INTERPOL

ASPJOC

INTERPOL ASIA AND SOUTH PACIFIC CYBER THREAT ASSESSMENT

REPORT 2025/2026

LEGAL DISCLAIMER

TABLE OF CONTENTS

FOREWORD

The Asia and South Pacific region is home to some of the world's fastest-growing digital economies – and, increasingly, some of its most determined cybercriminals. Rapid connectivity has unlocked immense opportunity, but uneven cybersecurity maturity across the region continues to create openings that transnational actors are quick to exploit.

This 2025/2026 INTERPOL Asia and South Pacific Cyber Threat Assessment Report provides a crucial, evidence-based analysis of the multifaceted threats that define our current reality. From the alarming rise of artificial intelligence (AI)-enabled deepfake scams and industrial-scale fraud operations, to the persistent scourge of ransomware and the spread of infostealer malware, the challenges are formidable. We are witnessing a surge in cyber-enabled criminal operations across Southeast Asia. Transnational organized crime groups have stepped up their activities and established extensive scam centres that, in some cases, resemble modern-day slavery. These developments remind us that cybercrime results not only in economic losses, but also in a profound human toll. The findings within these pages – drawn from the invaluable contributions of our member countries and trusted private-sector partners – underscore a clear and urgent message: our adversaries are organized, innovative, and relentless.

Through INTERPOL's Global Cybercrime Programme and the dedicated efforts of ASPJOC, we are strengthening the bonds of international cooperation. In February 2025, Operation SECURE brought together 26 countries from this region to target infostealers and associated infrastructure in the region. The operation resulted in arrests, server seizures, the takedown of more than 20,000 malicious IPs and domains, and hundreds of thousands of victim notifications – tangible outcomes that demonstrate what coordinated action can achieve and that we intend to scale in the year ahead. The insights contained in this report are more than a summary of threats; they are a call to action. They demand a renewed commitment from all stakeholders – law enforcement, governments, and the private sector – to work in concert. We must continue to break down the silos that impede our progress, invest in the skills and technologies that will define the future of policing, and strengthen the legal frameworks that enable us to bring criminals to justice.

As my team is based at the INTERPOL Global Complex for Innovation (IGCI) in Singapore, we have a personal connection to this region. I extend my sincere gratitude to all the member countries and partners who contributed to this vital report. Your collaboration is the cornerstone of our collective defence. Together, we will continue to build a more resilient and secure digital future for the Asia and South Pacific region – and for the world.

Neal Jetton
Director, Cybercrime
Executive Directorate Investigation Support
INTERPOL

ABBREVIATIONS AND ACRONYMS

ASPJOC	Asia and South Pacific Joint Operations against Cybercrime
ASP Desk	Asia and South Pacific Desk
AI	Artificial Intelligence
AV	Anti-Virus
BEC	Business E-mail Compromise
CaaS	Crimeware-as-a-Service
C2	Command and Control
CAR	Cyber Activity Report
DDoS	Distributed Denial of Service
DNS	Domain Name System
DLP	Data Loss Prevention
EDR	Endpoint Detection and Response
FCDO	Foreign, Commonwealth & Development Office, United Kingdom
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
IOC	Indicator Of Compromise
JC3	Japan Cybercrime Control Centre
MaaS	Malware-as-a-Service
Microsoft's DCU	Microsoft's Digital Crimes Unit
MFA	Multi-Factor Authentication
OS	Operating System
PII	Personal Identifiable Information
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RaaS	Ransomware-as-a-Service
RAT	Remote Access Trojan
TLS	Transport Layer Security
UNODC	United Nations Office on Drugs and Crime
USB	Universal Serial Bus
SIEM	Security Information and Event Management
SMB	Server Message Block
SMS	Short Message Service
SSO	Single Sign-On
VPN	Virtual Private Network
XDR	eXtended Detection and Response

ACKNOWLEDGEMENT

This report has been prepared by the Asia and South Pacific Desk through the Asia and South Pacific Joint Operations against Cybercrime (ASPJOC), a project funded by the United Kingdom's Foreign, Commonwealth & Development Office (FCDO). For questions about the report, please contact Aspdesk@interpol.int.

This report represents the outcome of an in-depth analysis of information collected from diverse sources, including member countries in the Asia and South Pacific region, as well as INTERPOL's private-sector partners. In addition, intelligence and operational insights from INTERPOL have been utilized to inform and enhance the report, providing a comprehensive and nuanced perspective on the issues.

We sincerely thank the 18 member countries of the Asia and South Pacific region that responded to INTERPOL's cyber threat assessment survey. Their responses provided valuable insights that shaped this report. The questionnaire addressed a range of topics, including the scale and types of cybercrime observed, emerging threats, national response capacities, legislative and regulatory measures, and key challenges faced in their respective countries. The information shared through these responses was instrumental in developing a comprehensive understanding of the regional cyber threat landscape and informing the findings of this report. We also gratefully acknowledge the efforts of the law enforcement community in the Asia and South Pacific region who protect and serve their citizens every day.

INTERPOL

Foreign, Commonwealth & Development Office

EXECUTIVE SUMMARY

Cybercrime in the Asia and South Pacific region continues to escalate in scale, complexity, and impact, posing significant risks to national security, economic stability, and public trust in digital systems. The region's rapidly expanding digital economy, combined with significant disparities in cybersecurity maturity, has created an attractive and diverse environment for cybercriminal activity.[1]

Threat actors, ranging from lone offenders to sophisticated and organized crime groups, exploit vulnerabilities through ransomware attacks, financial fraud, business e-mail compromise (BEC), data breaches, and widespread infostealer malware campaigns. Strong connectivity enables operations even in remote locations, while limited cybersecurity resilience in the lesser developed parts of the Asia and South Pacific region provides threat actors with accessible entry points into broader regional and global networks.

Recent operations and intelligence-sharing initiatives led by INTERPOL's Asia and South Pacific Cybercrime Desk (ASP Desk) highlight a marked rise in credential harvesting and infostealer malware distribution. These campaigns frequently act as preludes to more destructive attacks such as fraud, espionage, and account takeovers.

Cybercriminals are also increasingly adopting cutting-edge strategies and advanced technologies, including deepfakes, ransomware-as-a-service (RaaS) models, cryptocurrency-based money laundering, AI-enabled attacks, and dark web marketplaces for illegal goods and stolen data.

In response, law enforcement organizations across the region – supported by INTERPOL – are scaling up joint efforts to combat cybercrime. These include the coordination of operations against cybercriminal infrastructure, collaborative investigations, specialized training initiatives, and the creation of policies to improve cyber resilience. Strong partnerships with the private sector remain essential to detecting emerging threats and disrupting illegal activities.

Moving forward, the INTERPOL ASPJOC team will intensify strategic efforts to strengthen cross-border collaboration, coordinate impactful operations, and systematically identify threat actors and dismantle the malicious infrastructures they rely on across the region.

1. ADMM Cybersecurity and Information Centre of Excellence, The Cyber Domain (Cybersecurity Centre Report, 1 September 2024), https://www.acice-asean.org/files/cybersecurity%20centre%20reports/sep_24_cyber.pdf (accessed 28 August 2025).

1. INTRODUCTION

The Asia and South Pacific region is home to some of the world's most technologically advanced economies.[2] Overall, the region's digital sector has grown at an unprecedented pace, propelled by rising Internet penetration, mobile connectivity, and increasing reliance on digital financial and communication systems. This rapid expansion – combined with the widespread adoption of cloud computing, AI, mobile banking, and remote work – has not only accelerated digital transformation, but also made the region an attractive target for cybercriminals.[3] In addition, the speed of this transformation has exposed many organizations to critical security gaps, including limited cloud security safeguards, inadequate incident response readiness, and insufficient cross-border information sharing, creating opportunities for a cybercriminal ecosystem that is becoming increasingly complex and globally interconnected.[4]

At the same time, criminal organizations are exploiting the region's uneven cybersecurity landscape. While the most developed digital economies have comparatively robust cybersecurity frameworks and are better equipped to handle cyberattacks, others – including many small island states and developing countries in the Pacific – face severe obstacles in terms of institutional preparedness, technical know how, and resources. These disparities make them highly vulnerable, both to direct targeting and to being used as gateways for further malicious activity. Jurisdictions with less robust legislation, fragmented enforcement, and limited technical capacity are particularly attractive to threat actors, who often operate with a low likelihood of being identified or prosecuted. In recognition of these escalating threats, the INTERPOL Asia and South Pacific Cybercrime Desk (ASP Desk) has stepped up efforts to coordinate regional responses and foster collective resilience.

The ASP Desk supports intelligence driven investigations, operational collaboration, and capacity-building initiatives targeted at enhancing cybersecurity throughout the region by collaborating with national law enforcement agencies, foreign partners, and private sector stakeholders.

This report assesses cybercrime threats and trends in the Asia and South Pacific region from January 2024 to March 2025. For the purposes of this report, "cybercrime" refers to both cyber-dependent crimes (such as ransomware, phishing, distributed denial-of-service attacks, and distribution of infostealer malware) and cyber-enabled crimes (such as online scams and identity theft). Drawing on a questionnaire sent to law enforcement from the region, as well as on insights from the private sector partners, case studies from recent operations, and in-depth analysis of emerging threats, the report highlights critical vulnerabilities, cross-border issues, and the growing use of cutting-edge technologies like AI, ransomware as-a-service (RaaS), and cryptocurrency laundering.

By offering practical findings and strategic recommendations, our objective is to guide operational priorities, promote greater international cooperation, and inform regional policy development. As cyber threats continue to grow in sophistication and scale, building a coordinated and proactive response is crucial to preserving the digital security and economic prosperity of the Asia and South Pacific region.

2. INTERPOL, ASPJOC – INTERPOL Asia and South Pacific Joint Operations on Cybercrime (INTERPOL, 1 June 2024 – 31 March 2025), https://www.interpol.int/en/Crimes/Cybercrime/Projects/ASPJOC-INTERPOL-Asia-and-South-Pacific-Joint-Operations-on-Cybercrime (accessed 28 August 2025).

3. Gullapalli, "Why is the Asia Pacific region a target for cybercrime – and what can be done about it?" (World Economic Forum, 12 June 2023), https://www.weforum.org/stories/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/ (accessed 28 August 2025).

4. Telecom Review Asia, "Asia's Digital Revolution: Driving Connectivity, Commerce and Innovation" (featured article, 31 August 2023), https://www.telecomreviewasia.com/news/featured-articles/3574-asia-s-digital-revolution-driving-connectivity-commerce-and-innovation (accessed 28 August 2025).

2. KEY CYBERCRIME TRENDS AND FIGURES IN THE ASIA AND SOUTH PACIFIC REGION

Cyber threats increased significantly in the Asia and South Pacific region in the past few years due to the swift adoption of digital technologies, disparities in cybersecurity maturity, and the growing sophistication of cybercriminals' strategies and methods.

- **Industrialization of cyber-enabled scam operations**
  In countries like Cambodia, Lao PDR, Myanmar, and the Philippines, transnational organized crime groups have stepped up their operations and established extensive scam centres. According to estimates, these operations, which frequently involve forced labour, have generated close to USD 40 billion a year, using strategies like romance baiting, phony investment schemes, and illegal online gambling.[5]

- **Escalation of ransomware attacks**
  The Asia and South Pacific region recorded more than 135,000 ransomware-related attacks in 2024, affecting sectors such as real estate, manufacturing, and financial services. Notably, a ransomware attack on Indonesia's National Data Centre disrupted over 280 essential services, including immigration and airport operations.[6]

- **Persistence of phishing and social engineering**
  Phishing remains a prevalent threat, with 5.5 out of every 1,000 individuals in the Asia and South Pacific region clicking on phishing links monthly. Cloud applications were the primary targets, accounting for 28 per cent of phishing clicks.[7]

- **Rapid growth of deepfake and AI-driven cybercrime**
  From February to June 2024, discussions about deepfakes on cybercriminal forums and Telegram channels popular among Southeast Asian threat actors increased by 600 per cent. These technologies have been used to perpetrate convincing scams, including several high-profile incidents involving the impersonation of business executives to authorize fraudulent transactions.[8]

- **Sharp increase in distributed denial-of-service (DDoS) attacks**
  DDoS attacks in the Asia and South Pacific region surged by 92 per cent in 2024 compared to the previous year. Government websites were the primary targets in the first half of the year due to major elections across the Asia and South Pacific region, while financial institutions faced increased attacks in the latter half.[9]

- **High prevalence of data breaches**
  In the Asia and South Pacific region, system intrusions accounted for approximately 80 per cent of all data breaches in 2024, with malware and ransomware present in 83 per cent and 51 per cent of cases respectively.[10]

---

5. Staff Reporter, Indonesia's National Data Centre Ransomware Attack: A Digital Governance Failure? (Fulcrum by the ISEAS – Yusof Ishak Institute, 8 August 2024), https://fulcrum.sg/indonesias-national-data-centre-ransomware-attack-a-digital-governance-failure/ (accessed 4 January 2026).

6. Staff Reporter, Over 135,000 ransomware attacks detected in Southeast Asia in 2024 (Singapore Business Review, 4 April 2025), https://sbr.com.sg/information-technology/news/over-135000-ransomware-attacks-detected-in-southeast-asia-in-2024 (accessed 28 August 2025).

7. Staff Reporter, Asia-Based Employees Click on Phishing Links at Twice the Global Rate: Netskope Report (AsiaBizToday, 12 December 2024), https://www.asiabiztoday.com/2024/12/12/asia-based-employees-click-on-phishing-links-at-twice-the-global-rate-netskope-report (accessed 28 August 2025).

8. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia (UNODC, 2024), https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf (accessed 28 August 2025).

9 StormWall, DDoS Trends and Statistics in APAC – 2024 Report (StormWall, 6 February 2025, https://stormwall.network/resources/blog/ddos-trends-apac-2024) (accessed 28 August 2025).

10 Verizon Business, 2025 Data Breach Investigations Report: System Intrusions Cause 80% of Asia-Pacific Data Breaches (Verizon, 23 April 2025, https://www.verizon.com/about/news/2025-data-breach-investigations-report-apac) (accessed 27 October 2025).

Focus on the distribution of detected malware types in the Asia and South Pacific region:[11]

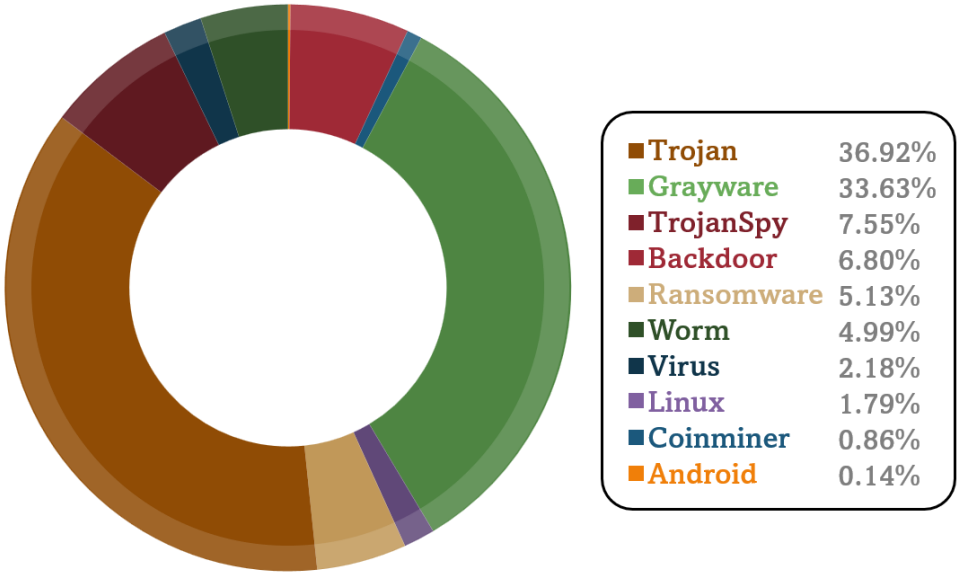


Figure 1: Distribution of malware types detected within the Asia and South Pacific region in 2024

Descriptions:

- **Trojan**: Malware that can cause unwanted system issues, data loss, and other malicious actions. Trojans are often downloaded from the Internet and installed by unsuspecting users.
- **Grayware:** Grayware is unwanted software that causes pop-ups or slow performance, or collects data without consent. It disrupts privacy and may expose systems to security risks.
- **TrojanSpy:** Secretly monitors users, capturing sensitive data like passwords and financial information through keystroke logging, screenshots, or recordings, and sends it to attackers.
- **Backdoor:** Backdoors are programs that let attackers remotely access and control computers, enabling stealthy credential theft and persistent connections.
- **Ransomware:** A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.
- **Worm:** A self-contained program (or set of programs) that can spread functional copies of itself or its segments to other computer systems. The propagation usually takes place via network connections or e-mail attachments.
- **Virus:** A computer program that can copy itself and infect a computer without a user's permission or knowledge.
- **Linux:** Malicious programs targeting Linux systems to steal data, disrupt operations, or gain control are increasingly being used, especially against servers and IoT devices.
- **Coinminer:** Cryptocurrency-mining malware targeting cryptocurrency wallets and crypto-related data.
- **Android:** Malware infecting Android devices to steal data, spy, or take control. It commonly spreads via malicious apps, phishing, or harmful links.

11 Trend Micro data provided to the Cyber Fusion Centre, 2024.

3. OVERVIEW OF CYBER THREATS ACROSS THE ASIA AND SOUTH PACIFIC REGION

The Asia and South Pacific region is experiencing a surge in cyber threats, driven by rapid digitalisation, intensifying geopolitical tensions, and the proliferation of advanced technologies. This section outlines the key cyber threats shaping the regional landscape through 2024 and into 2025.

3.1 The state of Cybercrime in Asia and the South Pacific

Countries across the Asia and South Pacific region face rising waves of cybercrime, each carrying significant economic consequences. To better understand these challenges, the ASP Desk conducted a member country survey, receiving responses from 18 countries. The findings provide important insights into how cybercrime is evolving in the region.

In the survey, more than half of INTERPOL member countries in the region reported that cybercrime accounted for more than 30 per cent of all crimes recorded nationally.[12] This indicates not only the growing prevalence of cybercrime offences, but also their increasing dominance compared to traditional crime types. Cyber threats are no longer isolated incidents – they have become persistent, large-scale challenges affecting multiple jurisdictions. This high incidence of cybercrime is closely linked to the region's rapid adoption of digital infrastructure. While digitalization has accelerated economic growth, connectivity, and financial inclusion, it has also exposed individuals, businesses, and governments to heightened risks.

The Asia and South Pacific region is impacted by a range of cyber threats, but online scams have emerged as the most widespread and financially damaging form of cybercrime. In fact, 33 per cent of INTERPOL's member countries surveyed reported over 10,000 cases of online scams. These operations rely heavily on phishing and social engineering tactics that exploit vulnerabilities across digital platforms, impacting a broad spectrum of victims including individuals, enterprises, and governmental bodies.

The economic impact of these threats is increasingly severe. Half of the surveyed countries reported financial losses exceeding USD 10,000, with several indicating losses of over USD 100 million. These findings underscore the fact that financial losses from cybercrime are systemic across the region and not limited to isolated, high-profile incidents. Notably, the sustained scale of scam operations contributes to deep and continuing economic harm.

Meanwhile, law enforcement agencies across the region face persistent operational challenges. Respondents to the ASP Desk's survey highlighted gaps in specialized forensic tools, limited access to targeted cybercrime training, and insufficient technical capacity as critical obstacles.

Overall, the findings from the survey reflect an urgent need for strengthened cross-border collaboration, improved intelligence sharing, and comprehensive capacity-building initiatives. To address some of these challenges, the ASP Desk will continue to actively facilitate webinars and expert-led events aimed at enhancing technical skills and bridging capability shortfalls. At the national level, sustained public awareness campaigns remain essential to reducing victimization rates, while agile prevention, detection, and response strategies are critical for adapting to an increasingly complex cybercrime ecosystem. Strengthening these measures is vital for safeguarding economic stability, maintaining public trust, and protecting the region's digital environment.

12 INTERPOL, Cyber Threat Assessment Survey, data provided by member countries, 2025.

3.1.1. Top five cybercrime types impacting the Asia and South Pacific region

The 18 member countries who participated in the ASP Desk's survey provided insights into the most prevalent and concerning categories of cybercrime observed within their jurisdictions. They were asked to rank the five most significant types of cybercrime based on the volume of reported cases. The findings offer a valuable overview of the current cyber threat landscape and highlight areas where law enforcement and partner organizations should focus their prevention and response efforts.

1. **Online scams and phishing**
   Online scams, including phishing-related offences, were identified as the most critical regional cyber threat with the highest volume of reported cases. These attacks continue to be highly effective due to their reliance on social engineering techniques, exploiting human trust rather than technical vulnerabilities. Recent trends indicate that phishing campaigns have evolved significantly, moving beyond generic mass e-mails to targeted spear-phishing, SMS-based phishing ("smishing"), and AI-generated messages that closely imitate legitimate communications. The prominence of phishing underscores that human behaviour remains the most exploited vulnerability in cybersecurity.

2. **Banking trojans and information-stealer malware**
   Banking trojans and information-stealing malware were ranked as the second most significant cybercrime. Malware families such as RedLine, LummaC2, and other variants are designed to exfiltrate sensitive financial data, login credentials, and personally identifiable information. The impact of these malware operations often extends beyond individual victims, contributing to large-scale financial fraud, account takeovers, and secondary ransomware distribution. This reflects the enduring prevalence and economic impact of credential-harvesting campaigns, particularly in regions with widespread adoption of online financial services.

3. **Ransomware**
   Ransomware continues to represent a significant regional threat, ranking third among all cybercrime cases in terms of volume. Attacks have grown increasingly sophisticated, often employing double extortion tactics, in which attackers both encrypt and threaten to leak sensitive data. The targeting of critical infrastructure, healthcare systems, and large enterprises has amplified the perceived severity of ransomware incidents, due to their potential to disrupt essential services and cause significant financial losses.

4. **Misinformation, manipulation, and deepfake-related crimes**
   Emerging threats involving misinformation and manipulation, including AI-generated "deepfakes", were cited as the fourth most pressing concern. Advances in AI now enable the creation of highly realistic synthetic media, which can be used to impersonate individuals, manipulate public discourse, or circumvent identity verification measures. This emerging threat shows how cybercrime is evolving rapidly, requiring law enforcement to address its psychological dimensions.

5. **Business e-mail compromise (BEC)**
   Survey respondents ranked business e-mail compromise (BEC) as the fifth highest cyber threat in terms of volume of cases. BEC schemes typically involve the impersonation of executives or trusted business partners to deceive employees into authorizing fraudulent transactions or disclosing sensitive information. Despite increased awareness and preventative measures, BEC remains a highly effective form of cyber-enabled fraud – with several high-profile incidents involving the use of AI – often leading to substantial financial losses across both public and private sectors. As cybercriminals exploit AI to enhance their operations, proactive threat detection and international cooperation will remain essential to strengthening global cyber resilience.

3.1.2. Top cyber threats originating from the Asia and South Pacific region

The Asia and South Pacific region also remains a significant source of web-based malicious activity. Cybercriminals based in, or using infrastructure hosted in, the region exploit rapid digital growth, high Internet penetration, and expanding online economies to launch or facilitate cybercrime operations. From fraudulent schemes and social engineering to malicious infrastructure and harmful content distribution, these threats target both individuals and organizations, aiming to steal data, extort funds, and/or disrupt operations. Increasingly, threat actors are leveraging automation, AI, and cross-border infrastructure to scale their operations and evade detection. Figure 2 illustrates the distribution of various cybercrime categories in the Asia and South Pacific region, highlighting scams and phishing as the most prevalent threats.

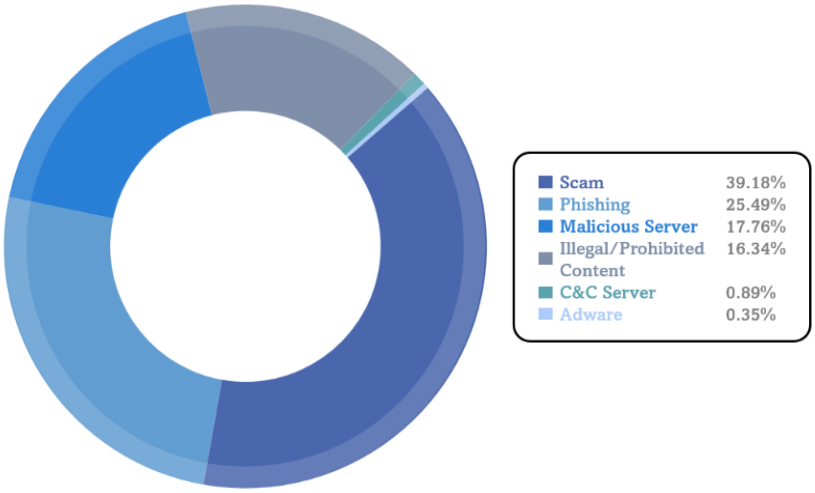


Figure 2: Distribution of cybercrime categories across the Asia and South Pacific region[13]
(Data source: Trend Micro data provided to the Cyber Fusion Centre)

Taken together, these threats highlight the critical need for stronger cybersecurity measures, public awareness, and coordinated regional defence efforts.[14]

13 Trend Micro data provided to the Cyber Fusion Centre, 2024.

14 Moises Benedict Carandang and Roxanne Jacutan, Southeast Asia is tackling cyberattacks on the underbanked, World Economic Forum, 15 October 2024, https://www.weforum.org/stories/2024/10/southeast-asia-tackling-cyberattacks-underbanked (accessed 28 August 2025).

Trends in malware: infostealer families across the Asia and South Pacific region

Data harvested by infostealers throughout Asia and the South Pacific are routinely converted into a valuable commodity traded on illicit marketplaces and dark web forums. Cybercriminals use these hidden communities to buy, sell and exchange stolen data, crimeware tools, and services. Markets typically advertise and trade stolen banking credentials and personally identifiable information (PII) – including names, addresses, and social security numbers, as well as corporate secrets.[15]

The data traded on these forums fuel a wide range of downstream crimes. Stolen credentials and PII enable identity theft, account takeover, large-scale financial fraud, and follow-on attacks such as ransomware or targeted intrusions. The anonymity afforded by the dark web and related forums amplifies the impact of successful malware campaigns and helps sustain a resilient, commercially organized cybercrime ecosystem.

The active sharing and sale of stolen data in these underground communities underscores the critical need for organizations in the Asia and South Pacific region to have strong security protocols and proactive threat intelligence. Early detection, rapid information sharing, and stronger public awareness all reduce the value of stolen data and limit opportunities for abuse.[16]

Following the conclusion of Operation Secure this year, the ASPJOC team identified the five most prevalent infostealer families in the Asia and South Pacific region. Table 1 summarizes these families and key details identified during the operation.

	About	Targeted countries	Monikers	Key Asia and South Pacific activities	Industries targeted
RedLine Stealer	RedLine is a frequently seen infostealer malware that targets login credentials, browser data, cryptocurrency wallets, and system information. Sold on cybercrime forums since 2020, it is popular due to its low cost and ease of use. RedLine spreads through phishing e-mails, malicious ads, and cracked software, making it a major threat to individuals and organizations alike.[17]	Cambodia, Fiji, Viet Nam, Kiribati, Laos, Nepal, Philippines, and Timor-Leste.	Redline, Redline infostealer, Trojan. Redline, Stealer. Redline, RedStealer	RedLine is the most popular infostealer in the Asia and South Pacific region due to its ability to effectively harvest sensitive data.[18] As a result, RedLine has become a leading cause of data breaches and financial theft in the area.	Healthcare, finance, education, logistics, retail, and e-commerce.

15 Flashpoint, Cybercriminals Exploiting Opportunities in Asia-Pacific Region, Flashpoint, 21 December 2018, (accessed 28 August 2025).

16 Poppy McPherson and Tom Wilson, Criminal networks in Southeast Asia flourish in Telegram's 'underground markets', UN says, Reuters, 7 October 2024, https://www.reuters.com/world/asia-pacific/criminal-networks-southeast-asia-flourish-telegrams-underground-markets-un-says-2024-10-07 (accessed 28 August 2025).

17 AntivirusAZ, RedLine Stealer Malware, AntivirusAZ, 2025, https://www.antivirusaz.com/security-center/virus-information/redline-stealer (accessed 28 August 2025).

18 INTERPOL ASPJOC Operation Secure data, 2024.

	About	Targeted countries	Monikers	Key Asia and South Pacific activities	Industries targeted
LummaC2	LummaC2, regarded as the world's largest infostealer, is a malware-as-a-service (MaaS) infostealer that has been available since August 2022 on forums. It primarily targets crypto wallets and 2FA browser extensions, then steals other sensitive data. Known for advanced evasion, it is spread via phishing and deceptive downloads.[19]	Indonesia, Philippines, Viet Nam, Thailand, China, Papua New Guinea, Malaysia, and Singapore.	Lumma Stealer, LummaC	LummaC2 Stealer malware disguises itself as legitimate apps (e.g. Notion, Capcut) and uses platforms like Steam to hide its command-and-control servers. Recently, Europol, in collaboration with Microsoft's Digital Crimes Unit (DCU) and Japan's Cybercrime Control Centre (JC3), coordinated an operation to dismantle the Lumma infostealer infrastructure.[20]	Healthcare, finance, telecommunications, gaming, and e-commerce.
LOKIBOT **Loki**	Lokibot is a trojan infostealer targeting Android and Windows devices. It spreads via phishing e-mails, malicious websites, and messaging apps, often using .iso file attachments to bypass security filters. Once installed, it steals credentials from browsers, e-mail clients, FTP software, messaging apps, and crypto wallets, and includes keylogging capabilities.[21]	Indonesia, Philippines, Viet Nam, Thailand, Malaysia, and Australia.	Lokibot, Loki PWS, Loki-bot	From 2024 to 2025, Lokibot contributed to a surge in credential theft, which was responsible for global cyberattacks that targeted this region. The manufacturing sector and finance/insurance were the most affected.[22]	Healthcare, finance, manufacturing and logistics, retail, and e-commerce.

19 Cybersecurity and Infrastructure Security Agency (CISA), Threat Actors Deploy LummaC2 Malware to Exfiltrate Sensitive Data from Organizations, CISA, 21 May 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141b (accessed 28 August 2025).

20 Europol, Europol and Microsoft disrupt world's largest infostealer Lumma, Europol, 21 May 2025 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world%E2%80%99s-largest-infostealer-lumma (accessed 28 August 2025).

21 Check Point Software Technologies, Lokibot Malware, Check Point Software Technologies https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/lokibot-malware (accessed 28 August 2025).

22 Cybersecurity Ventures, Asia Pacific Threat Landscape 2025, Cybersecurity Ventures, 2025, https://cybersecurityventures.com/report/asia-pacific-threat-landscape-2025 (accessed 28 August 2025).

	About	Targeted countries	Monikers	Key Asia and South Pacific activities	Industries targeted
 **Negasteal**	Negasteal is a .NET-based information stealer and remote access trojan (RAT) with keylogging capabilities. Discovered in 2014, it has been used in various malicious campaigns, exfiltrating data via web panels, FTP, or SMTP.[23]	India, Indonesia, Viet Nam, Philippines, Malaysia, Thailand, Singapore, and Australia.	Agent Tesla, AgenTesla, Agentsla, Tsla, Tesla	In April 2025, there was a surge in activity across countries in the Asia and South Pacific region, where Negasteal was distributed via phishing e-mails aimed at multiple sectors.[24]	Energy, manufacturing, logistics, and healthcare.
 **ZBot**	The ZBot infostealer was first identified in 2006 and quickly became notorious for targeting online banking credentials. Following the public leak of its source code, numerous variants emerged, including more sophisticated versions that enhanced its capabilities and evasion techniques.[25]	India, Japan, Thailand, Indonesia, Singapore, and Australia	ZeuS, ZeuS3, GoZeus, GameOver Zeus	The malware has been used in large-scale fraud operations, especially in countries with rapidly growing digital banking sectors across the region	Financial, healthcare, education, and e-commerce.

Table 1: Top five Infostealers in the Asia and South Pacific region
(Data source: Data collected from the ASPJOC Operation Secure)

23 Trend Micro, Negasteal Malware, Trend Micro, 16 July 2020, https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/negasteal (accessed 28 August 2025).

24 Infoblox, Agent Tesla Malspam Campaign Spoofs Bank Correspondence, Infoblox, 13 April 2021, https://blogs.infoblox.com/threat-intelligence/cyber-campaign-briefs/agent-tesla-malspam-campaign-spoofs-bank-correspondence (accessed 28 August 2025).

25 Eviden, Infostealer – Trends and How to Detect Them Before It's Too Late, Eviden, 17 July 2023, https://eviden.com/publications/digital-security-magazine/detect-early-respond-swiftly/infostealer-trends-and-how-to-detect-them-before-its-too-late/ (accessed 27 October 2025).

3.2 AI as an emerging driver of the cyber threat landscape

AI has rapidly become a defining feature of the cyber threat landscape in the Asia and South Pacific region. While governments and organizations increasingly rely on AI to strengthen detection and response capabilities, cybercriminals are equally exploiting AI to scale, automate, and enhance the effectiveness of their operations.

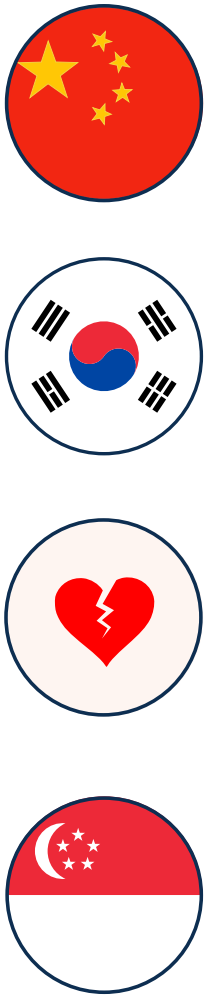
Cybercrime groups in Southeast Asia are using emerging technologies to conduct cyber-enabled "romance baiting" scams, which are estimated to have generated up to USD 37 billion in losses.[26] Criminals are also leveraging AI to craft more convincing phishing messages, create fake identities, and generate realistic deepfake content – all designed to evade security measures and better manipulate victims.

Member countries in the Asia and South Pacific region have reported a rapidly growing and diverse range of incidents involving AI-driven cyber-enabled crimes and the misuse of deepfake technology. These include the use of deepfake videos to impersonate public figures, celebrities, or business executives in fraudulent investment campaigns, deceiving the public into transferring money or disclosing sensitive information. Such schemes have resulted in significant financial losses and have targeted both individuals and institutions.

Beyond financial fraud, deepfake technology has also been misused for sexual exploitation, with manipulated videos and images being used to harass, blackmail, or coerce victims. In parallel, AI-assisted content generation has facilitated the spread of disinformation and defamatory material across social media platforms, impacting public trust, inciting social tensions, and even defaming political leaders or public officials in several jurisdictions. Generative AI has further been employed to create malware capable of overwriting or destroying digital files, adding new layers of automation and sophistication to cyberattacks.

26 UNODC, Billion-dollar cyberfraud industry expands in Southeast Asia as transnational organized crime groups evolve (UNODC, 7 October 2024), https://www.unodc.org/roseap/en/2024/10/cyberfraud-industry-expands-southeast-asia/story.html (accessed 28 August 2025).

MAJOR AI-DRIVEN INCIDENTS 2024-2025



February 2024

An employee at a multinational firm in Hong Kong, China was tricked into transferring USD 25 million after deepfake technology was used to impersonate executives in a video call.

August 2024

Authorities in South Korea investigated a surge in pornographic deepfakes targeting female students and teachers on Telegram, prompting new laws after over 800 cases were reported.

October 2024

Organized crime in Myanmar, Cambodia, and Laos used deepfakes in "romance baiting" scams, blending AI personas and social engineering to fuel USD 37 billion in regional cybercrime losses.[27]

March 2025

A finance director of a multinational corporation in Singapore nearly lost over USD 499,000 after participating in a Zoom call with deepfake impersonations of senior executives including the CEO and CFO.[28]

Figure 3: Timeline of AI-enabled cybercrimes in the Asia and South Pacific region (2024-2025)

27 UNODC, "Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia" (UNODC, October 2024), https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf (accessed 9 October 2025).

28 Straits Times, "Finance director nearly loses $670k to scammers using deepfakes to pose as company senior execs" (Straits Times, 7 April 2025), https://www.straitstimes.com/singapore/finance-director-nearly-loses-670k-to-scammers-using-deepfakes-to-pose-as-company-senior-execs (accessed 9 October 2025).

AI-powered cyberattacks across the Asia and South Pacific region

Between January and December 2024, over 6.5 billion cyber threats were detected and mitigated in the Asia and South Pacific region,[29] highlighting the aggressive and evolving nature of cyberattacks. While e-mail remained the most exploited attack vector, cybercriminals increasingly used AI to amplify the effectiveness of phishing and social engineering tactics. Threat actors leveraged AI-generated deepfakes to replicate legitimate communications with a high degree of realism, substantially enhancing the likelihood that victims would engage with malicious content. By analysing a victim's communication style and publicly available information, AI models can automatically craft persuasive phishing e-mails, texts, and even voice clones.[30]

AI has also been used to enhance file-based threats, enabling cybercriminals to create sophisticated and polymorphic malware concealed within seemingly harmless documents.[31] These threats are specifically engineered to bypass conventional security tools, posing significant challenges for endpoint protection systems.

In parallel, AI has accelerated the evolution of web-based attacks by automating the generation of malicious sites, creating spoofed login portals, and deploying adaptive exploit kits tailored to individual users and environments.[32] This intelligent automation amplifies the effectiveness of drive-by downloads, watering hole compromises, and credential theft operations.

Collectively, these advancements highlight the urgent need for equally sophisticated AI-driven cybersecurity measures,[33] alongside comprehensive user education, to counter increasingly adaptive and intelligent threat landscapes. Figure 4 below shows the percentage distribution of blocked cyber threats, with e-mail accounting for the majority, followed by file-based and web-based threats.

29 Trend Micro data provided to the Cyber Fusion Centre, 2024.

30 Palo Alto Networks, What Are Predictions of Artificial Intelligence (AI) in Cybersecurity?, Cyberpedia, https://www.paloaltonetworks.com.au/cyberpedia/predictions-of-artificial-intelligence-ai-in-cybersecurity (accessed 28 October 2025).

31 Liora Itkin, Polymorphic AI Malware: A Real-World POC and Detection Walkthrough, CardinalOps, 20 May 2025, https://cardinalops.com/blog/polymorphic-ai-malware-detection/ (accessed 28 August 2025).

32 Benedict Collins, Hackers are now mimicking government websites using AI – everything you need to know to stay safe, TechRadar, 11 August 2025, https://www.techradar.com/pro/security/hackers-are-now-mimicking-government-websites-using-ai-everything-you-need-to-know-to-stay-safe (accessed 28 August 2025).

33 Sam Sabin, Microsoft unveils AI agent that can autonomously detect malware, Axios, 5 August 2025, https://www.axios.com/2025/08/05/microsoft-ai-agent-malware-detection (accessed 28 August 2025).

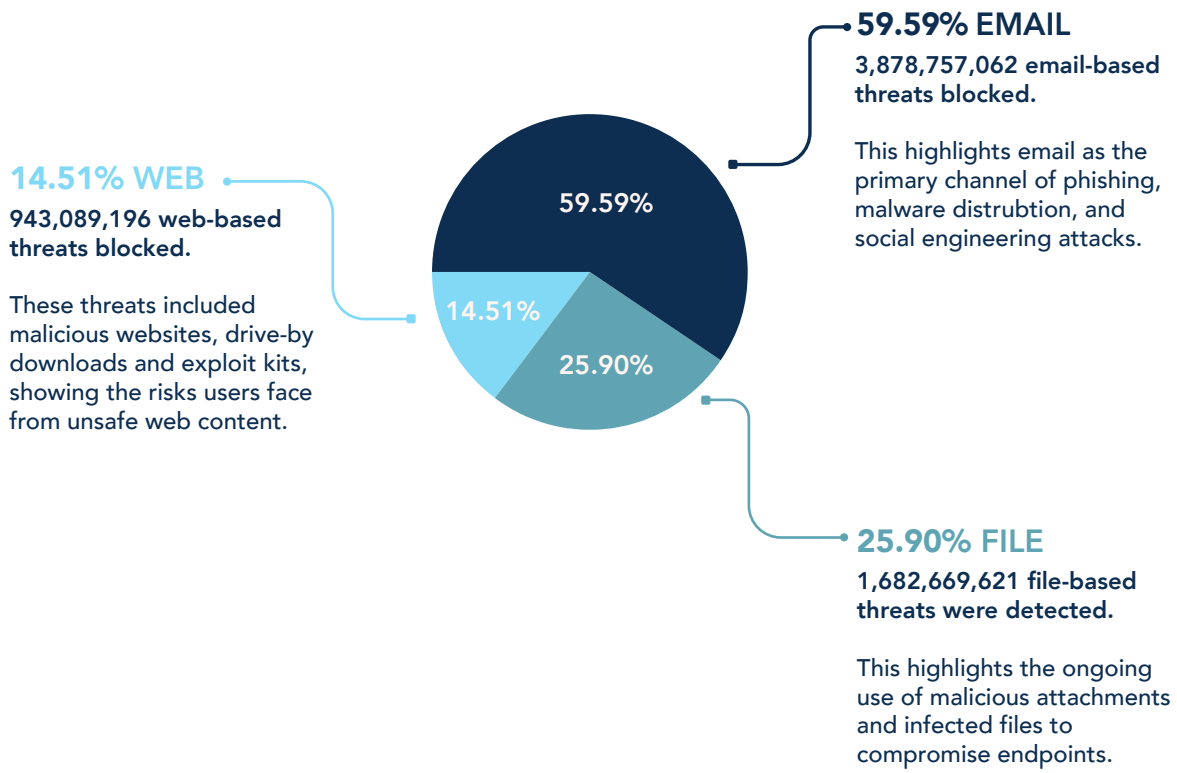


Figure 4: Distribution of threats blocked in the Asia and South Pacific region in 2024 (Data source: Trend micro data provided to the Cyber Fusion Centre)

To respond to these evolving threats, law enforcement agencies across member countries have integrated AI tools into both investigative and preventive operations. Examples of such measures include the development of deepfake detection systems in collaboration with academic and research institutions, AI enhanced platforms for identifying phishing websites and online scams, and AI-driven tools to monitor social media for criminal activities such as fraud, data leakage, and content promoting violence. These AI powered measures have enabled authorities to proactively detect emerging threats, track perpetrators, and mitigate the impact of cyber-enabled crimes more efficiently.

Nevertheless, INTERPOL's member countries continue to face challenges such as the rapid evolution of generative AI techniques, limitations in cross-border investigations, and the need for continuous capacity building to ensure that officers remain equipped to counter technologically sophisticated offenders.[34]

34 INTERPOL, Cyber Threat Assessment Survey, data provided by member countries, 2025.

4 ASIA AND SOUTH PACIFIC CYBERCRIME OUTLOOK: KEY EMERGING THREATS

Cybercrime in the Asia and South Pacific region is evolving rapidly, driven by technological innovation, expanding digital ecosystems, and increasingly organized criminal networks. Based on survey insights and in-house intelligence, the following section outlines the most significant emerging threats expected to shape the regional cybercrime landscape.

The expanding threat of AI in cybercrime

As previously stated, the misuse of AI in cyberattacks is no longer a future concern but an immediate operational reality. Going forward, AI is expected to be increasingly leveraged by malicious actors to increase the speed, scope, accuracy, and impact of their operations. These capabilities include generating realistic deepfakes, automating phishing at scale, deploying adaptive malware, and performing real-time vulnerability scanning.

Such developments risk significantly undermining existing defences, facilitating sophisticated fraud, impersonation, and intrusion techniques possible. As AI tools become more accessible, cyberattacks are expected to grow in complexity and volume, requiring law enforcement and security stakeholders to adopt more agile and proactive approaches.

To assist with this shift, INTERPOL's AI Toolkit provides a comprehensive framework for law enforcement agencies to develop and deploy AI responsibly.[35]

Emerging forms of fraud: scalable, adaptive and global

AI is also transforming the landscape of digital fraud, driving the emergence of more elaborate and deceptive schemes. Advanced scams increasingly involve AI-generated content such as manipulated audio, visuals, messages, and automated interactions that simulate legitimate communication across multiple platforms. These innovations are now powering large-scale scam ecosystems, including fake job offers, investment traps, romance baiting, and identity fabrication.[36]

A notable development is the expansion of scam call centres, which now form part of a global underground economy.[37] These centres frequently take advantage of lax enforcement and legal ambiguities while operating with little oversight. Reports indicate that criminal networks now use AI to plan schemes that include trafficking people into forced participation in scam activities and recruiting victims through deceptive job advertisements.[38]

Worryingly, once concentrated in specific regions, these operations have expanded into new regions, such as the Middle East, Latin America, Eastern Europe, West Africa, and parts of the United States. As a result, losses associated with these fraud operations are reaching multibillion-dollar levels worldwide. Even mature economies, often thought to have stronger cyber defences, are increasingly being targeted due to exploitable regulatory gaps and higher potential financial gain.

35 INTERPOL, Artificial Intelligence Toolkit, INTERPOL, https://www.interpol.int/How-we-work/Innovation/Artificial-Intelligence-Toolkit (accessed 29 August 2025).

36 Trend Micro, AI-Powered Scams: What a Threat Researcher Wants You to Know, Trend Micro, 18 July 2025, https://news.trendmicro.com/2025/07/18/ai-scams-threat-researcher (accessed 28 August 2025).

37 INTERPOL, INTERPOL releases new information on globalization of scam centres, INTERPOL, 30 June 2025, https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres (accessed 28 August 2025).

38 United Nations Office on Drugs and Crime, Inflection Point 2025 (Report, 2025), https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf (accessed 9 October 2025).

Cloud infrastructure as a growing target

As organizations across the region accelerate cloud adoption to improve scalability and collaboration, cybercriminals are exploiting misconfigured systems, weak encryption, insecure APIs, and insufficient monitoring. Threat actors are launching phishing campaigns, deploying malicious services, and stealing sensitive data from vulnerable environments. Ransomware, cloud jacking, and privacy violations are now frequent dangers. To mitigate these risks, businesses are highly encouraged to use automated monitoring, enforce strict cloud hygiene policies throughout their infrastructure, and perform frequent audits.[39]

Rise in identity-based attacks

Identity-based attacks are becoming more frequent. Traditional security measures like 2FA are becoming inadequate due to password reuse, compromised credentials, and vulnerabilities in single sign-on (SSO) systems.[40] Attackers create fake accounts, pose as users, and perpetrate fraud using credentials that have been stolen. A more robust option is adaptive verification, which authenticates users in real time according to their location, behaviour, and device integrity.

Upsurge in infostealer activities

Infostealer malware, which primarily targets sensitive data like financial information, personal information, and login credentials, remains an active threat. These tools are frequently used to facilitate downstream cybercrimes such as ransomware, fraud, identity theft, and broader cyber-enabled activity.

Established infostealer families like Lumma, Loki, and RedLine continue to evolve despite law enforcement efforts. The emergence of new crimeware variants further underscores the need for persistent vigilance, real-time intelligence exchange, and coordinated international action.

Weaponization of regulatory compliance by ransomware attackers

Ransomware groups have been observed to exploit companies' regulatory obligations to intensify pressure during extortion attempts. Threat actors now threaten to disclose alleged compliance violations to authorities unless ransoms are paid, significantly raising the legal and financial stakes for victims.

To counter this trend, organizations should strengthen their compliance frameworks and enhance incident response plans to handle both ransomware threats and regulatory requirements effectively.

These emerging threats signal a decisive shift in the cybercrime environment – one that is faster, more adaptive, and increasingly difficult to predict. Strengthening resilience across the Asia and South Pacific region will depend on early warning, coordinated action, and a shared commitment to confronting cybercrime at scale. As threats continue to evolve, building proactive, forward-looking defensive postures will be critical for the region's ability to detect, disrupt, and deter cybercriminal activity.

39 SentinelOne, 17 Security Risks of Cloud Computing in 2025, SentinelOne, 2025, https://www.sentinelone.com/cybersecurity-101/cloud-security/security-risks-of-cloud-computing (accessed 28 August 2025).

40 Secybersafe, Why 2-Factor Authentication (2FA) Would No Longer Be Sufficient in 2025, Secybersafe, 24 October 2024, https://secybersafe.com/blog/2024/10/24/why-2-factor-authentication-2fa-would-no-longer-be-sufficient-in-2025 (accessed 28 August 2025).

5 WAY FORWARD FOR PROACTIVE ACTIONS AGAINST EVOLVING CYBER CRIMES

Throughout 2024, countries across the Asia and South Pacific region adopted a diverse set of measures to address escalating cybercrime risks. Figure 5 summarizes the preventative actions implemented and the number of countries implementing each measure. These include the enactment of new laws targeting emerging forms of cyber-enabled crime, the bolstering of regional and cross-border partnerships, deeper engagement with industry stakeholders, and investments in more resilient digital defences. Some law enforcement agencies also prioritized capacity building for specialist units and undertook initiatives to raise digital literacy and risk awareness among communities. Collectively, these efforts demonstrate a strong regional commitment to adopting a proactive posture against cybercrime, to prevent and mitigate the impact of digital threats.

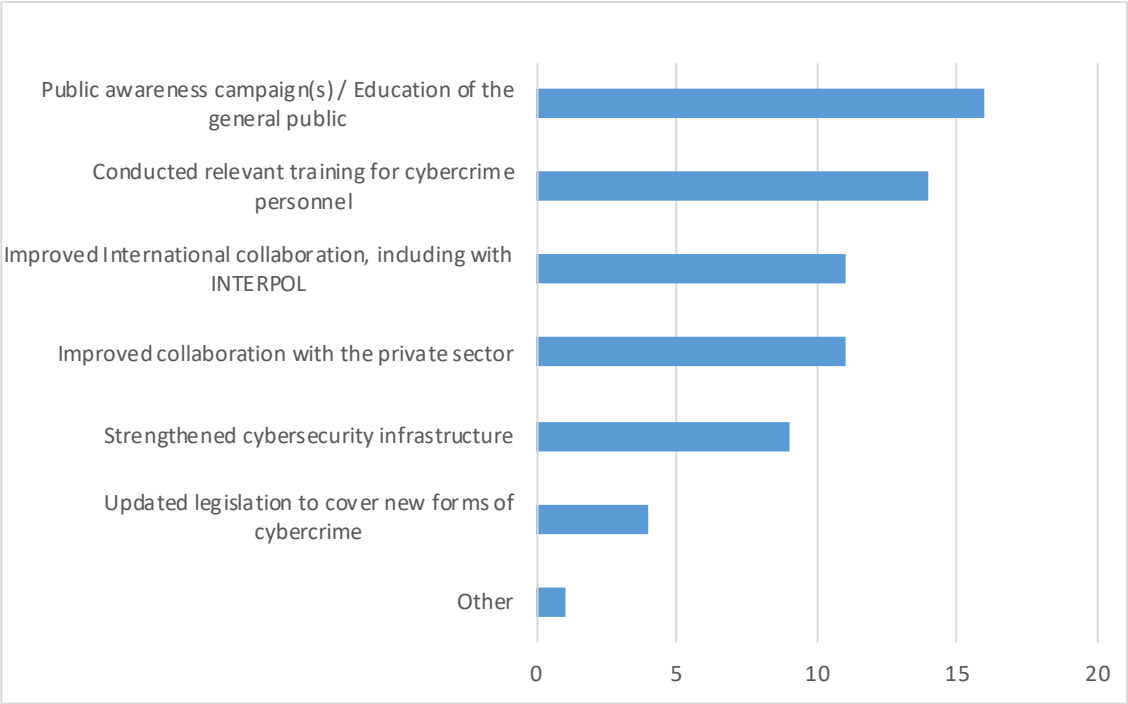


Figure 5: Preventative actions taken by member countries
Improved international collaboration

5.1 Key national cybercrime initiatives: legislation, capacity building and public awareness campaigns

Survey responses highlight a wide range of proactive actions undertaken by INTERPOL member countries across the Asia and South Pacific region in 2024 and 2025. For instance, most launched public awareness campaigns to inform citizens about cyber threats and promote good cybersecurity practices. Other key legislative, operational, and awareness initiatives include:

- **Republic of Korea**
  In response to a sharp rise in deepfake-related sex crimes in 2024 and 2025, the government launched coordinated countermeasures and intensive investigations. The Act on Special Cases Concerning the Punishment of Sexual Crimes was amended to criminalize possession of deepfake sexual materials and to increase penalties for their creation, processing, and distribution. The Korea National Police Agency (KNPA) integrated AI into its operations, including the deployment of a deepfake detection tool.

- **Indonesia**
  Indonesia expanded its Cybercrime Directorate, creating a task force for emerging threats and enhancing officer training through INTERPOL and private-sector partners. The Indonesia National Police (INP) adopted AI and big data technologies to support the detection of cybercrime activities. Indonesia also launched a nationwide Cybercrime Awareness Campaign targeting vulnerable groups via media and online platforms, which contributed to increased reporting and reduced victimization.

- **Hong Kong, China**
  The Hong Kong Police Force (HKPF) strengthened cybercrime prevention through new laws regulating virtual asset service providers, stablecoin issuers, and critical infrastructure cybersecurity. Other measures included the implementation of the SMS Sender Registration Scheme and a cybercrime law reform study to understand the challenges posed by rapid developments in information technology and the Internet. To reduce scam-related risks, HKPF also upgraded its "Scameter" tool to "Scameter+" with real-time scam alerts, integrating it with the banking system, and partnering with telecom providers to block fraudulent numbers and websites.

- **Philippines**
  The Philippines strengthened its cybercrime capabilities by implementing the National Cybersecurity Plan 2023-2028, enhancing government network security and achieving higher rankings in the United Nations Global Cybersecurity Index. Key legislative measures included amendments to the Anti-Financial Account Scamming Act, while proposed changes to the Cybercrime and Data Privacy Acts aim to strengthen privacy protections. A major preventive step was the nationwide ban on Philippine Offshore Gaming Operators (POGOs), disrupting networks linked to financial scams, money laundering, and other organized cybercrimes.

- **Japan**
  Japan's National Police Agency (NPA) launched a targeted awareness campaign to warn the public about the rising threat of DDoS attacks. The initiative included prominent alerts on the NPA's website and social media channels, as well as Google Ads to reach a wider audience, and was coordinated with Europol as part of a broader international effort. Running from December 2024 to March 2025, this campaign successfully generated around 30,000 search results linking to the warning page and displayed over 2,000 on-screen alerts, significantly increasing public awareness and encouraging proactive measures to mitigate potential attacks.

5.2. Adoption of AI – evidence of a proactive shift in regional law enforcement

Alongside these national initiatives, a complementary trend is the growing uptake of AI within law enforcement across the region – a practical signal of a broader shift to more proactive strategies against cybercrime. In the 2025 ASP Desk survey, 66.7 per cent of respondents reported that their agencies have already adopted AI tools and systems, while 33.3 per cent have yet to do so. This adoption reflects a growing recognition of AI's potential to enhance policing capabilities, particularly in responding to complex and evolving threats in cybercrime such as ransomware attacks, large-scale fraud, and transnational organized crime.

AI technologies are increasingly being used for predictive analytics, digital forensics, threat detection, and real-time intelligence processing. These capabilities enable agencies to respond faster, allocate resources more efficiently, and uncover patterns that may not be apparent through traditional investigative methods. Although adoption levels vary by country and capability, the trend toward AI integration highlights a regional shift towards embracing innovative technological solutions to strengthen the fight against cybercrime.

5.3. Proactive strategies to enable a whole-of-society response to cybercrime

Combating a fast-evolving cyber threat landscape requires a whole-of-society approach. Building on national initiatives, organizations and authorities should prioritize a set of forward-looking strategies. This includes:

- Integrating AI-powered security solutions
- Enhancing cloud security through strong encryption protocols and stringent access controls
- Establishing comprehensive incident response frameworks to address threats like ransomware attacks and the exploitation of regulatory compliance vulnerabilities – for example, Table 2 outlines some of the key cybersecurity measures that can be implemented to combat ransomware and infostealers
- Investing in continuous user education on emerging threat vectors
- Strengthening collaboration with industry partners for real-time threat intelligence sharing
- Ensuring alignment with evolving compliance standards remains critical.

Collectively, these measures can significantly strengthen defences against a rapidly evolving and increasingly sophisticated cyber threat landscape. Yet, meeting the scale and speed of today's challenges will require more than isolated national efforts. A truly effective response demands that all stakeholders – including law enforcement, governments, industry, and civil society – work together, share actionable information, and invest in the capabilities needed to detect, disrupt, and deter cybercriminals across the Asia and South Pacific region.

Best practices for organizations to combat ransomware and infostealers

The following table (see Table 2) outlines key cybersecurity measures that can be implemented to prevent the initial entry and spread of two major types of malware: ransomware and infostealers. While both share common attack vectors such as phishing and unpatched systems, each requires specific defensive strategies tailored to their behaviour and goals. These recommendations provide a foundation for reducing exposure and enhancing organizational resilience.

	Control Area	Ransomware Defences	Infostealer Defences
1	**E-mail security**	• Advanced spam/phishing filtering • Sandbox e-mail attachments and links • User training on phishing and macros.	• Block suspicious attachments/links • Detect credential phishing lures • Simulated phishing campaigns.
2	**Remote access**	• Disable Remote Desktop Protocol (RDP) if unnecessary • Use virtual private network (VPN) with multi-factor authentication (MFA) • IP allowlisting.	• Monitor remote access sessions • Block unknown access to credential systems • Alert on unusual session behaviour.
3	**Patch management**	• Regular OS and software patching • Vulnerability scanning • Detection of exploit attempts.	• Prioritize browser, plugin, and VPN patches • Focus on client-side vulnerabilities.
4	**Endpoint protection**	• Endpoint detection and response (EDR)/antivirus (AV) to block suspicious executions • Block lateral tools (e.g. PsExec, Server Message Block (SMB)) • Detect encryption behaviour.	• EDR to detect credential theft, keyloggers • Block access to credential managers and vaults.
5	**Access control**	• Enforce least privilege principle • Use role-based access control (RBAC) • Limit admin account use.	• Same as ransomware • Monitor credential access • Block credential dumping tools.
6	**Network segmentation**	• Segment critical servers from user endpoints • Block lateral movement paths.	• Isolate sensitive apps/systems • Restrict Internet access for vulnerable hosts.
7	**Backup and recovery**	• Maintain offline, encrypted, immutable backups • Regularly test recovery processes.	• Same as ransomware.
8	**Data loss prevention (DLP)**	• Not a primary control unless data exfiltration occurs.	• Detect unauthorized data transfers • Monitor clipboard and browser data access.
9	**Browser security**	• Not a common vector.	• Disable password storage and autofill • Enforce use of password managers • Block malicious browser extensions.
10	**Outbound network defence**	• Maintain offline, encrypted, immutable backups • Regularly test recovery processes.	• Domain name system (DNS) filtering • Transport layer security (TLS) inspection • Monitor for data exfiltration (e.g. hyper text transfer protocol (HTTP) POST).
11	**Peripheral device control**	• Restrict USB and external storage • Block autorun • Alert on new device activity.	• Same as ransomware • Block unauthorized access to local credentials.
12	**Threat detection and intelligence**	• Security information and event management (SIEM)/extended detection and response (XDR) alerting • Ransomware-specific Indicators of Compromise (IOCs).	• IOC feeds for known infostealers (e.g. RedLine, Raccoon) • Use honeypots and fake credentials to detect targeting.
13	**User awareness**	• Training on ransomware delivery methods (e.g. macros, phishing) • Encourage cautious file handling.	• Training on dangers of cracked software and fake updates • Promote strong password hygiene and MFA use.

Table 2: Best Practices to Defend Against Ransomware and Infostealers[41]

41 Open-source intelligence derived from research carried out by the Cyber Fusion Centre, 2024.

6 INTERPOL CYBERCRIME STRATEGY FOR THE ASIA AND SOUTH PACIFIC REGION

6.1 About INTERPOL

INTERPOL'S VISION: **"TOGETHER AGAINST CRIME"**

INTERPOL's recently launched Strategic Framework for 2026-2030 is built on the unified vision, "Together Against Crime", and its fundamental mission is "To connect and empower global law enforcement for a safer world". INTERPOL strives to be the leading voice of law enforcement worldwide, be the trusted global hub where law enforcement can securely communicate, share, and access critical police information, and provide world-class investigative and operational support to better combat transnational crime.

6.2 About the INTERPOL Cybercrime Programme

In today's rapidly evolving digital landscape, where over half the world's population faces potential cyber threats, the INTERPOL Global Cybercrime Programme leads and coordinates the international law enforcement community's efforts to prevent, detect, investigate, and disrupt cybercrime. Our work ultimately aims to strengthen member countries' capabilities to identify and apprehend cybercriminals, dismantle the malicious infrastructure they rely on, and recover criminal proceeds.

This commitment is guided by the INTERPOL Global Cybercrime Strategy, which is built around four key objectives:

- Foster a proactive and flexible approach to preventing and disrupting cybercrime by deepening collective understanding of the threat landscape through robust information-sharing and intelligence analysis
- Prevent, detect, investigate, and disrupt cybercrime with significant national, regional, and global impact by leading, coordinating, and supporting transnational operational efforts among member countries
- Strengthen member countries' strategies and capabilities to combat cybercrime by fostering open, inclusive, and diverse partnerships, and building trust across the global cybersecurity ecosystem
- Advance INTERPOL's leadership in global security by actively engaging with international forums on cybercrime and showcasing its capabilities.

INTERPOL implements this strategy through a simple and effective delivery model, consisting of three core pillars:

- **Cybercrime threat intelligence:** Delivering timely and comprehensive intelligence to tackle immediate and emerging cyber threats
- **Cyber capabilities development:** Strengthening strategies and enhancing capabilities through innovative initiatives and platforms
- **Cybercrime operations:** Supporting, coordinating and leading cross-border operations against cybercrime.

These pillars are underpinned by INTERPOL's extensive network of public-private partnerships, which leverages collective expertise to strengthen global cyber resilience.

For additional information on the INTERPOL Global Cybercrime Programme, please contact: **EDPS-CD@interpol.int**


.search-result-cell {
color: #fff;
float: left;
position: relative;
}
.js-hover-container {
position: relative;
}
div,
border: 0;
outline: 0;
font-size: 100%;
vertical-align: baseline;
background: transparent;
margin: 0;
padding: 0;
}

7 ABOUT THE INTERPOL ASIA AND SOUTH PACIFIC JOINT OPERATIONS ON CYBERCRIME

The Asia and South Pacific Joint Operations against Cybercrime (ASPJOC) is a project dedicated to combating cybercrime across the Asia and South Pacific region. It is implemented through a dedicated Asia and South Pacific Desk (ASP Desk), based at the INTERPOL Global Complex for Innovation (IGCI) in Singapore.

ASPJOC coordinates multinational cybercrime investigations, facilitates intelligence sharing, and supports the execution of joint operations targeting a wide range of cyber threats – including infostealers, phishing, banking malware, and ransomware. Through close collaboration with member countries, regional cybercrime units, and global partners, it enhances law enforcement capabilities, accelerates cross-border investigations, and delivers strategic threat assessments. The desk plays a pivotal role in unifying the regional response to cybercrime, supporting capacity building, and strengthening digital resilience across the Asia and South Pacific region.

Project overview

ASPJOC seeks to enhance the capabilities of Asian and South Pacific national law enforcement agencies in combating cybercrime by:

- Collecting and analysing intelligence on cybercriminal activities
- Encouraging cooperation and sharing best practices among Asia and South Pacific member countries
- Facilitating and executing intelligence-driven, coordinated actions against cybercrime.

Phase 1 of the project concluded in July 2025, successfully achieving all its objectives and laying a strong foundation for subsequent phases. Funded by the United Kingdom Foreign, Commonwealth & Development Office, it focused on the following member countries: Brunei, Cambodia, Indonesia, Lao PDR, Malaysia, Philippines, Singapore, Thailand, Viet Nam, Fiji, Kiribati, Marshall Islands, Nauru, Papua New Guinea, Samoa, Solomon Islands, Timor-Leste, Tonga, and Vanuatu.

Project activities

Through the ASP Desk, ASPJOC supports member countries in the fight against cybercrime in four core areas of work:

1. **Analytical support and threat intelligence**

   Publishing and distributing cyber threat assessments, advisories, and activity reports to provide Asia and South Pacific member countries with valuable insights into emerging cyber threats and trends, aiding resource allocation and strategic decision-making.

2. **Awareness-raising campaigns**

   Offering practical guidance on identifying relevant cyber threats, supporting law enforcement's prevention efforts for improved outcomes, and promoting good cybersecurity practices for individuals and organizations in the Asia and South Pacific region.

3. **Joint operational framework and working group meetings**

   Establishing secure platforms and mechanisms for effective information-sharing between Asia and South Pacific law enforcement agencies, intergovernmental organizations, and private sector partners to combat cybercrime.

4. **Investigative assistance and operational coordination**

   Leading intelligence-driven operations, coordinated actions, and disruption efforts against cybercrime, including dismantling malicious infrastructure and supporting our member countries in identifying and arresting the criminals operating in or impacting the Asia and South Pacific region.

The ASP Desk collaborates closely with regional stakeholders, the private sector, and other key partners to support law enforcement agencies in mitigating the impact of cybercrime.

INTERPOL

INTERPOL's role is to enable police in our 196 member countries to work together to fight transnational crime and make the world a safer place. We maintain global databases containing police information on criminals and crime, and we provide operational and forensic support, analysis services and training. These policing capabilities are delivered worldwide and support four global programmes: financial crime and corruption; counter-terrorism; cybercrime; and organized and emerging crime.

WWW.INTERPOL.INT

INTERPOL

@INTERPOL_HQ

INTERPOL_HQ

INTERPOL HQ

INTERPOL