Casino Royale: A Deep Exploration of Illegal Online Gambling

Hao Yang, Kun Du
Tsinghua University
{yang-h16,dk15}@mails.tsinghua.edu.cn

Yubao Zhang
University of Delaware
ybzhang@udel.edu

Shuang Hao
University of Texas at Dallas
shao@utdallas.edu

Zhou Li
University of California, Irvine
zhou.li@uci.edu

Mingxuan Liu
Tsinghua University
liumx96@gmail.com

Haining Wang
Virginia Tech
hnw@vt.edu

Haixin Duan*
Tsinghua University
Beijing National Research Center for Information Science and Technology
duanhx@tsinghua.edu.cn

Yazhou Shi, Xiaodong Su, Guang Liu, Zhifeng Geng
Baidu Inc
{shiyazhou,suxiaodong}@baidu.com
{liuguang03,gengzhifeng}@baidu.com

Jianping Wu
Tsinghua University
jianping@cernet.edu.cn

ABSTRACT

The popularity of online gambling could bring negative social impact, and many countries ban or restrict online gambling. Taking China for example, online gambling violates Chinese laws and hence is illegal. However, illegal online gambling websites are still thriving despite strict restrictions, since they are able to make tremendous illicit profits by trapping and cheating online players. In this paper, we conduct the first deep analysis on illegal online gambling targeting Chinese to unveil its profit chain. After successfully identifying more than 967,954 suspicious illegal gambling websites, we inspect these illegal gambling websites from five aspects, including webpage structure similarity, SEO (Search Engine Optimization) methods, the abuse of Internet infrastructure, third-party online payment, and gambling group. Then we conduct a measurement study on the profit chain of illegal online gambling, investigating the upstream and downstream of these illegal gambling websites. We mainly focus on promotion strategies, third-party online payment, the abuse of third-party live chat services, and network infrastructures. Our findings shed the light on the ecosystem of online gambling and help the security community thwart illegal online gambling.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
ACSAC '19, December 9–13, 2019, San Juan, PR, USA
© 2019 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-7628-0/19/12…$15.00
https://doi.org/10.1145/3359789.3359817

CCS CONCEPTS

• **Security and privacy** → *Web application security*.

KEYWORDS

Illegal Online Gambling, SVM, Web-based Measurement

ACM Reference Format:
Hao Yang, Kun Du, Yubao Zhang, Shuang Hao, Zhou Li, Mingxuan Liu, Haining Wang, Haixin Duan*, Yazhou Shi, Xiaodong Su, Guang Liu, Zhifeng Geng, and Jianping Wu. 2019. Casino Royale: A Deep Exploration of Illegal Online Gambling. In *2019 Annual Computer Security Applications Conference (ACSAC '19), December 9–13, 2019, San Juan, PR, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3359789.3359817

1 INTRODUCTION

Online gambling has been thriving in the last two decades, and it has become one of the most popular and lucrative businesses on the Internet. However, its thriving popularity brings negative impacts and unprecedented challenges for regulations. The problem could be further exacerbated due to its high-speed instant gratification and high level of privacy offered, as well as the abuse of trust in legal payment systems, resulting in pathological gambling. Moreover, the largely unsupervised electronic fund transfers of online gambling can be easily exploited by criminals to launder significant amounts of money.

The legal status of online gambling varies from different countries and regions around the world. Although online gambling is legal in most of European Union countries and several nations in the Caribbean, there are still many countries that restrict or ban online gambling. Illegal online gambling websites are those that target users living in gambling prohibited countries. Taking China for example, according to Chinese laws, operating online gambling websites or proxies is not permitted. However, there are a spate of online gambling websites targeting Chinese via various kinds of illegal advertisements [12]. Most of these illegal online gambling websites are operated outside of China (*e.g.*, Philippines) because of restrictive laws in China [7]. Moreover, abusing the support from legal third-party online payment channels makes illegal online gambling websites more trustworthy and hence attracting more players.

In this paper, we attempt to answer the following two questions: (1) how do miscreants operate illegal gambling websites? and (2) with different roles in operating gambling websites, how are they orchestrated? To this end, we conduct an empirical study on illegal gambling websites that target Chinese. We first develop a detection system to identify illegal gambling websites with the help of unlimited query interface of Baidu's search engine [5], and we successfully identify 967,954 illegal gambling websites. Then we examine the identified illegal gambling websites and investigate how migrants operate these gambling websites, including their promotion strategies, payment systems, and customer service applications.

Findings. We disclose the following strategies on which miscreants operate illegal gambling sites.

(1) Abuse of online payment. We find that illegal gambling websites stealthily employ legitimate online payment channels for their illegal transactions. This is due to the boost of online third-party payment systems, including Alipay [3] and WeChat Pay [35] in China. Although these popular third-party online payment systems have no intention to provide financial support for gambling business in China, there are still many malicious financial proxies that can abuse these online payment systems to support their illegal services. Actually we find that more than 322 small online third-party payment companies that provide illegal financial services and support transactions for online gambling websites by abusing normal Alipay and WeChat Pay channels.

(2) Abuse of outsourcing live chat services. We notice that most gambling websites prefer to outsource live chat services, instead of running their owns. In total, we find 8,387 abused outsourcing live chat services, and the most abused one is Provider Support [25], a typical outsourcing customer service provider. By outsourcing customer services, illegal gambling websites can enhance their credibility and attract more victims.

(3) Abuse of third-party cloud storage. The third-party cloud storage services are widely abused for hosting web resources of illegal gambling websites, especially images and videos. We find that a number of illegal gambling websites host their images in image hosting services like Sinaimg (http://www.sinaimg.cn/) and Alicdn (http://www.alicdn.com/). Our observation shows that online third-party storage providers can serve as a pinch point for detecting illegal gambling websites while being abused by illegal gambling websites.

(4) Promotion strategies. Illegal Gambling websites cannot promote their websites by using traditional SEO (Search Engine Optimization) methods due to their illegitimacy. Our work reveals three promoting strategies for illegal gambling websites, including gambling navigation[1], porn websites, and blackhat SEO. We further disclose several options on how illegal gambling websites conduct blackhat SEO and attract potential victims.

Contributions. We summarize our major contributions of this work as follows:

- A systematic analysis of online illegal gambling categories, their promotion strategies, and their network infrastructures. This can help us to understand how operators control a mass of illegal online gambling websites.
- The first measurement on the abuse of online third-party payment, outsourcing live chat services, and third-party cloud storage services by illegal gambling websites,
- The first measurement on promotion strategies employed by illegal gambling websites. The disclosure of their promotion strategies will help the security community to seek a more effective method to detect these websites.

Roadmap. The rest of this paper is organized as follows. In Section 2, we present the background and motivation for our research. In Section 3, we detail the system architecture and detection methods we used. In Section 4, we describe our measurement study on gambling websites. In Section 5, we present two case studies about payment change and withdrawal in gambling websites, showing how they evade detection and cheat users. In Section 6, we survey related work. Finally, in Section 7, we conclude the paper.

2 BACKGROUND

In this section, we present an overview of illegal online gambling business, including how an illegal online gmabling

[1]Gambling websites link to each other.

Figure 1: One gambling website that targets Chinese.

website operates, blackhat SEO, and illegal online payment. We further give a detailed description on how online payment works.

2.1 How an Illegal Online Gambling Website Operates.

Figure 1 shows an example of illegal gambling websites that target Chinese players. There are three main steps for a gambling website to gain profit: (1) advertising, (2) visiting, and (3) making payment.

For the first step, due to the fact that online gambling is forbidden in some countries and regions, gambling websites cannot conduct legal SEO to appear in the top of search results. However, illegal gambling sites are capable of utilizing blackhat SEO for promoting their websites and attracting players. In [8], Du *et al.* found a new method for blackhat SEO called "spider pool", and most of promotion contents are associated with illegal gambling websites. Players who want to gamble can visit a gambling website through hyperlinks in blackhat SEO pages. If they are interested in the types of gambling in the site, they can make payments and play. Figure 2 illustrates the procedure of online gambling based on a customer's visiting path.

2.2 Blackhat SEO.

SEO is an appointment between website and search engine, assisting search engine algorithms to extract useful information from a webpage quickly and accurately. Search engine manufactures announce their SEO white paper [14] for encouraging its legal use, which is called whitehat SEO.

However, for illegal websites (*e.g.*, contents about drugs and arms purchase and sale), they cannot reach good ranking in search result pages because their content is forbidden in certain countries and regions. So, illegal websites abuse whitehat SEO methods to manipulate search results deliberately by keyword stuffing, cloaking, and many others. This is called blackhat SEO.

Keyword stuffing is first presented in [22]. Its key feature is to fill keywords in all corners of a webpage, even in invisible parts (*e.g.*, meta tag's content, page element with invisible property or beyond user visual scope). Cloaking is another method for blackhat SEO proposed in [15]. It utilizes the difference between a normal user's web browser and a search engine crawler, and presents two different contents accordingly. It can cheat a search engine to gain high page ranking for a malicious website.

2.3 Online Payment.

The ultimate goal of a gambling website is to make profit. So online payment plays an important role in online gambling. In general, players can make payment or withdraw on gambling websites at any time via online payment. Unlike using credit cards and online banking [11], players in China prefer to use third-party online payment like Alipay or WeChat pay. These two payment systems have occupied more than 92% market shares of online payment in China [24]. Throughout this paper, "online payment" is interchangeable with "third-party online payment".

To complete a transaction via online payment, there are 11 main steps: (1) A user applies for a bank card (regardless of credit card or debit card). (2) The user registers an online payment account, and binds to the credit cards or debit cards. (3) A merchant registers an online payment account, binds to the company's banking account and applies for a third-party payment service. (4) The third-party payment provider gives merchant ID, payment gateway URL, public Key, private key, and signature method to the merchant if the merchant's application is approved after auditing. (5) The merchant sets up a website for business. (6) When users make payment, the merchant will send requests to the third-party online payment gateway with parameters of total payment amount, merchant ID, return URL, notification URL, and other information. (7) The payment gateway generates payment URL and gives the merchant the URL in forms of a QR Code. (8) The merchant exhibits the QR Code to users. (9) Users scan the QR Code with online payment application and make the payment to the online payment provider. (10) The online payment provider checks the payment amount requested and received. If correct, it informs the merchant with a positive response. All messages to the merchant are hashed with the signature method and the signature is encrypted with the

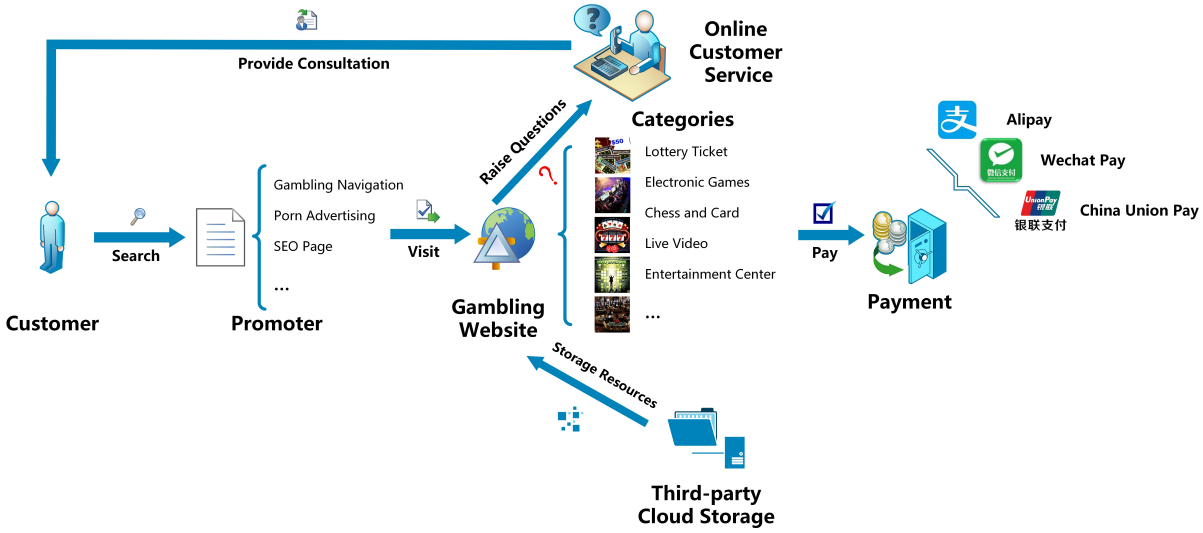

Figure 2: Online Gambling Architecture.

merchant's public key. (11) When the merchant receives payment messages, it checks the signature with the merchant's private key. If correct, it further checks the payment amount with the payment requested. If they match, the payment process is finished.

However, in China there are three unique features in online payment. (1) Third-party online payment like Alipay or WeChat pay has been very prevalent in China, while online banking remains the dominant method for making payment. These online payment methods are usually provided by IM (Instant Messaging) chat tools like AliWangWang and WeChat. Benefiting from the prevalent use of IM chat tools, online payment has been thriving in China.

(2) For Alipay and WeChat pay, these two are not traditional banking and their businesses are not restrictively supervised. So, these two online third payment channels can provide payment services to other merchants and manufactures without restrictive auditing.

(3) There are more than 100 online payment channels that are built on the top of these two main payment channels. To attract more customers, they lower the bar for their customers' auditing. Therefore, miscreants can easily abuse these online payment channels to conduct malicious activities.

3 ANALYZING ILLEGAL GAMBLING WEBSITES

In this section, we describe the dataset and methodology that we use for the in-depth analysis of illegal gambling websites and auxiliary modules, including promotion module and online payment module. Illegal gambling websites and auxiliary modules work together like an industry chain. We also present an overview of illegal online gambling and provide a detailed inspection on auxiliary modules.

3.1 Overview

Figure 3 summarizes our analysis methodology. First, we start with a set of URLs provided by Baidu search engine, and crawl the webpage of each URL. Second, we build a content based classifier to distinguish gambling webpages from others. Then, after the detection phase, we analyze the webpages that are used to promote these gambling websites. Forth, we analyze the content of gambling webpages to count the game types that involve in. Finally, we extract the online payment channels, outsourcing live chat services, and image storage services used by gambling websites.

3.2 Illegal Gambling Detection

The first challenge of our work is to detect illegal gambling websites. There are two major concerns here: the accuracy of detecting illegal gambling pages and how to obtain the dataset of webpages used for detection and ensure its diversity (*i.e.*, representativeness).

We obtain 50,000 illegal gambling webpages and 50,000 normal webpages that are verified by Baidu, which serve as the ground truth for our detection (labeled as $data_{training}$). To ensure the diversity of webpages, we cooperate with Baidu (the largest search engine in China), who provides 10 million URLs indexed by their crawlers, and we crawl the HTML content of each URL. We label the dataset as $data_{total}$.

We build an SVM (Support Vector Machine) classifier to group different types of webpages (gambling and the others) based on $data_{training}$. The procedure is shown in Figure 4. We read raw HTML content from all webpages and extract

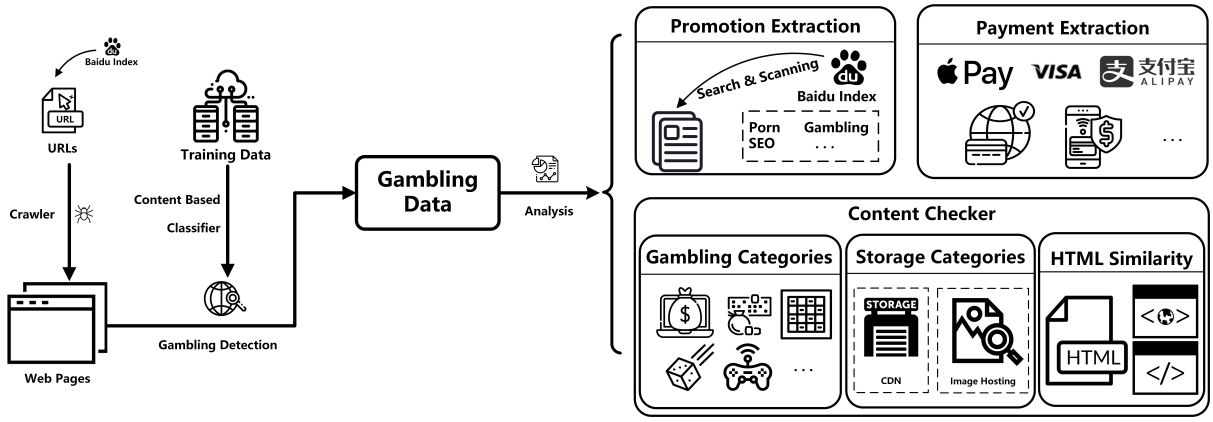

Figure 3: System Architecture.

text from various HTML tags. The HTML tags used here are <title>, <meta>, <li>, <a>, <h1>, <h2>, and <h3>. We select these tags because they play a more important role in the ranking of search engines than others [28]. With the text extracted from webpages, we first tag the text and remove the stopwords while retaining the verbs and nouns. Then we calculate the information gain and chi-square of each word, and retaining the top 20,000 words of these two features. Finally, we concatenate the left words to a new sentence. Each sentence is converted to vector by the TF-IDF (Term Frequency-Inverse Document Frequency) method. Using these vectors for testing in the next step. We then adopt 10-fold cross validation. In each fold, the dataset is split into training/testing sets with a ratio of 80/20. Our SVM classifier can achieve 99.99% of accuracy and 96.1% of precision-recall ratio.

With our classifier, we inspect these 10 million URLs in $data_{total}$, which include various TLDs (Top Level Domains, *e.g.* .com, .cn, .pw, .xyz, and .info). We deploy our classifier in a workstation with 12 cores E5 CPU and 128GB memory. As a result, 967,954 suspected illegal gambling webpages are identified. We label these as $Sites_{gamble}$. Due to the limit of ground truth, we manually check some parts of these results. We randomly select 2,000 pages from suspected illegal gambling webpages and inspect their content manually. We confirm that 1,997 of them are indeed illegal gambling pages. We examine the three falsely identified webpages and find that all of them have few content, and hence we cannot treat them as illegal gambling websites affirmatively.

3.3 Promotion Strategy

We further investigate the strategies on how these illegal gambling websites promote themselves to appear in search results. We collect 106,430,755 URLs from Baidu with hyperlinks pointing to illegal gambling sites, referred to as the

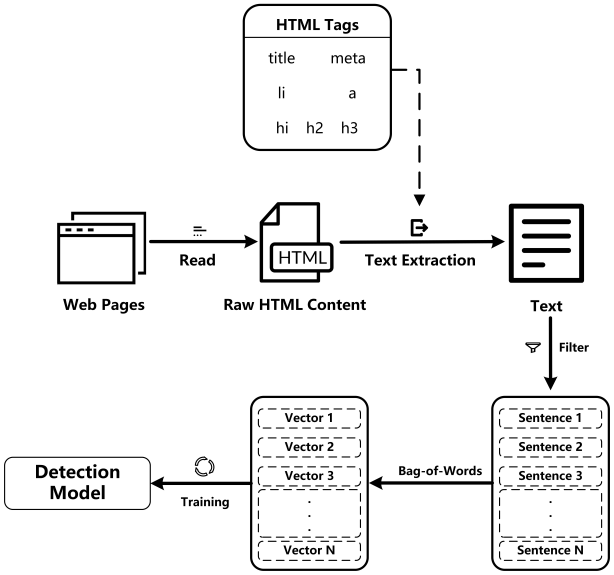

Figure 4: Gambling Detection Procedure.

upstream of illegal gambling sites. It is reasonable to assume that if a website points to a target site, it promotes the target site more or less. We label these upstream sites of illegal gambling sites as $Sites_{promotion}$.

3.4 Content Checker

The content checker aims at analyzing the gambling types, the content in the illegal gambling sites, and the structure similarity of gambling webpages. In order to increase the attraction to potential players, illegal gambling sites present all the game types they can offer in the homepage. We can leverage this characteristic to extract the game types without registering or logging into gambling sites. We manually check all the HTML templates, and find that most of them

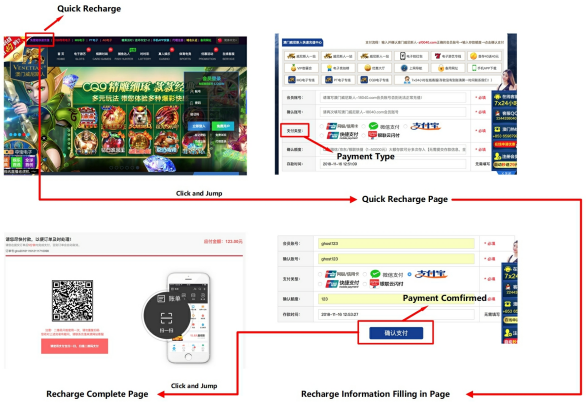

Figure 5: Example of Quick Payment.

put the type title in tags. After extracting all the game type titles, we employ NLP similarity tools (*e.g.*, text2vec) to cluster different game type titles based on their semantic distance.

Besides game types, images play an important role in illegal gambling websites. They make illegal gambling websites more attractive while costing much more storage resources. In order to know more details on how illegal gambling websites store their image resources, the content checker also extracts all the image links from illegal gambling webpages.

To analyze the structure similarity of those webpages in $Sites_{gamble}$, we first extract all the HTML tags and sort them in the order that they appear in the HTML file. Then we utilize a python library for HTML similarity clustering named "page-compare" [13] to calculate the similarity between every two pages. This step is time-consuming because it needs to compare every two pages and time complexity is $N \times (N-1)$ if we have N pages. We deploy this step into Baidu Hadoop cluster servers, costing 2,000 computational nodes 14 days to finish.

3.5 Payment Extraction

We conduct a measurement study on online third-party payment channels. Note that traditional extraction methods are impossible to extract the online third-party payment channels from illegal gambling websites, since it requires us to register on each website and then make actual online payments to finish the extraction. We find a new payment channel in illegal online gambling sites named *quick payment*, which can be utilized by researchers to extract payment information quickly and precisely without registration. In a quick payment scenario, a player can make a payment even without logging into the sites. The player just needs to fill the account name, the payment amount, and select a payment method. After that, the player will be redirected to a payment webpage to complete the online payment. The entry of quick payment usually appears in the homepage of illegal gambling websites. Therefore, we can extract the quick payment page without registration or login. We extract the pair of payment information (*i.e.*, anchor text and link) corresponding to the online payment channel from each webpage in $Sites_{gamble}$. If the text contains the payment content, we mark it as potential payment links. Then we crawl pages according to all potential payment links, and use the structure similarity check method mentioned above. We cluster online payment webpages based on the HTML template they use. Finally, we manually check each template to confirm whether the webpage using the template is a payment webpage. The details of the process are shown in Figure 5.

4 MEASUREMENT

4.1 Overall statistics

We conduct a measurement study on the illegal gambling websites and their auxiliary modules. Through the measurement, we obtain a deeper understanding about how illegal online gambling sites operate, how they abuse network infrastructure and how they gain profit.

4.2 Gambling Categories

Within the 967,954 identified illegal online gambling sites, we investigate different types of gambling and the popularity of each type. We extract gambling category from HTML content by analyzing its structure and keywords. Then we cluster similar titles using text2vec [30]. We find the top five main clusters of gambling categories are lottery ticket (LT, 49.35%), electronic games (EG, 24.22%), entertainment center (EC, 10.96%), chess and card (CC, including mahjong, 9.70%) and live video (LV, 5.76%). From the result we can see that lottery ticket is the most popular gambling category. We infer this is because lottery ticket is one of the easiest games to play and players are familiar with the lottery games such as sport lottery.

For lottery ticket, Figure 6 shows the top 10 subtypes, which comprises more than 20% of this category. Among them, Shishi Cai and Liuhe Cai are the most popular, which is in accordance with the discoveries of prior relevant works [8, 37].

For electronic games, the top 5 types are "EG Games" (6.22%), "MG Games" (4.98%), "PT Games" (3.91%), "AG Games" (3.44%) and "BBIN Games" (2.91%). Most of electronic games are named according to their game content or the corporation that designs and develops the game. The top 5 types make up more than 20% of electronic games.

Chess and card games, such as Baccarat and Slot Machine, are better known types of gambling. We find the top 5 types are "Chess Card Games" (8.22%), "Baccarat in Macao"

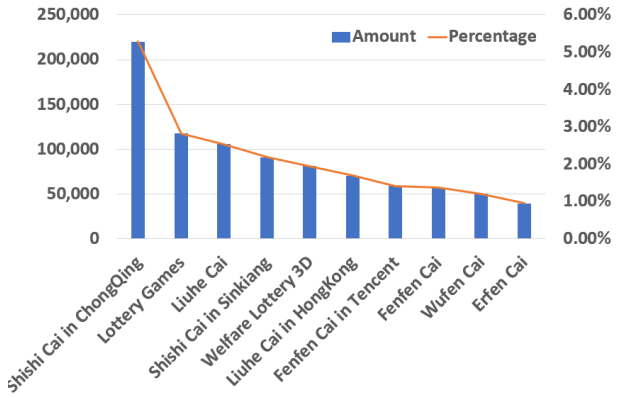

Figure 6: Lottery Ticket Types.

(4.65%), "Slot machine" (4.08%), "MG Slot" (4.03%) and "Baccarat" (3.87%). We can see that Baccarat and slot machine are also common games in illegal gambling sites.

Live video of the gambling place is integrated by more and more websites in recent years since it can audit how the gambling process goes. Illegal gambling sites present live video of the gambling room with a mobile phone. If players suspect the video is fake, he can call that mobile phone and look for the sight of mobile ringing and shining in the video. However, it has been reported that live video can be faked to show the mobile phone feature [1]. In this work, we do not check the trustworthiness of the video while we focus on the ratio of video providers. We count the top 5 providers and find that they occupy 42.69% in live video gambling, including "Reality Show" (18.21%), "AB live video" (8.70%), "CG live video" (8.03%), "LMG live video" (4.61%) and "BG live video" (3.14%).

Finally, we look into the companies behind the entertainment centers, which are brands shared among different gambling websites. The top 5 types of entertainment centers in our result are "Crown Sports" (7.42%), "Jinsha in Macao" (4.78%), "Pujing in Macao" (3.72%), "Pujing Gambling" (1.89%) and "Newest Crown site" (1.33%). All these entertainment centers are owned by one of the 6 companies in Macao: SJM, MGM, Wynn, Melco PBL, Galaxy and VML [36]. This result shows Macao dominates the online gambling business.

4.3 Promotion Strategy

In some countries or areas, advertising the gambling sites is not allowed but still there are players accessing the sites. We want to investigate how these illegal gambling sites attract players but there are two major challenges: (1) It is impossible to identify and crawl all advertisements due to their large quantity. (2) There is no link in the illegal gambling sites that can lead the visitor to the upstream promotion sites. To address those chalenges, we leverage the data indexed by search engines. We obtain webpages that Baidu's bots crawl in a whole day, and identify promotion webpages which contain hyperlinks to or embed advertisements of the illegal gambling sites. We detected 106,340,755 webpages. This dataset is labeled as $Site_{promition}$. Then we classify these promotion webpages with the method describe in Section 3.3.

Table 1: Promotion Categories.

No.	Category	Count	Percentage
1	Gambling	60,258,410	56.6%
2	Porn	25,520,594	23.9%
3	Blackhat SEO	20,651,751	19.5%
4	Total	106,430,755	100%

We show our results in Table 1. We can see that most of promotion webpages are also gambling sites. They link to each other to form a dense link graph. The second type of site is porn and the third is blackhat SEO. Blackhat SEOers prefer leverage the high rank website to promote illegal gambling sites, such as compromised websites with high rank. Surprisingly, blackhat SEO sites are not the most frequently employed method, which implies that gambling sites and porn sites are more effective in promotion.

4.4 Network Infrastructure

In this section, we inspect the distribution of suspected illegal gambling sites in different TLDs (Top Level Domains), IP addresses, registrants / registrars. All these network components are abused in setting up a illegal gambling site.

TLD Distribution. In 2011, ICANN opened the registration for new gTLD [29]. Due to the low price and loose regulation by the new gTLD registrars, domains under new gTLDs have attracted a lot of attention from underground economy [8]. Table 2 lists the distribution of illegal gambling sites across TLDs. On the other hand, our result shows traditional TLDs are still favored: the top 10 popular TLDs, which are associated with more than 96% gambling domains, consists of 7 traditional TLDs and only 3 new gTLDs. Nearly 60% of illegal gambling websites use TLD *.com*. Although registering a domain under *.cn* requires an ICP (Internet Content Provider) license in China [26], it is the second most popular TLD, suggesting there may be flaws of ICP regulation.

IP and AS Distribution. We are also interested how the illegal gambling sites are hosted. We get the present and historical IP addresses of all domains by querying the APIs provided by Farsight passive DNS [10] and Qihoo 360 passive DNS [2]. Then we identify their ASes using the ip2asn tables provided in [18]. Table 3 lists top 10 ASes and their country distribution. We can see that 9 of the top 10 ASes are located in US, possibly because of different regulation law in US.

Table 2: TLD Distribution.

No.	TLD&SLD	Category	Count	Percentage
1	.com	Traditional TLD	600,959	62.08%
2	.cn	Traditional TLD	188,613	19.48%
3	.club	New gTLD	33,211	3.43%
4	.com.cn	SLD	30,950	3.20%
5	.top	New gTLD	28,414	2.94%
6	.net	Traditional TLD	22,726	2.34%
7	.cc	Traditional TLD	12,374	1.28%
8	.tw	Traditional TLD	5,955	0.61%
9	.vip	New gTLD	4,448	0.46%
10	.org	Traditional TLD	4,401	0.45%
Total	-	-	932,051	96.29%

Table 3: Top Ten ASNs for Hosting Gambling Sites(sorted by domain count).

No.	ASN	Country	IP	Domain
1	AS40676	United States	54,330	80,361
2	AS18978	United States	42,682	74,654
3	AS15003	United States	50,445	66,556
4	AS18779	United States	42,063	54,783
5	AS35916	United States	36,982	51,325
6	AS26658	United States	11,414	34,614
7	AS38179	Australia	11,872	25,363
8	AS33330	United States	11,872	25,363
9	AS13335	United States	18,581	23,308
10	AS54600	United States	16,049	21,525
Total	-	-	299,042	457,470

Registrar and Registrant Distribution. WHOIS information of a domain contains its registration information like registrar and registrant, and we inquiry this information for all domains. While recently due to the enforcement of GDPR, most of the registrars stopped to provide WHOIS information to public, we are able to finish our query before GDPR come into effect [2] fortunately. The top ten registrars are listed in Table 5. It is interesting that the registrars except GODADDY.COM are all located in China, which implies the flaws of regulation in China's domain registration.

[2]https://eugdpr.org/

Then we extract registrant email addresses and list study the the top ten registrants who own most of domains. Table 5 lists the registrants who has not set privacy protection and Table 6 lists the registrants who has set email address as private. By comparing these two tables, we can see Table 6 has about 5.5 times more domains than Table 5 in total. This implies that illegal gambling websites extensively employ privacy setting to hide their owners' identities. Moreover, we find some email addresses (*e.g.*, yu*in*pi*a@163.com) have also shown in previous works [8, 37], suggesting those shady registraints are able to keep their business running for long time and serving completely different underground businesses.

4.5 Abuse of Third-party Cloud Storage

We find that illegal gambling sites utilize beautiful images to decorate their websites and attract users' attention, most of which are external images stored in third-party storage. We investigate how third-party storage is abused for this purpose. Illegal gambling sites also embed external javascripts stored in third-party storage but this is not covered by this measurement. This is because most of javascripts that illegal gambling sites use are common javascript libraries, like jQuery hosted in https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js, so there is no pattern unique to them. Nonetheless, images in illegal gambling websites are often different from what are observed on legal sites.

We extract hyperlinks pointing to storage in HTML tag `<img>` from illegal gambling sites. Table 7 lists the categoris of those storage. We observe that illegal gambling sites prefer third-party cloud storage rather than CDN. We infer this is due to the content check mechanism enforced by CDN providers. We list the URLs of the top 10 abused storage sites in Table 8. A typical example of image hosting is shown in Sina blog [3]. In our measurement, *sinaimg* is the fifth largest site serving images to illegal gambling sites. Since *sinaimg* provides information to locate Sina Weibo [4] account who has uploaded this images, we extract 1,214 Sina Weibo accounts from the 229,972 identified sinaimg links. The result shows that a small group of Sina Weibo accounts provide image storage for more than 200,000 illegal gambling sites. We speculate that these Sina Weibo accounts are likely to be operated by the owners of illegal gambling sites.

4.6 Use of Online Customer Service

There are three main ways for gambling websites to offer customer service to their customers: (1) Message board. Gambling website creates a page for the customer to leave message, and the customer will be contacted later on. However,

[3]http://wx2.sinaimg.cn/large/0065w7B7gy1fi2xauuq47g30qo01omyp.gif
[4]Sina Weibo is a Chinese microblogging application, similar to Twitter.

Table 4: Top Ten Registrars.

No.	Registrar	Count	Percentage
1	GODADDY.COM, LLC.	130,582	13.49%
2	CHENGDU WEST DIMENSION DIGITAL TECHNOLOGY CO., LTD.	79,497	8.21%
3	XINNET TECHNOLOGY CORPORATION	77,456	8.00%
4	ALIBABA CLOUD COMPUTING LTD.	59,044	6.10%
5	HICHINA ZHICHENG TECHNOLOGY LTD.	50,936	5.26%
6	ENAME TECHNOLOGY CO., LTD.	48,166	4.98%
7	BIZCN.COM, INC.	37,542	3.88%
8	Beijing Lanhai Technology CO., Ltd.	19546	2.02%
9	Xiamen Nawang Technology CO., Ltd.	19,021	1.97%
10	22NET, INC.	15,839	1.64%
Total	-	537,629	55.54%

Table 5: Top Ten Registrant Email Addresses (with privacy protection).

No.	Registry	Count
1	yu*in*pi*a@163.com	8,913
2	13*35*46*6@qq.com	6,105
3	90*57*3*7@qq.com	5,830
4	ya*ma*yu*in*zh*owo@126.com	4,463
5	cs*78*11*35@gmail.com	3,357
6	qa*qa*18*6@163.com	3,016
7	dt*59*@outlook.com	2,975
8	14*65*27*5@qq.com	2,568
9	yu*in*pi*a@sina.com	2,488
10	29*61*55@qq.com	2,260
Total	-	41,975

Table 6: Top Ten Privacy Protection Email Addresses.

No.	Registry	Count
1	abuse@godaddy.com	53,261
2	domainabuse@service.aliyun.com	29,286
3	supervision@xinnet.com	28,882
4	abuse@list.alibaba-inc.com	28,343
5	westdomain@gmail.com	18,177
6	abuse@bizcn.com	15,067
7	abuse@namebright.com	14,037
8	yuming@yinsibaohu.aliyun.com	13,932
9	abuse@ename.com	13,795
10	abuse@22.cn	11,749
Total	-	226,529

few sites use it due to the slow response time. (2) Social network applications. Gambling websites leave their social network accounts information to serve as customer service on their websites, so that players can contact them directly

Table 7: Gambling Image Storage Statistic.

No.	Type	Site Count	Link Count	Percentage
1	Local Storage	440,253	8,702,216	45.48%
2	Image Hosting	237,197	4,831,317	24.50%
3	Remote Server	215,278	4,517,975	22.24%
4	CDN	75,226	1,375,212	7.78%
Total	-	967,954	19,426,720	100%

Table 8: Top Ten Storage Sites.

No.	Type	Site Count	Link Count	Percentage
1	weibo-hk.com	59,563	406,315	13%
2	51yes.com	43,201	46,413	9.80%
3	alicdn.com	26,823	203,226	35.70%
4	clsj365.com	25,666	2,871,335	5.80%
5	sinaimg.cn	24,846	229,972	5.60%
6	yb6.me	16,395	73,121	3.70%
7	igsttech.com	14,809	15,244	19.70%
8	ppbk9.com	10,858	55,347	6.90%
9	cloud-mgr.com	8,997	278,599	2.00%
10	nnc02.com	7,462	7,462	1.70%

in person. The most common social accounts used in gambling sites include Tencent QQ [5] account, Wechat account, E-mail address, phone number and *etc.* Social network is not widely used here because it can reveal private information of these illegal gambling site controllers. (3) Third-party customer service. During our measurement, we notice that

[5]Tencent QQ is a Chinese messaging application.

illegal gambling sites use third party online customer service like live800.com, providesupport.net. This characteristic enables us to look into the abused online customer service providers and cluster the illegal gambling sites according based on this information.

During this measurement, we first extract customer service URL in different illegal gambling sites and obtain 8,387 different customer service URLs from 133,874 suspiciously illegal gambling sites. It's worth noting that each URL represents a unique account registered in the customer service provider. For example, *0n7w61u9pi8zo0uvfo1jjtmraq* contains the account information of the URL *https://messenger.providesupport.net/messenger/0n7w61u9pi8zo0uvfo1jjtmraq.html*. The top 10 URLs are shown in Table 9. We can see that the first two customer service URLs appear in more than 12,000 suspiciously illegal gambling sites. This indicates that these 6,000 suspiciously illegal gambling sites are likely operated by the same groups or individuals. The total top 10 customer service URLs cover 41,646 (31.1% of 133,874) gambling websites, indicating that there are a few groups or individuals who control a large number of suspiciously illegal gambling sites.

Then we sort customer service URLs by the number of accounts registered by suspiciously illegal gambling sites. Here, we use effective second-level domain (e2LD) to represent customer service providers. Table 10 lists the top 10 customer service providers. We can see the provider abused most is livechatvalue.com. More than 34,000 gambling sites utilize this provider. Note that both the 4th and the 5th e2LD belong to Tencent, of which one is for PC and the other is for mobile.

4.7 Abuse of Third-party Payment Channel

Gambling sites widely employ third-party payment channel due to its convenience and reliability. We investigate third-party payment channels and find more than 1,140 third-party payment channels abused by illegal gambling site. We extract the domain of these payment channels from Sites_{gamble}, and find them in 67,633 gambling websites.

Then we check the structure difference between the payment sites by using the similarity checker illustrated in Section 3.3, and found 17 different website template. According to the structure characteristic, we divide these payment website into two categories. One provides QR code (users can make a payment through scanning the QR Code) and the other requires filling credit card information (users need to submit the credit card information to make a payment).

We extract the payment methods from all the payment websites, as shown in Table 11. We observe that online gambling sites contains all the payment methods that are widely used by people. For example, Alipay is the most popular payment method in China, which also appears in nearly 90% of illegal gambling websites. In addition, illegal gambling sites frequently change the recipient accounts to evade the law enforcement. We monitored the recipient accounts of 100 gambling websites for a month. We observed that 63 of them change their recipient accounts and 47 of them switched their payment methods during this period. More details are illustrated in Section 5.1.

4.8 Summary

From measurements and analysis results illustrated in this section, we find that there exist a number of groups or individuals who control a large number of suspiciously illegal gambling sites. Here, we summarize the findings mentioned above and conduct a further analysis on the groups or individuals.

If two different gambling sites share the same recipient account or customer service URL, we consider these two gambling sites are operated by the same group or individual. We obtain 6,581 different groups or individuals behind suspiciously gambling sites (6,581 clusters). Then we use the similarity algorithm illustrated in Section 3.4 to extract HTML templates in each cluster. The result is shown in Table 12. We find that each cluster contains a large number of domains while a quite small number of HTML templates and domain name patterns. It indicates that the operator leverages a few HTML templates to construct a number of illegal gambling sites automatically to reduce the labor overhead, which on the other hand enables us to detect illegal gambling sites via the HTML templates. We also find that most of domains in the same cluster are often hosted in the same IP or the same AS.

We further illustrate the strategy of operating illegal gambling sites. First of all, operators usually provide different types of games in the website. In the deployment of the website, the operators purchase a large number of domain names and deploys them in servers on different AS in order to evade detection. For the domain name selection, the operators choose a plurality of domain names for bulk registration and management. For the content of the website, operators prefer to use images extensively. In order to reduce the cost, the operators utilize public cloud storage (sinaimg, CDN *etc*) to store the website resources, especially images. For the choice of customer service, they usually purchase online third-party service. For the most important part (*i.e.*, payment channel), the operators use a variety of different payment methods at the same time (including Wechat pay, alipay, *etc*), and change the recipient accounts to avoid risks. After the deployment is completed, promotion plays an important role to attract potential customers. The navigation

Table 9: Online Customer Service URL Appearance Count.

No.	Customer Service URL	Count
1	https://messenger.providesupport.net/messenger/0n7w61u9pi8zo0uvfo1jjtmraq.html	6,202
2	tencent://message/?uin=67393111&Menu=yes	6,202
3	https://chat.manbetx800.net/chat/chatClient/chatbox.jsp?companyID=666&configID=6	5,055
4	https://www.weibo.com/6594879087/profile?topnav=1&wvr=6&is_all=1	5,055
5	http://tieba.baidu.com/home/main?id=d7c3e4b8**?t=1532162862&fr=userbar&amp	5,054
6	http://tieba.baidu.com/home/main?un=ManBetX**&ie=utf-8&fr=frs&id=cd474d**	5,011
7	https://vp8.livechatvalue.com/chat/chatClient/chatbox.jsp?companyID=80002422&configID=2826	3,108
8	tencent://message/?uin=9883833&Menu=yes	2,160
9	https://static.meiqia.com/dist/standalone.html?_=t&eid=85712	2,160
10	https://messenger5.providesupport.com/messenger/1kkiwwjouqjol1tcbl52i7uka6.html	1,639
Total	-	41,646

Table 10: Online Customer e2LD Appearance Count.

No.	e2LD	count
1	livechatvalue.com	34,042
2	live800.com	18,586
3	providesupport.com	16,829
4	qq.com	15,911
5	tencent://	12,604
6	providesupport.net	11,287
7	meiqia.com	10,307
8	learnsaas.com	6,677
9	53kf.com	3,574
10	duokebo.com	2,111
Total	-	131,928

Table 11: Top Ten Third Payment Services.

No.	Payment	Count	Percentage
1	Alipay	1,019	89.4%
2	Wechat Pay	584	51.2%
3	China UnionPay QR Code	565	49.6%
4	QQ Pay	414	36.3%
5	Online Bank	389	34.1%
6	JD Pay	247	21.7%
7	China UnionPay Card	234	20.5%
8	Tenpay	42	3.7%
9	Baidu Pay	32	2.8%
10	Suning Pay	25	2.2%

and pornography websites are the most common promotion channels they use.

5 CASE STUDIES

In this section, we investigate the recipient accounts of online payment that illegal gambling websites use during the tracing period. Then we try to withdraw money from illegal gambling websites to verify their trustworthiness. We also inspect the variation of gambling types during the FIFA World Cup 2018 and show a burst of soccer gambling websites during that period.

Table 12: Top Ten Cluster Characteristic.

No.	Domain	Template	Pattern	AS	Percentage
1	19,936	79	1,236	51	2.06%
2	11,325	53	1,097	37	1.17%
3	9,311	30	873	43	0.96%
4	7,689	127	948	23	0.79%
5	6,986	74	712	39	0.72%
6	6,474	35	455	34	0.67%
7	6,264	99	769	44	0.65%
8	5,853	33	343	31	0.60%
9	5,447	61	537	37	0.56%
10	5,312	42	522	41	0.55%
Total	84,597	-	-	-	8.74%

5.1 Recipient Account

There are two main reasons why illegal online gambling websites change their recipient accounts of online payment: (1) Avoid being tracked. The owners of gambling websites are required to provide authentic personal information when they open banking accounts, which results in the possibility of being tracked. Therefore, they vary their recipient accounts of online payment to avoid the tracking. (2) Malicious report from peer competitors. Since online gambling has very high profits, the competition is fierce. The losers will submit the information of winners to supervision organizations, with the purpose of bringing troubles to them. So, frequently changing recipient account is a common phenomenon in online gambling websites.

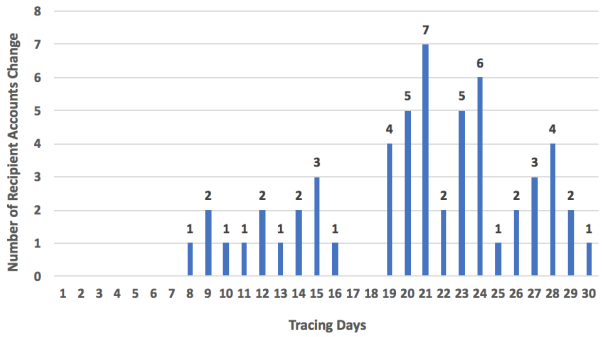

Figure 7: The Change of Recipient Account within One Month.

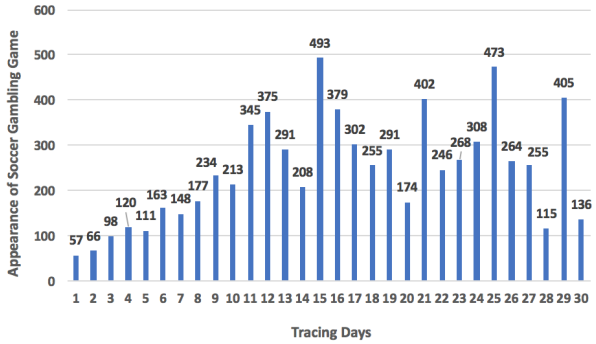

Figure 8: Soccer Gambling Websites Change During FIFA World Cup.

To demonstrate how frequently a recipient account of online payment changes, we trace 100 illegal gambling sites for one months (from August 1st to August 31st, 2018). Without loss of generality, the selected illegal gambling sites have various IP addresses, WHOIS information, and templates, such that these gambling sites are not from the same owner. The payment channels and recipient accounts that they use are also different. During this period, we build a crawler to visit the payment page of each gambling site every day, and collect the recipient account information. The result shows that 56 sites change their recipient accounts during the period. Besides recipient account, they also change the payment channels, and 43 of them change their payment channels during the same period. The dynamics of account change is shown in Figure 7.

5.2 Trustworthiness of illegal gambling sites

As we know, illegal online gambling sites act as a part of underground economy to gain enormous profits. Whether or not gambling sites grant the request of a player's money withdrawal determines their trustworthiness. If the request is declined or delayed to process, the player likely will lose the deposited money. This inspires us to conduct a measurement study on how easy or difficult to withdraw the deposited money from gambling sites.

To illustrate whether illegal gambling sites allow players to withdraw money anytime as they claimed, we make deposits in 20 gambling sites. We do not play any games and withdraw the deposited money right after making the payment. We withdraw successfully only from 8 sites. Then we contact with customer services belong to the other 12 sites, and they inform us that the withdrawal process will finish in about one week. However, we have not received any withdrawal money even two months later. This shows that a significant proportion of illegal gambling sites are not trustworthy and they gain profits even by cheating on players.

5.3 Gambling type migration

Illegal online gambling sites change their gambling types based on social trending events to attract more players, such as FIFA World Cup. We conduct a measurement study on the change of gambling type during the FIFA World Cup 2018.

We trace 10,000 illegal gambling sites from June 1st to June 30th, 2018 during the period of FIFA World Cup. We crawl the homepage of these gambling sites each day, and collect the soccer gambling content. Figure 8 shows the varying number of soccer gambling websites. We can see that during the World Cup, there are a burst of soccer gambling websites: 7,372 of them have soccer gambling games. This indicates that the gambling sites adjust their content according to the hot events. And it also implies that it is easy and convenient for illegal gambling site owners to create a different type of gambling websites.

6 RELATED WORK

In [19], Chris *et al.* analyzed the benefit chain of spam (a type of blackhat SEO) in underground economy. In [20], Damon *et al.* explained the complex role of payment processing in monetizing of abuse-advertised goods. In [34], Wang *et al.* inspected the effectiveness of interventions in counterfeit luxury goods promotions and investigated underground economy from blackhat SEO sites. In [31], Kurt *et al.* discussed ad injection while users visiting the Internet and identified a set of malicious software. In [16], Thomas *et al.* conducted a survey on the flow of capital within the black market and discussed the emerging market of modern criminal entrepreneurs that incorporated dozens of components into entirely new criminal endeavors. In [27], Rafique *et al.* presented an analysis of the free live streaming service ecosystem. In previous studies [21], [4], [17], researchers showed that illegal online services often exploit the shared domain or shared domain hosting facilities for malicious purposes, which is similar to the abuse of network infrastructures by gambling sites.

In [23], Portnoff *et al.* proposed an automated top-down approach for analyzing underground forums and distinguishing black pages from white ones. In [9], Greg *et al.* developed a method for identifying products being bought and sold in online cybercrime forums by using NLP models. In our work, we employ NLP models to distinguish gambling games. In [6], Brunt *et al.* analyzed the payment intervention on a DDoS-for-Hire service, and showed that customers had switched from a regulated payment method to Bitcoin. We also analyzed the payment for illegal gambling sites. The difference is that illegal gambling sites prefer to use online payment rather than Bitcoin. In [32], Tian *et al.* examined the effectiveness of payment by Visa Asia against banks and found the Bank of China supported counterfeit luxury goods merchants continuously for two year research period. In [33], Rolf *et al.* tracked the evolution of commoditization on underground markets and identified the market supply for most components.

7 CONCLUSION

In this paper, we conduct the first comprehensive analysis on illegal online gambling ecosystems that target Chinese players. We identify illegal gambling websites from blackhat SEO pages and characterize the abuse of third-party online payment, outsourcing customer services, and third-party cloud storage services. We conduct a measurement study on the profit chain of illegal online gambling. We observe that third-party online services involuntarily help miscreants run gambling websites, such as image hosting infrastructures and outsourcing customer services. We also find that third-party online payment channels (*e.g.*, Alipay and WeChat pay) play a key role in the profit chain of illegal online gambling, which can thus be leveraged to thwart illegal online gambling.

8 ACKNOWLEDGEMENT

We thank anonymous reviewers for their insightful comments. This work was partially supported by the Natural Science Foundation of China (U1836213, U1636204) and the BNRist Network and Software Security Research Program (Grant No.BNR2019TD01004), as well as the U.S. National Science Foundation (CNS-1618117).

REFERENCES

[1] 1396mm.com. 2019. The possibility and feasibility of online casino video cheat. https://www.1396mm.com/article/detail/142368.html.

[2] 360.com. 2019. Network Security Research Lab at 360. https://netlab.360.com/.

[3] alipay.com. 2019. Alipay. https://www.alipay.com/.

[4] Sumayah Alrwais, Xiaojing Liao, Xianghang Mi, Peng Wang, XiaoFeng Wang, Feng Qian, Raheem Beyah, and Damon McCoy. 2017. Under the shadow of sunshine: Understanding and detecting bulletproof hosting on legitimate service provider networks. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 805–823.

[5] baidu.com. 2019. Baidu Search Engine Homepage. https://www.baidu.com.

[6] Ryan Brunt, Prakhar Pandey, and Damon McCoy. 2017. Booted: An Analysis of a Payment Intervention on a DDoS-for-Hire Service. In *Workshop on the Economics of Information Security*.

[7] casino.org. 2018. Chinese Workers in Manila are Enslaved by Gaming Operator. https://www.casino.org/news.

[8] Kun Du, Hao Yang, Zhou Li, Haixin Duan, and Kehuan Zhang. 2016. The Ever-Changing Labyrinth: A Large-Scale Analysis of Wildcard DNS Powered Blackhat SEO. In *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX, 245–262.

[9] Greg Durrett, Jonathan K Kummerfeld, Taylor Berg-Kirkpatrick, Rebecca S Portnoff, Sadia Afroz, Damon McCoy, Kirill Levchenko, and Vern Paxson. 2017. Identifying products in online cybercrime marketplaces: A dataset for fine-grained domain adaptation. *arXiv preprint arXiv:1708.09609* (2017).

[10] farsightsecurity.com. 2019. Passive DNS historical internet database: Farsight DNSDB. https://www.farsightsecurity.com/solutions/dnsdb/.

[11] Jason Franklin, Adrian Perrig, Vern Paxson, and Stefan Savage. 2007. An inquiry into the nature and causes of the wealth of internet miscreants.. In *ACM conference on Computer and Communications Security*. 375–388.

[12] gamblingsites.org. 2019. Gambling Market in the Philippines Is Gaining Speed. https://www.gamblingsites.org/news/the-philippines-gambling-market-isnt-slowing-down/.

[13] github.com. 2015. TeamHG-Memex/page-compare: Simple heuristic for measuring web page similarity. https://github.com/TeamHG-Memex/page-compare.

[14] google.com. 2019. Search Engine Optimization (SEO) Starter Guide. https://support.google.com/webmasters/answer/7451184?hl=en.

[15] Marco Gruteser and Dirk Grunwald. 2003. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st International conference on Mobile Systems, Applications and Services*. ACM, 31–42.

[16] Kurt Thomas Danny Yuxing Huang, David Wang Elie Bursztein Chris GrierD, Thomas J Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, and Giovanni Vigna. 2015. Framing dependencies introduced by underground commoditization. In *Workshop on the Economics of Information Security*.

[17] Damilola Ibosiola, Benjamin Steer, Alvaro Garcia-Recuero, Gianluca Stringhini, Steve Uhlig, and Gareth Tyson. 2018. Movie pirates of the caribbean: Exploring illegal streaming cyberlockers. In *Twelfth International AAAI Conference on Web and Social Media*.

[18] iptoasn.com. 2019. Free IP address to ASN database. https://iptoasn.com/.

[19] Chris Kanich, Nicholas Weaver, Damon McCoy, Tristan Halvorson, Christian Kreibich, Kirill Levchenko, Vern Paxson, Geoffrey M Voelker, and Stefan Savage. 2011. Show Me the Money: Characterizing Spam-advertised Revenue. In *USENIX Security Symposium*. 15–15.

[20] Damon McCoy, Hitesh Dharmdasani, Christian Kreibich, Geoffrey M Voelker, and Stefan Savage. 2012. Priceless: The role of payments in abuse-advertised goods. In *Proceedings of the 2012 ACM conference on Computer and Communications Security*. ACM, 845–856.

[21] Najmeh Miramirkhani, Oleksii Starov, and Nick Nikiforakis. 2016. Dial one for scam: A large-scale analysis of technical support scams. In *In Proceedings of the 24th Network and Distributed System Security Symposium (NDSS 2017)*. Internet Society.

[22] Alexandros Ntoulas, Marc Najork, Mark Manasse, and Dennis Fetterly. 2006. Detecting spam web pages through content analysis. In *Proceedings of the 15th international conference on World Wide Web*. ACM, 83–92.

[23] Rebecca S Portnoff, Sadia Afroz, Greg Durrett, Jonathan K Kummerfeld, Taylor Berg-Kirkpatrick, Damon McCoy, Kirill Levchenko, and Vern Paxson. 2017. Tools for automated analysis of cybercriminal markets. In *Proceedings of the 26th International Conference on World Wide Web*. 657–666.

[24] prcfe.com. 2018. Alipay vs WeChat Pay. http://www.prcfe.com/news/2018/0303/230675.html.

[25] providesupport.com. 2019. Live Chat Support on Your Website. https://www.providesupport.com/.

[26] quantil.com. 2019. A Guide to ICP Certification in China. https://www.quantil.com/content-delivery-insights/icp-certification-china/.

[27] M Zubair Rafique, Tom Van Goethem, Wouter Joosen, Christophe Huygens, and Nick Nikiforakis. 2016. It's free for a reason: Exploring the ecosystem of free live streaming services. In *Proceedings of the 23rd Network and Distributed System Security Symposium (NDSS 2016)*. Internet Society.

[28] searchenginejournal.com. 2018. How Important Is an H1 Tag for SEO? https://www.searchenginejournal.com/how-important-is-h1-tag-for-seo/261547/.

[29] GreenSec Solutions. 2016. new gTLD Statistics by Top-Level Domains. https://ntldstats.com/tld.

[30] text2vec.org. 2017. Documents similarity. http://text2vec.org/similarity.html.

[31] Kurt Thomas, Elie Bursztein, Chris Grier, Grant Ho, Nav Jagpal, Alexandros Kapravelos, Damon McCoy, Antonio Nappa, Vern Paxson, Paul Pearce, et al. 2015. Ad injection at scale: Assessing deceptive advertisement modifications. In *2015 IEEE Symposium on Security and Privacy*. IEEE, 151–167.

[32] Hongwei Tian, Stephen M Gaffigan, D Sean West, and Damon McCoy. 2018. Bullet-proof payment processors. In *APWG Symposium on Electronic Crime Research (eCrime), 2018*. IEEE, 1–11.

[33] Rolf Van Wegberg, Samaneh Tajalizadehkhoob, Kyle Soska, Ugur Akyazi, Carlos Hernandez Ganan, Bram Klievink, Nicolas Christin, and Michel Van Eeten. 2018. Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, 1009–1026.

[34] David Y Wang, Matthew Der, Mohammad Karami, Lawrence Saul, Damon McCoy, Stefan Savage, and Geoffrey M Voelker. 2014. Search+seizure: The effectiveness of interventions on seo campaigns. In *Proceedings of the 2014 Conference on Internet Measurement Conference*. ACM, 359–372.

[35] weixin.qq.com. 2019. WeChat Pay. https://pay.weixin.qq.com/.

[36] worldcasinodirectory.com. 2019. Macau casinos and gambling guide. https://www.worldcasinodirectory.com/macau.

[37] Hao Yang, Xiulin Ma, Kun Du, Zhou Li, Haixin Duan, Xiaodong Su, Guang Liu, Zhifeng Geng, and Jianping Wu. 2017. How to learn klingon without a dictionary: Detection and measurement of black keywords used by the underground economy. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 751–769.