Vault Viper: High Stakes, Hidden Threats

Infoblox Threat Intel ⋮ ⋮ 10/23/2025

Executive Summary

Southeast Asia's cyber threat landscape is evolving faster than ever before, resulting in unprecedented financial losses and security implications increasingly being felt around the world.

This transformation has been marked by the rapid proliferation of industrial-scale scam centers and cyber-enabled fraud operations throughout the region, conservatively generating tens of billions of dollars annually.[1] It has been driven by sophisticated Asian criminal groups and interconnected networks of human traffickers, underground bankers, data brokers, and other service providers—particularly those involved in online gambling which has served as a major front for concealing diversified cybercriminal and money laundering operations in and beyond the region.[2,3,4,5,6]

Against this backdrop, in February 2025, Infoblox Threat Intel, in collaboration with the United Nations Office on Drugs and Crime (UNODC) Regional Office for Southeast Asia and Pacific,[7] set out to examine a cluster of illegal online gambling and cyber-enabled fraud platforms operated by criminal networks based in Cambodia. Over the course of the investigation, however, we uncovered important connections to one of Asia's leading iGaming software

suppliers or “white labels”—an entity we observed not only servicing these criminal groups but also distributing a custom browser found to have significant security implications for users. Considering the popularity and the amount of traffic reaching the command-and-control (C2) domains, we estimate the install base in the millions.

Advertised as “privacy-friendly” and offering the ability to bypass censorship in countries where online gambling is prohibited, the Universe Browser (寰宇浏览器) routes all connections through servers in China and covertly installs several programs that run silently in the background. While unable to verify that the Universe Browser has been used for malicious purposes, we are concerned about the hidden elements of the browser, including key logging, surreptitious connections, and changes to the network configurations of the device. These features are consistent with remote access trojans (RATs) and other malware increasingly being distributed through Chinese online gambling platforms, and importantly highlight the growing sophistication and threat posed by these historically overlooked criminal networks. In the hands of a malicious actor—a triad for example—this browser would serve as the perfect tool to identify wealthy players and obtain access to their machine. Leveraging DNS analysis, reverse engineering, and various threat hunting and investigative techniques, this research has ended a decade’s long mystery by unmasking the network behind this complex operation—the Baoying Group—and ties it back to one of Asia’s most prolific criminal organizations—the Suncity Group—and its leader, convicted Triad boss, Alvin Chau. We are tracking this actor and their infrastructure as Vault Viper. This work builds on Infoblox’s past discovery of Vigorish Viper,[8] representing the second in a series of previously unreported threat actors and criminal service providers operating in plain sight at the intersection of online gambling, cyber-enabled fraud, high-tech money laundering, and human trafficking.

This report covers our discovery of Vault Viper, detailing its technical profile, security implications, and ties to transnational organized crime. It traces tens of thousands of associated domains—with several still currently in use by documented criminal networks—documenting Vault Viper’s vast DNS footprint, C2 infrastructure, unique tooling, and ownership structure concealed through a tangled web of companies registered in dozens of countries.

By outlining how Vault Viper works, along with the broader criminal ecosystem it helps to service and sustain, we hope to inspire research by others into the shadowy world of sophisticated Asian crime syndicates and cyber-enabled fraud. We trust that this report will also provide a foundation for heightened awareness, accelerated solutions, and deeper collaboration between security researchers, governments, and international and industry partners to address the complex and evolving threats emerging from Southeast Asia.

Background

Asian crime syndicates have proven highly entrepreneurial and tech savvy, commonly masking their criminal operations and illicit financial flows as legitimate tech-related business interests and investments. While many sectors are targeted by these powerful networks, this has been most apparent in the case of cash-intensive businesses such as casinos, junkets, and the severely underregulated online gambling platforms around which regional crime groups have converged.[9]

Online gambling has been widely designated as high risk in many parts of the Asia-Pacific and other regions, commonly used by organized crime to conceal industrial-scale cyber-enabled fraud operations and launder billions in criminal proceeds.[10,11,12,13,14] Criminal groups engaged in this shadowy industry have built out their portfolios in jurisdictions deeply challenged by weak regulatory frameworks and low levels of investor screening, threat awareness, and enforcement capabilities, creating a fertile criminal operating environment.

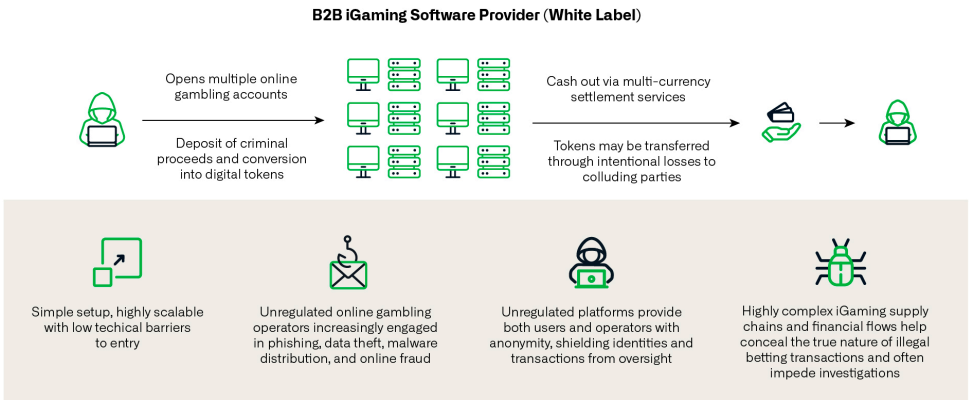

Figure 1. Utility of online gambling operations for criminal actors

In recent years, these networks have aggressively diversified their business lines by pivoting from online gambling into cybercrime and online fraud, exploiting gaps in regulations of complex supply chains, transactions, and revenue streams involved in online gambling. This transformation has necessitated the continued evolution of their tradecraft, culminating in a robust criminal ecosystem involving layers of technical, financial, and legal obfuscation, and a dependence on obscure third-party service providers and infrastructure used to impair investigators, overwhelm regulatory systems, and drive further expansion.

Down the Rabbit Hole: From Bolai to Baoying

Building on past research into Vigorish Viper which demonstrated similar levels of technical sophistication and criminal service provision, in early 2025, Infoblox Threat Intel identified a cluster of online gambling websites known by regional law enforcement to be operated by criminals engaged in large-scale online fraud, money laundering, human trafficking, and homicide. In addition to sharing similar web templates and game offerings, DNS analysis confirmed that all entities in the cluster redirected to the same iGaming software provider.

One particular entity within the cluster is Bolai Casino, also known as Brilliancy Sihanoukville Development and Investment (铂莱娱乐城). Bolai is a rapidly expanding criminal entity based in one of Southeast Asia's major cybercrime centers, Sihanoukville, Cambodia. In addition to its land-based casino operations and documented allegations of human trafficking,[15,16] Bolai runs an online gambling website and Telegram channel dedicated to hundreds of so-called supply and demand groups that serve to connect criminals engaged in money laundering and informal cross-border money transfer or underground banking. The entity was implicated in a joint Thai-Cambodian law enforcement operation in 2022, resulting in the dismantlement of a sizable pig butchering operation based within the Bolai Hotel and Casino resort.

We were curious. Who and what was servicing Bolai's online operations and infrastructure? Had they developed these iGaming capabilities in house? Were the links between the online gambling sites and organized crime simply an outlier? Not quite.

By analyzing the DNS records, we soon realized that what we had found was but one node in a sprawling network of criminal infrastructure humming beneath the surface.

Figure 2. Bolai Entertainment City and new Bolai compound in Sihanoukville, Cambodia (Source: Douyin)

White labels are large business-to-business service providers offering turnkey iGaming solutions that allow customers to launch fully functional gambling websites with minimal technical involvement. White labels typically integrate a suite of services, including various casino games and sportsbooks, backend management tools for user data, affiliate systems, analytics, fraud monitoring, customer support integration, and optional know your customer (KYC) and anti-money laundering (AML) compliance modules. The software is highly customizable, allowing for localization in language, payment options, promotions, and integration of crafty software solutions designed to bypass censorship, ensure privacy, and dodge law enforcement in jurisdictions where online gambling is strictly prohibited. Specific payment solutions are also offered, including illegal crypto exchanges and criminal payment providers such as Huione, EBPay, CGPay, and networks of organized money mules.

DNS is critical for illegal online gambling operators to maintain high availability to their users and provide resilience against enforcement actions. Their dependence on large sets of domain names creates a footprint. However, mapping these networks through DNS can be challenging. Illegal operators use elaborate web architecture consisting of large numbers of randomly generated domain names to spread their infrastructure and hedge against disruptions caused by domain blocking or suspensions. White labels and operators (clients) often use offshore or privacy-protecting registrars, utilizing DNS management services that facilitate rapid domain changes and redirection whenever needed. Those operating in black markets also employ content delivery networks (CDNs) and distributed denial-of-service (DDoS) protection services to ensure uptime and mitigate traffic monitoring by authorities, while domain fronting is commonly used to obscure the actual server endpoints. Despite these various configurations and

tactics, we discovered a distinct DNS fingerprint for Vault Viper, making it possible to trace, map out, and attribute the activity.

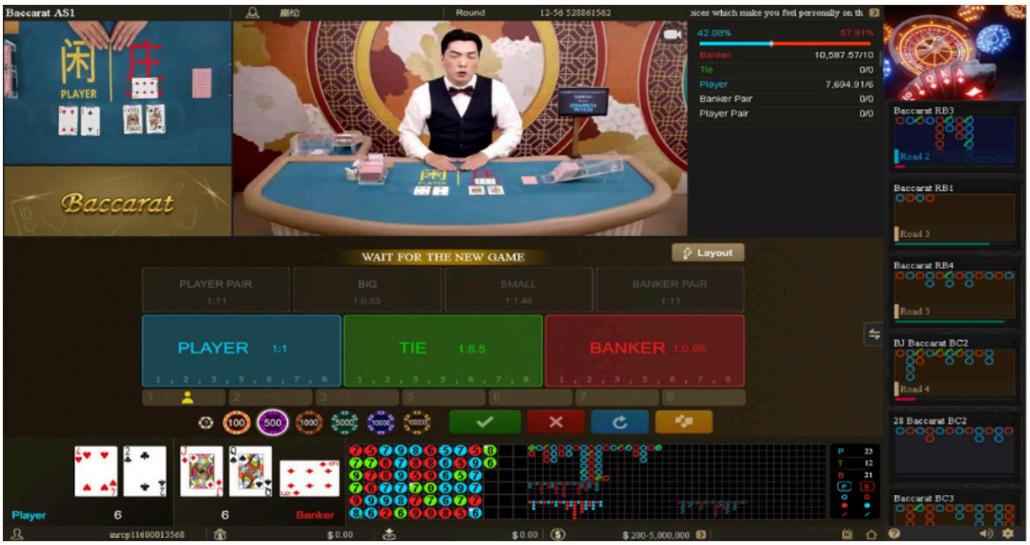

Figure 3. Screenshot of live BBIN Baccarat gameplay (Source: BBIN)

Baoying Group and the BBIN White Label

Founded in Taiwan more than two decades ago, Vault Viper, formally known as Baoying Group (寶盈集團) and BBIN, is made up of an intricate global network of technology, property development, investment companies, and obscure offshore holdings. The group has established several hotels and casinos as well as large-scale technology and data operations in Southeast Asia as a leading iGaming service provider, enabling its online gambling brand, BBIN, to emerge as one of the largest turnkey solutions in Asia. The BBIN brand is ubiquitous on bōcài[17] websites, alongside other market leaders, including Evolution, PGSoft, Asia Gaming (AG) or Sexy Gaming (AE Sexy or Awesome Entertainment). The organization behind Fun Null, ACB.NET, also used the BBIN logo, although it is unclear whether a formal business relationship existed. Fun Null made news after they acquired a domain name present in millions of websites worldwide and leveraged it to inject malicious code.

The Vault Viper platform offers a fully customizable white label solution covering everything from platform development and game integration to backend management, security, and payment processing. As examined below, it also offers a variety of unique features geared toward users and clients operating in unregulated black markets—but could it really be a criminally implicated online gambling platform without having secured official sponsorships with some of the biggest football clubs in the world? No sweat, BBIN has got that covered.

Figure 4. BBIN promotional content showcasing sponsorships with Atletico Madrid and Borussia Dortmund football clubs (Source: BBIN)

Figure 5. BBIN's official partners, a mix of Western providers and bōcài groups (Source: BBIN)

Baoying Group has maintained a large operational base in the Philippines since 2006, particularly in the Clark Freeport and Special Economic Zone, through several companies and fronts. The full extent of the Group's operations and ownership structure, however, are largely concealed through an intricate web of companies and shell structures registered in dozens of countries in Asia, Europe, Latin America, and the Pacific Islands. As examined in the section below, we were able to identify over 1,000 unique name servers hosting thousands of active websites dedicated to illegal online gambling, including several known to be operated by criminal groups engaged in large-scale cyber-enabled fraud, money laundering, and other crimes.

These findings are consistent with prior reporting by regional law enforcement which has repeatedly implicated BBIN in servicing illegal operators and criminal groups across East and Southeast Asia. This includes direct connections to major Hong Kong and Taiwan-based Triad groups including the Bamboo Union, Four Seas Gang, Tian Dao League or Sun Alliance, and others operating in Cambodia, mainland China, Lao PDR, Malaysia, and the Philippines. In three major cases between 2017 and 2023, BBIN was found to have facilitated more than US $770 million in illegal online betting transactions and cross-border value transfers for hundreds of thousands of users using Triad operated websites—a small figure in relation to the billions of dollars the platform is believed to have laundered since its inception.[18,19,20]

Adding to these concerns and Baoying's longstanding record of criminal activity, however, is a custom browser, Universe Browser, promoted to their users that has behavior consistent with malware. While Baoying may not be trusted by law enforcement, it is by online gamblers; they use their status as a trusted iGaming solution to push the software to its users.

Figure 6. BIN-based Bolai Online Casino and distribution of the Universe Browser. Screenshot of illegal online gambling platform operated by Bolai Casino (100319[.]net) displaying a link to download Universe Browser alongside integration of Huione Pay and other payment processors. (Source: Bolai Casino, August 2025)

Discovery in DNS

Technical Analysis: The Universe “Privacy” Browser

BBIN offers a two-click download of the Universe Browser across all supported websites for both Android and Windows, and it is also available for iPhone through the official Apple App store. The modified Chrome-based browser, offered since at least 2014, was developed specifically for Baoying Group to help users bypass accessibility and transaction restrictions. This ability to circumvent local restrictions and internet censorship is particularly vital for operators targeting black markets such as China where online gambling is illegal. Different versions of the Universe (or BB) Browser show a long history of antivirus detection and attempts at detection evasion. The browser’s ability to download and execute binaries, inject code into IEXPLORE[.]EXE, and install system hooks to monitor clipboard content, are all classic malware behavior and common features of information stealers.

The specific detection name, propagation method, functionality, and related C2s all point to Vault Viper. The samples have been seen all over Southeast Asia, including Cambodia, as shown by Figure 7. Figure 8 shows the multiple uses of Universe Browser for Vault Viper.

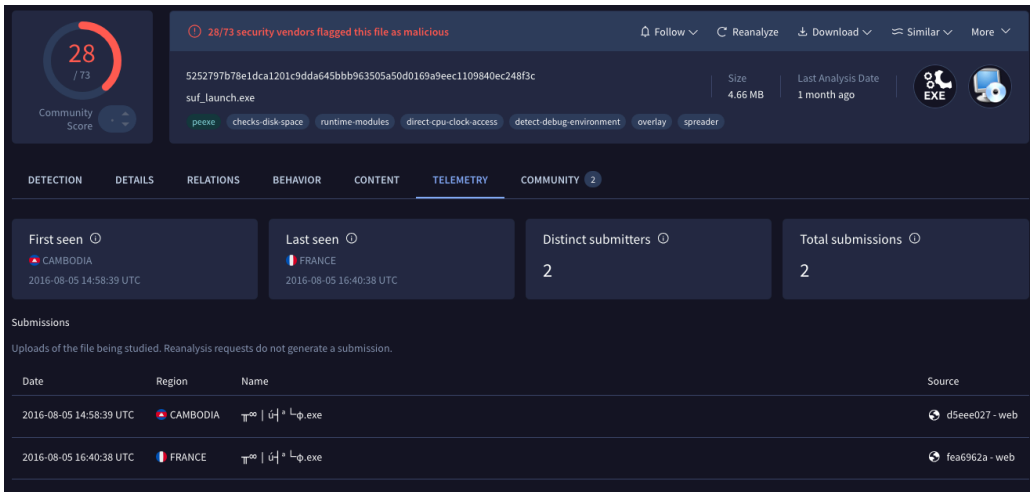

Figure 7. Vault Viper-related sample uploaded from Cambodia

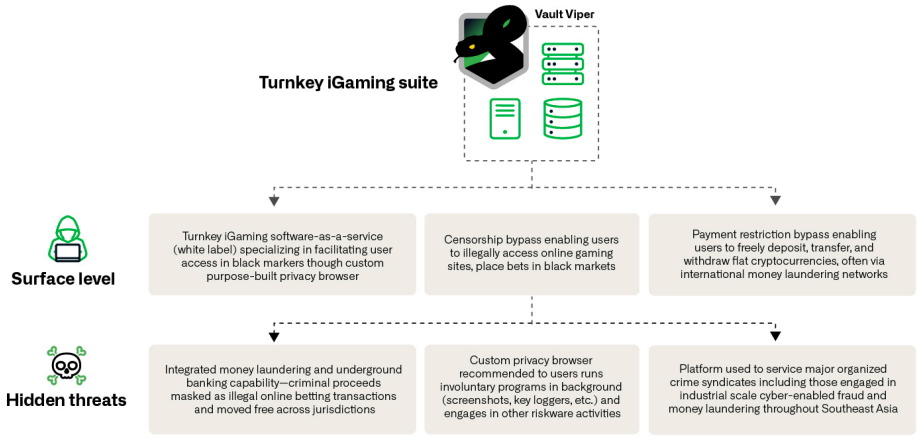

Figure 8. Simplified model of Vault Viper riskware

Upon installation, the browser immediately checks for user location, language, and indications that it is running in a virtual machine (VM) or sandbox—a common technique used by malware to obstruct analysis. Once all checks have passed, the browser will wait for some time before connecting to specific actor-controlled IP addresses in mainland China, Hong Kong SAR, and Taiwan. Once connected, the user is presented with a modified version of Chromium which purports to offer a secure tunnel service between the user and a VPN server, to ensure both privacy and protection of user data. Unknown to the user, however, the browser's installer proceeds to introduce a number of persistent programs that run silently in the background. The technical analysis below is limited to the Windows variant of the Universe Browser.

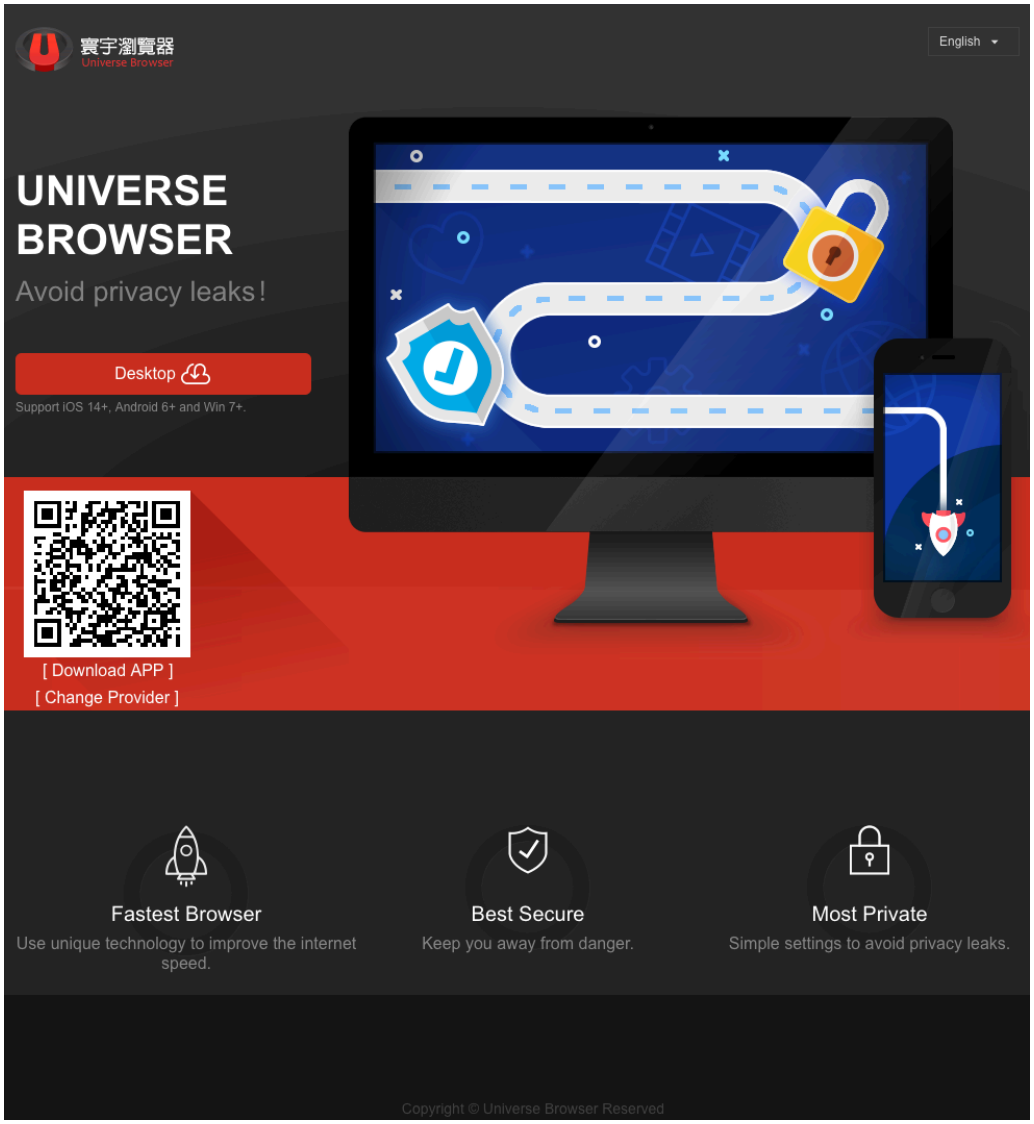

Figure 9. Universe Browser download page

Windows Variant

Analysis of the Windows sample, named “UB-Launcher.exe,” suggests it is rarely detected by antivirus engines. The download page usually looks like Figure 9. Upon execution, the installer immediately checks the locale as well as several VM checks before downloading the actual software. This payload contains a Chrome installer as well as a 7ZIP archive named “Application.7z,” copying both to the %APPDATA%/local/UB folder. “Application.7z” contains several dynamic link libraries (DLLs) used by the QT5 engine, a popular graphical user interface (GUI) for Windows apps, as well as five binaries and two specific browser extensions. The dropper will then install the Chrome version, copy the zipped extensions into the folder, and replace the Chrome.exe binary by “UB-Launcher.exe,” turning a legitimate Chrome installation into the “Universe Browser.” Chrome functionalities are stored in the “chrome_elf.dll,” which is invoked at runtime by the new “UB-Launcher.exe.” The installer will then achieve persistence by adding “UB-Launcher.exe” to the startup registry, which proceeds to run “UBMaintenanceservice.exe” (UB Security Management) which in turn calls “UBService.exe”’ (UB Networking Service). Figure 10 shows the software’s folder structure after successful installation.

```
UB/
└── Application/
    ├── extensions/
    │   ├── lineSelector/
    │   │   ├── troubleshooting/
    │   │   │   └── UBFirewallTool.exe
    │   │   └── UBIEAdapter.exe
    │   └── screenshot/
    ├── UBDownloader.exe
    ├── UB-Launcher.exe
    ├── UBMaintenanceService.exe
    ├── UBRun.exe
    └── UBService.exe
```

Figure 10. Simplified folder schema

Using the Universe Browser

After installation, the user is presented with a similar yet inauthentic default homepage emulating Google Chrome. Some Chrome functionality is disabled, including Dev Tools and chrome:// pages. Additionally, nearly every setting is inaccessible. The user agent is also modified to include a UB/{version} string at the end of the Chrome user agent to enable connections to be routed through a local and then remote proxy, thereby complicating analysis of traffic. Two extensions are added to the browser by default and visible from the start page. This includes “Screenshot” and “lineSelector,” both of which are specific to Vault Viper and not offered on the official Chrome Store. Figure 11 shows the default home screen.

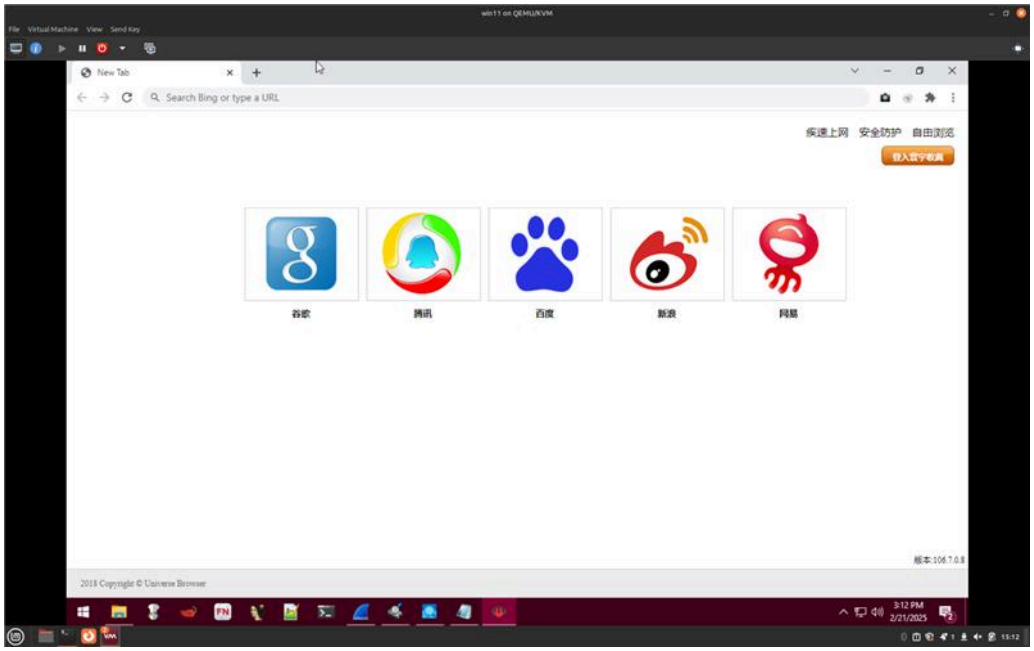

Figure 11. Universe Browser default screen

Screenshot and lineSelector

When accessed, the built-in extension, “Screenshot,” allows the user to take a screenshot of its current Universe Browser screen and upload it to a specific folder on ub66[.]com. The lineSelector extension—or more accurately “com.ub66.firewalltool”—is far more interesting. Browsing its “manifest.json” file, for instance, reveals it can connect to certain domains using a very specific URL structure related to crypto payments. The extension will connect to a ub66[.]com subdomain to check the geolocation of the victim’s computer. The rest of the code references UBIEAdapter.exe—a QT5 binary packed with UPX—and detailed logic to assign preferred domains and IPs (likely proxies) to the browser. This extension seems able to detect whether the user is connecting to an online gambling domain operated by Vault Viper. In this case, the lineSelector button will change color and indicate possible “routes” (线路). It is unknown whether this refers to agent business lines or proxy servers, likely both. This is apparent in Figure 12. The page does not appear different, but the connections through a proxy and the detection of the Universe Browser flag are probably handled specifically on the server side.

Figure 12. Universe Browser knows when the user is browsing on a BBIN website

Main Functionality: Examining the UBService Binary

UBService is the largest and most important of the Universe Browser binaries. It is run at every boot by UBMaintenanceService. UBService handles connections with the proxies and manages routes. It also creates a local interface and offers exposed call endpoints for other Universe Browser binaries to use through QT calls. UBService is another QT5 app containing several embedded resources, in particular a large SQLITE3 table containing encrypted records. The QT5 resources files—usually contained in a .rcc header—are now compressed using a variant of zLib and encrypted. The program also contains various anti-debugging techniques, such as unique seeds, preventing execution if a debugger is attached. The relationship between binaries is represented in Figure 13.

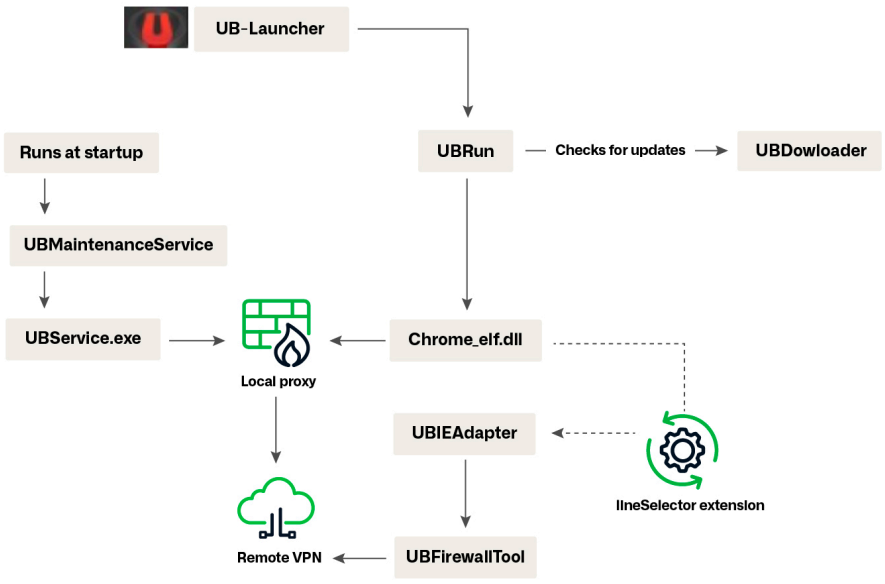

Figure 13. Interaction between Universe Browser binaries

Upon execution, the program will generate anti-debugging seeds, unpack its memory, and set up an interface for fetching and managing updates. The binary will subsequently reach out to pb88[.]ac101[.]net to check for updates before generating a unique hardware ID based on time and local interfaces. This UID will then be sent to Google Analytics on two different endpoints before the resources are unpacked, using an encryption key stored at "/files/key/keys" to decrypt its local SQLITE database. This encrypted database appears to contain a timestamp and SOCKS5 proxy traffic routes that will be used by the rest of the Universe Browser ecosystem. Figures 14 and 15 show part of the API management functions.

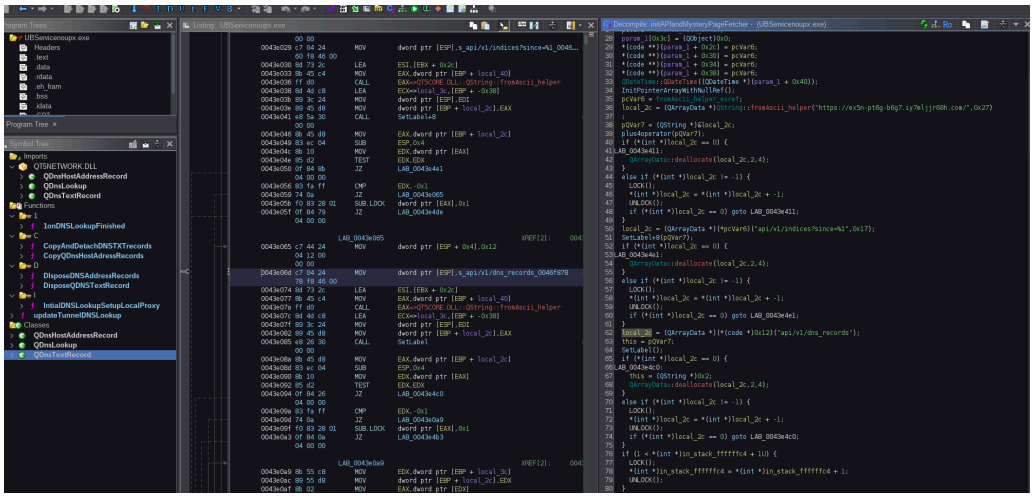

Figure 14. Decompiled functionality related to API management

Figure 15. API returning encrypted DNS records

Entries from the local database are subsequently sent to a remote endpoint and compared with the expected results. This allows the software to check its current version, assess connection speed, and find its external IP, among other functions.

Once the database is set up, the program will change the default DNS resolver to Alibaba. UBService then attempts to load content on several dictionary domain generation algorithm (DDGA) domains, which return a 418 error code. The 418 error code is not widely used compared to 404 Not Found or 403 Unauthorized. But hidden in those pages are several encrypted keys always starting with #9@B@9#, as shown in Figure 16. Those keys appear to be used in a different part of the program, used to decrypt the updated routes sent by the API domain. This is handled by a "BRouteManager" routine.

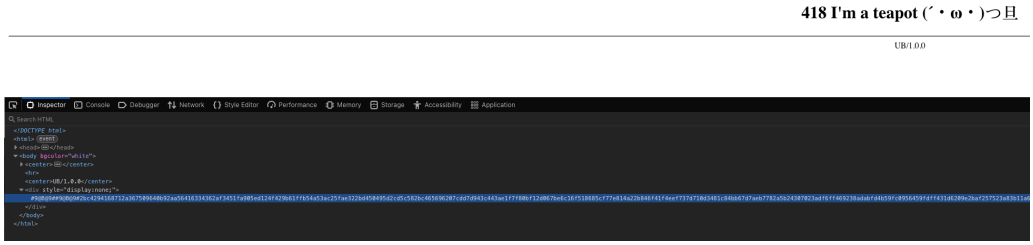

Figure 16. Key hidden on a 418 error page

In what follows, the service then queries several static, hardcoded domains for DNS TXT records which can contain any sort of encrypted data, as displayed in Figure 17 and 18. Derived keys from those records are used to set up Secure Shell (SSH) connections to various static IPs in China, advertised as SOCKS5 proxies, but we suspect to also be C2 servers. After analyzing the hosts, we identified four additional IP addresses sharing the same exact private key. Those IPs were associated with mobile applications signed by BBIN. Figure 19 shows a simplified diagram of the complete operations of UBService.

g1uvvowzz2.bzta2gq4.com@8.8.8.8 (Google):

```
g1uvvowzz2.bzta2gq4.com. 1200   IN      TXT     "bc0e36a457150bc8e47f1e258b908c"
g1uvvowzz2.bzta2gq4.com. 1200   IN      TXT     "bc0f32a4511b10d7ef7904398a98"
g1uvvowzz2.bzta2gq4.com. 1200   IN      TXT     "b90a2cbb561410d7e776043e89"
g1uvvowzz2.bzta2gq4.com. 1200   IN      TXT     "bc0f32a4511b10d7e17d04388e"
g1uvvowzz2.bzta2gq4.com. 1200   IN      TXT     "b90a2cbb561510d2e4601b3c8c"
```

---

hmbmmmuztj.wajn69nk.com@8.8.8.8 (Google):

```
hmbmmmuztj.wajn69nk.com. 1200   IN      TXT     "bc0f32a4511b10d7ef7904398a98"
hmbmmmuztj.wajn69nk.com. 1200   IN      TXT     "bc0f32a4511b10d7e17d04388e"
hmbmmmuztj.wajn69nk.com. 1200   IN      TXT     "b90a2cbb561410d7e776043e89"
hmbmmmuztj.wajn69nk.com. 1200   IN      TXT     "bc0e36a457150bc8e47f1e258b908c"
hmbmmmuztj.wajn69nk.com. 1200   IN      TXT     "b90a2cbb561510d2e4601b3c8c"
```

Figure 17. TXT records used as keys

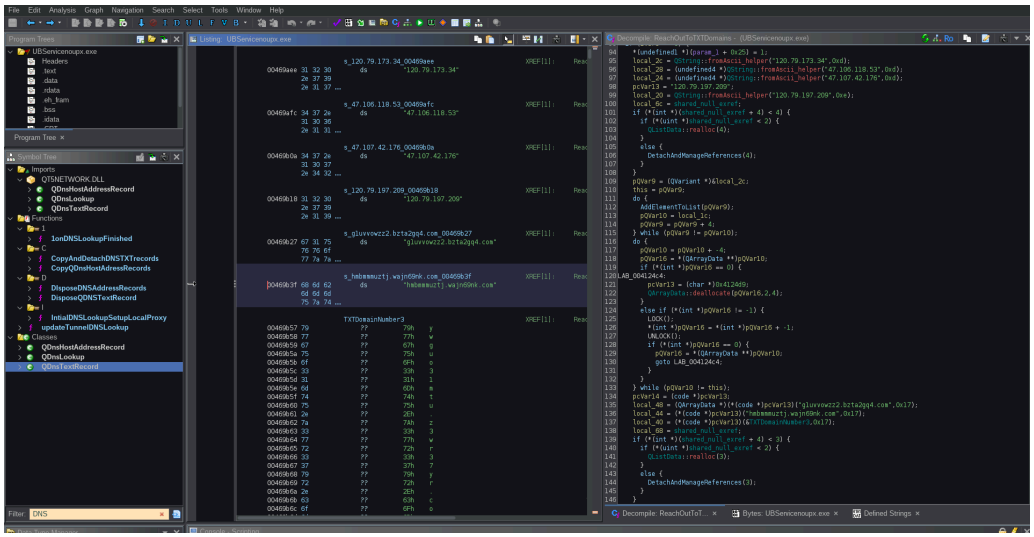

Figure 18. Decompiled code querying encrypted DNS records

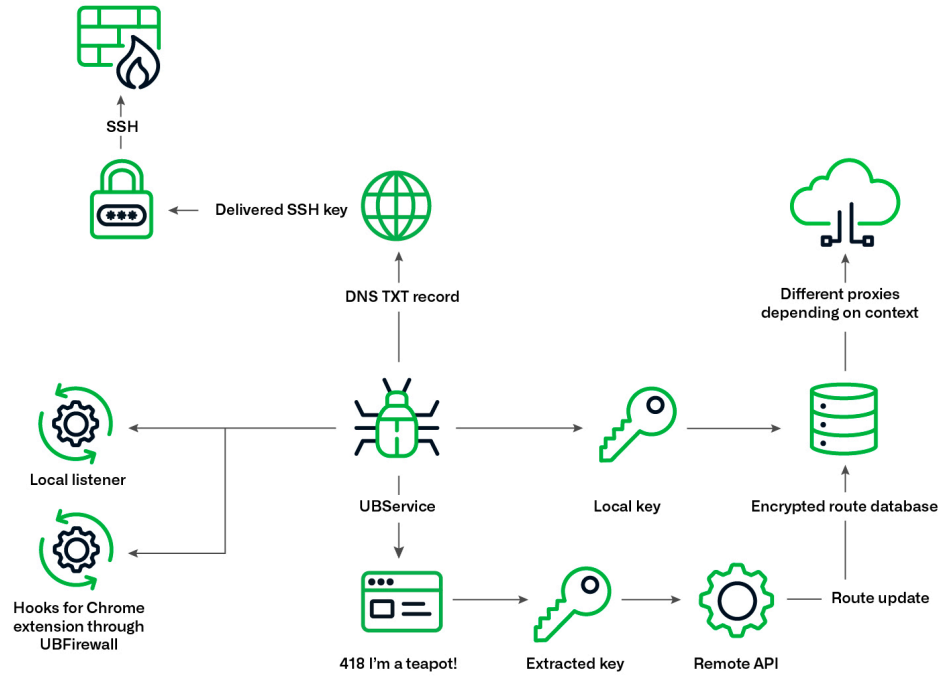

Figure 19. Simplified diagram of UBService's operations

Associated Mobile Applications

Vault Viper also distributes Universe Browser as a mobile application. The actor has created dozens of other mobile applications signed by BBIN and dedicated to specific online gambling platforms. We were unable to thoroughly test these as many operations are now offline. The mobile apps do not appear to contain any identified malware, but request for very broad permissions to be granted. It is also notable that they will not run if the device is rooted or attached to a debugger.

Vault Viper also advertises UBAuth, a multi-factor authorization app designed to work only with BBIN's own websites. Use of this app appears mandatory to withdraw funds from BBIN-supported online gambling platforms. UBAuth achieves persistence by creating a scheduled task and refuses to run if the phone is rooted or being debugged.

Vault Viper Network Infrastructure

Vault Viper uses at least a dozen domains spread across its own ASN, WOODSNET-PH, Amazon Web Services (AWS), and Chinese cloud provider, Alibaba, to control, manage, and update its software. Tunnel domains—through which player traffic is routed—are hosted on Western public clouds including Google's, but the most important domains to the group, serving as C2s (e.g., ac1091[.]net) or hosting their illegal casino customers, are all found in the same ASN.

At present, the ASN WOODSNET-PH (AS55547) is almost entirely dedicated to hosting unregulated online gambling websites in the Philippines, many of which are tied to verified criminal networks operating globally and running on BBIN infrastructure while also promoting the Universe Browser.

2024 Ban of Philippine Offshore Gaming Operators (POGOs)

While the Philippines has long served as an unregulated online gambling hub targeted by organized crime over the past decade, in July 2024, the country announced a nationwide ban on Philippine Offshore Gaming Operations (POGOs), citing escalating criminality, corruption, and infiltration of local political institutions as the primary catalysts. Although marketed as legitimate gaming enterprises, these operations had become deeply entwined with illicit activities, including large-scale cyber-enabled fraud, money laundering, human trafficking, kidnapping, torture, and murder—with POGOs and the broader online gambling industry effectively serving as fronts for organized crime. In response, Executive Order No. 74 was issued later that year by President Ferdinand Marcos Jr., mandating the immediate closure of all POGOs operations by year-end. Sweeping law enforcement raids targeting criminal operations that have moved deeper underground continue at scale today, highlighting the resilience of these syndicates and their complex business networks.

Numerous artifacts across Universe Browser and mobile app code mention "bbin", "bb-in", "bbinbrowser" or "bbbrowser" (Figure 20 is an example). The C2 domains are usually signed with SSL certificates mentioning BBIN, Taiwan, as shown in Figure 21 and 22. The brand is also prominently and proudly displayed on all gambling domains distributing the Universe Browser. Moreover, while not all BBIN content is hosted on this ASN, this ASN exclusively hosts content dedicated to BBIN. Going back in time, we can see the ASN's IP space slowly filling with Asian gambling domains, all using BBIN's templates and technology.

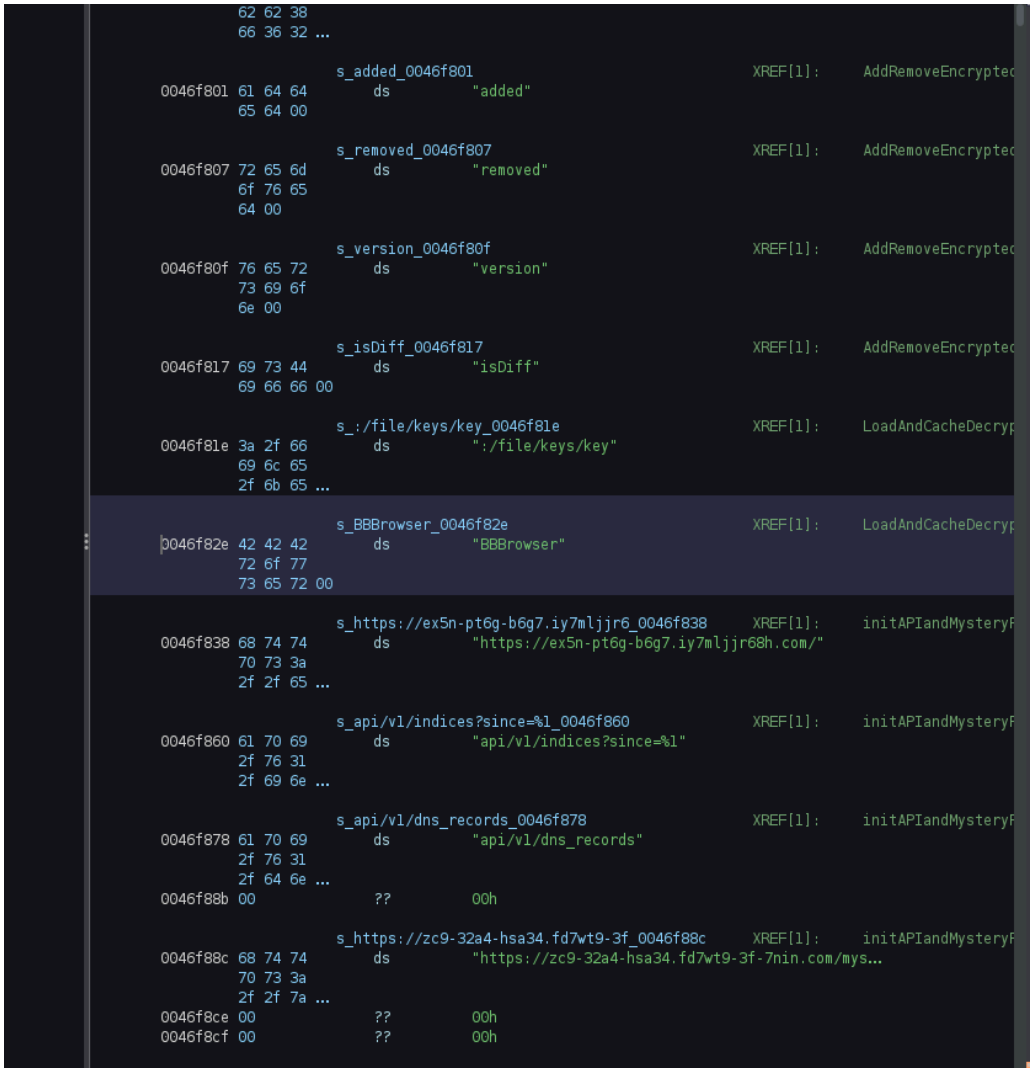

Figure 20. Example of a “BB Browser” string forgotten in a UBrowser binary

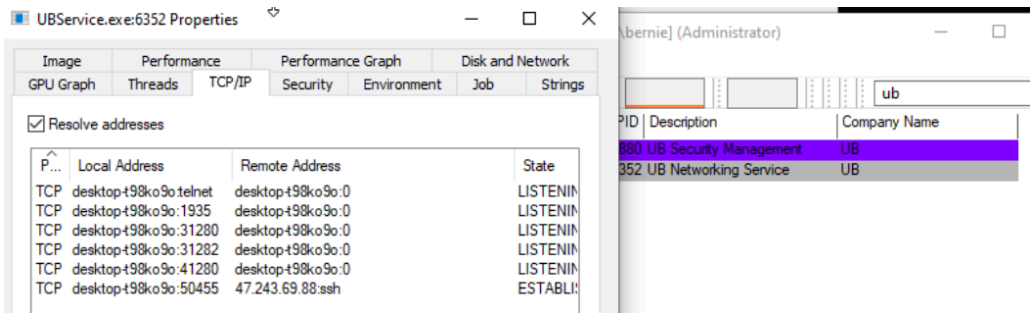

Figure 21. Universe Browser establishing an SSH connection to 47.243.69[.]88

Android Info

Summary

Android Type	APK
Package Name	bbin.mobile.yj8ub6rndt
Main Activity	com.google.android.apps.chrome.Main
Internal Version	1000
Displayed Version	40.560.3.1000
Minimum SDK Version	19
Target SDK Version	29

Certificate Attributes

Valid From	2015-01-07 06:58:48
Valid To	2069-10-10 06:58:48
Serial Number	7aa463fe
Thumbprint	2195d638cc3c5212156c00dfc0df3ff8fed00594

Certificate Subject

Distinguished Name	C:tw, CN:kingsley, L:taiwan, O:bbin, ST:taiwan, OU:bbin
Common Name	kingsley
Organization	bbin
Organizational Unit	bbin
Country Code	tw
State	taiwan
Locality	taiwan

Certificate Issuer

Distinguished Name	C:tw, CN:kingsley, L:taiwan, O:bbin, ST:taiwan, OU:bbin
Common Name	kingsley
Organization	bbin
Organizational Unit	bbin
Country Code	tw
State	taiwan
Locality	taiwan

Permissions

Figure 22. Android application communicating with 47.243.69[.]88, one of the identified C2s hosted on Alibaba. It was signed by BBIN, Taiwan.

Vault Viper uses authoritative servers which adhere to a specific naming convention: several letters and numbers followed by “cne”. For example, bolai777[.]com uses 589988cne[.]com, while ac101[.]net uses 88ylccne[.]com, connecting the main Bolai casino domain with the UBrowser C2 domain. The naming convention provides one mechanism to trace related domains over time. Through these we were able to unravel the actor’s domain history.

Other evidence demonstrated that AS55547 is tied to Vault Viper through a convoluted chain of shell companies described in the *Network Attribution: Unmasking Vault Viper* section of this report.

Ac101[.]net

In addition to operating its own ASN, Vault Viper maintains long-standing C2 infrastructure via ac101[.]net, a domain active since at least 2006 and historically leveraged to distribute a wide range of malicious payloads.[21, 22] This unusually deep operational history provides rare visibility into the evolution of the group’s tradecraft. Early-stage tooling consisted of crude C++ applications invoking the system’s default browser to access gambling sites, later progressing to DNS resolver–changer utilities and eventually a fully functional proxy service. Universe Browser progressively replaced their older BB Browser, despite their functionalities generally remaining the same.

Initial distribution campaigns of the custom browser were hampered by high detection from security products. Installers downloaded additional binaries and DLLs directly from ac101[.]net, routinely triggering antivirus signatures. In a notable 2013 incident, development machines themselves were compromised by the RAMNIT worm,[23] resulting in injected RAMNIT code coexisting with early Universe Browser builds and representing a unique case of adversary tooling being cross contaminated by unrelated malware. The same phenomenon was observed with PARITE[24] and ALMAN.[25]

The current Universe Browser release (v119.7.10 at time of writing) reflects Vault Viper's most advanced iteration to date, exhibiting enhanced evasion against static antivirus detection. Beyond browser builds, ac101[.]net infrastructure has also distributed malicious Visual Basic scripts (.vbs)[26] designed to modify DNS resolver settings on targeted Windows hosts to Vault Viper-controlled infrastructure, including domains such as ddns[.]bbin[.]net and dedicated IP ranges. An example is included in Figure 23. These DNS manipulations facilitate both sustained C2 communications and victim traffic redirection, underscoring the group's enduring reliance on network-layer manipulation as part of its broader collection and exploitation strategy.

```
Const STR_NEWDNS1 = "114.114.114[.]114"
Const STR_NEWDNS2 = "168.95.1[.]1"
strWinMgmt = "winmgmts:{impersonationLevel=impersonate}"
Set objNICs = GetObject( strWinMgmt ).InstancesOf("Win32_NetworkAdapterConfiguration"
)
For Each objNIC In objNICs
If objNIC.IPEnabled Then
objNIC.SetDNSServerSearchOrder Array(STR_NEWDNS1,STR_NEWDNS2)
End If
```

Figure 23. Example of VBS script in use in 2010 to change player's DNS resolvers

Testmyuser0009

Further investigation into AC101 infrastructure revealed a public GitHub repository[27] under the handle "testmyuser00009," containing multiple unfinished, predominantly web-based projects directly referencing AC101-hosted URLs for UBrowser binaries. While potentially the work of a Chinese-speaking affiliate, the repository yielded notable artifacts, including several iterations of a project titled BankReptile—an incomplete banking malware framework implemented via a Windows Forms application. BankReptile was designed to launch a browser instance through a locally invoked proxy, enabling credential interception and the exfiltration of financial data, suggesting developmental experimentation with targeted financial fraud capabilities within Vault Viper's broader toolset.

Network Attribution: Unmasking Vault Viper

By leveraging historical passive DNS (pDNS) data and our expertise in analyzing and mapping complex, transnational organized crime networks, we managed to gain a better understanding of Vault Viper's operations. Aided immensely by several historical operational security (OpSec) errors, we identified dozens of companies and individuals involved. Information consisting of overlaps in IP addresses, WHOIS data, specific DNS patterns, SSH keys, and other data points were corroborated and ultimately validated by hundreds of corporate documents, legal records, and court filings obtained and examined by Infoblox Threat Intel.

Level 1: BBIN

Pivoting off of BBIN's current ASN, WOODSNET AS55547, and its former ASN, EAGLENET AS55303, which both use the same email, aaa1490@gmail[.]com, we were able to trace operations back to Philippines-registered companies, Woodsdale Ventures and Eaglesky Technology, subsidiaries of parent company, BB International Leisure and Resort Development, the scale of which is visible in Figure 24. The Group has maintained a large operational base in the Philippines since 2006, particularly in notorious Clark Freeport and Special Economic Zone, and appears to have circumvented the Executive Order banning POGOs by running its large-scale technical operations from within the country's autonomous Cagayan Economic Zone Authority (CEZA).

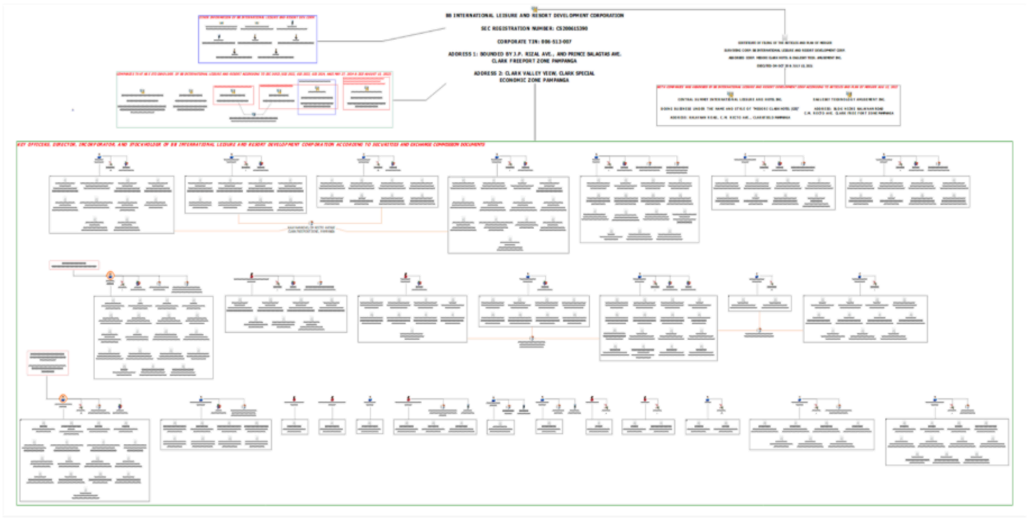

Figure 24. Depiction of Baoying corporate network in the Philippines, 2025, demonstrating the scale of the infrastructure (not intended for readability)

Like many Asian criminal networks, the true nature of the group's operations is concealed by public-facing businesses including real estate development, luxury hotels, a licensed casino,[28] and even a large waterpark, as well as a large Telegram channel servicing tens of thousands of users. They are largely masked through a tangled web of companies and obscure shell structures registered in countries and territories including Belize, the British Virgin Islands, China (including Hong Kong, Macau, and Taiwan), Malta, and Samoa, with BBIN-supported online gambling websites regularly displaying iGaming authorizations from regulators in the Isle of Man, Macau, Malta, and the Philippines, including the country's regulator, PAGCOR, and CEZA.

One of the key figures associated with Baoying Group and BBIN appears to be Taiwan-born Yang, Jen-Chieh (楊仁傑), who is listed as director and majority shareholder across many associated holding and investment companies around the world, including Belize-registered Treasure Prosper—an entity which held 99.99 percent of Baoying shares before corporate restructuring in 2023.[29] Despite these overlapping ownership interests, however, our investigation did not uncover any evidence that Yang Jen-Chieh himself had knowledge of or was involved with any cybercriminal activities. Current ownership is more complex, as illustrated by Figure 25.

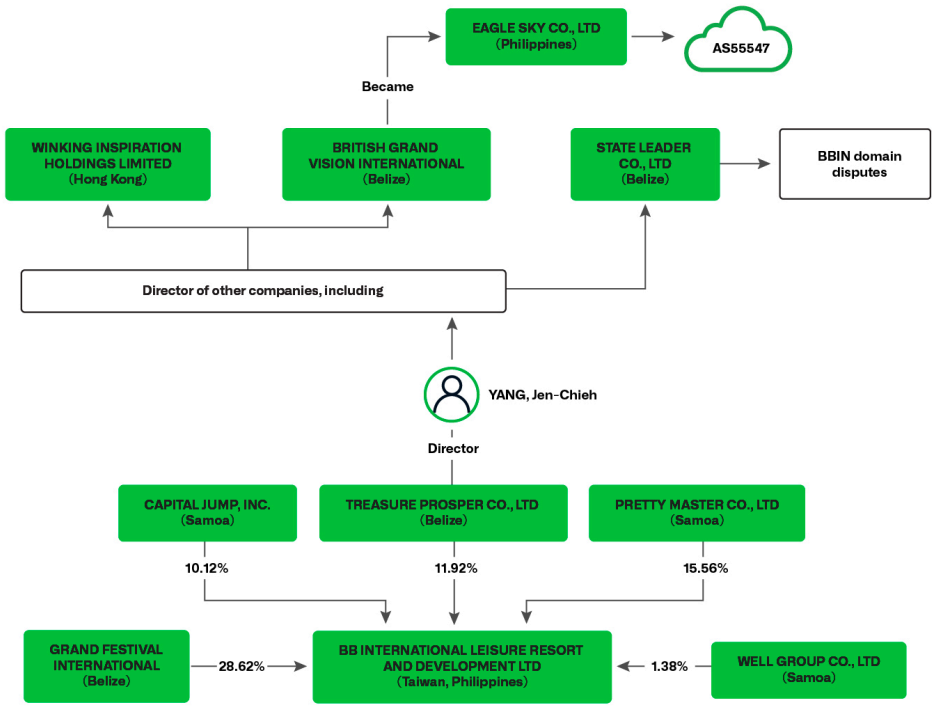

Figure 25. Simplified Baoying shareholder structure and extended corporate network, based on corporate filings

One key company under the new structure is Belize-registered, State Leader Co. Over the years, multiple domains associated with Baoying have been registered using email address easytalk@gmail[.]com. That same email address was also used to register a domain for Taiwan-registered La Pluma Fashion Group Co., Ltd—a company that was involved in the development of Esball and other casinos operated by Vault Viper.

An archived snapshot of the Esball app, developed by La Pluma Fashion Group, is shown in Figure 26. Esball development was later taken over by Cyberland Game Studio Ltd, the current UBrowser devs for iOS.[30]

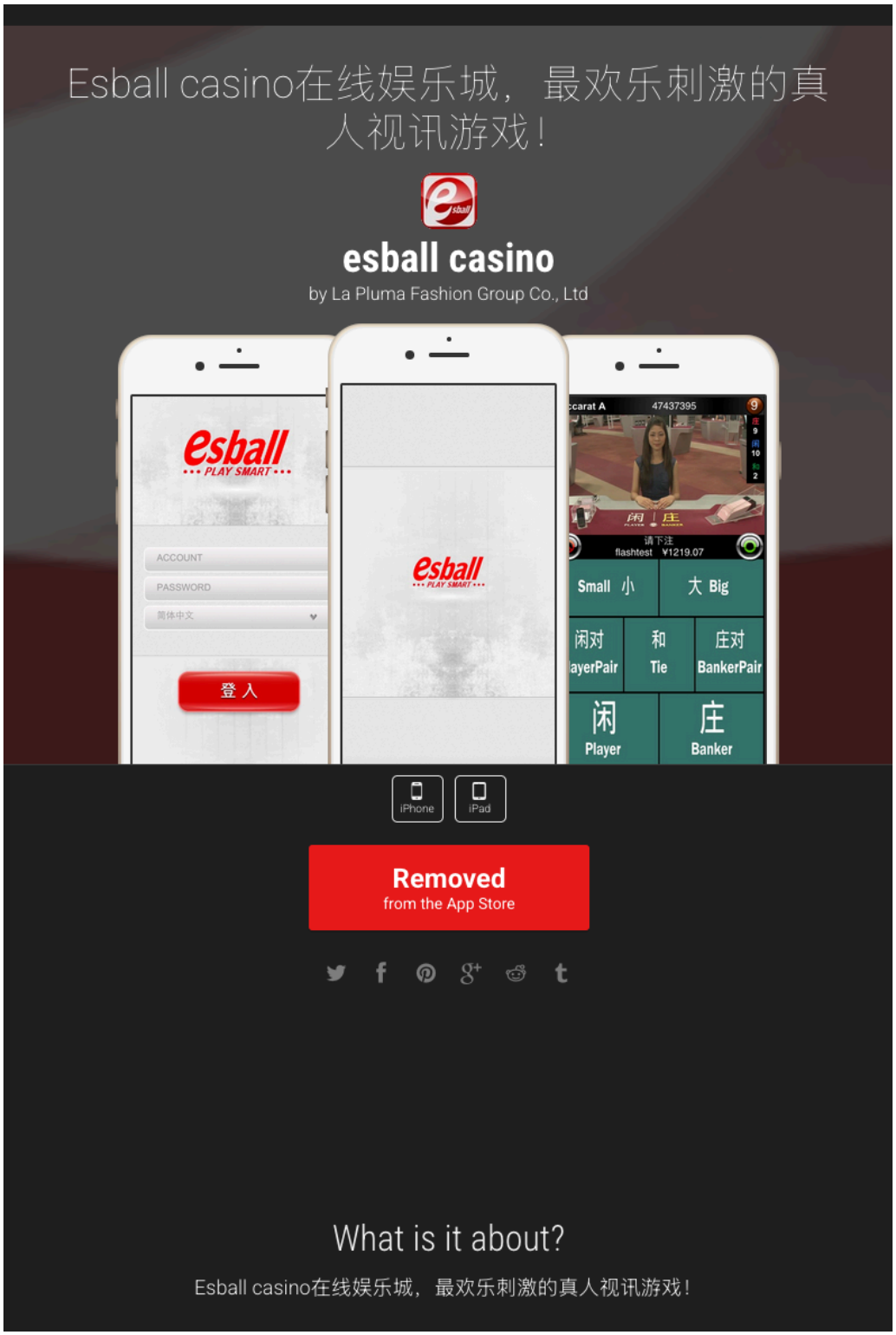

Figure 26. Archived page for Esball iOS, developed by La Pluma Fashion Group

The same email also registered a domain for Sytnet, another Taiwan-based company offering IT services, and more surprisingly, TG Airways. Indeed, at some point Baoying controlled several airplanes and was able to pick up players all over the world. We uncovered an old lawsuit mentioning TG Airway's majority stakeholder—BBIN—related to the sale of two 737 Boeing airplanes.[31] Other companies were mentioned in this 2006 arrest report in the Philippines.[32]

Pivoting further off various registries, corporate documents, and legal filings, we discovered that State Leader Co, Ltd. shares several of its addresses, directors, and/or technical relationships with a group of companies including Allied Mass Holdings, Chief One Technology, High Honest International, Leader Hill Technology, Pretty Master Co., and Saint Wealth Ltd. While ultimate ownership of these seemingly related entities remains unknown, it is worth noting that, between 2002 and 2017, Chief One and Leader Hill Technology were named among a group of defendants in two separate multi-million-dollar online fraud incidents targeting Ferrari North America and California-registered Wismettac Asian Foods.[33] While public information and case disclosure is limited, both incidents refer to injunction requests seeking to prevent "dissipation" of victim funds across multiple bank accounts, likely indicating the attempted use of online gambling platforms to transmit, obscure, and ultimately launder proceeds of fraud. To be clear, none of this documentation indicates criminal or civil wrongdoing by any of the companies mentioned.

Legal filings also draw connections between Hong Kong-registered online gambling businesses, Baoying Digital Technology and Winking Asia—another entity led by Baoying's Yang Jen-Chieh. We confirmed Winkings a was licensed online gambling operator in the United Kingdom through the one and only TGP Europe, an Isle of Man white label formerly operated by convicted crime boss, Alvin Chau Cheok-wa, and his Suncity Group—until recently, the world's biggest junket operator.

These legal fillings do not establish any participation in criminal law violations by Yang Jen-Chieh.

Level 2: Alvin Chau and Suncity Group

Extensive analysis of available corporate and DNS records, criminal court proceedings, and related legal filings and case documents reveal substantial linkages between Baoying Group and a notorious organized crime syndicate led by Suncity Group founder, Alvin Chau.

As highlighted by Chinese authorities during his final sentencing hearing, Chau was found to have been the majority shareholder of Bao Ying (寶盈),[34] holding 66.67 percent ownership as of January 2023.[35] Prosecutors specifically noted that Chau's stake in the company, among several other leading iGaming platforms his network had infiltrated and utilized as proxies, had been used to increase the operating capital to scale up illegal betting and underground banking operations while also helping to decentralize and offset Suncity's risk. They concluded that Suncity, at the time responsible for as much as 50 percent of high-roller gambling turnover in Macau,[36] and proxies including Baoying, ultimately served as a sophisticated front for organized crime[37]—with related criminal investigations in other jurisdictions revealing its involvement in large-scale money laundering and underground banking-as-a-service[38, 39]. Figure 27 represents Alvin Chau next to his indictment, while Figure 28 shows the embedding of BBIN on one of Suncity's online platforms.

More than this, analysis of historical DNS records reveals brands identified with Suncity were sharing infrastructure with a small yet meaningful number of gambling domains, many of which were licensed through TGP Europe. While we initially discarded these findings as coincidence, our investigation points to a significant Suncity nexus, culminating in relationships between TGP Europe, the 138[.]com and Sunbet[.]com gambling sites, and the abovementioned Winking Asia. We uncovered additional information connecting these and other seemingly unrelated companies back to the Suncity/TGP nexus but are not publishing it at this time.

Figure 27: Alvin Chau (left) and his indictment (right) (Source: Suncity Group and Macao Special Administrative Region Primary Court Second Criminal Court Collegiate Panel Ordinary Criminal Case No. CR2-22-0147-PCC)

Alvin Chau was convicted in January 2023 and sentenced to 18 years in prison on over 100 charges relating to facilitating illegal bets exceeding HK $823.7 billion (US $105 billion) between March 2013 and March 2021 through multiplier betting,[40] utilizing Suncity corporate, financial, and technological infrastructure, resources, and partnerships to conceal related transactions.[41,42] Digital evidence and other data recovered and reported by Chinese authorities notably indicate that at least 300 billion yuan (US $42 billion) in illegal bets were processed through the group's offshore online betting operations between 2015 and 2021.[43]

Figure 28. BBIN embedded within former Suncity online betting platform (Source: Suncity Group (2019) and Associated Press (2021))

In addition to Alvin Chau, the Wenzhou Intermediate People's Court convicted 36 individuals affiliated with the syndicate, finding that the group provided cross-border currency exchange and settlement services and collected gambling debts through asset management companies and underground banks it had established in mainland China.[44] The court determined that between 2016 and 2021, the Suncity-linked network had expanded to more than 280 mainland Chinese shareholder-level agents who capitalized the shadow business, as well as more than 38,000 multi-level gambling agents and promoters, and 80,000 clients (players).[45] Separately, in February 2024, authorities in Hubei sentenced 13 senior members of a Philippine-based illegal offshore gambling network specifically using Suncity and BBIN infrastructure to recruit and service more than 250,000 gamblers across 25 Chinese provinces, with the network facilitating illegal bets exceeding 1.6 billion yuan (US $220 million).[46]

Associated offshore Suncity operations were also identified by authorities in Australia, Cambodia, the Philippines, Vietnam, and many others, with the syndicate extensively documented servicing major criminal groups around the world—particularly those engaged in cyber-enabled fraud and drug trafficking—as well as threat actors attributed to the Democratic People's Republic of Korea (DPRK) Reconnaissance General Bureau (RGB). As examined below, the syndicate also shares a close relationship with Vigorish Viper and is likely part of an extended criminal network.

Links to Vigorish Viper and a Broader Criminal Ecosystem

As a quick refresher: Vigorish Viper is a highly sophisticated Chinese organized-crime syndicate unearthed by Infoblox and reported in July 2024.[47] It operates an integrated cybercrime supply chain that encompasses custom software, DNS configurations, website hosting, mobile apps, encrypted communications, and payment systems, all designed to enable primarily Chinese-facing illegal online gambling operations and associated financial flows. The group exploits high-profile European football club sponsorships to covertly promote these gambling platforms, leveraging the sports teams' reach to attract clients while maintaining plausible deniability.

Affiliated with the criminally implicated Yabo Group[48] which is referenced throughout the software and infrastructure and likely to have developed the software and DNS network, Vigorish Viper was found hosting over 170,000 active domains, deploying multi-layer DNS CNAME traffic distribution systems (TDSs) and JavaScript-based cloaking techniques to evade detection. Like Vault Viper, its criminal portfolio, however, extends far beyond illegal online betting, with documented links to large-scale money laundering and human trafficking throughout Southeast Asia—and to no surprise, really. Suspected to be at the center of these operations, according to authorities and researchers alike, is U.K. and U.S.-sanctioned Dong Lecheng[49,50] and, yet again, Alvin Chau, Suncity Group and TGP Europe.

Figure 29. Alvin Chau (left) and Dong Lecheng (right) in transit from Cambodia to Macau with business associates

Chinese-born, Dong Lecheng, also known in Cambodia as Heng Tong following his naturalization in 2014, is widely cited across Chinese criminal records over the past two decades for his involvement in various cross-border crimes between China and Myanmar. He is photographed in Figure 29 next to Alvin Chau. Through his Yunnan Jincheng Group, Lecheng developed a portion of Cambodia's infamous "Chinatown" cyberscam compound in Sihanoukville, alongside his crown jewel, the Golden Sky Sun Hotel and Casino, located directly adjacent and shown in Figure 30. According to Chinese authorities and testimonies from victims of human trafficking, torture, and enslavement, as of early 2023, operations within the Chinatown compound were extensively dedicated to online fraud and supporting illegal online betting websites, including Yabo.[51] This was further substantiated by the Yingshang County Public Security Bureau of Fujian in June 2023 which issued a criminal notice following a multi-year investigation concerning illegal online gambling and cyber-enabled fraud operations housed in "Chinatown" and the Sunshine Bay Hotel, another nearby compound controlled by Dong's extended network.[52]

Figure 30. Chinatown compound and Golden Sun Sky Entertainment, Sihanoukville, Cambodia, 2023 (Source: Bloomberg and Voice of Democracy)

As illustrated by the photographs in Figure 31 and 32, Lecheng operated within elite criminal and political business circles, most apparent through his dealings with Alvin Chau and the extended family network of Senator Kok An—one of Cambodia's wealthiest men currently wanted by Thai authorities together with other members of his family in connection to scam centers and money laundering. In 2018, Alvin Chau expanded Suncity operations into Cambodia, partnering with Lecheng and the Kok network to bring in Suncity technical expertise and solutions to manage and operate Golden Sun Sky for the small fee of US $360 million. In addition, the group facilitated the establishment of Suncity VIP rooms and related businesses owned and operated by Rithy Samnang, since-deceased son-in-law of Senator Kok An, and his brother, Rithy Raksmei, also known as Xie Liguang and Ken Oriya. This notably includes the

RSX Investment Co, which was used by the network to secure online gambling licensing to cover the Chinatown compound via the infamous U.K.-sanctioned K.B. Hotel and Casino, also known as Kaibo Park (凯博园区), and facilitate “financial arrangements and remittance advice” for users. Figure 31 and 32 show Dong Lecheng with several notable individuals, including Kok An and Rithy Raksmei.

Figure 31. U.K.-sanctioned Dong Lecheng pictured alongside Senator Kok An, criminally implicated Rithy Raksmei, Rithy Samnang, and convicted Triad boss Alvin Chau (Source: Instagram (left) and Suncity Group (right), 2018 – 2021)

Figure 32. UK-sanctioned Dong Lecheng pictured attending business meeting and signing ceremony alongside Senator Kok An, criminally implicated Rithy Raksmei, and Rithy Samnang (Source: Instagram (left) and Suncity Group (right), 2018 – 2021)

Interestingly, specific IP ranges tied to Vault Viper peering to AS55547 have been observed in connection to the Suniway network and a prolonged, targeted DDoS campaign against several Filipino investigative journalists and human rights organizations, as documented by Qurium.[53] According to researchers, attacks targeted local entities critical of POGOs seeking to expose links to organized crime and online gambling, specifically originating from two subnets, 125.252.99[.]0/24 and 261.244.184[.]0/24, tying back to Eaglenet and BBIN. While inconclusive, the case is consistent with the network’s broader criminal behavior, representing an additional example tying this infrastructure to cybercrime operations.

Taken together, these documented partnerships and connections to cybercrime help us contextualize Vault Viper as a critical component of infrastructure and tradecraft that has not only helped launder billions for sophisticated Asian crime networks but also carries with it major security implications for millions of unsuspecting users around the world.

Security Assessment and Conclusion

Our research supports the conclusion that Vault Viper’s development and deployment of a custom browser platform serve as a multi-purpose exploitation and criminal service framework. In addition to servicing criminal operations and illegal bettors, its capabilities include interception of network traffic, persistent user surveillance, and a backdoor enabling deployment of additional payloads. This operational flexibility positions the browser as a modular C2 vector for identification of interesting targets and follow-up infections.

Long-running C2 domains have been evolving for years, casting doubts on its mere use as a supposed privacy browser and raising serious concerns over its possible security implications. In addition to identifying instances of contamination by other malware, as well as a custom banking trojan found mentioning the same C2s,[54] Vault Viper has spent the better part of the past two decades fine-tuning their binaries to avoid antivirus detection. While this may

align with their stated purpose and objectives as a privacy-oriented browser, commercial apps are also regularly abused by cybercriminals, and we feel the need to draw a fine line on this one for several reasons.

For starters, Vault Viper's abovementioned antivirus detections could, on one hand, be false positives—after all, they are based mostly on heuristics. But we fail to identify a scenario in which injecting code into iexplore[.]exe, for instance, alongside event hooking and VM and debugging detection and obfuscation, is necessary for a fork of Chrome. This is particularly true given the backdrop of illegal gambling that the browser is designed to facilitate. Beyond bad coding practices, these deliberately enabled functionalities and behavior appear to extend beyond that of a typical "privacy-oriented browser," representing something more typical of malware. The program's integration of several covert persistence and communication mechanisms to and from Vault Viper, alongside its packing typology and use of encrypted data to hinder analysis, further support this assessment.

More than this, Universe Browser has been modified to remove many functionalities that allow users to interact with the pages they visit or inspect what the browser is doing. The right-click settings access and developer tools, for instance, have all been removed, while the browser itself is run with several flags disabling major security features including sandboxing, and the support of unsecure SSL protocols, greatly increasing risk when compared with typical mainstream browsers.

Vault Viper exploits the illegal betting market by offering gamblers a tool that promises secrecy and access, while treating them with outright contempt—their compulsion to wager is leveraged to extract even more value. In addition to profiting from the stakes themselves, Vault Viper can siphon off personal and financial data, monetizing it in ways the victims cannot contest, since their own participation in illegal activity prevents them from seeking recourse. It is not inconceivable that what presents itself as a convenient gateway to underground online casinos likely doubles as a trap engineered to milk users for everything they are worth.

Despite the suite being marketed as a solution to apparent "payment issues," controlled testing (constrained by legal and operational risk protocols) found no functional changes to payment mechanisms, indicating a possible social engineering lure rather than a legitimate feature. That said, while the Universe Browser may be effective in allowing users to bypass the Great Firewall and other state-level censorship efforts, its proxy architecture is generally unsophisticated, with the client relying on a basic SOCKS5 implementation via Qt with hardcoded cryptographic material obfuscated across multiple files. This reflects an approach unlikely to withstand deep packet inspection (DPI) by state-level network defenses, further reinforcing the assessment that its stated purpose is a façade for more covert and potentially malicious objectives.

All in all, by routing all user traffic through Vault Viper–controlled infrastructure, the browser carries a high risk of credential compromise and data exfiltration. Given the actor's established links to Chinese organized crime, downstream threats include targeted account and device takeover, online fraud, and integration of harvested data into broader cybercrime ecosystems. The observed tooling, victim targeting, and infrastructure control collectively indicate that Universe Browser is not a benign circumvention tool, but rather a high-risk collection and exploitation platform embedded within Vault Viper's broader criminal enterprise.

Taken together, the technical shortcomings, deceptive marketing, and centralized infrastructure control point to a platform deliberately engineered for exploitation rather than user benefit. Universe Browser is not merely a circumvention tool gone rogue, but rather represents a purpose-built vehicle for sustained surveillance, data theft, and criminal monetization under the direction of a sophisticated criminal network.

Although the distribution of riskware by an iGaming platform of BBIN's size is unprecedented by all accounts, this case is consistent with a broader trend which has seen Asian crime syndicates involved in online gambling developing increasingly advanced capabilities and technical infrastructure and ultimately evolving into more sophisticated cyberthreat actors. The investigation into Vault Viper demonstrates that Baoying Group's BBIN operations extend far beyond online gambling technology, in fact serving as a cornerstone of large-scale criminal infrastructure in Asia. Our analysis shows that its custom browser, DNS infrastructure, and integrated services function as a multi-purpose exploitation framework enabling persistent access, credential theft, and large-scale monetization, all while it blends into both consumer and enterprise environments. More than representing a unique technical threat, however, Vault Viper serves as a key enabler of transnational organized crime in Southeast Asia, with proven ties to multi-billion-dollar laundering, human trafficking, and cybercrime rings.

As these operations continue to scale and diversify, they are marked by growing technical expertise, professionalization, operational resilience, and the ability to function under the radar with very limited scrutiny and oversight. This evolution is rapidly transforming the regional threat landscape into one of the most dynamic and underestimated challenges confronting the international community at scale today. Unregulated online gambling, long treated as a peripheral or altogether insignificant issue and threat, has proven to be a highly practical vector for cyber-enabled crime and large-scale money laundering. By exposing what we now know about Vault Viper and the extended criminal ecosystem it has supported for decades, we hope this report will increase awareness, understanding, and interest into this category of threat actors, and contribute meaningfully to the growing body of

research and policy discussions aimed at disrupting, mitigating, and responding to these sophisticated criminal networks.

Indicators

Those indicators can also be found in our open GitHub repository.

Indicator	Type	Description
0592aad472bbadeb6edc55573d7bcd2cff560504de5c94d8e1600188f143e523	sha256	Windows installer
ac101[.]net	Domain	Additional downloads
yts79y3-zew6s.p0bgceeug-l[.]com ex5n-pt6g-b6g7.iy7mljjr68h[.]com	Domain	API/DNS records domains
zw6q9v-k6vczr[.]com qzvj52cv-typf[.]com mzim-e83ja-5wm[.]com fvwy-i65-82meq[.]com c2a-ut9fj-2v7m[.]com b9gw-g5p-9x7mq[.]com	Domain	DNS/proxy servers
d1ko2n56twscbk.cloudfront[.]net ub.zhanglijuanlawyer[.]com chu-shi-biao.s3-website.ap-northeast-2.amazonaws[.]com d38z5zttlbg669.cloudfront[.]net	Domain	Proxy domains
cdn.mr3yh8er[.]com cdn.n4dhx7bt[.]com	Domain	Download CDN
phone589[.]com ag04vip[.]com boss04vip[.]com	Domain	Ac101 clones
ub66[.]net ub66[.]io ub66[.]me huanyuliulanqi[.]com eamix[.]cn 650llq[.]cm ub66[.]com	Domain	Advertisement page, first-level C2s
g1uvvowzz2.bzta2gq4[.]com hmbmmmuztj.wajn69nk[.]com ywguo31mtu.z3wr37yr[.]com	Domain	DNS TXT key distribution domains
120[.]79[.]173[.]34 120[.]79[.]197[.]209 47[.]107[.]42[.]176 47[.]106[.]118[.]53 47[.]243[.]69[.]88 47[.]243[.]172[.]76 146[.]88[.]164[.]244 146[.]88[.]165[.]78	IP	Alibaba SSH IPs
h9pvs-2eanqhz.csqq2g-fzc5i5[.]com/mysteries-pages/418.html zc9-32a4-hsa34.fd7wt9-3f-7nin[.]com/mysteries-page/418.html	URL	418 pages with hidden keys
xn--29s7ix44lsga.ub66[.]com xn--29s7i934gspn.ub66[.]com xn--29s7inly9ib.ub66[.]com	Domain	

Footnotes

1. In the United States alone, authorities reported more than US $5.6 billion in financial losses to cryptocurrency scams in 2023, with an estimated US $4.4 billion attributed to so-called “pig butchering” schemes most prevalent in Southeast Asia. Regionally, countries in East and Southeast Asia combined have lost up to an estimated US $37 billion to cyber-enabled fraud during that same year according to latest available data, with much larger estimated losses being reported globally.
2. Vigorish Viper: A Venomous Bet, 2024, Infoblox Threat Intelligence.
3. Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, January 2024, United Nations Office on Drugs and Crime (UNODC). https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf

4. Confronting the Threats to Integrity – Illegal Betting Markets and Disruptive Technology, August 19, 2024, Asian Racing Federation Council. https://cdn.prod.website-files.com/5fbe2bde2b2ef4841cd6639c/66c3fbbe8dcb63d3472b0ba3_ARF%20Confronting%20the%20Threats%20to%20Integrity%20Re
5. Money Laundering National Risk Assessment Report, October 30, 2024, Monetary Authority of Singapore. https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/money-laundering-national-risk-assessment
6. Online Gambling Red Flags and Typologies Report, May 2025, Isle of Man Financial Intelligence Unit. https://www.fiu.im/media/1245/online-gambling-typology-2025.pdf
7. Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia, April 2025, UNODC. https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf
8. Vigorish Viper: A Venomous Bet, Infoblox Threat Intelligence.
9. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking, and Technological Innovation in Southeast Asia: A Shifting Threat Landscape, October 2024, UNODC. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf
10. Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, UNODC, March 2024. https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf
11. How Organised Crime Operates Illegal Betting, Cyber Scams & Modern Slavery in Southeast Asia, Asian Racing Federation, Hong Kong Jockey Club, October 2023. https://cdn.prod.website-files.com/5fbe2bde2b2ef4841cd6639c/651e891f6cca0e3f417cd876_How%20Organised%20Crime%20Operates%20Illegal%20Betting%
12. Confronting the Threats to Integrity – Illegal Betting Markets and Disruptive Technology, November 6, 2023, Asian Racing Federation. https://cdn.prod.website-files.com/5fbe2bde2b2ef4841cd6639c/66c3fbbe8dcb63d3472b0ba3_ARF%20Confronting%20the%20Threats%20to%20Integrity%20Re
13. Money Laundering Risk Assessment Report Singapore 2024, May 2024, Money Laundering Authority of Singapore. https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/amld/2024/money-laundering-national-risk-assessment.pdf
14. National Statement on eGaming and Financial Crime: Activities, Risk Appetite and Mitigation, May 2025, Isle of Man Financial Intelligence Unit. https://www.gov.im/news/2025/may/29/island-national-risk-appetite-statement-published/
15. Scam Trafficking Rescues on the Rise, July 12, 2022, Voice of Democracy. https://vodenglish.news/scam-trafficking-rescues-on-the-rise-regional-media/
16. Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, UNODC.
17. Bōcài (菠菜), literally meaning “spinach,” is a euphemism widely used in Chinese underground discourse to denote illegal gambling activities, particularly unregulated online gambling services. The term allows participants to discuss these illicit operations while avoiding direct reference to gambling (赌博), which may be subject to censorship or legal scrutiny. In this context, “bōcài” specifically indicates the provision of illegal online gambling as a service.
18. Jiuquan City, Suzhou District Court, Press Release, March 2023.
19. People’s Court of Yongding District, Zhangjiajie City, Hunan Province, Press Release, November 2017.
20. Taiwan National Police Agency, Central Investigation Bureau, Press Release, June 2024.
21. VirusTotal. https://www.virustotal.com/gui/domain/pb88.ac101.net/relations
22. Internet Archive. https://web.archive.org/web/*/pb88.ac101.net*
23. VirusTotal. https://www.virustotal.com/gui/file/f6741f9cbc9daeec916fc1bdcd51ff4a35b3d6ca89bb4bef58d31ba54abac850
24. VirusTotal. https://www.virustotal.com/gui/file/b9b0e148935b35f8ccb2082cfcd5a7a5d5184de1a7314d8a688bd84268ef3afc
25. VirusTotal. https://www.virustotal.com/gui/file/4431b25aff1aa297830c665c8d609ca8c5ed44d81225f19d3f03d549524aa056
26. VirusTotal. https://www.virustotal.com/gui/url/fa337d1b812926eacbc5ee1349c1d3311a043c9c8c372db07feb6fc0d6bd9cdf
27. GitHub. https://www.github.com/testumyser0009/
28. Licensed for land-based casino operations, not online gambling operations.
29. Uniquely aligns with the time of Alvin Chau’s arrest in Macau.
30. AppAdvice. https://appadvice.com/game/app/esball-casino/866953566
31. BB In Technology Co., Ltd. v. JAF LLC, 242 F.R.D. 632
32. NBI sues 3 Taiwanese, Canadian for illegal casino in Clark, October 27, 2006, TMCNet, Technology Marketing Corporation. https://www.tmcnet.com/usubmit/2006/10/27/2021979.htm
33. vLex. https://vlex.hk/vid/wismettac-asian-foods-inc-851831582
34. The Chinese name of BBIN is Bao Ying Group (寶盈集團). A literal translation of the two characters Bao (寶, simplified 宝) and Ying (盈) is “prosper treasure.”

35. Acusação do Ministério Público, n.º: 1345/2022. https://www.court.gov.mo/sentence/zh-9f8cd198757f3527.pdf
36. Hong Kong Jockey Club, Asian Racing Federation, 2023.
37. Acusação do Ministério Público, n.º: 1345/2022.
38. Casino Inquiry, 2021, Parliament of New South Wales, Australia. https://www.parliament.nsw.gov.au/la/papers/Pages/tabled-paper-details.aspx?pk=79129
39. Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, UNODC.
40. Multiplier betting, also known as “tok dai” (托底), refers to a form of “under-the-table gambling” in which a bet formally denominated at the casino gambling tables represents only a fraction of the total amount of a private bet made between gamblers and junket operators to avoid gaming revenue levies. It allows clients to pre-negotiate their preferred payment method, betting currency, and cash-out method while increasing the commissions received by VIP junket promoters, and can be used as a tactic to conceal the total amount of money transmitted through the casino by an individual bettor and obfuscate the source and destination of funds. Such arrangements are understood to have grown in popularity due to most junket customers in Macau SAR originating from mainland China. These customers do not—and in any case cannot—bring money with them to play due to strict capital controls and a nation-wide gambling ban in mainland China, and instead rely on credit issued by junket agents. For instance, should a customer request a HK $1 million credit, the junket agent can request the casino to provide HK $100,000 worth of chips, with the understanding between the junket agent and customer that a ten times multiplier is in effect.
41. Public Prosecutor’s Office of Macau SAR. Investigation file no. 3472/2020, prosecution charge no: 1345/2022.
42. Acusação do Ministério Público n.º: 1345/2022.
43. China Central Television, Government of the People’s Republic of China, January 2024.
44. Wenzhou City Public Security Bureau, 26 November 2021.
45. Acusação do Ministério Público n.º: 1345/2022.
46. Shasi District Procuratorate of Jingzhou City, People’s Procuratorate of HuBei, Press Release, September 2024.
47. Vigorish Viper: A Venomous Bet, Infoblox Threat Intelligence.
48. Amid mounting law enforcement and 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.
49. Office of Financial Sanctions Implementation HM Treasury, Global Human Rights Sanctions, Financial Sanctions Notice, December 2023. https://www.gov.uk/government/news/uk-and-allies-sanction-human-rights-abusers
50. Transnational Criminal Organizations Designations; Burma-related Designations; Global Magnitsky Designations; Cyber-related Designations, September 8, 2025, United States Treasury Office of Foreign Assets Control. https://ofac.treasury.gov/recent-actions/20250908
51. China Youth Daily, Communist Youth League of China, 2023. http://zqb.cyol.com/html/2023-06/06/nw.D110000zgqnb_20230606_2-05.htm
52. Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, UNODC.
53. What is hosted at the Suniway network? April 2019, Qurium Media Foundation. https://www.qurium.org/alerts/what-is-hosted-at-suniway-network/
54. GitHub. https://github.com/testumyser0009/xiaozhushou2/

+2