Cyber Threat Landscape Energy Sector - 2025

March 2026

Prepared by

Asia Information Sharing & Analysis Center Limited

Prepared for

Corporate Members

Asia-ISAC

Table of Contents

Asia-ISAC Overview

NO COMPANY IN ASIA SHOULD FACE CYBER THREATS ALONE

Vision

The Asia Information Sharing & Analysis Center (Asia-ISAC) is the region's first cross-industry, non-profit cyber intelligence network dedicated to trusted threat sharing and secure AI adoption. As cyberattacks grow more sophisticated and the cost of data breaches continues to rise, Asia-ISAC enables organizations to collaborate, share intelligence, and strengthen their collective cyber resilience.

Mission

- Enable secure, sustainable, and trusted information sharing
- Unlock business innovation and growth with secure AI
- Provide early warnings on emerging cyber threats
- Strengthen cyber resilience

Executive Summary

Asia Energy Industry 2025

US$3 Trillion

Geography

47 Countries

Companies in Asia

500,000+

What this report covers

This Cyber Intelligence Report provides an overview of the cyber threat landscape targeting the Energy sector across Asia in 2025. The scope includes:

- Regional coverage across East Asia, Southeast Asia, South Asia, West Asia, and Oceania.
- Impacts spanning both information technology (IT) and operational technology and industrial control systems (OT/ICS) environments, including grid, refinery, and distribution operations.
- Analysis of notable incidents, threat actors, malware families, and exploited vulnerabilities.

Key findings and highlights

The energy sector across Asia remains a primary target for sophisticated cyber adversaries due to its role as the backbone of national security and economic stability. As digital transformation continues to bridge the gap between traditional information technology and operational environments, the attack surface has expanded significantly. Across Asia, this evolution has led to a more volatile cyber threat environment.

Key findings for Asia's 2025 threat landscape include:

- Critical infrastructure remains a top target, with OT/ICS disruption increasingly paired with data-theft and double extortion schemes.
- Financial losses from major incidents in 2025 approximately US$400 million across the region, alongside significant operational downtime and public disruption.
- State-linked activity escalated in politically sensitive geographies, indicating continued convergence of geopolitics and cyber operations.
- Legacy exposures and edge infrastructure (e.g., VPN/ADC) continue to be leveraged for initial access and ransomware deployment.

Major attacks and business impact

The year 2025 has been characterized by a series of high-impact cyber operations that moved beyond simple data theft to cause significant physical and economic disruption. These incidents demonstrate a sophisticated understanding of industrial control systems and a willingness by threat actors to target the essential services that underpin modern society. From ransomware-induced blackouts to state-sponsored grid interference, the following cases highlight the severe operational and financial consequences facing the Energy sector in Asia.

Major attacks and business impact include:

- **NightSpire ransomware** disrupted a Southeast Asian energy provider's OT control systems, causing multi-day blackouts and >US$230 million losses.
- **LockBit 3.0** impacted fuel distribution across Java (Indonesia), causing broad logistical delays and tens of millions in losses.
- Targeted refinery attack (Middle East) used **custom malware against SCADA**; production halted ~72 hours, >US$100 million impact.
- **Australian utility breach** exposed data of 750k customers and disrupted smart monitoring; remediation costs >US$50 million.

In summary, these incidents collectively represent approximately US$400 million in direct financial losses, illustrating that the cost of a breach now extends far beyond immediate recovery to include massive downstream economic damage.

Actionable intelligence in this report

This report provides actionable intelligence and insights to support a clearer understanding of the threat landscape and enable proactive action.

- **Top threat actors** active against the energy sector in Asia.
- **Malware used** by these actors and relevant tradecraft.
- **Vulnerabilities exploited** in IT/OT environments in the Energy sector.
- **Recommendations** mapped to observed threat behaviors to strengthen resilience.

Key Threat Landscape Insights

Threat Analysis

The 2025 threat landscape for the energy sector reveals a sophisticated and increasingly dangerous environment where digital vulnerabilities translate directly into physical and economic consequences. As energy providers integrate more connected technologies to improve efficiency, they inadvertently expand the attack surface for both cybercriminals and nation-state actors. The following insights distill the most critical trends observed across Asia, highlighting the shift from simple data theft to the systemic disruption of essential services.

~40%

Increase in cyber attacks

(Source: CLUSIT 2025 Report)

KEY INSIGHTS:

- **Critical Infrastructure Remains Highly Targeted:** The growing reliance on operational technology (OT), such as SCADA and ICS frameworks, makes the energy sector increasingly vulnerable to both ransomware and state-sponsored attacks.
- **Financial and Operational Repercussions are Enormous:** Attacks such as those by LockBit and NightSpire demonstrate direct financial losses exceeding hundreds of millions of dollars, while also inflicting major disruptions due to energy shortages.
- **State-Sponsored Attacks Continue to Escalate:** Incidents targeting Taiwan's energy grid highlight the intertwining of geopolitics with cyber warfare.
- **Data Breaches Compound Damage:** Breaches of energy utilities in Australia demonstrated that compromised customer and operational data lead to cascading financial and reputational risks.

In summary, these insights underscore that the energy sector is facing increasingly coordinated threats to industry stability. The convergence of massive financial liabilities, geopolitical maneuvering, and the vulnerability of legacy OT systems creates a high-stakes environment where a single breach can have multi-million dollar repercussions. Moving forward, the industry must recognize that cybersecurity is a fundamental component of operational resilience and energy stability.

Summary of Major Incidents

Summary of major incidents for the Asia energy sector with the most severe impacts in terms of operational disruptions, financial damage, and/or sensitive data compromises.

These cyber incidents can provide insights on the gravity of the cyberattacks including the business and economic impact of these incidents. Furthermore, the primary threat actor and attack details are indicated to provide a better understanding of who and how the attack was conducted successfully.

1. Ransomware Attack on Southeast Asian Energy Provider

- Date & Region: May 2025, Southeast Asia
- Summary: A ransomware attack by the NightSpire group disabled control systems at a major Southeast Asian energy provider for 18 days, leading to widespread energy distribution disruptions across multiple provinces.
- Attack Details: By targeting operational technology (OT) control systems in the energy provider, attackers halted distribution, causing widespread blackouts that lasted several days. **NightSpire threatened a double extortion scheme**, demanding ransom for the decryption keys and threatening to leak sensitive operational details about the network.
- Impact: Severe energy shortages across affected provinces, disrupting daily life and industrial productivity. Financial losses exceeded US$230 million, including ransom demands and recovery costs.
- This incident highlighted vulnerabilities in critical industrial control systems (ICS) against ransomware attacks.
- Attribution: NightSpire ransomware group.

18	US$230M+
Days disrupted	Financial losses (estimated)

2. LockBit 3.0 Attack on Fuel Distribution in Indonesia

- Date & Region: Early 2025, Indonesia (Southeast Asia)
- Summary: A LockBit 3.0 ransomware attack significantly disrupted fuel distribution across Java island in Indonesia, one of the region's most densely populated areas.
- Attack Details: LockBit group exploited a vulnerability in the company's IT infrastructure, gaining access to mission-critical systems controlling fuel storage and distribution. They encrypted operational files and threatened to release sensitive data about Indonesia's fuel infrastructure as part of a double extortion tactic.

- Impact: Delays in fuel distribution caused logistical chaos in supply chains and energy shortages across Java. Tens of millions of dollars were lost due to ransom demands, losses in fuel revenues, and production delays.
- Underlined how energy distribution systems are prime targets for ransomware attackers in Southeast Asia.
- Attribution: LockBit ransomware group.

3. Cyberattack on Middle Eastern Oil Refinery

- Date & Region: February 2025, Middle East
- Summary: A targeted cyber-physical attack on a leading oil refinery in the Middle East sabotaged key industrial control systems, halting production temporarily and raising concerns over cyber threats to petrochemical facilities.
- Attack Details: The attackers targeted SCADA (Supervisory Control and Data Acquisition) systems with a custom-built malware variant, aiming to disrupt production cycles and exfiltrate sensitive operational processes. Though officially contained within 72 hours, the attack underscored vulnerabilities in critical operational technology (OT).
- Impact: Significant operational shutdown for three days. Financial losses estimated to exceed US$100 million due to lost production.
- Industry regulators called for urgent reforms in OT cybersecurity following the attack.
- Attribution: Unknown (suspected state-sponsored actors).

72	US$100M+
Hours disrupted	Financial losses (estimated)

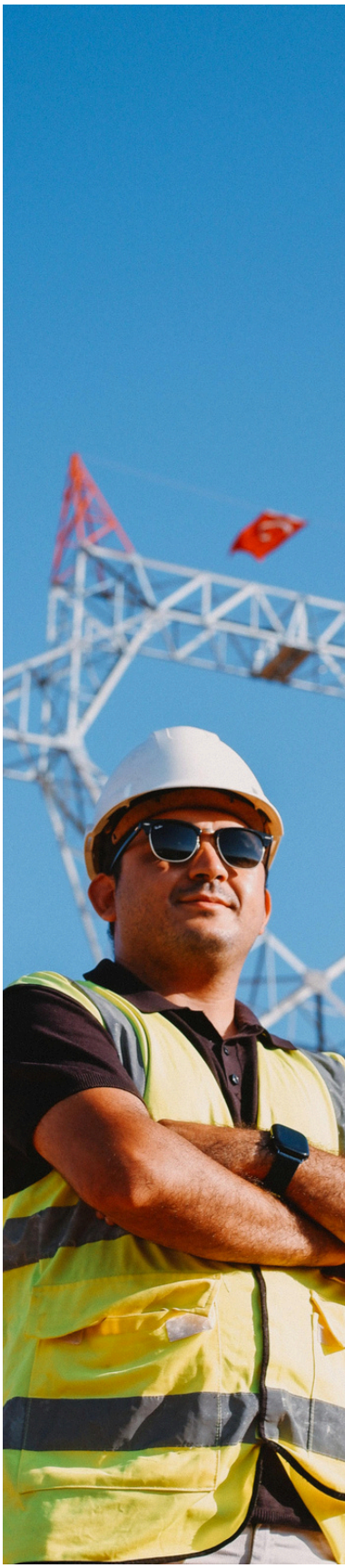
4. State-Sponsored Attack on Taiwanese Energy

- Date & Region: 2025, Taiwan (East Asia)
- Summary: 961 million cyberattack intrusion attempts targeted Taiwan's critical infrastructure averaging to 2.63 million per day with the energy sector seeing the most attacks. The attackers deployed advanced persistent threat (APT) tactics.
- Attack Details: Threat actors probed network equipment and industrial control systems - including petroleum, electricity, and natural gas operations. Threat actors infiltrated the energy grid's network management systems using spear-phishing emails and planted malware capable of manipulating grid operations.
- Impact: Undisclosed financial losses.
- Highlighted escalating geopolitical tensions driving cyber conflict in East Asia.
- Attribution: Assessed with moderate confidence to involve state-backed actors.

5. Cyber Breach of Utility Provider in Australia

- Date & Region: March 2025, Australia
- Summary: A major utility provider overseeing power and water distribution suffered a significant breach where attackers exfiltrated sensitive customer data and disrupted digital monitoring systems, leading to delays in service management.
- Attack Details: The breach targeted digital twin technology and smart monitoring systems for infrastructure, exposing sensitive operational insights and customer billing records. Attackers used the exfiltrated data to launch follow-up phishing attacks targeting affected customers.
- Impact: Leakage of private utility data of 750,000 customers. Financial losses estimated due to reconfiguration and remediation exceeded US$50 million.
- Stressed the need for better cybersecurity practices in sectors relying on smart infrastructure.
- Attribution: Likely a cybercriminal group motivated by financial gain.

750K	US$50M+
Customer private data	Financial losses (estimate)



6. Pakistan Petroleum Limited (PPL)

- Date & Region: August 6, 2025, Pakistan
- Summary: A ransomware intrusion occurred, targeting IT infrastructure.
- Attack Details: Portions of PPL's IT infrastructure were encrypted. The attack was contained by isolating non-critical IT services. Indicators of Compromise (IOCs) / Tactics, Techniques, and Procedures (TTPs) likely involved ransomware encryption tools. Initial infiltration vector not explicitly shared, but similar attacks often include phishing or remote service exploitation.
- Impact: No access to critical systems was achieved. No sensitive data was compromised. Partial service disruption. Losses were not disclosed.
- Attribution: Specific attacker group unknown. However, it aligns with financially motivated ransomware patterns.

Recommendations

Strengthen the cybersecurity posture

These recommendations are made based on lessons learned and key challenges faced in the incidents highlighted in the Energy sector.

Poor IT/OT segmentation remains widespread, enabling lateral movement and exposing gaps in cybersecurity architecture and implementation. At the same time, attackers are increasingly exploiting phishing, third-party vulnerabilities, and remote access services as primary entry points. These risks are further compounded by continued reliance on outdated email and software systems, along with challenges in modernizing or replacing legacy infrastructure.

By adopting these measures, energy companies can significantly bolster their defenses against emerging malware tactics, targeted attacks, and supply chain vulnerabilities while ensuring compliance with regulatory mandates and industry standards.

Strengthen OT/ICS Defenses

Adopt advanced monitoring tools to secure operational systems, including SCADA and energy grid infrastructure. Segment OT from IT, implement allowlisting, and conduct tabletop exercises for grid impact scenarios.

Use Threat Intelligence

Partner with national and regional alliances, like Asia-ISAC, to obtain early indicators, TTPs, and mitigation playbooks for ransomware and APT campaigns.

Geopolitical Preparedness

Coordinate defensive strategies for critical infrastructure beyond enterprise security—include incident command structures, regulatory engagement, and business continuity planning.

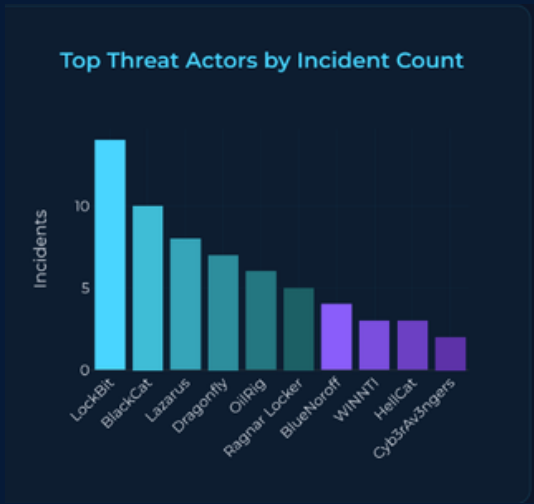
Customer Data Protection

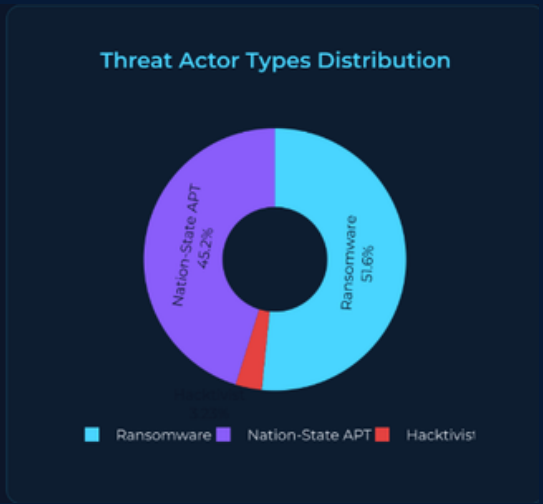
Enforce encryption at rest/in transit, strong Identity Access Management for privileged access, continuous exposure management, and rapid takedown for post-breach phishing.

Summary of Top Threat Actors, Malware, and Vulnerabilities

Top 10 Most Active Threat Actors Targeting the Energy Sector

The following threat actors have aggressively targeted the energy industry in Asia as identified across the Asia-Pacific, Australia, South Asia, Central Asia, and the Middle East regions in 2025. These actors are ranked based on the total number of documented attacks, business impact (financial losses, operational disruptions, data compromises), geopolitical influence, and attributed methodologies.





Threat Actor	Type	Number of Recorded Incidents
LockBit (3.0)	Ransomware	14
BlackCat (ALPHV)	Ransomware	10
Lazarus Group	Nation-State APT	8
Dragonfly (APT33)	Nation-State APT	7

Threat Actor	Type	Number of Recorded Incidents
OilRig (APT34)	Nation-State APT	6
Ragnar Locker	Ransomware	5
BlueNoroff (APT Subgroup)	Nation-State APT	4
WINNTI Group	Nation-State APT	3
HellCat	Ransomware/ Infostealer	3
Cyb3rAv3ngers	Hacktivist	2

(*Number of Recorded Incidents based on observed and attributed incidents in 2025 datasets)

Top Vulnerabilities Targeted by Threat Actors

A defining characteristic of the 2025 threat landscape is the breadth of vulnerabilities being actively exploited against the energy sector — spanning modern browser engines, enterprise networking appliances, legacy Windows infrastructure, and emerging IoT/IIoT devices.

Threat actors have demonstrated a clear ability to chain these vulnerabilities together, moving laterally from IT environments into sensitive OT systems. The following table highlights the most critical CVEs and device-level flaws observed in active exploitation campaigns targeting organizations in the energy sector across Asia.

CVE	Description	Threat Vector	Impact
CVE-2025-5419	Chromium V8 heap corruption allowing remote code execution (RCE)	RCE in browsers	Exploitation via industrial HMIs and management systems leveraging Chromium

CVE	Description	Threat Vector	Impact
CVE-2025-6543	Citrix NetScaler denial-of-service (DoS) vulnerability	Denial-of-Service (DoS)	Operational disruptions in VPNs/ load balancers crucial for energy companies
CVE-2025-43200	Apple zero-click logic exploit, enabling device compromise	Spyware/ Credential Theft	Infiltration of employee/executive devices can steal credentials and sensitive details
CVE-2023-3519	RCE vulnerability in Citrix NetScaler Gateway/ADC, used for ransomware attacks and persistence	Ransomware/ Persistence	Continued exploitation highlights weak patch management in energy systems
CVE-2025-24016	Wazuh server deserialization flaw allowing remote code execution	Exploitation in compliance tools	Affects monitoring and compliance tools central to critical energy infrastructures
CVE-2020-1472	Legacy vulnerability enabling privilege escalation in Windows servers and domain controllers	Privilege Escalation	Still exploited due to unpatched legacy systems in energy environments
CVE-2025-33053	WebDAV path control issue allowing unauthorized file access	Lateral Movement / Data Access	Compromises OT/IT environments integrating WebDAV for industrial/ enterprise collaboration
CVE-2024-7755	IoT device vulnerability enabling unauthorized data access or remote control	IoT/IIoT device exploitation	Affects remote asset monitoring in industrial/energy environments
CVE-2025-3248	Langflow unauthenticated RCE allowing exploitation of open-source platforms	Exploiting hybrid architectures	Industrial systems using open-source tools risk malicious control in hybrid IT/ OT

Top Malware Families Targeting the Energy Industry

The energy sector continues to face sustained and increasingly sophisticated malware activity, with adversaries leveraging both legacy ICS-specific toolsets and modern ransomware-as-a-service (RaaS) ecosystems to disrupt operations, extort organizations, and penetrate OT environments. The convergence of IT and OT systems, combined with the sector's reliance on aging industrial control platforms, makes malware campaigns particularly impactful.

The following list captures the most prominent malware families observed targeting energy organizations, spanning ICS-specific disruptive frameworks, credential-stealing trojans, ransomware groups, and emerging AI-assisted offensive tooling.

Key Observations:

- ICS-tailored malware remains active and relevant. Threats like BlackEnergy, Industroyer/CrashOverride, and Triton/Trisis demonstrate continued adversary interest in OT protocol manipulation, SIS system compromise, and infrastructure sabotage.
- Credential theft is still a critical early-access vector. Malware like Qbot accelerates intrusions by enabling lateral movement and ransomware deployment.
- AI-augmented malware is emerging. Tools like SugarGh0st RAT illustrate the shift toward AI-driven reconnaissance, automation, and exploit generation targeting complex hybrid IT/OT networks.
- Business impact centers on operational disruption. Malware targeting the energy sector frequently causes downtime, service degradation, reputational damage, and—in ICS-specific cases—real safety risks.

Malware Name	Type	Description	Tactics Used	Impact
BlackEnergy	ICS-specific Trojan	Historically used in attacks against ICS, enabling sabotage and disruption	Spear-phishing to deploy malware in critical OT	Disrupted ICS operations; targeting SCADA systems

Malware Name	Type	Description	Tactics Used	Impact
Industroyer/ CrashOverride	ICS-disruptive Malware	Designed to disrupt power grids, targeting operations and control protocols like IEC 60870-5-104 and IEC 61850.	Exploitation of OT protocols	Weaponized in attacks on energy grids; capable of causing blackouts or operational failure.
Clop	Ransomware	Targeted critical energy infrastructure for data encryption and extortion	Phishing and exploiting exposed application s	RaaS attacks with financial and operational disruption
Darkside	Ransomware	Known for the 2021 Colonial Pipeline attack; continues targeting OT networks	Double extortion tactics	Operational shutdowns and reputational damage
Qbot	Botnet/ Banking Trojan	Used to achieve initial access by stealing credentials or dropping additional payloads like ransomware	Phishing emails for initial access	Target internal systems; precursor to ransomware
Triton/Trisis	ICS-specific malware	Targets safety instrumented systems (SIS) in industrial control environments.	Advanced ICS attack techniques	Threatens safety by disabling critical safety mechanisms

Contact Us

Asia-ISAC

Website

www.asia-isac.org

Email

help@asia-isac.org

LinkedIn

www.linkedin.com/company/asia-isac