Cyber Threat Landscape Telecom - 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 Telecoms Sector 2025

$1.5 Trillion

Consumers served

2.0 Billion

Telecom Companies in Asia

1,000

What this report covers

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

- Regional coverage across East Asia, Southeast Asia, South Asia, West Asia (Middle East) and Oceania.
- Impacts spanning telecom and 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.

Key findings and highlights

The year 2025 marked a significant escalation point for the telecom sector 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.

The 2025 Asia telecom sector key trends 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 West Asia 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's economies.
- **Rise of Spyware Tools for Telecom Exploits:** Asia telecom ecosystems faced increased threats from spyware.

Major attacks and business impact

The Asia-Pacific region has seen a sharp rise in high-profile cyberattacks targeting telecommunications and critical infrastructure. These incidents underscore the growing vulnerability of essential services to sophisticated threat actors, with consequences ranging from massive data breaches to operational paralysis — affecting tens of millions of consumers and costing hundreds of millions of dollars in financial losses and remediation.

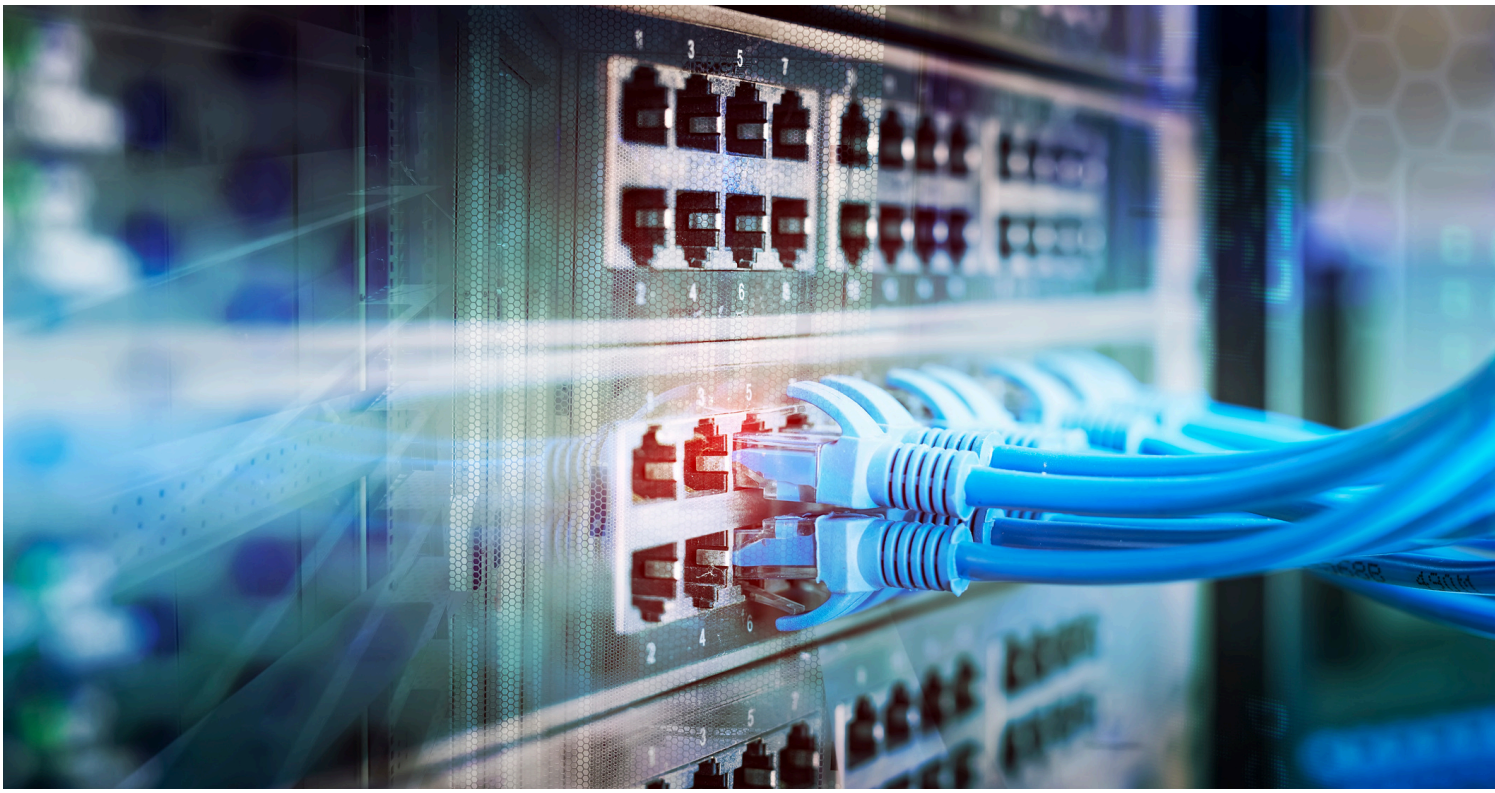
- **SK Telecom HSS and USIM Breach (South Korea)** resulted in penalties of US$97 million, and over 23 million subscribers received free USIM replacements.
- **Optus Cyber Attack (Australia)** resulted in costs exceeding US$107 million in remediation efforts and impacted 14 million customers (2022 incident included for relevance and context).
- **KLIA Ransomware Attack (Malaysia)** disrupted the aviation telecom systems in the Kuala Lumpur International Airport resulting in major flight delays and significant service outages.

These three incidents collectively illustrate a broadening threat landscape — from subscriber data theft (SK Telecom), to mass personal data exposure (Optus), to operational infrastructure disruption (KLIA). As telecom systems become ever more deeply embedded in national infrastructure, the stakes of inadequate cybersecurity continue to rise dramatically.

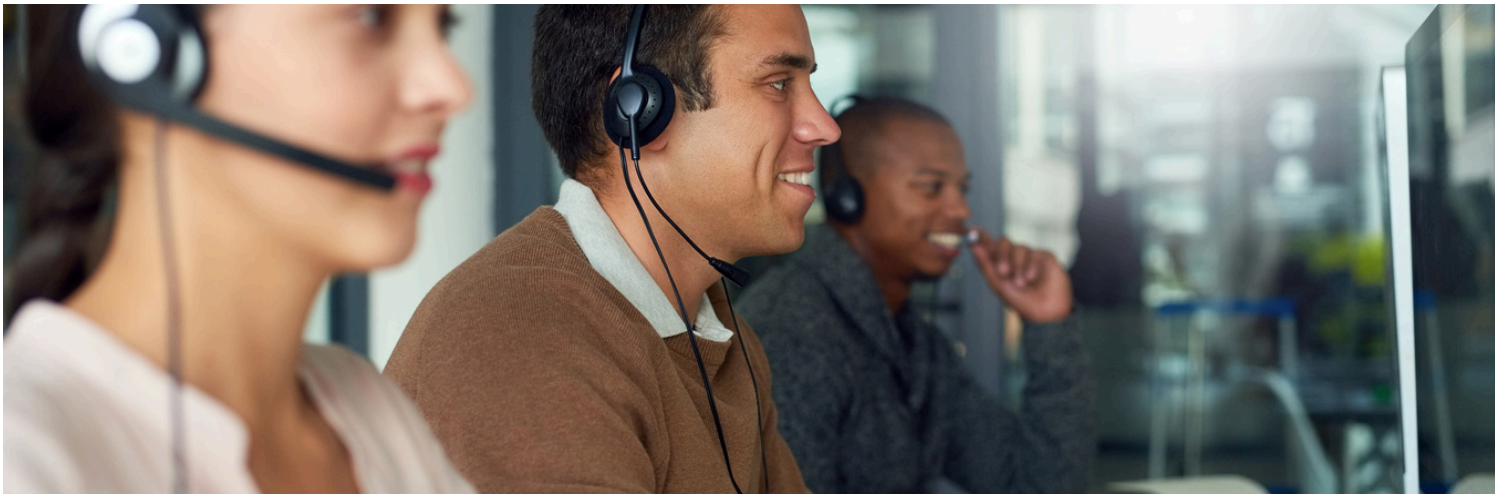
Actionable intelligence in this report

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

- **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 sector.
- **Recommendations** mapped to observed threat behaviors to strengthen resilience.



Key Threat Landscape Insights



Threat Analysis

The Asian telecommunications sector in 2025 faces a threat environment that is increasingly complex, targeted, and high-impact. Cyberattacks are no longer isolated criminal opportunism — they have evolved into sophisticated, multi-layered operations that blend financial motives with geopolitical agendas. Threat actors, increasingly including state-aligned groups, are deliberately targeting telecom infrastructure as a strategic lever: disrupting economies, harvesting intelligence, and exploiting the region's vast and rapidly expanding digital connectivity.

40%

2025 estimate increase in telecom cyber incidents

KEY INSIGHTS:

- **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).
- **Regional Specificity in Targeting:** East Asia and West Asia were prominent hotspots, facing state-aligned and critical infrastructure threats.
- **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.
- **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.
- **IoT infrastructure vulnerabilities are critical:** Botnets like Mirai caused unprecedented damage.

The convergence of these trends reflects a maturing threat landscape in which telecommunications infrastructure has become a high-value strategic target. As the backbone of data flows and communications, disruptions to telecom networks can have cascading impacts across financial systems, public services, supply chains, and national security. Addressing these risks requires a more proactive approach to cybersecurity and crisis response planning.

Summary of Major Incidents

Summary of key cyberattacks for the telecom sector with the most severe impacts in terms of operational disruptions, financial losses, and/or private 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 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.

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 US$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

10 HRS
outage duration

US$10M
ransom demand

2. Fog Ransomware Attack – 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 were identified in earlier intelligence reporting)
- Impact: Theft of 4GB of sensitive corporate telecom business data, later published on the dark web.
- 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 – West Asia

- Date: April-May 2025
- Impact: A 236% increase 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 West Asia.
- 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 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

- 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 – West Asia

- 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

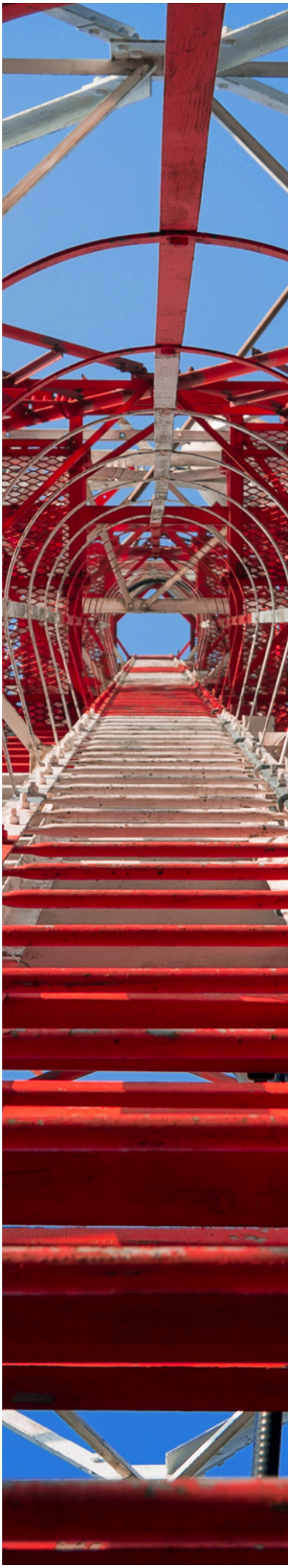
- Date: January-June 2025
- Impact: A 70% increase in spyware attacks on telecom service providers in countries like Indonesia, Thailand, and Vietnam.
- Target and Technique: Cybercriminals focused on mobile devices and backbone telecom services to intercept communications and steal corporate and user 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 undetected. Exfiltration of 26.96 million IMSI records and 9.82 GB of USIM metadata allowed attackers to potentially perform SIM-swapping attacks and impersonation.
- 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 US$107 million (estimated equivalent) 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



Recommendations

Strengthen the cybersecurity posture

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

The telecom sector 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.

Zero Trust Security Architecture

Enforce a Zero-Trust Framework and implement strict Identity and Access Management (IAM) solutions coupled with multi-factor authentication (MFA).

IoT Security

Configure default IoT devices with unique authentication mechanisms to reduce botnet vulnerabilities.

Cyber Threat Intelligence

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

Network Visibility and Monitoring

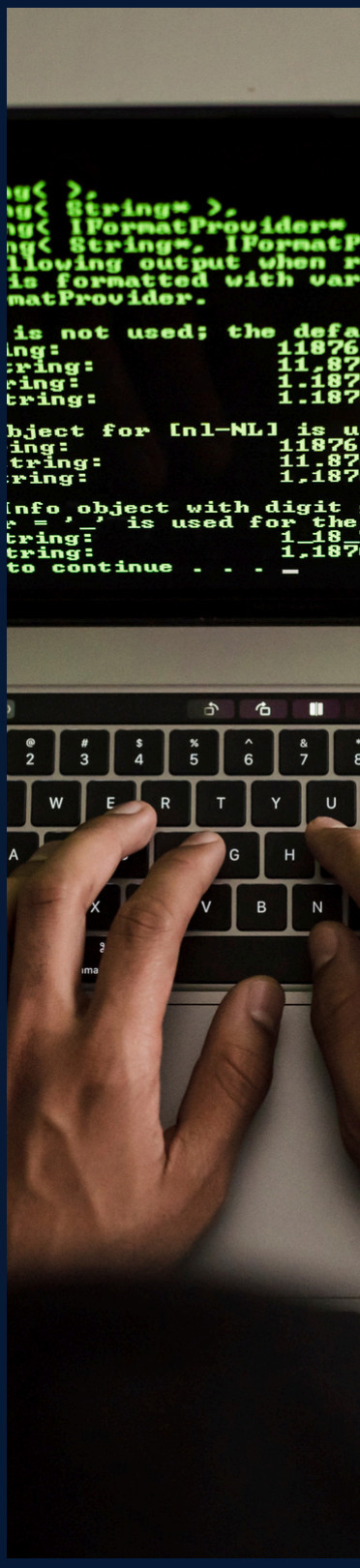
Deploy AI-driven real-time detection of anomalous behaviors targeting endpoints and networks.

Supply Chain Risk Audits

Perform regular reviews of third-party vendors, especially for telecom hardware.

Summary of Top Threat Actors, Malware, and Vulnerabilities

Top 10 Most Active Threat Actors Targeting the Telecom Sector



Asia's telecommunications sector in 2025 is being pursued by a concentrated and highly capable set of threat actors — ranging from state-sponsored Advanced Persistent Threat (APT) groups executing long-term espionage campaigns, to ransomware syndicates running industrialized, profit-driven attack operations.

These threat actors are identified based on Asia-ISAC analysis of incident frequency, operational impact, and corroborated intelligence from partner and open-source reporting across the region.

What makes the current threat landscape particularly dangerous is the diversity of both motivation and methodology: nation-state actors such as Lazarus Group, MirrorFace, and Weaver Ant operate with near-unlimited patience and resources, embedding themselves deep within telecom infrastructure to steal intellectual property, harvest credentials, and establish persistent footholds for future exploitation.

Ransomware groups like LockBit, Qilin, and PlayCrypt have industrialized their operations through Ransomware-as-a-Service (RaaS) models, enabling even low-skill affiliates to launch devastating attacks against telecom operators across the region.

Together, these identified groups represent the most active and capable actors in the cyber threat environment facing Asia's telecom sector. They collectively target operators across at least 15 countries, exploiting everything from unpatched legacy equipment to sophisticated supply chain vulnerabilities, and are driven by objectives spanning financial gain, geopolitical intelligence, and strategic infrastructure disruption.

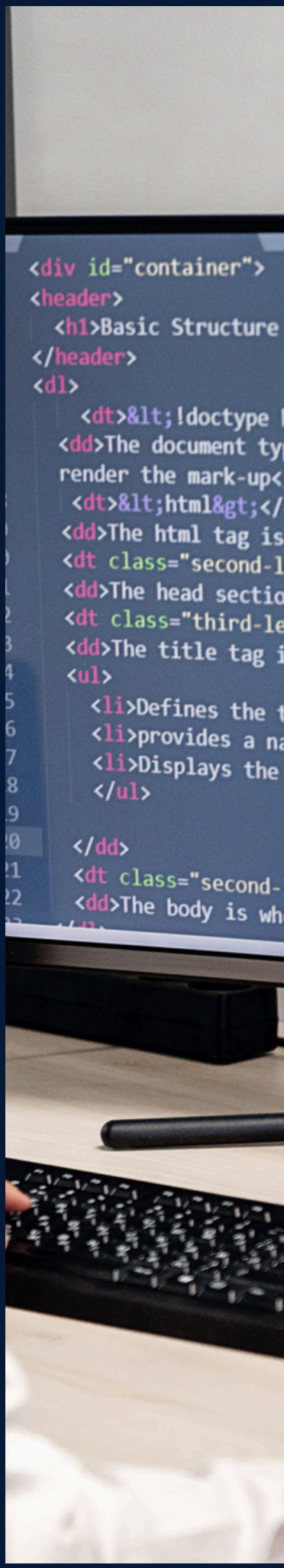
Key Observations

Nation-State Dominance — Espionage Outweighs Financial Crime: The threat actor landscape is overwhelmingly dominated by state-sponsored APT groups, with 7 out of 10 identified actors being nation-state affiliated. Unlike financially motivated ransomware gangs, these actors — Lazarus Group, Gallium, and SideWinder — operate with strategic patience, maintaining silent persistent access within networks over extended periods.

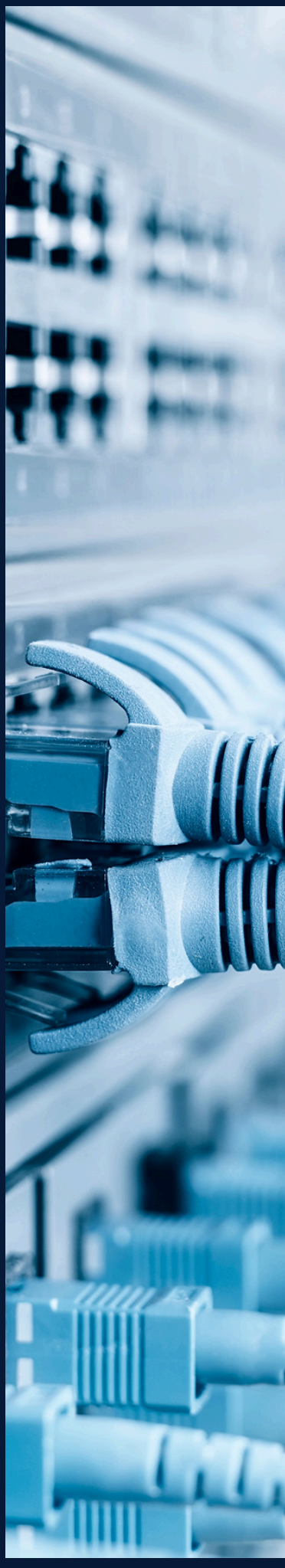
Southeast Asia as the Primary Battleground: Across all 10 threat actors, Southeast Asia emerges as the most consistently targeted sub-region — with the Philippines, Malaysia, Vietnam, Indonesia, and Thailand appearing repeatedly across target profiles. This concentration reflects Southeast Asia's combination of rapidly expanding 5G infrastructure, relatively immature cybersecurity posture, fragmented regulatory environments, and heightened geopolitical significance.

Convergence of APT & Ransomware Tactics: Perhaps the most alarming development is the blurring of boundaries between nation-state and criminal methodologies. Ransomware groups like Qilin and LockBit are adopting APT-grade techniques — stealth operations, living-off-the-land binaries (LOLBins), and Rust-based encryptors — while nation-state actors increasingly deploy ransomware as a cover for espionage, using it to destroy forensic evidence or distract defenders while exfiltrating sensitive data.

Threat Actor	Type	Key Targets	Methods
Lazarus Group	Nation-State APT	Telecommunications, cryptocurrency platforms, and finance sectors	Phishing campaigns disguised as recruitment messages, ransomware deployment, and data theft
MirrorFace	Nation-State APT	Telecommunications, cryptocurrency platforms, and finance sectors	Multi-vector espionage campaigns focused on intellectual property theft and organizational blueprints
Weaver Ant	Nation-State APT	Telecom providers in Southeast Asia	Advanced web shell tactics, recursive HTTP tunneling, trojanized DLLs, and persistent access technique
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



Threat Actor	Attack Type	Techniques	Impact
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
Mustang Panda	Nation-State APT	Telecom companies and in Southeast Asia	Phishing, malware payload delivery, zero-day exploitations, supply chain attacks
LockBit	Ransomware	Telecom sectors and ISPs in Vietnam, Malaysia, and the Philippines	Ransomware-as-a-Service (RaaS), exploiting vulnerabilities (e.g., Atlassian Confluence)
Gallium	Nation-State APT	Telecommunications providers in Asia-Pacific	Leveraging modified utilities, network exploitation, and aggressive credential harvesting
SideWinder	Nation-State APT	Regional telecom providers, particularly Pakistan and East Asia	Spear-phishing campaigns, malware exploitation, credential theft
Qilin	Ransomware	Telecoms providers in Malaysia and Indonesia	Rust-based encryptors, RaaS affiliate platforms, stealth operations using living-off-the-land binaries (LOLBins)
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 sector 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.

The vulnerabilities described in this section represent commonly observed patterns based on aggregated threat intelligence and may include representative or modeled scenarios.

Key Observations
Legacy & Unpatched Vulnerabilities Remain the Most Dangerous Entry Points: The presence of CVE-2016-5195 (Dirty COW) — a nearly decade-old vulnerability — appearing in 2025 attacks, including the SK Telecom BPFDoor intrusion, is a very alarming signal in this dataset. Despite being publicly disclosed and patched in 2016, it was successfully exploited for over 3 years.
The Attack Chain Has Matured — From Initial Access to Full Infrastructure Control: Threat actors are executing sophisticated, multi-stage attack playbooks with increasing precision across Asia's telecom networks. No single CVE tells the full story — it is their combined, chained exploitation that makes modern attacks against telecom infrastructure so difficult to detect and contain.
The Attack Surface Has Expanded Beyond Traditional Network Boundaries: The CVE landscape in 2025 reveals that the telecom threat surface now extends far beyond core network equipment into cloud platforms, IoT ecosystems, virtualized environments, and enterprise SaaS applications.

CVE	Description	Threat Vector	Impact
CVE-2016-5195	Linux Backdoor BPFDoor Campaign (“Dirty COW”	Privilege escalation vulnerability in Linux kernel race-condition copy-on-write subsystem	Enables an attacker to escalate privileges to root, compromising system integrity

CVE	Description	Threat Vector	Impact
CVE-2021-44228	Critical RCE vulnerability in widely used Apache Log4j library	Exploited in numerous attacks targeting enterprise applications, leading to data theft and ransomware deployment	Allows attackers to execute arbitrary code remotely on servers running vulnerable version
CVE-2025-1624	Privilege escalation flaw in Linux Kernel eBPF subsystem	Actively exploited by APTs, including Lazarus Group and Sandworm, in targeted attacks on critical infrastructure	Enables an attacker to escalate privileges to root, compromising system integrity
CVE-2025-2389	Authentication bypass in Microsoft Azure AD Connect	Used in credential-stuffing attacks to compromise cloud-hosted resources and exfiltrate sensitive enterprise data	Attackers can gain unauthorized access to Azure environments by bypassing MFA restrictions
CVE-2025-0356	Persistent Cross-Site Scripting (XSS) in Salesforce enterprise instances	Observed in phishing campaigns where attackers redirected users to spoofed login pages, compromising corporate credentials	Permits attackers to inject malicious scripts, leading to phishing or credential harvesting
CVE-2025-0171	Buffer overflow vulnerability in Cisco IOS XR software	Used by nation-state actors to disrupt telecom operations in espionage campaigns	Allows remote attackers to crash devices or execute malicious code on core network routers
CVE-2025-5210	Command injection flaw in IoT devices running Huawei LiteOS	Exploited in botnets like Mirai to launch DDoS attacks on cloud-hosted VPN gateways	Provides remote attackers control of compromised IoT ecosystems, such as smart home devices

Top Malware Families Targeting the Telecom Sector

The telecom sector, 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 prioritized list of top 10 malware families used by the top threat actors targeting the telecom sector, along with their functionality, methods of exploitation, and their attributions.

This section profiles each malware family, draws cross-incident patterns, and identifies the key insights and trends influencing the telecom malware threat landscape into 2026.

Insights & Trends:

- **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:

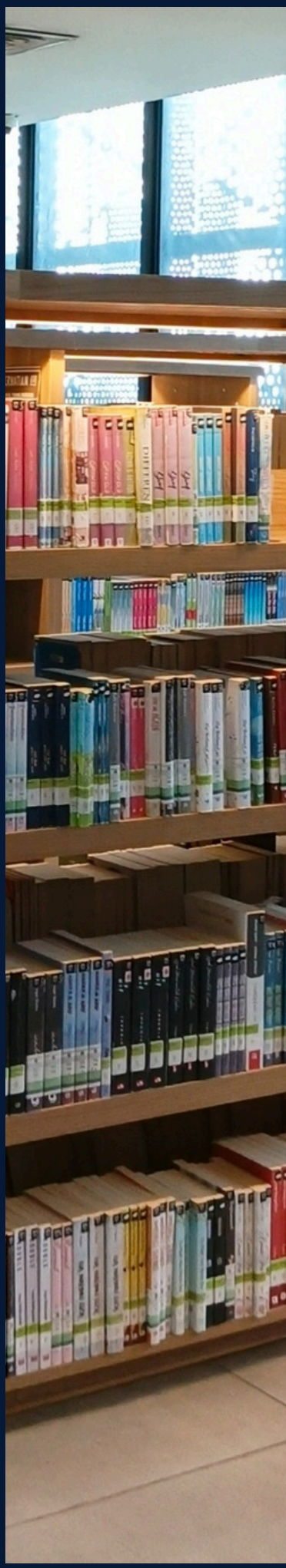
- **Enhanced Endpoint Security Measures:** Deploy behavioral analysis solutions to detect and mitigate RATs and data stealers like ArechClient2 and VenomRAT.
- **Comprehensive Vulnerability Management:** Patch critical vulnerabilities exploited by malware like ZPHP and SocGholish across web-based systems.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

Name	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)	Loaded with legitimate binaries like Trend Micro/Bit Defender
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 framework
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 West Asia & Asia-Pacific
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

Malware Name	Type	Techniques	Target	Impact
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 cookies, and financial data	Endpoint devices within telecom enterprises	Cybercrime operators using MaaS	Found frequently in campaigns linked to 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

References:

1. 2025 Global Cybersecurity Breach Analysis: Comprehensive Report. The year 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 Cyberattacks, 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 Cyberattacks 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 Cyberattacks of 2025 & Their Impact on Global Cybersecurity. In 2025, cyberattacks didn't just steal data or lock networks. They disrupted telecom, telecommunications, aviation and entire supply.
10. Data Breaches 2025: Biggest Cybersecurity Incidents So Far. Millions of consumers were victims of these data breaches, with causality linked to unauthorized access and ransomware.
13. ToolShell vulnerability leads to compromise. ToolShell vulnerability exploited shortly after its public disclosure in July 2025 to breach a telecommunications company.



Contact Us

Asia-ISAC

Website

www.asia-isac.org

Email

help@asia-isac.org

LinkedIn

www.linkedin.com/company/asia-isac