
SILENT PUSH
Mapping The Triad Nexus & FUNNULL CDN Cyber Threats
192.158.1.38
Tracking a Chinese Content Delivery Network Hosting Pig Butchering & Money Laundering Sites
192.158.1.38
January 2024
192.158.1.38
Presented by Zach Edwards, Senior Threat Analyst – Silent Push

°7ƶijţ} ЄĂ‹ , ţαţXœ} } œvv
8Є2 ijó

1. Polyfill[.]io Supply Chain Attack Timeline
2. ACB Group Ownership Details
3. Hosting Pig Butchering Sites for *Years*
4. Mapping FUNNULL CNAME Chains
5. FUNNULL CDN Infrastructure Details
6. Online Gambling Sites for Money Laundering
7. Recruiting Money Movers (Tether + Telegram)
8. Retail Phishing Scam
9. Summary
10. Open Questions
11. Collaboration is Key

Polyfill[.]io Supply Chain Attack Timeline

FUNNULL executed the largest corporate supply chain attack in 2024...

February 2024

FUNULL acquires Polyfill[.]io:
The polyfill[.]io domain was a legacy JavaScript product embedded into hundreds of thousands of the biggest websites on the internet.

July 25, 2024

Sansec Warns of Polyfill[.]io, Google takes action:
Sansec reported the new Chinese owner was maliciously redirecting mobile users. On the same day, Google started blocking ads for sites that used Polyfill.

July 28, 2024

Researchers uncover 8 domains associated with FUNNULL supply chain attacks:
While researching polyfill[.]io several organizations were able to connect the efforts back to at least June 2023 and these other domains: bootcdn[.]net, bootcss[.]com, staticfile[.]net, staticfile[.]org, unionadjs[.]com, xhsbpza[.]com, union[.]macoms[.]la, newcrbpc[.]com.

July 27, 2024

June 27, 2024
Namecheap takes over Polyfill[.]io Domain:
To prevent ongoing abuse, Namecheap took over the Polyfill[.]io domain, essentially ending the supply chain attack.

ABC Group Ownership Details

The ACB Group website - acb[.]bet - was online until June 2024, and seemingly went offline / dark due to the polyfill[.]io scandal.

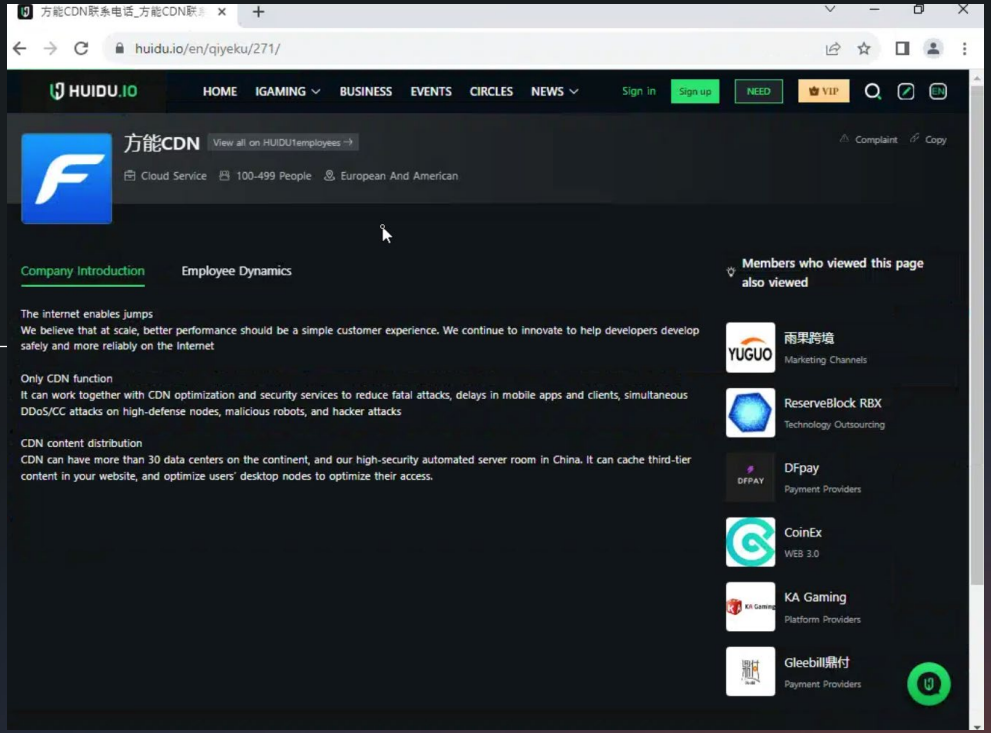
ACB Group claimed to own quite a few sports and online betting companies, along with "funnull[.]io"

爱世博 ACB GROUP

ABC Group Ownership Details

A web entry we found on HUIDU[.]io, an information hub for the online gaming industry, included a “Company Introduction” for FUNNULL CDN :

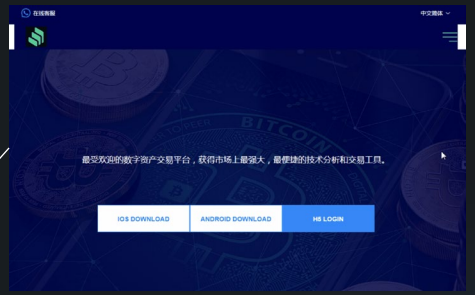
“CDN can have more than 30 data centers on the continent and **our high-security automated server room in China**.”

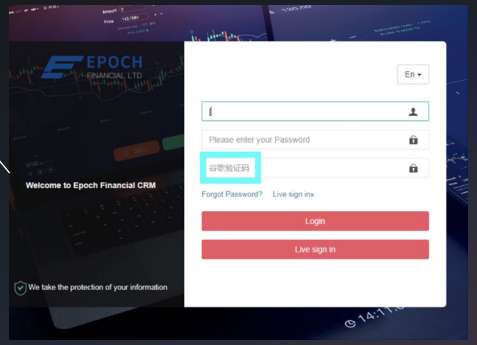


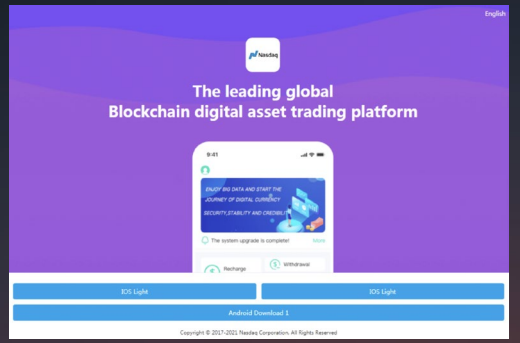
FUNNULL CDN Hosting Pig Butchering Sites for Years

In 2022, our team uncovered a large cluster of fake trading apps impersonating well-known financial organizations, including the **Australian Securities Exchange (ASX), Coinbase, CoinSmart, eToro, and Nasdaq.**

This same investigation uncovered fake financial job scams employing pig butchering techniques, with portions hosted on FUNNULL CDN infrastructure.



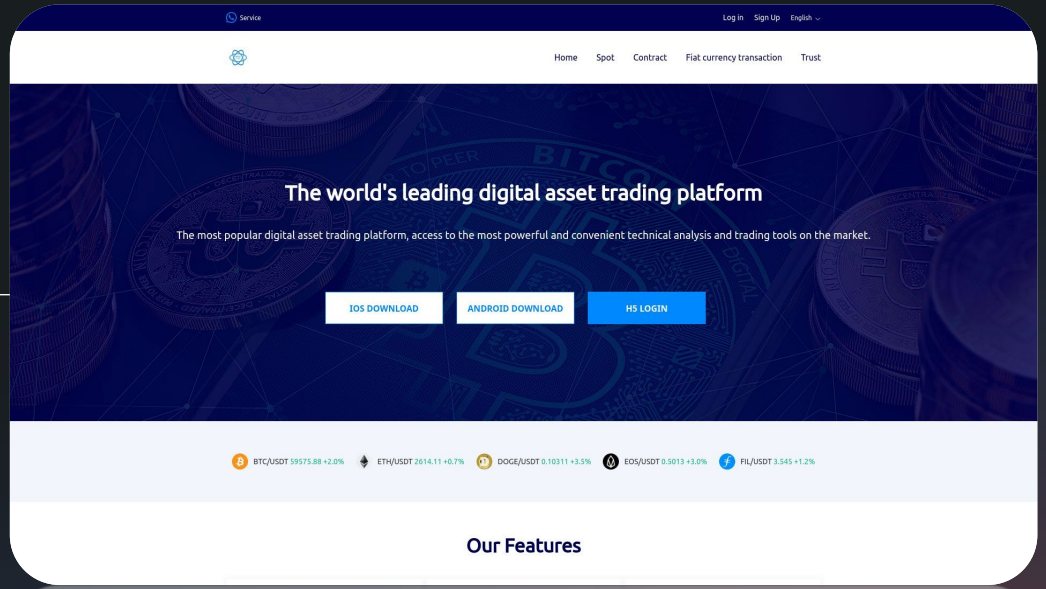




FUNNULL CDN Hosting Pig Butchering Sites for Years

At its peak in 2022, this pig butchering infrastructure on FUNNULL CDN had thousands of active domains...

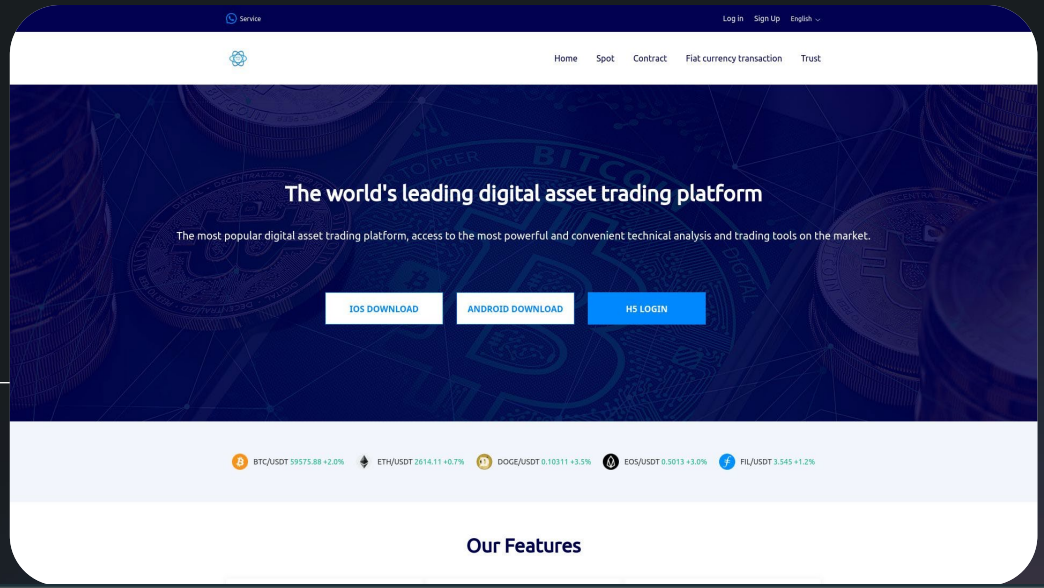
While more modest in 2024, this malicious cluster still has some active sites, including cmegrouphkpd[.]info, which hosted a fake trading platform abusing CME Group's brand and logo for the past two years.



FUNNULL CDN Hosting Pig Butchering Sites for Years

This domain cmegrouphkpd[.]info being live for 2+ years also helps to map CNAME record changes across the FUNNULL CDN.

This domain had a CNAME record pointing to *.funnull[.]vip between February and March 2022, changing to *.funnull01[.]vip between March 2022 and June 2024, and since then, switching to *.fn03[.]vip.



Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen	TTL	Type
www.cmegrouphkpd.info	-	6ce0a6db.u.fn03.vip	-	2024-06-24 00:23:42	2024-08-04 22:45:59	300	CNAME
www.cmegrouphkpd.info	-	vk6a2rmn-u.funnull01.vip	-	2022-05-20 19:05:13	2024-06-20 04:27:48	300	CNAME
www.cmegrouphkpd.info	-	vk6a2rmn-u.funnull.vip	-	2022-02-27 06:55:26	2022-05-07 09:02:13	300	CNAME

Mapping FUNNULL CNAME Chains

Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen	TTL	Type
6ce0a6db.u.fn03.vip	-	0e6de73d2.n.fnvip100.com	-	2024-03-17 11:08:08	2024-08-06 07:08:25	600	CNAME

FUNNULL maps client domains to a CNAME record like *.fn03[.]vip

The second CNAME hop is from the *.fn03[.]vip record mapped to another CNAME at *.fnvip100[.]com

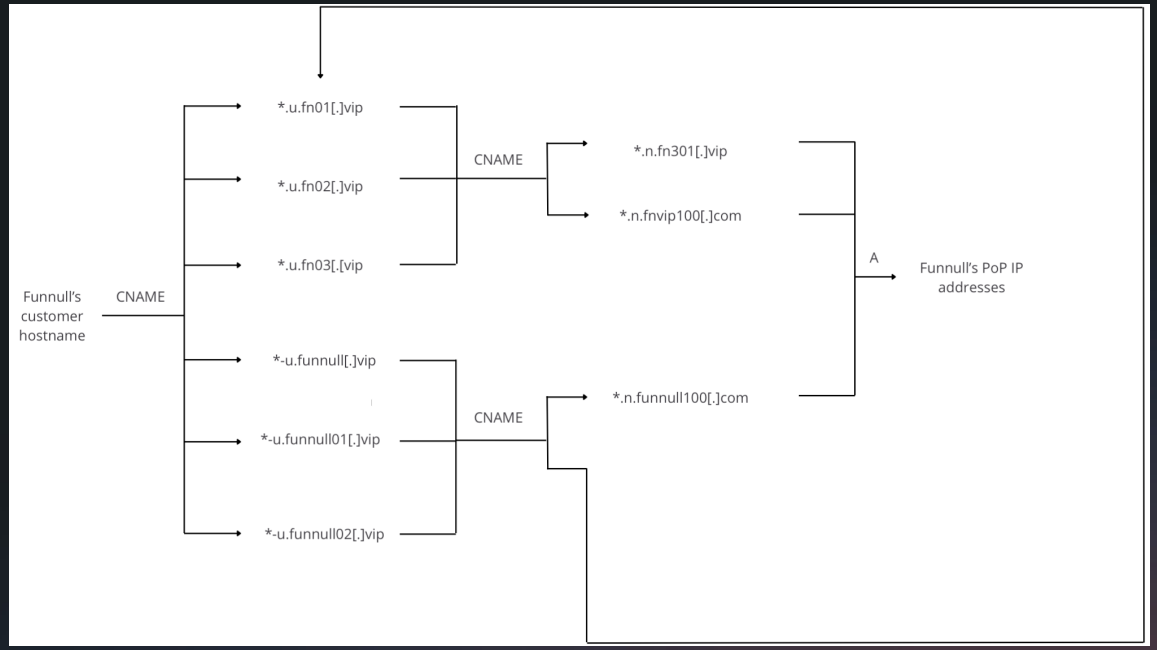
The DNS resolver follows the resolution chain and redirects to the IP address of its “Point of Presence” (PoP) with the fastest response, as seen here:

Query	Answer	Answer ASN	First Seen	Last Seen	Type
0e6de73d2.n.fnvip100.com	137.220.202.119	152194	2024-04-25 06:04:16	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	27.124.12.150	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	27.124.12.151	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	27.124.12.148	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	137.220.225.183	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	52.247.251.209	8075	2024-07-21 07:48:11	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	20.205.19.56	8075	2024-06-27 19:28:27	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	27.124.12.153	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	223.26.61.46	152194	2024-06-09 05:53:39	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	20.205.129.121	8075	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	137.220.225.81	152194	2024-06-26 09:07:54	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	27.124.12.152	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	27.124.12.149	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A

Mapping FUNNULL CNAME Chains

As a result, these CNAME chains can be used to map FUNNULL's entire customer infrastructure on its CDN and obtain the IP addresses of its PoP network.

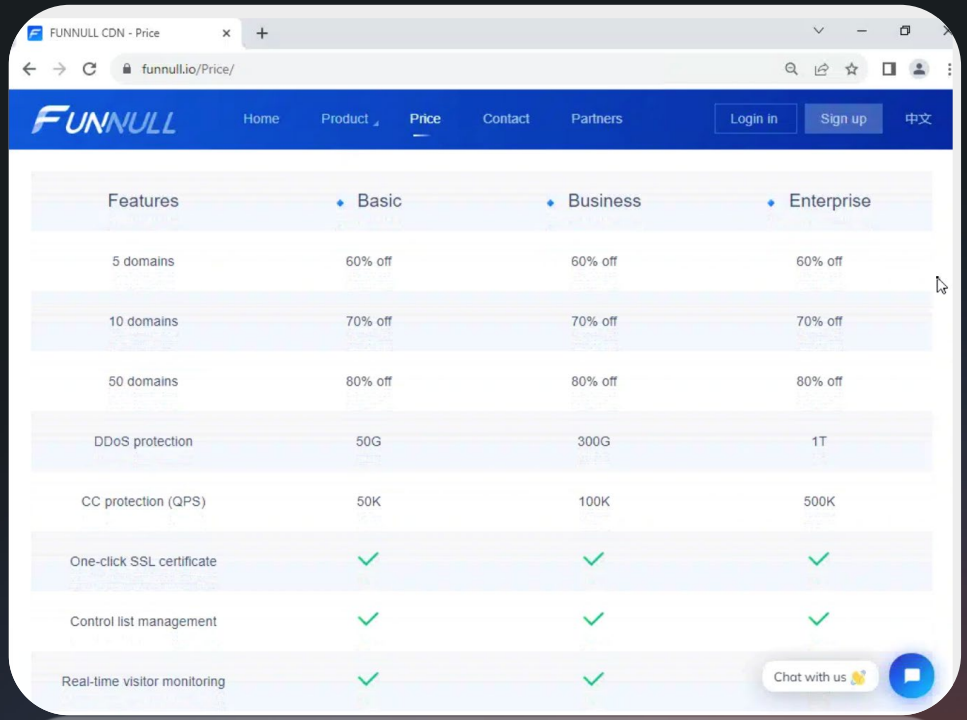
We identified over 200,000 unique hostnames being proxied through this network over the past month alone - more than 95% of the hostnames were created with DGAs - and 1.5 million reverse CNAME records lookups have been collected since 2021.



FUNNULL CDN Infrastructure Details
Bulk Domain Hosting

The FUNNULL CDN pricing page suggests a unique business model that likely only appeals to very specific types of organizations.

The pricing includes three tiers for managing a single domain, with different amounts of bandwidth per tier, yet immediately below these options are details about bulk domain management, **with 80% discounted rates for clients with 50 domains or more.**



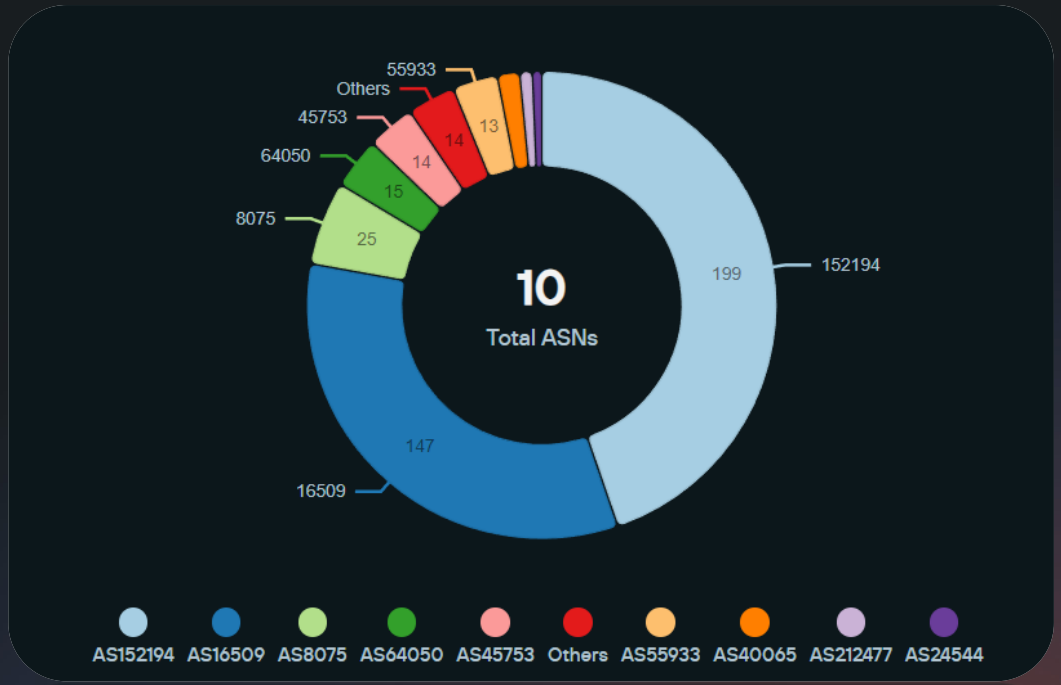
FUNNULL CDN Infrastructure Details
Consistent Error Pages

When navigating to a domain not completely configured to work with the FUNNULL CDN, an error page with a consistent theme referencing “FUNNULL” renders, which looks like this:

FUNNULL CDN Infrastructure Details
IPs from Microsoft, Amazon & Other Sources

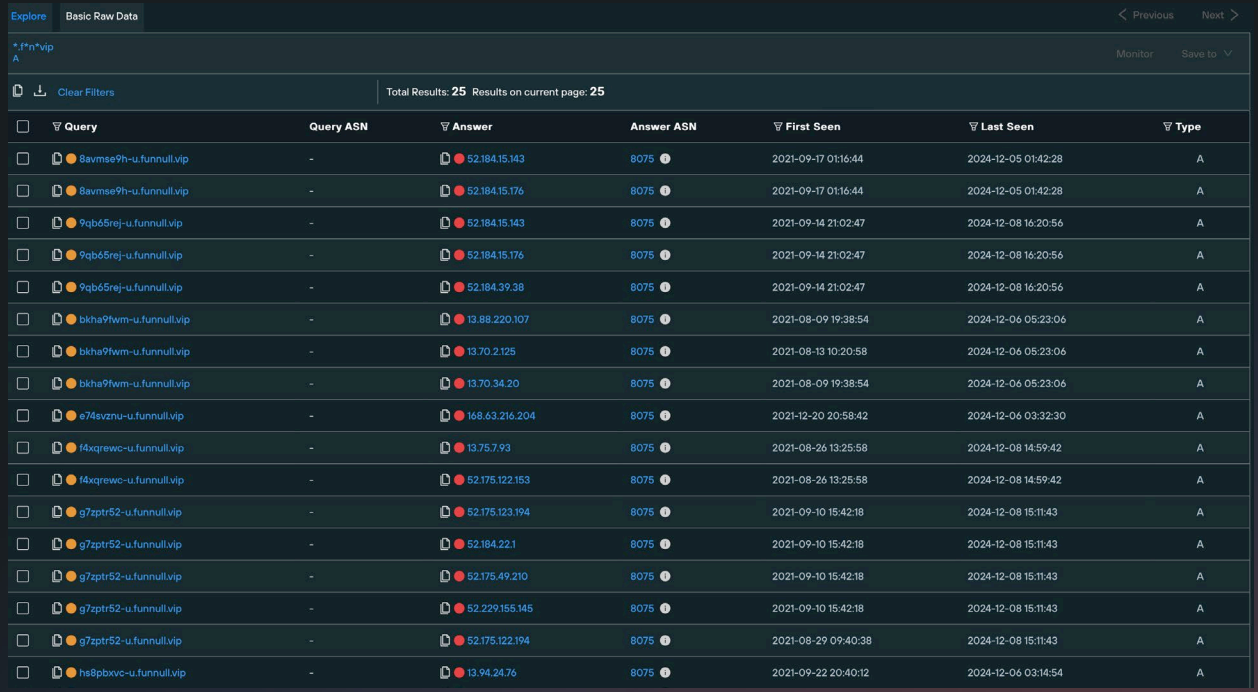
Silent Push identified close to 500 of FUNNULL's IPs active in the last week and, as expected, a large portion of these were located in Asian ASNs, such as AS152194 (China Telecom Global), AS45753(NETSEC-HK Netsec Limited), and AS55933 CLOUDIE-AS-AP Cloudie Limited, among others.

Surprisingly, we discovered that **nearly 40% of the CDN's PoPs were IP addresses** belong to AS8075 (MICROSOFT) and AS16509 (AMAZON), two major US-based cloud providers.



FUNNULL CDN Infrastructure Details
Continued…

Using Silent Push's extensive PADNS data, we confirmed that FUNNULL has been renting Microsoft's IP space and using it to accelerate its customers' infrastructure, since at least 2021.



Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen	Type
8avmse9h-u.funnull.vip	-	52.184.15.143	8075	2021-09-17 01:16:44	2024-12-05 01:42:28	A
8avmse9h-u.funnull.vip	-	52.184.15.176	8075	2021-09-17 01:16:44	2024-12-05 01:42:28	A
9qb65rej-u.funnull.vip	-	52.184.15.143	8075	2021-09-14 21:02:47	2024-12-08 16:20:56	A
9qb65rej-u.funnull.vip	-	52.184.15.176	8075	2021-09-14 21:02:47	2024-12-08 16:20:56	A
9qb65rej-u.funnull.vip	-	52.184.39.38	8075	2021-09-14 21:02:47	2024-12-08 16:20:56	A
bkha9fwm-u.funnull.vip	-	13.88.220.107	8075	2021-08-09 19:38:54	2024-12-06 05:23:06	A
bkha9fwm-u.funnull.vip	-	13.70.2.125	8075	2021-08-13 10:20:58	2024-12-06 05:23:06	A
bkha9fwm-u.funnull.vip	-	13.70.34.20	8075	2021-08-09 19:38:54	2024-12-06 05:23:06	A
e74svznu-u.funnull.vip	-	168.63.216.204	8075	2021-12-20 20:58:42	2024-12-06 03:32:30	A
f4xqrewc-u.funnull.vip	-	13.75.7.93	8075	2021-08-26 13:25:58	2024-12-08 14:59:42	A
f4xqrewc-u.funnull.vip	-	52.175.122.153	8075	2021-08-26 13:25:58	2024-12-08 14:59:42	A
g7zptr52-u.funnull.vip	-	52.175.123.194	8075	2021-09-10 15:42:18	2024-12-08 15:11:43	A
g7zptr52-u.funnull.vip	-	52.184.22.1	8075	2021-09-10 15:42:18	2024-12-08 15:11:43	A
g7zptr52-u.funnull.vip	-	52.175.49.210	8075	2021-09-10 15:42:18	2024-12-08 15:11:43	A
g7zptr52-u.funnull.vip	-	52.229.155.145	8075	2021-09-10 15:42:18	2024-12-08 15:11:43	A
g7zptr52-u.funnull.vip	-	52.175.122.194	8075	2021-08-29 09:40:38	2024-12-08 15:11:43	A
hs8pbxvc-u.funnull.vip	-	13.94.24.76	8075	2021-09-22 20:40:12	2024-12-06 03:14:54	A

FUNNULL CDN Infrastructure Details
IP Locations

Across 438 IPs in the FUNNULL CDN, the vast majority are hosted in Hong Kong, Japan and Singapore. 20 IPs are currently hosted in the U.S.

Online Gambling Sites for Money Laundering: 40,000 Questions…

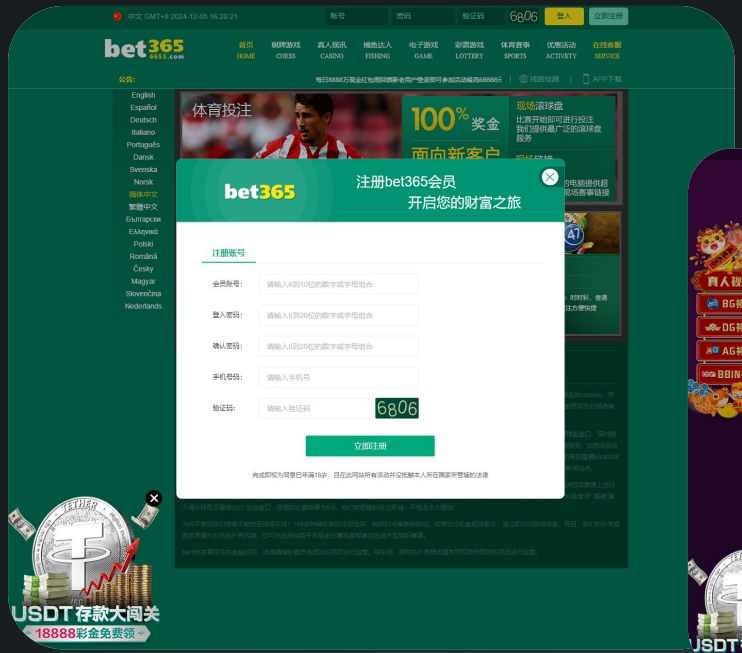
Our team found around **40,000 suspect gambling websites** hosted on FUNNULL CDN.

This is very rare to see, so our team began a deeper investigation.

The number of distinct brands hosted on this gambling infrastructure—**roughly a dozen unique brands**—was exceedingly low compared to the total number of websites.

Our team was able to parse and segment this gambling network based on the **brand favicons** being used.

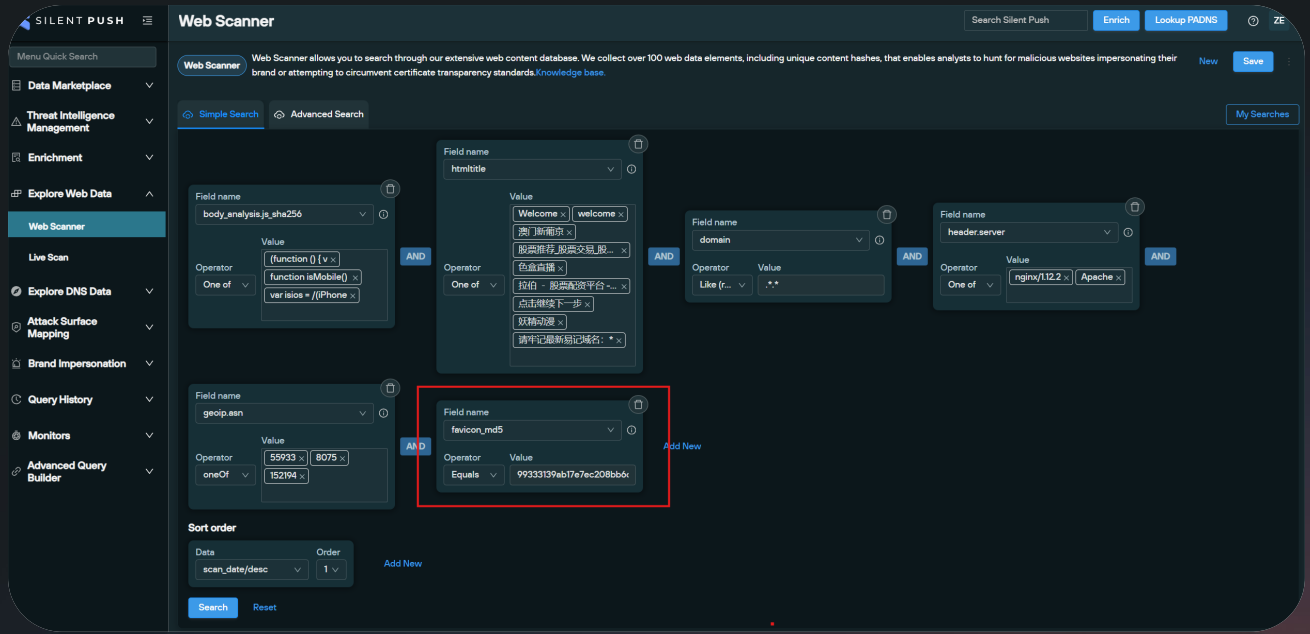
Online Gambling Sites for Money Laundering:
Suspiciously Similar Offers (Tether Lottery)



Online Gambling Sites for Money Laundering: Favicon Filtering for Brands

The online gambling sites for each brand can be found with a relatively complex query that doesn't restrict itself to a group of CNAMEs.

Instead, it uses on-content JavaScript, HTML titles, specific header.server values seen across any of three ASN ranges, and then the final brand favicon filter.

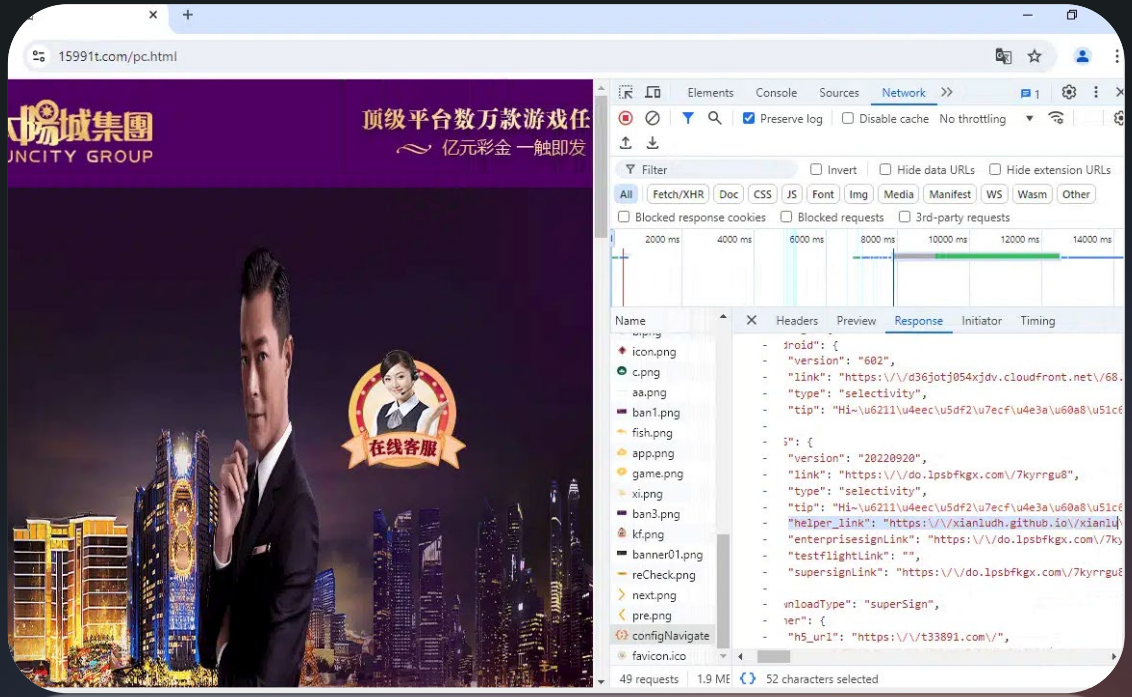


Online Gambling Sites for Money Laundering:
BWIN Confirms their Brand is being Abused

"Chris Alfred, a spokesperson for Entain, the parent company of Bwin, told TechCrunch that the company **'can confirm that this is not a domain we own so it appears the site owner is infringing on our Bwin brand so we will be taking action to resolve this.'"**

Online Gambling Sites for Money Laundering:
Source Code Connects Sites to Shared Owner

Analyzing one of the FUNNULL gambling domains 15991t[.]com also revealed an endpoint responsible for returning the configurations for that page, including a list of active mirrors as well as a GitHub account listed in the “helper_link” field, as seen here:

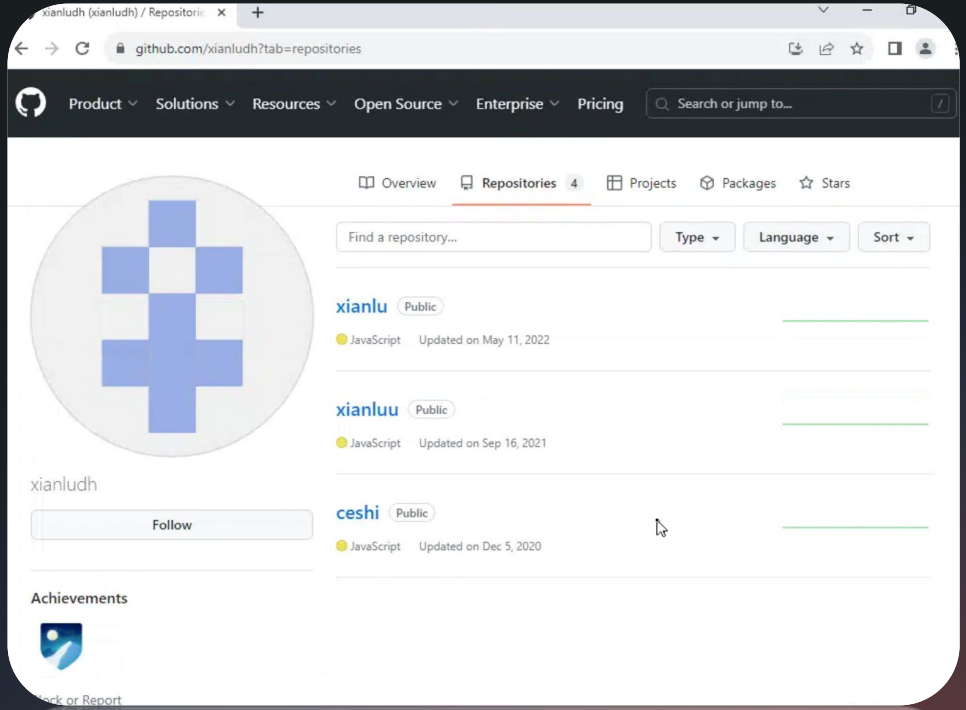


Online Gambling Sites for Money Laundering:
Source Code Connects Sites to Shared Owner

Browsing the Github account, we found three public repositories (github[.]com/xianludh?tab=repositories) containing templates used by sites hosted on FUNNULL.

The repositories contain source code for hundreds of suspect gambling applications, including the brands we had seen being proxied through FUNNULL.

This suggests they were derived from a common template or were potentially coded by the same developer.



Recruiting Money Movers (Tether + Telegram)

Our Analysts discovered that one of the pages within the “xianludh” GitHub repository had some page templates with very specific and interesting language, containing the phrase “跑分” – criminal jargon for money laundering – along with details in Mandarin about what appears to be a “money-moving[laundering]” network.

Recruiting Money Movers (Tether + Telegram)

The Github content about "money moving" was found on a live site hosted on FUNNULL – an identical copy – at aensnn[.]com.

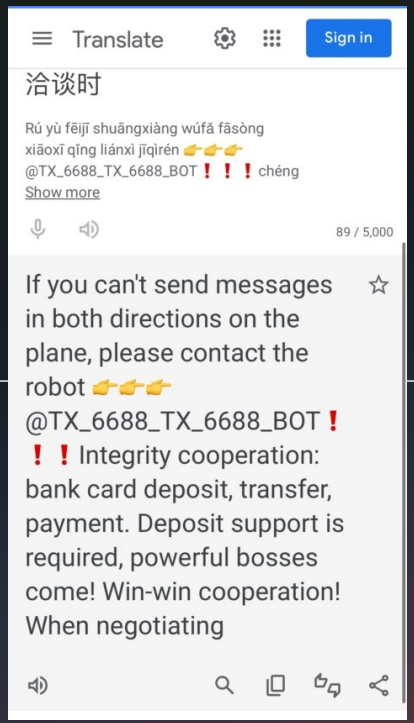
The page in the GitHub repository also included links to several live Telegram channels, as well as a Gmail address:

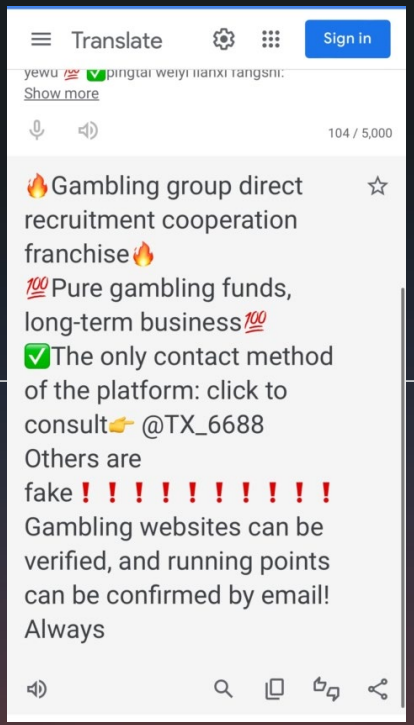
t[.]me/TX_6688
t[.]me/TX_8988
t[.]me/xxcc01
t[.]me/daivip88
t[.]me/Huawei_0
gushi083@gmail[.]com

Recruiting Money Movers (Tether + Telegram)

After accessing the Telegram links, our team roughly translated the relevant introduction messages.

This confirmed further links to the so-called “money-moving” networks:



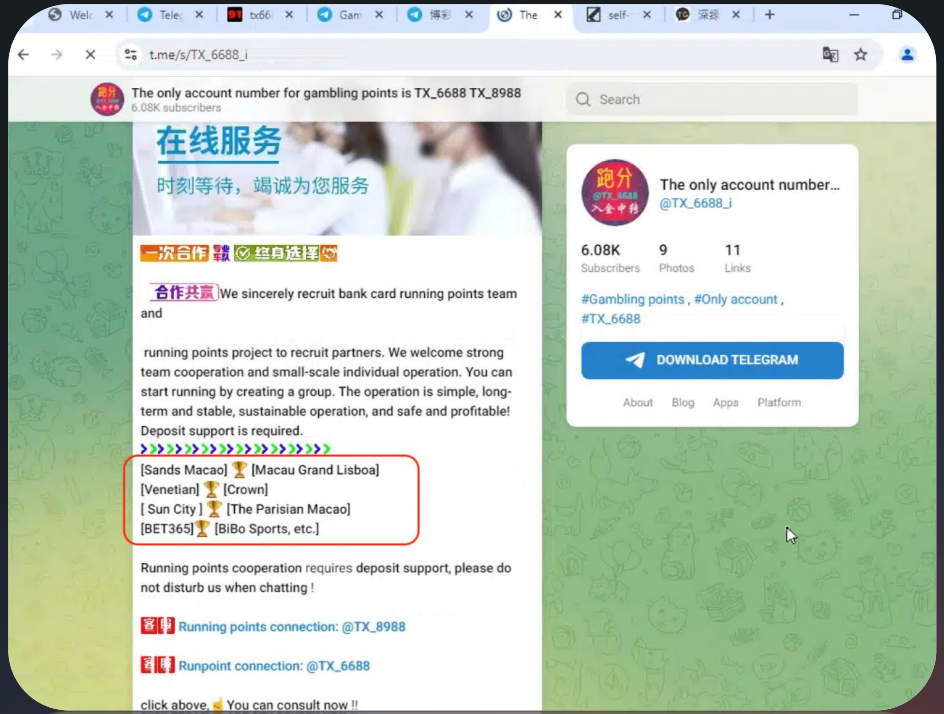


Recruiting Money Movers (Tether + Telegram)

We also found a Telegram channel (t[.]me/s/TX_6688_i) with the same profile photo and partially the same “6688” name.

This channel has public content that lists some of the brands seen on the suspect gambling websites hosted on FUNNULL.

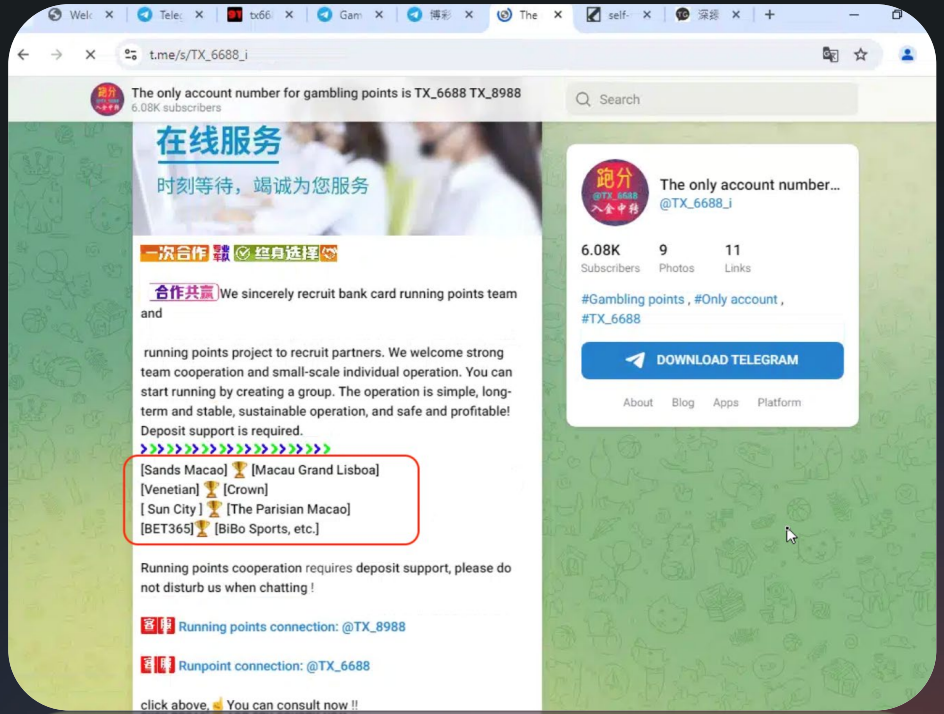
Their August 28th promo message translated into English via Google Translate highlighted 8 unique gambling brands with a message about running point schemes..



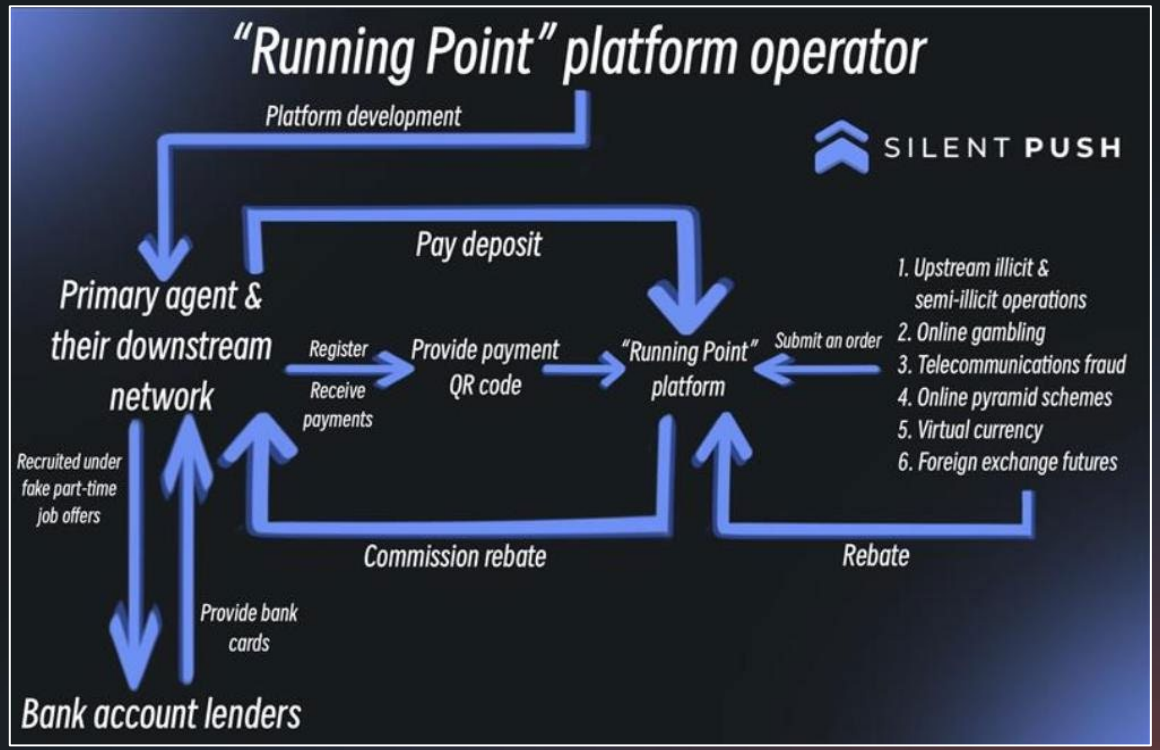
Recruiting Money Movers (Tether + Telegram)

“Cheng Zhao Bank Card Running Sub Team“
We sincerely recruit bank card running points team and running points project to recruit partners. We welcome strong team cooperation and small-scale individual operation. You can start running by creating a group. The operation is simple, long-term and stable, sustainable operation, and safe and profiable! Deposit support is required.

[Macau Jinsha] [Macau New Portuguese]
[Venetian] [Crown]
[Too sun City] [Macao Parisian]
[BET365] [Bingbo Sports, etc.]



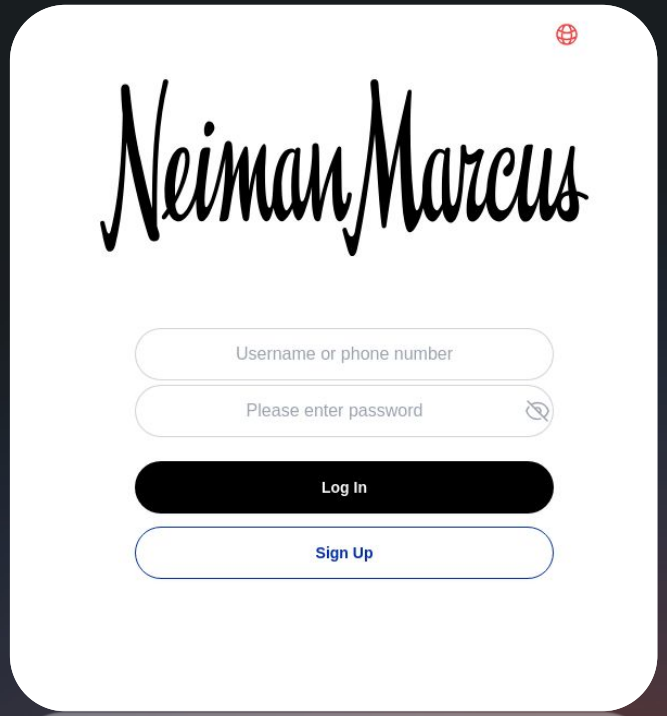
Recruiting Money Movers (Tether + Telegram)



Retail Phishing Scam on FUNNULL

While further researching sites hosted on the FUNNULL CDN, we found a large grouping of "retail phishing websites" targeting over 20 major brands:

Aldo, Asda, Bonanza, Cartier, Chanel, Coach, eBay, Etsy, Gilt Groupe, Inditex, Lotte Mart, LVMH, Macy's, Michael Kors, Neiman Marcus, OnBuy[.]com, Rakuten, Saks Fifth Avenue, Tiffany & Co., and Valentino.



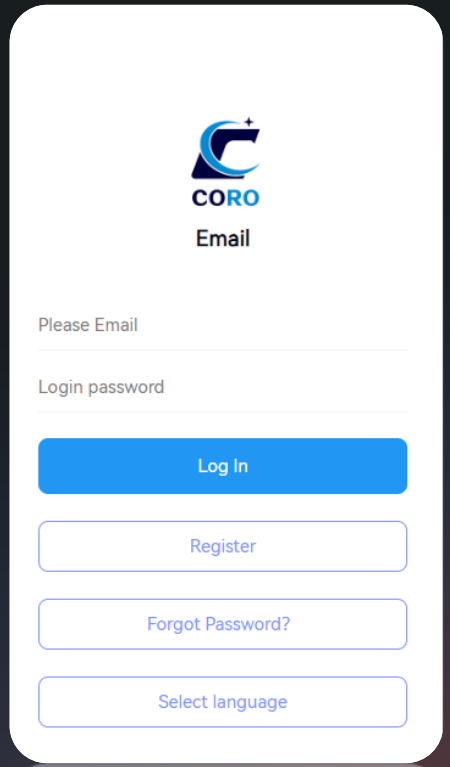
Retail Phishing Scam on FUNNULL – Shady CNAME

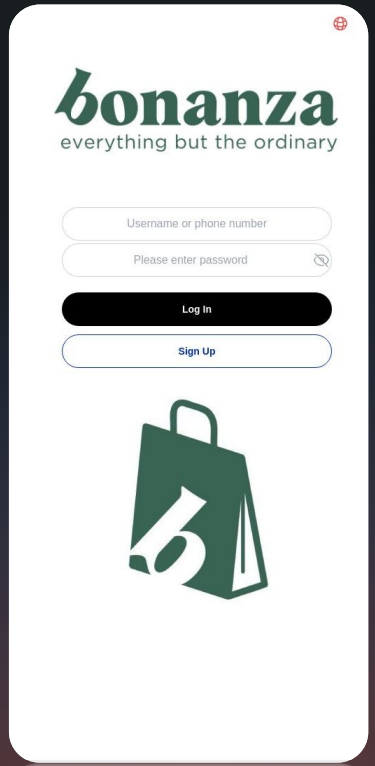
Our team discovered approximately 650 unique domains hosted on one specific FUNNULL **CNAME: 12abb97f.u.fn03[.]vip**

We soon realized that a chunk of these were pig butchering/investment phishing login pages, such as coroexchange[.]com.

Beyond the pig butchering sites, the only other websites hosted on this CNAME all appeared to be a new retail phishing campaign targeting major Western brands, with phishing login pages such as bonanza.jdfraa[.]com.

An entire CNAME dedicated to criminal phishing & pig butchering schemes.



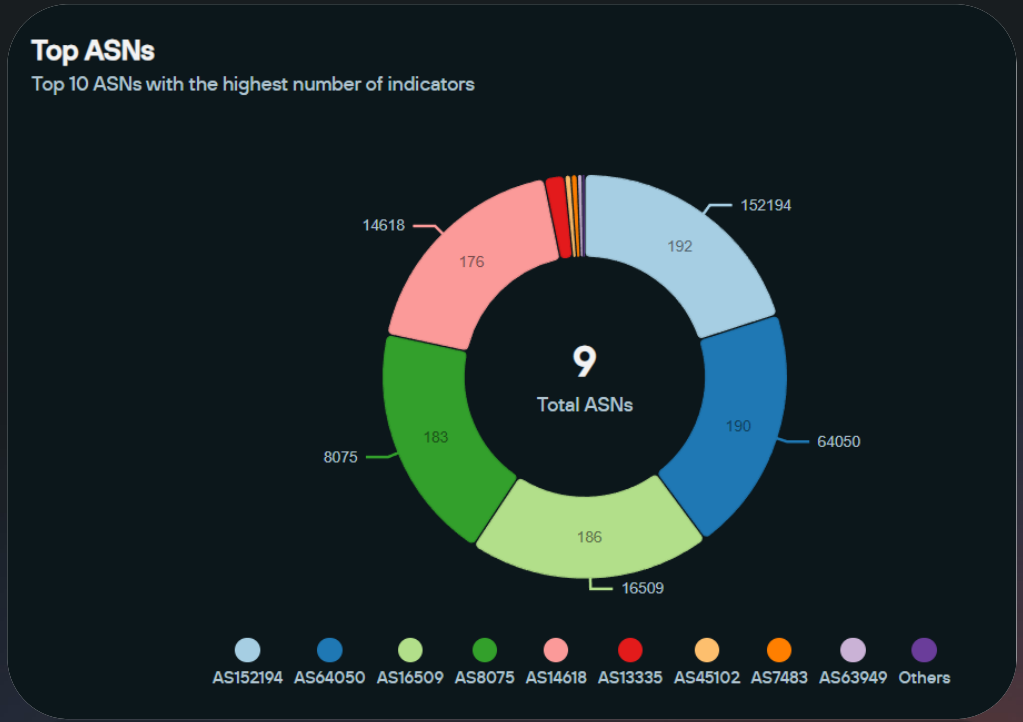


FUNNULL CDN Infrastructure Details – Retail Phishing

The retail phishing domains hosted on FUNNULL are seen across 9 ASNs

From highest to lowest density:

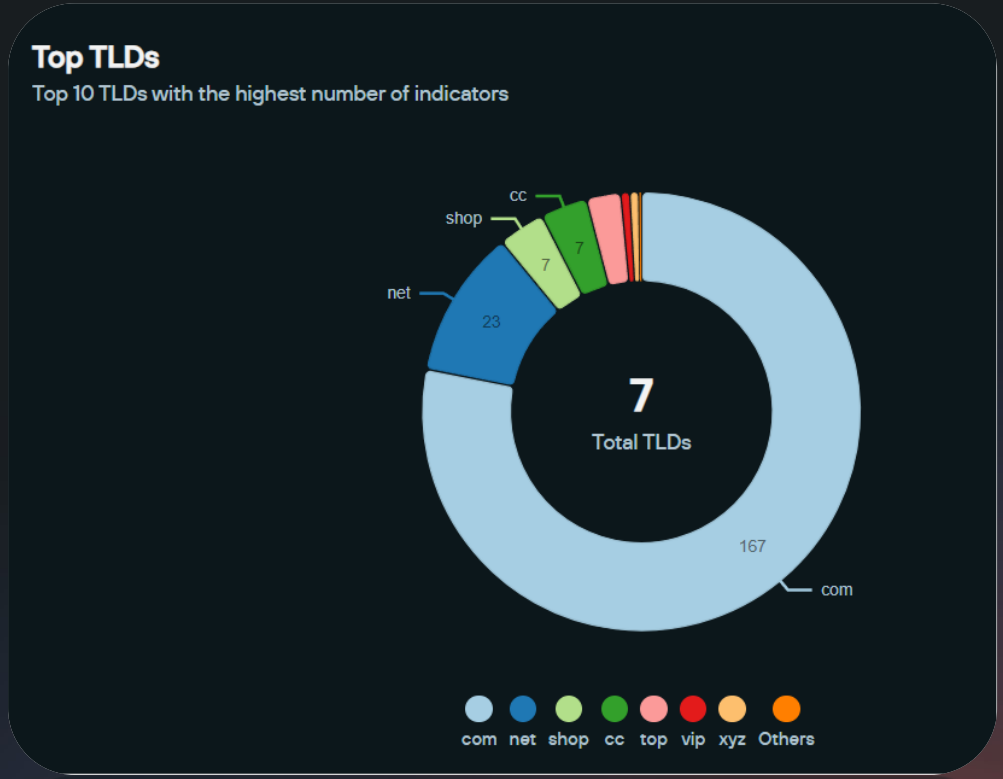
- CTGSERVERLIMITED-AS-AP CTG Server Limited, HK (152194)
- BCPL-SG BGPNET Global ASN SG (64050)
- BCPL-SG BGPNET Global ASN SG (16509)
- **MICROSOFT-CORP-MSN-AS-BLOCK US (8075)**
- **AMAZON-AES US (14618)**
- **CLOUDFLARENET US (13335)**
- ALIBABA-CN-NET Alibaba US Technology Co. Ltd. CN (45102)
- SKYCLOUD-NET Skycloud Computing co. Ltd. TW (7483)
- **Akamai (63949)**



Retail Phishing Scam

Most of the retail phishing sites are hosted on .com TLDs, but with some diversity:

- **.com - 167 sites**
- .net - 23 sites
- .cc - 7 sites
- .shop - 7 sites
- .top - 5 sites
- .xyz - 1 site
- .vip - 1 site



FUNNULL CDN Infrastructure Details – Retail Phishing

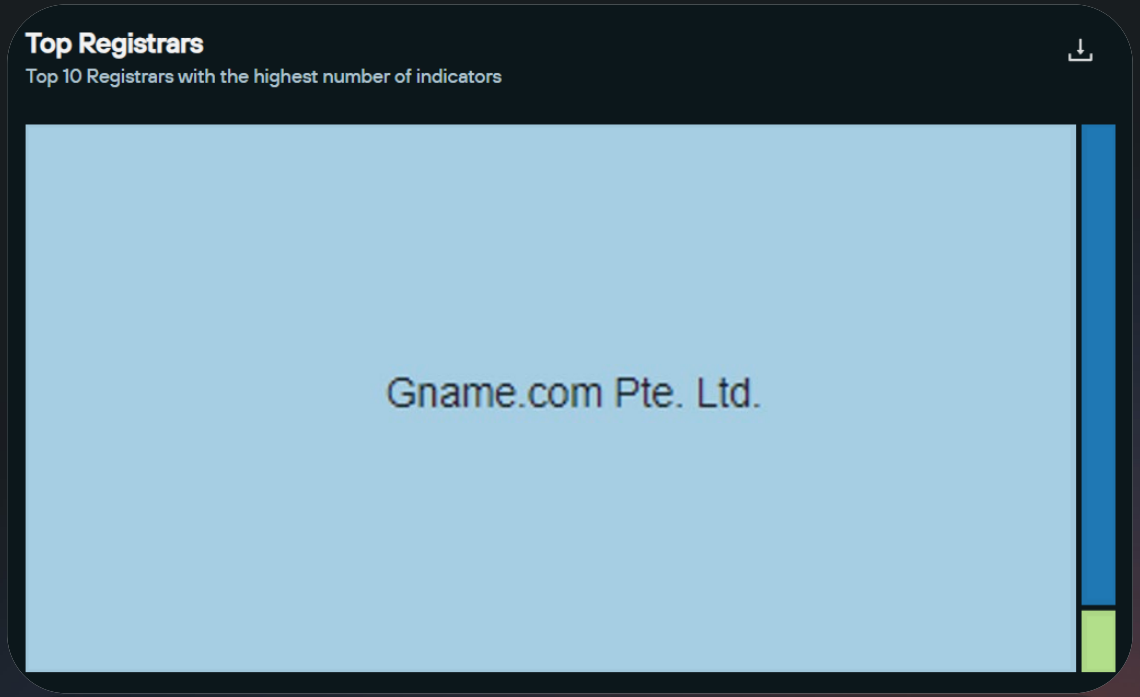
100% of the sites in the retail phishing network have Nameservers associated with "GNAME Pte. Ltd" -- gname[.]com – a registrar out of Singapore.

The records are from either "share-dns[.]com" (owned by GNAME), gname-dns[.]com, or gname[.]net

FUNNULL CDN Infrastructure Details – Retail Phishing

Nearly all sites on the retail phishing network are registered via "GNAME Pte. Ltd" -- gname[.]com – a registrar out of Singapore.

The patterns in registration, hosting & content on the sites further ties this to one threat actor group.



Summary

FUNNULL CDN – aka **Triad Nexus** -- has been hosting pig butchering scams since 2022. Essentially 100% of their clients are involved in some type of criminal scheme, with entire CNAME ranges dedicated to specific retail phishing and pig butchering efforts.

FUNNULL CDN is also hosting one of the largest networks of money mover websites on the internet, abusing the trademarks of online gambling brands. And if that wasn't bad enough, FUNNULL conducted a supply chain attack in 2024....

How can organizations work together to take down this network…?

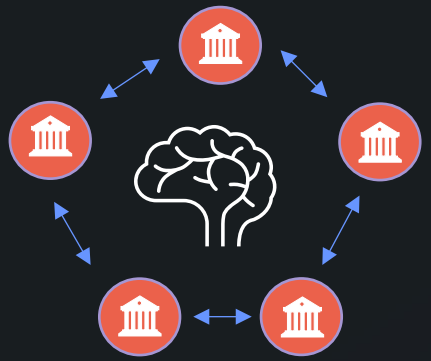
Open Questions About FUNNULL & Triad Nexus

- How much money has been lost to the FUNNULL pig butchering sites since 2022?
- Are there other CDNs where part of it is focused on acquiring illicit revenue and the other part is focused on laundering that revenue?
- How have these online gambling websites in Mandarin stayed while online abusing prominent brand names?
- How is the public being targeted with the retail phishing & pig butchering campaigns hosted on FUNNULL?
- Who is ultimately behind this massive network? How many hundreds / thousands of people are working on this illicit finance network on FUNNULL CDN?
- How can the cybersecurity industry collaborate to take down this network?

Collaboration is Key to Stopping Networks like FUNNULL

Delivers Insight *Delivers Insight*

Organization Knowledge Sharing → **Silent Push Knowledge Sharing** → **Law Enforcement**

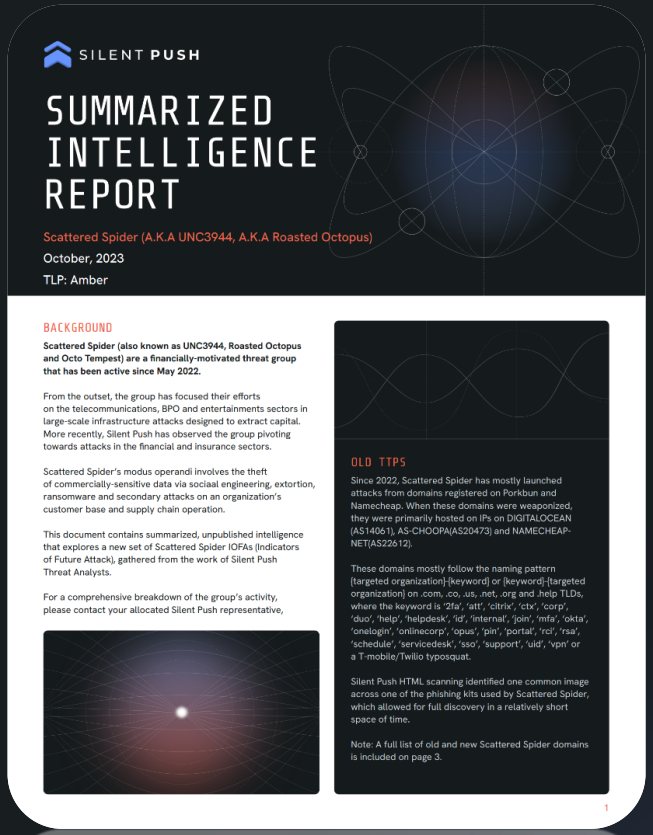


Orgs with visibility into money going into sites within the FUNNULL network should share those details with law enforcement or submit details via IC3[.]gov

SILENT PUSH

Orgs with visibility into other networks of websites conducting similar behaviors to FUNNULL would ideally share with vendors like Silent Push, to help map the architecture and detail the types of sites hosted on it.

Further share any new findings with law enforcement to have any chance of cleaning up these types of criminal financial networks.



Next Steps!

- **Register for our free Community Edition at www.silentpush.com**
- Join our socials and sign-up for research email alerts to learn about the latest findings from our Threat Analyst team
- Silent Push Enterprise Edition users have access to our TLP Amber reports with more information
- **Question about the presentation? zedwards@silentpush.com**

THANKS!