

Scam Compounds Brief

Issue No. 3 | April 2026



Foreign nationals arrested in Eswatini over “pig-butcher” scams.

The Scam Compounds Brief – Issue 3

Reporting period: 15 March to 14 April 2026

An evidence-based briefing on scam compounds and trafficking–fraud networks

About this Brief

The Scam Compounds Brief is an ongoing analytical series by Humanity Research Consultancy Limited (HRC) that examines the evolution of transnational criminal networks, primarily Chinese-speaking syndicates, operating scam facilities. Each issue identifies emerging operational patterns, enforcement actions, and structural shifts across affected jurisdictions.

By drawing on open-source intelligence — including content from niche social media platforms — the brief translates and contextualises information that is often inaccessible to international audiences. Rather than providing high-frequency updates, the series synthesises broader trends and surfaces specific leads that may not be fully documented elsewhere. This provides unique insight into the shifting dynamics of the online scam industry. The brief aims to promote greater visibility and scrutiny, equipping governments, law enforcement, researchers, and civil society with the evidence needed to address these evolving threats.

How to cite this publication

Chiang, M., Kasper, E. (2026, April). *The Scam Compounds Brief: Issue 3*. Humanity Research Consultancy.

Sources and verification note

This briefing draws on official statements, open-source reporting, court judgments, and monitored online channels, including Chinese-language sources and closed messaging platforms. Where information cannot be independently verified, it is indicated as reported or alleged. Identifying details are removed to protect individuals at risk.

Notice on access to sensitive content

For security and ethical reasons, direct links to social media posts that may indicate criminal activity are not published in this brief. Such materials can be made available upon request to law enforcement authorities or accredited researchers, subject to appropriate verification of credentials.

Content

1. Leadership Attitude.....	3
1.1 International.....	3
1.2 Cambodia.....	3
1.3 Myanmar.....	4
2. Raids, Escapes, and Deportations.....	4
3. Arrest, Prosecution, and Sentencing of Ringleaders.....	6
4. Scam Expansions.....	8
Sri Lanka.....	8
Eswatini.....	8
Myanmar.....	9
Laos.....	9



Figure 1. Seized phones handled by the FBI and the Thai police. Source: FBI.gov

1. Leadership Attitude

1.1 International

A new INTERPOL Global Fraud Taskforce, [Operation Shadow Storm](#), brings together 196 countries to target scam compounds, particularly in Southeast Asia, following a summit attended by 40 ministers, 100+ countries, and 300 industry leaders. The initiative responds to data showing that around two-thirds of scams affecting the UK originate overseas. Recent coordinated operations have already led to arrests and takedowns, including a case involving nearly £400,000 in losses, while the UK's wider fraud strategy is backed by £250 million and addresses a crime affecting 1 in 14 adults and 1 in 4 businesses.

The UK has intensified its response to scam compounds through [a new round of sanctions](#) targeting key infrastructure and financial enablers in Southeast Asia. Measures focus on entities linked to Cambodia's largest known compound, #8 Park, reportedly capable of holding up to 20,000 trafficked workers, as well as Xinbi, a major crypto-based marketplace used to sell stolen data and facilitate scam operations. These actions build on earlier UK and US sanctions that triggered over £1 billion in asset freezes and seizures and contributed to the closure of hundreds of scam centres.

1.2 Cambodia

Cambodia has [drafted its first law](#) targeting online scam centres, after vowing to shut them down by the end of April. "This law is the most important legal instrument for Cambodia in combating scams online, fighting money laundering and demonstrating that Cambodia is not a paradise or a safe haven for criminals," Information Minister Neth Pheaktra said in a statement. The new legislation approved by the Cabinet sets five to 10 years in prison and a fine of 500 million to 1 billion riels (\$125,000-250,000) for organising or directing a technology fraud site. In case of human trafficking or violence, detention or confinement, the penalties range from 10 to 20 years plus a fine of up to 2 billion riels (\$500,000).

Seven months into Cambodia's crackdown on scam compounds, [the crisis persists](#). Authorities report that around 50% of remaining operations have been shut down in 2025, but the total number of active compounds and victims remains unknown, with thousands of trafficked individuals still stranded. In 2025 alone, Cambodians lost approximately \$45 million to scams, with only \$20 million recovered. The industry has trafficked hundreds of thousands of foreigners, while law enforcement capacity remains limited at roughly one officer per 3,100 citizens. Despite high-profile asset seizures, including \$15 billion linked to Prince Bank, and increased enforcement efforts, large-scale operations continue, highlighting the gap between official claims and on-the-ground realities.

1.3 Myanmar

In March, the chief of the Thai armed forces arrived in Naypyitaw for [talks with junta leader Min Aung Hlaing](#), just as the U.S. denounced Myanmar as a key hub for online scam centres. Thailand has been unusually active in engaging the junta lately. On Feb. 25, Thai Air Force chief Sakesan Kantha met Min Aung Hlaing and Ye Win Oo in Naypyitaw, later inspecting an honour guard with his Myanmar counterpart Tun Aung. The Thai ambassador, a senior Thai army general, and Thailand's foreign minister have all held separate meetings with junta officials in recent weeks. The uptick in diplomacy comes as Thailand, Myanmar and China coordinate their own operations against scam-centre networks. Bangkok is also keen to reopen border gates—which have been shut for months due to clashes between junta forces and Karen armed groups around Myawaddy—for trade worth billions of baht.

2. Raids, Escapes, and Deportations

A growing job scam crisis has left [over 100 Kenyan nationals](#) trafficked into scam compounds in Myanmar, with 39 currently imprisoned for alleged involvement in illegal online operations. The case reflects a recurring pattern in Southeast Asia, where victims are recruited through fraudulent job offers, then coerced into scam activities and criminalised by local authorities.

Myanmar authorities continue to [repatriate foreign nationals](#) linked to scam operations, including the recent transfer of a South Korean citizen involved in telecom fraud. Between 30 January 2025 and 24 March 2026, authorities identified and detained 14,616 illegal immigrants, of whom 13,336 have been deported via Thailand, with 1,280 still awaiting repatriation. While these figures indicate large-scale enforcement efforts, they also reflect the significant volume of foreign nationals embedded within scam compound networks, as well as the reliance on cross-border cooperation to manage their removal rather than dismantling underlying operations.

[More than 100 Liberian nationals](#) have been trafficked into scam compounds in Cambodia after being recruited through fraudulent job offers, with victims reporting over a year of confinement and forced participation in illegal activities. Following a raid, many were released but remain stranded without basic support, facing potential 5–10 year prison terms due to immigration status. The case reflects a broader trend in which thousands of African nationals have been lured into Southeast Asian scam compounds in recent years. Limited embassy representation and capacity in the region have left many facing prolonged detention or homelessness after rescue, highlighting significant disparities in consular support and persistent gaps in victim protection and repatriation pathways.

[Vietnam has prosecuted 343 individuals](#) linked to scam compounds in Cambodia, following the repatriation of nearly 400 nationals. Many were recruited through fraudulent job offers and trafficked to sites such as Poipet casino complexes, where they were forced to carry out online scams. The case underscores the critical importance of victim identification and the non-punishment principle, as many individuals appear to have been coerced yet were still subjected to penalties, with over 330 fined for illegal border crossing.

[Authorities in northern Vietnam](#) have dismantled three scam rings involving 43 foreign nationals from South Korea, China, Malaysia, Myanmar, and Taiwan, exposing a multi-layered operation directed by Chinese masterminds based in Cambodia. The networks targeted victims in South Korea and China, generating at least 1.2 billion KRW (approx. USD 800,000), with proceeds channelled through Chinese-controlled accounts and wages paid in USDT.

[A recent case in India](#) highlights the continued globalisation of scam compound-style operations. Indian authorities dismantled a network operating from a villa in Lonavala, where four individuals were arrested in connection with a ₹97.7 lakh (approx. USD 117,000) investment scam. Investigations revealed that the operation was remotely controlled by handlers based in Hong Kong, with on-site actors monitored 24/7 via webcams to ensure compliance and rapid fund transfers. The structure closely mirrors Southeast Asian scam compounds, with a clear division between offshore controllers and local operators, the use of fake employment front companies, and the routing of funds through multiple bank accounts before conversion into cryptocurrency (USDT) and transfer abroad. This case underscores how the scam compound model is increasingly decentralised and portable.

Unverified testimonies from multiple sources allege abuse and extortion across several immigration detention centres in the region, with [Siem Reap](#) cited as one example. Reported conditions include confiscation of belongings, severe overcrowding (e.g. 22 people in a small room), and fees of up to USD 1,000 for basic rights such as phone access or release, alongside charges for food and medical care. While these claims cannot be independently verified, they point to broader concerns about post-rescue exploitation and corruption risks, where individuals exiting scam compounds may face further coercion within detention systems, undermining victim protection and recovery efforts.



Figure 2. Unverified testimonies described severe conditions at the Siem Reap immigration detention centre.



Figure 3. Unverified testimonies circulating online reported no resting facilities at Phnom Penh's immigration detention centre, where detainees are forced to sleep sitting upright.

3. Arrest, Prosecution, and Sentencing of Ringleaders

Lin Bingwen (林秉文), a Taiwanese organised crime-linked figure in the regional gambling industry, was [shot dead in Cambodia](#) after attackers fired 29 rounds, with his usual three bodyguards absent, raising suspicions of internal leaks. He was a key figure in Taiwan's "88 Club" money laundering case involving approximately \$680 million, which implicated over 20 senior police officials. The case underscores the overlap between cross-border gambling, illicit finance, and corruption, with clear parallels to the financial networks supporting scam compound operations in Southeast Asia.

According to an official Chinese government statement, on 1 April 2026, Chinese authorities, with support from Cambodian counterparts, [repatriated Li Xiong](#) (李雄), a core member of the Chen Zhi criminal network, from Phnom Penh. Li, identified as a former chairman of Huione (汇旺集团) under the Prince Group, is accused of involvement in illegal gambling, fraud, and money laundering-related offences.



Figure 4. Huione Pay store in Cambodia. Source: [Zhihu](https://www.zhihu.com).

In a [recent case](#) reflecting ongoing corruption risks around scam compound enforcement, two former Cambodian police officers have been tried for accepting \$774,000 in bribes to secure the release of 43 Thai nationals arrested in a 2025 raid on an online scam operation in Poipet. The individuals were ultimately deported, while the officers—who face 5–10 years’ imprisonment if convicted—have confessed. Four additional suspects remain at large, underscoring persistent integrity challenges within enforcement efforts.

[A South Korean court has sentenced a man](#) in his 20s to four years’ imprisonment for facilitating a victim’s recruitment into a scam operation in Cambodia and embezzling proceeds from a “borrowed” bank account. The victim, also in his 20s, was trafficked to Cambodia to work with a voice phishing network and was later tortured and found dead after failing to deliver expected funds. The case highlights the coercive and violent enforcement mechanisms within scam compound operations, as well as the role of external facilitators in source countries who enable recruitment and financial flows.

[South Korean police have arrested 42 individuals](#), including affiliates of a Cambodia-based criminal network, linked to a scam that defrauded over 1,400 victims of 6.7 billion KRW (approx. USD 5 million) through online secondhand trading platforms. The operation involved purchasing or coercively obtaining accounts from youths, including 19 minors, to facilitate fraud.

Taiwanese prosecutors have [indicted 10 individuals](#) for laundering more than NT\$33 billion (approx. USD 1.03 billion) in illicit online gambling proceeds through Macau casinos. The scheme relied on recruiting money mules, who used credit card prepayment mechanisms to inflate spending limits, then travelled to Macau to convert funds into casino chips and back into cash, earning 3–4.5% commissions. While investigators directly traced NT\$278 million through mule activity, the broader network handled significantly larger volumes, highlighting the scale and sophistication of cross-border gambling-linked money laundering. The case underscores the continued use of casino systems as laundering nodes, with structural parallels to financial flows supporting scam compound operations in the region.

4. Scam Expansions

Sri Lanka

China's embassy has responded to [recent arrests of online fraud suspects in Sri Lanka](#), noting that some scam networks have shifted into the country following crackdowns in established hubs such as Cambodia and Myanmar. The statement frames this as a displacement effect, where enforcement pressure pushes operations into new jurisdictions.

Eswatini

[In several recent operations in Eswatini](#), authorities arrested over [140 foreign nationals](#), including individuals from China, Brazil, Indonesia, Taiwan, Cambodia, Malaysia, the Philippines, and Nepal in connection with “pig-butcher” scam networks operating from locations converted into coordinated fraud centres. The cases reflect a clear continuation of scam compound modus operandi seen in Southeast Asia, where transnational groups operate from centralised locations to conduct long-term social engineering scams. Tactics included building trust over weeks or months, directing victims to controlled investment platforms, and using staged environments such as a fake police station to impersonate authorities and coerce payments.

Further investigations have revealed that members of the syndicate were not operating from a single location, but were instead [spread across different rented houses](#), mainly along the Mbabane-Manzini corridor. This suggests that the operational model developed in Southeast Asian scam compounds is not only persisting but also being exported globally, with mobile, multi-national teams replicating the same structures and methods in new jurisdictions.



Figure 5. Eswatini authorities arrested over 140 foreign nationals, including individuals from China, Brazil, Indonesia, Taiwan, Cambodia, Malaysia, the Philippines, and Nepal, in connection with “pig-butchering” scam networks. Source: [Times of Eswatini](#).

Myanmar

Despite ongoing conflict and targeted strikes, scam compounds in Myanmar’s Myawaddy region [continue to expand under DKBA-linked control](#). The number of scam sites has increased from 19 in 2025 to 22 by March 2026, with new compounds constructed in remote and forested areas to reduce vulnerability to attacks. Construction is highly organised and rapid, with facilities built within 2–4 months, supported by cross-border supply chains from Thailand, Chinese technical oversight, and locally produced materials. This expansion, even amid active fighting and international sanctions, underscores the industrial scale and adaptability of scam compound operations, which continue to grow rather than contract under pressure.

Laos

Unverified reports circulating in Chinese-language sources claim that in late March 2026, [three Chinese nationals were found dead in the Mekong River](#), including bodies showing signs of strangulation and concealment in metal containers, suggesting possible execution-style killings. These accounts link the incidents to escalating violence among criminal groups allegedly displaced by intensified crackdowns on scam compounds in Cambodia, with some networks reportedly moving into Laos and competing over territory and financial routes.

[Unverified reports](#) circulating in Chinese-language sources allege that on 8 April 2026, three Chinese nationals linked to a company identified as “Dajunfu Investment (达骏富投资有限公司)” were shot dead in Salavan Province, Laos, in what has been described as an execution-style killing on a remote road. The victims, reportedly aged between 29 and 36, were found beside a pickup truck with fatal gunshot wounds. However, the incident has not been reported by major Lao, regional, or international media outlets, and cannot be independently verified. This highlights the limited transparency and reporting environment in Laos, where serious incidents may go unreported. As such, the case should be treated with caution, though it reflects broader concerns about the potential spillover of transnational criminal activity into less-scrutinised jurisdictions.

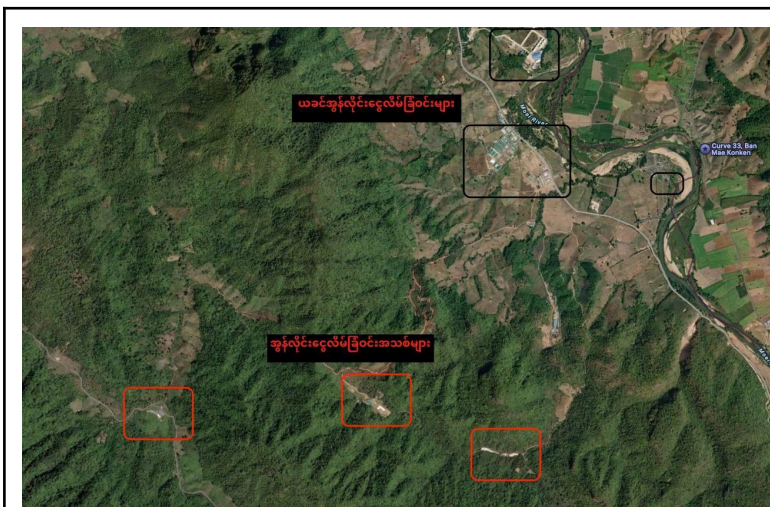


Figure 6. The number of scam sites in Myanmar’s Myawaddy region has increased to 22 by March 2026, with new compounds constructed in remote and forested areas to reduce vulnerability to attacks.



Figure 7. In late March 2026, three Chinese nationals were found dead in the Mekong River.