegger became aware on the afternoon of Thursday 15 October; the platform was a legacy application already migrated to a secure environment and not fully decommissioned; taken offline the same day; no customer data was collected on it; no evidence that databases or core systems were accessed; affected franchisees, operators and managers being contacted; the Information Regulator will be notified
Confidence	CONFIRMED on the company's statement and MyBroadband's verification of the exposed data; the cause attributed by the anonymous poster is that poster's account

The item is small in records and useful in kind. The failure was a decommissioning failure, by the company's own description, and the exposed records were those of the people who run the business, which is the population a business email compromise campaign wants.²² One detail travels to other estates: an application that shows a login page is unprotected if the data arrives before the login, a pattern worth testing on every internally built dashboard. The distinguishing observations are the section 22 notice and whether the regulator's online reporting platform shows it. First reported by MyBroadband on 16 October 2026. Detection relevance: none beyond the inventory action in Section 1.

3.5 INC-2026-W43-05: Aeroklas Duys Listed by Deadlock, the Group's Second South African Name [CLAIMED]

Sector	Manufacturing (automotive accessories; industrial engineering)
Organisation	Aeroklas Duys (Pty) Ltd, domain aeroklasduys.co.za; by the aggregator's description a joint venture between the Duys Engineering Group, founded in South Africa in 1960, and Aeroklas of Thailand's Eastern Polymer Group (the company site could not be read) ⁹
Listing	Indexed by ransomware.live at 17:50 UTC on Monday 12 October 2026 from Deadlock's site, estimated attack date 12 October. No data size, sample, deadline or published-data marker. Infostealer panel: one employee record, twelve passwords
The group	Deadlock has 107 listings in 42 countries on the aggregator, first indexed 15 June 2026, six in October; its first South African listing was the Furniture Bargaining Council on 24 August (W36); ZeroFox read its clearnet leak site in June at about 80 victims, 57 per cent in Europe and Russia, manufacturing the largest sector, and assessed an even chance that many listed victims were in fact compromised. WatchGuard's June analysis: active since mid-2025, custom stream cipher, a Session identifier in the note, an HTML note that embeds the leak site and a chat, proxy addresses in Polygon smart contracts, vulnerable-driver abuse to disable defences, initial access unknown
Statement	None. The company website could not be read by this collection (robots exclusion). No South African publication had carried the listing by 17 October
Confidence	CLAIMED. Threat-actor assertion only, from a group whose own evidence of intrusion ZeroFox found thin

The group carries the relevance here. Deadlock is an encrypting operation with a working leak site that has listed two South African organisations in seven weeks, and the aggregator's indicator and YARA feeds carry nothing for it; the only tooling indicators in the open record are WatchGuard's June sample hash, the Session contact channel and the AnyDesk and vulnerable-driver behaviours.^{10,26,32} The distinguishing observations are a company statement, a sample, and a third South African listing. First observed on the aggregator; no publication credit. Detection relevance: TH-2026-W43-07.

3.6 Carryovers

Tharisa (UmBra), W42. The W42 test is met by silence. The Q4 production report of Tuesday 13 October and the Valterra offtake announcement of 15 October say nothing about a cyber incident, no South African outlet has carried the listing, UmBra has added nothing since 10 October and its site was unavailable at the 18 October check with 30-day uptime of 56.7 per cent. The item stays CLAIMED and moves to the record; the company has not treated the listing as reportable.^{25,33,34}

LegalWise, Samwumed and Edcon (The Gentlemen), W41 and W42. A second week past the timers TechCentral reported: no published-data marker on any of the three records on 18 October, no sample, no statements. CLAIMED for the listings; LegalWise's and Samwumed's MIP exposure CONFIRMED on their own notices.^{35,6}

ATNS, W41. The Friday 16 October test passed with no contract award, statement, listing or section 22 notice located; no new reporting was located. The test closes as unobserved; the item stays CONFIRMED at the scope of the tender document and is carried as record only.

BlackLocks (Apollo 21 and ARCA Unlimited Architects), W40. The index stood at three on 18 October, newest listing 26 September. The W40 question closes as unanswered: two South African listings in one day from a group that then stopped.³⁶ CLAIMED for both.

BCX (INC Ransom), W41; Guardrisk and CoverCubed, W41; RelyComply (DireWolf), W39; Gauteng e-Panic, W40 (development above); 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; Rand Water, W37. No development on any of them beyond e-Panic; all stay at their prior ratings and are carried without re-argument. Microsoft's report, as TechCentral reads it, refers to Rand Water as hit in recent weeks without saying whether ransomware was involved; that adds nothing to the W37 record.⁸

30. Europ Assistance South Africa, corporate website, checked 18 October 2026 (returned only its title and description; no notice readable). <https://www.europassistance.co.za/>

31. EWN, Gauteng emergency app exposed users' private information, by Sara-Jayne Makwala King (15 October 2026). <https://www.ewn.co.za/2026/10/15/gautengs-emergency-app-exposed-users-private-information>

32. WatchGuard Secplicity, DeadLock ransomware group embeds data leak site within ransom note, by Ryan Estes (8 June 2026). <https://www.watchguard.com/wgrd-security-hub/secplicity-blog/deadlock-ransomware-group-embeds-data-leak-site-within-ransom>

33. Miningmx, Tharisa lifts Q4 production, keeps Karo on track, by Liesl Peyper (13 October 2026). <https://miningmx.com/2026-10-13-tharisa-lifts-q4-production-keeps-karo-on-track/>

34. ransomware.live, group page for UmBra, read 18 October 2026 (ten victims; none after 10 October; site unavailable, 30-day uptime 56.7 per cent; Tharisa unchanged). <https://www.ransomware.live/group/umbra>

35. ransomware.live, victim page for LegalWise (The Gentlemen), discovered 30 September 2026 03:40 UTC, re-read 18 October 2026 (no deadline, sample or published-data marker on the record). <https://ransomware.live/id/TGVnYWxXaXNIQHROzWdlbnRsZWllbg==>

36. ransomware.live, group page for BlackLocks, read 18 October 2026 (three victims, newest discovered 26 September 2026). <https://www.ransomware.live/group/blacklocks>

4. THREAT ACTORS

Three profiles and a set of notes. ByteToBreach, because it named Ampath and works differently from the ransomware groups this section usually carries; The Gentlemen, because it listed a South African name, Europ Assistance South Africa, in the week Microsoft ranked it fourth by leak-site postings; and Deadlock, because its second South African listing in seven weeks arrived with no indicators on the feed. A fourth note covers UTA0576, the actor Volexity ties to the Ivanti zero-day, and the groups that moved.

4.1 ByteToBreach: An Operator Who Exports Databases and Sells Them

KELA's profile, first published in November 2025 and updated in July 2026, describes a single operator active since at least June 2025 who sells and leaks databases taken from airlines, banks, universities and government bodies, posts on DarkForums, Dread, Telegram and Pastebin, and has run a WordPress site

styled as a penetration-testing firm with victims' logos shown as clients. KELA's July update assesses the operator as an individual in Oran, Algeria, on the strength of infostealer-recovered artefacts, and names a person; this report carries the assessment without the name.²⁴ The method, as KELA describes it, is exploitation of known weaknesses in cloud and corporate applications, reuse of credentials from stealer logs and phishing, brute force and misconfiguration, followed by export of employee records, databases and backups and public leaks to prove the claim; a hash-cracking service at 100 dollars a hash and, in a July 2026 Romanian case, an alleged ransomware deployment round out the record.²⁴ TechCentral adds the African track record: a 2025 claim against Seychelles Commercial Bank, which confirmed an incident without naming the actor, and 2026 claims against Sterling Bank, Remita and the Corporate Affairs Commission in Nigeria.¹ For a South African defender the point is that this actor does not encrypt and does not run a leak site with timers; it posts on a forum, offers samples, and sells. The Ampath containment list, an application vulnerability and a web server restored from backup, is consistent with that profile, and the hunt in TH-2026-W43-04 is built on the application-compromise pattern, because the actor publishes no tooling.

4.2 The Gentlemen: 38 Listings in the Window, a 33-Name Friday, and Fourth Place by Leak-Site Count

The index rose from 960 to 1,002 between the 11 and 18 October retrievals, after 39, 33 and 21 in the three weeks before; the group page read 999 at the time of the check, with 38 listings discovered between 11 and 17 October, five on 12 October and 33 on 16 October.^{7,6} The 16 October batch is the observation of the week for this group: MoneyGram, KFC, Confluent, BigID, a Japanese national university, Ecuador's national police and a Thai listed company went up with Europ Assistance South Africa in one morning. Microsoft's Digital Defense Report, covering July 2025 to June 2026, puts the group fourth by leak-site postings at six per cent, behind Qilin (16), Akira (8) and Play (7), and cautions that newer families including The Gentlemen are a much smaller share of its own telemetry, which may suggest, in Microsoft's words, that leak-site activity was heavily pushed to attract attention to these new offerings.⁸ Read against this week's batch, that caution is a working hypothesis awaiting a test: a 33-name day is consistent with either a large affiliate intake or with volume posted for effect, and the distinguishing observation is how many of the 33 confirm. The South African record is thirteen listings since January, twelve ZA-tagged and Samwumed under a Korean tag; the W42 hand search of the group page found nothing further under another flag this week.^{21,6} The indicator feed now holds 34 SHA-256, four SHA-1 and 48 MD5 hashes, eight address entries, six Tox and two Session identifiers and two email addresses. Seven of the addresses and the second Session identifier arrived in the 11 October retrieval and were missed by W42, which is corrected in Section 1; the 18 October retrieval adds one MD5 hash and a port-qualified entry for an address already listed.²⁰ TH-2026-W43-06 exports the rows that W40 and W42 did not.

4.3 Deadlock: Second South African Listing, No Feed Indicators

Deadlock has 107 listings in 42 countries on the aggregator, one more than a week earlier, first indexed on 15 June 2026 with an estimated first attack of 22 May; its October listings before Aeroklas Duys are in the United States, Spain, Italy and Greece, and its first South African one was the Furniture Bargaining Council on 24 August.^{10,21} The two June vendor analyses summarised in 3.5 add what the aggregator lacks: a Session identifier in the note, AnyDesk for persistence, proxy addresses held in Polygon smart contracts, vulnerable-driver abuse per Cisco Talos, one sample hash from early June 2026, and no public account of

initial access.^{26,32} The aggregator's indicator and YARA feeds hold no record for the group, so the hunt in TH-2026-W43-07 rests on the vendor sample hash, the Session channel, the AnyDesk and driver behaviours and the two leak-site addresses; the aggregator's record shows the clearnet address failing DNS resolution on 18 October.¹⁰

4.4 Notes: UTA0576, UmBra's Silence, and the Groups That Moved

UTA0576. Volexity's name for the actor it saw exploiting the Ivanti Connect Secure flaw from 3 October (Defused Cyber dates first attempts to 1 October), chaining the authentication bypass with a privilege-escalation flaw to root, pulling credentials from the appliance, taking Active Directory metadata, running a Kerberoasting and credential-testing tool and a Python LDAP tool that searched for administrator passwords and BitLocker recovery keys, then scrubbing logs. Volexity assesses the motive as criminal and reports that the actor deployed no web shell, re-exploiting the device for each command, which is why the Integrity Checker Tool found nothing.^{37,12} **UmBra** added no listing after 10 October; its site was unavailable at the 18 October check with 30-day uptime of 56.7 per cent and the aggregator marks it inactive for eight days. The W42 inference, an affiliate or rebrand with existing access, is neither strengthened nor weakened by a week of silence.³⁴ **Index movements** among the sixteen groups with a South African listing since 1 July, besides The Gentlemen in 4.2: Qilin 2,353 to 2,379, INC Ransom 969 to 977, Everest 409 to 416, LockBit 5.0 374 to 384, DragonForce 660 to 664, Deadlock 106 to 107, DireWolf 136 to 137, RansomHouse 212 to 213; the other seven (Krybit, Arcus Media, MedusaLocker, Payload, m3rx, BlackLocks and UmBra) did not move. The index grew from 407 to 410 groups on 0x00, hyflock and a group calling itself the seven deadly sins; the largest mover in the whole table was nOn, from 22 to 110, with no South African listing.⁷

37. The Hacker News, CISA urges immediate Ivanti Connect Secure updates as honeypots log 105 exploit attempts, by Ravie Lakshmanan (14 October 2026). <https://thehackernews.com/2026/10/cisa-urges-immediate-ivanti-connect.html>

5. CRITICAL VULNERABILITIES & CISA KEV

CISA added nine vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue between Sunday 11 and Saturday 17 October 2026: Ivanti Connect Secure CVE-2026-104935 and Windows Shell CVE-2026-96951 on Tuesday 13 October; Cisco Secure Email Gateway CVE-2026-76519, PAN-OS CVE-2026-0322 and the AhsayCBS pair CVE-2026-105133 and CVE-2026-105134 on Wednesday 14 October; Atlassian CVE-2026-21589 on Thursday 15 October; and BeyondTrust Remote Support CVE-2026-102764 and Fortinet CVE-2025-61624 on Friday 16 October. All nine carry three-day deadlines under BOD 26-04, the CISA directive that binds US federal agencies and that this report uses as a benchmark for everyone else; seven were past them on Monday 19 October and the two Friday entries fell due that day. The catalogue version used is 2026.10.16, released at 17:15 UTC on Friday 16 October, so any entry added on Saturday 17 October falls to W44; no entry was added on 9, 10, 11 or 12 October, which closes the W42 question about the SonicWall SMA 1000 flaw: it is not in the catalogue.¹¹ Every CVSS figure is from the NVD feed with its scoring source, with two exceptions: the Atlassian entry, which NVD had not scored at retrieval and which carries Atlassian's own 9.3 on CVSS 4.0, and the SonicWall July carryover, older than the feed's 45-day window. Every EPSS figure (FIRST's estimate of the probability of exploitation in the next 30 days) is from the FIRST feed, under the standing rule that a low EPSS never deprioritises a catalogue entry; the Ivanti entry's 0.26 and the Atlassian entry's 0.13 are the highest of the nine and the

BeyondTrust and Fortinet entries sit at 0.006, which says nothing about whether they are being used.^{38,39,16} The catalogue's ransomware-use field reads Unknown for all nine; Unknown means CISA has not recorded ransomware use, and the report never writes it as no. The forensicTriage flag reads Yes for eight and No for the Ahsay authentication entry.

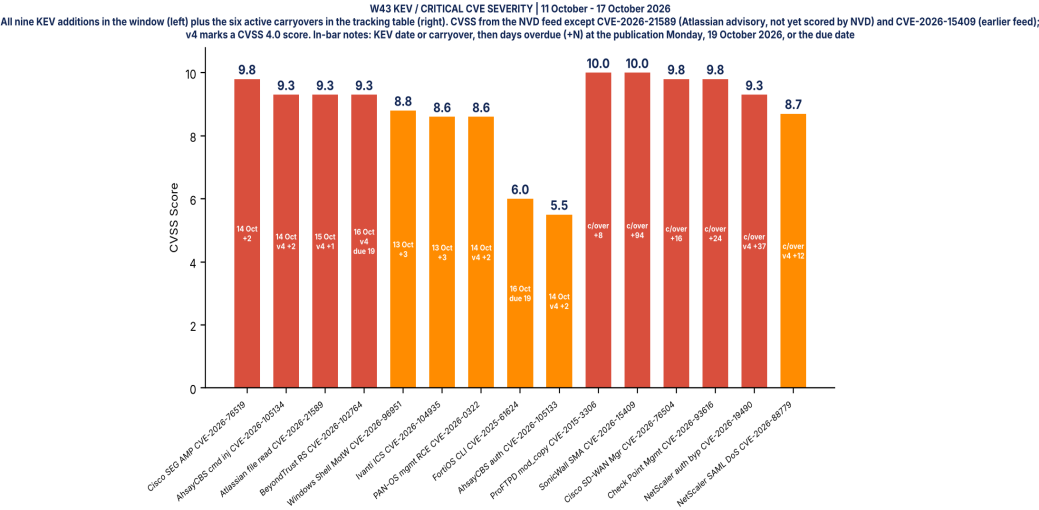
Ivanti Connect Secure CVE-2026-104935 is an authentication bypass by spoofing, CWE-290, scored 8.6 by Ivanti, that lets an unauthenticated remote attacker run commands; a single request with a crafted X-DSCGI-PATH header triggers it, per watchTowr.^{38,37} Part of the flaw was found internally and fixed in the July release 25.1.3.0, and exploitation began while Ivanti was backporting that fix; Ivanti's advisory of 13 October speaks of exploitation before disclosure affecting a limited number of customers, and the fixed builds are 25.1.1.2, 25.1.3.0 and 25.1.3.1 and 22.8R2.5, with 22.7 and below unaffected.^{40,12} Three facts carry the weight. Volexity's actor chained it with an unpatched privilege-escalation flaw that Ivanti plans to fix later; CISA says the Integrity Checker Tool may not detect exploitation because the commands run in memory, and prescribes network and memory forensics, then factory reset, upgrade or rebuild, restore, and rotation of every password, certificate and API key; and Previdian's honeypots logged 105 attempts from 50 addresses in Singapore and the United States by 14 October.^{12,37} Shadowserver counts more than 5,600 exposed hosts with the product's fingerprint worldwide; the South African panel has no corroborated query for it, which Section 7 records.^{12,19} Version 22.8 reaches end of life on 31 January 2027.³⁷

Cisco Secure Email Gateway CVE-2026-76519 is a relative path traversal in the Advanced Malware Protection feature, CVSS 9.8 from Cisco, reached by sending a crafted attachment through an appliance that has File Reputation enabled on a mail policy and Content Scanner Tools older than 25.3.0.5525; the result is an arbitrary file write and command execution as root. Cisco's advisory of 14 October says the PSIRT became aware of active exploitation in October 2026, gives no workaround, and fixes it in AsyncOS 15.5.5-014 and 16.5.0-780 or by updating Content Scanner Tools alone, which needs no restart. The compromise check is a grep of system_logs for "System Security" lines; a suspected-compromise line means TAC and the advisory's recovery steps, and Cisco advises reading firewall logs for the appliance's own uploads and downloads because root access lets the attacker clean the appliance logs.^{13,41} It is the second Secure Email Gateway entry in the catalogue in five weeks after CVE-2026-76461 of 14 September, and the third exploited flaw in the product line in a year after the AsyncOS zero-day of December 2025.^{11,41}

PAN-OS CVE-2026-0322 is code injection in the management interface, CVSS 8.6 on version 4.0 from Palo Alto Networks, needing valid credentials and network reach to the interface and yielding root; the vendor reports very limited exploitation, publishes three addresses, offers no workaround, and fixes it across the 10.2, 11.1, 11.2, 12.1 and 12.2 lines with the 11.2.16 build following on 15 October.^{14,42} The precondition is a credential, so the flaw is a reason to ask where the management interface is reachable from and whether any administrator credential has been in a stealer log, which the Section 7 infostealer panels show is not a hypothetical question for South African estates.

The remaining six. Windows Shell CVE-2026-96951, 8.8, is a command injection that bypasses Mark of the Web, the only one of the three zero-days in Microsoft's record 1,411-fix October release that was exploited, with no public detail on who used it or how; the same release ends updates for Windows 11 24H2 Home and Pro and Windows 10 Enterprise LTSC 2016.^{15,38} AhsayCBS CVE-2026-105133 (5.5 on version 4.0) and CVE-2026-105134 (9.3 on version 4.0) chain an authentication bypass in checkSysPwd with a command injection in the Replication Receiver's UpdateReceivers.do endpoint on a backup console sold to managed service providers. Huntress saw exploitation from 23:20 UTC on 7 October against at least five organisations, with JSP web shells, an XMRig miner named edge.exe run as a service called

MicrosoftEdgeUpdateSvc, a PowerShell script that hides from Task Manager, and in one case the vulnerable WinRingOx64.sys driver. The version the vendor called fixed, 10.3.4, is also affected, so the mitigation is to restrict the console to trusted addresses.^{43,17,38} Atlassian CVE-2026-21589, 9.3 by the vendor, reads any file under the web root whose path the attacker knows across eight Data Center products; Atlassian's advice is to take internet-exposed instances offline until patched or to block double dots adjacent to a slash, backslash or double colon, and it cannot confirm whether a given instance was affected; BleepingComputer's Patch Tuesday roundup records exploitation after a public proof of concept.^{16,15} BeyondTrust Remote Support CVE-2026-102764, 9.3 on version 4.0, is improper origin validation allowing file operations on the appliance; SaaS was patched on 9 October, self-hosted customers apply BT26-05, and the advisory makes no exploitation statement, so the catalogue entry is the evidence.^{44,11} Fortinet CVE-2025-61624, 6.0, is a CLI path traversal in FortiOS, FortiPAM, FortiProxy and FortiSwitchManager that lets an administrator with read-write permissions write or delete files; Fortinet's advisory of April now reads Known Exploited: Yes, and the fixed lines are FortiOS 7.6.5 and 7.4.10 with 7.2 and below told to migrate.^{45,38} **Exploited and not yet in the catalogue:** SonicWall SMA 1000 CVE-2026-102255, where Previdian counted 135 attempts from two US addresses from 8 October and SonicWall had not updated SNWLID-2026-0017 to say so by 12 October.¹⁸



W43 CISA KEV / Critical CVE Tracking (nine additions 13 to 16 October plus active carryovers)

Column notes: KEV Due is the BOD 26-04 deadline for US federal agencies, used here as a benchmark; OVERDUE +N counts days past it at Monday 19 October; RW is the catalogue's ransomware-use field; Triage is the catalogue's forensicTriage flag; ZA figures are VERIFIED Shodan exposure counts of a product family, which do not measure vulnerability.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-104935	Ivanti Connect Secure	8.6	Auth bypass by spoofing (unauth RCE)	16 Oct	KEV 13 Oct. OVERDUE +3. Zero-day, UTA0576 from 3 Oct. Fixed 25.1.1.2 / 25.1.3.0 / 25.1.3.1 / 22.8R2.5. ICT may not detect; X-DSCGI-PATH. No ZA label. RW Unknown. Triage Yes. EPSS 0.2598.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-96951	Microsoft Windows Shell	8.8	Command injection, MotW bypass	16 Oct	KEV 13 Oct. OVERDUE +3. Exploited zero-day in the October release; no public detail. RW Unknown. Triage Yes. EPSS 0.0151.
CVE-2026-76519	Cisco Secure Email Gateway (AMP)	9.8	Path traversal, root file write (unauth)	17 Oct	KEV 14 Oct. OVERDUE +2. Exploited in Oct. Content Scanner Tools 25.3.0.5525; grep System Security. Second SEG entry in five weeks. No ZA label. RW Unknown. Triage Yes. EPSS 0.0157.
CVE-2026-0322	Palo Alto Networks PAN-OS (mgmt)	8.6 (v4.0)	Code injection, root (authenticated)	17 Oct	KEV 14 Oct. OVERDUE +2. Very limited exploitation; three advisory IPs; no workaround. GlobalProtect query BROKEN. RW Unknown. Triage Yes. EPSS 0.0122.
CVE-2026-105134	Ahsay AhsayCBS (with CVE-2026-105133, 5.5 v4)	9.3 (v4.0)	OS command injection chain	17 Oct	KEV 14 Oct. OVERDUE +2. Exploited from 7 Oct (web shells, XMRig); 10.3.4 also affected; restrict console. No ZA label. RW Unknown. Triage Yes / No. EPSS 0.0478.
CVE-2026-21589	Atlassian Data Center (eight products)	9.3 v4*	Arbitrary file read (unauth)	18 Oct	KEV 15 Oct. OVERDUE +1. *Vendor score; NVD unscored. Offline until patched or block .. traversal. No ZA label. RW Unknown. Triage Yes. EPSS 0.1271.
CVE-2026-102764	BeyondTrust Remote Support	9.3 (v4.0)	Auth bypass, file operations	19 Oct	KEV 16 Oct. Due on publication day. BT26-05 patch (24.3.1 to 26.2.3); SaaS patched 9 Oct. No ZA label. RW Unknown. Triage Yes. EPSS 0.0060.
CVE-2025-61624	Fortinet FortiOS, FortiPAM, FortiProxy, FortiSwitchManager	6.0	CLI path traversal (admin)	19 Oct	KEV 16 Oct. Due on publication day. FG-IR-26-122 Known Exploited: Yes. Fixed 7.6.5 / 7.4.10. FortiGate 2,801 in ZA (family). RW Unknown. Triage Yes. EPSS 0.0058.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-88779	Citrix NetScaler (SAML)	8.7 (v4.0)	Memory overflow, DoS	7 Oct	Carryover. OVERDUE +12; September pair +19. CVE-2026-107406 fixed 9 Oct, absent from KEV. 146 in ZA. TH-2026-W42-01 stands.
CVE-2015-3306	ProFTPD and the AA26-281A set	10.0	File read / write (unauth)	11 Oct	Carryover. OVERDUE +8 with ONLYOFFICE, Struts, BIND, Strapi. 185 ProFTPD in ZA, 134 on 21. TH-2026-W42-03 stands.
CVE-2026-76504	Cisco Catalyst SD-WAN Manager	9.8	Auth bypass via URI encoding	3 Oct	Carryover. OVERDUE +16; FortiMail +15; Zammad pair +14; Apple +6. No ZA label.
CVE-2026-93616	Check Point Security Management	9.8	Path traversal, file upload	25 Sep	Carryover. OVERDUE +24 with CVE-2026-85102, F5 APM, Arista VCO; Zyxel +25; WSO2, Adobe 71362 +22; MikroTik 67279, SharePoint 65660, WordPress +21.
CVE-2026-19490	Citrix NetScaler ADC and Gateway	9.3 (v4.0)	Auth bypass (unauth)	12 Sep	Carryover. OVERDUE +37 with Cisco FMC 20079 (10.0) and FortiOS 25249; MikroTik pair +36 (3,947 in ZA); ScreenConnect, GitLab +35; SEG 76461 +32; ISE +30; kernel trio +28.
CVE-2026-15409	SonicWall SMA 1000	10.0	SSRF (unauth)	17 Jul	Carryover. OVERDUE +94 with 15410, both RW KNOWN; September pair +44; FMC 20316 (Known) +79; SharePoint 55040 +59; Zimbra +56; LiteLLM +119. CVE-2026-102255 not listed. SonicWall 1,206 in ZA.

Pattern note: four of the week's nine entries sit on appliances that terminate remote access or mail at the perimeter, and in two of them the vendor's own fix arrived after the exploitation. That is the fifth consecutive week in which an exploited network-edge flaw entered the catalogue, after NetScaler three times since September, FortiMail, Catalyst SD-WAN Manager, Check Point, F5 and the September Secure Email Gateway entry, and the operational lesson has stopped changing: the compromise check comes before the patch, because an appliance exploited before the fix existed is already compromised or it is not, and the upgrade does not tell you which.¹¹ The Ivanti entry sharpens it. CISA's own guidance says the vendor's integrity checker may not detect this intrusion, so the compromise check is log review for one header and four addresses, and the remedy on a hit is a rebuild; an estate that reads a clean checker result as a clean appliance has, on CISA's wording, established nothing.¹² The Ahsay entry is the other pattern of the week: a backup console with a vendor patch that does not work, exploited within three days of the CVE identifiers being published for cryptocurrency mining, where the victims are managed service providers' customers and the only mitigation is to stop the console answering the internet.¹⁷

38. NIST NVD, CVE API 2.0, CVSS base scores with scoring source for the 54 catalogue entries added in the last 45 days, 53 resolved, retrieved 18 October (feeds/nvd_cvss_2026-10-18.json). <https://services.nvd.nist.gov/rest/json/cves/2.0>

39. FIRST, EPSS API, scores for the same 54 entries, retrieved 18 October 2026 (feeds/epss_2026-10-18.json). <https://api.first.org/data/v1/epss>

40. Rapid7, Ivanti Connect Secure zero-day exploited in the wild (CVE-2026-104935) (13 October 2026). <https://www.rapid7.com/blog/post/etr-ivanti-connect-secure-zero-day-exploited-in-the-wild-cve-2026-104935/>

41. BleepingComputer, Cisco patches actively exploited Secure Email Gateway zero-day, by Sergiu Gatlan (14 October 2026). <https://www.bleepingcomputer.com/news/security/cisco-patches-actively-exploited-secure-email-gateway-zero-day/>

42. BleepingComputer, Palo Alto Networks warns of PAN-OS RCE flaw exploited in attacks, by Lawrence Abrams (14 October 2026). <https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-pan-os-rce-flaw-exploited-in-attacks/>

43. The Hacker News, Attackers exploit AhsayCBS flaws to deploy web shells and cryptominers, by Ravie Lakshmanan (9 October 2026). <https://thehackernews.com/2026/10/attackers-exploit-ahsaycbs-flaws-to.html>

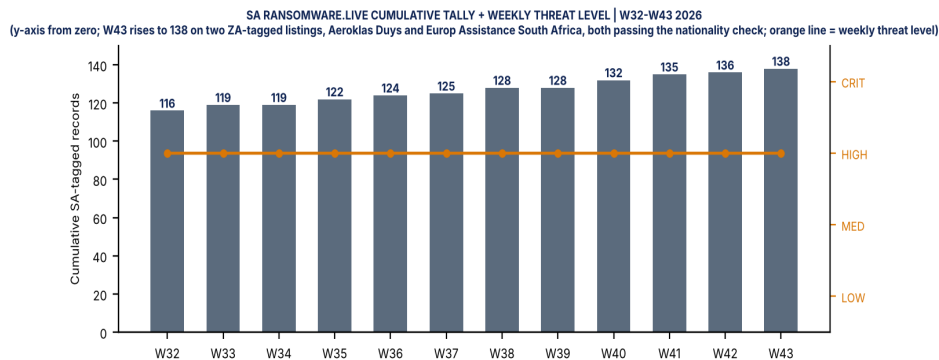
44. BeyondTrust, Security Advisory BT26-05, Remote Support improper origin validation, CVE-2026-102764 (15 October 2026). <https://www.beyondtrust.com/trust-center/security-advisories/bt26-05>

45. Fortinet PSIRT, FG-IR-26-122, Path traversal in CLI, CVE-2025-61624 (published 14 April 2026; Known Exploited: Yes when read 18 October 2026). <https://fortiguard.fortinet.com/psirt/FG-IR-26-122>

6. RANSOMWARE LANDSCAPE

The South African victim feed held 138 records when retrieved at 02:00 UTC on 18 October 2026, two more than the week before. The collection is country-scoped by path, the written file records 138 South African records against 138 returned, and the tier is the delayed free v2.²¹ A set-difference against the 11 October file returns two additions and zero removals, both discovered inside the window: Aeroklas Duys (Deadlock, 12 October 17:50 UTC) and Europ Assistance South Africa (The Gentlemen, 16 October 09:31 UTC). Both carry .co.za domains and South African operations and pass the nationality check without qualification, so the derived count equals the feed count. The aggregator's country page showed 138 with the same two newest.⁴⁶ The hand search for South African victims under other country tags covered The Gentlemen's 38 listings of the week and Deadlock's six October listings and found nothing further; it still covers only the groups that listed this week, and the name-keyed world-feed search remains a collector task.^{6,10}

Baseline at W42 close	136 records
New listings dated inside the window	2 with a ZA tag: Aeroklas Duys (Deadlock, 12 October); Europ Assistance South Africa (The Gentlemen, 16 October). None found under another tag for 11 to 17 October
Passing the nationality check	2 of 2, both on domain and operations. The aggregator's country field has invented a South African victim five times in the series and hidden two (RelyComply under GB, W39; Samwumed under KR, W41)
Delistings or restorations	None. Set difference against the 11 October file returns two additions and zero removals
End count at W43 retrieval	138 records, filter purity 1.0 in the run log and 138 of 138 tagged ZA in the file
Groups active against SA, rolling 120 days	17 by discovery date, unchanged; 16 groups hold a ZA-tagged listing discovered since 1 July. The boundary moves each week, so neither figure is a trend
Threat-level drivers	A confirmed pathology-group intrusion with a disputed 80 million-row claim; a 33-name leak-site batch carrying Europ Assistance South Africa; a second South African listing by an encrypting group with no public indicators; four exploited edge-appliance flaws in one week against a 2,801 FortiGate population and unmeasured Ivanti, Cisco and Palo Alto populations



Group notes. ByteToBreach, The Gentlemen and Deadlock are profiled in Section 4 and the index movements are in 4.4.⁷ The sixteen groups with a ZA-tagged listing since 1 July break down as The Gentlemen six, Krybit four, INC Ransom three, Deadlock and BlackLocks two each, and UmBra, Everest, LockBit 5.0, DireWolf, Qilin, MedusaLocker, Payload, m3rx, DragonForce, Arcus Media and RansomHouse one each.²¹ Microsoft's seventeen South African cases in the year to June, against seven the year before, is the third-steepest rise of the twelve countries its report singles out and the only African entry. Microsoft names no organisation behind the count, and its own caveat applies, since 5,798 of 8,521 global cases could not be attributed to a country and that pool shrank by 18 per cent, so part of any country increase is better attribution.⁸

Two patterns from the week for South African estates. The first is the arrival of a data-leak operator that does not encrypt: Ampath's intrusion produced no outage, no timer and no leak site, and the pressure came as a forum post with samples and a record count built to be quoted; the defence it calls for is the one in Section 1, an answer to the number prepared in advance. The second is the batch: a group posting 33 names in a morning, with Europ Assistance South Africa among them, is either taking affiliate intake at a new scale or inflating its board, and Microsoft's caution that the group's leak-site share far exceeds its telemetry share leans toward the second without settling it; the distinguishing observation is the confirmation rate of the 16 October batch over the next month.^{8,6}

The standing measurement caution applies: the victim feed is the delayed free tier, a listing dated inside this window may have been posted earlier, one posted late on Saturday 17 October may surface next week, and the window closes at the end of Saturday for the reason recorded in earlier editions.

46. ransomware.live, South Africa country page, cross-check only (138 victims, Europ Assistance South Africa and Aeroklas Duys newest, read 18 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 18 October 2026, and none is a count of vulnerable systems; the version and vuln filters are not available on this plan, rescan noise moves single counts by large fractions inside a day, and week-on-week movement is not reported as a finding.¹⁹ Only queries whose product facet corroborates the fingerprint are published. One of this week's nine additions has a figure: Fortinet FortiGate, 2,801 instances, 1,524 of

them on 10443, the SSL VPN portal's default port, 561 on 541 and 272 on 443; the figure measures the family, and the week's FortiOS flaw needs an administrator session, so it measures the population; exposure to that flaw is unknown. The rest of the panel: MikroTik RouterOS 3,947 (3,154 on the API port 8728); Citrix Netscaler 146 (106 on 443; the move from 125 is rescan noise by the standing rule); Cisco ASA WebVPN 357 (306 on 443); Microsoft SharePoint on-prem by http.component 800; WordPress by http.component 393, a floor; Apache Tomcat 925; Remote Desktop on 3389, 8,273; services on port 445, 5,617, of which 178 carry a Samba label; SonicWall by product string 1,206, replacing the withdrawn family sum (Section 1); ProFTPD 185, 134 on port 21; ownCloud 127; Metabase 116; MLflow 107; Ray 89; Langflow 72; Gitea 7; VMware vCenter 3; Artifactory 2.

Held, missing and omitted. Four of the week's additions have no Shodan product label and were held by the discovery stage: BeyondTrust Remote Support, AhsayCBS, Cisco Secure Email Gateway and the Atlassian products. The only Palo Alto query, an http.title match for GlobalProtect, has been BROKEN since August because its facet resolves to IIS, and no Ivanti Connect Secure query exists, so the week's two most urgent appliance flaws have no South African population figure. Check Point, F5 APM, WSO2, Adobe Commerce, Zyxel, Zammad, FortiMail, Catalyst SD-WAN Manager, BIND, Struts and ONLYOFFICE remain held; Strapi's http.component match is held for review; VeloCloud returns zero by two methods and stays PROVISIONAL. LiteLLM at 6,785 and ScreenConnect at 2,655 are not published as exposure figures for a seventh week, being port-scatter artefacts (top five ports nine, nine, eight, seven and seven, and four, three, two, two and two), and Langflow, MLflow and Ray are printed with the standing caveat that they show the same scatter at small totals, where a product facet of 100 per cent still corroborates the label and a count under 110 cannot mislead by thousands.¹⁹

7.2 Credential Exposure Around the Week's Listings and the Ampath Notice

The aggregator's infostealer panel (third-party stealer-log telemetry from HudsonRock and ParanoidLab shown on each victim page) for Europ Assistance South Africa shows 78 users, six employees and eleven third-party employees with stealer-log records, 1,470 passwords for the domain of which 60 are marked critical, and 19 external attack-surface findings; Aeroklas Duys shows one employee record and twelve passwords.^{5,9} These are counts of unknown age and say nothing about how either intrusion began. They bear on two of this week's catalogue entries directly: the PAN-OS flaw needs a credential and the FortiOS flaw needs an administrator, and a stealer log is where such credentials are found. For Ampath the relevant exposure is the patient side. The data categories in its notice are the fields a caller needs to pass as the laboratory, the medical scheme or a bank, and its own advice to patients, protective registration with the Southern African Fraud Prevention Service and suspicion of any unexpected request for banking details, is the right reading of that exposure.¹

7.3 The Edge Population the Week's Entries Describe

Three of the four edge entries have no South African figure, and that absence is itself the finding for this section: an Ivanti Connect Secure appliance, a Secure Email Gateway or a PAN-OS management interface reachable from the internet in South Africa cannot be counted by this collection, and the organisations running them are the only ones who know. The FortiGate figure is the one population that can be stated, 2,801 instances with 1,524 answering on the SSL VPN port, and it is the same population the FortiBleed

advisory of W42 addressed, so the user-list audit from that edition and the administrator-session precondition of this week's FortiOS entry point at the same control: who holds an administrator credential, where it has been, and whether the management plane answers the internet at all.^{19,45} The W42 NetScaler checks stand for the 146.

8. REGULATORY & POLICY

8.1 Ampath's Section 22 Notice as a Template, and the Number It Had to Answer

Section 22 of POPIA requires a responsible party that has reasonable grounds to believe personal information has been accessed by an unauthorised person to notify the Information Regulator and the data subjects as soon as reasonably possible, in a form that gives enough information for the data subject to take protective measures. Ampath's notice of 13 October, as the press carried it, does that in the way the regulator's own guidance describes: the categories of data, a description of the possible consequences, the measures taken, the advice to data subjects (do not engage with anyone claiming to hold the data, watch accounts and credit records, consider protective registration with the fraud prevention service) and the identity of the actor.^{1,2} What it did not do, and could not have done on 13 October, was state a number of individuals, and the actor supplied one instead. Ampath's answer the next day is the part other organisations should study: it explained the difference between a row and a person in one paragraph, conceded that information was affected, and asked the public to treat the actor's figure as unverified.⁴ The regulator's media page and enforcement register carried nothing on Ampath by 18 October, and the notice itself was not located on the company's site, so the record rests on the press.^{28,47,48} Bootlegger's statement of 16 October that it will notify the regulator is the week's second disclosure made before any actor or journalist forced it, for an exposure of franchisee and manager data.²²

8.2 Gauteng's Approach to SAPS and the Absence of a Research Safe Harbour

The Cybercrimes Act makes unlawful access to a computer system an offence under section 2 and unlawful interception of data under section 3, with no exception for security research or responsible disclosure; the only protection a researcher has is prosecutorial discretion and the facts. The Gauteng Department of e-Government's position, as its MEC put it to MyBroadband, is that opening a police case when a security breach is recorded is standard practice and that any possible illegal activity needs investigation, and it has told SAPS so; SAPS, by the department's account, advised that the developer as custodian should open the case.²³ The researcher's account is that the database answered without credentials and that no law was broken; the DA has asked the MEC to state the basis for charges and whether a case is registered.^{31,23} Two regulatory questions sit beside the legal one. The department's SMS to residents, sent after the fix, is the only notice they have received; it names no data category, no period of exposure and no regulator, and section 22 asks for more than that. And the department has not said whether it notified the Information Regulator, whose online reporting platform has existed since April 2025; the regulator's pages carried nothing on the matter on 18 October.²⁸ For a board the question is simpler than the law: whether the organisation's written response to an outside disclosure begins with the fix and the thanks or with the

charge.

8.3 Parliament, the Election and the State's Own Posture

The Defence Minister's written reply to Irvin Mogale MP, reported by MyBroadband on 17 October, describes the SANDF's posture against the Interpol assessment the question cited: security monitoring of its networks, monthly vulnerability assessments and two penetration tests a year, a Cyber Defence Strategy and Action Plan for 2025 to 2030, partnerships with SITA and the State Security Agency, and training at Stellenbosch University; the reply's own framing is professionalising and capacitating Cyber Command personnel.⁴⁹ The same article carries the Weather Service's account of the January 2025 RansomHub incident, which cut its fourth-quarter performance to 36 per cent of targets from 91 the quarter before, a quantified operational cost of ransomware on a South African state entity.⁴⁹ The local government elections are on Wednesday 4 November. The IEC's disinformation code has bound parties and candidates since 4 September, with a 36-hour retraction duty, a ban on fake accounts, bot networks and doxing, labelling of AI-generated content and Real411 as the reporting channel.²⁷ Telkom announced a R20 million connectivity partnership with the IEC on 16 October with no security content in the announcement, and the regulator's March 2024 statement on an IEC security compromise is the precedent for what the coming fortnight can produce.^{50,28} The heatmap movement in Section 2 rests on that calendar, and Section 11 sets the distinguishing tests.

8.4 Fraud Advisories and Awareness Month

October is Cybersecurity Awareness Month; the Film and Publication Board's campaign, carried by The Citizen on 17 October, is the basic hygiene list.⁵¹ BusinessTech's WhatsApp warning of the same day is more specific: account takeover through SIM swap and through links that register the account on another device, with the tell-tale a sudden loss of signal or a notice that the number is registered elsewhere, and Discovery Bank's line that a bank never asks a customer to approve a reversal; it carries BioCatch's survey figures of 85 per cent of banking leaders reporting more fraud attempts and 81 per cent estimating annual fraud losses above five million dollars.²⁹ MyBroadband's account of Kaspersky's darknet research puts a DDoS kit at one dollar and upwards, against Seacom's estimate of up to R2.5 million per attack for a South African company and the May 2026 week against SARS eFiling, News24 and BusinessTech at a 1 Tbps peak; with an election in a fortnight that belongs in the Section 11 watch.⁵² SARS's scams page carried nothing new on 18 October; SARS-SCAM-400 of 2 September remains the newest alert.⁵³

8.5 The Regulator's Record and Who to Call

The Information Regulator's enforcement notices register is unchanged, with the Gauteng Department of Health instrument of 10 June 2026 its newest entry, and the media page's newest item remains the 21 September advisory; the newest enforcement statement is 2 June. The MIP, RelyComply, e-Panic, Cartrack, CoverCubed and LegalWise matters are before the regulator with no public instrument, and Ampath and Bootlegger join the list of notified or to-be-notified compromises on which it has said nothing.^{47,28} **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 (csirt@sanren.ac.za) and UCT CSIRT (uctcsirt@uct.ac.za) for research and education, and the

Standard Bank Group and Vodacom teams for their own constituencies.⁵⁴ For a laboratory, scheme or administrator in Ampath's position the clocks are: as soon as reasonably possible to the Information Regulator under section 22; 72 hours to SAPS under section 54 of the Cybercrimes Act where the organisation is a financial institution or an electronic communications service provider; 24 hours to the Prudential Authority under Joint Standard 2 of 2024 for a regulated financial institution; and the Council for Medical Schemes or the Health Professions Council as the sector regulator where one applies.

47. Information Regulator, Enforcement notices register, checked 18 October 2026 (newest entry Gauteng Department of Health, 10 June 2026). <https://infoeregulator.org.za/enforcement-notice/>

48. Ampath Laboratories, website home page and news page, read 18 October 2026 (no incident notice on either; the section 22 notice quoted by the press was not located on the site). <https://www.ampath.co.za/>

49. MyBroadband, South African military responds to Interpol cyberattack warning, by Myles Illidge, on Defence Minister Angie Motshekga's reply to Irvin Mogale MP (17 October 2026). <https://mybroadband.co.za/news/security/672344-south-african-military-responds-to-interpol-cyberattack-warning.html>

50. IT-Online, Telkom ramps up digital infrastructure for Election Day (16 October 2026). <https://it-online.co.za/2026/10/16/telkom-ramps-up-digital-infrastructure-for-election-day/>

51. The Citizen, South Africans warned how one stolen password could expose their accounts, by Oratile Mashilo, on the Film and Publication Board's Cybersecurity Awareness Month campaign (17 October 2026). <https://www.citizen.co.za/news/south-africa/south-africans-warned-how-one-stolen-password-could-expose-their-accounts/>

52. MyBroadband, R16.50 destroy-a-company kit that causes R2.5 million in damage to South African organisations per attack, by Luis Monzon, on Kaspersky research and a Seacom estimate (16 October 2026). <https://mybroadband.co.za/news/security/672232-r16-50-destroy-a-company-kit-that-causes-r2-5-million-in-damage-to-south-african-organisations-per-attack.html>

53. SARS, Scams and phishing alerts page, checked 18 October 2026 (newest alert SARS-SCAM-400, fake High Court summons, 2 September 2026). <https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>

54. ransomware.live API, GET /csirt/ZA, six South African CSIRTs from the FIRST directory, retrieved 18 October 2026 (feeds/r1_csirt_za_2026-10-18.json). <https://api.ransomware.live/v2/csirt/ZA>

9. WEEKLY THREAT HUNT & IOCs

Eight missions. Three P1 cover the three exploited edge flaws with the vendors' own artefacts: Ivanti's header and Previdian's addresses, Cisco's log strings and version check, and Palo Alto Networks' three addresses and threat signatures. Five P2 cover the application-compromise and patient-fraud pattern the Ampath record describes, the AhsayCBS chain with Huntress's file and service names, the seven addresses on The Gentlemen's feed that earlier editions did not export, Deadlock's sample and behaviours, and Atlassian's traversal pattern.²⁰ Indicators come from vendor advisories, named responder reporting and the aggregator's per-group feeds; every atomic indicator is exported to iocs_w43.csv with the URL that supports it. The W42 NetScaler SAML, AA26-281A and FortiBleed missions and the W40 Gentlemen mission stand as written and are not reprinted.

TH-2026-W43-01: Ivanti Connect Secure: One Header, Four Addresses, and a Checker That May Not See It

P1 CRITICAL: zero-day exploited from 3 October; overdue from 17 October; no ZA figure

Hypothesis: An attacker has sent a crafted X-DSCGI-PATH request to an Ivanti Connect Secure gateway, bypassed authentication through CVE-2026-104935, chained a privilege-escalation flaw to root, and is pulling appliance credentials, Active Directory metadata and BitLocker recovery keys while re-exploiting the device for each command and clearing logs, so that the Integrity Checker Tool reports clean.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1068 (Exploitation for Privilege Escalation), T1003 (OS Credential Dumping), T1558.003 (Kerberoasting), T1087.002 (Domain Account Discovery), T1070 (Indicator Removal).

IOCs: Inbound requests carrying the header X-DSCGI-PATH; source addresses 216.73.160[.]59, 216.73.160[.]61, 216.73.160[.]210 and 45.8.19[.]111 (Previdian, honeypot attackers, 14 October); builds 25.1.1.1 and earlier, 25.1.2.2 and earlier, 22.8R2.4 and earlier; Volatility's indicators on its GitHub repository as cited by Rapid7.

Data Sources: Gateway web access and event logs (forwarded to a SIEM, since on-box logs were modified); network capture at the perimeter; domain controller 4769 events with RC4 service tickets from the appliance's address; LDAP query logs; memory image of the appliance if compromise is suspected.

Detection Guidance: On Monday 19 October upgrade to 22.8R2.5, 25.1.1.2, 25.1.3.0 or 25.1.3.1 and, before or after, search gateway logs since 1 October for the header string and the four addresses, and search domain logs for Kerberoasting and LDAP searches for ms-FVE-RecoveryPassword from the appliance's address. Treat a clean Integrity Checker result as no information. On any hit: back up the configuration, factory reset or rebuild, upgrade, restore, and rotate every password, certificate and API key the appliance held, per CISA. Sources: The Hacker News 14 October (Previdian addresses, Volatility findings), BleepingComputer 14 October (CISA guidance), Rapid7 13 October (versions), the catalogue entry.

TH-2026-W43-02: Cisco Secure Email Gateway: The grep, the Version Check and the Attachment Path

P1 CRITICAL: exploited in October; overdue from 18 October; second SEG entry in five weeks

Hypothesis: An attacker has sent a crafted attachment through a Secure Email Gateway with File Reputation enabled and Content Scanner Tools older than 25.3.0.5525, written a file to the operating system through CVE-2026-76519, and obtained root on the appliance, from which it is reading mail flow or staging onward access.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1566.001 (Spearphishing Attachment), T1505.003 (Web Shell), T1114 (Email Collection), T1070.002 (Clear Linux or Mac System Logs).

IOCs: Log lines in system_logs: System Security: Suspected compromise indicator was found (compromise); System Security: Security scan did not complete (contact TAC); System Security: No compromise indicator was found (clean). Content Scanner Tools version below 25.3.0.5525 from the contentscannerstatus command; AsyncOS below 15.5.5-014 or 16.5.0-780; File Reputation enabled under Advanced Malware Protection on any mail policy. The W39 mission's artefacts for CVE-2026-76461 remain in scope.

Data Sources: The appliance's system_logs on every cluster member; firewall and proxy logs for connections from the appliance's address to external hosts; mail logs for attachments that produced AMP scan errors; configuration audit logs.

Detection Guidance: On Monday 19 October run grep "System Security" system_logs on every appliance and cluster member and record the result; run contentscannerstatus and update Content Scanner Tools to 25.3.0.5525 or later, which needs no upgrade or restart; then schedule the AsyncOS upgrade. A suspected-compromise line is an incident: open the Cisco TAC case, renew credentials and cryptographic material, restrict access to the appliance, and read the firewall logs for the appliance's own outbound connections since 1 October, because root access allows the appliance logs to be edited. Sources: Cisco advisory cisco-sa-esa-afw-zqYJkxp, BleepingComputer 14 October, the catalogue entry.

TH-2026-W43-03: PAN-OS Management Interface: Three Addresses and the Credential Precondition

P1 CRITICAL: very limited exploitation per the vendor; overdue from 18 October; no ZA figure

Hypothesis: An attacker holding a valid PAN-OS administrator credential, taken from a stealer log, a prior intrusion or reuse, has reached the management interface over the network and used CVE-2026-0322 to execute code as root on a firewall or Panorama appliance.

MITRE ATT&CK: T1078 (Valid Accounts), T1190 (Exploit Public-Facing Application), T1068 (Exploitation for Privilege Escalation), T1601 (Modify System Image).

IOCs: Addresses 66.42.72[.]14, 208.83.239[.]114 and 149.248.47[.]234 (vendor advisory, associated with threat activity and limited exploit attempts); management-interface authentication from any address outside the organisation's administrative range; PAN-OS without the fixed hotfix for its maintenance release (the fixed builds per line are in iocs_w43.csv); Threat Prevention IDs 510046 and 510047 (content 9159-10287 or later, require SSL decryption, partial coverage per the vendor).

Data Sources: Management-plane authentication and configuration logs; Panorama audit logs; system logs for unexpected processes or file changes; threat logs for the two signature IDs; upstream firewall or router logs showing who reached the management port.

Detection Guidance: On Monday 19 October confirm whether any management interface is reachable from the internet and remove it; patch each line to its fixed release; search management authentication logs since 1 October for the three addresses and for any successful administrator login from outside the administrative range; reset every administrator credential that has appeared in a stealer log. Treat a hit on the three addresses as an incident. Sources: Palo Alto Networks advisory CVE-2026-0322, BleepingComputer 14 October, the catalogue entry.

TH-2026-W43-04: The Ampath Pattern: Application Compromise, Bulk Export, Forum Post

P2 HIGH: confirmed South African intrusion; actor publishes no tooling; patient-facing fraud follows

Hypothesis: A data-leak operator has exploited a vulnerability in an internet-facing application, used it to reach backing databases, exported whole tables over days or weeks, and is now offering samples on a criminal forum while contacting the organisation about payment; a second actor is using identity numbers and medical-scheme membership numbers from the set to impersonate the laboratory, the scheme or a bank to patients.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1213 (Data from Information Repositories), T1048 (Exfiltration Over Alternative Protocol), T1567 (Exfiltration Over Web Service), T1656 (Impersonation), T1598 (Phishing for Information).

IOCs: No atomic indicators are published for the Ampath intrusion and none are invented here. Actor handles from KELA: ByteToBreach on DarkForums, Dread and Telegram (@ByteToBreach); former Telegram names CvHNWwEG and inesslopez. Pattern indicators from Ampath's containment list: malicious addresses blocked, unauthorised files on a web server, compromised accounts, an application vulnerability, a web server restored from backup.

Data Sources: Web application and reverse-proxy access logs; database audit logs (bulk SELECT or export volumes per account per hour); egress volume by server; web server file-integrity monitoring; call-centre and fraud hotline logs for callers quoting membership numbers; the organisation's own name on DarkForums and Telegram.

Detection Guidance: From Monday 19 October, hunt for database accounts whose read volume in a day exceeds their 90-day median by an order of magnitude, for web servers with new files in web-accessible paths, and for outbound transfers from database or application hosts to addresses outside the organisation's providers. For the fraud stage, brief call centres that a caller quoting a correct medical-scheme number or payment date is not thereby verified, route impersonation reports to one queue, and count them weekly. Sources: TechCentral 14 October and ITWeb 15 October for the containment list; KELA for the actor profile; the detection logic is the report's own.

TH-2026-W43-05: AhsayCBS: Web Shells, a Miner Called edge.exe and a Patch That Does Not Work

P2 HIGH: exploited from 7 October; overdue from 18 October; victims are MSP customers

Hypothesis: An attacker has reached an AhsayCBS backup console from the internet, bypassed authentication through CVE-2026-105133 at checkSysPwd, injected commands through CVE-2026-105134 at the Replication Receiver's UpdateReceivers.do endpoint, dropped a JSP web shell, installed an XMRig miner as a Windows service, and may be using the same access to reach the backups the console manages.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1543.003 (Windows Service), T1496 (Resource Hijacking), T1036.005 (Match Legitimate Name or Location), T1068 (Exploitation for Privilege Escalation, vulnerable driver), T1562.001 (Impair Defenses).

IOCs: Request paths /rps/api/json/UpdateReceivers.do with a manipulated random parameter; files edge.exe (XMRig), msedge.exe (modified NSSM), Taskmgr.ps1, WinRingOx64.sys in the TEMP folder; service name MicrosoftEdgeUpdateSvc; JSP files new to the console's web directories; AhsayCBS 10.3.4 and earlier including the version the vendor called fixed; certutil.exe downloading a .sys file.

Data Sources: AhsayCBS web server access logs; Windows Security 4697 and System 7045 service-creation events; Sysmon 1, 11 and 13; EDR telemetry for certutil and PowerShell; CPU utilisation baselines; backup job logs for unexplained restores or deletions.

Detection Guidance: On Monday 19 October restrict every AhsayCBS console to trusted addresses or a VPN; search for the service name, the four file names and new JSP files; alert on service creation whose binary path is outside Program Files and on any process named edge.exe that is not Microsoft-signed. On a hit, Huntress's advice is a full restore of the host from a known-safe backup, since a web shell may remain; verify that backups the console manages were not touched. Managed service providers apply this per client tenant. Sources: BleepingComputer 9 October, The Hacker News 9 October, the catalogue entries.

TH-2026-W43-06: The Gentlemen: Seven Addresses Not Yet Exported, One New Hash, and Europ Assistance Listed

P2 HIGH: seven feed addresses missed since 11 October; CLAIMED listing in a 33-name batch

Hypothesis: An affiliate of The Gentlemen has encrypted or exfiltrated from a South African estate using the tooling catalogued in TH-2026-W40-06, with command or staging traffic to one of the addresses, or contact over the Session identifier, that the aggregator added to its indicator feed in October.

MITRE ATT&CK: T1486 (Data Encrypted for Impact), T1567 (Exfiltration Over Web Service), T1071 (Application Layer Protocol), T1657 (Financial Theft).

IOCs: Addresses on the feed since 11 October and not previously exported: 193.143.1[.]142, 194.87.31[.]69 (also listed with port 36137 since 18 October), 178.130.46[.]120, 193.228.128[.]2, 192.42.116[.]104, 89.185.80[.]134, 92.39.211[.]142; second Session identifier 050faeadd876483d807abfc0fd70274d31f42bbc8a8e1c1abc626a70fe62ae3f2d; MD5 886888ccad9b4726c095fd42fce9ea22 added 18 October. Unchanged: 34 SHA-256, four SHA-1, 47 earlier MD5, six Tox identifiers, the first Session identifier, two email addresses and the ransom-note YARA rule, all exported in W40. Europ Assistance South Africa listed 16 October 09:31 UTC.

Data Sources: Firewall and proxy logs for the seven addresses; EDR hash telemetry; the W40 YARA rule on file servers and backup shares; dark-web monitoring for the organisation's own name under any country tag.

Detection Guidance: On Monday 19 October add the seven addresses and the hash to blocklists and retro-hunt 30 days of proxy and firewall logs for them; re-run the W40 YARA rule. The feed gives no role for the addresses (C2, staging or scanning), so a hit is a lead for investigation and a block, and no more. For an insurer, administrator or scheme the standing action is the own-name watch across aggregators with the country field ignored, since this group listed 33 names in one morning. Sources: the aggregator's indicator feed (api.ransomware.live/v2/iocs/thegentlemen), retrievals of 4, 11 and 18 October; the victim page.

TH-2026-W43-07: Deadlock: A Session Identifier in the Note, AnyDesk, and a Driver That Blinds the EDR

P2 HIGH: second South African listing in seven weeks; one vendor sample hash; initial access unknown

Hypothesis: An affiliate of Deadlock has gained access to a South African estate by a method the public record does not describe, installed AnyDesk for persistence, loaded a vulnerable driver to disable endpoint protection, exfiltrated data, and run a custom-cipher encryptor that drops a text note and an HTML note carrying a Session identifier and an embedded copy of the leak site.

MITRE ATT&CK: T1219 (Remote Access Software), T1068 (Exploitation for Privilege Escalation, vulnerable driver), T1562.001 (Impair Defenses), T1486 (Data Encrypted for Impact), T1491.001 (Internal Defacement), T1567 (Exfiltration Over Web Service).

IOCs: Sample SHA-256 9e69862c4a5b34c12c10fbf2d345e7fd654c71adcb5f9b6524d7a54209fce343 (WatchGuard, compiled early June 2026); leak sites deadlock.liveblog365[.]com (clearnet, failing DNS on 18 October) and deadblogbdu5wprek7wa2o4ce7rnt6u6ntqeud3hzjvcveosgpsqqd[.]onion; an HTML ransom note with About, Chat and Blog tabs; a Session identifier in the note; AnyDesk installed outside change control; proxy addresses resolved from Polygon smart contracts (no addresses published). No record on the aggregator's indicator or YARA feeds.

Data Sources: EDR driver-load telemetry (Sysmon 6) and known-vulnerable-driver blocklist hits; AnyDesk installation and connection logs; DNS and proxy logs for the clearnet leak domain and for Polygon RPC endpoints from servers; file-creation telemetry for HTML notes on shares.

Detection Guidance: From Monday 19 October alert on a driver load from a user-writable path or a driver on the Microsoft vulnerable-driver blocklist; on AnyDesk appearing on a host where it is not an approved tool; on servers resolving blockchain RPC endpoints; and on HTML files dropped across a share within minutes. Search EDR hash telemetry for the WatchGuard sample. Sources: WatchGuard Secplicity 8 June, ZeroFox 29 June, the aggregator's group page; the MITRE mapping is the report's own.

TH-2026-W43-08: Atlassian Data Center: Traversal Requests Against Eight Products

P2 HIGH: exploited after a public proof of concept; overdue from 19 October; no ZA figure

Hypothesis: An attacker is sending requests with encoded or plain double-dot sequences adjacent to a slash, backslash or double colon to an internet-facing Bitbucket, Confluence, Jira, Jira Service Management, Bamboo, Crowd, Crucible or Fisheye Data Center instance, reading configuration files under the web root whose paths are known, and harvesting database credentials or secrets from them.

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

IOCs: Request URLs containing .. adjacent to /, \ or :: in plain or URL-encoded form (Atlassian's own blocking rule); versions below Bitbucket 9.4.26, 10.2.8 or 10.5.1, Confluence 9.2.26 or 10.2.19, Jira and Jira Service Management 9.12.40 or 5.12.40, 10.3.26 or 11.3.12, Bamboo 10.2.24 or 12.1.12, Crowd 6.3.7, 7.0.3, 7.1.7 or 7.2.4, Crucible and Fisheye 4.9.15; the catalogue entry; Atlassian states it cannot confirm whether a given Data Center instance was affected.

Data Sources: Reverse proxy and Tomcat access logs; WAF logs; application access logs; database authentication logs for new sources after a suspected read.

Detection Guidance: On Monday 19 October take any internet-exposed Data Center instance offline or put the WAF rule, the Tomcat RewriteValve or the Bitbucket urlrewrite rule in front of it, then patch to the maintenance release; search access logs since 5 October for the traversal pattern against known configuration file names and rotate any credential held in a file that was requested. Sources: Atlassian advisory of 5 October, BleepingComputer's 13 October Patch Tuesday roundup for the post-PoC exploitation, the catalogue entry.

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

- 1. Run the three edge compromise checks before the three edge patches, and record both, by Wednesday 21 October.** The Ivanti header and addresses, the Cisco log grep and the Palo Alto addresses are in TH-2026-W43-01 to 03. The checker that may not see the Ivanti intrusion is the lesson: a tool result covers only what the tool measures, so the log search decides.
- 2. Add a decommissioning check to change management.** Bootlegger's exposure was a migrated application still answering. For every system retired or migrated in 2026, confirm by Friday 23 October that the old endpoint returns nothing, and test every internally built dashboard for data delivered with the login page, which is a view-source test that takes a minute.
- 3. Put the backup, remote-support and firewall management consoles behind an allow-list by Wednesday 21 October.** AhsayCBS has no working patch; BeyondTrust Remote Support and PAN-OS management are in the catalogue; the common control is that none of them should answer an arbitrary internet address. Managed service providers apply it per tenant.
- 4. Build the database-export baseline the Ampath pattern needs, by Friday 30 October.** A data-leak operator's intrusion produces no encryption event to alert on; it produces a read volume. Establish, by account and by day, the normal read volume of every database holding personal information, and alert on an order-of-magnitude departure; TH-2026-W43-04 gives the structure.
- 5. Treat the Windows Mark of the Web bypass as a mail-gateway and endpoint policy item, since no indicators are public.** Apply the October release by Wednesday 21 October; block or sandbox container formats (ISO, IMG, VHD) and shortcut files at the gateway; and alert on Office or script hosts launched from a file in Downloads that carries no Zone.Identifier stream, which is the condition the bypass produces. The detection logic is the report's own.
- 6. Add the seven addresses, the Session identifier and the new MD5 on The Gentlemen's feed, and the Deadlock sample hash, to blocklists on Monday 19 October and retro-hunt 30 days.** All are in iocs_w43.csv with their sources; the W40 hash set stands.

Management (CISO / Board)

- 1. Commission by Friday 23 October the Ampath answer: a written, pre-approved response to a claimed record count, ready within 24 hours.** It needs three inputs the security team cannot supply alone: which systems hold one row per person and which hold one per event; who signs a section 22 notice and how fast; and what the organisation will say about banking and clinical or equivalent sensitive data when it does not yet know. Ampath produced that answer in a day; an answer that fast is rarely improvised, and the inputs above are what it needs.
- 2. Decide, as policy, what the organisation does when an outsider reports a flaw, and table it for the Monday 26 October agenda.** The Gauteng department's stated answer was to approach the police. The alternative is a published disclosure channel, a commitment not to pursue a good-faith reporter who stays

within the data needed to demonstrate the flaw, and a fix-first sequence. South African law gives no safe harbour, so the policy is the only one a researcher can rely on, and it is the board's to set.

3. Ask the risk committee, for Monday 26 October, for the edge-appliance inventory with a new column: whether a compromise check exists that the vendor's own tool does not perform. For Ivanti the answer this week is that CISA says the vendor's checker may not detect the current intrusion; for Cisco the check is a log grep; for Palo Alto it is a credential question. An inventory that lists patch level alone is the wrong instrument for the quarter the edge is having.

4. If the organisation administers insurance, claims or scheme business for others, assume a listing and plan its first 48 hours by Friday 23 October. The Gentlemen has listed four South African insurance names since 7 September, then Europ Assistance South Africa (an assistance and claims-administration company by the aggregator's description) among 33 names in one morning. The holding statement, the regulator notification record, the decision on engagement and the own-name watch are the W42 action; the Microsoft caution that this group's leak-site volume may be posted for effect is a reason to prepare the statement in advance; it does not excuse leaving it unwritten.

5. Put the election fortnight on the agenda for Monday 26 October. Local government elections are on 4 November; the public precedents are the 2024 IEC compromise statement and the May 2026 DDoS week against SARS eFiling and two news sites. For a municipality, a utility or a media organisation the questions are DDoS capacity, the integrity of public-facing results and notice pages, and who speaks if a hacktivist channel claims an outage that did not happen.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH, 26th CONSECUTIVE WEEK

The South African cyber threat level remains HIGH for a twenty-sixth consecutive week (11 to 17 October 2026). Escalation to CRITICAL was considered on Ampath and rejected: the incident is confirmed and the data set is large by any reading, but the company reports services operational and no clinical data evidence, no systemically important institution is out of service, and the actor's figure is unverified. De-escalation to MEDIUM was not in question with two new South African listings, a confirmed intrusion at a national pathology group, four exploited edge-appliance flaws in one week against unmeasured populations, and an election in a fortnight.

Rationale

A national pathology group confirmed an intrusion and a data-leak operator is selling the result.

Identity numbers with medical-scheme and payment data, taken through an application vulnerability by an actor whose model is the forum post, with the count disputed and the sample not yet published.

Four exploited edge flaws entered the catalogue in a week, two before a fix existed, and the populations are unmeasured. Ivanti Connect Secure with an integrity checker CISA says may not detect it, Cisco Secure Email Gateway for the second time in five weeks, PAN-OS management and FortiOS; 2,801 FortiGates are the only South African population this collection can count.

The Gentlemen listed Europ Assistance South Africa in a 33-name batch in the week Microsoft placed it fourth by leak-site postings. Thirteen South African names since January, five in insurance and administration since 7 September; what the batch means is the open question and the confirmation rate is the test.

Deadlock took a second South African listing in seven weeks with no indicators on the feed. An encrypting operation with a working leak site and a thin public record; the hunt rests on one vendor sample and behaviours.

The elections are on Wednesday 4 November. No hostile activity is observed; the score movement in Section 2 is forward-looking and rests on the calendar, the IEC's code and the 2024 precedent.

Next-Week Watch (W44)

Ampath. The distinguishing observations are a published sample on the forum (which would show which fields the actor holds), an Ampath count of individuals, an Information Regulator statement, and the first patient-targeted fraud reports quoting medical-scheme numbers. The notice itself should be located on the company's site or obtained; this edition cites it through the press.

Europ Assistance South Africa and the 16 October batch. A company statement; whether the record acquires a timer, a directory profile or a sample; and, for the batch, how many of the 33 confirm within a month. Confirmation by a third or more of the 33 within a month would weigh against Microsoft's attention-seeking reading; fewer than five confirmations would support it.

Aeroklas Duys and Deadlock. A company statement, a sample, or a third South African listing. Any incident responder's report on a Deadlock intrusion that names the initial access would fill the gap the public record has.

The e-Panic case. A registered case number and against whom; the departmental report the MEC has promised, with an exposure period and an access-log analysis; whether the regulator was notified and when. The Bootlegger section 22 notice is the small companion test.

The election fortnight. Three observations would distinguish a campaign from noise: an IEC or Real411 statement on volume or a specific operation; an outage of an IEC, municipal or media property attributed by the operator, as against a hacktivist channel's claim of one; and any defacement or data claim against a municipality. A claim without an operator's confirmation stays CLAIMED, as in May.

The catalogue. Whether SonicWall SMA 1000 CVE-2026-102255 is added, now two weeks after the first exploitation attempts; whether Ivanti publishes the privilege-escalation fix Volexity described and whether it enters the catalogue; and whether Atlassian or Cisco state exploitation volumes. The W42 NetScaler fortnight for a South African compromise runs to Sunday 25 October and closes next edition.

The Gentlemen's feed and UmBra's site. Whether the October additions to the indicator feed are followed by more, which would suggest a sample reached analysts; whether UmBra's site returns or the group lapses, which decides whether Tharisa's record is a one-week group's claim.

Collector tasks. Build Ivanti Connect Secure and PAN-OS exposure fingerprints, which the panel lacks; retire the SonicWall family sum in favour of the single product query; the port-concentration test, now seven weeks outstanding; the name-keyed world-feed search; the Saturday-evening media sweep; and the rule that a company check reads the media centre as well as the home page, applied this week to Ampath (home and news pages) and to Tharisa's SENS page.

Closed this week. The Tharisa production-report test (silence; stays CLAIMED, moves to record). The ATNS 16 October test (unobserved). The BlackLocks tempo question (unanswered; three listings since 5 September). The W42 SMA 1000 catalogue question (not added by 16 October; carried as a new question). Carried without re-argument: BCX, Guardrisk and CoverCubed, RelyComply, LegalWise, Samwumed and Edcon, Cell C Fibre, Cartrack, VSB Attorneys, Rohloff, The Courier Guy, Babcock, the Furniture Bargaining Council, Toyota's SMS provider, Implats, Hungry Lion and Rand Water.

12. OSINT SOURCES CONSULTED

All sources are TLP:CLEAR and publicly accessible, numbered in order of first citation. Every cited URL was retrieved and confirmed to contain the claim attributed to it, on 18 October 2026, with the exceptions this note records. The CISA catalogue URL is the public location of a file read locally. Ampath's section 22 notice is cited through TechCentral, MyBroadband, ITWeb and Bizcommunity because it was not located on the company's website. Ivanti's advisory for CVE-2026-104935 returned an error and is cited through Rapid7, The Hacker News and BleepingComputer. The Aeroklas Duys website refuses automated reading and the Europ Assistance website returned only its page title, so neither company's position could be checked beyond the absence of press coverage. The Microsoft Digital Defense Report is cited through TechCentral's reading and the report itself was not retrieved. The Sunday Times ATNS article carried no update and is not re-cited. **Collection notes.** The feed run completed at 02:05 UTC on 18 October 2026 and passed its integrity check; the victim feed and catalogue figures it produced are stated in Sections 5 and 6. The catalogue version is 2026.10.16, released 17:15 UTC on Friday 16 October, so additions of Saturday 17 October fall to W44. 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's index was unreadable by hand; the ITWeb item cited was reached by its own URL. **Corrections to prior editions.** The SonicWall family exposure figure (W40 2,912, W41 2,960, W42 2,965) summed five product strings, double-counted three of them and included a vendor-banner string whose facet is only 54 per cent SonicWall; it is withdrawn and replaced by the product:SonicWall count, 1,206 on 18 October. W42 described The Gentlemen's indicator feed as byte-identical to 27 September; the 11 October retrieval had added seven addresses and a Session identifier, exported this week. Both are in Section 1. **Exposure panel gap recorded.** No corroborated South African exposure query exists for Ivanti Connect Secure or for PAN-OS (the GlobalProtect title match remains BROKEN), so the two most urgent entries of the week carry no population figure. **Provenance of the machine-read feeds.** Every ransomware.live, NVD and EPSS figure was retrieved from those services' APIs and is cited as the endpoint called; the rendered ransomware.live pages are cited as cross-checks of records also present in the feed. **Figures withheld or held.** LiteLLM (6,785) and ScreenConnect (2,655) are disclosed here but not published as exposure figures, being port-scatter artefacts for a seventh week; the SonicWall family sum (3,266 this week) is withdrawn as above; Strapi's http.component match is held for review; VeloCloud's zero is PROVISIONAL; BeyondTrust Remote Support, AhsayCBS, Cisco Secure Email Gateway, the Atlassian products, BIND, Struts, ONLYOFFICE, Zammad, FortiMail, Catalyst SD-WAN Manager, Check Point, F5 BIG-IP APM, WSO2, Adobe Commerce and Zyxel have no product label and are held. **Description conflicts recorded.** The actor's 80 million figure for Ampath is carried beside the company's statement that it counts rows; the aggregator's description of Europ Assistance South Africa is not adopted; Atlassian's 9.3 is the vendor's score where NVD had none. **Attribution policy.** Where a publication broke a story this report names it and links to it. **Single-source disclosure.** The Microsoft figures (TechCentral); the SANDF reply, Bootlegger and the

Kaspersky and Seacom figures (MyBroadband); BioCatch (BusinessTech); the Previdian and SMA 1000 attempt counts (The Hacker News); the Deadlock sample hash (WatchGuard). **Claims deliberately excluded.** The Europ Assistance and Aeroklas Duys listings are carried as claims only; ByteToBreach's database and record counts are the actor's; KELA's attribution of the actor to a named individual is not repeated; the anonymous poster's account of how the Bootlegger application was built is that poster's; the aggregator's infostealer counts are third-party telemetry of unknown age; Microsoft's attention-seeking reading of The Gentlemen is carried as Microsoft's hypothesis; the Section 2 hacktivism movement rests on no observed campaign.

1. TechCentral, Ampath finds no evidence that test results were taken in breach, by Fanie van Rooyen (14 October 2026; quotes the 13 October notice and the 14 October statement). <https://techcentral.co.za/ampath-breach-no-evidence-test-results-taken/287314/>
2. ITWeb, Ampath downplays data breach claims, by Admire Moyo (15 October 2026; detection date 2 October, containment steps). <https://www.itweb.co.za/article/ampath-downplays-data-breach-claims/80KdWqDXQjmqbznQ>
3. MyBroadband, Attackers claim to have stolen 80 million South African patient records in massive Ampath Laboratories data breach, by Luis Monzon (13 October 2026). <https://mybroadband.co.za/news/security/672153-attackers-claim-to-have-stolen-80-million-south-african-patient-records-in-massive-ampath-laboratories-data-breach.html>
4. Bizcommunity, Ampath says data breach claims of 80 million patient records are overstated (14 October 2026; carries the 14 October statement). <https://www.bizcommunity.com/article/ampath-says-data-breach-claims-of-80-million-patient-records-are-overstated-303808a>
5. ransomware.live, victim page for Europ Assistance South Africa (The Gentlemen), discovered 16 October 2026 09:31 UTC, estimated attack date 14 October; no data size, deadline, sample or published-data marker; infostealer panel 78 users, 6 employees, 1,470 passwords (60 critical); read 18 October 2026. <https://www.ransomware.live/id/RXVyb3AgQXNzaXNOYW5jZSBtb3V0aCBBZnJpY2FAdGhIZ2VudGxlbWVw>
6. ransomware.live, group page for The Gentlemen, read 18 October 2026 (999 victims, 91 countries; 38 listings 11 to 17 October, 33 on 16 October; LegalWise, Samwumed and Edcon unchanged). <https://www.ransomware.live/group/thegentlemen>
7. ransomware.live API, GET /groups, 410 groups with victim counts, retrieved 18 October 2026 and compared with the 11 October retrieval (feeds/r1_groups_2026-10-18.json). <https://api.ransomware.live/v2/groups>
8. TechCentral, MIP attackers rank fourth on ransomware leak sites, says Microsoft, by Fanie van Rooyen, on the Microsoft Digital Defense Report 2026 (14 October 2026). <https://techcentral.co.za/microsoft-ransomware-south-africa-digital-defense-report-2026/287306/>
9. ransomware.live, victim page for Aeroklas Duys / Duys Engineering Group (Deadlock), discovered 12 October 2026 17:50 UTC, website aeroklasduys.co.za, no data size, deadline or published-data marker; infostealer panel 1 employee, 12 passwords; read 18 October 2026. <https://www.ransomware.live/id/QWVyb2tsYXNzaXN0YW5jZSBtb3V0aCBBZnJpY2FAdGhIZ2VudGxlbWVw>
10. ransomware.live, group page for Deadlock, read 18 October 2026 (107 victims, 42 countries; first discovery 15 June 2026; six listings in October). <https://www.ransomware.live/group/deadlock>
11. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.10.16, released 16 October 2026 17:15 UTC, retrieved 18 October (feeds/kev_2026-10-18.json). <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
12. BleepingComputer, CISA warns admins to immediately fix Ivanti flaw exploited as zero-day, by Sergiu Gatlan (14 October 2026). <https://www.bleepingcomputer.com/news/security/cisa-warns-admins-to-immediately-fix-ivanti-flaw-exploited-as-zero-day/>
13. Cisco, Security Advisory cisco-sa-esa-afw-zqYJkxjp, Cisco Secure Email Gateway Advanced Malware Protection arbitrary file write vulnerability (14 October 2026). <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkxjp>
14. Palo Alto Networks, Security Advisory CVE-2026-0322, PAN-OS: authenticated remote code execution in the management interface (14 October 2026, updated 15 October). <https://security.paloaltonetworks.com/CVE-2026-0322>
15. BleepingComputer, Microsoft October 2026 Patch Tuesday fixes 1,411 flaws, 3 zero-days, by Lawrence Abrams (13 October 2026). <https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2026-patch-tuesday-fixes-1-411-flaws-3-zero-days/>
16. Atlassian, CVE-2026-21589: arbitrary file access vulnerability impacts multiple products, security advisory (5 October 2026). <https://confluence.atlassian.com/security/cve-2026-21589-arbitrary-file-access-vulnerability-impacts-multiple-products-1870495748.html>
17. BleepingComputer, Unpatched AhsayCBS flaws exploited to deploy webshells, mine crypto, by Bill Toulas (9 October 2026). <https://www.bleepingcomputer.com/news/security/unpatched-ahsaycbs-flaws-exploited-to-deploy-webshells-mine-crypto/>
18. The Hacker News, Critical SonicWall SMA 1000 flaw targeted in 135 exploitation attempts after patch, by Ravie Lakshmanan (12 October 2026). <https://thehackernews.com/2026/10/critical-sonicwall-sma-1000-flaw.html>
19. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:01 UTC 18 October 2026 (feeds/shodan_za_2026-10-18.json). <https://www.shodan.io/search?query=country%3AZA>
20. ransomware.live API, GET /iocs/(group) for groups active against South Africa in the last 120 days, retrieved 18 October 2026 (feeds/r1_iocs_2026-10-18.json; The Gentlemen gained one address and one MD5 since 11 October; no Deadlock record). <https://api.ransomware.live/v2/iocs/thegentlemen>
21. ransomware.live API, GET /v2/countryvictims/ZA, 138 records, za_records 138 against server_returned 138, filter purity 1.0, FREE v2 tier (delayed relative to PRO), retrieved 02:00 UTC 18 October 2026 (feeds/ransomwarelive_za_2026-10-18.json). <https://api.ransomware.live/v2/countryvictims/ZA>
22. MyBroadband, CEO of top South African coffee franchise responds after vibe-coded web application exposed sensitive data, by Jan Vermeulen (16 October 2026). <https://mybroadband.co.za/news/security/672647-ceo-of-top-south-african-coffee-franchise-responds-after-vibe-coded-web-application-exposed-sensitive-data.html>
23. MyBroadband, Gauteng's plan to charge student who discovered a security flaw in R269-million app is absurd, by Luis Monzon (16 October 2026). <https://mybroadband.co.za/news/government/672623-gautengs-plan-to-charge-student-who-discovered-a-security-flaw-in-r269-million-app-is-absurd.html>
24. KELA, ByteToBreach: a deep dive into a persistent data leak operator (17 November 2025, updated 17 July 2026). <https://www.kelacyber.com/blog/byteto breach-a-deep-dive-into-a-persistent-data-leak-operator/>
25. Tharisa plc, SENS and RNS announcements page, read 18 October 2026 (Q4 and full-year production report, 13 October; Valterra offtake announcement, 15 October; neither mentions a cyber incident). <https://www.tharisa.com/sens-rns-announcements.php>
26. ZeroFox Intelligence, Flash report: DeadLock's ransomware leak site lists over 80 victims (29 June 2026). <https://www.zerofox.com/intelligence/flash-report-deadlocks-ransomware-leak-site-lists-over-80-victims/>

27. SANews, IEC gazettes code to tackle disinformation ahead of local elections (8 September 2026; code promulgated 4 September; elections 4 November 2026). <https://www.sanews.gov.za/node/84131>
28. Information Regulator, Media statements page, checked 18 October 2026 (newest item 21 September 2026; newest enforcement statement 2 June; nothing on Ampath, MIP or e-Panic). <https://infoeregulator.org.za/media-statements/>
29. BusinessTech, Warning for people using WhatsApp in South Africa, by Caitlyn Hilliard-Lomas (17 October 2026). <https://businesstech.co.za/news/telecommunications/880136/warning-for-people-using-whatsapp-in-south-africa/>
30. Europ Assistance South Africa, corporate website, checked 18 October 2026 (returned only its title and description; no notice readable). <https://www.europassistance.co.za/>
31. EWN, Gauteng emergency app exposed users' private information, by Sara-Jayne Makwala King (15 October 2026). <https://www.ewn.co.za/2026/10/15/gautengs-emergency-app-exposed-users-private-information>
32. WatchGuard Secplicity, DeadLock ransomware group embeds data leak site within ransom note, by Ryan Estes (8 June 2026). <https://www.watchguard.com/wgrd-security-hub/secplicity-blog/deadlock-ransomware-group-embeds-data-leak-site-within-ransom>
33. Miningmx, Tharisa lifts Q4 production, keeps Karo on track, by Liesl Peyper (13 October 2026). <https://miningmx.com/2026-10-13-tharisa-lifts-q4-production-keeps-karo-on-track/>
34. ransomware.live, group page for UmBra, read 18 October 2026 (ten victims; none after 10 October; site unavailable, 30-day uptime 56.7 per cent; Tharisa unchanged). <https://www.ransomware.live/group/umbra>
35. ransomware.live, victim page for LegalWise (The Gentlemen), discovered 30 September 2026 03:40 UTC, re-read 18 October 2026 (no deadline, sample or published-data marker on the record). <https://ransomware.live/id/TGVnYWxXaXNlQHRoZWdlbnRsZWllbg==>
36. ransomware.live, group page for BlackLocks, read 18 October 2026 (three victims, newest discovered 26 September 2026). <https://www.ransomware.live/group/blacklocks>
37. The Hacker News, CISA urges immediate Ivanti Connect Secure updates as honeypots log 105 exploit attempts, by Ravie Lakshmanan (14 October 2026). <https://thehackernews.com/2026/10/cisa-urges-immediate-ivanti-connect.html>
38. NIST NVD, CVE API 2.0, CVSS base scores with scoring source for the 54 catalogue entries added in the last 45 days, 53 resolved, retrieved 18 October (feeds/nvd_cvss_2026-10-18.json). <https://services.nvd.nist.gov/rest/json/cves/2.0>
39. FIRST, EPSS API, scores for the same 54 entries, retrieved 18 October 2026 (feeds/epss_2026-10-18.json). <https://api.first.org/data/v1/epss>
40. Rapid7, Ivanti Connect Secure zero-day exploited in the wild (CVE-2026-104935) (13 October 2026). <https://www.rapid7.com/blog/post/etr-ivanti-connect-secure-zero-day-exploited-in-the-wild-cve-2026-104935/>
41. BleepingComputer, Cisco patches actively exploited Secure Email Gateway zero-day, by Sergiu Gatlan (14 October 2026). <https://www.bleepingcomputer.com/news/security/cisco-patches-actively-exploited-secure-email-gateway-zero-day/>
42. BleepingComputer, Palo Alto Networks warns of PAN-OS RCE flaw exploited in attacks, by Lawrence Abrams (14 October 2026). <https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-pan-os-rce-flaw-exploited-in-attacks/>
43. The Hacker News, Attackers exploit AhsayCBS flaws to deploy web shells and cryptominers, by Ravie Lakshmanan (9 October 2026). <https://thehackernews.com/2026/10/attackers-exploit-ahsaycbs-flaws-to.html>
44. BeyondTrust, Security Advisory BT26-05, Remote Support improper origin validation, CVE-2026-102764 (15 October 2026). <https://www.beyondtrust.com/trust-center/security-advisories/bt26-05>
45. Fortinet PSIRT, FG-IR-26-122, Path traversal in CLI, CVE-2025-61624 (published 14 April 2026; Known Exploited: Yes when read 18 October 2026). <https://fortiguard.fortinet.com/psirt/FG-IR-26-122>
46. ransomware.live, South Africa country page, cross-check only (138 victims, Europ Assistance South Africa and Aeroklas Duys newest, read 18 October 2026, agreeing with the API file). <https://www.ransomware.live/country/ZA>
47. Information Regulator, Enforcement notices register, checked 18 October 2026 (newest entry Gauteng Department of Health, 10 June 2026). <https://infoeregulator.org.za/enforcement-notice/>
48. Ampath Laboratories, website home page and news page, read 18 October 2026 (no incident notice on either; the section 22 notice quoted by the press was not located on the site). <https://www.ampath.co.za/>
49. MyBroadband, South African military responds to Interpol cyberattack warning, by Myles Illidge, on Defence Minister Angie Motshekga's reply to Irvin Mogale MP (17 October 2026). <https://mybroadband.co.za/news/security/672344-south-african-military-responds-to-interpol-cyberattack-warning.html>
50. IT-Online, Telkom ramps up digital infrastructure for Election Day (16 October 2026). <https://it-online.co.za/2026/10/16/telkom-ramps-up-digital-infrastructure-for-election-day/>
51. The Citizen, South Africans warned how one stolen password could expose their accounts, by Oratile Mashilo, on the Film and Publication Board's Cybersecurity Awareness Month campaign (17 October 2026). <https://www.citizen.co.za/news/south-africa/south-africans-warned-how-one-stolen-password-could-expose-their-accounts/>
52. MyBroadband, R16.50 destroy-a-company kit that causes R2.5 million in damage to South African organisations per attack, by Luis Monzon, on Kaspersky research and a Seacom estimate (16 October 2026). <https://mybroadband.co.za/news/security/672232-r16-50-destroy-a-company-kit-that-causes-r2-5-million-in-damage-to-south-african-organisations-per-attack.html>
53. SARS, Scams and phishing alerts page, checked 18 October 2026 (newest alert SARS-SCAM-400, fake High Court summons, 2 September 2026). <https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>
54. ransomware.live API, GET /csirt/ZA, six South African CSIRTs from the FIRST directory, retrieved 18 October 2026 (feeds/r1_csirt_za_2026-10-18.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.