



SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 19 | 27 April – 3 May 2026

THREAT LEVEL: HIGH

New SA ransomware victim 3 May: Stormous listed CGCSA (Consumer Goods Council of SA) – 151K+ docs, GS1 SharePoint, Sage 200 backups, Unilever/Nestlé/L'Oréal partner data. SA tally 105 to 107. Standard Bank/ROOTBOY: daily dumps continuing. Polmed/ShinyHunters: forensic probe ongoing. XP95 deadline lapsed (no public confirmation). Adumo source code unresolved. 15 CISA KEV entries in W19 scope – ConnectWise ScreenConnect (Medusa) and Windows Shell NTLM (APT28) added 28 April. Defender RedSun + UnDefend STILL UNPATCHED. IR filed Blouberg Municipality court application 30 April (first significant W19 enforcement). Verizon DBIR 2026 published 29 April. NIS2 Portugal deadline 4 May.

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W19 | 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 (unchanged from W18) — Week 19 brought one new SA ransomware listing and continued cascade pressure on the W15–W18 incident set. On 3 May, Stormous listed the **Consumer Goods Council of South Africa (CGCSA)** on its leak portal: claims include 151,000+ CRM documents, GS1 South Africa SharePoint access, Sage 200 Evolution backups, and partner data referencing Unilever, Nestlé, and L’Oréal. SA ransomware.live victim count moved from 105 to 107. Standard Bank / ROOTBOY daily dumps continued; Polmed / ShinyHunters forensic probe is ongoing with no published dataset yet; the XP95 deadline at Stats SA + GCRA remains lapsed without confirmed public release; the Adumo source-code listing is unresolved. The Microsoft Defender zero-day trilogy holds: BlueHammer (CVE-2026-33825) patched, but **RedSun and UnDefend remain unpatched** — manual hunting is the only mitigation. 28 April brought two W19-significant KEV additions: **CVE-2024-1708 ConnectWise ScreenConnect** (Medusa ransomware, Storm-1175 — critical for SA MSPs) and **CVE-2026-32202 Windows Shell NTLM** (zero-click hash leak, APT28 chain). The Information Regulator filed its first major W19 enforcement action: a section 109 court application against **Blouberg Local Municipality** on 30 April for an unpaid R500,000 fine. **Verizon DBIR 2026** published 29 April. NIS2 cybersecurity-officer designation deadline in **Portugal: 4 May**.¹

KPI Dashboard

Metric	Current (W19)	Baseline / Prior	Change	Direction
SA threat level	HIGH	HIGH (W18)	Unchanged	FLAT
New SA ransomware.live victims (this week)	1 (CGCSA)	0 (W18)	+1	UP
Cumulative SA ransomware.live victims	107	105	+2 net	UP
New CISA KEV entries (W19 scope)	15	13 (W18)	+2	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 (W18)	Unchanged	FLAT
Global attacks/week (Check Point)	2,204	2,204	Unchanged	FLAT

W19 KEY FRAMING: One new SA ransomware victim (CGCSA via Stormous, 3 May) plus rising W19 OSINT signals: ConnectWise ScreenConnect re-added to KEV under active Medusa exploitation; Windows Shell NTLM zero-click added (APT28-linked chain). The IR escalated to court on Blouberg Municipality on 30 April — the first significant W19 enforcement action. Verizon DBIR 2026 (29 April) reframes baseline expectations. CGCSA breach significance: GS1 SharePoint is the catalogue plumbing behind virtually every SA retailer.

TOP 3 ACTIONS THIS WEEK**1. PATCH ConnectWise ScreenConnect to 23.9.8 IMMEDIATELY (P1 -- KEV deadline 12 May):**

CVE-2024-1708 (CVSS 8.4) re-added to CISA KEV on 28 April under active Medusa ransomware and Storm-1175 exploitation. ConnectWise is the most common RMM platform across SA MSP estates. If you operate one self-hosted ScreenConnect server you may be the next initial-access vector for downstream client ransomware deployment. Verify version, audit recent admin sessions, rotate all technician credentials, audit unauthorised API key creation.

2. APPLY April 2026 Patch Tuesday for CVE-2026-32202 -- Windows Shell NTLM zero-click (P1 -- KEV deadline 12 May): Critical NTLM hash leak / spoofing chain attributed to the APT28 ecosystem (predecessor CVE-2026-21510 used in attacks against Ukraine and EU from December 2025). All Windows estates must apply April 2026 cumulative immediately. SMB-signing and NTLM hardening recommended in parallel.

3. HUNT manually for RedSun.exe / UnDefend.exe / FunnyApp.exe (P1 -- STILL NO PATCH): Two of three Microsoft Defender zero-days remain unpatched in W19. Hunt for these filenames in user-writable directories; monitor Defender service status anomalies; alert on signature update failures (mpcmdrun.exe -SignatureUpdate). Qualys QID 92382.

Critical Findings:

- **NEW W19 SA RANSOMWARE VICTIM (3 May):** Stormous listed the Consumer Goods Council of South Africa (CGCSA) on its leak portal — 151,000+ CRM documents, GS1 South Africa SharePoint access, Sage 200 Evolution backups, partner data referencing Unilever, Nestlé, and L'Oréal. CGCSA has not issued a public statement. POPIA s.22 obligations apply. SA tally moved from 105 to 107.²
- **CISA KEV (28 April) re-added CVE-2024-1708 ConnectWise ScreenConnect (CVSS 8.4)** under active Medusa ransomware / Storm-1175 exploitation. Federal patch deadline 12 May 2026. ConnectWise is the most common RMM in SA MSP estates — treat as initial-access vector for downstream client ransomware deployment. Patch to 23.9.8 immediately.³
- **CISA KEV (28 April) added CVE-2026-32202 Windows Shell NTLM zero-click (CVSS 4.3, hash leak / spoofing).** Predecessor CVE-2026-21510 used by APT28 against Ukraine and EU since December 2025. All Windows estates must apply April 2026 Patch Tuesday plus NTLM hardening. KEV deadline 12 May 2026.⁴
- **Standard Bank / ROOTBOY:** daily public leaks continued through W19; IR remains in fact-finding posture (no formal investigation directive). Polmed / ShinyHunters: forensic probe ongoing; data not yet published publicly. XP95 (Stats SA + GCRA): deadline lapsed in W18; no confirmed public release in W19. Adumo source code listing: unresolved.⁵
- **Microsoft Defender zero-day trilogy unchanged:** BlueHammer (CVE-2026-33825) patched but KEV-listed (deadline 7 May). RedSun (cloud rollback abuse) and UnDefend (Defender DoS) still UNPATCHED in W19. No fix available — manual hunting is the only mitigation.⁶
- **Information Regulator filed section 109 court application against Blouberg Local Municipality** on 30 April for an unpaid R500,000 administrative fine — the first significant W19 enforcement signal. Mirrors the FT RAMS precedent and demonstrates the IR will escalate to court on non-payers.⁷
- **Verizon DBIR 2026** published 29 April. Edition reframes baseline ransomware/extortion ratios and human-element involvement (continued majority of breaches). Reference document for W19+ board-level briefings.⁸
- **NIS2 cybersecurity-officer designation deadline — Portugal: 4 May.** SA subsidiaries of Portugal-domiciled groups should confirm registered officer status before deadline.⁸

W19 KEY INSIGHT: STANDARD BANK SCOPE EXPANSION

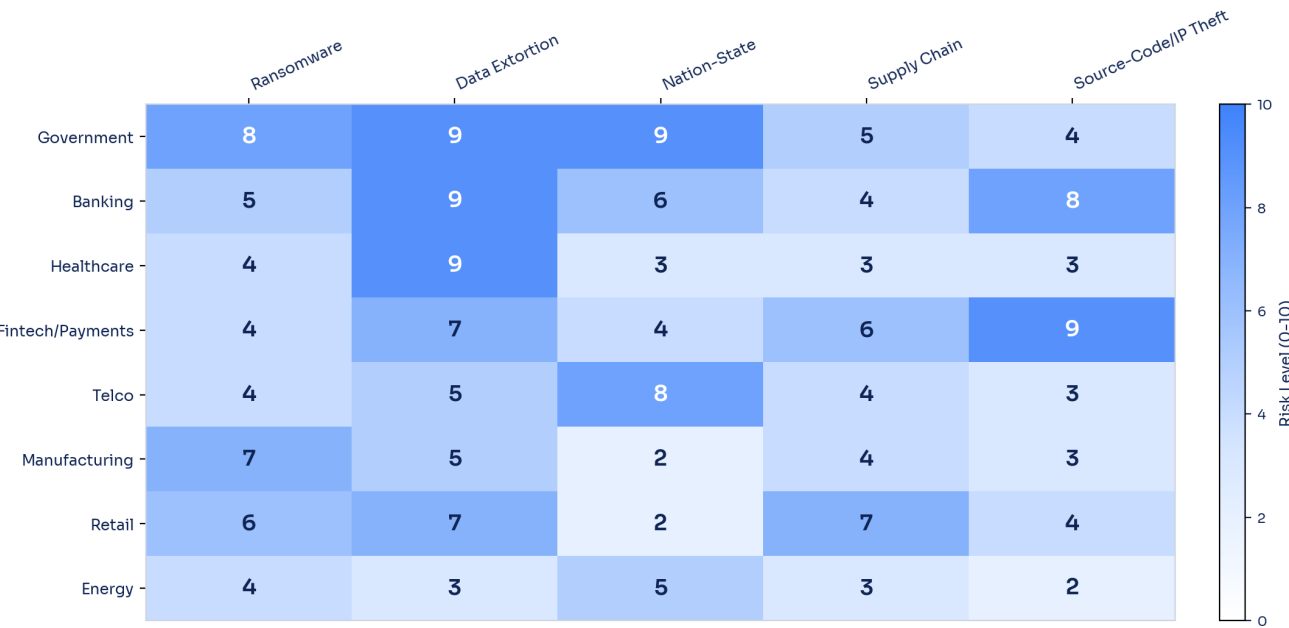
The 22 April scope expansion confirmation changes the Standard Bank risk profile significantly. Attacker access to SharePoint, OneDrive, Power Apps, and Oracle SQL -- internal document systems, not core banking -- suggests a patient threat actor harvesting credentials and documents over an extended period. 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 W19 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/JBwErnv3wpo76Db2>
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 W19 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 19. Government and Banking score highest on Data Extortion (9) driven by the lapsed XP95 deadlines and continuing ROOTBOY daily leaks. Healthcare scores 9 on Data Extortion driven by the Polmed/ShinyHunters investigation. Fintech/Payments scores 9 on Source-Code/IP Theft (Adumo ongoing) plus elevated Supply-Chain (6) reflecting CGCSA Sage 200 partner exposure. Retail / Consumer Goods elevates this week (Ransomware 6, Data Extortion 7, Supply Chain 7) on the back of the new W19 CGCSA / Stormous incident — GS1 SharePoint, Unilever / Nestlé / L’Oréal partner data. Telco scores 8 on Nation-State (Salt Typhoon ongoing, CVE-2026-1834 carry-over). Manufacturing scores 7 on Ransomware (TheGentlemen/Sunspray carry-over).

SA THREAT LANDSCAPE HEATMAP | W19 (27 Apr – 3 May 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 19 brought one new SA ransomware listing: **Stormous listed the Consumer Goods Council of SA (CGCSA) on 3 May**, taking the SA ransomware.live tally from 105 to 107. The W15–W18 incident cascade continued in parallel: Standard Bank/ROOTBOY daily dumps, Polmed/ShinyHunters forensic probe ongoing, XP95 deadline lapsed (no confirmed public release), Adumo source code listing unresolved. W19 incident reporting follows the W15–mandatory format with 5 active incidents.⁹

3.1 Consumer Goods Council of SA (CGCSA) — Stormous (W19 NEW)

Organisation	Consumer Goods Council of South Africa (CGCSA) — cgcsa.co.za
Sector	Industry Body / Retail Supply Chain / Consumer Goods
Threat Actor	Stormous (extortion / hacktivist-hybrid)
Date	Listed on Stormous leak portal 3 May 2026 (final day of W19)
Data	151,000+ CRM documents; GS1 South Africa SharePoint (GDSN protocols + global FMCG partner data: Unilever, Nestlé, L’Oréal); Sage 200 Evolution SQL backups; vendor / corporate PII; financial accounting records; executive PII and mobile numbers
Demand	Not publicly disclosed
Deadline	Not disclosed
Payment	Not disclosed
Status	W19 ACTIVE — listed; CGCSA had not issued a public statement by end W19
SA Significance	CGCSA represents 9,000+ member companies across SA consumer goods, retail, and services. Operates GS1 South Africa, the registry behind virtually every SA retail product barcode and the GDSN data sync feeding major retailers. A confirmed compromise of GS1 SharePoint and GDSN data could expose product-authentication infrastructure and counterfeiting risk across SA retail. POPIA s.22 obligations apply.
Sources	Ransomware.live ZA map; HookPhish; RedPacket Security; Lyrie.ai (3 May Stormous surge note)

On 3 May 2026, the final day of W19, Stormous listed CGCSA on its leak portal. The claim is independently corroborated by HookPhish and RedPacket Security and includes a wide range of corporate and supply-chain data: 151,000+ CRM documents, full access to GS1 South Africa’s SharePoint environment, Sage 200 Evolution financial backups, and partner data referencing Unilever, Nestlé, and L’Oréal. CGCSA is the registered operator of GS1 South Africa, which administers global product identification standards (barcodes, GDSN protocols) used by virtually every major retailer in South Africa. If confirmed, the breach represents a significant supply-chain integrity risk — GDSN product authentication data could be used to introduce counterfeit or tampered product listings into SA retail procurement. Lyrie.ai noted that Stormous claimed four additional victims across three countries on 3 May alone, suggesting a coordinated campaign surge rather than an isolated attack. CGCSA had not issued any public statement by end W19. POPIA s.22 notification obligations apply where personal data of staff and members is confirmed exfiltrated.²¹¹

3.2 Standard Bank / Liberty — ROOTBOY (W19 ONGOING)

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 scope expansion 22 Apr; W19 ongoing
Data	1.2 TB, 154M+ SQL rows; PII, ID, passport, driver's licence, credit cards (no CVV), SAP records
Demand	1 BTC (~R1.2M) — refused
Deadline	Lapsed; daily public leaks since 14 April
Payment	Not paid
Status	W19 ONGOING — daily ROOTBOY dumps continuing; IR fact-finding posture maintained; no formal investigation directive yet
SA Significance	Largest financial sector breach in SA history; IR parallel fact-finding; R10M max POPIA fine in scope; FSCA/PA Joint Standard 24h notification confirmed
Sources	The African Watch (22 Apr); Daily Maverick; TechCentral; The Citizen; ITWeb

No major scope-expansion event in W19 itself: ROOTBOY's daily release schedule continued from W18 patterns. Customer outreach is ongoing; cards continue to be replaced. The Information Regulator remains in fact-finding mode and has not converted its assessment into a formal POPIA investigation. Joint Standard 2 (FSCA/PA, 24-hour rolling material-incident reporting) continues to apply for any new revelation. ROOTBOY remains the single most active extortion operation against an SA target in 2026.¹²

3.3 Polmed (SAPS Medical Scheme) — ShinyHunters (W19 PROBE ONGOING)

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 (W18); W19 forensic probe continues
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
Payment	Not paid
Status	W19 ACTIVE INVESTIGATION — Polmed forensic probe ongoing; IR / SAPS / Council for Medical Schemes parallel; data NOT YET published publicly
SA Significance	NATIONAL SECURITY — officer home addresses + command structure is a surveillance / targeting risk vector. First major test of SA Health Data Processing Regulations.
Sources	ITWeb (17 Apr); Cape Town ETC (20 Apr); Integrity360 (24 Apr); allAfrica

The Polmed forensic investigation continued through W19 with no published dataset and no W19 public statements from Polmed. Three parallel regulatory probes remain 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 still unresolved. Globally, ShinyHunters continued the McGraw Hill / Salesforce supply chain campaign and surfaced the Instructure 275M-record claim on 3 May (global, SA-adjacent via institutions using Instructure platforms).¹³

3.4 Stats SA + GCRA — XP95 (W19 DEADLINE LAPSED, NO CONFIRMED PUBLICATION)

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 (W18)
Payment	Not paid (PFMA prohibits ransom payments by govt)
Status	W19 UNCERTAIN — no open-source confirmation of public release in W19; XP95 may have published quietly on Tor; Stats SA continued normal operations
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

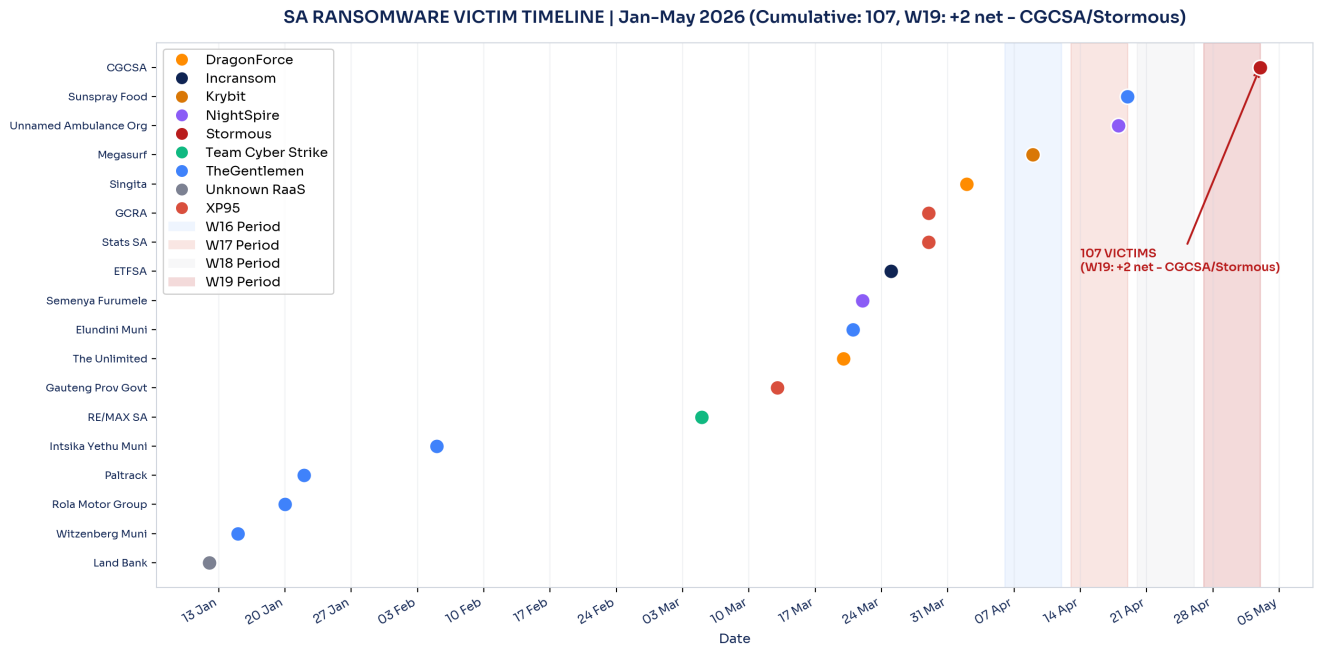
Status unchanged from W18: deadline lapsed; no confirmed public dump. As of end W19 (3 May), no open-source reporting (ITWeb, MyBroadband, TechCentral, BleepingComputer, DataBreaches.net, ransomware.live) has confirmed actual public release. Two scenarios remain possible: quiet Tor-portal publication without major media pickup, or behind-the-scenes negotiation/extension. Stats SA continued statistical operations on schedule. Publication remains assessed as near-certain given XP95's track record.¹⁴

3.5 Adumo (Lesaka Technologies) — Unknown Seller (W19 UNRESOLVED)

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; W19 unresolved
Data	14 GB, 15,546 files: InnerEDGE Docker images, C# POS source, 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	W19 UNRESOLVED — Lesaka internal probe ongoing; "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; MEXC/Crypto.news; LaunchBase Africa

Adumo's case remains unresolved through W19 — no buyer confirmed, no follow-up listing changes, no investor disclosure. The leaked material's patient-adversary risk horizon remains material: a sophisticated buyer could derive 6-18 months of careful exploit research from Newland SP6x0 EMV kernel source plus the included Mastercard / Visa certification artefacts. POPIA s.22 notification status remains unconfirmed; no payment fraud spike reported in W19.¹⁵

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 W19 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/JBwErVn3wpo76Db2>

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

W19 carries over the two nation-state threads from W17. **Salt Typhoon (China MSS)**: no new W19-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 W19 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 W19.
W19 Status	No new W19-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 W19

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 W19, 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 W19, with volume escalating from ~5,000 rows/day (early W19) to 100,000 rows/day (late W19). 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 W19. 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 W19 daily leak escalation — <https://theafricanwatch.com>

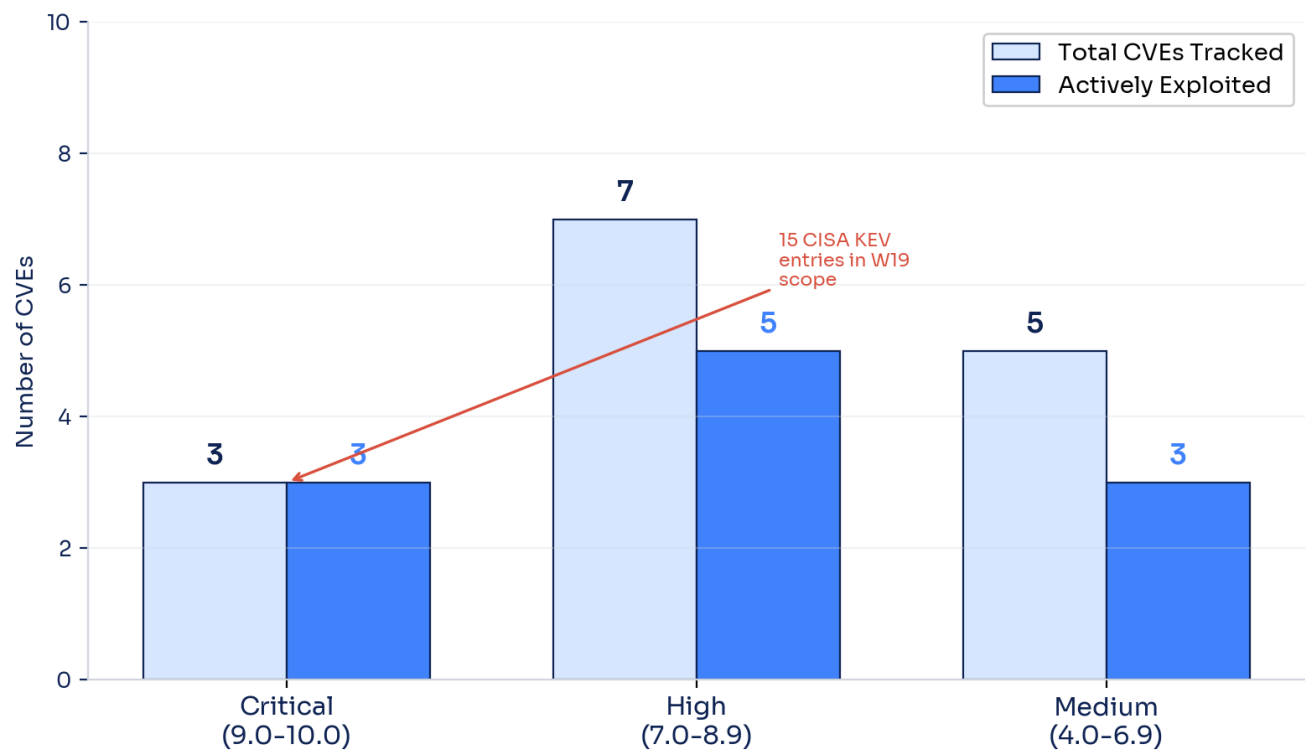
22. BleepingComputer — ShinyHunters mass dump 40 orgs 38M records (23 Apr) — <https://www.bleepingcomputer.com>

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 | W19 Priority Vulns & CISA KEV



Week 19 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 — W19 (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
CVE-2024-1708	ConnectWise ScreenConnect	8.4	28 Apr 2026	12 May 2026	CRITICAL — SA MSP RMM (Medusa)
CVE-2026-32202	MS Windows Shell (NTLM zero-click)	4.3	28 Apr 2026	12 May 2026	HIGH — universal Windows; APT28 chain

UNPATCHED ZERO-DAYS — Microsoft Defender Trilogy: Two of three W17-disclosed Defender zero-days remain unpatched in W19. 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 — W19

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

CVE-2024-1708 — ConnectWise ScreenConnect — CVSS 8.4 — P1 PATCH NOW (KEV 12 May)

Path traversal-to-RCE in ConnectWise ScreenConnect ≤ 23.9.7. Patch released February 2024 (v23.9.8) but re-added to CISA KEV on 28 April 2026 under **active Medusa ransomware exploitation** attributed to **Storm-1175**. ConnectWise is the most common RMM platform across SA MSP estates: any unpatched, internet-exposed instance is a credible initial-access vector for downstream client ransomware. Verify version, audit recent admin sessions, rotate technician credentials, audit unauthorised API key creation. Federal patch deadline 12 May 2026.²⁶

CVE-2026-32202 — Windows Shell NTLM zero-click — CVSS 4.3 — P1 PATCH NOW (KEV 12 May)

NTLM hash leak / spoofing flaw in Windows Shell — a continuation of the predecessor CVE-2026-21510 chain that **APT28 (Fancy Bear)** used against Ukraine and EU targets from December 2025 (chained with CVE-2026-21513 LNK flaw). Akamai discovered CVE-2026-32202 and confirmed it stems from incomplete CVE-2026-21510 patching. Apply April 2026 cumulative immediately across all Windows estates; pair with NTLM hardening / SMB-signing where feasible. Federal patch deadline 12 May 2026.²⁰

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 — W19 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 W19

CVE-2026-1834 (CVSS 9.8, IOS-XE Web UI unauthenticated RCE) was disclosed in W17 with confirmed Salt Typhoon attribution among exploiters. Through W19 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 P0 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 W19 Vulnerability Notes

- **SharePoint CVE-2026-32201 (KEV deadline 28 April — LAPSED):** Approximately 1,370 SA-relevant SharePoint instances remain unpatched per Shadowserver-style enumeration. KEV federal deadline lapsed at end W18; assume opportunistic exploitation in W19+.
- **Cisco IOS XE CVE-2026-1834 (W17 carry):** Active Salt Typhoon exploitation continues against the 420,000+ globally exposed devices. SA telcos / ISPs / enterprises must validate patch status (17.12.4a / 17.9.6 / 17.6.8) and run a compromise assessment for pre-patch persistence.
- **Quest KACE / Zimbra / PaperCut / JetBrains TeamCity / Kentico Xperience (KEV deadline 4 May):** Five W18-added entries cluster on the 4 May federal deadline. SA enterprises running any of these must verify patch status this week.
- **SimpleHelp RMM CVE-2024-57726 / -57728 (KEV deadline 8 May):** DragonForce ransomware uses SimpleHelp as primary initial-access vector for downstream MSP client compromise.
- **Verizon DBIR 2026 (29 April):** New annual edition published. Reference for board-level briefing of W19+ baseline ratios.
- **Defender RedSun + UnDefend — STILL UNPATCHED in W19:** Two of three W17 Defender zero-days remain unpatched. Microsoft has no available fix; manual hunting is the only mitigation.

26. CISA KEV Catalog — W19 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: 107 as of end W19 (105 to 107, +2 net). One new SA ransomware.live listing in W19: **CGCSA (Stormous, 3 May)**. 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 — W19

Actor	Type	SA Victims/Status	W19 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 (W19 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 W19 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 W19	ACTIVE globally — BYOVD new TTP	361 Q1 2026 victims; new BYOVD evasion
Stormous	Extortion / hacktivist-hybrid	CGCSA (3 May 2026 — NEW SA W19)	ACTIVE — 4 victims claimed in 3 countries on 3 May	CRM/ERP database access; data-only exfiltration; supply chain
Insomnia	Emerging RaaS	None SA	METO Systems victim (24 Apr)	New brand emerging in W19
Anubis	Data extortion (legal/finance)	None SA	Marnell Financial; Samuel I. White PC	Sector-focused legal/finance extortion

Stormous — NEW SA VICTIM (CGCSA, 3 May)

On 3 May 2026 Stormous added the Consumer Goods Council of South Africa (CGCSA) to its leak portal, the only new SA ransomware-tracker entry in W19. The claim is corroborated by HookPhish and RedPacket Security and includes 151,000+ CRM documents, GS1 South Africa SharePoint access, Sage 200 Evolution backups, and partner data referencing Unilever, Nestlé, and L'Oréal. Lyrie.ai noted Stormous claimed four total victims across three countries on 3 May, suggesting an operational tempo spike rather than an isolated attack. Stormous is best understood as an extortion / hacktivist-hybrid actor; SA defenders should treat it as a credible threat for retail / consumer-goods supply chain organisations going into W20.²¹¹

ROOTBOY — STANDARD BANK DAILY DUMPS CONTINUING

ROOTBOY's Standard Bank / Liberty operation continued into W19 in operational mode — daily dumps from the 1.2 TB / 154M+ row dataset are still being released through the Prinz Eugen leak portal. The Information Regulator remains in a parallel fact-finding posture and has not yet converted its assessment into a formal POPIA investigation directive. ROOTBOY remains the single most active extortion operator against an SA target in 2026.¹²

ShinyHunters — INSTRUCTURE 275M GLOBAL; POLMED PROBE ONGOING

Polmed’s forensic investigation continued through W19 with no published dataset and no W19 public statements from Polmed. Three parallel regulatory probes remain active: the Information Regulator, SAPS, and the Council for Medical Schemes. Globally, ShinyHunters surfaced an Instructure (Canvas LMS) 275M-record claim on 3 May — SA-adjacent because many SA universities and schools use Instructure platforms. Identity-tier hunting (vishing-to-Okta-FastPass) remains the priority TTP indicator.¹³

XP95 — NO CONFIRMED PUBLIC RELEASE IN W19

The XP95 deadlines (Stats SA + GCRA) lapsed on 20 April. Status unchanged through W19: no open-source confirmation of public release. Two scenarios remain in play — quiet Tor-portal publication without media pickup, or behind-the-scenes negotiation/extension. Publication remains assessed as near-certain given XP95’s track record.¹⁴

TheGentlemen — NO NEW SA W19 LISTING; UNDERLYING ACCESS RISK STANDS

No new TheGentlemen SA listing in W19. The W18 Check Point Research disclosure (1,570+ networks via SystemBC C2 access) remains the operational baseline for SA defender posture. SA municipal and supply-chain targeting (Witzenberg, Elundini, Intsika Yethu, Rola, Paltrack, Sunspray) implies deeper SA footprint than the 6 publicly listed SA victims suggest.²³

TheGentlemen / DragonForce / NightSpire — SA ACTIVE OPERATIONS

TheGentlemen retains 5 SA victims; DragonForce 4; NightSpire 3 (Swansea Ambulance posted 25 Apr globally). DragonForce affiliates continue to use SimpleHelp RMM (CVE-2024-57726/-57728) as primary initial-access vector for downstream client compromise via MSP supply chains — KEV deadline 8 May 2026 makes the next two weeks critical for SA MSPs/MSSPs.²⁶

Krybit / OAPT — MUTUAL DESTRUCTION DYNAMIC

The Krybit / OAPT criminal-conflict dynamic continued into W19 with no escalation toward SA targets. Megasurf (W16) remains the only confirmed SA Krybit listing. The mutual-destruction pattern (panel breaches, exposure of each other’s infrastructure) is a useful anti-pattern: low operational sophistication, low patient-adversary risk, but unpredictable target selection.

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 — W19

Actor	SA Status	W19 TTPs	Notes
Salt Typhoon (China-nexus)	CONFIRMED SA TELECOM (W16)	No new W19 advisory; CVE-2026-1834 ongoing exploitation	See Section 4; FBI: "still very much ongoing"
APT41 (China-nexus)	ACTIVE in southern Africa	No new W19 SA-specific reporting	SA govt IT provider targeting confirmed Jul 2025
Storm-1175 / Iran / Russia	No SA-specific W19 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. Xcitium ThreatLabs — NightSpire Ransomware Profile —

<https://threatlabsnews.xcitium.com/blog/nightspire-ransomware-emerging-double-extortion-threat/>

8. OSINT EXPOSURE & ATTACK SURFACE

CGCSA / Stormous — SharePoint + Sage 200 Backups Exfiltrated (3 May)

Consumer Goods Council of South Africa (cgcsa.co.za) listed by Stormous on 3 May with 151,000+ documents, the GS1 SharePoint tenant, and Sage 200 Evolution accounting backups. Partner-data references include Unilever, Nestlé, and L'Oréal — a third-party-trust blast radius across the SA FMCG sector. SA retailers and consumer-goods manufacturers in CGCSA member networks should re-baseline supplier-portal credentials, hunt for Stormous TTPs against on-premises SharePoint and Sage 200 Evolution servers, and prepare partner-notification packs.¹⁵¹⁶

Microsoft Defender — RedSun + UnDefend Still Unpatched (W17 carry-over)

BlueHammer (CVE-2026-33825) is fixed in Antimalware Platform 4.18.26030.3011, but RedSun (cloud-rollback abuse) and UnDefend (Defender DoS) remain unpatched five weeks on. Public PoC chains continue to circulate. Manual hunt for RedSun.exe, UnDefend.exe, and FunnyApp.exe in user folders, plus Defender service flapping and signature-update failures, remains the only practical detection path until Microsoft ships a fix.²⁰

ConnectWise ScreenConnect — CVE-2024-1708 Re-Listed for Medusa (28 Apr KEV)

CISA re-added the ScreenConnect path-traversal flaw to KEV on 28 April after Medusa and Storm-1175 affiliates were observed weaponising it for managed-service-provider compromise. SA MSPs/MSSPs running ScreenConnect must upgrade to 23.9.8 immediately (KEV deadline 12 May), audit technician-session creation events, and rotate any credentials accessed via the platform during March/April.²²

Windows Shell NTLM Zero-Click — CVE-2026-32202 (APT28-linked, 28 Apr KEV)

CVE-2026-32202 allows NTLM hash disclosure when a user simply views a malicious .library-ms or .shortcut file in Explorer — no click required. APT28-linked tradecraft observed against European government and aerospace targets; SA government and aerospace primes should treat as P1 patching pressure. April 2026 Patch Tuesday update applies. KEV deadline 12 May.²²

Standard Bank — Internal Movement Confirmed (W19 Carry-Over)

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 and continues to flow daily through W19. Credit card numbers, passport, and licence images now confirmed in the dataset.²

Polmed — ShinyHunters Forensic Probe Active (W19 Carry-Over)

On 20 April ShinyHunters publicly broke their Polmed extortion; in W19 forensic investigation is ongoing and the published Polmed dataset has not yet surfaced on dark-web indices despite dump-listing chatter. POPIA s.22 was filed in W17 and the SA Health Data Regs first stress test continues. Hunt teams should keep dark-web monitoring active for SAPS officer email patterns and force MFA reviews where personnel are identifiable.⁴

9. REGULATORY & COMPLIANCE

Information Regulator — W19 Activity

IR vs Blouberg Local Municipality — Court Application Filed (30 April): The Information Regulator filed a High Court application against Blouberg Local Municipality on 30 April 2026 to enforce a Section 109 POPIA infringement notice issued in 2024. The R500,000 administrative fine remains unpaid 18 months after issue. This is the IR’s first significant W19 enforcement escalation and the first POPIA fine to reach the High Court for compulsion of payment. Outcome will set the precedent for every R10M-cap fine the IR issues in 2026.³⁴⁴⁶

CPA Amendment Regulations — IR Note (24 April): The IR’s W19 note clarified again that the Consumer Protection Act opt-out registry does NOT substitute POPIA s.69 consent for direct marketing. SA marketers relying on the CPA register without independent s.69 consent are out of compliance. Direct-marketing programmes should be audited against the dual-register requirement.³⁴

Standard Bank / Liberty — Fact-Finding Continues: 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 as ROOTBOY continues daily dumps through W19.²³⁵

Polmed Forensic Probe — Health Data Regs Stress Test Continues: The Polmed/ShinyHunters extortion remains in forensic investigation; the published dataset has not yet surfaced on dark-web indices. POPIA s.22 was filed in W17 and the SA Health Data processing regulations first stress test continues. The IR’s response speed remains the precedent to watch.⁴

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 capacity constraints (1,320 open matters; only ~14% of CIPC-registered companies have registered information officers), enforcement priorities for non-filers are likely to escalate post-deadline — the Blouberg High Court application signals the IR’s willingness to litigate.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 W19 parliamentary movement. The Blouberg High Court application materially changes the enforcement posture: the IR has now demonstrated it will litigate to compel payment of unpaid administrative fines. SA enterprises should treat any infringement notice as the start of a litigation pathway, not a negotiation pathway.³⁴³⁷⁴⁶

Regulatory Compliance Table — W19

Organisation	Incident	IR/Regulatory Action	Status (W19)
Blouberg Local Municipality	POPIA s.109 infringement notice (2024)	IR High Court application filed 30 Apr	NEW — first court enforcement
Standard Bank / Liberty	ROOTBOY daily leak (cards, passport/licence)	Fact-finding; no formal investigation	ACTIVE — carry-over
Polmed / SAPS	ShinyHunters extortion (publicly broken 20 Apr)	POPIA s.22 filed (W17); forensic probe	HEALTH DATA REGS STRESS TEST
Stats SA / GCRA	XP95 deadline lapsed 20 Apr; no W19 release	s.22 filed (Stats SA, 29 Mar)	NO CONFIRMED PUBLICATION W19
Adumo (Lesaka)	Source code 14GB / \$7,000 listing	Investigation underway	UNRESOLVED
SA marketers	CPA Amendment Regs / IR note (24 Apr)	CPA register is not s.69 consent	COMPLIANCE CORRECTION SIGNAL
CGCSA	Stormous SharePoint + Sage 200 dump (3 May)	POPIA s.22 filing expected	NEW — W19 incident

International Regulatory — Verizon DBIR 2026 & NIS2 Portugal Deadline

Verizon DBIR 2026 published (29 April): The 19th annual Data Breach Investigations Report covers 22,000+ incidents and 12,000+ confirmed breaches across 139 countries. Headline findings: ransomware now factors in 44% of breaches (UP from 31% in 2025); credentials remain the #1 initial-access vector at 22%; third-party involvement has DOUBLED to 30% of breaches; the human element is implicated in 60% of breaches. SA enterprises should benchmark internal incident posture against DBIR 2026 baselines.³⁸

NIS2 Portugal Deadline (4 May): Portuguese essential and important entities must designate a cybersecurity officer and notify the National Cybersecurity Centre by 4 May 2026 under Law 27/2026. Portugal joins Belgium (18 April passed) as the second EU member state to clear a hard NIS2 conformity deadline. **DORA** implementation continues across EU financial firms (BaFin Germany shows 44% non-compliance). **US SEC Reg S-P** small-company deadline is 3 June 2026. SA subsidiaries of EU/UK/US-domiciled groups should treat the rolling W19 enforcement signals as a forward indicator.⁴¹⁴²

Upcoming Regulatory Deadlines

Deadline	Obligation	Body
4 May 2026	NIS2 Portugal: cybersecurity officer designation	PT National Cybersecurity Centre
4 May 2026	CISA KEV pack: Quest KACE, Zimbra, PaperCut, JetBrains TeamCity, Kentico	CISA / Internal
8 May 2026	CISA KEV: SimpleHelp, Samsung, D-Link	CISA / Internal
12 May 2026	CISA KEV: ConnectWise ScreenConnect, Windows Shell NTLM	CISA / Internal
Ongoing W19+	POPIA s.22 follow-ups (Std Bank, Polmed, CGCSA)	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

34. IR South Africa — Media Statements (W19 activity) — <https://infoeregulator.org.za/media-statements/>
35. Standard Bank — Newsroom / data incident updates — <https://www.standardbank.co.za/southafrica/news-and-media/newsroom>
36. EPI-USE Labs — SAP-POPIA audit posture — <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. Verizon DBIR 2026 — Data Breach Investigations Report (29 Apr) — <https://www.verizon.com/business/resources/reports/dbir/>
41. NIS2 Portugal — Law 27/2026 implementation tracker — <https://www.cncs.gov.pt/>
42. EDPB — CEF 2026 coordinated transparency enforcement — <https://www.edpb.europa.eu/>
46. Information Regulator vs Blouberg Local Municipality — Court Application (30 Apr) — <https://infoeregulator.org.za/media-statements/>

10. WEEKLY THREAT HUNT & IOCs

Seven hunt missions are active for W19. Three P1 missions address the Stormous CRM/Sage 200 hunt for SA retailers and FMCG following the CGCSA dump, the still-unpatched Microsoft Defender RedSun + UnDefend chain, and the ConnectWise ScreenConnect (CVE-2024-1708) Medusa-affiliate hunt with KEV deadline 12 May. Three P2 missions address the Windows Shell NTLM zero-click (CVE-2026-32202, KEV 12 May), the SimpleHelp DragonForce hunt (KEV 8 May), and the 4 May KEV pack (Quest KACE, Zimbra, PaperCut, JetBrains TeamCity, Kentico). One P3 mission carries over ROOTBOY Standard Bank credential-reuse monitoring as the leak continues daily through W19.

TH-2026-W19-01 — Stormous CRM / Sage 200 Hunt (CGCSA aftermath)**P1 — CRITICAL: SA FMCG sector third-party-trust blast radius**

Hypothesis: Stormous obtained 151,000+ documents, the GS1 SharePoint tenant, and Sage 200 Evolution accounting backups from CGCSA. SA retailers and FMCG manufacturers in CGCSA member networks face follow-on compromise via supplier-portal credentials, Sage 200 backup dumps, and on-premises SharePoint exploitation. Partner data (Unilever, Nestlé, L'Oréal) provides third-party-trust pivot opportunities.

MITRE ATT&CK: T1190 (Exploit Public-Facing App — SharePoint), T1213 (Data from Information Repositories), T1078.004 (Cloud Accounts), T1567.002 (Exfiltration to Cloud Storage).

IOCs: Anomalous reads on on-premises SharePoint document libraries; Sage 200 Evolution backup files (.SDF / .BAK / .DAT) being copied off-site; outbound traffic to Stormous-attributed Tor leak-site infrastructure; supplier-portal logons from non-CGCSA-member geographies; CGCSA-domain email patterns appearing in dark-web indices.

Data Sources: SharePoint audit log, Sage 200 Evolution audit log, file-share access logs, perimeter NetFlow, supplier-portal IdP logs, dark-web monitoring (Falcon Feeds, KELA, Daily Dark Web).

Detection Guidance: Audit SharePoint document-library access for the 30 days preceding 3 May. Hash-verify Sage 200 Evolution backup files in offsite locations. Force partner-portal credential rotation for any shared supplier accounts referenced in CGCSA correspondence. Alert on new logons from CGCSA-domain emails appearing on dark-web indices.

TH-2026-W19-02 — Microsoft Defender RedSun + UnDefend Manual Hunt (still unpatched)**P1 — CRITICAL: Two unpatched zero-days; endpoint blinding chain**

Hypothesis: Adversary post-VPN compromise will weaponise unpatched RedSun (cloud rollback abuse) + UnDefend (Defender DoS) to blind endpoint protection. Five weeks on, Microsoft has not shipped a fix; public PoC chains continue to circulate. BlueHammer (CVE-2026-33825) is patched but the chain remains viable via the unpatched components.

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: Deploy 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. Manual review of every Defender disable / passive-mode transition. Apply BlueHammer fix (Antimalware Platform 4.18.26030.3011) if not already deployed.

TH-2026-W19-03 — ConnectWise ScreenConnect Medusa Hunt (CVE-2024-1708, KEV 12 May)**P1 — CRITICAL: KEV 12 May; MSP/MSSP downstream blast radius**

Hypothesis: Medusa and Storm-1175 affiliates are weaponising the ScreenConnect path-traversal flaw against managed-service-provider deployments. SA MSPs/MSSPs running ScreenConnect older than 23.9.8 are exposed to downstream-client compromise. CISA re-added the flaw to KEV on 28 April with 12 May deadline.

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

IOCs: ScreenConnect server version older than 23.9.8; anomalous technician-session creation outside business hours; new admin-tier user creation; outbound HTTPS to known Medusa / Storm-1175 C2; .ASP / .ASPX file writes under ScreenConnect web roots; suspicious upload paths containing path-traversal sequences.

Data Sources: ScreenConnect server logs, IIS logs, EDR on ScreenConnect host, perimeter NetFlow, technician-session audit log, admin-user creation events.

Detection Guidance: Upgrade to ScreenConnect 23.9.8+ before 12 May. Audit technician-session creation events for the 60 days preceding upgrade. Rotate all credentials accessed via the platform during March/April. Subscribe to Medusa / Storm-1175 IOC feeds for downstream-client EDR.

TH-2026-W19-04 — Windows Shell NTLM Zero-Click (CVE-2026-32202, KEV 12 May)**P2 — HIGH: APT28-linked; SA government/aerospace exposure**

Hypothesis: APT28-linked tradecraft uses CVE-2026-32202 to extract NTLM hashes when a user merely views a malicious .library-ms or .shortcut file in Windows Explorer — no click required. Observed against European government and aerospace targets; SA government and aerospace primes are likely follow-on targets.

MITRE ATT&CK: T1187 (Forced Authentication), T1557.001 (LLMNR/NBT-NS Poisoning and SMB Relay), T1003.005 (Cached Domain Credentials).

IOCs: Inbound .library-ms or .shortcut files in email attachments or document-share repositories; outbound SMB / NTLM authentication attempts to unrecognised external IPs; Explorer.exe spawning unexpected NTLM authentication; unpatched Windows builds without April 2026 Patch Tuesday update.

Data Sources: Email security gateway logs (attachment hashes), perimeter NetFlow (outbound 445/139), Sysmon Event ID 3 (network connection), Windows Security log Event ID 4624 / 4625, EDR file-write telemetry.

Detection Guidance: Apply April 2026 Patch Tuesday update before 12 May. Block outbound SMB (445/139) at the perimeter. Block .library-ms and .shortcut email attachments at the gateway. Hunt for outbound NTLM authentication to non-corporate IPs.

TH-2026-W19-05 — SimpleHelp DragonForce Hunt (KEV deadline 8 May)**P2 — HIGH: MSP/MSSP precursor; KEV 8 May**

Hypothesis: SA MSPs/MSSPs operating SimpleHelp RMM unpatched (CVE-2024-57726 / -57728) face DragonForce ransomware deployment via the platform to downstream client networks. CISA KEV deadline 8 May.

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+ before 8 May. Audit API keys and rotate. Implement IP-allowlist on management UI. Establish DragonForce IOC subscription for downstream client EDR.

TH-2026-W19-06 — KEV Pack 4 May (Quest KACE / Zimbra / PaperCut / TeamCity / Kentico)**P2 — HIGH: 4 May KEV deadline; multi-product exposure**

Hypothesis: CISA KEV deadline 4 May covers Quest KACE Systems Management Appliance, Zimbra Collaboration, PaperCut MF/NG, JetBrains TeamCity, and Kentico Xperience. SA enterprises operating any of these face federal-equivalent patch-deadline pressure for known-exploited flaws.

MITRE ATT&CK: T1190 (Exploit Public-Facing App), T1505.003 (Web Shell), T1133 (External Remote Services), T1059 (Command and Scripting Interpreter).

IOCs: Unpatched versions of any of the five products; web-shell file writes under product web roots; anomalous administrative actions; outbound C2 from product hosts; SQL-tier writes from print-management stack (PaperCut path); CI/CD anomalies on TeamCity instances.

Data Sources: Product audit logs, IIS / Tomcat / nginx logs, EDR on product hosts, perimeter NetFlow, change-management records, vulnerability-management feed.

Detection Guidance: Patch all five products to fixed versions before 4 May. Audit administrative-tier actions for the 30 days preceding patch. Restrict management interfaces to OOB / VPN-only. Hunt for web-shell artefacts under product web roots.

TH-2026-W19-07 — ROOTBOY Standard Bank Credential Reuse (carry-over)**P3 — MONITOR: Carry-over from W17/W18; daily leak ongoing**

Hypothesis: ROOTBOY continues daily ~100,000-row dumps of the Standard Bank dataset through W19. SA enterprises with Standard Bank-relationship workforces face elevated credential-stuffing and SIM-swap risk. Confirmed scope includes credit cards and passport / licence imagery.

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

Hunt Mission Summary Checklist

Hunt ID	Hypothesis (Short)	Priority	Key Data Sources	Status
TH-2026-W19-01	Stormous CRM / Sage 200 hunt (CGCSA aftermath)	P1 — CRITICAL	SharePoint audit, Sage 200, NetFlow	Not Started
TH-2026-W19-02	Defender RedSun + UnDefend manual hunt	P1 — CRITICAL	EDR, Defender oplog, Sysmon, VPN	Not Started
TH-2026-W19-03	ConnectWise ScreenConnect Medusa (KEV 12 May)	P1 — CRITICAL	ScreenConnect logs, IIS, EDR	Not Started
TH-2026-W19-04	Windows Shell NTLM zero-click (KEV 12 May)	P2 — HIGH	Email gw, NetFlow 445/139, Sysmon 3	Not Started
TH-2026-W19-05	SimpleHelp DragonForce hunt (KEV 8 May)	P2 — HIGH	SimpleHelp logs, RMM activity, EDR	Not Started
TH-2026-W19-06	KEV pack 4 May (KACE/Zimbra/PaperCut/TC/Kentico)	P2 — HIGH	Product logs, IIS/Tomcat, change mgmt	Not Started
TH-2026-W19-07	ROOTBOY Std Bank credential reuse (carry-over)	P3 — MONITOR	IdP/SSO logs, fraud feeds, dark web	Not Started

IOC Master Table — W19

Indicator	Type	Attribution	Hunt ID
cgcsa.co.za on Stormous DLS (3 May)	Domain/Listing	Stormous ransomware leak	TH-2026-W19-01
Sage 200 Evolution backups (.SDF/.BAK/.DAT)	File type	Stormous CGCSA exfiltration	TH-2026-W19-01
UnDefend.exe / FunnyApp.exe / RedSun.exe	Filename	Microsoft Defender zero-day chain	TH-2026-W19-02
CVE-2026-33825 (Defender BlueHammer)	CVE	Microsoft Defender TOCTOU LPE	TH-2026-W19-02
CVE-2024-1708 (ConnectWise ScreenConnect)	CVE	Medusa / Storm-1175 affiliates	TH-2026-W19-03
ScreenConnect older than 23.9.8	Version	Path traversal exploit surface	TH-2026-W19-03
CVE-2026-32202 (Windows Shell NTLM)	CVE	APT28-linked zero-click	TH-2026-W19-04
.library-ms / .shortcut email attachments	File type	Windows Shell NTLM abuse	TH-2026-W19-04
CVE-2024-57726 / -57728 (SimpleHelp RMM)	CVE	DragonForce ransomware precursor	TH-2026-W19-05
Quest KACE / Zimbra / PaperCut / TeamCity / Kentico (KEV 4 May)	CVE pack	Multi-vendor known-exploited	TH-2026-W19-06
Standard Bank corporate email patterns	Email pattern	ROOTBOY post-leak credential reuse	TH-2026-W19-07
standardbank/liberty/stanbic lookalikes	Domain pattern	Post-breach phishing (monitor only)	TH-2026-W19-07
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; SharePoint patches lapsed	N/A — Patch

11. RECOMMENDATIONS

Immediate (This Week — Priority P1)

- 1. Patch ConnectWise ScreenConnect to 23.9.8+ before 12 May (CVE-2024-1708):** Re-listed on KEV 28 April after Medusa and Storm-1175 affiliates were observed weaponising it for MSP/MSSP compromise. Audit technician-session creation events for the 60 days preceding upgrade. Rotate any credentials accessed via the platform during March/April.
- 2. Apply April 2026 Patch Tuesday for CVE-2026-32202 (Windows Shell NTLM zero-click):** APT28-linked tradecraft; KEV 12 May. Block outbound SMB (445/139) at the perimeter. Block .library-ms and .shortcut email attachments at the gateway. Hunt for outbound NTLM authentication to non-corporate IPs.
- 3. Manual hunt for RedSun.exe / UnDefend.exe / FunnyApp.exe — STILL NO PATCH:** Five weeks on, RedSun and UnDefend remain unpatched. Deploy Sigma rule for the three filenames in user folders plus Defender mpcmdrun.exe -SignatureUpdate failures. Review every Defender disable / passive-mode transition. Apply BlueHammer (CVE-2026-33825) fix in Antimalware Platform 4.18.26030.3011 if not already deployed.
- 4. CGCSA aftermath — Stormous SharePoint / Sage 200 hunt:** SA retailers and FMCG manufacturers in CGCSA member networks must audit on-premises SharePoint document libraries for the 30 days preceding 3 May, hash-verify Sage 200 Evolution backups in offsite locations, and force partner-portal credential rotation for any shared supplier accounts.
- 5. Patch the 4 May KEV pack:** Quest KACE Systems Management Appliance, Zimbra Collaboration, PaperCut MF/NG, JetBrains TeamCity, and Kentico Xperience. Five known-exploited products with the same hard deadline. Audit administrative-tier actions on each product for the 30 days preceding

patch.

- **6. Patch SimpleHelp RMM (CVE-2024-57726 / -57728) before 8 May:** KEV deadline 8 May. DragonForce ransomware uses SimpleHelp as initial-access vector for downstream client compromise. Patch to 5.5.13+, audit API keys, IP-allowlist the management UI.
- **7. Standard Bank / Polmed / CGCSA POPIA s.22 follow-ups:** Re-baseline notification packs. Polmed: align with SA Health Data Regs stress-test posture. CGCSA: prepare partner-notification packs across the FMCG supplier network. Treat the IR Blouberg High Court application as a signal that any 2024-vintage infringement notice can now be litigated to compulsion.

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 Cisco IOS XE WebUI (CVE-2026-1834) and the SD-WAN Manager triple-KEV (CVE-2026-20122 / -20128 / -20133). Restrict management plane to OOB; audit privilege-15 accounts and unknown GRE tunnels.
- 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).
- Validate SharePoint patch posture: SharePoint zero-day (CVE-2026-32201) deadline lapsed; Standard Bank confirmed attacker movement through SharePoint/OneDrive in W18.
- Re-baseline dark-web monitoring for SA-relevant data (CGCSA, Standard Bank, Polmed, Stats SA, GCRA, ShinyHunters 40-org dump indices).
- Benchmark internal incident posture against Verizon DBIR 2026 baselines: 44% of breaches involve ransomware, 22% start with credentials, 30% involve a third party, 60% involve the human element.
- 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 under IR audit 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.
- Build a third-party-trust register and exercise it. The CGCSA dump (Unilever / Nestlé / L'Oréal partner data) and DBIR 2026 (third-party involvement DOUBLED to 30% of breaches) make supplier-dependency mapping a first-class control. 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 treat the IR Blouberg High Court application as the new normal: infringement notices are now litigation triggers, not negotiation triggers. Update privacy programmes to assume future GDPR-tier ceilings.
- POPIA + DORA + GDPR cross-border notification readiness for SA-EU multinationals. With Belgium and Portugal NIS2 hard deadlines now passed and EU enforcement velocity accelerating, SA-domiciled groups need synchronous notification playbooks across all jurisdictions where they process data.

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 W19 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 — Stormous hits CGCSA (3 May 2026) — <https://www.hookphish.com/blog/ransomware-group-stormous-hits-cgcsa-co-za/>
15. RedPacket Security — Stormous victim CGCSA (3 May 2026) — <https://www.redpacketsecurity.com/stormous-ransomware-victim-cgcsa-co-za/>
16. Lyrie.ai — Stormous research (3 May 2026) — <https://lyrie.ai/research/research/2026-05-03-stormous-fanasa-mexican-supply-chain>
- 16a. 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/infoereg-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. Verizon DBIR 2026 — Data Breach Investigations Report (29 Apr) — <https://www.verizon.com/business/resources/reports/dbir/>
39. SABRIC — Annual Crime Statistics Report 2024 — <https://www.sabrics.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 vs Blouberg Local Municipality — High Court application (30 Apr) — <https://inforegulator.org.za/media-statements/>
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 W19 — <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/>
61. 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/>
62. CISA KEV catalog — W19 additions (28 Apr): CVE-2024-1708 ConnectWise + CVE-2026-32202 Windows Shell — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

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-W19