IJM

A Potential Nexus Between Forced Scamming and the Financially-Motivated Sextortion of Children

FUNDED BY:

Safe Online

Thomson Reuters™

Contents

Research Team

Chris Conrad, Eric Heintz, Marc Mace

Acknowledgements

IJM gratefully acknowledges the financial support provided for this research project by Safe Online. Safe Online is the only global investment vehicle dedicated to keeping children safe in the digital world. Through investing in innovation and bringing key actors together, Safe Online helps shape a digital world that is safe and empowering for all children and young people, everywhere. Learn more at https://safeonline.global/.

This project was also funded in part by the Thomson Reuters Social Impact Institute, which empowers nonprofit organizations around the world to drive meaningful change in the areas of access to justice, truth, and transparency. The Thomson Reuters Social Impact Institute, in collaboration with its people and partners, creates opportunities for innovation, community investment, volunteer impact, and sustainable corporate citizenship.

CyberTipline Report data used in the research project was provided by the National Center for Missing and Exploited Children.

Advertiser ID data used in the research project was sourced by NeXusData Solutions.

The opinions, findings, conclusions, and recommendations expressed herein are those of International Justice Mission and do not necessarily reflect those of Safe Online or the Thomson Reuters Social Impact Institute.

Key Definitions

Cyberscams

The use of internet technology such as websites, social media platforms, or messaging applications to defraud people.

CyberTipline Report

Reports received by the National Center for Missing & Exploited Children (NCMEC) related to child sexual exploitation, submitted by members of the public and by Electronic Service Providers (ESPs). NCMEC makes CyberTipline reports available to law enforcement agencies around the world, based on the apparent jurisdiction related to the reported incident.

Forced Scamming

Trafficking in persons for the purpose of exploitation of victims through forcing or otherwise compelling them to engage in cyberscams for economic gains of traffickers or exploiters.

Online Enticement

Involves an individual communicating with someone believed to be a child via the internet, with the intent to commit a sexual offense or abduction of the child. This is a broad category of online exploitation and includes sextortion.[1]

Sexual Extortion (or "Sextortion")

The blackmailing of a person using sexualized images of that person in order to extort sexual acts, money, or other benefits from them under threat of sharing the material without the consent of the depicted person.[2] When children are involved, sexual extortion is a form of child sexual exploitation.[3]

---

[1] *See* https://www.missingkids.org/theissues/onlineenticement
[2] *See* https://safeonline.global/wp-content/uploads/2025/04/Second-Edition-Terminology-Guidelines-final.pdf
[3] *See* https://www.missingkids.org/theissues/sextortion

Executive Summary

Through funding from Safe Online and the Thomson Reuters Social Impact Institute, International Justice Mission (IJM) conducted research to identify a nexus between two global, emerging crime types: the financially-motivated sextortion of children, and forced scamming — a form of labor trafficking that has emerged throughout Southeast Asia and is expanding to other locations. IJM's research project involved analysis of data from CyberTipline Reports submitted to the National Center for Missing and Exploited Children (NCMEC) between January 2022 and the end of August 2024, and internet infrastructure data tied to forced scamming locations in Southeast Asia. IP addresses from CyberTipline Reports categorized as "Online Enticement" were matched with IP addresses used by mobile devices in Southeast Asian forced scamming locations, resulting in matches through shared internet infrastructure with 18,017 CyberTipline Reports. Proximate internet connection timestamps were also compared to identify 493 CyberTipline Reports that are likely linked to these forced scamming locations. The study presents an approach that can be used by electronic service providers and law enforcement to identify specific locations and devices connected to sextortion incidents. It also underscores the importance of continued investigation into the intersection of financially-motivated sextortion of children and forced scamming.

Background

Cyberscams and Labor Trafficking in Southeast Asia

A combination of cyberscam operations and labor trafficking — what we refer to as "forced scamming" in this report — has emerged as a widespread and severe transnational crime throughout Southeast Asia. The crime involves hundreds of thousands of individuals from more than 60 countries around the world who have been trafficked into scam compounds and coerced into defrauding victims online.[4] This form of exploitation combines elements of human trafficking, cyber-enabled financial fraud, and organized crime. Forced scamming cases have been identified in Cambodia, Laos, Malaysia, Myanmar, and the Philippines, tied to criminal networks that operate with varying degrees of impunity. A recent UNODC report also details how this crime has started to spread to other regions, including Africa and Latin America.[5]

Forced scamming is rooted in the expansion of online fraud and scam operations, particularly those targeting foreign victims through investment and romance scams. The term "pig butchering" (杀猪盘, shāzhūpán) originated in China to describe long-term financial grooming scams where victims are "fattened up" before being defrauded. These operations have emerged in facilities throughout Southeast Asia, where the impacts of the COVID pandemic, weak regulatory oversight, and corruption facilitated their expansion.

To operate these scams, workers are lured from various countries, often recruited through fake job advertisements promising lucrative opportunities and targeted for their language, customer service, or internet technology-related skills. Upon arrival, they are transported to scam compounds, their passports are confiscated, and they may be subjected to threats of violence or physical and sexual abuse if they fail to meet scam quotas. Many are trained in psychological manipulation tactics to execute fraud schemes, which typically include romance scams and cryptocurrency investment fraud, fake loan and job recruitment scams, and impersonation fraud involving law enforcement or financial institutions. Those who resist or attempt to escape are beaten, resold to other scam operations, or subjected to other severe punishments, including torture and even killings.

REGIONAL HOTSPOTS OF FORCED SCAMMING INCLUDE:

- **Cambodia:** Scam compounds have been identified in former casino complexes and major development projects in Sihanoukville, Bavet City, Poipet, and other locations throughout Cambodia. Large, purpose-built complexes have also taken shape away from major cities. International pressure has led to limited crackdowns, but operations have persisted in many of the locations.
- **Myanmar:** Scam compounds have been identified in regions such as Myawaddy and Tachileik, along Myanmar's border with Thailand. These areas are controlled by armed groups and provide safe havens for scam syndicates, who are protected by local militias. Other compounds were known to operate along the border with China; however, these were largely shut down in late 2023. Activity is rumored to have begun again, but is likely outside the date range of this report.

---

[4] *United States Institute of Peace (USIP), "Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security". May 13, 2024,* https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security

[5] *United Nations Office on Drugs and Crime (UNODC), "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia". April 2025,* https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf

- **Laos:** Special economic zones, particularly the Golden Triangle, have become key centers for forced scamming.
- **The Philippines:** Cyberscam groups and labor trafficking cases have been identified in connection with Philippine offshore gaming operations (POGOs).
- **Indonesia & Malaysia:** Growing evidence suggests these countries are also home to forced scamming operations, especially in casino-linked facilities and urban fraud hubs.

Despite increasing regional and international attention, efforts to combat forced scamming have been inconsistent. Governments across Southeast Asia have conducted raids on scam compounds, but systemic corruption and political entanglements often limit meaningful enforcement. Meanwhile, organizations such as INTERPOL, the United Nations, and various non-governmental organizations have called for stronger cross-border cooperation to tackle forced scamming. Digital platforms and financial institutions are also under increasing pressure to enhance fraud detection measures to disrupt illicit financial flows. While some crackdowns have led to temporary disruptions, forced scamming continues to evolve, with syndicates relocating operations to new jurisdictions. The problem remains a significant human rights crisis and a major cyber-enabled crime challenge for the region and beyond.

IJM teams in the Southeast Asia region have been involved in addressing the issue of forced scamming since 2020. In Thailand, Cambodia, and Myanmar, IJM staff assist workers who have escaped or were released from scamming compounds after paying ransom. In collaboration with IJM's offices in the Philippines, Indonesia, and Malaysia, and with partners throughout the region, IJM ensures workers undergo a thorough victim identification process, addresses their immediate needs, and advocates for their rights within the justice system. IJM also works closely with relevant embassies and agencies to facilitate the safe and timely repatriation of survivors to their home countries and to open investigations and criminal prosecutions against traffickers.

Financially-Motivated Sextortion of Children

Sexual extortion (commonly referred to as "sextortion") involves the use of sexualized images of an individual to coerce them to engage in sexual contact, to provide additional sexual images, or to give up money or other benefits, typically under threat that the victim's images will be shared publicly. Financially-motivated sextortion is distinct from other forms of sextortion in that the primary goal of the perpetrator is financial gain. Typically, the perpetrator poses as a peer — often a young woman — and initiates contact through popular social media, messaging applications, or dating and gaming sites. After gaining the victim's trust, perpetrators manipulate the victim into sharing intimate images, which are then used to demand payment. This often includes threats to distribute the images to the victim's family, friends, or broader social network.

Over the past several years, the financially-motivated sextortion of children has emerged as a global and rapidly growing threat. According to Thorn's analysis of over 15 million CyberTipline reports submitted to the National Center for Missing and Exploited Children (NCMEC), the number of sextortion cases surged beginning in 2022, with an average of over 800 reports per week by 2023.[6] The Canadian Centre for Child Protection (C3P) also

[6] *Thorn and National Center for Missing and Exploited Children (NCMEC), "Trends in Financial Sextortion: An investigation of sextortion reports in NCMEC CyberTipline data". 2024,* https://info.thorn.org/hubfs/Research/Thorn_TrendsInFinancialSextortion_June2024.pdf

produced a report after conducting analysis of Reddit's r/Sextortion forum, and similarly found a sharp rise in victim disclosures of financially-motivated sextortion incidents, particularly among boys and young men.[7] The psychological toll and trauma inflicted on victims can be severe; in some cases, these incidents have led to suicide or other physical self-harm.

Perpetrators of financially-motivated sextortion often use multiple social media profiles and scripted messages to target numerous victims. Perpetrators are also known to use fake or AI-generated images to create these profiles, or have relied on hacked and stolen accounts of real users. One tactic involved cold-calling individuals on a WhatsApp video call, the caller displaying video or images of a nude individual, and then extorting the call recipient using screenshots taken during the call.[8] Another tactic involved a group of children in Australia who were targeted and told to send photos of their parent's ID cards, passports, or banking documents, instead of money.[9] Most of the perpetrators in financially-motivated sextortion incidents have been linked to criminal groups operating from Nigeria and Côte d'Ivoire, but some have also been linked to other countries, including ones in Southeast Asia.

In response to the global, emerging threat of financially-motivated sextortion, technology companies have sought to implement new safety features, such as stricter messaging settings for children and tools to detect interactions that indicate a risk of sextortion. Law enforcement agencies around the world have also issued public warnings and are attempting to investigate and disrupt sextortion networks.[10] Despite these efforts, there is a need for continued cross-sector collaboration, improved detection and reporting mechanisms, and global strategies to address the financially-motivated sextortion of children.

---

[7] *Canadian Centre for Child Protection, "An Analysis of Financial Sextortion Victim Posts Published on r/Sextortion". 2022,* https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

[8] *The Times of India, "Answering video calls from unknown numbers could mean falling into a sextortion trap: Tips to stay safe". April 10, 2023,* https://timesofindia.indiatimes.com/videos/in-depth/answering-video-calls-from-unknown-numbers-could-mean-falling-into-a-sextortion-trap-tips-to-stay-safe/videoshow/99362140.cms

[9] *Natasha Bita, "Overseas gangs target boys with sextortion". The Australian. November 9, 2023,* https://www.theaustralian.com.au/nation/overseas-gangs-target-boys-with-sextortion/news-story/a5953fe7205a2ee45dcc5fe38f00806e. *Accessed at* https://archive.is/ah2rR

[10] *Federal Bureau of Investigation (FBI), "Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes". June 5, 2023,* https://www.ic3.gov/PSA/2023/psa230605

A Potential Nexus Between Forced Scamming and the Financially-Motivated Sextortion of Children

A Potential Nexus Between Forced Scamming and the Financially-Motivated Sextortion of Children

As forced scamming and financially-motivated sextortion have emerged as growing crimes over the past several years, incidents reported in the media suggest a possible overlap between the two crimes. In early 2023, stories emerged from Northern Myanmar about labor trafficking victims forced to engaged in sex chat schemes with cyberscam targets.[11] Another example involved a group in Cambodia that would attempt to entice targets into an investment scam; if the financial investment scam was unsuccessful, the group would pivot to extortion via sexual images obtained through another type of scam. A victim of forced scamming from this group is quoted in the article: "The goal is to lure the targets into making large investments on a trading platform and if they don't agree, then the other way is to trick them into having video sex and forcing them to pay up."[12] Some reports have also indicated that women inside the scam operation are exploited and forced to participate in these schemes through the production of sexual content,[13] another example of how labor trafficking is involved in cyberscams operating from Southeast Asia.

While the majority of these incidents involved adults victimized by cyberscams, some of the incidents are reported to have involved children. One story involved requests for nude images from a 14-year-old girl, to be used as collateral for a falsified debt she incurred during a fictitious job application process.[14] Another involved two 12-year-old boys who were lured into online video chats and blackmailed with video recordings that showed them naked.[15] In cases involving children, however, it is not clear if cyberscams associated with forced scamming locations are intentionally targeting children, or if children are inadvertently targeted through broader, population-wide cyberscams.

---

[11] ဓဧယ, *"The hellish chambers of the Wa' region on the China-Myanmar border". Myanmar Now. February 28, 2023,* https://myanmar-now.org/mm/news/14085/

[12] *Bismee Taskin and Sharan Poovanna, "AI-aided sextortion, 'punishment rooms' & cyber slaves: Inside Cambodia's billion-dollar scam industry". The Print. April 1, 2024,* https://theprint.in/india/ai-aided-sextortion-punishment-rooms-cyber-slaves-inside-cambodias-billion-dollar-scam-industry/2022322/

[13] *Suneth Perera and Issariya Praithongyaem, "'My hell in Myanmar cyber slavery camp'". BBC. April 20, 2024,* https://www.bbc.com/news/articles/cw076g5wnr3o

[14] *Ronald Goh, "Singapore girl, 14, asked to send nudes to repay scam 'debt' up to $11,000". Yahoo! News. May 4, 2023,* https://sg.news.yahoo.com/singapore-girl-send-nudes-repay-scam-debt-091056961.html

[15] *Clifford Lo, "61 Hongkongers, including pair of 12-year-old boys, fall victim to 'sextortion' scams". South China Morning Post (SCMP). August 16, 2024,* https://www.scmp.com/news/hong-kong/law-and-crime/article/3274769/61-hongkongers-including-pair-12-year-old-boys-fall-victim-sextortion-scams . Accessed at https://archive.is/qCmqZ

Research

CyberTipline Reports

In partnership with the National Center for Missing and Exploited Children (NCMEC), IJM reviewed data related to over one million CyberTipline Reports (1,182,275) categorized as "Online Enticement" incidents, received by NCMEC between January 1, 2022, and August 31, 2024. Electronic service providers (ESPs) and members of the public use the CyberTipline to report suspected cases of child sexual exploitation. In conversation with NCMEC, Online Enticement was determined to be the category most likely to include incidents involving the financially-motivated sextortion of children. In total, the data reviewed included more than four million rows (4,178,519) and more than three million IP addresses (3,176,880), each row representing a combination of a masked CyberTipline Report ID, the date and time the report was received by NCMEC, an IP address used by a user account reported by the electronic service provider (ESP), and additional information about the type of IP address used, inferred location data, and date/timestamps associated with the user account's internet connection.

Figure 1 displays a timeline of these CyberTipline Reports based on the date the report was received by NCMEC, showing an overall increase in the number of CyberTipline Reports submitted over this period.

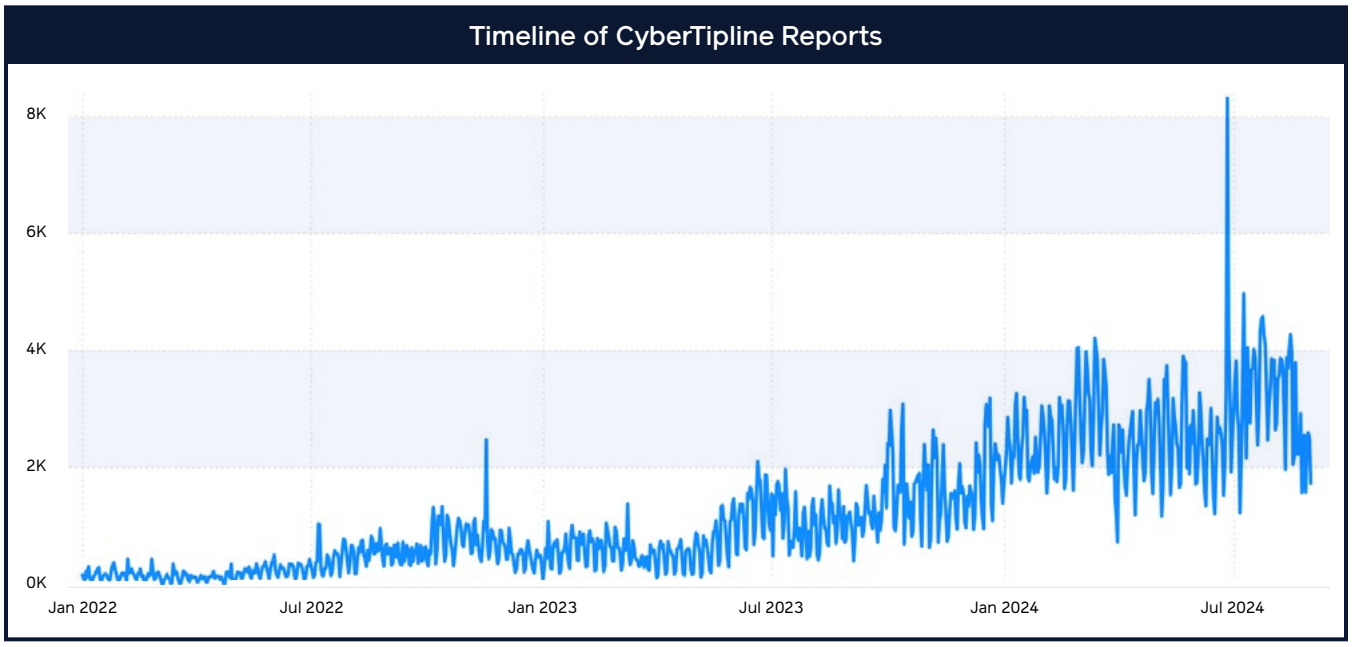


Figure 1: Timeline of Online Enticement CyberTipline Reports by date report was received by NCMEC (UTC).

Research began by filtering the data from NCMEC to identify only CyberTipline Reports that NCMEC had attributed to Cambodia, Laos, Myanmar, and Thailand – countries that are known to be associated with forced scamming locations. We included Thailand in the filtered data due to indications from IJM casework data and other research that some of the forced scamming locations in the region have relied on Thai internet service providers (ISPs) for their internet service. Our assumption is that although identified forced scamming locations have been in Myanmar, Cambodia, and Laos, a subset of these locations likely use IP addresses owned by ISPs in Thailand, and would therefore show up as attributed to Thailand in the CyberTipline data.

The filtered data included a total of 27,036 CyberTipline Reports and 85,585 IP addresses. The following is a breakdown of these results by country:

	Thailand	Cambodia	Myanmar	Laos
CyberTipline Reports	23,918	1,898	1,339	1,265
IP Addresses	75,558	3,713	2,410	2,019

*The counts of CyberTipline Reports and IP addresses for each country exceed the totals noted earlier, due to some CyberTipline Report/IP address rows in the data being attributed to multiple countries by NCMEC.

Figures 2-5 display the total count of Online Enticement CyberTipline Reports by month for the filtered countries. They show an overall increase in the number of CyberTipline Reports over the period of the study, with peaks throughout 2023 and in March 2024 for each country.

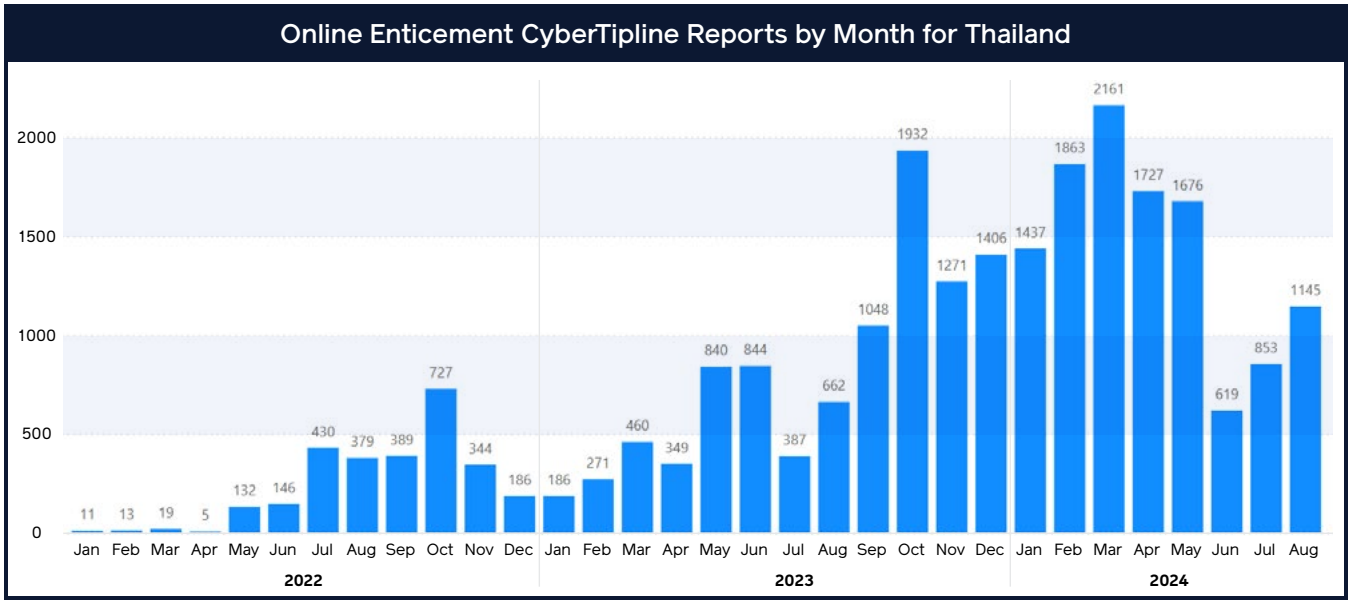


Figure 2: Monthly count of Online Enticement CyberTipline Reports for Thailand.

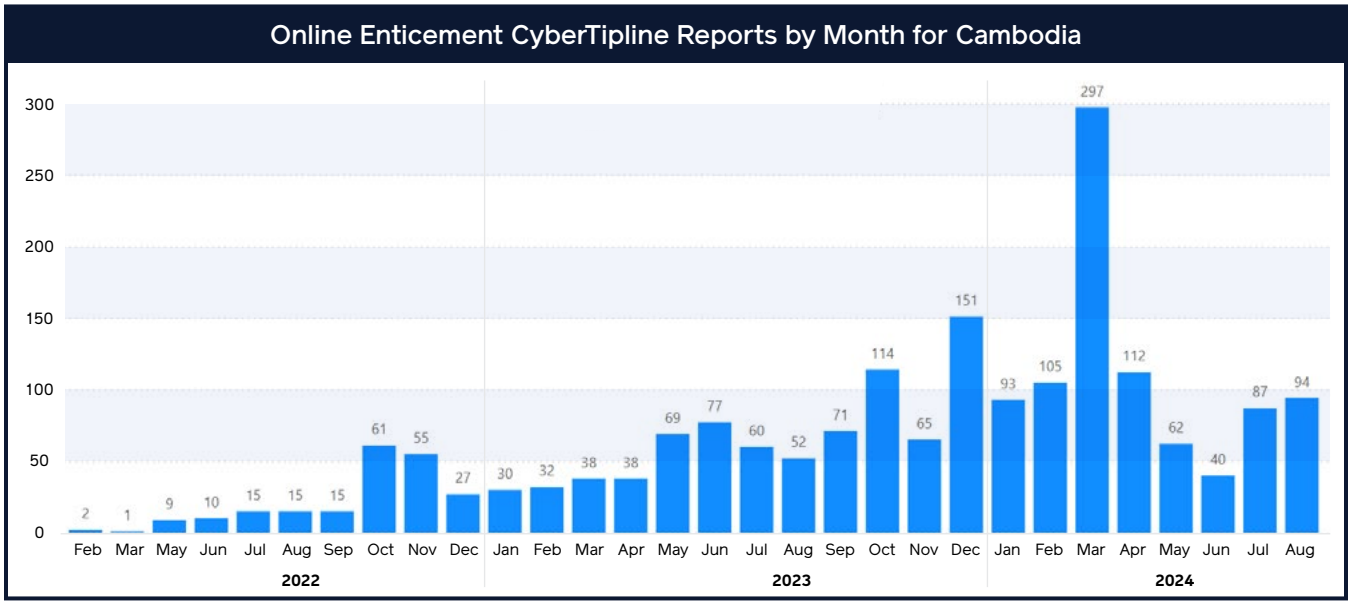


Figure 3: Monthly count of Online Enticement CyberTipline Reports for Cambodia.

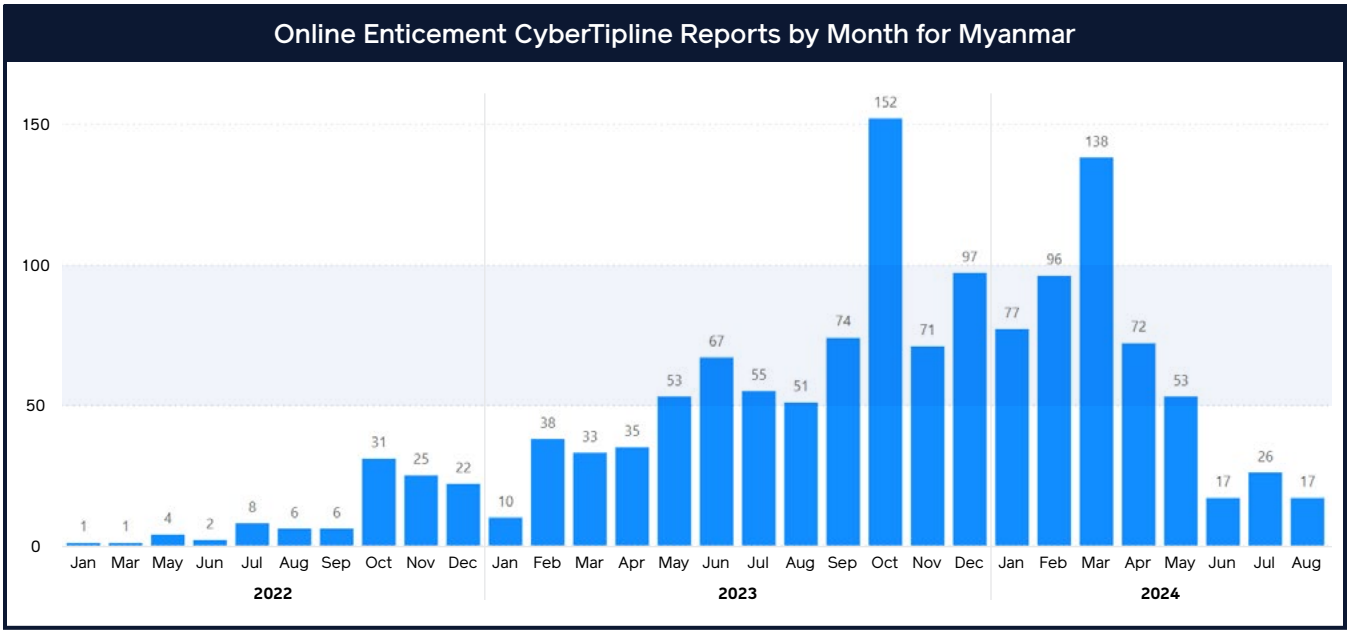


Figure 4: Monthly count of Online Enticement CyberTipline Reports for Myanmar.

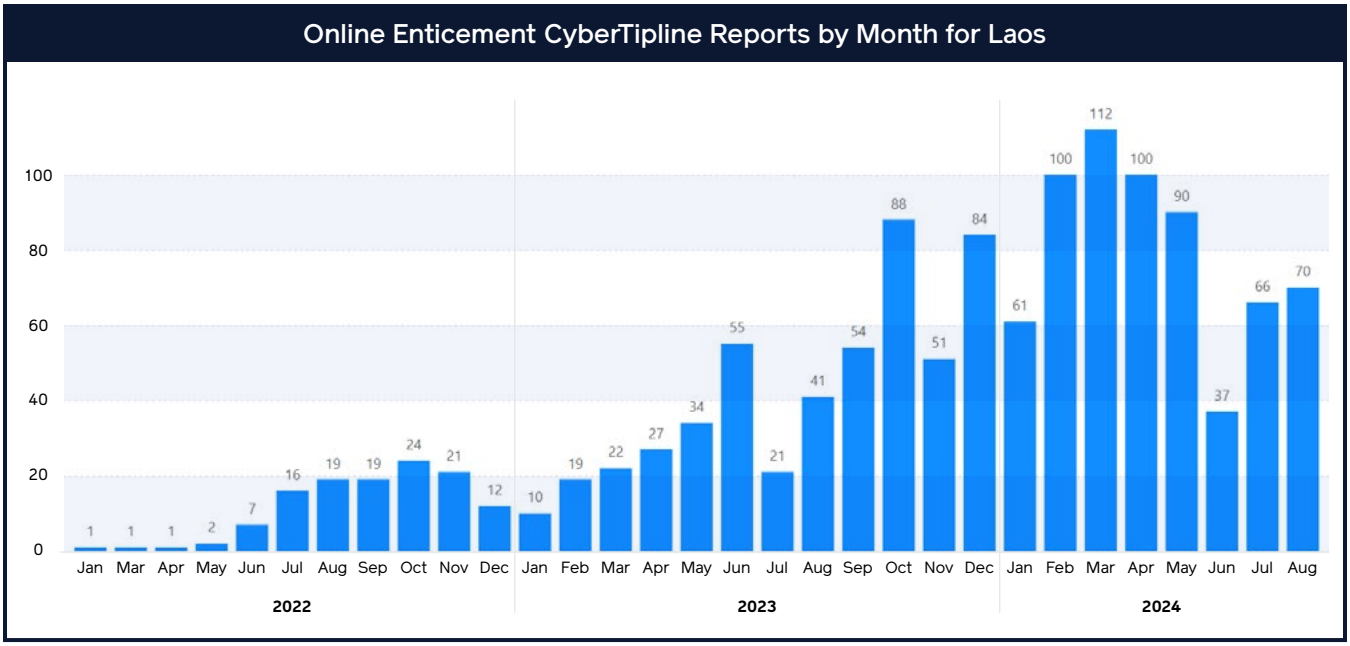
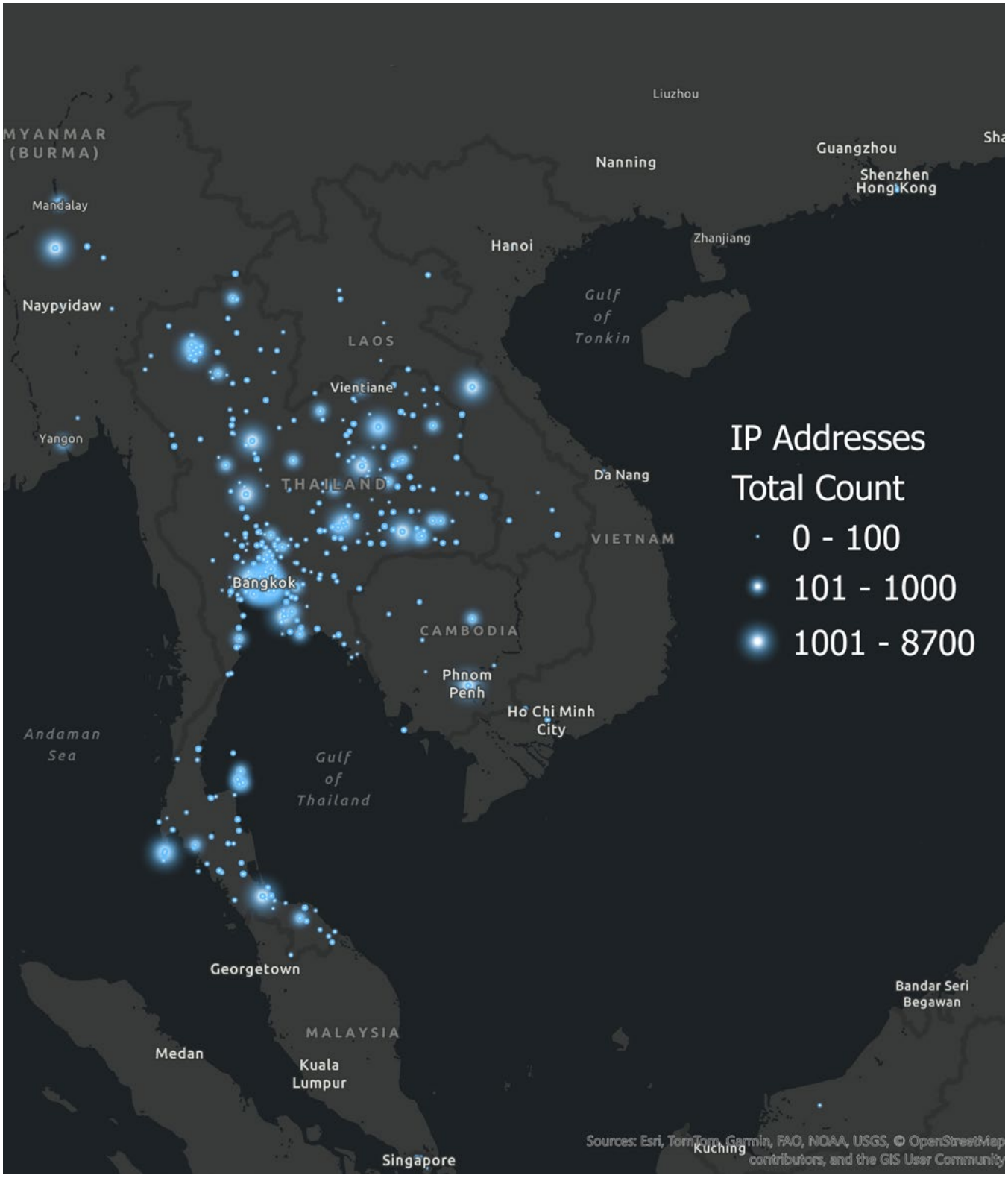


Figure 5: Monthly count of Online Enticement CyberTipline Reports for Laos.

IP Address Data

MaxMind's GeoIP lookup service was used to gather additional location and ISP information for the IP addresses in the filtered data. The geolocated IP addresses were then mapped using ArcGIS Pro software. Map 1 shows the geolocations with the total count of IP addresses attributed to each latitude/longitude.

Geolocation of Southeast Asia IP Addresses from NCMEC



Map 1: Geolocated IP addresses with total count for each latitude/longitude.

Finally, we examined the number of CyberTipline Reports tied to the ISP for each IP address. The following list includes the top 10 ISPs tied to Online Enticement CyberTipline Reports for the period of study:

The map of geolocated IP addresses and the associated ISP information shows that most of the internet infrastructure being used by online enticement suspects reported to the CyberTipline is in Thailand. For example, AIS, True, 3BB, DTAC, TOT, and CAT Telecom are all ISPs headquartered in Thailand (Metfone is headquartered in Cambodia, Cloudflare in the United States, and Star Telecom and Lao Telecom Communication in Laos).

ISP	CyberTipline Reports
AIS	12,853
True	11,476
3BB	5,354
DTAC	4,688
TOT	4,473
CAT Telecom	1,522
Metfone	946
Cloudflare	732
Star Telecom	691
Lao Telecom Communication	622

Advertiser ID Data

For the second phase of our research, we used advertiser ID data (also known as "ad-tech" or "Ad ID" data) as a more definitive means of finding links between CyberTipline Reports and forced scamming locations in Southeast Asia. Advertiser ID data is available from data brokers who provide commercial access to data collected from mobile device apps. These datasets include the advertiser ID of an Android or iOS device and location information (latitude/longitude data) from the device's GPS chip, connection to a cellular tower, or derived from an IP address. The datasets often also include an IP address and date/timestamp related to the device's internet connection.

IJM, through its casework and partnerships with other organizations, has confirmed the location of numerous forced scamming locations in Southeast Asia. For this study, IJM collected advertiser ID data from 44 of these identified forced scamming locations (27 in Cambodia, 16 in Myanmar, and 1 in Laos). Data collection resulted in over 300 million rows of data that included the advertiser ID of mobile devices used in these locations, the device's latitude/longitude, and the IP address and date/timestamp (UTC) of an internet connection by the device.

Microsoft Power BI was used to create a combined dataset with matches on the IP addresses from the collected advertiser ID data and the full set of NCMEC CyberTipline Report data (not filtered for Southeast Asia only) to better identify all potential matches between the two data sources. This new dataset included matches with 23,558 IP addresses from 18,017 CyberTipline Reports.

The next step involved identifying mobile devices that used an IP address close to the same date and time of the online enticement incident. The CyberTipline Report data included a column labeled "first_time_timestamp". Data in this field was blank for a portion of the CyberTipline Report data, but when available, provided information submitted by the reporting ESP about the first observed date/time the IP address was associated with a suspected user account. We chose to use the first_time_timestamp field with the assumption that it represented the date/time the suspected account was most likely created, while connected to the ESP's service using the IP address recorded. Many ESPs will flag and deactivate accounts that make use of virtual private network (VPN) or proxy services during account creation, so we decided the first_time_timestamp represented our best opportunity to identify an unmasked internet connection and accurate location data.

We adjusted the CyberTipline reports' date/timestamps to UTC time in Power BI and then calculated the difference in seconds between the first_time_timestamp field and the date/timestamp field in the collected advertiser ID data, filtering the data to examine a 12-hour (43,200 second) offset from the first_time_timestamp data. This provided us with a 24-hour period during which a mobile device located in one of the identified forced scamming locations was potentially tied to a CyberTipline Report via the matched IP address. The 24-hour period was chosen due to differences in the sources of the datasets, meaning that a device using a given IP address to create a user account on the service of a reporting ESP might be found in the advertiser ID data using the same IP address with a different online service, prior to or after creating the reported user account. Using this methodology and the 24-hour timeframe as our level of confidence, we identified 493 CyberTipline Reports likely tied to devices in 40 of the 44 identified forced scamming locations by 405 IP addresses.

	Locations	CT Reports	IP Addresses
Full period of study	44	18,017	23,558
24-hour timeframe	40	493	405

Figure 6 and the table below display the count of CyberTipline Reports tied to devices in the general area of interest for each of the identified forced scamming locations.

Area of Interest	Country	CyberTipline Reports
Bavet City	Cambodia	151
KK Park	Myanmar	116
Shwe Kokko	Myanmar	114
Tachileik	Myanmar	75
Sihanoukville	Cambodia	71
Poi Pet	Cambodia	52
Myawaddy	Myanmar	40
Golden Triangle SEZ	Laos	23
Chrey Thom	Cambodia	9
Saixigang Industrial Zone Project	Myanmar	6
Tai Chang	Myanmar	5
Bokor Mountain Compound	Cambodia	2
Long Bay	Cambodia	1
MDS Henghe Thmorda SEZ	Cambodia	1
Mongpauk	Myanmar	1

*The counts of CyberTipline Reports for each Area of Interest exceed the total noted earlier, due to some CyberTipline Reports being linked to multiple forced scamming locations.

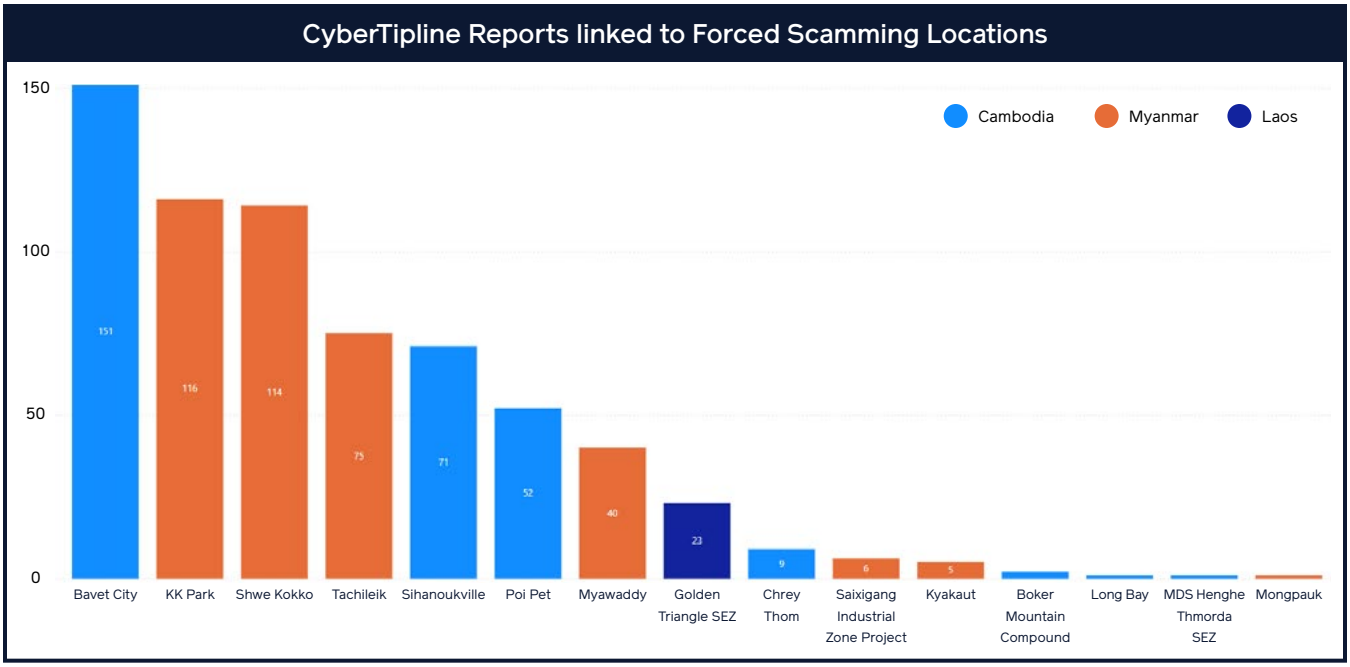


Figure 6: CyberTipline Reports linked to the general area of interest for known forced scamming locations via advertiser ID data (24-hr period).

Maps 2-6 display the advertiser ID data plotted on a map for the top five locations – Bavet City (Cambodia), KK Park (Myanmar), Shwe Kokko (Myanmar) Tachileik (Myanmar), and Sihanoukville (Cambodia).

Map 2: Bavet City, Cambodia - Advertiser ID location data linked to Online Enticement CyberTipline Reports via matched IP addresses and timestamp comparisons (24hr period).

Map 3: KK Park, Myanmar – Advertiser ID location data linked to Online Enticement CyberTipline Reports via matched IP addresses and timestamp comparisons (24hr period).

Map 4: Shwe Kokko, Myanmar – Advertiser ID location data linked to Online Enticement CyberTipline Reports via matched IP addresses and timestamp comparisons (24hr period).

Map 5: Tachileik, Myanmar - Advertiser ID location data linked to Online Enticement CyberTipline Reports via matched IP addresses and timestamp comparisons (24hr period).

Map 6: Sihanoukville, Cambodia - Advertiser ID location data linked to Online Enticement CyberTipline Reports via matched IP addresses and timestamp comparisons (24hr period).

Findings

Findings

Over the full period of the study (January 2022 through August 2024), we examined IP addresses shared between identified forced scamming locations in Southeast Asia and 18,017 CyberTipline Reports. When accounting for proximate timestamps between data submitted by the reporting ESP and advertiser ID data, we conclude that at least 493 of these CyberTipline Reports are likely connected to forced scamming locations. No exact timestamp matches were identified, possibly due to differences in the social media platforms and online services from which the two datasets were sourced. The collected data also indicated that devices in forced scamming locations (and the broader countries/region) frequently share IP addresses, likely due to limitations with IPv4 address technology. ISPs are known to implement network address translation (NAT) to overcome the challenges posed by a finite number of IPv4 addresses and a growing number of internet-connected devices.

The overall number of CyberTipline Reports linked to forced scamming locations, as identified through our research, suggests that cyberscams operating from forced scamming locations are likely not targeting children intentionally; rather, it is likely that children become victims through cyberscams that target broader populations. This is supported by anecdotal evidence from labor trafficking survivors who have recounted the types of cyberscams and individuals they were forced to target. However, locations identified through the research with a higher count of associated CyberTipline Reports (such as Bavet City and Sihanoukville in Cambodia, and KK Park and Shwe Kokko in Myanmar) are worth investigating in more depth, to determine if organized crime groups operating from these locations are using sextortion as a tactic and have chosen to target children.

An examination of the timeline and ISPs associated with the 493 CyberTipline Reports reveals several insights, when compared with the previous analysis of Online Enticement CyberTipline Reports filtered for Cambodia, Laos, Myanmar, and Thailand. Figure 7 displays the monthly count of CyberTipline Reports linked to Forced Scamming locations.

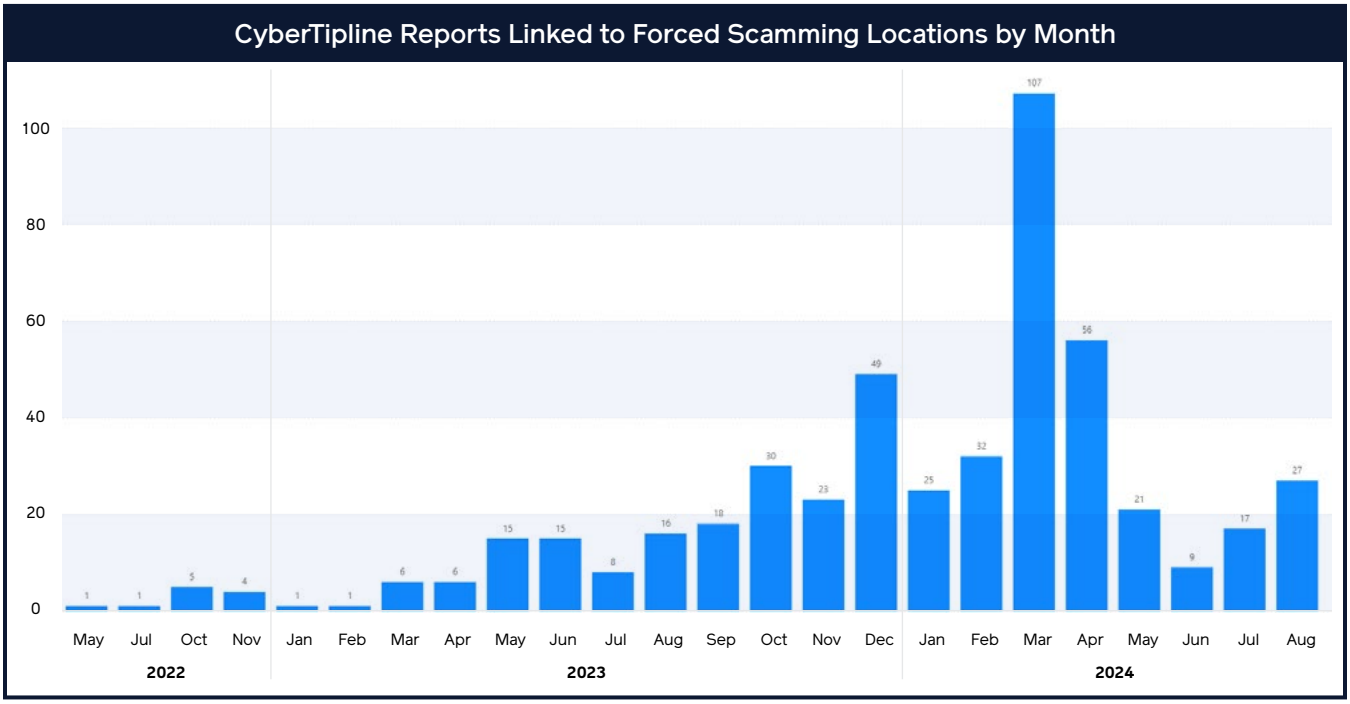


Figure 7: Monthly count of Online Enticement CyberTipline Reports linked to Forced Scamming locations.

There is an overall upward trend in the number of reports until March 2024, when the monthly count peaks. This peak is followed by a decrease from April to June 2024. We see the same peak in March 2024 and following decrease from April-June 2024 in the CyberTipline Report data for Cambodia, Laos, Myanmar, and Thailand, shown in Figures 2-5 earlier in the report. The causes behind this peak and drop-off shown in the data are unknown, but worth more investigation into what factors may have contributed to the decline.

We also examined the ISPs associated with the IP addresses in the matched data. The following list displays the top ISPs:

ISP	CyberTipline Reports
Cloudflare	124
Metfone	95
Smart Axiata	74
True	70
Cellcard	16
Star Telecom	15
AIS	14
Telnet Co.	10
Viettel Group	10
Angkor Data Communication	8
DTAC	8

Some of the same Thai ISPs are among the top 10 that were also observed in the unmatched data (i.e., True, AIS). However, Cloudflare tops the list within the matched data. The IP addresses associated with Cloudflare were used across multiple forced scamming locations in Myanmar – particularly Shwe Kokko, KK Park, and Tachileik.

Overall, simply relying on location information contained in the CyberTipline Report – or the IP address and its associated ISP or geolocation data – is not sufficient for establishing the true whereabouts of an Online Enticement incident. When combined with the advertiser ID dataset, the matched data reveals a potential nexus with forced scamming locations that would not otherwise have been known. For example, among the 493 CyberTipline Reports linked to forced scamming locations, we found that 129 of them were attributed to different countries within the NCMEC data (including 98 of these attributed to Thailand). Figure 8 shows these counts by country.

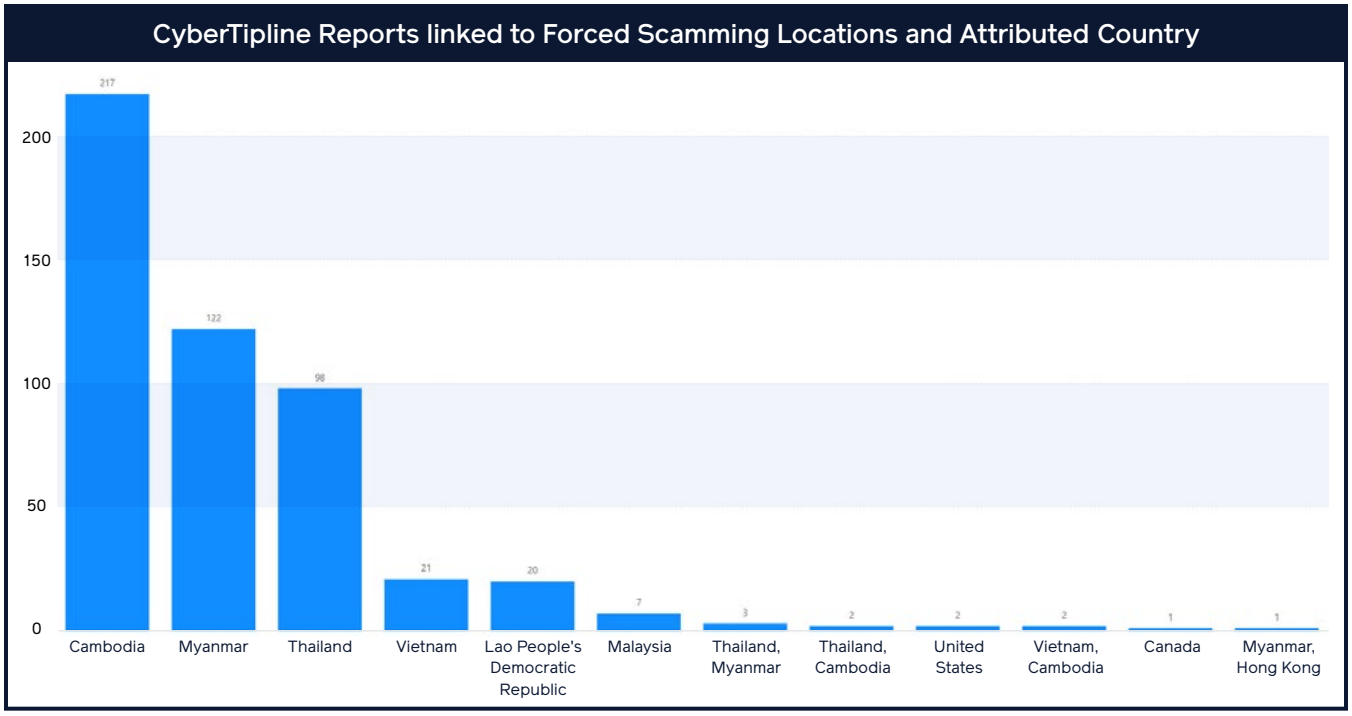


Figure 8: Count of Online Enticement CyberTipline Reports linked to Forced Scamming locations, by Country of Attribution.

Discovery of Additional Forced Scamming Locations

Working with advertiser ID data allowed us to also conduct searches using IP addresses and date/timestamps from the CyberTipline Reports to identify additional locations suspected of forced scamming. Through this approach, we identified locations in Cambodia and Myanmar that are potential sites of forced scamming, based on comparison with similar known forced scamming locations. The search process also identified 62 more CyberTipline Reports that may show links between sextortion of children incidents and forced scamming. These reports were associated with more than one device at the additional locations, and the devices examined did not move outside the vicinity of the location or appear elsewhere during a 24-hour time period. Locations also included links to more than one CyberTipline Report.

Maps 7 and 8 are examples of two of the locations identified using IP address and timestamp data from the CyberTipline Reports.

Map 7: Poi Pet, Cambodia – Additional location suspected of forced scamming, based on mobile device activity and CyberTipline Report data.

Map 8: Myawaddy, Myanmar – Additional location suspected of forced scamming, based on mobile device activity and CyberTipline Report data.

Limitations

Limitations

While our analysis shows a small proportion of CyberTipline Reports associated with forced scamming locations in Southeast Asia compared to the overall number of Online Enticement reports for the period (493:1,182,275), we suspect this constitutes only a portion of the potential matches. It is very likely this study undercounts the scale of the nexus between CyberTipline Reports and forced scamming locations for the following reasons:

- The Online Enticement category from NCMEC does not include all sextortion cases reported to NCMEC. For example, the vast majority of reports made by ESPs to NCMEC are categorized as CSAM (Child Sexual Abuse Material). A similar replication of our research methodology using this category of reports would potentially reveal additional connections to forced scamming locations.
- IP addresses flagged as "Proxy/Tor nodes" were excluded by NCMEC during the data pull. NCMEC was unable to estimate the quantity of data that was filtered out, which means there are likely additional matches that our research could not identify.
- Our collection of advertiser ID data is not a comprehensive picture of all internet-capable devices used at the forced scamming locations we examined. It is very likely that additional devices such as computers, cloud-based systems, or other devices exist beyond the scope of the advertiser ID data collected and may be tied to CyberTipline Reports. Additionally, the data sources for advertiser ID data are limited to specific apps and may not include the exact social media, messaging, dating, or other apps being used in sextortion cases and reported to NCMEC.

Finally, the CyberTipline Report data from NCMEC represents only a portion of actual online enticement cases that likely occurred during the period of study. Sextortion incidents are known to occur on other social media and messaging services that do not submit reports to NCMEC. Forced scamming operations in Southeast Asia target scam victims on a wide variety of social media platforms, messaging applications, and online dating services, which means that financially-motivated sextortion of children incidents may occur on these other online services but are not reported to NCMEC.

Recommendations

Recommendations

The findings of our study show a nexus between the financially-motivated sextortion of children and forced scamming locations in Southeast Asia. Continued study and investigation of the nexus will require further analysis of locations associated with forced scamming and collaboration between public institutions and private industry to detect, report, and investigate incidents.

For other investigators or researchers who may be interested in replicating this study, the data matching process could include more recent CyberTipline Report data, and include Proxy/Tor IP address data that was left out of our research. This would likely reveal new locations associated with forced scamming, and identify additional reports linking CyberTipline Reports to forced scamming locations.

For ESPs seeking to identify sextortion incidents on their platforms, we recommend cross-referencing user activity with IP addresses and locations tied to forced scamming hotspots, such as Myanmar's border regions, cities in Cambodia, and special economic zones throughout the region. Reported user accounts should also be examined for indicators of other fraud and scam activity, including activity that may not display sextortion as a tactic. CyberTipline Reports submitted to NCMEC should also include additional location information and date/timestamps associated with user account activity or IP address information, to better aid law enforcement in carrying out investigation of child sextortion incidents.

For law enforcement agencies or investigators of sextortion incidents, we recommend examining these incidents for evidence of any links to forced scamming locations in Southeast Asia. When looking at CyberTipline Reports or other sextortion incident information, the use of repeated phrases or scripts may be an indicator of organized scamming activity and links to forced scamming locations. References to cryptocurrency addresses or financial investment platforms may also be indicators. Also consider that some of the suspects involved may be victims of labor trafficking, coerced into sextortion schemes as part of broader scam operations.

For law enforcement agencies or investigators of forced scamming, we recommend examining evidence for indicators of sextortion as a tactic, such as the use of sexually explicit scripts or imagery. Scam compounds that show links to crimes against children should open the door for wider enforcement action against these locations, due to the fact that children are at risk if they are left continuing to operate.

International Justice Mission (IJM) is a global organization that protects people in poverty from violence. IJM partners with local authorities in 33 program offices in 19 countries to combat slavery, violence against women and children, and police abuse of power against people who are poor. IJM works to rescue and restore victims, hold perpetrators accountable, and help strengthen public justice systems.

IJM

International Justice Mission

PO Box 90580 | Washington, D.C. 20090

844.422.5878 | IJM.org