Regional Report: Asia-Pacific
October 2025

Stephanie Schneider
Cyber Threat Intelligence Analyst

Michael Kosak
Senior Principal Intelligence Analyst

Regional snapshot

The Asia-Pacific region (APAC) experiences high-frequency cyber espionage and financially motivated attacks involving phishing, data theft, ransomware, and network access sales. APAC remains a primary target for cybercriminals and nation-state actors due to its critical role in global manufacturing and logistics, as well as several key countries' strategic geopolitical roles.

MALWARE TAKES CENTER STAGE

A key threat to private and public sector entities in APAC are the widespread use of malware. Malware was involved in 83% of breaches in APAC last year, up from 58% from the year prior.[1] Infostealer malware remained prevalent, with Lumma accounting for the most observed malware in the region, followed by Atomic stealer in the top ten malwares targeting the region. Additionally, a persistent ransomware threat that heavily targets various sectors like Malaysia's manufacturing industry and Taiwan's financial sector. Ransomware was used in over half of regional breaches.[1] Australia was the most affected country by ransomware with the greatest number of victims listed on ransomware data leak sites (DLS's).

EMERGING TECHNOLOGY

AI-powered tactics are intensifying the threat landscape, enabling more effective, wider-scale attacks. Threat actors have adopted AI to enhance various stages of attacks, including reconnaissance, social engineering, malware, and obfuscation.

COMPETITION FUELS THREATS

Nation-state activity remains primarily focused on espionage, intellectual property (IP) theft, and financial gain. Geopolitical competition between China and the United States is the primary driver of cyber threats in the region. Geopolitical competition in the South China Sea is also a significant contributing factor. A series of joint country and US government-issued warnings about Chinese activities raise concerns about espionage activities targeting critical infrastructure. North Korean hackers have continued their usual cryptocurrency theft and have stolen over $2 billion so far this year to date by using sophisticated social engineering and posing as IT workers to gain access to organizations and raise funds for the regime.

Hacktivism and information operations pose a high-frequency, moderate-impact threat to entities operating in APAC. This activity is fueled by regional political tensions and are increasingly common, particularly related to high-priority areas linked to China, such as Taiwan.

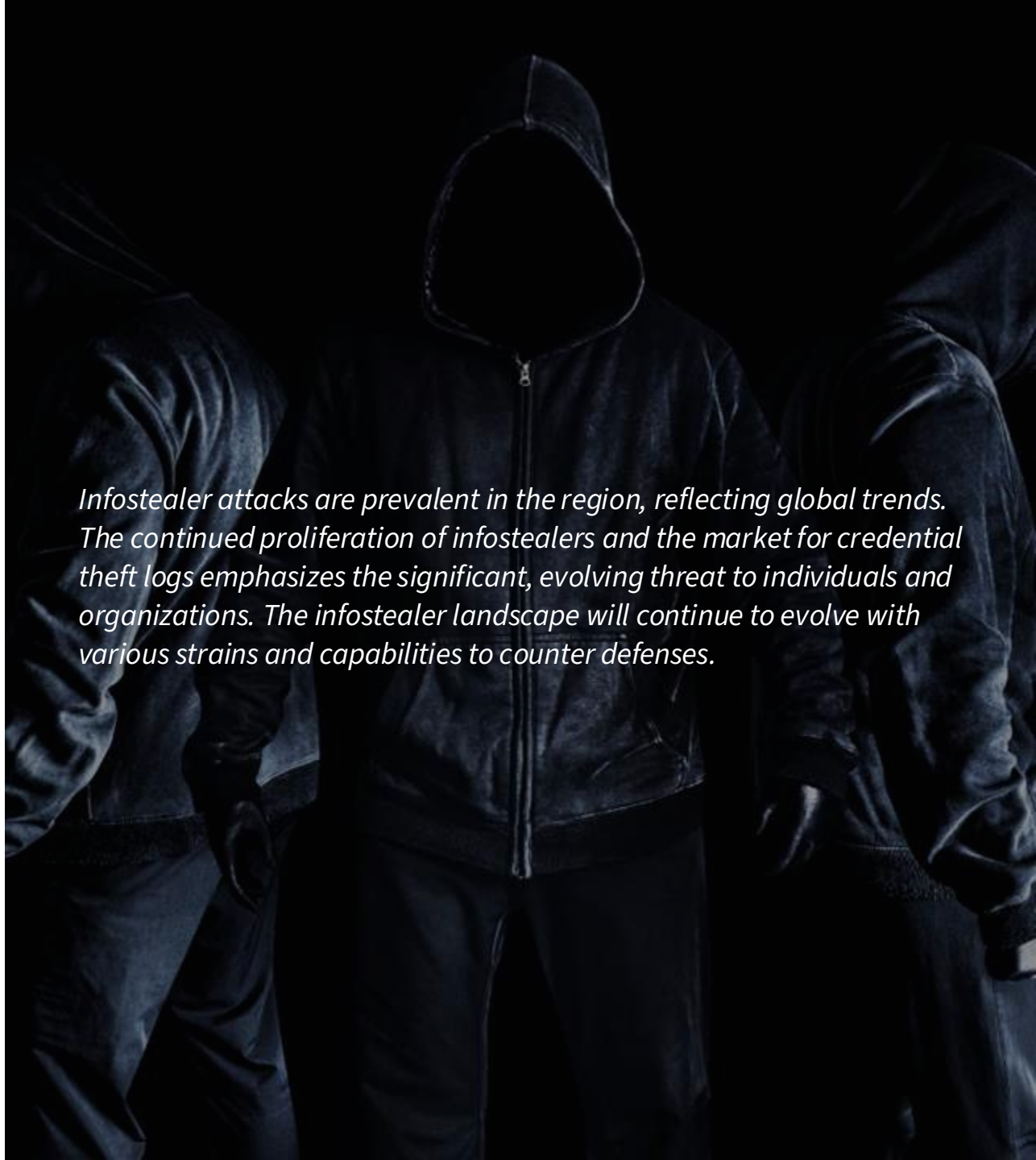
Trends on tap:
Infostealers on the rise

While Lumma has proven resilient following the coordinated law-enforcement takedown in May 2025, more infostealer families took advantage of the disruption and ramped up their activities. Active since February 2025, Acreed became the leading strain for credential theft logs on Russian Market following the Lumma takedown.

While Lumma strains persisted following the takedown, a targeted underground doxxing campaign in September exposed alleged Lumma core members in September. This campaign drove a migration of Lumma's customer base to other infostealer-as-a-service platforms, most notably Vidar and StealC.[2]

Several smaller strains have also emerged, including Katz, Bee, and Aura, reflecting a fractured infostealer marketplace likely in an attempt to avoid law enforcement action.[3]

For a deeper dive into the infostealer threat, we recommend referencing the Australian Signals Directorate's advisory "The silent heist: cybercriminals use information stealer malware to compromise corporate networks."[4]



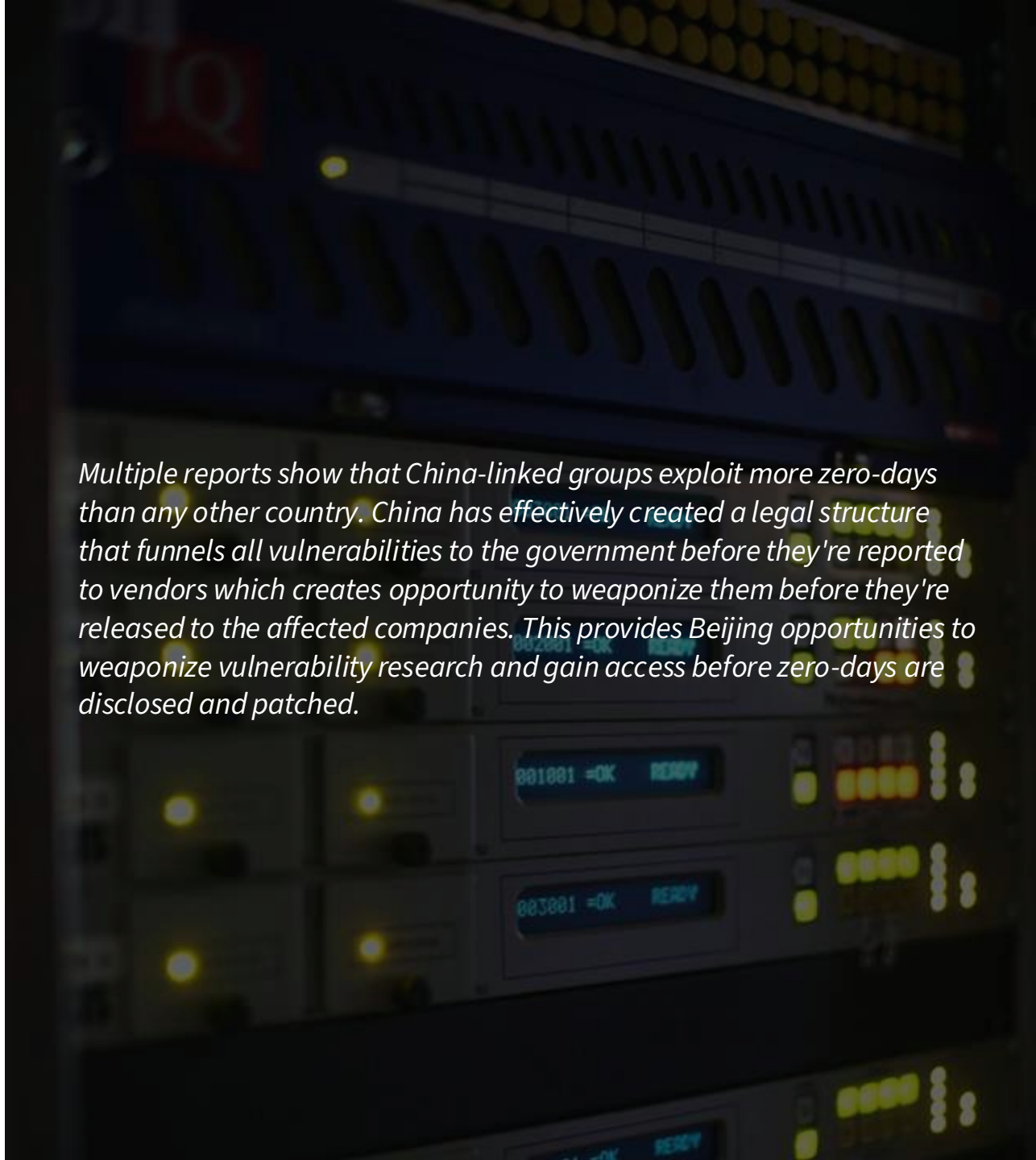
Infostealer attacks are prevalent in the region, reflecting global trends. The continued proliferation of infostealers and the market for credential theft logs emphasizes the significant, evolving threat to individuals and organizations. The infostealer landscape will continue to evolve with various strains and capabilities to counter defenses.

Trends on tap:
Zero-day attacks

The APAC region continues to be a significant target for sophisticated cyberattacks, including a notable prevalence of zero-day exploits leveraged by various state-sponsored and financially motivated actors to achieve their objectives.

Hackers are exploiting a previously unknown vulnerability in outdated Cisco security devices, which are used by governments, telecommunication firms, and critical infrastructure worldwide. Chinese state-sponsored and criminal cyberattacks on Cisco products have been ongoing for several years, with significant activity reported in 2024 and 2025. The Australian Cyber Security Centre (ACSC) has issued recent warnings about critical vulnerabilities in Cisco products that are being actively exploited by hackers without attribution. Some of these attacks have been attributed by third parties to Chinese state-sponsored groups.[5]

In October, OT-ISAC warned that Singapore's critical infrastructure is under active cyberattack by Chinese state-sponsored group UNC3886 who is exploiting zero-day vulnerabilities in Fortinet, VMware, and Juniper systems to gain stealthy, long-term access.[6] Active since at least 2022, UNC3886 is known for targeting defense, telecoms, finance, and OT/IT systems across the US and Asia.



Multiple reports show that China-linked groups exploit more zero-days than any other country. China has effectively created a legal structure that funnels all vulnerabilities to the government before they're reported to vendors which creates opportunity to weaponize them before they're released to the affected companies. This provides Beijing opportunities to weaponize vulnerability research and gain access before zero-days are disclosed and patched.

Trends on tap:
Supply chain compromises

Cybercriminals and nation-state groups use supply chain attacks to achieve espionage and financially-motivated objectives. According to ESET's SMB Cybersecurity Report 2024, 39% of respondents across APAC sited third-party vendor vulnerabilities as a leading cause of breaches.[7]

In September, the Shai-Hulud worm compromised npm packages, exposing companies and individuals to data theft and downstream supply-chain risks in APAC and globally. Attackers used a sophisticated phishing campaign to compromise a npm package maintainer's account, injecting malware into widely used JavaScript packages.[8] The next month, a second self-propagating worm named GlassWorm hit the DevOps space. GlassWorm primarily targets the VS Code extensions space and could possibly spread to other libraries like npm.[9]

In October, the Australian Signals Directorate (ASD) released a report highlighting new cybersecurity risks to organizational supply chains introduced by Artificial Intelligence (AI) and Machine Learning This is largely due to their reliance on a complex ecosystem of models, data, libraries and cloud infrastructure.[10]

Regarding hardware supply chain insertions, there are concerns China may have placed unreported devices, such as radios, in solar-powered highway infrastructure.[11] This announcement comes amid escalating government action over the presence of Chinese technology in America's transportation infrastructure.

These incidents underscore the complex and persistent nature of supply chain compromises in the APAC region. Over-dependencies on companies in hard and software supply chains present an effective attack vector for hackers who will continue to innovate their techniques to exploit trusted relationships, digital infrastructures, and emerging technologies.

Key regional incidents

Crimson Collective breached software company Red Hat.[12]

The Crimson Collective claimed to have breached Red Hat's internal consulting GitLab instance and stolen over 570 GB of data from 28,000 repositories. Crimson Collective is also reportedly going after AWS cloud instances, looking to compromise cloud infrastructure. The attack potentially affected customers include major corporations and government agencies.

The leaked client list shows that several industries with a strong presence in APAC were compromised, including financial services, telecoms, and technology, which are already top targeted sectors regionally. The campaign combining legitimate employee monitoring software with open-source penetration tools to build attack chains is covert and highly effective. Instead of deploying malware, attackers used repurposed legitimate tools to possibly harvest credentials and monitor employee behavior.

Multiple Australian telecommunication company breaches.[13]

In October, hackers breached the parent company of a major Australian phone and internet provider. Hackers accessed customer's emails addresses that led to unauthorized SIM swaps on 34 accounts. In August, another Australian telecom was impacted by a third-party breach that affected 280,000 people. Attackers gained access by using stolen employee credentials to infiltrate a third-party service provider and stole 1,700 customer modem passwords.[1]

The Australian Signals Directorate's Annual Cyber Threat Report 2024-25 noted an increase in malicious activity targeting critical infrastructure, including the telecommunications sector.

DPRK hackers stole over $2 billion in crypto.[14]

North Korean hackers have stolen an estimated $2 billion worth of cryptocurrency assets in 2025, marking the largest annual total on record. That brings the total confirmed amount stolen by the DPRK to more than $6 billion. Blockchain experts at Elliptic say that the amount is almost triple compared to 2024 and far exceeds the previous record of $1.35 billion from 2022, which was in large part due to the Ronin Network and Harmony Bridge attacks.

According to the United Nations and government agencies, these funds are used to further the development of nuclear weapons.

Qilin ransomware claims Asahi brewery attack, leaks data.

Qilin ransomware operators listed Japanese beer giant Asahi on its data leak site and claimed to have exfiltrated more than 9,300 files in 27GB of data. On September 29, the company suspended operations at six Japan-based facilities due to a cyberattack.

Qilin claims that the attack will cause Asahi to lose up to $335 million due to production disruptions at six breweries impacting thirty labels. This attack highlights manufacturing which was the most targeted industry in APAC, with Qilin listing the greatest number of manufacturing victims on its leak site.

Cyberespionage costs Australia $8 billion per year.

In the first of its kind report analyzing the cost of cyberespionage to the country, the Australian government found it was costing approximately $8 billion USD ($12.6 billion AUD) per year – split between loss of IP and response costs.

Australia faces a high level of threat from espionage and foreign interference, according to recent assessments from the Australian Security Intelligence Organisation (ASIO). Multiple countries, including China, Russia, and Iran, are actively involved in these operations.

Deep dive of the month

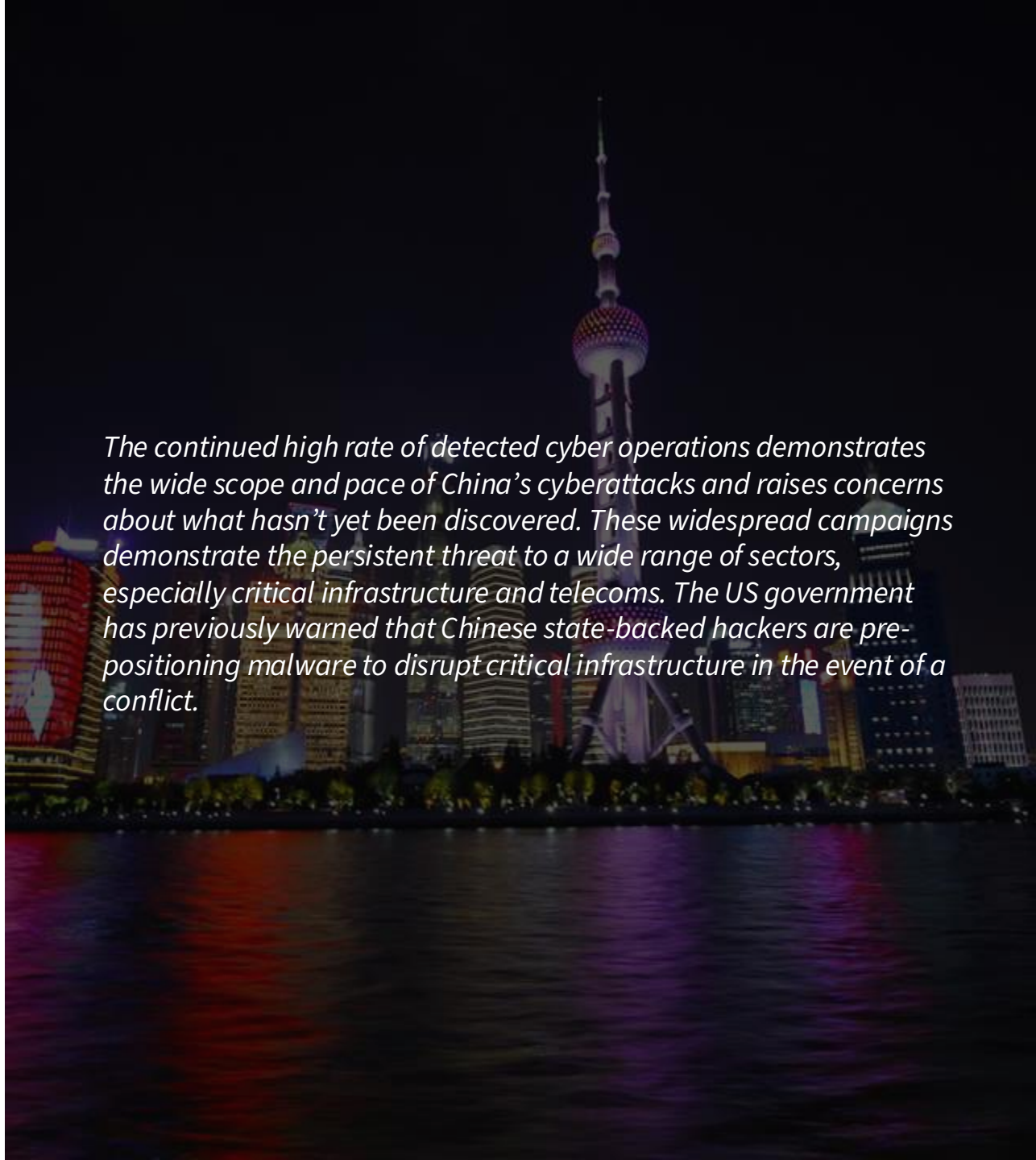
Chinese state-sponsored espionage campaigns remain advanced and persistent

- In August, a broad coalition of countries, including the Five Eyes Alliance (United States, Canada, New Zealand, Australia and the UK) and several others, signed onto a cybersecurity advisory detailing a large, ongoing Chinese-backed espionage campaign targeting networks globally, including the telecommunication and critical infrastructure sectors.[1]
- In a separate advisory, the US government warned of an ongoing Chinese-backed campaign in September targeting Cisco products to get access to networks.[2] They issued an emergency directive to federal agencies to address the issue. Cisco was initially engaged in May 2025 for attacks targeting zero-days in firewall and VPN software.
- Mandiant reported on an ongoing campaign of IP theft targeting software developers and law firms using Brickstorm malware. Mandiant determined that this campaign is related to the Cisco attacks, and both aim to collect intelligence in support of the ongoing trade war with the US.

Deep dive of the month

China espionage campaigns remain advanced and persistent

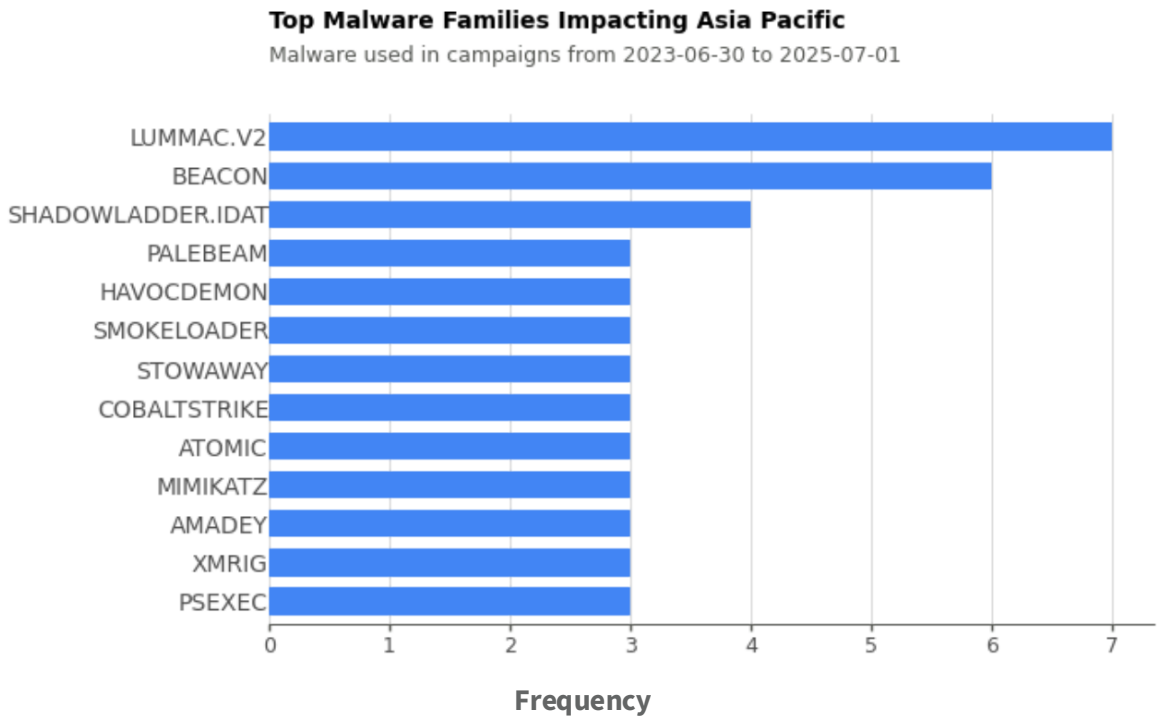
- Chinese state-sponsored Flax Typhoon exploited a geo-mapping tool called ArcGIS for over one year to maintain access to a victim organization's network. A weak administrator password was a key entry vector in this attack, and attackers were able to reset the password.[4] Flax Typhoon has previously targeted critical infrastructure, governments, and IT organizations. The compromise of a geo-mapping tool could pose national security threats, enable critical infrastructure attacks, and steal sensitive information.
- US officials also warned of the presence of unauthorized devices, including hidden radios, in solar-powered highway infrastructure linked back to China.[5] Suspected Chinese-manufactured equipment has also been found in European infrastructure.[6] These Chinese-linked devices have security implications, including sabotage and espionage, and highlight supply chain vulnerabilities. These findings correlate with an increased international focus on potential security vulnerabilities in critical infrastructure such as energy grids.



The continued high rate of detected cyber operations demonstrates the wide scope and pace of China's cyberattacks and raises concerns about what hasn't yet been discovered. These widespread campaigns demonstrate the persistent threat to a wide range of sectors, especially critical infrastructure and telecoms. The US government has previously warned that Chinese state-backed hackers are pre-positioning malware to disrupt critical infrastructure in the event of a conflict.

Top malware families targeting APAC

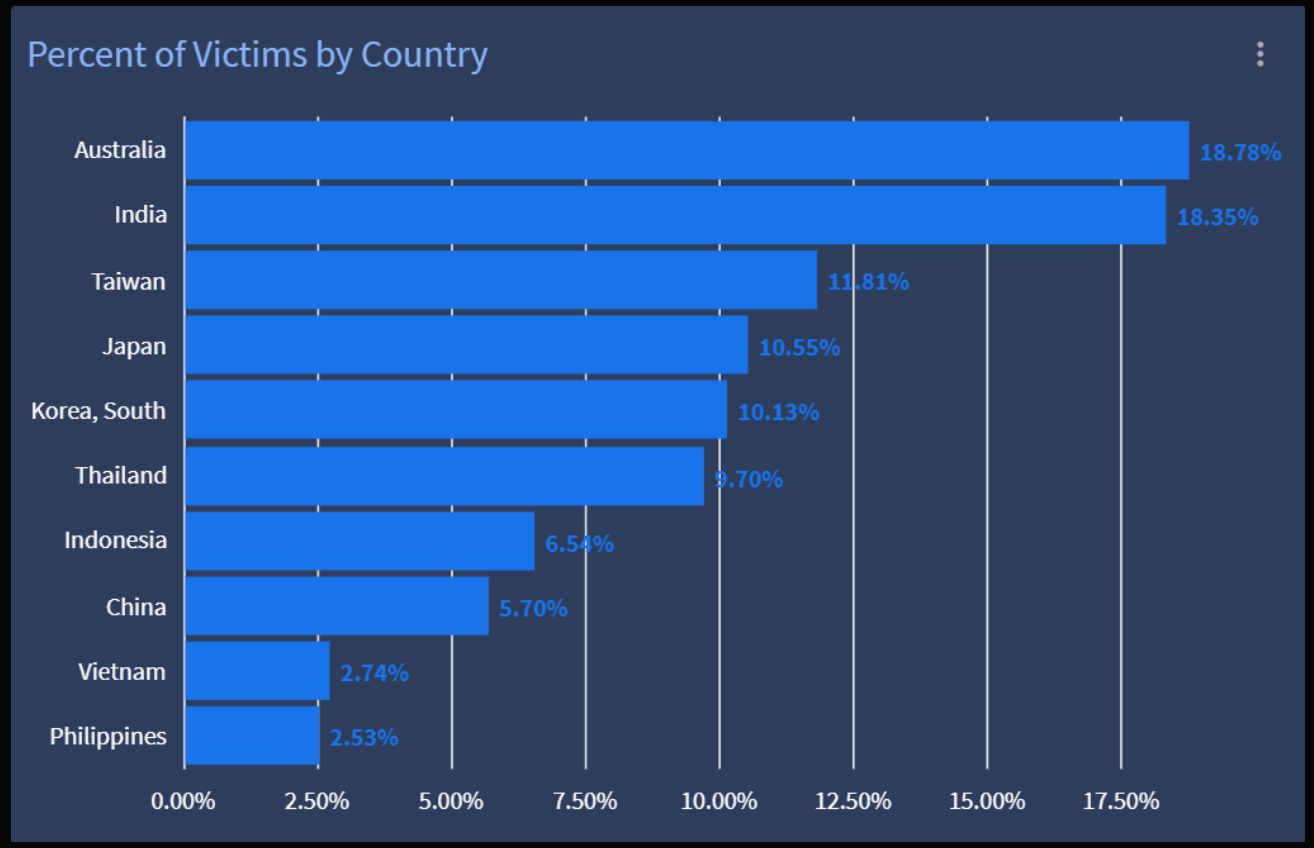
- The most common stealer variants impacting the region are Lumma and Atomic. Lumma was the most common malware strain targeting APAC overall, indicating a concentration of malware campaigns targeting credential theft. Although Lumma's infrastructure was disrupted in May, variants persist.
  - The Mimikatz credential dumping tool is a top malware capable of extracting plaintext passwords, hashes, and Kerberos tickets and enabling pass-the-hash/ticket attacks.
- The publicly available backdoors Beacon and Stowaway allow attackers to maintain access and control over a compromised system.
  - Stowaway has been used in Chinese state-sponsored campaigns targeting Southeast Asian governments, including an espionage campaign exploiting vulnerabilities in Ivanti Connect Secure VPN appliances.
- ShaddowLadder/IDAT/HijackLoader and SmokeLoader are modular loaders that deliver payloads and evade detection.
- Palebeam is a custom malware linked to Mysterious Elephant, a South Asia-linked advanced persistent threat group that primarily targets government and foreign affairs entities in Pakistan and other APAC countries. It is focused on stealing sensitive government and diplomatic data.
- Havoc Demon is an open-source RAT capable of taking full remote control, privilege escalation, credential dumping, and lateral movement. It has been used in advanced campaigns, including espionage and infrastructure targeting.



Source: Google Threat Intelligence

Ransomware by country

Companies in APAC listed on ransomware data leak sites (DLS's) (January 1-October 14, 2025)



Source: Google Threat Intelligence

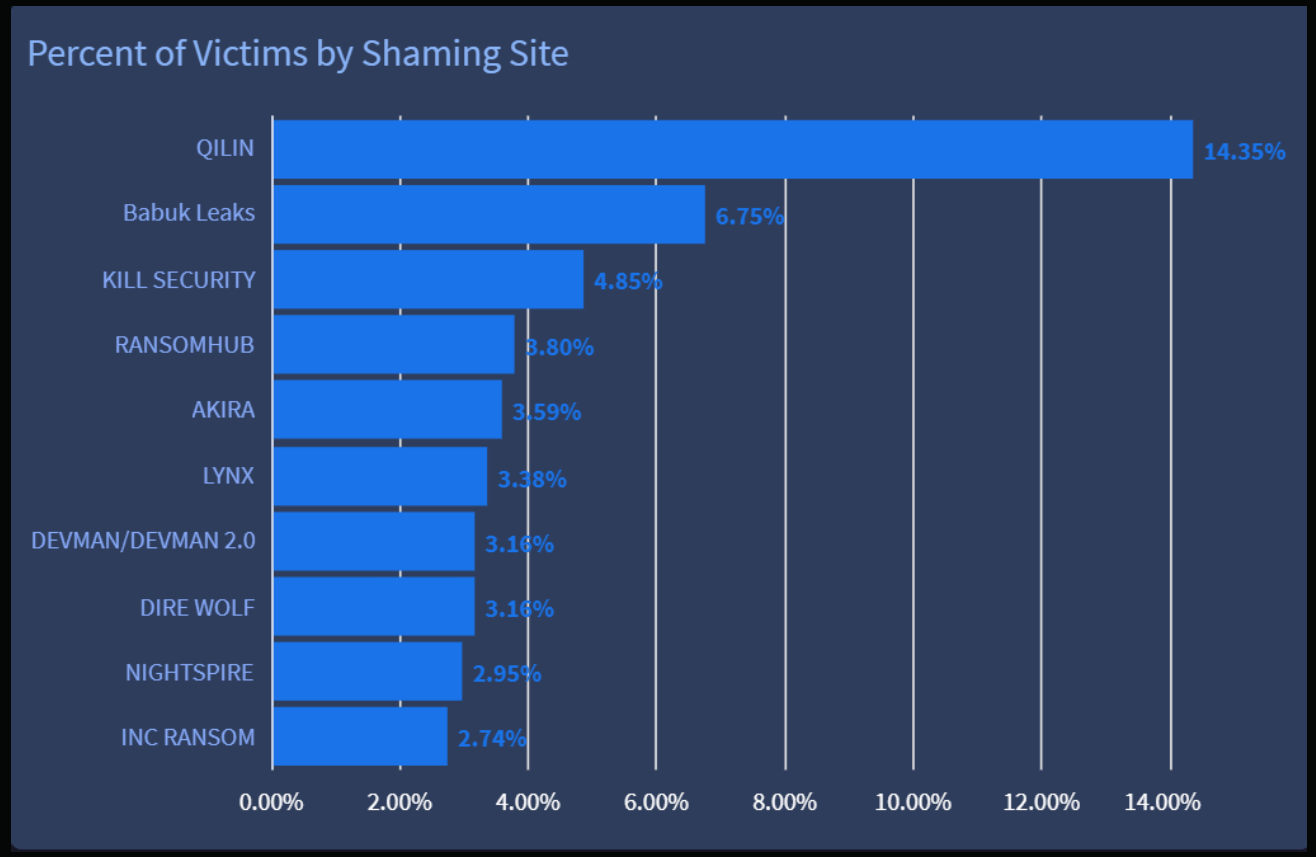
Ransomware poses one of the most pervasive threats to entities in APAC, targeting nearly all industries across both the private and public sectors. The top 5 victims regionally were Australia, India, Taiwan, Japan, and South Korea.

- **Australia** has faced a significant uptick of ransomware attacks in 2025, with some reports indicating a 110% rise year-over-year.[1] Australia was most targeted by Qilin (10%) and Akira (9%) ransomware groups. Legal & Professional Services (19%) was the top targeted industry in the country, followed by Healthcare (15%), Manufacturing (11%), Retail (9%), and Construction & Engineering (8%).
- **India** experienced a significant surge in ransomware in Q3 2025. India was most targeted by Kill Security (14%) and Babuk Leaks (9%). Attacks impacted critical sectors such as Manufacturing (17%), Technology (16%), and Financial Services (13%).
- **Taiwan** was predominantly targeted by CrazyHunter (18%) and Qilin (16%), and the country's significant Manufacturing industry (43%) was primarily affected.
- In **Japan**, Qilin (18%) was the most active, and primary victim industries included Manufacturing (42%) and Technology (14%).
- **South Korea** was overwhelmingly targeted by Qilin (69%), and victims from Financial Services (63%) were most listed on DLS's.

Of note, emerging ransomware groups have pivoted from popular hotspots to countries like Thailand, likely to evade detection and law enforcement action. For instance, the emergence of "Devman2" drove a 69% increase in Thailand-based DLS appearances from Q2 to Q3 2025. This new group has already listed over 25% of Thailand's organizations.[2]

Ransomware by hacker group

Companies in APAC listed on ransomware data leak sites (DLS's) (January 1-October 14, 2025)



Source: Google Threat Intelligence

Qilin listed the largest number of APAC entities (14%) on its DLS by a wide margin. The primary industries Qilin listed were Financial Services (49%) and Manufacturing (30%).

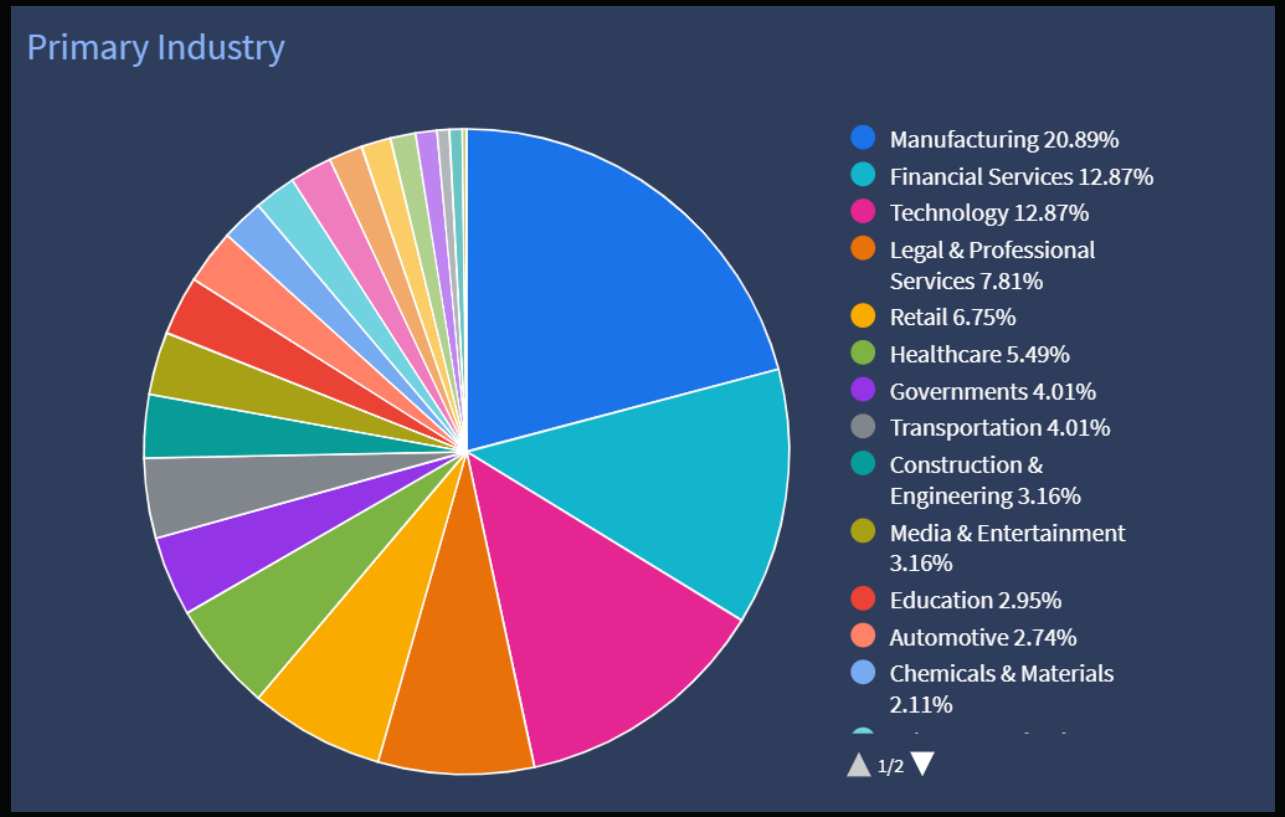
- A highly active and prominent group, Qilin operates as a structured Ransomware-as-a-Service (RaaS) model, offering a full-service cybercrime platform. Qilin targets large, high-value organizations globally with an emphasis on critical infrastructure entities.
- Their attacks have intensified, increasing the number of victims and adding a DDoS attack capability and legal support to increase pressure on victims. Qilin reached its highest number of listed organizations in a quarter in Q3 2025.[1]
- Qilin has increasingly shifted towards targeting Managed Service Providers (MSPs) through phishing campaigns and credential harvesting to gain access to multiple downstream victims.
- In October 2025, Qilin, LockBit, and DragonForce announced a formal alliance and invited other hackers to join their collaboration. It is currently unclear what impact this will have in the ransomware threat landscape.

Babuk Leaks, the second most common ransomware group targeting regional entities, primarily listed on its DLS regional victims from Government (38%), Technology (19%), and Financial Services (19%).

- Babuk's source code was leaked in 2021, complicating attribution because many variants emerged that used the source code. In January 2025, the Babuk Leaks DLS posted victims for the first time since July 2021, indicating possibly renewed activity.

Ransomware by industry

Companies in APAC listed on ransomware data leak sites (DLS's)
(January 1-October 14, 2025)



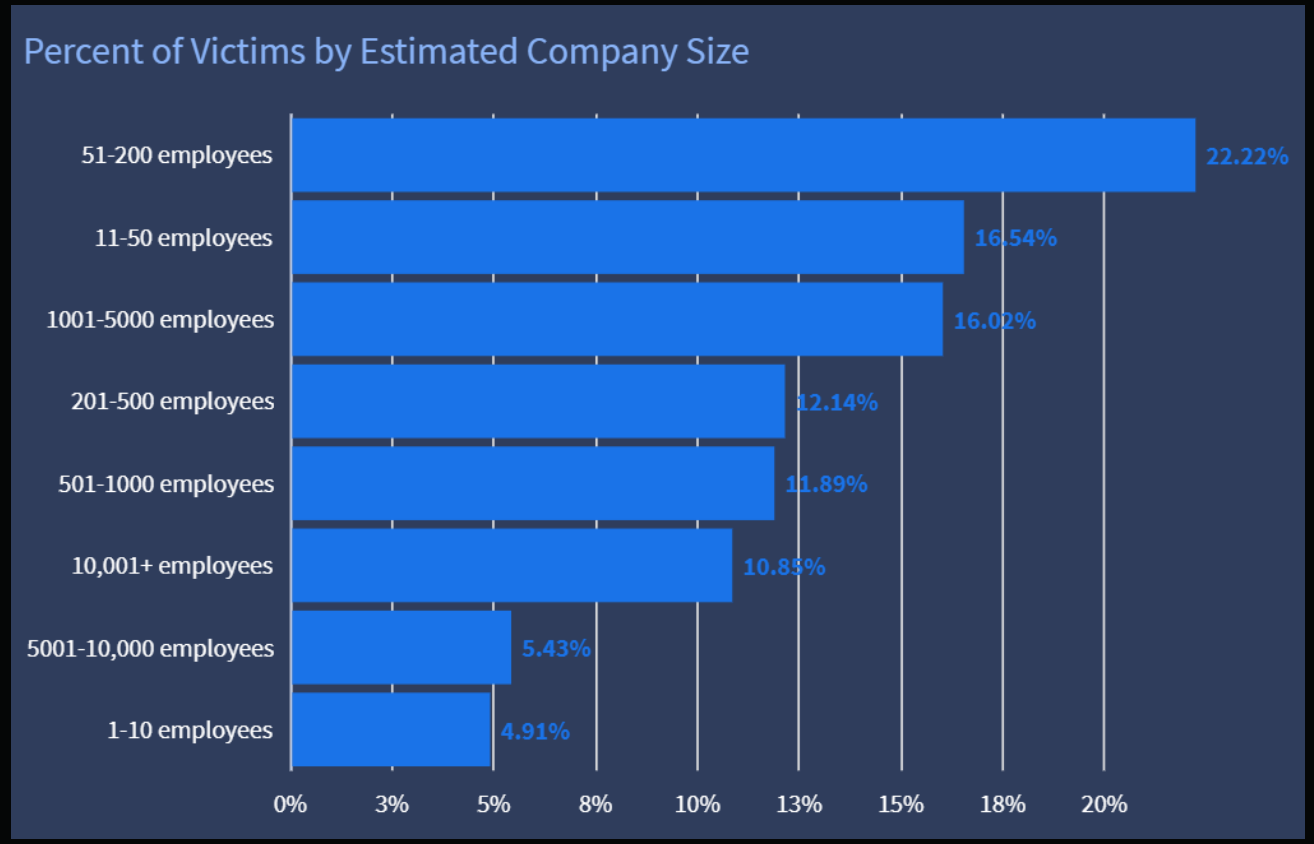
Source: Google Threat Intelligence

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

- **Manufacturing** was the most targeted industry in APAC (21%), with Qilin as the most common ransomware strain, and Taiwan seeing the greatest number of victims on its DLS.
- **Financial Services** (13%) – also prominent in Qilin (24%) victims posted on its DLS. Japan (21%) was the most targeted country in APAC for the Financial Services sector.
- **Technology** (13%) – Fog had the greatest number of regional Technology sector victims on its DLS. India's Technology sector was the most targeted in the region.

Ransomware by company size

Companies in APAC listed on ransomware data leak sites (DLS's) (January 1-October 14, 2025)



Source: Google Threat Intelligence

- APAC victims listed on ransomware data leak sites (DLSs) were primarily small and medium sized businesses (SMBs), indicating attackers' shift from larger to smaller enterprises.
- The two most targeted entities by company size were 51-200 employees (22%) and 11-50 employees (17%).
- SMBs are typically seen as low-hanging fruit due to their historically weaker security infrastructure and lower cybersecurity budgets, compared to larger entities.
- Midsize enterprises with between 1,001-5,000 employees were the third most targeted group by company size. These entities typically have valuable data and financial resources but have less robust defenses compared to larger enterprises.

How to avoid being a victim of infostealer malware

Infostealer malware is a widespread, growing threat. It is broadly used in indiscriminate campaigns, becoming stealthier and more dangerous. This can lead to identity theft, financial fraud, and other malicious attacks. Here are some steps you can take to protect yourself against infostealer malware.

TRAINING & AWARENESS

Organizations that provide cyber security awareness training for staff can prevent attacks by raising awareness of infostealers. Since infostealers are commonly distributed through phishing and malicious downloads, train employees to recognize social engineering and phishing attacks. Also consider email security tools that block suspicious emails or links.

ENABLE PHISHING-RESISTANT MFA

Implementing phishing-resistant multi-factor authentication (MFA) across all accounts. This prevents attackers from accessing accounts, even if they possess initial credentials. Use phishing-resistant MFA methods to counter advanced attacks like adversary-in-the-middle (AiTM) phishing that can try to steal session cookies to bypass MFA.

PASSWORD MANAGEMENT

Avoid reusing passwords to prevent a single breach from compromising multiple accounts. A password manager can help you stay safe by creating and storing different, strong passwords for every account, eliminating the need to remember them all.

PREVENT BROWSER SYNCHRONIZATION

This prevents passwords to your corporate systems are not accessible through personal devices. Avoid saving passwords in your browser and frequently clear your browser's cookies and cache to remove potentially stored data. Infostealers often target browser-stored data where they know sensitive information, including passwords, are often stored.

MONITOR FOR STOLEN CREDS

Proactively monitor the dark web for stolen corporate credentials. You can also check sites for potential exposure. This can alert you to a potential infection so you can take immediate action. Too often, we've observed attacks enabled by old credentials exposed on the dark web for years.

Want **more?**

🎧 **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.

Follow **The Phish Bowl**

YouTube **Spotify** **Apple**

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

Appendix – Sources

1. 2025 Data Breach Investigation Report (Verizon)
2. Shifts in the Underground: The Impact of Water Kurita's (Lumma Stealer) Doxxing. (Trend Micro)
3. Infostealers to Watch in 2025: Katz, Bee, Acreed, and More (Flashpoint)
4. The silent heist: cybercriminals use information stealer malware to compromise corporate networks (Australian Signals Directorate)
5. Cisco Firewall Zero-Days Exploited in China-Linked ArcaneDoor Attacks (Security Week)
6. OT-ISAC warns Singapore critical infrastructure of UNC3886 exploiting zero-days in Fortinet, VMware, Juniper systems (Industrial Cyber)
7. APAC SMB Cybersecurity Report 2024 (ESET)
8. "Shai-Hulud" Worm Compromises npm Ecosystem in Supply Chain Attack (Palo Alto Networks)
9. Self-Propagating GlassWorm Attacks VS Code Supply Chain (Dark Reading)
10. Artificial intelligence and machine learning: Supply chain risks and mitigations (Australian Signals Directorate)
11. Rogue communication devices found in Chinese solar power inverters (Reuters)