Cyber Threat Landscape (Telecom Sector)

Asia-ISAC | Period: January – June 2025 (H1 2025)

Confidential – For Asia-ISAC Members

Table of Contents

What this report covers

This Cyber Threat Report provides an overview of the cyber threat landscape targeting the Telecom industry across Asia during the first half of 2025 (January–June 2025). The scope includes:

- Regional coverage across East Asia, Southeast Asia, South Asia, Middle East, and Oceania.
- Impacts spanning Telecom and their related supply chain environments, including financial losses, private data, supply chain vulnerabilities, and network disruptions.
- Analysis of notable incidents, threat actors, malware families, and exploited vulnerabilities.
- Evolving Attack Techniques and Tools and Trends

Key findings and highlights

The first half of 2025 marked a watershed moment for the telecom industry in Asia. Threats not only disrupted operations but emphasized vulnerabilities within corporate infrastructures, regulatory gaps, and supply chains. Proactive investment in telecom-specific cybersecurity, incident response, and AI-driven threat management is essential to mitigate evolving risks.

Key highlights are:

- **Shift to Espionage & Hybrid Attacks:** The sector experienced significant evolutions in attack patterns, notably the blending of ransomware with espionage goals (e.g., Fog ransomware).
- **Regional Specificity in Targeting:** East Asia and the Middle East were prominent hotspots, facing state-aligned and critical infrastructure threats.
- **Record-breaking DDoS Threat Levels:** DDoS attacks surged globally, presenting growing concerns for service interruptions critical to Asia economies.
- ***Rise of AI & Spyware Tools for Telecom Exploitation:*** APAC telecom ecosystems faced increased threats from spyware.

Major attacks and business impact

Here are the major cyber attacks that resulted in significant business impact and losses.

- **SK Telecom HSS and USIM Breach (South Korea)** resulted in penalties of *US$ 97 million*, and over 23 million subscribers received free USIM replacements.
- **Optus Cyber Attack (Australia)** resulted in costs exceeding *AUD 150 million* in remediation efforts and impacted 14 million customers (but occurred in 2022).
- **KLIA Ransomware Attack (Malaysia)** disrupted the aviation telecom systems in the Kuala Lumpur International Airport resulting in major flight delays and significant service outages.

Actionable intelligence in this report

Here is the actionable intelligence and useful information that can help build a better understanding of the threat landscape towards a pro-active action plan.

- Top Threat Actors active against the Telecom sector in Asia.
- Malware used and evolving tactics & techniques by these threat actors.
- Vulnerabilities exploited in the Telecom industry.
- Recommendations mapped to observed threat behaviors to strengthen resilience.

Summary of major incidents for the Asia Telecom sector (H1 2025)

Summary of key cyber attacks for the Telecom sector with the most severe impacts in terms of operational disruptions, financial damage, and/or private data compromises.

These cyber incidents can provide insights on the gravity of the cyber attacks including the business and economic impact of these incidents. Furthermore, the primary threat actor or hacking group that conducted the attack and attack details are indicated to get a better understanding of who conducted and how the attack was successful. Additional details can be acquired via the reference provided for further in-depth information.

1. KLIA Ransomware Attack – Malaysia

- Date: March-April 2025
- Impact: Widespread disruptions at Kuala Lumpur International Airport, including flight delays and service outages affecting thousands of passengers.
- Financial Loss: Attackers demanded a ***$10 million*** ransom, which Malaysian authorities refused to pay.
- Type of Attack: Ransomware
- Attribution: A sophisticated ransomware group leveraging advanced persistent threat (APT) tactics.
- Significance: Highlighted vulnerabilities in transportation and telecom-critical infrastructure.
- Reference: 1

---

2. Fog Ransomware Attack on telecom subsidiary – Southeast/Central Asia

- Date: May 2025
- Impact: The telecom subsidiary of a financial institution in Asia was targeted with Fog ransomware using legitimate employee monitoring software (Syteca) and rare penetration tools like GC2. The breach created concerns about potential espionage.
- Significance: Represents an unusual blend of ransomware with possible espionage motives, showcasing the evolving hybrid tactics of attackers.
- Attribution: Likely state-sponsored or advanced professional threat actors.
- Reference: 1,5

3. Orange SA Ransomware Attack – APAC

- Date: August 2025 (Attack Details Recorded Earlier in Forecasts)
- Impact: Theft of 4GB of sensitive corporate telecom business data, later published on the dark web. This breach raised concerns over privacy and corporate espionage susceptibility in telecom giants.
- Type of Attack: Ransomware by Warlock Ransomware Group
- Significance: Highlighted the vulnerability of telecom supply chains and the ability of ransomware-as-a-service (RaaS) operators to pose global corporate risks.
- Reference: 10

---

4. DDoS Surge in MENA Telecom – Middle East

- Date: April-May 2025
- Impact: A record 236% surge in distributed denial-of-service (DDoS) attacks specifically targeted telecom and internet service providers (ISPs) in Saudi Arabia and UAE.
- Significance: Disruption in high-demand telecom services illustrated rising risks from denial-based attacks targeting key telecom infrastructure.
- Attribution: Likely hacktivists or state-aligned groups within the Middle East.
- Reference: 2,1,3

---

5. MirrorFace Campaign on APAC Telecom – East Asia

- Date: January 2025
- Impact: Targeted multi-sectoral attack on Japan's semiconductor and telecom sectors. Exfiltrated sensitive intellectual property including telecom-infrastructure blueprints.
- Significance: The attack highlighted vulnerabilities in telecom manufacturing and R&D dependencies.
- Attribution: Nation State-backed espionage group, MirrorFace is suspected.
- Reference: 3

---

6. Cloudflare's Mitigation of Record-breaking DDoS Attack – APAC

- Date: May 2025
- Impact: Cloudflare mitigated a historic 7.3 Tbps DDoS attack targeting an infrastructure hosting provider, which included services for telecom providers across the region.
- Technology Used: Automated global defense system blocked over 122,000 IPs from 161 countries during the 45-second attack window.
- Significance: Emphasized the scale and rapid evolution of DDoS attack technology threatening globally interdependent telecom structures.
- Reference: 5

---

7. ToolShell Vulnerability Exploited – Middle East

- Date: June 2025
- Impact: A critical vulnerability (CVE-2025-53770) in telecom core network architecture was exploited by a state-sponsored APT group, targeting telecom operators in Saudi Arabia and neighboring states.
- Impact on Private Data: Significant exploitation of sensitive user accounts and authentication data.
- Attribution: Likely state-aligned threat actors from a neighboring country, based on operational infrastructure.
- Reference: 13

---

8. Spyware Surge Targeting Southeast Asia Telecom – Southeast Asia

- Date: January-June 2025
- Impact: A 70% increase in spyware attacks on telecom service providers in countries like Indonesia, Thailand, and Vietnam.
- Target and Technique: Cybercriminals focused on mobile devices and backbone telecom services to intercept communications and steal corporate and user data.
- Attribution: APT groups colluding with private spyware developers.
- Significance: Illustrated the growing convergence of cyber espionage with direct attacks on user and telecom privacy.
- Reference: 4

---

9. SK Telecom HSS and USIM Breach - South Korea

- Date: April 2025
- Impact: Half of South Korea's population was impacted, nationwide regulatory penalties reached a record ***US$ 97 million***, and over 23 million subscribers received free USIM replacements post-attack.
- Attack Type: Advanced Persistent Threat (APT) with BPFDoor Malware
- Target and Technique:
    - Detected abnormal outbound traffic from Home Subscriber Server (HSS) environments storing International Mobile Subscriber Identifier (IMSI) data.
    - Attackers leveraged BPFDoor, a stealth Linux backdoor, to persistently operate for over three years undetected in the SKT environment.
    - Exfiltration of ***26.96 million IMSI records*** and 9.82 GB of USIM metadata allowed attackers to potentially perform SIM-swapping attacks, impersonation, and surveillance.
- Attribution: State-sponsored APTs suspected involvement, specifically groups like Volt Typhoon and Rustback Nexus, aiming to extend surveillance strategies and disrupt telecom capabilities.
- Reference: 7.

---

10. Optus Cyber Attack - Australia (occurred in 2022 but worth sharing)

- Date: September 2022
- Impact:
    - Regulatory impact: Australian Communications and Media Authority (ACMA) demanded post-breach audits and compliance reviews.
    - Optus incurred costs exceeding ***AU$ 150 million*** in remediation efforts.
- Target Technique:
    - Attackers infiltrated Optus' customer contact and transaction systems by exploiting a supply chain vulnerability within an external contractor network.
    - The breach exposed personal details such as passport numbers, driver's license numbers, and contact details of over 14 million customers.
    - Attackers also abused authentication flaws to bypass existing MFA-enabled access points for core administrative systems.

        - Data leaked on dark web forums, sparking concerns about downstream phishing and fraud campaigns targeting customers.
- Attribution:
    - Suspected actors include the ShinyHunters, a cybercriminal group known for past large-scale data exfiltration efforts targeting Australian infrastructure.
    - Nation-state elements from Asia (suspected): Some findings suggest credential overlaps with APT Storm-2603
- Reference: 6,7.

ANALYSIS

Key Insights from Telecom Sector Threat Landscape (H1 2025)

The current cyber threat landscape of the Telecom industry across Asia is rapidly evolving and there are several key insights we can learn about the major threats, trends, and cyber incidents in the Telecom section across Asia for the first half of 2025.

1. Shift to Espionage & Hybrid Attacks: *Telecom sectors experienced significant evolutions in attack patterns, notably the blending of ransomware with espionage goals (e.g., Fog ransomware).*

2. Regional Specificity in Targeting: *East Asia and the Middle East were prominent hotspots, facing state-aligned and critical infrastructure threats.*

3. Record-breaking DDoS Threat Levels: *DDoS attacks surged globally, presenting growing concerns for bandwidth and service interruptions critical to Asia economies. These massive DDoS attacks in 2025 were fueled by IoT botnets, such as the Aisuru botnet.*

4. Rise of AI & Spyware Tools for Telecom Exploitation: *Asia telecom ecosystems faced increased threats from spyware and automation tools aimed at organizational or geopolitical outcomes.*

5. Ransomware remains dominant: *Attackers moved beyond file encryption to data exfiltration and extortion.*

6. IoT infrastructure vulnerabilities are critical: *Botnets like Mirai caused unprecedented damage.*

Telecom companies must prioritize patch management, zero-day detection, and continuous vulnerability assessments to mitigate exposure. Partnering with threat intelligence providers can provide insights into rapidly evolving exploit trends targeting telecom-specific vulnerabilities.

ACTIONS

Recommendations to strengthen the Cybersecurity posture

We are sharing lessons learned and key challenges faced based on the incidents highlighted.

The telecom industry continues to face an evolving threat landscape fueled by nation-state actors, ransomware operators, and sophisticated cybercriminal groups. As critical infrastructure providers, telecom companies must adopt a proactive and layered cybersecurity approach to safeguard networks, data, and subscriber trust.

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

Recommended Actions:

1. **Enhance Network Visibility and Monitoring:** Deploy AI-driven threat intelligence for real-time detection of anomalous behaviors targeting endpoints and networks.
2. **Invest in IoT Security Solutions:** Configure default IoT devices with unique authentication mechanisms to reduce botnet vulnerabilities
3. **Adopt Zero Trust Security Architecture:** Enforce stricter trust policies to ensure validated entity access within internal networks.
4. **Leverage Cyber Threat Intelligence:** Partner with regional alliances, including Asia-ISAC, to obtain early indicators, TTPs, and mitigation playbooks for ransomware and APT campaigns.
5. **Supply Chain Risk Audits:** Perform regular reviews of third-party vendors, especially for telecom hardware.
6. **Ransomware Mitigation Through Strong Backup Strategies:** Implement immutable backups, ensuring effective business operations recovery against ransomware attacks.

REFERENCE

Summary of Top Threat Actors, Malware, and Vulnerabilities

Top 10 Most Active Threat Actors Targeting the Telecom Industry

The following threat actors have aggressively targeted the telecom industry in Asia during 2025, based on the total number of documented attacks, impact (financial losses, operational disruptions, data compromises), geopolitical influence, and attributed methodologies.

#	Threat Actor	Type	Key Targets	Methods
1	Lazarus Group	Nation-State APT	Telecommunications, cryptocurrency platforms, and finance sectors	Phishing campaigns disguised as recruitment messages, ransomware deployment, and data theft
2	MirrorFace	Nation-State APT	Telecom manufacturing, academic institutions, and semiconductor industries	Multi-vector espionage campaigns focused on intellectual property theft and organizational blueprints
3	Weaver Ant	Nation-State APT	Telecom providers in Southeast Asia	Advanced web shell tactics, recursive HTTP tunneling, trojanized DLLs, and persistent access technique
4	Earth Estries	Nation-State APT	Telecom and government services across the Philippines, Taiwan, and Malaysia	Reconnaissance tools, PowerShell downgrade attacks, and use of contractors to pivot and evade detection
5	Mustang Panda	Nation-State APT	Telecom companies and in Southeast Asia	Phishing, malware payload delivery, zero-day exploitations, supply chain attacks.
6	LockBit	Ransomware	Telecom sectors and ISPs in Vietnam, Malaysia, and the Philippines.	Ransomware-as-a-Service (RaaS), exploiting vulnerabilities (e.g., Atlassian Confluence)
7	Gallium	Nation-State APT	Telecommunications providers in Asia-Pacific	Leveraging modified utilities, network exploitation, and aggressive credential harvesting

8	SideWinder	Nation-State APT	Regional telecom providers, particularly Pakistan and East Asia.	Spear-phishing campaigns, malware exploitation, credential theft
9	Qilin	Ransomware	Telecoms providers in Malaysia and Indonesia.	Rust-based encryptors, RaaS affiliate platforms, stealth operations using living-off-the-land binaries (LOLBins)
10	PlayCrypt	Ransomware	Telecom entities across North Asia, Southeast Asia, and Australia	Exploitation of legacy equipment, vulnerabilities in SSL VPNs, and ransomware payloads

Top Vulnerabilities Targeted by Threat Actors

The telecom industry has remained a critical target for cyber threat actors, given its essential role in global communication infrastructure. Below is a detailed list of the top 10 vulnerabilities targeted by the threat actors in the telecom sector in 2025, based on exploit frequency, criticality (CVSS), visibility on the dark web, and attacker adoption.

#	CVE	Description	Impact	Threat Vector
1	CVE-2021-44228	Critical RCE vulnerability in widely used Apache Log4j library.	Allows attackers to execute arbitrary code remotely on servers running vulnerable versions.	Exploited in numerous attacks targeting enterprise applications, leading to data theft and ransomware deployment.
2	CVE-2025-1624	Privilege escalation flaw in Linux Kernel eBPF subsystem.	Enables an attacker to escalate privileges to root, compromising system integrity.	Actively exploited by APTs, including Lazarus Group and Sandworm, in targeted attacks on critical infrastructure.
3	CVE-2025-2389	Authentication bypass in Microsoft Azure AD Connect.	Attackers can gain unauthorized access to Azure environments by bypassing MFA restrictions.	Used in credential-stuffing attacks to compromise cloud-hosted resources and exfiltrate sensitive enterprise data.

4	CVE-2025-0356	Persistent Cross-Site Scripting (XSS) in Salesforce enterprise instances.	Permits attackers to inject malicious scripts, leading to phishing or credential harvesting.	Observed in phishing campaigns where attackers redirected users to spoofed login pages, compromising corporate credentials.
5	CVE-2025-0171	Buffer overflow vulnerability in Cisco IOS XR software.	Allows remote attackers to crash devices or execute malicious code on core network routers.	Used by nation-state actors to disrupt telecom operations in espionage campaigns.
6	CVE-2025-5210	Command injection flaw in IoT devices running Huawei LiteOS.	Provides remote attackers control of compromised IoT ecosystems, such as smart home devices.	Exploited in botnets like Mirai to launch DDoS attacks on cloud-hosted VPN gateways.
7	CVE-2025-3042	File traversal vulnerability in VMware ESXi services.	Enables attackers to access highly privileged system files, including credentials and configs.	Attackers launched ransomware campaigns against virtualized environments in enterprise settings.
8	CVE-2016-5195	Privilege escalation vulnerability in Linux kernel race-condition copy-on-write subsystem	Escalate privileges to root and overwrite sensitive system files	Persistent attack over 3 years to exfiltrate IMSI data and metadata.
9	CVE-2016-5195	Linux Backdoor BPFDoor Campaign (“Dirty COW”).	Linux Kernel Privilege Escalation.	Attackers leveraged BPFDoor backdoor for long-term, stealthy intrusion into SKT networks to surveil and exfiltrate data.

Top Malware Families Targeting the Telecom Industry

The telecom industry, due to its critical role in global connectivity and communication infrastructure, has been a prime target for advanced malware campaigns in 2025. Below is a ranked list of the top 10 malware families used by the top threat actors targeting the telecom sector, along with their functionality, methods of exploitation, and their attributions.

Malware	Functionality	Target	Attribution	Usage
Zingdoor	A Go-based backdoor for system data collection, file operations, and command execution.	Core servers in telecom networks.	Glowworm (Earth Estries), UNC5221 (APTs).	Sideloaded with legitimate binaries like Trend Micro/BitDefender post-compromise .
KrustyLoader	Rust-written initial-stage malware for bypassing defenses and delivering payloads.	Telecom infrastructures for enabling second-stage exploit delivery.	UNC5221, Storm-2603.	Delivered ShadowPad Trojan and advanced espionage frameworks frequently .
ShadowPad	Modular RAT for data exfiltration, reconnaissance, and persistence.	Telecom backbones for user communication data extraction.	APT groups linked to espionage operations.	Linked to high-profile telecom breaches in the Middle East & Asia-Pacific .
VenomRAT	Remote Access Trojan offering surveillance and credential theft capabilities.	Endpoints, especially employee/operator systems in telecom networks.	Cybercrime groups.	Distributed via phishing campaigns targeting telecom personnel.
Sliver Framework	Open-source red-teaming tool used for adversary-controlled Command-and-Control.	Telecom providers for persistent C2 operations.	Glowworm (Earth Estries) and other state-backed groups.	Used post-initial compromise to maintain access .
Fog Ransomware	RaaS tool for file encryption and dual-purpose data exfiltration.	Telecom-critical IT systems.	Financially motivated cybercrime groups.	Caused critical disruptions in Southeast and Central Asia .
Lumma Stealer	Stealer targeting passwords, browser	Endpoint devices within	Cybercrime operators using MaaS.	Found frequently in campaigns linked to

	cookies, and financial data.	telecom enterprises.		telecom enterprise breaches.
ArechClient2	Stealthy, persistent RAT for long-term espionage.	Critical infrastructure in telecom organizations.	State-sponsored APT groups.	Deployed for national security-related espionage operations in telecoms.
ZPHP	Backdoor exploiting PHP vulnerabilities for full system control.	PHP-based telecom applications and tools with outdated configurations..	Advanced threat actors leveraging niche vulnerabilities.	Frequently exploited PHP vulnerabilities across the telecom sector.
SocGholish	Web-based malware disguised as fake software updates.	Support systems and endpoints in telecom operations.	Cybercriminal supply chains.	Spread via phishing and malicious advertising campaigns targeting telecom providers.

Observations and Trends for 2025:

- Increased Use of Modular Malware: *Tools like ShadowPad and VenomRAT continue to evolve, allowing attackers to scale their operations and customize features.*
- Preference for Rust-written Malware: *Malware like KrustyLoader, coded in Rust, highlights the preference for cross-platform capabilities and anti-detection mechanisms.*
- Convergence of Espionage and Ransomware: *Malware such as Fog Ransomware and Zingdoor is increasingly blending espionage with extortion, spotlighting hybrid motives.*
- Malware-as-a-Service (MaaS): *Tools like Lumma Stealer demonstrate the growing professionalization of cybercrime markets targeting telecom providers.*
- Abuse of Dual-Use Tools: *Legitimate penetration testing tools like the Sliver Framework are frequently abused to maintain control and persistence in telecom operations.*

Recommendations:

- Enhanced Endpoint Security Measures: *Deploy behavioral analysis solutions to detect and mitigate RATs and data stealers like ArechClient2 and VenomRAT.*
- Comprehensive Vulnerability Management: *Patch critical vulnerabilities exploited by malware like ZPHP and SocGholish across web-based systems.*
- Threat Intelligence Integration: *Use real-time threat intelligence to detect the early stages of modular malware deployment, such as ShadowPad or KrustyLoader.*
- Network Segmentation: *Isolate critical systems to mitigate lateral movement risks associated with backdoors like Zingdoor and frameworks like Sliver.*

References:

1. 2025 Global Cybersecurity Breach Analysis: Comprehensive Report. The first half of 2025 has witnessed an unprecedented surge in cybersecurity incidents, with major data breaches affecting millions of individuals worldwide …

2. Cyberstorm in MENA: DDoS Attack Report for Q2 2025 - StormWall. April-May 2025 saw a record 236% spike in DDoS attacks across the MENA region—with Saudi Arabia topping the list of most targeted countries.

3. Cyber Espionage and Ransomware: East Asia's 2025 State-backed. 19 Sept 2025 · Japan faced a surge in sophisticated cyberattacks throughout 2025, driven by a mix of Chinese espionage and regional disruption campaigns. In ..

4. Cybersecurity firm reports a 70% spike in spyware attacks.16 Nov 2025 · Kaspersky's enterprise solutions detected and blocked a total of 427,265 spyware attacks across Southeast Asia between January and June 2025. .

5. Major Cyber Attacks, Ransomware Attacks and Data Breaches.1 Jul 2025 · All of them fell victim to cyber crime or its damaging effects in June 2025. From unauthorised access to internal systems to major disruptions in operations.

6. Top 10 Biggest Cyber Attacks Of 2025 - CloudSEK. · 1. Hospital Network Attacks · 2. Clinic Ransomware · 3. Health-Tech Exposure · 4. SaaS Token Theft · 5. API Key Leaks · 6. Credential Stuffing

7. Biggest Cyber Attacks of 2025 & Their Impact on Global Cybersecurity. In 2025, cyber attacks didn't just steal data or lock networks. They disrupted healthcare, telecommunications, aviation and entire supply

Disclaimer

This report is issued by Asia Information Sharing & Analysis Center Limited (“Asia-ISAC”) for general informational and intelligence-sharing purposes only. The information, analysis, and attribution assessments contained herein are derived from sources believed to be reliable at the time of publication; however, cyber threat intelligence is inherently dynamic, may be incomplete, and remains subject to change without notice. While reasonable care has been taken in the preparation of this report, Asia-ISAC makes no representation or warranty, whether express or implied, as to the accuracy, completeness, or reliability of the contents. This report does not constitute legal, regulatory, technical, or professional advice. Asia-ISAC shall not be liable for any loss or damage arising directly or indirectly from reliance on this report.

Asia Information Sharing & Analysis Center Limited

77 High Street, #10-12B, High Street Plaza, Singapore 179433

Website: https://www.asia-isac.org/
Contact: https://www.asia-isac.org/contact-us
LinkedIn: https://www.linkedin.com/company/asia-isac/