



22 July, 2024

The Hydra

A whirlwind of short-lived Asian gambling brands have taken over European football in recent seasons. Now, a US cybersecurity firm has proof that they are nearly all one-and-the-same entity.

By Philippe Auclair

It's long been suspected that the myriad of illegal Asian-facing sports betting operators whose names appear on the shirts of Premier League clubs and their stadiums' advertising boards – often to disappear just as quickly, as they are not companies, but ephemeral brands which intend to escape detection by law enforcement agencies– are ultimately related to a handful of entities and individuals whose identity is carefully concealed. [Evidence collected by Josimar](#) has shown that the trademarks of many of these brands were owned by a single entity, Philippines-based BOE United Technology Corporation. What was missing until now was actual proof that the links between all of the brands concerned ran deeper than the registration of their trademarks, revealing as this may be. This is what a research conducted by an international team of researchers employed by [US cybersecurity firm Infoblox](#) appears to have established.

Their 68-page report, which Josimar was given exclusive access to, analysed the inner architecture of the tens of thousands of mirror websites operated by those brands and

found out that, in the end, all of them were essentially one and the same. They were branches of the same tree, springing out of the same roots, a tree around which was coiled a creature they named “Vigorish Viper”. That name refers to the profit (“vigorish” or “vig” for short in gambling slang) made on the back of unlucky bettors and the “convoluted brand relationships that the actor employs to route users to content”, to quote from the report. A snake? Perhaps more of a hydra, the beast from Greek mythology which was said to regrow two heads every time it lost one.

But no creature can move without leaving a track behind. In this case, the track was the digital fingerprints of the matrix the monster had emerged from. If the fingerprints matched, the entity had to be the same. And they are. But let’s start from the first step of the path which led to the nest.

What’s in a domain name?

How much is a domain name actually worth? Some can be purchased for loose change, while others are prized for their pithiness and can cost millions. The rule of thumb is: the shorter and simpler the domain, the more expensive. The buyer of voice.com paid more than 22 million US dollars just prior to the pandemic.

In this context, the snappy kb.com, first registered when the internet was in its infancy, could be expected to fetch a multi-million-dollar sum. But how much it was sold for to a Chinese individual based in Jiangsu province in July 2020, then transferred, first, to another Chinese buyer (from the Fujian province), then, finally, to an anonymous new owner in the Philippines a year later, is unknown. What is certain is that it must have been for a substantial amount.



The kb.com website as it looks when accessed from Hong Kong, July 2024.

This is what first caught the attention of the Infoblox researchers. How was such a relatively minor brand (it doesn't sponsor any teams in Europe's big four leagues) willing and able to purchase such an extraordinarily expensive piece of internet real estate? Josimar could only find one football club which had been commercially linked to them, Ligue 1's Girondins de Bordeaux, who signed a partnership deal with the brand in 2021.



All roads lead to Yabo

Digging deeper, these researchers found out that the name server domains used by kb.com had been registered in China under the name Yabo in 2020, [a name which will be familiar to Josimar readers](#).

For four years, from 2018 to 2021, no other Asian-facing sports betting operator was more active or visible than Yabo, who built up the most prestigious portfolio of partnerships ever assembled in world football. Manchester United, Bayern Munich, Paris Saint-Germain, AS Monaco, Milan, the Argentinian FA, Serie A and others all signed on the dotted line, with Yabo represented by their "CEO", one Dean Hawkes, whom Josimar discovered was a British male model and entrepreneur who had relocated to mainland China. Steven Gerrard, then the manager of Rangers, joined the Yabo team as a "brand ambassador".



(l.) Screenshot from Yabo website, celebrating the signing of a new partnership deal with Bayern Munich. (r.) Photograph taken at the 'signing ceremony' of Yabo's deal with Manchester United, featuring former MUFC players Bryan Robson, Wes Brown and Andy Cole, as well as Yabo 'CEO' Dean Hawkes.



(l.) Steven Gerrard promoting Yabo's sister brand OB ("only The Best") (r) Steven Gerrard wishing Yabo customers a happy Chinese Autumn Festival.

Then Yabo disappeared. Overnight, the clubs, leagues and federations they'd done deals with ceased to promote the brand. Why this happened was revealed at a [press conference](#) held in Sichuan in May 2021. A two-year police investigation had led to the identification of

80,000 agents employed by the criminal betting syndicate. Over 3,000 people were arrested, and Yabo ceased to function or at least not under that name. As the Chinese authorities acknowledged, the people who ran this gigantic operation were out of their reach, as they were based abroad. Yabo's head had been cut off, so it grew a new one: Kaiyun, which, since then, has established promotional and commercial relationships with just as impressive a group of A-list football partners: Chelsea, Inter, Real Madrid, Milan, Atlético de Madrid, Aston Villa and Borussia Mönchengladbach among others. Bayer Leverkusen confirmed to Josimar that they'd switched from Yabo to Kaiyun at the request of their client. The Argentinian FA did the same.



(l.) Press conference held in Sichuan, 12 May 2021, at which the dismantling of the Yabo syndicate was announced by Chinese law enforcement agencies. (r.) An arrest made during the “Refusal of Cross-Border Gambling” operation, mainland China, 2021.

The transition was seamless, for a good reason. Yabo and Kaiyun are just iterations of the same entity, and proof of it can be found by analysing DNS data.

What is DNS?

This acronym stands for “Domain Name System”, which is often described as “the phonebook of the internet”. Whereas humans will refer to a website by quoting its URL, such as “josimarfootball.com”, computers will identify the same entity by a series of numbers – such as 162.159.134.42 This is known as an “IP address”. DNS serves as a bridge between those two identifiers. Humans will type the website’s URL in their browser; their computer then sends a DNS query to a DNS server, which returns a numerical IP address. Contact is then established with the website.

Using DNS analysis as a platform, Infoblox researchers were able to establish direct links between kb.com and two other well-known Asian-facing sports betting operators. The first was Yabo. The second was OB Sports, also known as Oubao Sports, a former partner of Leicester City, Aston Villa and Juventus. But this was only the start. Following further

research, the “Vigorish Viper” eco-system quickly grew to include a multitude of other operators who were all connected to a set of shared IP addresses. Think of it as a map which would show you a multiplicity of routes, all of which lead to one destination. Even though that destination might bear different names, you’ll always end up in the same place.

The poet Gertrude Stein famously wrote “a rose is a rose is a rose”. Here, “Yabo is HTH is Leyu is...” *ad infinitum*.

Hiding in plain sight

What is extraordinary is that Yabo made no effort to hide this fact. In a jaw-dropping [video which Josimar just came across, posted in July 2022, one year after the Yabo raids, and can still be seen on YouTube](#), Yabo boasts of controlling “over 100 franchises”. Among these “franchises” are HTH (former or current partner of Real Madrid, Manchester United, Inter, Wolfsburg, Lille and Leicester City), Leyu (Chelsea, Atlético, Milan, PSG, Espanyol, Leicester, Borussia Mönchengladbach and Atalanta) and AYX (Monaco, Roma, Borussia Mönchengladbach and Atlético, again).

As shown in the screenshots below, taken from the company’s own presentation slides, Yabo subsidiary SKG also claims to be behind dozens of other brands. These include Bandao, also known as BOB88 and rebranded as Xing Kong (Napoli, Borussia Dortmund, Augsburg, Lyon, the FAs of Wales and the Netherlands).

And KB.com.



The Yabo/SKG “baowang” galaxy of brands as it appears in their own presentations.

This explains why the landing pages of most of these brands’ websites look almost identical, as shown here with KB.com and LZTY (former partner of Juventus).



KB, LZTY, spot the difference.

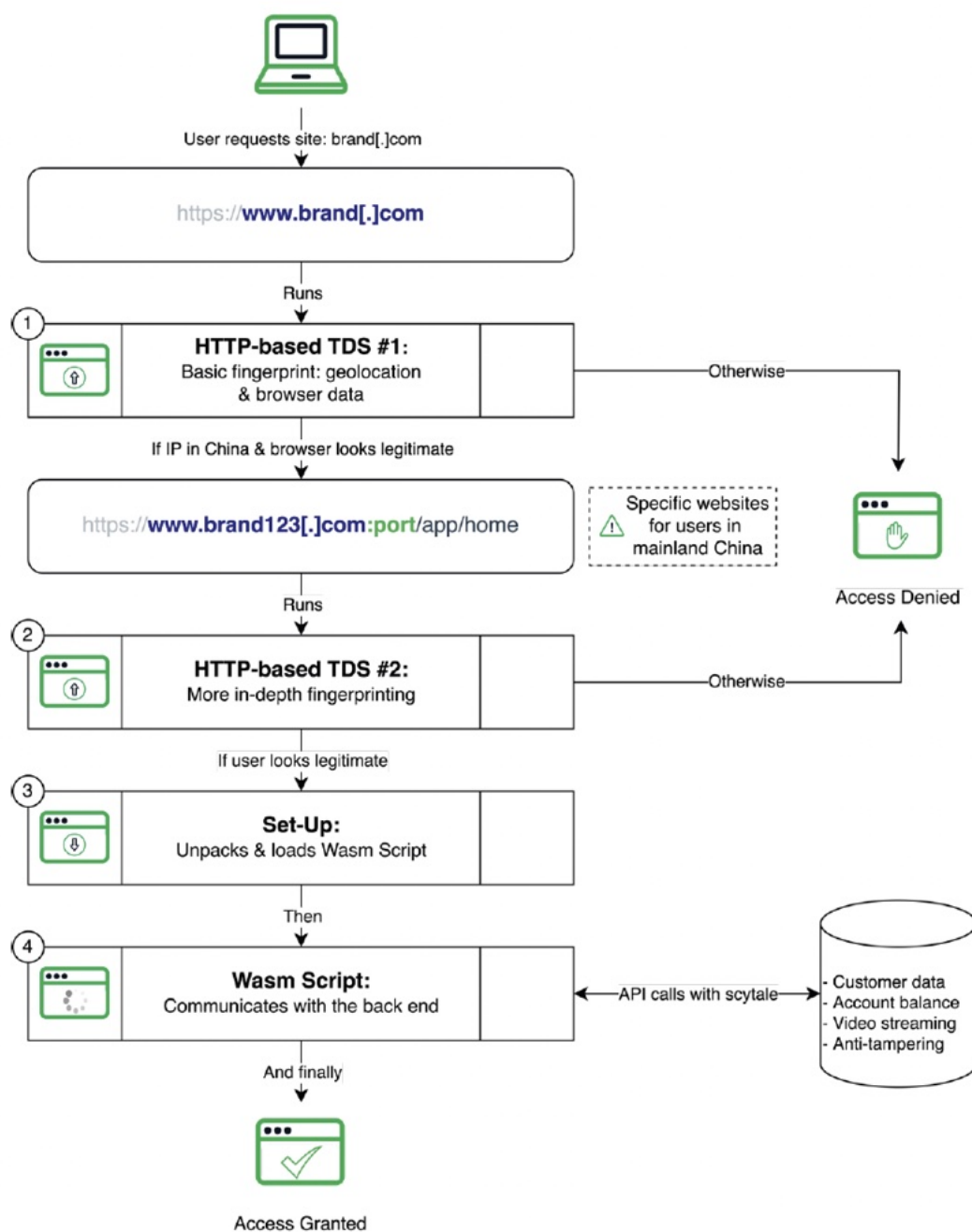
Not only that: Yabo also openly bragged about having designed a digital payment system through SKG which enables their customers to bypass local banking regulations in China.

Yet, at the same time, Yabo and its subsequent “viperish” iterations still try to muddy the waters and avoid detection. Customers are given instructions as to how they can bypass “normal” download procedures on app stores, “abusing features designed for beta testing applications”. Infoblox has also identified remarkably sophisticated defence mechanisms which are built into the operators’ digital platforms, all of which are protected by a Web Application Firewall (WAF). Yabo and other “Viper” websites will first verify the IP address of anyone attempting to access their platforms. They can then track mouse movements on the screen, distinguish between residential, mobile and commercial addresses in mainland China, redirect to unrelated websites when use of a Virtual Private Network (VPN) is detected, provide different content if accessed from the dark web browser Tor, etc, etc.

A major concern will be that Infoblox also established that customer support on “Viper” websites was provided by actual people, not AI tools or chatbots. In the wider context of the illegal Asian-facing gambling and sports betting industry, [where human trafficking and enslavement are rife](#), what is already a dark picture gets even darker.

170,000 identified “Viper” mirror websites

This complex structure requires an extraordinary fluid constellation of mirror websites to function at optimum level, something Josimar had identified as a key feature of the illegal Asian-facing sports betting industry ever [since we started investigating it three years ago](#). Infoblox identified “at least 170 000 websites” linked to the Yabo/Viper network as of February 2024. Given how new iterations are generated every single day, this figure is likely to be an under-estimate of their actual number. The regeneration process is continuous and fits within a process which is designed both to escape detection – and therefore prevent action – by the authorities and, at the same time, to enable gamblers to access the platforms as easily as possible. As shown in the figure below, the process requires an elaborate pathway from business to consumer; but the consumer will be totally unaware of it, whilst the regulators will find themselves lost in a digital jungle.



This set-up is not perfect. Programmers will get sloppy at times, forget to mask code and, sometimes, to remove mentions of other connected brands. The common denominator is that these brands ultimately rely on the same backend, source codes and DNS infrastructure. They are all part of what the Chinese industry calls a “baowang”, a “complete solution” for companies wishing to set up and operate an illegal gambling and sports betting website. The “baowang” associated with Yabo is KM Gaming, which appears to be one of their subsidiaries, as previously-mentioned SKG is; the “baowang” without which much – most – of the Asian-facing gaming sports betting industry could not exist.

The amounts of money generated by the illegal gambling industry, which the United Nations Office On Drugs And Crime (UNODC) estimated to be worth 1.7 *trillion* US dollars in its [December 2021 report](#), that is three times as much as the global narcotics trade, give an idea of how much money circulates through the Yabo “baowang” and its multitude of “viperish” incarnations. The Chinese authorities mentioned a figure of 15.7 billion dollars for the Yabo brand when they conducted their operation. Not turnover. 15.7 billion *profit*.

So what’s a few million for a domain name?