

Forum:[Hack Forums](#)

Thread: [Massive Chinese "Task Scam" Syndicate \(Crypto\) - Need Heavy Hitter for Backend](#)

NotJinx - April 26, 2026, 11:29 am

Massive Chinese "Task Scam" Syndicate (Crypto) - Need Heavy Hitter for Backend / DB Dump

What's up HF.

I've been tracking a massive, highly organized Chinese scam syndicate targeting the EU (specifically Spain right now). They run a classic "Task/Order Grabbing" Advanced Fee Fraud, entirely fueled by USDT/ETH. They are pulling in thousands of euros daily from victims.

I'm not asking for someone to hold my hand. I've already done deep recon on their entire infrastructure and successfully popped their live customer service panel.

The Setup (High Level): They run fake remote-job ads on Google leading to landing pages.

Traffic is dynamically routed via IP to specific WhatsApp groups (hundreds of them).

Each group is seeded with ~30 bot accounts pretending to be Spanish workers hyping up the "job". They run it like a meat grinder: they invite 2 real victims at a time into the group. Once those real victims do the tasks and get milked dry, they are immediately kicked out, and the cycle repeats endlessly with new victims.

Victims register on their main fake crypto/exchange platform to do "tasks" that eventually go into negative balance, forcing them to deposit real crypto to clear it. Manual deposits via live chat.

My Breach:

I managed to breach their live chat admin panel. They are using an open-source Go/PHP chat application and they left the default JWT signing key active. I generated a forged admin token, got in, and saw the absolute bloodbath. Thousands stolen, victims' IDs (passports/national IDs) uploaded, manual wallet addresses being dropped.

I was mapping their network, but I got detected and they forced a logout / rotated the secret.

What I Have (The Dossier):

I have compiled a detailed .txt file with: The exact URLs of their entry nodes, chat servers, and backend API.

The exact GitHub repos they cloned their frontend (Vue3) and backend (Java Spring Boot) from.

Proof of the chat breach and the exact tech stack.

What I Need:

I need a heavy hitter who specializes in API exploitation, Spring Boot vulnerabilities, or zero-days for these Chinese open-source frameworks (Yudao/RuoYi). Their frontend encrypts passwords with RSA, but their backend API actually accepts plaintext and throws length errors—their security is

sloppy.

I want someone to pop the backend, dump the DB, and ideally drain the manual wallets they use to collect the USDT.

I am not paying upfront for a "service". I am offering all my intel for a JV/revenge op. If you pop them, you keep the crypto you drain. I just want to see them burn.

PM me if you have the skills to hit a Spring Boot API and want the target dossier (.txt). Don't waste my time if you're a skid.

??????????? - April 26, 2026, 3:12 pm

(Apr 26, 2026 11:29 AM)NotJinx Wrote: [\[CITE\]](#) Massive Chinese "Task Scam" Syndicate (Crypto) - Need Heavy Hitter for Backend / DB Dump

What's up HF.

I've been tracking a massive, highly organized Chinese scam syndicate targeting the EU (specifically Spain right now). They run a classic "Task/Order Grabbing" Advanced Fee Fraud, entirely fueled by USDT/ETH. They are pulling in thousands of euros daily from victims.

I'm not asking for someone to hold my hand. I've already done deep recon on their entire infrastructure and successfully popped their live customer service panel.

The Setup (High Level): They run fake remote-job ads on Google leading to landing pages.

Traffic is dynamically routed via IP to specific WhatsApp groups (hundreds of them).

Each group is seeded with ~30 bot accounts pretending to be Spanish workers hyping up the "job". They run it like a meat grinder: they invite 2 real victims at a time into the group. Once those real victims do the tasks and get milked dry, they are immediately kicked out, and the cycle repeats endlessly with new victims.

Victims register on their main fake crypto/exchange platform to do "tasks" that eventually go into negative balance, forcing them to deposit real crypto to clear it. Manual deposits via live chat.

My Breach:

I managed to breach their live chat admin panel. They are using an open-source Go/PHP chat application and they left the default JWT signing key active. I generated a forged admin token, got in, and saw the absolute bloodbath. Thousands stolen, victims' IDs (passports/national IDs) uploaded, manual wallet addresses being dropped.

I was mapping their network, but I got detected and they forced a logout / rotated the secret.

What I Have (The Dossier):

I have compiled a detailed .txt file with: The exact URLs of their entry nodes, chat servers, and backend API.

The exact GitHub repos they cloned their frontend (Vue3) and backend (Java Spring Boot) from.

Proof of the chat breach and the exact tech stack.

What I Need:

I need a heavy hitter who specializes in API exploitation, Spring Boot vulnerabilities, or zero-days for these Chinese open-source frameworks (Yudao/RuoYi). Their frontend encrypts passwords with RSA, but their backend API actually accepts plaintext and throws length errors—their security is sloppy.

I want someone to pop the backend, dump the DB, and ideally drain the manual wallets they use to collect the USDT.

I am not paying upfront for a "service". I am offering all my intel for a JV/revenge op. If you pop them, you keep the crypto you drain. I just want to see them burn.

PM me if you have the skills to hit a Spring Boot API and want the target dossier (.txt). Don't waste my time if you're a skid.

Please connect on convo.

DramaKing - April 26, 2026, 3:47 pm

(Apr 26, 2026 11:29 AM)NotJinx Wrote: [\[CITE\]](#) Massive Chinese "Task Scam" Syndicate (Crypto) - Need Heavy Hitter for Backend / DB Dump

What's up HF.

I've been tracking a massive, highly organized Chinese scam syndicate targeting the EU (specifically Spain right now). They run a classic "Task/Order Grabbing" Advanced Fee Fraud, entirely fueled by USDT/ETH. They are pulling in thousands of euros daily from victims.

I'm not asking for someone to hold my hand. I've already done deep recon on their entire infrastructure and successfully popped their live customer service panel.

The Setup (High Level): They run fake remote-job ads on Google leading to landing pages.

Traffic is dynamically routed via IP to specific WhatsApp groups (hundreds of them).

Each group is seeded with ~30 bot accounts pretending to be Spanish workers hyping up the "job". They run it like a meat grinder: they invite 2 real victims at a time into the group. Once those real victims do the tasks and get milked dry, they are immediately kicked out, and the cycle repeats endlessly with new victims.

Victims register on their main fake crypto/exchange platform to do "tasks" that eventually go into negative balance, forcing them to deposit real crypto to clear it. Manual deposits via live chat.

My Breach:

I managed to breach their live chat admin panel. They are using an open-source Go/PHP chat application and they left the default JWT signing key active. I generated a forged admin token, got in, and saw the absolute bloodbath. Thousands stolen, victims' IDs (passports/national IDs) uploaded, manual wallet addresses being dropped.

I was mapping their network, but I got detected and they forced a logout / rotated the secret.

What I Have (The Dossier):

I have compiled a detailed .txt file with: The exact URLs of their entry nodes, chat servers, and backend API.

The exact GitHub repos they cloned their frontend (Vue3) and backend (Java Spring Boot) from.

Proof of the chat breach and the exact tech stack.

What I Need:

I need a heavy hitter who specializes in API exploitation, Spring Boot vulnerabilities, or zero-days for these Chinese open-source frameworks (Yudao/RuoYi). Their frontend encrypts passwords with RSA, but their backend API actually accepts plaintext and throws length errors—their security is sloppy.

I want someone to pop the backend, dump the DB, and ideally drain the manual wallets they use to collect the USDT.

I am not paying upfront for a "service". I am offering all my intel for a JV/revenge op. If you pop them, you keep the crypto you drain. I just want to see them burn.

PM me if you have the skills to hit a Spring Boot API and want the target dossier (.txt). Don't waste my time if you're a skid.

Now I am all for hitting back at scammers and taking their ill-gotten gain. I do suggest, however, filing a report with IC3 or other relevant agency on behalf of the victims. If they harden their infrastructure, maybe international authorities can track them down. The CCP doesn't deal nicely to unsanctioned cybercriminals.

ghhcchuffu - April 29, 2026, 4:47 am

Hello I'm on telegram and inside of massive Chinese scam compound crypto groups where they keep guides and stuff dm me I can try help you

faustussss - May 29, 2026, 10:54 am

I'm interested in learning more too

SIM-5783202 - September 8, 2026, 12:45 am

Hey interested in this let's see what I can do

los911 - September 25, 2026, 11:33 pm

Sorry to bump and old thread. This gave me PTSD as I got fucked by the exact same Chinese romance scam back in May last year <https://hackforums.net/showthread.php?tid=6296482>

Have a read

Did you have any luck?

Anvilpoint - September 27, 2026, 9:55 pm

At Anvilpoint we offer professional hacker-for-hire solutions. We'd be happy to assist you in this matter. You can view our posting [here](#).

Lefty - September 28, 2026, 5:09 am

That is actually insane, thanks for the heads up!