CYJAX

Turning Threats into Action
Threat Intelligence

# Fangxiao

## a Chinese Phishing Threat Actor

# Executive Summary

Phishing campaigns continue to grow more common globally, with over one million attacks observed in Q2 2022. They offer an easy and attractive way for cybercriminals to generate revenue, steal credentials and spread malware. Many sophisticated phishing kits have been developed. Some of these are sold on underground forums using a Malware-as-a-Service model, while others are used exclusively by a single threat actor group. Some cybercriminals also offer lead generation services, selling packages of clicks to fraudulent sites.

Cyjax has investigated a sophisticated, large-scale phishing campaign that exploits the reputation of international, trusted brands. It targets businesses in multiple verticals including retail, banking, travel, and energy. Promised financial or physical incentives are used to trick victims into further spreading the campaign via WhatsApp. Once victims are psychologically invested in the phish, they are redirected through a series of sites owned by advertising agencies, earning Fangxiao money. Victims end up in a wide range of suspicious destinations, from Android malware to fake gift card imposter scams.

We are tracking the threat actors behind this campaign as Fangxiao. We have assessed with high confidence that this group is based in China, and we have identified activity dating back to 2017 over more than 42,000 domains, allowing us to observe its development. Fangxiao has also exploited anxieties about world events, with some of their sites impersonating COVID-19 relief funds or posting as recruitment campaigns for deprived countries.

Fangxiao uses various strategies to stay anonymous: for example, most of their infrastructure is protected behind CloudFlare, and they rapidly change domain names. On one day in October 2022 alone, the group used over 300 new unique domains. However, during our investigation we were able to discover operational security failures and gain valuable insights about Fangxiao's operations. We have attached IOCs to this report.

# The First Fangxiao Sites

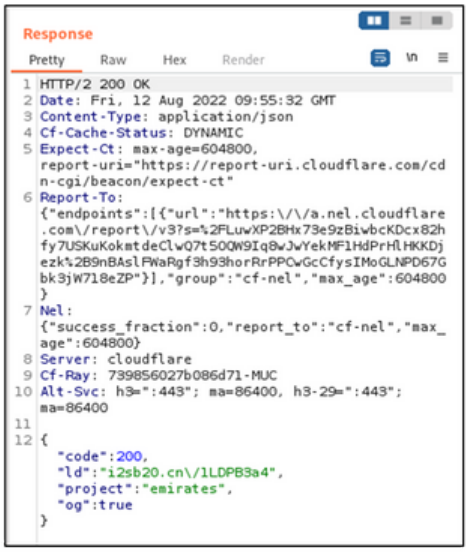


*Figure 1 - og55.php returns the fake survey URL. The 8-digit alphanumeric code returned in the URL is specific to the user's session.*

Users first interact with a series of sites controlled by the same actor. We have named this actor Fangxiao (simplified Chinese for "imitate"), after a URL parameter which often appears on sites they control.

Users arrive at a Fangxiao controlled site through a link sent in a WhatsApp message. This message has a link to a landing domain which specifies a brand to impersonate. Fangxiao uses well-known, trusted brands to build legitimacy with victims. Attempts to reach the endpoints on the root domain without specifying a brand return a 404 error.

These landing domains have followed several different naming schemes over the course of the investigation. Fangxiao has primarily appended two words from a wordlist together, using the .top TLD – for example, hxxp://chamberhike[.]top. They have also used domains with a six-character seemingly randomly generated alphanumeric code: for example, hxxp://mg7gir[.]cyou. These domains have used various registrars including Alibaba, west263, NameSilo, and Epik. All the landing and phishing domains are currently protected behind CloudFlare and are rotated extremely frequently. In one day in late October 2022, we identified over 300 brand new unique domains used by Fangxiao.

The landing domain redirects users to a main survey domain. As this changes frequently, the landing domains load a script from themselves (/j/og55.js?t=[timestamp]), shown in Figure 1. This sends a POST request to an endpoint, also located on the same site (/j/og55.php?t=[timestamp]). This returns the main survey domain – e.g., i2sb20[.]cn/1LDPB3a4/emirates/?_t=[timestamp]. This endpoint adds an 8-character alphanumeric string to the URL, to avoid enumeration of the main survey site. The generated URL expires after a period that has not been determined. Visiting it after expiry returns a 404.

Currently, most of the sites identified impersonate a wide variety of brands across multiple verticals. These include consumer goods, pharmaceuticals, food service, transport, and financial services. Over 400 organisations are currently being imitated, with that number continuing to rise. Companies affected include Emirates, Singapore's Shopee, Unilever, Indonesia's Indomie, Coca-Cola, McDonald's and Knorr. In one particularly memorable case, Fangxiao impersonates Christianity, Inc. The sites feature extensive localisation and will change the currency references as well as the pictures of the currency displayed depending on the geolocated IP address of the victim.

The fake survey site also contains a copyright statement at the bottom. The timer on the page adds to urgency and pressures victims to click through the phishing page. It has no impact on the behaviour of the page. Below the survey, the site shows victims dozens of fake comments.

Once victims have answered the survey questions and the site has "validated" their answers with an animation, they are told they can win prizes and they are asked to tap on a box. The site can require up to three taps for a "win," with usually either the second or third one telling them they have won what is usually a high value gift card. To claim this, they are told to share the phishing campaign via WhatsApp to "5 groups/20 friends". However, the button always requires thirteen taps to fill up the progress bar. Validation is done on the client side and can be bypassed by manipulating the javascript on the page.

Each session generates four unique URLs on the same domain through a call to another endpoint (/j/tb[x].php). The most common endpoint to appear is tb2.php, but we have identified endpoints that return domains at tb2.php-tb8.php, tb11.php-tb13.php, tb7.php, and tb55.php. The site then attempts to send a WhatsApp message with these URLs using the WhatsApp Custom URL Scheme.

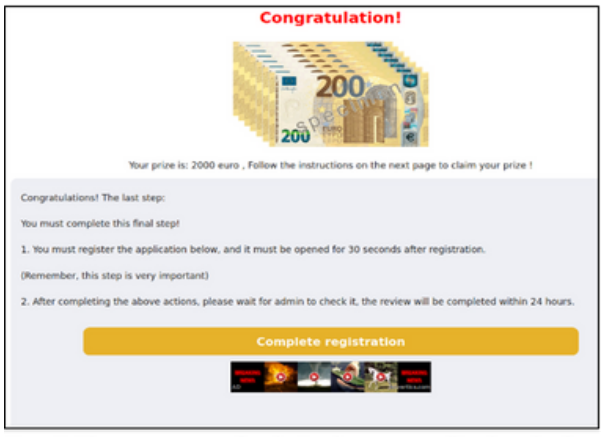


*Figure 2 - The page users see after sharing the message, telling them they have*

After the user has shared the campaign, the site directs them to click on a button (Figure 2) which will download an app. The user is asked to open this and leave it open for thirty seconds after installation. They are then told the admin will check their registration and contact them within 24 hours for their prize.

# Malicious Advertising

On the final Fangxiao-controlled page, users also see advertising (Figure 3). The site loads ads from two domains, ebaaa.xyz and qoaaa.com. The page also loads an advertisement for an advertising company, ylliX, from uprimp.com. The site does not display this image. Advertica, the company mentioned in the bottom right of the image, bills themselves as an “international online advertising company” which controls ylliX.

Online reviews for ylliX are negative, with users complaining that Google and Facebook have marked their websites as suspicious. Clicking on these ads redirects users through multiple domains in quick succession. The redirect destination depends on both the location and user-agent of the browser. There is currently no evidence that Fangxiao has control over the domains seen during these redirect chains. We investigated the types of redirects that were observed; some typical examples are included below. However, these are not exhaustive and likely change frequently as different organisations and actors buy advertising slots.

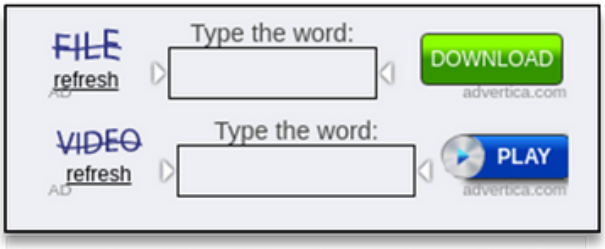


*Figure 3 - Advertising located on the final Fangxiao controlled page*

On the final Fangxiao-controlled page, users also see advertising (Figure 3). The site loads ads from two domains, ebaaa.xyz and qoaaa.com. The page also loads an advertisement for an advertising company, ylliX, from uprimp.com.

The site does not display this image. Advertica, the company mentioned in the bottom right of the image, bills themselves as an “international online advertising company” which controls ylliX.

Online reviews for ylliX are negative, with users complaining that Google and Facebook have marked their websites as suspicious. Clicking on these ads redirects users through multiple domains in quick succession. The redirect destination depends on both the location and user-agent of the browser. There is currently no evidence that Fangxiao has control over the domains seen during these redirect chains. We investigated the types of redirects that were observed; some typical examples are included below. However, these are not exhaustive and likely change frequently as different organisations and actors buy advertising slots.

With a UK IP and Android user-agent, we were redirected through several domains (Figure 4) before being served a malicious APK. Virustotal detects this file (MD5: b50ac5bbf505d3074ae55c520cc86774) as Triada, an Android trojan.

With a UK IP and iOS user-agent, the site redirected to an Amazon affiliate link (Figure 5). This allows whoever controlled the final redirect to take a commission from every Amazon purchase using the same device for the next 24 hours, potentially a major source of profit. The referral identifier used (mntzr-20) has been reported to Amazon.

With a Swiss IP and Internet Explorer user-agent, the site redirected to a SMS micropayment scam hosted on c001rsgm[.]com (Figure 6). Users are then told to click a button or scan a QR code which sends a SMS message to a list of twenty international numbers, which changes on each call to the endpoint. Text at the bottom of the page (in grey on a slightly lighter grey background) warns users they will be charged for these messages. The site also contains code that places this text just outside of the size of the user's browser and so the user must scroll to view it.

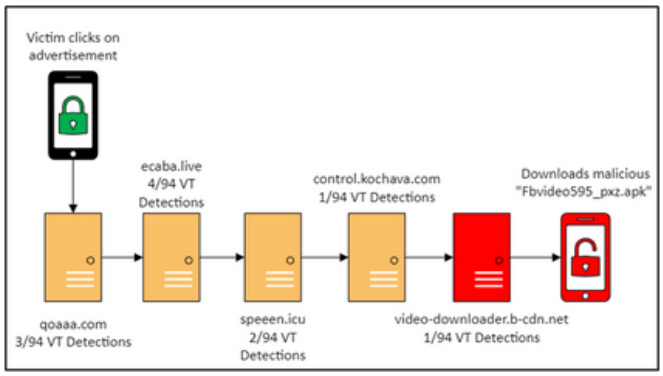


*Figure 4 - The redirect chain to a malicious APK*

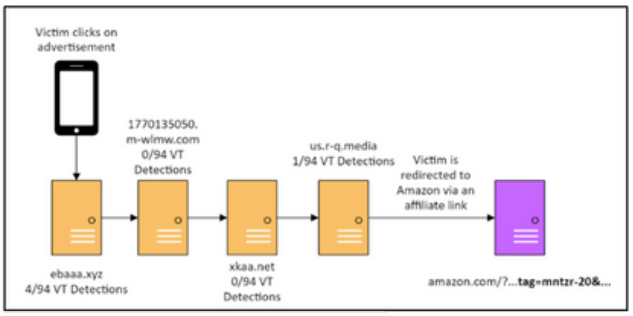


*Figure 5 - The redirect chain to Amazon*

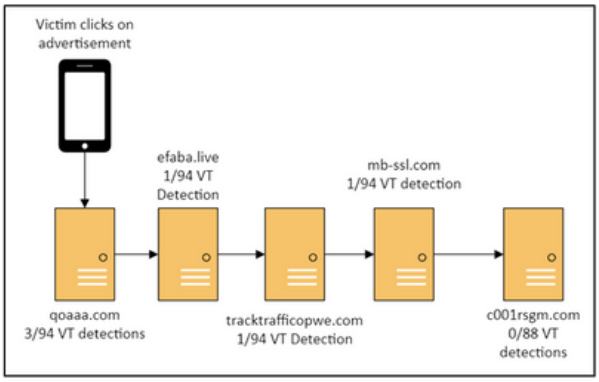


*Figure 6 - The redirect chain to the SMS micropayment scam*

# Lead Generation

Clicking on the “Complete registration” button calls another endpoint on the survey domain (/burl/index.php) with several parameters (type, _f=[brand], and _p).

This endpoint has historically redirected through a domain, getprize[.]club. Although the site remains hosted on 5.8.47.109:443 as of mid-August 2020, it is no longer available to most users due to DNS issues. Visiting the homepage of getprize[.]club returns a basic HTML document saying the site is “under construction.” In most cases, the site serves as one hop in a complex redirect chain.

For example, one of the sites that we were redirected to was a phishing site pretending to offer a supermarket voucher (hosted on portalpromotion.com) in return for personal details.

Since the fall of getprize[.]club, the endpoint has started redirecting victims through qoaaa[.]com, the site linked to via the ylliX ads. Although visiting qoaaa[.]com directly results in a 404 and blank page, DomainTools has its title saved as “Welcome to Affilist” (Figure 7). Affilist is an affiliate marketing company owned by Advertica, the company which owns ylliX.

A click on the “Complete registration” button with an Android user-agent will sometimes result in a download of the previously mentioned Triada malware. As victims are invested in the scam, keen to get their “reward”, and the site tells them to download the app, this has likely resulted in a significant number of infections.


*Figure 7 - The title of qoaaa.com according to DomainTools*

Another observed destination of this campaign is an app on the play store called “App Booster Lite - RAM Booster” with over a million downloads.

It asks for highly intrusive permissions and is full of ads, with every tap on screen resulting in a hard-to-close popup ad.

The app’s developer is called Locomind. The app is not available on the iOS app store. Their website, hxxp://locomind[.]net, is hosted on an IP (157.90.113.238) belonging to Hetzner Online GmbH, a German data center operator. This IP hosts fifteen other domains, most of which are adult sites such as hxxp://bigo-sext[.]com and hxxp://bigosext[.]com.

| Sites on 157.90.113.238 |
| --- |
| bigo-sext.com |
| bigosext.com |
| fidelityemail.com |
| fuck-out.com |
| fuckk-me.com |
| fuckk.me |
| fuckkme.com |
| fuckout.me |
| fuckt-me.com |
| fuckt.me |
| fucktme.com |
| holacode.io |
| krakenmare.io |
| locomind.net |
| luckykraken.com |

The shared IP between locomind[.]net and bigo-sext[.]com allows us to potentially deanonymize a few of the sites and calls into question the legitimacy of Locomind.

The IP also hosts another app development agency, Holacode. Their products include a similar phone cleaner app with over five million downloads, and a "spam shield" app with over 10,000 downloads. This app claims to "set you free from plenty fake and scam push notifications" and requests permission to manage and read all notifications on the victim's phone.

We have conducted preliminary static and dynamic analysis of the apps, analysing both, the currently available version and previous archived version from earlier in development. Across the apps we were able to discover the use of thirty-one different advertisement providers, each having varying degrees of trustworthiness; one provider includes IronSource which has had historic ties to malware. The comment section for each app on the Play Store shows hundreds of negative user experiences, with many suggesting fraudulent or questionable behaviour by the app (Figure 8).

Through analysis of the apps, we have determined that these utility applications are adware, but overall likely benign.

TLS certificate transparency records from crt.sh show several times when the bigosext[.]com, bigo-sext[.]com, and holacode[.]io certificates were renewed within minutes of each other.
The bigo-sext[.]com and bigosext[.]com sites are identical copies of each other. Both have a button that users are asked to click, which links to an offline site, pleasurefindyouhere[.]life.
Another one of the sites on the Hetzner IP is matchlab[.]me, a dating app developer whose apps on the Google Play store have large numbers of negative reviews calling them scams.

| TLS Certificate Renewal Overlaps | |
|---|---|
| **21/03/2022** | |
| 05**:56** | holacode.io |
| 05:**58** | bigosext.com |
| **21/05/2022** | |
| 06:**32** | bigosext.com |
| 06:**34** | holacode.io |
| 06:**35** | bigo-sext.com |
| 06:**35** | bigosext.com |
| 06:**36** | holacode.io |
| **20/07/2022** | |
| 05:**37** | bigo-sext.com |
| 05:**37** | bigosext.com |
| 05:**39** | holacode.io |
| 05:**39** | bigo-sext.com |
| 05:**40** | bigosext.com |
| 05:**41** | holacode.io |

There are also several lead generation and advertising agencies hosted on the same IP. As there are only a limited number of domains historically tied to this IP, it could be indicative that these domains are paid for by the same person, as opposed to being a shared gateway IP for completely unrelated sites. Two of these (luckykraken[.]com and krakenmare[.]io) have identical homepages with only the logos changed. Their websites claim that they provide increased user traffic and ad revenue to apps which sign up for their services. Clients of theirs can pay for clicks through to their sites.

Group 449, Grouped objectCertificate transparency data further shows links between these sites. The Let's Encrypt certificate for Holacode's mail server (Figure 9) shows that the app developers and lead generation agencies share a mail server with several other sites of interest. One of these is matchlab.me, a dating app developer whose apps receive negative reviews on the Play Store. Another domain on this certificate, adtraffico.com, is another lead generation agency, while a different site with this shared certificate, nftsco.in, is the site for an abandoned NFT project.

```
X509v3 Subject Alternative Name:
    DNS:mail.adtraffico.com
    DNS:mail.apperito.com
    DNS:mail.fidelityemail.com
    DNS:mail.holaco.de
    DNS:mail.holacode.io
    DNS:mail.holacode.tech
    DNS:mail.iconeyes.shop
    DNS:mail.italycoffee.shop
    DNS:mail.krakenmare.io
    DNS:mail.locandaitalia.shop
    DNS:mail.locomind.net
    DNS:mail.luckykraken.com
    DNS:mail.mailgun.fun
    DNS:mail.matchlab.me
    DNS:mail.nftsco.in
    DNS:mail.sendgrid.rest
```

*Figure 9 - Certificate Transparency Logs*

# Lateral Identification

Fangxiao has used over 24,000 landing and survey domains since the start of March 2022. They are currently using two Google Tag Manager codes (G-LW7434MYMN and G-5MMGBZGY1Q) which they have reused across thousands of their domains, allowing identification of other Fangxiao-controlled domains. The G-LW7434MYMN tag was first observed on urlscan.io 7 months ago. Searching for it leads to a previous report on Fangxiao by the CyberPeace foundation containing two new tags (G-GCJBWXZBX3, G-0C230YDF7G). Further pivoting through these tags identified a list of 33 Google Tags used by Fangxiao-controlled sites.

The threat actors have used subdomains targeted to specific brands, for example targeting the cryptocurrency firm Metamask using the URL metamask-io.quickdiate.com. Unfortunately, at time of identification this website was down, and we could not further analyse this site.

# The development of Fangxiao sites over time

URLScan provides a powerful capability to pivot through records with filenames. While analysing Fangxiao-controlled sites, we saw that they consistently loaded a script called "yuming.js." Yuming (域名) is the simplified Chinese for "domain name." Pivoting on this indicator through URLScan.io allowed us to locate and download approximately 46,000 unique scans which referenced over 13,600 unique domains, dating back to 2019.

One site found this way, recruitment.totalenergie.govservice[.]site, poses as a fake Total Energy recruitment campaign targeting Nigerians. Notably, this site has a user counter from supercounters.com, a website visitor tracking tool. This showed a peak of 303 visits on 4 August 2022 (Figure 10), with most users accessing the site from an Android smartphone (Figure 11).

Another fake job site, job4you[.]live, is targeted at South Africans and offers 10,000 jobs. The promise of jobs in countries with significant unemployment rates provides a powerful psychological incentive to trick users.


*Figure 10 - The fake recruitment site had over 1,000 visits*

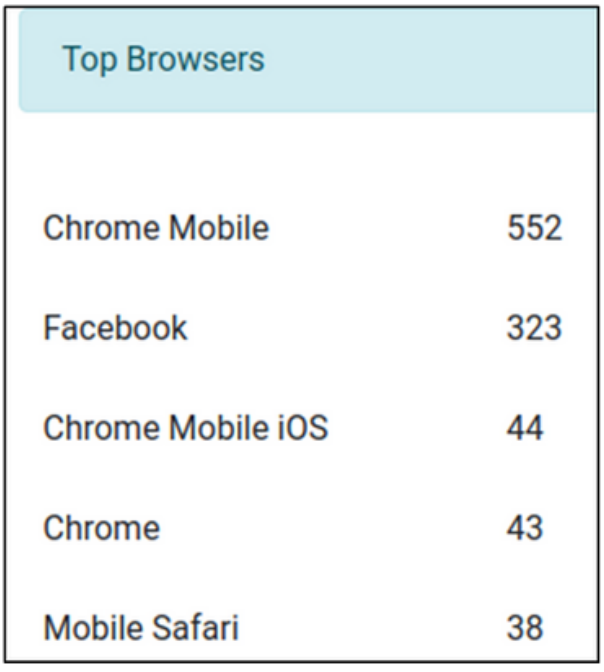


*Figure 11 - Most visitors to the site were on mobile*

Fangxiao has also taken advantage of global events such as the COVID-19 pandemic, hosting fake surveys for COVID relief funds (for example, on covid19.relief-fund[.]live). Some of the earliest scanned Fangxiao sites offered users free “WhatsApp Data” or additional data allowances for their internet contracts, as well as free laptops for those in need.

The gamification of the survey sites has also changed with time. A 2020 URLScan of vipwhatsapp[.]xyz shows a Fangxiao site containing a slot-machine style spinning game. The group has clearly spent a significant amount of time on developing and optimising their scam sites (Figure 12).

We continued to investigate URLScan data and found several other potential Fangxiao sites dating back to 2017; for example, a site offering users a free iPhone 7. The large amount of data available on URLScan means we were unable to investigate every lead. There may potentially be earlier Fangxiao sites that we have currently not identified.

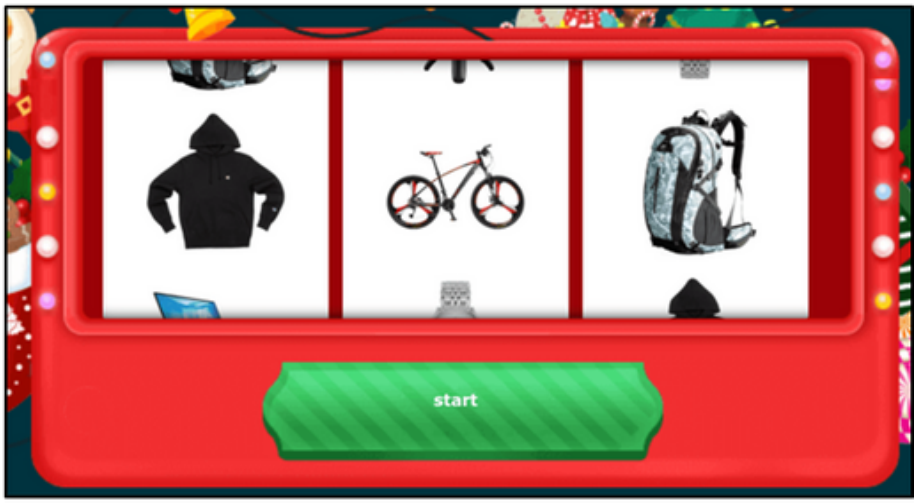


*Figure 12 - An old Fangxiao site featuring a different form of gamification*

# Widening the scope!

When redirecting through getprize[.]club, the fake survey sites set several URL parameters. We identified that without URL parameters, getprize[.]club displays a single piece of text stating “under construction”. When given the URL parameter set during the scam site redirect (/?u=r1lpd0d), getprize acts as a redirect domain.
However, with any change in URL parameter, getprize.club serves one of a series of explicit fake dating sites (Figure 13). These new fake surveys ask victims four benign questions (like the original Fangxiao survey sites). They are redirected via getprize[.]club/web/ to one of a series of fake dating sites. A list of fake sites is attached. The sites are run by several shell companies based in Cyprus, Bulgaria, Liechtenstein, Slovakis and Jamaica. A site registered in Slovakia (uberhookups[.]com) has T&Cs which state it is under Cypriot legal jurisdiction. This, as well as the redirects between them and significant structural overlap, suggests that the same actor runs the Cypriot and Slovak sites.

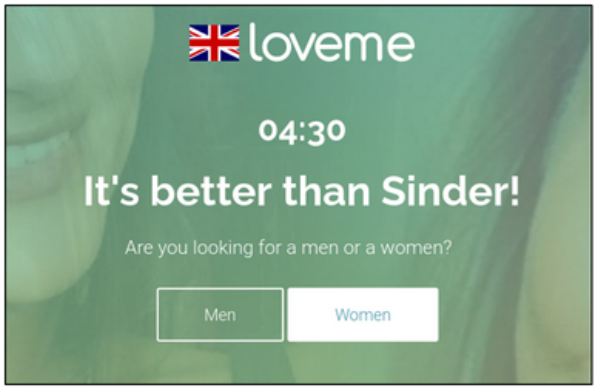


*Figure 13 - One of the pages shown on getprize.club*

The fake sites are full of bots and frequently nudge users for payment to unlock more features, with the promise of meeting someone for sex. One observed redirect chain sent analysts to bigosext1[.]com and displayed branding for a fake dating site called SpookChat. Another redirect chain from getprize[.]club sent users to mylocaldates1s.com.

This allowed us to link the Hetzner-run infrastructure on 157.90.113.238 to the actors behind getprize[.]club. Fuckt[.]me, a site on the Hetzner IP, contained a button which users were asked to click. This redirected them through hotpoint-ladies[.]com to mylocaldates1s.com.

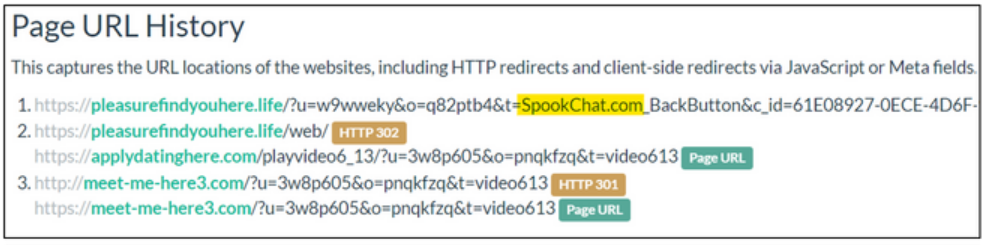


*Figure 14 - The Redirect Chain*

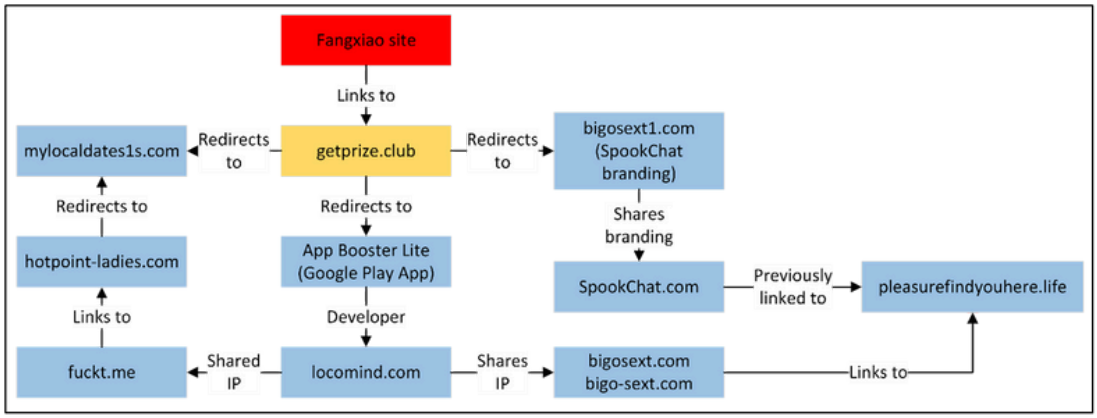


*Figure 15 - The complex web of links between the sites*

The two bigosext sites (bigosext[.]com and bigo-sext[.]com) are both identical to fuckt.me except for the link, which redirects to pleasurefindyouhere[.]life. This site is unfortunately now down. However, a search on URLScan revealed a February 27 2021 scan showing a pleasurefindyouhere[.]life URL containing a referrer from SpookChat.com (Figure 14).

The redirects, referrers and similar naming schemes make it highly likely that bigosext[.]com, bigo-sext[.]com, and bigosext1[.]com are run by the same threat actors. It is likely that fuckt[.]me (and any of the handful of other sites with similar naming on the Hetzner IP) are linked to the actors behind getprize[.]club. The shared /web/ endpoint suggests that getprize.club and pleasurefindyouhere.life run the same backend software. These links are shown in Figure 15.

The website for one of the apps Holacode develop, totalcleanerapp[.]com, is registered to a Russian email address (whitemore.h[at]mail.ru). This same address was used to register a site called tdsjsext[.]com. Tdsjsext is visually identical to getprize.club and so it is highly likely that getprize.club, totalcleanerapp.com (and therefore Holacode), and the fake dating sites are run by the same actors.

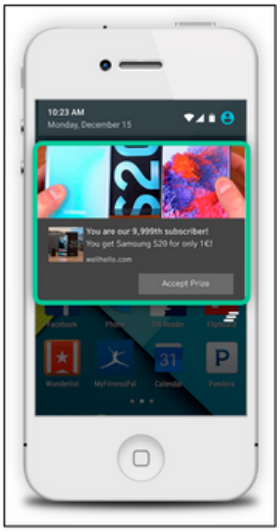

*Figure 16 - An example ad from the Moartraffic site*

Further investigation of the bigosext sites revealed a new domain – go.moartraffic[.]com. Moartraffic is a lead generation and advertising agency. The case studies on their websites show significant links between Moartraffic and several of the redirected-to sites. For example, wellhello[.]com is a fake dating site run by Morganite Ltd, a Cypriot shell company registered at the address of the "Boutique Management Consultancy" WBG Cyprus. A screenshot on the Moartraffic site shows a push notification ad served from wellhello (Figure 16). An inventory on their site (moartraffic[.]com/inventory, Figure 17) shows a list of different ad types with their pricings. There are three separate site types available for purchase – "internal dating network," "wellhello", and "external partners network".

| Site | Zone type | Zone | Size | Daily Avg Volume | Rate | Dating on dating rate |
|---|---|---|---|---|---|---|
| Internal Dating Network | Banner | Paid Mobile Header ENG | 300x50 | 1000 imps | $22.00 | $35.00 |
| Internal Dating Network | Banner | Paid Mobile Footer ENG | 300x250 | 2000 imps | $13.00 | $36.00 |
| Internal Dating Network | Banner | Free Mobile Header ENG | 300x50 | 3000 imps | $16.00 | $34.00 |
| Internal Dating Network | Banner | Free Mobile Footer ENG | 300x250 | 4000 imps | $13.00 | $29.00 |

*Figure 17 - The price list on the moartraffic site*

# Threat Actor attribution

We have considered various patterns of behaviour, OPSEC slip ups and metadata which suggest with a high likelihood that Fangxiao is a China-based threat actor.


*Figure 16 - The control panel on one of the Fangxiao sites*

The initial survey sites share a favicon of a heart on a white background. We searched the hash of the favicon (-1396821592) on Shodan to deanonymize some of the domains, finding IPs and allowing us to bypass some of Cloudflare's restrictions. Using this we identified a web service running on 35.195.98.72:8888 (Figure 18). This IP had hosted whatsappos[.]com, a Fangxiao site which had been online since at least 2020. Browsing to this service showed us a page written in Mandarin.

Further analysis of this page reveals it is a default page belonging to aaPanel, an open-source hosting control panel which allows quick deployment of many websites. The page being in Chinese further supports the hypothesis that Fangxiao is a China-based threat actor.

Although the landing domains frequently do not use TLS, the survey domains do. Fangxiao uses Let's Encrypt TLS certificates. Let's Encrypt backdates the Not Before time by an hour, and so by adding an hour to the timestamp on the certificate we can find when it was issued. We downloaded certificate data and identified 433 unique certificates from 2021-22 (Fig 19). In 2021, most certificate registrations were conducted at 01:00Z and were likely automated. In 2022, there was far more variability in the times that SSL certificates were valid from (Fig 20).

If these times are converted to GMT+8 (China Standard Time), the registration pattern matches with waking hours of 9am to 11pm, bar a few outliers. This is further compelling evidence that Fangxiao is a Chinese threat actor.

Further analysis of the group's TLS certificates showed that the operators worked more during the late night/early morning in 2020 than in 2021 (Fig 20). This dataset is not representative of all Fangxiao behaviour but still provides an interesting insight into the actions of the group and helps further back up the idea that this is a Chinese threat actor.

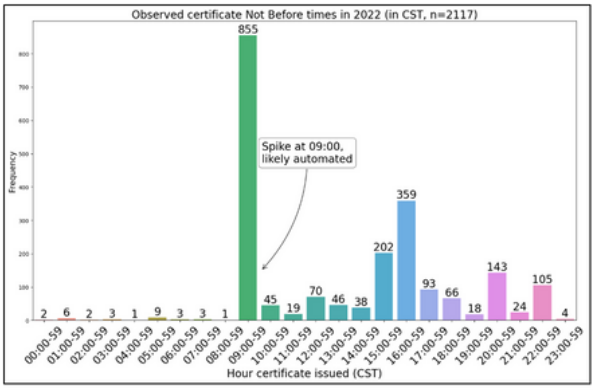


Figure 17 - Certificate issuance times in 2022

Analysis of TLS certificate issuance times showed no significant overlap in certificate issuance time between the domains on the Hetzner IP (holacode[.]io) and the Fangxiao domains downloaded from URLScan.

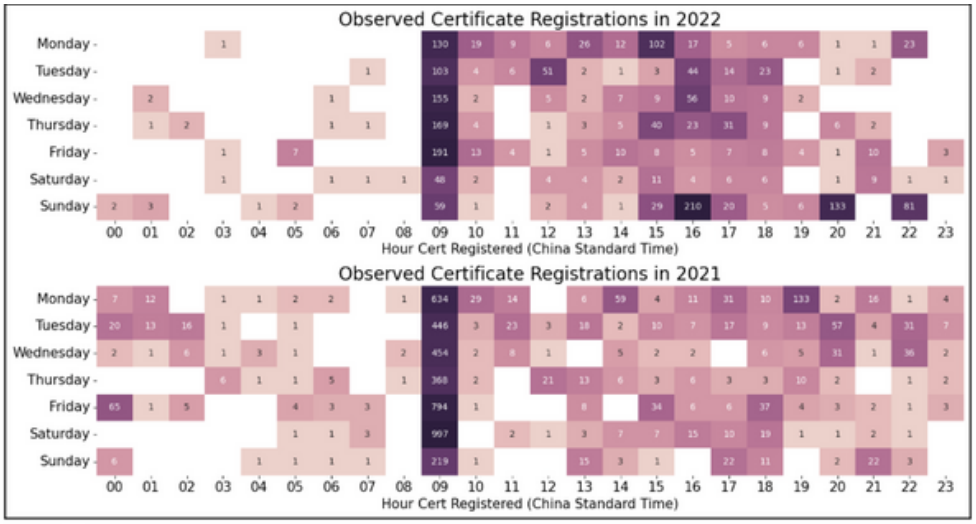


Figure 18 - Fangxiao certificate registration times in 2021 and 2022

We analysed WHOIS data belonging to 34,462 domains to try to obtain any trends or information leakages alluding to identities or infrastructure usage. There were forty-nine unique, non-third-party registrant emails identified (Appendix A). 17 were registered with rambler.ru, 3 with 163.com, one with Hotmail.com, 4 with gmail.com, one with yahoo.com, one with contact.gandi.net, and 22 with privacy-oriented hosts including: domaindiscreet.com (10), withheldforprivacy.com (5), privacyguardian.com (3), domprivacy.de (1), domainprivacygroup.com (1), privacy.above.com (1), whoisprivacyservice.org (1), protonmail.com (1), NameBrightPrivacy.com (1).

Fangxiao has used a variety of top-level domains, mainly .top (67%) and .cn (14%) TLDs. Comparing this with a smaller sample taken prior from the most modern section of the campaign, we learn that in the earlier stages of deployment, the group used more common TLDs and then switched over time to using .top. The .top TLD is commonly associated with fraudulent behaviour and is available for as little as $1.39 a year. This likely reflects Fangxiao's desire to reduce costs as they scale their business to be more profitable. Purchasing and replenishing their domain pool is likely to be their biggest cost.

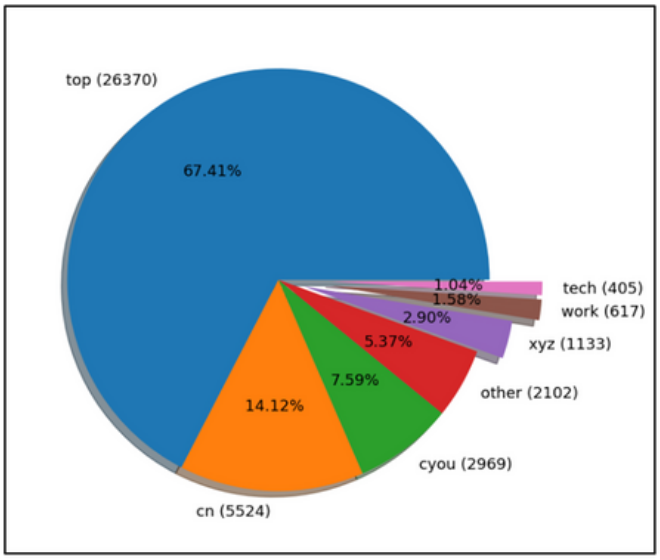


*Figure 19 - TLDs in the sample of domains*

In the sample, we identified 89 different domain registrars. A significant proportion of these are based in China; however the group also utilised well known trusted registrars such as GoDaddy, Namecheap and Wix. Notably, the domain registrar Epik was included in the list. Epik was breached in 2021 and several hundred gigabytes of data were dumped. Searching the breached Epik files found several other websites linked to one of the WHOIS emails (1domains12345@gmail.com). These included several pornographic sites but ultimately provided no further leads for investigation. Another email from the WHOIS data, seydor2kk@gmail.com, was included in the 2021 OGUsers breach. This username has been used for a variety of purposes such as uploading cracked games on a Russian forum and creating a dating profile on a predominantly Russian dating site.

# Conclusion

We assess that Fangxiao is a China-based threat actor likely motivated by profit. The operators are experienced in running these kinds of imposter campaigns, willing to be dynamic to achieve their objectives, and technically and logistically capable of scaling to expand their business.

The Fangxiao campaigns are effective lead generation methods which have been redirected to various domains, from malware, to referral links, to ads and adware. We attempted to find concrete evidence to link any of the payloads to the original Fangxiao campaign but were not able to do so. Despite this we can also not confirm these are separate entities.

What should be clear from this study is that Fangxiao's criminal actions, like those of all other cyber threat groups, are enabled by the internet infrastructure which we all rely on. As noted above, they deploy a variety of strategies to obscure their identity, such as the protection provided by CloudFlare. We all use the same platforms. It is difficult to see how this situation could be dealt with effectively and fairly, but certainly it is something which is worth consideration.

## Indicators Of Compromise

**Domains**
Available here: https://www.cyjax.com/resources/blog/fangxiao-a-chinese-threat-actor

**IP Addresses**
157.90.113.238

# Appendix A: Email Addresses

tisritetecifun853@rambler.ru

liangqing2442@163.com

morozov-2kcip@rambler.ru

01pevnv7emhiua5kho3ahs6g3u@domaindiscreet.com

0irp6pb2tsj3ebj9a1880n0e7c@domaindiscreet.com

1domains12345@gmail.com

2gofdlfkamiugaab94gr0r2p94@domaindiscreet.com

33cda6e32a2b41b4aea11ac14f7a2c87.protect@withheldforprivacy.com

3bk8tvbhh4h1r9mmfra7akrn0n@domaindiscreet.com

3po1egjt0qisba3v1qgd632tg8@domaindiscreet.com

439db602119844b182087093f8ff3e75.protect@withheldforprivacy.com

5f74286588d947e7b642eb68947fe486.protect@withheldforprivacy.com

90mdcb98tkibp9viviqopeikrc@domaindiscreet.com

94henniu888@protonmail.com

98anrv74lohedaq310as7tsmu1@domaindiscreet.com

a27qyllvvw@domprivacy.de

ae30eb109318e1d3eadcc4472d0238cb-1050201@contact.gandi.net

anisimov-7toma@rambler.ru

authorbeam@gmail.com

bp74l2upqohhmbjs5ejks6gph3@domaindiscreet.com

ca99717be53f48088d1a5e25754e8a1a.protect@withheldforprivacy.com

dafa05666@163.com

datagiftz.com@domainprivacygroup.com

demchenko-q841r@rambler.ru

fii9rvvekii62buiqfdqb4p5ei@domaindiscreet.com

filatova-br14y@rambler.ru

fsguitk8l0j8fbf9kt18904rir@domaindiscreet.com

liangqing2442@163.com

loginova4sete@rambler.ru

mamedov94aru@rambler.ru

moiseev.0ilqr@rambler.ru

morozov-2kcip@rambler.ru

nazarov-m45kg@rambler.ru

noskov_4yb9n@rambler.ru

odinokova_s86ti@rambler.ru

owner-3421256@phrase.com.whoisprivacyservice.org

panina.wa4nv@rambler.ru

peacchi@163.com

poliakova47s6d@rambler.ru

pw-3ad060b41c8bef48fb01e3b72da692ba@privacyguardian.org

pw-6b30cc57dc59a2a42ef86e53a4337d34@privacyguardian.org

pw-dd9e1a789e02bde9346fd7675432714e@privacyguardian.org

robertshawnrsxtqg@gmail.com

seydor2kk@hotmail.com

soniyayeasmin530@gmail.com

teukomcumbritise152@rambler.ru

TImasep@yahoo.com

tisritetecifun853@rambler.ru

tisritetecifun853@rambler.ru

TomAhvetClinic.net@NameBrightPrivacy.com

veselova44gu7@rambler.ru

viktoroibragimov@mail.ru

wealthstrategies4u.com@privacy.above.com