INTERPOL

ASIA AND SOUTH PACIFIC

CYBERTHREAT ASSESSMENT REPORT

AUGUST 2024

AUGUST 2024

CONTENTS

LEGAL DISCLAIMER

FOREWORD

Cybercriminality respects no borders impacting all communities globally posing a significant challenge to security across countries. The digital era has led to a greater reliance on online activities, which, in turn, has amplified the vulnerability of societies to cyber threats. These vulnerabilities are further exacerbated by the discrepancies in the capability and capacities of cyber law enforcement across different regions. This gap provides fertile ground for the expansion of criminal networks and opportunities to cause harm.

INTERPOL is committed to aiding its global membership in strengthening law enforcement capabilities and capacities to counter and combat cybercrime. INTERPOL extends a range of tools, platforms, and operational support, all aimed at enhancing cross-border police cooperation for a safer world. Within this context, the INTERPOL Cybercrime Programme plays a critical role in leading the law enforcement response to cybercrime on a global scale.

The foundations of these efforts are built on strong partnerships with collaboration and cooperation between diverse actors within the global cybersecurity ecosystem being essential. Their varied insights, expertise, and data are crucial for developing effective policy and operational responses to cybercrime. Through partnership, we combine our strengths, enabling us to become more resilient and agile in facing these threats.

Adopting a regional approach to operational coordination against cybercrime, INTERPOL recognizes that while cybercrime is a global challenge, each region has its unique response mechanisms. By understanding the evolving threats and their impacts within specific regions, we can target our combined efforts more effectively.

With these considerations in mind, INTERPOL has developed this Asia South Pacific Cyberthreat Assessment Report. The goal is to accurately gauge the cyberthreat landscape to offer targeted support, in the field of strategic and capabilities development, analytical support, and operational coordination. As identified by our Asia South Pacific membership, the report focuses on three main areas of interest: ransomware, online scams, and other trends. It then concludes suggesting recommendations to pave the way forward a safer region and world.

We express our gratitude to the member countries in the Asia South Pacific region and our partners for their continued commitment to this cause.

Craig JONES
Director, Cybercrime
Executive Directorate Police Services
INTERPOL

ABBREVIATIONS AND ACRONYMS

ASP	Asia and South Pacific
ASPJOC	Asia and South Pacific Joint Operation against Cybercrime
APAC	Asia Pacific region
AI	Artificial Intelligence
BEC	Business Email Compromise
C3DP	Cyber Capabilities & Capacity Development Project
CERT	Computer Emergency Response Teams
DDoS	Distributed Denial of Service
GLACY+	Global Action on Cybercrime Extended (currently GLACY-e)
IABs	Initial Access Brokers
IP	Internet Protocol
LLM	Large Language Models
RaaS	Ransomware-as-a-Service
RAT	Remote Access Trojan
SaaS	Scams-as-a-Service
SMEs	Small and Medium-sized Enterprises

ACKNOWLEDGEMENT

This assessment report was written by the Asia and South Pacific Cybercrime Operations Desk (ASP Desk) under the Asia and South Pacific Joint Operations Against Cybercrime (ASPJOC) and funded by the United Kingdom's Foreign, Commonwealth and Development Office (FCDO).

This report is based on the assessment of information provided to INTERPOL by relevant member countries and INTERPOL's private partners, including Bi.Zone, Fortinet, Group-IB, Kaspersky Lab, and Trend Micro.

NOTES ON THE METHODOLOGY USED FOR THE 2024 INTERPOL ASIA PACIFIC CYBERTHREAT ASSESSMENT REPORT

The 2024 INTERPOL Asia South Pacific Cyberthreat Assessment Report builds on previous editions to offer an in-depth analysis of the cyber threat landscape as experienced by Asia Pacific member countries. This edition presents a thorough analysis, focusing on key threats such as ransomware, business email compromise, and other forms of online scams. More than just identifying these pressing issues, the report also looks at the ongoing national initiatives aimed at bolstering cyber resilience across the continent. It concludes with actionable recommendations aimed at guiding future cybersecurity efforts on the continent.

The assessment draws mainly on intelligence and operational data resulting from INTERPOL's assistance to member countries in the region. Additional information comes from an INTERPOL-led survey, consisting of 40 quantitative and qualitative questions which were posed to member countries on the topic of prevention, detection, investigation, and disruption of cybercrime. Additionally, this dataset was complemented by strategic consultations with INTERPOL Gateway partners, such as Bi.Zone, Fortinet, Group-IB, Kaspersky Lab, and Trend Micro.

The Report itself does not include any data (i.e., police data) as defined in INTERPOL's Rules on the Processing of Data. All member countries and private entities involved have consented to the use and reference in this Report of the information they have provided to INTERPOL.

EXECUTIVE SUMMARY

This report presents INTERPOL's analysis of the main cyber threats affecting the Asia Pacific region, drawing on internal intelligence, operational insights, survey results, and contributions from private sector partners.

As the Asia Pacific (APAC) region undergoes substantial digital transformation, it confronts a dynamic cyber threat landscape. In 2023, APAC saw an increase in both sophisticated and less-targeted attacks, fueled by the widespread availability of cybercriminal tools like Scams-as-a-Service (SaaS). Phishing, the primary method for initial cyber intrusions, is likely to become more prevalent as SaaS platforms begin to integrate generative AI, enhancing scam effectiveness with localized language use. Concurrently, ransomware attacks surged by approximately 39%, notably affecting the manufacturing, real estate, and financial sectors.[1] The ransomware market's evolution, marked by a decrease in sophistication, indicates a changing threat dynamic. Additionally, the region faces threats from data extortion, increased compromised financial data, and a rise in info stealers and banking trojans, leveraging the booming digital financial services. These trends highlight the critical need for increased cyber resilience and cooperation across the region.

Efforts to combat these threats are ongoing, with countries enhancing the capabilities of their Computer Emergency Response Teams and increasing public and private sector cyber literacy. However, challenges remain in collaboration between law enforcement, the private sector, and the judiciary, complicated by the international nature of cybercrime and varying laws across jurisdictions. Moreover, a shortage of trained cybersecurity professionals continues to hinder effective cyber defense measures across the region.

INTERPOL, through its Asia and South Pacific Cybercrime Operations Desk, is actively supporting regional efforts to counter these threats. In addition, initiatives such as the Global Action on Cybercrime and the Cybercrime Capabilities and Capacity Development Project play a critical role in building best practices within law enforcement and enhancing the training of national agencies. As the region continues its digital advancement, the collaboration between INTERPOL, member countries, and private sector partners will be crucial in mitigating the impacts of cyber threats and ensuring a secure digital future for the Asia Pacific region.

1 Hxxps://www.group-ib[.]com/media-center/press-releases/hi-tech-crime-trends-2023-2024/

INTRODUCTION

The Asia Pacific (APAC) region, which is home to over half of the world's population, holds immense geopolitical, economic, and technological importance. Its countries are currently experiencing a rapid digital revolution, with advances in novel Information and Communications Technology (ICT) prompting huge developments across diverse sectors, facilitating economic development, health improvements, enhanced service provision, and remote learning and working opportunities. The number of internet users in Asia is increasing at an accelerated rate, with 67% of the population having access to the Internet. In Southeast Asia a dynamic and rapidly growing market exists, boasting over 400 million internet users and a flourishing digital economy. The internet penetration rate exceeds 70% in most parts of the region.[2]

The digital economy of Southeast Asia is projected to reach $1 trillion by 2030, largely driven by growth in e-commerce, digital payments, e-learning, and remote work. The region's digital growth is particularly evident in the emergence of digital financial services, for example, the adoption of utilizing e-wallets for text message-based transactions.[3] The digital payments market in APAC is projected to grow significantly, highlighting the shift towards mobile and electronic payment solutions.

However, despite the widespread adoption of ICT across many parts of the region, there continues to be a significant digital divide, characterized by the stark contrast in digital transformation capabilities among countries within the region.[4] Advanced economies such as China, Japan, the Republic of Korea, and Singapore exhibit high digital adoption and infrastructure levels. Meanwhile, the Pacific Islands face challenges in digital transformation, and there are noticeable differences in digital advancement across South-East Asia. This internal disparity underscores the uneven pace of digital progress and the need for targeted interventions to bridge the gaps in actions against cybercrime.

The rapid adoption of digital solutions, accelerated by the COVID-19 pandemic, which have often occurred without comprehensive security measures have left new vulnerabilities exposed in networks across the region. The significant manufacturing demand in countries like China, Taiwan, China, and Vietnam, particularly in the semiconductor industry, combined with the growing disparity of cybersecurity adoption and practices have left not only the regional but also the global supply chain vulnerable. This is reflected in the skills gap: although the APAC saw the highest increase in cybersecurity professionals in 2022 (15.6%), there is still an estimated gap of 2.16 million skilled cyber security workers.[5]

Addressing the digital disparity, digital literacy, and inadequate cyber preparedness is increasingly urgent for the region. Fortunately, countries have begun taking steps to address these. Many countries have dedicated resources to capacity building programs and other relevant initiatives. Within this context, INTERPOL is committed to supporting the region achieve these objectives through projects such as the Global Action on Cybercrime Projects (GLACY-E) and the Cybercrime Capabilities and Capacity Development Project (C3DP), which deliver critical activities aimed at building best practice in law enforcement agencies, and training exercises tailored to the needs of national agencies. These efforts are now integrated by the intelligence-led operational activities of the Asia and South Pacific Cybercrime Operations Desk (ASP Desk), under the Asia and South Pacific Joint Operations Against Cybercrime (ASPJOC).

2 Hxxps://www.statista[.]com/statistics/265156/internet-penetration-rate-in-asia/#:~:text=In%202022%2C%20the%20internet%20penetration,under%2071%20percent%20in%202022

3 Hxxps://asia.nikkei[.]com/EditorsPicks/Interview/ASEANs-digital-economy-growth-hinges-on-upskilling-BCG

4 Hxxps://www.repository.unescap[.]org/handle/20.500.12870/4630

5 Hxxps://www.isc2[.]org/Insights/2023/11/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-Workforce-Gap

OVERVIEW OF CYBER THREATS IN ASIA AND PACIFIC

In 2023 the APAC cyberthreat landscape remained dynamic, with the region seeing a rise in the number of sophisticated attacks, but also an increased proliferation of less sophisticated and un-targeted attacks caused by the democratization of cybercriminal tools. Based on intelligence and operational analysis from INTERPOL's regional activities, and enriched by the direct results of enquiries sent to ASPJOC member countries and information from private sector partners, INTERPOL has identified the following key threats and trends:

Threats

Online scams continue to be the most prolific threat across the region.

- Access to online scam tools is being democratized, as the number of 'Scams-as-a-Service' (SaaS) continue to rise. These platforms offer criminals the ability to create and run wide-ranging scams by automating the creation and distribution of phishing emails and collecting and distributing any data obtained to the criminals directly.
- Phishing is the main technique used for initial access in these scams. It remains the top tactic reported in both the Reconnaissance and Initial Access phases of an attack. Questionnaire respondents reported that both public and private entities did not offer adequate cyber security standards to educate employees against these emails; this is likely a reason for its proliferation across the region.
- Phishing emails targeting APAC are likely to rise in 2024 and 2025 as generative Artificial Intelligence (AI) is integrated into the SaaS platforms. Given that generative AI allows for machine translations with increasing accuracy, cybercriminals operating outside the region are likely to be able to use regional languages to craft phishing emails, limiting the poor native language efforts which are a key factor for identifying phishing emails.

Ransomware was a fast-growing threat in APAC, but its impacts and targets differed by subregion.

- In 2023 Ransomware attacks targeting the APAC region increased regionally by approximately 39%. While this is a rapid rise for the region, North America and Europe remain the most targeted regions. The sectors most targeted were manufacturing, real estate, and financial services.
- Initial Access Brokers (IABs) continued to play a key role in the ransomware ecosystem in the APAC region; however, the market shrunk slightly, and accesses were less sophisticated, indicating a shift in the market.
- Data extortion continues to play a key role in ransomware attacks, due to its reputational, financial, and regulatory impacts.

A variety of diverse threats continue to impact the APAC region.

- The number of compromised cards originating in APAC banks rose, likely due to the increase in online financial transactions, as well as the availability of data online.
- The number of info stealers and banking trojans specifically targeting the APAC region also increased, again exploiting the region's rapidly growing digital financial services markets.
- Data extortion attacks without the deployment of ransomware are increasingly evident, as groups seek to evade law enforcement action and further obfuscate their tools.

Trends

APAC countries are increasingly recognizing the need to increase cooperation and cyber resilience to mitigate and prevent attacks.

- Many countries have taken steps to increase the capacity of their national Computer Emergency Response Teams (CERTs). This has included establishing CERTs, refining reporting practices, and increasing the CERT's abilities to respond to threats in a timely manner.
- Many questionnaire respondents indicated that they were adopting or continuing cyber literacy programs both for the general public and for private organizations. These included days or weeks of awareness activities, specific trainings, and campaigns raising awareness of the most prevalent threats. Some countries also stated that they were increasing education for children and teenagers to build cyber awareness as standard practice.
- Countries are increasingly looking to collaborate at both a regional and national level, with countries creating legislation to align their own regulations and cyber security practices with international norms such as the Budapest Convention on Cybercrime. Other countries indicated that they were participating in regional groups such as the Australian-led Cyber and Critical Tech Cooperation Program[6] and the Cyber Smart Pacific Campaign, part of the PaCSON Awareness Raising Working Group.[7] In ASEAN, governments across the region have acknowledged the significance of leveraging the ongoing digital transformation and standardized policy tools to foster resilience, trust, and security in a thriving regional digital economy, as outlined in initiatives like the ASEAN Digital Masterplan 2025. **However, all countries highlighted significant challenges that remain in terms of effectively preventing, detecting, investigating, and disrupting cybercrime across the APAC region.**
- Current levels of collaboration between law enforcement and the private sector continues to prevent the investigation of cybercrime in a timely manner. This is reportedly particularly evident in collaboration with Internet Service Providers (ISPs) to identify, attribute, and trace cybercrimes.
- Current levels of collaboration between law enforcement and stakeholders such as internal judiciary also remains an issue, with respondents reporting that the international nature of these crimes complicates legal proceedings due to varying laws and regulations across jurisdictions.
- Insufficient cyber awareness and cyber hygiene by private companies continues to undermine cyber resilience across the region, with companies resistant to adopt cyber security standards.
- Many countries regionally report a shortage of trained cybersecurity professionals capable of mitigating or preventing the increasingly sophisticated attacks.

6 https://www.dfat.gov.au/about-us/business-opportunities/business-notifications/cyber-and-critical-tech-cooperation-program-standing-open-call-proposals

7 https://pacson.org/about-us

INSIGHT ON ASIA AND PACIFIC CYBERTHREATS TREND: 2024

The Asia and South Pacific region has become increasingly targeted throughout 2023. The following sections offer a comprehensive analysis of the leading cyber threats, identified by INTERPOL's member countries in Asia and the South Pacific in response to a questionnaire sent to all APAC member countries. The results are presented in order of the importance identified by the member countries.

Online scams

KEY POINTS:

- Online scams were the highest reported threat by respondents, affecting the entire region indiscriminately. This is consistent with previous reporting periods.
- The region has seen an increase in 'Scams-as-a-Service' platforms, which has democratised the ability to create and send campaigns at both a targeted and untargeted level.
- Financial extortion remains the main motivation for the majority of scam campaigns, with the most impactful being Business Email Compromise (BEC) scams, as these typically target organisations rather than private individuals.
- Southeast Asia is increasingly becoming a hub for scam centres, which indicates the wider professionalisation of the threat groups involved in the ecosystem, and the resilience these campaigns are likely to have against law enforcement action.

Online scams are a type of cybercrime in which individuals are coerced into providing personal, financial, or other sensitive information which can later be used for financial gain or be sold to further cybercriminals, or to directly deceive the individual into making fraudulent transactions. These scams can be high volume and untargeted to cover as wide a demographic as possible, such as in phishing campaigns, or highly targeted and low volume and designed to target specific individuals such as in Business Email Compromise (BEC) or Whaling scams. Such scams typically use social engineering tactics against victims, with phishing emails the most prominent tactic for reconnaissance and initial access.

Online Scams remain the most prominent crimes across the APAC region; however, typically vary in sophistication and targeting at a sub-regional level.

Online scams have evolved into a significant cyber threat across the APAC region, with a diverse range of tactics including investment scams, romance scams, job scams, e-commerce scams, and cryptocurrency scams.[8] The sophistication and targeting varies at a sub-regional and country level, for example, the Singapore Police Force highlighted that young adults (20-29) are major victims, typically to job and e-commerce scams.[9] These scams are typically highly sophisticated and include rounds of job interviews and tailored online adverts. Meanwhile, specific vulnerabilities in less digitally literate populations, such as those in the Pacific Islands, exacerbate the problem due to low cyber awareness. Based on the Pacific Cyber Security Operational Network (PaCSON) annual report 2022, online phishing and scams are the most commonly experienced cyber-related security threats that face the people of the Pacific Islands. In these areas, certain demographics such as the elderly, less-educated individuals, small businesses, and high-profile individuals, are at increased risk, often being targeted via social media and messaging platforms, based on the survey responses.

At the same time, the rise of 'Scams-as-a-Service' models has increased the volume and proliferation of campaigns by offering automated scam services.

In 2023 online SaaS platforms increased their breadth of targeting to include APAC countries or evolved to specifically target APAC countries. One such example is the Telegram-based network Classiscam, which offers associates the capability to utilize Classiscam-generated phishing kits to create fraudulent advertisements and web pages, predominantly targeting Singapore and Malaysia.[10]

8 Hxxps://pacson[.]org/sites/default/files/2023-08/PaCSON%20Annual%20Report%202022_ONLINE.pdf

9 Hxxps://www.channelnewsasia[.]com/singapore/scams-2023-increase-50-percent-job-e-commerce-measures-4128051

10 Hxxps://www.group-ib[.]com/media-center/press-releases/classiscam-2023/

The growth of these networks is indicative of the growing sophistication of the scam criminal ecosystem, and offers less-capable cybercriminals the ability to operate sophisticated scam campaigns previously outside of their capability: in its current iteration Classiscam associates need only to insert a link to the fraudulent product into a chatbot, which then automatically generates a full suite of phishing tools, including links to fake courier services, payment gateways, and refund processes.[11]

The rise of SaaS platforms is likely to be linked to the increasing sophistication of Large Learning Models (LLMs) and Generative AI. Given the diverse socio-cultural, economic, and linguistic nature of the APAC region, cybercriminals may have previously been prevented running successful phishing campaigns due to linguistic or cultural errors in their fraudulent communications which made them easily identifiable as fake. The incorporation of these tools into platforms such as Classiscam opens up APAC as a region to wider regional and international criminals.

Shutdown of a phishing platform

In 2022, the Singapore Police Force was a key participant in INTERPOL's Operation First Light, which involved more than 76 countries. During the operation, more than 2,000 persons were investigated and over 5,300 bank accounts were frozen in Singapore, leading to the recovery of more than $11.5 million. In addition, a total of more than $30 million worth of virtual assets were seized by Singapore's Anti-Scam Command office.

AI holds significant potential for cybercriminals conducting scam campaigns, particularly in enhancing the efficiency and effectiveness of attacks.

Not only are Generative AI and LLM tools being used to enhance the efficacy of campaigns targeting APAC countries, they can also reduce the resource needed to create broad campaigns. Traditionally, crafting a sophisticated phishing email is a labor-intensive process, requiring an average of 16 hours for a threat actor to create; however, AI is now able to generate a deceptive phishing email in five minutes, vastly reducing the labor needed.[12] This rapid production capability allows cybercriminals to scale their operations, increasing the potential volume of attacks as well as the sophistication. The increased use of AI in phishing emails was evident in the questionnaire results, where respondents identified that they had observed AI-generated phishing emails being sent to victims.

Financial gain remains the dominant motivation for scams in the APAC region, with extortion scams and BEC representing the biggest threats.

The majority of respondents indicated that the scams observed were all conducted with financial gain as the motivation; in particular extortion scams are the most dominant scheme in the APAC region. According to private partner TrendMicro's scam detection, Singapore has the highest number of detections for extortion spam schemes within the Asia and South Pacific region, nearly three times more compared to Thailand which has the second highest number of extortion spam scheme detections.

BEC is a highly targeted type of scam where a threat attacker gains access to a business email account, often at an executive level or of an influential figure in the legal, financial or IT departments, then uses that account to send out emails to convince further individuals to transfer money, sensitive information, or increase the threat actor's internal access. Common tactics include impersonating executives, vendors, or trusted partners to request fraudulent wire transfers, redirect invoice payments, or gain access to sensitive company IP.

BEC attacks are characterized by their targeted nature and reliance of social engineering techniques. According to statistics collected by TrendMicro in 2023, approximately 28% of their detections for BEC are concentrated in the APAC region. Member countries responded in the questionnaire that BEC

11 Ibid

12 Hxxps://www.securityintelligence.com/x-force/ai-vs-human-deceit-unravelling-new-age-phishing-tactics/

attacks targeting the region were primarily targeted at key sectors including government-owned corporations, the financial services sector, travel agencies, and import-export companies. These sectors are likely perceived by threat actors to be particularly vulnerable, given their high volume of financial transactions and the sensitive information they handle. Many respondents also reported a high level of targeting of Small and Medium-sized Enterprises (SMEs), likely due to the perception they have lower levels of cyber security awareness.

Cybercriminal activity around BEC is likely accelerating in pace and sophistication. Microsoft has observed a significant trend in attackers' use of automatic platforms for creating industrial-scale BEC campaigns. Those platforms sell an end-to-end service including templates, hosting and automated services for BEC. Adversaries using this SaaS receive credentials and the IP address of the victim.[13]

BEC threat actors then purchase IP addresses from residential IP services matching the victim's location creating residential IP proxies which empower cybercriminals to mask their origin. Now, armed with localized address space to support their malicious activities in addition to usernames and passwords, BEC attackers can obscure movements, circumvent "impossible travel" flags, and open a gateway to conduct further attacks. Microsoft has observed threat actors in Asia and an Eastern European nation most frequently deploying this tactic.

Law enforcement agencies in the region face significant challenges in combating BEC, according to responses to the APAC questionnaire.

Cybercriminals are increasingly using obfuscation techniques such as proxy servers and VPNs to mask their locations, making it difficult to trace their activities. Additionally, questionnaire respondents have reported that obtaining timely cooperation from ISPs can be challenging, delaying investigations. The international nature of these crimes also complicates legal proceedings due to diverse laws and regulations across jurisdictions. Furthermore, there is a notable shortage of skilled cybersecurity professionals capable of addressing the sophisticated nature of BEC attacks.

To mitigate the financial loss of BEC, APAC law enforcement agencies recommend prioritizing freezing confiscated accounts and enhancing international collaboration to help address jurisdictional challenges and streamline cross-border legal processes. Investing in skill development for cybersecurity professionals is crucial, including specialized training in handling BEC and forensic investigations. Establishing protocols for quicker and more effective communication with ISPs can also aid in timely data retrieval during investigations.

Addressing the challenges faced by law enforcement and adopting strategic recommendations can enhance the region's resilience against BEC and reduce the financial and operational damages caused by these sophisticated cyber-attacks.

An INTERPOL-led operation targeting malware and cyber fraud across Southeast Asia, codenamed «Killer Bee,» resulted in the arrest of three suspected global scammers in Nigeria. Conducted by the Economic and Financial Crimes Commission (EFCC) in Lagos and Benin City, this operation was part of a broader effort involving law enforcement agencies from 11 Southeast Asian countries. The suspects were linked to a Nigerian fraud syndicate using the Agent Tesla Remote Access Trojan (RAT) to reroute financial transactions and steal confidential details from corporate organizations, including oil and gas companies in Southeast Asia.

Southeast Asian scam centers are increasingly sophisticated and regionally prolific.

According to a United Nations report, Southeast Asia has increasingly become a host to scam centres.[14] These centres often draw in 'employees' by posting fraudulent job adverts, typically for jobs as programmers, marketers, or HR specialists. Once 'employed' by these centres, these individuals are then involved in committing other scams for the centre operators, such as romance and investment scams, cryptocurrency fraud, money laundering, and illegal gambling. These criminal networks establish sophisticated infrastructures including call centers, social media operations, app development, and extensive data collection systems. Despite numerous takedowns by authorities since 2016, these scam operations frequently resurface in new locations with enhanced setups.

14 Hundreds of thousands trafficked to work as online scammers in SE Asia, says UN report | OHCHR

Operation Storm Makers II mobilized law enforcement in 27 countries across Asia and other regions

During October 2023, INTERPOL collaborated with law enforcement agencies to identify the link between human trafficking and online scams. The majority of these cases remain concentrated in Southeast Asia, where the intersection of high internet penetration rates and varying levels of regulatory enforcement creates fertile ground for such illicit activities. The operation identified that victims are often lured through fake job ads and forced to commit online fraud on an industrial scale, while enduring abject physical abuse. Fraud schemes include fake cryptocurrency investments, as well as work-from-home, lottery and online gambling scams. The findings indicate that these cybercriminal activities are not only financially devastating but also contribute significantly to human exploitation and trafficking networks.

According to the inputs by the APAC member countries, their law enforcement authorities are facing common challenges.

Online scams represent critical and evolving cyber threats that require comprehensive and dynamic strategies for mitigation. There is a critical need for faster operational responses and enhanced public education to combat phishing. Innovative and adaptive countermeasures are necessary to keep pace with the evolving threat, emphasizing the need for continuous improvement in cybersecurity protocols and international cooperation.

Implementing these recommendations requires a coordinated and sustained effort across various stakeholders, including government bodies, private sectors, and international partners. By enhancing collaboration, leveraging technology, and focusing on public education, law enforcement agencies can significantly advance their capability to combat the complex challenge of online scams and phishing effectively.

Many countries in the APAC region reported establishing specialized anti online scams/frauds teams to effectively deal with these emerging crimes such as the Fraud Squad under the Criminal Investigations Division in Samoa, and the Anti-Scam Command (ASCom) in the Singapore Police Force (SPF), by integrating scam investigation, incident response, intervention, enforcement, and sense-making capabilities under a single umbrella.

Ransomware

KEY POINTS:

- The number of ransomware attacks in the APAC region rapidly increased in 2023, but the growth remained lower than North America and Europe
- Initial Access Brokers continued to play a key role in the ransomware ecosystem.
- Digital Extortion tactics continued to evolve with the Ransomware-as-a-Service industry.

Ransomware and digital extortion are increasing rapidly in the APAC region.

Ransomware and digital extortion attacks were identified by INTERPOL member countries as one of the most serious cyber threats faced across the continent. These attacks are of consistently high impact, given their financial impact (both direct from any ransom paid and functional impact), reputational impact (which can result in further loss of revenue), and regulatory impact. They can also severely disrupt critical national infrastructure and essential services, and cause harm to organisations and individuals whose details may be sold on and may be the victims of further criminal activities. Despite several high-profile disruptions of ransomware groups by law enforcement agencies in 2023 and the first half of 2024, ransomware continues to be a lucrative activity: according to cyber security company Chainalysis ransomware payments exceeded USD 1 billion globally in 2023.[15]

The rate of ransomware attacks targeting the APAC region increased rapidly in 2023, by approximately 39%. While this is a rapid rise for the region, it still remains low on average globally, with attacks against North American companies rising by 109%, and attacks against European companies rising by 52%. The number of ransomware attacks is also expected to be higher, due to victims choosing to pay ransomware, and some ransomware groups not operating Dedicated Leak Sites (DLS). India was a primary target for ransomware attacks, likely given its large number of businesses, and perceived low levels of cyber security, making it an attractive target for ransomware operators.[16]

This slower rise in comparison to global totals is likely due to the predominance of English and Russian-language ransomware variants: previously without the translation capabilities of generative AI the linguistic and cultural diversity of the region may have been perceived by threat actors as prohibitive. However, several high-profile attacks against organisations in the APAC region occurred in 2023, such as the Lockbit ransomware attack against Nagoya port in Japan in July 2023, the LockBit ransomware attack against a US unit of the International Commerce Bank of China in November 2023, and the exposure of 10 companies regionally in the Cl0p ransomware attack against the MoveIt File Transfer Service in May 2024.[17] Such high-profile attacks are likely to have acted as 'adverts' for other ransomware operators to target the region.

In 2023, the manufacturing sector became the most frequently targeted industry in the region, representing 16% of all companies whose data was posted on leak sites[18]. This high percentage underscores the vulnerability of manufacturing companies to cyber threats, likely due to the critical nature of their operations and the potentially valuable intellectual property they hold. The manufacturing sector in this region also holds a key strategic role in global supply chains, particularly in the IT sector, and is therefore likely perceived by cybercriminals as more likely to pay.

The real estate industry was the second most targeted, involved in 9% of attacks. The financial services industry ranked third, accounting for 8% of attacks. Despite the industry's robust security measures, the high value of financial data continues to attract cybercriminals. This highlights the persistent need for advanced cybersecurity protocols within financial services to protect against evolving threats.

15 Hxxps://www.chainalysis[.]com/blog/ransomware-2024/#:~:text=Ransomware%20payments%20in%202023%20surpassed,ransomware%20is%20an%20escalating%20problem.

16 Hxxps://www.group-ib[.]com/media-center/press-releases/hi-tech-crime-trends-2023-2024/

17 Hxxps://edition.cnn[.]com/2023/07/06/tech/japan-port-ransomware-attack/index.html

18 Ibid

The Initial Access Broker market continues to play a key role in the ransomware ecosystem in the APAC region.

IABs have played a critical role in the maturing Ransomware-as-a-Service sector ecosystem by providing initial access for more sophisticated attacks. This was particularly evident with the advent of Big Game Hunting (BGH) ransomware tactics in 2019, when cybercriminals applying to be part of an affiliate scheme would typically have to prove pre-existing access to proposed targets. This market grew during the COVID-19 pandemic when the rapid adoption of remote working often meant it was applied without adequate cyber security measures, and during which time IABs began to target RDP and VPN channels.

In 2023, the IAB market in the APAC region shrunk slightly with a 3% decrease in accesses put up for sale (439, as opposed to 453).[19] The most affected sectors were the military and government organisations, followed by the manufacturing industry and financial services, largely in line with the ransomware attacks observed during this period. The most targeted companies were India, China, Indonesia. However, sub-regional differences were observed: the number of offers of listings in China grew by 66%, while the number for Vietnam decreased by 57%.[20] The most active individual targeting the APAC region, identified by a cybersecurity company was an individual using the deep and dark web forum name 'sganarelle' or 'SGL'. The individual was observed placing 140 listings for sale, with prices ranging from USD 100 to USD 5,000.

The IAB market targeting APAC also shifted in capability in 2023. Group-IB identified that numbers of listings to corporate networks with user privileges increased by 79%: this could potentially indicate that increased cyber security measures are making it more difficult for IABs to obtain elevated access privileges.[21]

The Ransomware-as-a-Service (RaaS) industry continues to thrive

In 2023 the RaaS market consolidated, as the number of active groups declined, likely due to the saturation of the market in previous years. Nevertheless, the market continued to present an active threat to the region.

Of the groups targeting APAC, Bitwise Spider (LockBit), Alpha Spider (ALPHAV/BlackCat) and Graceful Spider (Cl0p) were the most active groups, with the LockBit ransomware alone accounting for 34% of the attacks, and the ALPHAV/BlackCat accounting for 12% of the attacks. The Cl0p ransomware ranked third, accounting for 6% of all ransomware attacks in the region, based on the cases reported on DLS. This is aligned with global statistics: Bitwise Spider and Alpha Spider had large numbers of associates in 2023 and were responsible for the most significant number of attacks, while Graceful Spider specifically targeted Managed File Transfer Solutions, such as GoAnywhere, which allowed it to multiply its numbers of victims from a single compromise.[22]

The LockBit ransomware infrastructure was targeted in a global law enforcement operation in February 2024, which resulted in the disruption of some of its infrastructure, the release of key builders and decryption key, and the identification of key Bitwise Spider members. While the group claimed that the disruption was minor, it has had a key impact on the group's reputation, with some extant RaaS groups stating that they will not take on anyone who was a previous LockBit operator.[23] As such, LockBit infections are likely to decrease in 2024/2025, although many of the LockBit builders remain publicly available and have already been incorporated into new ransomware variants. Similarly Alpha Spider conducted an exit scam in March 2023, in which the group claimed to have been disrupted by the FBI and took all its infrastructure offline to avoid paying its associates their share of any ransom or extortion demand collected.[24] As such ALPHAV/Blackcat infections are also likely to decrease in 2024/2025.

19 Hxxp://www.group-ib[.]com/resources/research-hub/hi-tech-crimes-trends-2023-apac/

20 Ibid

21 Ibid

22 Ibid

23 Hxxps:///.trendmicro[.]com/en_us/research/24/d/operation-cronos-aftermath[.]html

24 Hxxps://arstechnica[.]com/security/2024/03/alphv-ransomware-site-claims-it-was-seized-by-fbi-researchers-suspect-22m-scam/

Nevertheless, other ransomware groups are likely to continue to target the APAC region. For example, in February 2023, Tonga's government-owned telecom provider, Tonga Communications Corporation (TCC), announced that it had suffered a ransomware attack. TCC, which is responsible for all fixed telephone lines and dominates the market for dial-up and broadband services with a 70% share, stated that the ransomware encrypted parts of its system. The attack was subsequently attributed to the Medusa ransomware, an RaaS ransomware which typically exploits RDP vulnerabilities.[25] The attack on TCC is part of a broader trend of cyber-attacks targeting small island nations, including recent incidents in Guadeloupe and Vanuatu, which have typically targeted government and telecommunications services.

Digital Extortion continues to form a key part of the ransomware threat.

Digital extortion involves a threat actor exfiltrating data prior to encryption, and threatening to make it public or sell the data that was exfiltrated. The tactic has been used since at least as early as 2019 and continues to be used by RaaS threat actors. It has subsequently evolved with triple extortion tactics, in which data is first exfiltrated and encrypted, following which the ransomware operator may then initiate a DDoS attack against the impacted organization if it refuses to engage on the ransom demand. Additionally, there is also quadruple extortion, where data is exfiltrated and encrypted, followed by a DDoS attack or threat thereof. The threat actor may then contact clients or employees of the victim company, either to extort individual ransoms or to cause reputational damage.

In 2022, data theft occurred in 70% of ransomware cases, and continued to increase in 2023.[26] Additionally, many groups are starting to work across a variety of RaaS programs, or to adopt publicly available builders of popular ransomware and combine them together to form new ransomware variants. For example, in 2023, 'GhostSec' a group which runs a RaaS program titled 'GhostLocker' which has previously targeted Indonesia, India, Vietnam, Thailand, and Indonesia, announced a partnership with a second group 'Stormous', which runs a 'StormousX' program. Since the collaboration cybersecurity researchers announced an increase in attacks.[27] Similar collaborations could achieve wider global targeting.

Recognizing this challenge, INTERPOL, alongside fifty countries who are members of the International Counter Ransomware Initiative, issued a joint statement in November 2023, strongly discouraging organizations from paying ransomware demands.[28]

Operation Synergia conducted by INTERPOL from September to November 2023, targeted phishing, malware, and ransomware attacks, identifying 1,300 suspicious IP addresses or URLs. Involving 60 law enforcement agencies from over 50 countries, the operation led to 31 arrests and the identification of 70 additional suspects, with 70% of command-and-control servers taken down and the rest under investigation. APAC countries made significant contributions, with Hong Kong, China dismantling 153 servers and Singapore taking down 86. The operation highlighted the effectiveness of international cooperation among law enforcement, national authorities, and private sector partners.

25 Hxxps://therecord[.]media/tonga-is-the-latest-pacific-island-nation-hit-with-ransomware

26 Hxxps://hkcert[.]org/blog/ransomware-trends-q2-2023-surge-in-attacks-across-asia-pacific-persistent-multiple-extortion-and-evolving-threat-landscape

27 Hxxps://www.techradar[.]com/pro/security/these-two-ransomware-giants-are-joining-forces-to-hit-more-victims-across-the-world

28 The statement is available on the official website of the Counter Ransomware Initiative: https://counter-ransomware.org/briefingroom/8ed7d1de-1a74-4a36-a2df-d5950624ebd8

Further Trends

KEY POINTS:

- In 2023, database leaks continued to pose a significant threat, with the majority of compromised datasets appearing on dark web forums.
- The market for selling initial access to corporate networks within the APAC region has continuously adapted to meet the evolving demands of threat actors
- Cybercriminals increasingly utilized cloud technologies to scale their criminal operations.

Data extortion attacks

In response to increased law enforcement action and focus on ransomware, many ransomware operators are moving away from ransomware attacks to conduct data extortion attacks, in which sensitive data is exfiltrated without the deployment of ransomware. This is both to increase the groups' abilities to obfuscate their TTPs, and to minimize disruption to the victim, perceiving that this is less likely to draw law enforcement attention. Data extortion attacks are also less logistically demanding as the threat actor does not have to develop or purchase a ransomware or maintain persistence in a compromised network while the data encrypts. In 2023, cyber security firm Cisco Talos stated that it had observed a 22% rise in encryption-less data extortion attacks in Q2 2023.[29]

Info stealers and Banking Trojans

Info stealers are a type of malware that typically exfiltrates data such as browser-stored credentials, bank credentials, crypto-wallet information and browser-stored information. They are typically operated as a Malware-as-a-Service, and often form part of more complex banking trojan operations. Computers with corporate access are particularly vulnerable, as they can serve as gateways for broader attacks on corporate networks. The risks associated with under-monitoring such systems include severe security breaches, data leaks, and large-scale cyberattacks. These credentials, frequently found in stealer logs, are traded on dark web marketplaces, often with partial masking to hide sensitive details, and can be used as a tool for initial access in a more sophisticated attack.

Data from Trend Micro's Smart Protection Network in 2023 indicates that ASEAN countries experienced the most significant impact from this type of malware. Among the sectors, the manufacturing industry was the most affected, followed by the banking, retail, and telecommunications sectors. The landscape of tools used by cybercriminals is also evolving. According to the major cybersecurity firms, Vidar has been surpassed by META and Raccoon stealers, with RedLine Stealer also among the top three most utilized information stealers.[30]

New banking trojans targeting the APAC region were also identified. In October 2023, Group-IB's Threat Intelligence team discovered a new banking Trojan named GoldDigger. Both GoldDigger and its variant GoldDiggerPlus specifically target users in Vietnam, while another variant, GoldPickaxe was subsequently developed for Thailand. GoldPickaxe can target facial recognition data, likely in response to the 2023 Bank of Thailand mandated use of biometric identity verification through facial scans for transactions exceeding 50,000 baht.[31]

29 Hxxps://www.crn[.]com/news/security/as-ransomware-gangs-shift-to-data-extortion-some-adopt-a-new-tactic-customer-service
30 Ibid
31 Hxxps://www.group-ib.com/media-center/press-releases/goldfactory-ios-trojan/

Compromised Card Data available increased in 2023.

Group-IB's global threat report identified an increase of approximately 64% in APAC-derived bank cards available on diverse channels such as deep and dark web forums, dedicated Telegram groups, and public data leaks from 2022.

This increase in compromised cards is primarily due to the escalated use of JavaScript sniffers (JS-sniffers) and the rising popularity of Underground Clouds of Logs. These tools have become more prevalent in cybercriminal activities, facilitating the theft and sale of sensitive card information.

The increase in compromised card data highlights significant vulnerabilities in digital financial security within the APAC region, and suggests that financial institutions must enhance their security measures to protect cardholder information from such pervasive threats.

WAY FORWARD FOR PROACTIVE ACTIONS AGAINST EVOLVING CYBER THREATS IN THE ASIA AND SOUTH PACIFIC REGION

The APAC region has committed to responding to the cybercrime threat and building resilience.

The responses from the questionnaire reveal several public awareness campaigns initiated across the APAC region. These campaigns aim to educate the public about cyber threats and promote best practices for cybersecurity. Key cybercrime legislations and initiatives include:

In Fiji, the Cybercrime Act 2021 aligns the nation with the Budapest Convention on Cybercrime, establishing robust legal measures to combat cyber threats. Fiji's government also emphasizes cybersecurity in national initiatives, regularly disseminating security advisories and awareness notices to ministries and agencies.

Kiribati has enhanced its cybersecurity framework with the establishment of a National CERT (Computer Emergency Response Team), which improves the government's response to cyber incidents. The Ministry of Information, Communications, and Transport (MICT) conducts regular cybersecurity awareness training for schools and communities. The annual MICT Day further focuses on addressing current cybersecurity issues.

New Zealand has made significant strides with CERT NZ's standardized reporting templates, which improve incident response capabilities. The nation also actively participates in the Cyber Smart Pacific Campaign, part of the PaCSON Awareness Raising Working Group, which promotes simple actions for individual user cybersecurity. Additionally, CERT NZ runs an annual Cyber Smart Week and has launched mini-campaigns such as "Two-steps, Too Easy" and "Big Password Energy" to enhance public cybersecurity awareness.

Papua New Guinea operates its National CERT within the National Information & Communications Technology Authority (NICTA), addressing cybersecurity threats and incidents. The Department of Information, Communication, and Technology (DICT) engages in various awareness-raising activities, including the Safer Internet Day initiative, which promotes safe internet practices among the public.

The Solomon Islands has developed a Security Operations Centre (SOC) within the Solomon Islands Government (SIG) to ensure compliance with security standards. The government raises cybersecurity awareness through regular email newsletters, phishing simulations, and participation in the PaCSON Cyber Smart Pacific Campaign.

In Australia, the Cyber and Critical Tech Cooperation Program (CCTCP) enhances cyber resilience in partnership with Southeast Asian and Pacific countries. The Cyber Safety Pasifika program, led by the Australian Federal Police, raises cyber safety awareness and educates vulnerable communities in the Pacific region.

In the Philippines, the PNP Anti-Cybercrime Group (ACG) hosted the AngelNet Summit 2024 on April 12, 2024. During the summit, representatives from law enforcement agencies and the private sector discussed their efforts in protecting online spaces, particularly women and children, from internet dangers. Two initiatives were launched at the summit: AlengPulis and the CyberSquad. The CyberSquad is an avatar group of ACG officers that was co-designed with children. Additionally, the PNP ACG conducts regular public awareness campaigns through its PNP ACG Facebook page: PNP Anti-CyberCrime Group. These campaigns

feature 'Katropa Tips'—cybercrime prevention tips aimed at reinforcing its cyber awareness efforts in addition to seminars and training sessions for the government, private companies, and schools.

In Singapore, the Cybercrime Awareness Week was aimed at cybercrime capacity building, training, fostering ties with foreign LEAs and private stakeholders as well as raising cybercrime awareness and encouraging the adoption of cyber hygiene among LEA officers and the general public. This was done through a series of events of activities such as symposiums, seminars (physical & virtual) and public outreach roadshows in collaboration with Neighbourhood Police Centres. Cyber hygiene education materials were distributed to members of the public during crime prevention roadshows, with stakeholders from SPF, Cyber Security Agency of Singapore (CSA), Cybersecurity companies as well as Foreign law enforcement agencies.

The APAC region has implemented various legislations and awareness campaigns to combat cybercrime. These efforts aim to enhance national and regional cyber resilience, promote safe cyber practices, and improve public awareness about cyber threats.

In light of the changing and dynamic landscape, and responses from the questionnaire, there are several key motives that countries can take forward:

1. **Enhancing proactive intelligence operations,** by priotizing the collection and analysis of external threat intelligence and using the INTERPOL ASPJOC desk to share crucial and timely intelligence.
2. **Strengthening cybersecurity frameworks and legislation,** by aligning law enforcement and judicial frameworks regionally.
3. **Investing in Law Enforcement Capabilities,** to keep pace with the rapidly evolving cybercriminal tactics.
4. **Fostering Regional and International Cooperation,** to strengthen joint actions against cybercrime.
5. **Promoting Digital Security Awareness and Education,** by enhancing public education campaigns.
6. **Streamlining Reporting and Response mechanisms,** by leveraging technology to improve the operational response capabilities.
7. **Expanding collaboration with the private sector,** including creating partnerships for enhancing technological capabilities, sharing threat intelligence, and fostering joint efforts in dismantling malicious infrastructures.

In conclusion, as cyber threats continue to evolve in complexity and scale, it is imperative for Asia & South Pacific countries to adopt a proactive and collaborative approach to enhance cyber resilience. By implementing these strategic recommendations, the Asia & South Pacific region will be better equipped to mitigate the impact of cybercrime and safeguard their digital landscapes for a secure and prosperous future.

INTERPOL CYBER CAPABILITIES DEVELOPMENT AND CAPACITY BUILDING IN ASIA AND THE SOUTH PACIFIC

Current INTERPOL Cyber Capabilities Development Efforts

INTERPOL supports the strengthening and sustaining of the capabilities and capacities of law enforcement to counter cybercrime and cyber-enabled crime in the ASP region via the implementation of two main project streams.

The **Global Action on Cybercrime Projects** (GLACY, GLACY+, currently GLACY-e), funded by the Council of Europe, aims to strengthen capacities of States worldwide to apply legislation on cybercrime and electronic evidence and their abilities for effective international cooperation in this area.

The main activities of the GLACY Projects include: (i) promoting consistent cybercrime legislation, policies and strategies, (ii) building the capacity of police to investigate cybercrime and engage in effective police-to-police cooperation, and (iii) enabling criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence. Several ASP Member Countries such as Fiji, Tonga, Timor Leste, the Philippines, and Sri Lanka participate in these activities.

The **Cybercrime Capabilities and Capacity Development Project (C3DP),** funded by the US Department of State, seeks to enhance the knowledge and skills of law enforcement to counter cyber threats and to foster regional cooperation against cybercrime in Southeast Asia. The key areas of work of C3DP are: (i) delivering targeted trainings that equip officers with relevant cybercrime investigation knowledge and skills to address key cyber threats – particularly in the specialized areas of malware analysis and cryptocurrency investigation, and (ii) forming Regional Expert Groups to lead knowledge exchange, information sharing, peer mentoring, and investigative assistance in the said specialized areas.

C3DP is also engaged in (iii) conducting table-top exercises to enable officers to test and improve their responses to transnational cybercrime, as well as in (iv) developing an e-learning on Obtaining Cross-border Electronic Evidence and knowledge products such as the Guidelines for Seizing Virtual Assets, to broaden reach of cyber capacity building to our 196 Member Countries.

INTERPOL complements these efforts with other ad hoc initiatives that focus on building member countries' skills on cybercrime investigation and open-source intelligence as well as on raising awareness on key diplomatic discussions. On this last matter, throughout 2023 INTERPOL has been proactively engaging with key international cyber policy and legislative processes, most notably the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC)[32] and the Open-ended Working Group on security of and in the use of information and communications technologies.[33]

INTERPOL Cybercrime Global Capacity Building and Training Needs 2024

INTERPOL's Strategic Framework 2022-2025 highlights the Organization's commitment to support Member Countries in developing capabilities that maximize the capacity, knowledge, and skills of law enforcement globally. Every two years, INTERPOL's Capacity Building and Training (CBT) Directorate conducts a Global Training Needs Assessment (TNA) which serves as a mechanism for collecting feedback from different law enforcement stakeholders of our Member Countries on capacity building and training effectiveness and gaps. The Organization uses this feedback to ensure that services we provide in this area remain relevant and responsive to the evolving challenges of transnational crime.

The 2024 Global TNA indicates a robust demand for capacity building and training in cybercrime. The top Respondents emphasize the need for skills in the following key areas: (i) cybersecurity breach responses, (ii) cryptocurrency investigations, (iii) advanced OSINT techniques, and (iv) investigative techniques and tools to support international cybercrime investigations.

32 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

33 https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021

There is a collective call from respondents for developing expertise in data streams/network analysis to deepen understanding of network infrastructures, strategies to enhance cybersecurity and threat response, computer and mobile forensics, and malware analysis. Skills in cryptocurrency investigations emerges as a pressing focus with respondents stressing the necessity for 'full training' in open-source virtual assets tracing and effectively requesting data from exchanges.

Respondents also indicate a keen interest in learning techniques for conducting covert investigations on digital platforms, safely navigating and investigating the dark web, as well as acquiring deeper knowledge on emerging technologies like artificial intelligence, and virtual and augmented reality. Finally, the importance of trainings for obtaining cross-border electronic evidence, understanding of the legal frameworks for cross-jurisdictional crimes, and leveraging INTERPOL's capabilities are also highlighted.

INTERPOL

INTERPOL is the world's largest international police organization. Its role is to assist law enforcement agencies in the Organization's 196 member countries to combat all forms of transnational crime. It works to help police across the world to meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. The Organization's services include targeted training, expert investigative support, specialized databases and secure police communications channels.

INTERPOL'S VISION: «CONNECTING POLICE FOR A SAFER WORLD»

INTERPOL's vision is that of a world where each and every law enforcement professional will be able to use the Organization to securely communicate, share and access vital police information whenever and wherever needed, to ensure the safety of the world's citizens. INTERPOL constantly provides and promotes innovative and cutting-edge solutions to global challenges in policing and security.

ABOUT INTERPOL CYBERCRIME PROGRAMME

In a dynamic digital age, where over half the global population is at potential risk from cybercrime, the INTERPOL Global Cybercrime Programme stands in support of the international law enforcement community. We are dedicated to developing and leading a global response to prevent, detect, investigate and disrupt cybercrime – with the ultimate mandate to reduce its global impact and protect communities for a safer world.

The INTERPOL Global Cybercrime Strategy focuses on four main objectives:

- Enable a proactive and agile posture in the prevention and disruption of cybercrime by developing an in-depth understanding of the cybercrime threat landscape through information sharing and intelligence analysis.
- Effectively prevent, detect, investigate and disrupt cybercrime that causes a significant harm on a national, regional and global scale by leading, coordinating and supporting member countries in transnational operational activities.
- Support the development of strategies and capabilities of member countries in combating cybercrime by cultivating open, inclusive and diverse partnerships and building trust in the global cybersecurity ecosystem.
- Promote INTERPOL's role and capabilities in shaping global security by engaging with international forums in the field of cybercrime.

We implement our Strategy and objectives via a simple and constructive delivery model, which consists of three core pillars:

- Cybercrime Threat Response: Addressing immediate and emerging cyber threats with a rapid and coordinated response.
- Cybercrime Operations: Implementing a regionally focused operational strategy to combat cybercrime effectively.
- Cyber Capabilities Development: Enhancing strategies and capabilities through innovative projects and platforms.

Underpinning these pillars is our extensive public-private partnership, fostering collaboration and leveraging collective expertise to fight cybercrime.

For any further information, you are encouraged to contact us at the following email address: EDPS-CD@interpol.int

ABOUT INTERPOL ASIA AND SOUTH PACIFIC JOINT OPERATIONS ON CYBERCRIME (ASPJOC)

Project overview

ASPJOC aims to strengthen the capability of Asian and South Pacific (ASP) national law enforcement agencies to prevent, detect, investigate, and disrupt cybercrime by:

- gathering and analyzing information on cybercriminal activity;
- promoting cooperation and good practices amongst Asia and South Pacific member countries;
- facilitating and carrying out intelligence-led, coordinated action against cybercrime.

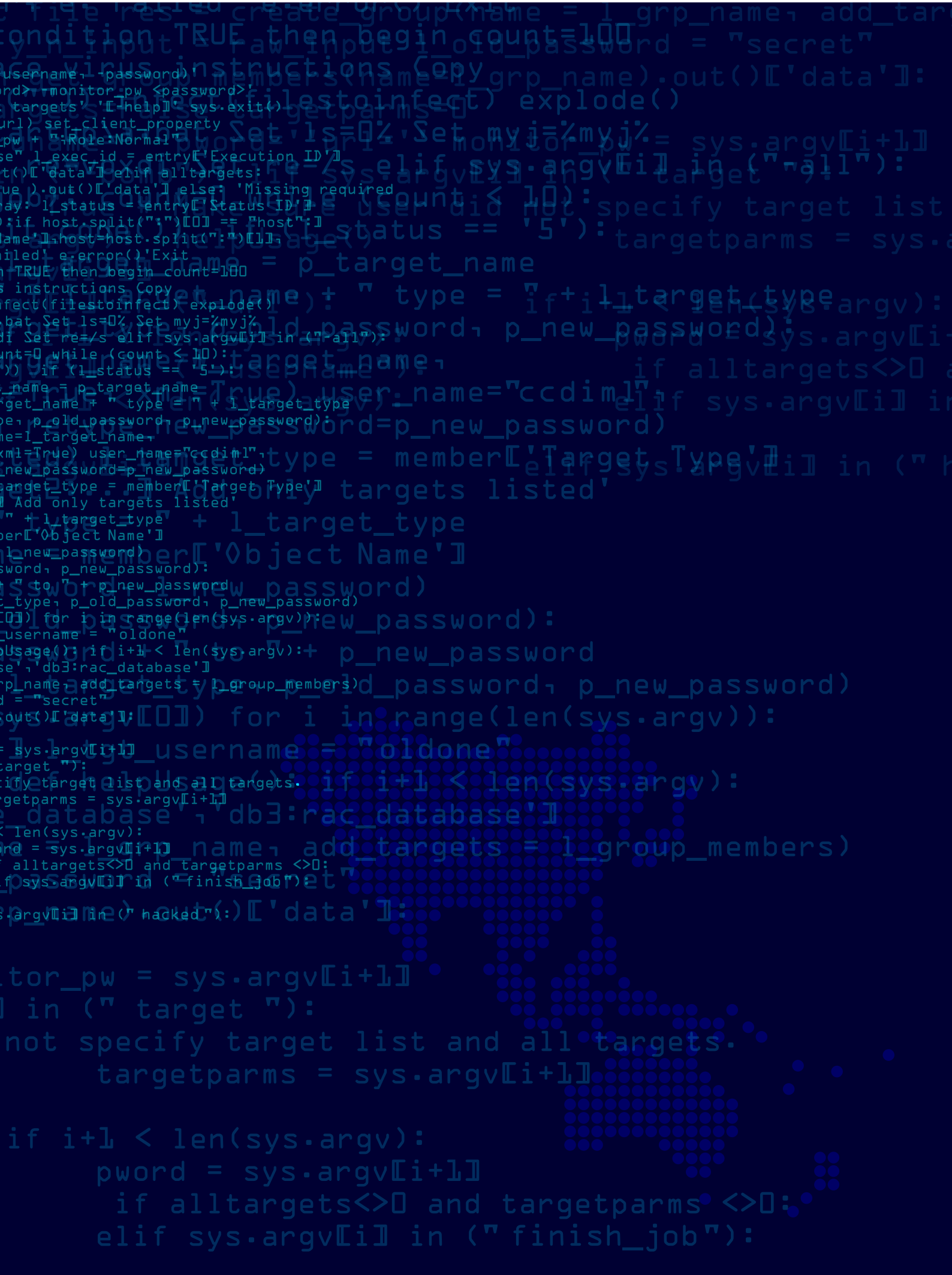
Phase 1 of the project runs from June 2024 to March 2025. It is funded by The United Kingdom Foreign, Commonwealth & Development Office and focuses on the following member countries: Brunei, Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand, Vietnam, Fiji, Kiribati, Marshall Islands, Nauru, Papua New Guinea, Samoa, Solomon Islands, Timor-Leste, Tonga, and Vanuatu

Project activities

INTERPOL implements ASPJOC through the INTERPOL Asia and South Pacific Cybercrime Operations Desk (ASP Desk). The ASP Desk supports member countries in the fight against cybercrime in four core areas of work:

1. **Analytical support and threat intelligence**
   Publishing and disseminating cyber threat assessments, advisories, and activity reports to equip ASP member countries with insights into the region's latest cyber threats and trends for resource prioritization and strategic decision-making.
2. **Awareness-raising campaigns**
   Providing practical guidance for detecting pertinent cyber threats, supporting law enforcement prevention efforts for improved operational outcomes, and promoting good cyber practices for individuals and organizations in the ASP region.
3. **Joint operational framework and working group meetings**
   Establishing mechanisms and platforms for secure and effective information sharing between ASP law-enforcement agencies, other intergovernmental organizations, and private sector partners in countering cybercrime.
4. **Investigative assistance and operational coordination**
   Driving intelligence-led operations, coordinated actions, and disruption efforts against cybercrime, related infrastructure, and its perpetrators operating in or affecting Asia and the South Pacific.

The ASP Desk also works in close partnerships with relevant regional stakeholders, the private sector, and other key partners to better assist law enforcement authorities in reducing the impact of cybercrime.



INTERPOL

ABOUT INTERPOL

INTERPOL is the world's largest international police organization. Its role is to assist law enforcement agencies in the Organization's 196 member countries to combat all forms of transnational crime. It works to help police across the world to meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. The Organization's services include targeted training, expert investigative support, specialized databases, and a secure police communications channel.

INTERPOL's VISION: «CONNECTING POLICE FOR A SAFER WORLD»

INTERPOL's vision is that of a world where each and every law-enforcement professional will be able to use the Organization to securely communicate, share and access vital police information whenever and wherever needed, to ensure the safety of the world's citizens. INTERPOL constantly provides and promotes innovative and cutting-edge solutions to global challenges in policing and security.