



SOUTH AFRICA

CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief, Week 42 | 4 October – 10 October 2026

THREAT LEVEL: HIGH

TLP: CLEAR

Report ID: SA-CTI-2026-W42 | Classification: TLP: CLEAR

Published Monday 12 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 (W42)**
- 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, 25th consecutive week (4 October - 10 October 2026)

Story 1. A ransomware group absent a week earlier from the index of ransomware.live, the leak-site aggregator this report collects from, listed Tharisa, the JSE- and LSE-listed platinum and chrome producer that mines in South Africa, with an 856 GB claim. UmBra's leak site was reported to the aggregator on 6 October, and by 10 October it carried nine victims in six countries by their descriptions. Tharisa was indexed at 08:23 UTC on 7 October.^{1,2,3} Tharisa had published nothing by the close of the window; its newest announcement on SENS, the JSE's regulatory news service, is the 30 September board change, and its investor calendar gives Tuesday 13 October (marked indicative) for the fourth-quarter production report, the first scheduled document that could address the listing.^{4,5} Rated CLAIMED: the volume, the data and the intrusion itself are the actor's assertions, and the aggregator itself marks the group as emerging and its claims as unverified; no South African publication had carried it by Saturday 10 October.

Story 2. The June breach of MIP Holdings, the insurance-software supplier whose stolen client data The Gentlemen has been publishing and extorting on since September, now reaches a fourth South African name: Hollard, Guardrisk, LegalWise and Samwumed; two of the four had told their members in June. Samwumed, the closed medical scheme for municipal workers in Cape Town, was listed by The Gentlemen at 03:40 UTC on 30 September in the same minute as LegalWise and Edcon, under a South Korean country tag that kept it out of the W41 edition; the correction below records it.^{6,7} LegalWise's media centre carries a statement of 26 June and an update of 6 July naming MIP Holdings as the third party and recording that its insurer, Legal Expenses Insurance Southern Africa (LEZA), notified the Information Regulator; Samwumed's section 22 notice of 29 June (the POPIA breach notification) names MIP as its former administration platform provider and says historical member data in MIP's legacy environment had not been deleted.^{8,9,10} TechCentral reported timers on the LegalWise, Samwumed and Edcon listings expiring around Friday 9 October, and none carried a published-data marker on Sunday 11 October; the listings stay CLAIMED and the two MIP exposures are CONFIRMED by the companies' own notices. First reported by TechCentral on 5 October 2026.

Story 3. CISA added six vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue in the window, one new NetScaler zero-day and five flaws published between 2015 and 2023 that a joint advisory shows a state-linked actor exploiting now.¹¹ Citrix's third NetScaler zero-day in a fortnight, CVE-2026-88779, crashes SAML-configured appliances and was exploited before its 3 October fix; CISA listed it on 4 October, and 125 instances are exposed in South Africa.^{12,13} The other five, ProFTPD CVE-2015-3306, ISC BIND CVE-2015-5477, Apache Struts CVE-2016-3081, ONLYOFFICE CVE-2021-3199 and Strapi CVE-2023-22894, are old flaws with fixes long available; CISA added them on Thursday 8 October on the strength of a seven-nation advisory on Chinese government-linked operators (working through the contractor Integrity Technology Group) with victims in Southeast Asia, Africa and North America; 185 ProFTPD instances are exposed in South Africa.^{14,15} Not yet in the KEV catalogue: a CVSS 10 SonicWall SMA 1000 flaw with honeypot attempts consistent with it since its 6 October fix, and an FBI and Secret Service advisory on FortiBleed citing SOCRadar's count of more than 86,644 compromised FortiGate devices.^{15,16}

W42 CORRECTIONS TO W41, two items. **First**, the W41 edition, covering 27 September to 3 October, counted three South African leak-site claims in its window. There were four. The Gentlemen listed Samwumed at 03:40 UTC on 30 September, in the same minute as LegalWise and Edcon, and the aggregator gave the record a South Korean country tag, so it was absent from the ZA-scoped feed and from the edition; it was found this week through TechCentral's reporting and confirmed on the aggregator's own record, whose description places the scheme in Cape Town.^{6,7} This is the second South African victim the aggregator's country field has hidden, after RelyComply under GB in W39. W41's statement that the group listed two South African names in one minute is corrected to three, its window count is corrected from three to four, and the Financial Services extortion score it set is unchanged because the row was already at the ceiling. **Second**, W41 stated that LegalWise's website carried no notice and that whether LegalWise was an MIP client was unknown. Both were wrong at publication: LegalWise's media centre has carried a statement since 26 June and an update since 6 July naming MIP Holdings, and the W41 check read the home page only.^{8,9} The LegalWise listing stays CLAIMED, because nothing shows the group holds LegalWise data, and the company's MIP exposure is CONFIRMED on its own statements. Both corrections are counted in the KPI row and recorded in Section 12.

KPI Dashboard

Metric	Current (W42)	Prior (W41)	Change	Direction
Overall SA threat level	HIGH	HIGH	No change (25th week)	FLAT
ransomware.live SA cumulative	136	135	+1	UP
SA claims discovered inside the window (ZA tag)	1	3	-2	DOWN
Window claims surviving the nationality check	1 of 1	3 of 3	n/a	n/a
SA victims found under another country tag (hand search of active groups' pages)	0	1 (corrected from 0)	-1	DOWN
SA organisations confirming a breach or supplier exposure in the window	0	1	-1	DOWN
New CISA KEV additions	6	7	-1	DOWN
KEV adds already overdue at publication	6	5	+1	UP
KEV adds with a published VERIFIED SA exposure figure	2 of 6	2 of 7	0	FLAT
Corrections issued to prior editions	2	1	+1	UP

Four notes on the table. The one claim is Tharisa, the only ZA-tagged record discovered between 4 and 10 October; the company is incorporated in Cyprus, holds its primary listing on the JSE and mines in South Africa, and it survives the nationality check (the report's test of whether a victim the aggregator tags ZA is in fact South African, applied because the tag has been wrong seven times this year) on its operations and listing with the domicile noted.¹⁷ The hand-search row is new to the table: it counts South African victims found under a country tag other than ZA, which a ZA-scoped feed cannot see; the W41 value is one by

correction (Samwumed) and the W42 value is zero, from a read of The Gentlemen's group page for every listing indexed between 1 and 10 October, reading each description for a South African location or domain.⁶ The confirmations row is zero: Tharisa had said nothing by 10 October, and the two company notices that resolve the LegalWise and Samwumed questions date from June and July and are not counted as confirmations made in this window. Shoprite's integrated report, which discloses four data breaches in its 2026 financial year, is carried as a disclosure in Section 3.4 and Section 8 with its release date unstated by the reporting.¹⁸ All six of the week's KEV catalogue additions were past their due date on Monday 12 October: the NetScaler entry by five days and the five advisory-driven entries, due Sunday 11 October, by one.¹¹

W42 KEY FRAMING: twice this week the record was already public and the report had not read it. A South African medical scheme sat on a leak site for eleven days under the wrong flag, and an insurer's own breach notice sat in its media centre for three months while the edition checked its home page. The lesson for the report is procedural and is recorded in Section 12. The lesson for a board is about sequence: LegalWise and Samwumed each published a third-party breach notice in June, and in the last week of September the group that holds the MIP data listed both of them; whether what it holds is theirs is unconfirmed, and the sequence is the point. For any organisation that disclosed a supplier breach this year the question is whether it planned for that second act, with a statement ready, its own name watched on leak sites under any country tag, and the regulator record in order, before the actor set a timer. On the technical side, NetScaler took its third zero-day in a fortnight against 125 exposed instances, CISA added five flaws from 2015 to 2023 to the KEV catalogue because a state-linked campaign with victims in Africa is exploiting them now, and the FBI and Secret Service repeated SOCRadar's count of more than 86,644 compromised FortiGate devices against a South African FortiGate population of 2,750.

TOP 3 ACTIONS THIS WEEK

1. On Monday 12 October, find every NetScaler that authenticates through SAML, run the compromise checks, then take it to 14.1-73.46 or 13.1-64.29. Two configuration strings decide scope, add authentication samlAction and add authentication samlIdPProfile; an appliance carrying either is exposed to the CVE-2026-88779 crashes and to the CVE-2026-107406 overflow Citrix fixed on 9 October, whatever it was patched to in September, and the later builds (13.1-37.283 on the FIPS and NDcPP line) cover both. Run the W41 artefact checks listed in TH-2026-W42-01 and the indicator-of-compromise script Citrix provides with bulletin CTX697174 first, keep the output, and pull the support bundle before patching any appliance with a reboot loop or a run of SAML failures since 1 October. The appliance owner reports to the CISO by Friday 16 October.

2. If your organisation published a third-party breach notice this year, prepare for the extortion stage of it by Friday 16 October. LegalWise and Samwumed told their members in June; the group set timers on them in late September. Have a holding statement that names the supplier and the data categories already disclosed, a watch on your own name and domain across leak-site aggregators with the country tag ignored, a decision taken in advance on engagement, and the dates and references of every notification already made to the Information Regulator, the Prudential Authority and the FSCA. For an insurer the W41 question stands: a written answer from each binder holder (an intermediary that issues cover on the insurer's behalf) and administrator on whether it was an MIP or RelyComply client; neither breach has a public client list, so the written answer is the only test.

3. Treat the five old flaws and the FortiGate credential campaign as one inventory exercise, closed by Friday 16 October. List every internet-facing ProFTPD, Apache Struts, Strapi, ONLYOFFICE Document Server and BIND instance and patch or retire it, checking ProFTPD for mod_copy and Struts for Dynamic Method Invocation; South Africa exposes 185 ProFTPD instances, 129 on port 21. On every FortiGate with an SSL VPN or administrative interface on the internet, end sessions, reset administrator and VPN credentials, require phishing-resistant MFA, take management off the internet, confirm PBKDF2 password storage, and search the local user list for the nineteen account names in the FBI advisory; any match is an incident regardless of patch level.

1. ransomware.live, victim page for Tharisa (UmBra), discovered 7 October 2026 08:23 UTC, estimated attack date 7 October 2026, 856 GB claimed, leak screenshot present, no deadline or published-data marker, infostealer panel empty; retrieved 11 October 2026; the same record is in the locally retrieved country feed. <https://ransomware.live/id/VGhhcmIzYUBVbUJyYQ==>

2. ransomware.live, group page for UmBra (marked New Group, Active; nine victims in five countries by 10 October 2026; ransom note readme.txt; onion address, email, Session and Telegram contacts), read 11 October 2026. <https://www.ransomware.live/group/UmBra>

3. JMousqueton/ransomware.live on GitHub, issue 392, [New Group] UmBra Group DLS (opened 6 October 2026; first listed victim Four Hands LLC; ransom extension .ub; note file REDME-UMBRA.txt). <https://github.com/JMousqueton/ransomware.live/issues/392>

4. Tharisa plc, SENS and RNS announcements page, checked 11 October 2026 (newest announcement 30 September 2026, board succession; Q4 FY2026 production report scheduled 13 October 2026; the only cyber-titled announcement is Cybersecurity incident, 19 December 2024). <https://www.tharisa.com/sens-rns-announcements.php>

5. Tharisa plc, Investor calendar, checked 11 October 2026 (13 October 2026 Q4 FY2026 production report; 30 November 2026 FY2026 results; the page states that dates are indicative only). <https://www.tharisa.com/investor-calendar.php>

6. ransomware.live, victim page for Samwumed (The Gentlemen), discovered 30 September 2026 03:40 UTC, estimated attack date 29 September 2026, country field KR, description places the scheme in Cape Town; no data size, deadline or published-data marker; read 11 October 2026. <https://www.ransomware.live/id/U2Ftd3VtZWRAZGhIZ2VudGxlbWVu>

7. TechCentral, Ransomware gang threatens to dump more South African client data, by Duncan McLeod (5 October 2026). <https://techcentral.co.za/ransomware-gang-south-african-client-data-legalwise-samwumed-edcon/286877/>

8. LegalWise, Statement regarding third-party cybersecurity incident (26 June 2026). <https://www.legalwise.co.za/media-centre/statement-regarding-third-party-cybersecurity-incident>

9. LegalWise, Important update regarding a third-party cybersecurity incident (6 July 2026; names MIP Holdings; LEZA has notified the Information Regulator). <https://www.legalwise.co.za/media-centre/important-update-regarding-a-third-party-cybersecurity-incident>

10. SAMWUMED, Data security breach notice in terms of section 22 of POPIA (page published 29 June 2026, modified 16 July 2026; names MIP Holdings (Pty) Ltd as former administration platform provider). <https://www.samwumed.org/notice-of-security-compromise-in-terms-of-section-22-of-the-protection-of-personal-information-act-4-of-2013-popia/>

11. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.10.08, released 8 October 2026 20:09 UTC, retrieved 11 October 2026 (feeds/kev_2026-10-11.json). <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

12. SOCRadar, CVE-2026-88779: Citrix NetScaler zero-day (6 October 2026; affected and fixed builds, SAML preconditions, detection guidance). <https://socradar.io/blog/cve-2026-88779-citrix-netscaler-zero-day/>

13. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:01 UTC 11 October 2026 (feeds/shodan_za_2026-10-11.json). <https://www.shodan.io/search?query=country%3AZA>

14. FBI, CISA, NSA and partner agencies, joint advisory AA26-281A, Chinese government-linked cyber threat actors combine automated and hands-on hacking tools to steal sensitive data (8 October 2026; PDF as published by IC3). <https://www.ic3.gov/CSA/2026/261008.pdf>

15. BleepingComputer, Max severity SonicWall SMA1000 flaw now exploited in attacks, by Sergiu Gatlan (9 October 2026; Previdian honeypot observations). <https://www.bleepingcomputer.com/news/security/max-severity-sonicwall-sma1000-flaw-now-exploited-in-attacks/>

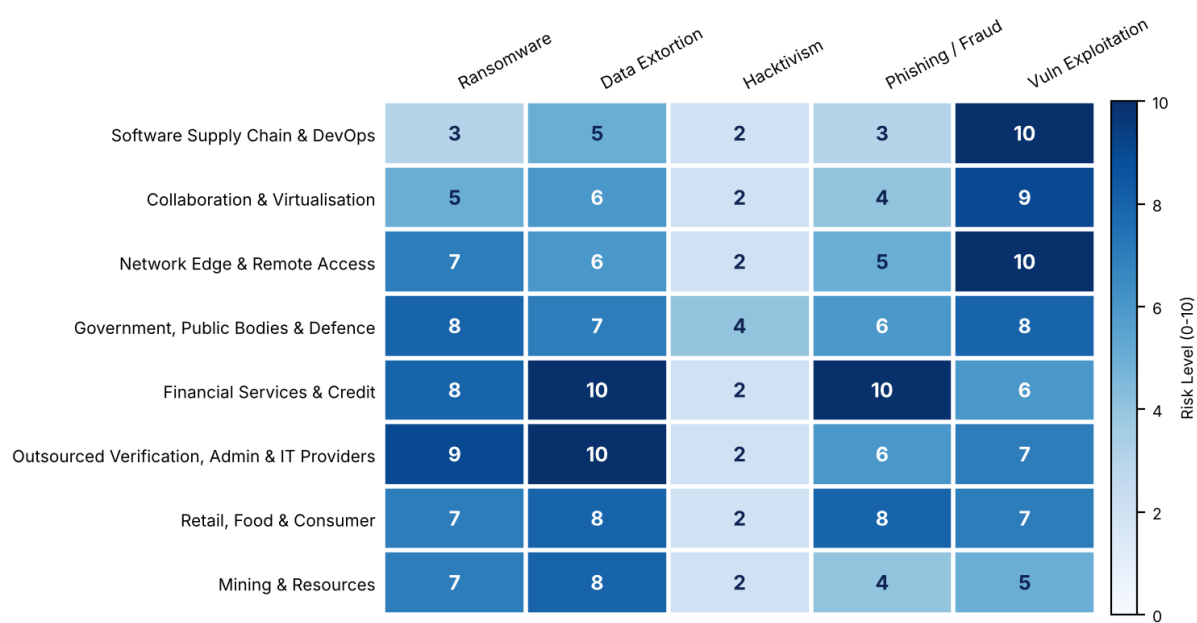
16. FBI and US Secret Service, joint cybersecurity advisory JCSA-20261006-01, FortiBleed operations continue targeting exposed systems leading to reports of lockouts (6 October 2026). <https://www.ic3.gov/CSA/2026/261006.pdf>

17. ransomware.live API, GET /v2/countryvictims/ZA, 136 records, za_records 136 against server_returned 136, filter purity 1.0, FREE v2 tier (delayed relative to PRO), retrieved 02:00 UTC 11 October 2026 and stored as feeds/ransomwarelive_za_2026-10-11.json. <https://api.ransomware.live/v2/countryvictims/ZA>

18. TechCentral, Shoprite ranks cybersecurity as its number one risk, by Duncan McLeod, on the Shoprite Holdings 2026 integrated report (9 October 2026). <https://techcentral.co.za/shoprite-cybersecurity-number-one-risk/287148/>

2. THREAT LANDSCAPE HEATMAP

South African Sector Threat Levels, Week 42 (4 October - 10 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 survives a nationality check, incidents confirmed by the organisation affected, catalogue additions affecting software the sector runs, VERIFIED South African exposure counts for that software, and reported fraud activity. A sector with no observation this week keeps its prior score, and a ceiling score of 10 is held.

One row retired, one row entered. Transport, Logistics and Fleet is retired: its only W41 observation was ATNS, which produced nothing new in the window and is carried in Section 3.5 and in the W43 watch until its Friday 16 October test; the row returns if that test produces an observation. Mining and Resources enters at ransomware 7, data extortion 8, hacktivism 2, phishing 4 and vulnerability exploitation 5, on the Tharisa listing and on Implats, carried since W37; the extortion score reflects an 856 GB claim against a listed producer by a group whose nine listings in five days were all accompanied by a data figure.^{1,2} Samwumed is a medical scheme and is scored under Financial Services and Credit, where the extortion score was already at the ceiling; the row's phishing and fraud score holds at 10 on the FSCA's warning about regulatory examination certificates bearing its branding and on the member-targeted phishing both Samwumed and LegalWise warn of.^{19,10}

Movements. No other cell moves. Network Edge and Remote Access holds at 10 on vulnerability exploitation with a third NetScaler zero-day, the SonicWall SMA 1000 request forgery and the FortiBleed advisory; its ransomware score holds at 7 because no South African incident has named an edge appliance as the entry point this quarter; the FBI's account of FortiBleed access being sold to INC/Lynx and Payload affiliates leaves open whether that will stay true.¹⁶ Software Supply Chain and DevOps holds at 10 on exploitation: the five KEV catalogue additions of 8 October are all components beneath applications, and the Atlassian file-read flaw reported exploited on 7 October reaches Bitbucket, Bamboo, Jira and Confluence Data Center.²⁰ Retail, Food and Consumer holds at 8 on extortion with Edcon's timer and Shoprite's disclosure of four breaches in its financial year.¹⁸ Government, Public Bodies and Defence holds at its W41 scores; the parliamentary reply that the Hawks registered eight cybercrime cases and made one arrest in three years is a capacity observation and does not move a threat score.²¹ The hacktivism column has not moved since W37; it stays in the matrix so that an observation has somewhere to land.

19. Moonstone, Warning over RE certificates bearing FSCA's and Moonstone's branding, on the FSCA statement of 6 October (8 October 2026). <https://www.moonstone.co.za/warning-over-re-certificates-bearing-fscas-and-moonstones-branding/>

20. Infosecurity Magazine, Critical flaw in multiple Atlassian products exploited in the wild, by Kevin Poireault (8 October 2026; CVE-2026-21589). <https://www.infosecurity-magazine.com/news/critical-vulnerability-atlassian/>

21. MyBroadband, South Africa faces 8,850 cyberattacks per month but made only 1 arrest in 3 years, by Luis Monzon, on a parliamentary reply by acting police minister Firoz Cachalia to Dianne Kohler Barnard MP (9 October 2026). <https://mybroadband.co.za/news/security/671568-south-africa-faces-8850-cyberattacks-per-month-but-made-only-1-arrest-in-3-years.html>

3. TOP SA INCIDENTS (W42)

Four items. One is a new group's claim against a listed mining company, two are the MIP cascade reaching a medical scheme and a legal-expenses insurer that had each told their members in June, and one is a retailer's own disclosure. 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-W42-01: Tharisa Listed by UmBra, a Group Six Days Old, With an 856 GB Claim [CLAIMED]

Sector	Mining and resources (platinum group metals and chrome)
--------	---

Organisation	Tharisa plc, incorporated in Cyprus, primary listing JSE (THA) with a standard listing on the LSE (THS); operating unit Tharisa Minerals with its mining operations in South Africa; development projects in Zimbabwe
Listing	Indexed by ransomware.live at 08:23 UTC on Wednesday 7 October 2026 from UmBra's onion site, estimated attack date 7 October. The record claims 856 GB and carries a leak screenshot; no sample, deadline or published-data marker. The aggregator marks the group as emerging and says its claims should be treated with caution until verified
The group	UmBra's leak site was reported to the aggregator's maintainers on 6 October with Four Hands LLC as its first listing. By 10 October the group page showed nine victims across six countries by their descriptions (the aggregator's country field resolves five): two universities in India, three Egyptian institutions including a technology firm, a Brazilian food company, a Saudi security firm, a US furniture maker and Tharisa; the note is readme.txt and the reported extension is .ub. Contacts on the feed are one email address, one Session identifier and one Telegram handle; no binary, hash or IP address is published for the group
Prior record	Tharisa disclosed a cybersecurity incident by SENS on 19 December 2024: unauthorised network activity, affected systems taken offline, operations unaffected, authorities informed, no actor named. No leak-site record for the company exists on the aggregator before this one
Confirmed	Nothing. The SENS and RNS page carries no announcement after 30 September; the investor calendar gives Tuesday 13 October, marked indicative, for the Q4 FY2026 production report. No South African publication had reported the listing by 10 October
Confidence	CLAIMED. Threat-actor assertion only, from a group with no track record. The nationality check is passed on operations and listing, with the Cyprus domicile noted; the aggregator's own description calls the company Cyprus-based

The listing is carried as the actor's. What can be said without adopting it is narrow: a listed company with continuing disclosure obligations on two exchanges had, by the close of the window, published nothing, and the production report scheduled for 13 October is a document in which a material incident would ordinarily be mentioned.^{4,5} The December 2024 incident is relevant for one reason only: it shows the company has a disclosure precedent of its own, by SENS, for a cyber incident with operations unaffected.²² The group is the observation that matters for other South African estates. Nine listings in five days from a site that did not exist on 5 October, every one with a data figure and most against universities and technology firms in the Global South, reads as an affiliate or rebrand with an existing stock of access, since a new intrusion capability does not produce nine victims in five days; that is an inference from tempo and is marked as one.^{2,3} The distinguishing observations are a Tharisa SENS, a published sample, and whether the group's other listings produce confirmations from their victims. Detection relevance: TH-2026-W42-02 carries the group's contact indicators and note name; there is no tooling to hunt for yet.

3.2 INC-2026-W42-02: Samwumed, Found Under a South Korean Tag, Had Named MIP in June [CLAIMED]

Sector	Medical scheme (closed, self-administered; municipal workers); scored under Financial Services and Credit
Organisation	SAMWUMED, Cape Town, a closed medical scheme founded in 1952 for municipal employees; samwumed.org

Listing	Indexed by ransomware.live at 03:40 UTC on Wednesday 30 September 2026 from The Gentlemen's site, estimated attack date 29 September, in the same minute as LegalWise and Edcon. Country field KR; description places the scheme in Cape Town. No data size, sample, deadline or published-data marker on the record when read on 11 October. TechCentral reported a countdown timer on the listing expiring around Friday 9 October
Prior record	A section 22 notice on the scheme's website, published 29 June 2026 and modified 16 July, reports that MIP Holdings (Pty) Ltd, the scheme's former administration platform provider, suffered unauthorised access to its Jira environment; that certain historical members' information stored in MIP's legacy environment had not been deleted; that names, historical membership numbers and treating doctors' details may be affected; and that the scheme is engaging MIP on its contractual obligations. The notice does not say whether the Information Regulator was notified
Statement	None on the listing. Samwumed had not responded to TechCentral or MyBroadband by 5 October and has not said whether the listed data is the MIP set
Confidence	CLAIMED for the listing. The scheme's exposure in the MIP incident is CONFIRMED on its own notice; whether the group holds the scheme's data, and whether it came from MIP, is unconfirmed and is not inferred from the timing

Two things follow from the record. The first is a correction, made in Section 1: the W41 window held four South African claims, and the aggregator's country field hid one, which is the second time in the series it has done so.⁶ The second is that the scheme's notice gives a specific account of what sat in MIP's environment: historical data from a former client which, in the notice's words, had not been deleted, and over which the scheme is engaging MIP on its contractual obligations; that, if it is what the group holds, means the Information Regulator's question of who the responsible party is has a further variant, a processor retaining data after the contract ended, if the listed data is what the group holds.^{10,23} The distinguishing observations are a Samwumed statement on the listing, a published sample in the format of the Hollard set, and any regulator reference. First reported, for the listing, by TechCentral on 5 October 2026; the scheme's notice is the primary source for its MIP exposure. Detection relevance: TH-2026-W40-06 (The Gentlemen's tooling) stands as written; member-targeted phishing using historical membership numbers is the scheme's own stated risk and is the subject of TH-2026-W42-07.

3.3 INC-2026-W42-03: LegalWise's Own June and July Statements Confirm Its MIP Exposure; the Listing Stays a Claim [CONFIRMED]

Sector	Financial services and credit (legal-expenses insurance)
Organisations	LegalWise South Africa (RF) (Pty) Ltd and its insurer Legal Expenses Insurance Southern Africa Limited (LEZA)
Statements	26 June 2026: MIP Holdings, a third-party technology service provider, identified unauthorised access to a legacy system used for software development and support; no evidence of unauthorised access to LegalWise's core systems, member databases or transactional platforms. 6 July 2026 update: the categories under assessment are personal information including names, identity numbers and contact details, membership information and banking details; LEZA has notified the relevant regulators including the Information Regulator; members will be contacted directly if affected; not aware of any fraudulent use. To MyBroadband on 5 October: declined to comment on whether it had been extorted; LEZA is managing the incident ²⁴

Listing	The Gentlemen, indexed 03:40 UTC 30 September; TechCentral reported a countdown timer expiring around 9 October and that the listing carries a business-directory profile and no sample. No published-data marker on the aggregator's record on 11 October ²⁵
Confidence	CONFIRMED for LegalWise's exposure in the MIP incident, on two statements on its own website. The listing and the group's possession of LegalWise data stay CLAIMED; TechCentral could not verify either

W41 asked whether LegalWise was an MIP client and said a LegalWise statement would resolve it; the statement had existed for three months and the edition did not find it,^{8,9} which is the second correction in Section 1 of this edition. What the statements add to the MIP record is a regulator conflict worth stating plainly. The Information Regulator told TechCentral on 25 September that it had received only MIP's notification; LegalWise's 6 July update says LEZA notified the Information Regulator, and Guardrisk says its binder holder CoverCubed notified the regulator too. Either the regulator's answer was narrower than it read, or these notifications were not received as section 22 notifications, and the report does not choose between the two.^{23,24} The size of the MIP set, as MIP's chief executive gave it to TechCentral, is the customers of about 45 insurers, about 400,000 records, and the Comparitech quarterly roundup of 7 October uses the MIP case as its example of a paid ransom followed by extortion of the supplier's clients.²⁶ First reported by TechCentral on 5 October 2026 for the timers. Detection relevance: the LegalWise record format, if published, is the thing to watch for in member-targeted phishing, and TH-2026-W42-07 applies.

3.4 INC-2026-W42-04: Shoprite Discloses Four Data Breaches in Its 2026 Financial Year [CONFIRMED]

Sector	Retail, food and consumer
Organisation	Shoprite Holdings Ltd, JSE-listed food retailer; Xtra Savings loyalty programme, Money Market Account with 4.3 million customers, Sixty60 delivery
Disclosure	Shoprite's 2026 integrated report, as reported by TechCentral on 9 October: information security including cyber risk is the first of six core risks; inherent risk rated critical, controls rated partially effective (the weakest of the six), residual risk medium; four data breaches in FY2026 against three in FY2025 and one in FY2024, all involving personal information, affecting 44 customers in FY2026, one in FY2025 and 1,437 in FY2024; a stated zero tolerance for security breaches and unmitigated critical vulnerabilities; cybersecurity posture hardening a named focus area; the audit and risk committee lists information security and AI guardrails among its FY2027 priorities
Confidence	CONFIRMED on the company's own report as read by TechCentral; the report's release date is not stated in the reporting and the item is single-sourced for this edition, which Section 12 records

The item is carried for what it shows about disclosure practice. A JSE-listed retailer has put a breach count, an affected-customer count and a controls rating that it describes as partially effective into a public document, which is more than any South African organisation named on a leak site this quarter has done in a statement.¹⁸ The four incidents are not described, so nothing can be said about their cause or whether any was a supplier case. For a board the useful comparison is with its own integrated report: whether it states a breach count at all, and whether its control effectiveness rating for cyber risk is the group's own assessment or the auditor's. Detection relevance: none.

3.5 Carryovers

ATNS, W41. The air navigation operator disclosed ransomware-linked malware in airport weather systems through a request for quotation for forensic services. No development in the window: no contract award, no statement, no leak-site listing, no section 22 notice located; the Friday 16 October test is set out in Section 11. CONFIRMED at the scope of the tender document.

BCX, W41. No Telkom or BCX statement on the INC Ransom listing; the company website carries no notice; the aggregator's record is unchanged. CLAIMED for the listing.²⁷

Edcon, W41. The former Edgars and Jet owner, in business rescue since 2020, listed by The Gentlemen on 30 September. TechCentral reports a countdown timer expiring around 9 October and that the listing carries a directory profile and no sample; no published-data marker on 11 October; whether Edcon was an MIP client remains unknown and is not inferred. CLAIMED.^{7,28}

Guardrisk and CoverCubed, W41. No development. Hollard's press-release page carries nothing on the matter. Guardrisk's account stands as its account.²⁹

RelyComply, W39. A third fortnight of silence; the notice still reads last updated 16 September; DireWolf's index moved from 135 to 136 on a listing elsewhere. CONFIRMED for the incident.³⁰

BlackLocks (Apollo 21 and ARCA Unlimited Architects), W40. The group's index stayed at three through 11 October; whether it lists a fourth victim anywhere by Friday 16 October decides if its two South African listings were a burst or a pattern. CLAIMED for both.

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

22. Mining Weekly, Tharisa assures stakeholders it is managing cybersecurity incident (19 December 2024).

<https://www.miningweekly.com/article/tharisa-assures-stakeholders-it-is-managing-cybersecurity-incident-2024-12-19>

23. TechCentral, Insurers carry the can for MIP breach, regulators say (25 September 2026).

<https://techcentral.co.za/insurers-mip-breach-regulators/286482/>

24. MyBroadband, Ransomware group threatens to leak customer data from top insurance companies in South Africa, by Luis Monzon (5 October 2026; cited for the companies' statements only, see the attribution note in Section 12). <https://mybroadband.co.za/news/security/670417-ransomware-group-threatens-to-leak-customer-data-from-top-insurance-companies-in-south-africa.html>

25. ransomware.live, victim page for LegalWise (The Gentlemen), discovered 30 September 2026 03:40 UTC, re-read 11 October 2026 (no deadline, sample or published-data marker on the record). <https://ransomware.live/id/TGVnYWxXaXNIQHROZWdlbnRsZWllbg==>

26. Infosecurity Magazine, Q3 2026 sets new record for ransomware attacks, by James Coker, on Comparitech's Q3 2026 roundup of 7 October (9 October 2026). <https://www.infosecurity-magazine.com/news/q3-new-record-ransomware/>

27. BCX, corporate website, checked 11 October 2026 (no notice, banner or statement on any incident). <https://www.bcx.co.za/>

28. ransomware.live, victim page for Edcon (The Gentlemen), discovered 30 September 2026 03:40 UTC, re-read 11 October 2026 (no deadline, sample or published-data marker on the record). <https://ransomware.live/id/RWRjb25AdGhIZ2VudGxlbWVU>

29. Hollard, Media centre press releases, checked 11 October 2026 (no item on the cyber matter).

<https://www.hollard.co.za/media-centre/press-releases>

30. RelyComply, RelyComply cyber incident: what happened and what you can do, official notice (published 16 September 2026; re-read 11 October 2026, page still reads last updated 16 September 2026).

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

4. THREAT ACTORS

Three profiles and a set of notes. UmBra, because it listed Tharisa in its first week of existence; The Gentlemen, because the MIP cascade now has four South African names and two of them had published notices in June; and the Integrity Technology Group cluster, because a seven-nation advisory put five of its exploited flaws into CISA's KEV catalogue and places its victims in Africa among other regions. Notes on the FortiBleed broker, Qilin, INC Ransom and the groups that did not move close the section.

4.1 UmBra: Nine Listings in Five Days on a Site Reported on 6 October

The group did not exist in the aggregator's index at the 4 October retrieval; the index count retrieved on 11 October gives it ten victims, one more than the nine on the group page as last updated on 10 October, and the page figure is used below. It is one of four groups added to the index in the week, alongside byod and vypr at seven each and scarlettgroup at one.³¹ Its leak site was reported to the aggregator's maintainers on 6 October with Four Hands LLC, a US furniture maker, as the first listing, a .ub extension and a note file named REDME-UMBRA.txt; the aggregator's own note record for the group is readme.^{3,32} By 10 October the group page showed nine victims across six countries by their descriptions, every one with a data figure and 14.3 TB claimed in total, with four universities among them and the rest technology, security services, furniture, food and mining.² The feed's indicator record for the group is contact information only: an email address at a privacy mail provider, a Session identifier and a Telegram handle; no hash, address, mutex or YARA rule exists for it yet, and the hunt in Section 9 is correspondingly thin.³³ The tempo, the ready-made data figures and the geographic spread are consistent with an affiliate or a rebrand bringing an existing stock of access to a new site; that is an inference from the first week and nothing more. The observations that would settle it are a leaked builder or sample tying the encryptor to a known family, a victim confirmation anywhere, and whether the site lasts: the aggregator recorded its uptime at 75 per cent over the period and the onion address as unavailable on 11 October.

4.2 The Gentlemen: Four South African Names in the MIP Set, Two of Them on Notice Since June

The index rose from 921 to 960 between the 4 and 11 October retrievals, 39 listings in a week after 33 and 21 in the two before, again the largest movement in the aggregator's table.³¹ Comparitech's third-quarter roundup, published 7 October and reported by Infosecurity Magazine, puts the group second in the world for July to September with 342 claimed victims, up 29 per cent on the quarter, behind Qilin's 357. It calls the quarter a record at 2,627 claimed attacks, up 27 per cent on the second quarter and 61 per cent on a year earlier, with finance the fastest-growing sector at 72 per cent, and it names the MIP case as its example of a paid ransom followed by extortion of the supplier's clients.²⁶ The South African record is now twelve listings since January: the eleven ZA-tagged ones counted in W41 and Samwumed under a Korean tag.^{17,6} The shape of the insurance thread has changed with this week's reading. Hollard's data was published; Guardrisk's listing, by the insurer's account, is binder-holder data; LegalWise and Samwumed each published a third-party breach notice naming MIP in June, and in the last week of September the group listed both with timers.^{24,9,10,7} The group has now listed four organisations that MIP's incident touched; whether the LegalWise and Samwumed data it claims came from MIP is unconfirmed, but if the

pattern holds the list of likely next listings is, in outline, already public: the roughly 45 insurers whose customers' records MIP says were taken. The group's indicator feed (34 SHA-256, four SHA-1 and 47 MD5 hashes, contact identifiers and a ransom-note YARA rule) is byte-identical to the 27 September retrieval, so the W40 hunt mission built on it, TH-2026-W40-06, stands as written.³³

4.3 The Integrity Technology Group Cluster: Eight Old Flaws, a Mailbox Bot and a Renamed VPN Client

The advisory of 8 October from the FBI, CISA, NSA and partner agencies in Australia, Canada, Japan, New Zealand, Spain and the United Kingdom describes Chinese government-linked operators enabled by the contractor Integrity Technology Group, with tactics the advisory says are consistent with the clusters vendors track as Flax Typhoon, Ethereum Panda and RedJuliett, against government, critical manufacturing, healthcare and information technology organisations in Southeast Asia, Africa and North America.^{14,34} The method is a scanning layer and a hands-on layer. The eight exploits were recovered from the operators' penetration-testing scripts, a set the advisory calls MicroScan; five entered the KEV catalogue this week and three were already in it, which The Hacker News identifies as Shellshock CVE-2014-6278, Pulse Connect Secure CVE-2019-11510 and GitLab CVE-2021-22205.³⁴ The hands-on tools are these. EBurst sprays passwords at Microsoft Exchange. A PHP bot the advisory calls Curlc4 pulls mail through Exchange Web Services, stages it as /var/tmp/.sess.zip and beacons to natcloudservice[.]com. A Linux tool named office-cli reads Microsoft 365 mail with a client ID, tenant ID and secret. DC.exe performs DCSync-style replication. Persistence is a SoftEther VPN client installed as conhost.exe or dllhost.exe outside System32, set to reconnect at start, with hub domains that include 98aiblog[.]com, hmbcloud[.]com and javacheck.ooguy[.]com. A dropper named live700_v1.exe launches DiagTrack.exe, which beacons to dns.studiocloud[.]xyz, and the one address named in the advisory body is 149.28.132[.]137.¹⁴ The advisory's own caveat applies: several indicators date to 2016 and are to be vetted before blocking. For a South African reader the relevance lies in the exploit list: these are flaws in components that sit under older web applications and file-transfer services, and 185 ProFTPD instances are exposed in the country.¹³ TH-2026-W42-03 carries the hunt.

4.4 Notes: the FortiBleed Broker, Qilin, INC Ransom and the Groups That Did Not Move

FortiBleed. The FBI and Secret Service advisory of 6 October describes an operation, which The Hacker News characterises as Russian-speaking, that scans for FortiGate SSL VPN portals, stuffs and sprays credentials from leak dumps and stealer logs, extracts and cracks hashes on a GPU cluster, creates administrative accounts for persistence, enumerates Active Directory, and sells the access; it cites SOCRadar's verified count of more than 86,644 compromised devices in 194 countries, a figure The Hacker News dates to 19 June, and links the buyers to INC/Lynx and Payload affiliates.^{16,35} Payload holds one South African listing since July and INC Ransom holds BCX, which is a reason to read the advisory as South African even though it names no country.¹⁷ **Qilin.** Japan's National Police Agency confirmed on 8 October that a 28-year-old Russian national accused of involvement in the group was arrested at an Osaka hotel in May and extradited to Germany in June over an alleged role in an attack on a German company; the group's index moved from 2,328 to 2,353 in the week and it led Comparitech's quarter.^{36,31,26} **INC Ransom** rose from 959 to 969; the BCX record is unchanged. **DireWolf** moved from 135 to 136; RelyComply's data has not been published. **BlackLocks** stayed at three. Warlock (the SharePoint-exploiting group profiled in W40)

and the unattributed NetScaler intrusion set profiled in W41 produced no new reporting in the window and are carried in the KEV table.³¹

31. ransomware.live API, GET /groups, 407 groups with victim counts, retrieved 11 October 2026 and compared with the 4 October retrieval (feeds/r1_groups_2026-10-11.json). <https://api.ransomware.live/v2/groups>

32. ransomware.live API, GET /ransomnotes/{group}, retrieved 11 October 2026 (feeds/r1_ransomnotes_2026-10-11.json; UmBra note filename readme). <https://api.ransomware.live/v2/ransomnotes/umbra>

33. ransomware.live API, GET /iocs/{group} for the groups active against South Africa in the last 120 days, retrieved 11 October 2026 (feeds/r1_iocs_2026-10-11.json; UmBra carries one Session identifier, one email address and one Telegram handle). <https://api.ransomware.live/v2/iocs/umbra>

34. The Hacker News, Flax Typhoon exploits five flaws as CISA sets October 11 deadline for federal agencies, by Ravie Lakshmanan (9 October 2026). <https://thehackernews.com/2026/10/flax-typhoon-exploits-five-flaws-as.html>

35. The Hacker News, FBI warns FortiBleed remains active after amassing 86,644 Fortinet device credentials, by Ravie Lakshmanan (7 October 2026). <https://thehackernews.com/2026/10/fbi-warns-fortibleed-remains-active.html>

36. The Record, Japan confirms arrest of Russian Qilin operative, extradition to Germany, by Jonathan Greig (9 October 2026). <https://therecord.media/japan-germany-ransomware-arrest>

5. CRITICAL VULNERABILITIES & CISA KEV

CISA added six vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue between Sunday 4 and Saturday 10 October 2026: NetScaler CVE-2026-88779 on Sunday 4 October, and ProFTPD CVE-2015-3306, ISC BIND CVE-2015-5477, Apache Struts CVE-2016-3081, ONLYOFFICE CVE-2021-3199 and Strapi CVE-2023-22894 on Thursday 8 October. The KEV catalogue records vulnerabilities by the date CISA obtains evidence of active exploitation, whatever the age of the flaw, which is why five entries this week are between three and eleven years old: the evidence for them arrived on 8 October with the joint advisory in Section 4.3. All six 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, and all six were past them on Monday 12 October. The KEV catalogue version used is 2026.10.08, released at 20:09 UTC on Thursday 8 October; any entry added on Friday 9 or Saturday 10 October falls to W43, and the SonicWall SMA 1000 flaw below is the candidate to check first.¹¹ Every CVSS figure is from the NVD feed with its scoring source, except the carryover scores for CVE-2026-55040 and CVE-2026-15409, which are older than the feed's 45-day window and are carried from earlier feeds; every EPSS figure (FIRST's estimate of the probability of exploitation in the next 30 days) is from the FIRST feed, and the standing warning holds that a low EPSS never deprioritises a catalogue entry.^{37,38} The catalogue's ransomware-use field reads Unknown for all six; Unknown means CISA has not recorded ransomware use, and the report never writes it as no. The catalogue also carries a forensicTriage field, tied in each entry to BOD 26-04's Forensics Triage Requirements; it reads Yes for four of the six (ProFTPD, Struts, Strapi and ONLYOFFICE) and No for BIND and the NetScaler entry. The report reads a Yes as CISA directing its agencies to collect evidence before remediating; the reading rests on the catalogue text, and the guidance document itself is not cited.

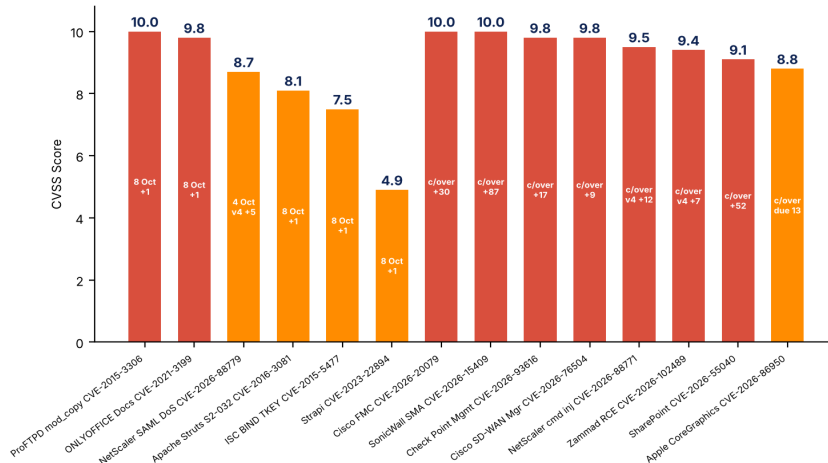
Citrix NetScaler CVE-2026-88779 is a memory overflow, CWE-119, scored 8.7 on CVSS 4.0 by Citrix, with high availability impact and no confidentiality or integrity impact in the vector; the established effect is a crash, and Citrix has not established code execution. It is reachable only on appliances configured as a SAML service provider or identity provider, which the configuration shows as add authentication samlAction or add authentication samlIdPProfile.^{37,12} Administrators reported crashes and reboot loops on fully patched appliances before Citrix published the CVE and fixed builds on Saturday 3 October; Citrix confirmed targeted attacks against unmitigated deployments, credited watchTower and Bishop Fox, and CISA listed it on Sunday 4 October with a due date of Wednesday 7 October.^{39,40,11} The fixed builds are

14.1-73.41 and 13.1-64.28, with 13.1-37.282 for the FIPS and NDcPP line; watchTower told The Register it suspects the flaw has been used to crash appliances on purpose so that the September pre-authentication flaw CVE-2026-88771 can be exploited faster, a suspicion the firm has not substantiated in public.^{12,39} Then on Friday 9 October Citrix published CVE-2026-107406, bulletin CTX697191, another memory overflow in the same SAML configurations that Citrix says could allow code execution as well as a crash, with no known exploitation. The fixed builds move again, to 14.1-73.46 and 13.1-64.29, so an appliance patched for the first SAML flaw needs patching again.⁴¹ South Africa exposes 125 NetScaler instances, 100 of them on 443, the same population as the September pair.¹³

The five additions of 8 October are the exploit list of the advisory in Section 4.3, and what distinguishes them is their age. ProFTPD CVE-2015-3306 is the mod_copy flaw: unauthenticated site cpfr and site cpto commands read and write arbitrary files; CVSS 10.0 scored by CISA as NVD's authorised data publisher (ADP), EPSS 0.9950, and 185 instances exposed in South Africa with 129 on port 21. ONLYOFFICE Document Server CVE-2021-3199 is a path traversal in an image-upload parameter when JWT is in use, leading to code execution; 9.8, EPSS 0.1935, fixed in 5.6.3. Apache Struts CVE-2016-3081, the S2-032 command injection through the method: prefix when Dynamic Method Invocation is enabled; 8.1, EPSS 0.9605. ISC BIND CVE-2015-5477, the TKEY query assertion failure that stops the resolver; 7.5 from CISA's ADP, EPSS 0.9941. Strapi CVE-2023-22894, cleartext storage reachable through the admin query filter by an attacker who already has admin-panel access (hence the low score), which the catalogue says chains with CVE-2023-22621 to code execution and which the catalogue says could be end-of-life; NVD scores it 4.9, The Hacker News prints 7.2, and the feed figure is used.^{11,37,38,34,13} Three of the five carry EPSS scores above 0.96, which is the reverse of the pattern the W32 edition recorded, where three newly exploited flaws scored near zero: the score leads where the exploit is a decade old and public, and lags where the flaw is new, so the number helps rank legacy exposure and says nothing useful about a zero-day.

Exploited and not yet in the catalogue. SonicWall published SNWLID-2026-0017 on Tuesday 6 October: CVE-2026-102255, a pre-authentication server-side request forgery in the SMA 1000 WorkPlace portal, CVSS 10.0 by the vendor, affecting 12.4.3-03526 and 12.5.0-02952 and earlier on the 6210, 7210 and 8200v, fixed in 12.4.3-03670 and 12.5.0-03082; SonicWall said it had no evidence of exploitation, and three days later Previdian told BleepingComputer its honeypots had seen attempts consistent with the flaw: an OPTIONS request to the WorkPlace Extraweb interface, a reach for the internal CouchDB on 127.0.0.1:5984, traversal into a design document to invoke _rewrite, and a basic-authentication header of admin:admin.^{42,15} The SonicWall family in South Africa is 2,965 instances across five product strings and cannot be narrowed to the SMA 1000 line.¹³ Atlassian CVE-2026-21589, published 5 October, is an unauthenticated file read in the shared web-resource plugin library across Bitbucket, Confluence, Jira Software, Jira Service Management, Bamboo and Crowd Data Center, Crucible and Fisheye, CVSS 9.3; VulnCheck recorded exploitation against Bamboo on 7 October and watchTower published a detection-artefact generator.²⁰ **Carryovers** moved only in their arithmetic and are in the table; the Apple CoreGraphics entry is the one item due after publication, on Tuesday 13 October, which is also Microsoft's October patch day and falls in the W43 window.

W42 KEV / CRITICAL CVE SEVERITY | 4 October - 10 October 2026
All six KEV additions in the window (left) plus the eight carryovers that most outrank them (right). CVSS from the NVD feed except CVE-2026-15409 and CVE-2026-55040 (earlier feeds); v4 marks a CVSS 4.0 score. In-bar notes: KEV date or carryover, then days overdue (+N) at the publication Monday, 12 October 2026, or the due date



W42 CISA KEV / Critical CVE Tracking (six additions 4 to 8 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 12 October; RW is the catalogue's ransomware-use field; Triage is the catalogue's forensicTriage flag; ZA figures are VERIFIED Shodan exposure counts, never vulnerability counts.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-88779	Citrix NetScaler ADC and Gateway (SAML SP or IdP only)	8.7 (v4.0)	Memory overflow, DoS (unauth)	7 Oct	KEV 4 Oct. OVERDUE +5. Crashes on patched appliances before the 3 Oct fix. Fixed 14.1-73.41 / 13.1-64.28; the 9 Oct builds 14.1-73.46 / 13.1-64.29 also cover CVE-2026-107406. 125 in ZA. RW Unknown. Triage No. EPSS 0.0059.
CVE-2015-3306	ProFTPD (mod_copy)	10.0	File read / write, SITE CPFR and CPTO (unauth)	11 Oct	KEV 8 Oct. OVERDUE +1. AA26-281A list. 185 in ZA, 129 on port 21, VERIFIED. Disable mod_copy or upgrade. RW Unknown. Triage Yes. EPSS 0.9950.
CVE-2021-3199	ONLYOFFICE Document Server	9.8	Path traversal, image upload with JWT (RCE)	11 Oct	KEV 8 Oct. OVERDUE +1. AA26-281A. Fixed at the 5.6.3 changelog entry the catalogue cites. No ZA label. RW Unknown. Triage Yes. EPSS 0.1935.
CVE-2016-3081	Apache Struts 2 (S2-032)	8.1	Command injection, method: prefix with DMI	11 Oct	KEV 8 Oct. OVERDUE +1. AA26-281A. Disable Dynamic Method Invocation; retire. No ZA label. RW Unknown. Triage Yes. EPSS 0.9605.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2015-5477	ISC BIND	7.5	TKEY assertion failure, DoS (unauth)	11 Oct	KEV 8 Oct. OVERDUE +1. AA26-281A. Rebuild any resolver this old. No ZA label. RW Unknown. Triage No. EPSS 0.9941.
CVE-2023-22894	Strapi (end-of-life versions)	4.9	Cleartext storage via admin filter; chains to RCE	11 Oct	KEV 8 Oct. OVERDUE +1. AA26-281A. NVD 4.9 (THN 7.2; feed used). No ZA label; held. RW Unknown. Triage Yes. EPSS 0.0361.
CVE-2026-88771	Citrix NetScaler ADC and Gateway	9.5 (v4.0)	Pre-auth RCE, default config	30 Sept	Carryover. OVERDUE +12 with DTLS CVE-2026-88772. TH-2026-W41-01 stands: examine before upgrading. Same 125 instances. EPSS 0.0108.
CVE-2026-76504	Cisco Catalyst SD-WAN Manager	9.8	Auth bypass via URI encoding	3 Oct	Carryover. OVERDUE +9; FortiMail CVE-2026-104286 +8; Zammad pair +7; Apple CVE-2026-86950 due 13 Oct. W41 log checks stand. No ZA label.
CVE-2026-93616	Check Point Security Management	9.8	Path traversal, file upload	25 Sept	Carryover. OVERDUE +17 with F5 APM CVE-2026-94127 and Arista VCO CVE-2026-93952; Zyxel +18. No ZA label.
CVE-2026-19490	Citrix NetScaler ADC and Gateway	9.3 (v4.0)	Auth bypass (unauth)	12 Sept	Carryover. OVERDUE +30 with Cisco FMC CVE-2026-20079 (10.0) and FortiOS; MikroTik pair +29 (4,615 in ZA); ScreenConnect and GitLab +28; Cisco SEG +25; ISE +23.
CVE-2026-55040	Microsoft SharePoint	9.1	Weak auth (JWT forgery)	21 Aug	Carryover. OVERDUE +52; 808 in ZA. Zimbra +49; SharePoint CVE-2026-65660 and WordPress +14; Adobe Commerce +15. TH-2026-W41-05 and 06 stand.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-15409	SonicWall SMA 1000	10.0	SSRF (unauth)	17 Jul	Carryover. OVERDUE +87 with CVE-2026-15410, both RW KNOWN; September SMA pair CVE-2026-83548 and 83549 +37; FMC CVE-2026-20316 (Known) +72; LiteLLM +112. New SMA 1000 SSRF CVE-2026-102255 not yet listed (TH-05). Family 2,965 in ZA.

Pattern note: the week's six divide by age, and age decides the work. The NetScaler entry is the third exploited zero-day on the same appliance class in a fortnight, and Citrix has shipped three fixed builds in twelve days (28 September, 3 October and 9 October, the last for a flaw not yet seen exploited), so a NetScaler kept current has been upgraded three times in that time; an estate that could not do that has a change-management problem rather than a patching problem. The other five are between three and eleven years old and entered the KEV catalogue only now because a state-linked contractor's scanning scripts were recovered with the exploits in them, which means the vulnerable population is whatever was never inventoried, and a patch cycle does not find it; ProFTPD carries a VERIFIED South African figure on the day of its addition because the product sits on one port and the fingerprint corroborates itself.^{11,13} The SMA 1000 is the item to watch across the two editions: a CVSS 10 flaw on an appliance line that already carries two catalogue entries with ransomware use Known, with honeypot attempts consistent with it three days after the fix and the catalogue decision falling after this edition's cut-off.¹⁵

37. NIST NVD, CVE API 2.0, CVSS base scores with scoring source for the 57 catalogue entries added in the last 45 days, retrieved 11 October 2026 (feeds/nvd_cvss_2026-10-11.json). <https://services.nvd.nist.gov/rest/json/cves/2.0>

38. FIRST, EPSS API, scores for the same 57 entries, retrieved 11 October 2026 (feeds/epss_2026-10-11.json). <https://api.first.org/data/v1/epss>

39. The Register, Citrix NetScaler security snafus get even worse amid more 0-day reports, by Jessica Lyons (5 October 2026). <https://www.theregister.com/security/2026/10/05/citrix-netscaler-security-snafus-get-even-worse-amid-more-0-day-reports/5301232>

40. Sophos, Citrix NetScaler vulnerability (CVE-2026-88779) in active exploitation (October 2026). <https://www.sophos.com/en-us/blog/citrix-netscaler-vulnerability-cve-2026-88779-in-active-exploitation>

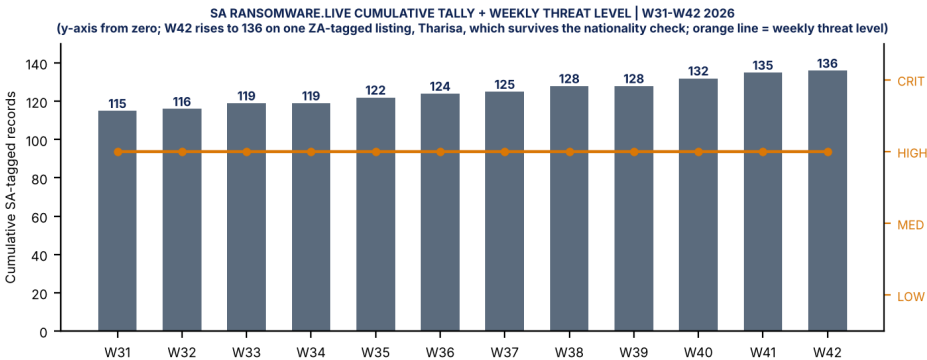
41. BleepingComputer, Citrix warns admins to patch new NetScaler RCE flaw immediately, by Sergiu Gatlan (9 October 2026; CVE-2026-107406, bulletin CTX697191). <https://www.bleepingcomputer.com/news/security/citrix-warns-admins-to-patch-new-netscaler-rce-flaw-immediately/>

42. The Hacker News, SonicWall patches CVSS 10.0 pre-authentication SSRF flaw in SMA1000 appliances, by Swati Khandelwal (7 October 2026; advisory SNWLID-2026-0017 of 6 October). <https://thehackernews.com/2026/10/sonicwall-patches-cvss-100-pre.html>

6. RANSOMWARE LANDSCAPE

The South African victim feed held 136 records when retrieved at 02:00 UTC on 11 October 2026, one more than the week before. The collection is country-scoped by path, the written file records 136 South African records against 136 returned, and the tier is the delayed free v2.¹⁷ A set-difference against the 4 October file returns one addition and zero removals: Tharisa (UmBra, 7 October 08:23 UTC), which survives the nationality check on its operations and listing with the Cyprus domicile noted, so the derived count equals the feed count. The aggregator's country page showed 136 with Tharisa newest.⁴³ The hand search for South African victims under other country tags was run this week by reading The Gentlemen's group page for every listing indexed from 1 to 10 October, which found nothing further; it was that reading, prompted

by TechCentral, that surfaced Samwumed under KR from the week before. The search still covers one group; the world feed remains a collector task.⁶



Baseline at W41 close	135 records
New listings dated inside the window	1 with a ZA tag: Tharisa (UmBra). None found under another tag for 4 to 10 October
Surviving the nationality check	1. Tharisa is Cyprus-incorporated with a JSE primary listing and its mining operations in South Africa; survives on operations and listing. The aggregator's country field has invented a South African victim five times in the series and hidden two (RelyComply under GB in W39; Samwumed under KR in W41, found this week)
Delistings or restorations	None. Set difference against the 4 October file returns one addition and zero removals
End count at W42 retrieval	136 records, filter purity 1.0 in the run log and 136 of 136 tagged ZA in the file
Groups active against SA, rolling 120 days	17 by discovery date, up from 16 on UmBra's entry; the boundary moves each week, so this figure is not a trend
Threat-level drivers	A new group's 856 GB claim against a listed mining company; The Gentlemen listing two organisations that had disclosed their MIP exposure in June, with what it holds unconfirmed; a third NetScaler zero-day against 125 exposed instances; five decade-old flaws on a state-linked exploit list with 185 ProFTPD instances exposed

Group notes. UmBra, The Gentlemen and the Integrity Technology Group cluster are profiled in Section 4. Among the groups in the aggregator's index that have listed South African organisations this year, the week's movements were The Gentlemen from 921 to 960, Qilin from 2,328 to 2,353, INC Ransom from 959 to 969, Everest from 404 to 409, LockBit 5.0 from 370 to 374, Krybit from 159 to 162, Arcus Media from 115 to 118, DragonForce from 657 to 660, MedusaLocker from 101 to 103, Payload from 75 to 76 and DireWolf from 135 to 136; m3rx, RansomHouse, BlackLocks and cmdorganization did not move. The index grew from 403 to 407 groups on UmBra, byod, vypr and scarlettgroup.³¹ Sixteen groups hold a ZA-tagged listing discovered since 1 July 2026 (the table's 17 counts from 13 June, a rolling 120-day window, and so includes one more); the three profiled in Section 4 are those with a South African listing or a published advisory in the window, and the rest are carried through the IOC export instead of the narrative.¹⁷ Comparitech's quarterly figures, with only 247 of 2,627 third-quarter claims confirmed by the organisations named, point the same way as this report's own count: this week one claim, zero confirmations.²⁶

Two patterns from the week for South African estates. The first is in Section 3: the organisations listed this fortnight by The Gentlemen are the ones MIP's incident already touched, and the next listings are likely to come from the same client list, so the question for an insurer, administrator or scheme is whether it was an MIP client; a listing, if it comes, follows from that. The second is in the KEV table: the oldest flaws in the catalogue this week carry the highest exploitation probabilities, and a state-linked operator is scanning for them in Africa; the population at risk is the file-transfer server, the content server and the resolver that nobody inventoried.¹⁴

The standing measurement caution applies. The victim feed is the free v2 tier and is delayed relative to the paid tier, so a listing dated inside this window may have been posted earlier, and one posted late on Saturday 10 October may not appear until next week's collection. The window closes at the end of Saturday because an earlier edition ran to Sunday midnight and missed two South African victims in the unobserved hours.

43. ransomware.live, South Africa country page, cross-check only (showed 136 victims with Tharisa newest when read on 11 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 11 October 2026, and none is a count of vulnerable systems; the version and vuln filters are not available on this plan, and rescan noise has moved single counts by more than 70 per cent inside a day, so week-on-week movement is not reported as a finding.¹³ Only queries whose product facet corroborates the fingerprint are published. Two of this week's six additions have a figure. Citrix Netscaler, by product match with the lowercase s that Shodan uses: 125 instances, 100 of them on 443, the population for the SAML pair and for the September entries. ProFTPD, added to the panel from the catalogue entry: 185 instances, 129 of them on port 21, 170 labelled ProFTPD, eleven ProFTPD mod_sftp and four ProFTPD or KnFTPD. Applying the port-concentration test: 70 per cent of the population on one port is the profile of a real product population, against the scatter that disqualifies LiteLLM and ScreenConnect, so the figure is published; the port test applies to product-facet queries, and the SharePoint and WordPress figures rest on the http.component match instead. The rest of the panel: MikroTik RouterOS 4,615 (3,686 on the API port 8728, 316 on 19999, 190 on 8333); FortiGate 2,750 (1,487 on 10443, 556 on 541, 266 on 443); Cisco ASA WebVPN 351 (307 on 443); Microsoft SharePoint on-prem by http.component 808; WordPress by http.component 404, a floor because component detection undercounts; Apache Tomcat 895; Remote Desktop on port 3389, 8,309; services answering on port 445, 5,545, of which only 172 carry a Samba label in the product facet; the SonicWall family 2,965 across five product strings, which cannot be narrowed to the SMA 1000 line; ownCloud 175; Metabase 118; MLflow 92; Ray 87; Langflow 75; Gitea 9; VMware vCenter 2; Artifactory 1.

Held and omitted. Three of the week's additions have no Shodan product label and were held by the discovery stage: ISC BIND, Apache Struts and ONLYOFFICE Docs. Strapi returned an http.component match whose product facet does not corroborate the family and is held for review. Check Point, F5 APM, WSO2, Adobe Commerce, Zyxel, Zammad, FortiMail and Catalyst SD-WAN Manager remain held from prior

weeks; VeloCloud returns zero by two methods and stays PROVISIONAL. LiteLLM at 6,826 and ScreenConnect at 2,644 are again not published as exposure figures, being port-scatter artefacts for a sixth week: their top five ports carry ten, seven, six, six and six instances and three, three, two, two and two respectively, against 3,686 on one port for MikroTik and 129 of 185 for ProFTPD. Langflow, MLflow and Ray are printed with the standing caveat that they show the same scatter at small totals.¹³ The KPI row counts two of six adds with a published figure.

7.2 Credential Exposure Around the Week's Listings

The aggregator's infostealer panel (third-party stealer-log telemetry from HudsonRock and ParanoidLab, shown on each victim page) for Tharisa carried no figures when read on 11 October, which is unusual for a company of its size and may reflect the record's age; it is not evidence of absence. Samwumed's record shows 94 users and two third-party employees with stealer-log records, 428 passwords of which six are marked critical, and eight external attack-surface findings, last queried at the moment of listing.^{1,6} These are third-party stealer-log counts of unknown age and they do not say how any intrusion began. For a medical scheme the relevant reading is the member side: 94 user credentials for the scheme's domain in stealer logs is the population most exposed to the phishing the scheme's own notice warns of.

7.3 What FortiBleed Means for the South African FortiGate Population

The 2,750 South African FortiGate instances are a count of exposure, and 1,487 of them answer on 10443, the port the SSL VPN portal uses by default. The FBI advisory's campaign needs nothing more than a reachable portal and a reused or weak credential, and its persistence step is a new administrative account on the firewall, which is why the action in Section 1 is a user-list search for the nineteen names the advisory records; a patch does not remove an account.^{13,16} The advisory's remedy list, in the order a South African administrator would apply it, is: remove management from the internet, end sessions, reset credentials, enforce phishing-resistant MFA, confirm PBKDF2 storage, review REST API keys and read the authentication and domain controller logs for the spraying that follows a successful login.

8. REGULATORY & POLICY

8.1 The MIP Cascade in the Notification Record: Who Has Told Whom

This week's reading adds two notices to the record of who notified in their own name after the MIP incident, and both predate the regulator's statement that it had received only MIP's. LegalWise's update of 6 July says its insurer LEZA notified the relevant regulators including the Information Regulator; Samwumed's section 22 notice of 29 June, modified 16 July, notifies its members and says nothing about the regulator.^{9,10} Set beside the regulator's answer to TechCentral on 25 September, that it had received only MIP's notification and that the obligation rests on each responsible party, the record now has at least one insurer saying it notified and the regulator saying it received one.²³ The report does not resolve that; the distinguishing observation is a further regulator answer naming the notifications it holds. Samwumed's notice adds a point of law the others do not: it describes MIP as a former provider and says historical member data in MIP's legacy environment had not been deleted, and that the scheme is

engaging MIP on its contractual obligations. Under POPIA a responsible party must not retain records longer than needed and an operator processes only on the responsible party's instruction; a processor holding a former client's data is a version of the question the regulator has been asked that the client itself has now put in writing.¹⁰

8.2 Parliament: Eight Cases, One Arrest, and a Weather Service Still Under Investigation

A written reply by the acting Minister of Police, Firoz Cachalia, to Dianne Kohler Barnard MP, reported by MyBroadband on 9 October, states that the Hawks registered eight cases under what the article calls the Cybercrimes Regulatory Framework in the past three years and made one arrest, a 30-year-old from Soweto charged with extortion and money laundering in an international sextortion matter in which forensic work has identified more than 50 further victims across jurisdictions; the investigation into the January 2025 ransomware attack on the South African Weather Service, linked to RansomHub, is ongoing with no arrest.²¹ The 8,850 attacks a month in the headline is Check Point's June telemetry, carried by the article and absent from the reply; the article does not say what the vendor counts or over what base, so the two figures cannot be compared. What matters is the reply's own figures: an electronic communications service provider or financial institution that reports a cybercrime to SAPS within 72 hours, as section 54 of the Cybercrimes Act requires of those two classes, is reporting into a unit that has registered eight such cases in three years. The reply document could not be located on the parliamentary question system by this collection and the item is single-sourced, which Section 12 records.

8.3 The Opt-Out Registry Opens, With a Fifteen-Day Comment Window on Its Guidelines

The National Consumer Commission launched the national opt-out registry in Pretoria on Wednesday 7 October, with Minister Parks Tau stating that the Commission will enforce the law in full from 15 April 2027. The sequence reported by TechCentral and Moonstone is: marketer registration opened on 15 September and runs to December; cleansing against the registry is free from December to April 2027; consumer pre-emptive blocks can already be registered against registered marketers. The money and the penalties: the 2026 registration fee is R2,574 with annual renewal at R1,930.50; the draft cleansing fee is 12 cents per blocked consumer identified (Moonstone and Werksmans; TechCentral prints 14 cents per entry, a conflict Section 12 records), with cleansed lists valid for 30 days; penalties run to the greater of R1 million or 10 per cent of annual turnover, with prosecution and up to twelve months' imprisonment in serious cases; and the draft guidelines gazetted on 2 October are open for comment for fifteen days.^{44,45} Two readings matter for a security and privacy function. Moonstone's is that financial institutions and insurers are in scope whenever a service contact turns into promotion, that a registered general block invalidates prior consent and that fresh consent cannot override it, and that complaints split between the Commission where a block exists and the Information Regulator where it does not, with the Regulator's chair saying POPIA must still be complied with. Werksmans' is that monthly uploads of customer databases to a state platform for matching may be an information matching programme under POPIA, that the draft carries no security, retention or breach provisions for that data, and that fifteen days could be argued to be insufficient; the firm asks for a suppression-list download model and a consultation well beyond fifteen days.^{45,46} The comment window closes on Saturday 17 October by TechCentral's account.⁴⁴

8.4 Disclosure Practice and Fraud Advisories: Shoprite, the FSCA, Capitec and Business Email

Shoprite's integrated report, as reported by TechCentral on 9 October, is carried in Section 3.4 as the week's example of a listed company stating a breach count and a controls rating in a public document.¹⁸ The FSCA said on 6 October that EduMe with Sandile November (Pty) Ltd was producing and selling regulatory examination certificates bearing the FSCA's and Moonstone's branding without authorisation, marketed through Facebook and WhatsApp; Moonstone is the only approved examination body for the categories concerned and the advice is that every RE communication, examination and payment goes through it directly.¹⁹ Capitec is rolling out a free Scam Checker in its app that rates a submitted link, message or screenshot from low to high risk without blocking anything, built on Amazon Bedrock, and says the tool will feed its fraud teams the account numbers and payment references it extracts from scam sites; the bank's chief information officer's framing is that most scams start with a message.⁴⁷ On the same theme MyBroadband reports, from Interpol's 2026 assessment, that 70 per cent of business email compromise detections in Africa originated in South Africa, and carries a reader-forwarded notice from the Kanonkop wine estate that its email system was briefly compromised and an unauthorised message sent, with the subject line of a tender document; the estate had not responded by publication and the item is PROBABLE on the forwarded notice.⁴⁸ SARS's scam page could not be read by this collection on 11 October and no SARS alert is cited this week; the newest known, from the W41 check, remains SARS-SCAM-400 of 2 September.

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; the media statements page shows a media advisory of 21 September on an access-to-information dialogue, which is an event notice, and its newest enforcement statement remains 2 June. The MIP, RelyComply, Gauteng e-Panic, Cartrack, CoverCubed and, on LEZA's account, LegalWise matters are before the regulator with no public instrument on any of them.^{49,50} **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 for research and education, and the Standard Bank Group and Vodacom teams for their own constituencies.⁵¹ For a medical scheme or an insurer in Samwumed's or LegalWise's position the three clocks set out in W40 apply: 24 hours to the Prudential Authority under Joint Standard 2 of 2024 for a regulated financial institution, 72 hours to SAPS under section 54 of the Cybercrimes Act where the organisation is a financial institution or an electronic communications service provider, and as soon as reasonably possible to the Information Regulator under section 22, with the Council for Medical Schemes as the sector regulator for a scheme.²³

44. TechCentral, You can join South Africa's spam registry now, but it won't bite until May, by Fanie van Rooyen (8 October 2026). <https://techcentral.co.za/opt-out-registry-spam-calls-may-2027/287094/>

45. Moonstone, Opt-out rules bring financial services into the compliance net (8 October 2026). <https://www.moonstone.co.za/opt-out-rules-bring-financial-services-into-the-compliance-net/>

46. Werksmans Attorneys, Blocking growth? Why the NCC's draft opt-out registry guidelines need revisiting, by Ahmore Burger-Smidt and Boitumelo Khwene (9 October 2026). <https://werksmans.com/blocking-growth-why-the-nccs-draft-opt-out-registry-guidelines-need-revisiting-you-were-only-given-15-days-to-comment-what-are-you-doing/>

47. MyBroadband, Good news for Capitec customers, by Hanno Labuschagne (10 October 2026). <https://mybroadband.co.za/news/security/671199-good-news-for-capitec-customers-2.html>
48. MyBroadband, Email accounts taken over in South Africa, by Luis Monzon (9 October 2026). <https://mybroadband.co.za/news/security/671057-email-accounts-taken-over-in-south-africa.html>
49. Information Regulator, Enforcement notices register, checked 11 October 2026 (newest entry Gauteng Department of Health, 10 June 2026). <https://infoeregulator.org.za/enforcement-notice/>
50. Information Regulator, Media statements page, checked 11 October 2026 (newest item a media advisory of 21 September 2026 on an access-to-information dialogue; newest statement on enforcement 2 June 2026). <https://infoeregulator.org.za/media-statements/>
51. ransomware.live API, GET /csirt/ZA, six South African CSIRTs from the FIRST directory, retrieved 11 October 2026 (feeds/r/_csirt_za_2026-10-11.json). <https://api.ransomware.live/v2/csirt/ZA>

9. WEEKLY THREAT HUNT & IOCs

Seven missions, ordered with the new group's indicators after the NetScaler item. Three P1 cover the three edge-appliance items: the NetScaler SAML pair with Citrix's configuration strings and crash signatures, the Integrity Technology Group exploit list and persistence with the advisory's own artefacts and query syntax adapted from Inception Security's post,⁵² and FortiBleed with the FBI's account names. Three P2 cover UmBra's contact indicators, the SonicWall SMA 1000 request-forgery pattern Previdian described, and the Akira intrusion Huntress mapped,⁵³ whose toolmarks are the generic ransomware playbook a South African SOC should be able to find on any week. One P3 covers the member-targeted phishing that Samwumed and LegalWise warn of. Indicators come from vendor advisories, the joint advisory, named responder reporting and the aggregator's per-group feeds, and the atomic detail is exported to iocs_w42.csv instead of being repeated in full here.³³ The Gentlemen's hashes are unchanged since W39 and TH-2026-W40-06 stands as written; the W41 SD-WAN Manager, FortiMail, INC Ransom, Zimbira and SharePoint missions likewise stand and are not reprinted.

TH-2026-W42-01: NetScaler SAML: Crash Loops, Three Fixed Builds and the Pre-Patch Checks

P1 CRITICAL: exploited before the 3 October fix; 125 exposed in ZA; overdue since 7 October

Hypothesis: An attacker has crashed, or is repeatedly crashing, a NetScaler ADC or Gateway configured as a SAML service provider or identity provider through the memory overflow CVE-2026-88779, possibly to force reboots that assist exploitation of the September command injection CVE-2026-88771, and the appliance has been patched for the September pair but not for the two SAML flaws.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1499.004 (Application or System Exploitation), T1505.003 (Web Shell, from the W41 chain), T1552.004 (Private Keys).

IOCs: Configuration strings add authentication samlAction and add authentication samlIdPProfile (in-scope test); builds below 14.1-73.41 / 13.1-64.28 / 13.1-37.282 FIPS (CVE-2026-88779) and below 14.1-73.46 / 13.1-64.29 / 13.1-37.283 (CVE-2026-107406); the W41 artefacts for the September chain, nsginstaller[0-9].deb or .sig under /var/netscaler/gui/vpn/scripts/linux/, HTTP_NSC_LDAP, HTTP_NSC_CLIENTTYPE and HTTP_X_UX request headers, /tmp/.uxdport, SUID /bin/sh, and an archive of /flash/nsconfig.

Data Sources: ns.conf; /var/log/ns.log and the AAA and SAML authentication logs; appliance uptime and reboot history; NetScaler Console CVE Detection, Impacted Instances; the output of Citrix's indicator-of-compromise script; the HA pair's failover log.

Detection Guidance: Run the two configuration greps on every appliance on Monday 12 October; any hit is in scope. On those, pull the reboot history since 1 October and treat an unexplained restart loop, repeated authentication service crashes or a run of SAML failures as grounds to collect the support bundle before patching. Run the W41 checks and Citrix's script, archive the output with the change ticket, then upgrade to 14.1-73.46 or 13.1-64.29, which cover both SAML flaws. A clean indicator-script result is not proof of absence; the W41 rotation list (administrator and directory bind credentials, TLS private keys, SSH host keys) applies to any appliance that was internet-facing while unpatched for the September pair. Sources: SOCRadar 6 October, The Register 5 October, BleepingComputer 9 October, the catalogue entry.

TH-2026-W42-02: UmBra: Contact Indicators and the Note Name of a Group With No Tooling Yet

P2 HIGH: a six-day-old group with a South African listing; contact indicators only

Hypothesis: An affiliate of the UmBra site has encrypted a South African estate with a payload that appends .ub, dropped a note named readme.txt or README-UMBRA.txt, and directed the victim to the group's email, Session or Telegram contact.

MITRE ATT&CK: T1486 (Data Encrypted for Impact), T1491.001 (Internal Defacement, ransom note), T1567 (Exfiltration Over Web Service), T1657 (Financial Theft).

IOCs: Note filenames readme.txt and README-UMBRA.txt; file extension .ub; contact email UmBraSup@proton.me; Session identifier 05e968dec429b5136fd94eccbec67ce1c56c7ba10014e35a70cc60dba3d58f2836; Telegram handle UmBraBreach; onion address umbra7isogjsgcdndz3uu6qvl5zftjptt6s3iuecjlwbt4yqyvrhcid.onion. No hash, address, mutex or YARA rule exists for the group on the feed.

Data Sources: File-creation telemetry on file servers and backup shares; EDR note-drop detections; email and web proxy logs for the contact addresses; dark-web monitoring for the organisation's own name under any country tag.

Detection Guidance: Alert on mass creation of files with the .ub extension or on a note named README-UMBRA.txt; add the contact strings to email and proxy watchlists. The practical hunt for a mining or industrial estate this week is the generic one in TH-2026-W42-06, because the group's intrusion tooling is unknown and the tempo suggests it is somebody else's. Sources: the aggregator's group page and feed, GitHub issue 392 of 6 October.

TH-2026-W42-03: Integrity Technology Group: Five Old Exploits, a Mail Bot and SoftEther as conhost.exe**P1 CRITICAL:** five KEV entries due 11 October; victims in Africa; 185 ProFTPD exposed in ZA

Hypothesis: A state-linked operator has used MicroScan-class scanning scripts to exploit ProFTPD mod_copy (CVE-2015-3306), ONLYOFFICE Document Server (CVE-2021-3199), Apache Struts S2-032 (CVE-2016-3081), ISC BIND TKEY (CVE-2015-5477), Strapi (CVE-2023-22894), Shellshock, Pulse Connect Secure or GitLab on an internet-facing host, sprayed passwords at Exchange with EBurst, pulled mailboxes with the Curlc4 bot or office-cli, run DC.exe for DCSync replication and installed SoftEther VPN under a Windows system binary name for persistence.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1110.003 (Password Spraying), T1114.002 (Remote Email Collection), T1003.006 (DCSync), T1036.005 (Match Legitimate Name or Location), T1572 (Protocol Tunneling), T1560 (Archive Collected Data).

IOCs: Process names conhost.exe or dllhost.exe running outside System32, or with SoftEther product metadata (vpnclient, vpnbridge); files live700_v1.exe, DiagTrack.exe, Curlc4.txt, DC.exe, office-cli, /var/tmp/.sess.zip, staging names 001.gif, Css.js, M2k.js, M2k_list.js, M2k_ui_adm.js, Include.png, All_scanner_vXX.pl.gz; domains dns.studiocloud[.]xyz, natcloudservice[.]com, upl.natcloudservice[.]com, 98aiblog[.]com, hmbcloud[.]com, hmbcloud[.]net, hmbipic-01[.]com, iepl.node[.]cm, javacheck.ooguy[.]com, javaupdate.giize[.]com, sexytube0[.]com, twimg.co[.]uk; address 149.28.132[.]137; FTP commands SITE CPFR and SITE CPTO; Struts requests with method: in the parameter name; BIND TKEY queries from untrusted sources. The advisory's full IP list runs to several hundred entries with first-seen and last-seen dates, several from 2016, and is to be vetted before blocking.

Data Sources: FTP server logs (xferlog, proftpd.log); web server access logs for Struts, Strapi and ONLYOFFICE paths; named query logs; Exchange IIS logs (401 responses with Win32 status 1326 or 2148074252 against EWS and OWA); Security event 4662 with the directory replication GUIDs from accounts that are not domain controllers; Sysmon 1, 3 and 22; EDR process and DNS telemetry; Microsoft 365 sign-in and MailItemsAccessed audit logs.

Detection Guidance: Inventory first: list every internet-facing ProFTPD, Struts, Strapi, ONLYOFFICE and BIND instance and patch or retire it by Friday 16 October, checking ProFTPD for mod_copy loaded and Struts for Dynamic Method Invocation. Then hunt: process events where the image name is conhost.exe or dllhost.exe and the path is not System32; 4662 replication events from non-DC accounts; EWS and OWA 401 bursts from one source against many users; DNS and proxy hits on the listed domains; FTP logs for SITE CPFR or CPTO. Sources: joint advisory AA26-281A as published by IC3, The Hacker News 9 October, the catalogue; query syntax adapted from Inception Security's post.

TH-2026-W42-04: FortiBleed: Harvested SSL VPN Credentials and Attacker-Created Administrators

P1 CRITICAL: more than 86,644 compromised devices in 194 countries (SOCRadar count, cited by the FBI and USSS); 2,750 FortiGate exposed in ZA

Hypothesis: An initial-access broker has logged into a FortiGate SSL VPN portal with a stuffed, sprayed or previously harvested credential, cracked stored hashes, created an administrative account for persistence, enumerated Active Directory, and sold the access to an INC, Lynx or Payload affiliate.

MITRE ATT&CK: T1078 (Valid Accounts), T1110.003 (Password Spraying), T1110.004 (Credential Stuffing), T1136.001 (Create Account: Local Account), T1087.002 (Domain Account Discovery), T1021 (Remote Services).

IOCs: Local administrator or VPN accounts named adminin, admin, forticloud-tech, gttadmin, Technical_support, my_admin, fortiAdmin, fgtsecure, districtadmin, roadmin, adminsslvpn, support_fortinet, forti_support2, forticloud-sync, pakedge, system_config, itadmin, IT_Manager or fgtsec that the organisation did not create; administrator passwords stored with a legacy SHA-256 hash instead of PBKDF2; REST API keys with no owner; SSL VPN logins from residential or hosting ranges followed by LDAP or SMB enumeration.

Data Sources: FortiGate event logs (admin login, config change, user add); SSL VPN logs (tunnel up, failed logins by source); FortiAnalyzer or syslog; domain controller 4625 and 4771 bursts after a VPN login; LDAP query logs; Active Directory account-enumeration telemetry.

Detection Guidance: On Monday 12 October export the local user and administrator list from every FortiGate and match it against the nineteen names; any match is an incident regardless of patch level. Then apply the advisory's sequence: remove management from the internet, end sessions, reset credentials, enforce phishing-resistant MFA, confirm PBKDF2, review API keys. Hunt the VPN logs for a successful login preceded by many failures from the same source, and the domain logs for enumeration within the hour after it. Sources: FBI and USSS JCSA-20261006-01, The Hacker News 7 October, the Shodan panel for the population.

TH-2026-W42-05: SonicWall SMA 1000: The WorkPlace Request-Forgery Pattern Seen on Honeypots

P2 HIGH: CVSS 10 by the vendor; attempts within three days of the fix; not yet in the KEV catalogue

Hypothesis: An attacker is probing an SMA 1000 appliance's WorkPlace portal with the CVE-2026-102255 request forgery to reach the internal CouchDB service and invoke its design-document rewrite function, using default credentials, as a first step to unauthorised operations on the appliance.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1078.001 (Default Accounts), T1210 (Exploitation of Remote Services).

IOCs: An OPTIONS request to the WorkPlace Extraweb interface; a request path or parameter reaching 127.0.0.1:5984; traversal into a CouchDB design document and a call to its _rewrite function; an HTTP Basic Authorization header for admin:admin; firmware 12.4.3-03526 or 12.5.0-02952 and earlier on the 6210, 7210 or 8200v.

Data Sources: SMA 1000 appliance management console logs and web access logs; upstream WAF or reverse-proxy logs; NetFlow from the appliance to its own loopback is not observable, so the external request pattern is the hunt.

Detection Guidance: Apply the hotfix to 12.4.3-03670 or 12.5.0-03082 on Monday 12 October; the appliance restarts. Search the access logs since 6 October for OPTIONS requests to the WorkPlace interface and for the strings 5984 and _rewrite in any request. The SMA 100 series and firewall SSL VPN are not affected by this flaw. Sources: BleepingComputer 9 October for the honeypot pattern, The Hacker News 7 October for the versions, SonicWall advisory SNWLID-2026-0017 as reported.

TH-2026-W42-06: Akira Playbook: RDP From an Unknown Workstation to Shadow-Copy Deletion and Encryption**P2 HIGH:** Huntress's September intrusion; generic artefacts every estate should be able to find

Hypothesis: An affiliate has reached an endpoint over RDP from a workstation the organisation does not own, stopped the endpoint protection services from its console, dumped LSASS with procdump from C:\PerfLogs, deployed a GOST tunnel as svchost.exe in C:\PerfLogs\Temp, ran rclone, deleted shadow copies and encrypted the Shares tree; Huntress gives no clock times, and places the tunnel about four hours after encryption began, so the order of the middle steps is not fixed.

MITRE ATT&CK: T1021.001 (Remote Desktop Protocol), T1562.001 (Disable or Modify Tools), T1003.001 (LSASS Memory), T1090 (Proxy), T1567.002 (Exfiltration to Cloud Storage), T1490 (Inhibit System Recovery), T1486 (Data Encrypted for Impact).

IOCs: Workstation name C1IFRYXI in RDP logon events; GOST tunnel C2 64.227.4[.]134; C:\PerfLogs\Temp\svchost.exe SHA-256 d00833318a04caa019c6f95dcb3598ad947d405010bfb2f3cbd04530a00bc3a4 loading config.dll; C:\storage\win.exe SHA-256 1f1bb322591b6d27fd2946e373d7d2efc2f4e1e66818846060d391600b600fba; procdump.exe and rclone launched from C:\PerfLogs; Service Control Manager 7036 stopped events for the four Bitdefender Endpoint services; PowerShell Get-WmiObject Win32_Shadowcopy piped to Remove-WmiObject.

Data Sources: TerminalServices-RemoteConnectionManager and Security 4624 type 10 events; System log 7036; PowerShell script block logs; EDR process telemetry with parent paths; shellbags on the affected host; the domain controller's EDR alerts.

Detection Guidance: Alert on any svchost.exe whose path is not System32 or SysWOW64; on procdump or rclone anywhere under C:\PerfLogs; on four or more endpoint-protection service stops within a minute; and on the shadow-copy removal command line. Correlate an RDP logon from a workstation name absent from the asset register with any of these in the following 24 hours. Sources: Huntress 6 October; the MITRE mapping is the report's own.

TH-2026-W42-07: MIP-Set Phishing: Members and Policyholders Targeted With Their Own Records**P3 MEDIUM:** the risk both Samwumed and LegalWise state in their notices; no actor artefacts

Hypothesis: A fraudster holding records from the MIP set (names, identity numbers, historical membership or policy numbers, treating doctors, banking details) is contacting members and policyholders by email, SMS or telephone, impersonating the scheme, the insurer or a bank, to harvest OTPs and banking credentials or to lodge fraudulent claims.

MITRE ATT&CK: T1566 (Phishing), T1598 (Phishing for Information), T1656 (Impersonation), T1657 (Financial Theft).

IOCs: Inbound messages to members quoting a historical membership or policy number; sender domains that resemble samwumed.org, legalwise.co.za or hollard.co.za; claims submitted against historical membership numbers; calls to the schemes' fraud lines reporting impersonation. No actor infrastructure is published for this activity and none is invented here.

Data Sources: The organisation's own inbound mail gateway and brand-impersonation monitoring; domain registration watch on look-alike names; claims-system anomaly reports on historical member numbers; the fraud hotline log; SAFPS registrations.

Detection Guidance: Register look-alike domains for watch; route member reports of impersonation to one queue and count them weekly; flag claims against membership numbers closed before 2026; brief call-centre staff that a caller quoting a correct historical membership number is not thereby verified. Sources: Samwumed section 22 notice, LegalWise update of 6 July; the detection logic is the report's own.

52. Inception Security, AA26-281A: hunt SoftEther VPN renamed as conhost.exe (9 October 2026; a vendor's hunt-query translation of the advisory, used for query structure only). <https://www.inceptionsecurity.com/post/aa26-281a-softether-conhost-hunt>

53. Huntress, Up a creek without a command line: mapping an Akira ransomware attack, by Harlan Carvey and Lindsey O'Donnell-Welch (6 October 2026). <https://www.huntress.com/blog/mapping-akira-ransomware-attack>

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

- 1. Make the SAML configuration test the first NetScaler task on Monday 12 October, and move every in-scope appliance to the 9 October builds.** Two configuration strings decide scope; the September patch does not cover the two SAML flaws; and the pre-patch checks from W41 still come first because the command-injection chain leaves evidence the upgrade may remove.
- 2. Run the component inventory the advisory implies, in addition to the product inventory you already have.** ProFTPD, Struts, Strapi, ONLYOFFICE and BIND are components under file-transfer portals, old intranet applications and resolvers, and a product inventory does not list them. Scan your own ranges for them, compare against the 185 ProFTPD instances the country exposes, and retire what cannot be patched by Friday 16 October.
- 3. Audit every FortiGate's local user list this week and treat the nineteen names as indicators, whatever the firmware.** The campaign is credential-based and its persistence is an account, so the hunt is a user-list diff and a PBKDF2 check; the firmware version does not answer it.
- 4. Watch your own name on leak sites without trusting the country tag.** Samwumed sat under KR for eleven days. A monitoring rule keyed on the organisation's name, domain and common misspellings, across the aggregators, with the country field ignored, would have caught it on 30 September.
- 5. Put the generic Akira artefacts into standing detections.** A svchost.exe outside System32, procdump or rclone under C:\PerfLogs, four protection-service stops in a minute, and the WMI shadow-copy deletion are four signals the Huntress case produced and that affiliate intrusions commonly produce, and they need no threat intelligence subscription to detect.

Management (CISO / Board)

- 1. Ask whether the organisation has planned for the extortion stage of a supplier breach it has already disclosed.** LegalWise and Samwumed told their members in June and were listed with timers in late September. The plan is a holding statement, a decision in advance on engagement, a monitoring rule on the organisation's own name, and the regulator notification record ready to produce, by Friday 16 October.
- 2. Settle, for each administrator, binder holder and former provider, whether it still holds your data and whether it was an MIP or RelyComply client.** Samwumed's notice says a former provider still held historical member data; the regulator has said the duty follows the responsible party. A written answer from each counterparty, and a deletion certificate from each former one, is the evidence a board can show.
- 3. Benchmark your own integrated report against Shoprite's disclosure.** A breach count, an affected-customer count and a controls-effectiveness rating in a public document is now the practice of at least one JSE-listed retailer; the question for an audit committee is whether its own report says as much, and whether its cyber controls rating is management's or an independent assessor's.

4. Keep the edge-appliance inventory on the risk register and add a column for the number of emergency upgrades this quarter. A NetScaler needed three fixed builds in twelve days. An estate that cannot absorb that has a change-management constraint that the board should know about before the next zero-day.

5. Decide by Friday 16 October whether to comment on the opt-out registry guidelines, and who owns the registry relationship. The fifteen-day window closes on 17 October; on Werksmans' reading the draft turns every telephone or digital marketing function into a monthly data transfer to a state platform with no stated security terms, and on the NCC's own account a registered block overrides prior consent. Both are decisions that belong with the information officer and the board as well as the marketing team.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH, 25th CONSECUTIVE WEEK

The South African cyber threat level remains HIGH for a twenty-fifth consecutive week (4 to 10 October 2026). Escalation to CRITICAL was not seriously in question: the week's South African claim is unconfirmed, the listings against the insurer and the scheme follow their own June disclosures and are unconfirmed as to what the group holds, no South African organisation reported an outage, and the state-linked campaign's African victims are unnamed. De-escalation to MEDIUM was considered on the single new listing and rejected: a third NetScaler zero-day against 125 exposed instances, a CVSS 10 SMA 1000 flaw with exploitation attempts and no KEV catalogue entry yet, the FortiBleed figures the FBI advisory cites against 2,750 exposed FortiGates, and a new group's 856 GB claim against a listed producer are each sufficient on their own to hold the level.

Rationale

The edge took three new reasons to act in one week. A NetScaler SAML zero-day exploited before its fix, an SMA 1000 request forgery with honeypot attempts consistent with it three days after its fix, and an FBI and Secret Service advisory citing SOCRadar's count of more than 86,644 compromised FortiGate devices, against South African populations of 125 NetScalers, 2,965 across the SonicWall family (not narrowable to the SMA 1000) and 2,750 FortiGates.

The Gentlemen is listing organisations MIP's incident already touched. Two of this fortnight's names had published notices in June; what the group holds for each is unconfirmed, and the rationale rests on the pattern itself. If it holds, the population of likely next listings is, in outline, public.

A state-linked operator's exploit list entered CISA's KEV catalogue with Africa named as a victim region. Five flaws from 2015 to 2023, added on 8 October because they are being exploited now, three of them with exploitation probabilities above 0.96, against components that are rarely inventoried; 185 ProFTPD instances are exposed in the country.

A new group listed a listed company and nobody has said anything. Tharisa's claim is unverified, the group is six days old, and the company's next scheduled document is on Tuesday 13 October; the absence of a statement is itself the open question.

Next-Week Watch (W43)

Tharisa. The distinguishing observations are a SENS or RNS announcement, a mention in the 13 October production report, a published sample on the group's site, and a South African publication carrying the listing. Silence through the production report leaves the item CLAIMED and says something about how a dual-listed company reads materiality.

UmBra's second week. Whether the site survives, whether any of its nine victims confirms, and whether a sample or builder ties the encryptor to a known family. A tenth listing with a data figure and no victim confirmation anywhere keeps the rebrand inference alive without proving it.

The MIP timers. Direct observation of the group's site for LegalWise, Samwumed and Edcon after the 9 October expiry; a published sample in the Hollard record format; a Samwumed statement on whether the listed data is the MIP set; any statement from Edcon's business rescue practitioners. A listing against any further insurer on MIP's client list is the expected next observation and should be checked under every country tag.

The regulator conflict. A further Information Regulator answer naming which section 22 notifications it holds in the MIP matter would resolve whether LEZA's and CoverCubed's filings were received as such. Without it the conflict stands as recorded.

The SMA 1000 KEV decision. Whether CVE-2026-102255 was added on 9 or 10 October, after this edition's catalogue cut-off, or in the W43 window; either way it is the first item to check in the next feed, together with Microsoft's 13 October releases.

ATNS and BCX. The Friday 16 October test for ATNS stands as set in W41: contract award, a statement with a detection date or family, a leak-site listing, or a section 22 notice. For BCX, a Telkom statement, a published sample, or a municipal customer naming an application.

BlackLocks. The index stood at three through 11 October; if nothing is added by Friday 16 October, the question W40 raised, whether two South African listings on one day signalled a group working this country, closes as unanswered.

A South African NetScaler compromise. The W41 fortnight ran to 11 October with no South African organisation reporting a NetScaler intrusion; the item closes as unobserved, with the standing caveat that absence is not evidence, and the SAML pair resets the question for a further fortnight to Sunday 25 October.

Collector tasks. The port-concentration test, now six weeks outstanding and applied by hand this week; a world-feed search keyed on South African names and domains with the country field ignored, which Samwumed shows is needed; a rule that a company check reads the media centre as well as the home page; and the Saturday-evening media sweep recorded after ATNS.

Closed this week. The LegalWise client question, by the company's June and July statements. The W41 fortnight test for a South African NetScaler compromise, as unobserved. Carried without re-argument: Guardrisk and CoverCubed, RelyComply, Cell C Fibre, Cartrack, VSB Attorneys, Rohloff, The Courier Guy, Babcock, the Furniture Bargaining Council claim, Toyota's SMS provider, Implats, Hungry Lion, the Gauteng e-Panic exposure 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 11 October 2026, with the exceptions this note records: the CISA catalogue URL is the public location of a file read locally; CISA's own advisory page for AA26-281A returned an error to this collection and the advisory is cited from the PDF published by IC3; the SonicWall PSIRT page for SNWLID-2026-0017 returned no advisory text and the advisory is cited through The Hacker News and BleepingComputer; the Citrix bulletins CTX697174 and CTX697191 are cited through SOCRadar, The Register, Sophos and BleepingComputer; the SARS scams page could not be read and no SARS item is cited; the ITWeb security index could not be read on 11 October and no ITWeb item is cited; the parliamentary reply reported by MyBroadband could not be located on the parliamentary question system and rests on that article. **Collection notes.** The feed run completed at 02:05 UTC on 11 October 2026 and passed its integrity check with exit status 0; the victim feed and catalogue figures it produced are stated in Sections 5 and 6. The catalogue version is 2026.10.08, released 20:09 UTC on Thursday 8 October, so additions of Friday 9 and Saturday 10 October fall to W43. The RSS sweep read 58 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. **Two corrections to W41.** Samwumed, listed 30 September under a KR tag, was missed; W41's window count of three is corrected to four. LegalWise's website carried statements of 26 June and 6 July naming MIP Holdings; W41's statement that it carried no notice, and that the client question was open, was wrong at publication because the check read the home page only. Both are recorded in Section 1; the process rules that follow are in Section 11. **Provenance of the machine-read feeds.** Every ransomware.live, NVD and EPSS figure in this report was retrieved from those services' APIs and the sources are cited as the endpoints actually called; the rendered ransomware.live pages used, the country page, the group pages for UmBra and The Gentlemen and the victim pages, are cited as cross-checks of records also present in the feed, except Samwumed's, which is absent from the ZA-scoped feed by the aggregator's own tag. **Figures withheld or held.** LiteLLM (6,826) and ScreenConnect (2,644) are disclosed here but not published as exposure figures, being port-scatter artefacts for a sixth week; Strapi's 57 by http.component is held for review; VeloCloud's zero is PROVISIONAL; 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 Hacker News prints CVSS 7.2 for Strapi CVE-2023-22894 where the NVD feed gives 4.9; the feed is used. GitHub issue 392 names the UmBra note REDME-UMBRA.txt where the aggregator records readme; both are carried. TechCentral prints the opt-out cleansing fee as 14 cents per entry where Moonstone and Werksmans give 12 cents per blocked consumer, and Werksmans dates free cleansing from January where the other two say December; the 12 cents and December are carried as the majority reading. Sophos dates Citrix's disclosure of CVE-2026-88779 to 4 October where SOCRadar and The Register give 3 October; the report uses 3 October for the fix and 4 October for the catalogue listing. The aggregator calls Tharisa Cyprus-based and tags it ZA; the report states both. **Attribution policy.** Where a story was broken by a publication this report names who broke it, links to them, and summarises only what the intelligence judgement requires. The compiler of this report is quoted in MyBroadband's 5 October article; that article is cited for the companies' statements only and the timers and client-status findings rest on TechCentral's article of the same day. **Single-source disclosure.** The parliamentary reply on MyBroadband; Shoprite's integrated report on TechCentral; the Kanonkop notice on MyBroadband; the

Qilin arrest on The Record's account of the National Police Agency; the Comparitech figures on Infosecurity Magazine; the SMA 1000 honeypot pattern on BleepingComputer's account of Previdian; the Atlassian exploitation on Infosecurity Magazine's account of VulnCheck; the Akira intrusion on Huntress alone. **Claims deliberately excluded.** The Tharisa, LegalWise, Samwumed and Edcon listings are carried as claims only; UmBra's 856 GB is the actor's figure; the aggregator's infostealer counts are third-party telemetry of unknown age; the inference that UmBra is a rebrand or affiliate with existing access is marked as an inference; watchTower's reading that the NetScaler crashes assist exploitation of the September flaw is carried as a hypothesis; the Interpol 70 per cent figure is carried as MyBroadband reports it and the assessment itself was not re-read this week. The FortiBleed count of 86,644 is SOCRadar's, cited in the FBI and Secret Service advisory and dated to 19 June by The Hacker News; the report does not present it as a federal count.

- ransomware.live, victim page for Tharisa (UmBra), discovered 7 October 2026 08:23 UTC, estimated attack date 7 October 2026, 856 GB claimed, leak screenshot present, no deadline or published-data marker, infostealer panel empty; retrieved 11 October 2026; the same record is in the locally retrieved country feed. <https://ransomware.live/id/VGhhcmlyYUBvUjYyYQ==>
- ransomware.live, group page for UmBra (marked New Group, Active; nine victims in five countries by 10 October 2026; ransom note readme.txt; onion address, email, Session and Telegram contacts), read 11 October 2026. <https://www.ransomware.live/group/UmBra>
- JMousqueton/ransomware.live on GitHub, issue 392, [New Group] UmBra Group DLS (opened 6 October 2026; first listed victim Four Hands LLC; ransom extension .ub; note file REDME-UMBRA.txt). <https://github.com/JMousqueton/ransomware.live/issues/392>
- Tharisa plc, SENS and RNS announcements page, checked 11 October 2026 (newest announcement 30 September 2026, board succession; Q4 FY2026 production report scheduled 13 October 2026; the only cyber-titled announcement is Cybersecurity incident, 19 December 2024). <https://www.tharisa.com/sens-rns-announcements.php>
- Tharisa plc, Investor calendar, checked 11 October 2026 (13 October 2026 Q4 FY2026 production report; 30 November 2026 FY2026 results; the page states that dates are indicative only). <https://www.tharisa.com/investor-calendar.php>
- ransomware.live, victim page for Samwumed (The Gentlemen), discovered 30 September 2026 03:40 UTC, estimated attack date 29 September 2026, country field KR, description places the scheme in Cape Town; no data size, deadline or published-data marker; read 11 October 2026. <https://www.ransomware.live/id/U2Ftd3VtZWRAZGhlZ2VudGxlbWVU>
- TechCentral, Ransomware gang threatens to dump more South African client data, by Duncan McLeod (5 October 2026). <https://techcentral.co.za/ransomware-gang-south-african-client-data-legalwise-samwumed-edcon/286877/>
- LegalWise, Statement regarding third-party cybersecurity incident (26 June 2026). <https://www.legalwise.co.za/media-centre/statement-regarding-third-party-cybersecurity-incident>
- LegalWise, Important update regarding a third-party cybersecurity incident (6 July 2026; names MIP Holdings; LEZA has notified the Information Regulator). <https://www.legalwise.co.za/media-centre/important-update-regarding-a-third-party-cybersecurity-incident>
- SAMWUMED, Data security breach notice in terms of section 22 of POPIA (page published 29 June 2026, modified 16 July 2026; names MIP Holdings (Pty) Ltd as former administration platform provider). <https://www.samwumed.org/notice-of-security-compromise-in-term-s-of-section-22-of-the-protection-of-personal-information-act-4-of-2013-popia/>
- CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.10.08, released 8 October 2026 20:09 UTC, retrieved 11 October 2026 (feeds/kev_2026-10-11.json). <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- SOCRadar, CVE-2026-88779: Citrix NetScaler zero-day (6 October 2026; affected and fixed builds, SAML preconditions, detection guidance). <https://socradar.io/blog/cve-2026-88779-citrix-netscaler-zero-day/>
- Shodan country:ZA exposure panel, VERIFIED results only, retrieved 02:01 UTC 11 October 2026 (feeds/shodan_z_a_2026-10-11.json). <https://www.shodan.io/search?query=country%3AZA>
- FBI, CISA, NSA and partner agencies, joint advisory AA26-281A, Chinese government-linked cyber threat actors combine automated and hands-on hacking tools to steal sensitive data (8 October 2026; PDF as published by IC3). <https://www.ic3.gov/CSA/2026/261008.pdf>
- BleepingComputer, Max severity SonicWall SMA1000 flaw now exploited in attacks, by Sergiu Gatlan (9 October 2026; Previdian honeypot observations). <https://www.bleepingcomputer.com/news/security/max-severity-sonicwall-sma1000-flaw-now-exploited-in-attacks/>
- FBI and US Secret Service, joint cybersecurity advisory JCSA-20261006-01, FortiBleed operations continue targeting exposed systems leading to reports of lockouts (6 October 2026). <https://www.ic3.gov/CSA/2026/261006.pdf>
- ransomware.live API, GET /v2/countryvictims/ZA, 136 records, za_records 136 against server_returned 136, filter purity 1.0, FREE v2 tier (delayed relative to PRO), retrieved 02:00 UTC 11 October 2026 and stored as feeds/ransomwarelive_z_a_2026-10-11.json. <https://api.ransomware.live/v2/countryvictims/ZA>
- TechCentral, Shoprite ranks cybersecurity as its number one risk, by Duncan McLeod, on the Shoprite Holdings 2026 integrated report (9 October 2026). <https://techcentral.co.za/shoprite-cybersecurity-number-one-risk/287148/>
- Moonstone, Warning over RE certificates bearing FSCA's and Moonstone's branding, on the FSCA statement of 6 October (8 October 2026). <https://www.moonstone.co.za/warning-over-re-certificates-bearing-fscas-and-moonstones-branding/>
- Infosecurity Magazine, Critical flaw in multiple Atlassian products exploited in the wild, by Kevin Poireault (8 October 2026; CVE-2026-21589). <https://www.infosecurity-magazine.com/news/critical-vulnerability-atlassian/>
- MyBroadband, South Africa faces 8,850 cyberattacks per month but made only 1 arrest in 3 years, by Luis Monzon, on a parliamentary reply by acting police minister Firoz Cachalia to Dianne Kohler Barnard MP (9 October 2026). <https://mybroadband.co.za/news/security/671568-south-africa-faces-8850-cyberattacks-per-month-but-made-only-1-arrest-in-3-years.html>
- Mining Weekly, Tharisa assures stakeholders it is managing cybersecurity incident (19 December 2024). <https://www.miningweekly.com/article/tharisa-assures-stakeholders-it-is-managing-cybersecurity-incident-2024-12-19>
- TechCentral, Insurers carry the can for MIP breach, regulators say (25 September 2026). <https://techcentral.co.za/insurers-mip-breach-regulators/286482/>
- MyBroadband, Ransomware group threatens to leak customer data from top insurance companies in South Africa, by Luis Monzon (5 October 2026; cited for the companies' statements only, see the attribution note in Section 12). <https://mybroadband.co.za/news/security/670417-ransomware-group-threatens-to-leak-customer-data-from-top-insurance-companies-in-south-africa.html>

25. ransomware.live, victim page for LegalWise (The Gentlemen), discovered 30 September 2026 03:40 UTC, re-read 11 October 2026 (no deadline, sample or published-data marker on the record). <https://ransomware.live/id/TGVnYwXaXNIQHROzWdlbnRsZWl1bg==>

26. Infosecurity Magazine, Q3 2026 sets new record for ransomware attacks, by James Coker, on Comparitech's Q3 2026 roundup of 7 October (9 October 2026). <https://www.infosecurity-magazine.com/news/q3-new-record-ransomware/>

27. BCX, corporate website, checked 11 October 2026 (no notice, banner or statement on any incident). <https://www.bcx.co.za/>

28. ransomware.live, victim page for Edcon (The Gentlemen), discovered 30 September 2026 03:40 UTC, re-read 11 October 2026 (no deadline, sample or published-data marker on the record). <https://ransomware.live/id/RWRjb25AdGhIZ2VudGxlbWVu>

29. Hollard, Media centre press releases, checked 11 October 2026 (no item on the cyber matter). <https://www.hollard.co.za/media-centre/press-releases>

30. RelyComply, RelyComply cyber incident: what happened and what you can do, official notice (published 16 September 2026; re-read 11 October 2026, page still reads last updated 16 September 2026). <https://relycomply.com/relycomply-cyber-incident-what-happened-and-what-you-can-do/>

31. ransomware.live API, GET /groups, 407 groups with victim counts, retrieved 11 October 2026 and compared with the 4 October retrieval (feeds/r1_groups_2026-10-11.json). <https://api.ransomware.live/v2/groups>

32. ransomware.live API, GET /ransomnotes/{group}, retrieved 11 October 2026 (feeds/r1_ransomnotes_2026-10-11.json; UmBra note filename readme). <https://api.ransomware.live/v2/ransomnotes/umbra>

33. ransomware.live API, GET /iocs/{group} for the groups active against South Africa in the last 120 days, retrieved 11 October 2026 (feeds/r1_iocs_2026-10-11.json; UmBra carries one Session identifier, one email address and one Telegram handle). <https://api.ransomware.live/v2/iocs/umbra>

34. The Hacker News, Flax Typhoon exploits five flaws as CISA sets October 11 deadline for federal agencies, by Ravie Lakshmanan (9 October 2026). <https://thehackernews.com/2026/10/flax-typhoon-exploits-five-flaws-as.html>

35. The Hacker News, FBI warns FortiBleed remains active after amassing 86,644 Fortinet device credentials, by Ravie Lakshmanan (7 October 2026). <https://thehackernews.com/2026/10/fbi-warns-fortibleed-remains-active.html>

36. The Record, Japan confirms arrest of Russian Qilin operative, extradition to Germany, by Jonathan Greig (9 October 2026). <https://therecord.media/japan-germany-ransomware-arrest>

37. NIST NVD, CVE API 2.0, CVSS base scores with scoring source for the 57 catalogue entries added in the last 45 days, retrieved 11 October 2026 (feeds/nvd_cvss_2026-10-11.json). <https://services.nvd.nist.gov/rest/json/cves/2.0>

38. FIRST, EPSS API, scores for the same 57 entries, retrieved 11 October 2026 (feeds/epss_2026-10-11.json). <https://api.first.org/data/v1/epss>

39. The Register, Citrix NetScaler security snafus get even worse amid more 0-day reports, by Jessica Lyons (5 October 2026). <https://www.theregister.com/security/2026/10/05/citrix-netscaler-security-snafus-get-even-worse-amid-more-0-day-reports/5301232>

40. Sophos, Citrix NetScaler vulnerability (CVE-2026-88779) in active exploitation (October 2026). <https://www.sophos.com/en-us/blog/citrix-netscaler-vulnerability-cve-2026-88779-in-active-exploitation>

41. BleepingComputer, Citrix warns admins to patch new NetScaler RCE flaw immediately, by Sergiu Gatlan (9 October 2026; CVE-2026-107406, bulletin CTX697191). <https://www.bleepingcomputer.com/news/security/citrix-warns-admins-to-patch-new-netscaler-rce-flaw-immediately/>

42. The Hacker News, SonicWall patches CVSS 10.0 pre-authentication SSRF flaw in SMA1000 appliances, by Swati Khandelwal (7 October 2026; advisory SNWLID-2026-0017 of 6 October). <https://thehackernews.com/2026/10/sonicwall-patches-cvss-100-pre.html>

43. ransomware.live, South Africa country page, cross-check only (showed 136 victims with Tharisa newest when read on 11 October 2026, agreeing with the API file). <https://www.ransomware.live/country/ZA>

44. TechCentral, You can join South Africa's spam registry now, but it won't bite until May, by Fanie van Rooyen (8 October 2026). <https://techcentral.co.za/opt-out-registry-spam-calls-may-2027/287094/>

45. Moonstone, Opt-out rules bring financial services into the compliance net (8 October 2026). <https://www.moonstone.co.za/opt-out-rules-bring-financial-services-into-the-compliance-net/>

46. Werksmans Attorneys, Blocking growth? Why the NCC's draft opt-out registry guidelines need revisiting, by Ahmore Burger-Smidt and Boitumelo Khwene (9 October 2026). <https://werksmans.com/blocking-growth-why-the-nccs-draft-opt-out-registry-guidelines-need-revisiting-you-were-only-given-15-days-to-comment-what-are-you-doing/>

47. MyBroadband, Good news for Capitec customers, by Hanno Labuschagne (10 October 2026). <https://mybroadband.co.za/news/security/671199-good-news-for-capitec-customers-2.html>

48. MyBroadband, Email accounts taken over in South Africa, by Luis Monzon (9 October 2026). <https://mybroadband.co.za/news/security/671057-email-accounts-taken-over-in-south-africa.html>

49. Information Regulator, Enforcement notices register, checked 11 October 2026 (newest entry Gauteng Department of Health, 10 June 2026). <https://infoeregulator.org.za/enforcement-notice/>

50. Information Regulator, Media statements page, checked 11 October 2026 (newest item a media advisory of 21 September 2026 on an access-to-information dialogue; newest statement on enforcement 2 June 2026). <https://infoeregulator.org.za/media-statements/>

51. ransomware.live API, GET /csirt/ZA, six South African CSIRTs from the FIRST directory, retrieved 11 October 2026 (feeds/r1_csirt_za_2026-10-11.json). <https://api.ransomware.live/v2/csirt/ZA>

52. Inception Security, AA26-281A: hunt SoftEther VPN renamed as conhost.exe (9 October 2026; a vendor's hunt-query translation of the advisory, used for query structure only). <https://www.inceptionsecurity.com/post/aa26-281a-softether-conhost-hunt>

53. Huntress, Up a creek without a command line: mapping an Akira ransomware attack, by Harlan Carvey and Lindsey O'Donnell-Welch (6 October 2026). <https://www.huntress.com/blog/mapping-akira-ransomware-attack>

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.