ThreatBook

2026 Mid-Year Asia-Pacific Threat Landscape Report

Australia · Singapore · Indonesia · Malaysia · Hong Kong

July 2026

Executive Summary

This report covers the period from June 2025 to June 2026 and presents a comprehensive assessment of cybersecurity threats across the Asia-Pacific region, drawing on 15,205 recorded security incidents. The threat landscape showed a structural increase in risk, driven by rapid digital-economy expansion, sustained geopolitical friction, reconfiguration of supply chains, and the proliferation of digital identity and mobile finance.

Key findings:

- **Data breaches** dominated the threat landscape, accounting for 39.91% of all incidents (8,856 cases). 80% originated from active system intrusion rather than misconfiguration, and 51% of breaches involved ransomware.
- **Ransomware** accounted for 18.33% (4,068 incidents). Despite law-enforcement disruption of major groups, over 120 new ransomware brands emerged, and victim counts surged 58% year over year. The dual-extortion model—encryption and exfiltration—is now standard.
- **Phishing** reached 18.30% (4,061 incidents), with AI-generated phishing emails accounting for 80% of detected volume and achieving click rates exceeding 50%. Attack channels have diversified beyond email into SMS, QR codes, instant messaging, and OAuth abuse.
- **APT activity** accounted for 17.87% (3,966 incidents), with Lazarus, APT36, Kimsuky, Salt Typhoon, and SideWinder among the most active groups. Some state-linked actors are shifting from intelligence collection toward persistent pre-positioning in communications backbones and critical infrastructure.
- **Supply chain attacks** (2.16%) remained low in volume but high in blast radius, with SaaS integration chains, software dependency poisoning, and emerging AI supply chain vectors all recording significant incidents.
- The **top five target countries**—China, India, Australia, Japan, and South Korea—accounted for 61.78% of all incidents. Government, technology, and financial services were the three most targeted sectors.

The report provides in-depth country analyses for Australia, Singapore, Indonesia, Malaysia, and Hong Kong, examining attack-type composition, industry targeting, active ransomware groups, and APT threats specific to each market.

1. Overall Threat Landscape

During the reporting period, cybersecurity risk in the Asia-Pacific region showed a structural increase. Rapid digital-economy expansion, sustained spillover from geopolitical friction, reconfiguration of manufacturing and technology supply chains, and the spread of digital identity and mobile finance made government, financial services, technology, telecommunications, and manufacturing persistent high-value targets for attackers. Network attacks are shifting from single-system intrusions toward systemic pressure centered on identity, data, supply chains, connectivity, and business continuity. At the same time, cross-border criminal ecosystems in Asia-Pacific are accelerating industrialization. AI deepfake fraud, industrialized scam centers, ransomware, business email compromise, infostealers, and DDoS remain expanding cybersecurity threats across the region.

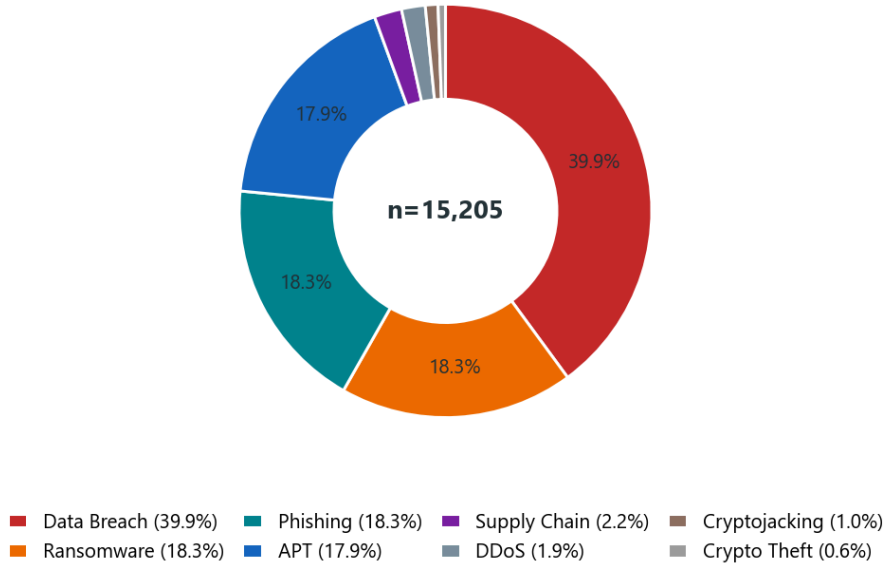
From a regional economic structure perspective, Asia-Pacific is a major hub for global manufacturing, electronics, semiconductor assembly and test, automotive components, shipping and logistics, cloud services, data centers, and cross-border finance. As supply chains disperse into Southeast and South Asia, more mid-sized manufacturers, IT service providers, outsourcers, logistics firms, and local fintech companies have entered attackers' field of view. Software vendors, cloud accounts, remote-management platforms, file-transfer systems, customer-service platforms, code repositories, API tokens, and third-party service providers are becoming key entry points attackers use to reach multiple downstream organizations.

This report recorded 15,205 security incidents over the past year. The data show that Asia-Pacific risk is concentrated in four main activity types: data breaches, ransomware, phishing, and APT activity. Data breach incidents totaled 8,856, accounting for 39.91% and representing the dominant risk form; ransomware incidents totaled 4,068, or 18.33%; phishing incidents totaled 4,061, or 18.30%; and APT incidents totaled 3,966, or 17.87%. In practice, these incident types interconnect during real attacks: phishing and credential exposure provide entry, system intrusion and malware establish control, stolen data feeds ransomware, fraud, and dark-web trade, and APT activity maintains long-term access against government, telecommunications, technology, finance, and critical infrastructure targets.

Rank	Incident Type	Count	Share
1	Data Breach	8,856	39.91%
2	Ransomware	4,068	18.33%
3	Phishing	4,061	18.30%
4	APT	3,966	17.87%
5	Supply Chain Attack	479	2.16%
6	Denial of Service	412	1.86%
7	Cryptojacking	220	0.99%

Rank	Incident Type	Count	Share
8	Cryptocurrency Theft	129	0.58%

Figure 1-1 · Incident Type Share (%)



Source: ThreatBook APAC threat intelligence · n = 15,205 incidents

Figure 1-1. Incident type share (%)

Data breach incidents hold absolute dominance. With 8,856 incidents and a 39.91% share, data breaches rank first among all incident types, accounting for nearly 40% of total incidents and far exceeding any other single threat category. Industry research data indicate that during 2025, 80% of data breaches in the region originated from system intrusion—attackers actively breached network perimeters, moved laterally, and exfiltrated data rather than relying on simple misconfigurations or accidental exposure. During these breach campaigns, malware use rose from 58% in the prior year to 83%, indicating that most intrusions involved malware deployment and execution; among all malware observed, ransomware was especially prominent, with 51% of breach incidents involving ransomware attacks in which attackers encrypted or stole data and then demanded payment. From an initial-access perspective, 31% of breaches began with software vulnerability exploitation, and zero-day flaws in perimeter devices and VPNs became primary breakthrough points. Monitoring data from this reporting period indicate that this structural pattern is continuing and deepening. Once customer identity data, business files, source code, supply chain materials, and internal credentials are exposed, they quickly enter downstream stages such as fraud, ransom negotiation, dark-web trade, and secondary intrusion, forming a "breach-exploitation-rebreach" cycle that causes long-cycle security and trust losses far beyond the incident itself.

Ransomware ranked second with 4,068 incidents and an 18.33% share, reflecting that Asia-Pacific has become an important monetization market for data extortion and one of the fastest-growing, highest-efficiency regional markets in the global ransomware ecosystem. In recent years, international law-enforcement operations disrupted major ransomware groups such as LockBit and ALPHV/BlackCat, yet total attack volume rose rather than fell—after large affiliate networks dispersed, more than 120 new ransomware brands emerged, and victim counts surged 58% year over year. From an initial-access perspective for ransomware, vulnerability exploitation remained the most common technical root cause for the third consecutive year, accounting for 32%; stolen credentials accounted for 23%, malicious email for 19%, and phishing for 18%; meanwhile, 57% of initial ransom demands and 52% of actual payments reached USD 1 million or more. For Asia-Pacific customers, the practical pressure from ransomware attacks now extends beyond whether systems are encrypted, and increasingly comes from public data release, customer notification, regulatory disclosure, supply chain delivery disruption, business interruption, and reputational loss.

Phishing incidents reached 4,061, accounting for 18.30%, nearly matching ransomware in scale. E-commerce platform impersonation accounted for nearly half of phishing incidents; online payment and financial-banking targets together accounted for about 30% of regional phishing. Voice phishing, SMS phishing, and QR-code phishing continued to grow rapidly, and 30% of phishing attacks no longer relied solely on email but extended across SMS, QR codes, instant messaging, phone-based social engineering, mobile app installation, cloud-account authorization, and OAuth-connected application abuse across multiple communication channels. Because mobile users in Asia-Pacific are accustomed to handling various transactions through digital service channels, the threat was further amplified: in markets such as Singapore, Hong Kong, and Thailand, attackers distributed malicious APKs through fake government notices, tax reminders, bank verification prompts, wedding invitations, and even power-bank rental QR codes, intercepted OTPs, and took over financial accounts. AI involvement is also fundamentally increasing phishing success rates. AI-generated phishing emails accounted for 80% of detected phishing volume, with click rates exceeding 50%.

APT incidents ranked fourth with a 17.87% share. Over the past year, Asia-Pacific remained at the intersection of U.S.-China technology competition, semiconductor supply chain adjustment, tensions related to the South China Sea and Taiwan Strait, security issues on the Korean Peninsula, South Asian geopolitical confrontation, and maritime-rights friction in Southeast Asia. Major APT threats targeting Asia-Pacific came from persistently active groups including Lazarus, APT36, Kimsuky, APT37, APT41, Salt Typhoon, and SideWinder, with primary targeting of government and public services, telecommunications and communications infrastructure, technology and semiconductor supply chains, financial services and crypto assets, and defense-industrial and energy sectors. Lazarus focused mainly on South Korea, Hong Kong, and Singapore, emphasizing intelligence theft and financial theft, with especially prominent activity in cryptocurrency. During this reporting period, in November 2025 the group compromised the hot wallet of South Korea's largest exchange Upbit and stole approximately USD 36 million in Solana-ecosystem tokens; in April 2026, Lazarus breached Drift Protocol after months of social-engineering penetration against the target security team and extracted USD 285 million within 12 minutes; in the same month it also exploited a single-point cross-chain bridge validation flaw to attack Kelp DAO and steal USD 292 million. In April 2026 alone, Lazarus stole approximately USD 577 million across two DeFi attacks,

accounting for 76% of global cryptocurrency theft during the same period. In addition, SideWinder conducted multiple waves of phishing attacks against diplomatic targets in Pakistan, Sri Lanka, and Bangladesh from June through August 2025 during the India-Pakistan conflict, with attack tempo closely aligned to the conflict timeline; APT36 continued targeting South Asian government and defense targets with remote-access tools such as CrimsonRAT amid India-Pakistan geopolitical confrontation; APT41 targeted government, technology, and telecommunications targets in Asia-Pacific through public application vulnerabilities and supply chain intrusion; and Mustang Panda quickly resumed targeted attacks against Asia-Pacific and Japan using a new modular .NET RAT framework after law-enforcement disruption. Activity by Salt Typhoon (confirmed in August 2025 to have compromised more than 200 telecommunications organizations across 80 countries) and Volt Typhoon (characterized in early 2026 as "pre-positioning ahead of conflict") indicates that some state-linked attackers in Asia-Pacific are no longer pursuing traditional intelligence theft alone, but are establishing persistent strategic presence in communications backbones and critical infrastructure that can be activated if geopolitical conflict escalates.

Supply chain attacks accounted for 2.16%. Although lower in volume than the top four categories, their risk must be measured by impact radius. During the reporting period, affected industries concentrated in technology, government, financial services, manufacturing, and Technology-Cybersecurity. Asia-Pacific supply chain attacks can be summarized in three main lines. First, third-party service providers and SaaS integration chains: a Philippine outsourced customer-service platform used by Australia's Qantas was compromised, leading to a breach affecting 5.7 million customer records; stolen OAuth tokens related to Salesloft and Drift affected more than 700 downstream organizations; and attacks against a South Korean hosting provider affected multiple financial institutions—outsourced customer service, CRM integration, and hosting providers are becoming transmission nodes that convert single-platform risk into multi-customer data risk. Second, software dependency and distribution chains: the Shai-Hulud worm self-propagated from a single npm package to more than 800 packages and extended to PyPI; the Notepad++ update mechanism was hijacked by Lotus Blossom to deliver targeted payloads to Southeast Asian government and telecommunications targets; and Lazarus continued disguising popular libraries on npm to induce developers to install backdoors—package managers, update mechanisms, and developer credentials have become entry points for penetrating technology firms and government and financial system vendors. Third, AI supply chain chains: a LiteLLM supply chain intrusion exposed 500,000 API keys and cascaded to downstream AI data firms; malicious model repositories appeared on Hugging Face; and batch malicious Agent plugins appeared in the OpenClaw skills marketplace—model components, inference services, and Agent tools are becoming new trusted intermediary layers, while traditional security tools show extremely low detection rates for such threats. Asia-Pacific concentrates large volumes of software outsourcing, fintech R&D, manufacturing collaboration, and enterprise AI applications; compromise of any intermediate node in the supply chain can propagate rapidly downstream along outsourcing, integration, and dependency relationships.

The most prominent trend in Asia-Pacific DDoS attacks is a shift from technical incidents to geopolitical tools. Asia-Pacific DDoS attacks grew 106% year over year in 2025, with increases concentrated in geopolitical conflict time windows: the India-Pakistan conflict, Thailand-Cambodia border confrontation, Taiwan Strait tensions, and Russia-Japan friction each produced corresponding DDoS attack surges in

cyberspace. This indicates that DDoS in Asia-Pacific is no longer only a technical method, but is becoming a normalized digital instrument of geopolitical expression—when conflict escalates, DDoS attacks almost synchronously begin, with multi-directional, multi-camp hacker groups attacking one another and forming a "digital accompanying battlefield." Meanwhile, DDoS attacks themselves are evolving from "broad flooding" toward "precision strikes": Q4 2025 recorded the largest single attack on record at 31.4 Tbps, botnet average scale reached 120,000 devices (up 60% year over year), but API-layer attacks grew 86% year over year, as attackers shifted firepower from the bandwidth layer to the business-logic layer. By industry impact, government (21%), telecommunications (18%), and financial services (16%) were the top three Asia-Pacific DDoS targets; financial services DDoS attacks in the second half of the year surged 245% year over year, and median attack duration increased 738%—the threat DDoS poses to financial-service availability is upgrading from "brief interruption" to "sustained pressure."

Structural change in cryptojacking incidents is reflected in attack-surface migration: from end-user browsers and personal devices toward cloud workloads and containerized infrastructure. The underlying logic is economic efficiency—cloud instances provide far greater compute than personal endpoints, and after compromise attackers do not bear electricity or hardware costs; victims effectively "pay" mining costs through abnormally inflated cloud bills (data show a single incident can cause more than USD 300,000 in cloud computing charges). During this reporting period, exposed Docker APIs, Kubernetes misconfigurations, and stolen cloud credentials became the three main entry points, and professional mining groups such as TeamTNT, WatchDog, and Kinsing continued building automated attack chains around these entry points—from discovery of exposed instances to miner deployment in as little as 10 minutes. More notably, cryptojacking attacks are extending into AI infrastructure: in April 2026, the ComfyUI botnet deployed dual-currency miners on more than 1,000 publicly exposed AI tool instances, and malicious containers also exhibited worm characteristics for automatic propagation. Asia-Pacific cloud infrastructure is large in scale and growing faster than the global average; many small and medium enterprises lack mature practices in container orchestration and cloud identity management, making the region a high-incidence area for cloud cryptojacking attacks. From a defense perspective, cryptojacking incidents themselves have limited harm, but they often serve as an "early indicator" of cloud security posture—instances that can be mined can also be used for data theft, backdoor implantation, or lateral movement; the low barrier to cryptojacking precisely exposes deeper cloud security gaps.

2. Target Country/Region Distribution

By target country and region distribution, China, India, Australia, Japan, and South Korea ranked in the top five, with a combined share of approximately 61.78%. This distribution indicates that Asia-Pacific attack activity concentrates in large digital economies, manufacturing powers, high-value data markets, and regional critical infrastructure nodes.

Rank	Country/Region	Count	Share
1	China	3,299	15.39%

Rank	Country/Region	Count	Share
2	India	3,144	14.67%
3	Australia	2,537	11.84%
4	Japan	2,282	10.65%
5	South Korea	1,978	9.23%
6	Singapore	963	4.49%
7	Vietnam	838	3.91%
8	Thailand	808	3.77%
9	Indonesia	767	3.58%
10	Malaysia	623	2.91%
11	Pakistan	594	2.77%
12	Philippines	544	2.54%
13	New Zealand	365	1.70%
14	Hong Kong	329	1.53%
15	Bangladesh	305	1.42%
16	Southeast Asia	269	1.25%
17	Cambodia	240	1.12%
18	Myanmar	173	0.81%
19	Other	813	3.79%

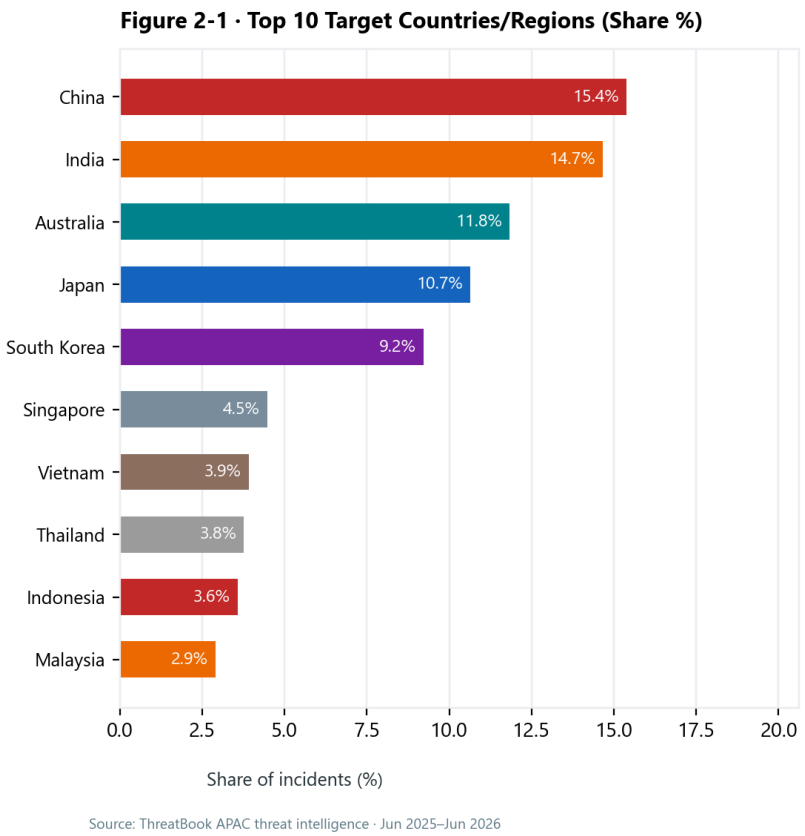


Figure 2-1. Top 10 target countries/regions (share %)

China, India, Australia, Japan, and South Korea together accounted for 61.78% and ranked at the top of Asia-Pacific targeting. Economic scale, digital-asset density, industrial-intelligence value, and geopolitical sensitivity together form the structural reasons for high attack concentration in this tier. China ranked first at 15.39%. Threats during this period showed parallel patterns of "data-asset hunting" and "critical infrastructure penetration": large government and enterprise datasets continued circulating on the dark web, and data aggregation and secondary resale formed a mature underground industry chain; at the same time, external attackers extended targeting to time-synchronization infrastructure such as timing centers, directly threatening power dispatch, financial transactions, and aerospace telemetry systems that depend on precise timing, with attack objectives extending from the data layer to operational foundations. India followed at 14.67%. Opportunistic attacks and targeted operations have long coexisted: financial, healthcare, and government systems processed more than 2.9 million security incidents throughout the year; during the India-Pakistan conflict, groups such as APT36 simultaneously conducted targeted penetration against government and defense targets, with both threat types overlapping and keeping India under sustained high-intensity defensive pressure.

Australia (11.84%) saw its threat focus shift from data theft toward system control. Security alerts targeting critical infrastructure more than doubled year over year during this period, with sustained pressure on government, financial services, healthcare, and telecommunications; notably, in more than half of critical infrastructure incidents, attackers' primary objective was not data acquisition but actual control of core systems. Japan (10.65%) semiconductor, aerospace, and advanced manufacturing sectors have long

remained focal points for multi-state APT penetration. In February 2026, semiconductor test-equipment giant Advantest suffered a ransomware attack, a typical example of sustained manufacturing pressure. South Korea (9.23%) threats were highly concentrated in North Korea–linked groups. Lazarus, Kimsuky, and APT37 remained active during this period around crypto-asset theft and government intelligence collection, dominating the vast majority of APT incidents in South Korea.

Singapore (4.49%), Vietnam (3.91%), Thailand (3.77%), Indonesia (3.58%), and Malaysia (2.91%) formed a second tier with a combined 19.66%. A shared characteristic of this tier is that digitalization has outpaced security capability building, attack surfaces continue expanding with business growth, and defensive systems and security regulation have not kept pace. Singapore's actual risk exposure is significantly higher than its incident share suggests. As an Asia-Pacific financial center and regional data hub, Singapore handles cross-border data flows and financial transaction volumes far exceeding its economic size. In July 2025, APT group UNC3886 compromised Singapore critical infrastructure, triggering the country's largest-scale cybersecurity response operation on record. Vietnam faces more geopolitically driven targeted penetration, Indonesia is a major ransomware victim country, and Thailand's threat profile falls between the two.

Attack peaks in Pakistan and Bangladesh (1.42%) closely aligned with the India-Pakistan conflict timeline; as conflict escalated, cyberattacks almost synchronously surged, and periodic fluctuations in incident volume directly mapped geopolitical tension levels. Cambodia (1.12%) and Myanmar (0.81%) showed distinctly different characteristics—transnational organized crime groups established large-scale telecom fraud infrastructure in both countries, making them simultaneously cybercrime export bases and priority targets for international joint law-enforcement action, with attack scale clearly exceeding levels expected for their economic size. Hong Kong (1.53%) ranked 14th, with incident volume at a mid-to-low level in Asia-Pacific, but risk should not be judged by count alone. As a core connectivity node in Asia-Pacific capital markets, successful intrusion against multinational headquarters in Hong Kong often provides attackers lateral access to Asia-Pacific subsidiary networks, with potential impact from a single intrusion far exceeding the incident number itself.

3. Affected Industry Distribution

By target industry distribution, government, technology, and financial services ranked in the top three, with a combined share of approximately 39.27%; the top five industries together accounted for approximately 50.43%. Industry distribution reflects three main lines: government, technology, and financial services form the baseline of Asia-Pacific attack activity; manufacturing, healthcare, and education face more pronounced ransomware and data-breach pressure; although telecommunications and energy rank below the top three by volume, they carry higher APT and long-term penetration value because of communications, energy, and critical infrastructure functions.

Rank	Industry	Share
1	Government	15.38%

Rank	Industry	Share
2	Technology	12.01%
3	Financial Services	8.73%
4	Manufacturing	5.61%
5	Technology-Cybersecurity	5.55%
6	Healthcare	4.13%
7	Education	3.64%
8	Telecommunications	3.46%
9	Energy	2.31%
10	Healthcare-Medical Services	2.18%

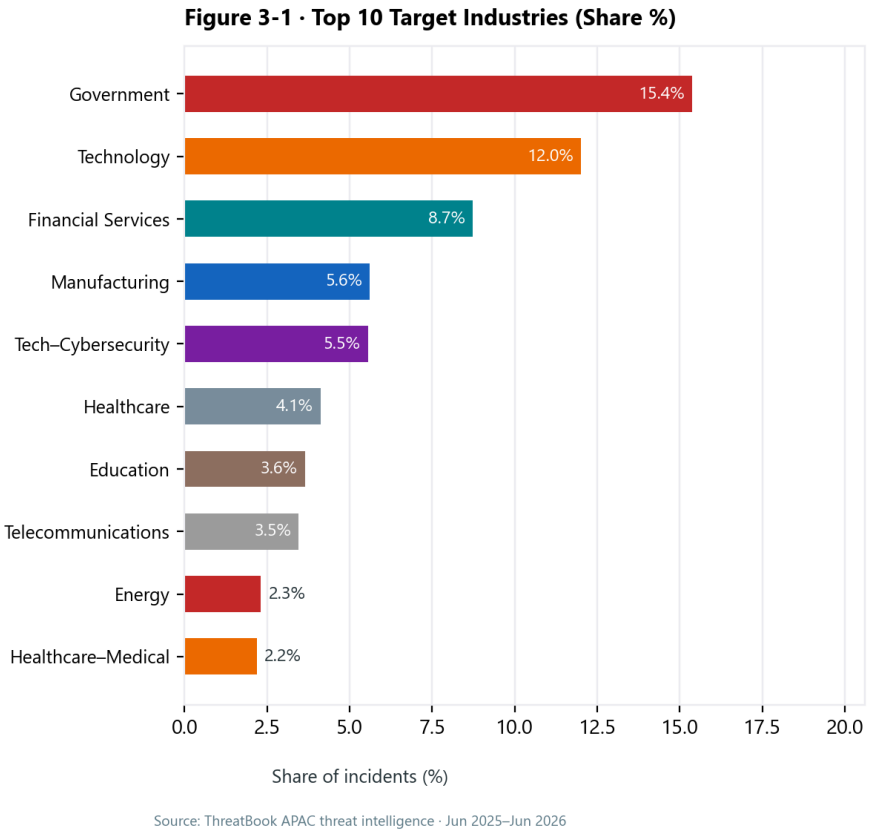


Figure 3-1. Top 10 target industries (share %)

Within industries, by counting each Asia-Pacific country/region separately when a single incident involved multiple countries/regions, the top ten industries showed clear differences in country targeting. Government, financial services, telecommunications, and energy concentrated more in large digital economies and critical infrastructure nodes such as China, India, Australia, Japan, and South Korea; in technology and Technology-Cybersecurity, China, India, Japan, South Korea, and Australia held primary positions, reflecting concentration in cloud services, software supply chains, code assets, and security-

service ecosystems; manufacturing centered on Japan, India, China, Australia, and South Korea, consistent with Asia-Pacific distribution of advanced manufacturing, automotive, electronics, and semiconductor supply chains; in healthcare, medical services, and education, Australia, India, China, Japan, and South Korea ranked higher, indicating that high-disclosure markets, population scale, and public-service digitalization jointly shaped industry risk exposure.

Industry	Target Country/Region Distribution	Top Attack Types	Top Threat Actor Tags	Risk Assessment
Government	India 15.24% China 15.12% Australia 10.89% South Korea 9.70% Japan 9.04%	Data Breach 37.67% APT 25.37% Phishing 19.48% Ransomware 12.15%	APT36 2.82% Qilin 2.55% LockBit 2.19% Kimsuky 1.98% Lazarus 1.91%	Digital identity, credential data, government email, public-service systems, and policy intelligence under simultaneous pressure
Technology	China 23.17% India 14.72% Japan 10.63% South Korea 9.52% Australia 9.44%	Data Breach 41.27% Phishing 19.71% APT 18.16% Ransomware 11.79%	Lazarus 4.42% ShinyHunters 2.44% Qilin 2.27% SilverFox 2.15% LockBit 1.98%	Cloud accounts, SaaS, code repositories, APIs, software vendors, and customer systems becoming entry points
Financial Services	India 17.79% China 13.58% South Korea 11.17% Australia 11.14% Japan 10.12%	Data Breach 38.93% Phishing 23.95% Ransomware 16.79% APT 14.40%	Lazarus 6.36% Qilin 4.54% LockBit 3.56% Akira 2.67% Scattered Spider 2.00%	Overlapping risk across customer identity, payment accounts, mobile finance, crypto assets, and cross-border settlement
Manufacturing	Japan 18.83% India 14.12% China 13.01% Australia 11.90% South Korea 8.67%	Data Breach 36.28% Ransomware 31.69% APT 13.68% Phishing 13.15%	Qilin 7.59% Akira 4.21% LockBit 3.03% Clop 2.96% ShinyHunters 1.81%	Production stoppage pressure, supply chain delivery, design materials, and industrial-intelligence value jointly amplifying risk
Technology-Cybersecurity	China 18.85% India 14.51% South Korea 12.05% Japan 11.61% Australia 11.41%	Data Breach 38.70% Phishing 20.93% APT 17.38% Ransomware 16.06%	Lazarus 4.51% LockBit 3.55% Clop 3.28% Scattered Spider 2.94% Akira 2.73%	Security vendors, IT service providers, cloud providers, and security management platforms carrying downstream amplification effects

Industry	Target Country/Region Distribution	Top Attack Types	Top Threat Actor Tags	Risk Assessment
Healthcare	Australia 19.30% India 14.71% China 11.40% Japan 11.21% South Korea 9.13%	Data Breach 37.03% Ransomware 26.48% Phishing 16.77% APT 13.57%	Qilin 5.76% Akira 3.22% ShinyHunters 2.92% Clop 2.75% LockBit 2.45%	Patient identity, medical records, insurance data, and medical continuity creating dual pressure
Education	Australia 14.73% India 14.17% China 13.81% Japan 12.89% South Korea 10.01%	Data Breach 37.78% Ransomware 20.78% Phishing 18.51% APT 16.36%	Qilin 4.37% ShinyHunters 3.76% Akira 2.71% Clop 2.49% LockBit 2.05%	Campus accounts, open networks, research data, and faculty/student identity data showing clear exposure
Telecommunications	China 18.67% India 15.25% Australia 10.31% South Korea 10.13% Japan 8.60%	Data Breach 40.58% APT 23.26% Phishing 15.47% Ransomware 12.00%	Salt Typhoon 3.81% Volt Typhoon 3.09% Lazarus 2.99% Qilin 2.68% APT41 2.37%	Communications backbones, perimeter devices, operator core networks, and subscriber data holding strategic value
Energy	India 14.33% China 12.34% Australia 12.18% Japan 11.68% South Korea 9.94%	Data Breach 35.26% APT 25.98% Ransomware 18.76% Phishing 15.77%	Qilin 4.01% Akira 2.27% Lazarus 1.67% Volt Typhoon 1.47% KTA007/Clop/ShinyHunters each 1.47%	IT/OT boundary, contractor remote access, and critical infrastructure continuity risks prominent
Healthcare-Medical Services	Australia 24.06% India 16.72% Japan 12.95% China 9.38% South Korea 6.63%	Data Breach 41.90% Ransomware 32.39% Phishing 14.89% APT 7.86%	Qilin 8.66% LockBit 4.61% Clop 2.93% Akira 2.93% RansomHub 2.65%	Medical service disruption, patient data exposure, billing systems, and third-party healthcare IT risks prominent

4. Highly Active Ransomware and Data-Extortion Groups

1. Overall Trends

During the reporting period, ransomware incidents in Asia-Pacific accounted for 27.3% of all security incidents in the same period, making ransomware the second-largest incident type after data breaches. Attack density increased significantly in the second half of 2025, with October and November as annual peaks, reflecting ransomware groups' operational rhythm of concentrated end-of-year attacks. From January through May 2026, monthly frequency declined somewhat from the second-half 2025 peak but remained above Q1 2025 levels. By attack model, dual extortion—encryption and exfiltration—has become the mainstream pattern. In intelligence data, 62.9% of ransomware incidents were also tagged as data breach incidents. In addition, approximately 8.9% of ransomware incidents also involved phishing, and 5.4% also involved APT activity, indicating crossover between ransomware attack chains and phishing delivery and advanced persistent penetration.

2. Target Country/Region Distribution

By ransomware targeting across Asia-Pacific countries, Australia, Japan, and India ranked in the top three, with the three countries together accounting for approximately 40% of total Asia-Pacific ransomware country hits. China and South Korea followed closely. Within Southeast Asia, Thailand, Singapore, Malaysia, and Indonesia also faced elevated ransomware pressure. The high rankings of Australia and Japan are directly related to the economic weight of manufacturing and healthcare in the Asia-Pacific region, and also reflect relatively greater transparency in data-breach notification regimes in both countries, which results in more incidents being recorded in intelligence data.

3. Affected Industry Distribution

Manufacturing ranked first among all industries, accounting for 21.0% of all ransomware incidents, followed by financial services (17.8%), technology (14.5%), and government (13.9%). Healthcare (including the medical-services subcategory, combined 18.4%) would rank second after manufacturing if merged. Manufacturing's leading position reflects core industry characteristics: production-line stoppages cause direct hourly losses and delivery breaches trigger chain compensation, leaving enterprises little room to delay in ransom negotiations and producing higher payment willingness than most industries. Healthcare's high ranking follows similar logic—hospitals cannot suspend operations, patient data is highly sensitive, and dual extortion is especially damaging.

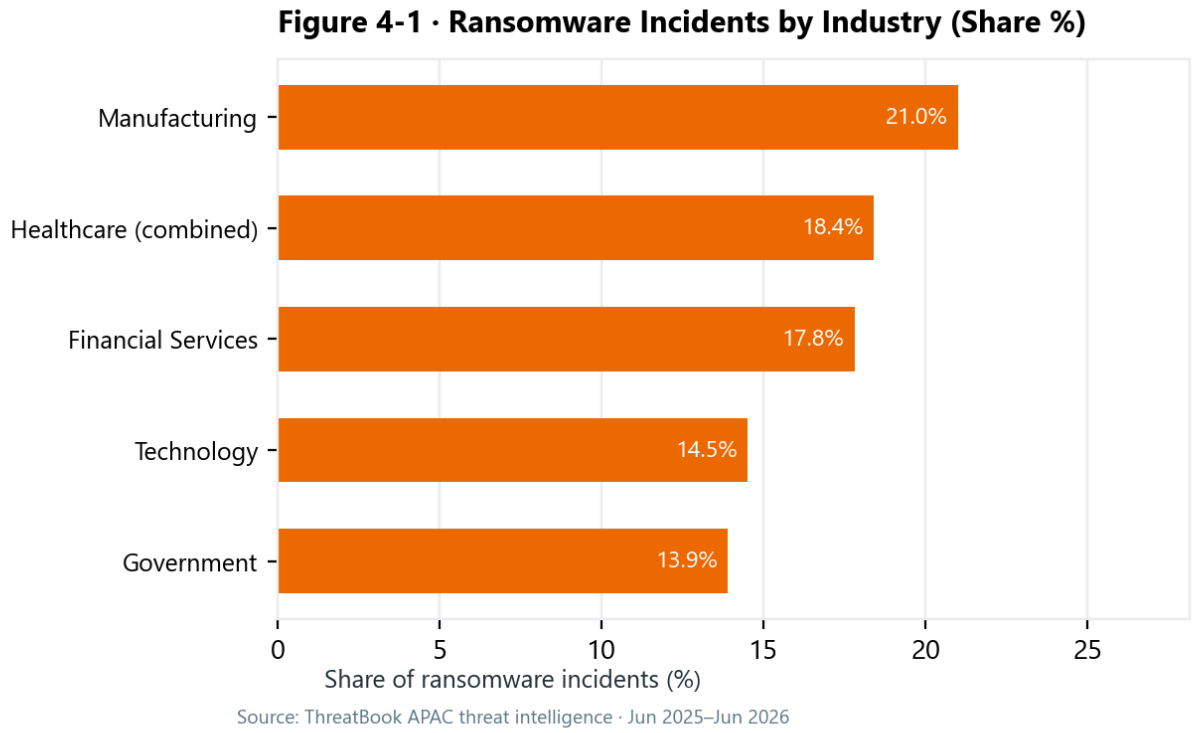


Figure 4-1. Ransomware incidents by industry (share %)

4. Active Ransomware Groups

Intelligence data during this period show a ransomware ecosystem pattern of "concentration at the top and dispersion in the long tail." The top 5 groups together accounted for 27.3% of all ransomware incidents, the top 10 for 39.4%, and the top 20 for 56.1%; more than 40% of ransomware incidents were distributed among a large number of smaller organizations ranked below 20.

Rank	Group	Share	Primary Target Industries	Primary Target Countries
1	Qilin	12.5%	Manufacturing, Healthcare, Government	Japan, Australia, South Korea
2	Clop	4.6%	Manufacturing, Healthcare, Government	Australia, Japan, South Korea
3	Akira	4.2%	Manufacturing, Healthcare, Government	Australia, Japan, India

Rank	Group	Share	Primary Target Industries	Primary Target Countries
4	Incransom	3.1%	Manufacturing, Healthcare, Business	Australia, Japan, India
5	thegentlemen	2.9%	Manufacturing, Government, Healthcare	Thailand, China, Japan
6	LockBit	2.7%	Government, Manufacturing, Healthcare	China, Australia, India
7	Scattered Spider	2.6%	Aviation, Government, Financial Services	Australia, India, South Korea
8	Everest	2.3%	Manufacturing, Healthcare, Government	India, Japan, South Korea
9	Lynx	2.3%	Manufacturing, Government, Healthcare	Australia, Singapore, Japan
10	Safepay	2.2%	Manufacturing, Healthcare, Government	Australia, Japan, Singapore
11	DragonForce	2.2%	Government, Manufacturing, Healthcare	Australia, India, Japan
12	devman	2.1%	Manufacturing, Healthcare, Technology	Thailand, China, India
13	ShinyHunters	2.0%	Government, Education, Healthcare	Australia, South Korea, India
14	Nightspire	1.8%	Manufacturing, Healthcare, Technology	India, Japan, Thailand
15	RansomHouse	1.7%	Manufacturing, Healthcare, Energy	Japan, China, Australia
16	Warlock	1.6%	Government, Technology, Manufacturing	China, Japan, Australia
17	Sinobi	1.4%	Manufacturing, Healthcare,	India, Australia, China

Rank	Group	Share	Primary Target Industries	Primary Target Countries
			Government	
18	worldleaks	1.4%	Manufacturing, Government, Healthcare	India, Australia, Japan
19	RansomHub	1.3%	Manufacturing, Government, Healthcare	India, China, Australia
20	Medusa	1.2%	Healthcare, Government, Education	Australia, India, Thailand

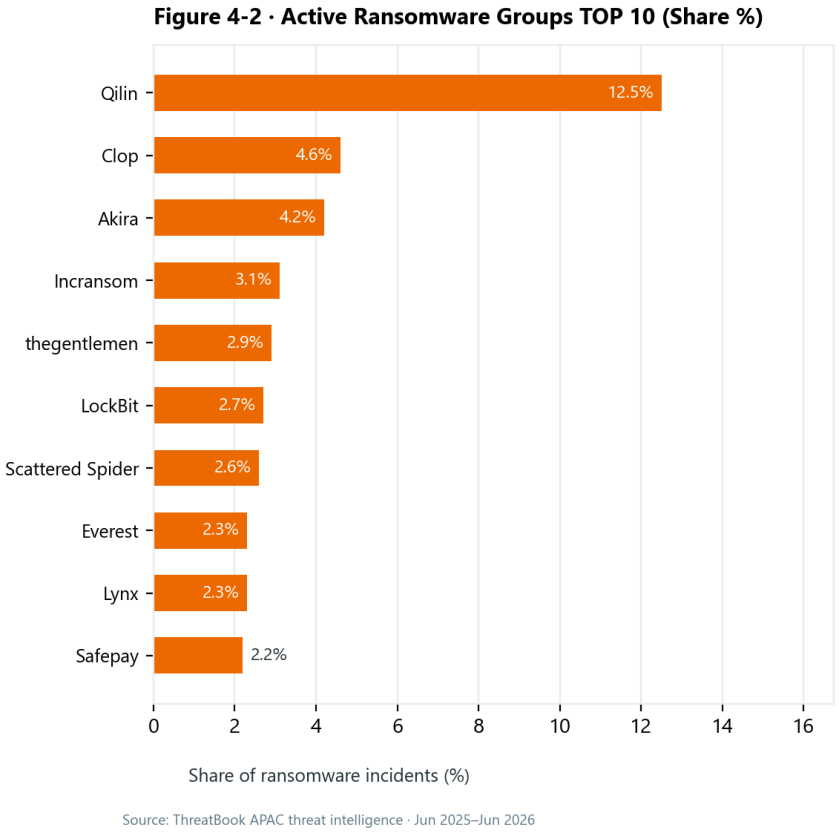


Figure 4-2. Active ransomware groups TOP 10 (share %)

5. High-Risk APT Groups

1. Overall Trends

During the reporting period, APT incidents in the Asia-Pacific region accounted for 22.8% of all security events, making APT the third-largest incident category after data breaches and ransomware. Unlike the "high-frequency burst" pattern of ransomware, APT attacks showed a more even temporal distribution, with sustained high activity throughout 2025 and no pronounced peak comparable to the October–November ransomware surge—consistent with APT groups' operational characteristic of persistent penetration and long-term presence.

By co-occurring features, 77.3% of APT incidents were also tagged as data breach events; 37.4% involved phishing; 14.9% also involved ransomware; and 5.8% involved supply-chain attacks. The high co-occurrence of APT and data breaches reflects that intelligence theft remains the core objective of current APT attacks, while the nearly 15% APT–ransomware overlap indicates that some nation-state attackers are using ransomware as a secondary monetization or cover mechanism. Supply-chain attacks account for a higher share of APT incidents (5.8%) than of ransomware incidents, indicating that supply-chain penetration is more often used as an advanced intrusion path for APT than as a bulk propagation tool for ransomware.

2. Target Region Distribution

Country distribution of APT attacks differs markedly from ransomware. China ranked first among Asia-Pacific APT targets by a clear margin, followed by South Korea and India; the three countries combined accounted for more than half of all country-level APT hits in the region. Japan and Australia ranked fourth and fifth. APT incident country distribution maps more directly onto the geopolitical landscape: the Korean Peninsula axis, the South Asia axis, and major-power competition directions form the three primary geopolitical axes of Asia-Pacific APT activity.

3. Target Sector Distribution

Government dominates APT incidents far above other sectors, accounting for more than one-third of all APT events. Defense ranks prominently in APT incidents, reflecting the national-security focus of APT targeting. Technology (including the Technology-Cybersecurity subcategory) accounts for approximately 41% of APT incidents combined; the high share of the Technology-Cybersecurity subsector reflects sustained APT attention to security infrastructure—vulnerabilities in perimeter devices, security products, and IT management platforms are repeatedly exploited by nation-state attackers as initial access and persistence footholds. Telecommunications also ranks significantly higher in APT incidents than in the

overall incident mix; long-term penetration of telecommunications infrastructure by Salt Typhoon and APT41 makes telecommunications one of the most strategically sensitive sectors in the APT domain.

4. Active APT Groups

In intelligence data for this reporting period, the top five groups combined accounted for 18.4%; the top 10 for 27.4%; and the top 20 for 39.5%. More than 60% of APT incidents were distributed outside the top 20, reflecting a more dispersed participant base in the APT ecosystem.

Rank	Group	Share	Primary Target Sectors	Primary Target Countries
1	Lazarus	5.7%	Financial Services, Technology, Cryptocurrency Exchanges	South Korea, China, Japan
2	APT36	4.3%	Government, Government Public Services, Defense	India, Pakistan, Vietnam
3	Kimsuky	3.2%	Government, Financial Services, Technology	South Korea, Japan, China
4	APT37	2.7%	Government, Government Public Services, Technology	South Korea, Japan, India
5	SilverFox	2.5%	Government, Technology, Cybersecurity	China, India
6	HoneyMyte	2.1%	Government, Financial Services, Government Public Services	India, Thailand, Myanmar
7	SideWinder	1.7%	Government, Defense, Cybersecurity	Pakistan, Bangladesh, India
8	MuddyWater	1.5%	Government, Manufacturing, Education	South Korea, India, Japan
9	UNC3886	1.3%	Government, Technology, Telecommunications	Singapore, China, South Korea

Rank	Group	Share	Primary Target Sectors	Primary Target Countries
10	NOKKI	1.3%	Government, Financial Services, Defense	South Korea, Australia

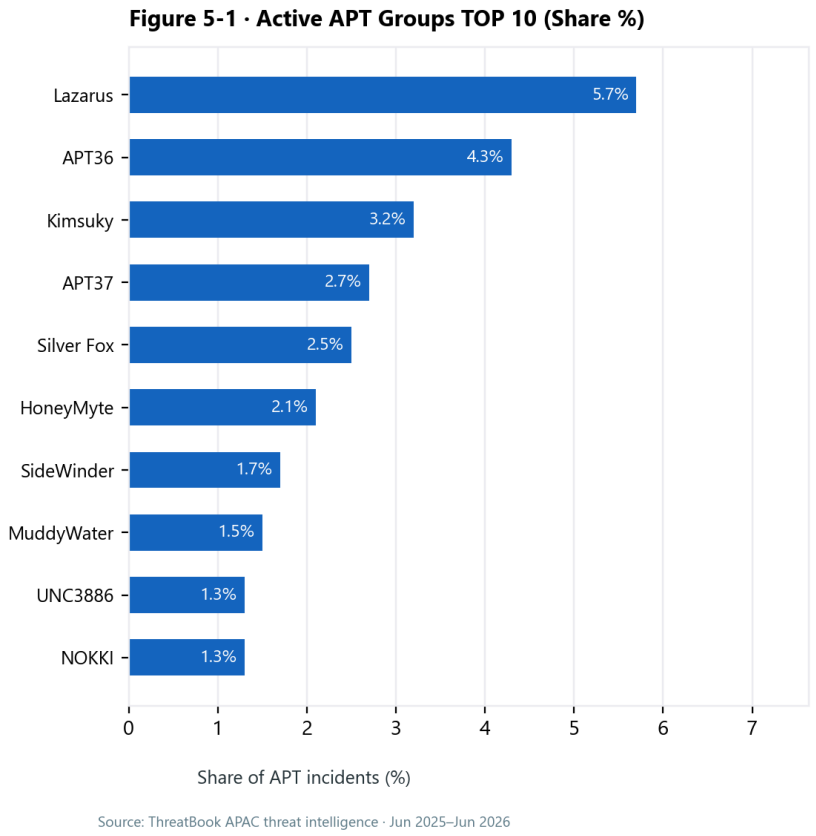


Figure 5-1. Active APT groups TOP 10 (share %)

Lazarus ranked first among APT groups at 5.7%. Its target structure is the most distinctive among major APT groups—financial services and cryptocurrency exchanges combined form its primary attack direction rather than the government and defense focus typical of most APT groups. This pattern corresponds directly to North Korea's strategic need to obtain foreign currency through cyber operations; Lazarus's financial orientation is the most pronounced among major threat groups.

APT36 ranked second (4.3%). Its targets are almost entirely concentrated in government, government public services, and defense, with India and Pakistan as primary target countries—among the highest sector-concentration profiles of any APT group.

On the Korean Peninsula axis, Kimsuky (3.2%) and APT37 (2.7%) ranked third and fourth. Both prioritize South Korean government and technology sectors, forming a functional division with Lazarus's financial preference: Lazarus handles foreign-currency acquisition; Kimsuky and APT37 handle political intelligence collection. NOKKI (1.3%) also targets South Korean government and financial sectors, further increasing APT density on the peninsula axis.

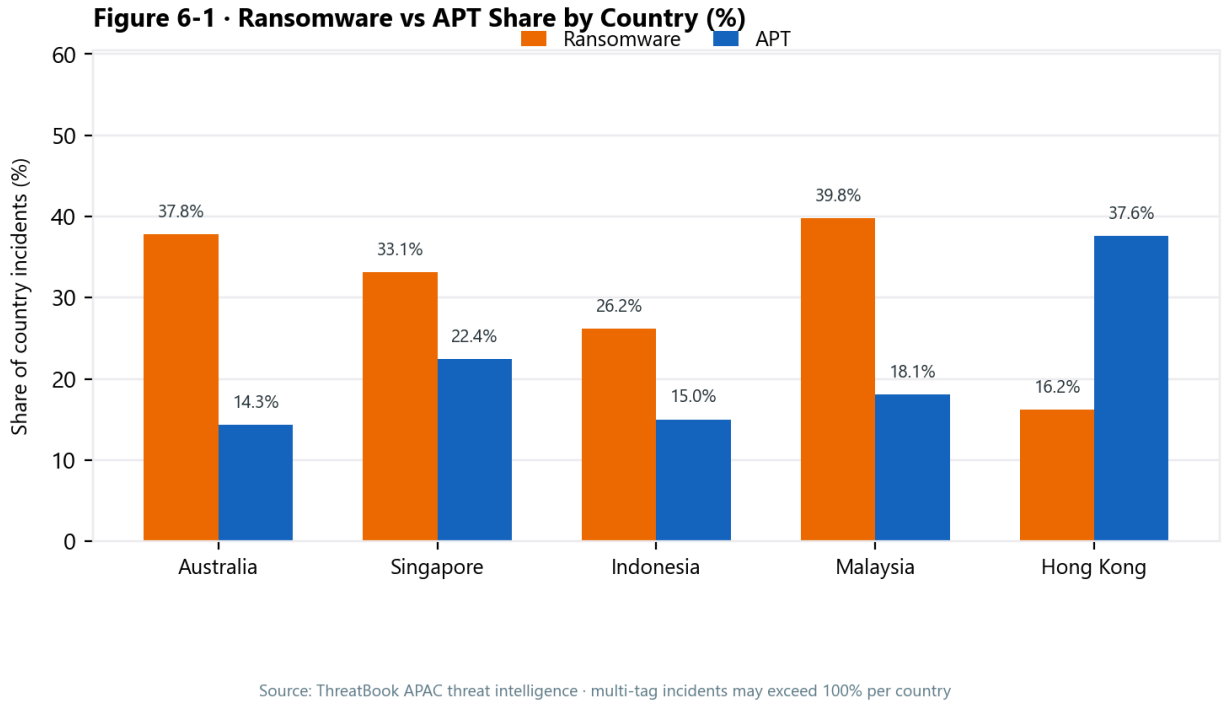


Figure 6-1. Ransomware vs APT share by country (%)

6. Key Country/Region Threat Landscape Analysis

6.1 Australia: Government and Customer-Data Industries Under Pressure, Ransom Returns Amplified by Disclosure Environment

During the reporting period, Australia's cybersecurity posture exhibited a clear "dual-pressure" profile. On one side, ransomware groups continued data theft and monetization against high-value commercial sectors including manufacturing, construction, aviation, retail, healthcare, and financial services. On the other, APT groups maintained long-term penetration against strategically valuable domains including government, telecommunications, transportation, energy, and fintech. The two threat types pursue different objectives but reflect the same underlying reality: as a highly digitized advanced economy, Australia holds large volumes of reusable identity data, mature outsourcing and SaaS service chains, and critical infrastructure status within the Indo-Pacific security architecture.

1. Attack Type Analysis

Attack Type	Share of Country Incidents
Data Breach	52.3%

Attack Type	Share of Country Incidents
Ransomware	37.8%
Phishing	25.4%
APT Attack	14.3%
Supply Chain Attack	3.2%
DDoS Attack	2.8%

Data breach was Australia's most prominent incident type at 52.3%, with more than half of incidents involving sensitive information exfiltration. This category statistically overlaps with ransomware and APT activity—nearly half of data breach incidents were also tagged as ransomware (47.8%), and roughly one quarter also involved APT (23.8%)—which contributes to the elevated overall share. Even after removing overlap with ransomware and APT, more than one third of data breach incidents occurred independently as non-ransomware, non-APT leaks, indicating that data exfiltration risk in Australia is not driven by ransomware alone.

During the reporting period, Australia experienced multiple major standalone data breach incidents: in March 2026, Qantas suffered a social-engineering attack against overseas call-center staff, resulting in exposure of 5.7 million customer records on Salesforce; in December 2025, the University of Sydney's online code repository was accessed without authorization, exposing personal information of more than 27,000 faculty and students; in November 2025, travel platform Luxury Escapes was compromised via SQL injection, with 62,000 user records and payment data offered for sale on dark web markets; in the same month, defense contractor IKAD Engineering was continuously penetrated for approximately 150 days through a known VPN gateway vulnerability, with more than 800 GB of defense-sensitive data stolen. These cases span aviation, education, travel, and defense, with exfiltration paths including social engineering, exposed code repositories, web application vulnerabilities, and long-term network device persistence—reflecting systemic weaknesses in identity verification, third-party access control, and exposure management. Data breach is no longer merely a byproduct of ransomware but an independent, high-frequency risk surface.

Ransomware ranked second by share at 37.8%, with the largest deviation from the global mean (+10.5 percentage points), making Australia the country under the heaviest ransomware pressure among the five. 69.3% of ransomware incidents also involved data breach, above the global rate of 62.9%, indicating that dual extortion is the standard attack pattern against Australia. Amendments to Australia's *Security of Critical Infrastructure Act* and *Privacy Act* strengthened breach notification obligations; attackers exploit this by adding threats to report to regulators as additional leverage, turning data breach itself into ransom currency. Phishing accounted for 25.4%, close to the global mean, and serves as the primary precursor to ransomware and data breach. APT activity accounted for 14.3%, 8.5 percentage points below the global mean, indicating that commercialized crime dominates Australia's threat landscape while state-sponsored espionage exists but is not the primary driver by incident volume.

2. Victimized Industry Distribution

Table 6-3 Australia Top 10 Victimized Industries

Rank	Industry	Share
1	Government	12.1%
2	Technology	8.4%
3	Healthcare	7.6%
4	Financial Services	7.3%
5	Manufacturing	5.9%
6	Education	5.3%
7	Cybersecurity	4.2%
8	Medical Services	3.2%
9	Aviation & Transport	2.9%
10	Telecommunications	2.9%

Government was Australia's most targeted industry (12.1%), with threats from two directions: commercial ransomware groups (29% of government incidents) pursuing ransom through dual extortion, and state-sponsored APT groups (25%) penetrating government networks for intelligence collection. The two threat types are comparably active—a structure relatively unique among Asia-Pacific countries, where government sectors elsewhere are overwhelmingly ransomware-dominated with APT shares far below Australia's. This aligns with Australia's Five Eyes membership and core role in the Asia-Pacific security framework, placing government agencies simultaneously as high-value ransom targets for criminal groups and priority intelligence targets for nation-state adversaries. Technology ranked second (8.4%), with threats primarily from data breach (70%) and phishing (39%); ransomware accounted for 36%. The combination indicates technology firms face credential theft, data exfiltration, and system encryption concurrently.

Healthcare ranked third (10.8%), one of the few Asia-Pacific countries with healthcare in the top three. Threats were primarily ransomware-driven (51%), far above other industries, because healthcare system downtime directly affects patient safety and creates maximum ransom payment pressure. Financial services ranked fourth (7.3%), with the highest phishing (48%) and data breach (78%) shares across all industries; the core threat is credential theft and account takeover. Manufacturing (5.9%) and education (5.3%) ranked fifth and sixth, each with ransomware shares near half (manufacturing 48%, education 37%), but with different attack logic. Manufacturing's strong dependence on production continuity and high downtime cost makes it a traditional target for Qilin, Akira, and Clop.

3. Highly Active Ransomware Groups

Rank	Group	Share of Country Ransomware	Primary Target Industries
1	Qilin	11.5%	Manufacturing, Construction
2	Scattered Spider	6.0%	Aviation & Transport, Retail
3	Akira	5.8%	Manufacturing, Financial Services

Qilin

Qilin is one of Australia's primary persistent ransomware threats. Its target industries concentrate in manufacturing, construction, and financial services, followed by education, healthcare, business services, and logistics. This distribution indicates Qilin in Australia primarily targets entity-sector and professional-service organizations with high business-continuity requirements, dense contract and customer data, and significant reputational loss when data is publicly released.

Specific victims span construction engineering, manufacturing, finance, logistics, education, and IT services. Construction and engineering targets include Talisman Civil and Hunter Construction Group; manufacturing and transport-related targets include Malibu Boats Australia and Menzies Group; financial services targets include Skeggs Goldstien and Generation Life; education and services targets include Belmont Christian College, Australian College of Business Intelligence, Bluize, and B dynamic Logistics. Common characteristics: organizational scale is not necessarily the largest, but once business documents, customer records, contract data, or internal operational files are published, customer notification, regulatory communication, contract disputes, and reputational damage pressure escalate rapidly.

Qilin operates as a ransomware-as-a-service model, relying on affiliates for intrusion and ransom conversion. Common initial access methods include spear-phishing, credential theft, remote access entry abuse, and VPN or perimeter device vulnerability exploitation. Post-compromise, the group typically exfiltrates data first, then applies file encryption and dark web naming for dual extortion. Research also observed Qilin using Windows Subsystem for Linux to run Linux encryptors in Windows environments to evade some endpoint detection; the group has also been linked to Check Point VPN vulnerability exploitation, indicating attack paths are not dependent on a single vulnerability but selected based on target exposure to maximize ransom return.

Scattered Spider

Scattered Spider is the most typical identity-attack group in Australia's ransomware and data-extortion activity. During the reporting period, Scattered Spider's target industries concentrated heavily in aviation and retail, followed by insurance, government, cybersecurity, automotive, financial services, and technology. This distribution shows Scattered Spider in Australia does not prioritize traditional manufacturing or construction targets but instead targets service industries with large customer data volumes, customer-service outsourcing workflows, cloud identity systems, and CRM platforms.

Qantas customer data breach is one of Scattered Spider's most representative cases in Australia. The incident exposed that aviation enterprises' core risk lies not only in flight systems but also in loyalty programs, call centers, third-party customer service, and customer relationship management platforms. Beyond Qantas, this dataset includes the group's attack records against Salesforce CRM environments and insurance, retail, and automotive-related targets. Common characteristics: long identity-verification chains, numerous outsourced roles, and customer-service permissions proximate to customer data—once attackers bypass MFA or induce help desk account resets, data theft can be completed without large-scale malware deployment.

Scattered Spider's core technique is social engineering—SIM swapping, impersonating IT help desks to obtain MFA tokens, and penetrating Okta/Azure AD for domain-wide privileges—without relying on traditional vulnerability exploitation. Associated tools include WarZone RAT, Vidar Stealer, RaccoonStealer, and Teleport data exfiltration tools. The group's threat focus is converting people and identity processes into intrusion entry points. For Australia, these techniques are especially suited to aviation, retail, and insurance industries that heavily depend on customer service, loyalty systems, and outsourced services.

Akira

Akira is a significant ransomware threat to Australia's manufacturing, financial, and energy sectors. Target industries concentrate in manufacturing and financial services, followed by energy, technology, government, legal services, telecommunications, healthcare, and construction. Akira in Australia primarily selects organizations with high business-continuity requirements, complex remote-access systems, and deep IT/OT interconnection.

Specific victims span automotive parts manufacturing, financial leasing, energy, technology, and professional services, including Helical Auto Technology, LeasePLUS, Intellect Systems, Woodside, and Regency Media. Focus on manufacturing and energy enterprises indicates Akira prefers targets where shutdown, contract delay, supply chain disruption, and sensitive file exfiltration create compound pressure. Attacks on financial leasing, legal services, and technology firms reflect the group's equal emphasis on ransom value of customer records, contract materials, and internal business data.

Akira's common initial entry points include stolen credentials, exposed VPNs, SonicWall SSL VPN, Cisco ASA/FTD perimeter devices, and remote management tool abuse. Post-compromise, attackers typically use Mimikatz, PowerShell, RMM tools, and lateral movement to expand privileges, then encrypt or publish on dark web markets after data theft. Unlike Scattered Spider's identity-focused social engineering, Akira operates more as a perimeter device and remote-access exposure ransom converter.

4. Active APT Groups

During the reporting period, North Korean Lazarus conducted multiple targeted attacks against Australia's cryptocurrency and technology industries; Russian APT29 and APT28 posed sustained threats from government intelligence and military logistics directions respectively.

Lazarus

Lazarus is one of Australia's most significant North Korea-related cyber threats. The group and its associated ecosystem have long targeted financial services, cryptocurrency, Web3, technology enterprises, and software developers, pursuing both fund theft and acquisition of credentials, code, wallet keys, and internal enterprise access. For Australia, Lazarus's threat focus is not traditional perimeter disruption but crypto assets, remote hiring, developer identity, and cloud access permissions.

By attack method, Lazarus affects relevant Australian industries through three primary paths. First, fake recruitment and developer phishing. Attackers pose as recruiters, investment institutions, or project partners, contacting developers or crypto industry practitioners via LinkedIn, job platforms, Discord, Telegram, GitHub, and similar channels, inducing download of "interview projects," "test code," or "meeting tools." These projects typically contain JavaScript, Python, npm packages, VS Code configurations, or malicious scripts that, when executed, steal browser credentials, wallet information, code repository access tokens, and cloud accounts. This technique is common in Lazarus activities including Contagious Interview and Operation Dream Job.

Second, North Korean IT worker infiltration. Attackers do not directly exploit vulnerabilities to penetrate enterprises but pose as remote software engineers, system administrators, or outsourced developers to enter enterprise work environments, bypassing hiring review through forged identities, proxy interviews, remote desktop, VPN, virtual office addresses, and third-party payment accounts. Once inside, they can access code repositories, customer data, internal tickets, cloud platforms, and production environments—generating income for North Korea through salaries while potentially enabling subsequent data theft, code implantation, or ransomware. This threat is especially relevant to Australia's technology, recruitment, fintech, and outsourced development industries, which heavily depend on remote hiring and cross-border developers.

Third, crypto asset and financial credential theft. Lazarus and associated groups have long targeted cryptocurrency exchanges, Web3 projects, blockchain infrastructure, and fintech enterprises through malicious recruitment, fake investment communications, malicious code repositories, phishing pages, and supply chain poisoning to steal private keys, seed phrases, API tokens, and internal enterprise credentials. Australia has an active fintech and Web3 ecosystem; once developers or operations staff are socially engineered, attackers may enter enterprise wallet management, code deployment, and cloud service chains through personal endpoints.

The most explicit Australia-related case during the period was a North Korean IT worker threat conference held in Sydney in 2026 by Australia, the United States, and Canada. The conference targeted Australian technology, recruitment, and financial industry personnel, emphasizing enterprise identification of North Korean IT workers posing as remote technicians. Public reporting indicated participants included government agencies, security vendors, and approximately 80 Australian industry representatives, indicating the issue has escalated from ordinary phishing to recruitment, outsourcing, and enterprise identity governance risk. This case reflects Australia faces not single malware attacks but compound threats of personnel identity entering enterprise systems.

Another case illustrating the attack chain is Lazarus-related developer phishing activity. Public research repeatedly disclosed attackers sending seemingly normal GitHub projects, npm packages, or interview tasks with embedded malicious scripts. After victims run the code, malware collects system information, browser data, crypto wallet information, and access tokens, then connects to attacker infrastructure. This attack chain has direct reference value for Australia because local fintech, Web3, and software outsourcing enterprises similarly depend on GitHub, npm, remote interviews, and developer collaboration tools.

APT29 / Midnight Blizzard

APT29 belongs to Russia's Foreign Intelligence Service (SVR) and is the primary Russian APT threat to Australian government and defense sectors. Intelligence data during the period included 5 Australia-related incidents, with attack methods centered on large-scale credential theft and government agency penetration.

In October 2024, APT29 launched large-scale malicious RDP phishing attacks, delivering signed RDP configuration files via spear-phishing emails impersonating Microsoft and AWS, successfully penetrating more than 200 government, military, think tank, and academic research institutions across the UK, Australia, Japan, and other countries. Attackers registered 193 proxy domains and 34 malicious RDP backend servers, using PyRDP man-in-the-middle proxy tools to intercept and manipulate RDP connections, stealing hard drive contents, clipboard data, and authentication credentials. In Q1 2025, APT29-associated password-spraying attacks surged, with attacks against Cisco ASA VPN systems increasing 399% year-over-year; healthcare was the primary target, with Australia listed as an affected country. In February 2026, APT29 device-code phishing attacks covered more than 340 organizations in the United States, Australia, Canada, Germany, and New Zealand, using OAuth device authorization flows to steal Microsoft 365 session tokens—stolen tokens remained valid even after victims reset passwords. Affected industries included construction, manufacturing, healthcare, legal, and government.

For Australia, APT29's threat concentrates on government and defense intelligence collection—the group, known for the SolarWinds supply chain attack, has long targeted Western government agencies, diplomatic missions, and think tanks; Australia as a Five Eyes member falls within its priority target scope. The ASD 2024-25 Annual Report listed APT29 among national-level threats requiring attention.

APT28 / Fancy Bear

APT28 belongs to Russia's Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) and is an explicitly named national-level threat in the ASD 2024-25 Annual Cyber Threat Report. In May 2025, ASD jointly issued an advisory with the United States, United Kingdom, France, Germany, and more than 20 other countries, noting APT28 has continuously attacked Western logistics, transport, and technology enterprises supporting Ukraine aid since 2022, targeting defense contractors, port operators, airlines, rail operators, and IT service providers. Attack methods include password spraying, spear-phishing, Microsoft Exchange mailbox permission tampering, and VPN vulnerability exploitation (including WinRAR vulnerability CVE-2023-38831).

In period intelligence data, APT28 appeared in 8 Australia-related incident summaries. In the May 2025 global technology and logistics industry attack campaign, APT28 primarily used credential brute-forcing

and known software vulnerability exploitation, with Australia listed as an affected country. In the March 2025 global shipping industry threat analysis, APT28 focused on attacking NATO supply chains supporting Ukraine; the same report noted Russia-linked RedCurl executed more than 40 attacks against entities in Australia, Singapore, and Hong Kong. BadPilot, a sub-group of Seashell Blizzard (APT44 / Sandworm) under the same Russian GRU, was explicitly warned by Microsoft in February 2025 to have expanded attack targets from Ukraine to the United States, United Kingdom, Canada, and Australia, targeting energy, telecommunications, shipping, defense industry, and government sectors.

As a Ukraine aid participant and core U.S. military ally in the Asia-Pacific, Australia's defense industry, logistics enterprises, and technology companies fall within APT28 and the broader Russian GRU cyber operations target scope. ASD explicitly assesses such attacks will continue.

6.2 Singapore: Regional Hub Profile Drives Interwoven Technology, Financial, and Telecom Risk

During the reporting period, Singapore's cybersecurity posture exhibited typical "hub-type risk" characteristics: economic crime groups focus on regional headquarters, customer data, fintech, and enterprise service systems, while nation-state or advanced persistent-capability groups prioritize telecommunications backbone, perimeter devices, cloud environments, and cross-border financial connections. Neither threat type targets only Singapore's local market but attempts to leverage Singapore's ability to connect Southeast Asian customers, capital, data, and enterprise networks to amplify impact.

1. Attack Type Analysis

Attack Type	Share of Country Incidents
Data Breach	49.9%
Ransomware	33.1%
APT Attack	22.4%
Phishing	17.9%
Supply Chain Attack	2.6%
Cryptojacking	2.3%
DDoS Attack	1.7%
Cryptocurrency Theft	1.2%

Data breach was Singapore's highest-share incident type, with 49.9% of incidents involving data exfiltration. Among data breach incidents, 40.9% were also tagged as ransomware, 34.5% as APT, and 31.3% occurred independently without ransomware or APT dependency. This structure indicates Singapore's data breaches serve simultaneously as ransom groups' monetization leverage, long-term

intelligence collection outcomes, and results of cloud account compromise, third-party access, misconfiguration, and enterprise service platform exposure. For regional headquarters, a single breach often simultaneously involves multi-country customers, cross-border contracts, employee identity, and regional operational data—the actual impact radius exceeds local victim counts.

Ransomware accounted for 33.1%, slightly below the Asia-Pacific country average, but 61.7% of ransomware incidents also involved data breach, indicating dual extortion has become a common pattern. Ransomware incidents including LSM Lee, Dacon Networks, Hexacon Construction, KTL Offshore, Singapore Buddhist Welfare Services, Hollysys Asia Pacific, and LHT Holdings covered manufacturing, construction, energy, welfare services, and industrial automation, showing ransomware groups do not select only financial institutions but prioritize organizations with strong business continuity, dense contract materials, multiple regional customers, or high industrial operational dependence.

APT attacks accounted for 22.4%, 6.1 percentage points above the Asia-Pacific country average—a key differentiator from ordinary commercial ransomware markets. Phishing accounted for 17.9%, lower in volume than Australia and Hong Kong, but targeted inducement of executives, fintech practitioners, developers, and telecom operations personnel carries higher conversion value. Supply chain attacks accounted for only 2.6%, which does not indicate lower risk; Singapore enterprises heavily depend on regional MSPs, cloud platforms, customer service, industrial control suppliers, and cross-border SaaS—a single compromised trusted node may spread to multiple countries and industries.

2. Victimized Industry Distribution

Rank	Industry	Share
1	Government	12.6%
2	Technology	12.3%
3	Financial Services	9.0%
4	Manufacturing	6.2%
5	Technology-Cybersecurity	4.6%
6	Healthcare	3.7%
7	Telecommunications	3.5%
8	Construction	3.4%
9	Education	3.1%
10	Energy	3.0%

Government was Singapore's most targeted industry (12.6%), with threats primarily from APT attacks (32%) and data breach (49%); APT share exceeded ransomware (24%)—unique among the five countries' government sectors, where Australia, Malaysia, and others show ransomware shares above APT.

Technology ranked second (12.3%), with threats primarily from data breach (56%) and APT attacks (26%); ransomware share was only 19%, below the national mean. Technology's high breach rate reflects many multinational technology firms establishing Asia-Pacific regional headquarters in Singapore; data asset value makes them priority targets for APT and data theft. Phishing share was 24%, reflecting social-engineering attacks against technology practitioners (such as BlueNoroff's fake Zoom meeting attacks).

Financial services ranked third (9.0%), the industry with the densest threat mix—data breach share 71% and phishing share 40%, both highest across all industries. As the world's fourth-largest financial center, Singapore financial customer data carries extremely high dark web monetization value. In February 2025, Singapore-headquartered exchange Bybit suffered a Lazarus attack with losses of approximately USD 1.5 billion.

Manufacturing and construction threats were primarily ransomware-driven—manufacturing ransomware share 50%, construction 64%, both far above the national mean. Although Singapore is not a major manufacturing nation, it plays a critical node role in the global semiconductor supply chain; production line shutdown may trigger cross-border delivery defaults, creating extreme ransom payment pressure during negotiations. Construction consists largely of SMEs with weak security posture; Qilin and Safepay concentrated attacks on construction firms (including Hexacon Construction, Straits Construction, RDC Architects, Greyform).

Telecommunications ranked seventh by incident volume but APT share was 36%, highest across all industries; UNC3886's penetration of all four telecom operators makes telecommunications the industry under greatest national-security pressure in Singapore. Healthcare and education showed clear growth in 2026, with threat pressure spreading from IT-intensive industries toward traditional service sectors.

3. Highly Active Ransomware Groups

Qilin

Qilin's concentration in Singapore (16.7%) exceeds its share in Australia, making it the absolute leader in Singapore's ransomware ecosystem, operating in dual-extortion mode. Associated tools include the NETXLOADER loader and Lumma Stealer infostealer, with delivery via ClickFix social-engineering lures. Qilin's industry coverage in Singapore is extremely broad—manufacturing, government, finance, energy, construction, and education are hit with near-indiscriminate scope. Specific cases: in December 2025, construction firm Hexacon Construction was attacked with threats to leak sensitive data including engineering drawings, financial records, and contract archives; in the same month, technology firm Dacon Networks was compromised. In October 2025, Southeast Asia's largest printing company KHL Printing was attacked with threats to leak sensitive data; in the same month, wine and spirits distributor Platinum Wines & Spirits had data stolen and offered for download on dark web markets. In September 2025, global leading palm oil enterprise Musim Mas Group and asset management firm Dblock were attacked in succession. In May 2025, urban development firm Straits Construction's internal documents and project images may have been leaked. In January 2025, architectural design firm RDC Architects had data leaked with planned dark web public download. In 2026, Qilin remained active—manufacturing firm LSM Lee's critical operational files were encrypted, and energy firm RMZ Oilfield Engineering was attacked. Qilin's

concentrated attacks on Singapore manufacturing have clear economic logic: Singapore is a critical node in the global semiconductor supply chain; production line shutdown may trigger cross-border supply chain disruption, creating extreme ransom payment pressure during negotiations.

Lynx

Lynx targets manufacturing, offshore engineering, construction, and business services more heavily. The group tends to select enterprises with high operational dependence, dense file systems and engineering materials, and short recovery windows. For offshore engineering and manufacturing firms, stolen data involves not only financial files but potentially equipment, supplier, customer order, and project delivery materials. Attack pattern: encrypt victim systems and publicly release internal materials for pressure. In December 2025, oil, gas, and offshore energy firm KTL Offshore was attacked, with sensitive operational, financial, and engineering documents potentially leaked. In August 2025, offshore marine industry firm HK Hardware & Engineering and pressure-sensitive adhesive manufacturer American Biltrite Far East (ABFE) were attacked on the same day, showing Lynx's operational pattern of concentrated "sweep" attacks against the same industry within short timeframes. In July 2025, Lynx attacked premium brands—Richard Mille Asia, D'League, and IT services firm ITACCESS were compromised in succession, with leaked internal materials potentially involving proprietary information. In January 2025, government-linked institution Singapore Co-operative Enterprises (SCE) was attacked, raising public-sector data security concerns. Lynx showed no new Singapore incidents in 2026, but the group remains highly active globally (20 organizations attacked in a single day in January 2026); attack focus may have shifted from Southeast Asia to other regions.

Safepay

Safepay prioritizes construction and manufacturing, employing modern dual-extortion strategy. In January 2025, construction firm Greyform was attacked resulting in data breach. In July 2025, telecom and technology firm Naxis was encrypted with ransom demanded. In December 2025, Singapore Buddhist Welfare Services (SBWS) was attacked. Safepay specifically targets resource-limited non-profit and welfare institutions, exploiting moral pressure to force ransom payment; beneficiary, donor, and volunteer health records and financial assistance records may have been stolen. In February 2026, accounting services firm AT Adler was attacked, showing Safepay expanding toward professional services.

4. Active APT Groups

Singapore's largest APT threat comes primarily from North Korean Lazarus and BlueNoroff targeted attacks against cryptocurrency and fintech.

Lazarus

Lazarus is the primary North Korea-linked cyber threat facing Singapore during the current period. The group and its associated ecosystem have long focused on cryptocurrency, Web3, fintech, and software development, with operational objectives spanning both fund theft and long-term penetration—pursuing direct on-chain asset theft while systematically acquiring wallet keys, developer credentials, enterprise cloud permissions, and code repository access. For Singapore, Lazarus's threat center of gravity lies not in

traditional government network intrusion or critical infrastructure disruption but in sustained penetration capability against the crypto asset ecosystem, third-party software trust chains, developer identity systems, and remote employment channels. During this period, Lazarus affected relevant Singapore industries through three primary paths. First, supply chain trust chain hijacking. Attackers no longer directly attack exchanges or end enterprises but shift penetration targets upstream to third-party infrastructure they depend on. In the February 2025 Bybit incident, Lazarus first used social engineering to compromise a developer endpoint at multi-signature wallet provider Safe{Wallet}, then laterally penetrated the code deployment system and implanted malicious JavaScript during a routine update, so that each confirmation operation by multi-signature approvers on hardware wallets effectively became blind signing of fraudulent transactions. In the April 2026 KelpDAO cross-chain bridge theft of USD 292 million, the technique was identical—attackers manipulated off-chain infrastructure to trick the bridge into releasing funds for a nonexistent burn operation; on-chain transaction records appeared fully legitimate, and routine monitoring could not capture the anomaly. Singapore is the Asia-Pacific's largest concentration of crypto funds and exchanges; many institutions share the same wallet infrastructure, signing services, and smart contract audit vendors. In this highly interconnected ecosystem, a single upstream supply chain attack can trigger industry-wide cascading impact.

Second, fake recruitment and developer-targeted phishing. Attackers long pose as recruiters, venture partners, legal counsel, or project collaborators, proactively contacting crypto industry practitioners and developers via LinkedIn, Telegram, Discord, GitHub, and similar channels, using "interview projects," "test code," or "collaboration tools" as lures to induce target download of malicious payloads. After execution, payloads steal browser credentials, wallet extension data, code repository access tokens, and cloud accounts; attackers conduct deep profiling of targets in advance to ensure highly personalized social-engineering content. This technique runs through Lazarus's sustained activities including Operation Dream Job and Contagious Interview. Project founders, fund managers, and blockchain engineers in Singapore's Web3 ecosystem are among the most densely targeted groups for this attack type.

Third, North Korean IT worker identity infiltration. Unlike the first two technical attack paths, this route's characteristic is "people entering enterprises before vulnerabilities." Okta's large-scale survey released in 2025 tracked more than 130 North Korea-linked false identities that collectively participated in more than 6,500 job interviews across more than 5,000 enterprises; Singapore was explicitly listed as a priority infiltration target outside the United States. Meanwhile, as North Korean IT workers expanded into Asia-Pacific and Europe, they added Singapore citizenship to their forged nationality lists, using stolen passports and forged identity documents to pass hiring review. This threat is especially prominent for Singapore's technology, fintech, and outsourced development industries because these sectors heavily depend on remote hiring and cross-border developers, and as a regional headquarters location, enterprise internal access permissions often cover Southeast Asian multi-country business lines. North Korea is known to use Singapore private entities as springboards for both real-world and cyberspace operations. As of April 2026, North Korea-linked hackers accounted for 76% of global cryptocurrency theft value during the same period from just two attacks, with cumulative historical theft reaching USD 6.75 billion. In aggregate, Singapore faces not single-dimensional malware attacks but a systematic compound threat spanning supply chain manipulation, developer social engineering, and personnel identity infiltration.

BlueNoroff

BlueNoroff is a Lazarus ecosystem cluster focused on financial asset theft, but during this period its independent operational tempo, dedicated tool chain, and clear target preferences make it a threat entity requiring separate assessment. More critically, compared with the Lazarus core cluster, BlueNoroff's activity against Singapore has more direct, attributable public evidence support. Singapore is BlueNoroff's second-largest victim country globally after the United States. Its threat focus concentrates heavily on cryptocurrency and Web3 enterprise executives, fintech decision-makers, and developer supply chains.

By attack path, BlueNoroff affected relevant Singapore industries through two primary means during this period.

First, AI deepfake video-conference targeted social engineering. Attackers impersonate legal executives or venture partners in the fintech sector, sending meeting invitations to targets via Calendly with links pointing to carefully forged Zoom or Teams pages. After victims enter, they see a convincing video-conference interface that simultaneously executes two operations in the background: covert capture of the victim's live camera feed and deployment of ClickFix-style clipboard hijacking attacks. After compromise, a multi-stage credential extraction pipeline starts immediately—first stealing Telegram desktop sessions to hijack the victim's social accounts for contacting the next batch of targets, then injecting AES-encrypted shellcode into Chromium-based browsers to bypass browser security mechanisms and directly extract master encryption keys and locally stored credentials, primarily targeting cryptocurrency wallet extensions. By activity tempo, this campaign surged sharply in mid-2025, peaked at 121 monthly incidents in March 2026, and shows sustained acceleration overall. 80% of identified targets are active in cryptocurrency, blockchain finance, or related investment fields, with CEOs and founders accounting for 45%. Singapore crypto industry executives and fintech decision-makers routinely use video-conference tools for cross-border business communication and have natural trust in calendar-invitation meeting workflows—precisely constituting the ideal target surface for this attack path.

Second, multi-registry supply chain poisoning targeting the developer ecosystem. From January to April 2026, BlueNoroff-associated cluster UNC1069 deployed approximately 1,700 malicious software packages across five major package manager registries—npm, PyPI, Go, Rust, and PHP—constituting the largest single multi-registry supply chain attack on record. Malicious packages use pre-install hooks to trigger payloads the instant developers run npm install, completing compromise before any manual code review stage. Singapore is Southeast Asia's largest blockchain and fintech developer community; many development teams directly pull dependencies from these public registries in daily CI/CD pipelines. Once developer endpoints are compromised, attackers can penetrate upstream along code deployment chains to reach enterprise wallet management systems, transaction signing services, and production environments.

6.3 Indonesia: Government and Finance Rank High, Mobile Identity Fraud Chains Prominent

Indonesia accounted for 4.9% of Asia-Pacific incidents, with an annualized growth rate of +35.0% in 2026—the fastest among the five priority countries—with threat posture accelerating deterioration. Indonesia's threat structure is shaped by three concurrent lines: government data exposure from large-scale digital governance and decentralized local systems, identity fraud chains formed by mobile banking, e-wallets, and instant messaging adoption, and ransomware and business-continuity pressure on manufacturing, mining, energy, aviation, and agricultural enterprises.

1. Attack Type Analysis

Table 6-10 Indonesia Attack Type Distribution

Attack Type	Share of Country Incidents
Data Breach	49.4%
Ransomware	26.2%
Phishing	22.4%
APT Attack	15.0%
DDoS Attack	4.6%
Supply Chain Attack	2.2%
Cryptocurrency Theft	1.9%

Data breach was the most prominent security incident type in Indonesia during this period, accounting for 49.4% of all samples. By overlapping tags, 33.8% were associated with ransomware activity and 23.7% carried APT tags, with cross-tagging between the two categories. This structure means that nearly half of data exfiltration did not originate from advanced group-directed theft or as byproducts of ransomware activity but from more foundational exposure—misconfigured government databases, inadequate protection on local government portals, weak permission management on education platforms, and external service interfaces without desensitization. Period incidents already covered police systems, audit agencies, traffic management, school account systems, online ticketing platforms, and local financial service platforms, with leaked content spanning identity information, financial records, student files, travel trajectories, and public-service relationship data.

Ransomware accounted for 26.2% of all incidents, below the combined level of the five priority countries and regions, but internal structure warrants attention: 63.8% of ransomware incidents also involved data exfiltration, indicating the dual-extortion model has stabilized in Indonesia. Unlike Australia's ransomware ecosystem—where pressure leverage primarily depends on regulatory disclosure obligations and reputational damage from customer notification—Indonesia's ransom returns are built more on physical operational disruption: manufacturing shutdown, mining and energy project delays, aviation and logistics

chain breaks, agricultural supply rhythm obstruction, and local public services falling into unavailable states. In other words, attackers exploit not compliance pressure but the fragility of business continuity itself.

Phishing accounted for 22.4%; APT attacks accounted for 15.0%; both threats in Indonesia show characteristics deeply bound to mobile entry points. High-frequency attack templates in samples start with forged government notifications, tax documents, and WhatsApp messages, inducing users to sideload malicious APKs with payloads covering Android remote-control Trojans, banking Trojans, OTP SMS interceptors, and fake login pages. Delivery logic is highly consistent: establish initial trust through government or bank brands, guide users to complete application installation or credential submission, obtain SMS permissions and then hijack sessions and take over accounts—the pivot of the entire chain lies in systematic exploitation of user trust habits rather than technical vulnerability breakthrough. DDoS attacks accounted for 4.6%; absolute share is limited but concentrated on government portals and public-service systems—such targets are highly sensitive to short-term availability disruption, and hacktivist forces continue to use government system reachability itself as a pressure lever.

2. Victimized Industry Distribution

Table 6-11 Indonesia Top 10 Victimized Industries

Rank	Industry	Share
1	Government	35.1%
2	Technology	17.8%
3	Financial Services	16.7%
4	Education	11.7%
5	Manufacturing	11.3%
6	Healthcare	10.2%
7	Cybersecurity	9.8%
8	Government Public Services	9.6%
9	Energy	7.2%
10	Telecommunications	5.8%

Government ranked first at 35.1%; combined with government public services (9.6%), government-related incidents total nearly 45%, approaching half of all samples. This proportion far exceeds the other four priority countries and regions, reflecting that Indonesia's government system—from central ministries to local administration, from government databases to public-facing online services—bears disproportionate pressure across the attack surface. Government and government public services ranking first and eighth rather than merged into one category itself indicates different exposure logic: the former involves more targeted penetration and data theft of institutional networks, while the latter points more to foundational exposure of local portals, outsourced systems, and public entry points.

Technology (17.8%) and cybersecurity (9.8%) combined for 27.6%, forming the second-largest attacked cluster after government. Both industries entering the top ten points to a structurally significant risk for Indonesia's digitalization process: software vendors, hosting service providers, and security service providers are not only direct attack victims but also underlying nodes on which government, financial, and education industry digital operations depend—their compromise propagates impact downstream along service relationships.

Financial services accounted for 16.7%, close to the technology industry, indicating attacks against Indonesia's financial system have reached stable scale rather than scattered incidents. Education ranked fourth at 11.7%, at a relatively high level among the five priority countries and regions, consistent with Indonesia's rapid education platform digitalization outpacing security investment. Manufacturing (11.3%), healthcare (10.2%), and energy (7.2%)—three real-economy industries—combined for 28.7%, indicating attacker target selection has expanded from information-intensive industries to operation-intensive industries, where core risk lies not in data exposure but business interruption. Telecommunications (5.8%) ranked last by share, but given telecom infrastructure's carrying role for all the above industries, its strategic value as an attack entry point exceeds what incident volume reflects.

3. Highly Active Ransomware Groups

TheGentlemen

TheGentlemen first appeared in July 2025, operating in RaaS mode with extremely rapid growth—35 victims listed in Q4 2025, surging to 182 in Q1 2026, becoming the world's second-most-active ransomware group during the same period. GuidePoint assesses this explosive growth most likely indicates experienced associated operators and management teams driving the brand behind the scenes. Technically, the group possesses cross-platform encryption capability (Windows/Linux/ESXi), employs dual-extortion mode, and completes initial breakthrough via exposed VPN and Active Directory weaknesses.

In Indonesia, TheGentlemen concentrated attacks on manufacturing and transport targets with the highest downtime cost. In February 2026 it attacked state-owned airline Garuda Indonesia with a 72-hour negotiation deadline before full data leak; during the same period it attacked Astra Otoparts (Japanese automotive parts joint venture) and chemical enterprise PT Pupuk Iskandar Muda. By global target distribution, TheGentlemen maintained high activity in both Thailand and Indonesia, showing clear Southeast Asia regional operational preference—unlike most ransomware groups centered on North America and Europe, this group treats Southeast Asian real-economy sectors as its core harvest zone.

Everest

Everest has been active since late 2020; early activity focused on encryption ransomware, later gradually shifting toward pure data extortion—stealing sensitive data and threatening public sale without necessarily deploying encryption payloads. Initial breakthrough primarily relies on stolen credentials, phishing delivery, and exposed unpatched services; after entering internal networks, the group uses legitimate management tools for lateral movement to blend into normal traffic. The group is known for

targeted selection rather than indiscriminate scanning, focusing on mid-to-large institutions in government, healthcare, manufacturing, and IT services.

In Indonesia, Everest's preference for government targets warrants attention. In April 2026 it attacked Indonesia's Customs Analytics Platform, with leak pages pointing to public-sector data exfiltration; in the same month it attacked e-commerce platform Tokoparts with threats to publicly release data. Globally, Everest victims concentrate in North America and Europe; Indonesia is one of its few priority Asia-Pacific focus countries. Continuous selection of government institutions and local platforms as targets indicates the group has independent judgment of Indonesian public-sector data value and payment willingness rather than opportunistic scanning results.

Incransom

Incransom has been active since mid-2023, using strong encryption algorithms to lock files, primarily delivering payloads via phishing emails and compromised websites. Global victims concentrate in North America, Europe, and Australia, but in Indonesia the group concentrated attacks on high-value entities in energy and manufacturing.

In November 2025 it attacked Sarulla Operation, one of the world's largest geothermal power operators, with leaked content covering administrative records, financial data, budgets, user information, and more than 1,000 passport records; during the same period it attacked industrial manufacturing firm PT Wiraswasta Gemilang Indonesia (chemicals and lubricant production). Both incidents targeted critical operational nodes in Indonesia's resources and energy industries; depth of leaked data—passport records, contract files, account details—far exceeded ordinary database exposure, directly exposing weak internal data classification and access control at critical infrastructure operators. Incransom completely disappeared from Indonesia samples in 2026, possibly undergoing rebranding or law enforcement intervention.

4. Active APT Groups

Indonesia's APT threats primarily originate from North Korea, Southeast Asian financial crime groups, and South Asia.

Lazarus

Lazarus's impact on Indonesia during this period primarily manifested as spillover coverage from multi-country coordinated vulnerability exploitation activities rather than targeted penetration against Indonesian entities. Attack paths follow two lines.

First, indirect spillover from supply-chain-level vulnerabilities. In December 2025, the critical React Server Components vulnerability (CVE-2025-55182) was exploited by multiple APT groups including Lazarus for remote code execution, affecting more than 30 organizations, with Indonesia's financial and retail industries listed as affected targets.

Second, developer social engineering targeting the cryptocurrency ecosystem. Lazarus has long delivered malicious code repositories to Web3 and cryptocurrency developers via LinkedIn fake recruitment, using

"interview projects" and "test code" as lures to steal wallet credentials and cloud access permissions. Indonesia has more than 18 million cryptocurrency users and is one of Southeast Asia's largest crypto markets—this user base naturally places it within coverage of Operation Dream Job-class activities.

GoldFactory

GoldFactory is the threat organization causing the most direct, largest-scale actual harm to Indonesian end users during this period. The group is an East Asia-background financial crime organization that launched large-scale mobile financial fraud across Southeast Asia from October 2024, with attack chains starting in Thailand, expanding through Vietnam, and entering Indonesia by mid-2025. By December 2025, Group-IB had identified more than 3,000 malicious artifacts causing at least 11,000 infections, of which approximately 63% of modified counterfeit banking app variants targeted the Indonesian market, with approximately 2,200 infections occurring in Indonesia.

The attack chain is highly localized. Attackers proactively contact potential victims by phone, impersonating government staff to guide them to click malicious links in instant messaging applications; links point to phishing pages impersonating Google Play, inducing installation of malicious APKs containing Gigabud, MMRat, or Remo remote-control tools. In January 2026, GoldFactory further aligned attack themes with Indonesia's tax filing season, impersonating the official tax platform Coretax to launch a new large-scale phishing wave, integrating phishing websites, WhatsApp social engineering, malicious APK sideloading, and vishing into a complete device-control and fund-transfer chain.

The most notable technical feature is biometric data theft capability. The latest variant Gigaflower supports approximately 48 remote-control commands, including real-time screen streaming via WebRTC, keylogging and interface manipulation via accessibility services, displaying forged system update and PIN entry interfaces to steal personal information, and extracting text from ID document photos. More critically, GoldFactory uses impersonated banking apps to guide victims through "facial verification" workflows, collecting facial biometrics for AI deepfakes to bypass bank biometric authentication defenses.

GoldFactory precisely exploits the structural gap in Indonesia's "mobile-first" internet market—mobile payment penetration is growing rapidly, but anti-fraud mechanisms and app store sideloading controls lag severely, and the gap between the two provides sustained soil for large-scale mobile infections.

SideWinder

SideWinder is an India-linked veteran espionage group active since 2012. Kaspersky characterizes it as "one of the Asia-Pacific region's most aggressive threat groups." During this period the group completed strategic expansion in two directions: geographic scope extended from traditional South Asian targets (Pakistan, Sri Lanka, Nepal) to Southeast Asia; industry focus expanded from government and military entities to maritime infrastructure, logistics, and nuclear energy. In tracking from H2 2024 through 2025, Kaspersky explicitly detected SideWinder attack activity in Indonesia. Analysis further confirmed SideWinder began attacking Thailand in late 2025 and expanded targets to Indonesia in early 2026.

At the attack technique level, SideWinder's core initial intrusion path is spear-phishing delivery of Office documents containing exploit code, using CVE-2017-11882 to trigger a multi-stage infection chain

ultimately deploying .NET downloader ModuleInstaller and advanced in-memory espionage tool StealerBot. SideWinder established standardized operational workflows around Windows service persistence, staged payload delivery, and rapid C2 infrastructure rotation, so defenders may face redeployment within hours after completing remediation. Once its tools are identified, SideWinder can generate new modified versions within five hours to evade detection.

Indonesia is both a SideWinder maritime infrastructure attack target and within coverage of its diplomatic entity attacks. As the world's largest archipelagic nation with more than 17,000 islands and extensive port infrastructure, Indonesia's maritime intelligence value aligns closely with SideWinder's current industry preferences.

6.4 Malaysia: Government, Manufacturing, and Finance Under Parallel Pressure; Semiconductor and Public-Safety Systems Hold Intelligence Value

During the reporting period, Malaysia’s cybersecurity risk landscape reflected a structure of parallel commercial ransomware, supply chain propagation, and public-safety intelligence collection. Government, financial services, healthcare, and enterprise services faced sustained data breach and ransomware pressure, while electronics manufacturing, semiconductor packaging and testing, automotive, energy, aviation, and public-safety systems carried higher industrial and strategic value. Malaysia is targeted not only because of local market scale; its position in global electronics manufacturing and Southeast Asian supply chains means a single identity or technology service provider compromise can simultaneously affect local enterprises, multinational customers, and upstream/downstream projects.

1. Attack Type Analysis

Attack Type	Share of Incidents in Country
Data Breach	50.3%
Ransomware	39.8%
Phishing	21.7%
APT	18.1%
DDoS	2.2%
Supply Chain Attack	2.2%
Cryptocurrency Theft	0.9%
Cryptojacking	0.2%

Note: A single incident may be tagged with multiple attack types; therefore, the sum of percentages does not equal 100%.

Ransomware is the most prominent deviation in Malaysia's threat structure, at 39.8%—a complete mirror of Hong Kong's 16.2%. As Asia-Pacific economies, the two play sharply different roles in attacker calculus: Malaysia is a profit venue for ransomware operators; Hong Kong is an intelligence-collection venue for APT groups. Malaysia's high ransomware pressure stems from industrial structure itself—semiconductor packaging and testing, automotive manufacturing, palm oil processing, construction, and healthcare are sectors with significant downtime costs. Production line interruption, project delay, and suspension of patient services can be converted directly into negotiation leverage; attackers need not rely on regulatory disclosure or reputational pressure to establish coercion.

APT activity accounts for 18.1%, roughly five percentage points below the five-country average. This lower share reflects both limitations in advanced-threat detection and attribution in Malaysia and, to some extent, ransomware activity "crowding out" attention on the threat landscape—similar to Indonesia. The internal structure of APT incidents cannot be overlooked: 81.0% involved data breach and 45.2% involved phishing, indicating that once activity reaches APT tier, attack chains almost invariably include intelligence theft and social-engineering entry points, with attacker intent clearly oriented toward credential acquisition and file exfiltration.

Phishing overall accounts for 21.7%, below Indonesia, but distribution characteristics differ markedly. Phishing density in financial services (35.0%) and government (29.7%) is significantly above the overall level, indicating that phishing in Malaysia concentrates on targeted delivery to high-value sectors rather than broad mobile-side propagation as in Indonesia.

2. Victim Industry Distribution

Rank	Industry	Share
1	Government	13.2%
2	Technology	9.0%
3	Financial Services	8.2%
4	Manufacturing	8.1%
5	Healthcare	4.5%
6	Energy	3.6%
7	Education	3.3%
8	Telecommunications	2.8%
9	Construction	2.7%
10	Technology – Cybersecurity	2.6%

Manufacturing and construction are Malaysia's most typical "operational ransomware" targets. Ransomware share in manufacturing is 42.9%; in construction it reaches 58.5%—the highest among all industries across the five countries. APT share is only 16.5% and 7.3%, respectively. Cases along manufacturing, assembly, engineering, and headquarters file systems—including the Penang

semiconductor packaging and testing cluster (Intel, AMD, Broadcom), automotive manufacturing (Tan Chong Motor Holdings—Crypto24 stole over 300 GB of data), Fujitsu Components Malaysia (attacked by Qilin), construction group Kerjaya Prospek Group, and engineering consultancy Meinhardt—indicate attackers are seeking high-downtime-cost targets across these sectors.

Financial services show the most complete "ransomware + data + phishing" composite structure among the five countries: ransomware 43.0%, data breach 71.0%, phishing 35.0%—each the highest for that industry across the five countries. This means attackers not only encrypt systems but also exfiltrate large volumes of customer data and use phishing as an initial entry vector. In April 2025, Bursa Malaysia (Malaysia's stock exchange) suffered trading account compromise leading to unauthorized stock transactions. Once financial data is exfiltrated, impact extends beyond a one-time breach—data enters dark web markets for secondary use in account takeover, identity fraud, and targeted scams.

Government is one of few Malaysian industries where APT share exceeds ransomware (APT 27.1% vs. ransomware 20.6%), with phishing also elevated at 29.7%. This structure resembles government sectors in Singapore and Hong Kong, indicating sustained intelligence-collection activity by nation-state actors against Malaysian government targets. Telecommunications shows higher APT share (29.3%); Malaysia connects to South China Sea submarine cable nodes, and intelligence value of telecom infrastructure remains a persistent draw.

Healthcare (ransomware 46.9%, APT only 12.5%), energy (ransomware 42.3%), and education (breach 53.3%) all showed accelerated growth in 2026. Malaysia's "MyDigital" national digital transformation program is pushing these traditional sectors online, but security investment lags severely behind digitalization pace—healthcare's ransomware share is the highest across all industries, indicating this sector is paying the most direct price for "fast rollout, slow protection."

3. Highly Active Ransomware Groups

Qilin

Qilin is the most prominent ransomware group in Malaysia during this period, accounting for 16.8% of Malaysian ransomware incidents. Confirmed targets span telecommunications (XOX Mobile), technology (SFG Technology), restaurant chains (Oriental Castle), and roughly ten local industries including construction, manufacturing, and aviation. Breadth of coverage indicates Qilin has established a stable affiliate target pool in Malaysia.

Attack entry typically involves administrator credentials purchased on the dark web or direct scanning of exposed boundary devices such as VPN, RDP, and FortiOS. After network access, attackers use tools such as Mimikatz and NirSoft to steal credentials, then move laterally via PsExec and WMI, and modify Active Directory Group Policy Objects to expand RDP access. During data exfiltration, packed files are typically transferred to external servers via Rclone and MegaCMD; finally, all AD-managed endpoints and VMware ESXi hosts are encrypted, VSS shadow copies are deleted synchronously, and partial data is published on leak sites with countdown timers to apply pressure. For Malaysian enterprises, supplier account review, VPN credential rotation, and GPO modification monitoring are the most direct defensive priorities.

Devman

Devman's most representative Malaysia incident this period is HeiTech Padu—a local technology company handling government and critical-industry projects—where approximately 60 GB of data was stolen and a high ransom demand was issued. Remaining records primarily involve unnamed local enterprises; overall public technical profiling remains insufficient.

Available intelligence indicates Devman habitually uses stolen credentials or password-spraying attacks, entering target networks via VPN or RDP, with overall technique prioritizing data theft over encryption—publishing partial data to prove intrusion authenticity before forcing targets into negotiation. The deeper risk of the HeiTech Padu incident lies in its status as an IT service provider—shared administrator accounts, remote support tools, and centrally stored customer data can all become lateral propagation paths toward downstream customers, with risk transmitted along the entire customer chain.

Crypto24

Confirmed Crypto24 targets in Malaysia include Palmgold Management and Warisan TC Holdings, with additional incidents recorded in transportation and manufacturing. Target selection shows clear preference—attackers pursue not only large production enterprises but holding and management entities controlling subsidiary permissions, customer assets, or supply chain data. Once a group headquarters is compromised, propagation across subsidiaries is possible via shared identity systems and file servers.

Technically, Crypto24's most distinctive feature is the custom RealBlindingEDR tool, designed specifically to disable EDR/XDR protections post-compromise—its core differentiator from other ransomware groups. The attack flow includes credential theft, scheduled-task persistence, cloud-service transfer of exfiltrated data to reduce detection probability, and finally snapshot deletion followed by encryption of business systems. After a ransom claim, enterprises should treat whether data was copied as a separate issue independent of encryption events, while reviewing full access logs for cloud accounts, file shares, VPN, and external management tools.

4. Active APT Groups

Lazarus

Lazarus is the most threatening North Korea–linked attack group facing Malaysia's financial sector, conducting targeted attacks against banks, securities firms, and fintech companies with fund theft as the primary objective. In 2025, Lazarus attacked a Southeast Asian bank, using Excel attachments disguised as compliance documents to lure financial practitioners into clicking, exploiting an undisclosed Microsoft zero-day for interaction-free intrusion, loading a customized rootkit for kernel-level privileges, and ultimately stealing approximately USD 40 million. Malaysia was listed among affected countries.

At the technical level, Lazarus's weaponization of legitimate system tools further increases detection difficulty. An April 2025 report covering multiple countries including Malaysia disclosed that Lazarus used Windows' built-in mavinject.exe to inject malicious DLLs into normal processes such as explorer.exe. mavinject.exe carries a Microsoft signature and is whitelisted by most security solutions; the attack

involved no suspicious file drops and no new process creation, rendering traditional signature detection ineffective. Defense should shift toward process behavior baseline monitoring with dedicated alerting on anomalous mavinject.exe invocation.

Lazarus's financial-theft sub-group BlueNoroff launched GhostCall and GhostHire social-engineering attack lines against the blockchain industry in 2025. GhostCall targets technology company and venture capital executives via forged Zoom meeting links; GhostHire poses as recruiters distributing malicious "test assignments" through GitHub to reach developers—both leveraging generative AI to improve localization of social-engineering scripts. Confirmed impact includes India, Turkey, Australia, and other countries; no public reports of Malaysia-based victims exist. Malaysia's rapidly growing fintech ecosystem and relatively high Web3 developer density fit BlueNoroff's typical target profile—once a developer endpoint is compromised, attackers can simultaneously obtain code repository tokens, cloud keys, and wallet permissions, crossing R&D and fund boundaries from a single entry point.

SideWinder

SideWinder is the South Asia–linked threat most warranting attention in Malaysia's government and maritime sectors. Active since 2012, the group showed two notable shifts in 2025: first, targets expanded from traditional South Asian government and military institutions to Southeast Asian maritime and logistics industries, with Malaysia—as a core Malacca Strait shipping nation and South China Sea submarine cable node—explicitly on target lists; second, attack chains evolved from CVE-2017-11882 Office exploit documents to PDF+ClickOnce infection chains, specifically bypassing macro-blocking policies deployed by modernized organizations.

Operationally, SideWinder sends phishing emails via domains impersonating government agencies, with attachments as PDFs forged as official notices or meeting credentials containing a "Download latest Adobe Reader" button. Clicking triggers a ClickOnce deployment chain ultimately delivering StealerBot—a modular .NET information-stealing tool with reverse shell, screenshots, keylogging, password harvesting, remote desktop credential theft, and file exfiltration capabilities. Between March and September 2025, attackers conducted at least four delivery waves against targets, each using different lure themes (inter-ministerial meetings, transfer orders, maritime policy notices, etc.). This multi-wave, theme-rotation delivery pattern indicates SideWinder conducts prior research on each target's role and dynamically adjusts lure content based on current events.

Malaysia has numerous government agencies with uneven central and local protection levels; SideWinder may prioritize entry through weaker local nodes or peripheral maritime departments with weaker email security and endpoint management, then use obtained internal documents and contact lists to expand laterally toward higher-value central institutions. Defense should focus on three areas: gateway-level blocking of ClickOnce and .application file types; sandbox detection triggered by non-standard PDF behavior (embedded download links, anomalous JavaScript); and alerting rules for StealerBot behavioral signatures (anomalous screenshot frequency, bulk file enumeration, encrypted outbound traffic outside business hours).

6.5 Hong Kong: Government, Technology, Finance, and Telecommunications Concentrated; Identity and Data Risk Outweigh Traditional Ransomware

During the reporting period, Hong Kong threats concentrated in government, technology, financial services, telecommunications, and cybersecurity—high-sensitivity sectors—and reflected a structure of high APT tagging and identity-attack weight with low traditional ransomware weight. As an international financial center, cross-border enterprise hub, and high-density communications market, attackers place greater emphasis on accounts, customer data, trading relationships, enterprise technology environments, and communication connections than on large-scale endpoint encryption alone.

1. Attack Type Analysis

Attack Type	Share of Incidents in Region
Data Breach	58.6%
APT	37.6%
Phishing	29.0%
Ransomware	16.2%
DDoS	6.2%
Supply Chain Attack	2.9%
Cryptojacking	1.9%
Cryptocurrency Theft	1.4%

Data breach accounts for 58.6%—the highest proportion among the five focus countries/regions. Among data breach incidents, 52.8% also carry APT tags and 20.3% also carry ransomware tags, indicating Hong Kong data outflow more often overlaps with long-term espionage, account compromise, and remote-control attacks rather than primarily serving as a ransomware adjunct. Once government, financial, technology, telecommunications, and enterprise service data is exfiltrated, it can be used for cross-border business fraud, precision phishing, fund theft, and sustained approach to high-value individuals.

APT-tagged incidents account for 37.6%—21.3 percentage points above the five-country composite level; phishing at 29.0% is also notably elevated. These proportions primarily reflect threat-type annotation density in the dataset rather than confirmed intrusion counts. Under an analytical scope excluding China-linked threats by organizational profile, Hong Kong should focus on three paths: targeted social engineering against virtual-asset and technology personnel; theft of multinational enterprise and shipping commercial intelligence; and remote control and data wiping of mobile endpoints. Period samples include BlueNoroff's GhostCall/GhostHire activity, RedCurl-related shipping threat materials, NOKKI/Konni mobile attacks, and Hong Kong Post EC-Ship platform attacks and SMS impersonation incidents.

Ransomware accounts for 16.2%—less than half the five-country composite level—but 73.5% of ransomware incidents involve data breach, indicating Hong Kong ransomware risk leans toward "data ransom" rather than pure encryption shutdown. DDoS at 6.2% is also notably above composite levels, reflecting sensitivity of financial trading, public services, telecommunications, and public-opinion events to availability attacks.

2. Victim Industry Distribution

Rank	Industry	Share
1	Government	14.8%
2	Technology	14.0%
3	Financial Services	8.6%
4	Manufacturing	6.2%
5	Telecommunications	5.4%
6	Technology – Cybersecurity	5.3%
7	Healthcare	3.7%
8	Education	3.3%
9	Business	2.3%
10	Energy	2.1%

Note: A single incident may involve multiple attack types; therefore, percentages overlap and are not summed.

Hong Kong's industry threat landscape is distinctive: except for manufacturing and healthcare, APT share exceeds ransomware in every industry—a pattern unique among the five countries, reflecting comprehensive intelligence-theft penetration across Hong Kong sectors.

Government and technology rank nearly equal (14.8% and 14.0%) with highly similar threat structures—APT share at 44.4% and 34.9%, respectively, with ransomware below 15% in both. Technology industry share is the highest among the five countries, because numerous multinational technology companies place Asia-Pacific R&D centers in Hong Kong; compromising these institutions can yield technology roadmaps and intellectual property covering entire regions. 60% of APT attacks target commercial entities rather than government institutions—completely opposite to global norms, a direct reflection of Hong Kong as a commercial intelligence hub.

Financial services (8.6%) shows the most noteworthy threat structure: phishing at 44.7% is highest; APT at 38.3% is also prominent; ransomware is only 8.5%. Hong Kong's financial sector faces core risk of "being penetrated" rather than "being encrypted." A representative case is the 2024 AI deepfake video conference scam against the Hong Kong branch CFO of multinational engineering firm Arup: fraudsters used AI voice and video cloning to impersonate the CFO and multiple colleagues, instructing wire transfers of USD 25

million during a live Zoom call—amounts within the employee's approval authority did not trigger secondary authorization. Hong Kong's multilingual environment and complex regulatory framework yield phishing success rates of 39.8%—65% above global average—language and institutional complexity themselves becoming weaknesses attackers can exploit.

Manufacturing (6.2%) is the only industry where ransomware and APT shares are equal (both 35.3%), facing dual pressure from commercial ransomware and nation-state espionage. All three top ransomware groups primarily target manufacturing.

Telecommunications (5.4%—highest among five countries) shows APT share of 36.4% and ransomware only 6.1%. Hong Kong hosts multiple international submarine cable landing stations and is a key Asia-Pacific internet traffic exchange point; intelligence value of telecom infrastructure remains a persistent draw.

Healthcare (3.7%) and education (3.3%) both trend upward in 2026. Healthcare ransomware share at 36.0% is highest across all industries—one of few Hong Kong sectors where ransomware dominates. Education APT share at 45.0% is conversely highest across all industries, contrasting with institutions typically viewed as "soft targets"—Hong Kong universities' international cooperation networks and cross-border research data make them high-value intelligence-collection entry points.

3. Highly Active Ransomware Groups

Qilin

Qilin is the most prominent ransomware group in Hong Kong during this period, primarily targeting manufacturing and technology. On June 5, 2025, Qilin attacked Hong Kong chip design company AppoTech, which focuses on system-on-chip (SoC) solutions covering Bluetooth, audio, video, Wi-Fi, and microcontroller applications, with operations in Shenzhen, Zhuhai, Taiwan, and the United States. In this attack Qilin stole proprietary design data and internal files and published them on a dark web Tor site without encrypting systems; the leak page did not specify a ransom amount. From September through November 2025, Qilin attacks across multiple Hong Kong industries continued this "data exposure first, no system lock" pattern—sharply contrasting with its Kuala Lumpur International Airport attack in Malaysia, which demanded USD 10 million and involved full encryption.

Clear business logic underlies this difference: in infrastructure scenarios with extremely high downtime costs, encryption maximizes negotiation leverage; in IP-intensive technology scenarios, once chip design files enter dark web markets, competitors and nation-state actors can both obtain them—data exposure itself constitutes sustained, irreversible threat, with coercion effect potentially deeper than encryption. Qilin affiliates enter networks via phishing, leaked credentials, and boundary vulnerabilities, then conduct data theft and leak-site pressure. For Hong Kong technology enterprises, access control over design files, source code, and technical documentation, plus monitoring of anomalous large-scale file access, are the most direct defensive priorities.

Nightspire

Nightspire was first identified in early 2025 and compromised at least 64 organizations across 33 countries between March and June. Its core Hong Kong incident is the March 2025 attack on listed company Far East Consortium International Limited (Far East Consortium, FEC)—systems were compromised on March 5; attackers stole 250 GB of data and set March 28 as the dark web publication deadline. The Office of the Privacy Commissioner for Personal Data received notification on March 17 and initiated compliance review per procedure. On the same March 5, integrated environmental services company Wai Hong Environmental Services Limited was also compromised; 30 GB of data was published on March 15; the Privacy Commissioner received notification on March 20. FEC spans property development, Dorsett Hospitality International, and car park management, with total assets exceeding HKD 54.8 billion and operations across Hong Kong, mainland China, Australia, Malaysia, Singapore, the UK, and New Zealand—meaning a single Hong Kong intrusion exposed data involving commercial secrets across seven markets.

Nightspire's attack chain relies entirely on legitimate tools with no custom malware. Initial entry is exposed RDP with weak credentials; post-compromise access is maintained via Chrome Remote Desktop and AnyDesk; Everything searches for high-value files; 7-Zip packages them; MEGAsync uploads to MEGA cloud storage; finally a Go-language encryptor traverses directories, encrypts files, and appends the ".nspire" suffix, while also encrypting OneDrive synchronized files. Every tool in the chain is legitimate enterprise operations software—traditional endpoint protection can hardly trigger alerts at any single stage. This pure LOLBins pattern imposes clear defensive requirements on Hong Kong enterprises: behavioral detection for RDP exposure, parallel use of unconventional remote-control tools, large-scale file enumeration, and anomalous cloud storage exfiltration—not reliance on malware signature identification.

Akira

Akira is linked to former Conti members, with over 250 global victims and ransom demands exceeding USD 40 million—second only to Qilin as the largest globally active ransomware group this period. In February 2025, Akira attacked Thong Sia Group—regional distributor of Seiko products in Hong Kong, Singapore, Malaysia, Brunei, and Macau—leaking financial data, payment details, audit reports, employee passports, and customer personal information. Thong Sia's multi-country distribution network means this intrusion simultaneously exposed commercial data and customer privacy across five markets, with attack impact propagating along supply chains upstream and downstream. Records also indicate Akira attacked a Hong Kong maritime investment group; that case became the core sample for analyzing Akira's Hong Kong attack techniques this period.

Akira habitually obtains initial access via unpatched VPN service vulnerabilities or stolen RDP credentials, then extensively uses LOLBins and remote management tools to extend dwell time, deploying dual-platform encryptors targeting both Windows and Linux/VMware ESXi. In the Hong Kong maritime investment group case, attackers obtained initial access via VPN login, moved laterally to Veeam backup servers and Hyper-V virtualization environments, destroyed backups before encrypting production systems—a "cut recovery paths first, then encrypt" strategy leaving victims unable to self-recover and shifting negotiation leverage entirely to attackers. Akira's average detection time in Hong Kong reached

37 days; dwell capability approaches APT levels, indicating penetration depth into Hong Kong enterprise network environments should not be underestimated.

4. Active APT Groups

Lazarus Group

Lazarus is the most significant North Korea–related cyber threat in Hong Kong. The group and its associated ecosystem have long targeted cryptocurrency exchanges, Web3 projects, blockchain infrastructure, fintech companies, and software developers—objectives include both large-scale direct fund theft and acquisition of private keys, seed phrases, API tokens, enterprise internal credentials, and code repository access. For Hong Kong, Lazarus threat focus lies not in traditional boundary breach but in the unique attack surface formed by Hong Kong as Asia-Pacific cryptocurrency trading center, offshore financial hub, and concentration of multinational Asia-Pacific headquarters—once a Hong Kong node is breached, attackers can leverage it to penetrate associated subsidiary networks distributed across Asia-Pacific.

By attack vector, Lazarus affects Hong Kong-related industries through three primary paths. The first is fake recruitment and developer phishing. Attackers pose as recruiters, venture capital firms, or project partners, reaching Hong Kong local cryptocurrency industry practitioners and Web3 developers via LinkedIn, Discord, Telegram, and GitHub, inducing downloads of "interview projects," "test code," or "meeting tools." These projects typically contain malicious JavaScript, Python scripts, or poisoned npm packages that, when executed, steal browser credentials, cryptocurrency wallet information, code repository access tokens, and cloud accounts. From January through July 2025, Lazarus continuously deployed over 234 malicious packages on npm and PyPI, potentially exposing over 36,000 global developers; Hong Kong and Asia-Pacific Web3 and blockchain developers fall within attack exposure range. This technique is common in Lazarus's Contagious Interview and Operation Dream Job sustained campaigns.

The second is supply chain attacks against Hong Kong cryptocurrency exchanges and fintech enterprises. Attackers do not directly target end users but compromise third-party signing tools or multi-signature management platforms enterprises depend on, tampering with underlying transaction logic without changing frontend display to achieve large-scale asset transfer. On February 21, 2025, Lazarus compromised Safe{Wallet} developer environments, injecting malicious code into AWS S3–hosted frontend files, and within seven minutes stole approximately USD 1.46–1.5 billion (401,346 ETH) from Bybit exchange—the largest cryptocurrency theft in history. Bybit CEO Ben Zhou publicly disclosed that stolen funds were obfuscated through multiple layers via mixing protocols and cross-chain tools including Wasabi Wallet, Tornado Cash, Railgun, Thorchain, and eXch, ultimately entering P2P and OTC channels for cash-out. ZachXBT previously disclosed that a Chinese OTC trader assisted Lazarus in converting tens of millions of dollars from multiple hack attacks into cash since 2022, with channels associated with Hong Kong and Southeast Asian OTC networks.

The third is direct endpoint attacks against Hong Kong cryptocurrency industry practitioners. In May 2025, Lazarus shifted targets from large institutions to small and medium cryptocurrency merchants, directly

stealing over USD 5.2 million from one merchant and transferring funds via mixing tools—publicly tracked and disclosed by on-chain analyst ZachXBT. Such attacks indicate Lazarus targets have expanded from large exchanges alone to small and medium financial services practitioners, with both attack threshold and target scope continuously widening.

Earth Bluecrow

Earth Bluecrow (also known as Red Menshen, DecisiveArchitect, Red Dev 18) is the most covert APT threat facing Hong Kong telecommunications, financial services, and critical infrastructure. The group uses the BPFDoor backdoor as its core tool, focusing on kernel-level long-term persistence on Linux systems to establish persistent access within target networks as foundation for long-term intelligence collection and lateral penetration. For Hong Kong, Earth Bluecrow threat focus lies not in direct destruction but in silent network persistence—average dwell time reaches 8.7 months, twice the global average, with almost no alerts triggered during this period.

By attack capability, Earth Bluecrow's core strengths manifest at three levels. First is BPFDoor kernel-level stealth technology. BPFDoor uses Berkeley Packet Filtering (BPF) technology, activating the backdoor via a "magic packet" mechanism without opening any listening ports, completely bypassing conventional firewall rules and port-scan detection. In April 2025, Trend Micro disclosed Earth Bluecrow deployed in Hong Kong a previously unreported BPFDoor controller component that can open reverse shells on compromised servers, achieving deep penetration of target networks. Victims covered Linux server environments across Hong Kong telecommunications, financial services, and retail sectors; specific institutions were not disclosed.

Second is cross-border lateral penetration capability. Hong Kong multinational enterprise headquarters hold special strategic value for Earth Bluecrow: successfully compromising one Hong Kong-based multinational typically enables lateral penetration into 8 to 12 subsidiary networks distributed across Asia-Pacific, forming an intelligence collection system covering entire regions. The group also recorded attack activity in South Korea, Malaysia, Myanmar, and Egypt during the same period; Hong Kong is its most valuable single-point target in Asia-Pacific operations.

Third is long-term pre-positioning against infrastructure. In May 2026, Hong Kong Police Cyber Security and Technology Crime Bureau formally disclosed in the *2025 Cybersecurity Report*: in assessments of over 100,000 critical infrastructure network assets, police identified malicious activity by five international hacker groups targeting Hong Kong critical infrastructure; 7.8% of assets had system vulnerabilities; and attackers had pre-positioned access within infrastructure networks—fortunately reported in time so services were not interrupted by attacks. Earth Bluecrow TTPs closely match attack patterns described in that report.

About ThreatBook

Founded in 2015, ThreatBook is The Agentic Security Company. Our technical core combines field-tested Agentic AI with one of the world's deepest threat intelligence engines protecting Cloud, Network, Edge, and Endpoint as a single, integrated security foundation. Our AI-native SecOps agents and AI security solutions run alongside ThreatBook's threat intelligence, detection, and response portfolio to give enterprises a security capability that is continuously improving, field-tested against the latest attacks, and built to adapt and stay resilient with the threat landscape.

contactus@threatbook.io

www.threatbook.io

@ThreatbookLabs

linkedin.com/company/threatbook