



SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 17 | 13-19 April 2026

THREAT LEVEL: CRITICAL

Standard Bank 1.2TB data publicly released by ROOTBOY — Africa's largest bank. XP95 deadline TODAY (20 Apr). PoImed (100K+ SAPS officers). Adumo POS source code. Cisco IOS-XE CVSS 9.8 zero-day (Salt Typhoon). 167 MS CVEs. SA victim count: 105.

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W17 | Classification: TLP:WHITE

© 2026 Digital Progression | dpcyber.co.za

TABLE OF CONTENTS

- 1. Executive Summary
- 2. Threat Landscape Heatmap
- 3. SA Cyber Incidents & Breaches
- 4. Nation-State: Salt Typhoon & Cisco IOS-XE Zero-Day
- 5. Active Threat Campaigns
- 6. Critical Vulnerabilities
- 7. Threat Actor Profiles & Ransomware Activity
- 8. OSINT Exposure & Attack Surface
- 9. Regulatory & Compliance
- 10. Weekly Threat Hunt & IOCs
- 11. Recommendations
- 12. OSINT Sources Consulted

1. EXECUTIVE SUMMARY

Overall Threat Level: CRITICAL (upgraded from HIGH in W16) — Week 17 represents SA’s most severe concurrent cyber crisis on record. Standard Bank, Africa’s largest bank by assets, had 1.2TB of client data publicly released by threat actor ROOTBOY — 154 million SQL rows including client names, ID numbers, account details, and limited credit card data. The XP95 20 April deadline arrives at the end of this reporting window, with both Statistics South Africa (453K+ records) and the Gauteng City Region Academy (429K+ student records) legally prohibited from paying ransoms. ShinyHunters targeted Polmed — the SAPS medical scheme serving 100,000+ police officers — creating direct physical safety risk to law enforcement personnel. Adumo, SA’s largest independent payments processor processing R80B+ annually, had POS source code and chip-and-PIN certification artefacts offered on the dark web. Cisco IOS-XE CVE-2026-1834 (CVSS 9.8) is actively exploited as a zero-day with direct Salt Typhoon relevance to the confirmed SA telecom compromise. Microsoft’s April Patch Tuesday addressed 167 CVEs — the second-largest ever — including 2 zero-days.¹

KPI Dashboard

Metric	Current (W17)	Baseline / Prior	Change	Direction
SA cyberattacks/week	2,204	1,619 (2025 avg)	+36% YoY	UP
SA ransomware victims total	105	104 (W16 end)	+1 this week	UP
New SA victims (W17)	2 (Sunspray + Ambulance Org)	1 (W16 Megasurf)	+1	UP
POPIA notifications Q1 2026	788 (IR disclosure 14 Apr)	202 (2021/22 full year)	+15x since 2021	UP
CISA KEV new entries W17	7	2 (W16)	+5	UP
Critical CVEs actively exploited	6	4 (W16)	+2	UP
Latest SA ransom demand	\$100K / R1.7M (XP95)	\$100K / R1.7M (W16)	Unchanged	FLAT
SA avg recovery cost (excl. ransom)	R24M (Sophos 2025)	R19M (2024 Sophos)	+26% YoY	UP

ANOMALY FLAG: SA faces simultaneous crises across four sectors in a single week: Government (XP95 deadline), Banking (Standard Bank 1.2TB release), Law Enforcement (Polmed/SAPS), and Payment Infrastructure (Adumo POS). This is an unprecedented convergence. The Cisco IOS-XE zero-day (CVE-2026-1834) adds fresh attack surface directly relevant to the confirmed Salt Typhoon SA telecom compromise.

TOP 3 ACTIONS THIS WEEK

- 1. ACTIVATE POPIA SECTION 22 RESPONSE PLANS (P1 — URGENT):** Standard Bank’s 1.2TB data is now public. Organisations holding Standard Bank-sourced client data face second-order notification obligations. Polmed’s ShinyHunters breach affects 100K+ police officers. Assess your exposure and prepare s.22 notifications immediately.
- 2. EMERGENCY PATCHING — CISCO IOS-XE + FORTINET EMS + MICROSOFT (P1):** CVE-2026-1834 (Cisco IOS-XE CVSS 9.8, actively exploited zero-day — Salt Typhoon relevance); CVE-2026-21643 (Fortinet EMS CVSS 9.1, CISA deadline 16 Apr PASSED); CVE-2026-32201 (SharePoint zero-day); CVE-2026-33824 (Windows IKE CVSS 9.8). Patch all immediately. Upgrade Cisco IOS XE to 17.12.4a or later.
- 3. KERBEROS RC4 AUDIT BEFORE JULY ENFORCEMENT (P1):** Microsoft Phase 2 enforcement began 14 April. RC4-dependent service accounts will fail. Run List-AccountKeys.ps1 and Get-KerbEncryptionUsage.ps1 scripts. Monitor Event Log IDs 201-209. Full enforcement with no rollback begins July 2026 — remediate now.

Critical Findings:

- Standard Bank — 1.2TB data publicly released by ROOTBOY on 14-17 April. ~154 million SQL rows claimed: client names, ID numbers, account numbers, BBBEE data, limited credit card numbers/expiry (no CVV). Africa's largest bank by assets. IR conducting parallel fact-finding.²
- XP95 20 April deadline arrives at the end of W17. Stats SA (154GB/453K files) and GCRA (147GB/429K files) both refused payment under PFMA. Data publication is near-certain within hours of deadline.³
- Polmed (SAPS medical scheme) — ShinyHunters extortion targeting 100,000+ police officers and their dependants. Criminal case filed under Cybercrimes Act. Direct physical safety risk: prior incident showed gang harassment following police officer data exposure.⁴
- Adumo (Lesaka Technologies, JSE-listed) — POS source code and chip-and-PIN certification artefacts for R80B+/year payment infrastructure offered for \$7,000 on dark web. If authentic, enables card-present fraud at scale across 29,000 merchants.⁵
- Cisco IOS-XE CVE-2026-1834 (CVSS 9.8) — actively exploited zero-day for 11 days before patch. 420,000+ exposed devices globally. Salt Typhoon directly relevant to SA telecom infrastructure.⁶
- Microsoft April Patch Tuesday: 167 CVEs (2nd largest ever), including CVE-2026-33824 (Windows IKE CVSS 9.8) and 2 zero-days. Kerberos RC4 Phase 2 enforcement now active.⁷
- SAP BW/BPC CVE-2026-27681 (CVSS 9.9) — SQL injection allowing low-privilege user to fully compromise database. CRITICAL for SA enterprise given SAP dominance.⁸

SECTOR SPOTLIGHT: FINANCIAL SERVICES — UNPRECEDENTED CONCURRENT ATTACKS

Financial services is the most at-risk sector this week. Standard Bank — Africa's largest bank by assets — had 1.2TB of client data publicly released by ROOTBOY, including ~154 million SQL rows with client names, ID numbers, account numbers, and limited credit card data. Simultaneously, Adumo (SA's largest independent payments processor, R80B+ annually) had POS source code and chip-and-PIN certification artefacts offered for sale on the dark web for \$7,000. The IR disclosed 788 breach notifications in Q1 2026 alone and is conducting parallel investigations. FSCA Joint Standard 2 creates dual regulatory exposure for all regulated financial institutions. The combination of a mega-breach at the country's largest bank and infrastructure-level payment processor targeting represents an unprecedented week for SA financial services cybersecurity.²⁵

1. ITWeb — SA Cyber Threat Intelligence W17 — <https://www.itweb.co.za>

2. ITWeb — Hackers publicly release Standard Bank data (17 Apr) — <https://www.itweb.co.za/article/hackers-publicly-release-data-stolen-from-standard-bank/KBpdg7pmKwmMLEew>

3. ITWeb — Stats SA confirms data breach — <https://www.itweb.co.za/article/stats-sa-confirms-data-breach-as-hackers-demand-r17m-ransom/JBwErnv3wpo76Db2>

4. ITWeb — SAPS medical aid scheme probes breach (17 Apr) — <https://www.itweb.co.za/article/saps-medical-aid-scheme-probes-potential-data-breach/P3gQ2MGA5VNvnRD1>

5. ITWeb — Adumo payment tech exposed (17 Apr) — <https://www.itweb.co.za/article/adumo-payment-tech-exposed-hackers-offer-data-for-7-000/KWEBb7yLwdAvmRjO>

6. SPOTO — Cisco IOS-XE CVE-2026-1834 Critical Advisory — <https://cciedump.spoto.net/news/cisco-warns-of-critical-ios-xe-vulnerability-actively-exploited-in-global-networking-infrastructure-attacks-april-2026.html>

7. BleepingComputer — Microsoft April 2026 Patch Tuesday (167 CVEs) — <https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2026-patch-tuesday-fixes-167-flaws-2-zero-days/>

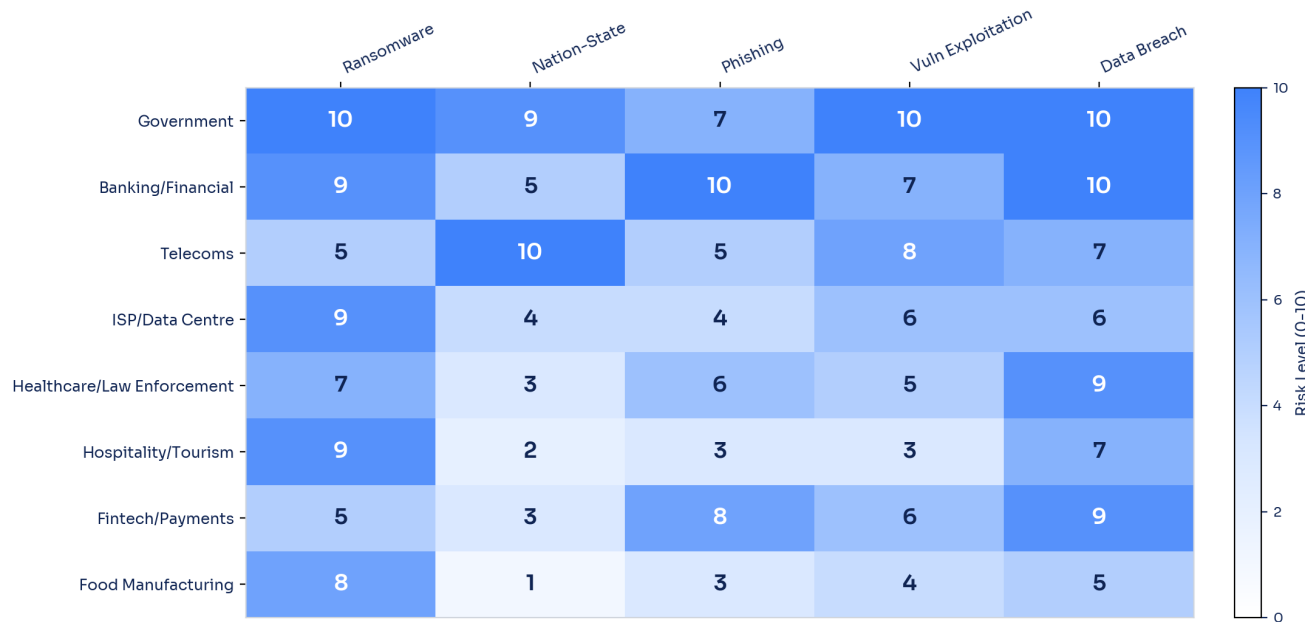
8. The Hacker News — SAP/Adobe/Fortinet Critical Patches April 2026 — <https://thehackernews.com/2026/04/april-patch-tuesday-fixes-critical.html>

2. THREAT LANDSCAPE HEATMAP

The heatmap below maps eight key South African sectors against five threat categories, rated 0-10 based on active threat intelligence, confirmed incidents, and vulnerability exposure during Week 17. Government remains at MAXIMUM across ransomware, vulnerability exploitation, and data breach — driven by the XP95 20 April deadline. Banking/Financial is at MAXIMUM for phishing (Standard Bank data enabling impersonation campaigns) and data breach (1.2TB public release). Telecoms is at MAXIMUM for

Nation-State/APT (Salt Typhoon + CVE-2026-1834). Healthcare/Law Enforcement scores 9 on data breach (Polmed/ShinyHunters). Fintech/Payments scores 9 on data breach (Adumo). Food Manufacturing enters the heatmap following the Sunspray Food (TheGentlemen) incident.

SA THREAT LANDSCAPE HEATMAP | W17 (13-19 Apr 2026)



Methodology: Risk levels are assessed using: (a) confirmed incidents in the reporting period, (b) active threat actor campaigns targeting the sector, (c) vulnerability exposure, and (d) regulatory scrutiny. **Critical (9-10)** = active exploitation or confirmed breach; **High (7-8)** = credible active threat; **Medium (4-6)** = elevated baseline risk; **Low (1-3)** = standard risk posture.

3. SA CYBER INCIDENTS & BREACHES

Week 17 adds two new confirmed SA ransomware victims (Sunspray Food and an unnamed ambulance/care organisation), escalates the Standard Bank / ROOTBOY situation to full data publication, introduces two significant new incidents (Polmed and Adumo), and brings the XP95 deadline to its conclusion. The SA cumulative ransomware victim count stands at **105** as of 19 April 2026. W17 is the most operationally complex week in SA cyber threat intelligence history.⁹

3.1 Standard Bank — ROOTBOY (W17 ESCALATED)

Organisation	Standard Bank of South Africa (standardbank.co.za) + Liberty Group (liberty.co.za)
Sector	Banking / Financial Services / Insurance
Threat Actor	ROOTBOY (dark web handle; identity unattributed)
Date	Intrusion: late February 2026 (~3 weeks inside network); data released publicly 14-17 April 2026
Data	~1.2TB exfiltrated; ~154M SQL rows claimed: client names, ID/registration numbers, contact details, account numbers, BBBEE categorisation, VAT numbers, limited credit card numbers/expiry dates (CVV not compromised). SharePoint, OneDrive, Power Apps, AppDynamics, Jira, Confluence, Citrix, Oracle/SQL databases claimed.
Demand	1 bitcoin (TechCentral) — Standard Bank declined to confirm/deny payment
Deadline	Data released without confirmed deadline expiry — published 14-17 April 2026
Payment	No confirmed payment. Credit cards being proactively replaced.
Status	DATA PUBLICLY RELEASED. Enhanced fraud monitoring. External cyber experts engaged. IR conducting parallel fact-finding.
SA Significance	Africa’s largest bank by assets. One of SA’s largest financial data releases on record. 154M SQL rows affect millions of clients. Second-order phishing/impersonation risk for all affected clients.
Sources	ITWeb (17 Apr), TechCentral (16 Apr), Standard Bank official update (14 Apr), The Citizen (13 Apr)

ROOTBOY claims to have spent approximately three weeks inside Standard Bank’s network from late February 2026, accessing SharePoint, OneDrive, Power Apps, Jira, Confluence, Citrix, and Oracle/SQL databases. The publicly released dataset includes client names, ID numbers, account numbers, BBBEE categorisation, and limited credit card numbers (CVV not compromised). Core transactional banking systems were not accessed and no funds were affected. Standard Bank confirmed regulatory notification, external cybersecurity expert engagement, and proactive credit card replacement for affected accounts. The Information Regulator confirmed a parallel fact-finding investigation examining access controls, authentication, encryption, network security, and logging. No formal enforcement notice had been issued as of 19 April. The Liberty Group breach (disclosed 24 March) is a related but legally separate incident involving different datasets through the same intrusion campaign.²¹⁰

3.2 XP95 / Statistics South Africa + GCRA — Deadline Day (W17 CRITICAL)

Organisation	Statistics South Africa (statssa.gov.za) + Gauteng City Region Academy (gcrabursary.gauteng.gov.za)
Sector	Government / National Statistics; Government / Education / Bursaries
Threat Actor	XP95 (pure data-extortion group; no encryption; first emerged March 2026; Windows 95-styled leak site on Tor)
Date	Exfiltration: late March 2026; deadline: 20 April 2026 (end of W17 window)
Data	Stats SA: 154 GB / 453,362 files — HR job-seeker portal (names, CVs, ID numbers, contact details). GCRA: 147 GB / 429,473 files — bursary/scholarship records (student PII, academic transcripts, ID documents). Gauteng Provincial: 3.8TB / 3.67M files.
Demand	\$100,000 USD (R1.7M) each — Stats SA; \$25,000 Gauteng Provincial
Deadline	20 April 2026 — TODAY (last day of W17 reporting window)
Payment	Refused — PFMA legally prohibits SA government entities from paying ransoms
Status	As at 19 April: no data published yet. 20 April = deadline day. Publication is near-certain.
SA Significance	882K+ citizens face identity theft risk. No precedent for SA government bulk data publication at this scale. XP95 precedent: Eholo Health Spain data released promptly after non-payment.
Sources	ITWeb, DataBreaches.net, UpGuard, Stats SA official statement, Breachsense, BlackFog

Stats SA confirmed non-payment under PFMA and filed a POPIA s.22 notification with the Information Regulator on 29 March. GCRA has not publicly confirmed non-payment but its silence is operationally equivalent. XP95’s operational precedent is unambiguous: Eholo Health (Spanish healthcare software provider) data was publicly released after the victim refused \$300,000. XP95 also expanded internationally this week, targeting Healthdaq (Dublin) on 13 April — demonstrating active operational tempo. The Information Regulator has not issued any advisory to the 882K+ potentially affected data subjects. Stats SA’s PFMA constraint makes payment legally impossible, but the downstream fraud, identity theft, and phishing risk to affected South Africans will persist for years post-publication.³¹¹

3.3 Polmed (SAPS Medical Scheme) — ShinyHunters (W17 NEW)

Organisation	Polmed — Medical Scheme for South African Police Service (SAPS) members and dependants
Sector	Healthcare / Medical Insurance / Law Enforcement (indirect)
Threat Actor	ShinyHunters (prolific international extortion group; responsible for McGraw Hill, Figure Finance, Rockstar Games, and ~400 Salesforce Experience Cloud breaches in 2026)
Date	Extortion email to Polmed: 25 March 2026; public disclosure: 16-17 April 2026
Data	Personal information of SAPS members (police officers) and their dependants. Forensic investigation ongoing — exact scope not confirmed. Healthcare records combine identity, financial, and medical information.
Demand	Extortion-type communication received; specific demand not publicly stated
Deadline	Not confirmed publicly
Payment	Unknown — investigation ongoing
Status	ACTIVE INVESTIGATION. Independent forensic specialists appointed. Criminal case at Brooklyn Police Station. POPIA s.22 filed with IR. All members notified.
SA Significance	CRITICAL — Police personnel data creates direct physical safety risk. Prior incident: 37-year-old SAPS anti-drug officer’s family faced 3+ years of gang harassment after data leak. Command structure exposure enables blackmail.
Sources	ITWeb (17 Apr), allAfrica (16 Apr), Apple Podcasts/Cyber Brief SA (19 Apr)

Polmed confirmed receipt of a ShinyHunters extortion communication on 25 March 2026 and publicly disclosed the incident on 16-17 April. SAPS Brigadier Athlenda Mathe confirmed police are investigating. A criminal case was opened at Brooklyn Police Station under the Cybercrimes Act. The significance extends beyond data privacy: SAPS medical records include officer deployment status, physical locations, and medical conditions — data that could enable targeted violence against officers by criminal networks. ShinyHunters is operating a parallel global campaign simultaneously targeting McGraw Hill via Salesforce Experience Cloud. SA law enforcement data is among the highest-value targets for organised crime.⁴¹²

3.4 Adumo (Lesaka Technologies) — POS Source Code on Dark Web (W17 NEW)

Organisation	Adumo (wholly-owned subsidiary of Lesaka Technologies, JSE-listed; adumo.com)
Sector	Fintech / Payment Processing
Threat Actor	Unattributed — listed on dailydarkweb.net
Date	Discovery: 17 April 2026
Data	15,546 files (~14GB): POS source code, debugging tools, low-level documentation, chip-and-PIN transaction details, Mastercard and Visa certification artefacts. Offered for \$7,000 (R114,920).
Demand	\$7,000 USD (sale price on dark web)
Deadline	For sale — no ransom deadline
Payment	N/A — data offered for commercial sale, not ransom
Status	UNDER INVESTIGATION. Adumo denies consumer data breach; states material routinely shared with partners. Investigation ongoing; authenticity unverified.
SA Significance	SA's largest independent payments processor (R80B+ annually, 29,000 merchants, SA/Namibia/Botswana/Kenya). Source code could enable card-present fraud at scale. Lesaka group processes R270B annually, serving 1.7M consumers.
Sources	ITWeb (17 Apr), LaunchBase Africa (17 Apr), MyBroadband (17 Apr)

Adumo issued a public statement on 17 April denying any consumer data breach and characterising the material as routinely shared with external partners. Independent expert assessment is more cautionary: "In a payments ecosystem, this type of information is extremely sensitive and typically tightly controlled. A buyer could mimic transactions and, combined with other stolen data, facilitate fraud at scale." The chip-and-PIN certification artefacts from Mastercard and Visa are particularly sensitive — these are used to certify POS terminals for transaction processing and could enable the creation of fraudulent certified devices. If authentic, this represents a systemic financial fraud enablement risk across Adumo's entire 29,000-merchant network.⁵¹³

3.5 Sunspray Food Ingredients — TheGentlemen (W17 NEW)

Organisation	Sunspray Food Ingredients (Sunspray Solutions Pty Ltd — sunspray.co.za)
Sector	Food Manufacturing / FMCG
Threat Actor	TheGentlemen (global RaaS — 182 victims in Q1 2026, 2nd most active globally)
Date	Attack estimated: 26 March 2026; discovery/listing: 19 April 2026
Data	Unknown volume — not disclosed on leak site
Demand	Unknown
Deadline	Unknown
Payment	Unknown — no Sunspray public statement
Status	Listed on TheGentlemen dark web leak site. No public statement from Sunspray.
SA Significance	105th SA ransomware victim. TheGentlemen has now targeted municipalities, automotive, logistics, and food manufacturing across SA. Broad sector indiscrimination.
Sources	Ransomware.live, Breachsense, HookPhish

Sunspray Food Ingredients is South Africa's largest independent manufacturer of spray-dried food ingredients, supplying caramel powders, fat powders, fruit/vegetable powders, and creamers. In 2023, Israeli company Turpaz Industries acquired a 55% controlling stake. The listing brings the SA cumulative

ransomware victim count to 105. TheGentlemen is the second-most active ransomware group globally in Q1 2026 per GuidePoint Security GRIT data (182 victims), having expanded from 35 victims in Q4 2025. Their SA targeting now spans municipalities (Witzenberg, Intsika Yethu, Elundini), automotive (Rola Motor Group), logistics (Paltrack), and now food manufacturing.¹⁴¹⁵

3.6 Unnamed SA Ambulance/Care Services — NightSpire (W17 NEW)

Organisation	Unnamed South African ambulance/emergency care services organisation (partially redacted as "S***s*a A**u***e C***s" on threat intelligence feeds)
Sector	Healthcare / Emergency Services
Threat Actor	NightSpire (double-extortion; 175 total victims; 74 in Q1 2026 alone)
Date	Attack estimated: 17 April 2026; discovery: 18 April 2026
Data	Unknown — investigation ongoing
Demand	Unknown (NightSpire demands typically \$150K-\$2M)
Deadline	Unknown
Payment	Unknown — no public statement
Status	Encryption confirmed. Ransom demand issued. No data released yet.
SA Significance	Emergency services are critical national infrastructure. NightSpire has prior confirmed SA victims: Eastern Cape DTHS (Nov 2025), Ingonyama Trust Board (Jun 2025), Semenya Furumele (Mar 2026).
Sources	TweetThreatNews (X), ransomware.live ZA map

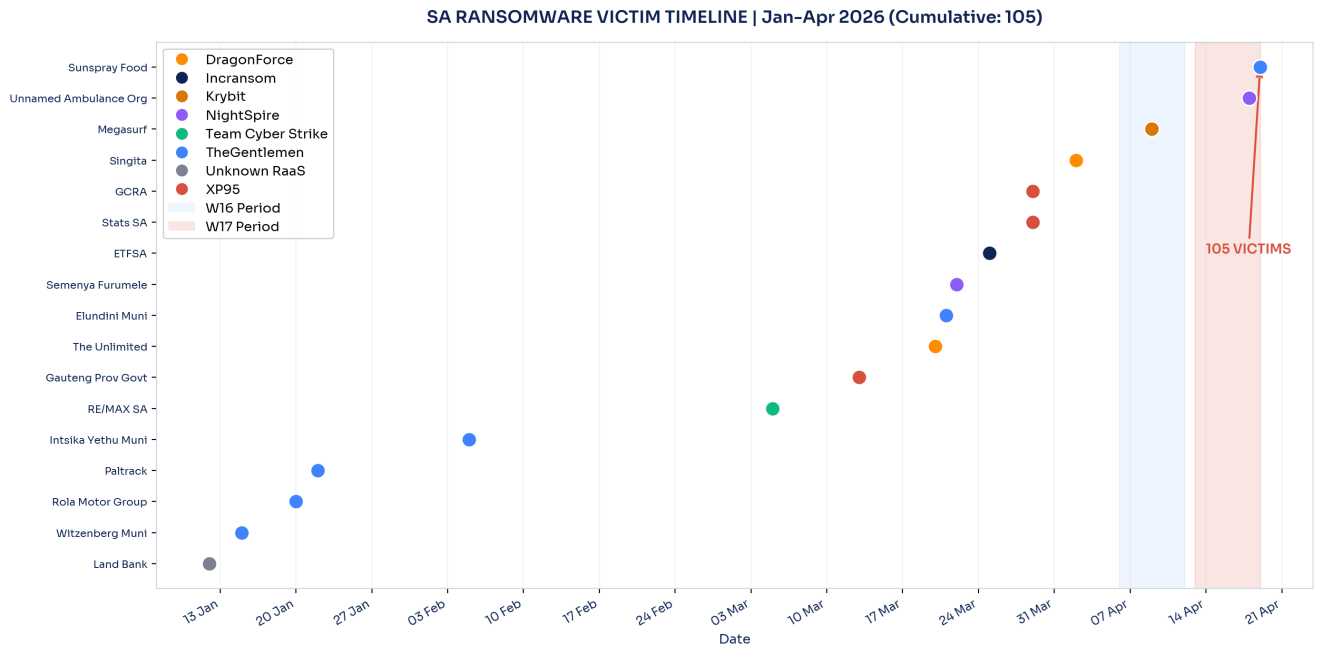
NightSpire emerged in early 2025 and shifted to full double-extortion (encryption plus exfiltration) in April 2025. The group has a documented pattern of South African targeting. An attack on an ambulance or emergency care services provider represents a direct risk to human life: encrypted patient records and dispatch systems can delay emergency response. NightSpire’s primary attack vector is CVE-2024-55591 (Fortinet authentication bypass). SA emergency services operators should verify this patch has been applied and conduct a compromise assessment.¹⁶

3.7 Carry-Over Incidents — W16 Status Updates

CARRY-OVER INCIDENT STATUS (W16 to W17)

- Megasurf / Krybit:** No confirmed data publication in W17. FalconFeeds noted a ~18-19 April implied deadline. Krybit was simultaneously involved in a criminal-on-criminal conflict with OAPT (see Section 7). Megasurf has issued no public statement.
- Singita / DragonForce:** No W17 updates. Singita continues to maintain public silence. 43GB luxury hospitality data (high-net-worth passport copies, payment details) remains held on DragonForce leak site.
- ETFSA / Incransom:** No new W17 developments. Threat remains live.
- Liberty Group / Standard Bank:** SEE SECTION 3.1 — ESCALATED to full data publication this week.

SA Ransomware Victim Timeline — Jan-Apr 2026



9. Ransomware.live — South Africa Victim Map — <https://www.ransomware.live/map/ZA>

10. TechCentral — Standard Bank breach fallout deepens (16 Apr) — <https://techcentral.co.za/standard-bank-data-breach-fallout-deepens/280322/>

11. DataBreaches.net — XP95 SA Government Victims — <https://databreaches.net/2026/03/30/south-african-government-agency-and-sp-anish-psychological-software-provider-victims-of-cyberattacks-by-xp95/>

12. allAfrica — Hackers attack police medical aid (16 Apr) — <https://allafrica.com/stories/202604160282.html>

13. LaunchBase Africa — Adumo source code leak (17 Apr) — <https://launchbaseafrica.com/2026/04/17/south-african-fintech-adumo-investigates-alleged-source-code-leak/>

14. HookPhish — TheGentlemen hits Sunspray Food — <https://www.hookphish.com/blog/ransomware-group-thegentlemen-hits-sunspray-food/>

15. Breachsense — Sunspray Food Breach — <https://www.breachsense.com/breaches/sunspray-food-data-breach/>

16. Ransomware.live / TweetThreatNews — NightSpire SA Ambulance Org — <https://www.ransomware.live/map/ZA>

4. NATION-STATE: SALT TYPHOON & CISCO IOS-XE ZERO-DAY

Salt Typhoon’s confirmed SA telecom compromise gains new urgency in W17: Cisco disclosed CVE-2026-1834 (CVSS 9.8, actively exploited zero-day) — a unauthenticated RCE in the IOS-XE Web UI. This represents fresh, unpatched attack surface on the exact infrastructure class Salt Typhoon previously compromised. Cisco’s Talos researchers assessed one cluster of CVE-2026-1834 exploitation with "moderate confidence" as state-sponsored.¹⁷¹⁸

Attribution	Salt Typhoon (China-nexus) — also tracked as Earth Estries / GhostEmperor / FamousSparrow / RedMike / UNC2286. Ministry of State Security (MSS), Chengdu.
SA Status	Confirmed: at least one unnamed SA telecommunications provider compromised (Recorded Future Insikt Group / TechCrunch March 2026). No SA government response.
W17 CVE	CVE-2026-1834 — Cisco IOS-XE Web UI RCE, CVSS 9.8, actively exploited zero-day for ~11 days before patch. Fresh attack surface on same infrastructure class.
Historical TTPs	CVE-2023-20198 (CVSS 10.0) + CVE-2023-20273 (CVSS 7.2) chained for privilege-15 account creation. GRE tunnel persistence. Custom malware: SNAPPYBEE, GHOSTSPIDER, MASOL RAT, ZINGDOOR, DEMODEX rootkit. JumbledPath for hop chains.
Global Scope	AT&T, Verizon, T-Mobile, CenturyLink (US), UK/EU telecoms, Mytel (Myanmar), Italy, Thailand, and confirmed SA. 80+ countries. FBI confirmed "still very much ongoing" Feb 2026.

SA Government Response	NO PUBLIC ADVISORY issued. No SSA/DCDT/ICASA guidance. Affected telecom identity not disclosed. Critical regulatory gap.
Detection	Cisco IOS XE Web UI Checker tool; audit privilege-15 accounts; check for unauthorised GRE tunnels; SNMP poll anomalies; run Salt Typhoon Talos detection playbook.
Sources	Recorded Future (Insikt Group), TechCrunch, Security Affairs, Trend Micro Earth Estries report, Cisco Talos, Censys

CVE-2026-1834 — Why This Matters for SA

CVE-2026-1834 is a unauthenticated RCE in the Cisco IOS-XE Web UI. It was exploited in the wild for approximately 11 days before the patch was published. SANS ISC honeypots detected scanning from 5 April 2026. Over 420,000 internet-facing IOS-XE devices are globally exposed. Salt Typhoon's confirmed method includes exploiting IOS-XE vulnerabilities to create privilege-15 accounts and establish GRE tunnel persistence for long-term data exfiltration. CVE-2026-1834 provides a new, unpatched entry point on infrastructure that Salt Typhoon has already demonstrated the capability and intent to compromise in SA. Any SA telecom, ISP, or enterprise running IOS-XE with an internet-facing web management interface must treat this as a PO emergency patch.⁶¹⁷

Recommended Detection Actions

- Patch Cisco IOS XE to 17.12.4a, 17.9.6, or 17.6.8 or later immediately. Run Cisco's free IOS XE Web UI Checker tool.
- Disable web UI if immediate patching is not possible: "no ip http server" + "no ip http secure-server"
- Audit all privilege-level-15 local accounts on IOS-XE devices — any undocumented priv-15 account is a PI incident
- Execute "show ip tunnel" on all edge routers and look for undocumented GRE tunnel entries
- Compare running-config to known-good baseline; any delta not matching change management records is suspicious
- Review SNMP poll logs: Salt Typhoon uses SNMP from unexpected external IPs to enumerate network topology
- Check for SNAPPYBEE / GHOSTSPIDER indicators on network infrastructure and adjacent Linux servers
- Restrict web UI access to dedicated management VLANs / out-of-band networks immediately

17. Recorded Future — RedMike/Salt Typhoon SA Telecom Confirmed —

<https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices>

18. TechCrunch — Salt Typhoon SA Telecom Confirmed (9 Mar 2026) —

<https://techcrunch.com/2026/03/09/salt-typhoon-china-who-has-been-hacked-global-telecom-giants/>

19. Security Affairs — Salt Typhoon IOS-XE SA — <https://securityaffairs.com/174226/apt/salt-typhoon-exploited-cisco-ios-xe-flaws.html>

20. Cisco Talos — CVE-2026-1834 Advisory — <https://cciedump.spoto.net/news/cisco-warns-of-critical-ios-xe-vulnerability-actively-exploited-in-global-networking-infrastructure-attacks-april-2026.html>

5. ACTIVE THREAT CAMPAIGNS

5.1 Banking Fraud Surge Post-Standard Bank Data Release

The public release of Standard Bank's client data on 14–17 April creates an immediate, large-scale phishing and impersonation risk. The dataset includes client names, ID numbers, account numbers, and contact details — a complete profile for targeted social engineering. SABRIC 2024 data confirms the baseline: digital banking fraud surged 86% to ~98,000 incidents (R1.888B losses); banking app fraud represents 65% of all digital fraud (R1.2B+ losses); card-not-present fraud accounts for 85.6% of card fraud (R1.466B losses). Standard Bank issued client helplines: 0860 123 000 (personal/private banking) and 0860 109 075 (business banking). All Standard Bank clients should be treated as high-risk for targeted phishing attempts in the coming weeks.²¹²²

5.2 Contagious Interview — Expanded to 5 Package Ecosystems

The North Korean Contagious Interview campaign has expanded beyond npm and PyPI to include **Go, Rust, and PHP** package ecosystems. Over 1,700 malicious packages have been published since January 2025. The campaign delivers BeaverTail and InvisibleFerret info-stealers via fake interview tasks, and a modular Node.js backdoor (OtterCookie). A new VSCode attack vector executes malicious repository code on folder-open via runOn: folderOpen tasks. SA developers in AI, data science, fintech, and software outsourcing are at direct risk. Hardcoded MongoDB credentials in C2 infrastructure reveal 26 "tenant_*" databases suggesting possible SaaS victims.²³²⁴

5.3 Krybit vs OAPT Criminal Conflict

On 13 April, criminal threat actor OAPT published what it claims is the complete Krybit ransomware administration panel database, including victim records, operator credentials, five cryptocurrency wallet addresses, and confirmation of **zero paid ransoms**. This is the first substantive operation confirming OAPT has real technical capability. Krybit retaliated by listing "Hacked OAPT" as a victim on 14 April — assessed by Yazoul Security as likely fabricated. Krybit added 6 new global victims in W17 (none SA), bringing their total to 18. The Megasurf (SA) data publication deadline (~18–19 April) passed without confirmed data release.²⁵

21. SABRIC — Annual Crime Statistics Report 2024 —

<https://www.sabric.co.za/wp-content/uploads/2025/09/CRIME-STATISTICS-REPORT-2024.pdf>

22. Youverify — SA Banking Fraud Prevention 2026 — <https://youverify.co/blog/financial-fraud-prevention-south-african-banks>

23. The Hacker News — DPRK Contagious Interview 1,700 Packages (8 Apr) —

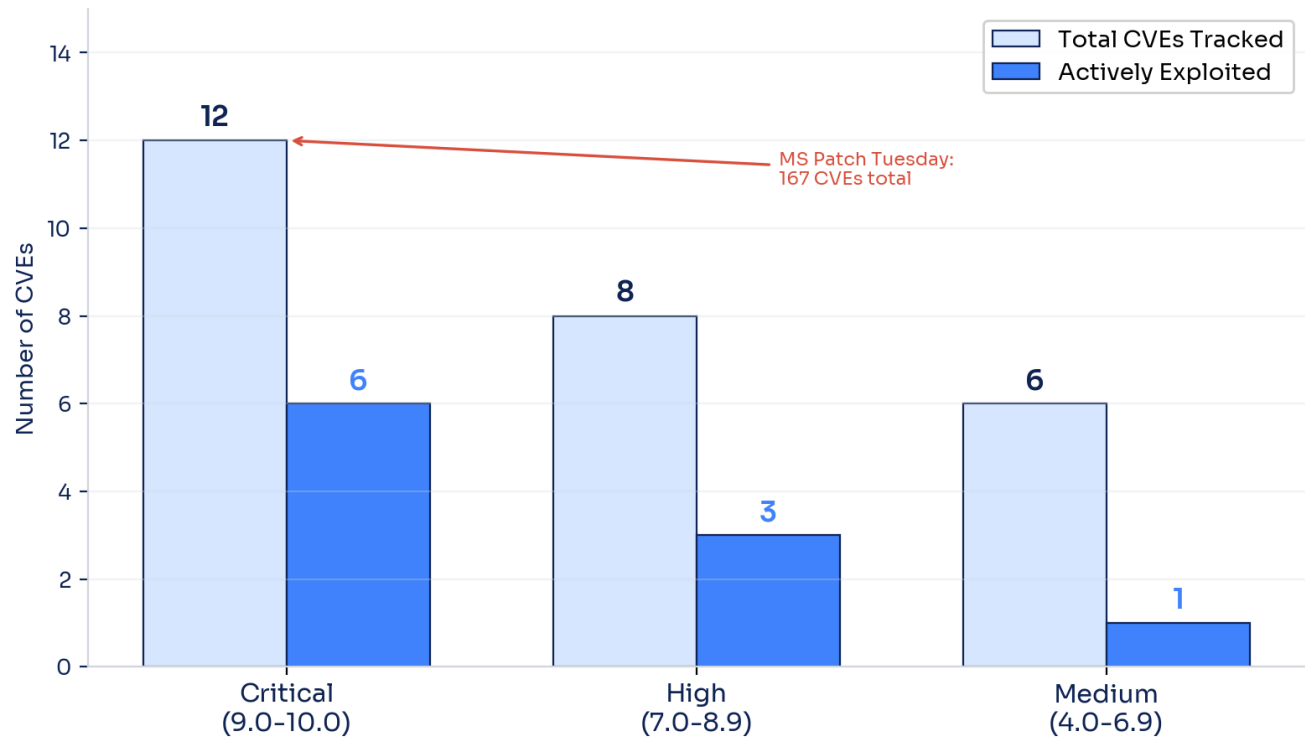
<https://thehackernews.com/2026/04/n-korean-hackers-spread-1700-malicious.html>

24. Microsoft Security Blog — Contagious Interview Enterprise Intrusions — <https://www.microsoft.com/en-us/security/blog/2026/03/11/contagious-interview-malware-delivered-through-fake-developer-job-interviews/>

25. The Register — OAPT Krybit Panel Breach (14 Apr) — https://www.theregister.com/2026/04/14/Oapt_krybit_spat/

6. CRITICAL VULNERABILITIES

CVE SEVERITY DISTRIBUTION | W17 Priority Vulns & CISA KEV



Week 17 is one of the most active patch weeks of 2026. Microsoft Patch Tuesday addressed **167 CVEs** — the second-largest in history. CISA added **7 new KEV entries** on 13-14 April spanning Fortinet, Adobe, and legacy Microsoft products. Cisco disclosed CVE-2026-1834 (CVSS 9.8, actively exploited). SAP patched a CVSS 9.9 SQL injection. The SA SSA CSIRT published a Fortinet advisory (8 April) and a Cisco advisory (2 April) directly relevant to SA enterprises.⁷²⁶

CISA KEV Additions — W17

CVE ID	Product	CVSS	Date Added (KEV)	Federal Due Date	SA Relevance
CVE-2026-21643	Fortinet FortiClient EMS	9.1	13-14 Apr 2026	16 Apr (PASSED)	CRITICAL — SA mid-market dominant
CVE-2026-34621	Adobe Acrobat Reader/DC	8.6	13 Apr 2026	27 Apr 2026	HIGH — ubiquitous in SA legal/govt
CVE-2023-21529	Microsoft Exchange Server	8.8	13-14 Apr 2026	27 Apr 2026	HIGH — dominant SA enterprise email
CVE-2025-60710	Windows Host Process Tasks	7.8	13-14 Apr 2026	27 Apr 2026	MEDIUM — all Windows environments
CVE-2023-36424	Windows CLFS Driver	7.8	13-14 Apr 2026	27 Apr 2026	MEDIUM — local privilege escalation
CVE-2012-1854	Microsoft VBA (legacy)	7.8	13-14 Apr 2026	27 Apr 2026	MEDIUM — SA govt legacy systems
CVE-2020-9715	Adobe Acrobat Reader	7.8	13-14 Apr 2026	27 Apr 2026	MEDIUM — legacy Acrobat

BREAKING CHANGE — Kerberos RC4 Phase 2 (14 April): Microsoft Phase 2 enforcement began 14 April. Domain controllers now default to AES-SHA1-only tickets. RC4-dependent service accounts will begin failing. Monitor Event Log IDs 201-209. Run List-AccountKeys.ps1 and Get-KerbEncryptionUsage.ps1. Mixed Windows/Linux/NFS environments in SA mining and finance are at highest risk. Full enforcement (no rollback) begins July 2026.

Priority Vulnerability Matrix — W17

CVE ID	Vendor/Product	CVSS	Exploited?	SA Relevance
CVE-2026-1834	Cisco IOS-XE Web UI	9.8	YES (zero-day, 11d)	CRITICAL — Salt Typhoon; 420K+ devices
CVE-2026-20147/80/86	Cisco ISE	9.9	Not yet confirmed	CRITICAL — dominant SA NAC platform
CVE-2026-27681	SAP BW/BPC	9.9	Not confirmed	CRITICAL — dominant SA ERP/finance
CVE-2026-20184	Cisco Webex SSO	9.8	Not confirmed	HIGH — action required: upload new SAML cert
CVE-2026-33824	Windows IKE Service	9.8	Not exploited	HIGH — all Windows Server environments
CVE-2026-21643	Fortinet FortiClient EMS	9.1	YES (KEV 16 Apr)	CRITICAL — companion to W16 zero-day; patch 7.4.7
CVE-2026-34621	Adobe Acrobat Reader	8.6	YES (since Nov 2025)	HIGH — open PDF = exploitation
CVE-2026-32201	Microsoft SharePoint	6.5	YES (zero-day)	HIGH — treat as critical despite CVSS

Top Priority CVE Details

CVE-2026-1834 — Cisco IOS-XE Web UI — CVSS 9.8 — PO EMERGENCY

Unauthenticated RCE in the Cisco IOS-XE Web UI. Exploited as a zero-day for approximately 11 days before patch publication on 8 April 2026. SANS ISC honeypots detected scanning from 5 April. 420,000+ internet-facing IOS-XE devices globally. Affected platforms include ASR 1000, ISR 4000, Catalyst 9000/3850, Nexus 9000, and Cisco 9800 WLC. Patch to IOS XE 17.12.4a, 17.9.6, or 17.6.8. Direct Salt Typhoon relevance. IOC: anomalous HTTP POST to management URIs; unauthorised privilege-level-15 user accounts.²⁰

CVE-2026-20147 / CVE-2026-20180 / CVE-2026-20186 — Cisco ISE — CVSS 9.9 — P1 CRITICAL

Three separate OS command injection vulnerabilities in Cisco Identity Services Engine (ISE), all rated CVSS 9.9. CVE-2026-20180 and CVE-2026-20186 are exploitable with read-only admin credentials — the lowest possible access level. Full root privilege escalation confirmed. No workarounds available — patching is the only mitigation. Cisco ISE is the dominant NAC/policy platform in SA banks, telcos, and government networks. Patch to ISE 3.1 Patch 11 / 3.2 Patch 10 / 3.3 Patch 11 / 3.4 Patch 6 / 3.5 Patch 3.²⁷

CVE-2026-27681 — SAP BW/BPC — CVSS 9.9 — P1 CRITICAL

SQL injection in the ABAP upload functionality of SAP Business Warehouse and Business Planning and Consolidation. A low-privileged SAP BW/BPC user can upload a file containing arbitrary SQL that is executed against the data store — enabling full database compromise, data exfiltration, or destruction. SAP BW/BPC is the dominant enterprise reporting and financial consolidation platform for large SA companies in mining, banking, retail, and government SOEs. Apply SAP Security Note #3719353 immediately. Interim workaround: revoke S_GUI authorization Activity 60 (Upload).⁸

CVE-2026-34621 — Adobe Acrobat Reader — CVSS 8.6 — P1 CRITICAL (Zero-Day since Nov 2025)

Prototype pollution zero-day in Adobe Acrobat Reader. Exploited since at least November 2025 before disclosure. Opening a malicious PDF triggers embedded JavaScript that steals local files via util.readFileIntoStream() and exfiltrates via RSS.addFeed(). No special privileges required — opening the document is sufficient. PDF workflows are universal in SA legal, financial, and government sectors. Update to Acrobat/Reader DC 26.001.21411 immediately.²⁸

CVE-2026-33824 — Windows IKE Extensions — CVSS 9.8 — P1 CRITICAL

Unauthenticated RCE via crafted IKEv2 packets to any Windows machine with IKEv2 enabled. No user interaction required. All Windows Server versions affected. The highest-rated vulnerability in the April 2026 Patch Tuesday. Apply April 2026 Patch Tuesday immediately, prioritising all Windows Servers.⁷

CVE-2026-20184 — Cisco Webex SSO Certificate Bypass — CVSS 9.8 — P2

Improper certificate validation in Cisco Webex SSO integration enables an unauthenticated remote attacker to impersonate any Webex user. Cloud-side fix already deployed by Cisco, but **customers using SSO must manually upload a new IdP SAML certificate to Control Hub** — without this customer action, the fix is not applied. Widely used in SA enterprise and government post-COVID. Requires customer action today.²⁹

26. The CyberSignal — CISA 7 KEV Entries W17 —

<https://www.thecybersignal.com/cisa-expands-kev-catalog-with-seven-actively-exploited-flaws-across-microsoft-adobe-and-fortinet/>

27. The Hacker News — Cisco ISE/Webex Critical Patches (Apr 2026) —

<https://thehackernews.com/2026/04/cisco-patches-four-critical-identity.html>

28. The Hacker News — Adobe CVE-2026-34621 Zero-Day — <https://thehackernews.com/2026/04/adobe-patches-actively-exploited.html>

29. BleepingComputer — Cisco Webex Requires Customer Action —

<https://www.bleepingcomputer.com/news/security/cisco-says-critical-webex-services-flaw-requires-customer-action/>

30. Microsoft TechCommunity — Kerberos RC4 Phase 2 (16 Apr) — <https://techcommunity.microsoft.com/discussions/windowsserver/phase-2-of-kerberos-rc4-hardening-begins-with-the-april-2026-windows-security-up/4511702>

7. THREAT ACTOR PROFILES & RANSOMWARE ACTIVITY

SA Ransomware Victim Count: 105 as of end W17 (up from 104 at end W16). Net new W17: Sunspray Food (TheGentlemen, +1 confirmed) and unnamed SA ambulance organisation (NightSpire). Standard Bank (ROOTBOY) and Polmed (ShinyHunters) are data extortion incidents not tracked in the ransomware.live count. Adding XP95's three SA government victims would bring the effective total to 108.⁹

Active SA-Relevant Threat Actor Summary — W17

Actor	Type	SA Victims/Status	W17 Activity	Primary TTPs
ROOTBOY	Data Extortion	Standard Bank 1.2TB released	ESCALATED — data publicly released 14-17 Apr	Network intrusion; database exfiltration; dark web release
XP95	Data Extortion	Stats SA, GCRA, Gauteng Prov Govt	CRITICAL — deadline TODAY (20 Apr)	Tor DLS; BreachForums; pure extortion; no encryption
ShinyHunters	Data Extortion	Polmed (NEW)	ACTIVE — 100K+ SAPS officers targeted	Global prolific group; extortion email; parallel campaigns
TheGentlemen	RaaS	Sunspray Food (NEW) + 5 prior SA	2nd most active globally Q1 2026	Broad sectoral targeting; municipalities to food manufacturing
NightSpire	RaaS (double extortion)	Unnamed ambulance org (NEW)	ACTIVE — encryption confirmed	CVE-2024-55591 (FortiOS); \$150K-\$2M demands
Salt Typhoon	Nation-State (China)	Unnamed SA telecom confirmed	CVE-2026-1834 new attack surface	IOS-XE exploit; GRE tunnels; passive interception; SNAPPYBEE
DragonForce	RaaS	Singita (carry-over)	No new SA victims W17	Double extortion; 80% affiliate payout; 431+ global victims
Krybit	RaaS	Megasurf (W16)	OAPT exposed admin panel; zero paid ransoms	ISP/DC targeting; double extortion; criminal conflict with OAPT

ROOTBOY — MOST SIGNIFICANT SA INCIDENT W17

ROOTBOY publicly released 1.2TB of Standard Bank client data on 14-17 April. ROOTBOY claims ~3 weeks of undetected access inside Standard Bank’s network from late February, accessing SharePoint, OneDrive, Jira, Confluence, Citrix, and Oracle/SQL databases. The ~154 million SQL row claim — if authentic — constitutes one of the largest single financial data releases in SA history. ROOTBOY is an unattributed individual or small group, not a known organised ransomware operation. The 1 bitcoin ransom demand was declined. Data has been publicly released and is now in circulation on dark web forums.²¹⁰

XP95 — CRITICAL: DEADLINE TODAY

XP95’s 20 April deadline for Stats SA and GCRA data arrives at the end of the W17 reporting window. Pure data-extortion model: no encryption, Telegram-only C2, data auctioned on Tor and BreachForums. This week XP95 also demonstrated geographic expansion by targeting Healthdaq (Dublin/Northern Ireland) on 13 April — an Irish healthcare recruitment platform used by all five Northern Ireland HSC Trusts. The Healthdaq breach (500K+ healthcare worker files including passports, background checks, vaccine records) confirms XP95’s operational tempo. Operational precedent from Eholo Health (Spain) confirms data release after non-payment.³³¹

ShinyHunters — POLMED/SAPS HIGH PRIORITY

ShinyHunters is a prolific international extortion group responsible for breaches at McGraw Hill, Figure Finance, Rockstar Games, and approximately 400 Salesforce Experience Cloud instances in early 2026. The Polmed extortion email was sent on 25 March — same week as SA bank breaches, suggesting coordinated or opportunistic multi-target campaign against SA. The SAPS data is among the highest-value targets for SA organised crime: police officer identities, command structures, and medical conditions could facilitate targeted violence, extortion, or undermining of law enforcement operations.⁴¹²

TheGentlemen — EXPANDING SA SECTOR COVERAGE

TheGentlemen emerged in August 2025 and became the second-most active ransomware group globally in Q1 2026 (182 victims per GuidePoint Security GRIT). Their SA targeting now spans municipalities (Witzenberg, Intsika Yethu, Elundini), automotive (Rola Motor Group), logistics (Paltrack), and now food manufacturing (Sunspray Food). This broad sectoral indiscrimination suggests automated scanning and opportunistic targeting rather than sector-specific focus. SA organisations across all sectors should include TheGentlemen in their threat model.¹⁴³²

NightSpire — EMERGENCY SERVICES TARGETING

NightSpire’s 18 April claim against an unnamed SA ambulance/care organisation extends their SA targeting to emergency services — critical national infrastructure. NightSpire shifted to full double-extortion in April 2025 and claimed 74 victims in Q1 2026 alone. Their confirmed SA victim list now includes Eastern Cape DTHS (Nov 2025), Ingonyama Trust Board (Jun 2025), Semenya Furumele (Mar 2026), and this unnamed ambulance organisation. Primary attack vector is CVE-2024-55591 (Fortinet FortiOS authentication bypass). Emergency services operators must verify this patch and conduct compromise assessments.¹⁶³³

Nation-State / APT Activity — W17

Actor	SA Status	W17 TTPs	Notes
Salt Typhoon (China-nexus)	CONFIRMED SA TELECOM	CVE-2026-1834 adds fresh IOS-XE attack surface this week; GRE tunnel persistence	See Section 4; FBI confirms "still very much ongoing"
APT41 (China-nexus)	ACTIVE in southern Africa	SA govt IT provider targeting confirmed Jul 2025	Credentials, source code, communications targeted
Sharp Dragon (China-nexus)	EXPANDING to Africa	RoyalRoad-lured phishing; Cobalt Strike; GoAnywhere CVE	No confirmed SA victims yet; monitoring warranted

31. Silicon Republic — XP95 Targets Healthdaq Dublin (13 Apr) — <https://www.siliconrepublic.com/enterprise/new-xp95-hacker-group-targets-dublin-recruitment-platform-healthdaq>

32. Industrial Cyber — GuidePoint GRIT Q1 2026 Ransomware Report — <https://industrialcyber.co/reports/ransomware-reaches-elevated-new-normal-as-attack-volumes-hold-steady-into-2026-reshape-baseline-risk-expectations/>
33. Xcitiium ThreatLabs — NightSpire Ransomware Profile — <https://threatlabsnews.xcitiium.com/blog/nightspire-ransomware-emerging-double-extortion-threat/>

8. OSINT EXPOSURE & ATTACK SURFACE

Standard Bank Client Data in Circulation

1.2TB of Standard Bank client data is now publicly available on dark web forums. Names, ID numbers, account numbers, and contact details are available to any threat actor. All Standard Bank clients are now at elevated risk for targeted phishing, impersonation, SIM-swap attacks, and identity fraud. Security teams at all organisations that share client data with Standard Bank or accept Standard Bank-issued documents for verification should assess their exposure.²

Cisco IOS-XE Global Exposure — 420,000+ Devices

Over 420,000 internet-facing Cisco IOS-XE devices are globally exposed to CVE-2026-1834. Censys tracking confirms SA telecom and enterprise WAN infrastructure is in scope. Salt Typhoon has already demonstrated operational capability against SA IOS-XE infrastructure. Any SA organisation with internet-facing IOS-XE should treat this as a breach-in-progress until patched and verified.²⁰

SAP BW/BPC Low-Privilege Exploitation Risk

CVE-2026-27681 (CVSS 9.9) means any SAP BW/BPC user — including low-privilege read-only analysts — is now a potential attacker with the ability to fully compromise SAP databases. SA enterprises using SAP BW/BPC for financial consolidation should treat this as a highest-priority patch and immediately revoke S_GUI Activity 60 (Upload) as an interim mitigation.⁸

Adumo POS Source Code — Supply Chain Fraud Risk

If the Adumo source code and chip-and-PIN certification artefacts are authentic, any buyer gains the technical knowledge to create counterfeit-certified POS terminals compatible with Adumo's Mastercard and Visa certifications. Organisations in Adumo's 29,000-merchant network should monitor for anomalous card-present transaction patterns and review their payment terminal firmware integrity.⁵

Contagious Interview Package Ecosystem Expansion

1,700+ malicious packages now span npm, PyPI, Go, Rust, and PHP. A new VSCode attack vector executes on folder-open. Port 1244/tcp is a confirmed IoC for C2 communication. SA developers should block port 1244/tcp, audit all packages from unknown authors installed since January 2025, and enforce VSCode task policies. SA fintech and crypto sector developers (Luno, VALR, JSE fintechs) are high-value targets.²³

Polmed SAPS Officer Data — Physical Safety Risk

100,000+ police officer identities, medical conditions, and deployment information are now in ShinyHunters' possession. If this data is published, SA criminal networks will immediately exploit it. Law enforcement agencies should immediately activate enhanced personnel security protocols, brief affected officers, and monitor for targeted harassment or intimidation of SAPS members.⁴

9. REGULATORY & COMPLIANCE

Information Regulator — W17 Escalations

788 Q1 2026 Breach Notifications (14 April disclosure): The Information Regulator exclusively disclosed to ITWeb on 14 April that it received 788 data breach notifications from South African organisations in Q1 2026 (January-March). IR spokesperson Nomzamo Zondi stated that information supplied by organisations "is not enough for thorough investigations," and the IR is sending information notices to obtain further details. At approximately 263 notifications/month, this reflects a 15-fold increase from 202 in the full year 2021/22. The IR currently has 1,320 open matters and only 14% of CIPC-registered companies have registered information officers.³⁴

Standard Bank / Liberty Group Parallel Investigation: IR confirmed on 13 April it is conducting parallel fact-finding examining access controls, authentication, encryption, network security, firewall/IDS, and monitoring/logging. No formal investigation or enforcement notice had been issued as of 19 April. Adv Tshepo Boikanyo confirmed: "We are also conducting our own fact finding over the view of to determine whether we are going to go the route of a formal investigation." The Standard Bank and Liberty breach simultaneously triggers FSCA/PA Joint Standard 2 obligations (24-hour material incident reporting, effective June 2025).²³⁵

Polmed (SAPS Medical Scheme) s.22 Filed: Polmed notified the Information Regulator under POPIA s.22 on 17 April following the ShinyHunters extortion. Criminal case opened at Brooklyn Police Station under the Cybercrimes Act. This is the correct procedural response — a positive contrast to GCRA’s continued silence.⁴

POPIA Enforcement Posture

The IR’s acknowledged capacity constraints (1,320 open matters, 86% IO non-compliance rate) mean enforcement against Standard Bank/Liberty is unlikely to materialise before Q3 2026. Draft POPIA amendments proposing direct fines and removal of the remediation window are in preparation but require parliamentary passage. The maximum POPIA administrative fine remains R10M (~EUR 520,000) — the IR has flagged this as an inadequate deterrent compared to GDPR’s EUR 20M ceiling. New health data processing regulations effective 6 March 2026 directly apply to the Polmed breach.³⁴³⁶

Regulatory Compliance Table — W17

Organisation	Incident	IR/Regulatory Action	Status (W17)
Standard Bank / Liberty	1.2TB release; ROOTBOY	Parallel fact-finding; info notice sent	ACTIVE — no formal enforcement yet
Polmed / SAPS	ShinyHunters extortion; 100K+ officers	POPIA s.22 filed 17 Apr; criminal case	ACTIVE INVESTIGATION
Stats SA	XP95 extortion (154GB)	s.22 filed 29 Mar; no IR advisory to subjects	CRITICAL — deadline today
GCRA	XP95 extortion (147GB)	No s.22 confirmed; no IR action	CRITICAL — regulatory gap
Land Bank	RaaS attack Jan 2026	s.22 filed; remediation monitored	Remediation ongoing (target Sep 2026)
SABS	Ransomware Nov 2024	AG audit; DA calls for urgency	Still recovering — 15+ months

Cybercrimes Act — Enforcement Gap

The Inclusive Society Institute’s April 2026 Occasional Paper confirmed: despite 100,000+ banking-related cyberattacks in 2024, SAPS recorded only 544 formal cybercrime cases — an 86% under-reporting/enforcement gap. The Polmed criminal case filing is a positive development. SA loses approximately R2.2 billion annually to cyberattacks with limited criminal accountability.³⁷

International Regulatory — EU NIS2 Belgium Deadline Passed

Belgium became the first EU member state to reach a hard NIS2 conformity assessment deadline on **18 April 2026**. The broader EU NIS2 first compliance audit deadline for most member states is **30 June 2026**. SA subsidiaries of EU-headquartered companies in covered sectors (energy, banking, health, digital infrastructure, food, manufacturing) face Group-level compliance obligations. Board members face personal liability for systematic NIS2 failures. Fines: up to EUR 10M or 2% global annual turnover for essential entities.³⁸

Upcoming Regulatory Deadlines

Deadline	Obligation	Body
20 April 2026 (TODAY)	XP95 data publication deadline — Stats SA + GCRA	XP95 / IR / Stats SA / GCRA
24-hour rolling	FSCA/PA Joint Standard 2: material incident reporting	FSCA / Prudential Authority
ASAP	POPIA s.22 breach notifications (Standard Bank, Polmed, Adumo)	Information Regulator
27 April 2026	CISA KEV deadline: Adobe Acrobat, MS Exchange, Windows CLFS, VBA	CISA / Internal
30 June 2026	EU NIS2 first compliance audit (most EU states)	EU National Authorities
30 June 2026	PAIA annual report submission	Information Regulator
July 2026	Kerberos RC4 Phase 3 enforcement — no rollback option	Microsoft / Internal DC teams
H1 2026	FATF Mutual Evaluation on-site assessment (SA)	FATF / ESAAMLG
September 2026	Land Bank remediation plan target	Land Bank / IR

34. ITWeb — InfoReg raises alarm, 788 Q1 2026 breach notifications (14 Apr) — <https://www.itweb.co.za/article/info-reg-raises-alarm-as-data-breaches-hit-788-in-q1/Pero3MZ3wzoqQb6m>

35. Channel Africa — IR still assessing Standard Bank/Liberty (13 Apr) — <https://www.channelafrica.co.za/channelafrica/news/sa-regulator-still-assessing-standard-bank-liberty-data-breach/>

36. Mayet Law — POPIA enforcement 2026 key developments — <https://mayet.law/popia-enforcement-in-south-africa-key-2026-developments-and-what-businesses-must-do-now/>

37. Inclusive Society Institute — Securing SA Cybersecurity Blueprint (Apr 2026) — <https://www.inclusivesociety.org.za/post/securing-the-future-blueprint-for-solving-south-africa-s-cybersecurity-crisis-in-the-age-of-ai>

38. D3 Security — NIS2 SOC Audit Readiness 2026 (18 Apr) — <https://d3security.com/blog/nis2-soc-audit-readiness-2026/>

10. WEEKLY THREAT HUNT & IOCs

Six hunt missions are active for W17. Three P1 missions address near-certain data publication, the largest SA banking data release, and an actively exploited nation-state zero-day. Three P2 missions address law enforcement data exploitation, payment infrastructure threats, and supply chain attacks.

P1 — CRITICAL: Deadline today; publication near-certain

TH-2026-W17-01 — XP95 Post-Deadline Data Monitoring

Hypothesis: XP95 will publish Stats SA (154GB/453K files), GCRA (147GB/429K student records), and potentially Gauteng Provincial (3.8TB) data on or after 20 April 2026. Bulk SA government PII will appear on Tor-hosted leak sites, BreachForums, and Telegram channels.

MITRE ATT&CK: T1657 (Financial Extortion), T1491.002 (Defacement/Leak Site), T1048 (Exfiltration Over Alt Protocol), T1567 (Exfiltration to Cloud Storage/Telegram)

IOCs: XP95 Tor DLS (Windows 95-styled UI); BreachForums profile "xp95" (created March 2026); Telegram groups distributing SA government PII; bulk CSV/ZIP files with .gov.za domain data appearing on paste sites; ID number patterns in format YYMMDDGGGSAZ

Data Sources: Tor Browser monitoring of XP95 DLS; BreachForums monitoring; Telegram channel monitoring; external threat intelligence feeds (Breachsense, ransomware.live); OSINT monitoring for .gov.za email lists on paste sites

Detection Guidance: Monitor for bulk statssa.gov.za / gcra.gov.za email addresses appearing on BreachForums, Telegram, or paste sites. Alert on XP95 Tor DLS update notifications. If data is published, immediately assess whether your organisation collected Stats SA job applicant data or GCRA student data to determine s.22 obligations.

P1 — CRITICAL: 1.2TB data publicly released; immediate fraud risk

TH-2026-W17-02 — ROOTBOY Standard Bank Credential Exploitation

Hypothesis: ROOTBOY's publicly released Standard Bank dataset (154M SQL rows: names, ID numbers, account numbers) is now available to any threat actor. Credential stuffing, targeted phishing, and SIM-swap attacks targeting Standard Bank clients will begin immediately.

MITRE ATT&CK: T1078.001 (Default Accounts / Credential Stuffing), T1566.001 (Spearphishing Attachment), T1539 (Steal Web Session Cookie), T1185 (Man-in-the-Browser)

IOCs: Surge in Standard Bank client phishing domains (standardbank-security[.]co.za, stanbicsecurity[.]com etc.); login attempts from new IPs on Standard Bank customer accounts; SIM swap requests for Standard Bank-registered numbers; credential stuffing against banking portals using leaked ID+account combinations. IOC domains: [DO NOT CLICK — monitor only]

Data Sources: Standard Bank fraud monitoring feeds; phishing domain registration alerts (domain typosquatting on "standardbank", "stanbic", "liberty"); SIEM alerts on high-volume failed login attempts; SIM swap notification systems; bank helpline call volume monitoring

Detection Guidance: Alert on new domain registrations containing "standardbank", "liberty", "stanbic" within 48 hours of data release. Monitor for spike in banking fraud attempts using ID numbers that follow SA format. If your organisation processes Standard Bank client data for any purpose, assess whether the released dataset creates second-order POPIA breach notification obligations.

P1 — CRITICAL: Nation-state; actively exploited zero-day

TH-2026-W17-03 — Cisco IOS-XE CVE-2026-1834 / Salt Typhoon Persistence

Hypothesis: CVE-2026-1834 (CVSS 9.8, actively exploited zero-day) provides fresh attack surface on SA telecom and enterprise Cisco IOS-XE infrastructure. Salt Typhoon, which confirmed compromise of an SA telecom provider, may exploit this vulnerability for re-entry or lateral movement.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1572 (Protocol Tunneling / GRE), T1136.001 (Create Local Account), T1098 (Account Manipulation), T1046 (Network Service Scanning)

IOCs: Anomalous HTTP POST requests to /webui/ URIs on IOS-XE devices; new privilege-level-15 local accounts on network devices not matching change records; undocumented GRE tunnel entries (show ip tunnel); SNMP polls from unexpected external IPs; C2: aar.gandhibludtric[.]com (38.54.63[.]75); C2: esh.hoovernamosong[.]com (158.247.222[.]165); SoftEther VPN: vpn114240349.softether[.]net

Data Sources: IOS-XE syslog (HTTP access logs, privilege escalation events); TACACS+/RADIUS accounting logs; NetFlow/IPFIX for GRE tunnel traffic; Cisco IOS-XE audit trail; network device AAA logs; SIEM correlation for IOS-XE web UI access patterns

Detection Guidance: Run Cisco IOS XE Web UI Checker tool on all internet-facing devices. Compare running-config to known-good baseline. Any unexplained privilege-15 account or GRE tunnel entry is a P1 incident. Block IOS-XE web UI access from internet immediately ("no ip http server" + "no ip http secure-server"). Patch to 17.12.4a, 17.9.6, or 17.6.8.

TH-2026-W17-04 — Polmed/ShinyHunters SAPS Data Exploitation**P2 — HIGH: Law enforcement safety risk; physical harm potential**

Hypothesis: ShinyHunters possesses personal data of 100,000+ SAPS officers and their dependants. If this data is published, criminal networks with known interest in police personnel will immediately exploit it for targeted harassment, extortion, or operational intelligence.

MITRE ATT&CK: T1657 (Financial Extortion), T1491.002 (Leak Site Publication), T1589 (Gather Victim Identity Information), T1598 (Phishing for Information — follow-on spearphishing)

IOCs: ShinyHunters BreachForums / Telegram posts offering Polmed SAPS data; domains impersonating Polmed (polmedmembers[.]co.za etc.); spearphishing emails targeting @saps.gov.za addresses; communications claiming to have "information" about SAPS officers (extortion); Port 1244/tcp from any Polmed internal network (indicator of possible ShinyHunters C2)

Data Sources: Polmed network monitoring; SAPS corporate email gateway (phishing attempts); BreachForums/Telegram monitoring for Polmed data listings; law enforcement intelligence feeds; SAPS member complaint reports

Detection Guidance: Alert on any BreachForums/Telegram post referencing "Polmed", "SAPS medical", or SA police personnel. Notify all SAPS members of the breach and advise enhanced personal security practices. Brief SAPS management to implement officer safety protocols. If Polmed data is published, SAPS HR should initiate a full member notification programme.

TH-2026-W17-05 — Adumo POS Source Code Exploitation**P2 — HIGH: Payment infrastructure integrity risk**

Hypothesis: If the Adumo POS source code and chip-and-PIN certification artefacts are genuine, threat actors who purchase them could develop counterfeit-certified POS terminals or identify exploitable weaknesses in Adumo's transaction processing to facilitate card-present fraud at scale across 29,000 merchants.

MITRE ATT&CK: T1584 (Acquire Infrastructure), T1553 (Subvert Trust Controls), T1600 (Weaken Encryption), T1656 (Impersonation)

IOCs: Anomalous transaction patterns in Adumo merchant network (unusual approval rates, unusual card-present BIN patterns); POS terminal firmware versions not matching authorised baseline; card-present fraud spikes at specific merchant categories served by Adumo; darkweb posts offering "Adumo" or "Lesaka" payment integration capability

Data Sources: Adumo transaction monitoring (anomaly detection on approval/decline ratios); Mastercard/Visa fraud monitoring feeds; merchant POS terminal inventory (firmware baseline); SABRIC card fraud reporting; Lesaka/Adumo security operations

Detection Guidance: Adumo should immediately assess the authenticity of the leaked material and engage Mastercard and Visa to review whether any issued certifications are now compromised. Merchants should audit POS terminal firmware against authorised versions. Monitor for card-present fraud rate anomalies in Adumo-connected merchant networks.

TH-2026-W17-06 — Contagious Interview Supply Chain (5 Ecosystems)

P2 — HIGH: 1,700+ malicious packages across 5 ecosystems

Hypothesis: North Korean Contagious Interview actors have deployed 1,700+ malicious packages across npm, PyPI, Go, Rust, and PHP. SA developers in fintech, AI, and software outsourcing may have installed compromised packages or opened malicious repositories, resulting in credential theft and persistent backdoor access.

MITRE ATT&CK: T1195.001 (Compromise Software Dependencies), T1566.003 (Phishing via Service — Upwork/LinkedIn), T1204.002 (Malicious File Execution), T1059.007 (JavaScript), T1059.006 (Python), T1547.001 (Startup Folder), T1555 (Credential Theft)

IOCs: Stage 1 C2: task-hrec.vercel.app, kb102531x.vercel.app, brantwork.vercel.app. Stage 2 C2 IPs: 147.124.213.232, 147.124.212.125, 216.250.251.87, 45.43.11.199, 66.235.63.55. Port: 1244/tcp, 1249/tcp. Malicious npm package: "license-utils-kit". Poisoned Axios npm (WAVESHAPER.V2). XOR keys: G01d*8@(), !!!HappyPenguin1950!!!. RSA pub SHA256: 40b59567a2b580f1952dadae5dd586895b2316e590b84842f89aed1675f2d707

Data Sources: EDR (npm/node/python/go/rust process trees and network connections); developer workstation proxy logs; SIEM (port 1244/tcp outbound); endpoint AV/XDR telemetry; CI/CD pipeline package integrity monitoring; VSCode extension and task policy audit

Detection Guidance: Block port 1244/tcp outbound on all developer workstations. Run Socket.dev or equivalent SCA against all packages installed since January 2025. Check for "license-utils-kit" in npm, and any Axios version installed or updated in April 2026 (WAVESHAPER.V2 was delivered via compromised maintainer account). Alert on VSCode runOn:folderOpen tasks in cloned repositories. Flag all incoming developer job offers requesting repository cloning from unknown recruiters.

Hunt Mission Summary Checklist

Hunt ID	Hypothesis (Short)	Priority	Key Data Sources	Status
TH-2026-W17-01	XP95 post-deadline data monitoring	P1 — CRITICAL	Tor DLS, BreachForums, Telegram, TI feeds	Not Started
TH-2026-W17-02	ROOTBOY Std Bank credential exploitation	P1 — CRITICAL	Fraud monitoring, phishing alerts, SIEM	Not Started
TH-2026-W17-03	Cisco IOS-XE CVE-2026-1834 / Salt Typhoon	P1 — CRITICAL	Syslog, NetFlow, AAA, IOS-XE audit	Not Started
TH-2026-W17-04	Polmed/ShinyHunters SAPS data exploitation	P2 — HIGH	BreachForums monitor, SAPS network, email GW	Not Started
TH-2026-W17-05	Adumo POS source code fraud exploitation	P2 — HIGH	Transaction monitoring, POS firmware audit	Not Started
TH-2026-W17-06	Contagious Interview 5-ecosystem supply chain	P2 — HIGH	EDR, Proxy, SIEM, SCA tools, VSCode policy	Not Started

IOC Master Table — W17

Indicator	Type	Attribution	Hunt ID
api.telegram.org / 149.154.160.0/20	Domain/IP Range	XP95 C2 / exfiltration channel	TH-2026-W17-01
xp95 [BreachForums profile]	Account/Profile	XP95 extortion group	TH-2026-W17-01
standardbank-security[.]co.za (pattern)	Domain pattern	Post-breach phishing (monitor only)	TH-2026-W17-02
task-hrec.vercel.app	C2 Domain	Contagious Interview Stage 1	TH-2026-W17-06
147.124.213.232 / 147.124.212.125	IP Address	Contagious Interview Stage 2 C2	TH-2026-W17-06
1244/tcp, 1249/tcp	Port	Contagious Interview C2 (Express.js)	TH-2026-W17-06
license-utils-kit [npm]	Package name	Contagious Interview Windows implant	TH-2026-W17-06
WAVESHAPER.V2 [Axios npm]	Malware	Contagious Interview via poisoned maintainer	TH-2026-W17-06
aar.gandhibludtric[.]com (38.54.63[.]75)	C2 Domain/IP	Salt Typhoon (SNAPPYBEE C2)	TH-2026-W17-03
esh.hoovernamosong[.]com	C2 Domain	Salt Typhoon (SNAPPYBEE)	TH-2026-W17-03
vpn114240349.softether[.]net	VPN endpoint	Salt Typhoon network obfuscation	TH-2026-W17-03
CVE-2026-1834 (Cisco IOS-XE)	CVE	Salt Typhoon / unattributed exploitation	TH-2026-W17-03
CVE-2026-21643 (Fortinet EMS)	CVE	Unattributed — active exploitation	N/A — Patch
CVE-2026-27681 (SAP BW/BPC)	CVE	Unattributed — patch immediately	N/A — Patch
CVE-2026-34621 (Adobe Acrobat)	CVE	Active exploitation since Nov 2025	N/A — Patch
CVE-2026-32201 (SharePoint zero-day)	CVE	Actively exploited in wild	N/A — Patch

11. RECOMMENDATIONS

Immediate (This Week — Priority P1)

- **1. Activate POPIA s.22 response plans NOW:** Standard Bank 1.2TB data is public. Assess whether your organisation holds Standard Bank-sourced client data. Polmed affects 100K+ SAPS officers. If you process data from either entity, draft s.22 notifications and individual notification templates immediately. Deadline: this week.
- **2. Emergency patch: Cisco IOS-XE to 17.12.4a / 17.9.6 / 17.6.8:** CVE-2026-1834 (CVSS 9.8) actively exploited zero-day with direct Salt Typhoon relevance. Disable web UI immediately if patching is not immediate: "no ip http server" + "no ip http secure-server". Audit all privilege-15 accounts.
- **3. Upgrade Fortinet FortiClient EMS to 7.4.7:** CVE-2026-21643 (CVSS 9.1, CISA KEV 16 April deadline — PASSED). Both CVE-2026-35616 and CVE-2026-21643 are fixed in 7.4.7. Treat any EMS instance still running 7.4.5/7.4.6 as compromised.
- **4. Apply SAP Security Note #3719353:** CVE-2026-27681 (CVSS 9.9) — any SAP BW/BPC user can fully compromise your database. Interim: revoke S_GUI Authorization Activity 60 (Upload). Emergency for SA mining, banking, and retail SAP environments.
- **5. Upload new IdP SAML certificate to Cisco Webex Control Hub:** CVE-2026-20184 (CVSS 9.8) — without this customer action, the cloud-side patch is not effective. Required on all Cisco Webex SSO deployments.
- **6. Apply Microsoft April Patch Tuesday / Kerberos RC4 audit:** Monitor Event IDs 201-209 on DCs. Run List-AccountKeys.ps1. Patch CVE-2026-33824 (Windows IKE CVSS 9.8) and CVE-2026-32201

(SharePoint zero-day). July 2026 = no rollback for Kerberos RC4.

Short-Term (Next 30 Days)

- Patch Cisco ISE to fixed versions (3.1 Patch 11 / 3.2 Patch 10 / 3.3 Patch 11 / 3.4 Patch 6 / 3.5 Patch 3) for CVE-2026-20147/20180/20186 (CVSS 9.9 cluster — read-only admin = full root RCE).
- Update Adobe Acrobat/Reader DC to 26.001.21411 (CVE-2026-34621, CISA KEV, due 27 April). PDF-opening = exploitation. SA legal, financial, and government teams are highest risk.
- Apply Microsoft Exchange Server patch for CVE-2023-21529 (CVSS 8.8, CISA KEV, due 27 April).
- Audit npm/PyPI/Go/Rust/PHP packages installed since January 2025 on all developer workstations. Block port 1244/tcp outbound. Check for Contagious Interview IoCs. SA fintech and crypto-sector teams are highest priority.
- Conduct a full IOC sweep for Salt Typhoon SNAPPYBEE/GHOSTSPIDER indicators on SA telecom and enterprise IOS-XE infrastructure, even on patched devices — persistence may survive patching.
- If your organisation operates in Adumo's merchant network: audit POS terminal firmware against authorised baseline; monitor for card-present fraud rate anomalies.
- Assess FSCA/PA Joint Standard 2 compliance exposure from Standard Bank/Liberty breach if your organisation is a regulated financial institution.

Strategic

- The concurrent Standard Bank (1.2TB), Polmed (SAPS officers), Adumo (payment infrastructure), and XP95 (government bulk PII) crises in a single week demonstrate SA's systemic exposure. A national Cyber Crisis Coordination Committee — with DCDT, SARB, SAPS, ICASA, and the IR — needs standing activation protocols for concurrent multi-sector crises.
- Salt Typhoon's confirmed SA telecom targeting with no SA government advisory, no ICASA mandate, and no known remediation programme represents the most critical unaddressed systemic risk in the SA threat landscape. ICASA must develop a telecoms-specific cybersecurity incident reporting mandate equivalent to POPIA and Joint Standard 2.
- The PFMA prohibition on ransom payment is sound policy but requires compensating controls: air-gapped backups, encrypted databases, rapid data classification capability, and a national incident response fund. Legislative consideration is required before the next XP95-class event.
- The IR's 86% IO non-compliance rate (only 14% of companies have registered information officers) is now a crisis-level governance failure. Mandatory registration enforcement, not voluntary compliance, is required given the volume and severity of breaches.

12. OSINT SOURCES CONSULTED

The following open-source intelligence sources were consulted in the preparation of this report. All sources are TLP:WHITE and publicly accessible.

1. ITWeb — Hackers publicly release Standard Bank data (17 Apr) — <https://www.itweb.co.za/article/hackers-publicly-release-data-stolen-from-standard-bank/KBpdg7pmKwmMLEew>
2. TechCentral — Standard Bank breach fallout deepens (16 Apr) — <https://techcentral.co.za/standard-bank-data-breach-fallout-deepens/280322/>
3. Standard Bank — Official 14 April data incident update — <https://www.standardbank.co.za/southafrica/news-and-media/newsroom/an-important-data-incident-update-14-april>
4. The Citizen — Information Regulator to probe Standard Bank (13 Apr) — <https://www.citizen.co.za/lifestyle/technology/information-regulator-probe-standard-bank-data-breach/>
5. CentralNews — IR probes Standard Bank and Liberty (14 Apr) — <https://centralnews.co.za/information-regulator-of-south-africa-probes-major-data-breaches-at-standard-bank-and-liberty-group/>
6. ITWeb — Stats SA confirms data breach (29 Mar) — <https://www.itweb.co.za/article/stats-sa-confirms-data-breach-as-hackers-demand-r17m-ransom/JBwErVn3wpo76Db2>
7. UpGuard — Stats SA Data Breach 2026 — <https://www.upguard.com/news/statistics-south-africa-data-breach-2026-03-31>

8. DataBreaches.net — XP95 SA Government Analysis — <https://databreaches.net/2026/03/30/south-african-government-agency-and-spanish-psychological-software-provider-victims-of-cyberattacks-by-xp95/>
9. Breachsense — GCRA Breach Listing — <https://www.breachsense.com/breaches/the-gauteng-city-region-academy-bursary-data-breach/>
10. ITWeb — SAPS medical aid scheme probes breach (17 Apr) — <https://www.itweb.co.za/article/saps-medical-aid-scheme-probes-potential-data-breach/P3gQ2MGA5VNvnRD1>
11. allAfrica — Hackers attack police medical aid scheme (16 Apr) — <https://allafrica.com/stories/202604160282.html>
12. ITWeb — Adumo payment tech exposed for \$7,000 (17 Apr) — <https://www.itweb.co.za/article/adumo-payment-tech-exposed-hackers-offer-data-for-7-000/KWEBb7yLwdAvmRjO>
13. LaunchBase Africa — Adumo source code leak investigation (17 Apr) — <https://launchbaseafrica.com/2026/04/17/south-african-fintech-adumo-investigates-alleged-source-code-leak/>
14. HookPhish — TheGentlemen hits Sunspray Food — <https://www.hookphish.com/blog/ransomware-group-thegentlemen-hits-sunspray-food/>
15. Breachsense — Sunspray Food Data Breach (8 Apr) — <https://www.breachsense.com/breaches/sunspray-food-data-breach/>
16. Ransomware.live — South Africa Victim Map — <https://www.ransomware.live/map/ZA>
17. Recorded Future — RedMike/Salt Typhoon Cisco IOS-XE SA Telecom — <https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices>
18. TechCrunch — Salt Typhoon SA Telecom Confirmed (9 Mar 2026) — <https://techcrunch.com/2026/03/09/salt-typhoon-china-who-has-been-hacked-global-telecom-giants/>
19. Security Affairs — Salt Typhoon IOS-XE SA Telecom — <https://securityaffairs.com/174226/apt/salt-typhoon-exploited-cisco-ios-xe-flaws.html>
20. SPOTO — CVE-2026-1834 Cisco IOS-XE Critical Advisory (Apr 2026) — <https://cciedump.spoto.net/news/cisco-warns-of-critical-ios-xe-vulnerability-actively-exploited-in-global-networking-infrastructure-attacks-april-2026.html>
21. The Hacker News — Cisco ISE / Webex Critical Patches (Apr 2026) — <https://thehackernews.com/2026/04/cisco-patches-four-critical-identity.html>
22. BleepingComputer — Microsoft April 2026 Patch Tuesday (167 CVEs) — <https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2026-patch-tuesday-fixes-167-flaws-2-zero-days/>
23. CrowdStrike — April 2026 Patch Tuesday Analysis — <https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-april-2026/>
24. Microsoft TechCommunity — Kerberos RC4 Phase 2 (16 Apr) — <https://techcommunity.microsoft.com/discussions/windowsserver/phase-2-of-kerberos-rc4-hardening-begins-with-the-april-2026-windows-security-up/4511702>
25. The Hacker News — Adobe CVE-2026-34621 Zero-Day Actively Exploited — <https://thehackernews.com/2026/04/adobe-patches-actively-exploited.html>
26. The Hacker News — SAP/Adobe/Fortinet Critical Patches April 2026 — <https://thehackernews.com/2026/04/april-patch-tuesday-fixes-critical.html>
27. CSO Online — April Patch Tuesday Roundup — <https://www.csoonline.com/article/4158706/april-patch-tuesday-roundup-zero-day-vulnerabilities-and-critical-bugs.html>
28. The CyberSignal — CISA 7 KEV Entries W17 — <https://www.thecybersignal.com/cisa-expands-kev-catalog-with-seven-actively-exploited-flaws-across-microsoft-adobe-and-fortinet/>
29. ITWeb — InfoReg raises alarm, 788 Q1 2026 notifications (14 Apr) — <https://www.itweb.co.za/article/info-reg-raises-alarm-as-data-breaches-hit-788-in-q1/Pero3MZ3wzoqQb6m>
30. Mayet Law — POPIA Enforcement 2026 Developments — <https://mayet.law/popia-enforcement-in-south-africa-key-2026-developments-and-what-businesses-must-do-now/>
31. ITLawCo — Information Regulator 2026/27 Annual Performance Plan — <https://itlawco.com/information-regulator-2026-27-annual-performance-plan/>
32. Silicon Republic — XP95 Targets Healthdaq Dublin (13 Apr) — <https://www.siliconrepublic.com/enterprise/new-xp95-hacker-group-targets-dublin-recruitment-platform-healthdaq>
33. The Register — OAPT Krybit Panel Breach (14 Apr) — https://www.theregister.com/2026/04/14/Oapt_krybit_spat/
34. Industrial Cyber — GuidePoint GRIT Q1 2026 Ransomware Report — <https://industrialcyber.co/reports/ransomware-reaches-elevated-new-normal-as-attack-volumes-hold-steady-into-2026-reshape-baseline-risk-expectations/>
35. Trend Micro — Earth Estries (Salt Typhoon) Report — https://www.trendmicro.com/en_us/research/24/k/earth-estries.html
36. The Hacker News — DPRK Contagious Interview 1,700 Packages (8 Apr) — <https://thehackernews.com/2026/04/n-korean-hackers-spread-1700-malicious.html>
37. Microsoft Security Blog — Contagious Interview Enterprise Intrusions (11 Mar) — <https://www.microsoft.com/en-us/security/blog/2026/03/11/contagious-interview-malware-delivered-through-fake-developer-job-interviews/>
38. IOL/Sophos — SA Ransomware Recovery Costs R24M (Sophos 2025) — <https://iol.co.za/business-report/economy/2025-07-04-ransomware-recovery-costs-south-african-businesses-r24-million-on-average-report-finds/>
39. SABRIC — Annual Crime Statistics Report 2024 — <https://www.sabric.co.za/wp-content/uploads/2025/09/CRIME-STATISTICS-REPORT-2024.pdf>
40. TechCentral — Gaping holes in SA government cyber defences (2 Apr) — <https://techcentral.co.za/gaping-holes-in-south-african-government-cyber-defences/279769/>
41. D3 Security — NIS2 SOC Audit Readiness 2026 (18 Apr) — <https://d3security.com/blog/nis2-soc-audit-readiness-2026/>
42. Inclusive Society Institute — SA Cybersecurity Blueprint (Apr 2026) — <https://www.inclusivesociety.org.za/post/securing-the-future-blueprint-for-solving-south-africa-s-cybersecurity-crisis-in-the-age-of-ai>
43. WatchTower — CVE-2026-35616 Fortinet FortiClient EMS Zero-Day Analysis — <https://watchtower.com/resources/fortinet-forticlient-ems-zero-day-cve-2026-35616-active-exploitation-underway/>
44. Censys — Salt Typhoon Persistent Threat Tracking — <https://censys.com/blog/the-persistent-threat-of-salt-typhoon-tracking-exposures-of-potentially-targeted-devices/>
45. BlackFog — State of Ransomware 2026 — <https://www.blackfog.com/the-state-of-ransomware-2026/>

This report is classified TLP:WHITE. It may be distributed without restriction. Information sourced from publicly available OSINT. No classified or restricted sources were used. Prepared by Digital Progression | dpcyber.co.za | DP-CTI-2026-W17