

# Salted Leeches

An investigation into a Chinese online scam ring infrastructure

## TL;dr

CyberCyberLabs security researches Noam Rotem and Ran Locar have exposed a large scam operation believed to be operated by a Chinese criminal organizations and targeting vulnerable gig-job seekers in the US, UK, and Europe. The operation uses somewhat known brands, usually of rising start-ups but sometimes established companies like Booking, Expedia, and Spotify, and creates fake websites masquerading as these companies. It then publishes "remote work" ads, sometimes on fake websites they build themselves, and directly contact victims via WhatsApp. The research exposes dozens of platforms used to scam people in a "recharge scam", providing a unique view of their network infrastructure, back-office systems, crypto wallets containing tens of millions of US dollars siphoned from the victims, as well as their entire database of operations, transactions, and identities. It also includes WhatsApp chats between the victims and the operators, along with technical evidence pointing towards Chinese individuals operating from Hong Kong, mainland China, Cambodia, and Myanmar.

It is very important to stress: None of the companies mentioned in this report are associated with the scammers. Their names were simply dragged into the scam by the operators of the scam network.

None of the companies were breached, nor did the operators of this scam networks get a foothold inside their infrastructure. They only leveraged their brand reputation in order to scam innocent people looking for a job.

Full disclosure: The criminal organization targeted a company where mr. Rotem, one of the authors of this report, is acting as CTO.

## The scam

During the work on this project we have been in contact with several victims who were scammed. They were kind enough to provide us with WhatsApp communication between them and the scammers, as well as inside understanding of the different stages of the scam. The following section is a summary of their stories as well as a lot of technical evidence, including access to the scammers back-office systems.

### Step 1: The Approach

Several victims said they were contacted by a WhatsApp account "regarding a recent job application". For example, in Sweden, the scammers used the site worklifthub[.]com, and then moved to employfocushub[.]com to create a trusted context for the initial approach. The domains were registered in late December 2024 and early January 2025, in Turkey and the Bahamas. Other cases used totally legitimate job-seeking websites, so the approach seemed more natural. The texts are always cheerful, full of positive emojis, and almost always reply very quickly.

The recruiters introduce themselves as employees of a branch in a non-brand company, but

The recruiters introduce themselves as employees of a branch in a non-brand company, but one that yields positive google results; these are mostly B2B companies that are not known to the general public, but are known within the industry. If the victim searches for the name of the company, they will find a lot of information from trusted sources. The scammers register multiple domains with permutations around the target company name (they have an affinity to the .top tld) reflecting the type of work. for example, they would register [company]-seo.top and [company]ppc.cc if the "job" is related to SEO or PPC advertising. They also register a unique high-entropy domain to be their back-office gateway.

The sites are well built, and the victims, who are often blinded by the prospect of employment, are often persuaded that this is a real website.

## Step 2: The Job

All of the platforms we've investigated are very similar in the "jobs" they offer. While the details vary, in most cases the role of the employee is to write reviews to products promoted by the original company. However, these reviews are not going anywhere. there's even an "Automatic Comment" button on some of the sites. Their sole purpose is to keep the victim busy, give them a sense of doing something of value, and to prepare them for the next phase.

For each review entered by the victims, they receive between 10-70 cents, depending on the industry. There are limits on the number of "tasks" each employee can do per day, usually newcomers have a limit of 50 tasks per day, putting the potential profit from this job at around \$5-\$35 per day. Still, not bad for an easy work-from-home gig that takes up to an hour to complete

## Step 3: The Opportunity

After a few days of doing the menial work described in the previous step, opportunity knocks. When the victim logs in and tries to complete their daily tasks, they are presented with an error. There are not enough funds in their balance to keep working. When they contact customer service (yes, each site has a dedicated customer service system, and a very efficient one at that) they are surprised to find out that they can now make much more money! Instead of getting paid cents for their boring work, they can now make tens, sometimes hundreds of dollars per task.

There is a small hiccup, though. The higher value tasks require a certain balance, which is always slightly above what the user has. If only there was a way for them to get this task done they could triple their investment. High value tasks could include purchasing a product for an end-customer on behalf of the 'company', under the promise that the employee would be rewarded.

For example, the "company" needs to buy a certain product for a certain client, but alas, they can't do it right now. If only the loyal employee would be able to make this purchase, when the end-customer pays this loyalty would be rewarded greatly. If the employee agrees, they must send a certain type of cryptocurrency (usually ETH tokens like USDC or USDT to a wallet address given to them by the operators. If not, at great risk to themselves, the handlers of the victim are willing to "gift" this money out of the goodness of their heart.

When the deal goes through, the victim is overjoyed to see his balance increases, and in many cases will issue a withdrawal, which will be fulfilled. When the employee then wants to make another "task", their balance is not high enough, so they need to **re-charge** their balance. This is where the name **re-charge fraud** comes from, and this is exactly how it works. The employee keeps loading their own funds into the scammers wallets just so they can keep on working.

## Step 4: The slaughter

By the time they realize what's going on, their withdrawal requests are ignored, and their accounts are frozen. The victim was butchered, taken for thousands, sometimes tens of thousands of their hard earned currency, and is left with nothing.

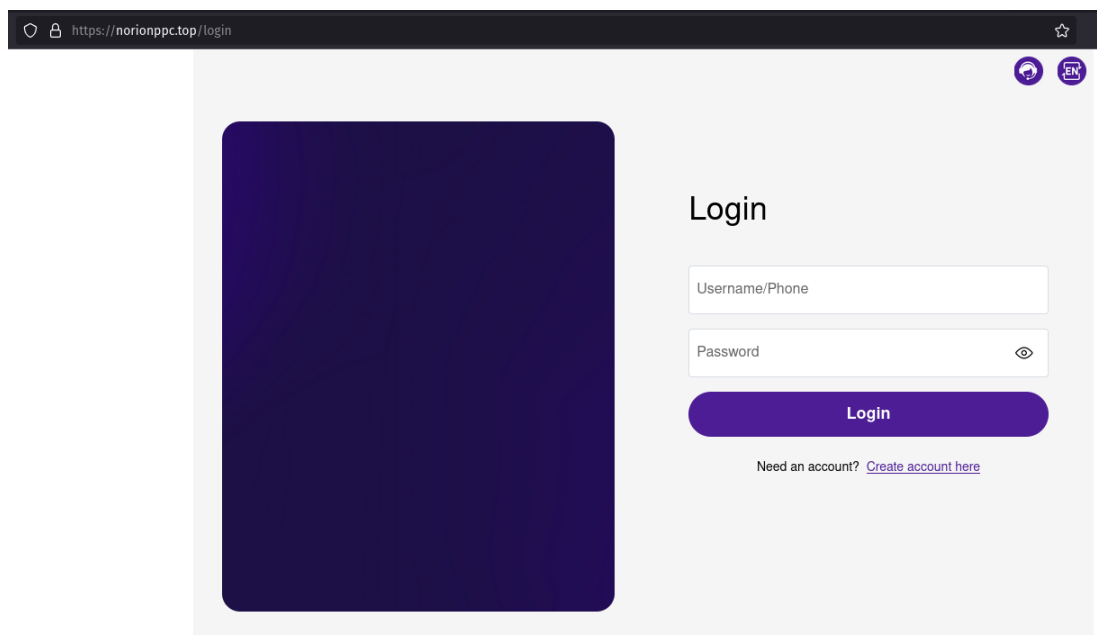
Some of the victims realize the scam when they try to reach out to the real company the scammers are impersonating, only to learn there is no "UK branch", and that the real company had nothing to do with the "work" they were "hired" to do. Going to the police doesn't help either, as the crime was out of the local jurisdiction, and the perpetrators are unknown. This is how the scammers harvest tens of millions of dollars from vulnerable victims, looking for a low paying job, and ending up in a much worse situation than before they started working.

## The systems

Each such operation is split into 2 systems. One is referred to as "the front-end", this is the fake website where the "work" of the employees take place. Let's take for example the website pretending to belong to an asset tokenization platform "Norion".

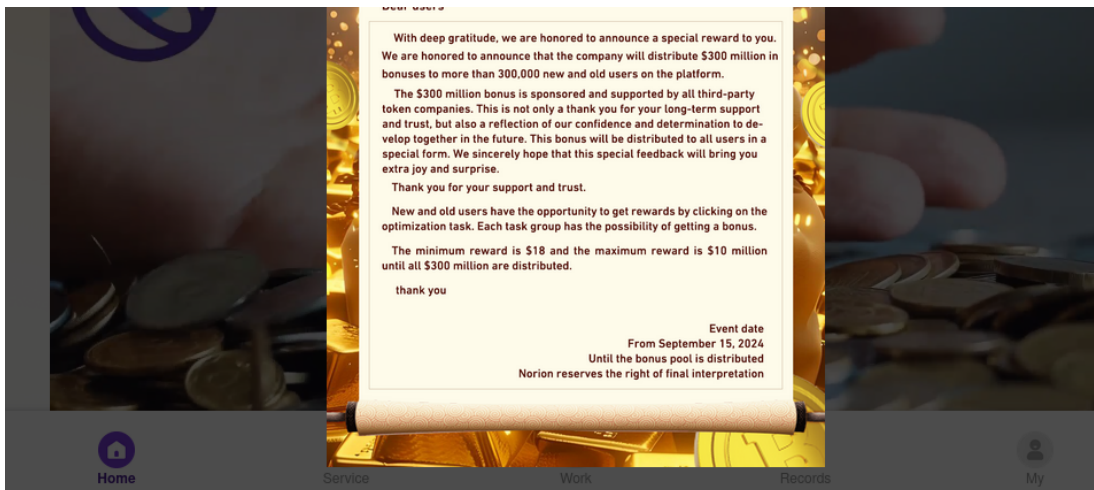
### The Front-End

This is how the front-end log-in page looks like. Notice the domain "norionppc.top", which is how the "job" is marketed to the victims. "It's an SEO/PPC operation, nothing shady":

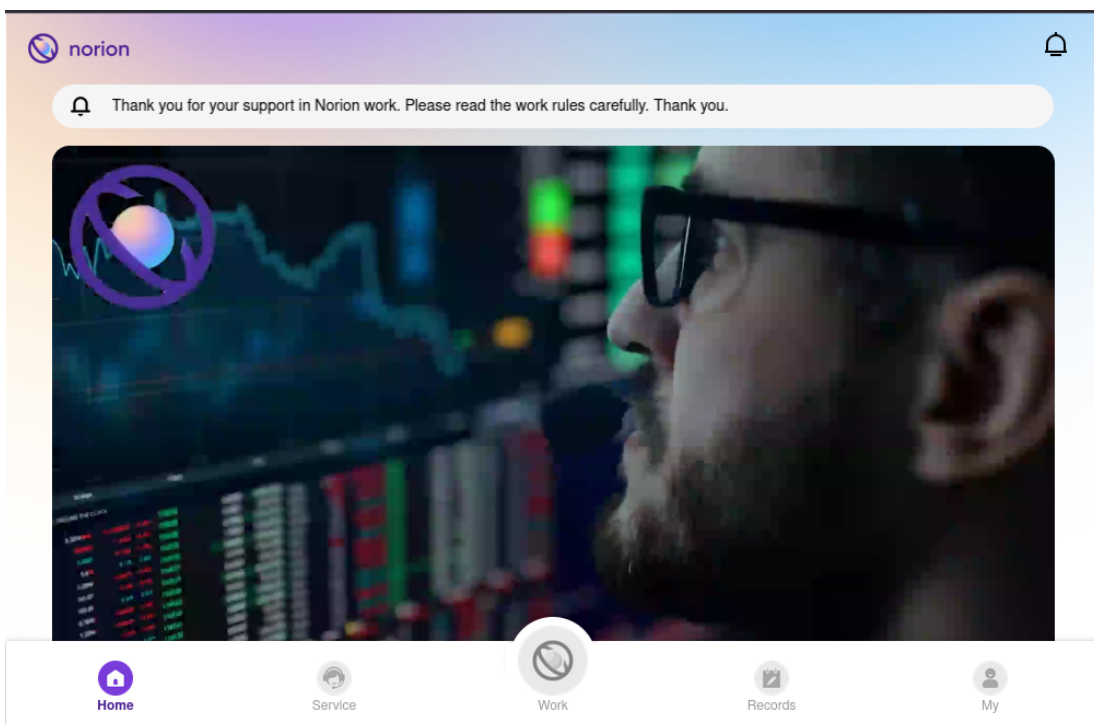


Right after the user logs in, they are presented with what the scammers call a "certificate". A fake image designed to inspire trust. In some cases it's "signed" by the CEO of the company, in this case, it's advertising a \$300 million bonus that will be distributed between the employees based on their performance up to \$10 million per person:

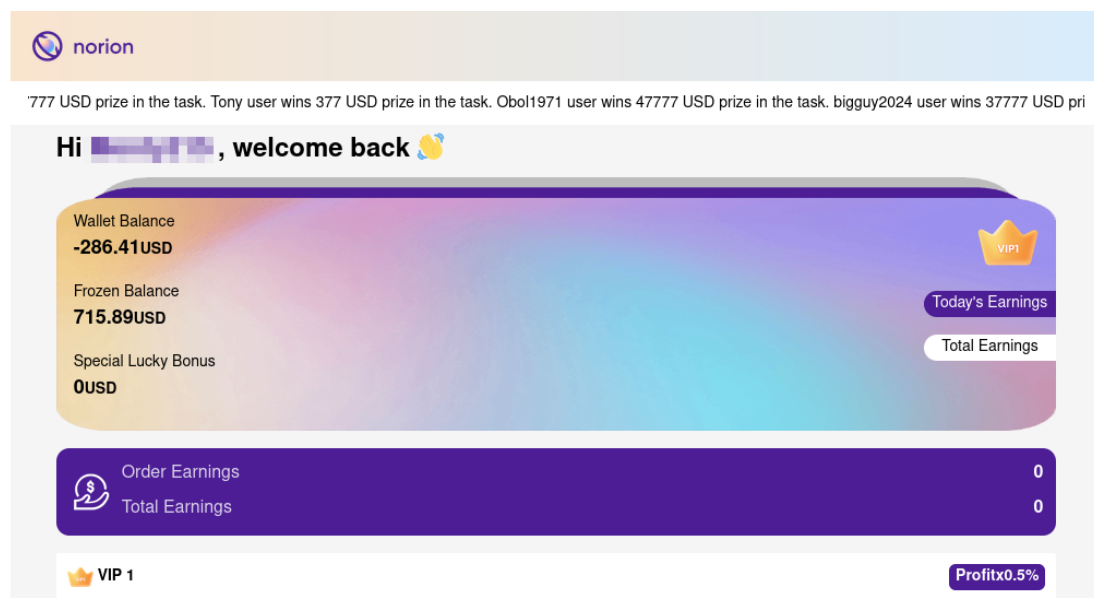


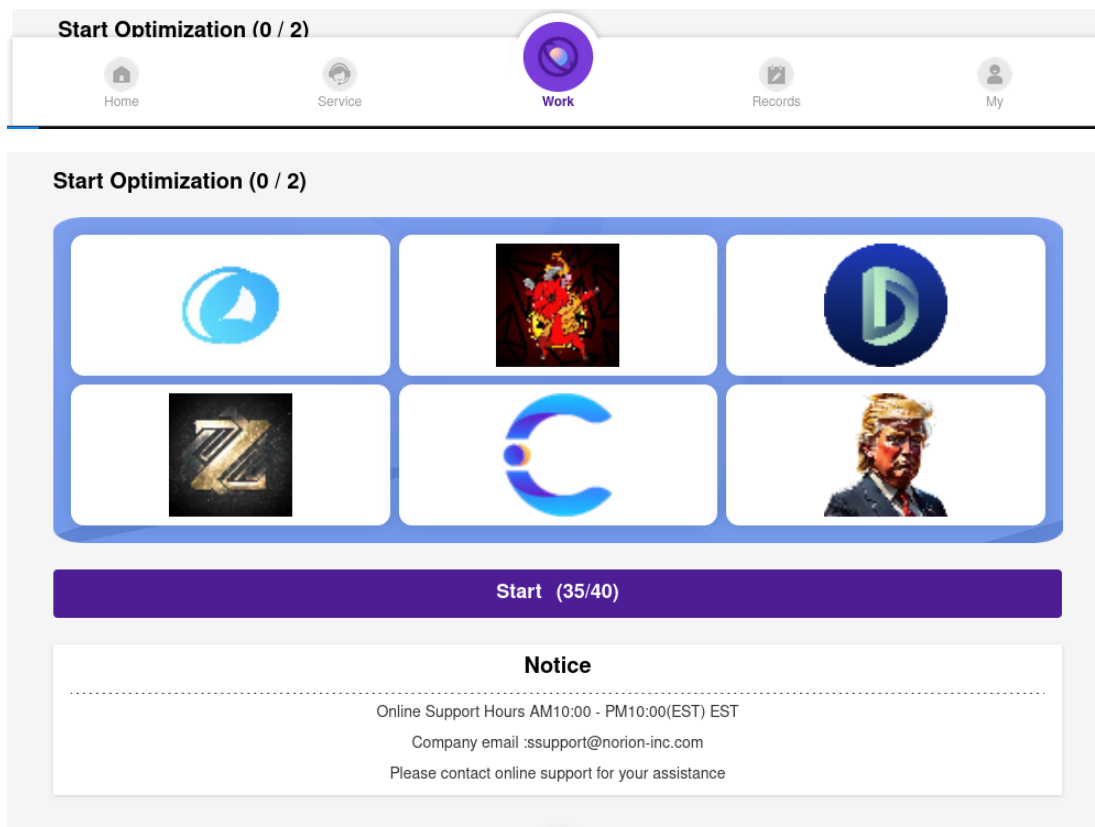


Then an impressive corporate video is displayed, and the employees can start their daily tasks

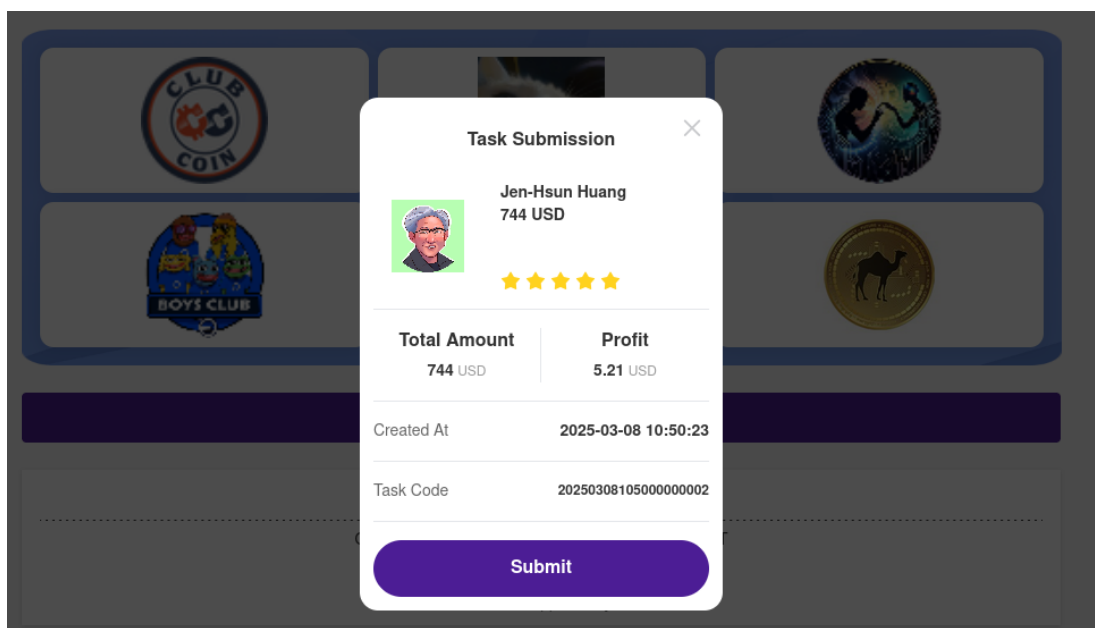


the big "work" button in the bottom center of the page, leads the user to a gamified version of what a lemur thinks people who work in an office do:



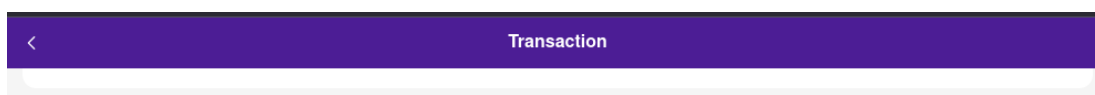


Clicking on "Start" shows a modal with a "Task". It shows the amount of the transaction, and the expected profit from it.



Clicking "Submit" simply says "Task submitted", that's all this "work" is. The employee balance is deducted until the transaction is approved, and that's it. The employee now expects a profit of \$5.21 to be added to their balance once it's done. \$5.21 for clicking a button, not a bad job to have.

Another part of the "front-end" includes a way to withdraw or deposit funds, as well as seeing the transactions history. Here you can see that the user started off as described in "Step 2" of the scam, making a few cents per "task". They received a \$10 "sign-up" bonus at January 25th so that they can start working, and immediately started making money:



<b>Subordinate commission return</b> 2025-01-25 13:48:33	1.22 USD
<b>Subordinate commission return</b> 2025-01-25 13:47:38	0.64 USD
<b>Subordinate commission return</b> 2025-01-25 13:47:30	1.33 USD
<b>Subordinate commission return</b> 2025-01-25 13:47:24	0.67 USD
<b>Subordinate commission return</b> 2025-01-25 13:47:13	1.3 USD
<b>Registration bonus</b> 2025-01-25 12:42:36	10 USD

This is how their "profit" is explained:

<b>Commission return</b> 2025-01-25 14:04:41	0.14 USD
<b>Principal return</b> 2025-01-25 14:04:41	27 USD
<b>Task</b> 2025-01-25 14:04:38	-27 USD

You put it a certain amount (\$27 in the example above), you get it back + a commission, in this case, due to the low value of the original transaction, it's 14 cents.

only 3 hours into the job, the employee is stuck and is convinced to deposit \$30 so that they can continue. after this, their commission rises to 30 cents. A 100% increase in just a few hours, not bad.

<b>Commission return</b> 2025-01-25 15:07:00	0.3 USD
<b>Principal return</b> 2025-01-25 15:07:00	59 USD
<b>Task</b> 2025-01-25 15:06:58	-59 USD
<b>Deposit</b> 2025-01-25 15:05:58	30 USD

However, only 4 days into the work, the commission suddenly spike. no more \$0.14, it's now \$11.21 per task! a whopping 7907%! this employee is a meteor!

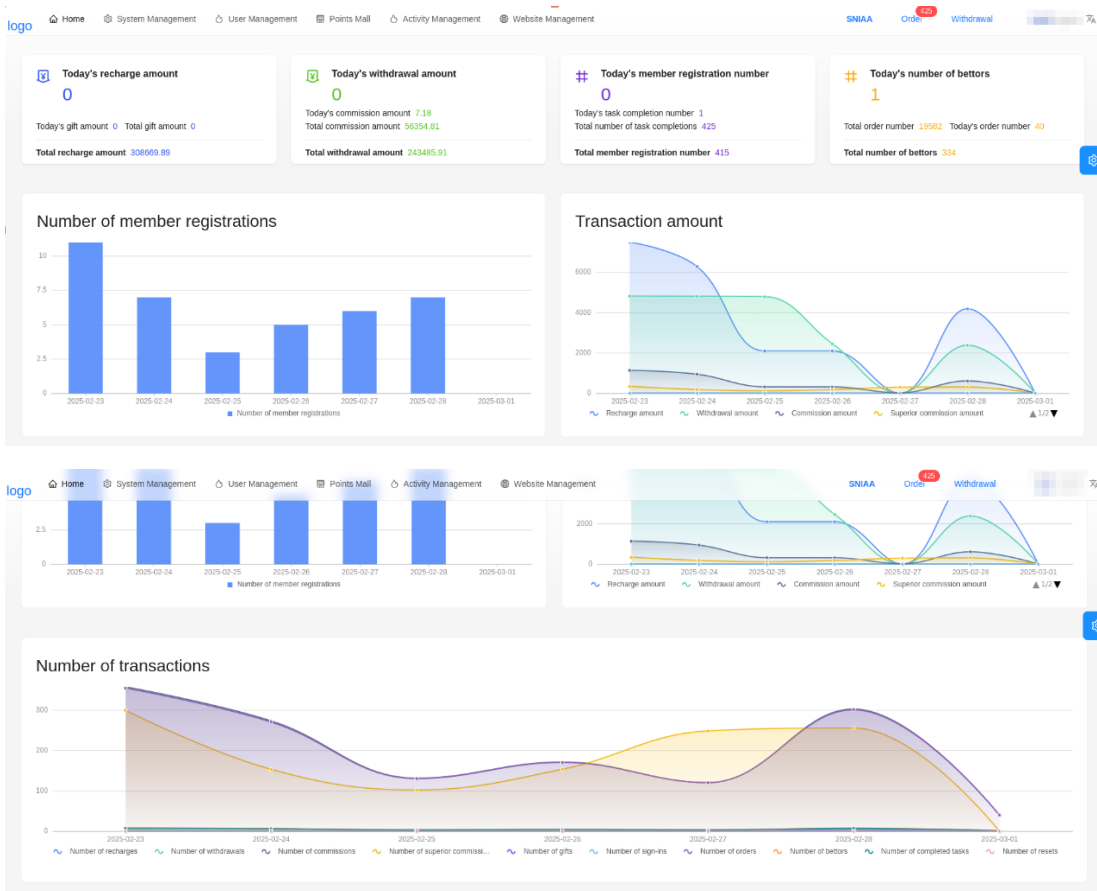
<b>Commission return</b> 2025-01-29 14:30:29	11.21 USD
---	-----------

Principal return	2025-01-29 14:30:29	224.27 USD
Deposit	2025-01-29 14:29:59	148.56 USD

The employee is ecstatic, deposits are pouring in, until one day - poof - they can't withdraw any more.

## The Back-End

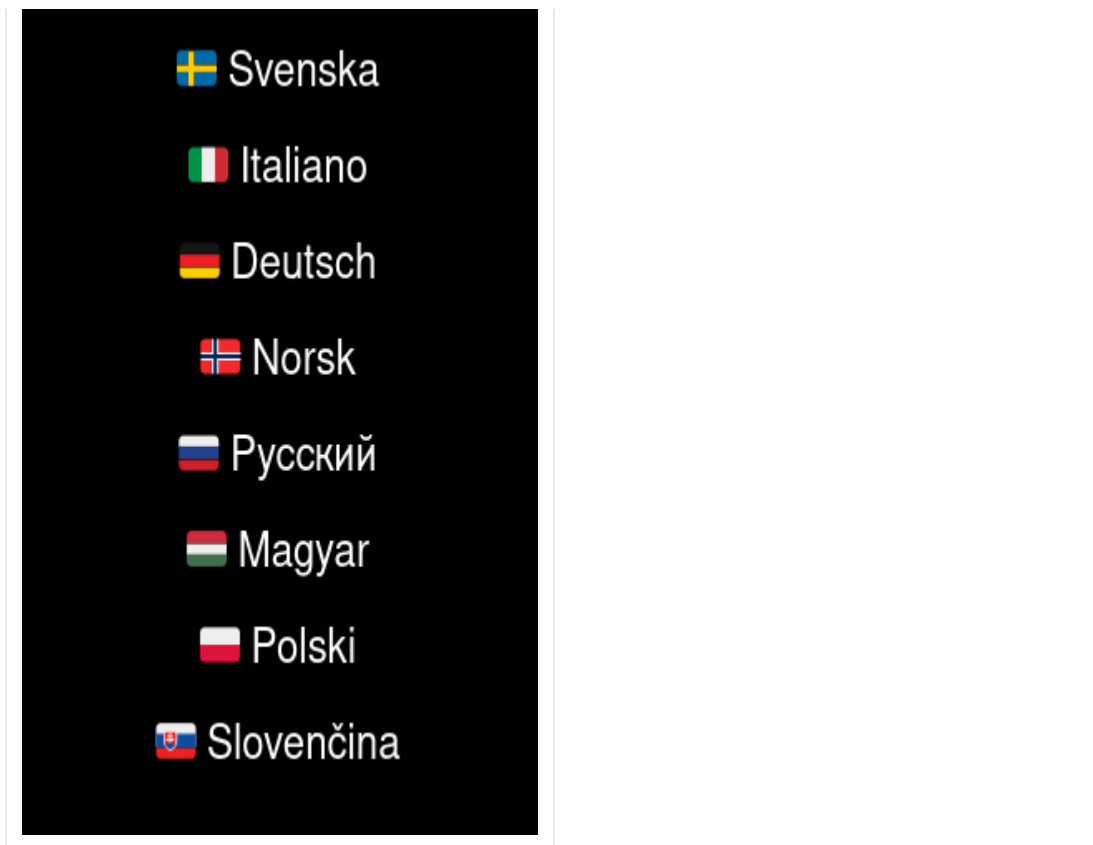
Meanwhile, the operators of the platform, uses a completely different system, they call "The Back-End" or "The Marketing". A dashboard with nice graphs and summaries is presented to the administrators:



However, unlike the front-end which supports no less than 12 languages, the Back-End supports only 2: English and Chinese. Target audiences are clear.

Front-End languages	Back-End languages





It allows full control over the "front-end" and its users, which are called "members", allowing the "users", who are the operators of the scam and their accomplices, full control over their status. They can "gift" funds for users, they can reduce them, freeze them, and watch their behavior:

ID	Username	Phone number	Email	Birthday	VIP level	Parent user name	Task Progress	Sign-in days	Bala	Operation
1400	Merius2	[REDACTED]	[REDACTED]@gmail.com	-	VIP 1	阿里	40 / 40	0	69.0	Up and Down Reset Order
1390	PD855	[REDACTED]	-	-	VIP 2	Bighenn38	50 / 50	0	1885	Up and Down Reset Order
1399	Bighenn38	[REDACTED]	[REDACTED]@gmail.com	-	VIP 1	群弟77	40 / 40	0	72.3	Up and Down Reset Order
1389	FA038	[REDACTED]	-	-	VIP 2	Diop	50 / 50	0	1825	Up and Down Reset Order
1398	Diop	[REDACTED]	[REDACTED]@gmail.com	-	VIP 1	白冰	36 / 40	2	-312	Up and Down Reset Order
1388	FA037	[REDACTED]	-	-	VIP 2	Justin7	50 / 50	0	1829	Up and Down Reset Order
1397	Justin7	[REDACTED]	[REDACTED]@gmail.com	-	VIP 1	白冰	40 / 40	0	72.1	Up and Down Reset Order

The systems we have observed while working on this report hold between hundreds and thousands of "members" each, including their contact details, crypto wallets, IP addresses showing their locations, and the amounts they have lost to the scam. Almost all of the victims are from western countries such as the US, UK, Sweden, Germany, Austria, France, and others.

The "Users", on the other hand, are from very specific geographies. with names that google translate explains as "Lucky", "Fly", and "Comes with beans" all written in Chinese. "Users" can be either "administrators" or "agents" with the latter have much limited access. the screenshot below is of an Administrator:



User management	Product Management	Points Account	Gift Management	Points Order	Strategy Management	Role Management	Group management	Organization Management
Organization Management								
Position Management								
User management								
Permission management								
File management								
Operation Log								

Username:  Phone numb:  Organization:

ID	Username	Phone number	Organization	Avatar	Name	Gender	Is it enabled	Is it frozen	Email	Operation
193	沙皮	331235456	总部	-	沙皮	Male	Enable	No	-	Modify Copy
192	熊二	33212	总部	-	熊二	Male	Enable	No	-	Modify Copy
181	幸运	51232131325	总部	-	幸运	Male	Enable	No	-	Modify Copy
163	勇敢	56454564	总部	-	总部	Male	Enable	No	-	Modify Copy
162	阿里	523121515	总部	-	阿里	Male	Enable	No	-	Modify Copy
161	胖弟	1231231231	总部	-	胖弟	Male	Enable	No	-	Modify Copy
131	阿东	85221545646	总部	-	阿东	Male	Enable	No	-	Modify Copy

1-17 of 17 items

under the "Operation Log", each read, write, and update, is logged with the details of the user who performed it.

Operation log

Delete

<input type="checkbox"/>	ID	Resources	Username	IP	Address	Status	Creation time	Duration (milliseconds)	Method	Request address
<input type="checkbox"/>	61745	查询等级[marketing:level...	阿东	154.222.64.208	Cambodia[Phnom Penh]...	200	2025-02-28 10:31:59	67	GET	/marketing/levels/list
<input type="checkbox"/>	61744	查询出金类型[marketing:...	林枫	154.222.64.208	Cambodia[Phnom Penh]...	200	2025-02-28 10:00:28	188	GET	/marketing/withdrawal..
<input type="checkbox"/>	61743	查询提现记录[marketing:...	林枫	154.222.64.208	Cambodia[Phnom Penh]...	200	2025-02-28 10:00:28	76	GET	/marketing/withdrawal..
<input type="checkbox"/>	61742	查询充值记录[marketing:r...	林枫	154.222.64.208	Cambodia[Phnom Penh]...	200	2025-02-28 10:00:27	104	GET	/marketing/rechargeRe
<input type="checkbox"/>	61741	查询会员[marketing:mem...	林枫	154.222.64.208	Cambodia[Phnom Penh]...	200	2025-02-28 10:00:25	95	GET	/marketing/members/p.

601-620 of 62065 items

<

1

>

29

30

31

32

33

>

20 / page

Go to

Page

We have downloaded and analyzed all actions performed by the operators, and found that all administrators are working from Cambodia, Hong Kong, Myanmar, and mainland China, whereas the "agents" may be located in the US (New York, New Jersey, Florida, California, are popular locations) and Europe. These agents are acting as recruiters, gaining profits from the people they lure into the scam like any other MLM fraud. We have found several US citizens, among them a self-titled "coach" from Florida who is offering abstinence workshops while working from home to recruit new victims for this Chinese scam operation.

Looking at the access log of the "Users" (administrators), the accepted language for all of them in the HTTP headers sent on every request to the server is Chinese, further contributing to the attribution.

Other than that you can find the expected configuration options of any CMS, including the support links and phone numbers, Notifications sent out to all users, Banners for various parts of the front-end platform, and more:

Customer service list

Name	serial number	picture	Is it enabled	Link
WhatsApp-CS5	1		Enable	https://wa.me/+140...
WhatsApp-CS4	2		Enable	https://wa.me/+120...
WhatsApp-CS3	3		Enable	https://wa.me/+120...
WhatsApp-CS2	4		Enable	https://wa.me/+120...

☐ WhatsApp-CS1
 5
 
 Enable
 https://wa.me/+18...

× Modify

2

\* Registration gift amount

\* Minimum balance for transactions

\* Member withdrawal status
 

☐ Disable
 ☒ Enable

\* Minimum credit score for member withdrawal

\* Minimum withdrawal amount for members

\* Maximum withdrawal amount for members

\* Maximum withdrawal amount for a single day on the platform

\* Withdrawal handling fee rate
  %

\* Parent-level commission percentage
  %

Match range (%)
 

~

\* Service time range
 

×

\* Trading time range
 

→

\* Withdrawal is prohibited after recharge
 

☒ No
 ☐ Yes

\* Is there a limit to the minimum balance level for withdrawals?
 

☒ No
 ☐ Yes

\* Withdrawal time range
 

→

\* Whether to submit tasks automatically
 

☒ No
 ☐ Yes

\* Start task delay in milliseconds

\* Submit task delay in milliseconds

Cancel OK

From the dates in the database it seems that the operation has been active since at least November of 2023, with records of stolen funds going back to December of that year.

An administrator of the back-end has almost full control over every part of the scam, including the commission values, service and trading times, minimum and maximum limits for various actions, and more.

## Telegram

Most of the systems reviewed in this report, each on its own dedicated server, use the exact same telegram bot called "Wotlk" to communicate with the "super administrators". Luckily, they provide the key and secret to this bot:

Name

Wotlk

Token

80623...LZosLS3j

With these credentials we have listened in on some of their conversations, all in Chinese, collecting member details of the "super group" as they call themselves, sporting Telegram premium memberships.

```

{
  "ok": true,
  "result": [
    {
      "update_id": 348395801,
      "message": {
        "message_id": 6779,
        "from": {
          "id": 6082188801,

```

```

        "is_bot": false,
        "first_name": "Wotlk",
        "username": "wotlk_king"
    },
    "chat": {
        "id": -1002356990938,
        "title": "系统待处理问题",
        "type": "supergroup"
    },
    "date": 1741364299,
    "message_thread_id": 6770,
    "reply_to_message": {
        "message_id": 6770,
        "from": {
            "id": 6119699846,
            "is_bot": false,
            "first_name": "凯撒-宏鑫科技",
            "username": "mumuzibb",
            "is_premium": true
        }
    },

```

and the administrator:

```

    {
        "user": {
            "id": 6119699846,
            "is_bot": false,
            "first_name": "凯撒-宏鑫科技",
            "username": "mumuzibb",
            "is_premium": true
        },
        "status": "creator",
        "is_anonymous": false
    }
}

```

Some of the messages in this channel are about improvement of the platform (all messages are sent in Chinese, we use Google translate to be able to read them in English):

The bonus needs to be added with an effective time (for the delayed issuance function), with a pure front-end display function, without any restrictions, this effective time can be modified. \n\nIn addition, the front-end bonus is counted whether the current interface can meet the current interface, the amount that has been collected and the amount to be collected

and

I want to add another type to the backend banner management to give the frontend to use when logging in to the page? Will there be an interception?

## Database access

Examining the database, we found that each 'back-end' server hosts its own instance. All of

them share the same schema, further establishing that they are running the same platform, but each one has different data inside.


```
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] wotlk

Database: wotlk
[78 tables]
+-----+
| t_account          |
| t_activity         |
| t_activity_account |
| t_activity_account_prize |
| t_activity_partner |
| t_activity_prize   |
| t_additional_commission |
| t_app              |
| t_app_channel      |
| t_award             |
| t_award_push       |
| t_banner            |
| t_bulletin          |
| t_bulletin_locale  |
| t_category          |
| t_channel           |
| t_customer_service |
| t_even              |
| t_even_detail       |
| t_file              |
```

The administrator UI provides control to all data and settings in the Database.


## Crypto

During our investigation we identified several cryptocurrency wallets used to send and receive funds from this enterprise. We believe we identified one of the master wallets sending hundreds of thousands of dollars worth of crypto to another wallet at address which holds, at the time of writing, over 50 million USD in various tokens, including the trump meme coin:

Balances <sup>?</sup>		~ \$ 1,156,160.60 (+0.34%)
<u>Ethereum</u>	540.3806212032927  ETH	\$ 1,156,109.60 (+0.34%)
<u>PayPal USD</u>	51.013749 PYUSD	\$ 50.99 (+0.01%)

<u>Black Agnus</u>	3,333,333.00 FTW \$ 0.00 (-5.25%)
--------------------	--------------------------------------

<u>Balances</u> <sup>?</sup>	~ \$ 50,175,683.81 (-0.02%)
<u>Ethereum</u>	2,047.4802769520159  ETH \$ 4,380,452.44 (+0.34%)
<u>Global Dollar</u>	20,629,377.7188 USDG \$ 20,621,666.40
<u>PayPal USD</u>	11,537,802.300925 PYUSD \$ 11,533,009.77 (+0.01%)
<u>PAX Gold</u>	2,024.4421339 PAXG \$ 5,949,384.78 (+0.27%)
<u>Pax Dollar</u>	2,911,506.075848465 USDP \$ 2,910,094.36 (-0.04%)
<u>USD Coin</u>	1,935,338.97003 USDC \$ 1,935,302.99
<u>Aave</u>	6,839.66148989 AAVE \$ 1,294,580.89 (-0.26%)
<u>Uniswap</u>	138,794.25974172 UNI \$ 953,419.19 (-0.93%)
<u>Chainlink</u>	37,068.98309135 LINK \$ 544,450.82 (-4.61%)
<u>Matic Network</u>	222,918.41468577646 MATIC \$ 53,252.76 (+0.34%)
<u>TRUMP MEME</u>	23,760.00 MEME \$ 65.10 (+401.43%)

## Summary of attribution

There are many indicators that point to the operators of this operation as being connected to China:

1. Accepted languages in the HTTP headers of the operator calls are all **zh-CN** , (on telegram we have seen administrators identifying with **zh-hans** , a less common Chinese locale) which indicates that the browser, or operating system default language, is Chinese.
- 2 While the front-end system aimed at the victims shows various languages, none of them is

- While the front-end system aimed at the victims shows various languages, none of them is Chinese, the back-end system, which is used by the operators, supports English and Chinese, and these languages only. This may point that the operators work in one of those two languages.
3. Usernames of the operators are in Chinese characters, spelling words in Chinese.
4. Specifically, the administrator of the Telegram group (mumuzibb) is using Chinese, and participates in Chinese chats on Telegram

Telemetrio  
https://telemetr.io › Home › Global › Translate this page

海华G0118供押5888u宏鑫职业fb股票粉公群（月付）

... mumuzibb 业务频道: https://t.me/HXJTHWDF 注意核对是否是公群管理员, 谨防模仿骗子. 0. 10. 欢迎淘宝刷单—单500—单—结账淘宝刷单—单500—单—结账请在两分钟前回答9 ...

Telemetr.io  
https://telemetr.io › channels › quote › Translate this page

海华G0118供押5888u宏鑫职业fb股票粉公群（月付）

... mumuzibb 公群TRC地址: TRdrUgcF62EpUw9fRQEMUyKkHQ4oyrfCPy 【宏鑫职业FB股票粉】公群! 欢迎入驻! 总群: @HHCH 公群: @haihuaEE ————, 20. 8 ...

5. The internal communication within the "Super group" on telegram and other platforms is done in Chinese.
6. The code contains comments in Chinese
7. IP addresses of some of the operators are from China, while other from neighboring Hong Kong, a special administrative region controlled by China.
8. Looking at the first operations logs, the first user who set up the "websites" and "users" (other operators), using the user ID 1 and the name **wotlk** used IP addresses from Hong-Kong, with Chinese locale. Once the initial setup was done by **wotlk**, he invited user **admin** who also used Chinese locale, with a Cambodian IP address. Other administrators phone numbers start with +95, which is the country code for Myanmar, a known location of Chinese scam factories.
9. Telegram channel: communication is in Chinese.
10. Crypto wallets are linked to Chinese individuals.
11. Some of the file storage uses the Alibaba Cloud, the largest cloud computing company in China.

## List of domain names and IP addresses

Analyzing the first domains we encountered we found that they are hosted on CIDR 137.220.170.0/24 belonging to CTG Server Limited, a hosting provider operating in South East Asia. Based on our past experience we tried looking for domains with the similar pattern on neighboring IP addresses, as well as other CIDRs belonging to the same provider.

Using Hurricane Electric (bgp.he.net) and Security Trails (securitytrails.com) reverse IP searches, we compiled a list of domains and IP addresses set up by the fraudsters as part of this scam. The 'impersonated brand' is a best-effort attempt to deduce the brand the site is trying to impersonate, based on logos, name similarity and other graphics

Domain	Impersonated brand	Vertical
neon-ppc.top	Neon Growth	Marketing

neon-seo.top	Neon Growth	Marketing
neon-web.top	Neon Growth	Marketing
neonbusiness.top	Neon Growth	Marketing
neondatainc.top	Neon Growth	Marketing
neonwebsite.top	Neon Growth	Marketing
ngbusinessllc.top	Neon Growth	Marketing
tus2v1fhta.top	Neon Growth	Marketing
rktdatappcllc.top	Rocket Marketing	Marketing
rktmktdosllc.top	Rocket Marketing	Marketing
rocket-marketing-ppc.top	Rocket Marketing	Marketing
rocket-marketing-seo.top	Rocket Marketing	Marketing
rocket-marketing.top	Rocket Marketing	Marketing
rocket-mkt.top	Rocket Marketing	Marketing
rocketseoinc.com	Rocket Marketing	Marketing
tc5la9xvzm.top	Rocket Marketing	Marketing
evenboundppc.top	evenbound.com	Marketing
evenboundseo.top	evenbound.com	Marketing
rc7odfr90x.top	evenbound.com	Marketing
work.evenboundppc.top	evenbound.com	Marketing
work.evenboundseo.top	evenbound.com	Marketing
foymabphwx.top	rapchat.com	Music
ppc-rap-chat.top	rapchat.com	Music
rapchatdatainc.top	rapchat.com	Music
rapchatdataseo.top	rapchat.com	Music
rapchatppcspace.com	rapchat.com	Music
seo-rap-chat.top	rapchat.com	Music
my0x9jorxv.top	Smart Link	Marketing
smart-link-business.top	Smart Link	Marketing
smart-link-data.top	Smart Link	Marketing
smart-link-date.top	Smart Link	Marketing
smart-link-dos.top	Smart Link	Marketing
smart-link-ppc.top	Smart Link	Marketing



smart-link-pcp.top	Smart Link	Marketing
smart-link-seo.top	Smart Link	Marketing
smartlinkbusiness.top	Smart Link	Marketing
smartlinkdigital.top	Smart Link	Marketing
smartlinkppcinc.top	Smart Link	Marketing
apexarc-ai.com	Apex Arc	Marketing
apexarc-business.com	Apex Arc	Marketing
apexarc-data.com	Apex Arc	Marketing
apexarc-pcp.com	Apex Arc	Marketing
apexarc-ppc.com	Apex Arc	Marketing
apexarc-x.com	Apex Arc	Marketing
apexarcaisite.com	Apex Arc	Marketing
global.apexarcaisite.com	Apex Arc	Marketing
zhtaibj8.com	Apex Arc	Marketing
2f3rmggrz1.top	Jasper AI	Marketing
datajasperinc.top	Jasper AI	Marketing
gg2kxe6s67.top	Jasper AI	Marketing
jasperppc.top	Jasper AI	Marketing
jasperseo.top	Jasper AI	Marketing
seojasperllc.top	Jasper AI	Marketing
norionbusiness.top	norion.com	Crypto
noriondata.com	norion.com	Crypto
norionpcpinc.top	norion.com	Crypto
norionppc.top	norion.com	Crypto
norionseo.top	norion.com	Crypto
p1ouw3i5wp.top	norion.com	Crypto
d5654g7jj.top	VistaRise Hospitality Services India	Travel
vistarise.top	VistaRise Hospitality Services India	Travel
vistarisebusiness.top	VistaRise Hospitality Services India	Travel
vistarisedata.top	VistaRise Hospitality Services India	Travel
vistariseppc.top	VistaRise Hospitality Services India	Travel
vistariseseo.top	VistaRise Hospitality Services India	Travel

cisiondataspace.com	cision.com	Marketing
cisionpcpinc.com	cision.com	Marketing
cisionppc.top	cision.com	Marketing
n8jhepwdl9.top	cision.com	Marketing
6zw0xaubym.com	Digital Connect	Marketing
digitalconnect-seo.com	Digital Connect	Marketing
digitalconnect-x.com	Digital Connect	Marketing
digitalconnectai.com	Digital Connect	Marketing
digitalconnectbusiness.com	Digital Connect	Marketing
digitalconnectdata.com	Digital Connect	Marketing
digitalconnectppc.com	Digital Connect	Marketing
global.digitalconnect-seo.com	Digital Connect	Marketing
global.digitalconnectai.com	Digital Connect	Marketing
global.digitalconnectbusiness.com	Digital Connect	Marketing
global.digitalconnectdata.com	Digital Connect	Marketing
global.digitalconnectppc.com	Digital Connect	Marketing
cognitopsppc.com	cognitops.com	Software
cognitopsseo.com	cognitops.com	Software
q17dkahubn.com	cognitops.com	Software
firstpier-dataseo.com	firstpier.com	Marketing
global.firstpier-dataseo.com	firstpier.com	Marketing
p3et31p3hh.top	firstpier.com	Marketing
delantedata.com	delante.co	Marketing
g4xst1jqj9.top	delante.co	Marketing
ppc-delante.com	delante.co	Marketing
0j10uc2xf6.top	fera.ai	Marketing
5rydfzf73g.com	fera.ai	Marketing
fera.biz	fera.ai	Marketing
fera.ltd	fera.ai	Marketing
global.fera.biz	fera.ai	Marketing
global.fera.ltd	fera.ai	Marketing

tkmallpromohub.top	fera.ai	Marketing
blixauro-ppc.com	blixauro.com	Marketing
blixauro-seo.com	blixauro.com	Marketing
blixaurobusiness.com	blixauro.com	Marketing
blixaurodataspace.com	blixauro.com	Marketing
blixauropcpinc.com	blixauro.com	Marketing
zldty07di5.com	blixauro.com	Marketing
bookingpcp.com	booking.com	Travel
bookingppc.com	booking.com	Travel
expediappc.top	expedia.com	Travel
expediaseo.top	expedia.com	Travel
f1ebp8t25j.com	expedia.com	Travel
j816emy69b.top	quantcast.com	Marketing
ooit5xn0l1.top	quantcast.com	Marketing
quant-cast-data.top	quantcast.com	Marketing
quant-cast-pcp.top	quantcast.com	Marketing
quant-cast-ppc.top	quantcast.com	Marketing
quant-cast-seo.top	quantcast.com	Marketing
quantbusinessgp.top	quantcast.com	Marketing
quantcastdatainc.top	quantcast.com	Marketing
quantcastppc.top	quantcast.com	Marketing
quantcastseo.top	quantcast.com	Marketing
quantcastseollic.top	quantcast.com	Marketing
quantdatainc.top	quantcast.com	Marketing
backend.roadrunnerseoinc.top	Road Runner Records	Music
backend.rralbumspromo.top	Road Runner Records	Music
backend.rrmusicalbumspromo.top	Road Runner Records	Music
backend.rrmusicppcspace.top	Road Runner Records	Music
backend.rrmusicpacewebplayer.top	Road Runner Records	Music
backend.rrrecordsclub.com	Road Runner Records	Music
backend.rrrecordsgroupboost.com	Road Runner Records	Music
backend.rrrecordsmusicplayer.com	Road Runner Records	Music

backend.rrrecordsspace.com	Road Runner Records	Music
road-runner-web.top	Road Runner Records	Music
roadrunnermusicSPACE.top	Road Runner Records	Music
roadrunnerseoINC.top	Road Runner Records	Music
rralbumsPROMO.top	Road Runner Records	Music
rrmusicalbumsPROMO.top	Road Runner Records	Music
rrmusicDATAINC.top	Road Runner Records	Music
rrmusicDATASPACE.top	Road Runner Records	Music
rrmusicPPCSpace.top	Road Runner Records	Music
rrmusicPROMOHUB.top	Road Runner Records	Music
rrmusicRECORDSPPC.top	Road Runner Records	Music
rrmusicSPACE.top	Road Runner Records	Music
rrmusicSPACEwebPLAYER.top	Road Runner Records	Music
rrmusicwebPLAYER.top	Road Runner Records	Music
rrrecordsclub.com	Road Runner Records	Music
rrrecordsgroupBOOST.com	Road Runner Records	Music
rrrecordsmusicPLAYER.com	Road Runner Records	Music
rrrecordsspace.com	Road Runner Records	Music
76worh4afo.top	digital-hunch.com	Marketing
digital-hunch-PPC.top	digital-hunch.com	Marketing
digital-hunch-SEO.top	digital-hunch.com	Marketing
rn2j7kne0z.top	thinktandem.io	Marketing
think-tandem-PPC.top	thinktandem.io	Marketing
think-tandem-SEO.top	thinktandem.io	Marketing
269nrl8mvm.top	brandnitions.com	Marketing
brandnitions.top	brandnitions.com	Marketing
brandnitionsDATA.com	brandnitions.com	Marketing
brandnitionsPCP.com	brandnitions.com	Marketing
brandnitionsPPC.top	brandnitions.com	Marketing
brandnitionsSEO.top	brandnitions.com	Marketing
business-omnITail.top	omnITail.net	Marketing

data-omnital.top	omnital.net	Marketing
omnital.top	omnital.net	Marketing
omnitalppc.top	omnital.net	Marketing
omnitalseo.top	omnital.net	Marketing
1ybpcshop.top	Zuchetti	Travel
1ybseomall.top	Zuchetti	Travel
businesslybra.com	Zuchetti	Travel
lybrapromohub.com	Zuchetti	Travel
zzx26cha6b.com	Brenton Way	Marketing
brenton-way-ppc.com	Brenton Way	Marketing
brenton-way-seo.com	Brenton Way	Marketing
wsx3umkwgb.com	Brenton Way	Marketing
8pvsrpd53.com	U production Group	Marketing
uproductiongroupboost.com	U production Group	Marketing
uproductionpromomusic.com	U production Group	Marketing
<u>hyperguestseo.top</u>	HyperGuest	Travel
<u>mbuox3iyzx.top</u>	HyperGuest	Travel
<u>hyperguestppc.top</u>	HyperGuest	Travel
nxnbusinessinc.top	Nexxen	Marketing
work.nexxen.net	Nexxen	Marketing
9bcu6lzmvu.top	Nexxen	Marketing
groupboostwish.top	WISH	
wishppcinc.top	WISH	
w-i-s-h-promohub.top	WISH	
wishdatallc.top	WISH	
8hqbtcaif.top	WISH	
shirudigidata.top	ShiruDigi	Marketing
xrag5tsiov.top	ShiruDigi	Marketing
shirudigiseo.top	ShiruDigi	Marketing
propointppcllc.top		
54kciga7qo.top		
global-propointppcinc.top		

global.propointseoinc.top		
propointseoinc.top		
global.propointppcllc.top		
sound-cloud-dataseo.top	SoundCloud	Music
sound-cloud-business.top	SoundCloud	Music
datasoundcloud.top	SoundCloud	Music
backend.datasoundcloud.top	SoundCloud	Music

## Technical infrastructure

The infrastructure of the scam network is designed using outdated technologies and methodologies. It is evident that the individual responsible for their technology has extensive experience in software development. However, their approach suggests a lack of exposure to the significant technological advancements of the past 15 years. This outdated perspective has also resulted in a complete disregard for operational security (OpSec) best practices, leaving the entire network highly vulnerable to exposure.

The software is developed in Java; however, database statements are concatenated rather than prepared, a practice that was common in the early 2000s but is now considered outdated and insecure. While some passwords are hashed using bcrypt—an algorithm introduced in the late 1990s—others are stored without any encryption or hashing. Additionally, critical credentials, including Alibaba Cloud access keys and Telegram administrative secrets, are not encrypted. Some of these sensitive details are even exposed in the user interface, further compromising security and potentially revealing the identities of those involved in the operation.

The hosting infrastructure is configured in a manner that suggests a lack of technical expertise rather than a deliberate strategy. By adopting modern DevOps practices, the operation could reduce costs by tens of thousands of dollars per month while significantly improving security and performance. The reliance on outdated hosting methods, rarely seen in contemporary systems, results in both excessive expenses and increased vulnerabilities. This combination of inefficiency and poor security measures suggests that those behind the operation are not highly skilled technologists but rather individuals adhering to outdated methodologies.

## Wider Context

In recent months, an increasing number of media outlets have reported on the emergence of Chinese "Scam Factories" that engage in the kidnapping of individuals, holding them captive, and coercing them into perpetrating scams against Western targets. Victims who fail to meet the quotas imposed by their captors face severe punishment and humiliation. Investigative pieces from prominent organizations such as the [BBC](#), [New York Times](#), [CNN](#) have highlighted these operations, featuring interviews with victims and shedding light on the brutal and inhumane conditions within these facilities.

While we cannot definitively link the operation discussed in this report to the "[KK Park](#)" compound in Myanmar—allegedly run by Chinese criminals targeting Westerners through tactics such as "recharge scams"—there are notable similarities between the two, including a direct connection between the Chinese operators and agents in Myanmar.

This report aims to be the first to provide a detailed examination of the technological infrastructure utilized against the victims of these scams, rather than focusing solely on the human trafficking aspect of those forced to execute the scams. By uncovering the underlying infrastructure, we hope to assist future researchers in identifying and exposing similar operations.

## Who we are

Noam Rotem and Ran Locar are members of CyberCyber Labs, a loosely organized group of security researchers who scan the web to find and report data leaks before they can be exploited. Some of our past discoveries include [the personal data of everyone in Ecuador](#), [Biostar2 biometric system](#), [the US domestic drone platform](#) and many others.