JANUARY 2026

REGIONAL THREAT REPORT

APAC

STEPHANIE SCHNEIDER

CYBER THREAT
INTELLIGENCE ANALYST

MICHAEL KOSAK

SENIOR PRINCIPAL
INTELLIGENCE ANALYST

REGIONAL SNAPSHOT

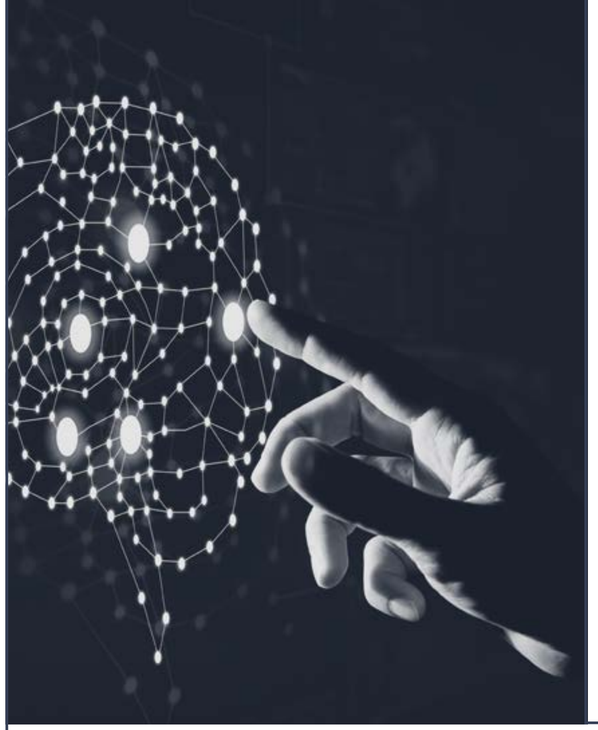
The pace and scope of cyber threats in the Asia-Pacific (APAC) region remained high over Q4 2025. In region, significant incidents involved significant data breaches due to stolen credentials and insider threats, DPRK cryptocurrency theft, and state-backed cyberespionage campaigns.

Artificial intelligence (AI) is a force multiplier, increasing both offensive and defensive capabilities in a constant arms race. While attackers are adopting new tactics incorporating AI, attacks will continue to primarily originate from traditional methods and be enhanced by this technology, as opposed to being revolutionary transformed.

Vulnerability exploitation is widespread, impacting entities globally and in region. Several recent zero days have been attributed to Chinese state-backed hackers have exploited several recent zero days, demonstrating Beijing-aligned cyber actors' abilities to develop and quickly capitalize on new vulnerabilities.

Infostealers continued to drive much of the threat activity within the APAC cyber threat environment over Q4 2025, as part of a continued trend. To address this threat, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released a fireside chat in early December highlighting the threat to all Australians, ranging from individuals to large businesses.

Ransomware remains a prevalent threat to the regions. Amongst Asia-Pacific countries, India and Australia were the two most targeted by ransomware and extortion groups in 2025. Reflecting global trends, Manufacturing was the most targeted sector and Qilin was the most active group in-region.



ARTIFICIAL INTELLIGENCE (AI) IS A FORCE MULTIPLIER, INCREASING BOTH OFFENSIVE AND DEFENSIVE CAPABILITIES.

VULNERABILITY EXPLOITATION IS WIDESPREAD, IMPACTING ENTITIES GLOBALLY AND IN REGION.

INFOSTEALERS CONTINUED TO DRIVE MUCH OF THE THREAT ACTIVITY WITHIN THE APAC CYBER THREAT ENVIRONMENT OVER Q4 2025

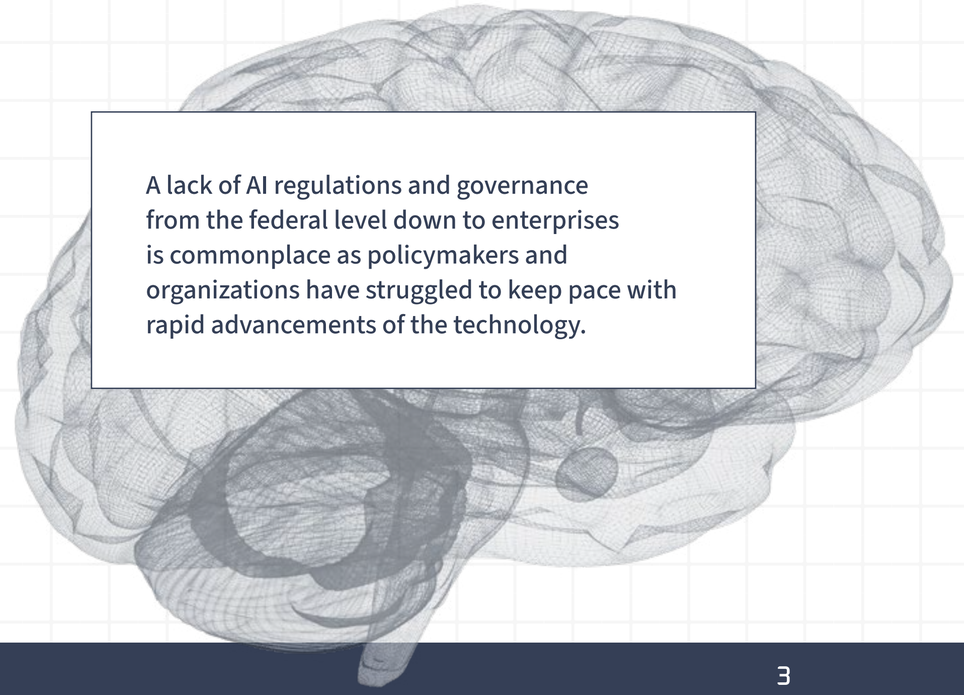
ARTIFICIAL INTELLIGENCE IS A FORCE MULTIPLIER

2025 saw the rapid adoption of AI globally as threat actors and defenders alike race to use the technology to enhance their efforts against the other. To date, AI has enhanced existing capabilities rather than transformed them into something completely new. AI now enables attackers to conduct larger, more targeted attacks and lowers the bar for less skilled hackers to launch attacks. In 2026, cyber attacks will likely continue to stem from traditional means, such as exposed credentials or vulnerability exploitation, and will be enhanced by AI measures.

Widespread adoption of AI has been used to partially automate ransomware attacks, enhance social engineering attacks using generative AI like deepfakes to conduct more convincing vishing (vishing) campaigns, and commit fraud. Looking ahead, AI-enabled malware will likely become more autonomous to conduct attacks. AI-enabled malware can adapt and pivot campaigns in real time by generating scripts, altering codes to avoid detection, and creating malicious functions on demand. Cybercriminals have adopted new tactics like AI sidebar spoofing and slopsquatting, in addition to traditional cyber tactics like prompt injection attacks. Attackers will also likely test methods to conduct fully automated AI attacks.

AI has already transformed threats regionally. For instance, the digital fraud landscape in Asia-Pacific has evolved as synthetic personal data attacks increased 142% year-on-year. This is indicative of digital fraud shifting to become more sophisticated as high-quality fraud attacks increased 180% globally. The rapid rise of deepfakes has also driven some fraudulent activity, such as advanced impersonation scams. Singapore experienced a decline in overall fraud growth but reported a 158% increase in deepfake incidents primarily related to fraudulent e-wallet registrations. 84% of APAC organizations believe AI will play a major role in future threat scenarios, yet only 42% reportedly have formal policies governing its secure use. Additionally, employees are increasingly exposing sensitive data through AI tools and personal cloud applications. In Australia, intellectual property (42%), source code (31%), and regulated data (20%) are most commonly leaked, with 55% of individuals using personal AI accounts for work. Platforms like LinkedIn, OneDrive (95%), Google Drive (94%), Facebook (93%), and ChatGPT (85%) amplify risks, creating an attack surface that attackers can exploit using AI-powered scraping and intelligence gathering.

Cyber criminals have also targeted vulnerabilities in AI applications such as Agentic AI, browser AI assistants, and large language models (LLMs). In 2026, we anticipate more data poisoning and attacks targeting AI companies directly, given the trove of valuable data they process and store. We're seeing some of these attacks already. Agentic browsers, or AI browsers, inherit the legacy attack surface of traditional browsers (i.e., CVE exploits, malicious extensions, etc.) while introducing new AI-specific attack surfaces (i.e., prompt injection, data leakage, etc.) A recent report by Cloudflare showed a surge in attacks targeting AI companies in Q3 2025, which coincided with increased public debate over AI regulations.



A lack of AI regulations and governance from the federal level down to enterprises is commonplace as policymakers and organizations have struggled to keep pace with rapid advancements of the technology.

VULNERABILITIES UNDER EXPLOITATION EVERYWHERE

Several recently reported vulnerabilities are allegedly linked to Chinese-backed hackers. China has historically been the biggest perpetrator of using zero-day exploits, mainly focusing on devices that lack endpoint detection and response capabilities. Chinese-backed hackers are also notorious for exploiting known vulnerabilities, sometimes within hours of public disclosure.

- (US, Australia say 'MongoBleed' bug being exploited) In late December, US and Australian cyber agencies confirmed a new vulnerability dubbed "MongoBleed" is under active exploitation. MongoBleed affects several versions of MongoDB's database management system and allows anyone to steal database passwords, AWS secret keys and more.

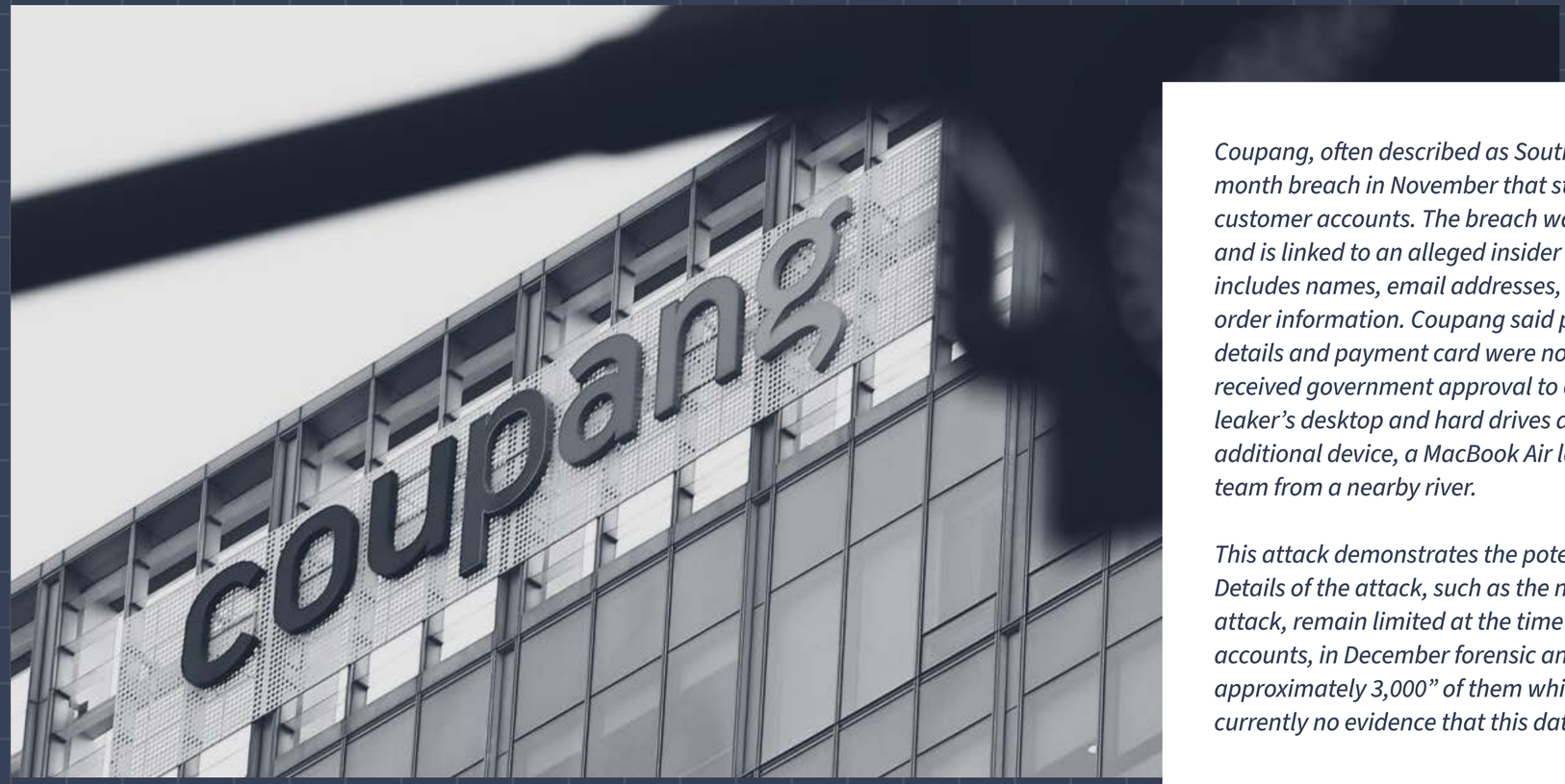
- (Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System) The Australian Signals Directorate (ASD) previously warned that Chinese state-sponsored cyber threat actors are targeting networks globally, including, but not limited to, telecommunications, government, transportation, lodging, and military infrastructure networks.

- They've successfully gained initial access by exploiting publicly known common vulnerabilities found in firewalls, routers, and more. This warning was part of a Cybersecurity Advisory released by several international authoring and co-sealing agencies.

- Hackers possibly linked to China's Ministry of State Security (MSS) swiftly exploited a critical vulnerability in React Server Components (aka React2Shell), leading to privilege escalation, data theft, and ransomware. Many of these attacks are automatic and widespread, with over 50 confirmed organizations that were compromised just one week after initial reporting, and thousands more at risk globally. Several China-nexus groups began exploiting the maximum-severity vulnerability hours after public disclosure, and others nation-state actors, cybercriminals, and ransomware gangs quickly followed. Since automation is widespread, the FBI and CISA issued alerts outlining the activity. (Researchers track dozens of organizations affected by React2Shell compromises tied to China's MSS)

- (Chinese attackers exploiting zero-day to target Cisco email security products) Cisco said it became aware that Chinese-backed hackers (tracked as UAT-9686, overlapping with APT41) were exploiting a vulnerability (CVE-2025-20393) in a widely used email management tool in mid-December. The vulnerability affects appliances within certain internet-facing ports that are running Cisco's AsyncOS Software for its Secure Email Gateway and Secure Email and Web Manager. The hackers used a persistence tool called AquaShell to maintain their access and take other actions against a reportedly "limited subset of appliances."

SOUTH KOREA'S E-COMMERCE GIANT COUPANG EXPERIENCES BREACH.



Coupang, often described as South Korea's version of Amazon, discovered a multi-month breach in November that started in June and affected up to 33.7 million customer accounts. The breach was reportedly conducted using overseas servers and is linked to an alleged insider who is a Chinese national. Exposed information includes names, email addresses, phone numbers, shipping addresses and some order information. Coupang said passwords and other account information, payment details and payment card were not exposed. In late December, Coupang said it received government approval to contact the leaker and successfully retrieved the leaker's desktop and hard drives after an initial meeting. As a result of questioning, an additional device, a MacBook Air laptop, was identified and then recovered by a diving team from a nearby river.

This attack demonstrates the potential widespread damage from insider threats. Details of the attack, such as the nature of the breach and methods used in the attack, remain limited at the time of reporting. While the attacker accessed 33 million accounts, in December forensic analysts reported they only "retained user data from approximately 3,000" of them which was allegedly deleted. The company said there is currently no evidence that this data was sold or shared with third parties.

SOURCE

NORTH KOREA REMAINS TOP CRYPTO THIEF IN 2025.

DPRK hackers are responsible for most cryptocurrency thefts in 2025, marking a record-breaking year for crypto crime, according to Chainalysis' annual report. North Korean hackers stole more than $2 billion worth of cryptocurrency this year, representing almost 60% of all stolen assets. This figure is $681 million more than what the country's hackers are estimated to have stolen in 2024. North Korea focused on targeting large, centralized targets with significant reserves in 2025. Funds were stolen through hacking crypto services themselves, targeting individuals with large assets, and planting insiders at crypto companies.

North Korea continues to conduct financially motivated theft targeting cryptocurrency to bypass international sanctions and fund its regime. Since Chainalysis began tracking the figures in 2022, North Korea has stolen $6.75 billion in crypto. The United Nations said last year that it is tracking dozens of incidents over a five-year period that have netted North Korea about $3 billion.

SOURCE

JAPANESE MEDIA GIANT NIKKEI'S RECORDS WERE EXPOSED VIA STOLEN SLACK CREDENTIALS.

Unspecified hackers gained unauthorized access to Nikkei's internal Slack communication system after employee's personal computer was infected with malware (possibly an infostealer), allowing attackers to steal and use Slack authentication credentials to gain access to employee accounts. The attack purportedly exposed data linked to more than 17,000 people, including its employees and business partners. The company identified the incident in September and implemented security measures in response, such as changing passwords.

This breach underscores the risks of hybrid work arrangements, where employees may use personal devices to access corporate networks. While details of this incident remain limited at the time of reporting, infostealers are a common initial access vector to gain unauthorized access to networks by stealing credentials and other sensitive information.

SOURCE

JAPAN'S ASKUL TARGETED AS PART OF WIDER RANSOMWARE ATTACK ON JAPANESE RETAILERS DISRUPTING SUPPLY CHAINS.

Japanese office and household goods retailer Askul was hit by a ransomware attack in October that disrupted its ordering and logistics systems for about six weeks. The ransomware group RansomHouse exposed contact information and inquiry details from users of Askul, Lohaco, and Soloel Arena, in addition to supplier data on internal servers. The attack disrupted supply chains for several Japanese retailers, including Ryohin Keikaku.

The ransomware attack on Askul is part of a larger wave of recent ransomware attacks against major Japanese firms. Active since March 2022, RansomHouse is known for its extortion tactics and has been linked to Russia-aligned threat actors, including Alphv/BlackCat, LockBit 3.0 and RagnarLocker.

SOURCE

NEW PAKISTAN ESPIONAGE CAMPAIGN TARGETS INDIAN GOVERNMENT AND UNIVERSITIES.

Pakistan-linked hackers target Indian government, universities in new spying campaign | The Record from Recorded Future News

Pakistan-backed APT36 (aka Transparent Tribe) launched a new cyberespionage campaign targeting Indian government, academic, and strategic institutions. Spearphishing emails including a ZIP archive contained a malicious file that appeared to be a PDF that delivered two malware components, ReadOnly and WriteOnly, when opened. Cyfirma reported that the malware can remotely control infected machines, exfiltrate data and carry out persistent surveillance.

Ongoing geopolitical tensions continue to fuel cyberespionage campaigns between Pakistan and India. Another Pakistan-linked threat actor Cosmic Leopard carried out a years-long espionage campaign against Indian government agencies and defense and technology companies last year.

SOURCE

DEEP DIVE OF THE MONTH

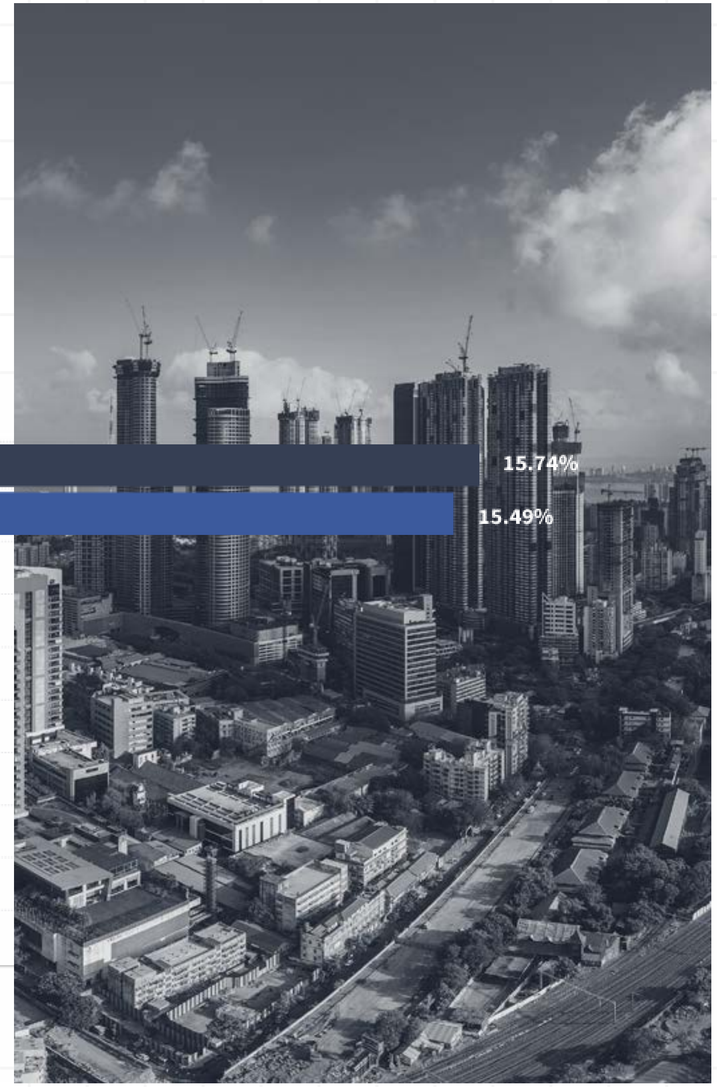
INFOSTEALERS

For this month's deep dive, we are again focusing on infostealers. Not only have infostealers continued to be a driving force within the APAC cyber threat environment over the quarter, but they have also proven to be a consistently growing threat over the last few years and have been an integral part of major cyber breaches conducted by both cybercriminals and nation-states. In fact, we expect infostealers to remain one of the major cyber threats in 2026 with continued growth both in number of malware families and number of credentials stolen.

Infostealers continue to pose such a threat in the region that the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released a fireside chat in early December highlighting the threat to all Australians, ranging from individuals to large businesses. The chat, led by ACSC chief Stephanie Crowe, features a wide-ranging discussion of the threats posed by infostealers, the impact they have had, and what steps individuals and organizations can take to protect themselves. LastPass was fortunate enough to participate in this conversation along with experts from Australia's myGov and Yubico. The video can be viewed here and ACSC's advice on how to protect yourself from information stealing malware can be found in more detail here.

RANSOMWARE BY COUNTRY

India (15.7%) and Australia (15.5%) were by far the most targeted countries by ransomware and extortion groups in 2025, followed by Japan (9.5%), Thailand (8.4%), and Taiwan (8.2%) rounding out the Top 5 targeted countries in the region.



The US, Canada, and Mexico ransomware data analyzed in this report includes the following date range: Jan 1, 2025-Dec 1, 2025

RANSOMWARE BY HACKER GROUP

- Consistent with previous reporting throughout 2025, Qilin remained the most active ransomware group in the region in Q4.
- A few notable ransomware players were more active in the region in Q4 compared to the rest of the year. The Gentlemen was the rising star, taking a big bite out of Vietnam and the Healthcare sector. LockBit, Cl0p, and INC Ransom were also in the top five list, and Nightspire also jumped up the list.

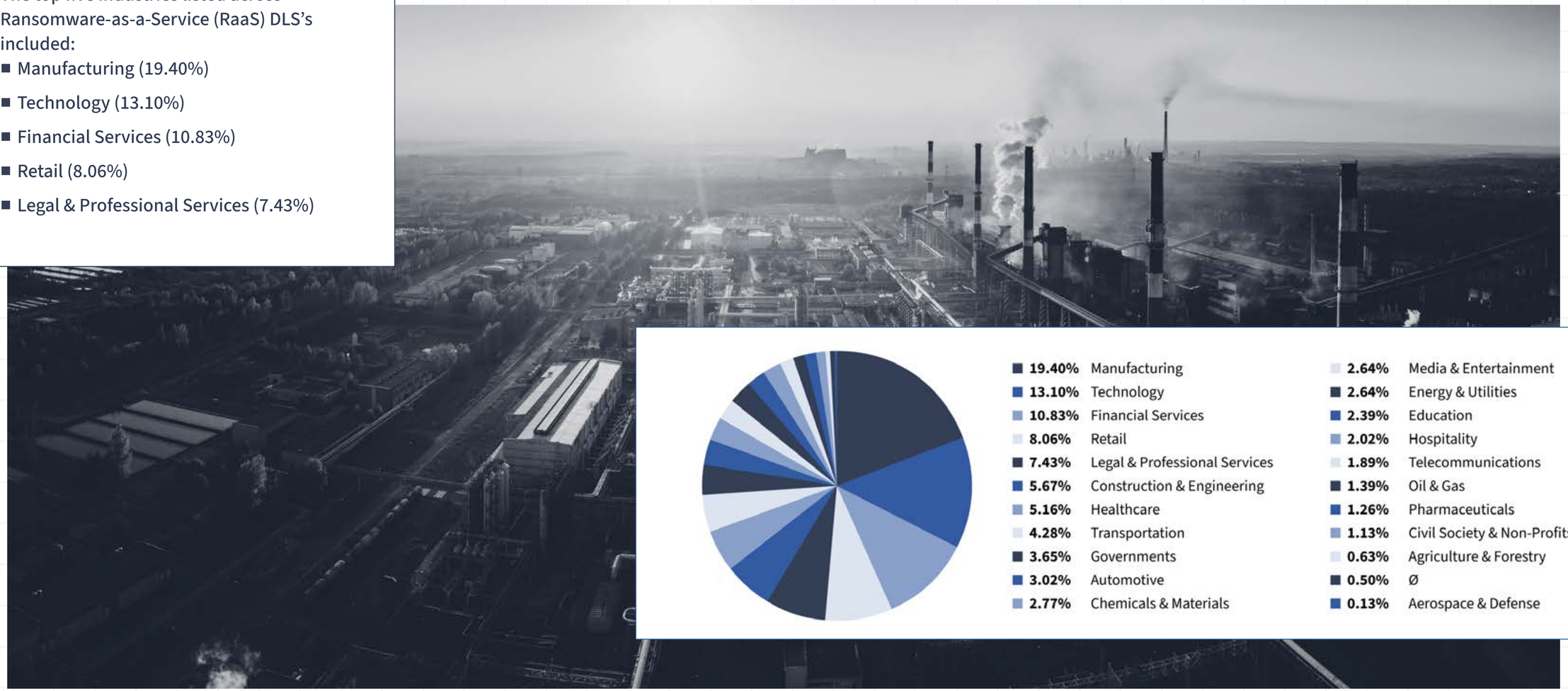
PERCENT OF VICTIMS BY SHAMING SITE

The US, Canada, and Mexico ransomware data analyzed in this report includes the following date range: Jan 1, 2025-Dec 1, 2025

RANSOMWARE BY INDUSTRY

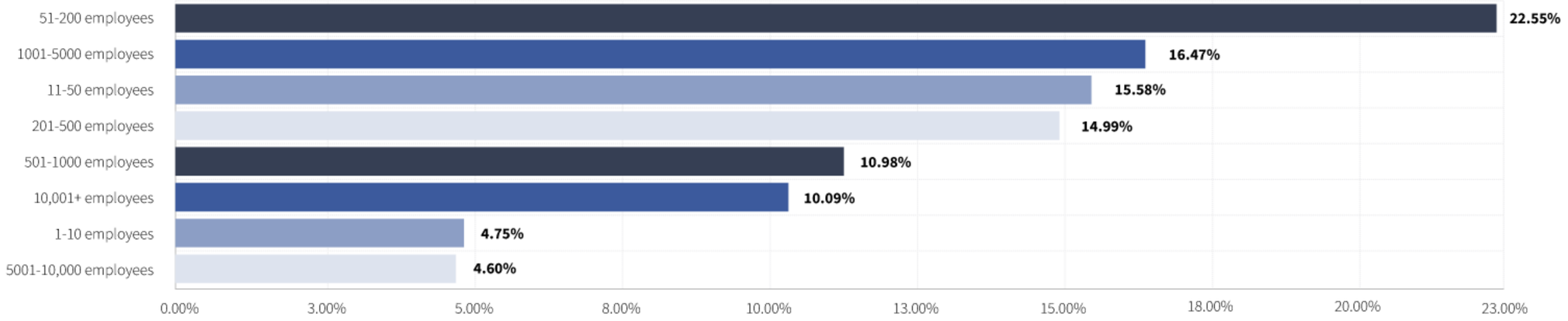
The top five industries listed across Ransomware-as-a-Service (RaaS) DLS's included:

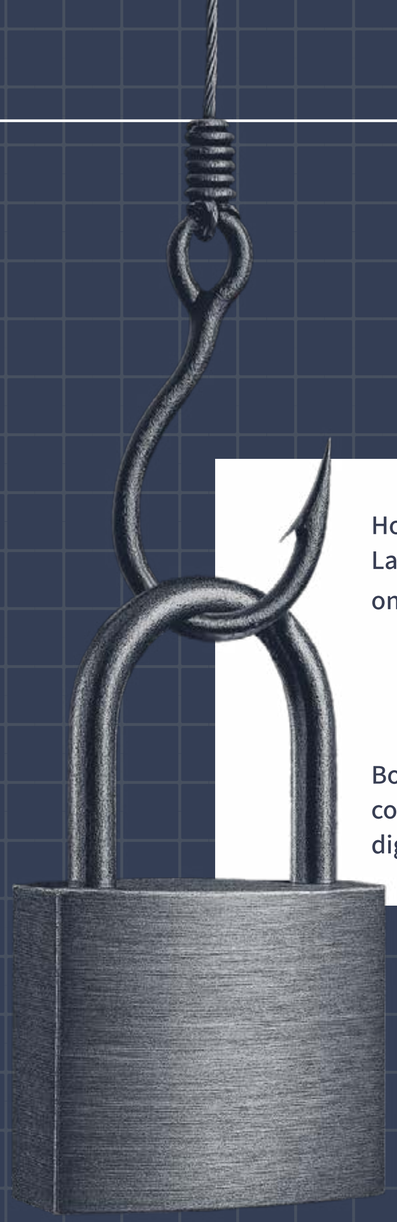
- Manufacturing (19.40%)
- Technology (13.10%)
- Financial Services (10.83%)
- Retail (8.06%)
- Legal & Professional Services (7.43%)



PERCENT OF VICTIMS BY ESTIMATED COMPANY SIZE

The sweet spot for Asia-Pacific companies by size most often listed on DLS's was between 51-200 employees, or mid-sized businesses. This company size segment may be appealing for cybercriminals because they offer a favorable balance of valuable data and sufficient funds to pay demanded ransom payouts, paired with perceived vulnerabilities and weaker defenses compared to large enterprises.





Hooked on cybersecurity? Dive into The Phish Bowl podcast, where the LastPass TIME team's Stephanie Schneider and Mike Kosak cast a wide net on the latest on cyber threats, trends, and tales from the digital deep.

Bookmark the LastPass Threat Intel blog for news on real-time threats, commentary on cybersecurity trends, and best practices to stay safe in the digital world.