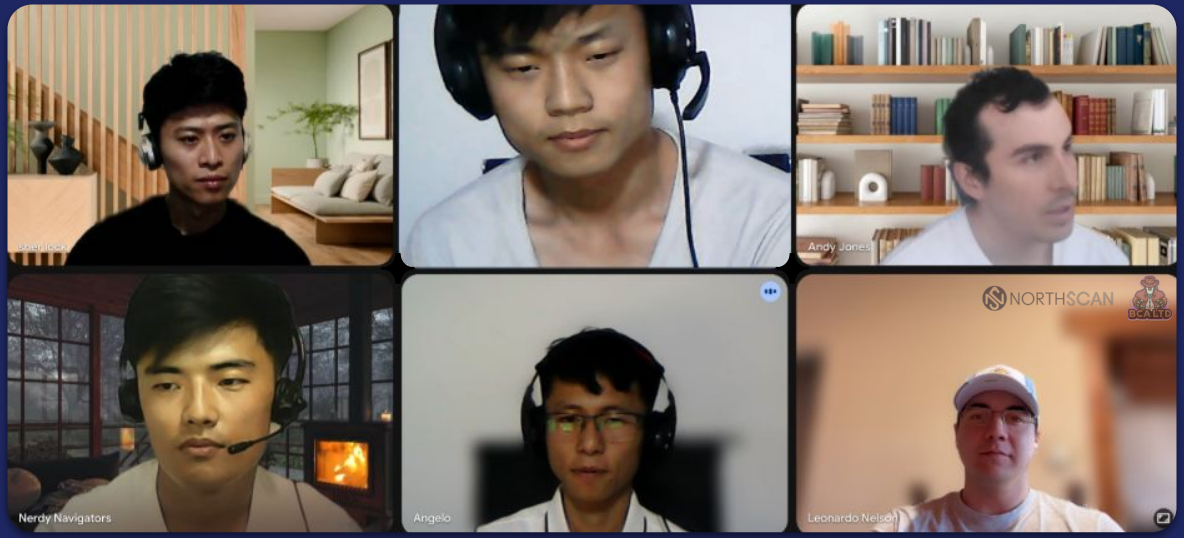
# SMILE, YOU'RE ON CAMERA!

A Live Stream from Inside Lazarus' IT Workers Scheme




*An investigation by BCA LTD, NorthScan & ANY.RUN*

# About Us

## Heiner García Pérez 🇨🇴

**Researcher & Strategic intelligence Analyst**

Founder of **NorthScan**

Cyber Threat Intelligence - **Telefonica Tech**

Intelligence Contributor **- Security Alliance (SEAL)**

# About Us


## Mauro Eldritch 🇦🇷

**Hacker & Speaker**.

Founder **BCA LTD** (@BirminghamCyber) & **DC5411**.

Leader @ **Bitso Quetzal Team**.

Spoke at **DEF CON** (x15), **Hacker Halted** and 60+ events.

*I cyberbully Threat Actors for a living.*

# About Famous Chollima

## A Division of Lazarus APT 🇰🇵

- Seek jobs in Western companies posing as developers & engineers
- Primary targets: Finance, Crypto/Web3, Healthcare sectors
- They rely on Western cooperators (aware or not)
- They use fake IDs, establish shell companies and abuse H1B visas

## Objectives

- Corporate Espionage & Intellectual Property Theft
- Revenue generation for the sanctioned DPRK regime
- Financing the ballistic missile programme

CROWDSTRIKE

# The IT Workers Scheme

## OPTION 1

**20%**

Salary Cut

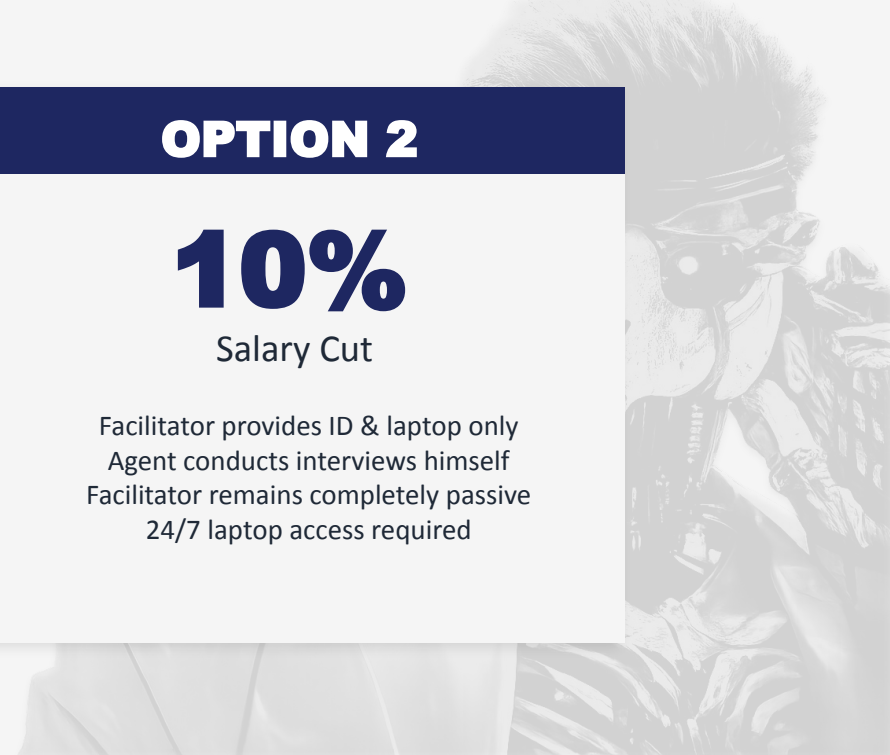
A facilitator acts as the frontman
Has to attend all interviews
Handles daily stand-ups
Lazarus agents act as ghost developers

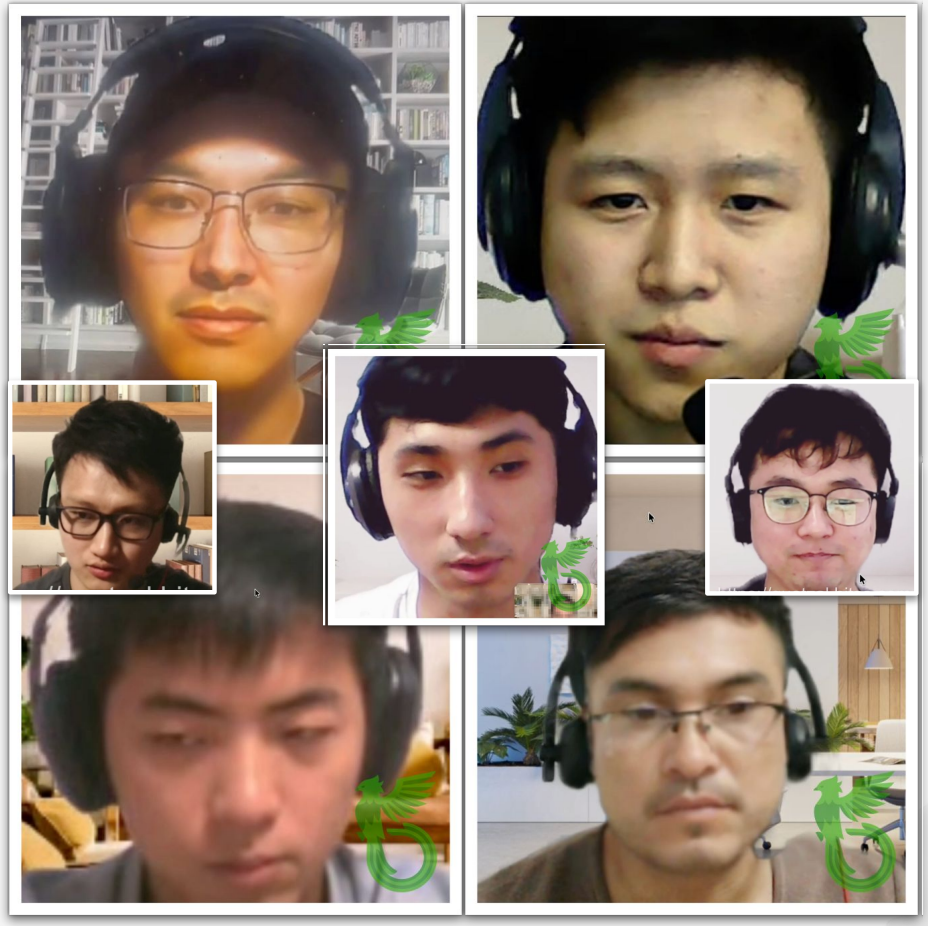
## OPTION 2

**10%**

Salary Cut

Facilitator provides ID & laptop only
Agent conducts interviews himself
Facilitator remains completely passive
24/7 laptop access required





# Interview with the Chollima

> Bitso Quetzal Team


## Smile, You’re on Camera!

> ANY RUN, NorthScan, BCA LTD

# About this talk

## Novel Investigation

First-ever **real-time** documentation of North Korean IT worker infiltration operations from the inside.

## Controlled Environment

Extended ANY.RUN sandboxes captured every click, file action, and network request in real-time.

## Raising the stakes

During the first chapter we posed as facilitators. Now, we're posing as an attractive DeFi company!

NORTHSCAN ANY.RUN BCA LTD

# Tape A: “Hello DEF CON”

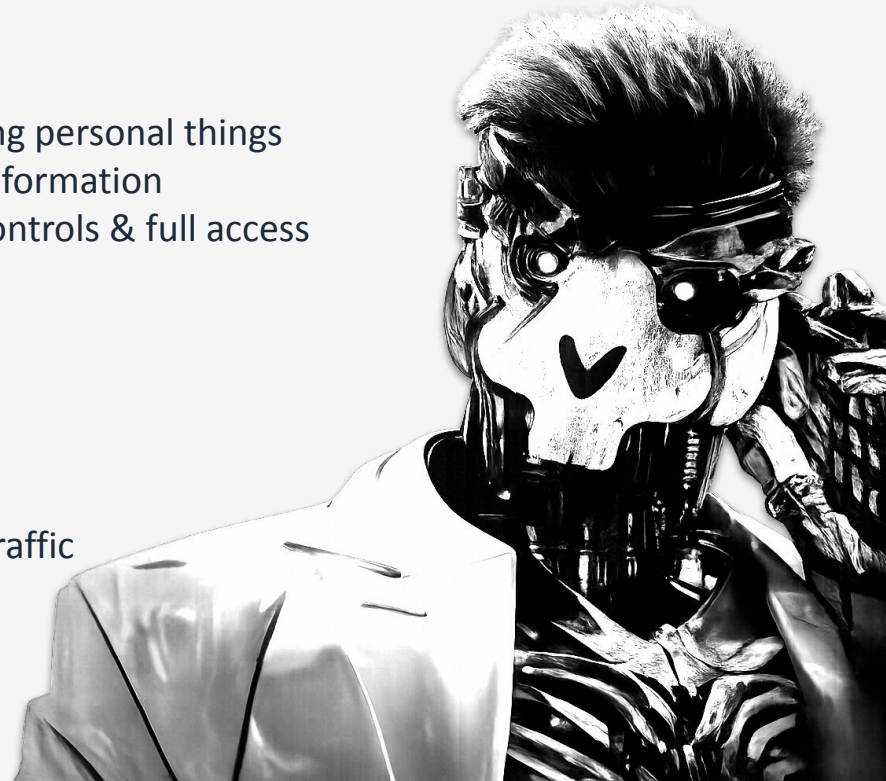
# Our approach

## Stage 1: Infiltration (NorthScan)

- Recruiting a DPRK cluster into our DeFi company
- Conducting friendly and relaxed interviews and asking personal things
- Drafting contracts and requesting IDs and Banking Information
- Create a sense of a trust-based workplace with no controls & full access
    - And of course, lots of money

## Stage 2: Containment (BCA LTD & ANY.RUN)

- Set up a simulated VDI farm in ANY.RUN sandboxes
- Recorded activity in real time: clicks, files, network traffic
- Analyzed toolchain and TTPs
- Real-time intelligence gathering



# The recruiter: Andy Jones

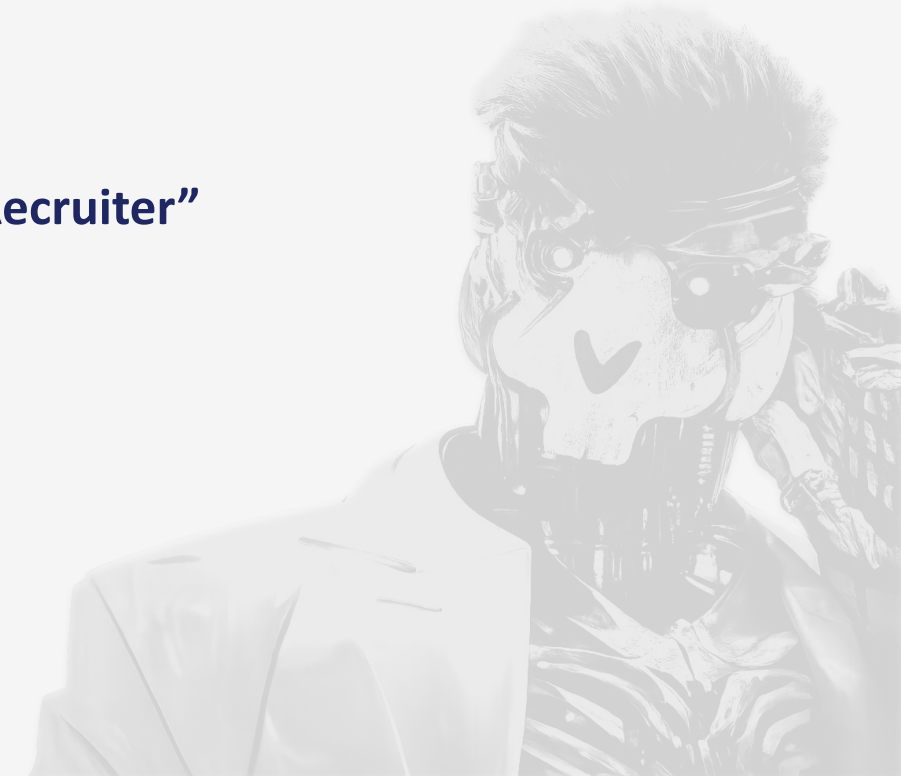
## Identity Selection

- A developer previously contacted by DPRK agents: Andy Jones (*See Ep. 1*)
- Reinforced the image of a U.S.-based developer willing to assist them

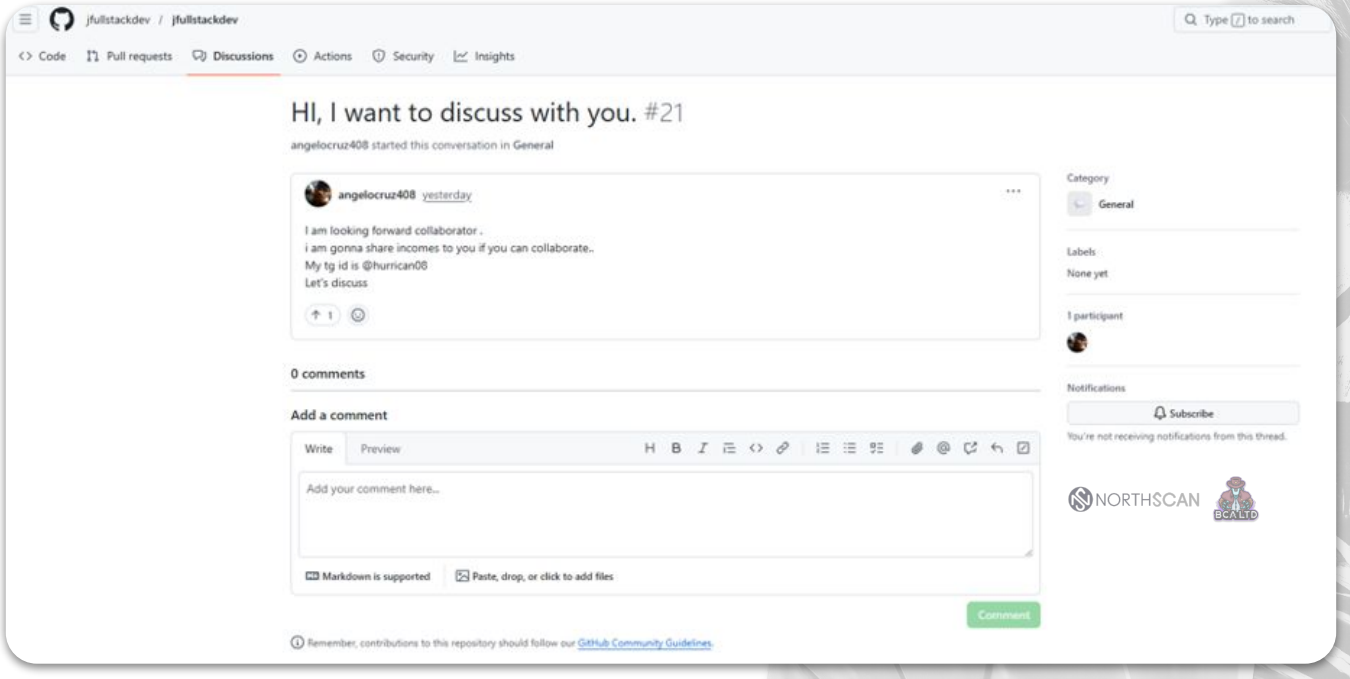
## Building Trust Strategy

- Introduced the first DPRK IT Worker to “a friend’s DeFi company”
- As a new startup, they could secure privileged positions early
- Trust-based environment, so we asked them to bring “friends”
- Of course, all friends were other DPRK IT Workers

# Tape B: “The Recruiter”



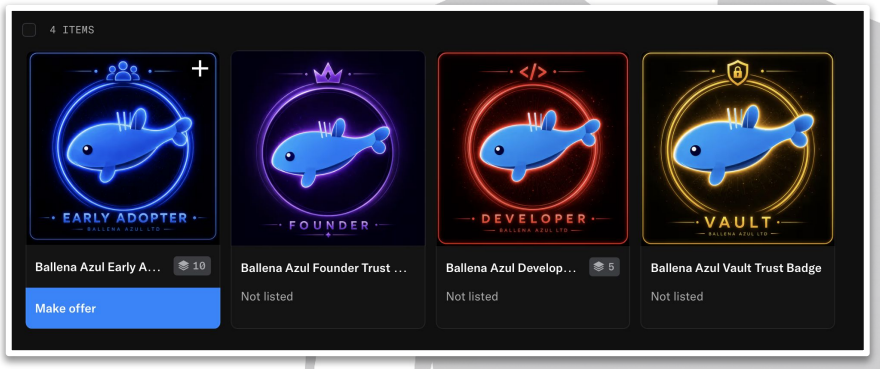
# The Recruiter: Angelo Cruz



# The Recruiter: Angelo Cruz


# The Company: Ballena Azul LTD





# The Company: Ballena Azul LTD

## BALLENA AZUL LTD

Company number **13407189**

Follow this company

Overview | Filing history | People | More

Officers | Persons with significant control

**Filter officers**

Current officers

**1 officer / 0 resignations**

**COSITORTO, Leonardo Nelson**

Correspondence address
**4 Orsett Terrace, London, England, W2 6AZ**

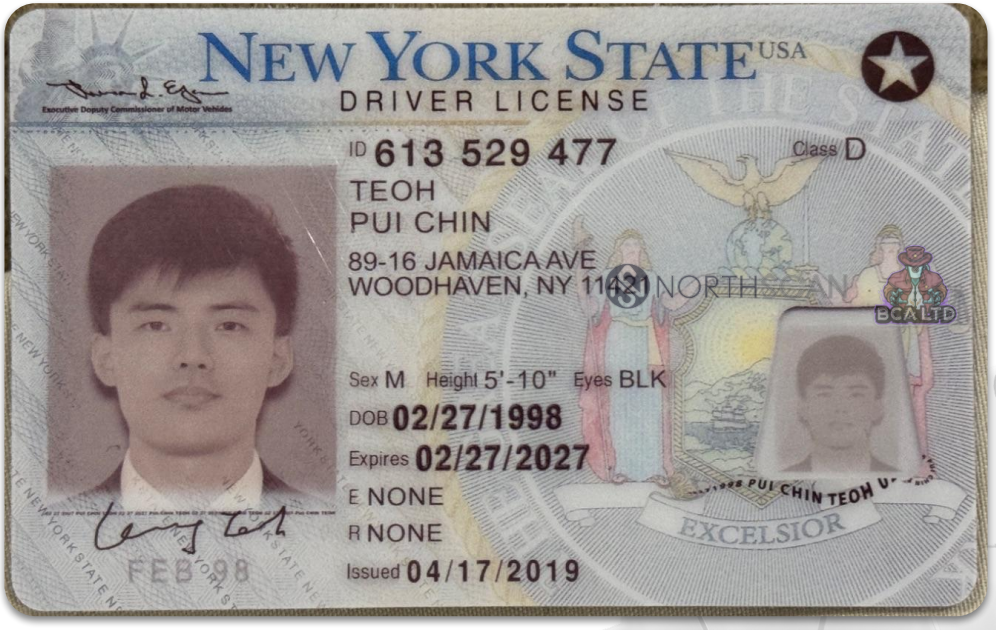
| Role | Date of birth | Appointed on |
|---|---|---|
| **Director** | **April 1970** | **18 May 2021** |

| Nationality | Country of residence |
|---|---|
| **Argentine** | **England** |


# The Developers: Angelo

# The Developers: Jack

# The Developers: Lucas

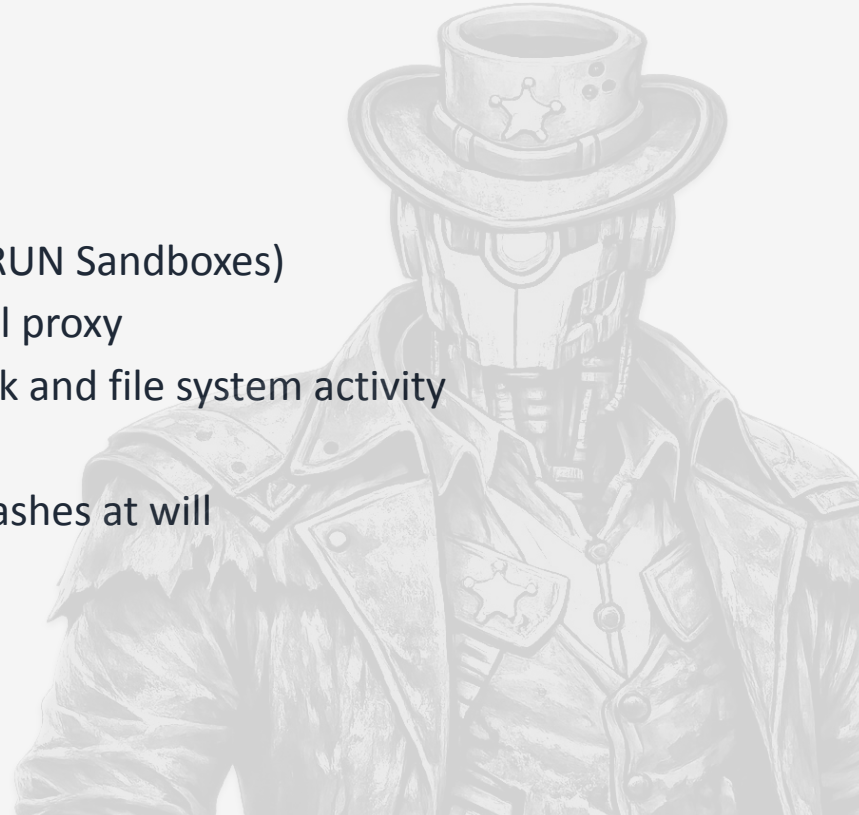


# Tape C: “Meet & Greet”

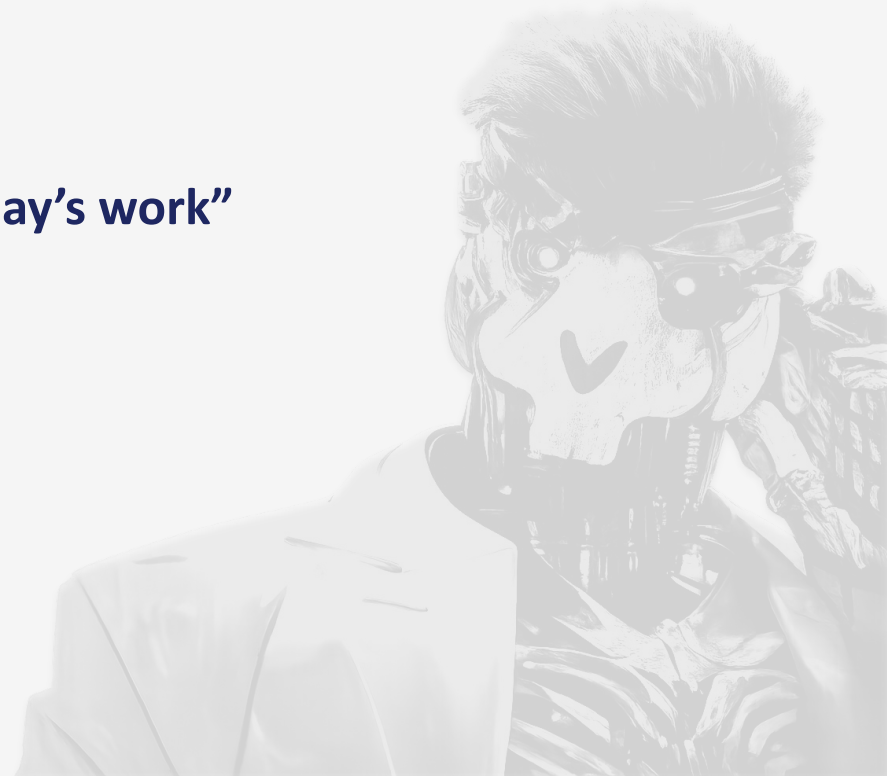
# Sandboxes & Chollimas

## Infrastructure & Control Setup

- Created fake Windows 10/11 “VDIs” (ANY RUN Sandboxes)
- Sandboxes routed through a U.S. residential proxy
- Full real-time monitoring of screen, network and file system activity
- All activity is recorded on video
- Ability to cut internet access or simulate crashes at will



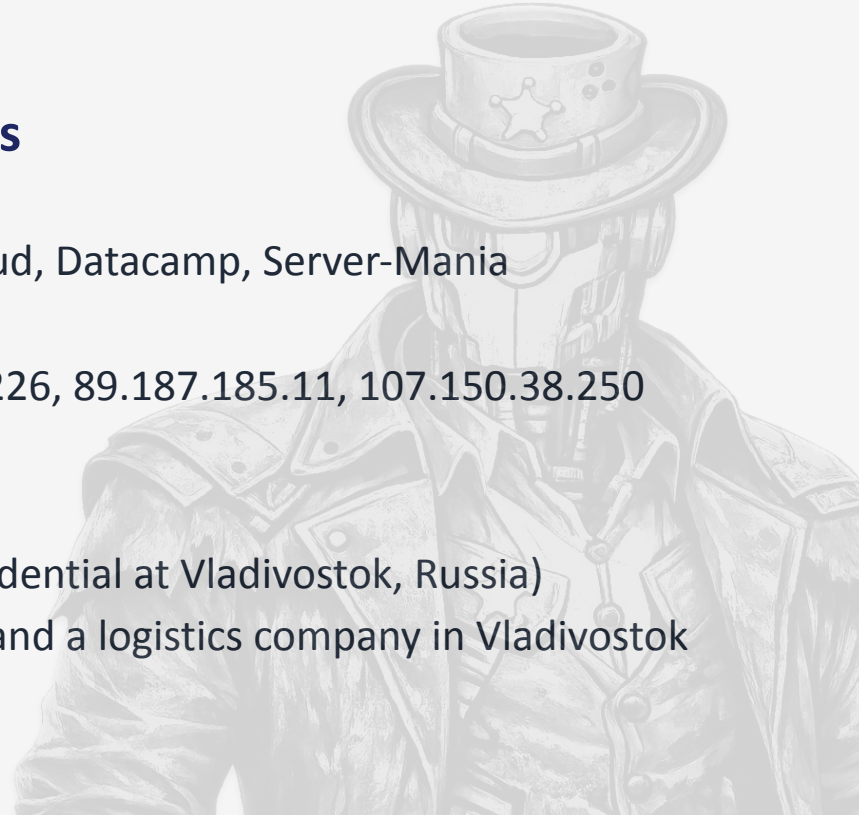
# Tape D: “A hard day’s work”



# Sandboxes & Chollimas

## IP Addresses: VPN, VPS and OPSec Fails

- **Observed VPS**: Gorilla Servers, Alibaba Cloud, Datacamp, Server-Mania
- **VPN nodes**: 104.250.148.58, 192.200.115.226, 89.187.185.11, 107.150.38.250 (AstrillVPN)
- **An interesting finding**: 62.33.223.165 (Residential at Vladivostok, Russia)
  - We identified an associated “owner” and a logistics company in Vladivostok



RESIDENTIAL

CANARY TOKENS


## Your Canarytoken was triggered

**Slow redirect** Canarytoken has been triggered by the Source IP
**62.33.223.165**

Reminder
DPRK - Slow Redirect I (Ballena Azul Website)

Source IP
62.33.223.165

Date
2026/05/27

Time
20:09 UTC

User agent
Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/148.0.0.0 Safari/537.36

ASTRILL VPN

CANARY TOKENS


## Your Canarytoken was triggered

**Slow redirect** Canarytoken has been triggered by the Source IP
**192.200.115.226**

Reminder
DPRK - Slow Redirect I (Ballena Azul Website)

Source IP
192.200.115.226

Date
2026/06/19

Time
13:42 UTC

User agent
Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/149.0.0.0 Safari/537.36

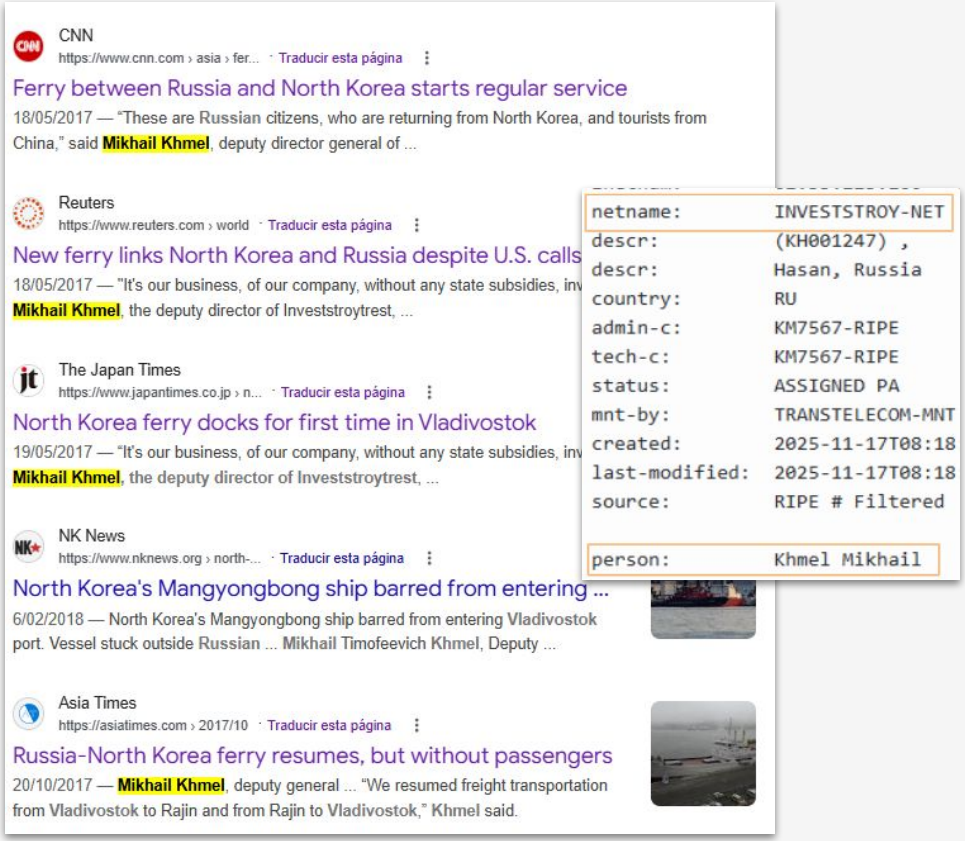
```
inetnum:        62.33.223.160 - 62.33.223.175
netname:        INVESTSTROY-NET
descr:          (KH001247) ,
descr:          Hasan, Russia
country:        RU
admin-c:        KM7567-RIPE
tech-c:         KM7567-RIPE
status:         ASSIGNED PA
mnt-by:         TRANSTELECOM-MNT
created:        2025-11-17T08:18:39Z
last-modified:  2025-11-17T08:18:39Z
source:         RIPE # Filtered

person:         Khmel Mikhail
address:        Vladivostok Russia
phone:          +7 423 2496560
nic-hdl:        KM7567-RIPE
mnt-by:         Mikhail_Kmel-1
created:        2017-09-15T01:53:10Z
last-modified:  2017-09-15T01:53:10Z
source:         RIPE
```

| PID | Process name | CN | IP | Port | Domain | ASN |
|---|---|---|---|---|---|---|
| 8060 | AnyDesk.exe | | 62.33.223.165 | 7070 | – | TRANSTELECOM Moscow, Russia |
| 8060 | AnyDesk.exe | | 62.33.223.165 | 60289 | – | TRANSTELECOM Moscow, Russia |

FirmsData.ru
https://firmsdata.ru vladivostok

**Услуги экспедирования грузов. Найдено 466 компаний в ...**

+74[redacted]96560. Топ-логистик на карте Владивостока. Топ-логистик. Компания грузоперевозок. ул. Фонтанная, 40. +79510275743. Habway на карте Владивостока. Habway.



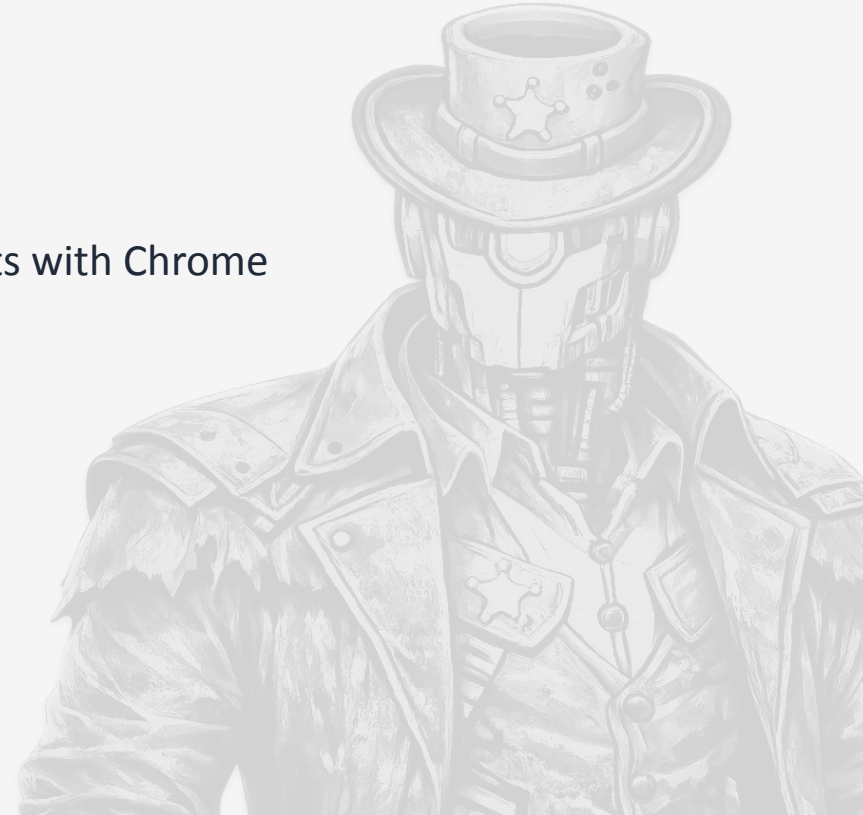

- **Mikhail Khmel** is a representative of **InvestStroyTrest**, a Russian company historically involved in operating a ferry service between Rajin/Rason, North Korea, and **Vladivostok**, Russia

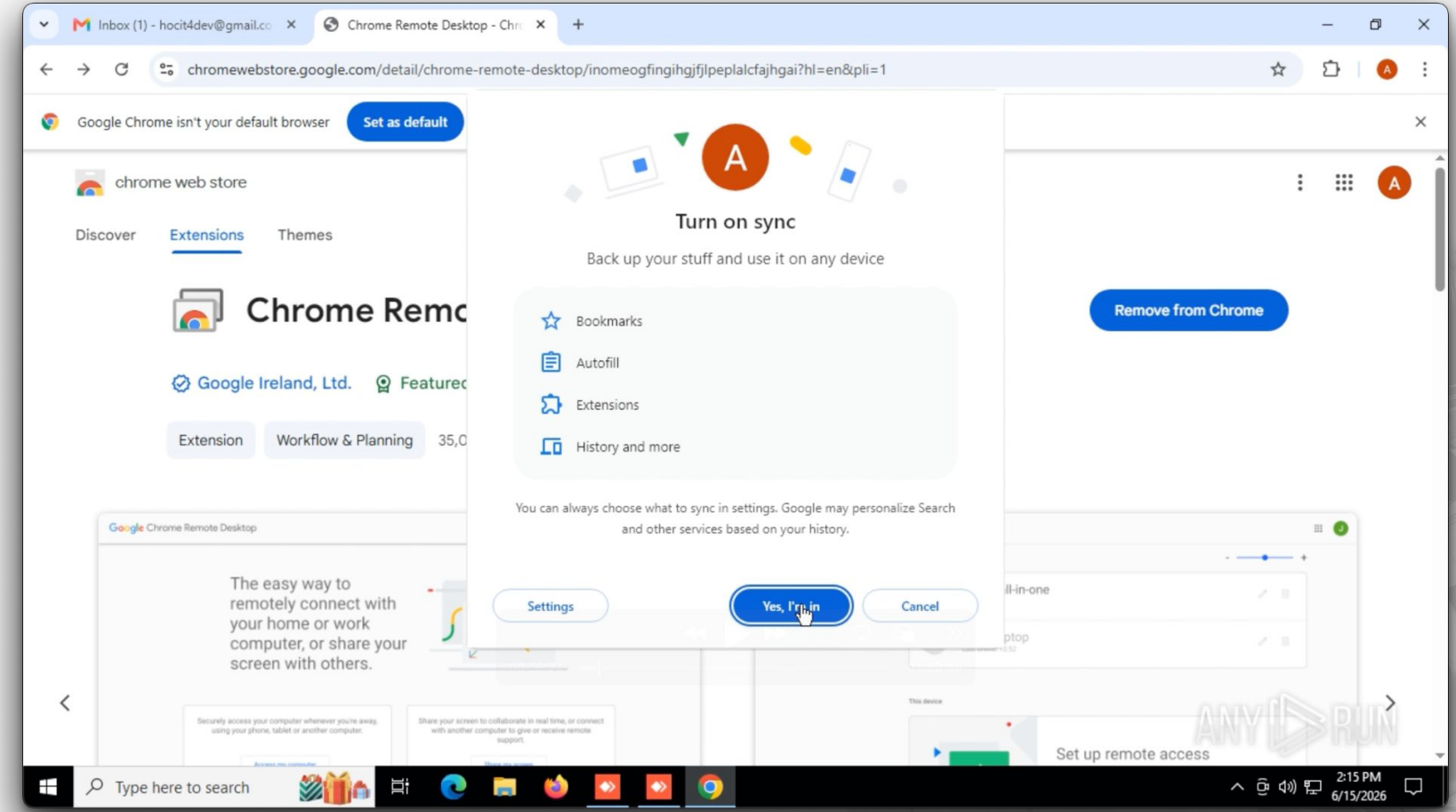
- Multiple independent sources have since associated **InvestStroyTrest linked** or **TransTeleCom** assigned infrastructure with North Korean internet connectivity, DPRK IT-worker operations, and **DPRK aligned cyber activity**.

# Sandboxes & Chollimas

## Google Sync

- The operators synced their Google Accounts with Chrome
- This allowed us to access their data.
  - Web Search History
  - Accounts and Passwords
  - Installed Extensions

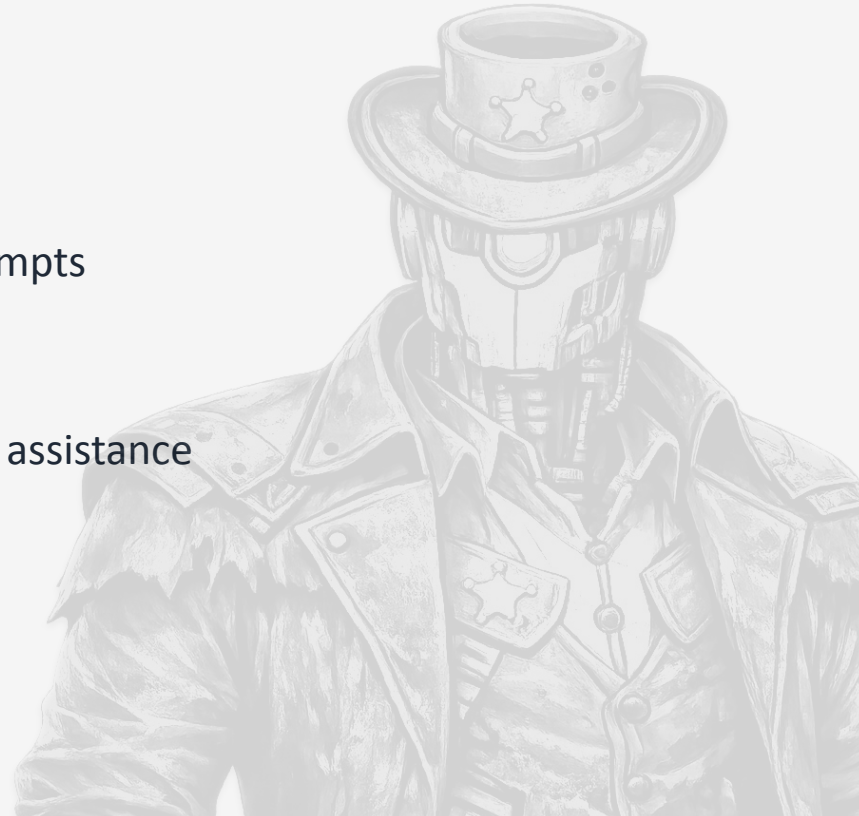



Inbox (1) - hocit4dev@gmail.co
Chrome Remote Desktop - Chr
chromewebstore.google.com/detail/chrome-remote-desktop/inomeogfingihgjfjlpeplalcfajhgai?hl=en&pli=1
Google Chrome isn't your default browser
Set as default
chrome web store
Discover
Extensions
Themes
Chrome Remo
Google Ireland, Ltd.
Featured
Extension
Workflow & Planning
Turn on sync
Back up your stuff and use it on any device
Bookmarks
Autofill
Extensions
History and more
You can always choose what to sync in settings. Google may personalize Search and other services based on your history.
Settings
Yes, I'm in
Cancel
Remove from Chrome
Google Chrome Remote Desktop
The easy way to remotely connect with your home or work computer, or share your screen with others.
Set up remote access
Type here to search
2:15 PM
6/15/2026

# Famous Chollima Toolkit

## AI Powered Job Seeking Tools

- Saved Prompts for GPT: Bookmark LLM prompts
- Simplify Copilot: Autofill job applications
- AIApply: Automate job seeking workflows
- Final Round AI: Real-time interview answer assistance



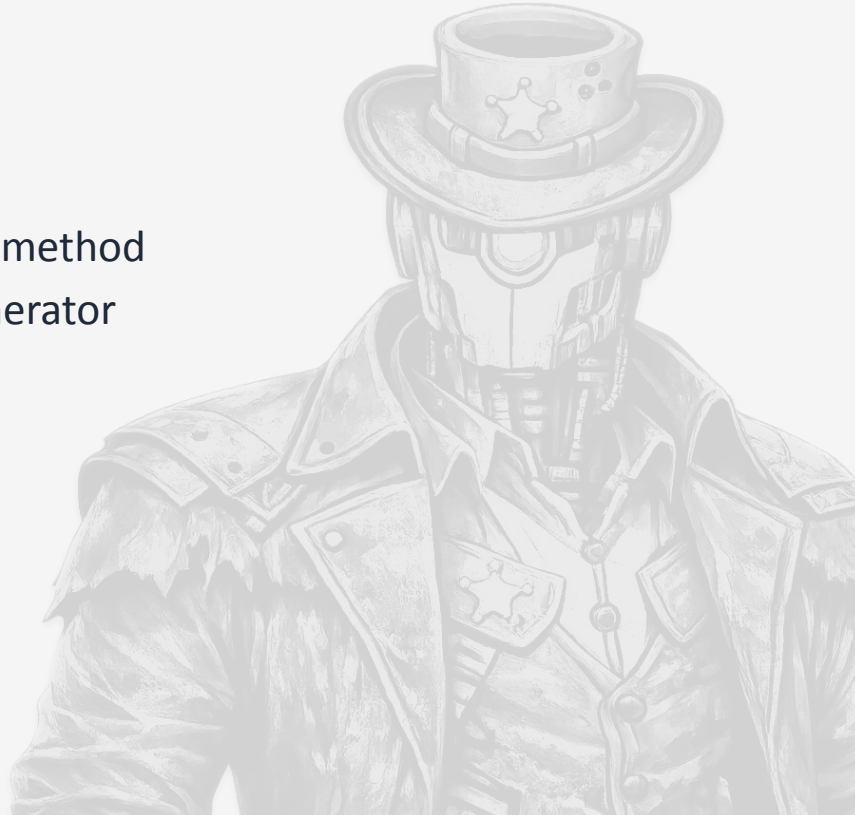
# Famous Chollima Toolkit

## Security & Access Tools

- AnyDesk: Primary remote desktop tool
- Google Remote Desktop: Secondary access method
- OTP.ee / Authenticator.cc & 2fa.cn: OTP generator
- Astrill VPN: Preferred VPN service

## System tools

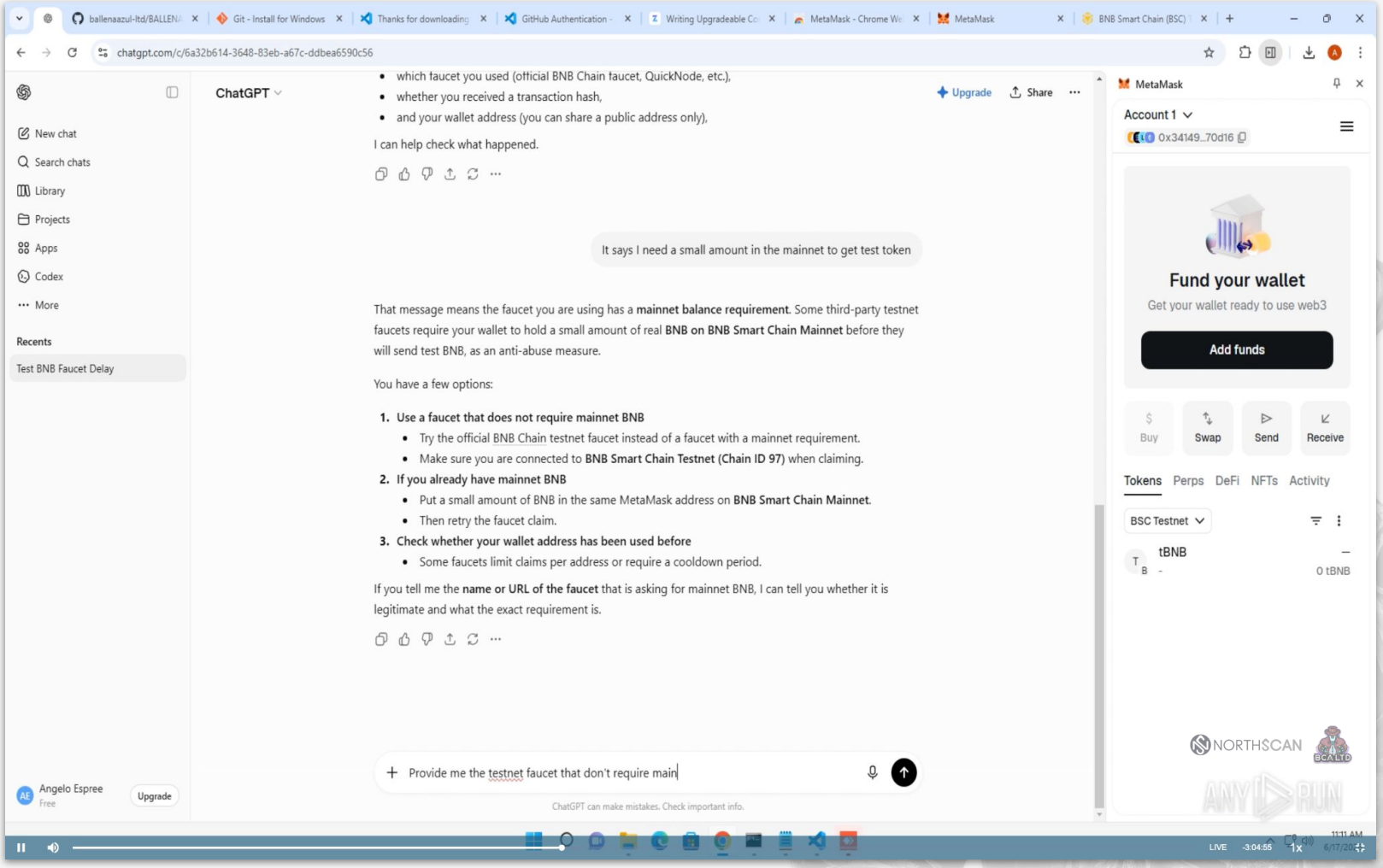
- sysinfo, dxdiag
- wmic

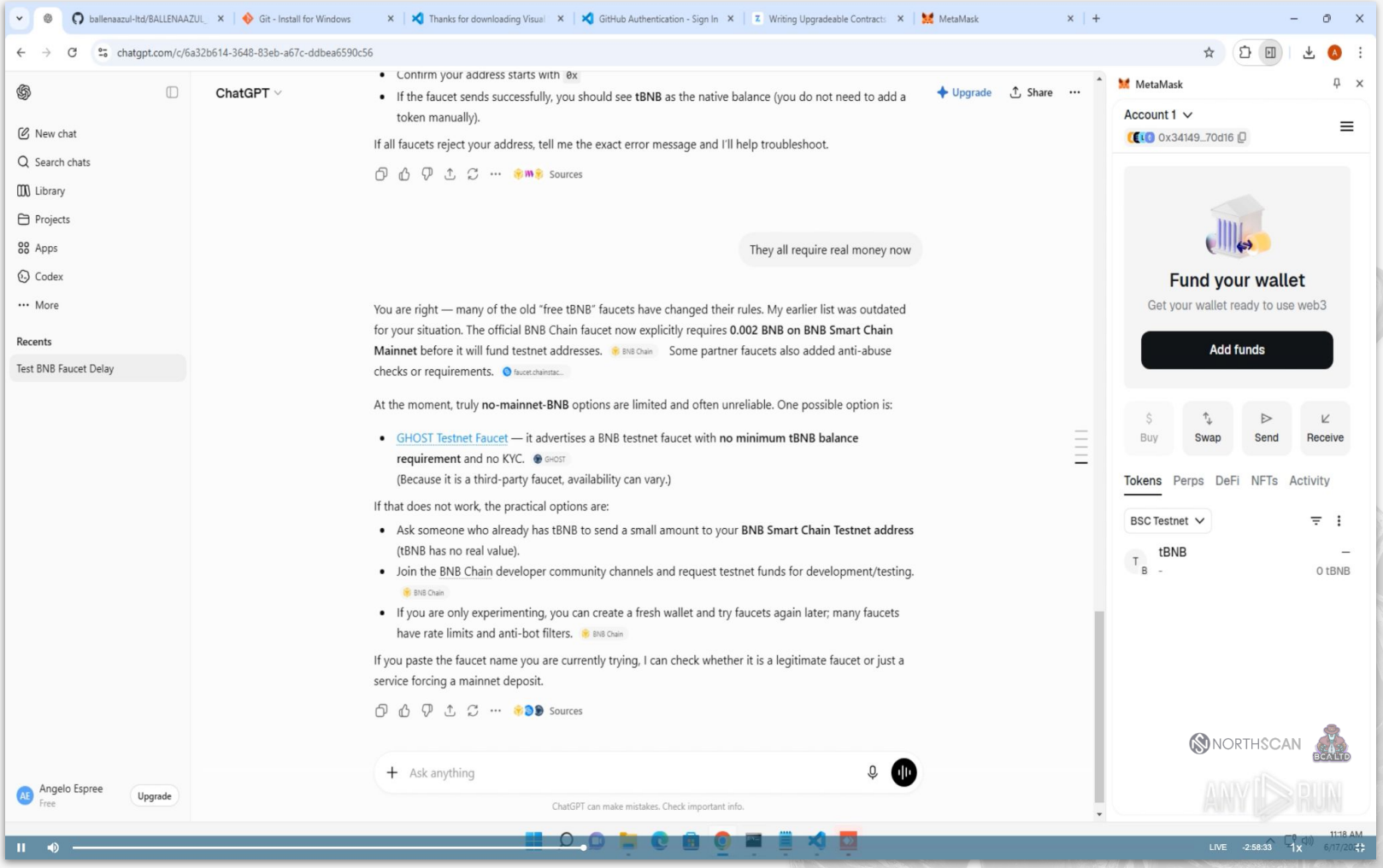


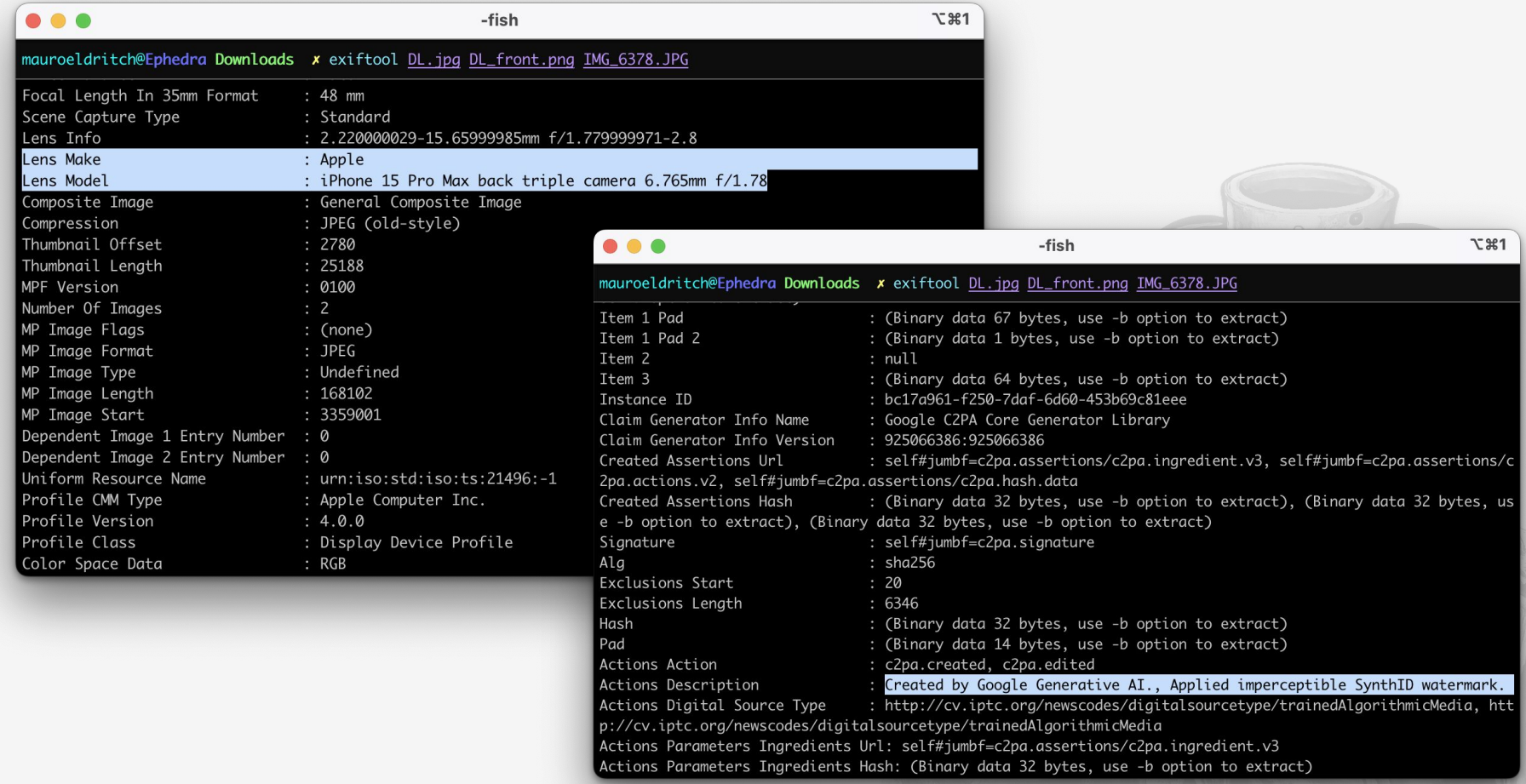
# Famous Chollima Toolkit

## Other legit services and platforms abused

- Cursor, Visual Studio Code, Remix
- ChatGPT, Google Gemini
- MetaMask, OpenSea
- ip8.com
- Github
- Chrome Remote Desktop


ballenaazul-ltd/BALLENA
Git - Install for Windows
Thanks for downloading
GitHub Authentication -
Writing Upgradeable Co
MetaMask - Chrome We
MetaMask
BNB Smart Chain (BSC)
chatgpt.com/c/6a32b614-3648-83eb-a67c-ddbea6590c56
ChatGPT
Upgrade
Share
New chat
Search chats
Library
Projects
Apps
Codex
More
Recents
Test BNB Faucet Delay
Angelo Espree
Free
Upgrade
which faucet you used (official BNB Chain faucet, QuickNode, etc.),
whether you received a transaction hash,
and your wallet address (you can share a public address only),
I can help check what happened.
It says I need a small amount in the mainnet to get test token
That message means the faucet you are using has a mainnet balance requirement. Some third-party testnet faucets require your wallet to hold a small amount of real BNB on BNB Smart Chain Mainnet before they will send test BNB, as an anti-abuse measure.
You have a few options:
1. Use a faucet that does not require mainnet BNB
Try the official BNB Chain testnet faucet instead of a faucet with a mainnet requirement.
Make sure you are connected to BNB Smart Chain Testnet (Chain ID 97) when claiming.
2. If you already have mainnet BNB
Put a small amount of BNB in the same MetaMask address on BNB Smart Chain Mainnet.
Then retry the faucet claim.
3. Check whether your wallet address has been used before
Some faucets limit claims per address or require a cooldown period.
If you tell me the name or URL of the faucet that is asking for mainnet BNB, I can tell you whether it is legitimate and what the exact requirement is.
Provide me the testnet faucet that don't require main
ChatGPT can make mistakes. Check important info.
MetaMask
Account 1
0x34149...70d16
Fund your wallet
Get your wallet ready to use web3
Add funds
Buy
Swap
Send
Receive
Tokens
Perps
DeFi
NFTs
Activity
BSC Testnet
tBNB
0 tBNB
NORTHSCAN
BCALTO
ANY.RUN
LIVE
-3:04:55
1x
11:11 AM
6/17/2026


ballenaazul-ltd/BALLENAAZUL_
Git - Install for Windows
Thanks for downloading Visual
GitHub Authentication - Sign In
Writing Upgradeable Contracts
MetaMask
chatgpt.com/c/6a32b614-3648-83eb-a67c-ddbea6590c56
ChatGPT
Upgrade
Share
New chat
Search chats
Library
Projects
Apps
Codex
More
Recents
Test BNB Faucet Delay
Angelo Espree
Free
Upgrade
Confirm your address starts with 0x
If the faucet sends successfully, you should see tBNB as the native balance (you do not need to add a token manually).
If all faucets reject your address, tell me the exact error message and I'll help troubleshoot.
Sources
They all require real money now
You are right — many of the old "free tBNB" faucets have changed their rules. My earlier list was outdated for your situation. The official BNB Chain faucet now explicitly requires 0.002 BNB on BNB Smart Chain Mainnet before it will fund testnet addresses. BNB Chain Some partner faucets also added anti-abuse checks or requirements. faucet.chainstac...
At the moment, truly no-mainnet-BNB options are limited and often unreliable. One possible option is:
GHOST Testnet Faucet — it advertises a BNB testnet faucet with no minimum tBNB balance requirement and no KYC. GHOST
(Because it is a third-party faucet, availability can vary.)
If that does not work, the practical options are:
Ask someone who already has tBNB to send a small amount to your BNB Smart Chain Testnet address (tBNB has no real value).
Join the BNB Chain developer community channels and request testnet funds for development/testing. BNB Chain
If you are only experimenting, you can create a fresh wallet and try faucets again later; many faucets have rate limits and anti-bot filters. BNB Chain
If you paste the faucet name you are currently trying, I can check whether it is a legitimate faucet or just a service forcing a mainnet deposit.
Sources
Ask anything
ChatGPT can make mistakes. Check important info.
MetaMask
Account 1
0x34149...70d16
Fund your wallet
Get your wallet ready to use web3
Add funds
Buy
Swap
Send
Receive
Tokens
Perps
DeFi
NFTs
Activity
BSC Testnet
tBNB
0 tBNB
NORTHSCAN
BCALTD
ANY.RUN
LIVE
-2:58:33
1x
11:18 AM
6/17/20


-fish
⌥⌘1
mauroeldritch@Ephedra Downloads ✗ exiftool DL.jpg DL_front.png IMG_6378.JPG
Focal Length In 35mm Format : 48 mm
Scene Capture Type : Standard
Lens Info : 2.220000029-15.65999985mm f/1.779999971-2.8
Lens Make : Apple
Lens Model : iPhone 15 Pro Max back triple camera 6.765mm f/1.78
Composite Image : General Composite Image
Compression : JPEG (old-style)
Thumbnail Offset : 2780
Thumbnail Length : 25188
MPF Version : 0100
Number Of Images : 2
MP Image Flags : (none)
MP Image Format : JPEG
MP Image Type : Undefined
MP Image Length : 168102
MP Image Start : 3359001
Dependent Image 1 Entry Number : 0
Dependent Image 2 Entry Number : 0
Uniform Resource Name : urn:iso:std:iso:ts:21496:-1
Profile CMM Type : Apple Computer Inc.
Profile Version : 4.0.0
Profile Class : Display Device Profile
Color Space Data : RGB
-fish
⌥⌘1
mauroeldritch@Ephedra Downloads ✗ exiftool DL.jpg DL_front.png IMG_6378.JPG
Item 1 Pad : (Binary data 67 bytes, use -b option to extract)
Item 1 Pad 2 : (Binary data 1 bytes, use -b option to extract)
Item 2 : null
Item 3 : (Binary data 64 bytes, use -b option to extract)
Instance ID : bc17a961-f250-7daf-6d60-453b69c81eee
Claim Generator Info Name : Google C2PA Core Generator Library
Claim Generator Info Version : 925066386:925066386
Created Assertions Url : self#jumbf=c2pa.assertions/c2pa.ingredient.v3, self#jumbf=c2pa.assertions/c2pa.actions.v2, self#jumbf=c2pa.assertions/c2pa.hash.data
Created Assertions Hash : (Binary data 32 bytes, use -b option to extract), (Binary data 32 bytes, use -b option to extract), (Binary data 32 bytes, use -b option to extract)
Signature : self#jumbf=c2pa.signature
Alg : sha256
Exclusions Start : 20
Exclusions Length : 6346
Hash : (Binary data 32 bytes, use -b option to extract)
Pad : (Binary data 14 bytes, use -b option to extract)
Actions Action : c2pa.created, c2pa.edited
Actions Description : Created by Google Generative AI., Applied imperceptible SynthID watermark.
Actions Digital Source Type : http://cv.iptc.org/newscodes/digitalsourcetype/trainedAlgorithmicMedia, http://cv.iptc.org/newscodes/digitalsourcetype/trainedAlgorithmicMedia
Actions Parameters Ingredients Url: self#jumbf=c2pa.assertions/c2pa.ingredient.v3
Actions Parameters Ingredients Hash: (Binary data 32 bytes, use -b option to extract)

# Framing Chollimas

## Looking for investors

- We needed more multimedia evidence
- So we set up a call with a “VC interested in our company”

- Turns out, that VC was actually **Yohan Yun**
  - A recognized journalist from **Cointelegraph**!

# Tape E: “Imposters”

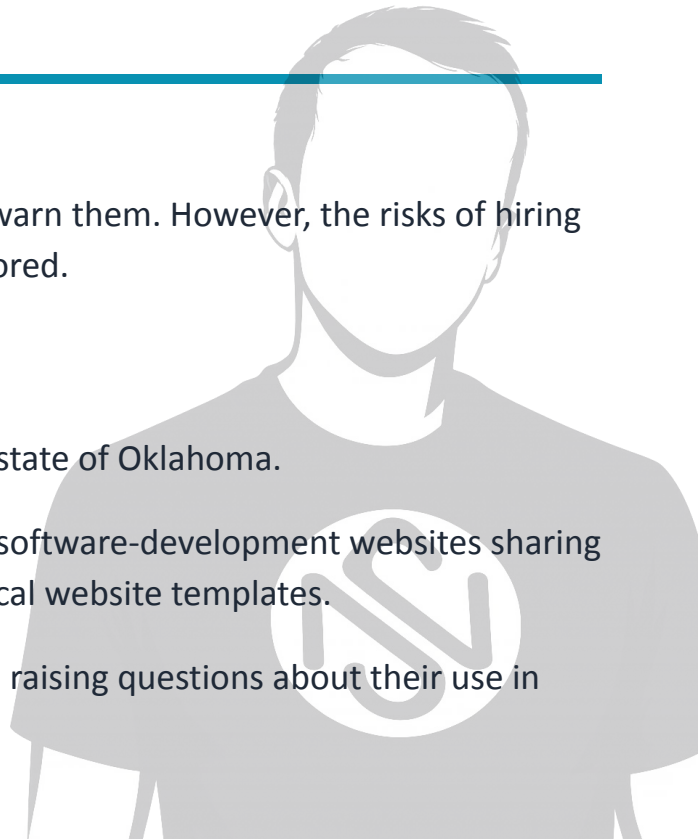
# Beyond the hunting grounds

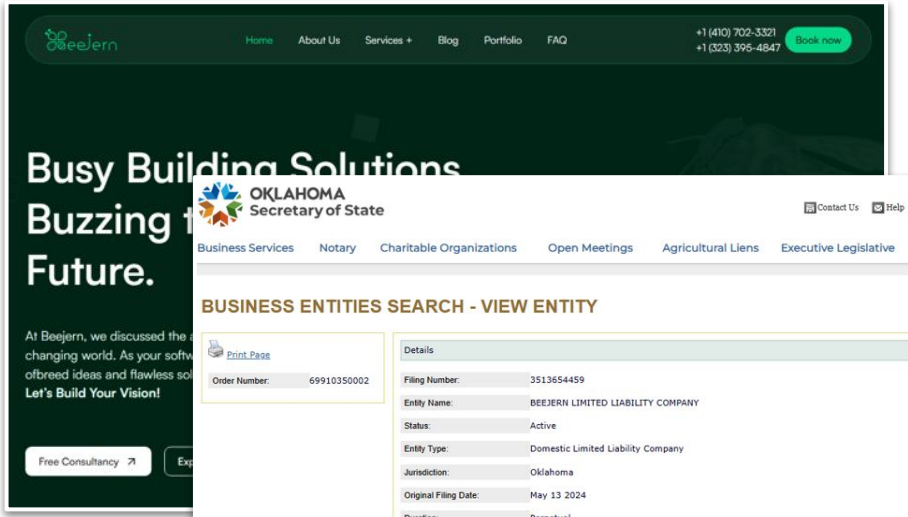
## Tracing their online presence across services

- When potential victims are identified, we attempt to contact and warn them. However, the risks of hiring or working with these individuals are often underestimated or ignored.

## Fake workers, fake companies

- An example is Beejern, currently registered as an active LLC in the state of Oklahoma.
- In a parallel investigation we have identified clusters of Web3 and software-development websites sharing phone numbers, addresses, service descriptions, and nearly identical website templates.
- Some of these companies also appear to use the H-1B visa system, raising questions about their use in broader operational networks.



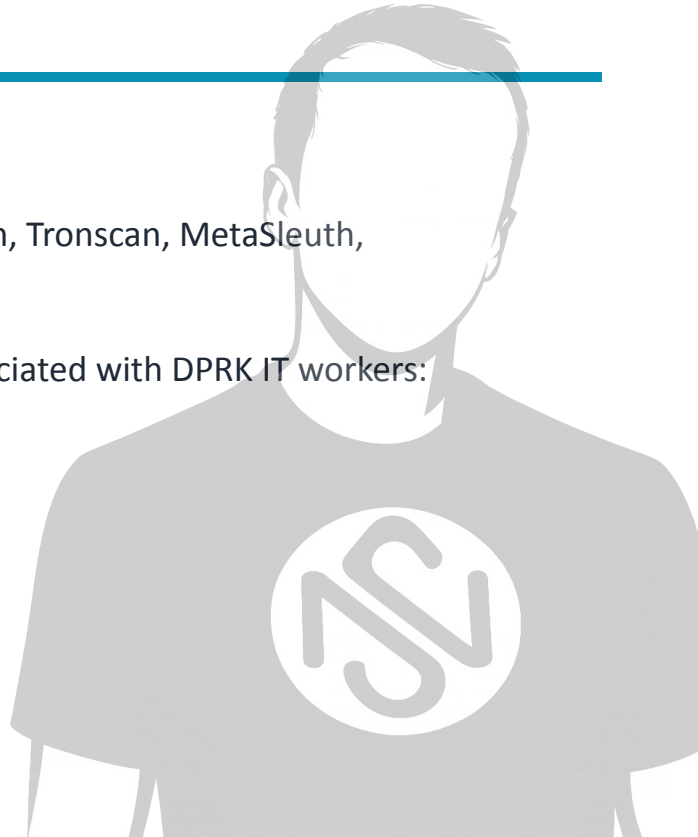

Beejern
Home
About Us
Services +
Blog
Portfolio
FAQ
+1 (410) 702-3321
+1 (323) 396-4847
Book now
Busy Buildi
Buzzing
Future.
At Beejern, we discussed the
changing world. As your softw
ofbreed ideas and flawless so
Let's Build Your Vision!
Free Consultancy
OKLAHOMA
Secretary of State
Contact Us
Help
Business Services
Notary
Charitable Organizations
Open Meetings
Agricultural Liens
Executive Legislative
BUSINESS ENTITIES SEARCH - VIEW ENTITY
Print Page
Order Number: 69910350002
Details
Filing Number: 3513654459
Entity Name: BEEJERN LIMITED LIABILITY COMPANY
Status: Active
Entity Type: Domestic Limited Liability Company
Jurisdiction: Oklahoma
Original Filing Date: May 13 2024
Duration: Perpetual
Entity Address: 9905 S PENNSYLVANIA AVE, STE A OKLAHOMA CITY, OK, 73159, USA
Registered Agent Information
Name: NORTHWEST REGISTERED AGENT, LLC
Effective: May 13 2024
Address: 9905 S PENNSYLVANIA AVE
STE A
City,State,ZipCode: OKLAHOMA CITY OK 73159
FILING HISTORY :
Document Number Filing Type Filing Date
65498520002 Articles of Organization May 13, 2024
70053340002 Annual Certificates March 16, 2025

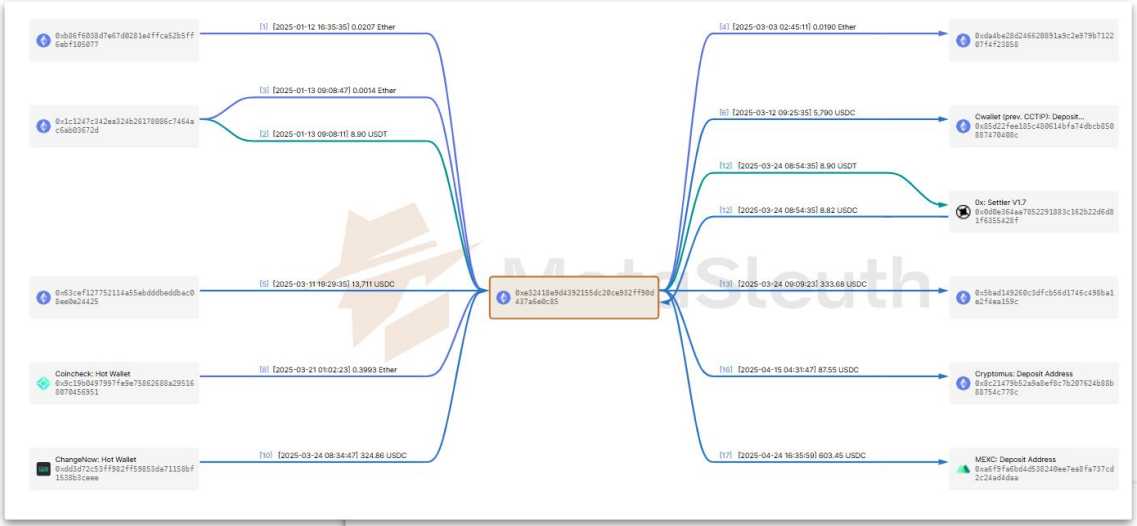
# Follow the money

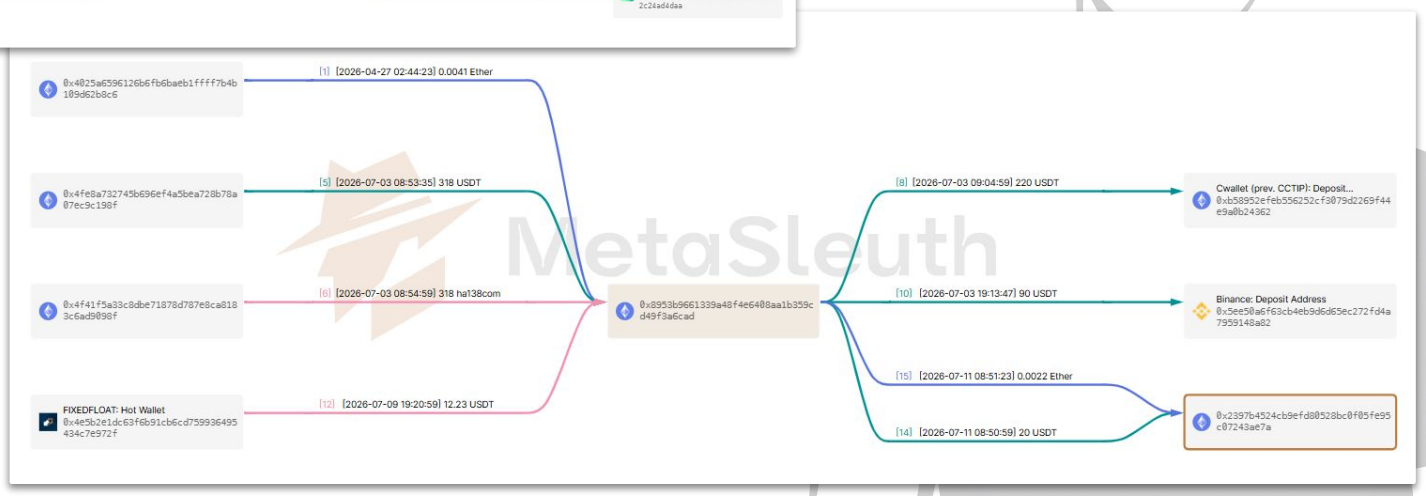
## Tracing crypto assets obtained by DPRK IT Workers

- We conduct similar investigations using tools such as: Etherscan, Tronscan, MetaSleuth, Breadcrumbs.app, Arkham Intelligence and others

- Types of services commonly observed across most wallets associated with DPRK IT workers:
  - No-KYC Swap: FixedFloat, ChangeNow
  - Bridge / Cross-Chain: Wormhole
  - Wallet: Metamask, Cwallet
  - CEX: Kucoin, Binance, MEXC




0xb86f6038d7e67d0281e4ffca52b5ff6ebf105077
[1] [2025-01-12 16:35:35] 0.0207 Ether
0x1c1247c342ea324b26178086c7464ac6ab03672d
[3] [2025-01-13 09:08:47] 0.0014 Ether
[2] [2025-01-13 09:08:11] 8.90 USDT
0x63cef127752114a55ebdddbeddbac08ee0e24425
[5] [2025-03-11 19:29:35] 13,711 USDC
Coincheck: Hot Wallet
0x9c19b0497997fe9e75862688a295168070456951
[8] [2025-03-21 01:02:23] 0.3993 Ether
ChangeNow: Hot Wallet
0xdd3d72c53ff982ff59853de71150bf1538b3ceee
[10] [2025-03-24 08:34:47] 324.86 USDC
0xe32418e9d4392155dc20ce932ff90d437a60c85
[4] [2025-03-03 02:45:11] 0.0190 Ether
0xda4be28d246620891a9c2e979b712207f4f23858
[6] [2025-03-12 09:25:35] 5,790 USDC
Cwallet (prev. CCTIP): Deposit...
0x85d22fee185c480614bfa74dbcb85087470480c
[12] [2025-03-24 08:54:35] 8.90 USDT
[12] [2025-03-24 08:54:35] 8.82 USDC
0x: Settler V1.7
0x0d0e364aa7852291883c162b22d6d81f6355428f
[13] [2025-03-24 09:09:23] 333.68 USDC
0x5bad149260c3dfcb56d1746c498ba1e2f4ea159c
[16] [2025-04-15 04:31:47] 87.55 USDC
Cryptomus: Deposit Address
0x8c21479b52a9a8ef0c7b207624b88b88754c778c
[17] [2025-04-24 16:35:59] 603.45 USDC
MEXC: Deposit Address
0xaf9fa6bdd538240ee7ea8fa737cd2c24ad4daa


0x4025a6596126b6fb6baeb1ffff7b4b109d62b8c6
[1] [2026-04-27 02:44:23] 0.0041 Ether
0x4fe8a732745b696ef4a5bea728b78a07ec9c198f
[5] [2026-07-03 08:53:35] 318 USDT
0x4f41f5a33c8dbe71878d787e8ca8183c6ad9098f
[6] [2026-07-03 08:54:59] 318 ha138com
FIXEDFLOAT: Hot Wallet
0x4e5b2e1dc63f6b91cb6cd759936495434c7e972f
[12] [2026-07-09 19:20:59] 12.23 USDT
0x8953b9661339a48f4e6408aa1b359cd49f3a6cad
[8] [2026-07-03 09:04:59] 220 USDT
Cwallet (prev. CCTIP): Deposit...
0xb58952efeb556252cf3079d2269f44e9a0b24362
[10] [2026-07-03 19:13:47] 90 USDT
Binance: Deposit Address
0x5ee50a6f63cb4eb9d6d65ec272fd4a7959148a82
[15] [2026-07-11 08:51:23] 0.0022 Ether
[14] [2026-07-11 08:50:59] 20 USDT
0x2397b4524cb9efd80528bc0f05fe95c07243ae7a

# Follow the people

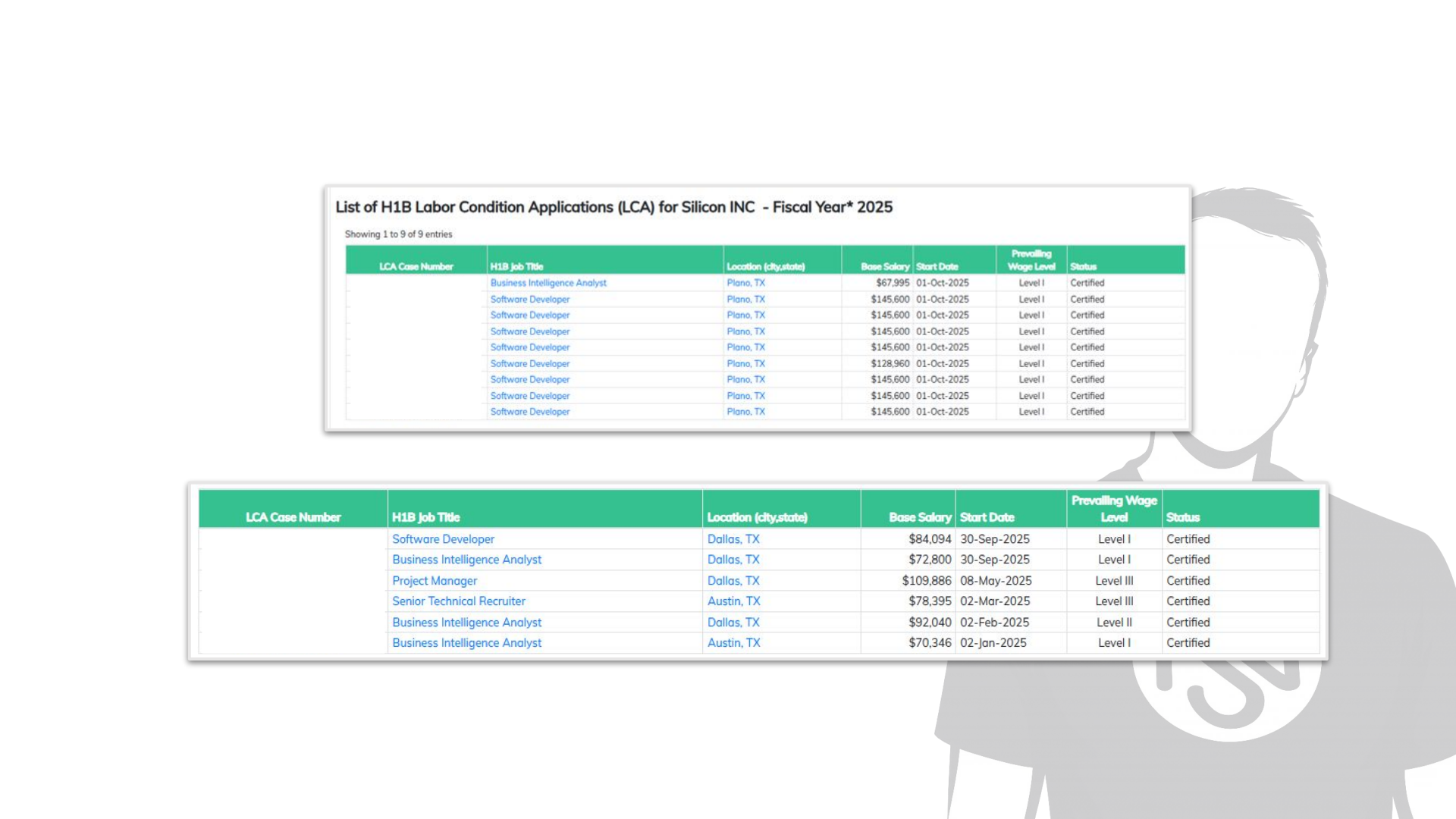
## Tracing potentially suspicious H-1B applicants and sponsoring employers

- Parallel investigation tracking a suspected coordinated network of shell companies, nominee executives, and financial vehicles operating across California, Wyoming, Texas, and New Jersey
- At least 30 companies under three phone numbers linking to unrelated companies across multiple industry sectors: technology, pharmaceuticals, trucking, real estate, finance, and more
- Three individuals dominate the corporate officer record landscape and together they appear as officers, agents, or COOs across dozens of registered entities, and H1B visa filings

## List of H1B Labor Condition Applications (LCA) for Silicon INC - Fiscal Year* 2025

Showing 1 to 9 of 9 entries

| LCA Case Number | H1B Job Title | Location (city,state) | Base Salary | Start Date | Prevailing Wage Level | Status |
|---|---|---|---|---|---|---|
| | Business Intelligence Analyst | Plano, TX | $67,995 | 01-Oct-2025 | Level I | Certified |
| | Software Developer | Plano, TX | $145,600 | 01-Oct-2025 | Level I | Certified |
| | Software Developer | Plano, TX | $145,600 | 01-Oct-2025 | Level I | Certified |
| | Software Developer | Plano, TX | $145,600 | 01-Oct-2025 | Level I | Certified |
| | Software Developer | Plano, TX | $145,600 | 01-Oct-2025 | Level I | Certified |
| | Software Developer | Plano, TX | $128,960 | 01-Oct-2025 | Level I | Certified |
| | Software Developer | Plano, TX | $145,600 | 01-Oct-2025 | Level I | Certified |
| | Software Developer | Plano, TX | $145,600 | 01-Oct-2025 | Level I | Certified |
| | Software Developer | Plano, TX | $145,600 | 01-Oct-2025 | Level I | Certified |



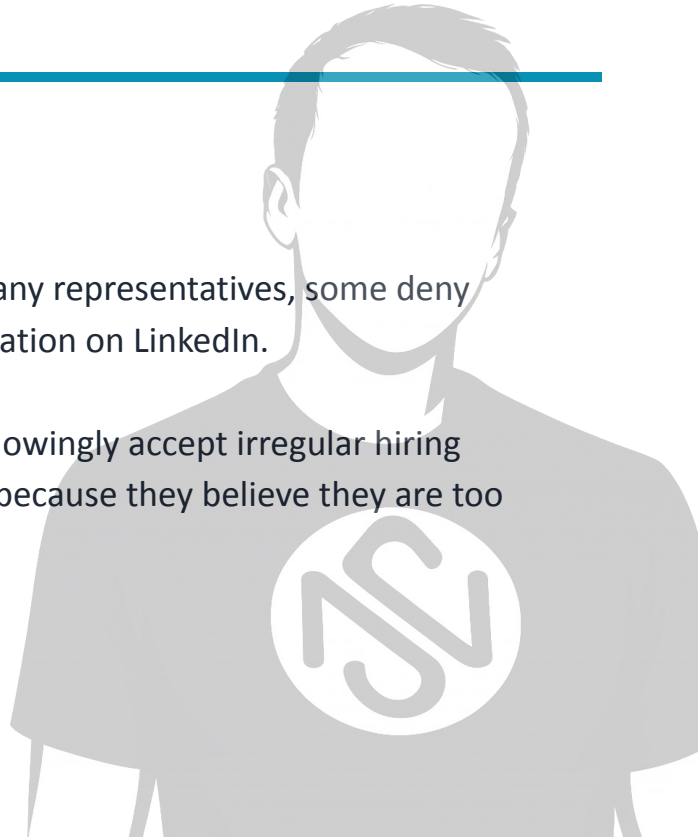
| LCA Case Number | H1B Job Title | Location (city,state) | Base Salary | Start Date | Prevailing Wage Level | Status |
|---|---|---|---|---|---|---|
| | Software Developer | Dallas, TX | $84,094 | 30-Sep-2025 | Level I | Certified |
| | Business Intelligence Analyst | Dallas, TX | $72,800 | 30-Sep-2025 | Level I | Certified |
| | Project Manager | Dallas, TX | $109,886 | 08-May-2025 | Level III | Certified |
| | Senior Technical Recruiter | Austin, TX | $78,395 | 02-Mar-2025 | Level III | Certified |
| | Business Intelligence Analyst | Dallas, TX | $92,040 | 02-Feb-2025 | Level II | Certified |
| | Business Intelligence Analyst | Austin, TX | $70,346 | 02-Jan-2025 | Level I | Certified |

# Follow the people

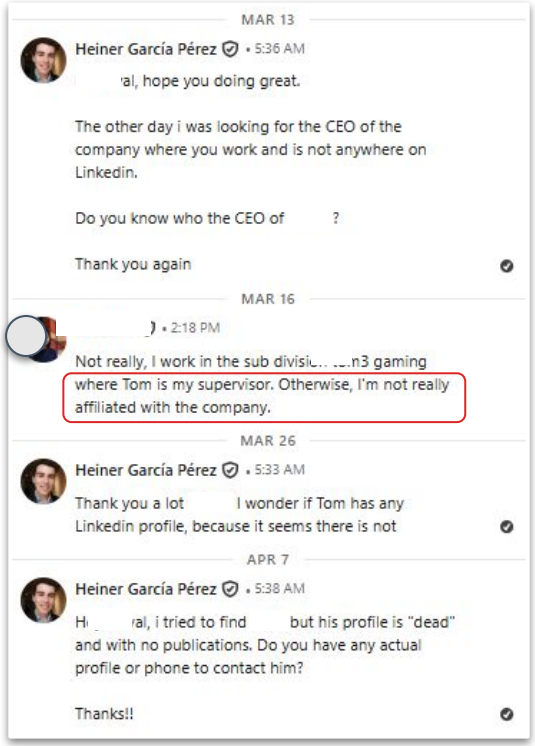
## Loose lips sink ships

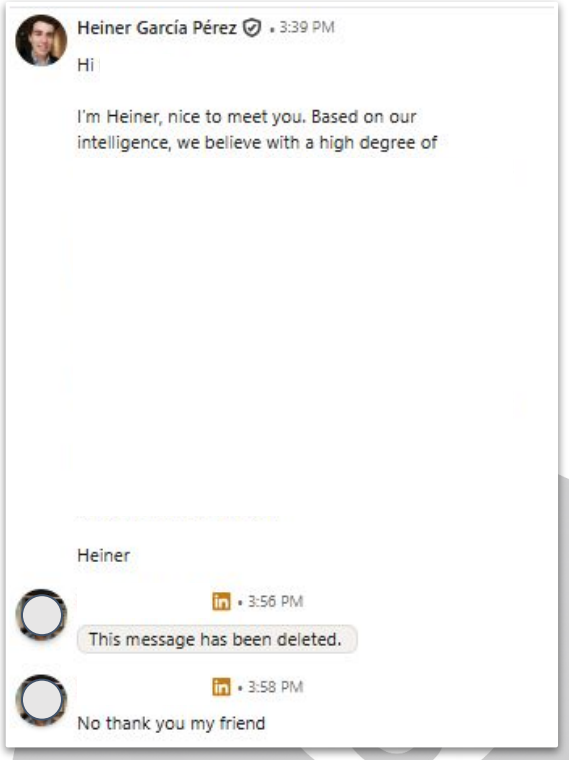
- When we contact individuals listed as H-1B applicants or company representatives, some deny any connection to the company despite publicly listing the affiliation on LinkedIn.

- In other cases, companies or individuals downplay the issue, knowingly accept irregular hiring arrangements because of lower labor costs, or dismiss the risk because they believe they are too experienced or cautious to be fooled




MAY 21
Heiner García Pérez • 1:08 PM
Hello,
Nice to meet you!
Heiner García Pérez • 10:22 PM
Hello Hanlin, im trying to reach Tom, is there any possibility to speak with anyone at your company?
thank you!
MAY 27
Heiner García Pérez • 12:52 PM
Hey Hanlin, nice to meet you
MAY 29
Heiner García Pérez • 10:52 AM
Sorry the impatience Hanlin, is there any way i can contact someone from the company you work for?
Ive tried writing to the mail you have listed at your website
Thank you!


MAR 13
Heiner García Pérez • 5:36 AM
al, hope you doing great.
The other day i was looking for the CEO of the company where you work and is not anywhere on Linkedin.
Do you know who the CEO of ?
Thank you again
MAR 16
• 2:18 PM
Not really, I work in the sub divisi... ...n3 gaming where Tom is my supervisor. Otherwise, I'm not really affiliated with the company.
MAR 26
Heiner García Pérez • 5:33 AM
Thank you a lot I wonder if Tom has any Linkedin profile, because it seems there is not
APR 7
Heiner García Pérez • 5:38 AM
H al, i tried to find but his profile is "dead" and with no publications. Do you have any actual profile or phone to contact him?
Thanks!!


Heiner García Pérez • 3:39 PM
Hi
I'm Heiner, nice to meet you. Based on our intelligence, we believe with a high degree of
Heiner
• 3:56 PM
This message has been deleted.
• 3:58 PM
No thank you my friend

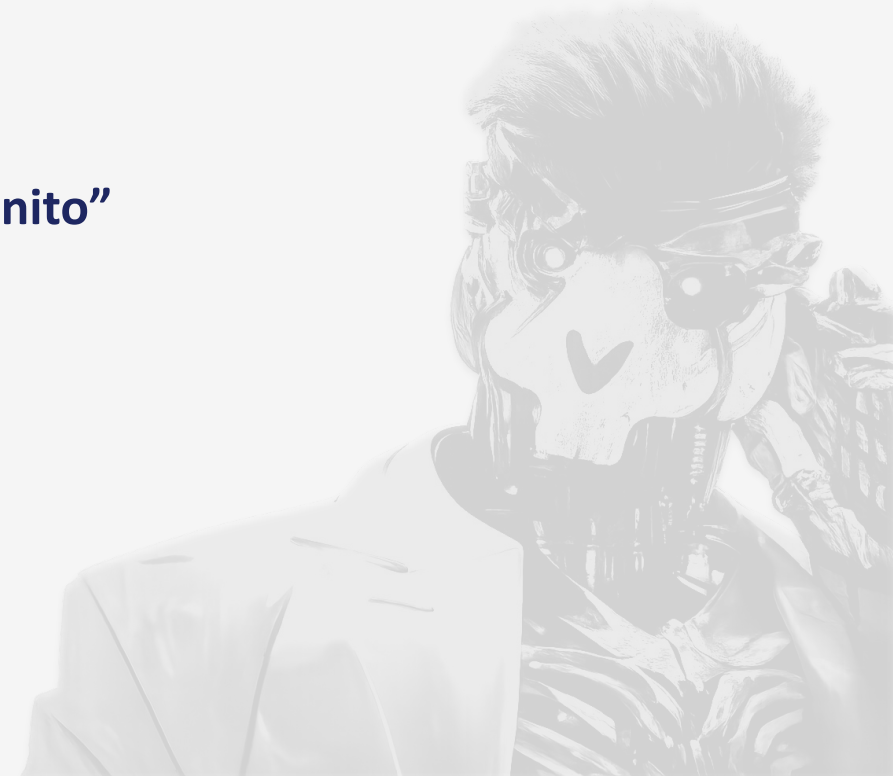
# Taming Chollimas

## Confronting the IT Workers

- After gathering enough evidence, it was time to stop.

- Since they lied about their identities…
  - We had to set up a meeting with our lawyer, Benito.

# Tape F: “Benito”

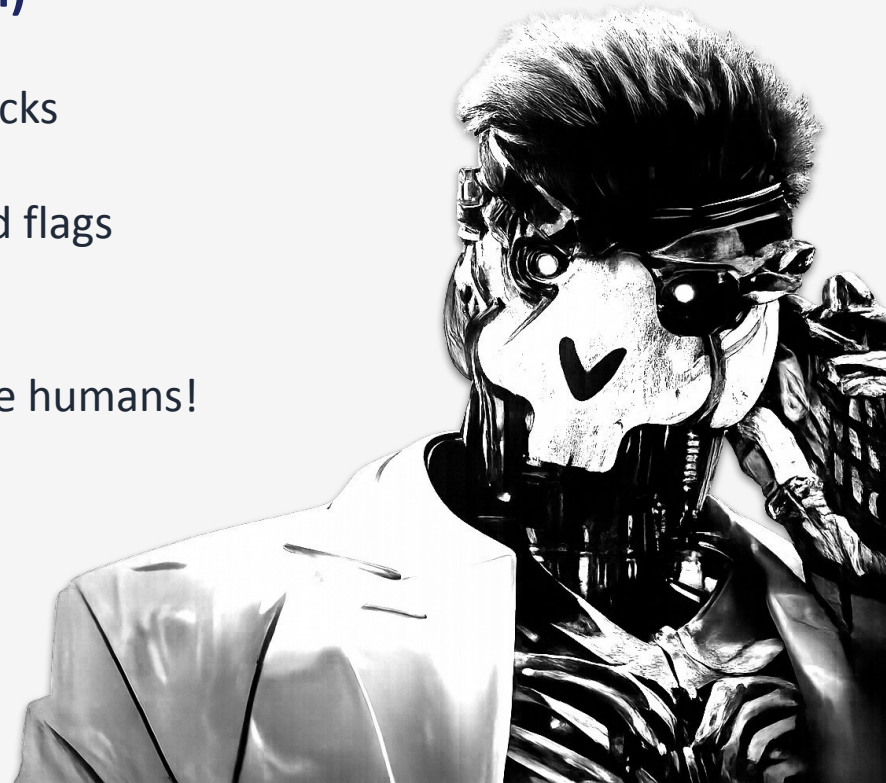



I’m going to be as forthcoming as I can be, Mr Anderson.
It seems you’ve been living two lives, Mr Anderson.

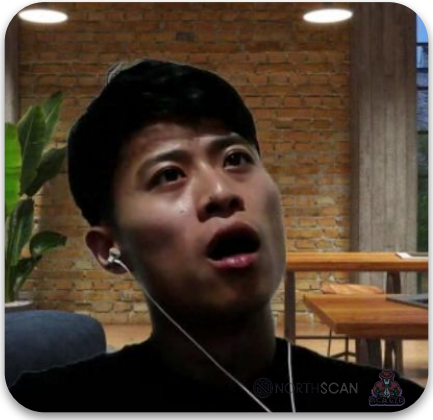
# Taming Chollimas

## Protecting yourself (and your organisation)

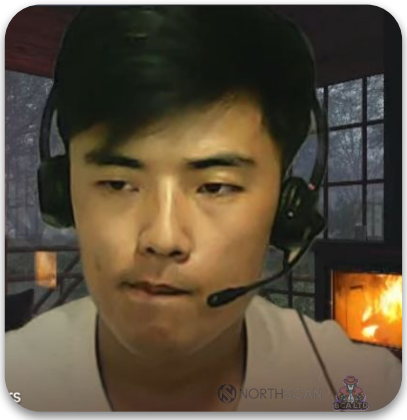
- Conduct rigorous KYC and background checks
- Train talent acquisition teams to detect red flags
- Not every time HUMINT works.
  - But *most of the time*, threat actors are humans!
- **Block the hell out of AstrillVPN!**
- Record their faces! Make them *Famous*!



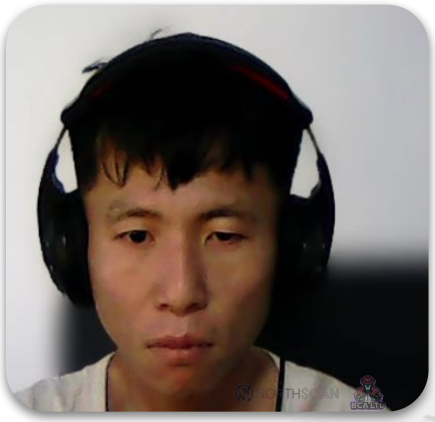
# Always doubt!

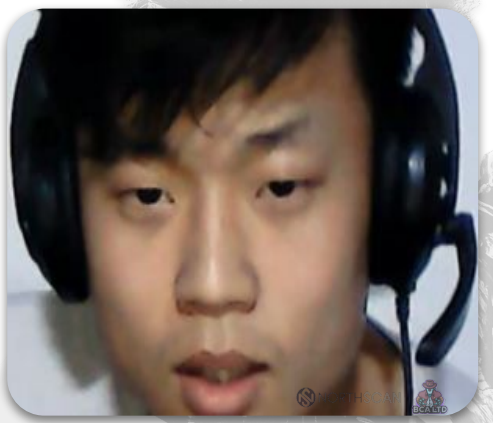



# Trust no one!

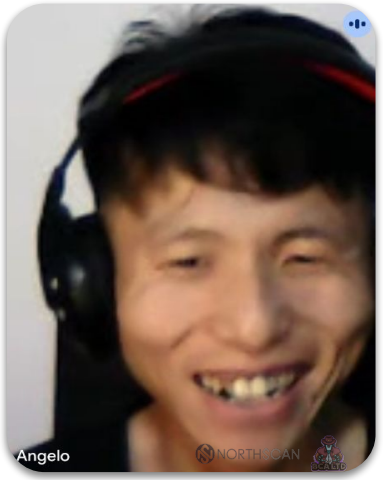


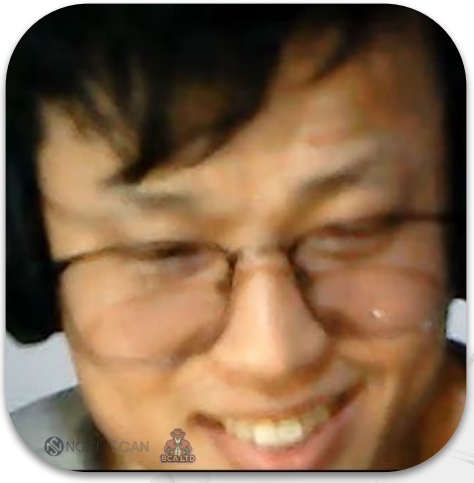


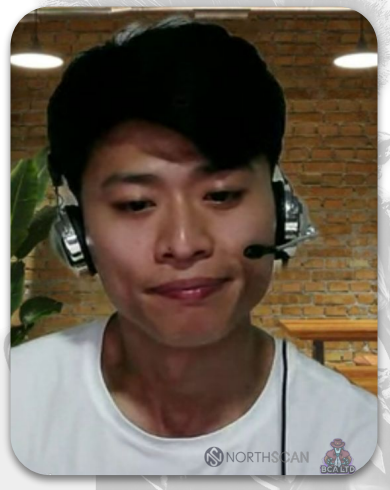




# Smile! You're on camera!





# Smile! You're on camera!

# Thank you!


**Heiner García Pérez**

@0xFigo on X
https://northscan.co



**Mauro Eldritch**

@MauroEldritch on X
https://bca.ltd/