global china pulse.

01
24

SCAMMED: DISSECTING CYBER SLAVERY IN SOUTHEAST ASIA

This text is taken from *Global China Pulse*: Volume 3, Issue 1, 2024.

From Hacker to Cyber Threat Investigator

Hiếu Minh Ngô, once convicted and jailed for hacking activities, has now dedicated himself to raise awareness about online scams and shut down the perpetrators.

Investigating Cyber Threats: A Conversation with Hiếu Minh Ngô

Mark BO,
Hiếu MINH NGÔ

Hiếu Minh Ngô, also known as Hieu PC, was born in Gia Lai, Vietnam. His involvement in hacking led him down a path of identity theft and cybercrime, resulting in his arrest and a 13-year prison sentence in the United States for stealing and selling the data of more than 200 million Americans. Upon completing his sentence and returning to Vietnam in 2020, Ngo focused on improving cybersecurity practices and fighting against fraud. He joined Vietnam's National Cybersecurity Center as a cybersecurity expert and later launched Chongluadao, an initiative to protect internet users from scams. He is currently employed part-time at TRM Labs, serving as a cyber threat investigator.

Mark Bo: Can you tell me a little about your background and the nature of your work as it relates to the issue of cyber scams originating in Southeast Asia?

Hiếu Minh Ngô: I've been looking at the industry since 2020, conducting threat analysis and investigating how it works. When I started to see reports about the spread of scams originating from Southeast Asia, I wanted to know what was really happening. The deeper I got into this, the more I realised that this was a whole different level. We're talking about an entire economy, a scam pandemic that can target anyone online.

I decided then to create a new anti-scam organisation called ChongLuaDao. Since then, I've been collaborating with many anti-scam groups and companies around the world. I've learned that while we can slow the scammers down, disrupting them is very difficult. I work with other specialists to locate scam websites and get them shut down. The sooner we can get them shut, the better for everyone. We cannot stop them, and they can easily create new platforms, but this slows them and buys us time to raise awareness and educate people on how to spot and avoid scams.

I collaborate with law enforcement and, if we get lucky, we can track down the scammers. If they are in Vietnam the police may be able to apprehend them, although mostly the operators are based in neighbouring countries. It is more common that we track down people in Vietnam who are involved in laundering the proceeds of the scams conducted in places like Cambodia and Myanmar.

This is my job, but it is also personal. I also want to help the victims. Back in the days when I was a hacker, I hurt people, I stole data and identities. Now I am still hacking, but I hack the scammers, and I feel happy as I am able to help police in Vietnam and some international law enforcement agencies to gain deeper insights into the industry and the techniques they use. This has also led to some arrests, and I'm very happy about that. Unfortunately, it is very hard to help people get their money back. Usually, once it's gone, it's gone.

MB: Is the Vietnamese public targeted by the industry? How big a role do Vietnamese nationals play in the regional scam workforce?

HMN: Online scams are targeting many people in Vietnam, but the whole world is affected. Studies have found that a huge number of people in Vietnam are targeted by scams. One found that 70 per cent of people surveyed in Vietnam reported receiving some kind of scam message every month, usually by phone call, SMS, message app, or social media.

When we look at this industry, we need to think about two main groups of victims: the people being scammed, and those who are cyber slaves, lured into the compounds, trapped, and forced to work.

I am contacted daily by scam victims. My organisation has set up community platforms with over 20,000 members where people can send information if they have been scammed. They can also share information about websites or messages that they have received and check whether they are scams. We record this information and advise people to be cautious if we identify a potential scam. We are now working on a new website to handle this service and encourage victims to report more. The more data we have, the easier it is for us to help and to map the trends.

I am also often contacted by people trapped inside the compounds and stay in touch with them when I can. Some can provide information, and I have been able to support the rescue of some by connecting them with anti–human trafficking groups and law enforcement. Recently, I helped a Vietnamese man trapped in Myanmar, although he still had to pay a ransom to get out. He was able to get to Thailand, but we had to support him financially to pay immigration fines and purchase a flight back to Vietnam. It is very dangerous to contact people from inside the compounds though, and generally the most common way to get out is by escaping or paying the ransom.

In my research, I have found that the bosses are usually Chinese or Taiwanese, rarely Vietnamese, although Vietnamese nationals play a major role. They may be part of the scam workforce, sometimes working under conditions resembling modern slavery. Some hold management roles, and often these people climb to a management position after working in the industry long term, but usually the more senior people are Chinese.

Raising Awareness
Hiếu Minh Ngô at a TEDx talk in 2023. Source: *TEDx Talks*.

They also play a role in human trafficking, approaching people via social media or Telegram and then luring them through legitimate channels or smuggling them to neighbouring countries. There are some creative ways used to target people—for example, 'shark lenders' run websites that provide loans to desperate people with very high interest rates. When they can't pay them back, their debt accumulates, then the shark lenders share their information with recruiters, who then approach them with offers of high-paying jobs, which they are more likely to accept.

IT support is very important. Technicians manage the website and applications and make sure they are running well, protect them from hacking, and generally make sure their infrastructure is secure. Marketing and search engine optimisation (SEO) specialists are also important. Their job is to make sure that scam websites and applications are prominent in search engine results, which increases the chances that victims will see the operator's online gambling and scam sites.

The scam industry needs a large amount of mule bank accounts to move stolen money around. To do this they steal accounts from people, but also buy or rent accounts. They target students, young people, or people with low incomes and pay them to open a bank account or virtual currency wallets and hand over the details. We've also seen people set up companies that are then used to register bank accounts to launder funds. Sometimes a single company will open hundreds of accounts.

Vietnamese nationals are involved, but these operations are multinational. In some cases, a scam compound will have multiple apartment-style buildings with many floors. You might find Africans in one office or on one floor, Vietnamese in another, Indians in another, and so on. These places are highly secure and controlled, with multiple gates and security guards to make sure nobody can escape. The industry needs workers from different countries, and it works with traffickers from those countries, wherever they are.

MB: What do you think are the main challenges faced by those trying to combat the industry?

HMN: The operators are increasingly sophisticated, and we are chasing a moving target.

Data are a key foundation of the industry. Scam operators obtain personal data and use them to target people, and they can easily purchase this from many online marketplaces. Hackers harvest data and sell it via Telegram groups and other places. They are also able to steal people's identities and use this to target victims, tricking them into giving up information or money. Preventing this harvesting and trading of personal data is a major challenge.

Malicious websites and apps are also a huge problem. Scam websites impersonate or hack government platforms. Scammers can build websites rapidly, often copying legitimate websites. When they are shut down, they quickly set up a new one. With SEO professionals working for the scam operations, they can make their platforms appear high up in Google searches, so people assume they are legitimate. Also scam texts and messages can include malicious links, sometimes pretending to be from an official agency or bank. Once clicked, these links download malware and the scammers can get full access to a device. I've traced a lot of these fake platforms and can see in the code they usually use Chinese text, meaning the developers are most likely Chinese.

This kind of technical work is often outsourced, and website design and maintenance, hacking services, and personal data can all be obtained by scam operators quite cheaply. It is also possible to buy social media accounts that have been stolen or curated, and scammers use these identities to trick people into thinking they are real people. If you look on Telegram, you can find hundreds of groups selling all these things. Because this system is quite decentralised, it is often difficult to pin down.

MB: Over the past few years there have been several police raids and crackdowns on the industry in different parts of Southeast Asia. We've also seen global law enforcement take action to freeze crypto wallets suspected of holding the proceeds of online fraud. Do you think regional and global law enforcement are taking this more seriously now? Have their efforts had any significant impact?

HMN: They may have been a bit slow to react, but I think they see this as a serious concern now. I am also often approached by private sector stakeholders now for advice or information and have discussed and provided advice to groups including Google and Meta, as well as international organisations such as the United Nations Office on Drugs and Crime, and this is clearly high on their agenda.

This issue is transnational, and one person like me cannot do much alone. I can get a website or application shut down one day, but the next minute they open a new one. I hope we can build better international cooperation and work together to fight the scam industry.

Meta is working on ways to protect people using their platforms, but it is challenging as their platforms are huge. I've discussed with them the possible uses of AI, using keywords that the scam ads and profiles use a lot. When detected, they are blocked and eliminated as soon as possible. I think Facebook and Google are starting to take this issue more seriously now.

To be honest, even though we see some crackdowns at the local level, they are not enough. Clearly some countries like Cambodia and Myanmar have not done enough. Corruption limits the effectiveness of crackdowns and, although we have seen law enforcement operations and some shutdowns, these sites reopen again a few months later. That's why we need global cooperation, and major powers like the United States and China, as well as the United Nations, and global law enforcement like Interpol and Europol need to work together to shut down the scam centres and go after the bosses. As their methods get more sophisticated, this cooperation is the only way we can bring down this monster, but we need to move faster. ●