CYBER THREAT ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

June 2, 2022

Chinese Cybercrime in Neighboring Countries

This report examines cybercrimes perpetrated by Chinese-speaking threat actors in countries neighboring China over the last year. In particular, it pertains to the theft and sale of personally identifiable information (PII), cross-border gambling and money laundering, e-commerce and online romance scams, and possible advanced persistent threat (APT) actors engaging in cybercrime. This report, which used the Recorded Future® Platform, the dark web, and open sources, will be of interest to researchers of cybercrime and the region's geopolitics.

Executive Summary

As China continues to tighten its control of the internet and crackdown on cybercrime by using methods such as internet cleanup campaigns, the banning of cross-border gambling, the tightening of anti-money laundering laws, increased pornography censorship, and the banning of cryptocurrency trading, cybercrime has been driven to many of its neighboring countries where such laws and regulations are more limited and there is less government surveillance. Furthermore, economic hardship due to a slowing economy and extremely strict COVID-19 lockdowns have forced more people to engage in scams and cybercrime to pay their bills, including traveling across borders to engage in criminality.

Given the geographical proximity, language and cultural similarities, and lack of laws and regulations, some border regions such as the Wa State of Myanmar have become fertile grounds for Chinese cybercrime. Sophisticated cybercrime syndicates have developed online romance scams through social engineering for the purposes of stealing cryptocurrency and blackmailing victims. In addition, many neighboring countries have long been targets of Chinese APT groups. Armed with technical skills and attack infrastructure, some of these APT actors take up cybercrime to supplement their regular income, and some of the obtained data and access that appear to be APT exploits are advertised on Chinese-language dark web marketplaces.

Key Findings

- Because PII data is easily monetized and can be used as a vector for other forms of cybercrime, some Chinese threat actors continue to collect, harvest, and trade compromised PII data from neighboring countries in East, South, and Southeast Asia.
- Government crackdowns on gambling and money laundering in China have pushed such activities to countries in Southeast Asia, including the Philippines, Cambodia, Vietnam, Malaysia, and Myanmar, due to their lack of related laws and enforcement. Gambling activities in these countries are usually associated with other types of criminality, specifically human trafficking, kidnapping, extortion, forced labor, prostitution, and other crimes. Unsanctioned online gambling websites are also advertised on both social media and dating platforms to lure victims into gambling and then stealing their money.
- Sophisticated cryptocurrency-stealing scams originating in China, which use social engineering tactics to lure victims from dating applications (apps) to fraudulent cryptocurrency trading platforms, are spreading from Asia to the West.
- There is growing evidence that Chinese APT threat actors, such as APT41, are engaging in financially motivated cybercrime such as cryptocurrency theft. Data and access likely obtained by APT exploits have also appeared on Chinese-language dark web marketplaces and are being monetized.

Threat Analysis

This report is based on a year-long investigation — from May 2021 to May 2022 — of a number of Chinese-speaking threat actors offering to sell compromised PII, corporate records, and other stolen items on Chinese-language dark web marketplaces. The results of that investigation, along with analysis of Recorded Future's data sets and knowledge of crime-related activities being conducted by Chinese-speaking threat actors, revealed the most common types of cybercrime conducted by Chinese-speaking cybercriminals, both on the dark web and publicly accessible sites, specifically in countries neighboring China:

- The theft and sale of PII data, which is frequently sold on Chinese-language dark web marketplaces and can be used as a vector to carry out many other forms of cybercrime
- Illegal gambling: legal gambling that is pushed out to some neighboring countries due to its ban in China, is often tied to money laundering, and can also lead to human trafficking, kidnapping, extortion, forced labor, prostitution, and other crimes
- E-commerce scams originating in China that use a variety of tactics to acquire customer payment data
- Increasingly sophisticated online romance scams affecting victims beyond Asia
- The report also presents evidence of connections between Chinese APT and cybercriminal activities in neighboring countries based on both industry reporting and data from the Recorded Future Platform.

PII Theft From Neighboring Countries

The sale of PII is a staple on Chinese-language dark web marketplaces, and PII data from citizens of neighboring countries is widely offered on these sources. Threat actors rely on a plethora of tactics, techniques, and procedures (TTPs) to obtain PII and protected health information (PHI), including keyloggers and infostealers, bankin web injects, spam and phishing attacks, sniffers, and database breaches. Once PII data has been harvested, a threat actor can use it to carry out additional attacks through identity theft, social engineering, account takeover, phishing/spear phishing, business email compromise (BEC), credential stuffing and brute force attacks, and phone-related scams (vishing and smishing).

According to Revenera Compliance Intelligence data, as of February 2021, China leads the world in software piracy, and many of China's neighboring countries are in the top 20. Among them are Russia (#2), India (#5), South Korea (#9), Vietnam (#11), Taiwan (#12), and Hong Kong (#14). Pirated software leads to vulnerable networks, which become easy targets for hackers.

A number of threat actors appear to work in groups to provide foreign PII data as part of their offerings on Chinese-language dark web marketplaces. One of these groups is 海量数据工作室 (Massive Data Studio), which is referenced on both the Exchange Market and the now-defunct Tea Horse Road Market by 7 different threat actors. Another one is 十年老店 (10-Year-Old Shop), which is referenced on the Exchange Market by 10 different threat actors. Some of the offerings appeared to be data seen in previous breaches, such as the ParkMobile breach and the Coinbase breach, which threat actors parsed based on location and offered as different data batches. Some typical PII data offerings from neighboring countries are listed in the table below.

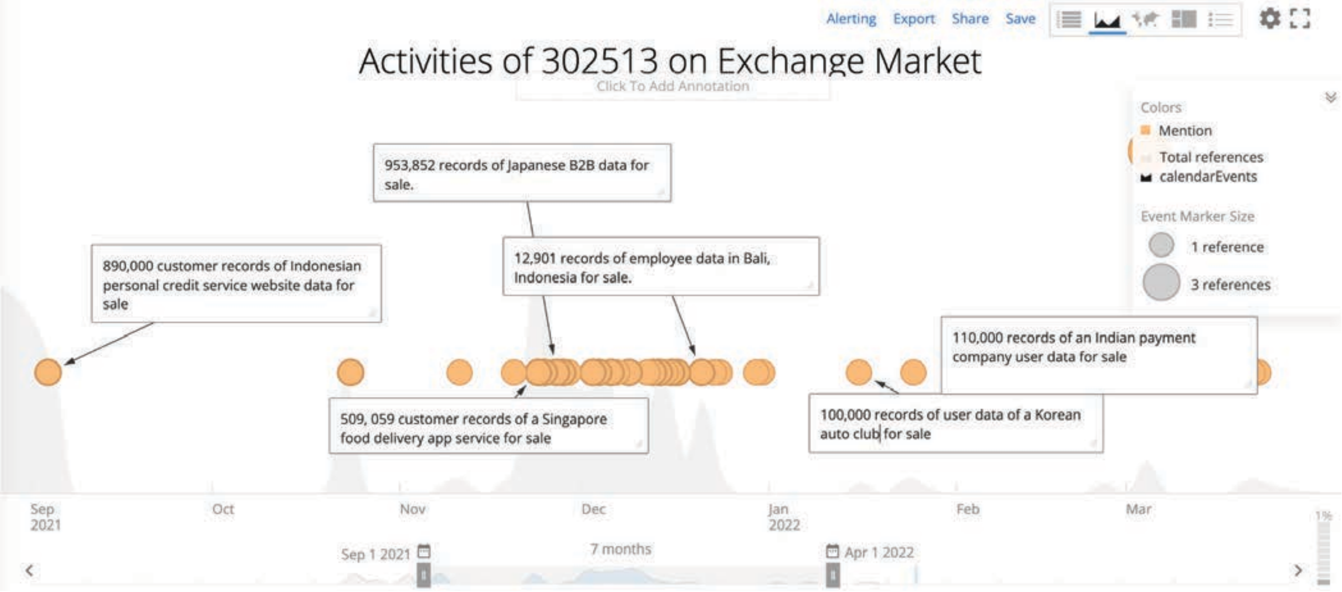

Alerting
Export
Share
Save
Activities of 302513 on Exchange Market
Click To Add Annotation
Colors
Mention
Total references
calendarEvents
Event Marker Size
1 reference
3 references
953,852 records of Japanese B2B data for sale.
890,000 customer records of Indonesian personal credit service website data for sale
12,901 records of employee data in Bali, Indonesia for sale.
110,000 records of an Indian payment company user data for sale
509, 059 customer records of a Singapore food delivery app service for sale
100,000 records of user data of a Korean auto club for sale
Sep 2021
Oct
Nov
Dec
Jan 2022
Feb
Mar
Sep 1 2021
7 months
Apr 1 2022

Figure 1: Activities of 302513 on Exchange Market from September 1, 2021, to March 31, 2022 (Source: Recorded Future)

Threat Actor	Activities
"302513"	In December 2021, the threat actor advertised on the Chinese-language Exchange Market 493,692 records of customer data from a merchant platform company that provides financing and transaction technology in India, and asked $100 for the data set. The data fields include transaction IDs, merchant names and addresses, models of cell phones used for payment, payment card numbers, contact names, cell phone numbers, times of payment, transaction amounts, and others.
"302513"	In December 2021, the threat actor advertised on the Exchange Market 100,000 records of loan application data with PII related to Russian residents and asked $80 for the data set. The data fields include applicant names, phone numbers, email and physical addresses, marital status, passport information, financial status, employment information, and others.
"646464"	In November 2021, the threat actor advertised on the Exchange Market 100,000 records of cryptocurrency traders from Hong Kong and asked $500 for the data set. The data fields include names, genders, cell phone numbers, cities, personal ID numbers, dates of birth, places of birth, marital status, employers, and registration dates from a cryptocurrency trading platform. The data likely came from an October 2021 breach.
"476577"	In June 2021, the threat actor advertised on Tea Horse Road Market 1.1 million records of customer PII from a South Korean web portal, and asked $299 for the data set. The data fields include names, dates of birth, personal ID numbers, credit card numbers with card verification values (CVVs), addresses, expiration dates associated with accounts, and phone numbers. The threat actor claimed that the data was leaked on January 28, 2021, and left a Telegram handle of @Xigua366 as a point of contact.
"9484"	In July 2021, the threat actor advertised on Tea Horse Road Market more than 500,000 records of cell phone data from Taiwan and asked $200 for the data set. The data fields include real names and nicknames, email and physical addresses, dates of birth, cell phone numbers and carriers, passwords (encoded by MD5 hash generators), and the last IP addresses used for logins.

Among the threat actors who specialize in selling foreign PII data, threat actor 302513 in particular is very active on the Exchange Market. A bulk of the listings include data leaks containing PII of customers, users, or residents from neighboring countries. 302513's victims are not limited to Asian countries; the threat actor also sells data from organizations located in the US, UK, and Europe. 302513's credibility is high: the threat actor has been active since the relaunch of Exchange Market in Q4 of 2019 and has made over 100 posts advertising leaked data sets from international entities.

Cross-Border Gambling and Related Crimes

Background Information

China loses an estimated 1 trillion RMB ($155 billion) annually due to cross-border gambling, since all forms of gambling, except state-run lotteries, are illegal in mainland China. Additionally, China's Cyberspace Administration actively blocks domestic users from accessing gambling websites. Despite these restrictions, we continue to see offshore casino operators target Chinese gamblers and evade blocking by operating online gambling websites to connect gamblers, casinos, and proxies, further fueling illegal cross-border gambling activities between China and countries in Southeast Asia.

On March 1, 2022, China's National People's Congress officially passed an amendment to its criminal law, punishing anyone who solicits mainland Chinese citizens to gamble outside of the country's borders and anyone involved in the establishment and management of cross-border casinos. As of April 2021, China's Ministry of Public Security cracked down on and seized thousands of gambling-related operations, including more than 3,400 online gambling platforms and 2,800 illegal payment platforms and underground banks. These crackdowns have resulted in approximately 110,000 people being detained based on over 17,000 cases related to cross-border gambling. In 2020, more than 600 Chinese suspects involved in cross-border gambling activities were arrested in joint operations with law enforcement in the Philippines, Malaysia, Myanmar, and Vietnam, suggesting that these countries are hotspots for illegal gambling activity.

As of November 2021, Chinese prosecutors have indicated that they are targeting online casinos after a number of operators allegedly used internet platforms to get around China's laws against gambling. Organizers were accused of leading a syndicate that opened online gambling platforms abroad, arranging for Chinese nationals to gamble, lending them large sums, and providing clearing services through an underground bank. Casinos are also disguising their operations as platforms for chess and non-gambling card games to bypass restrictions imposed by the Chinese government.

Recruitment Process for Cross-Border Gambling

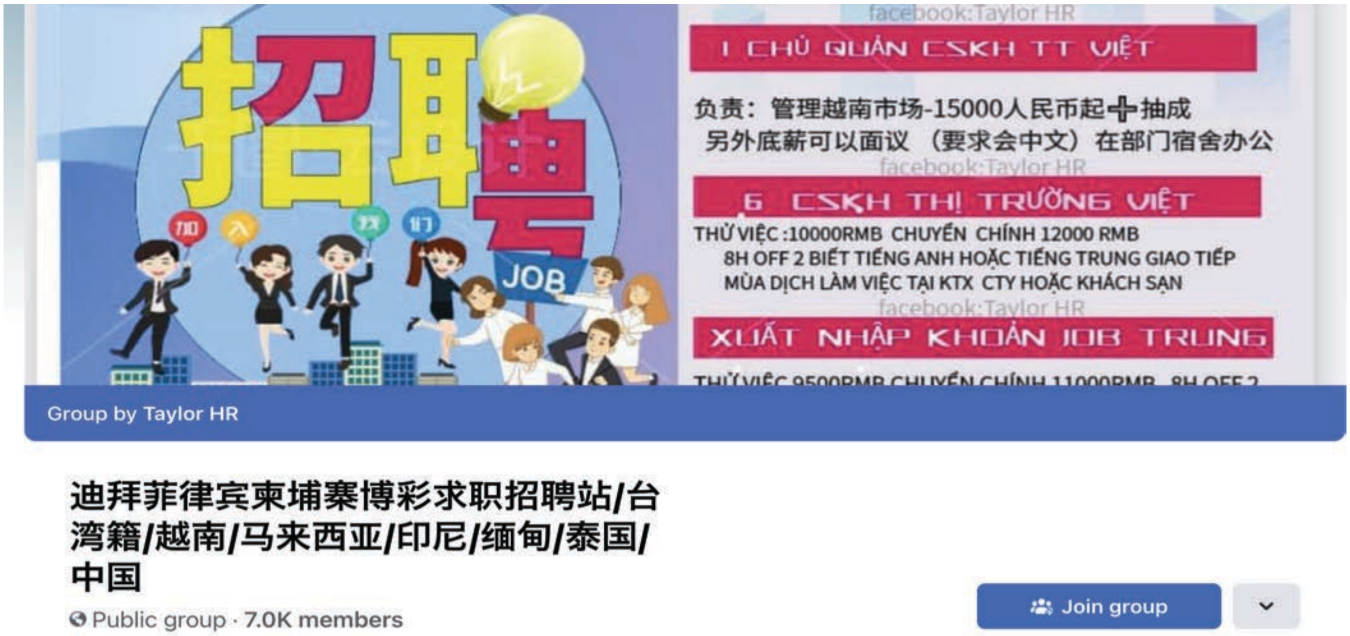
Recruitment of cross-border gambling staff is usually facilitated by the use of social media and messaging applications. Recruiters generally target Chinese nationals who are already residing in foreign countries, as such advertisements are illegal in mainland China. These advertisements are usually written in Chinese to communicate with Chinese speakers.

One such advertisement is openly recruiting individuals to perform customer service, promotion, and human resource-related work. The advertised wages are also much higher than the average income in China. Workers at offshore casinos expect to be paid 144,000 to 240,000 RMB ($21,722 to $36,200) annually, which is about the same as or slightly higher than the annual salaries of workers residing in major, tier-one cities such as Beijing and Shanghai who have annual salaries of 166,803 and 149,377 RMB, respectively, based on 2019 data.

Salaries advertised by offshore casino operators are comparable to or even more lucrative than those in well-paying fields such as information transmission, software development, and information technology. Most Chinese nationals do not reside in cities like Shanghai and Beijing and do not possess the high-level technical skills needed in the most well-paid economic sectors. Because of this, these advertisements for work at offshore casinos are extremely attractive to Chinese nationals who reside outside of major cities, in regions where average annual wages fall between 67,000 and 99,000 RMB.

In the face of slowing GDP growth due to massive energy cutbacks, shipping disruptions, and a deepening property crisis, as well as China's Zero-COVID policy that has resulted in highly restrictive lockdowns, these jobs are especially attractive to Chinese citizens experiencing economic hardship. It is unknown, however, whether Chinese nationals will actually be paid the advertised wages when they arrive in countries such as the Philippines or Cambodia to work as operators of offshore casinos. One reason to doubt the validity of the salary offers is that the number of valid work passes is extremely limited. And as seen in the case of the "Pastillas" scheme in the Philippines, described later in this report, the nature of the work and evidence of illegal entry would draw the attention of the authorities to Chinese nationals working without valid employment passes.

There are also accounts of casino operators luring Chinese and Taiwanese individuals to work outside of China by promising lucrative salaries that never materialized. For example, a Taiwanese individual named Wu Keng-Hao was turned into a "POGO work slave" and sold to at least 2 Chinese groups running POGOs (Philippine Offshore Gaming Operators). The modus operandi of such POGO companies is to encourage Chinese and Taiwanese nationals to work in the Philippines but then to give them a much lower salary than what was agreed upon. When the victims refuse to accept the new terms and conditions of employment, the operators kidnap them and force their relatives to pay a ransom for their safe release. Another case involved a Taiwanese national who had her passport confiscated. She was forcibly transferred to a POGO company, abused physically and mentally, and forced to work until she was rescued by Philippine security forces in February 2020. Such violations of human rights in the form of human trafficking, enslavement, and torture are not limited to POGO companies in the Philippines; they are also found in Southeast Asian countries such as Cambodia and Myanmar.



1 CHỦ QUẢN CSKH TT VIỆT

负责：管理越南市场-15000人民币起+抽成
另外底薪可以面议（要求会中文）在部门宿舍办公

6 CSKH THỊ TRƯỜNG VIỆT

THỬ VIỆC :10000RMB CHUYỂN CHÍNH 12000 RMB
8H OFF 2 BIẾT TIẾNG ANH HOẶC TIẾNG TRUNG GIAO TIẾP
MÙA DỊCH LÀM VIỆC TẠI KTX CTY HOẶC KHÁCH SẠN

XUẤT NHẬP KHOẢN JOB TRUNG

THỬ VIỆC 9500RMB CHUYỂN CHÍNH 11000RMB 8H OFF 2

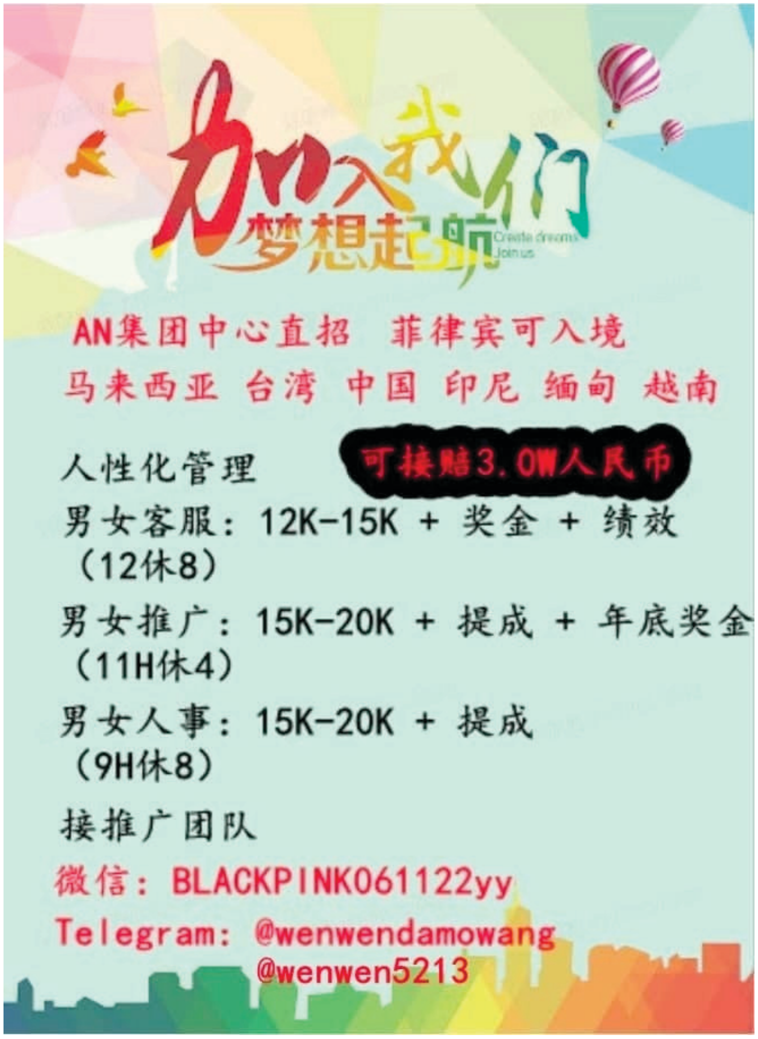
Group by Taylor HR

迪拜菲律宾柬埔寨博彩求职招聘站/台湾籍/越南/马来西亚/印尼/缅甸/泰国/中国

Public group · 7.0K members

Figure 2: A Facebook group looking to hire Chinese/Taiwanese/Vietnamese/Malaysian/Indonesian/Burmese/Thai nationals to work in offshore casinos located in the Philippines and Cambodia (Source: Facebook)

Gambling Website URL	Name of Website	Domain Registration Date	IP Address
https://www.me88pro2[.]com	me88	June 27, 2021	104.21.81.176 Recorded Future Risk Score: 25
https://www.me88plus[.]com	me88	June 27, 2021	104.21.85.171 Recorded Future Risk Score: 5
https://www.me88game[.]com	me88	June 16, 2021	104.21.21.98 Recorded Future Risk Score: 25
https://www.me88play1[.]asia	me88	February 6, 2022	172.67.188.18 Recorded Future Risk Score: 5
https://www.maxim88sg[.]com	Maxim88	May 1, 2020	104.26.12.124 Recorded Future Risk Score: 25
https://www.max88sg[.]com	Maxim88	May 1, 2020	172.67.172.97 Recorded Future Risk Score: 5
https://www.bk8evo[.]com	BK8	February 10, 2021	172.67.159.68 Recorded Future Risk Score: 5
https://www.bk8sgs[.]com	BK8	April 26, 2021	104.21.77.224 Recorded Future Risk Score: 5



AN集团中心直招　菲律宾可入境
马来西亚 台湾 中国 印尼 缅甸 越南

人性化管理　可接赔3.0W人民币

男女客服：12K-15K + 奖金 + 绩效（12休8）

男女推广：15K-20K + 提成 + 年底奖金（11H休4）

男女人事：15K-20K + 提成（9H休8）

接推广团队

微信：BLACKPINK061122yy

Telegram：@wenwendamowang
@wenwen5213

Figure 3: A typical recruitment advertisement for individuals to perform customer service, promotion, and human resource-related work. WeChat ID “BLACKPINK061122yy” and Telegram accounts “@wenwendamowang” and “@wenwen5213” were listed as contact details. Workers can be expected to be paid 144,000 to 240,000 RMB annually. (Source: Facebook)

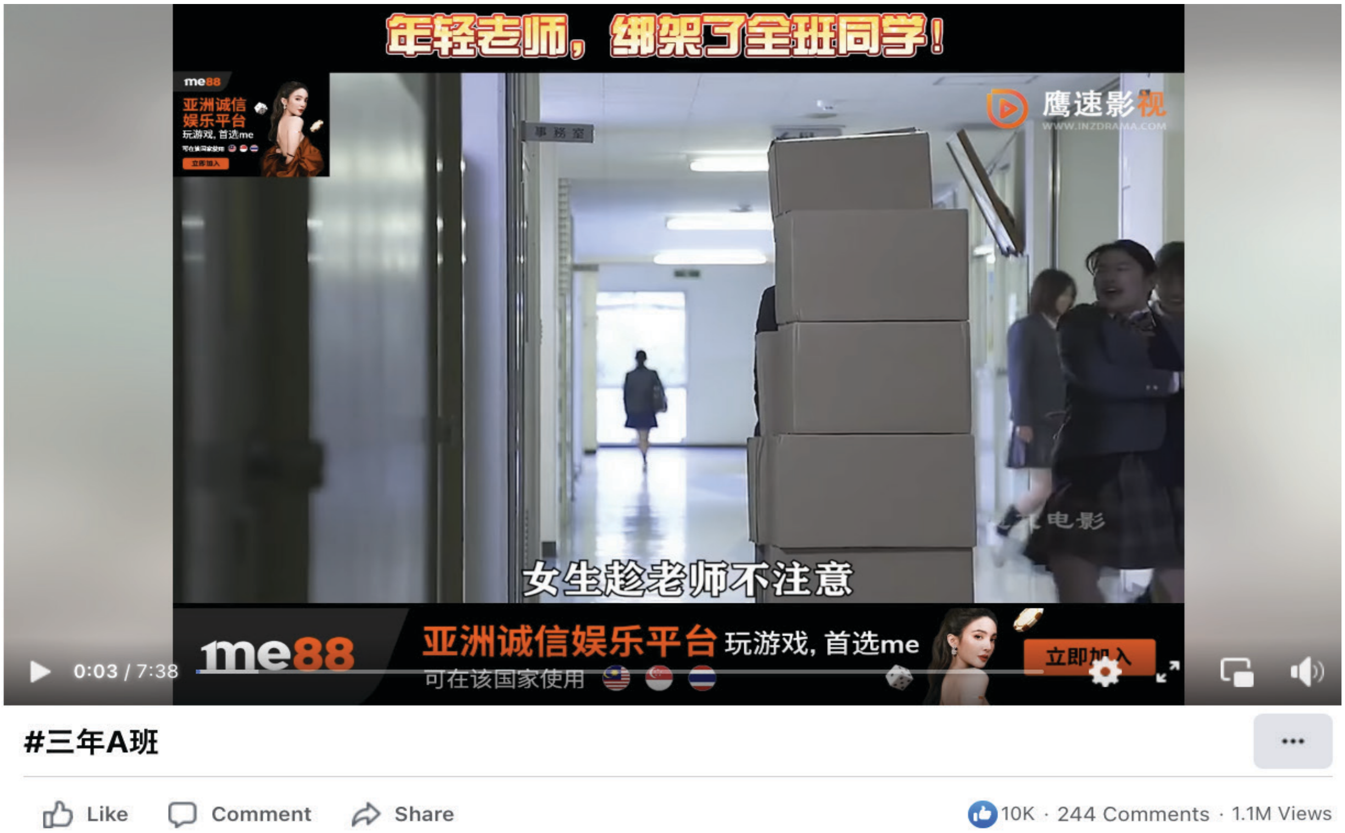
Risks of Gambling Online on Unsanctioned Websites

Advertisement of Gambling Websites on Social Media Pages

Research across social media platforms led to the identification of groups that post illegal video streams of popular movies or video clips with watermarks that advertise both their gambling websites and their free movie streaming websites. The insertion of watermarks is likely an attempt to lure gamblers to these types of websites, and could also be a tactic to evade the platforms’ fraud detection measures. The legitimacy of these gambling websites is dubious; some may have been set up for phishing purposes and may also contain malware that poses risks to viewers.

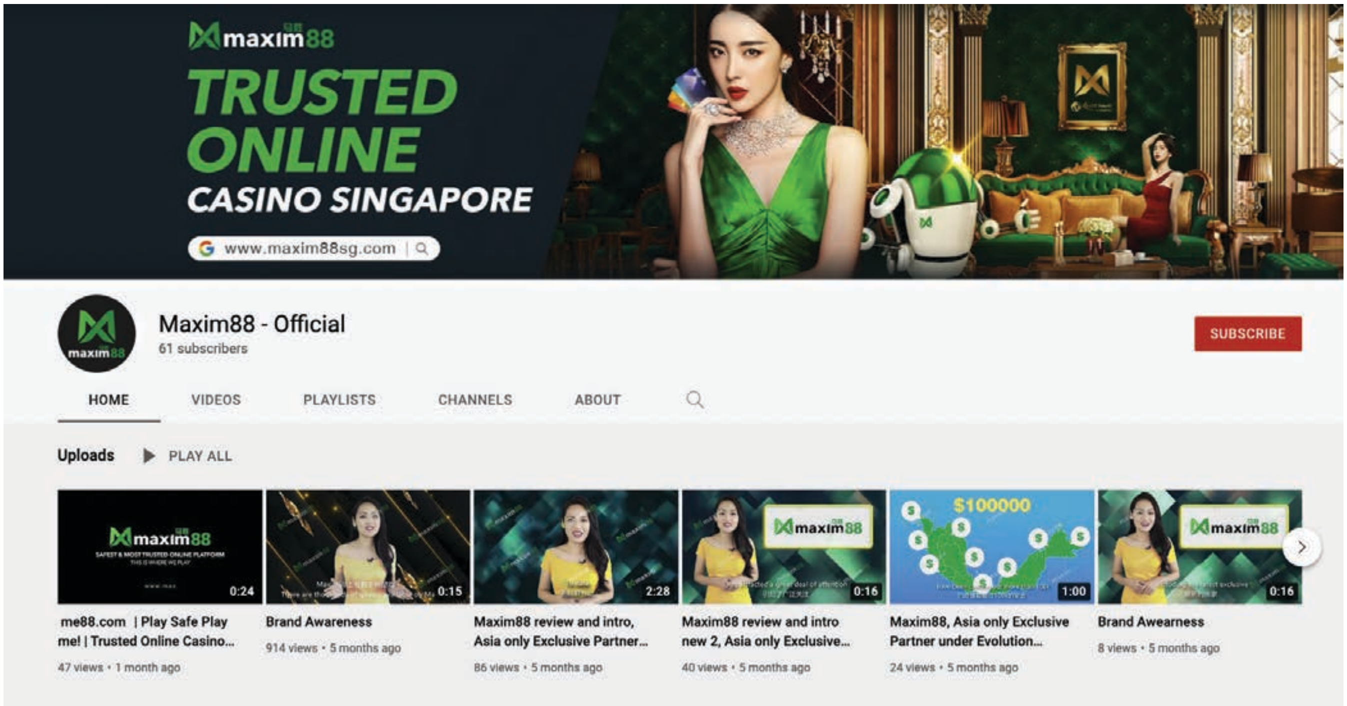
For example, the Facebook group 鹰速电影 Inzdrama has posted video clips with multiple gambling website watermarks to advertise both the Inzdrama movie streaming website1 and online gambling websites such as BK8, me88, and Maxim88. The video clips are usually narrated in Mandarin, as the target audience is Chinese-speaking communities in Southeast Asian countries such as Malaysia, Singapore, and Thailand. All 3 online gambling operators advertise their services through their YouTube channels and aggressively promote their websites through social media. The Inzdrama streaming website, which is in simplified Chinese, requires the user to install an application to stream any video content on the webpage.

[1] hxxps://inzdrama[.]com/



#三年A班

Figure 4: In a post by Facebook group 鹰速电影 Inzdrama targeting Chinese speakers based in Malaysia, Singapore, and Thailand, watermarks belonging to the online gambling platform "me88" are applied to the video clip from a popular movie. The watermark asks people to sign up and play immediately on "me88", which claims to be a trusted gaming platform in Asia. Recorded Future is unable to determine whether this platform is legitimate. Online gambling is only legal through exempt operators, and me88 is not licensed by the Singapore government to provide online gambling services. (Source: Facebook)



Maxim88 - Official
61 subscribers

me88.com | Play Safe Play me! | Trusted Online Casino...
47 views • 1 month ago

Brand Awareness
914 views • 5 months ago

Maxim88 review and intro, Asia only Exclusive Partner...
86 views • 5 months ago

Maxim88 review and intro new 2, Asia only Exclusive...
40 views • 5 months ago

Maxim88, Asia only Exclusive Partner under Evolution...
24 views • 5 months ago

Brand Awearness
8 views • 5 months ago

Figure 5: YouTube channel belonging to Maxim88, an unsanctioned online casino in Singapore. Other similar online casinos such as BK8 and me88 also have their own Youtube channels, but the channels have very few subscribers (less than 300). (Source: Youtube)

There were multiple advertisements for the domains me88, Maxim88, and BK8, and the layouts of these websites were almost identical to each other. In the table below, websites with Recorded Future risk scores of 25 are flagged as recent phishing hosts.

Social Engineering Tactics to Lure Victims to Join Online Gambling Platforms

According to the Beijing Traffic Management Bureau, these are the key tactics used by Chinese scammers to lure people into betting money on a bogus online gambling platform:2

1. Introducing potential victims to a bogus online gambling website by offering an easy way to earn money through gambling
2. Teaching the potential victim how to use the platform and manipulating the back-end system to allow them to win some money, which entices them to invest more money into the platform
3. Requiring that in order to play, a gambler must first transfer the gambling funds to a designated account through online banking; and whether they win or lose, the gambler will not be able to cash out the account balance
4. Presenting winners with a message indicating that the website is undergoing maintenance when they attempt to withdraw cash from the platform; while waiting to cash out, some victims may continue to gamble and thus lose all their previous wins and their deposit of gambling funds
5. Responding to victims who contact customer service with delay tactics that may include the banning of the gambling account, thus preventing any withdrawals

According to the Singapore Police Force (SPF), the number of cases of fake gambling platform scams in Singapore increased by more than 18 times between 2019 and 2020, with a total of 299 reported cases. Scammers often befriend victims through online dating platforms before introducing them to online betting applications or websites. To place bets, victims are required to register on the platform and deposit money into a bank account in exchange for betting credits. Victims will then be informed that their betting accounts have been frozen and that they must deposit more money in order to cash out their winnings. Once a victim makes the additional deposit, the website becomes inaccessible and the scammers cannot be contacted.

The syndicate groups operating unsanctioned online gambling websites have a clear and proven method of luring unsuspecting victims into gambling on the fake platforms: fueling their gambling addiction by allowing them to win small amounts of money and then delaying the cashing-out process. Online gambling in Singapore is only legal through exempt operators, and only Singapore Pools and Singapore Turf Club have been granted the legal right to operate online gambling. Gambling websites such as me883 and Maxim884 are not considered legal avenues for gambling in Singapore. Online gambling is also illegal in Malaysia; the only legal entity is a land-based casino in Genting Highlands. Unsanctioned online gambling platforms continue to advertise themselves aggressively on social media sites and use sophisticated social engineering techniques to lure people based in Singapore and Malaysia to join these illegal platforms. Online gambling websites like Maxim88 even claim to be the most trusted legal online casino in Singapore, a ploy that might mislead many users who are unfamiliar with the legality of online gambling in that country.

Cross-Border Gambling in the Philippines

The Philippines is considered one of the hotbeds for cross-border gambling and is expected to expand. According to PAGCOR (Philippines Amusement and Gaming Organization), the official gaming regulator in the Philippines, POGOs contribute $1.87 billion to the Philippine economy annually, and taxes and fees collected from POGOs are around $670 million per year. Although POGOs are government-sanctioned legal entities, illegal activities and corruption are often involved in their operations, as detailed later in this report.

As the target audience is mainly Chinese nationals, most POGO operators are Chinese. The types of POGO workers include dealers, customer service agents, and IT workers. The games are tailored to Asian tastes and include baccarat, sic bo (a Chinese dice game), and blackjack. They are played in real-time online and allow players from various countries, including China, to place bets remotely.

Because POGOs exert a strong influence on the Philippines' economy, the labor department continued to issue alien employment permits (AEP) to Chinese workers even at the height of COVID-19 lockdowns. From January to September 2020, of the 83,204 AEPs that were issued, 81.5% went to Chinese nationals, who were mostly employed under "administrative and support service activities". And because POGO operations are mainly driven by Chinese players and the programs being developed and used are in the Chinese language, Chinese nationals are needed to operate POGOs on Philippine soil.

[2] hxxp://jtgl.beijing.gov[.]cn/jgj/lszt/659722/10897626/10897770/index.html

[3] hxxps://www.me88plus[.]com/en-sg/home

[4] hxxps://www.maxim88sg[.]com/en-sg/home

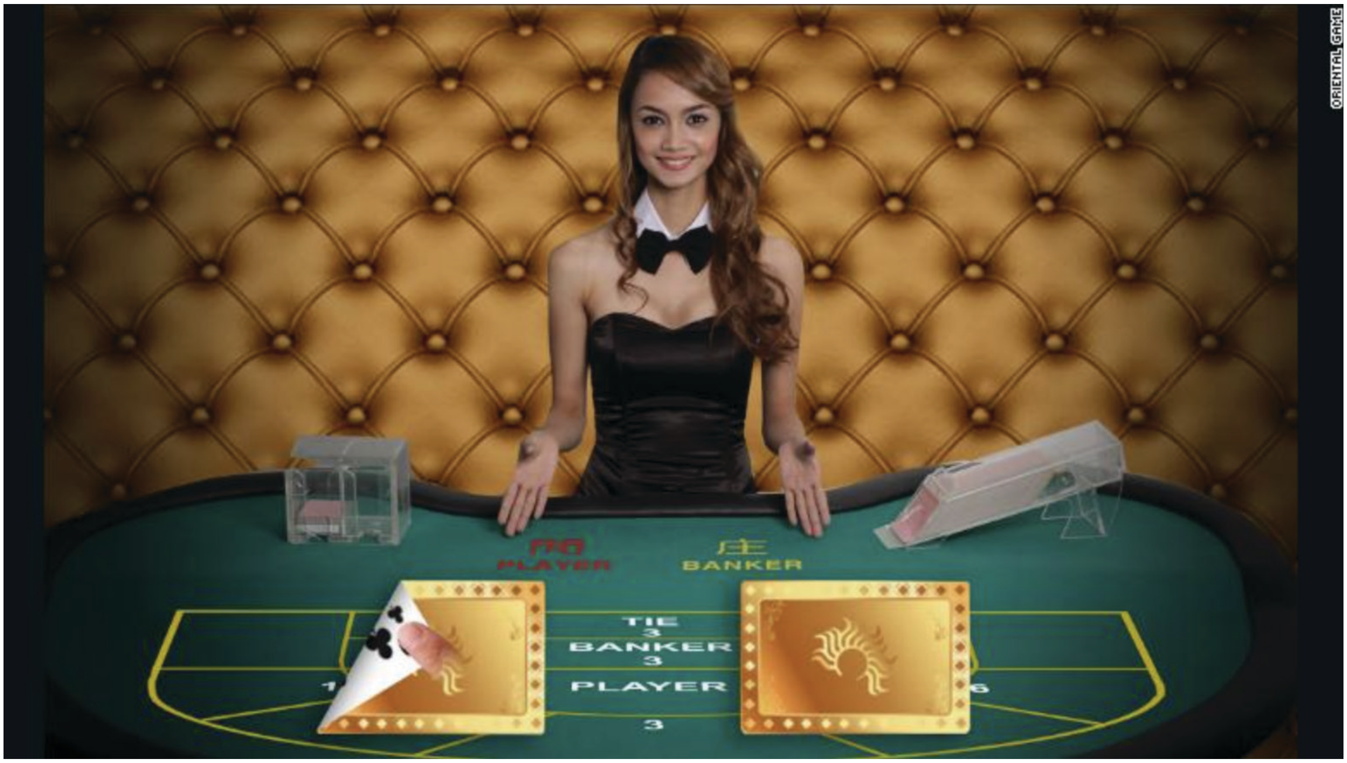


Figure 6: Online casinos operated by POGOs allow players to wager money from abroad on games carried out in real life in the Philippines. (Source: CNN)

"Pastillas" Corruption Scheme

Under the "Pastillas" Scheme, each arriving Chinese national reportedly pays out a P10,000 ($200) service fee, of which P2,000 ($40) will be divided among officials of the Bureau of Immigration's (BI) Travel Control and Enforcement Unit, the immigration supervisor, and the terminal head on duty. The rest of the payout will be given to tour operators and syndicates who transport Chinese nationals from the airport to POGO facilities. According to a Senate hearing in February 2020, corrupt immigration officials allegedly received an estimated total of P10 billion ($198.67 million) in kickbacks from Chinese nationals who were promised seamless entry into the country for a P10,000 service fee. The hearing exposed the level of influence offshore gaming operators had on the Philippines' BI, where a high percentage of airport immigration staff at every level was under the payroll of POGOs. According to the hearing, of the 1.8 million Chinese nationals who entered the Philippines in previous years, only 800,000 of them were tourists or students who applied for real visas, which illustrates the scale of offshore gambling activities in the Philippines — the number of Chinese nationals working for POGOs is much higher than what is officially seen in the issuance of AEPs by the labor department. As Philippines senator Risa Hontiveros remarked, "somebody sold our country's borders for Chinese money".

In May 2020, PAGCOR issued a statement denouncing all forms of illegal gambling in the country, both land-based and online; illegal or non-registered gaming operators have since been officially classified as NOGOs (non-registered offshore gaming operators).

Gambling and Human Trafficking in Cambodia

According to an article published by the Thomson Reuters Foundation, foreign workers and tourists stranded in Cambodia during the COVID-19 pandemic have been trafficked and forced to work in sophisticated online scams. Of the trafficking victims interviewed, 9 revealed that they were lured by social media advertisements promising well-paid jobs in call centers, but ended up in shuttered hotel casinos and guarded compounds where they had their passports confiscated before being put to work online. Online gambling has been linked to such cases, in which Chinese nationals as young as 15 years old have been trafficked and forced to work in online gambling and scam companies in Sihanoukville, Cambodia. Most of these victims were lured primarily by online posts promising well-paying and relaxing jobs and are being trafficked from Southern China overland through Vietnam or by sea to Cambodia. Victims trafficked into Cambodia usually arrived without passports and became easy targets for enslavement.

In one high-profile case reported in February 2022 by multiple international news outlets, a Chinese man was lured to Cambodia by a fake job advertisement and held captive as a "blood slave" for months. Beginning in August 2021, the man's captors reportedly took 27 ounces (almost 800 milliliters) of blood from him each month, leaving him just enough blood to replenish his blood supply; the blood was believed to have been sold online to private buyers. A normal blood donation usually takes 16 ounces (473 milliliters) of blood, and donors wait at least 8 weeks before donating again. When the victim reportedly refused to join the online fraud operation upon arriving in Cambodia, gang members threatened to sell him to organ harvesters. They beat the victim and others into submission using electric prods and forcibly took their blood.

Even though Cambodia has officially banned online gambling since 2019 and law enforcement authorities have raided some online gambling and scam companies, corruption and poor law enforcement have allowed these illegal companies to continue to operate in Cambodia.

Cybercrime in Myanmar

In a similar fashion, Chinese syndicates have lured Chinese nationals from mainland China to northern Myanmar by posting lucrative job advertisements on China's domestic social media platforms. Once the Chinese nationals arrive in Myanmar, their passports are taken away and they are left with no choice but to work as mercenaries, swindlers, prostitutes, or drug dealers.

According to Reuters, which cited a report from the United States Institute of Peace, Chinese syndicates have been able to operate freely due to the socio-political environment in Myanmar after the February 1, 2021 coup. As a result of the coup, economic conditions worsened and a rise in lawlessness created conditions for an increase in criminal activity, especially in northern Myanmar. Large-scale Chinese criminal groups have long been operating in northern Myanmar, using it as a base for well-organized telecoms and internet fraud scams as well as for hosting illegal casinos.

Non-compliance and poor performance would often result in severe physical violence towards the detainees, including beating sessions, torture, and rape, at places controlled by the Chinese syndicates. The scam ring bosses would commonly employ a taser baton to mete out physical punishment to males and females alike. According to the Global Anti-Scam Organization,[5] more than 100,000 Chinese nationals in the region are currently involved in telecom fraud, and scam ring bosses are luring other victims to join online gambling scams. According to an official in Myanmar, the majority of those who illegally traveled from China to northern Myanmar to commit telecom fraud and other crimes have criminal records in China as well.

Mitigation Efforts by Chinese Authorities

Authorities in China are in the midst of combating such cross-border fraud activities, attempting to lure back fugitive criminals who commit fraud based in Myanmar by threatening to restrict them and their family members from accessing welfare, subsidies, and public services in China. An unconfirmed leaked spreadsheet, compiled by Chinese public security authorities, revealed that more than 141,000 Chinese nationals have been classified as fraudulent actors who should return to China. More drastic measures were taken by 4 Chinese provincial authorities (in Fujian, Hunan, Guizhou, and Guangxi), such as demolishing the properties owned by fraudulent actors on the list, painting "homes of frauds" on their houses, and reportedly threatening to stop their children from going to school. Suspects in Myanmar also risk losing their household registration permit and being prohibited from returning to China.

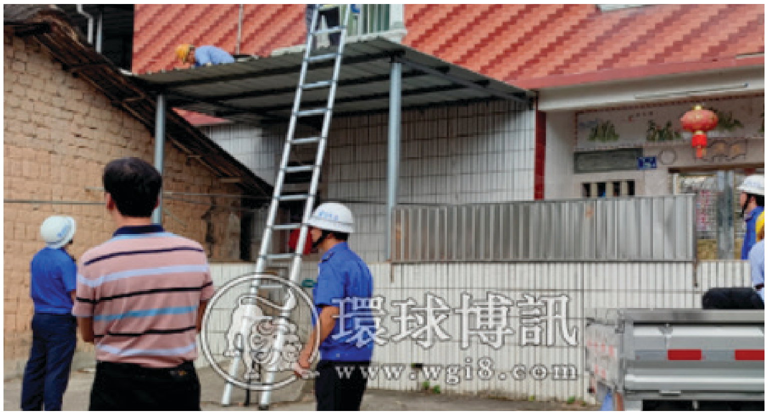


Figure 8: A shed attached to a house in China belonging to a Chinese national in Myanmar who is classified as a "scammer" will be demolished because the suspect failed to return to China (Source: Global Anti Scam-Org)

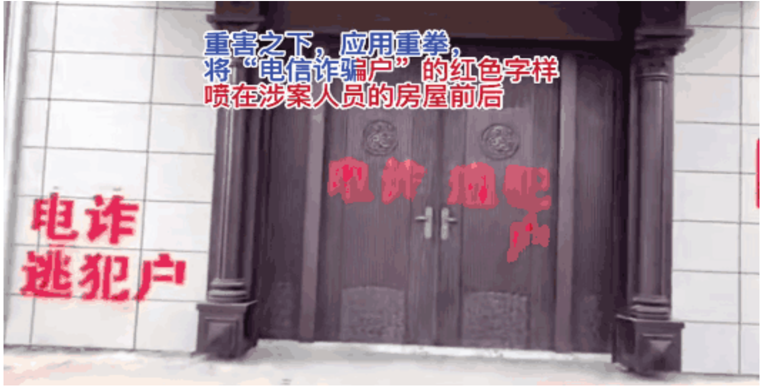
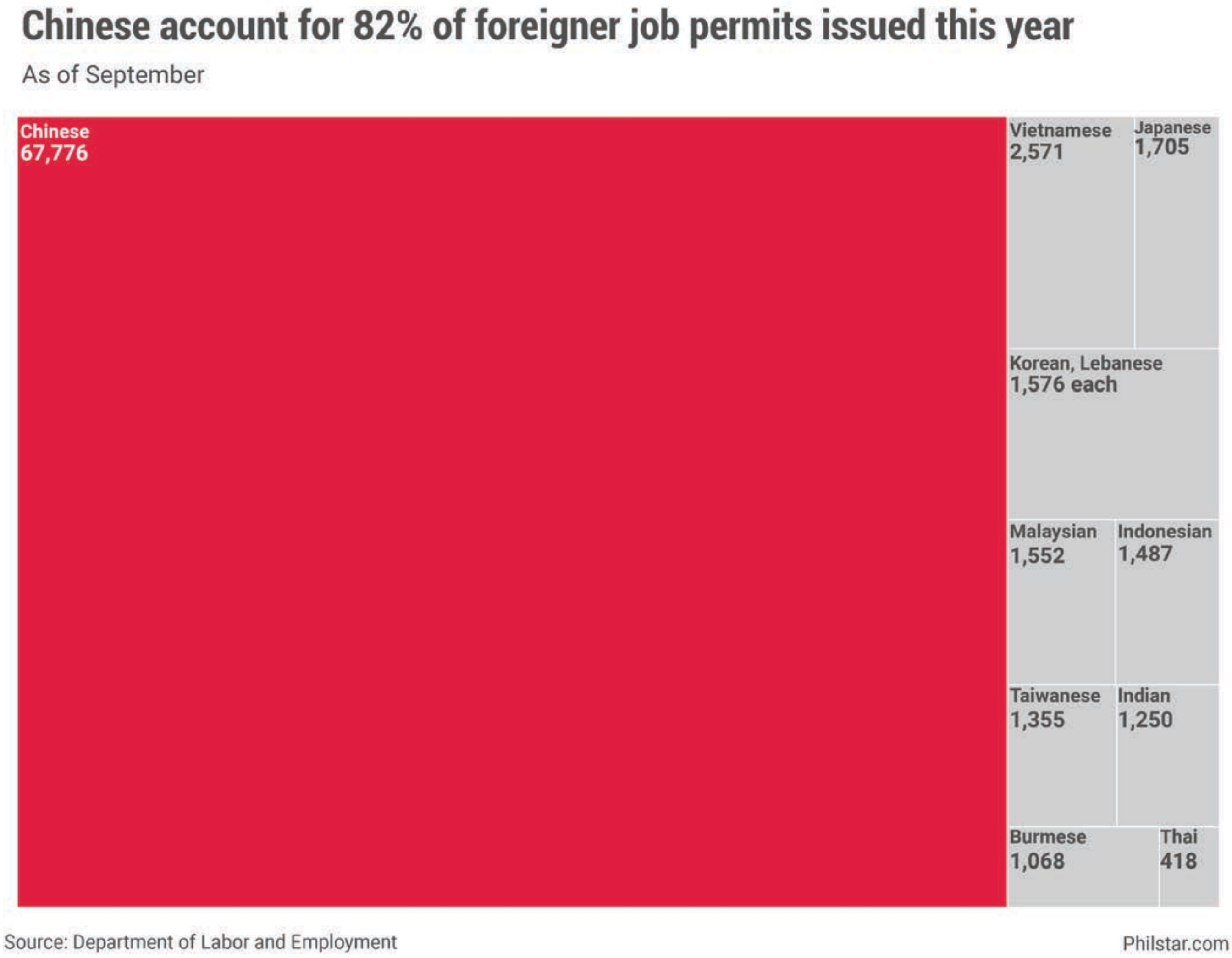


Figure 9: A house belonging to an online fraudulent actor marked with a painted message: "House belonging to online fraudster fugitive" (Source: Ifeng[6])

[5] https://www.globalantiscam.org/post/some-chinese-lured-by-high-paying-jobs-end-up-in-telecom-fraud-prostitution-in-myanmar This story contains graphic images and videos.

[6] hxxps://tech.ifeng[.]com/c/87Ri7dFkqCE



Chinese account for 82% of foreigner job permits issued this year

As of September

Source: Department of Labor and Employment

Philstar.com

Figure 7: Number of AEPs issued to foreigners in the Philippines during the period of January to September 2020, when 81.5% of AEPs were issued to Chinese nationals (Source: Philstar)

Human abduction and scam tactics have been seen since 2019 on Chinese social media websites such as the Reddit equivalent Zhihu. Social media discussions on Zhihu have stated that it is largely safe to work in Cambodia[7] and Myanmar,[8] and postings suggest that a large number of Chinese nationals are working in legitimate jobs in these countries. However, there have also been posts that acknowledge the risks involved in working overseas, especially for online gambling organizations.

The Chinese government's recall of its citizens emptied many shops and buildings in Wa State, the region of Myanmar neighboring China, and has had a significant impact on the local economy. Due to its dependency on China in trade, the local authorities of Wa State announced that they would investigate people and companies involved in telecommunications fraud and online gambling, while simultaneously working with Chinese authorities to repatriate suspects.

E-Commerce Scams Targeting Online Shoppers

Financially motivated threat actors based in China have perpetrated a variety of e-commerce scams. A report by Gemini Advisory found that US and European banks have experienced a spike in e-commerce fraud linked to China-based websites connected to the domain ename[.]net. Gemini assessed that these China-based domains were not infected through Magecart attacks, but were malicious websites that stole payment card data from victims and sold that data across various dark web marketplaces. Gemini also determined that nearly 200 scam websites were linked to the Chinese acquiring bank Jilin Jiutai Rural Commercial Bank Co. Ltd.

[7] hxxps://www.zhihu[.]com/question/267538920

[8] hxxps://zhuanlan.zhihu[.]com/p/362749048

In December 2020, Chinese hackers from Guangdong and Henan provinces attempted to scam millions of e-commerce customers in India by sending bogus links to promotions (in a copycat of a legitimate e-commerce sale) through a messaging app to trick customers into believing they could win free smartphones. Based on an investigation by India's Cyber Peace Foundation, the domain links from the phishing messages were found to be registered in the Guangdong and Henan provinces in China to a company named Fang Xiao Qing, and were hosted in Belgium and the US. The same TTPs (tactics, techniques, and procedures) that took advantage of the e-commerce sales event in India could easily be adopted by retailers in other countries.

Online Romance Scams

CryptoRom Scams

On March 16, 2022, SophosLabs uncovered social engineering attacks that leverage a combination of romantic lures and cryptocurrency fraud to infect victims with the "CryptoRom" malware. In this campaign, CryptoRom uses legitimate iOS features, such as TestFlight and WebClips, to place URLs to specific (malicious) web pages on the home screens of users' iOS devices. CryptoRom campaigns are well-organized and skilled in identifying and exploiting vulnerable users based on their demographics, interests, and technical abilities.

The campaigns work by approaching potential targets through dating apps before moving the conversation to messaging apps. The threat actors then prompt the victims to download a cryptocurrency trading application that is designed to freeze their funds. In October 2021, SophosLabs observed previous variants of social engineering techniques that mimicked app store pages to deceive victims into installing rogue iOS apps. SophosLabs also noted that threat actors were using proprietary programs and software to deliver malware and bypass security screening protocols.

In one of the CryptoRom URLs, researchers found IP addresses related to fake iOS app store hosting pages. One of the apps in the fake app store is named "RobinHand", which is designed to mimic the popular trading application RobinHood and uses a similar logo. Cybercriminals tricked victims who were hoping to make a quick profit into installing the trojanized app. SophosLabs also observed CryptoRom's Android variant.

While this type of scam initially focused on Asian victims, SophosLabs documented the global expansion of such scam campaigns in October 2021. This type of threat is very active and continues to affect victims around the world, in some cases costing them their life savings. This type of scam is well known in mainland China as 杀猪盘 ("pig butchering scam"), which usually involves building a romantic relationship with victims before persuading them to make a fraudulent investment involving cryptocurrencies or foreign exchanges and shares. A search across the Recorded Future Platform identifies many mentions of "pig butchering scam" on both dark web sources and messaging channels.

As a precautionary measure, SophosLabs reported all the CryptoRom-related websites and apps to Apple and Google. Users should refrain from downloading apps from untrusted sources, use apps with end-to-end encryption for communication, and keep devices' operating systems and applications' firmware current with the latest updates to help mitigate against potential attacks. The full list of indicators of compromise (IOCs) can be found in SophosLab's GitHub repository.

Other Online Romance Scams Perpetrated by Chinese-Speaking Threat Actors

In May 2021, Hangzhou police arrested more than 170 individuals involved in cybercrimes. Many crimes involved 裸聊敲诈 (naked chat blackmail), 投资诈骗 (investment scams), and 钓鱼木马 (phishing trojan). These arrests illustrate the prominence and frequency of scams across China-based messaging and dating platforms as well as US-based applications.

According to Recorded Future's data sets from December 2020 to December 2021, the term "naked chat" was referenced in multiple sources, including mainstream news, torrent sites, blogs, and social media platforms. Chinese cybercrimes appear to be very organized, with sound planning and tactics to bait legitimate users, especially on dating platforms.

It is relatively easy to create multiple male and female fake personas on social media platforms. Attractive pictures of individuals and a well-established timeline consisting of ordinary day-to-day activities such as traveling, cooking, and studying are very often enough to make a profile appear to be valid. These fake accounts are designed to bait as many viewers as possible into following the account, which would further convince others of the accounts' authenticity. Creating these accounts requires a considerable amount of time and effort, and cybercriminals do not want them to be banned, so they will usually try to take the conversation to another messaging platform by asking for additional personal information such as the viewer's ID on other platforms. The practice of maintaining social media accounts to use them for fraudulent purposes is known as 养号 ("raising an account").9

[9] hxxp://www.xinhuanet[.]com/legal/2020-11/09/c_1126713598.htm

For example, a fake social media account can appear to be legitimate if the user has a 2018 join date and consistent weekly postings describing what a normal person usually does on a daily basis. Older (legitimate) accounts can also be bought by threat actors. After beginning a chat with a potential victim, the threat actor will attempt to ask the victim to continue the conversation on other messaging platforms that do not require a long period of profiling.

Once the conversation moves to a separate platform, the threat actor will usually attempt to get the potential victim to invest in dubious investment schemes or to engage in a naked chat session together. Once a victim falls prey to such tactics, they usually incur monetary losses by losing money in the dubious investment scam or paying money to the threat actor who is blackmailing them with nude photos and videos they obtained from the victim during the chat.

These types of scams on dating applications result in a negative experience for legitimate users who are genuinely interested in meeting people for serious relationships and cause users to leave the platform due to the surge in fake user accounts created to scam victims.

Possible Advanced Persistent Threat (APT) Crossovers

Neighboring countries have long been targets of China-based APT groups with a wide range of motives. Some of these state-sponsored intrusion activities are aimed at undermining geopolitical rivals during times of conflict, such as the targeting of the Indian power sector by RedEcho; some are intended as a means of reconnaissance, such as the targeting of the Tibetan diaspora in India by RedAlpha; and some are aimed at furthering China's regional influence, in particular the implementation of the Belt and Road Initiative, such as in the targeting of one of Afghanistan's largest telecommunications providers, an attack that was linked to 4 distinct Chinese state-sponsored threat actor groups. According to the reporting from Intrusion Truth, a website dedicated to unmasking Chinese APT groups and related research,

> *MSS (Ministry of State Security) regional departments recruit Chinese criminals to conduct offensive cyber [sic] for the state. We now know this model is evolving, with regional bureaus outsourcing requirements to hackers not simply based in their region, but across the Chinese mainland – sharing expertise between provinces and seemingly working to one, broad model of a criminal, contracted service.*

This hacking-for-hire model suggests a high likelihood of some overlap between Chinese APT actors and cybercriminals.

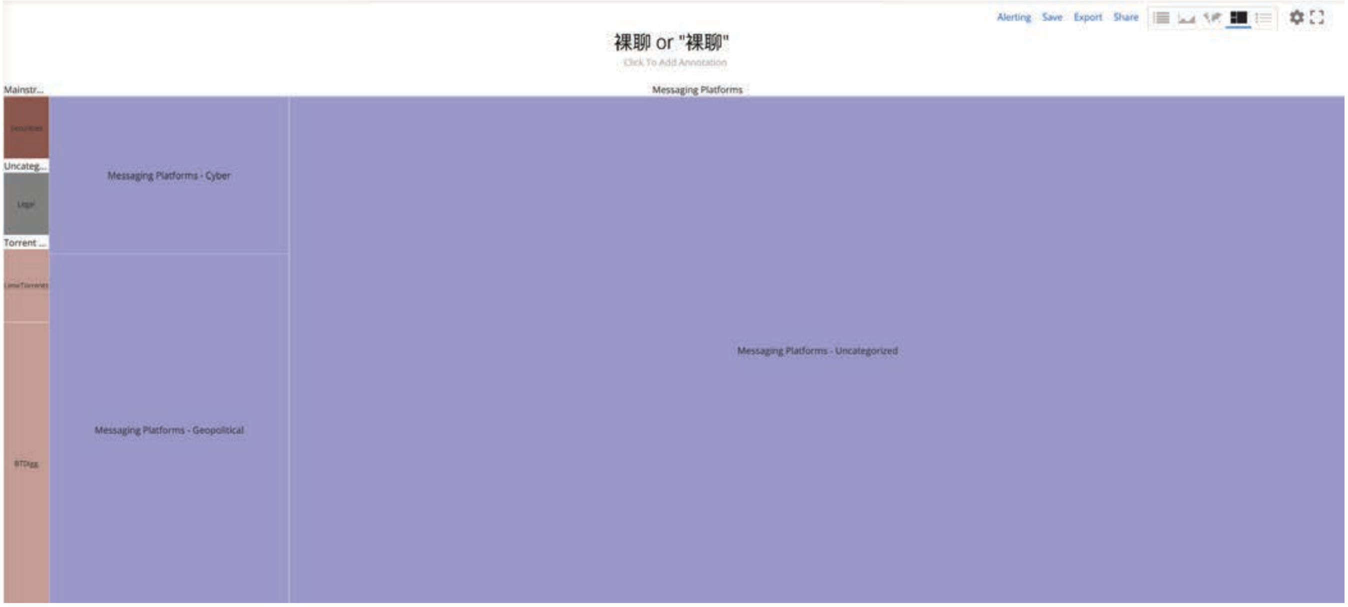


Figure 10: Chinese sources that referenced "naked chat" (Source: Recorded Future)

APT Actors Engaging in Cybercrime

One prominent example of APT groups engaging in cybercriminal activity is APT41. According to a 2019 report from FireEye, threat actors were observed targeting video gaming companies in East and Southeast Asia. This seemed unusual given the state-sponsored goals that likely drive the group's targeting of the healthcare, high-tech, and political sectors. However, some of APT41's early operations driven by personal gain used techniques that would later become pivotal in executing supply chain compromises. Learning to access video game production environments enabled APT41 to develop the TTPs that were later used to inject malicious code into software updates, such as an instance of inserting CRACKSHOT backdoor into a Southeast Asian video game distributor in July 2018.

Throughout the group's observable history, APT41 has consistently run its own financially motivated campaigns concurrently with espionage operations. The operational times for APT41 espionage operations are relatively close to Chinese work hours (in UTC +8, China's time zone). In contrast, the group's financially motivated activity targeting the video game industry tends to occur much later in the day. In at least one case, the group targeted cryptocurrencies that had a connection to an online video gaming platform. In June 2018, APT41 sent spear phishing emails containing an invitation to join a decentralized gaming platform linked to a cryptocurrency service that had positioned itself as a medium of exchange for online games and gambling websites. In October 2018, the group compiled an instance of XMRig, a Monero cryptocurrency mining tool, demonstrating a continued interest in cryptocurrency.

Suspected Data Offerings From APT Activities on the Dark Web

Some unusual offerings have been found on Chinese-language dark web marketplaces that resemble data and accesses obtained through APT activities rather than typical cybercriminal offerings such as stolen data and basic malware. Some were posted on defunct forums, making it impossible to engage with the threat actors to confirm the origin of the offerings. It may be that APT threat actors are trying to use the obtained access and data for personal financial gain once they are no longer needed for mission purposes. Some apparent examples of such efforts are listed below.

Threat Actor	Intelligence
"injection"	On August 10, 2021, the threat actor advertised 7 databases from a Southeast Asian government on the now-defunct Chinese-language Loulan City Market for $50. The seller posted some data samples for the purpose of verification. Industry sources indicated that the LuminousMoth APT that is connected to China has claimed over 1,000 victims in Myanmar and the Philippines. While the credibility of injection is low as the threat actor made no other postings on the Loulan City Market, there is another highly credible threat actor also using the handle "Injection" who posted similar offerings on the seized English-language Raid Forums, such as the advertisement of another country's public health records on September 27, 2021. It is unknown if these 2 threat actors are the same.
"a0981934130"	On December 4, 2021, the threat actor advertised purported national defense secrets from Taiwan including intelligence from its Army, Navy, and Air Force bases as well as weapons on the now-defunct Chinese-language Dark Web Exchange. The threat actor asked for $20 from forum users wanting to preview the information. No APT group can be linked to the information advertised.

Threat Actor	Intelligence
"guoguo123"	On November 9, 2021, the threat actor advertised 45 GB of PII from agents of the "Iranian Secret Service" (a direct translation) for $1,000 on Dark Web Exchange. The information includes names, phone numbers, home addresses, photos, and detailed job descriptions. If the information offered by the threat actor is true, the compromised data is likely related to The Ministry of Intelligence of the Islamic Republic of Iran (vaja[.]ir). No APT group can be linked to the information advertised.
Multiple Dark Web Markets and Data Dumps	On July 13, 2021, a telecommunications company in Nepal was reportedly targeted by Chinese hackers. According to reports, there is no proof that a Chinese group was behind the attack. However, the company stated that China has often surveilled them, which led them to believe that Chinese hackers could have been behind this attack. The data stolen from the telecom server was reportedly being sold on the dark web. A search on the Recorded Future Platform shows that the data from the company are found in multiple dark web marketplaces and data dumps. On June 28, 2021, Recorded Future's Insikt Group published a report identifying a suspected Chinese state-sponsored group, tracked as Threat Activity Group 22 (TAG-22), targeting telecommunications, academic, research and development, and government organizations in Nepal, the Philippines, Taiwan, and less recently Hong Kong. The report identified 3 organizations as the end targets of TAG-22 intrusion activity.

Chinese Nationals Assisting North Korean Threat Actors in Money Laundering

There have been some high-profile cases of Chinese nationals assisting North Korean APT threat actors with money laundering operations. In one instance, between December 2017 and April 2019, 2 Chinese nationals, 田寅寅 (Tian Yinyin) and 李家东 (Li Jiadong), helped North Korean threat actors to launder $100 million worth of cryptocurrency using prepaid gift cards and other methods, which were then used to buy bitcoins on other cryptocurrency exchanges. The North Korean threat actors are believed to be linked to the Lazarus Group, a criminal enterprise linked to North Korea with a reputation for cryptocurrency theft and conducting various high-profile cyberattacks. A total of $250 million worth of cryptocurrency was stolen from an exchange, and both Chinese nationals were indicted by the US Department of Justice on March 2, 2020.

Outlook

The Chinese cybercriminal underground has shown remarkable resilience despite the Chinese government's tightening control over the internet. Since the publication of the Insikt report "Illegal Activities Endure on China's Dark Web Despite Strict Internet Control", a number of Chinese-language dark web sources mentioned in the report have gone offline. However, new marketplaces and forums continue to emerge to take their place. Chinese-speaking threat actors will no doubt continue to trade stolen PII data and other illicit commodities on dark web marketplaces, encrypted messaging apps, and other sources. In addition, cybercrime originating in China has grown in sophistication by incorporating social engineering tactics along with malware development to target victims' cryptocurrency wallets.

Chinese-run illegal online casinos outside of China will likely see an increase in scale and quantity due to the massive crackdown on online gambling inside China. Chinese syndicates will likely continue to bribe immigration and law enforcement officials in countries throughout Southeast Asia to allow Chinese nationals to travel to those countries and perform illegal online gambling operations and broadcast the games to players in China. These syndicates will also likely continue to pursue a target audience of Chinese-speaking people within and outside China's borders while possibly providing a money laundering venue for criminals.

With the increased acceptance of cryptocurrency as well as its rise in value, Chinese threat actors will continue to perpetuate cryptocurrency stealing schemes by creating fake trading apps on both iOS and Android platforms and using social engineering tactics to lure victims into installing these apps on their devices. The apps may contain malware or be designed to lock victims' funds into the bogus trading platforms. Threat actors also allow initial users to partially cash out their winnings to gain legitimacy and popularity, which will likely lead to good ratings on the iOS and Android app stores and help advertise the scheme through word of mouth, in order to attract more investors before running off with the stolen funds. Initially, Chinese threat actors appeared to be targeting mostly Chinese-speaking victims due to the ease of communication, when the majority of victims were Chinese nationals or Chinese diaspora communities overseas. As the scams become more successful and grow in sophistication, however, criminal organizations appear to enlist the services of fluent speakers of various languages in order to orchestrate the malicious schemes on a global scale. Non-Chinese threat actors are adopting similar tactics.

Given Chinese APT groups' continued targeting of neighboring countries and the practice of hiring contract hackers to conduct state-sponsored intrusion activities, there will likely be continued overlap between their operations and cybercriminal activities. In addition, as China's cybercriminal underground continues to gain visibility, it is drawing the attention of well-known threat actors. wazawaka, the well-known threat actor behind the Babuk ransomware, launched the ransomware-oriented RAMP Forum in July 2021 with English/Chinese-language interfaces and sought collaboration from Chinese-speaking threat actors. Although these activities could be nothing more than a smokescreen for wazawaka to cover their tracks or shift blame, it illustrates the increasing visibility of Chinese-speaking threat actors in the global cybercrime landscape.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.