infoblox

Threat Intel

VIGORISH VIPER: A VENOMOUS BET

Authors:
Maël Le Touz
Jacques Portal
Renée Burton
Elena Puga

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This groundbreaking report unveils the discovery of a technology suite and its connection to Chinese organized crime, money laundering, and human trafficking throughout Southeast Asia. The technology suite is composed of software, Domain Name System (DNS) configurations, website hosting, payment mechanisms, mobile apps, and more—a full cybercrime supply chain. Tens of seemingly unrelated gambling brands that advertise by way of sponsorship deals with European sports teams use this technology. The owners of these brands prey on residents of Greater China and on victims across the globe to take advantage of the US$1.7 trillion illegal gambling economy.[1] We've named the actor who designed, developed, and operates this supply chain: **Vigorish Viper**.

We are highly confident that Vigorish Viper's technology suite was developed by the Yabo Group (also known as Yabo Sports or Yabo). Watchdogs believe the notorious Yabo controls "possibly the biggest illegal gambling operation targeting Greater China" and have directly tied them to practices of modern slavery.[3] For example, human trafficking victims in forced labor camps linked to Yabo on the Cambodia–Laos border must "staff" gambling operations and run so-called pig butchering scams. The victims, most of whom are Chinese, provide customer support for Yabo's websites as well as those of several other betting brands.[4] We found that the brands at the center of these labor camps are connected in multiple ways, including through their use of the Vigorish Viper's technology suite: While these brands appear distinct, they operate more like the branches of a franchise.

Although our research indicates that Vigorish Viper is likely synonymous with Yabo, the real identities behind Yabo remain unknown. As such, Yabo itself is merely one face for an unknown organized crime syndicate. This report focuses on the technology, network operations, and supply chain of Vigorish Viper rather than the financial and humanitarian crimes reportedly committed by their alter ego Yabo. The full scope of crimes by Vigorish Viper (and by implication, Yabo) is unknown to us.

UNODC

The United Nations Office on Drugs and Crime (UNODC) concluded that "organized crime groups running many of these (online casino) operations have done so with growing sophistication, through the use of data mining and processing, blockchain technology and, increasingly, generative artificial intelligence".[2] Vigorish Viper software and infrastructure are representative of this sophistication.

1 https://www.unodc.org/unodc/press/releases/2021/December/first-ever-global-report-on-corruption-in-sport-flags-urgent-need-for-unified--international-response-to-corrupt-practices-in-sport.html last accessed April 29, 2024

2 https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf last accessed April 29, 2024

3 How Organised Crime Operates Illegal Betting, Cyber Scams & Modern Slavery in Southeast Asia, October 2023. The Asian Racing Federation (ARF) Council on Anti-Illegal Betting and Related Financial Crime. https://www.asianracing.org/aib/resources last accessed April 29, 2024

4 Yabo Sports (博体育), BOB Sports and Boya Group (博雅集), also known as KOK Sports (KOK体育), are all reported to use the same labor camps.

Connections to European Sports Betting

Vigorish Viper is intimately connected to an ongoing controversy in Europe surrounding the use of football club sponsorships to illegally advertise gambling sites in Asia, particularly in Greater China. Criminal syndicates have drawn sports teams into their illicit activities and leveraged the teams' popularity as a force multiplier. Through a series of shell companies using fake identities and credentials, the Chinese organized crime groups establish brand presence, typically represented by a so-called white label intermediary who provides local representation and bona fides. Players wear the sponsor's logo on their shirt during games, or the logo is advertised on pitchside boards of the stadium, or both. The games are broadcast in China, often illegally, where viewers are enticed to visit the website and bet on their favorite club (see Figure 1). This sponsorship charade has been the subject of robust reporting by investigative journalists and watchdogs over the past several years. Vigorish Viper technology connects most of these stories together and places Yabo at the heart of the controversy.

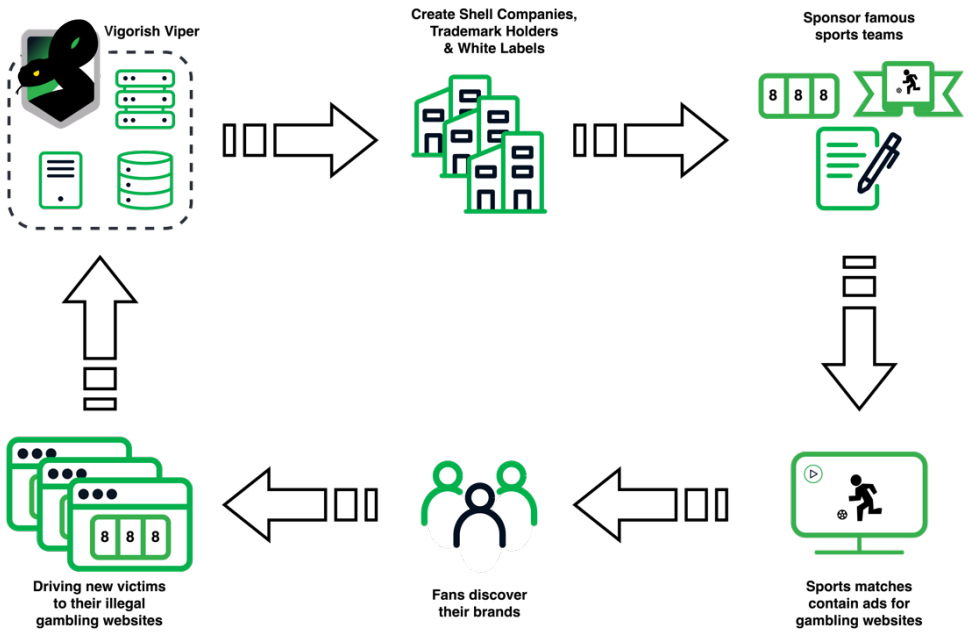


Figure 1. An overview of the Vigorish Viper sports sponsorship scheme

The brazen scheme to victimize Chinese residents through European football sponsorships was, and remains, very successful. It was not until April 2023, after extensive reporting by major outlets, that the U.K. Gambling Commission sanctioned white label provider TGP Europe for "anti-money laundering and social responsibility failures."[5] The commission suspended 14 brands and seized the U.K.-related domain names; 11 were brands associated with Vigorish Viper, including Yabo. When we say they remain very successful, it's because to a great degree their European operations continue, having negotiated new sponsorship deals with French, Spanish, and other European teams. And in spite of the sanctions and additional license

5 https://www.gamblingcommission.gov.uk/news/article/gambling-business-tgp-europe-fined-gbp316-250 last accessed April 29, 2024

conditions, TGP Europe still acts as a white label provider for five of Vigorish Viper's brands. Moreover, at least eight top English football clubs currently have sponsorship deals with Vigorish Viper's brands.[6]

Disclaimer: While this paper refers to the sponsorship of professional sports clubs by various gambling companies, it does not allege any wrongdoing/illegal activity by the sports clubs. References to these clubs are solely for analytical purposes.

Connections to Yabo

For the gambling brands, Vigorish Viper's technology underpins all aspects of the user experience, from the website to chat apps and payment systems. References to Yabo are littered throughout the software and the infrastructure, making it abundantly clear that Yabo developed the software and DNS network. The entire suite includes custom cryptography, branding services, website templates and hosting, mobile apps, secure communications, advertising, and more. It is even likely that Vigorish Viper created the anonymous cryptocurrency payment provider that is embedded into all of their applications. This broad scope of technology made Yabo/Vigorish Viper a sweeping monolithic entity by 2020.

> Gambling is almost completely illegal in Greater China, and yet it is estimated that citizens in the region bet nearly **US$850 billion** annually.

Amid media scrutiny, Yabo was dissolved in 2022, but the remnants of the company were essentially laundered into a series of new entities, including Kaiyun Sports, KM Gaming, Ponymuah, and SKG. While at face value these new companies appear independent, evidence shows they are not. Together the newly established companies make up a supply chain for Vigorish Viper to continue operations unabated and under less scrutiny.

Vigorish Viper's software and infrastructure are sophisticated. The actor has implemented multiple, layered traffic distribution systems (TDSs) using DNS CNAME records and JavaScript, essentially creating a series of gates to protect their systems from unwanted scrutiny. They extensively profile the users, including continuously monitoring mouse movements and evaluating IP addresses. There are multiple versions of the software, and the most advanced version is reserved for the Chinese brands. Vigorish Viper hosts over 170k domain names and tens of brands in an infrastructure that is directly tied to Hong Kong and China.

This report covers our discovery of Vigorish Viper, details of the technical platform, its ties to organized crime, and its role in the European football sponsorship scandals. The material is divided into several chapters.

6 https://www.playthegame.org/news/a-match-made-in-heaven-the-explosion-of-betting-ads-in-european-football/ last accessed April 29, 2024

- Chapter One introduces the sports sponsorship controversy in the context of illegal gambling in Greater China and the role of organized crime. It also furnishes background on the so-called *baowang* economy, which provides "full package" white label technical services for illegal gambling in the region.
- Chapter Two describes our discovery of Vigorish Viper and the impact to our customer networks.
- Chapter Three delves into the technical aspects of Vigorish Viper's software and reveals the breadth of brands found in the network.
- Chapter Four discusses the attributes of Yabo and the obfuscated transformation of Yabo into a set of new commercial entities.
- Chapter Five details the current state of the Vigorish Viper's baowang supply chain.
- The appendices include additional story lines we uncovered during this research and supporting materials.

Why Vigorish Viper?

Vigorish Viper is a name derived from the gambling world's exorbitant fees levied on unlucky bettors. The term *vigorish*, or *vig* for short, is used by organized crime syndicates to refer to these fees. Viper refers to the complex combination of TDSs and convoluted brand relationships that the actor employs to route users to content.

CHAPTER ONE: CHINESE GAMBLING AND SPONSORSHIPS

This chapter provides an overview of how illegal gambling in China, organized crime, and certain European sports licensing are related. It includes some initial findings that tie Vigorish Viper to these controversial sponsorships. It then introduces a particular segment of the illegal gambling economy that caters to online gambling known as the baowang economy. Whereas European football sponsorships are often handled through a white label that provides a legal front for the brand, the baowang economy provides white label technical services for online illegal gambling. Vigorish Viper operates a full supply chain within the baowang economy.

Facebook account promoting money-making potential of gambling apps tied to Vigorish Viper

The Great Sponsorship Scheme

There is a significant amount of media and watchdog coverage of Chinese gambling, organized crime, and the links to sports licensing. We only provide a cursory introduction to the topic and encourage reading the original references to gain a better understanding of these complex subjects.

In spite of severe restrictions, gambling is very popular throughout Southeast Asia and particularly in China and Hong Kong. **It is estimated that bets by residents of Greater China account for more than half of the global illegal gambling economy.**[7] The United Nations Office on Drugs and Crime (UNODC) forecasts a 36% market growth for gambling in the ASEAN region by 2030. Aside from the semi-autonomous region of Macau, casino establishments exist in areas surrounding China, including countries such as Laos and the Philippines. Prior to the COVID-19 pandemic, there was a robust underground tourism industry for gambling, particularly targeting young men.[8] Illegal gambling has had significant economic impacts on the PRC. Beijing authorities reported a record outflow of cash from their economy in 2016: US$725 billion, largely due to cross-border illegal gambling. This outflow destabilized their currency, the renminbi (RMB), and the PRC government was forced to commit US$1 trillion to reverse the effect.[9]

The impact to China of illegal gambling is not only economic. The Asian Racing Federation has reported that illegal gambling in Southeast Asia is controlled by organized crime syndicates and is fueled by modern slavery in which a majority of the victims are Chinese.[10] The organized crime groups who control the vast majority of the illicit services in the region are often referred to as triads.[11] The UNODC published a comprehensive report in January 2024 on illegal gambling in Asia, highlighting the close relationship between triads and their transnational organizations.[12] The UNODC report concluded:

> *Online casinos and cyberfraud have also recently mushroomed across Southeast Asia, particularly in the Mekong since the onset of the COVID-19 pandemic. Alarmingly, organized crime groups running many of these operations have done so with growing sophistication, through the use of data mining and processing, blockchain technology and, increasingly, generative artificial intelligence.*

As a result of the economic and human toll, **China has made significant efforts to stop illegal gambling over the past several years**, arresting gambling operators, agents, and bettors alike. In 2019, the PRC government launched an effort coined Operation Chain Break that targeted entities outside of the mainland. This initiative, which involved international cooperation,

7 https://agbrief.com/news/cambodia/11/10/2023/greater-china-possibly-accounted-for-half-of-global-illegal-betting-turnover-report/ last accessed April 29, 2024

8 https://www.theworldofchinese.com/podcasts/gambling-in-china-how-covid-19-helped-the-industry-grow/ last accessed April 29, 2024

9 https://www.nytimes.com/2016/04/08/business/dealbook/china-foreign-exchange-reserves-rise.html last accessed April 29, 2024

10 https://www.asianracing.org/aib/resources last accessed April 29, 2024

11 https://en.wikipedia.org/wiki/Triad_(organized_crime) last accessed April 29, 2024

12 https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf last accessed April 29, 2024

included actions against both physical and online establishments with mixed legal statuses, collectively known as the gray market, which had previously operated freely in the Philippines and around the region. A September 2021 report by the Asian Racing Foundation concluded:

> *Combating illegal betting is clearly extremely important to Beijing. … Betting operators in so-called grey markets should be aware that their operations targeting Mainland China customers now may be considered outright criminal rather than operating in a legal grey area, regardless of licensing status outside China.* [13]

The Chinese government also cracked down on their own citizens, passing legislation in 2021 that made gambling punishable by up to 10 years in prison.[14] In May 2022, the government said it had identified 90,000 people crossing borders since 2021 to gamble and had broken up 260 gangs facilitating such travel.[15] The PRC government intercepted flights to the Philippines that were reportedly filled with Chinese nationals destined for work in casinos.

Operation Chain Break led to high-profile charges of organized criminal gambling and money laundering against Hong Kong–based Suncity Holdings in November 2021.[16] Suncity was at that time Macau's biggest casino junket with an estimated annual profit of US$2.3 to $2.5 billion. Suncity's CEO, Alvin Chau, was convicted in January 2023 and sentenced to 18 years in prison on charges related to illegal gambling, organized crime, and fraud.[17] Suncity has long been accused of criminal activity, including ties with forced labor camps.[18] For example, Chau signed a US$360 million agreement with Golden Sky Casino for "management and consultancy services" in 2018. The sprawling complex on the Cambodia–Laos border was reportedly used to staff support services for Yabo and other illegal gambling brands with forced labor.[19]

In early 2023, investigative journalists uncovered ties between Suncity's Alvin Chau and the Isle of Man company TGP Europe, which was at the center of a controversy surrounding English Premier League sponsorships.[20] TGP Europe provides U.K. gambling licenses to foreign entities through so-called white label deals.[21] By establishing a U.K. footprint, the foreign company can contract with the sports team to wear their logo on shirts and display it throughout the stadium. **Journalists reported that it was impossible to trace the true ownership of these companies because of the complex series of shell companies and fake identities involved.** Their searches typically dead-ended in the Philippines or the British Virgin Islands (BVI). Making the

13 https://www.asianracing.org/aib/resources last accessed April 29, 2024

14 https://agbrief.com/news/china/09/04/2021/chinas-cross-border-gambling-fight-steps-up-a-notch/ last accessed April 29, 2024

15 https://agbrief.com/news/china/13/05/2022/china-imposing-strict-exit-controls-on-suspected-cross-border-gamblers/ last accessed April 29, 2024

16 https://agbrief.com/news/china/26/11/2021/china-issues-warrant-for-arrest-of-suncitys-alvin-chau-for-gambling-activities/ last accessed April 29, 2024

17 https://apnews.com/article/sports-betting-china-business-6c8edb2e86ff291d01cf49d9ed598bec last accessed April 29, 2024

18 How Organised Crime Operates Illegal Betting, Cybercrime Scams, and Modern Slavery in Southeast Asia https://assets-global.website-files.com/5fbe2bde2b2ef4841cd6639c/651e891f6cca0e3f417cd876_How%20Organised%20Crime%20Operates%20Illegal%20Betting%2C%20Cyber%20Scams%20%26%20Modern%20Slavery%20in%20SEA_FINAL.pdf last accessed April 27, 2024

19 Voluntary Announcement Strategic Partnership with Golden Sun Sky Entertainment Co., LTD. https://www1.hkexnews.hk/listedco/listconews/sehk/2018/0905/ltn20180905525.pdf last accessed April 27, 2024

20 https://www.online-casinos.com/news/industry/premier-league-linked-to-alvin-chau.html last accessed April 29, 2024

21 https://josimarfootball.com/2023/03/14/the-missing-link/ last accessed April 29, 2024

connection between Alvin Chau and TGP Europe was the result of a multi-year investigation into the financial relationships between dozens of entities and created a definitive link between Chinese organized crime and European sports sponsorships.

These sponsorships were established with English Football League clubs, but most notably with teams in the English Premier League. The English Premier League is the most-watched football league in the world, with an estimated 4.7 billion viewers, many in Asia. The logos, including domain names like `fun88[.]com` and `ob[.]com` were televised repeatedly during every match. These sponsorship deals provide substantial income to the team; for example, Manchester United reportedly earned US$3.5 million yearly from their deal with Yabo.[22]

In addition to logo placement on players' shirts, the betting company was often allowed to advertise throughout the stadium. These "technology sponsorships" that allow pitchside advertising have a significant impact on viewers. Researchers in the U.K. studying the impact of sponsorship brands on viewers of English Premier League games found that gambling site logos were shown up to 3,500 times in a televised game and concluded that pitchside hoardings were responsible for over 50% of viewer impressions.[23,24] Although sponsorship costs the gambling firms millions of dollars each year, they receive advertising in a closed market where the potential profit is in the hundreds of billions annually.

The sponsorships are designed to target residents of Greater China. Although advertised on the shirts of European football players, the advertisements are in Mandarin, not the local language. Moreover, the websites advertised are not accessible in Europe; they are reserved for residents of China and Hong Kong.

TGP Europe was sanctioned in April 2023 by the U.K. Gambling Commission for not upholding its responsibilities as a white label provider, specifically those responsibilities related to preventing money laundering and their "social responsibilities" as a representative of the gambling firm. A number of domains were seized as a result. **Eleven of the 14 brands included in the sanctions used Vigorish Viper's platform.** Figure 2 shows the suspension page for `ob[.]com`, which belongs to OB Sports and is also referred to as Oubao, and Figure 3 presents the announcement of a partnership between OB Sports and Aston Villa football club.

22 https://www.sportsintegrityinitiative.com/the-trillion-dollar-gambling-game/ last accessed April 27, 2024

23 https://www.theguardian.com/society/2023/jul/17/more-betting-firm-logos-in-televised-football-games-than-thought-study-finds-premier-league last accessed April 29, 2024

24 Gambling, cryptocurrency, and financial trading app marketing in English Premier League football https://osf.io/preprints/osf/uv974 last accessed April 27, 2024

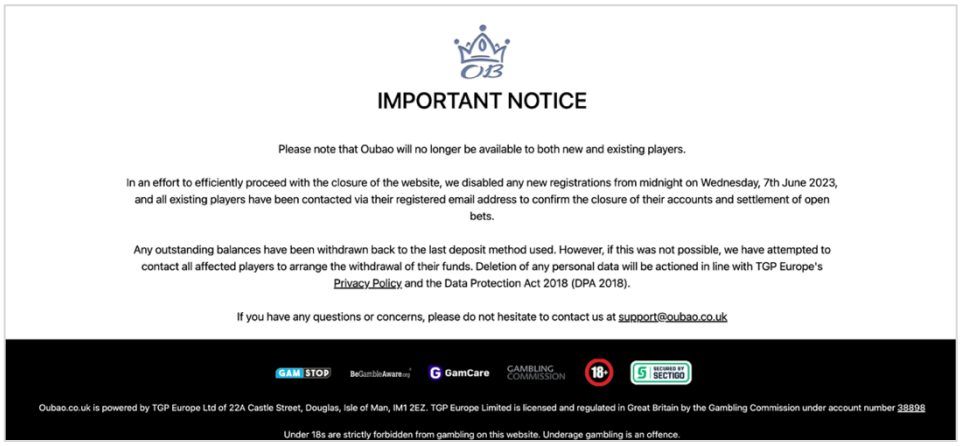


Figure 2. The brand Oubao (OB Sports) was among those included in sanctions by the U.K. Gambling Commission in April 2023; this brand was advertised in China as `ob[.]com` *and is part of Vigorish Viper's network*

Figure 3. Aston Villa announcement of a new video by its Principal Partner, OB Sports. OB Sports is one of the companies whose domains were seized in actions by the U.K. Gambling Commission; it is part of Vigorish Viper's network.

It is not only English football clubs that are engaged in these sponsorships. A number of other European teams have multi-year deals with the mysterious sponsoring firms. In our investigation, we found relationships between domains hosted by Vigorish Viper and teams in the U.K., France, Spain, and other countries. Cricket and *kabaddi* teams in India and elsewhere have also entered into sponsorship agreements to advertise Vigorish Viper brands.[25,26] Because of Vigorish Viper's operational complexities, it can be challenging to associate a team sponsorship, gambling brand, and domain name. As a result, there are likely more sponsorships between Vigorish Viper's brands and European teams than we have validated.

25 https://www.gamblinginsider.com/news/23479/fun88-announces-partnership-with-dabang-delhi-kabaddi-club last accessed April 29, 2024

26 https://www.cricketworld.com/fun88-announces-daren-sammy-as-brand-ambassador/71517.htm last accessed April 29, 2024

包网 The Baowang Economy

While many of the sponsorship deals in Europe use a white label provider to front the brand, the technology underpinning illegal gambling in Greater China also relies on white labeling. White label providers in this context are front-end software companies that are responsible for a specific part of the casino infrastructure: hosting the front-facing page and handling API requests to game and payment providers. These white label providers offer a range of services; customers can purchase components and construct their own sites or rely on the provider to create and operate their site.

A large number of shadowy companies advertise "White Label Casino Services," target Chinese speaking players, and claim they are licensed by regulators. These services are competing with each other for clients and a share of the illegal gambling market. Some of the white label providers steal screenshots from their competitors' websites, claiming that they were the original developer. The providers create a large number of website clones, using different IPs, registrar information, and DNS infrastructure. Each one of those clones contains slightly different information, a tactic meant to shield the advertised companies from scrutiny. Online gambling businesses rely on agents, who might have a personalized page for their customers or manage a cloned website. In addition, many copycat sites are attempting to siphon gambling business from the original ones; Appendix A details one example of this.

The myriad domain names, infrastructure, and websites all blur the line between original and copycat gambling companies, obfuscating the real relationship between the entities. In fact, finding a company name, an address, a phone number, or even an email is quite rare. Moreover, these organizations primarily conduct business through Telegram, further adding to the obfuscation.

The most comprehensive white label service contains all elements of the online gambling economy, from infrastructure to technical support and is advertised on the Chinese internet as 包网 or baowang, meaning "full package" or "full bundle." With a baowang service, every aspect of the business is outsourced to the white label provider.

Creating a white label casino website costs around US$10,000 in the baowang economy with additional fees taken on bets, deposits, and withdrawals. This website creation is typically done by agents using brands established by organized crime syndicates. Once the website is configured, the agent has to market it to bring in gamblers. To accomplish this, agents use direct advertising, search engine optimization (SEO), personal relationships, ads on social media, Telegram groups, and other means.

The white label service provider is responsible for hosting the website, ensuring its availability and integrity, and splitting earnings from the site with others, including with third-party game providers and payment providers. The white label provider also operates the connection to payment providers. Each of these payment providers accepts different currencies, has different geofencing capabilities, and offers different rates for players and intermediaries. In the baowang economy, they will integrate different game providers and streaming services. Each gambling platform is ultimately composed of many seemingly independent services that unrelated companies provide.

The economy is organized into multiple layers of entities with separate functions, which shields the operators from scrutiny and legal consequences. If an individual website was involved in money laundering, all the providers, white labels, hosters, and payment providers can claim they *couldn't possibly* know about it and thus escape jeopardy. This lack of accountability led to an extreme fragmentation of the casino services market, with dozens of individual companies under obscure ownership involved with each website.

Dozens of baowang providers exist with various legal statuses. They are often incorporated in tax havens or countries with a closed company register (e.g., Belarus) and repackage the offerings from game providers into comprehensive websites. Most advertise a website creation time under 10 minutes, under keywords like "Turnkey Games" or "White Label iGaming"; advertisements for these services never mention gambling or betting.

Figure 4 provides an overview of the many components in the supply chain of the baowang economy.

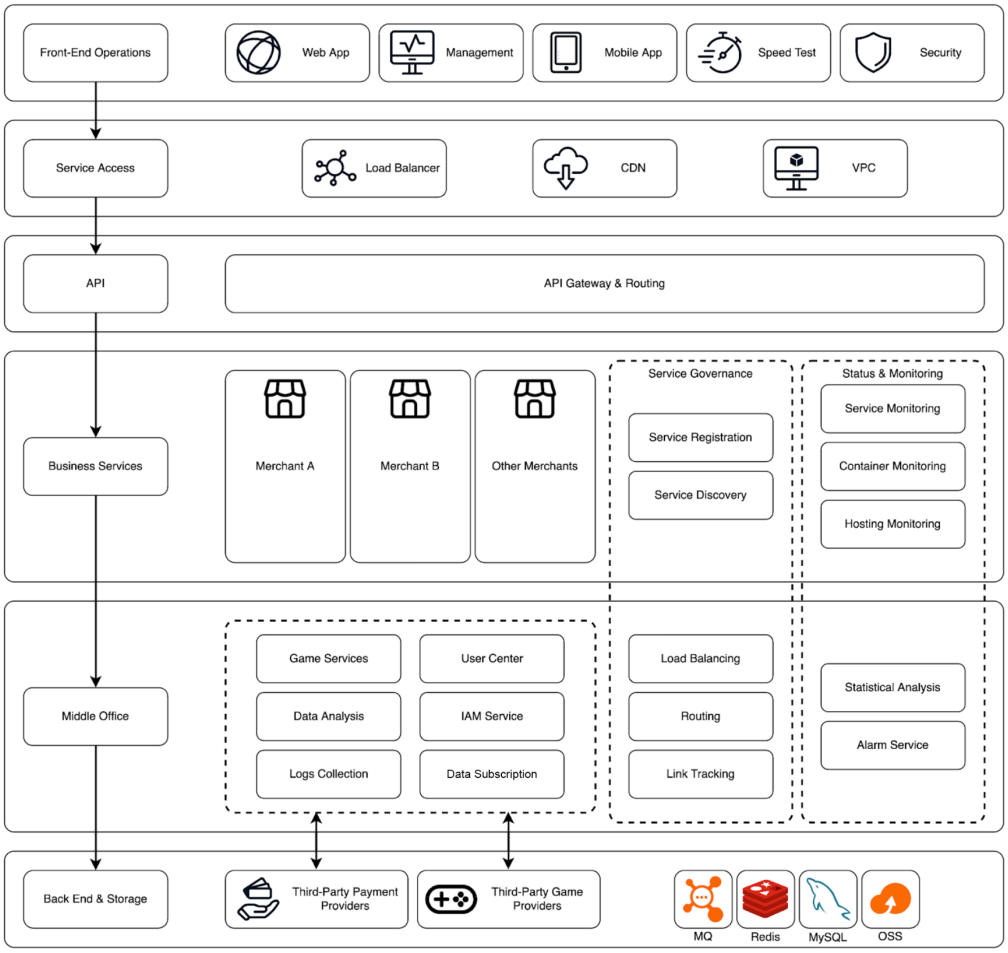


Figure 4. The components of the supply chain within the baowang economy

CHAPTER TWO: DISCOVERY IN DNS DATA

Our investigation was triggered by a single anomalous domain. In this chapter, we describe why that domain, kb[.]com, stood out in a sea of domains we see every day. We show how the gambling site hosted at the domain appears to a user in China and how those users are lured into making large, regular sporting bets on Vigorish Viper's platform. We demonstrate the initial ties between Chinese organized crime, Yabo Sports, entities sanctioned by the U.K. Gambling Commission, and kb[.]com. Using queries observed at our DNS resolvers, we demonstrate that this criminal enterprise extends well beyond the boundaries of Greater China.

Down the Rabbit Hole: kb[.]com

When we started investigating Vigorish Viper, one domain name stood out: kb[.]com. This was before we had discovered the link to TGP Europe and English Premier League scandals. In particular, there were two gnawing questions about the domain and why it was hosted with what appeared to be a sketchy service provider:

- Why kb[.]com? This domain is undoubtedly one of the most valuable domain names in the world. Based on the history of domain name sales, the legacy of the domain and how many ways it can be interpreted, the domain name value is likely over US$5 million, possibly a lot more.[27] Why use such an extremely valuable asset for gambling? Our investigation provided an answer to that question.
- Why use Chinese name servers? All DNS queries going into and out of Chinese IP space pass through the Great Firewall, subject to inspection and alteration. With the Chinese government making big efforts to crack down on players and providers alike, why serve DNS directly from there? It seems extraordinarily risky, and we still have no good answer to that question.

The domain kb[.]com is special in ways unrelated to gambling. Because the domain is so short, so old (originally registered in 1995), and easily interpreted to mean different things, it is widely used around the globe in Active Directory and DNS configurations as a search domain. Many people don't realize that the use of domain names that you can't control, such as kb[.]com, will cause DNS queries to leak to the name server of the domain owner and can be collected across the internet. We can see from global passive DNS traffic, as well as traffic at our own resolvers, that kb[.]com is among those domains widely used by organizations that don't own the domain. In addition, it has been widely used in malware as a red herring. Finally, it is one of many domains being used by a Chinese state actor to probe open DNS resolvers across the internet, as we reported in our blog on Muddling Meerkat. The combination of all these factors means that there are a lot of DNS queries made for kb[.]com around the world, and most of them are unrelated to its current use as a gambling site.

We know that kb[.]com was sold by its original owner, a U.S. marketing firm, to someone in the Jiangsu province of China in mid-July 2020. The domain was again transferred in 2021 to an anonymous entity in the Philippines. Unfortunately, domain name sales are typically not publicly disclosed and so neither the price nor the buyers are known. It is also quite possible that the second transfer was not a sale but just a change of record by the domain owner, an action that is common in domain registrations.

27 https://en.wikipedia.org/wiki/List_of_most_expensive_domain_names

We also know that the **name server domains used by `kb[.]com` are registered in China under the name "yabo"** in April 2020. These name servers also host `yabo[.]com`, the domain name for Yabo Sports. Yabo claimed to be the largest online integrated entertainment platform in the Chinese market in 2021.[28] It was among the companies included in the regulatory sanctions against TGP Europe, and it was brought into the spotlight after entering into a multi-year deal with Manchester United as its official betting partner, while using hired models to pose as their CEO in photographs. Journalist Philippe Auclair, who has reported extensively on the murky Asian sports industry, said about Yabo Sports:

> *Manchester United is thought to have earned 3.5 million euro a year from its deal with Yabo Sports [emphasis added], a Chinese betting company which has also counted Leicester City as a 'global partner.' Remarkably, Yabo, a company which was registered in 2018, managed to build a quite extraordinary portfolio of such partnerships within a year of its creation, signing deals with the Argentina National Football Team, Hertha BSC, AS Monaco, Serie A, Copa América, and FC Bayern Munich amongst others. AC Milan followed in October 2020. Just as remarkably, Yabo Sports does not appear to have any presence on social media, which begs the question: who is using their platform?*[29]

The specific name servers used by `kb[.]com` and `yabo[.]com` appear to have served only a handful of other domains since the name server domain itself was created. The other notable domain name on those servers is `yibo[.]com` of Yibo Sports, the official regional betting partner of the Dutch football team Amsterdam Ajax from 2020 to 2022. The name server domain name**,** `ybvipdns[.]com` likely stands for "Yabo VIP DNS"; the limited use of this particular server for other domains gives us high confidence that `kb[.]com` and Yabo Sports share a special relationship.

KB Sports garnered sponsorships with the French club Girondins from 2020 to 2023.[30] (See Figure 5.) This deal explicitly authorized them to use LED technology on the coveted pitchside advertisements that adorn the stadiums. The technology enables streaming versions of home games to appear to viewers in certain regions. The audience in Asia was exposed to the sponsor and domain name hundreds of times in a single game.

28 https://www.abnewswire.com/pressreleases/yabothe-largest-online-integrated-entertainment-platform-in-the-chinese-market_542161.html last accessed April 29, 2024

29 https://www.sportsintegrityinitiative.com/the-trillion-dollar-gambling-game/ last accessed April 29, 2024

30 https://www.girondins.com/fr/news/32838/kb-sports-et-le-club-font-equipe last accessed April 29, 2024

Figure 5. Chinese domain `kb[.]com` displayed on a deal between KB Sports and the French football club Girondins in October 2023

Unfortunately, we don't know much about KB Sports itself. Like that of the investigative journalists who tackled the corporate identities behind other Asian betting firms, our research led to a series of questionable profiles and entities. According to its empty LinkedIn profile, KB Sports is based in Hong Kong.[31] With no followers and no posts, it follows exactly one company, AG Entertainment in Manila. AG Entertainment boasts in its LinkedIn profile that it provides "the best server and system platform environment, all gambling brands and suppliers are the same as those of Macau casinos, ensuring professionalism and excellence."[32] As of late-January 2024, its website, `www.ag96[.]vip`, as provided on LinkedIn, redirects to Priceline, a well-known travel company unrelated to Chinese gambling.

FC Girondins announced its deal for the 2021 to 2022 season with KB Sports on its website and on LinkedIn.[33] The post was liked by KB Sports and football fans. In a response to the post, "Anna S." said, "Together we make it happen!" intimating some connection between herself and the deal. In that same LinkedIn comment thread, Richard Diet, the head of sponsorship for FC Girondins, congratulates Anna.

But who really is Anna S.? Her title on LinkedIn is "Global Sponsorship Activation Director" at "Sports Company." She has 469 connections with no posts, an unusual combination that threat intelligence groups like ours often associate with fake accounts. Her LinkedIn bio is detailed, claiming she "independently launched partnerships with world-renowned football clubs," including teams in the English Premier League, Spain, Italy, and France. She lists her location as both Mexico and California, formerly of Hong Kong.[34] While her profile says she was educated at Goshen University, a university that doesn't appear to exist, she follows Goshen

31 https://www.linkedin.com/in/kb-ty-48b991217/ last accessed April 29, 2024

32 https://www.linkedin.com/company/ag%E4%BA%9A%E6%B8%B8%E9%9B%86%E5%9B%A2/about/ last accessed April 29, 2024

33 https://www.linkedin.com/posts/fc-girondins-de-bordeaux_sports-activity-6850777817332887552-wuSH/ last accessed April 29, 2024

34 https://www.linkedin.com/in/anna-s-4494941a7/ last accessed April 29, 2024

College, a small self-described Christ-centered Mennonite college in Indiana with under 800 students. We also know she is one of 161 followers of Outlast Sports and Entertainment of Singapore. With a generic name like Anna, no real company name, and a vague, rare job title, it's difficult to learn much more about her.

kb[.]com logo placement in an ad

As with all of the controversial domains, kb[.]com is not available to users in France or elsewhere in Europe. Attempts to visit the site will result in the display of a splash page commonly used by Vigorish Viper that says the page is not available in your region (see Figure 6). **However, it is accessible from mainland China and the SARs of Hong Kong and Macau.** When visited from one of those areas, the user is redirected to another domain—for example, kb830[.]com. The redirection domain changes over time. Additionally, all "right click" functionality is disabled on the site, as is text selection, hindering efforts to investigate or copy the site.

Figure 6. Vigorish VIper access denied page

Figure 7 shows the website as seen from a residential Chinese IP address. Although the websites can be accessed from China, **there are numerous security mechanisms in place even after the page initially loads**, and the server will disconnect if it suspects the user is not a legitimate gambler. The server is continually monitoring the user's actions, as well as their connection. The content is entirely in Mandarin and no translation is available. The web pages contain images of various sports figures and scantily clad young women. The site offers a wide range of categories in which to bet, including football, NBA, soccer, lottos, casino games, online

games, and VIP tables. The site also offers QR codes to download iOS and Android apps. Most of the functionality is behind a login prompt. In addition, the site hosts a support page, offering instant chats with customer support in a web app, but also links to Skype and QQ, a Chinese instant messaging service. Based on our experiments with the site, we believe that this customer support is live and not an AI chatbot. The site also includes fake links to official companies at the bottom of the pages.

Figure 7. Sample `kb[.]com` page images as seen from China

If the user stays idle for some time, and their browsing activity is deemed authentic by the numerous fingerprinting routines run by the server, a random ad is displayed. Most of these advertise financial bonuses for a limited time under conditions that the user bets regularly. The one in Figure 8 offers up to RMB 10,000 (US$1,500) if the user deposits at least RMB 500,000 (US$70,000) over the course of a week.

活动内容

活动期间，会员当日有效投注额满足≥2,000元，即可获得最高2,888元彩金奖励，并记录一次签到（共10日）。若10日累计存款金额满足≥10,000元，且满足≥8日满签可额外获得最高9,888元彩金奖励。

每日有效投注额	每日奖励	10日累计存款金额	≥8日满签彩金
≥2,000	3	10,000	18
≥8,000	10		88
≥30,000	38		198
≥100,000	98	100,000	688
≥160,000	188		1,088
≥300,000	388		1,988
≥600,000	788	500,000	4,088
≥800,000	1,088		5,288
≥1,800,000	2,888		9,888

注：（1）若只满足特定投注条件或者存款条件，均可做降档处理。
（2）≥8日满签彩金按照签到期间的最低档位计算。

Figure 8. An advertisement to kb[.]com users offering up to RMB 10,000 (US$1,500) if a user deposits RMB 500,000 (US$70,000) in 10 days

Using DNS records, we were able to connect `kb[.]com` to OB Sports and Yabo Sports, both of which were entangled in the English Premier League controversy. Figure 9 illustrates the relationships among KB Sports, Yabo Sport, OB Sports, and Vigorish Viper. It remains a mystery how these domains are able to operate undetected with Chinese name servers and a seeming complete disregard for government crackdowns.

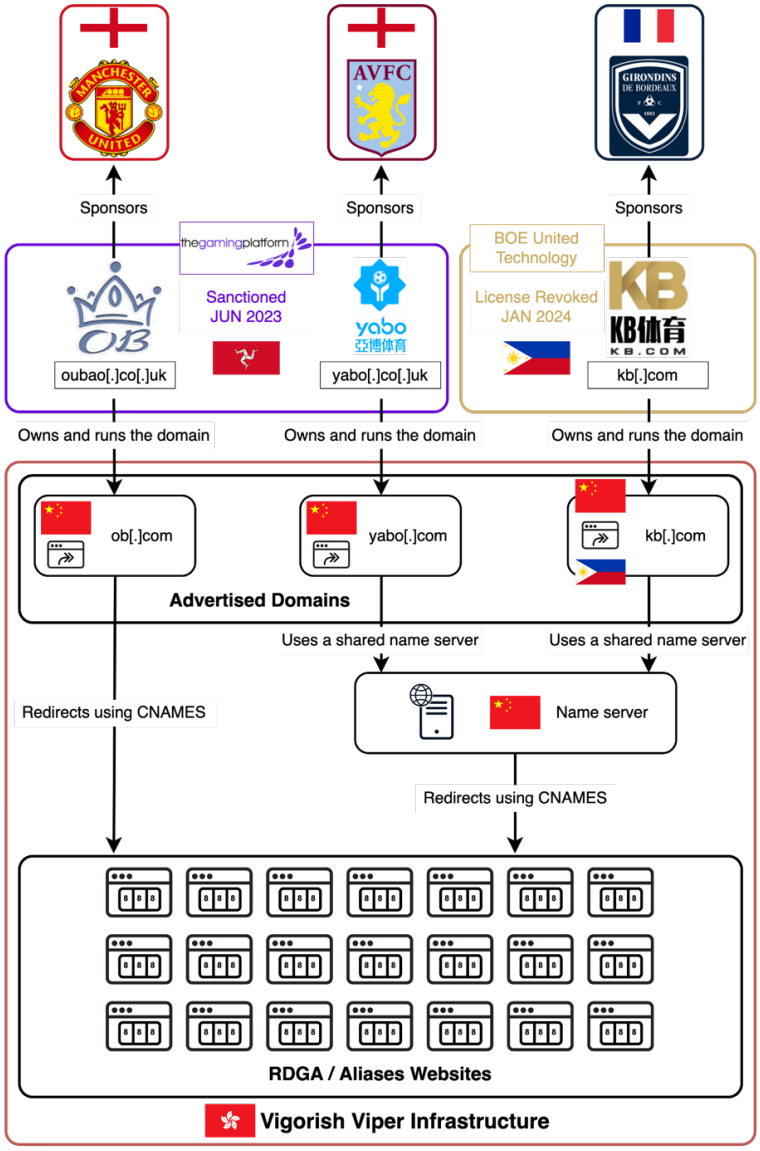


Figure 9. The relationship between Vigorish Viper, `kb[.]com`, and known sanctioned entities

Impact Outside of Greater China

While the high-profile sports sponsorship brands served by Vigorish Viper are limited to users in Greater China, Vigorish Viper's operations target users globally. We found a persistent and broad presence of Vigorish Viper in our customer networks. Using DNS query logs from

December 2023, we created a network graph between the domain names and resolution IP addresses. In our graph:

- The nodes were domains and resolution IP networks (/23 network) associated with Vigorish Viper.
- An edge existed between a domain and a network if a resolution from the domain into that network was observed.
- An edge was annotated with Vigorish Viper's CNAME domain.

The resulting graph had several connected components, as Figure 10 shows. While an individual connected component may incidentally combine multiple brands associated with Vigorish Viper, it serves as an effective first pass at understanding how the domains are related to each other.

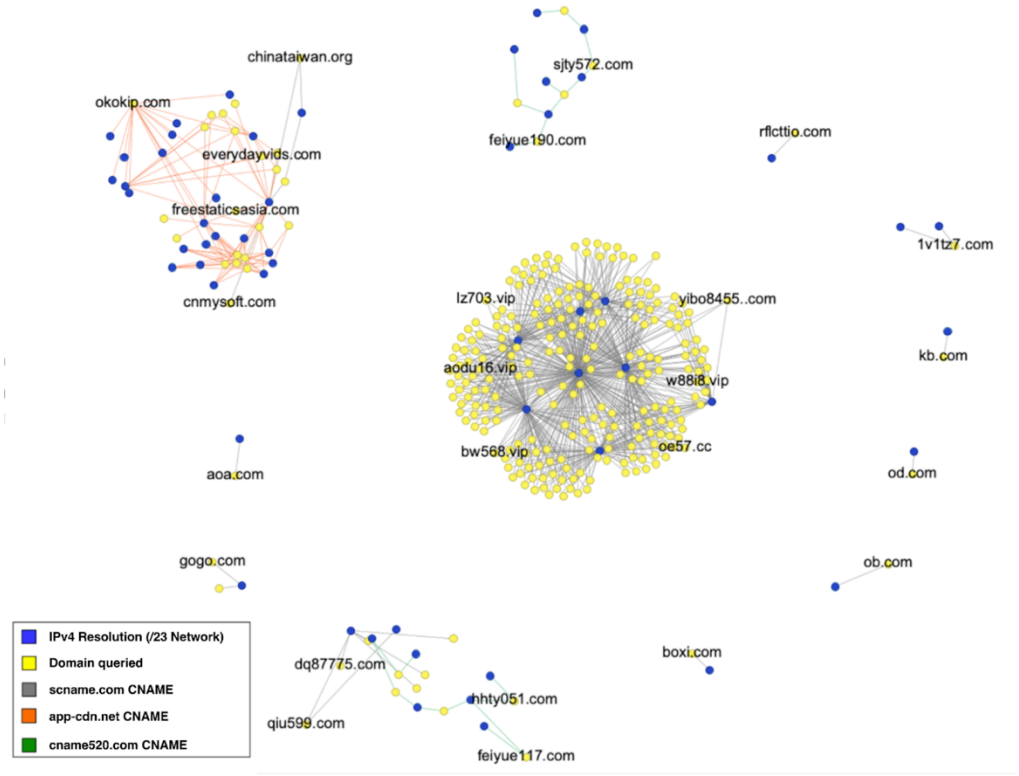


Figure 10. Vigorish Viper's domains resolved at Infoblox DNS resolvers in December 2023 and the associated IPv4 resolution network; edges are colored by the CNAME domain used

What we noticed immediately was that some of Vigorish Viper's activity contains a tightly connected network of several IP networks and many domains, while others are very isolated. At the center of Figure 10 is a connected component that is typical of what we observe for Chinese gambling sites: a large number of domains connected to a set of shared IP addresses, creating a highly connected graph. These domains are often short lived and the actor creates and registers many new domains every day, usually with a registered domain generation algorithm (RDGA). This type of configuration allows for security both through the obscurity of Vigorish Viper's infrastructure and the volume of domains.

In addition to the use of RDGAs for domain creation, we see that Vigorish Viper's clients use domains that are similar to those typically used for scams and phishing attacks, such as `everydayvids[.]com` and `freestatisticsasia[.]com`. Finally, we see a number of very short domain names, like `kb[.]com`, with isolated resolution IPs.

CHAPTER THREE: BRANDS AND TECHNOLOGY

This chapter discusses Vigorish Viper's brands and their technology suite. We have identified dozens of brands in Vigorish Viper's network, some through DNS configurations and others through trademark relationships. Our research found that most brands associated with the European sports sponsorship controversy were part of Vigorish Viper's network, but in addition to those, there were many more.

In order to protect itself from scrutiny, Vigorish Viper uses a defense-in-depth strategy that prevents access to its websites from unwanted visitors. They not only geofence on IP addresses, but they also can detect the use of a VPN. They use complex JavaScript to determine whether a user is genuinely interacting with the site, measuring mouse movements as well as information available in user agent strings. Vigorish Viper utilizes multiple traffic distribution systems (TDSs) to implement these controls. The result is a convoluted chain of domain name redirections that is possibly the most complex system we have encountered.

Vigorish Viper's Brands

Nearly all of the brands included in media coverage of the questionable European sports sponsorship deals are associated with Vigorish Viper, and we have identified dozens more. Of the 14 domains that the U.K. Gambling Commission shuttered in the April 2023 sanctions on TGP Europe, 11 were hosted by Vigorish Viper.[35] As of April 2024, TGP Europe serves as a white label for 5 of Vigorish Viper's brands. Although it was initially difficult to identify and tie together these brands due to the complexity of their infrastructure and how they obfuscate their domain names, we eventually discovered that they proudly advertise the brands in their promotional material (see Figure 11).

35 https://www.gamblingcommission.gov.uk/public-register/business/detail/domain-names/38898 last accessed April 29, 2024

Figure 11. A Vigorish Viper promotional image showing brand logos

In some ways, it is **simpler to say what brands are not part of Vigorish Viper's activities.** When considering Asian betting companies that were covered by investigative journalists and have questionable backstories, we have only found a handful that appear to have no link to Vigorish Viper. The brands included in the U.K. Gambling Commission sanctions with no obvious tie to Vigorish Viper are:

- 138
- 19bet
- i8bet

Other gambling sponsorship brands that were included in reporting by investigative journalists and have no known Vigorish Viper tie include:

- bk8
- br88
- 12bet
- w88

In November 2023, Play the Game reported that one company, BOE United, had active trademarks or trademark applications for a dozen betting sponsorship companies.[36] These brands were all associated with Vigorish Viper, and we used our knowledge of the technology suite to extend Play the Game's findings to connect many more brands. Combining information found in the database of the World intellectual Property Organization (WIPO) with the historical DNS resolution records, we found four additional license/trademark owners related to Vigorish Viper. Some of them were previously included in reporting on Yabo by journalists. The following companies have filed trademark applications for Vigorish Viper's brands:

- BOE United
- Mustafar Limited (Isle of Man)
- Tianyu Technology Inc (Philippines)

36 https://www.playthegame.org/news/mapping-the-territory-of-footballs-lucrative-pact-with-illegal-sports-gambling/ last accessed April 29, 2024

- Rapoo Pro Technology Limited (Philippines)
- Infovine (Philippines)
- Cryonix (Philippines)
- 978 Tech N.V.

Figure 12 shows logos of Vigorish Viper's brands discovered through a combination of trademark applications and DNS infrastructure.

Figure 12. A partial listing of brands in Vigorish Viper's sprawling infrastructure

Vigorish Viper's brands can be recast and connected to different logos and domain names. This lack of transparency adds complexity to the problem of tying brands to each other, to Vigorish Viper and to different sponsors. For example, there are at least three different brand representations of K8 tied to Vigorous Viper, each with different logos and website format.[37] One of these sites even mixes K8 and K9 branding on the same page.

Traffic Distribution Systems

Vigorish Viper operates multiple TDSs, some based on DNS CNAME records. In the simplest terms, a **traffic distribution system** is designed to connect audiences to website traffic. The term TDS is derived from the legitimate online marketing sector, wherein these systems help advertisers reach the consumers most likely to purchase their products. Malicious actors also want to maximize the effectiveness of their operations by making the right connections, but they may also want to prevent certain users, particularly those in the security industry, from visiting their sites. While traditionally implemented as scripts and databases on a website, a TDS can be established and run in many ways.[38]

In addition to TDS systems implemented with a script embedded in the website, actors use DNS in different ways to achieve their goals. A DNS **CNAME TDS** is one such technique in which DNS CNAME records are used to redirect traffic from one domain through another. We first described this technique in our reporting on the threat actor Savvy Seahorse.[39] There are several different methods for implementing a CNAME TDS. Savvy Seahorse, for example, controls both the TDS and the malicious campaigns. They have implemented their TDS so they can redirect a large number of domains to a small set of scam sites, the content of which turns over regularly. Savvy Seahorse registers the domains, manages the TDS, and creates the websites, but uses commercial hosting for the content.

Vigorish Viper typically embeds domain names within a CNAME record. The record may change over time, but there is a direct correspondence between the two; in DNS these are called the canonical name and alias. The CNAME record hostname includes a time-dependent hostname. For example, the domain `kokd08c[.]com` had a CNAME record containing

```
f6b3880f.kokd08c.com.cname.scname[.]com
```

The domain `scname[.]com` is owned by Vigorish Viper and is one of many used in their operations. For this particular CNAME domain, the subdomain "`cname`" is always present. In this example, the hostname `f6b3880f` is a value that changes when the IP address changes.

The example in Figure 13 comes from a query made to our resolvers and demonstrates how Vigorish Viper combines multiple TDSs to control content access.[40] The complete resolution

37 https://urlscan.io/result/65041b39-0f96-434f-9dd8-8500d39036fa/, https://urlscan.io/result/6ea3c58b-7032-42f8-af0f-b5215a872096/, https://urlscan.io/result/bda458b8-868c-491f-a40e-4a2150e9a777/

38 https://blogs.infoblox.com/cyber-threat-intelligence/cybercrime-central-vextrio-operates-massive-criminal-affiliate-program/ last accessed April 29, 2024

39 https://blogs.infoblox.com/cyber-threat-intelligence/beware-the-shallow-waters-savvy-seahorse-lures-victims-to-fake-investment-platforms-through-facebook-ads/ last accessed April 29, 2024

40 https://urlscan.io/result/c0fbd7dc-b8c8-4c46-a705-88dba86e4815/ last accessed April 29, 2024

sequence leads to a gambling site branded as Baibo. The original domain name was `w8818[.]vip`. When this domain is resolved, if the client location conditions are met, it returns a CNAME result that then resolves to an IP address belonging to a Hong Kong–based internet service provider (ISP). The website then fingerprints the user device and redirects to a second domain, in this case `w5553[.]vip`.[41] This second domain is also geofenced and mapped to another CNAME domain. The landing page is found on an unusual port, in this case 35524, and requires the accompanying "i-code." A hyperlink on that page points the user to download the app, on yet another domain with another unusual port. This third domain is again part of a CNAME TDS and geofenced.

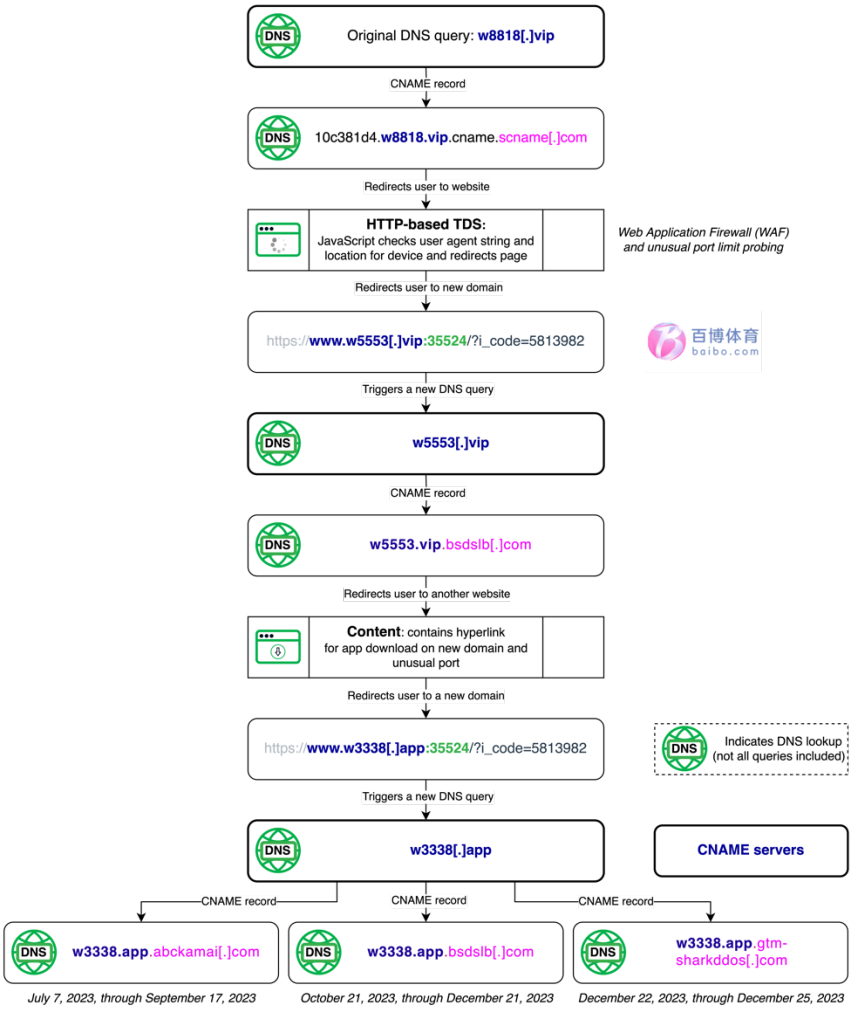


Figure 13. The relationship between DNS domains and Vigorish Viper TDSs, while connecting to Baibo and downloading the app; bold boxes identify CNAME domains

In the example in Figure 13, the chain of TDSs checking for user device and location information led to DNS resolutions for six domains, three of which were CNAMEs (bold boxes).

41 https://urlscan.io/responses/6187c4b5e4080f80360c183e387330600273251b2d98f40e7afdadb95c1fdf47/ last accessed April 29, 2024

In some cases, Vigorish Viper's activities may contain even more layers of obfuscation.[42] The CNAME domain for w3338[.]app has changed over time, which is common for Vigorish Viper's domains. There are two distinct sets of CNAMEs used over several years and they serve different purposes. For example, we can think of the resolution of w8818[.]vip to 10c381d4.w8818.vip.cname.scname[.]com as part of the first CNAME TDS, whereas resolution of www[.]w3338[.]app to w3338.app.abckamai[.]com is part of the second CNAME TDS.

We encountered a dizzying array of Vigorish Viper's defense mechanisms during our investigation. Using multiple VPNs and TOR to access content, we found that:

- They can distinguish between residential, mobile, and commercial IP addresses in China.
- They sometimes restrict TOR exit nodes and other times provide different content.
- They may initially load the site and then use an HTTP 403 (Forbidden) redirection to a seemingly unrelated domain–for example, loa24xr9z-kv-0uh6iq81gnf[.]com.
- They can identify when a VPN is in use during a session and then use HTTP 403 redirection.

In some cases, the CNAME record embeds the original domain—for example, w8818[.]vip had this record value:

10c381d4.w8818[.]vip.cname.scname[.]com

However, in other cases, the CNAME record is more opaque. We are not certain why there is a difference. For example, in January 2024, k8vip[.]com had a CNAME record containing okokip[.]com. One example of that format is:

a7e470c4.okokip[.]com.cname.app-cdn[.]net

All of this redirection requires a large number of domains. As of early February 2024, there are at least 170k active domains in Vigorish Viper's network, and likely many more. These domains are used to support different functions within their system, and while most have CNAME records, some do not.

In Appendix B, we include code snippets that demonstrate the multiple HTTP-based TDSs that Vigorish Viper uses. However, the real functionality of Vigorish Viper's fingerprinting is far too complex to demonstrate with sample code. In the next section, User Experience, we will provide an overview of some of these fingerprinting mechanisms.

42 https://urlscan.io/result/3fa18320-1f9a-4efc-b0ea-c74ebf95b75e/ last accessed April 29, 2024

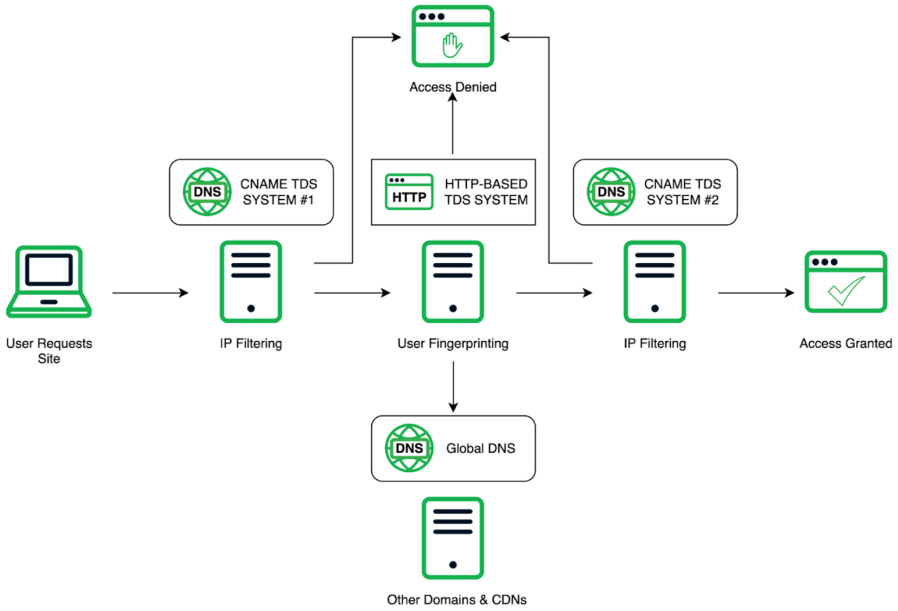


Figure 14. The relationship between various TDSs and DNS associated with Vigorish Viper and the final landing experience for the user

User Experience

Figure 14 offers an overview of the experience a user encounters when accessing a branded site associated with Vigorous Viper, for example, `kb[.]com`. Unbeknownst to them, their **IP address is first checked before the domain is even resolved.** They are then subject to a series of fingerprinting actions based on their device and location, and another series of checks on their IP address. After users make it through the first three TDS controls, another website is loaded. It is usually a domain created by a dictionary domain generation algorithm (DDGA) and using the brand as a prefix, such as `kb7890[.]com:<random_port>`.

The site continues to monitor the user behavior after initially loading. It will periodically check for the integrity of content, if there is any activity on the website, and if the activity looks automated. All of **Vigorish Viper's websites are protected by a web application firewall (WAF)**. If the activity is deemed inauthentic, or when specific brands want to avoid automatic scanning, it serves a puzzle CAPTCHA and the user has to solve it. The CAPTCHA is also served when trying to reach customer support. Figure 15 offers an example. This same protection also exists in the mobile apps and will appear even when there is no internet connection. When the puzzle is solved, it creates cookies named `waf_captcha_marker` and `pdcdn_captcha_token`.

Figure 15. The puzzle presented to restrict access to Vigorish Viper help pages

We were able to determine that the **customer support agents were real people and not AI chatbots.** This finding is consistent with previous reporting by investigative journalists who have described large numbers of Chinese citizens being relocated to the Philippines to support gambling operations. An example of the support chat appears in Figure 16. While the UI may differ across sites, the underlying technology and networking are all the same.

Figure 16. The chat portal for HTH, a sponsor of European football teams among those included in sanctions by the U.K. Gambling Commission in 2023; the slider will reveal a CAPTCHA puzzle

Once Vigorish Viper determines that the user is a human, they begin offering bonuses for regular gambling and technical advice to avoid discovery. Users attempting to access the gambling apps may be given instructions on how to bypass normal download procedures through the Apple and Google Play stores.[43] In most cases, the sites offer their own mechanism to download the app, abusing features designed for beta testing applications (Figure 17).

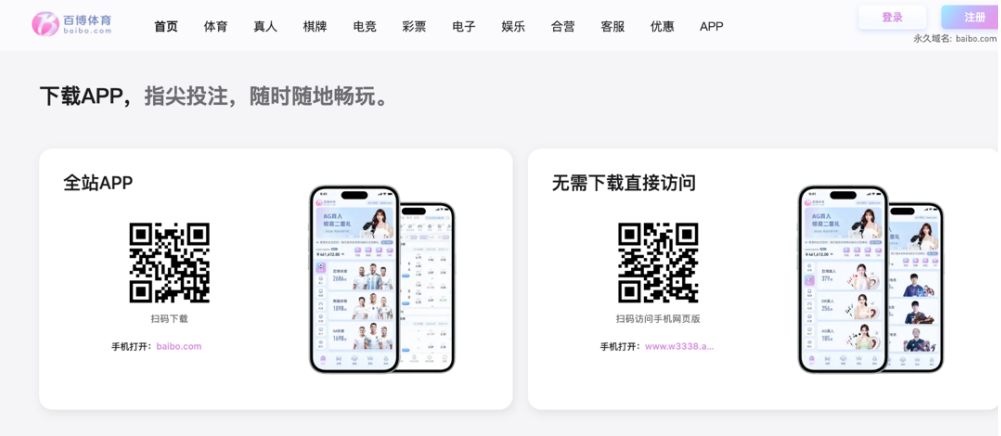


Figure 17. Mobile apps offered from the Vigorish Viper site `baibo[.]com`

Platform users have a range of methods they can use to pay. Vigorish Viper's code is so full of obfuscation that even the backend parameters for payment are hidden. The payment options include WeChat Pay, EBpay, Ali Pay, JD Pay, KOIPay, AstroPay, YunShanFu, UniPay, Net Pay, Fast Pay, and NetBank.

While users can bet and interact directly with the website, **the system strongly encourages them to engage with the so-called agents**. The agents recruit gamblers, and in exchange, earn a share of the losses accrued by those they draw into the platform. Sometimes agents will place bets on behalf of the individuals and manage the deposits and crypto wallets. This assistance makes it easier for visitors to gamble, whether they are wealthy individuals without technical knowledge, people wanting to be shielded from prosecution, or young users with mobile devices.

Agents can be recruited directly on the internet or they can be former gamblers coerced into working off their debts. In certain cases, they are held responsible for the debts accumulated by those they recruit. Monitors of the illegal gambling trade in Asia have concluded that some agents are part of a human trafficking operation. Vigorish Viper's website technology and API are set up specifically to track the agents, as well as the money they are owed. Agent affiliation is at the heart of the business model, whether by choice or force. We will provide more details of this economic model in Chapter Five, which covers Vigorish Viper's baowang economy.

43 https://theathletic.com/3029318/2021/12/28/revealed-the-obscure-gambling-firms-with-untraceable-employees-working-with-your-football-club/ last accessed April 29, 2024

Gamblers and their agents communicate through chat apps that Vigorish Viper has developed. Many of the apps have icons and names that appear to imitate Snapchat or other popular IM software; see Figure 18. Vigorish Viper's apps provide encrypted communications and advertise privacy. However, unlike popular Chinese messengers such as Weibo, the custom apps are not monitored or censored by the Ministry of Internal Security.

Finally, **although these chat apps appear distinct, fundamentally they are all the same.** They have the same backend as the major branded websites and they use the same evasion techniques. The developers also use similar mechanisms to bypass code reviews for iOS and Android devices.

Figure 18. The website for `snaptalk3[.]cc`

Vigorish Viper's network is vast and offers users access to a full spectrum of vices. While victims undoubtedly know they are engaging in illegal activity, they are unlikely to be aware that the brands they see advertised are all connected and that their devices are subject to malware as a result of visiting these sites. Vigorish Viper's mobile applications are distributed outside of the official app stores, circumventing security reviews and exposing users to considerable risk.

Separately, criminal organizations have stolen the personal identities and credentials of gamblers, including Vigorish Viper's users, through the use of fake websites and by hacking gambling sites. In Appendix A, we describe one fake website operator that we discovered during our research, and in Appendix D, we show how Chinese hackers are stealing user credentials to the sites.

Under the Hood

This section provides more technical details about how Vigorish Viper's sites operate. **Central to their platform is a very large, embedded WebAssembly (Wasm) file** that exists on both the mobile and desktop sites. Vigorish Viper's sites:

- Always offer the same visual template, and the same categories of games: live casino games, lotteries, betting for eSports and live sports (mostly football and basketball), and a collection of quick online games (fishing, virtual roulette, etc.).

- Run multiple versions of their front-end code, which includes a variable amount of sophistication and obfuscation.
- Rely heavily on control flow obfuscation and bogus debugging statements to hamper analysis.
- Incorporate a sophisticated encryption algorithm dubbed "scytale" to stream gambling data from the backend. This algorithm also verifies the integrity of the data.
- Store a large number of unique domains locally, in an AES-encrypted file. Those domains are used for illegally streaming games or hosting mobile applications.
- Abuse `fingerprint[.]com` fingerprinting services to avoid scraping by third parties.
- Include DNS prefetch queries for certain content, presumably to optimize performance while still geofencing the material.
- Use variable redirection with an HTTP-based TDS to different domains based on user fingerprinting.
- Use uncommon and highly varied ports for TCP access to websites.
- Include parameters in the landing page URLs, typically including `i_code=<random number>`.
- Use fixed API keys on most services and reuse encryption keys across brands and websites.
- Have historically used direct IP address connections but evolved to use a wide range of domains.
- Grab the current time from their servers in multiple ways over time, presumably to use for live matches and cryptographic purposes.
- Abuse the STUN protocol to identify the client's IP address.
- Use `sribgio[.]com` or other copycat domains for their CRM platform.
- Stream matches and betting data through WebSocket and MQTT requests to domains hosted by Zhejiang Taobao Network Co. (Taobao), a Chinese ISP owned by Alibaba.

Figure 19 illustrates the overall process between when a user attempts to navigate to one of Vigorish Viper's brands—for example, `kb[.]com`—and the ability to place bets.

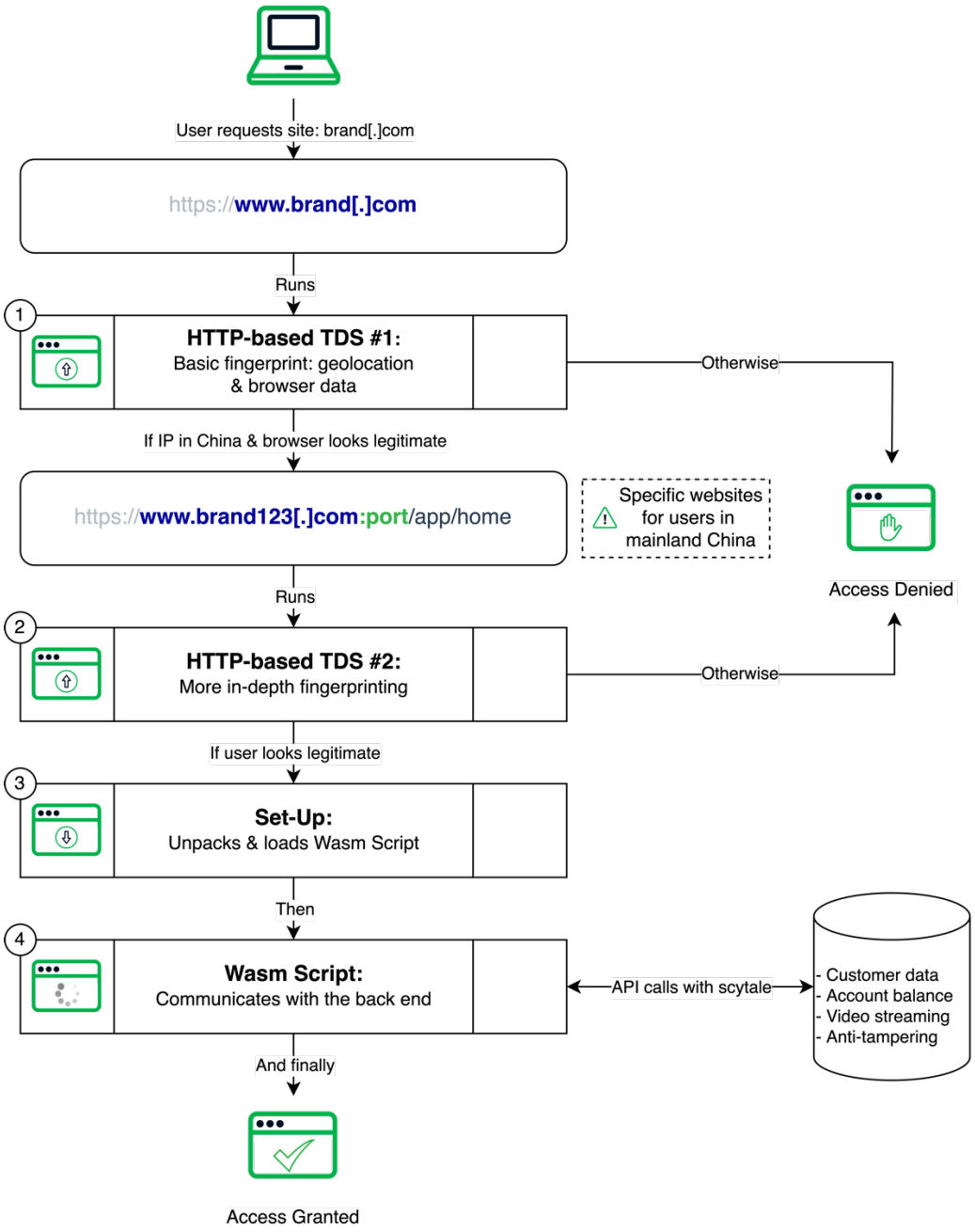


Figure 19. An overview of the steps that occur between when a user attempts to visit one of Vigorish Viper's brand domains and when they are allowed to bet on the site

Once the client has passed through the initial CNAME TDS barrier, their connection enters the HTTP-based TDS.

Step 1: The process always starts with a JavaScript loader (`loader_v<version>.js`), which is a heavily obfuscated, third-party commercial JavaScript applet that fingerprints browsers. At this step it will fingerprint the user beyond the IP-based screening that occurred within the first CNAME TDS. Then the loader is downloaded from `fpnpmcdn[.]net` and reaches out to other

domains operated by `fingerprinting[.]com` (`aps1.fptls4[.]com` and `aps1.fptls[.]com`). All of Vigorish Viper's domains use the same API key for these connections. If the fingerprinting API deems the browser authentic, and the geolocation checks still return a valid country, the website will start serving its content.

Step 2: After a connection is made to the redirected URL, the second phase of fingerprinting begins. Note that the redirection URL, as we described earlier, is always for a different domain than the original brand, and the connection is often made on a nonstandard port. Additionally, the DNS resolution for that redirection domain occurs through a second CNAME TDS, as shown earlier in Figure 14. Throughout the entire user experience, Vigorish Viper is diligently protecting their content.

Step 3: Following the second stage of heavy fingerprinting, the JavaScript code unpacks a large Wasm application that can exceed 400 MB and exists in both actor-controlled websites and mobile applications.

Step 4: The Wasm application is used to communicate regularly with the backend through encrypted calls. Every few seconds, the app makes an encrypted query through the API, and the integrity of the communication is verified at multiple points to prevent tampering with the games. These API calls use HTTP POST requests with the application type scytale, a reference to an ancient tool used for transposition ciphers. We were unable to determine whether Vigorish Viper is using a third-party tool for this purpose or has implemented their own system.

The JavaScript calling the API and unpacking the .wasm file exceeds 17k lines and is heavily obfuscated. After deobfuscating it, we can see that the API enables:

- Automatic and configurable setup of websites with customizable themes, account IDs, customer service URLs, and more
- Retrieval of customer information, including name, phone number, account balance, account numbers, VIP status, and other details
- Fetching and streaming of live videos and audio, either of sports matches or live casino games with a croupier
- Handling of bets in real time and with the ability to bet in multiple "rooms"
- A complete interface with banks, online payment solutions (Alipay, direct transfers, and the like) or cryptocurrencies, allowing the user to make withdrawals, deposit money, transfer it to a credit card, and perform other tasks
- Creation of mobile applications for Android and iOS, and retrieval of download links. For iOS apps, this includes a self-signed certificate and a link to another domain hosting the .ipa file. This bypasses AppStore security checks by abusing the less-restricted mechanism used for testing an application, rather than downloading a regular app
- Retrieval of current games and betting odds

Most of the site functionality relies on a separate group of websites, specializing in video, app distribution, or football streaming. Information about those websites is held in local storage on the user's device, and Figure 20 gives an example of that content.

Key	Value
buried_point_from	
navCurrent	dz
QRCODEID-6aa8a346-c1ee-47a6-9054-afda88708671	"https://www.ym251.app:30011/?sport=1"
navIndex	0
QR_ID077CB826-01F0-4A2E-ABF1-C6E8FF370BFF	"https://www.ymvip9.com:35531"
QRCODEID_APPDOWN_FROSTED2_3	"https://download.6524oe.com/files/package/yamei_0818141511.apk"
buried_point_r_code	
QR_IDC82D01F0-D879-4B74-AE94-4F43ED689B99	"https://www.ymvip9.com:35531"
QR_IDD837B317-0D04-4A99-A33C-255E20AA909D	"https://www.ym251.app:30011/?sport=1"
QR_IDAE0BCBC8-A108-4D94-8261-D6088D7403D8	"https://www.ym1370.com:35524"
buried_point_i_code	
lastRoute	/login
QRCODEID-c74f8616-250e-40e9-8da7-6f566d01e589	"https://www.ym1370.com:35524"

Figure 20. An example of data stored by Vigorish Viper on the user's device

Over time, Vigorish Viper's software, TDSs, and networking have all evolved. The actor also appears to use the most advanced defenses for their most valuable content—the major sponsorship brands and associated domains that specifically target Chinese residents, including version 3.8.32 of the loader. In contrast, for example, sites targeting Vietnamese speakers used version 1.11.3 of the loader in early February 2024.[44] (See Figure 21.) Although less sophisticated, these domains often still have geofencing in place to limit access to certain regions.[45]

Figure 21. The webpage for `k8[.]cc` targets Vietnamese speakers; this site used version 1.11.3 of the JavaScript loader in February 2024

The logic of all the different websites and their communication with the backend are the same, even though the websites are written by different people with varying degrees of skill and the variation in code or tools is not consistent with changes in branding. These inconsistencies between websites have allowed us to better understand how Vigorish Viper's technology suite and operations work.

44 https://urlscan.io/result/1c115fd5-fa38-4024-9108-66906ffe69aa/#summary

45 https://urlscan.io/result/80264fc3-0fc7-41c5-b300-eef3c0dd21c3/

The website developers are often carefree and make a number of operational security (OPSEC) slipups, including forgetting to use the obfuscated versions of the JavaScript code they usually use. On more than one occasion, developers forgot to remove mentions of other brands. They also consistently reused API, AES, and XOR keys throughout the code. Some examples of shared code and contact information appear in Figures 22 and 23. **The fact that most domains rely on the same backend helps us to assess with a high degree of confidence that** the large number of brands are mainly created to confuse investigators.


```
{
    "data": {
        "api_name": "FBTY",
        "client_maintain": "0",
        "cn_beg_maintenance_time": "2024-02-26 13:55:00",
        "cn_end_maintenance_time": "2024-02-26 15:35:00",
        "id": "66",
        "information": "场馆维护中，期间可前往半岛体育场馆进行游戏，感谢您的支持！",
        "maintain_endtime": "2024-02-26 15:35:00",
        "maintain_starttime": "2024-02-26 13:55:00",
        "on_line": "0",
        "rebate_copy": "",
        "recommend_text": "FB SPORTS",
        "recommend_venue_name": "OBSPORT",
        "recommend_venue_title": "半岛体育",
        "time_desc": "2024-02-26 13:55:00至2024-02-26 15:35:00",
        "web_rebate": ""
    },
    "message": "查询成功",
    "status_code": 6000
}
```


*Figure 22. Decrypted backend communication from a Bandao Sports-branded website; the "recommended venue title" is named after other brands such as OB Sports and FB Sports and it will be displayed as "**半岛体育**", which matches Bandao*

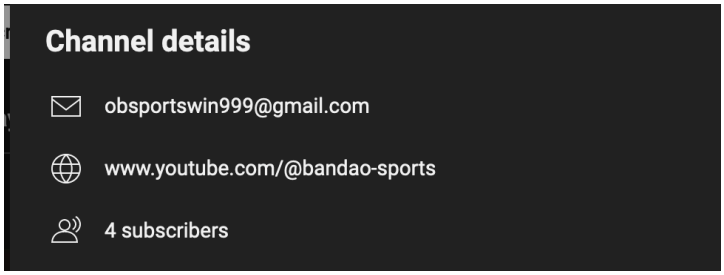


Figure 23. The official Bandao Sports YouTube account using an OB Sports email

A Vast Enterprise

In addition to gambling, **Vigorish Viper's CNAME TDSs serve illegal streaming and pornography sites.** In our research, we have established disjointed sets of CNAMEs that are used as TDSs for their most advanced software and high-profile brands. In addition, we have found other sets of CNAMEs that have many intersections, share a similar structure, and host similar content. Vigorish Viper uses all of these possible CNAMEs and a massive number of domains to support a sprawling enterprise targeting users throughout Southeast Asia and the region's diaspora.

Some of the domains used for streaming are long-registered domains that Vigorish Viper picked up after the original registration expired. For example, `chinataiwan[.]org` is a long-registered domain that Vigorish Viper acquired after it was dropped by its former owner in 2022. It originally hosted a consolidated news site aimed at an audience in Taiwan.[46] However, as Figure 24 shows, it now hosts advertisements for live sports streaming services. Unlike the high-profile sponsorship brands, Vigorish Viper appears to distribute many of these domains via spam messages. The spam messages may have references to promotional codes and are overall less sophisticated than Vigorish Viper's primary networks. We have found these types of sites to be prevalent across our customer networks, adding to the likelihood they were distributed via spam.

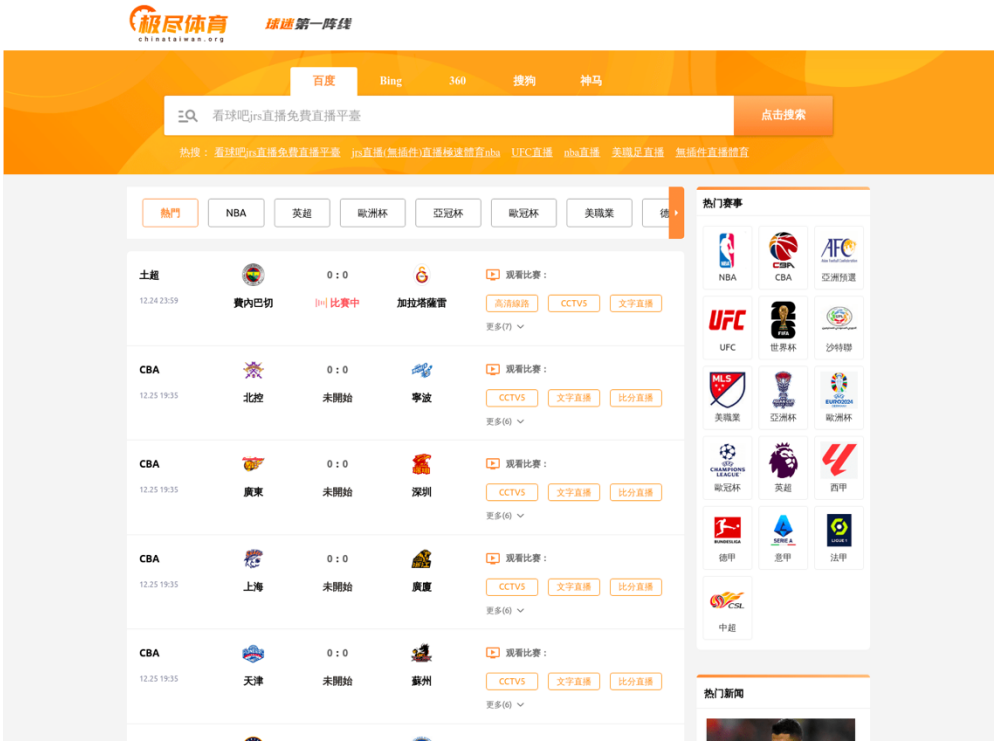


Figure 24. The website hosted at `chinataiwan[.]org` offers sports streaming services

We also know that Vigorish Viper's brands heavily recruit affiliate advertisers. By directing users to their websites, users gain commissions, including Bitcoin referral programs.[47] Members of the casino who successfully draw in new users in most cases receive bonuses that enable them to gamble more, rather than get cash payouts. Some of Vigorish Viper's brands, like TLCBet, claim that affiliates can receive 25 to 45% of the revenue generated from recruited players.[48]

There appears to be general network segmentation within Vigorish Viper's network for different activities; however, on a fairly regular basis, the segmentation will be broken, creating a bridge

46 https://web.archive.org/web/20100418204924/http://www.chinataiwan.org/ last accessed April 29, 2024

47 https://bitcoincasinoaffiliates.com/referral-program/ last accessed April 29, 2024

48 https://bitcoincasinoaffiliates.com/review/tlcbet/ last accessed April 29, 2024

between activity that otherwise appears independent. For example, DNS queries for the domain `chinataiwan[.]org` have contained both CNAME records that are subdomains of `scname[.]com` and of `greywolffast[.]com`. The former, `scname[.]com`, is tightly connected with Vigorish Viper's most valuable and protected content, while `greywolffast[.]com` is used for a broader set of gambling, streaming, and pornography sites. This is not an isolated example. These overlaps lead to a series of small clusters of CNAME TDS domains and a sprawling set of illegal content all leading back to the Yabo Group through network connections, registration information, hosting, and software.

CHAPTER FOUR: THE CHANGING FACES OF YABO

Based on our accumulated evidence, **we have concluded that Vigorish Viper's technology suite and network were developed by Yabo**. Several investigative journalists have tried to unmask the individuals behind the mysterious Asian betting sponsors and were unable to find the true owners due to the complex financial structures that are in place. We faced similar challenges with Vigorish Viper. Some gambling sites state that the parent company is incorporated in a specific jurisdiction (often the British Virgin Islands) on a specific date, but it turns out to be either impossible to verify or verifiably false. New brands are constantly being created, and others are being repurposed. There is an independent series of shell companies for each brand, and those shell companies often have names similar to unrelated companies or "competitors" of the brand. Vigorish Viper and their clients often use two or three letters for branding (DB, KB, FB, OB, etc.) and switch between Western and Chinese script, creating further ambiguity. The advantage that we had in tracing and mapping Vigorish Viper, in comparison to doing the same for individual brands, was through **commonalities in the source code and DNS infrastructure**. Because of the tangled and murky ownership of the gambling companies, we are unable to determine how many of Vigorish Viper's brands are ultimately controlled by the owners of Yabo. If you feel like this sounds confusing, you're not alone and you're not wrong—read on!

In the sections that follow, we will illustrate the complexity of attribution by starting with Yabo Sports, the company most definitively linked to Vigorish Viper's software, and analyzing its connections with other entities. Keeping track of all the company names and their relationship with Yabo is difficult. These are the critical findings detailed in the rest of this chapter:

- We know that Yabo Sports is integrally tied to Vigorish Viper's development and operation.
- Yabo Sports, also called Yabo Group, was trademarked by Tianyu Technologies and used as a sponsorship brand.
- Watchdog groups and investigative journalists have labeled Yabo Sports as an organized crime syndicate.
- In December 2022, as Yabo became embroiled in controversy, it announced a new flagship brand, Kaiyun Sports, to "circumvent the potential restrictions of international antitrust regulations."[49]
- Yabo was reportedly dissolved about the same time, but before that happened, Yabo also announced an exclusive API partnership with OB, also known as Only the Best. Yabo and

49 https://www.linkedin.com/pulse/kaiyun-new-high-end-brand-created-yabo-group-eve-2022-ayesha-khatun/ last accessed April 29, 2024

OB were marketed as separate entities, but their networking, DNS configurations (both tied to Vigorish Viper), and social media indicate they are one and the same.

- OB was, at least partially, integrated into another company, DB Games, whose website offers white label gambling services that also match those enabled by Vigorish Viper.
- In 2023, a newly formed company, Ponymuah, acquired OB and seems to have acquired DB Gaming as well, essentially bringing together the original Yabo technology (i.e., Vigorish Viper–related) components.
- Ponymuah falsely claims to be a registered gambling provider in the British Virgin Islands.
- The Ponymuah CEO appears to be a puppet figure whose only established credentials connect him with Tianyu Technologies, the trademark holder and former operator of Yabo Sports.

Through a maze of connections, we can conclude that Vigorish Viper now falls under Ponymuah and that Ponymuah is likely controlled by the same individuals as the original Yabo Group.

Yabo Sports Technology

The story of Yabo Sports is complex. In any narrative, Yabo Sports plays a pivotal role in Vigorish Viper's far-reaching criminal operations. We found references to **Yabo Sports and Yabo in Vigorish Viper's software, in registration data, and in name server domain names**. Yabo Sports is used interchangeably with Yabo Group. Yabo is connected to Tianyu Technologies and Cryonix through trademark filings, both based in the Philippines. The former is also directly linked to a number of other controversial sports sponsors. Both companies claim to develop gaming technology and have registered in the Philippines as offshore gambling (PAGCOR) enterprises. The PAGCOR license for Cryonix appears to still be valid in 2024.[50]

So what is Yabo Sports? It is an extraordinarily controversial betting sponsor. In spite of being established only six years ago, Yabo Sports is a giant in Greater China. According to the Asian Racing Foundation's 2022 "State of Illegal Betting Report," **a single agent syndicate promoting Yabo in a single province earned Chinese yuan (CNY) 6 million (US$925,000) per day** in 2019 and had made CNY 100 billion (US$1.5 billion) in profit over time. Authorities said Yabo had 80,000 agents and 5.8 million customers in Sichuan Province alone (7% of Sichuan's population).[51] Yabo Sports reportedly dissolved in 2022; however, the data we have indicates that instead of truly disbanding, the company has rebranded and evolved.

While Yabo Sports claimed to be registered and regulated in the British Virgin Islands, the BVI government's Financial Services Commission (FSC) issued a public statement in October 2020 to refute these claims and to make it clear that "the entity has never been licensed or regulated by the FSC to carry on any type of financial services business."[52] The statement went on to say "The FSC hereby informs the public that YABO SPORTS AND ASIA GAMING is not a British Virgin Island (BVI) registered company and has never been licensed or regulated to carry on investment business, or any financial services business, in or from within the Territory."

50 http://www.amlc.gov.ph/images/PDFs/LIST%20OF%20REGISTERED%20DNFBPs.pdf last accessed April 29, 2024

51 https://assets-global.website-files.com/5fbe2bde2b2ef4841cd6639c/62844a249c7d1e17ec718f02_State-of-Illegal-Betting-2022_v11-RGB-opt.pdf last accessed April 29, 2024

52 https://www.bvifsc.vg/library/alerts/public-statement-17-2020-yabo-sports-and-asia-gaming last accessed April 29, 2024

In advance of the 2022 Qatar World Cup, the **Yabo Group (Yabo Sports) launched Kaiyun Sports as the new flagship brand for the company.** A short article on LinkedIn stated that "Kaiyun Sports has the same product design as Yabo Sports, but has more generous preferential policies."[53] In other words, Kaiyun offers more promotions to entice users to play for longer periods of time. Figure 25 shows a World Cup–themed advertisement for Kaiyun Sports. This brand launch came when Yabo Sports deals in England and elsewhere were under great scrutiny.

Figure 25. Yabo Group announces a new Kaiyun Sports brand, essentially to replace the controversial Yabo Sports for the 2022 World Cup in Qatar

Kaiyun Sports was immediately placed under the same scrutiny. **Similar to Yabo Sports, Kaiyun Sports claimed to be registered in the BVI, but reporters could find no evidence supporting that claim.**[54] What journalists found was that the purported Chief Marketing Officer, and only named individual connected to the company, did not appear to exist. In spite of these concerns, English Premier League team Nottingham Forest entered into a shirt licensing deal with Kaiyun Sports in August 2023, using TGP Europe as a white label provider.[55] As of April 2024, Kaiyun is a sponsor of four top English teams, but the U.K. website still shows no content (see Figure 26).

53 https://www.linkedin.com/pulse/kaiyun-new-high-end-brand-created-yabo-group-eve-2022-ayesha-khatun/ last accessed April 29, 2024

54 https://www.dailymail.co.uk/sport/football/article-12462035/Nottingham-Forest-announce-controversial-shirt-sponsorship-deal-online-betting-firm-Kaiyun-Sports-despite-concerns-club-quoted-Kaiyun-chief-does-not-appear-exist.html last accessed April 29, 2024

55 https://www.dailymail.co.uk/sport/football/article-11661895/MPs-want-investigation-links-jailed-Chinese-billionaire-clubs-betting-partners.html last accessed April 29, 2024

Figure 26. Tweet demonstrating that Yabo's "premier" brand Kaiyun had no U.K. website presence in April 2024

Yabo Rebranding Over Time

In addition to creating the Kaiyun brand, **Yabo also "partnered" with another company named OB as its exclusive API provider.** OB is also known as OBGM and Only the Best in various literature. To illustrate how confusing the business relationships in this economy can be, we strongly suspect but are unable to confirm whether OB is related to OB Sports, aka Oubao, the owner of the domain `ob[.]com`, a brand cited in the U.K. Gambling Commission sanctions, although they share the same initials and are both intricately tied to Yabo.[56] An announcement of the OB partnership with Yabo is shown in Figure 27. A Kaiyun GitHub page offers a template website closely resembling one of Vigorish Viper's but lacking specific security and API features.[57] Additionally, the links in the template website point to live websites controlled by Vigorish Viper.

56 https://www.playthegame.org/news/meet-the-hydras-tracing-the-illegal-gambling-operators-that-sponsor-football/ last accessed April 29, 2024

57 https://kaiyuntiyu.github.io/ last accessed April 29, 2024

Figure 27. OB was announced as the exclusive API partner for Yabo before it was dissolved

Although they were marketed as separate entities, **we have a high degree of confidence that OB and Yabo were controlled by the same individuals.** Both companies shared servers and IP addresses over a long period of time, and the `yabogm[.]com` website displayed a phone number tied to OB before being taken offline.[58] As we'll see through the remainder of this chapter, the entities surrounding Vigorish Viper and Yabo continue to morph over time and yet remain intertwined, through mergers, acquisitions, and rebrands.

In 2022, some portion of OB became DB Games, aka Duobao Gaming, another company with questionable credentials. The name "duobao" means treasure hunt in Mandarin. The domain name `obgm[.]com` was previously used to host a website for OB and now redirects to `dbgaming[.]com`, a domain name owned by DB Games. The website hosted at this domain name claims DB Gaming is licensed by the Curaçao Gaming Control Board (Dutch Caribbean). However, no company with a fitting name exists in Curaçao, and according to online records in April 2024, `dbgaming[.]com` was not licensed to operate in the country.[59]

The DB Gaming website lists a number of the brands present in Chinese illegal gambling, and it offers a full explanation of the payment structure and costs associated with running an illegal gambling website for Chinese users. Its website offerings explicitly list payment amounts for players in China (see Figure 28).

58 https://web.archive.org/web/20200805071313/https://www.yabogm.com/ last accessed April 29, 2024

59 https://www.curacao-egaming.com/public-and-players/authenticity last accessed April 29, 2024

DB GAMING Home Products Collaboration Sub-line products Latest News About Us Contact Us Careers

External Game API

Sports	Supported languages	Demo Site	Rate (China)	Rate (Southeast Asia)	Rate (South Latam)	Wallet Type
FB体育	CN/TC/EN/VN/JP/TH/AR/DE/ES/FR/India/KR/PT/RU	fb.vip/ns-official-pc/index.html	(0-3M) 10% (3-6M) 9% (6M-10M) 8% 10M>7%			Transfer Wallet/Single Wallet
SABA沙巴	CN/TC/EN/TH/VN/ID/PT	sabab2b.com	(0-2.5M)10% (2.5M – 6M) 9% (6M – 8M) 8% 8M> 7%			Transfer Wallet/Single Wallet
IM	CN/EN/TH/VN/ID	inplaymatrix.com/products/imesports/index_cn.html	< 2.5M 10% (2.5 – 5M) 9% (5M – 25M) 8% 25M> 7%			Transfer Wallet/Single Wallet

Live Casino	Supported languages	Demo Site	Rate (China)	Rate (Southeast Asia)	Rate (South Latam)	Wallet Type
Evolution	All Languages		(0 – 1M) EUR 13% (1– 3M) > EUR 11% 3M > EUR 9%	(0 – 0.25M) EUR 11% (0.25– 0.5M) > EUR 10% 0.5M > EUR 9%		Transfer Wallet/Single Wallet
DG	All Languages		(0 – 3M) 8% (3M – 5M) 7% (5M – 10M) 6% (>10M) 5.5%			Transfer Wallet/Single Wallet

Figure 28. DB Gaming External Game API offerings; these include targeted languages and the rate for China and Southeast Asia

The DB Gaming website also offers examples of administration panels for a site purchased from them (Figure 29). The **communication of these panels** with the backend and image hosting servers **matches the frontend** we have observed **on thousands of Vigorish Viper's websites**. The demo website showcases streaming games, whether it is football or eSports. The video player includes highlight detection, replay, some voice commentary in Chinese, and real-time animations if no video is available or bandwidth is limited.

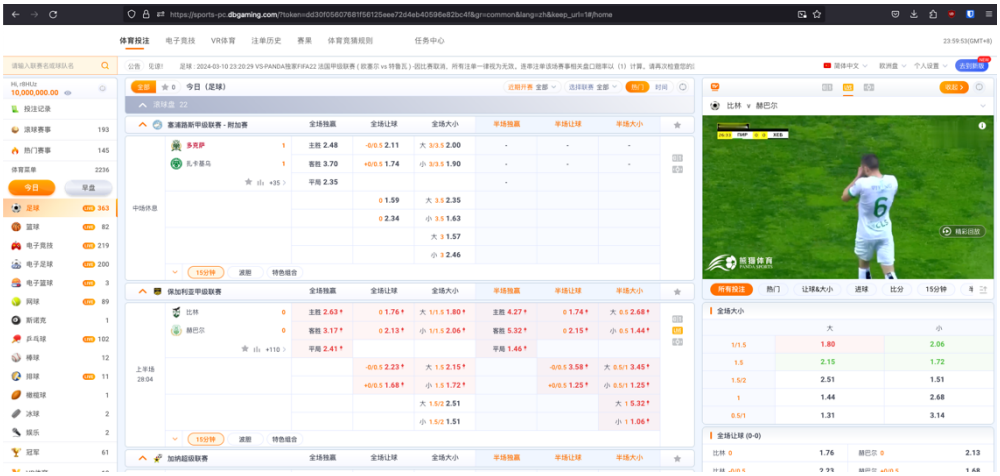


Figure 29. Screenshot of the template admin website offered by DB and Ponymuah, branded Panda Sports

On February 1, 2023, a company named Ponymuah acquired and merged with OB. Ponymuah is sometimes referred to as Ponymuah Games. The only traces of this transaction we have found are images posted on social media. Figure 30 shows an image we found that announced the partnership online. One has to wonder whether it was just a name change or a real merger. **Ponymuah seems to have taken over both OB and DB Gaming's operations.** All three entities share the same social media accounts (see Figure 31).

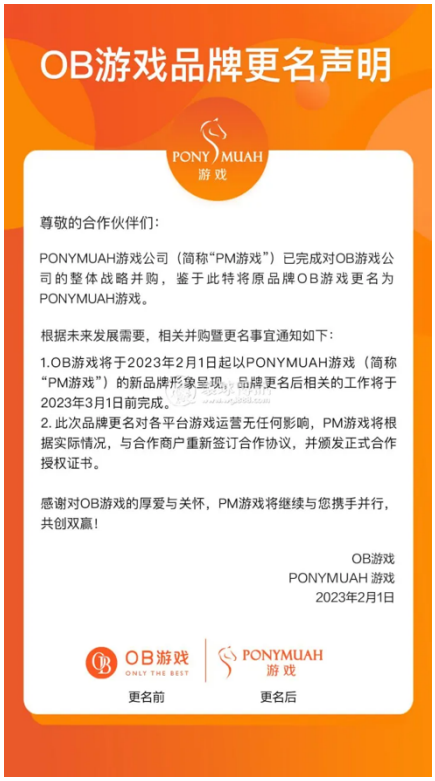


Figure 30. Image shared on Chinese social media advertising the partnership between OB and Ponymuah

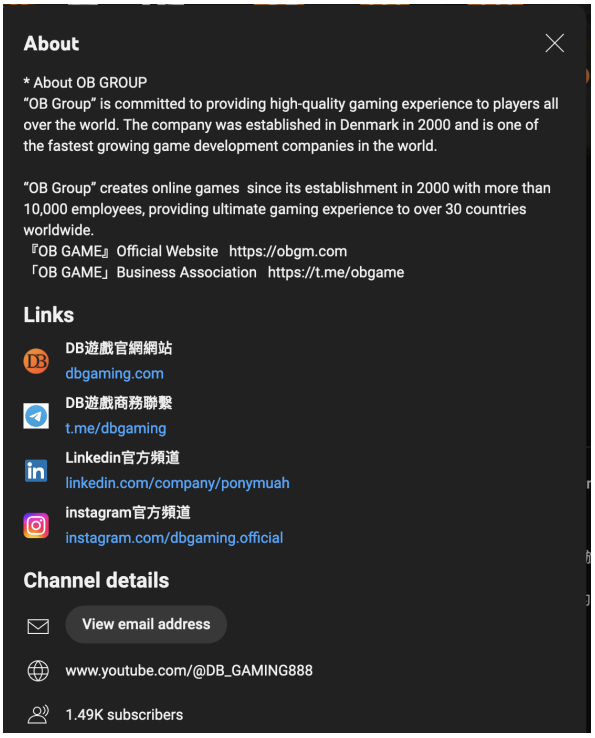


Figure 31. Ponymuah, DB, and OB (OB Group) using the same social media account.

Yabo's Latest Identity: Ponymuah Ltd.

Is Ponymuah a distinct entity from Yabo?[60] **We assess that most likely they are one and the same, and that the Yabo infrastructure (i.e., Vigorish Viper's) was not dismantled but essentially transferred to new entities.** The connections between the two companies are significant. As of April 2024, all of Vigorish Viper's domains still contain references to Yabo in their code. Ponymuah's purported CEO, whose LinkedIn picture is a stock photo, lists his previous employment as CEO of Infovine Inc., which is an accredited service provider licensed by PAGCOR and used by Infiniweb Technology Inc. Infiniweb lists only two providers: Infovine Inc. and Tianyu Technology Inc. Tianyu operated the Yabo brand and owns the Yabo trademark.

60 For more details about Yabo, please refer to the "The State of Illegal Betting" 2023 annual report from the Asian Racing Foundation.

Infinweb was also mentioned in a number of reports on illegal gambling and football sponsorships.[61] Infovine has hired dozens of non-Filipinos, all Chinese speaking, since the beginning of 2024.[62]

While DB and OB do not appear to be related to established companies, Ponymuah Technology LTD was incorporated on November 8, 2022, in Cyprus under number HE 440148. The company was founded only two months prior to its acquisition of OB.

While Ponymuah may be a registered commercial entity, it advertises false credentials and provides conflicting information about its business. At one point, marketing materials claimed, "PM Games [Ponymuah] is registered in the British Virgin Islands and has legal licenses issued by the European Malta Authority (MGA) and the Philippine Government Commission (PAGCOR)."[63] Other press releases mention the company is headquartered in Ireland.[64] There is no evidence to support these claims, but that didn't prevent the company from attending one of the largest events dedicated to gambling in the Philippines, SiGMA Summit, in the presence of PAGCOR.[65] In fact, Ponymuah won the 2023 SiGMA Award for "Integrated Game Provider of the Year," among categories such as "Crypto Games Platform of the Year" and "Online Junket of the Year."[66] Figure 32 provides a screenshot from the Ponymuah website.

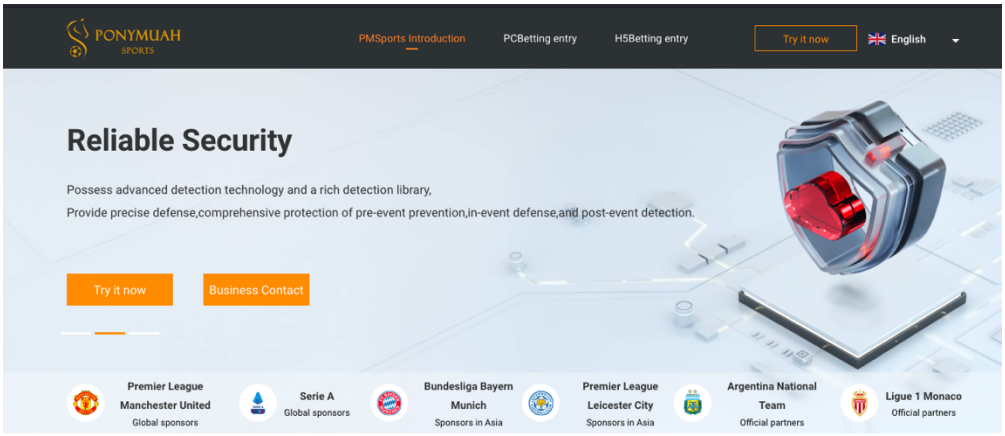


Figure 32. Screenshot from sports[.]ponymuah[.]com; shows an interesting list of sponsors

Officially, Ponymuah is only a service provider whose API services are consumed by casinos owned by unrelated third parties. **In reality, the subdomain `sports[.]ponymuah[.]com` is identical to the DB Gaming offering and hosted on the same IP.** The infrastructure overlaps with Yabo and they use a similar shared file structure (Figure 33).

61 https://www.ft.com/video/4bf67319-ce1e-4d13-a49d-120e12cc7d3d last accessed April 29, 2024

62 https://issuu.com/businessmirror/docs/businessmirror_march_8_2024 last accessed April 29, 2024

63 http://web.archive.org/web/20240311134043/https://jtzs.vip/pm%E6%B8%B8%E6%88%8F%E7%AE%80%E4%BB%8B last accessed April 29, 2024

64 http://web.archive.org/web/20240315142015/https://pm-tw.org/pmponymuah/ last accessed April 29, 2024

65 https://twitter.com/SiGMAworld_/status/1678705110216499200 I https://www.instagram.com/p/Cu-38mryasA/ last accessed April 29, 2024

66 web.archive.org/web/20240311134855/https://www.pmyx.games/blog/ponymuah-games-2023 last accessed April 29, 2024

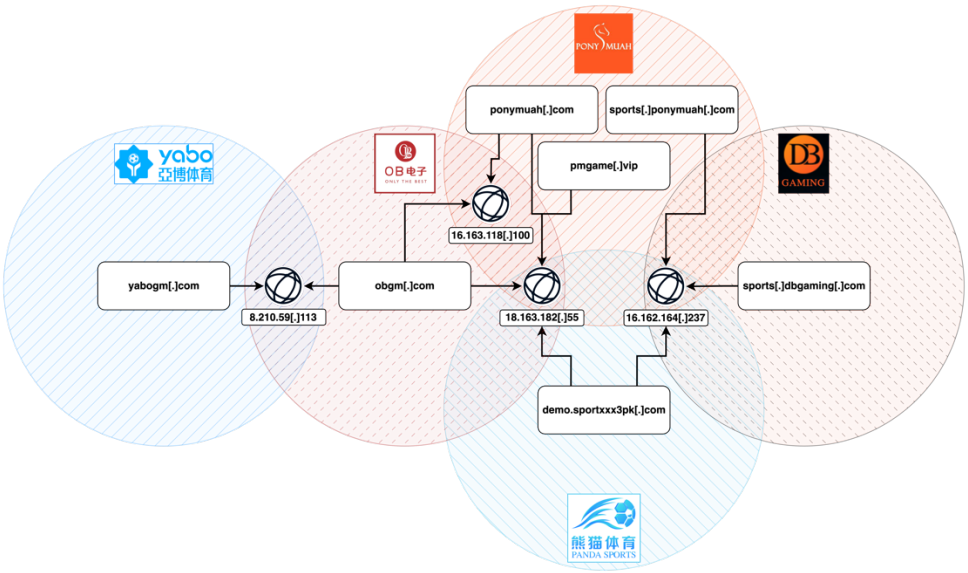


Figure 33. Infrastructure overlap between Yabo, OB, Ponymuah, DB, and Panda Sports. All of these entities are part of Vigorish Viper's network

Far from being just a shell company or an API provider, **Ponymuah is actively involved in recruiting developers, croupiers, and models** (see Figure 34). It seems to be responsible for hosting and live streaming VIP games.[67] While the Western pages of the company only relay job offers related to technology, a number of pages offer croupier jobs to Chinese-speaking job seekers as well as those from the Philippines.

67 https://yabo-tw.com/pm/ last accessed April 29, 2024

📌 Amendable in shifting schedules

Position: Model Dealer | Salary 64K up to 150K
Work location: Pasay only
Qualifications:
📌 Height at least 5'6 ft. and up
📌 Must be 21yo and not more than 27yo. (looking young)
📌 Must have experience in fashion modelling, runway, car show, commercial model or in a beauty pageant.
📌 Pleasing personality
📌 Must be pretty, photogenic with a good smile
📌 Preferably with small body frame and slim arms
📌 Tattoo(s) or scar(s) must concealable
📌 No sweaty hands
📌 Hair at least shoulder length
📌 Braces upon screening is allowed, but once hired you have to remove it.
📌 Full time positions only (NO WORKING STUDENT ALLOWED)
📌 Must be willing to work in Pasay City
📌 Amendable in shifting schedules

OTHER BENEFITS:
- Free Food (during working hours)
- Chinese Holiday bonuses
- Full attendance and KPI bonus (upon regularization)

#PremiereHRRecruitmentInc #ModelDealer #OnlineCasinoDealer #Datang #OBGaming #oblivegaming #phrcareers #oblivecasino #ponymuah #pmlivecasino #ponymuahcasino

Figure 34. Recruitment ad for Ponymuah aka OB Gaming in the Philippines; local recruitment is only carried through social media

The people behind Ponymuah even recorded a music video with a popular Vietnamese influencer and a local DJ.[68] It features wads of cash and poker chips, as well as scantily clad women and expensive cars. The video is posted on one of its websites next to a Karl Marx quote stressing the importance of the collective, in a beautiful display of the contradictions of Chinese society.

Ponymuah also appears to have international operations and ties to Russian-speaking countries. In particular, some of the individuals involved with Ponymuah are Ukrainian nationals who previously created a Chinese-language payment application using cryptocurrencies. Some social media posts mention the company could move some of its operations to Dubai, in another effort to avoid accountability. **The identity of Ponymuah's owners or managers is still a mystery.** The Cyprus LLC was incorporated by a nominee, and there is no information on its operation in the Philippines. While social media pages exist for some low-level employees, there is no mention of any director or executive anywhere. An issue of *SiGMA* magazine lists a "Yoo Tan" as "Chief Mareting Officer" [sic]. This is the only issue

68 https://www[.]youtube[.]com/watch?v=7up3wnrvNpU

where Ponymuah is mentioned and the only headshot in the magazine where the person has their back turned to the camera (see Figure 35). A "Rachel Platten" is sometimes credited as CEO but seems as real as Yoo Tan.

Figure 35. Excerpt from SiGMA magazine issue number 23, published July 12, 2023[69]

Ponymuah is part of a web of interrelated companies with shadowy ownership that cooperate in the underground gambling economy where Vigorish Viper has such a large presence. As we will see in the next chapter, it is difficult to determine where one of these purportedly distinct organizations ends and another begins.

CHAPTER FIVE: VIGORISH VIPER'S BAOWANG

In Chapter Two, we described the baowang economy. In this chapter, we detail the Vigorish Viper's supply chain within that economy. Specifically, we discuss the different companies that have emerged following the dissolution of Yabo and their relationship to one another. Our research concludes that in all likelihood, Yabo, and thereby Vigorish Viper, have been dismantled into companies that in combination make up an entire supply chain. In doing so, they have further obfuscated the financial trails and reduced the likelihood of interference from law enforcement.

The Recruiting Guild

In the gaming economy, we expect to have independent parties operating at different points along the supply chain. In particular, we know that while Ponymuah is the principal game provider for Vigorish Viper, the games need to be packaged with other offerings and made available on websites. **Vigorish Viper's games are solely distributed and packaged by KM Gaming**, ostensibly acting as an independent party from Ponymuah. A third company, Smart King Games (SKG Bowang), is also used as another name for KM and at one point announced "The senior management of KM Baowang Company decided that from August 1, 2023, Smart King Games (SKG Bowang) will officially change its name to KM Baowang. This decision symbolizes that KM Bao Network is about to open a new chapter of development, bringing new experiences and opportunities to partners and users."[70]

69 https://issuu.com/sigmapublication/docs/sigma_23_manila_rgb_issuu

70 http://web.archive.org/web/20240420153604/https://www.kmbwzs.com/text015/ last accessed April 29, 2024

The relationship between Ponymuah and KM Gaming is convoluted, and **the evidence indicates they are all operated by the same group, formerly known as Yabo**. Figure 36 shows the Facebook page of a Ponymuah affiliate advertising KM Baowang. White labels rely on a list of independent agents, maybe contracting with several companies at the same time. But KM and SKG appear to share agents, all using "zhaoshang" in their pseudonyms. Zhāoshāng is the pinyin for 招 or 商 and means "to recruit, to consult" or "investment promotion." Figure 37 shows an ad from SKG proclaiming its relationships with the most established brands and particular sponsorships over several years of its history; these sponsorships and timeline align perfectly with known Yabo brands and sponsorships. In addition to KM Gaming and SKG, we have identified several smaller entities that are all operating under the same group. Figures 38 through 40 show advertising material for some of these brands.

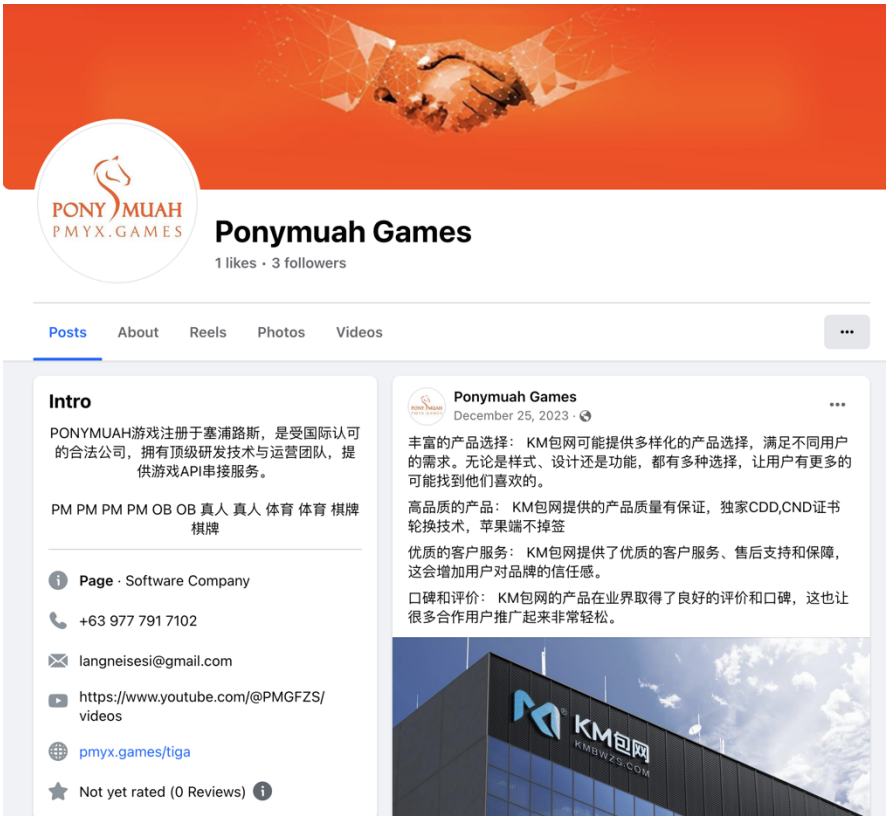


Figure 36. A Facebook page from a Ponymuah affiliate shares advertisements for KM Baowang

Figure 37. Advertisement from SKG flaunting its sponsorship relationships between 2018 and 2021. The marketing text boasts about its partnerships and mentions its "worldwide, rock solid reputation." All the football teams cited here partnered with Yabo

For simplicity, we will refer to the entire group as KM Baowang. This group is responsible for selling, creating, and hosting illegal gambling websites. The main website, `km-gaming[.]com`, advertises a long list of websites all using Vigorish Viper's technology. The YouTube page of a KM Baowang affiliate mentioning a number of the Vigorish Viper brands can be seen in Figure 41. KM even offers advice on how to establish a gambling brand, which begins by choosing a good domain name. It states: "If your [domain] name is not correct, you will not be able to sell well." See Appendix B.

Figure 38. Slides from a marketing deck, branded for both KM and SKG brands, showcasing their achievements

Figure 39. Fake gambling licenses mentioning the YABO group advertised by KM

Figure 40. Promotional picture of a KM Baowang website listing some of the white labels they operate

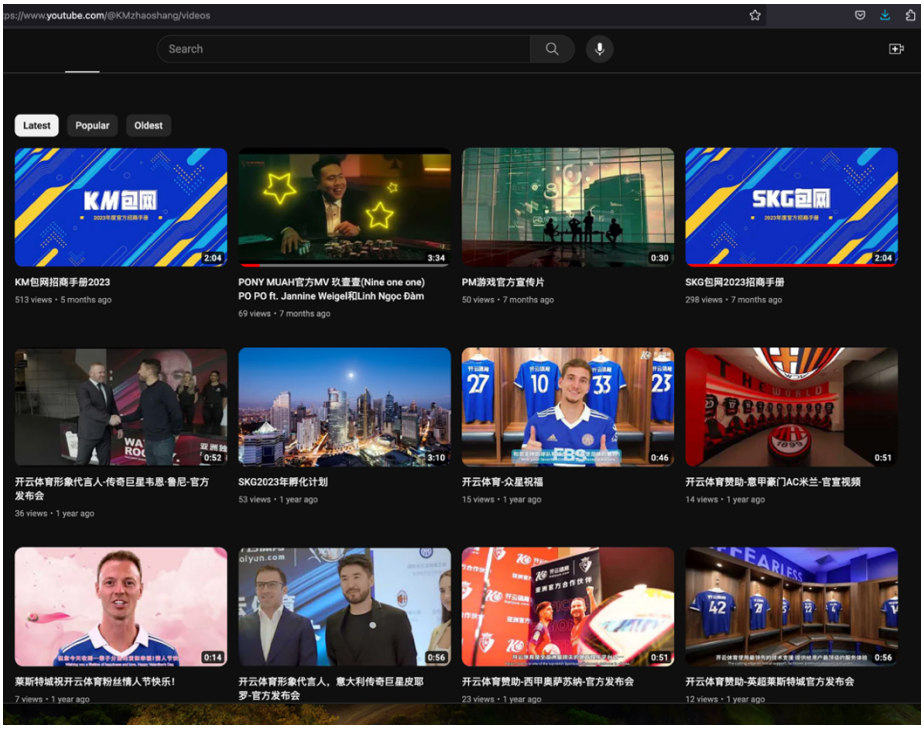


Figure 41. YouTube page of a KM Baowang affiliate, containing mentions of OB, SKG, Ponymuah, and Kaiyun

The KM Baowang demo website, `web[.]kwmbw[.]vip`, has all of the characteristics of one of Vigorish Viper's. Interestingly, it is using a KM logo instead of one of the numerous brands we've become familiar with, showcasing the power of white label branding. All of the expected features from a Vigorish Viper site are present, including specific API keys and coding mistakes; see Figure 42.

Figure 42. Capture of the example website advertised by KM Baowang; the specific API key matches those used in Vigorish Viper's websites

The homepage says KM is a shorthand for Kevin Melo Games and employs 3,000 people. A web page lists different members of the team; however, it appears that none of these people exist as their biographies are made up and their photos are stock images (see Figure 43). Instead of redirecting to their social media profiles, the Facebook and Instagram buttons redirect to SKG or other KM-branded websites.

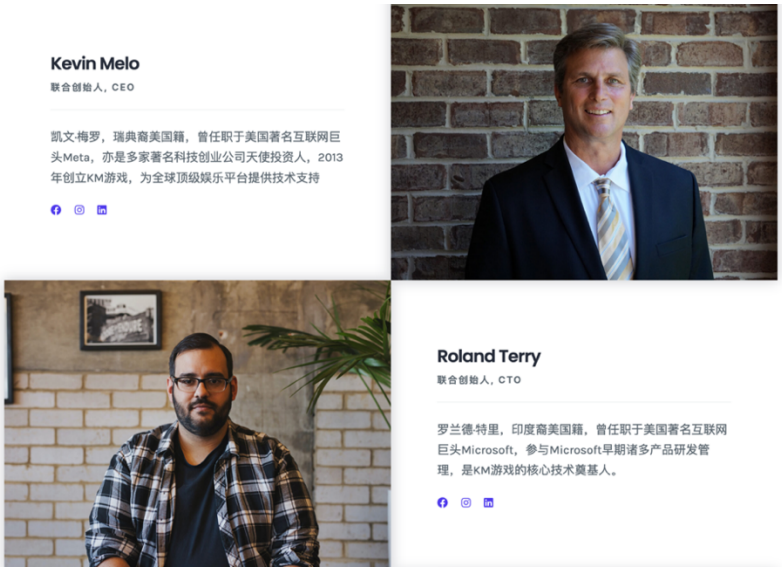


Figure 43. Stock pictures and fake biographies of the team

The About page on the website explains KM Group (KM集团) was created in 2008 in the British Virgin Islands and employs 2,000 people. No company matching the name of Kaiyun, KM集团, 开云体育, or Kering could be found registered in the BVI or elsewhere. KM Group previously claimed on its website to have created the Kaiyun Sports brand (开云体育), as well as a number of other Vigorish Viper brands, including HTH, Leyu, AYX, and BOB Sports.[71]

The evidence provided in this section, along with a host of other supporting source material, indicates that KM Group and Ponymuah are one and the same and that they are very likely still controlled by the individuals behind Yabo. These corporations are part of a large number of entities directly connected to Vigorish Viper and Yabo since 2018, most of which use fake identities and information as credentials for their existence.

A Special Payment Provider: EBpay

Gamblers must register a means to pay for their bets, and the options available in Vigorish Viper's websites vary based on the location of the users. All of the websites integrate the crypto company EBpay as a payment solution **for users in mainland China**. EBpay appears to be used primarily, if not solely, for Chinese gambling applications and is **currently a sponsor of several**

71 https://web.archive.org/web/20240314150317/https://jtzs.vip/%E9%9B%86%E5%9B%A2%E7%AE%80%E4%BB%8B last accessed April 29, 2024

European football teams.[72,73] On most of Vigorish Viper's websites, a specific version of EBpay is offered to users geolocated in Mainland China, while the rest of the audience has to use different payment providers. EBpay advertises on its website the ability to "play games anytime anywhere globally." The crypto wallet uses Tether (USDT) or ETH, allowing anonymous payments.

EBpay boasts 5,000 employees and is apparently incorporated in Mainland China, under Unified Social Credit Code 91510107MA6BG1GQ25,[74] as "Chengdu Nodebai Network Technology Co. Ltd."[75] Despite numerous Western reports of a blanket ban on cryptocurrencies in China, it seems the government left a bit of leeway and still allows investors and companies to operate, albeit under more scrutiny than earlier.[76] **EBpay marketing materials mention the absence of a transaction limit and the possibility of having an account "without using your real name."** EBpay offers both an OTC exchange to convert fiat currency to USDT or Bitcoin, as well as its own token named EB Coin, which is based on USDT and therefore tied to the U.S. dollar. Another version is pegged to the value of the RMB. EBpay products are sometimes offered as white label offerings—for example, KoiPay for gambling websites using the KOI brand.

Evidence indicates EBpay is controlled by Vigorish Viper/KM Baowang/Yabo. The EBpay customer support app is from Vigorish Viper and it uses Vigorish Viper's DNS TDS for the related domains. From this shared use, there is no doubt of a direct connection between the two companies. In addition to Vigorish Viper's infrastructure, EBpay uses a separate DNS-based TDS to facilitate other operations for its payment services. The official EBpay Telegram channel regularly advertises KM Baowang as a "partner" under the same "business ventures." EBPay was also associated with BIB Exchange, a cryptocurrency derivative company headquartered in Belize but operating from the Philippines and China. The `bibvip[.]com` website shares its hosting with a large number of Chinese gambling websites. BIB Exchange also integrated gambling with cryptocurrency trading, by allowing individuals to predict the outcome of matches and earn tokens in return.

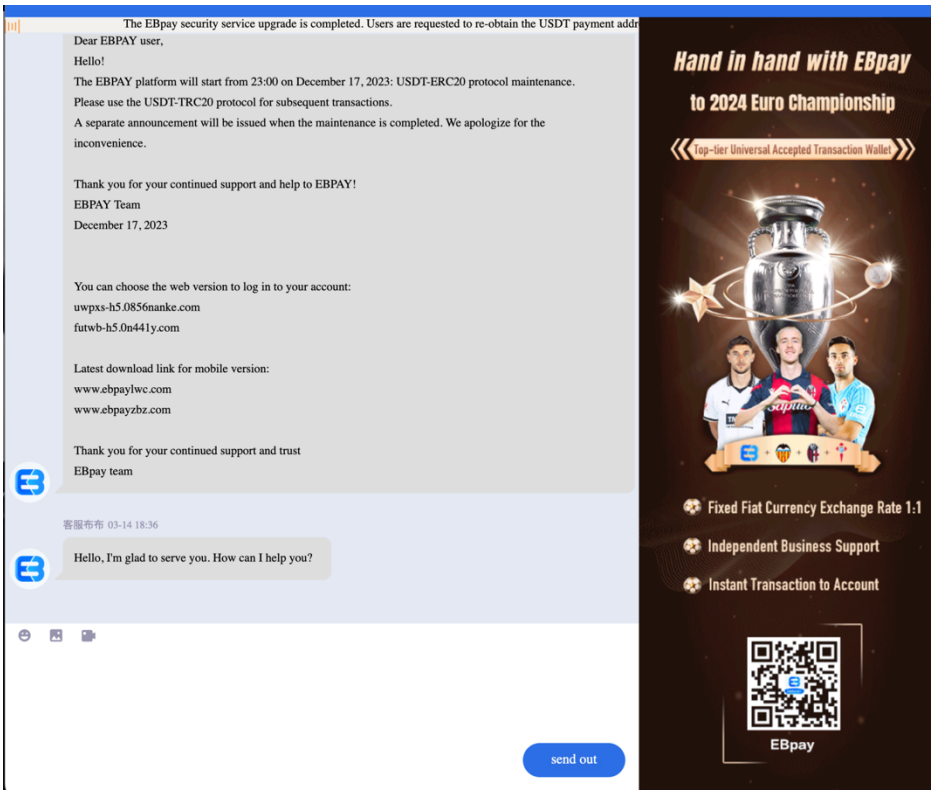
72 https://rccelta.es/en/club/actualidad/ebpay-nuevo-patrocinador-oficial-del-rc-celta/ last accessed April 29, 2024

73 https://onefootball.com/en/news/ebpay-becomes-bologna-fcs-official-regional-partner-in-asia-38920896 last accessed April 29, 2024

74 http://web.archive.org/web/20240314161158/https://help.ebpay20.net/yin-si-tiao-kuan/ last accessed April 29, 2024

75 成都诺手贝网络科技有限公司, https://aiqicha.baidu.com/company_detail_93360048555426 last accessed April 29, 2024

76 https://www.coindesk.com/consensus-magazine/2024/02/05/china-never-completely-banned-crypto/ last accessed April 29, 2024



Customer service support for EBpay, note the gambling ad on the right

CONCLUSION

DNS analytics were the key to finding and then unraveling Vigorish Viper's technology suite and operations and to connecting the most high-profile, controversial sports sponsorship brands in the world. We were able to leverage our expertise in DNS and cybercrime to determine that many of the Chinese organized crime entities uncovered by investigative journalists are using the same network and the same software. Both the DNS and the software tie Vigorish Viper's entire enterprise to Yabo Sports or Yabo Group. Their reach extends to dozens of brands, possibly hundreds, and targets users beyond Southeast Asia. In spite of the massive number of domain names, websites, and accompanying applications, along with overt presence in the public eye, Vigorish Viper is operating directly and inexplicably in the PRC without meaningful consequence.

Infoblox recommends blocking DNS resolution of all domains associated with Vigorish Viper due to the connection with organized crime. In addition, we recommend user awareness training on the dangers of illegal gambling. Cybercriminal use of lookalike domains and mirroring sites of established legitimate betting companies can cost users their life savings. At the same time, Vigorish Viper and similar providers enable the broad range of crime associated with illegal betting, including scams and modern slavery. By preventing access to them and to lookalike domains to major betting platforms, organizations can protect their users from exploitation.

Finally, traffic distribution systems are a key mechanism for cybercriminals to operate for a long time without detection. We have found repeatedly that vast DNS networks have persisted for years, serving up scams, stealing user credentials, and delivering malware. Vigorish Viper's network is just one more example. Our hope is that industry, academia, and government institutions will look at new avenues to detect and control these hidden operators, and thereby combat the current economic trend of cybercrime.

INDICATORS OF ACTIVITY

This section includes a selection of Vigorish Viper's indicators of activity (IOAs). Indicators are also available in our GitHub repository.

CNAMES

CNAMES	abckamai[.]com app-cdn[.]com cname520[.]com greywolffast[.]com scname[.]com

Examples of Gambling Sites

Advertised	Alias
kb[.]com	109kb[.]com kb1009[.]vip kb643[.]vip kb748[.]vip kb7890[.]com kb913[.]vip kb950[.]vip kbbet47[.]com kbbet86[.]com kbbet8[.]vip kbbet99[.]com kbet498[.]com kbet668[.]com kbty138[.]com kbty150[.]com kbvip240[.]vip kbvip88[.]com kbvip99[.]com
ob[.]com	ob5723[.]com ob5724[.]com ob5725[.]com ob5726[.]com ob5727[.]com ob5728[.]com

Advertised	Alias
	obbet1628[.]com obbet1917[.]com obbet2912[.]com obbet3177[.]com obbet3180[.]com obbet3185[.]com obet3548[.]com obvip3683[.]com obvip3767[.]com oubao1361[.]com
yabo[.]com	8279[.]hk yabo1001[.]com yabo1008[.]com yabo1029[.]com yabo1065[.]com yabo1178[.]com yabo1200[.]com yabo1218[.]com yabo1219[.]com yabo1229[.]com yabo123456[.]com yabo1238[.]com yabo1276[.]com yabo1316[.]com yabo1391[.]com yabo1518[.]com yabo1549[.]com yabo1589[.]com yabo1666[.]com yabo1898[.]com yabo1993[.]com yabo777777[.]com yaboyaboapp[.]com yb1444[.]com yb3336[.]com yb3338[.]com yb3650[.]com
kaiyun[.]com	kyty1[.]com kyty2[.]com kyty3[.]com kyty4[.]com kyty5[.]com kyty6[.]com kyty7[.]com kyty9[.]com kyty10[.]com kyty11[.]com kyty22[.]com

Advertised	Alias
	kyty33[.]com kyty55[.]com kyty77[.]com kyun1[.]com kyun3[.]com kyun4[.]com kyun6[.]com kyun7[.]com kyun9[.]com
baibo[.]com	1766qq[.]com 22887788[.]com 6616bb[.]com 666352[.]cn b11338[.]com baibo22[.]com baibo55[.]com baibo66[.]com bb66636[.]com bb66688[.]com bb88878[.]com bgqn[.]trade cddy[.]trade u12222[.]com u66677[.]com u69888[.]com w2222[.]vip w5551[.]vip w5553[.]vip w8818[.]vip
hth[.]com	157[.]mk 181hthvip[.]com 191hthvip[.]com 193hthvip[.]com 205hthvip[.]com 2150hthty[.]com hth268[.]cn hth67888[.]com hth888[.]cn hth9[.]uk hthbet600[.]com hthbet601[.]com hthbet602[.]com hthbet603[.]com hthbet604[.]com j8sud6[.]vip jg1ajj[.]vip mip4tr[.]vip nda8bq[.]vip

Advertised	Alias
	o3zgmx[.]vip
fun88[.]com	fun118[.]com fun138[.]com fun555[.]com fun580[.]com fun581[.]com fun688[.]com fun808[.]com fun88asia[.]com fun88asia1[.]com nzfai128[.]net
yibo[.]com	yibo1071[.]com yibo2588[.]com yibo3999[.]com yibo5413[.]com yibo6869[.]com yibo7575[.]com yibo88[.]cc yibo8916[.]com yibo898[.]com yibobet1341[.]com yibobet2032[.]com yibobet2604[.]com yibobet2637[.]com yibobet274[.]com yibobet2750[.]com

Other IOAs

Main Article	ag96[.]vip bibvip[.]com chinataiwan[.]org everydayvids[.]com freestatisticsasia[.]com k8vip[.]com kokd08c[.]com loa24xr9z-kv-0uh6iq81gnf[.]com okokip[.]com snaptalk3[.]cc sribgio[.]com w3338[.]app w5553[.]vip w8818[.]vip web[.]kwmbw[.]vip ybvipdns[.]com
Appendix A: A Hall of Mirrors	hxxps://yamei-sports[.]com hxxps://hth-cn[.]com

	hxxps://aoa-sport[.]com hxxps://ob-entertainment[.]com hxxps://bob-sports[.]com hxxps://yabo7890[.]com hxxps://168-sports[.]com hxxps://tianbo-sports[.]com hxxps://kok-sports[.]com hxxps://sports-leyu[.]com hxxps://mile-m6[.]com hxxps://ayx-cn[.]com hxxps://jbo-cn[.]com hxxps://vwin-sports[.]com hxxps://betasia-vc[.]com hxxps://deal4bet[.]com J9[.]com
Appendix B: TDS Redirection Samples	hxxps://www[.]ftbeab[.]xyz:9553 hxxps://www[.]dtcbd3[.]xyz:9518 hxxps://www[.]o0f58d[.]com:8004 hxxps://www[.]zun4ww[.]xyz:8002 hxxps://www[.]80yxdi[.]xyz:8663 hxxps://www[.]dpy2kl[.]com:7443 hxxps://www[.]ti9xmb[.]com hxxps://sogou[.]baidu[.]loa24xr9z-kv-0uh6iq81gnf[.]com:53001 hxxps://www[.]vhc8nx[.]com
Appendix C: Advice for Establishing a Brand	zmty[.]com ayx[.]com 168[.]com 168ty[.]com yb[.]com oubao[.]com
Appendix D. Hackers Target Vigorish Viper Users	hxxps://www[.]no0po[.]com:9520

APPENDIX A: A HALL OF MIRRORS

Cybercriminals will take advantage of any opportunity to defraud people, both users and even other criminals. Legitimate gambling companies often face the challenge of mirror sites that are established to siphon customers away from one offshore site to their own: one illegal site taking business from another.[77] Through SEO or social media, victims are led to join the fake sites. After investing their life savings, they could lose it all with no legal recourse.

Vigorish Viper is no exception. In January 2024, we found that a YouTube channel called Deal4Bet had created a series of lookalike domains to the original Vigorish Viper betting domains and had pirated sponsorship announcements to drive traffic to the fake platform.[78]

77 https://www.businessinsider.com/inside-the-world-of-illegal-online-gambling-in-china-2022-9 last accessed April 29, 2024

78 https://www.youtube.com/@deal4bet/videos last accessed April 29, 2024

(See Figure A1.) For example, Deal4Bet posted the video announcing the relationship between KB Sports and the French Girondin team but included a link to `kb-sports[.]com`, not `kb[.]com`.

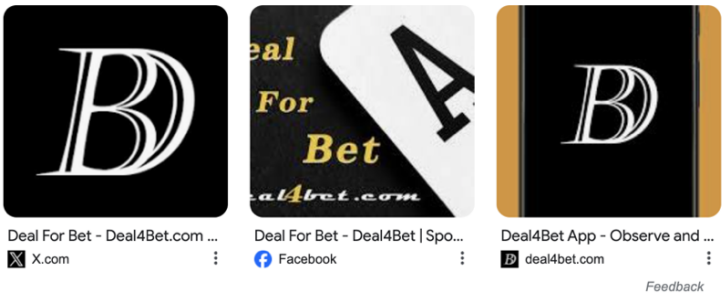


Figure A1. Social media and web results for Deal4Bet, a fraudulent betting platform

Deal4Bet owned at least 26 lookalike domains in January 2024. In addition to its YouTube channel, it has or has had YouTube, Facebook, Instagram, Telegram, and Twitter accounts. As Figure A2 shows, its Mandarin channel claimed to have nearly 64k subscribers and hosted a variety of sports videos. All of the channel videos contain links to its website and to lookalike domains that mimic the original brand.

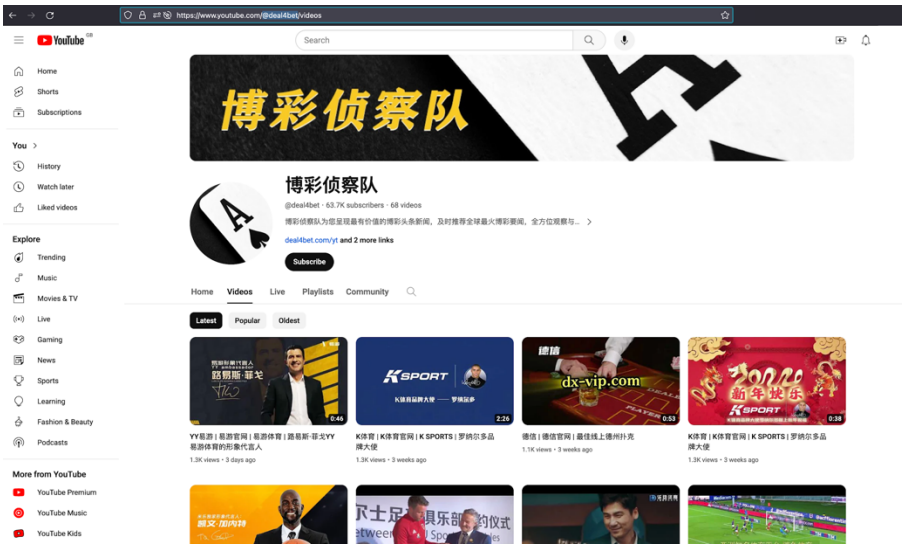


Figure A2. The Deal4Bet YouTube channel in early January 2024 claimed many European sports sponsorships

Deal4Bet claimed to be an objective recommendation site, giving users advice on which offshore gambling sites provided the best returns and service. Users were then led to mirror sites rather than the original one. Figure A3 shows the main page for the site, including reviews, special deals, and hyperlinks. Several of the Vigorish Viper's brands were included in the Deal4Bet lookalike domains, along with other major non-Chinese companies like BetWay (see Figure A4).

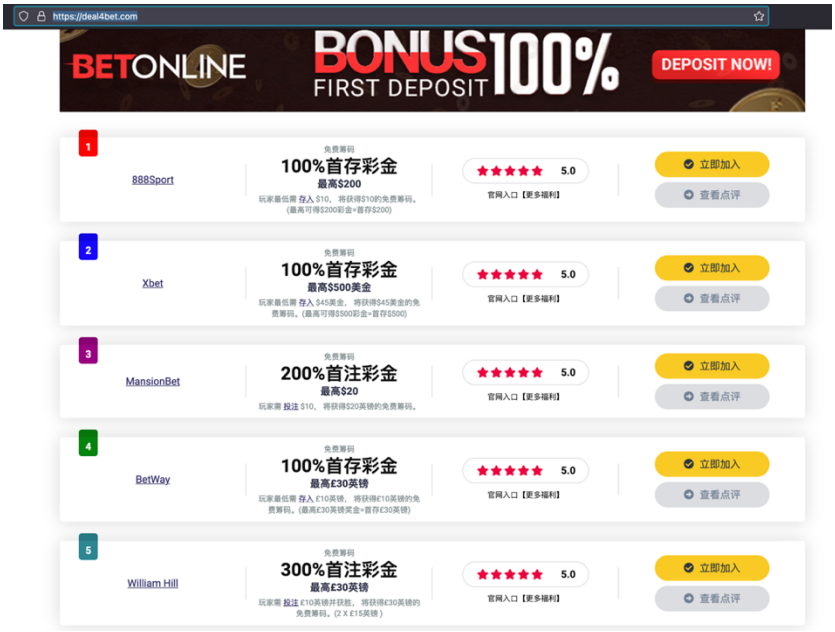


Figure A3. The Deal4Bet website gave users recommendations and links to fake betting sites

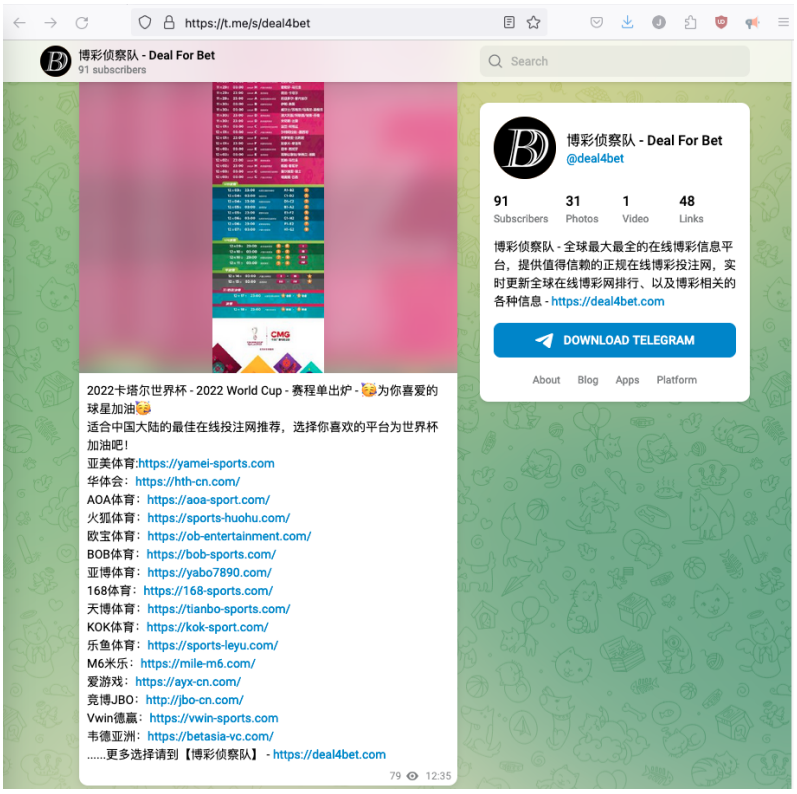


Figure A4. Deal4Bet lookalike domains and several Vigorish Viper domains

After we began investigating Deal4Bet in January, it hid all of its content, moving its gambling videos on YouTube to private status and replacing them with a set of benign, unrelated cat

videos. As Figure A5 illustrates, it also changed its display name from Deal4Bet to Happy Here. The newly visible videos were uploaded three years ago, indicating that Deal4Bet had prepared in advance to quickly change its content. The main website and fake betting sites were no longer operating in early February 2024.

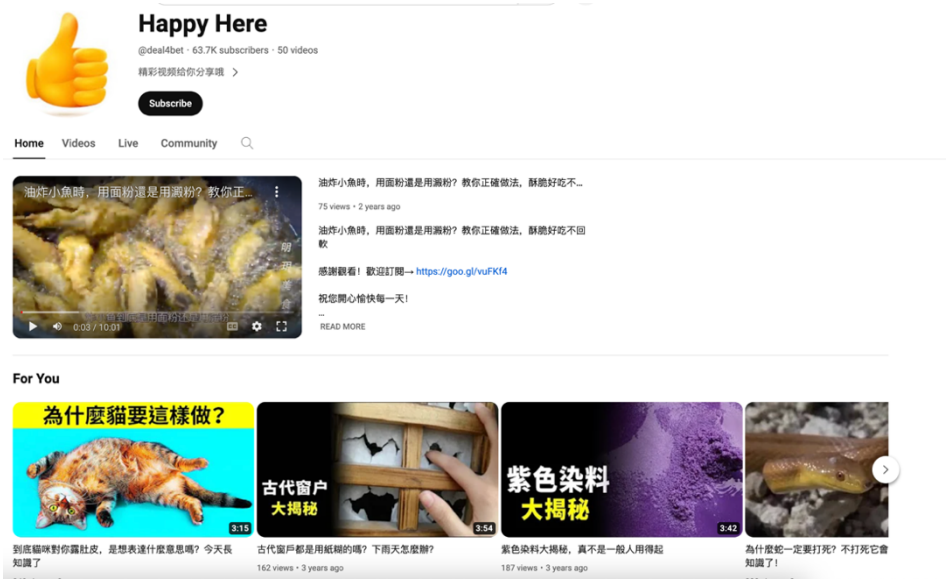


Figure A5. The rebranded Deal4Bet YouTube channel after they removed all of their gambling content following our investigation

As of mid-April, its website came back online. We assumed that it would at least rebrand to have some semblance of deniability, but it is back just as it was before February. Its YouTube channel has gained hundreds of thousands of subscribers, which are presumably bots considering the engagement on most of their videos. Even though its videos are now dedicated to gambling, all of them are new videos. In addition, it created at least three different YouTube channels, one of which seemingly has more than a million subscribers, yet usually around 1,500 views per video.

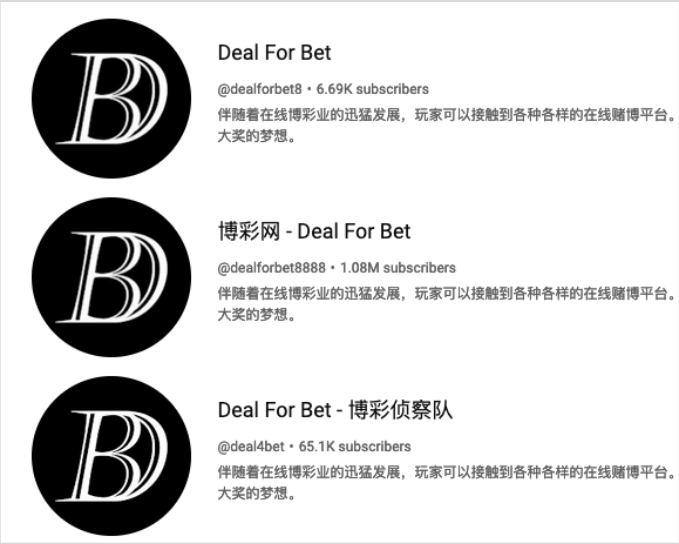


Figure A6. Deal4bet's three new YouTube channels

While Deal4Bet is the largest fake betting network we saw, including its own app and many websites, there are others. In particular, there are numerous YouTube channels promoting brands using lookalike domains. Because the original betting companies largely avoid social media and leverage a series of fake identities and shell companies themselves, there is a lot of opportunity to scam innocent people.

For example, there are a number of YouTube channels and other media sites promoting the J9 Casino brand. The links within all of this content lead to fake mirror sites. The International Basketball Federation (FIBA) partnered with Philippines-based J9 as its official betting partner in 2021.[79] While `J9[.]com` may be fully above board, users are drawn into sites that convince them to play and then steal all their funds. Multiple testimonials on the website TrustPilot claim that J9 stole thousands of dollars from them.[80] Unfortunately, in the murky world that is gambling and sports sponsorships, it is impossible to tell whether it was J9 itself or fake sites that stole their money.

APPENDIX B: TDS REDIRECTION SAMPLES

Vigorish Viper uses multiple HTTP-based TDSs to control access to content based on IP location and device type. The actor can detect the difference between residential and enterprise IP addresses in China prior to resolving the domain and uses User Agent strings to redirect based on the type of device. Most of the code used in the operation is difficult to follow, but there are a few examples of JSON that demonstrate the initial layer of browser fingerprinting that is commonly used.

In one configuration, the user information is checked with a script that includes this snippet.

79 https://www.fiba.basketball/news/global-partnership-with-j9-set-to-bring-fans-across-the-globe-closer-to-the-game last accessed April 29, 2024

80 https://www.fiba.basketball/news/global-partnership-with-j9-set-to-bring-fans-across-the-globe-closer-to-the-game last accessed April 29, 2024

```
var reg = /(Baiduspider|361Spider|YisouSpider|YandexBot|Sogou inst spider|Sogou web
spider|spider)/i;
if (!reg.test(navigator.userAgent)) {
let flag =
navigator.userAgent.match(/(phone|pad|pod|iPhone|iPod|ios|iPad|Android|Mobile|BlackBerry|IEMob
ile|MQQBrowser|JUC|Fennec|wOSBrowser|BrowserNG|WebOS|Symbian|Windows Phone)/i);
if (flag) {
//æ‰<æœº
window.location.href = 'https://sogou.baidu.loa24xr9z-kv-
0uh6iq81gnf[.]com:53001/?loginURL=https://www.vhc8nx[.]com/entry/login&agent_code=9487417';
} else {
// PC
_src = 'https://www.ti9xmb[.]com/register/?i_code=9487417'
}
```

Below is a second example that is used with the CNAME `app-cdn[.]com`.[81]

```
line = {
    ky  : '34814978',    // 开云
    leyu: '7853629',    // 乐鱼
}

var link = {
    kyPc    : 'https://www.dpy2kl.com:7443/register/?i_code=' + line.ky,  // KY pc 链接    kyH5    :
'https://www.80yxdi.xyz:8663/entry/register/?i_code=' + line.ky,  // KY h5 链接
    kyApp   : 'https://www.zun4ww.xyz:8002/?i_code=' + line.ky,  // KY h5 链接
    leyuPc  : 'https://www.o0f58d.com:8004/register/?i_code=' + line.leyu,  // leyu pc 链接
    leyuH5  : 'https://www.dtcbd3.xyz:9518/entry/register/?i_code=' + line.leyu,  // leyu h5 链接
    leyuApp : 'https://www.ftbeab.xyz:9553/?i_code=' + line.leyu,   // leyu app 链接
}
function clickFun(key) {
    let u = navigator.userAgent;
    let Agents = ["Android", "iPhone", "webOS", "BlackBerry", "SymbianOS", "Windows Phone", "iPad",
"iPod"];
    let flag = true;
    for (let i = 0; i < Agents.length; i++) {
        if (u.indexOf(Agents[i]) > 0) {
            flag = false;
            break;
        }
    }

    if (key === 'kaiyun'){
        flag ? window.open(link['kyPc']) : window.open(link['kyH5'])
    }else if(key === 'leyu'){
        flag ? window.open(link['leyuPc']) : window.open(link['leyuH5'])
    }else{
        window.open(link[key])
    }
}
```

81 https://urlscan.io/responses/3a0e81177b8864c368038035317f13393b9888c6a905eac24acc6f917be77bfb/ last accessed April 29, 2024

APPENDIX C: ADVICE FOR ESTABLISHING A BRAND

This appendix includes an English translation of a message originally published by KM | SKG on its Facebook page. This post was intended to give potential customers advice on how to create a gambling brand. It provides specific details that tie KM to Vigorish Viper and Yabo. It has been edited for clarity and brevity. The source material is available at https://www.facebook[.]com/KMbaowang.

SKG baowang recommendation: Authoritative guide to naming your platform
If your name is not correct, you will not be able to sell well.
Brand naming makes this thing big or small. Seriously, a good name determines the life and death of the platform. No one can deny that a good brand name is a plus for the platform at any level, and it is the pre-work with the largest impact and the lowest cost. The editor-in-chief has participated in the naming of dozens of new platforms, large and small.

First step: domain name
Domain names are the first step in brand naming. Even if you have a great idea, if your brand name can't buy a matching domain name, it's a big [issue]. You should first choose a domain, then a brand, then a logo. A simple and easy-to-remember domain name will make your brand more widely spread, easier to be remembered by users, [it will allow you to not lose contact with your audience].

Choose a domain name [and] pay attention to the following points:
First: buy on GoDaddy, never choose a domestic cloud service provider such as Alibaba Cloud. For well-known reasons, all domestic website registrations are to be recorded [by the state], and there are constant issues in choosing domestic companies as cloud service providers. [You] must choose a .com TLD. A lot of people feel like they can pick a .VIP or .club TLD, it would be cheaper and good enough to host a website.

But in fact .com, as the first generation of initial domain name suffix, has become a subconscious input choice for most people. If you don't want the precious [money] you have spent on the publicity fee to run to other people's [business] - [the .com TLD] has the highest investment value. Domain name investment [is] an "old" business, a quality domain name will continue to rise in value.

Second point: the shorter the main domain name, the better. In general, the shorter the domain name, the more expensive the price, the shorter the better the memory, the [higher] the [volume of traffic], the greater the competition, the higher the investment value naturally rises. Ob[.]com is definitely better than oubao[.]com and yb[.]com is naturally better than yabo[.]com and 168[.]com is naturally better than 168ty[.]com.

It is recommended that you choose the shortest domain name within the scope of your budget, preferably a combination of letters, followed by a combination of letters + numbers, preferably not more than 5 words, 3 or 4 letters are best. Pure numbers are not recommended, as they are difficult to remember and difficult to associate with a brand. Don't think that short letter domain

names are very expensive. Many 4 character domain names are only tens of thousands of yuan. For example, I search for a combination casually: zmty[.]com.[82]

Second step: brand name
After buying a good domain name, you'll have to come up with a brand name. For this, you'll need to be creative and it might require ideas from the whole team.

For example, if you buy ayx[.]com domain name, you can name the brand name "love games" or "love credit"; if you buy hth[.]com domain name, you can name the brand name "Chinese experience" or "Hetaiheng." Using the domain name I casually searched above - zmty[.]com- : If you buy it, you can name the brand name "Zunma Sports." When taking a brand name, pay attention to the following points:
[...]
The shorter the brand name, the better, two words > three words > four words. The shorter the easier it is to remember.
[...]
Brand name suffix: In general, depending on the platform's main game type you can use the brand name everywhere, but some prefer to tailor it to a specific target audience. Thus, the main sports [gambling domain] can be named "XX Sports", the main casino [domain] can be named "XX Entertainment", the main comprehensive [domain] can be named "XX City."
[...]
Avoid taking brand names that have nothing to do with the domain name, this will increase the burden of brand memory, and it will not be good for brand building and communication in the long term. For example, it is difficult to form an association between the domain name W88 and the brand.

Avoid using English words, if you are not targeting the international market, it is best not to use English words to define domain names and brand names. [Case in point:] FUN88, not everyone can understand what FUN means, which makes it more difficult to remember brands and domain names.
[...]

Third step: brand logo
After completing the first two steps, basically the tone of the brand has been set. Taking the domain name I searched for randomly above, zmty[.]com is a good four-character domain name. Zm is interpreted as Zm [Zen Ma], then the brand logo can naturally revolve around the two cores of "Zen" and "horse" [Ma] [...]

[82] The domain shown below is priced at ¥87,945, which is about US$12,000.

Finally, through a combination of domain names, brands, graphics, we produced a simple but practical brand.

We also have completed a platform brand logo from scratch, from a four-character short domain name to an easy to remember brand name. The cost of the entire brand design including the domain name is under 100,000 yuan [about US$13,000].

A good name doesn't necessarily make you successful, but successful people have a good name.

If you still have any questions about the name, please contact our business manager to help solve it. SKG package network provides you with a full set of brand design, domain name purchase, brand consulting.

APPENDIX D: HACKERS TARGET VIGORISH VIPER'S USERS

The traffic to gambling websites is so noticeable that Chinese hackers target user accounts and attempt to steal gambling data to sell financial information. The accounts are hijacked through stealers or, more frequently, captured directly on the wire using deep packet inspection (DPI). This also allows the buyers of the stolen accounts to change the results or the odds of the bets. Other buyers can also set up their own capture filter, allowing them to target specific brands or be active only for certain events, such as the World Cup. In the same effort, individuals have started developing tools to hack Vigorish Viper's websites and extract credit card information. Cybercriminals seek gambling user data to blackmail individuals, steal trading data from agents, or simply to steal financial information.

Figure D1. A Chinese data broker advertising gambling data obtained through DPI. Example translation, 4+: "high-quality materials, large quantities of products. Exclusive to self-operated daily gambling three-network dpi line. We have dpi access to extract chess games/sports lottery/other lottery from websites. Lots of data available. Bulk orders encouraged, night and day releases."

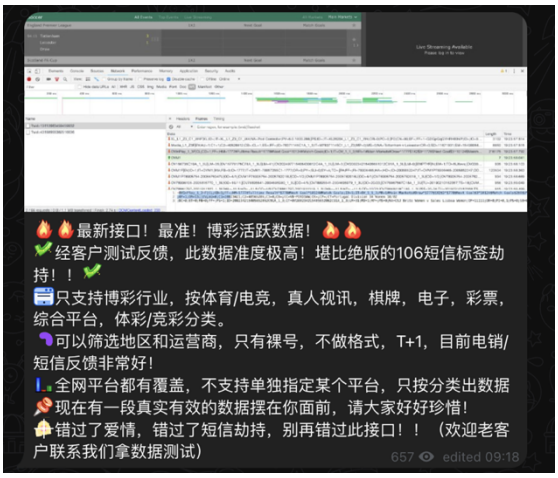


Figure D2. Advertisement for stolen data. The embedded image matches Vigorish Viper's backend

Figure D3. Advertisement for data stolen from fun88[.]com

Figure D4. A YouTuber advertising a hacking tool designed for Vigorish Viper websites. It uses a built-in browser to steal the cookie authentication token, once a user is logged in. The tool then allows credit card stuffing.

INFOBLOX THREAT INTEL

Infoblox Threat Intel is the leading creator of original DNS threat intelligence, distinguishing itself in a sea of aggregators. What sets us apart? Two things: mad DNS skills and unparalleled visibility. DNS is notoriously tricky to interpret and hunt from, but our deep understanding and unique access to the internet's inner workings allows us to track down threat actors that others can't see. We're proactive, not just defensive, using our insights to disrupt cybercrime where it begins. We also believe in sharing knowledge to support the broader security community by publishing detailed research and releasing indicators on GitHub. In addition, our intel is seamlessly integrated into our Infoblox DNS Detection and Response solutions, so customers automatically get its benefits, along with ridiculously low false positive rates.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240528v1