OT-ISAC CLEAR *– Recipients may share* ***TLP:CLEAR*** *information without restriction.* ***TLP:CLEAR*** *information may be distributed freely, subject only to copyright controls. It is suitable for public release, including to media, the wider community, and external stakeholders, because it poses no foreseeable risk of misuse in its current form.*

OT-ISAC Threat Intelligence Report:

APAC Critical Infrastructure Cyber Threat Outlook: 2025 Actor Highlights and 2026 Defensive Priorities

This information is provided as-is for informational purposes only and comes with no expressed or implied warranties. You (and any individual or entity you represent) bear full responsibility for all actions and omissions made based on this information. OT-ISAC disclaims any responsibility or liability for any such actions or omissions.

In the spirit of community-driven effort, we'd like to encourage our Members and Partners to share information to enable our community better to defend itself and improve situational awareness. ***Most importantly - If your organization requires direct assistance from OT-ISAC, feel free to reach out to us directly - our team will work with you to ensure all necessary support is available through the member submission and RFI process.***

Executive Summary

Based on official reporting and official/industry advisories published in 2025, OT-ISAC observed two dominant threat streams shaping cyber risk to APAC critical infrastructure: (1) state-linked intrusion activity associated with long-dwell access to high-leverage infrastructure layers (including network/edge and virtualisation/management planes), and (2) ransomware/extortion ecosystems increasingly enabled by identity-led access, exploitation of exposed edge systems, and affiliate-driven operations. Public disclosures rarely confirm direct OT compromise; however, operational risk remains material due to dependency on shared IT systems that underpin safety, continuity, and production/logistics workflows.

2026 outlook*: OT-ISAC assesses these patterns are likely to persist, with identity-driven access and exposure management remaining decisive defensive priorities.*

Threat actor clusters watchlist for critical infrastructure

Threat actor cluster	Why they matter for critical infrastructure	Typical initial access (high-level)
UNC3886 (state-linked; industry attribution)	Singapore's CSA stated it detected UNC3886 activity "in parts of our critical infrastructure" and is leading investigations; 2025 reporting characterised the threat as serious and affecting essential services. Singapore government communications in 2025 referenced sophisticated TTPs (including LoTL techniques and use of zero-day exploits).	Targeting high-leverage infrastructure layers for long-dwell access, including activity involving network/edge and virtualisation environments.
Medusa (RaaS)	The #StopRansomware advisory states that as of Feb 2025, Medusa developers/affiliates impacted 300+ victims, including across critical infrastructure sectors.	Credential-driven access (including phishing) and exploitation of unpatched internet-facing services; theft + extortion + encryption are common outcomes.
Akira (RaaS)	The #StopRansomware advisory update (13 Nov 2025) describes Akira's continued threat and evolution, including activity affecting virtualised environments and an incident involving encryption of Nutanix AHV VM disk files.	Credential abuse and exploitation of edge/VPN weaknesses to gain initial footholds; lateral movement via common admin tooling; impact includes encryption/extortion and expansion into virtualisation layers.
Qilin (RaaS; industrial targeting highlighted in 2025 telemetry)	Industrial ransomware telemetry published in 2025 indicates Qilin remained highly active against industrial organisations, and that ransomware activity can translate into real operational disruption in some cases. OT-ISAC treats this as an operational signal for APAC CI because industrial disruption	Affiliate-driven intrusions leveraging exposed infrastructure and common enterprise footholds; enterprise IT compromise can cascade into disruption of production-supporting systems.

	frequently cascades through shared IT and plant-supporting services.	
Play (RaaS)	CISA issued updated guidance on Play ransomware on 4 Jun 2025, reflecting new TTPs and updated indicators, reinforcing Play as a persistent ransomware threat relevant to critical infrastructure defenders.	Credential-led access and exploitation of exposed services/known weaknesses, followed by rapid lateral movement and extortion/encryption operations.
INC Ransom (RaaS)	Industrial telemetry published in 2025 places INC among the ransomware operations contributing materially to industrial targeting, which OT-ISAC treats as relevant to APAC critical infrastructure due to industrial supply-chain dependencies and shared services exposure.	Affiliate-driven intrusions via common enterprise footholds (edge exposure, credential abuse, remote tooling), with downstream disruption risk to industrial operations.

Additional actors observed (claim-led; lower confidence)

Threat actor cluster	Why it matters	Typical initial access (high-level)
Anubis (emerging; claim-led)	In 2025 reporting, Anubis appears mainly as an emerging RaaS brand that claims victims via leak-site postings (e.g., reporting tied to the Aussie Fluid Power incident). This is useful as an operational signal, but attribution is not equivalent to victim or authority confirmation.	Not consistently documented in authoritative 2025 advisories; current visibility is primarily post-compromise extortion-site claims rather than a well-described access pattern.

OT-ISAC synthesis*: OT-ISAC assessed this watchlist by correlating official advisories, reputable reporting, and industrial telemetry, then translating it into operational priorities for APAC critical infrastructure – particularly where IT compromise can cascade into OT disruption.*

OT-ISAC analytic judgment

Public reporting on critical infrastructure incidents frequently stops at "IT disruption" or "data theft," and rarely confirms direct OT compromise. OT-ISAC assesses that the most consequential outcomes for critical infrastructure are typically enabled by two recurring pathways:

- **Identity compromise**: credential theft and abuse of helpdesk/account recovery workflows to obtain or escalate access.
- **Edge and management-plane access**: compromise of internet-facing services, network edge devices, and virtualisation/management platforms.

These access paths materially increase the likelihood of operational disruption because they sit upstream of many systems that support safety, continuity, and production/logistics, meaning OT impact can occur even when OT networks are not publicly reported as compromised.

What critical infrastructure defenders should prioritize in 2026

- **Harden identity for privileged workflows**: implement phishing-resistant MFA for administrators; tighten helpdesk verification; secure MFA enrolment and password reset processes; monitor for anomalous authentication and reset activity.
- **Reduce edge and management-plane exposure**: rapidly patch or mitigate high-risk internet-facing services (VPNs, remote access gateways, perimeter devices); monitor virtualisation/management-plane access; minimise standing admin access and enforce least privilege.
- **Prioritise by exploitation risk, not CVSS alone**: integrate CISA's Known Exploited Vulnerabilities (KEV) Catalog into remediation and compensating controls, especially for exposed systems.
- **Adopt an OT exposure management approach**: prioritise remediation where known exploitation + insecure internet exposure + ransomware/extortion relevance converge; validate segmentation and remote access boundaries between IT and OT-adjacent environments.
- **Constrain supplier blast radius**: enforce least privilege and segmentation for vendor access; require strong authentication and logging; rotate credentials after supplier incidents; embed security requirements into contracts and third-party assurance.

Reference

[1] Singapore CSA - "Media Statement on our responses to APTs", https://www.csa.gov.sg/news-events/press-releases/media-statement-on-our-responses-to-apts/

[2] Reuters - "China denies link to espionage group accused of attacking Singapore critical infrastructure", https://www.reuters.com/world/china/china-denies-link-espionage-group-accused-attacking-singapore-critical-2025-07-21/

[3] CISA - "Scattered Spider (AA23-320A)", https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

[4] CISA - "CISA and Partners Release Updated Advisory on Scattered Spider Group" (Alert), https://www.cisa.gov/news-events/alerts/2025/07/29/cisa-and-partners-release-updated-advisory-scattered-spider-group

[5] CISA - "#StopRansomware: Medusa Ransomware (AA25-071A)", https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a

[6] CISA - "#StopRansomware: Akira Ransomware (AA24-109A)", https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

[7] CISA - "CISA and Partners Release Advisory Update on Akira Ransomware" (Alert), https://www.cisa.gov/news-events/alerts/2025/11/13/cisa-and-partners-release-advisory-update-akira-ransomware

[8] Dragos - "Dragos Industrial Ransomware Analysis: Q3 2025", https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q3-2025

[9] Claroty - "State of CPS Security: OT Exposures 2025", https://claroty.com/resources/reports/state-of-cps-security-ot-exposures-2025