SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief — Week 11 | 7–13 March 2026

THREAT LEVEL: ELEVATED

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Generated: 13 March 2026

Report ID: DP-CTI-2026-W11 | Classification: TLP:WHITE

1. Table of Contents

2. Executive Summary

Overall Threat Level: ELEVATED — South Africa's cyber threat environment remains under sustained pressure from ransomware operators, state-sponsored espionage groups, and financially motivated criminal networks. This week's dominant stories include the parliamentary disclosure of the Land Bank ransomware attack, the discovery of Lynx ransomware targeting Lion of Africa Insurance, and confirmation that Salt Typhoon continues targeting SA telecoms.

3 hrs SA org breach frequency	**2,145/wk** Cyberattacks targeting SA (Jan 2026, +36% YoY)	**2,898** POPIA breach notifications (2025/26 YTD)
R24M Average ransomware recovery cost	**91** Total SA ransomware victims tracked	

Key Findings

- **Land Bank ransomware** disclosed in parliament — 5 BTC ransom demanded; no payment made; board/HR/governance data exfiltrated.[1]
- **Lynx ransomware** hit Lion of Africa Insurance (discovered 13 March 2026) — double extortion; .LYNX file encryption.[2]
- **Salt Typhoon** (China) confirmed targeting SA telecoms — 200+ companies breached globally; FBI says threat is "still very much ongoing".[3]
- **New POPIA health data regulations** in force since 6 March 2026 — immediate compliance required; R10M penalties for non-compliance.[4]
- **Google Chrome zero-days** (CVE-2026-3909, CVE-2026-3910), **Cisco CVSS 10.0 flaws**, and **Microsoft Patch Tuesday** (84 CVEs) demand urgent patching.[5]

KEY RECOMMENDATION: Patch Cisco Secure FMC (CVSS 10.0), Chrome zero-days, and Microsoft March updates immediately. Block Lynx and RedNovember IOCs at perimeter. Review health data processing operations for new POPIA regulations. Verify MFA is enforced on all VPN appliances.

[1] ITWeb — Land Bank ransomware, https://www.itweb.co.za/article/land-bank-tightens-security-after-ransomware-attack/raYAyMorlOl7J38N
[2] Ransomware.live — Lion of Africa / Lynx, https://www.ransomware.live/id/QWZyaWNhIEluc3VyYW5jZUBseW54
[3] TechCrunch — Salt Typhoon global telecom hack, https://techcrunch.com/2026/03/09/salt-typhoon-china-who-has-been-hacked-global-telecom-giants/
[4] ITLawCo — POPIA health data regulations 2026, https://itlawco.com/popia-health-data-regulations-2026/
[5] BleepingComputer — Chrome zero-days, https://www.bleepingcomputer.com/news/google/google-fixes-two-new-chrome-zero-days-exploited-in-attacks/

3. SA Cyber Incidents & Breaches

3.1 Land Bank Ransomware Attack

The Land and Agricultural Development Bank of South Africa suffered a ransomware attack on **12 January 2026**, disclosed publicly through Finance Minister Enoch Godongwana's parliamentary reply on **7–9 March 2026**.[6] The attackers demanded **5 Bitcoin (~R5.4 million)**; the bank confirmed no ransom was paid.[7]

Attack Date	12 January 2026
Disclosure	7–9 March 2026 (parliamentary reply)
Attack Type	Ransomware (RaaS model, double extortion)
Ransom	5 BTC (~R5.4M) — NOT paid
Threat Actor	Unidentified RaaS group
Initial Access	Vulnerability on internet-facing server
Systems Affected	Non-SAP servers encrypted; laptops encrypted; file server exfiltrated
Data Exfiltrated	Board/committee docs, corporate governance, HR records, organisational records
Regulatory	SAPS (17 Jan), Info Regulator (16 Jan), Prudential Authority (29 Jan), SSA (9 Feb)

3.2 Unnamed SA Bank — Ransomware

A separate unnamed major South African bank reportedly suffered a double-extortion ransomware attack in early 2026. The incident caused intermittent ATM outages, disrupted online banking sessions, and delayed card transactions at retail POS terminals nationwide.[8] The bank has not been publicly identified.

3.3 Insider Threat Landscape

Mimecast research published 5 March 2026 found that **46% of SA organisations** report increased malicious insider incidents, with an average of 6 insider-related incidents per month — matching the negligent/accidental mistake rate for the first time.[9]

3.4 Breach Frequency & Trends

Tanosec's 2026 Annual Threat Intelligence Report documents a **60% surge in data breaches** in South Africa.[10] IT-Online/Palo Alto Unit 42 reporting (11 March) confirms SA organisations are being **breached every 3 hours**, with identity weaknesses present in ~90% of breaches. The Information Regulator receives approximately **284 breach notifications per month**.[11]

[6] ITWeb — Land Bank tightens security, https://www.itweb.co.za/article/land-bank-tightens-security-after-ransomware-attack/raYAyMorlOl7J38N
[7] IOL — Land Bank ransomware, R5.4M ransom, https://iol.co.za/business/2026-03-09-ransomware-attack-on-land-bank-hackers-demand-r54-million-confirms-godongwana/
[8] Priviso — SA bank ransomware analysis, https://www.priviso.co.za/insights/south-africa-bank-ransomware-2026.html
[9] Memeburn — Insider threats SA, https://memeburn.com/2026/03/insider-threats-south-africa/
[10] Tanosec — 60% surge in SA breaches, https://www.facebook.com/mycitybfn/posts/tanosecs-2026-annual-threat-intelligence-report-documents-a-60-surge-in-data-bre/924917166912595/
[11] IT-Online — SA breached every 3 hours, https://it-online.co.za/2026/03/11/sa-organisations-are-breached-every-three-hours/

4. Active Threat Campaigns

4.1 Salt Typhoon (China) — Telecom Espionage

Salt Typhoon (aka GhostEmperor, FamousSparrow) has breached **200+ companies globally across 80+ countries**, including confirmed SA telecom targeting.[12] The FBI confirmed in February 2026 that the threat is "still very much ongoing".[13]

TTPs: Exploitation of Cisco IOS-XE routers at network perimeter; targeting LAWFUL INTERCEPT systems; passive intelligence collection (metadata, call records, network topology); silent operation without disruptive payloads; access maintained for months to years. **MITRE ATT&CK:** T1190 (Exploit Public-Facing Application), T1557 (Adversary-in-the-Middle).

4.2 RedNovember (China-linked) — SSA Breach Allegation

RedNovember (TAG-100, Storm-2077) is alleged to have breached the South African State Security Agency (SSA) in September 2025.[14] The group exploits perimeter VPN appliances (SonicWall, Cisco ASA, Fortinet, Palo Alto) and deploys the Go-based **Pantegana** backdoor, **Cobalt Strike**, and **SparkRAT** via **LESLIELOADER** phishing payloads.[15]

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1071 (Application Layer Protocol), T1059.001 (PowerShell), T1105 (Ingress Tool Transfer), T1583 (Acquire Infrastructure).

4.3 APT41 / Brass Typhoon (China) — Government Espionage

APT41 (Wicked Panda, Barium) targeted government IT services in Southern Africa in July 2025 — the first confirmed activity from this APT in Africa.[16] TTPs include custom malware deployment, credential harvesting, and long-term dwell-time persistence. **MITRE ATT&CK:** T1078 (Valid Accounts), T1555 (Credentials from Password Stores).

4.4 Kasablanka — Emerging North African APT

Kasablanka, a Morocco-origin group, is transitioning from hacktivism to espionage. Active since 2021, it targets North African government/energy sectors using spearphishing, **QuasarRAT**, **njRAT**, and C2 via Telegram bots with domain fronting.[17] Expanding operational profile increases future SA government targeting risk.

4.5 Russia & Iran — Global Campaigns with SA Exposure

Google Threat Intelligence Group advisory (February 2026) warned of 8 Russia-linked actors, China-linked zero-day exploitation groups, and Iranian threat actors using spoofed job portals — all with indirect SA exposure risk due to underfunded defences and shared supply chains.[18]

[12] TechCrunch — Salt Typhoon global list, https://techcrunch.com/2026/03/09/salt-typhoon-china-who-has-been-hacked-global-telecom-giants/
[13] CyberScoop — FBI Salt Typhoon ongoing, https://cyberscoop.com/fbi-salt-typhoon-ongoing-threat-cybertalks-2026/
[14] TechCabal — Africa breaches 2025, https://techcabal.com/2025/12/30/cyber-breaches-became-harder-to-hide/
[15] Recorded Future — RedNovember research, https://www.recordedfuture.com/research/rednovember-targets-government-defense-and-technology-organizations
[16] Africa Defense Forum — APT41 Southern Africa, https://adf-magazine.com/2025/08/prolific-chinese-cyber-espionage-group-attacks-southern-africa/
[17] BrandDefense — Kasablanka APT, https://brandefense.io/blog/kasablanka-apt-group/

[18] ITWeb — SA cyber defences exposed, https://www.itweb.co.za/article/sas-cyber-defences-exposed-as-global-threats-intensify/dgp45qaBbB5vX9I8

5. Ransomware Activity

5.1 Lynx — Lion of Africa Insurance (March 2026)

Lynx ransomware (rebranded INC Ransomware, RaaS) attacked **Lion of Africa Insurance Company Ltd** (Sandton, 100–249 employees). Estimated attack date: 6 March; discovered 13 March 2026.[19] Lynx employs double extortion — encrypts files with .LYNX extension (AES + Curve25519 key exchange) and exfiltrates data. Uses Restic for exfiltration and SoftPerfect NetScan for discovery.

5.2 LockBit 5 — Diesel-Electric Group / Bosch SA

LockBit 5 targeted the Diesel-Electric Group (Bosch Service Dealers, e-CAR Service Centers). Discovery date: 1 March 2026; estimated attack: 26 February 2026.[20]

5.3 The Gentlemen — Multiple SA Victims

The Gentlemen (emerged Sept 2025; 78 victims in Feb 2026 alone) have specifically targeted multiple SA organisations.[21] TTPs include Advanced IP Scanner, PowerRun.exe privilege escalation, BYOVD anti-AV, GPO modification for domain-wide deployment, and WinSCP exfiltration. Ransom note: **README-GENTLEMEN.txt**.

Victim	Sector	Group	Discovered
Witzenberg Municipality	Government	The Gentlemen	2026-01-20
Rola Motor Group	Automotive	The Gentlemen	2026-01-20
Paltrack	Logistics	The Gentlemen	2026-01-20
Intsika Yethu Municipality	Government	The Gentlemen	2026-02-15

5.4 Vect — EnerTec & Hytec SA

Vect ransomware targeted EnerTec (Manufacturing; discovered 24 Feb; data LEAKED) and Hytec SA (Engineering; discovered 6 Jan; status: NEGOTIATING — all data exfiltrated including PII).[20]

5.5 SA Ransomware Victims Summary (2026 YTD)

Organisation	Sector	Threat Group	Date	Status
Lion of Africa Insurance	Insurance	Lynx	2026-03-13	Active
Diesel-Electric Group	Automotive	LockBit 5	2026-03-01	Active
EnerTec	Manufacturing	Vect	2026-02-24	Leaked
Intsika Yethu Municipality	Government	The Gentlemen	2026-02-15	Active
Witzenberg Municipality	Government	The Gentlemen	2026-01-20	Active
Rola Motor Group	Automotive	The Gentlemen	2026-01-20	Active
Paltrack	Logistics	The Gentlemen	2026-01-20	Active
Land Bank	Financial	Unknown RaaS	2026-01-12	Resolved

Organisation	Sector	Threat Group	Date	Status
Hytec SA	Engineering	Vect	2026-01-06	Negotiating

5.6 Global Ransomware Landscape

Group	Activity Level	Typical Targets
Qilin	#1 — 104 victims (Feb 2026)	Broad cross-sector
The Gentlemen	#2 — 78 victims (Feb 2026)	Manufacturing, Govt, Automotive
CL0P	#3 — 49 victims (Feb 2026)	Enterprise, Finance
Akira	Active	Engineering, Healthcare
LockBit 5	Active — SA targeting	Broad
Lynx	Active — SA targeting	Insurance, SMB

[19] Ransomware.live — Lion of Africa / Lynx, https://www.ransomware.live/id/QWZyaWNhIEluc3VyYW5jZUBseW54
[20] Ransomware.live — South Africa map, https://www.ransomware.live/map/ZA
[21] MOXFIVE — The Gentlemen Threat Actor Spotlight, https://www.moxfive.com/resources/moxfive-threat-actor-spotlight-the-gentlemen

6. Critical Vulnerabilities

This section covers critical and actively exploited vulnerabilities disclosed during March 6–13, 2026. CISA added 4 vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog this week.[22] Microsoft Patch Tuesday addressed 84 CVEs including 2 zero-days.[23] Google Chrome patched 2 actively exploited zero-days on March 13.[24]

CVE ID	Vendor/Product	CVSS	Description	Exploitation	Patch
CVE-2026-20079	Cisco Secure FMC	10.0	Auth Bypass Root	Not yet	Yes
CVE-2026-20131	Cisco Secure FMC	10.0	RCE (Java Deser.)	Not yet	Yes
CVE-2025-26399	SolarWinds WHD	9.8	RCE (Deser.)	YES — Warlock	Yes
CVE-2026-21643	FortiClient EMS	9.8	SQL Injection (Pre-Auth)	Not yet	Yes
CVE-2019-17571	SAP FS-QUO	9.8	Code Injection (Log4j)	No	Yes
CVE-2026-21536	MS Devices Pricing	9.8	RCE (server-side)	Auto-mitigated	N/A
CVE-2026-24858	FortiOS SSO	9.4	Auth Bypass	YES — CISA KEV	Yes
CVE-2026-27685	SAP NetWeaver	9.1	Deser. RCE/EoP	No	Yes
CVE-2025-68613	n8n Automation	9.9	RCE	YES — CISA KEV	Yes
CVE-2026-21262	MS SQL Server	8.8	EoP sysadmin	No (public)	Yes
CVE-2026-1603	Ivanti EPM	8.6	Auth Bypass	YES — CISA KEV	Yes
CVE-2026-26110	MS Office	8.4	RCE (Preview Pane)	No	Yes
CVE-2026-22719	VMware Aria Ops	8.1	Command Injection RCE	YES — CISA KEV	Yes
CVE-2026-3909	Chrome / Skia	High	OOB Write	YES — in wild	Yes
CVE-2026-3910	Chrome / V8	High	Inappropriate Impl.	YES — in wild	Yes
CVE-2026-21385	Qualcomm/Android	7.8	Memory Corruption	YES (limited)	Yes
CVE-2021-22054	Omnissa WS1 UEM	7.5	SSRF	YES — CISA KEV	Yes

[22] CISA KEV Catalog, https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[23] The Hacker News — MS Patch Tuesday March 2026, https://thehackernews.com/2026/03/microsoft-patches-84-flaws-in-march.html
[24] BleepingComputer — Chrome zero-days, https://www.bleepingcomputer.com/news/google/google-fixes-two-new-chrome-zero-days-exploited-in-attacks/

7. Phishing & Social Engineering

7.1 AI-Powered Banking Fraud

AI-powered vishing and smishing campaigns continue to target customers of **FNB, Standard Bank, Absa, Nedbank, and Capitec**. Threat actors use deepfake audio/video, SIM swap fraud, and fake login pages for credential harvesting.[25] Digital banking fraud incidents **doubled** in 2024 (31,612 64,000 cases), with losses exceeding **R1.4 billion**.[26]

Metric	Value
Digital banking fraud cases (2024)	64,000 (+103% YoY)
Digital banking fraud losses	R1.4 billion
Share of all financial crime	65.3%
BEC case increase (2024)	+26%
Average BEC loss (global)	$137,000
SIM swap fraud annual cost	>R5 billion
BEC + FTF share of cyber insurance claims	58%

7.2 Business Email Compromise (BEC)

SABRIC reported a **26% rise in BEC cases** in 2024.[27] Leading scenarios include CEO fraud, invoice/supplier fraud, payroll diversion, and property transaction interception. Average global BEC loss: **$137,000** per incident. BEC and funds transfer fraud account for **58% of all cyber insurance claims**.[28]

7.3 Fake CAPTCHA Lures

CrowdStrike's 2026 Global Threat Report documents a **563% increase** in fake CAPTCHA lures used to deploy info-stealers, clipboard hijackers, and RATs. These campaigns affect SA users via malvertising on legitimate news sites and compromised WordPress deployments.[29]

[25] IOL — The message looks real, it isn't, https://iol.co.za/personal-finance/2026-03-07-the-message-looks-real-it-isnt/
[26] iAfrica — SABRIC 2024 crime statistics, https://iafrica.com/sabric-warns-of-rising-ai-powered-fraud-in-south-africa-despite-overall-drop-in-financial-crime/
[27] Yolo Telecoms — SA BEC surge, https://www.yolo.co.za/blog/south-africas-cybercrime-surge
[28] Coalition — 2026 Cyber Claims Report, https://markets.businessinsider.com/news/stocks/coalition-s-2026-cyber-claims-report-finds-initial-ransom-demands-surged-47-but-most-businesses-refuse-to-pay-1035901580
[29] CrowdStrike — 2026 Global Threat Report, https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-global-threat-report-findings/

8. Regulatory & Compliance

8.1 POPIA Health Data Regulations (6 March 2026)

The Information Regulator published binding **Regulations Relating to the Processing of Data Subjects' Health Information** (Government Gazette No. 54268, Notice No. 7198), signed 27 February and in force **6 March 2026**.[30] Eight categories of responsible party must comply immediately: insurance companies, medical schemes, managed healthcare organisations, administrative bodies, pension funds, employers, and institutions acting on their behalf.

Key obligations: Map every health data processing instance to POPIA section 27; maintain security safeguards (confidentiality, integrity, availability); duty of confidentiality; cross-border transfer restrictions under section 72(1). **Penalties: up to R10 million** in administrative fines; criminal prosecution possible.[31]

8.2 Information Regulator Performance Data

Metric	Value
Security compromise notifications (2025/26 YTD)	2,898
Growth from 2021/22 baseline	~15× (202 2,898)
Finalised compromises (in-year)	1,578
Open unresolved matters	1,320
Registered information officers	69,040
CIPC-active companies	~490,000
Information officer compliance rate	~14%
Completed enforcement matters (all time)	4 + WhatsApp settlement

The Regulator disclosed these figures at its 2026/27 Annual Performance Plan consultation on 5 March 2026.[32] CEO Mosalanyane Mosala publicly acknowledged the Regulator "struggles with responsiveness".

8.3 Updated Enforcement Guidance (23 February 2026)

The Information Regulator issued updated enforcement guidance signalling a more assertive approach. Priorities: lawful basis for processing, adequate security safeguards, proper incident response, timely breach notifications, and accountability frameworks (Information Officer registration).[33]

8.4 SARB & FSCA Directives

SARB Directive 1 of 2024 (NPS cybersecurity): Requires governance plans, ISO 27001/NIST CSF 2.0 alignment, quarterly resilience testing, 24-hour incident reporting, and 2-hour RTO for critical financial systems.[34] **FSCA + PA Joint Standard 2 of 2024** (effective 1 June 2025): Annual cybersecurity strategy review, MFA/encryption, continuous monitoring, and third-party risk management for all regulated financial institutions.[35]

8.5 DCDT–Netherlands MoU (3 March 2026)

DCDT signed a cybersecurity and digital innovation MoU with the Netherlands on 3 March 2026, covering AI governance, cybersecurity cooperation, digital skills development, and a joint Southern Africa–Netherlands Cyber Security School.[36]

8.6 Cybercrimes Act Status

The Cybercrimes Act (No. 10 of 2020) has been in partial force since 1 December 2021. The separate Cybersecurity Bill remains in development with no gazette date announced. AI legislative policy framework targeted for finalisation by 2027 under a sector-specific multi-regulator model.

Key Compliance Deadlines

Regulation	Effective Date	Urgency	Status
POPIA Health Data Regulations	6 March 2026	IMMEDIATE	In force now
FSCA Joint Standard 2 of 2024	1 June 2025	Ongoing	Active compliance phase
SARB Directive 1 of 2024	17 August 2024	Ongoing	Compliance required
POPIA Amendments (draft)	TBD	Strategic	Parliamentary process
AI Policy Framework	2027 (target)	Strategic	Cabinet approval phase

[30] ITLawCo — POPIA health data regulations, https://itlawco.com/popia-health-data-regulations-2026/
[31] Bowmans — POPIA health information regulations, https://bowmanslaw.com/insights/south-africa-popia-health-information-regulations-cross-the-finish-line/
[32] ITLawCo — Information Regulator 2026/27 APP, https://itlawco.com/information-regulator-2026-27-annual-performance-plan/
[33] Attorneys360 — Updated enforcement guidance, https://attorneys360.co.za/2026/02/23/information-regulator-issues-updated-enforcement-guidance-under-popia/
[34] Michalsons — SARB cybersecurity directive, https://www.michalsons.com/blog/sarb-cybersecurity-and-cyber-resilience-directive/78268
[35] EBNET — FSCA Joint Standard, https://www.ebnet.co.za/fsca-publishes-final-joint-standard-on-cybersecurity-and-cyber-resilience-requirements-for-financial-institutions/
[36] DCDT — SA-Netherlands ICT partnership, https://www.dcdt.gov.za/media-statements-releases/646-south-africa-and-the-netherlands-strengthen-ict-partnership-to-drive-digital-innovation-and-cybersecurity.html

9. OSINT Exposure

9.1 44.5 Million SA Identity Records Exposed

Researchers discovered three misconfigured servers exposing 252 million identity records across 7 nations, with approximately **44.5 million South African records** — nearly the entire adult population. Data included full names, national ID numbers, dates of birth, home addresses, and contact details.[37]

9.2 Pretoria Bar Alleged Breach

The Pretoria Society of Advocates (pretoriabar.co.za) was allegedly exposed on a dark web forum on 3 February 2026 — **2,427 records** including email addresses, names, usernames, and phone numbers. No official confirmation; HIBP has not yet indexed this breach.[38]

9.3 SA-Hosted Malware Infrastructure

URLhaus analysis identified 7 South African IP addresses actively serving malware payloads (AS37153 xneelo Pty Ltd). These are primarily IoT botnet payloads (Mirai variants, BusyBox exploitation).[39]

IP Address	Malware Paths	Assessment
154.222.30.227	/debug.dbg, /ppc, /x86_64, /arm7	Multi-arch botnet
156.229.163.77	/n2/mips, /n2/x86, /n2/mpsl	Mirai-variant IoT
156.229.118.153	/33969/	Dropper staging
156.229.164.94	/n2/mips, /n2/x86, /n2/teleport	Mirai-variant IoT
156.246.93.156	/proxy, /busybox-armv7l	BusyBox/IoT compromise
156.246.95.51	/bot.sh, /bot.x86_64, /bot.armv5l	Multi-arch bot
156.248.148.165	/81/hiddenbin/dvr1.sh	DVR exploit

9.4 HIBP Breaches Affecting SA Users

Global breaches added to HIBP in January 2026 with significant SA user impact:[40]

Breach	Domain	Breach Date	Records
Instagram	instagram.com	7 Jan 2026	6,215,150
Under Armour	underarmour.com	17 Nov 2025	72,742,892
BreachForums 2025	breachforums.hn	11 Aug 2025	672,247

[37] BiometricUpdate — 252M identity records exposed, https://www.biometricupdate.com/202509/misconfigured-servers-expose-252-million-identity-records-across-seven-nations
[38] UpGuard — Pretoria Bar breach, https://www.upguard.com/news/pretoriabar-co-za-data-breach-2026-02-05
[39] abuse.ch URLhaus, https://urlhaus.abuse.ch/downloads/text_recent/
[40] HaveIBeenPwned API, https://haveibeenpwned.com/

10. Indicators of Compromise (IOCs)

10.1 Ransomware IOCs

Indicator	Type	Attribution
lynxch2k5xi...onion	TOR C2	Lynx Ransomware
lynxblogxut...onion	TOR Leak Site	Lynx Ransomware
lynxblogco7...onion	TOR Leak Site	Lynx Ransomware
b1d81e8bbecccc547645d17395538a2d	MD5	Lynx
a20886a5b378624d16972db66bd4e7e1	MD5	Lynx
f16238836909d07f86154c5ccbade96a	MD5	Lynx
30656c737338818bee8cc3591e3f3dcc	MD5	Lynx
571684f28ce1cf4d8236dbd46ef6f7f0	MD5	Lynx
65c0c7c9fe6bc1d5296447aae6c6c14c	MD5	Lynx
d972bbbb3edb0e5ab5751b911f3dda17	MD5	Lynx
.lynx / README.txt	File indicators	Lynx encrypted files
README-GENTLEMEN.txt	Ransom note	The Gentlemen

10.2 APT / Espionage IOCs

Indicator	Type	Attribution
198[.]98[.]50[.]218	IP — Pantegana C2	RedNovember
209[.]141[.]46[.]57	IP — Recon/C2	RedNovember
209[.]141[.]47[.]6	IP — Recon/C2	RedNovember
205[.]185[.]126[.]208	IP — Pantegana C2	RedNovember
209[.]141[.]57[.]116	IP — Pantegana C2	RedNovember
download[.]offiec[.]us[.]kg	Domain — Payload	RedNovember
login[.]offiec[.]us[.]kg	Domain — Phishing	RedNovember
1e37efcd3cd647e6ce5414...5c90b	SHA256 — PDF lure	RedNovember
9a1077f57bac5610d44ac4...47b79	SHA256 — Word doc	RedNovember
pan[.]xj[.]hk	File-sharing infra	RedNovember

10.3 SA-Hosted Malware Infrastructure

Indicator	Type	Assessment
154.222.30.227	IP (ZA)	Botnet payload server
156.229.163.77	IP (ZA)	IoT botnet
156.229.118.153	IP (ZA)	Dropper staging
156.229.164.94	IP (ZA)	IoT botnet
156.246.93.156	IP (ZA)	BusyBox exploit
156.246.95.51	IP (ZA)	Multi-arch bot
156.248.148.165	IP (ZA)	DVR exploit

11. Recommendations

IMMEDIATE — This Week

- Update Google Chrome to 146.0.7680.75/76 — two actively exploited zero-days (CVE-2026-3909, CVE-2026-3910).
- Patch Cisco Secure FMC to latest version — CVSS 10.0 authentication bypass and RCE; no workarounds available.
- Apply Microsoft March 2026 Patch Tuesday — 84 CVEs including 2 publicly disclosed zero-days.
- Patch SAP NetWeaver (CVE-2026-27685, CVSS 9.1) and SAP FS-QUO (CVE-2019-17571, CVSS 9.8).
- Patch VMware Aria Operations (CVE-2026-22719) — CISA KEV; FCEB deadline 24 March.
- Block all Lynx and RedNovember IOCs at perimeter firewalls and SIEM detection rules.
- Review health data processing for new POPIA regulations (in force 6 March) — map lawful basis for each instance.
- Verify MFA is enforced on ALL VPN appliances — RedNovember and Salt Typhoon actively exploit VPN edge devices.

SHORT-TERM — This Quarter

- Conduct organisation-wide phishing simulation focusing on banking impersonation and fake CAPTCHA lures.
- Audit Information Officer registration with the Information Regulator (only 14% compliance rate nationally).
- Implement BEC detection rules: monitor for email forwarding rule changes, new inbox rules, and mailbox delegate access.
- Review telecoms provider SIM-swap controls and implement callback verification for number porting.
- Threat hunt for Salt Typhoon TTPs on Cisco IOS-XE routers and lawful intercept infrastructure.
- Upgrade n8n workflow automation to v1.120.4+ (CISA KEV, CVSS 9.9).
- Patch FortiClient EMS 7.4.4 to 7.4.5 (CVE-2026-21643, pre-auth SQL injection).

STRATEGIC — Long-Term

- Prepare for POPIA amendments — the Regulator is shifting from "correct and remedy" to direct consequences for non-compliance.
- Invest in AI-powered threat detection to counter AI-generated phishing, deepfake vishing, and automated attack chains.
- Consider external cyber risk scoring — by 2026, external risk ratings will influence corporate creditworthiness in Africa.
- Align cybersecurity programme to NIST CSF 2.0 / ISO 27001 as required by SARB Directive and FSCA Joint Standard.
- Establish board-level cyber risk reporting with quantified risk metrics and scenario-based tabletop exercises.
- Develop ransomware-specific incident response playbook with offline backup verification and communication templates.

12. OSINT Sources Consulted

The following open-source intelligence sources were consulted in the preparation of this report:

#	Source	URL
1	Ransomware.live — SA victims	https://www.ransomware.live/map/ZA
2	Ransomware.live — Lion of Africa / Lynx	https://www.ransomware.live/id/QWZyaWNhIEluc3VyYW5jZUBseW54
3	Dark Web Informer — March 2026	https://darkwebinformer.com/ransomware-attack-update-march-9th-2026/
4	Comparitech — Jan 2026 Ransomware Roundup	https://www.comparitech.com/news/ransomware-roundup-january-2026/
5	Tech4Law — Land Bank ransomware	https://www.tech4law.co.za/news-in-brief/security-news-in-brief/hacker...
6	IOL — Land Bank / identity theft	https://iol.co.za/news/south-africa/2026-02-25-from-ransomware-to-iden...
7	Priviso — SA bank ransomware	https://www.priviso.co.za/insights/south-africa-bank-ransomware-2026.h...
8	MOXFIVE — The Gentlemen	https://www.moxfive.com/resources/moxfive-threat-actor-spotlight-the-g...
9	CyHawk Africa — The Gentlemen SA	https://cyhawk-africa.com/ransomware/thegentlemen-ransomware-group-all...
10	Breachsense — Feb 2026 Ransomware	https://www.breachsense.com/ransomware-reports/february-2026/
11	BlackFog — State of Ransomware 2026	https://www.blackfog.com/the-state-of-ransomware-2026/
12	Picus Security — Lynx TTPs	https://www.picussecurity.com/resource/blog/lynx-ransomware
13	TechCrunch — Salt Typhoon global list	https://techcrunch.com/2026/03/09/salt-typhoon-china-who-has-been-hack...
14	CyberScoop — FBI Salt Typhoon	https://cyberscoop.com/fbi-salt-typhoon-ongoing-threat-cybertalks-2026...
15	Recorded Future — RedNovember	https://www.recordedfuture.com/research/rednovember-targets-government...
16	The Hacker News — RedNovember	https://thehackernews.com/2025/09/chinese-hackers-rednovember-target.h...
17	Africa Defense Forum — APT41	https://adf-magazine.com/2025/08/prolific-chinese-cyber-espionage-grou...
18	TechCabal — Africa breaches 2025	https://techcabal.com/2025/12/30/cyber-breaches-became-harder-to-hide/
19	ITWeb — SA cyber defences exposed	https://www.itweb.co.za/article/sas-cyber-defences-exposed-as-global-t...
20	IT-Online — Breached every 3 hours	https://it-online.co.za/2026/03/11/sa-organisations-are-breached-every...
21	ITWeb — 2,100 attacks/week	https://www.itweb.co.za/article/sa-firms-hit-by-over-2-100-cyber-attac...
22	BrandDefense — Kasablanka APT	https://brandefense.io/blog/kasablanka-apt-group/
23	IOL — Phishing scams March 2026	https://iol.co.za/personal-finance/2026-03-07-the-message-looks-real-i...
24	SABRIC — AI Scam Alert	https://www.sabric.co.za/ai-powered-scams-expected-to-increase-during-...
25	iAfrica — SABRIC 2024 statistics	https://iafrica.com/sabric-warns-of-rising-ai-powered-fraud-in-south-a...
26	GSMA — Scam Signal SA launch	https://www.gsma.com/newsroom/article/scam-signal-launches-in-south-af...
27	Coalition — 2026 Cyber Claims	https://markets.businessinsider.com/news/stocks/coalition-s-2026-cyber...
28	CrowdStrike — 2026 Global Threat Report	https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-global-threat-...
29	abuse.ch URLhaus	https://urlhaus.abuse.ch/downloads/text_recent/
30	CISA KEV Catalog	https://www.cisa.gov/known-exploited-vulnerabilities-catalog
31	The Hacker News — MS Patch Tuesday	https://thehackernews.com/2026/03/microsoft-patches-84-flaws-in-march....
32	BleepingComputer — Chrome zero-days	https://www.bleepingcomputer.com/news/google/google-fixes-two-new-chro...
33	ITLawCo — POPIA health data regs	https://itlawco.com/popia-health-data-regulations-2026/
34	ITLawCo — IR 2026/27 APP	https://itlawco.com/information-regulator-2026-27-annual-performance-p...
35	Bowmans — POPIA health regs	https://bowmanslaw.com/insights/south-africa-popia-health-information-...
36	DCDT — SA-Netherlands MoU	https://www.dcdt.gov.za/media-statements-releases/646-south-africa-and...
37	BiometricUpdate — 252M records	https://www.biometricupdate.com/202509/misconfigured-servers-expose-25...
38	UpGuard — Pretoria Bar breach	https://www.upguard.com/news/pretoriabar-co-za-data-breach-2026-02-05

This report is classified TLP:WHITE and may be distributed without restriction. Information is provided as-is for situational awareness and does not constitute legal advice. All source URLs were verified at time of research (13 March 2026). Threat landscape evolves rapidly; reassess within 7 days.