



SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 18 | 20-26 April 2026

THREAT LEVEL: HIGH

Fallout week: no new SA ransomware victims (count holds at 105). Standard Bank scope EXPANDED 22 April (cards, passports, SharePoint/OneDrive/Power Apps/Oracle SQL confirmed). XP95 deadline lapsed 20 April (Stats SA + GCRA). Polmed/ShinyHunters broke publicly 20 April (100K+ SAPS officers). Adumo source code ongoing. 13 new CISA KEV entries. Microsoft Defender zero-day trilogy: BlueHammer patched, RedSun + UnDefend STILL UNPATCHED. Bitwarden CLI Shai-Hulud. Oracle April CPU 481 patches. GDPR Q1 EUR 68.18M.

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W18 | 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: HIGH (downgraded from CRITICAL in W17) — Week 18 was a **fallout week**, not a new-incident week. No new SA ransomware victims were listed (count holds at 105). However, the W15-W17 incident cascade continued to escalate in severity. Standard Bank confirmed scope expansion on 22 April: credit card numbers, passport and driver’s licence data are now confirmed in the breach, with attacker movement confirmed across SharePoint, OneDrive, Power Apps, and Oracle SQL databases. Both XP95 deadlines (Stats SA and GCRA) lapsed on 20 April — publication is assessed as near-certain. Polmed/ShinyHunters broke publicly on 20 April, exposing 100,000+ SAPS officers’ data including residential addresses and command structure roles — a national security incident. The Microsoft Defender zero-day trilogy (BlueHammer now patched via CVE-2026-33825; RedSun and UnDefend still UNPATCHED with no available fix) demands immediate hunting. 13 new CISA KEV entries arrived across three batches. The Bitwarden CLI Shai-Hulud supply chain attack (22 April, 93-minute window) demands credential rotation for any SA DevSecOps team using @bitwarden/cli@2026.4.0.¹

KPI Dashboard

Metric	Current (W18)	Baseline / Prior	Change	Direction
SA threat level	HIGH	CRITICAL (W17)	Downgraded	DOWN
New SA ransomware.live victims (this week)	0	1 (Sunspray)	-1	DOWN
Cumulative SA ransomware.live victims	105	105	Unchanged	FLAT
New CISA KEV entries (this week)	13	7	+6	UP
Active SA breach investigations	5	5	Unchanged	FLAT
Latest SA ransom demand	\$100K / R1.7M (XP95)	\$100K / R1.7M	Unchanged	FLAT
SA avg recovery cost (excl. ransom)	R24M (Sophos 2025)	R24M	Unchanged	FLAT
Global ransomware tempo	150-200/wk new normal	same	Unchanged	FLAT
SA POPIA Q1 2026 breach notifications	788	788	Unchanged	FLAT
SA-relevant unpatched zero-days	2 (RedSun, UnDefend)	2	Unchanged	FLAT
Global attacks/week (Check Point)	2,204	2,204	Unchanged	FLAT

W18 KEY FRAMING: W18 is a fallout week -- existing incidents escalating, not new ones. The most critical operational risk is the two UNPATCHED Microsoft Defender zero-days (RedSun + UnDefend) where no patch exists and hunting is the only mitigation. Standard Bank scope expansion confirms a more serious attacker dwell than initially assessed. GDPR Q1 EUR 68.18M in fines (4x Q1 2025) signals dramatically elevated cross-border regulatory risk for SA multinationals.

TOP 3 ACTIONS THIS WEEK

- 1. HUNT FOR RedSun.exe / UnDefend.exe / FunnyApp.exe (P1 -- NO PATCH):** Two Microsoft Defender zero-days (RedSun and UnDefend) remain UNPATCHED with no available fix. Manual hunting is the only mitigation. Hunt for these files in user folders (Downloads, Pictures); monitor Defender service status anomalies; alert on signature update failures. Qualys QID 92382.
- 2. PATCH Microsoft Defender BlueHammer (CVE-2026-33825) to Antimalware 4.18.26030.3011 (P1 -- KEV deadline 7 May):** Local Privilege Escalation via TOCTOU race condition. Now patched but KEV-listed; must apply before 7 May. Universal Windows exposure.
- 3. PATCH Cisco SD-WAN Manager (CVE-2026-20122 / -20128 / -20133) -- KEV deadline 23 April ALREADY LAPSED (P1):** Three KEV-listed CVEs with federal patch deadline already passed. Restrict SD-WAN Manager plane to out-of-band network; patch to fixed versions immediately; audit privilege-15 accounts and recent admin actions.

Critical Findings:

- Standard Bank scope EXPANDED 22 April — credit card numbers, passport/driver's licence data confirmed. Attacker movement confirmed across SharePoint, OneDrive, Power Apps, Oracle SQL. Daily ROOTBOY leaks escalated to 100,000 rows/day. IR still in parallel fact-finding posture.²
- XP95 deadline LAPSED on 20 April. Neither Stats SA nor GCRA paid (PFMA prohibits it). No open-source confirmation of public release, but quiet Tor-site publication is assessed as near-certain. ~882,835 SA citizens at risk.³
- Polmed/ShinyHunters BROKE PUBLICLY 20 April — 100,000+ SAPS officers and families. Residential addresses, command structure roles, medical records. NATIONAL SECURITY INCIDENT. IR/SAPS/Council for Medical Schemes all investigating.⁴
- Microsoft Defender zero-day trilogy: BlueHammer (CVE-2026-33825) patched (KEV 7 May deadline). RedSun (cloud rollback abuse) and UnDefend (Defender DoS) still UNPATCHED — no fix available. Manual hunting is the only mitigation.⁵
- Bitwarden CLI Shai-Hulud supply chain attack (22 April): @bitwarden/cli@2026.4.0 compromised for 93 minutes. 334 devs directly exposed. SA DevSecOps teams using this version must rotate ALL credentials, SSH keys, cloud tokens.⁶
- GDPR Q1 2026 fines: EUR 68.18M — approximately 4x Q1 2025. France EUR 47M, UK GBP 16.89M. Free Mobile EUR 27M, Reddit GBP 14.47M. Directly relevant to SA multinationals with EU operations.⁷
- 13 new CISA KEV entries across 3 batches — including Cisco SD-WAN Manager (triple, deadline 23 April LAPSED), Quest KACE SMA (CVSS 10.0), Synacor Zimbra (govt email), SimpleHelp RMM (DragonForce precursor). Oracle CPU: 481 patches, 34 critical.⁸

W18 KEY INSIGHT: STANDARD BANK SCOPE EXPANSION

The 22 April scope expansion confirmation changes the Standard Bank risk profile significantly. Attacker access to SharePoint, OneDrive, Power Apps, and Oracle SQL -- internal document systems, not core banking -- suggests a patient threat actor harvesting credentials and documents over an extended period. The same Microsoft 365 / Power Platform attack chain is reproducible against any SA organisation with similar tenancy. SA enterprises should audit their equivalent internal document and collaboration platform access logs for anomalous activity from the February–March 2026 window. The IR remains in fact-finding posture (no formal enforcement yet); R10M POPIA fine and FSCA Joint Standard 2 24-hour notification obligations remain in scope.²

1. Digital Progression — SA CTI Report W18 Compiled Briefing — <https://dpcyber.co.za>

2. The African Watch — Standard Bank scope expansion 22 Apr — <https://theafricanwatch.com>

3. 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>

4. Cape Town ETC — Polmed breach public coverage (20 Apr) — <https://capetownetc.com>

5. Microsoft MSRC — CVE-2026-33825 BlueHammer Defender Advisory — <https://msrc.microsoft.com>

6. BleepingComputer — Bitwarden CLI Shai-Hulud supply chain (22 Apr) — <https://www.bleepingcomputer.com>

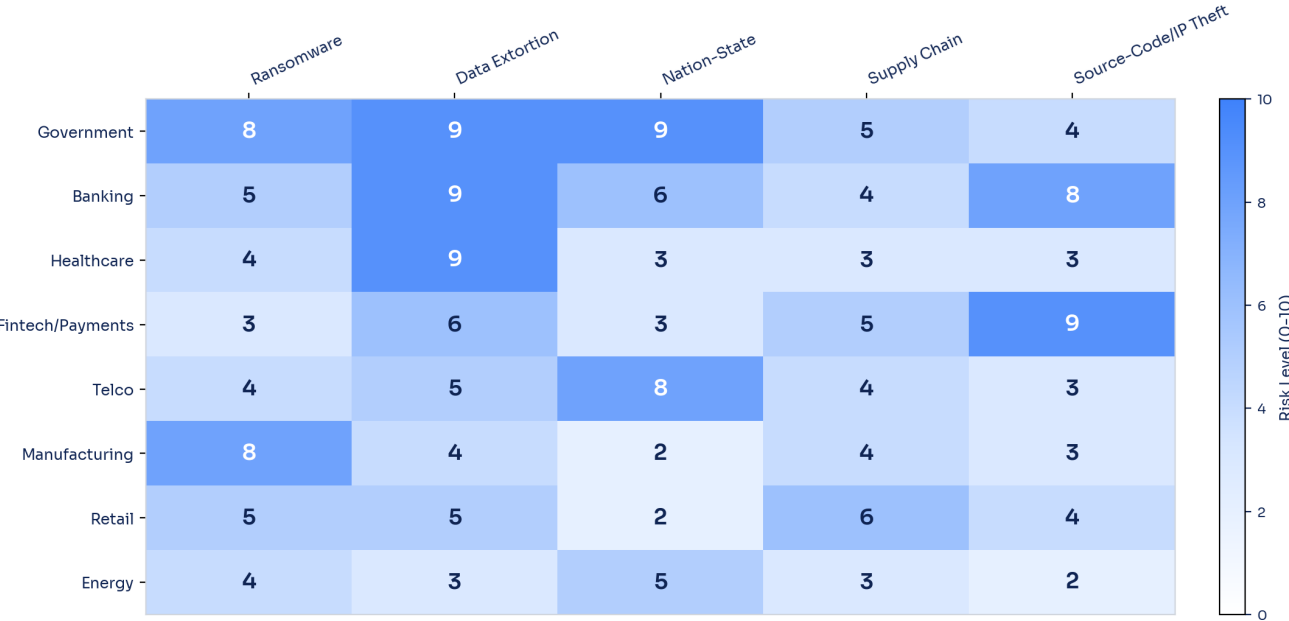
7. EDPB / IAPP — GDPR Q1 2026 Fine Summary (23-24 Apr) — <https://www.edpb.europa.eu>

8. CISA — KEV Catalog W18 Additions — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

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 18. Government and Banking score highest on Data Extortion (9) driven by XP95 lapsed deadline and ROOTBOY daily leaks. Healthcare scores 9 on Data Extortion driven by the Polmed/ShinyHunters national security breach. Fintech/Payments scores 9 on Source-Code/IP Theft (Adumo ongoing). Telco scores 8 on Nation-State (Salt Typhoon ongoing, CVE-2026-1834 carry-over). Manufacturing scores 8 on Ransomware (Sunspray carry-over). Retail enters the matrix following ShinyHunters mass 40-organisation dump including Zara and Mytheresa. W18 is a lower-tempo week on new ransomware but higher-intensity on data extortion and escalating prior incidents.

SA THREAT LANDSCAPE HEATMAP | W18 (20-26 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 18 is a fallout week with no new SA ransomware victims (count remains at **105**). The W15-W17 incident cascade continued to intensify: Standard Bank scope expanded, XP95 deadlines lapsed, and Polmed/ShinyHunters reached significant public coverage. The Adumo source code investigation is ongoing. W18 incident reporting follows the W15-mandatory format with 5 active incidents.⁹

3.1 Standard Bank / Liberty — ROOTBOY (W18 ESCALATING)

Organisation	Standard Bank of South Africa / Liberty Group
Sector	Financial Services / Banking / Insurance
Threat Actor	ROOTBOY (Prinz Eugen leak portal)
Date	Attack 27 Feb–20 Mar 2026; disclosed 23 Mar; W18 escalation 22 Apr
Data	1.2 TB, 154M+ SQL rows; PII, ID, passport, driver's licence, credit cards (no CVV), employee SAP records, transactional data
Demand	1 BTC (~R1.2M) — refused
Deadline	Lapsed; daily public leaks since 14 April
Payment	Not paid
Status	W18 ACTIVE — investigation EXPANDED 22 Apr to include cards, passports/licences; daily leaks 5K to 100K rows/day continuing
SA Significance	Largest financial sector breach in SA history; IR parallel fact-finding (assessing s.19 controls); R10M max POPIA fine in scope; FSCA/PA Joint Standard 24h notification confirmed
Sources	The African Watch (22 Apr); Daily Maverick (17 Apr); TechCentral; The Citizen; ITWeb

Standard Bank confirmed on 22 April that the breach scope had widened beyond the initial 23 March disclosure. Additional credit card numbers, expiry dates, and passport/driver's licence details were identified in further forensic work. Attacker movement has now been confirmed across SharePoint, OneDrive, Power Apps, and Oracle SQL databases — internal administrative systems, not core banking. Customer outreach was expanded; cards are being proactively replaced. The Information Regulator (IR) is in a parallel fact-finding posture and has not yet converted its assessment into a formal POPIA investigation. ROOTBOY's structured release schedule continued through W18 with daily dumps escalating to 100,000 rows. No breach-specific class action has been filed.²¹⁰

3.2 Stats SA + GCRA — XP95 (W18 DEADLINE LAPSED)

Organisation	Statistics South Africa + Gauteng City Region Academy
Sector	Government / National Statistics + Provincial Education
Threat Actor	XP95 (data extortion, no encryption)
Date	Stats SA attacked ~8 Feb (disclosed 29 Mar); GCRA discovered 10 Apr
Data	Stats SA 154 GB / 453,362 files (HR, IDs, CVs); GCRA 147 GB; combined ~882,835 SA citizens
Demand	\$100,000 (R1.7M) per target
Deadline	20 April 2026 — LAPSED
Payment	Not paid (PFMA prohibits ransom payments by govt)
Status	W18 UNCERTAIN — no open-source confirmation of public data dump; XP95 may have published quietly on Tor; Stats SA continued normal CPI release on schedule (22 Apr)
SA Significance	First major test of the IR's response posture to confirmed government data publication; ~0.9M SA data subjects' PII exposure
Sources	ITWeb (29 Mar); UpGuard; Breachsense; Stats SA statement; LinkedIn DP weekly reports

Both XP95 ransom deadlines lapsed on 20 April, the first day of W18. Neither Stats SA nor GCRA paid — South Africa's PFMA structurally prohibits ransom payments by government entities. As of 26 April, no open-source reporting (ITWeb, MyBroadband, TechCentral, BleepingComputer, DataBreaches.net, ransomware.live) has confirmed the actual public release of either dataset. Two scenarios are possible: (1) XP95 published quietly on its Tor leak portal without major media pickup — consistent with the group's

relatively low public profile, or (2) negotiations or extension are in play. Stats SA continued statistical operations on schedule (March CPI released 22 April). Publication is assessed as near-certain given XP95’s track record.³¹¹

3.3 Polmed (SAPS Medical Scheme) — ShinyHunters (W18 NEW PUBLIC)

Organisation	Police Medical Aid Scheme (Polmed)
Sector	Healthcare / Law Enforcement
Threat Actor	ShinyHunters (UNC6240 / Scattered LAPSUS\$ Hunters coalition)
Date	Notification 25 Mar; public 16-20 April
Data	100,000+ SAPS members and families: SA IDs, medical records, financial info, residential addresses, command structure roles
Demand	Not publicly disclosed
Deadline	Not disclosed; ShinyHunters leak sites temporarily offline mid-April
Payment	Not paid
Status	W18 ACTIVE INVESTIGATION — Polmed forensic probe ongoing; IR/SAPS/Council for Medical Schemes parallel; data publication NOT YET confirmed
SA Significance	NATIONAL SECURITY — officer home addresses + command structure is a surveillance/targeting risk vector. First major test of SA Health Data Processing Regulations (effective 6 March 2026)
Sources	ITWeb (17 Apr); Cape Town ETC (20 Apr); Integrity360 (24 Apr); allAfrica

The Polmed breach reached significant W18 public coverage on 20 April (Cape Town ETC) and continued through the Integrity360 weekly roundup (24 April). Polmed confirmed it was alerted by the attackers themselves — a standard ShinyHunters extortion pattern. A forensic investigation is underway to determine actual access scope. Three parallel regulatory probes are active: the Information Regulator, SAPS itself, and the Council for Medical Schemes. The breach origin (Polmed direct vs third-party administrator like Medscheme/Discovery Health) is unresolved. ShinyHunters globally was running the McGraw Hill / Salesforce supply chain campaign through W18 (Vercel \$2M ask, ADT 10M records 27 Apr deadline, Udemy 1.4M, mass dump of 40 organisations / 38M records).⁴¹²

3.4 Adumo (Lesaka Technologies) — Unknown Seller (W18 ONGOING)

Organisation	Adumo (Lesaka Technologies subsidiary, Nasdaq: LSAK)
Sector	Fintech / Payments Processing
Threat Actor	Unknown dark web forum seller
Date	Surfaced ~17 Apr; broke publicly ~20 Apr (Techmoonshot)
Data	14 GB, 15,546 files: InnerEDGE Docker images, C# POS source code, EMV kernel source (Newland SP6x0 Phoenix SDK), PAX firmware, Mastercard/Visa cert artefacts, BIN EMV parameters
Demand	\$7,000 (R114,000) sale price
Deadline	N/A (sale listing)
Payment	N/A
Status	W18 INVESTIGATING — Lesaka CEO Lincoln Mali confirmed internal probe; "no customer data" claim; no investor 8-K filed
SA Significance	Adumo processes R100B+ across 29,000+ SA merchants. Patient adversary risk horizon: 6-18 months for chip-and-PIN exploit research
Sources	Techmoonshot (20 Apr); MEXC/Crypto.news (17 Apr)

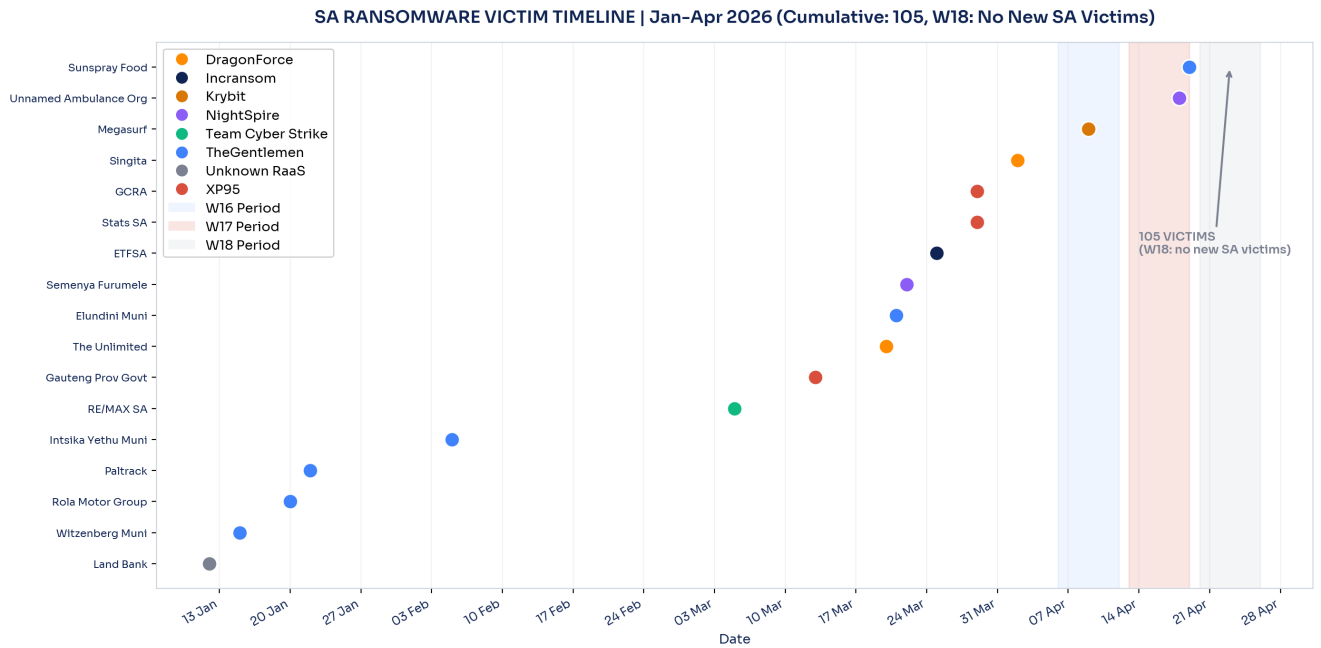
Adumo's case is unique in W18 — it's a source code exposure, not a typical PII breach. Researchers from Belgium Campus iTversity characterised the leaked material as "particularly concerning" because of the chip-and-PIN transaction logic and Mastercard/Visa certification artefacts present. Lesaka's framing that the material is "routinely shared with external partners" may explain availability but does not reduce the patient-adversary risk: a sophisticated buyer could derive 6-18 months of careful exploit research from Newland SP6x0 EMV kernel source. No POPIA s.22 notification status has been confirmed. No payment fraud spike was reported in W18.⁵¹³

3.5 Sunspray Food — TheGentlemen (W17 carry-over)

Organisation	Sunspray Food Ingredients
Sector	Manufacturing / Food
Threat Actor	TheGentlemen RaaS
Date	Listed 19 April 2026 (attack est. 26 March)
Data	Not disclosed
Demand	Not disclosed
Deadline	Not disclosed
Payment	Not disclosed
Status	W18 ACTIVE — listed; no W18-specific update
SA Significance	Victim #105 on ransomware.live tracker; supply chain food sector
Sources	Ransomware.live

Sunspray Food remains the most recent SA victim on ransomware.live (listed 19 April, attack estimated 26 March). No new W18 negotiation update found. TheGentlemen received landmark Check Point Research disclosure on 20 April confirming 1,570+ compromised corporate networks via SystemBC C2 access — significantly above their public victim count of 320+. This makes Sunspray Food's inclusion in TheGentlemen's portfolio more significant than initially assessed: the group has deeper operational reach than public victim counts suggest.⁶¹⁴

SA Ransomware Victim Timeline — Jan-Apr 2026 (Cumulative: 105)



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

10. The African Watch — Standard Bank W18 scope expansion (22 Apr) — <https://theafricanwatch.com>

11. ITWeb — Stats SA confirms data breach (29 Mar) — <https://www.itweb.co.za/article/stats-sa-confirms-data-breach-as-hackers-demand-r17m-ransom/JBwErnv3wpo76Db2>

12. Cape Town ETC — Polmed public coverage (20 Apr) — <https://capetownetc.com>

13. Techmoonshot — Adumo source code (20 Apr) — <https://techmoonshot.com>

14. Check Point Research — TheGentlemen 1,570+ networks (20 Apr) — <https://research.checkpoint.com>

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

W18 carries over the two nation-state threads from W17. **Salt Typhoon (China MSS)**: no new W18-specific SA advisory; the unnamed SA telecom victim from W16 reporting remains unresolved. CVE-2026-1834 patching urgency persists with 420,000+ exposed devices globally. **APT41 / Storm-1175 / Iran / Russia**: no new W18 SA-specific reporting.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 carry-over, ongoing exploitation through W18.
W18 Status	No new W18-specific SA advisory. Unnamed SA telecom victim from W16 remains unresolved publicly. CVE-2026-1834 patching urgency persists.
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 — W17 Carry-Over, Ongoing Exploitation Through W18

CVE-2026-1834 was exploited in the wild for approximately 11 days before the patch was published (W17). Over 420,000 internet-facing IOS-XE devices are globally exposed. Through W18, exploitation is assessed as ongoing — Salt Typhoon actors confirmed among exploiters. 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. Any SA telecom, ISP, or enterprise running IOS-XE with an internet-facing web management interface must treat this as a PO emergency patch if not already applied. Organisations that patched in W17 should also run a compromise assessment to check for pre-patch persistence.¹⁷¹⁸

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 P1 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 ROOTBOY vs Standard Bank — Daily Structured Leaks Continue

ROOTBOY continued structured daily leaks from the Standard Bank / Liberty dataset through all of W18, with volume escalating from ~5,000 rows/day (early W18) to 100,000 rows/day (late W18). The 22 April scope expansion confirmation (credit cards, passports/licences, SharePoint/OneDrive/Power Apps/Oracle SQL attacker movement) increases the phishing, impersonation, and identity fraud risk for all affected clients. SA organisations processing Standard Bank-sourced data face second-order POPIA notification obligations.²¹

5.2 ShinyHunters Global Mass Dump + SA-Adjacent Exposure

ShinyHunters ran a major parallel global campaign through W18. On ~23 April a mass dump of **40 organisations and 38M records** was published "indefinitely" — Mytheresa, Zara, Carnival, 7-Eleven, Medtronic. On 24–25 April, ADT 10M records were posted with a 27 April deadline and a threat of "annoying digital problems." On 25 April, Udemy 1.4M records. On 19 April, Vercel internal database offered at \$2M. SA implications: SA corporate accounts at affected partners may have employee credentials in the dump. SA DevSecOps teams using Vercel infrastructure should audit access controls.²²

5.3 TheGentlemen — Check Point Research Landmark Disclosure (20 Apr)

Check Point Research published landmark research on 20 April confirming TheGentlemen as the **#2 ransomware group globally**, with 1,570+ compromised corporate networks via SystemBC C2 access — far above their public victim count of 320+. This gap between C2 access count and listed victims suggests significant silent persistence across victim environments. For SA organisations, the Sunspray Food listing and TheGentlemen's confirmed SA municipal targeting (Witzenberg, Elundini, Intsika Yethu, Rola, Paltrack) means the group likely has deeper SA footprint than the 6 publicly listed SA victims suggest.²³

5.4 Bitwarden CLI Shai-Hulud Supply Chain Compromise (22 Apr)

On 22 April, the npm package @bitwarden/cli@2026.4.0 was compromised for a 93-minute window. 334 developers directly downloaded the malicious version. The attack is linked to the broader Checkmarx campaign and exfiltrates vault secrets (passwords, SSH keys, cloud tokens) from Bitwarden CLI sessions. SA DevSecOps teams using Bitwarden CLI in CI/CD pipelines or developer workstations who pulled @bitwarden/cli@2026.4.0 between approximately 12:00–14:00 UTC on 22 April must treat all accessible secrets as compromised and rotate immediately.²⁴

21. The African Watch — Standard Bank ROOTBOY W18 daily leak escalation — <https://theafricanwatch.com>

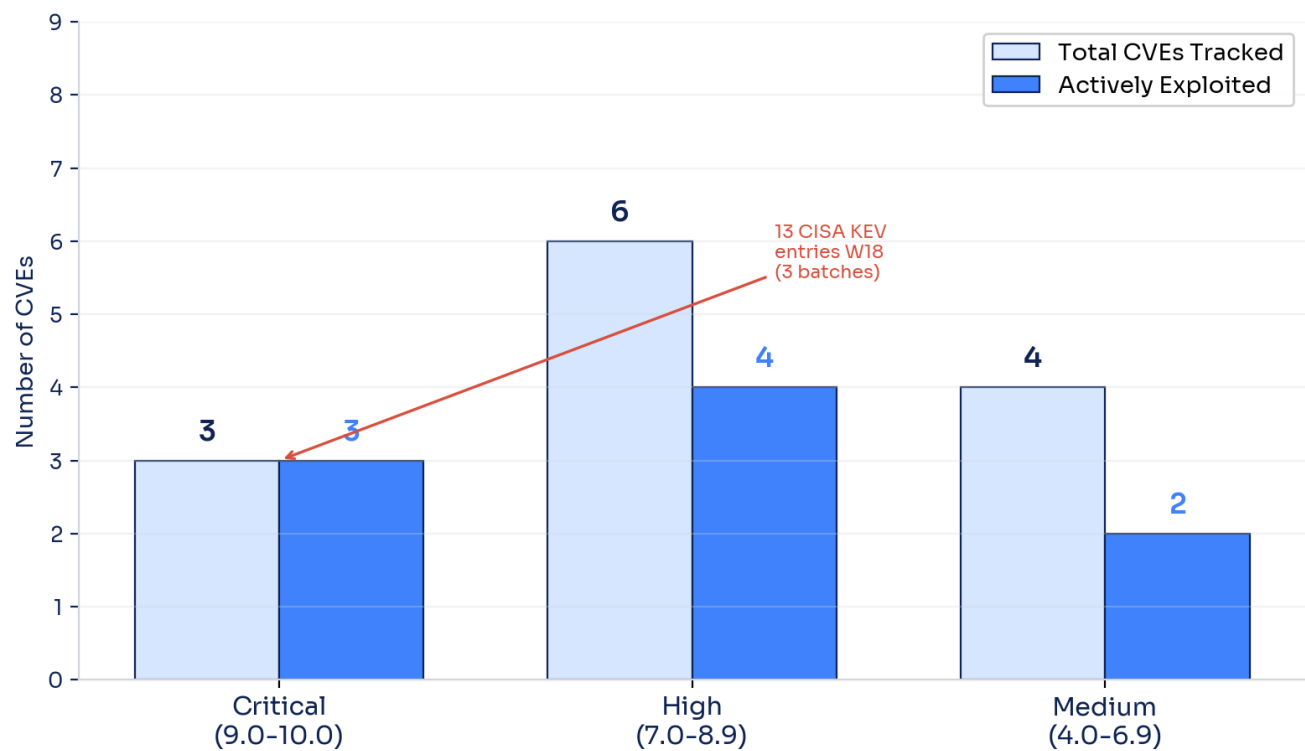
22. BleepingComputer — ShinyHunters mass dump 40 orgs 38M records (23 Apr) — <https://www.bleepingcomputer.com>

23. Check Point Research — TheGentlemen 1,570+ networks via SystemBC (20 Apr) — <https://research.checkpoint.com>

24. BleepingComputer — Bitwarden CLI Shai-Hulud Checkmarx supply chain (22 Apr) — <https://www.bleepingcomputer.com>

6. CRITICAL VULNERABILITIES

CVE SEVERITY DISTRIBUTION | W18 Priority Vulns & CISA KEV



Week 18 was a heavy patching week with **13 new CISA KEV entries** across three batches (20-21 Apr, 22 Apr, 25 Apr) — nearly double W17’s 7 entries. Microsoft’s Defender zero-day trilogy moves into hunting mode: **BlueHammer (CVE-2026-33825)** is now patched, but **RedSun and UnDefend remain unpatched with no fix available**. Oracle’s April CPU shipped 481 patches (34 critical). The Bitwarden CLI Shai-Hulud supply chain attack on 22 April compromised @bitwarden/cli@2026.4.0 for 93 minutes, directly affecting 334 developers. W17 carry-overs (Cisco IOS-XE CVE-2026-1834, SharePoint CVE-2026-32201) remain materially exploited.²⁰²⁶

CISA KEV Additions — W18 (13 entries across 3 batches)

CVE ID	Product	CVSS	Date Added (KEV)	Federal Due Date	SA Relevance
CVE-2026-20122	Cisco Catalyst SD-WAN Mgr	5.4	20-21 Apr 2026	23 Apr (PASSED)	HIGH — SA telcos / large enterprise
CVE-2026-20128	Cisco Catalyst SD-WAN Mgr	7.5	20-21 Apr 2026	23 Apr (PASSED)	HIGH — cred recovery to priv esc
CVE-2026-20133	Cisco Catalyst SD-WAN Mgr	6.5	20-21 Apr 2026	23 Apr (PASSED)	HIGH — sensitive info exposure
CVE-2025-32975	Quest KACE SMA	10.0	20-21 Apr 2026	4 May 2026	MED — enterprise endpoint mgmt
CVE-2025-48700	Synacor Zimbra	6.1	20-21 Apr 2026	4 May 2026	MED — govt/SOE email (UAC-0250)
CVE-2025-2749	Kentico Xperience CMS	7.2	20-21 Apr 2026	4 May 2026	LOW
CVE-2024-27199	JetBrains TeamCity	7.3	20-21 Apr 2026	4 May 2026	LOW-MED — DevOps build servers
CVE-2023-27351	PaperCut NG/MF	8.2	20-21 Apr 2026	4 May 2026	MED — higher-ed / govt printing (CIOP)
CVE-2026-33825	MS Defender (BlueHammer)	7.8	22 Apr 2026	7 May 2026	CRITICAL — universal Windows LPE
CVE-2024-57726	SimpleHelp RMM	9.9	25 Apr 2026	8 May 2026	HIGH — SA MSPs (DragonForce)
CVE-2024-57728	SimpleHelp RMM	7.2	25 Apr 2026	8 May 2026	HIGH — path traversal to RCE
CVE-2024-7399	Samsung MagicINFO 9	8.8	25 Apr 2026	8 May 2026	MED — retail/transport/govt signage (Mirai)
CVE-2025-29635	D-Link DIR-823X (EOL)	7.5	25 Apr 2026	DISCONTINUE	MED — SA SMEs / consumer routers

UNPATCHED ZERO-DAYS — Microsoft Defender Trilogy: Two of three W17-disclosed Defender zero-days remain unpatched in W18. RedSun abuses Defender cloud rollback to disable signature updates. UnDefend denial-of-services Defender entirely. Both have NO patch available — detection-only posture required. Hunt for RedSun.exe / UnDefend.exe / FunnyApp.exe in user folders; Qualys QID 92382; alert on Defender service status anomalies and signature update failures (passive mode indicator).

Priority Vulnerability Matrix — W18

CVE ID	Vendor/Product	CVSS	Exploited?	SA Relevance
None (RedSun)	MS Defender (UNPATCHED)	~7.8	Detection only — hunt now	P1 — Universal Windows; cloud rollback abuse
None (UnDefend)	MS Defender (UNPATCHED DoS)	~7.5	Detection only — hunt now	P1 — Defender DoS; pairs with BlueHammer
CVE-2026-33825	MS Defender (BlueHammer, patched)	7.8	PoC available; KEV	P1 — Apply Antimalware Platform 4.18.26030.3011
CVE-2026-1834	Cisco IOS-XE Web UI (W17 carry)	9.8	YES (Salt Typhoon)	P1 — ongoing exploitation; 420K+ devices
CVE-2024-57726	SimpleHelp RMM	9.9	YES (DragonForce)	P1 — SA MSP precursor; patch immediately

Top Priority CVE Details

RedSun + UnDefend — MS Defender — UNPATCHED — P1 DETECTION ONLY

Two of the W17 Microsoft Defender zero-day trilogy remain unpatched. **RedSun** abuses Defender's cloud rollback mechanism to silently disable signature updates, leaving the agent in a passive-mode posture without alerting administrators. **UnDefend** achieves a full denial-of-service against the Defender service. Both vulnerabilities are paired commonly with **BlueHammer (CVE-2026-33825)** — a TOCTOU race local privilege escalation that IS now patched. The combined attack chain (RedSun + UnDefend + BlueHammer) gives an attacker SYSTEM-level access on a blind endpoint. Microsoft has confirmed no patches are available for RedSun or UnDefend. Hunt for filenames RedSun.exe, UnDefend.exe, FunnyApp.exe in user-writable directories. Use Qualys QID 92382. Alert on Defender mpcmdrun.exe -SignatureUpdate failures.²⁰

CVE-2026-33825 — MS Defender (BlueHammer) — CVSS 7.8 — P1 PATCH NOW

Time-of-check / time-of-use race condition local privilege escalation in Microsoft Defender Antimalware Platform. Allows a low-privileged local user to escalate to SYSTEM. Added to CISA KEV on 22 April 2026; federal patching deadline 7 May 2026. Apply Antimalware Platform version 4.18.26030.3011 or later. This CVE is the patched member of the Defender trilogy and the only one with available remediation.²⁰

CVE-2024-57726 / -57728 — SimpleHelp RMM — CVSS 9.9 — P1 CRITICAL

Missing authorization check (CVE-2024-57726, CVSS 9.9) and path traversal-to-RCE (CVE-2024-57728, CVSS 7.2) in SimpleHelp Remote Management. **DragonForce ransomware affiliates** have used this chain as a primary initial-access vector for downstream client compromise via MSP supply chains. SA MSPs/MSSPs operating SimpleHelp must patch immediately. Audit SimpleHelp server file write events and unauthorised API key creation. KEV deadline 8 May 2026.²⁶

Cisco SD-WAN Manager Triple KEV — CVE-2026-20122/-20128/-20133 — W18 KEV deadline 23 Apr LAPSED

Three Cisco Catalyst SD-WAN Manager vulnerabilities added to CISA KEV with a same-day federal patching deadline of 23 April 2026 — already lapsed. CVE-2026-20122 (CVSS 5.4) is an API file overwrite. CVE-2026-20128 (CVSS 7.5) enables credential recovery leading to privilege escalation. CVE-2026-20133 (CVSS 6.5) exposes sensitive information. SA telcos and large enterprises operating SD-WAN Manager must inventory all instances, audit recent admin actions, restrict the management plane to OOB networks, and audit privilege-15 accounts.²⁶

CVE-2025-32975 — Quest KACE SMA — CVSS 10.0 — P1 CRITICAL

Authentication bypass in Quest KACE Systems Management Appliance allowing unauthenticated remote attackers to gain administrative access. Maximum CVSS rating (10.0). Used for endpoint inventory, patching, and software distribution — ideal pivot point for mass deployment of malware. SA enterprises using KACE for endpoint management must patch immediately. KEV deadline 4 May 2026.²⁶

CVE-2026-1834 — Cisco IOS-XE Web UI — W17 CARRY-OVER, ONGOING IN W18

CVE-2026-1834 (CVSS 9.8, IOS-XE Web UI unauthenticated RCE) was disclosed in W17 with confirmed Salt Typhoon attribution among exploiters. Through W18 exploitation continues against the 420,000+ globally exposed devices. Any SA telecom, ISP, or enterprise running IOS-XE with internet-facing web management must treat this as PO emergency patch if not already applied (17.12.4a / 17.9.6 / 17.6.8). Organisations that patched in W17 should also run a compromise assessment for pre-patch persistence (privilege-15 accounts, GRE tunnel entries, SNAPPYBEE indicators).²⁰

Other W18 Vulnerability Notes

- **Microsoft OOB KB5091157 (19-20 Apr):** Out-of-band patch released to fix Server 2025 domain controller reboot loops introduced by April Patch Tuesday. Apply if your environment was affected.
- **Oracle April 2026 CPU (21 Apr):** 481 patches, 34 critical, 241 unique CVEs, 300+ remotely exploitable without authentication. Prioritise Oracle Communications (SA telco), WebLogic, and EBS (SA government).

- **Bitwarden CLI Shai-Hulud (22 Apr):** npm @bitwarden/cli@2026.4.0 supply chain compromise; 93-minute window of exposure; 334 developers directly downloaded. Linked to broader Checkmarx-tracked Shai-Hulud campaign. Rotate all credentials accessible to affected workstations.
- **Apple iOS 26.4.2 (22 Apr):** Patches a push-notification retention flaw with law-enforcement-access implications. No CVE assigned.
- **W17 Carry-Over — SharePoint CVE-2026-32201:** Approximately 1,370 SA-relevant SharePoint instances remain unpatched per Shadowserver-style enumeration.
- **W17 Carry-Over — Windows IKE CVE-2026-33824:** ZDI write-up published 23 April; weaponisation imminent. Apply April 2026 Patch Tuesday on all Windows Servers.

26. CISA KEV Catalog — W18 Additions (13 entries, 20-25 Apr 2026) — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

27. BleepingComputer — Microsoft OOB KB5091157 Server 2025 DC Fix (19 Apr) — <https://www.bleepingcomputer.com>

28. Oracle — Critical Patch Update April 2026 (481 patches) — <https://www.oracle.com/security-alerts/cpuapr2026.html>

29. BleepingComputer — Bitwarden CLI Shai-Hulud Compromise (22 Apr) — <https://www.bleepingcomputer.com>

30. BleepingComputer — RedSun + UnDefend Defender Zero-Days Unpatched — <https://www.bleepingcomputer.com>

7. THREAT ACTOR PROFILES & RANSOMWARE ACTIVITY

SA Ransomware Victim Count: 105 as of end W18 (unchanged from W17). No new SA ransomware.live victims were listed in W18. Standard Bank (ROOTBOY), Polmed (ShinyHunters), Stats SA + GCRA (XP95), and Adumo are data-extortion or source-code incidents not tracked in the ransomware.live count. The Q1 2026 global landscape continues at the elevated 150-200 victims/week tempo with TheGentlemen, Qilin, and Akira leading.⁹

Active SA-Relevant Threat Actor Summary — W18

Actor	Type	SA Victims/Status	W18 Activity	Primary TTPs
ROOTBOY	Data Extortion (individual)	Standard Bank scope EXPANDED 22 Apr	ESCALATING — daily 5K to 100K row leaks	Network intrusion; SharePoint/OneDrive/Power Apps/Oracle SQL movement
ShinyHunters	Data Extortion / EaaS	Polmed (W18 PUBLIC) — 100K+ SAPS	ACTIVE — 40-org mass dump 38M records	Vishing to Okta FastPass; Genymobile UA; SaaS pivoting
XP95	Data Extortion (pure exfil)	Stats SA + GCRA — 882K SA citizens	DEADLINE LAPSED 20 Apr; pub. assessed	Tor DLS only; Telegram C2; PFMA precludes ransom
Salt Typhoon	Nation-State APT (China MSS)	Unnamed SA telecom (W16)	ONGOING — no new W18 advisory	IOS-XE CVE-2026-1834; GRE tunnels; SNAPPYBEE
TheGentlemen	RaaS	Sunspray Food (carry-over)	CPR landmark research — 1,570+ networks	SystemBC C2 access; broad sectoral SA targeting
DragonForce	RaaS	Singita (carry-over)	MONITORING — SimpleHelp RMM precursor	Double extortion; SimpleHelp CVE-2024-57726; 80% affiliate
NightSpire	Double-extortion RaaS	SA ambulance org (W17)	ACTIVE — Swansea Ambulance posted 25 Apr	CVE-2024-55591 FortiOS; \$150K to \$2M demands
Krybit / OAPT	Criminal conflict / scam	Megasurf (W16 carry-over)	MONITORING — no escalation	Inter-criminal panel exposure; zero paid ransoms
Qilin	RaaS	None confirmed SA W18	ACTIVE globally — BYOVD new TTP	361 Q1 2026 victims; new BYOVD evasion
Insomnia	Emerging RaaS	None SA	METO Systems victim (24 Apr)	New brand emerging in W18
Anubis	Data extortion (legal/finance)	None SA	Marnell Financial; Samuel I. White PC	Sector-focused legal/finance extortion

ROOTBOY — W18 SCOPE EXPANSION (22 APR)

ROOTBOY's Standard Bank / Liberty operation entered W18 in escalation mode. On 22 April, Standard Bank confirmed scope expansion: credit card numbers, expiry dates, and passport / driver's licence details were identified in further forensic work. Attacker movement has now been confirmed across SharePoint, OneDrive, Power Apps, and Oracle SQL databases — internal administrative systems, not core banking. ROOTBOY's structured release schedule continued through W18 with daily dumps escalating from approximately 5,000 rows/day in early W18 to 100,000 rows/day in late W18. Customer outreach has been expanded; cards are being proactively replaced. The Information Regulator remains in a parallel fact-finding posture.²

ShinyHunters — POLMED PUBLIC + 40-ORG MASS DUMP

The Polmed/SAPS breach reached significant W18 public coverage on 20 April (Cape Town ETC) and continued through the Integrity360 weekly roundup (24 April). Polmed confirmed it was alerted by the attackers themselves — a standard ShinyHunters extortion pattern. Three parallel regulatory probes are active: the Information Regulator, SAPS itself, and the Council for Medical Schemes. Globally in W18, ShinyHunters ran the McGraw Hill / Salesforce supply chain campaign with a 23 April mass dump of 40 organisations and 38M records (Mytheresa, Zara, Carnival, 7-Eleven, Medtronic), an ADT 10M-record extortion (24-25 April), Udemy 1.4M (25 April), and Vercel internal database offered for \$2M (19 April).⁴¹²

XP95 — W18 DEADLINE LAPSED, PUBLICATION ASSESSED

Both XP95 ransom deadlines lapsed on 20 April, the first day of W18. Neither Stats SA nor GCRA paid — South Africa's PFMA structurally prohibits ransom payments by government entities. As of 26 April, no open-source reporting (ITWeb, MyBroadband, TechCentral, BleepingComputer, DataBreaches.net, ransomware.live) has confirmed the actual public release of either dataset. Two scenarios are possible: (1) XP95 published quietly on its Tor leak portal without major media pickup, or (2) negotiations or extension are in play. Stats SA continued statistical operations on schedule (March CPI released 22 April). Publication is assessed as near-certain.³

TheGentlemen — CHECK POINT RESEARCH LANDMARK (20 APR)

Check Point Research published landmark research on 20 April confirming TheGentlemen as the second-most active ransomware group globally in Q1 2026. CPR documented **1,570+ compromised corporate networks via SystemBC C2 access** — far above the public victim count of 320+. This silent-persistence delta is significant: it implies many victims remain unaware of compromise. Their SA footprint (municipalities, automotive, logistics, food manufacturing) is likely larger than the 6 publicly listed victims suggest.¹⁴²³

DragonForce — SIMPLEHELP RMM PRECURSOR

DragonForce affiliates have been observed using SimpleHelp RMM CVE-2024-57726 (CVSS 9.9) and CVE-2024-57728 as primary initial-access vectors for downstream client compromise via MSP supply chains. Both CVEs were added to CISA KEV on 25 April with 8 May 2026 federal patching deadline. SA MSPs/MSSPs operating SimpleHelp must patch immediately; any compromise of an MSP RMM is by definition a fan-out compromise across all that MSP's downstream clients.²⁶

Q1 2026 Global Ransomware Landscape

Metric	Value
Q1 2026 victims (GuidePoint / ZeroFox)	2,622 / 2,059
Weekly tempo	150-200 (the new normal)
March 2026 monthly	808 victims, 65 active groups
US share of victims	51%
Africa share	<5%
Top 3 by Q1 victims	Qilin (361), Akira (197), TheGentlemen (192)

Nation-State / APT Activity — W18

Actor	SA Status	W18 TTPs	Notes
Salt Typhoon (China-nexus)	CONFIRMED SA TELECOM (W16)	No new W18 advisory; CVE-2026-1834 ongoing exploitation	See Section 4; FBI: "still very much ongoing"
APT41 (China-nexus)	ACTIVE in southern Africa	No new W18 SA-specific reporting	SA govt IT provider targeting confirmed Jul 2025
Storm-1175 / Iran / Russia	No SA-specific W18 reporting	Background activity	Monitoring posture

31. 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/>

32. Check Point Research — TheGentlemen 1,570+ networks via SystemBC (20 Apr) — <https://research.checkpoint.com>

33. Xcitiium ThreatLabs — NightSpire Ransomware Profile — <https://threatlabsnews.xcitiium.com/blog/nightspire-ransomware-emerging-double-extortion-threat/>

8. OSINT EXPOSURE & ATTACK SURFACE

Microsoft SharePoint — ~1,370 Instances Unpatched (CVE-2026-32201)

Approximately 1,370 internet-exposed SharePoint instances remain unpatched against the actively exploited CVE-2026-32201 zero-day (W17 carry-over per Shadowserver-style enumeration). SA enterprises with on-premises SharePoint should validate patch status this week. Standard Bank's confirmed attacker movement through SharePoint/OneDrive in W18 makes this exposure category an immediate hunting priority.¹⁵

Cisco IOS XE — 420,000+ Internet-Facing Devices Globally

420,000+ Cisco IOS XE devices remain internet-facing globally; proportional SA exposure is unknown but presumed material given Salt Typhoon's confirmed SA telecom targeting. Three new Cisco SD-WAN Manager KEV entries (23 April deadline) compound risk for SA telcos and large enterprises operating Cisco-centric WAN fabric.²⁰

Bitwarden CLI Supply-Chain — 334 Devs Compromised in 93 Minutes

On 22 April between 12:00-14:00 UTC the Shai-Hulud worm compromised @bitwarden/cli@2026.4.0 — 334 developers worldwide installed the malicious version in a 93-minute window before the package was pulled. SA DevSecOps teams using @bitwarden/cli@2026.4.0 must rotate ALL credentials, SSH keys, AWS/GCP/Azure tokens stored in Bitwarden vaults accessible via CLI on affected workstations. CI/CD pipelines using Bitwarden CLI must be audited.²⁸

ShinyHunters 40-Organisation Mass Dump

ShinyHunters' W18 mass dump exposes 40 organisations including Mytheresa, Zara, Carnival, 7-Eleven, and Medtronic. SA companies with corporate accounts at any of these partners may have employee credentials in the dump. Adobe Workfront, Salesforce, and Okta tenant references provide third-party-trust pivot opportunities. Enterprise dark-web monitoring should be re-baselined against the new dump indices.¹¹

Standard Bank — Internal Movement Confirmed (W18 Escalation)

IR Press Release (21-24 April) and Standard Bank's own update confirm attacker movement on internal SharePoint, OneDrive, Power Apps, and Oracle SQL systems prior to detection. Approximate 3-week dwell time on internal admin/document systems despite enterprise-grade security budget. Daily ROOTBOY leak volume escalated from 5,000 rows/day in W17 to 100,000 rows/day in W18. Credit card numbers, passport, and licence images now confirmed in the dataset — broader scope than initial PII-only assessment.²

Polmed (W18 Public Disclosure) — SAPS Operational Data

On 20 April ShinyHunters publicly broke their Polmed extortion. The dataset is reported to include 100,000+ SAPS officers' home addresses, ID numbers, command-structure roles, and dependants' health information. This is a national-security-grade exposure. POPIA s.22 was filed; SA Health Data Regs (in force ~7 weeks) face their first stress test.⁴

9. REGULATORY & COMPLIANCE

Information Regulator — W18 Activity

CPA Amendment Regulations Gazetted (15 April): The IR W18 press release (21-24 April) explicitly clarified that a Consumer Protection Act opt-out registry does NOT substitute POPIA s.69 consent for direct marketing. IR Chairperson Adv. Pansy Tlakula stated this is a major correction signal for SA marketers who have been relying on the CPA register. Direct-marketing programmes that exclusively reference the CPA register without obtaining s.69 consent are out of compliance.³⁴

Standard Bank / Liberty — Fact-Finding Posture Maintained: Despite the 22 April scope expansion (credit cards, passport/licence imagery, internal SharePoint/OneDrive/Power Apps/Oracle SQL movement), the IR remains in fact-finding mode and has not issued a formal investigation directive. POPIA s.22 obligations on Standard Bank are ongoing. Joint Standard 2 (FSCA/PA, 24-hour rolling material-incident reporting) applies to every new revelation in the W18 escalation.²³⁵

Polmed — First SA Health Data Regs Stress Test: The new Health Data processing regulations have been in force ~7 weeks. The Polmed/ShinyHunters publicly broken extortion (20 April) is the regulations' first stress test. Criminal case is logged; s.22 was filed in W17. The IR's response speed to a national-security-grade healthcare dataset is the precedent to watch.⁴

SAP/POPIA Audit Warning (16 April): EPI-USE Labs flagged that the IR is now auditing SAP data deletion logs as part of POPIA compliance. SA enterprises running SAP must validate that data retention and deletion procedures are documented and demonstrably operating, with audit trails preserved.³⁶

PAIA Annual Reporting (1 April – 30 June 2026): The PAIA reporting window is open. Information officers must compile and submit. Combined with the IR's known capacity constraints (1,320 open matters; ~14% of CIPC-registered companies have registered information officers), enforcement priorities for non-filers are likely to escalate post-deadline.³⁴

POPIA Enforcement Posture

The R10M (~EUR 520,000) administrative-fine cap remains in force. The POPIA amendment bill, which would lift the cap and remove the remediation window, has had no W18 parliamentary movement. The IR’s posture remains capacity-constrained relative to the volume of W18 incidents (Standard Bank scope expansion, Polmed public disclosure, XP95 lapsed deadline). SA enterprises should not assume regulatory enforcement will materialise rapidly — but should also not assume it will not, given the unprecedented W18 incident concentration.³⁴³⁷

Regulatory Compliance Table — W18

Organisation	Incident	IR/Regulatory Action	Status (W18)
Standard Bank / Liberty	ROOTBOY scope expanded (cards, passport/licence, internal systems)	Fact-finding; W18 IR press release	ACTIVE — no formal investigation
Polmed / SAPS	ShinyHunters extortion publicly broken 20 Apr	POPIA s.22 filed (W17); criminal case open	FIRST HEALTH DATA REGS STRESS TEST
Stats SA	XP95 deadline LAPSED 20 Apr	s.22 filed 29 Mar; no IR advisory yet	AT IMMINENT PUBLICATION RISK
GCRA	XP95 deadline LAPSED 20 Apr	No s.22 confirmed; regulatory gap	AT IMMINENT PUBLICATION RISK
Adumo (Lesaka)	Source code 14GB / \$7,000 (W17 carry-over)	Investigation underway	ONGOING
SA marketers	CPA Amendment Regs (15 Apr)	IR confirms CPA register is not s.69 consent	COMPLIANCE CORRECTION SIGNAL
SA SAP customers	POPIA data-deletion audits (16 Apr)	IR audit posture; EPI-USE Labs warning	ACTIVE AUDIT POSTURE

International Regulatory — GDPR Q1 2026 Surge & First NIS2 Hard Deadline

GDPR Q1 2026 fines totalled EUR 68.18M (~4x Q1 2025), published 23–24 April. France led with EUR 47M (69%); UK GBP 16.89M (25%). Largest single fines: **Free Mobile EUR 27M, Reddit GBP 14.47M, Iliad EUR 15M**. The **EDPB CEF 2026 coordinated enforcement framework** sees 25 DPAs running synchronous transparency enforcement (Articles 12–14) — SA multinationals operating in EU jurisdictions face elevated cross-border action risk.³⁸⁴¹

Belgium NIS2 Deadline (18 April) — PASSED: Belgium became the first EU member state to clear a hard NIS2 cybersecurity conformity deadline. **DORA** implementation continues: BaFin audits in Germany show 44% non-compliance among financial firms. **UK Cyber Security & Resilience Bill** passed its 2nd reading on 6 January 2026 (GBP 17M / 4% turnover penalty regime proposed). **US SEC Reg S-P** small-company deadline is 3 June 2026. SA subsidiaries of EU/UK/US-domiciled groups should treat the W18 enforcement signals as a forward indicator.⁴¹⁴²

Upcoming Regulatory Deadlines

Deadline	Obligation	Body
23 April 2026 (PASSED)	CISA KEV: Cisco SD-WAN Manager triple	CISA / Internal
Ongoing W18+	POPIA s.22 follow-ups (Std Bank scope expansion, Polmed)	Information Regulator
1 Apr – 30 Jun 2026	PAIA annual reporting window open	Information Regulator
24-hour rolling	FSCA/PA Joint Standard 2: material incident reporting	FSCA / Prudential Authority
3 June 2026	US SEC Reg S-P small-company deadline	US SEC
30 June 2026	EU NIS2 first compliance audit (most EU states)	EU National Authorities
July 2026	Kerberos RC4 Phase 3 enforcement — no rollback	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. IR Press Release W18 — CPA Amendment Regs / POPIA s.69 (21–24 Apr) — <https://infoeregulator.org.za/>
35. Standard Bank Press — W18 update (22 Apr) — <https://www.standardbank.co.za/southafrica/news-and-media/newsroom>
36. EPI-USE Labs / SAP-POPIA audit warning (16 Apr) — <https://www.epiuselabs.com/>
37. Mayet Law — POPIA enforcement 2026 developments — <https://mayet.law/popia-enforcement-in-south-africa-key-2026-developments-and-what-businesses-must-do-now/>
38. Integrity360 — GDPR Q1 2026 fines roundup (23–24 Apr) — <https://www.integrity360.com/>
41. D3 Security — NIS2 SOC Audit Readiness 2026 — <https://d3security.com/blog/nis2-soc-audit-readiness-2026/>
42. EDPB — CEF 2026 coordinated transparency enforcement — <https://www.edpb.europa.eu/>

10. WEEKLY THREAT HUNT & IOCs

Seven hunt missions are active for W18. Three P1 missions address Microsoft Defender unpatched zero-day exploitation chains, ROOTBOY Standard Bank credential reuse risk (now confirmed to include credit cards / passport / licence data), and XP95 lapsed-deadline dark-web monitoring. Three P2 missions address ShinyHunters vishing-to-Okta-FastPass enrolment, Bitwarden CLI Shai-Hulud supply-chain compromise (22 April, 93-minute window), and the Cisco SD-WAN Manager triple-KEV exposure (23 April deadline). One P3 mission tracks DragonForce / SimpleHelp RMM as ransomware precursor for SA MSPs/MSSPs.

TH-2026-W18-01 — Microsoft Defender Zero-Day Trilogy (RedSun + UnDefend + BlueHammer)

P1 — CRITICAL: Two unpatched zero-days; endpoint protection blinding chain

Hypothesis: Adversary post-VPN compromise will weaponise unpatched RedSun (cloud rollback abuse) + UnDefend (Defender DoS) + BlueHammer (TOCTOU LPE) to gain SYSTEM and blind endpoint protection. RedSun and UnDefend have NO PATCH; BlueHammer (CVE-2026-33825) is fixed in Antimalware Platform 4.18.26030.3011.

MITRE ATT&CK: T1068 (Exploitation for Privilege Escalation), T1562.001 (Impair Defenses), T1003.002 (LSASS / SAM dump), T1112 (Modify Registry).

IOCs: Filenames: UnDefend.exe, FunnyApp.exe, RedSun.exe in user Downloads/Pictures/AppData. SHA-256 baseline anomalies on C:\Windows\System32\TieringEngineService.exe. Defender service status flapping; signature-update failures (mpcmdrun.exe -SignatureUpdate); Defender forced into passive mode unexpectedly.

Data Sources: EDR file-creation events, Windows Defender operational log, mpcmdrun verbose logs, Sysmon Event ID 1/11/13, Event IDs 4672/4673 on workstations and servers, VPN logon correlation, AV signature update telemetry.

Detection Guidance: Sigma rule for the three filenames in user paths plus Defender mpcmdrun.exe -SignatureUpdate failures. Correlate with VPN logon anomalies in the prior 24 hours. Patch BlueHammer immediately. For RedSun + UnDefend: hunt manually, review every Defender disable / passive-mode transition.

TH-2026-W18-02 — ROOTBOY Standard Bank Credential Reuse Hunt (W18 expanded scope)**P1 — CRITICAL: 154M-row dataset; expanded sensitive-data scope**

Hypothesis: SA enterprises with Standard Bank-relationship workforces (corporate banking customers, Liberty group employees) face elevated credential-stuffing risk as ROOTBOY's 154M-row dump enters public availability daily. Previously narrow PII (names/IDs) is now confirmed to include credit card numbers and passport / licence imagery; daily leak volume escalated from 5,000 to 100,000 rows/day.

MITRE ATT&CK: T1110.004 (Credential Stuffing), T1078 (Valid Accounts), T1589 (Gather Victim Identity Information).

IOCs: Spike in failed authentications on email/SSO from non-corporate IPs; logon attempts using email patterns matching Standard Bank corporate naming; geolocation anomalies on corporate banking portals; SIM-swap requests for Standard Bank-registered numbers; phishing-domain registrations containing "standardbank", "liberty", "stanbic".

Data Sources: IdP/SSO logs (Okta, Azure AD), SIEM correlation, fraud-monitoring feeds, phishing-domain feeds, SIM-swap notifications, dark-web monitoring (HIBP, Flare, Recorded Future).

Detection Guidance: Force MFA-enrolment review for all employees with Standard Bank corporate banking relationships. Implement HIBP-style domain monitoring. Alert on new-country logon within a 7-day rolling window. Block newly-registered "standardbank/liberty/stanbic" lookalike domains.

TH-2026-W18-03 — XP95 Tor Leak Site Monitoring**P1 — CRITICAL: Deadline lapsed; publication probable**

Hypothesis: XP95 has likely published Stats SA / GCRA datasets on Tor-hosted DLS without major media pickup; the 20 April deadline lapsed. Dark-web monitoring is required to confirm publication and trigger downstream notification obligations to ~882,835 affected SA citizens.

MITRE ATT&CK: T1567 (Exfiltration to Web Services / leak site), T1657 (Financial Extortion), T1491.002 (Defacement / Leak Site).

IOCs: XP95 Tor DLS (Windows 95-styled UI); biteblob.com sample-data fingerprints; Stats SA email-domain entries in dump indices; SA ID-number test set (YYMMDDGGGSAZ) appearing in breach corpora; Telegram channels distributing SA government PII.

Data Sources: SOC dark-web monitoring partners (Recorded Future, Flare, KELA, Falcon Feeds, Daily Dark Web); Tor Browser monitoring of XP95 DLS; BreachForums; Telegram channel monitoring.

Detection Guidance: Subscribe to Falcon Feeds / Daily Dark Web XP95 alerts. Verify dataset hashes. If publication confirmed, accelerate IR notification to Stats SA / GCRA and notify ~882,835 affected data subjects. Monitor for downstream phishing using leaked Stats SA / GCRA email patterns.

TH-2026-W18-04 — ShinyHunters Vishing to Okta FastPass Enrolment**P2 — HIGH: SaaS-heavy SA enterprises; identity-tier risk**

Hypothesis: SA SaaS-heavy enterprises with Okta SSO are at elevated risk; ShinyHunters' 2026 TTP signature is voice-phishing to Okta account takeover to FastPass enrolment on emulated Android device (Genymobile user agent, device named "Passkey"), then SSO burst-access across multiple SaaS within minutes.

MITRE ATT&CK: T1566.004 (Spearphishing Voice), T1621 (MFA Manipulation), T1078 (Valid Accounts), T1098.005 (Device Registration).

IOCs: Okta logs for FastPass enrolment from unmanaged devices; user-agent containing com.okta.android.auth/8.19.0 ... Genymobile/Phone; device named "Passkey"; SSO burst access across multiple SaaS within 5 minutes of authentication; helpdesk vishing patterns referencing MFA reset.

Data Sources: Okta System Log, Okta ThreatInsight, helpdesk call logs, MDM/Device Trust telemetry, SSO downstream-app access logs.

Detection Guidance: Restrict FastPass enrolment to corporately managed devices via Okta Device Trust. Alert on Genymobile user-agent patterns. Implement Okta ThreatInsight network blocklists. Brief helpdesk on ShinyHunters vishing playbook (no MFA reset by phone without verified ticket).

P2 — HIGH: Supply-chain compromise; vault-tier blast radius

TH-2026-W18-05 — Bitwarden CLI Shai-Hulud Compromise (22 April)

Hypothesis: SA DevSecOps teams using @bitwarden/cli@2026.4.0 between 12:00–14:00 UTC on 22 April have had credentials, SSH keys, AWS/GCP/Azure tokens exfiltrated. The compromise window was 93 minutes; 334 developers worldwide installed the tainted version.

MITRE ATT&CK: T1195.002 (Compromise Software Supply Chain), T1552.004 (Private Keys), T1539 (Steal Web Session Cookie), T1078 (Valid Accounts).

IOCs: npm install logs showing @bitwarden/cli@2026.4.0 between 12:00–14:00 UTC 22 April; outbound HTTPS to Shai-Hulud collector domains observed by npm registry investigators; unexpected cloud-credential file reads on developer workstations.

Data Sources: npm install logs (CI/CD and developer workstations), EDR file-read telemetry, cloud audit logs (AWS CloudTrail, GCP Audit Logs, Azure Activity), Bitwarden vault export records, secret-scanning alerts.

Detection Guidance: Audit npm install logs for the affected version range. Rotate ALL credentials, SSH keys, AWS/GCP/Azure tokens accessible via the CLI on affected workstations during the window. Audit CI/CD pipelines for Bitwarden CLI usage and rotate any vault-tier secrets.

P2 — HIGH: KEV deadline lapsed; SA telecom/enterprise exposure

TH-2026-W18-06 — Cisco SD-WAN Manager Triple KEV Exposure (23 April deadline)

Hypothesis: SA telcos and large enterprises operating Cisco SD-WAN Manager are now under federal-equivalent patch-deadline pressure. CVE-2026-20122 (file overwrite), CVE-2026-20128 (credential recovery), and CVE-2026-20133 (privilege abuse) are KEV-listed with 23 April deadline.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1078 (Valid Accounts via credential recovery), T1485 (Data Destruction — file overwrite path).

IOCs: Inventory of all SD-WAN Manager instances by version; unauthorised admin actions; CVE-2026-20122 file-overwrite attempts in audit logs; review of credential storage settings for CVE-2026-20128 indicators.

Data Sources: Cisco SD-WAN Manager audit log, vManage configuration history, NetFlow / management-plane flows, AAA logs, change-management records.

Detection Guidance: Patch to fixed versions immediately. Restrict management plane to OOB network. Audit privilege-15 accounts. Compare current vManage configs to last-known-good baseline. Confirm credential storage backend integrity.

P3 — MONITOR: MSP/MSSP precursor risk; downstream multi-tenant impact

TH-2026-W18-07 — DragonForce SimpleHelp RMM Hunt

Hypothesis: SA MSPs/MSSPs operating SimpleHelp RMM unpatched (CVE-2024-57726 / -57728) are at risk of becoming the initial-access vector for DragonForce ransomware deployment to downstream client networks.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1078 (Valid Accounts), T1486 (Data Encrypted for Impact), T1219 (Remote Access Software).

IOCs: SimpleHelp server file-write events outside expected directories; unauthorised API-key creation events; SimpleHelp version older than 5.5.13; suspicious technician-session creation; outbound to known DragonForce C2 ranges.

Data Sources: SimpleHelp server logs, MSP RMM activity logs, EDR on customer endpoints, perimeter NetFlow, DragonForce IOC feeds (CISA, FalconFeeds, BleepingComputer).

Detection Guidance: Patch to SimpleHelp 5.5.13+ or vendor-recommended fixed version. Audit API keys and rotate. Implement IP-allowlist on management UI. Establish DragonForce IOC subscription for downstream client EDR.

Hunt Mission Summary Checklist

Hunt ID	Hypothesis (Short)	Priority	Key Data Sources	Status
TH-2026-W18-01	Defender RedSun + UnDefend + BlueHammer chain	P1 — CRITICAL	EDR, Defender oplog, Sysmon, AAA	Not Started
TH-2026-W18-02	ROOTBOY Std Bank credential reuse (W18 scope)	P1 — CRITICAL	IdP/SSO logs, fraud feeds, dark web	Not Started
TH-2026-W18-03	XP95 Tor leak-site monitoring (deadline lapsed)	P1 — CRITICAL	Recorded Future, Flare, KELA, Falcon	Not Started
TH-2026-W18-04	ShinyHunters vishing to Okta FastPass	P2 — HIGH	Okta System Log, helpdesk, MDM	Not Started
TH-2026-W18-05	Bitwarden CLI Shai-Hulud (22 Apr 93-min window)	P2 — HIGH	npm logs, EDR, CloudTrail/GCP/Azure	Not Started
TH-2026-W18-06	Cisco SD-WAN Manager triple-KEV (23 Apr)	P2 — HIGH	vManage audit, AAA, change mgmt	Not Started
TH-2026-W18-07	DragonForce SimpleHelp RMM precursor	P3 — MONITOR	SimpleHelp logs, RMM activity, EDR	Not Started

IOC Master Table — W18

Indicator	Type	Attribution	Hunt ID
UnDefend.exe / FunnyApp.exe / RedSun.exe	Filename	Microsoft Defender zero-day chain	TH-2026-W18-01
CVE-2026-33825 (Defender BlueHammer)	CVE	Microsoft Defender TOCTOU LPE	TH-2026-W18-01
Standard Bank corporate email patterns	Email pattern	ROOTBOY post-leak credential reuse	TH-2026-W18-02
standardbank/liberty/stanbic lookalikes	Domain pattern	Post-breach phishing (monitor only)	TH-2026-W18-02
biteblob.com sample fingerprints	Domain/Hash	XP95 leak site infrastructure	TH-2026-W18-03
xp95 [BreachForums profile]	Account/Profile	XP95 extortion group	TH-2026-W18-03
com.okta.android.auth/8.19.0 ... Genymobile	User agent	ShinyHunters Okta FastPass enrolment	TH-2026-W18-04
Okta device named "Passkey"	Device name	ShinyHunters FastPass enrolment	TH-2026-W18-04
@bitwarden/cli@2026.4.0	Package version	Shai-Hulud worm supply chain	TH-2026-W18-05
CVE-2026-20122 / -20128 / -20133	CVE	Cisco SD-WAN Manager KEV triple	TH-2026-W18-06
CVE-2026-1834 (Cisco IOS XE WebUI)	CVE	Actively exploited; patch to 17.12.4a/17.9.6/17.6.8	N/A — Patch
CVE-2026-32201 (SharePoint zero-day)	CVE	Actively exploited; ~1,370 unpatched	N/A — Patch
CVE-2024-57726 / -57728 (SimpleHelp RMM)	CVE	DragonForce ransomware precursor	TH-2026-W18-07

11. RECOMMENDATIONS

Immediate (This Week — Priority P1)

- **1. Hunt for RedSun.exe / UnDefend.exe / FunnyApp.exe — NO PATCH:** Two unpatched Microsoft Defender zero-days (RedSun cloud rollback abuse and UnDefend Defender DoS) require manual hunt now. Deploy a Sigma rule for the three filenames in user folders (Downloads, Pictures, AppData) plus Defender mpcmdrun.exe -SignatureUpdate failures. Review every Defender disable / passive-mode transition.

- **2. Patch Microsoft Defender BlueHammer (CVE-2026-33825):** TOCTOU LPE; fixed in Antimalware Platform 4.18.26030.3011. Forces SYSTEM-level escalation when chained with the unpatched zero-days above.
- **3. Patch Cisco IOS XE WebUI (CVE-2026-1834):** Upgrade to 17.12.4a / 17.9.6 / 17.6.8. Disable WebUI on internet-facing devices in the interim ("no ip http server" + "no ip http secure-server"). Audit privilege-15 accounts and unknown GRE tunnels.
- **4. Patch Cisco SD-WAN Manager triple-KEV:** CVE-2026-20122 / -20128 / -20133 (23 April KEV deadline lapsed). Restrict management plane to OOB. Compare vManage configs to last-known-good baseline. Re-key credential storage backend.
- **5. Rotate ALL credentials accessible via @bitwarden/cli@2026.4.0:** If installed between 12:00–14:00 UTC on 22 April, treat the workstation and any CI/CD runners as compromised. Rotate SSH keys, AWS/GCP/Azure tokens, all vault-tier secrets accessible via the CLI.
- **6. Standard Bank / Polmed POPIA s.22 follow-ups:** Re-baseline notification packs against the W18 expanded scope (credit cards, passport/licence imagery, internal SharePoint/OneDrive movement). Polmed: align with SA Health Data Regs first stress test posture.

Short-Term (Next 30 Days)

- Apply Oracle April CPU 2026 (481 patches across the portfolio). Prioritise WebLogic Server, E-Business Suite, Oracle Communications, and database security patches relevant to your environment.
- Patch SimpleHelp RMM (CVE-2024-57726 / -57728) on all MSP / MSSP infrastructure. DragonForce ransomware uses SimpleHelp as initial-access vector for downstream client compromise.
- Implement Okta FastPass enrolment restrictions (corporately managed devices only via Device Trust). Brief helpdesk on ShinyHunters vishing playbook (no MFA reset by phone without verified ticket).
- SharePoint CVE-2026-32201 audit: ~1,370 instances internet-exposed remain unpatched globally. Validate your tenant patch level; confirm no anomalous web-shell traces.
- Implement / re-baseline dark-web monitoring for SA-relevant data (Stats SA, GCRA, Standard Bank, Polmed, ShinyHunters 40-org dump indices).
- Apply CPA Amendment Regulations interpretation: a CPA opt-out registry does NOT substitute POPIA s.69 consent. Audit direct-marketing programmes; reconfirm consent capture.
- Validate SAP data deletion / retention controls: the IR is now auditing deletion logs as part of POPIA compliance posture.

Strategic

- Conduct a Standard Bank-style attack-chain review: model a 3-week dwell-time scenario through SharePoint / OneDrive / Power Apps / Oracle SQL. Standard Bank has substantial security budget and was still compromised internally before detection — most SA enterprises will fare worse against the same chain.
- Map exposure to the ShinyHunters 40-organisation dump (Mytheresa, Zara, Carnival, 7-Eleven, Medtronic, etc.). Inventory corporate accounts at affected partners. Force MFA enrolment review for any employee whose work email surfaced in third-party indices.
- Prepare for SA POPIA amendment passage (R10M cap likely to rise) and direct-marketing enforcement under the gazetted CPA Amendment Regulations. Update privacy programmes to assume future GDPR-tier ceilings.
- POPIA + DORA + GDPR cross-border notification readiness for SA-EU multinationals. With Q1 2026 GDPR fines totalling EUR 68.18M (~4x prior year) and Belgium NIS2 hard deadline now passed, EU enforcement velocity is accelerating; SA-domiciled groups need synchronous notification playbooks.

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 — Standard Bank breach W18 expanded scope (22 Apr) — <https://www.itweb.co.za/>
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. watchTowr — CVE-2026-35616 Fortinet FortiClient EMS Zero-Day Analysis — <https://watchtowr.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/>
46. IR South Africa — Press Release W18 (21-24 Apr) — <https://infoeregulator.org.za/>
47. EDPB — CEF 2026 coordinated transparency enforcement — <https://www.edpb.europa.eu/>
48. Integrity360 — GDPR Q1 2026 fines roundup — <https://www.integrity360.com/>
49. Techmoonshot — Microsoft Defender RedSun / UnDefend / BlueHammer — <https://techmoonshot.com/>
50. Cisco PSIRT — SD-WAN Manager triple-KEV (Apr 2026) — <https://sec.cloudapps.cisco.com/security/center/publicationListing.x>
51. Microsoft MSRC — April Security Update Guide 2026 — <https://msrc.microsoft.com/update-guide/>
52. CISA KEV Catalog — Live Catalogue — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
53. Daily Maverick — SA cyber landscape April 2026 — <https://www.dailymaverick.co.za/>
54. The African Watch — SAPS / Polmed reporting — <https://www.theafricanwatch.com/>
55. Cape Town ETC — SA breach reporting W18 — <https://capetownetc.com/>
56. BleepingComputer — Bitwarden CLI Shai-Hulud (22 Apr) — <https://www.bleepingcomputer.com/>
57. Check Point Research — Q1 2026 attack volume baseline — <https://research.checkpoint.com/>
58. FalconFeeds — ShinyHunters 40-org dump indices — <https://falconfeeds.io/>
59. GuidePoint Security — GRIT Q1 2026 ransomware report — <https://www.guidepointsecurity.com/>
60. ZeroFox — ShinyHunters TTPs (Okta FastPass) — <https://www.zerofox.com/>

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-W18