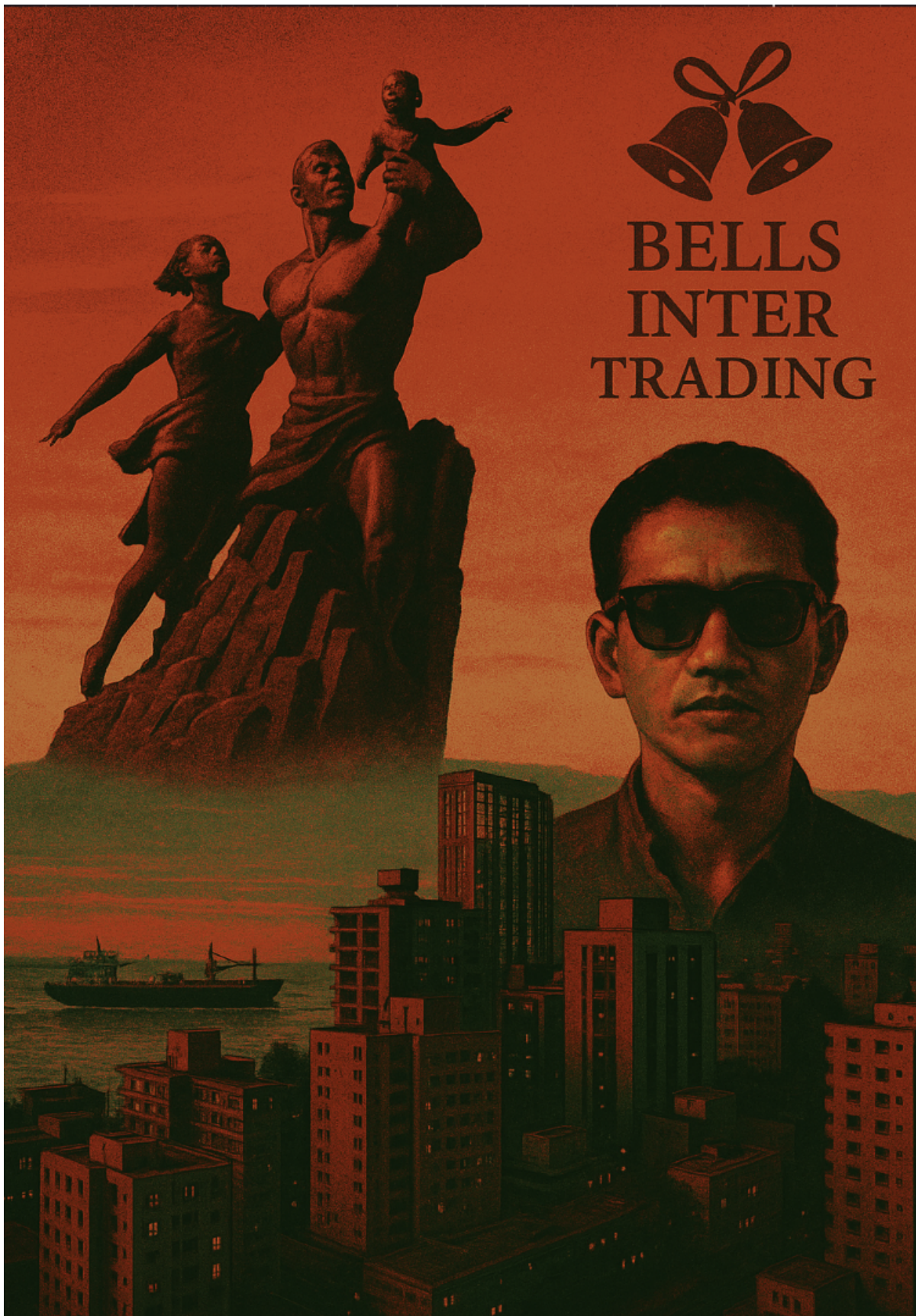


Bells Ringing in Dar es Salaam



Tracking connections between the BABYLONGROUP cluster, DeTankZone, and an IT Worker in Tanzania developing mobile VPN apps.

04 September 2025

Introduction.

Our last post on the IT Workers of BABYLONGROUP ended on a cliffhanger which briefly had us looking into a suspected IT Worker named Hailong Jin using the email `goldsea808@yahoo.com` and username `sujan198703`. As promised, in this post we will continue to follow Hailong Jin, and in the process shine light on how North Korea's web of fake shell companies operate in the world's seedy underbelly, and how it's IT Workers continue to infiltrate global markets.

Gold Seas and Jilin.

In our previous post we first encountered Hailong Jin after discovering a Github repository containing the same strings as seen in Moonstone Sleet's DeTankZone game, hosted by the account `sujan198703`. This account was tied to the email `goldsea808@gmail.com`, which also shares a sister account of `goldsea808@yahoo.com`.

```
public static AESCrypto instance;

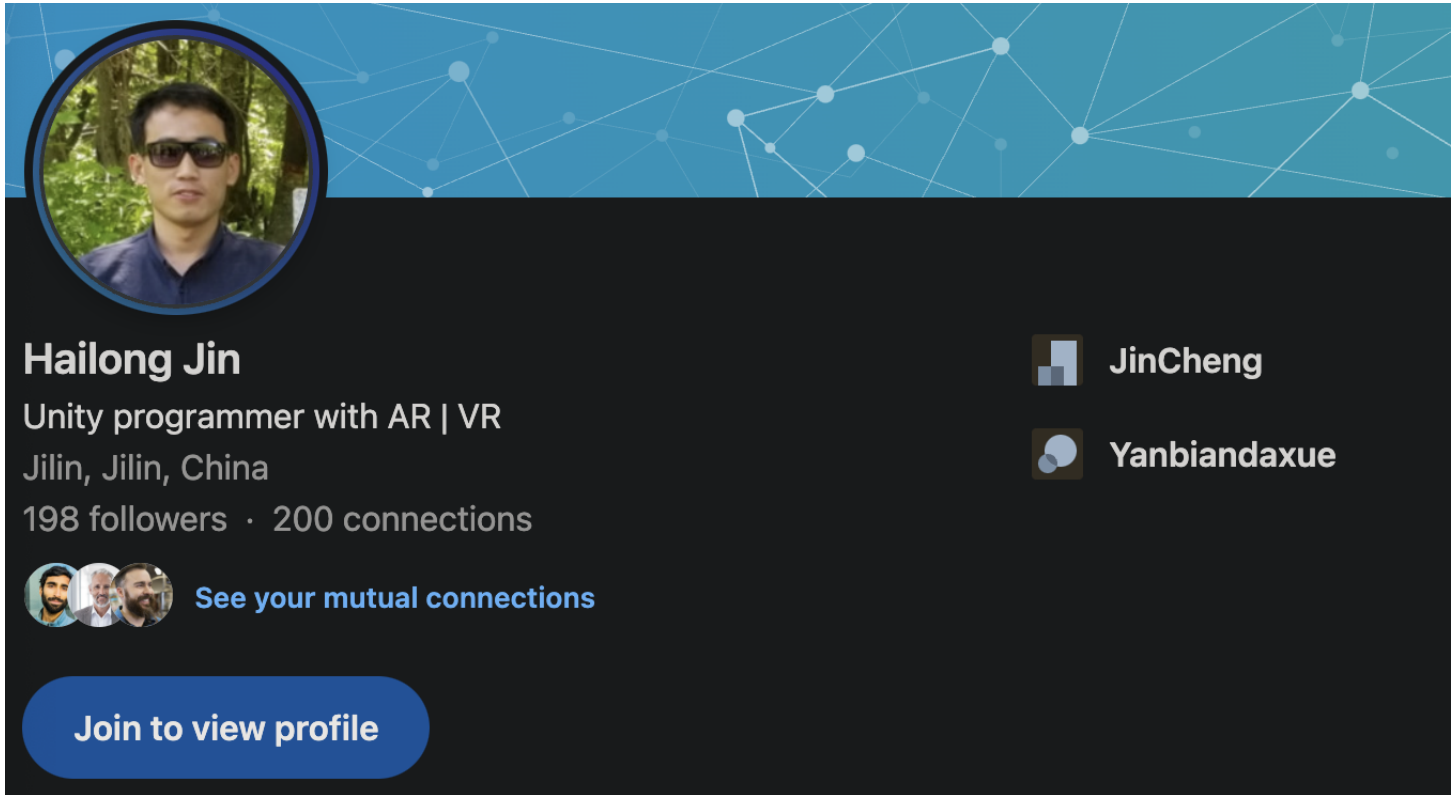
public AESCrypto()
{
    instance = this;

    Key = "Full Stack IT Service 198703Game";
    IV = "MatGoGameProject";

    // UnityEngine.Debug.Log("1. == Key Length : " + Key.Length);
    //     UnityEngine.Debug.Log("1. == Key : " + Key);
}
```



Code snippet from sujan198703's MatGoGame repo containing the same strings documented by Kaspersky


Pivoting off of the `goldsea808` username and emails proved fruitful, with `goldsea808@yahoo.com` being connected to the LinkedIn account of Hailong Jin - a Project Manager and Unity Programmer based in Jilin, China (a region bordering the DPRK):



The image shows a LinkedIn profile for Hailong Jin. The header has a blue background with a white network diagram. The profile picture is a circular image of a man with sunglasses. The name 'Hailong Jin' is in bold. The bio reads 'Unity programmer with AR | VR' and 'Jilin, Jilin, China'. It shows '198 followers · 200 connections'. To the right, there are two connection icons: 'JinCheng' and 'Yanbiandaxue'. Below the bio, there are three small profile pictures and the text 'See your mutual connections'. At the bottom, there is a blue button that says 'Join to view profile'.

Hailong Jin
Unity programmer with AR | VR
Jilin, Jilin, China
198 followers · 200 connections

 **JinCheng**
 **Yanbiandaxue**

 [See your mutual connections](#)

[Join to view profile](#)

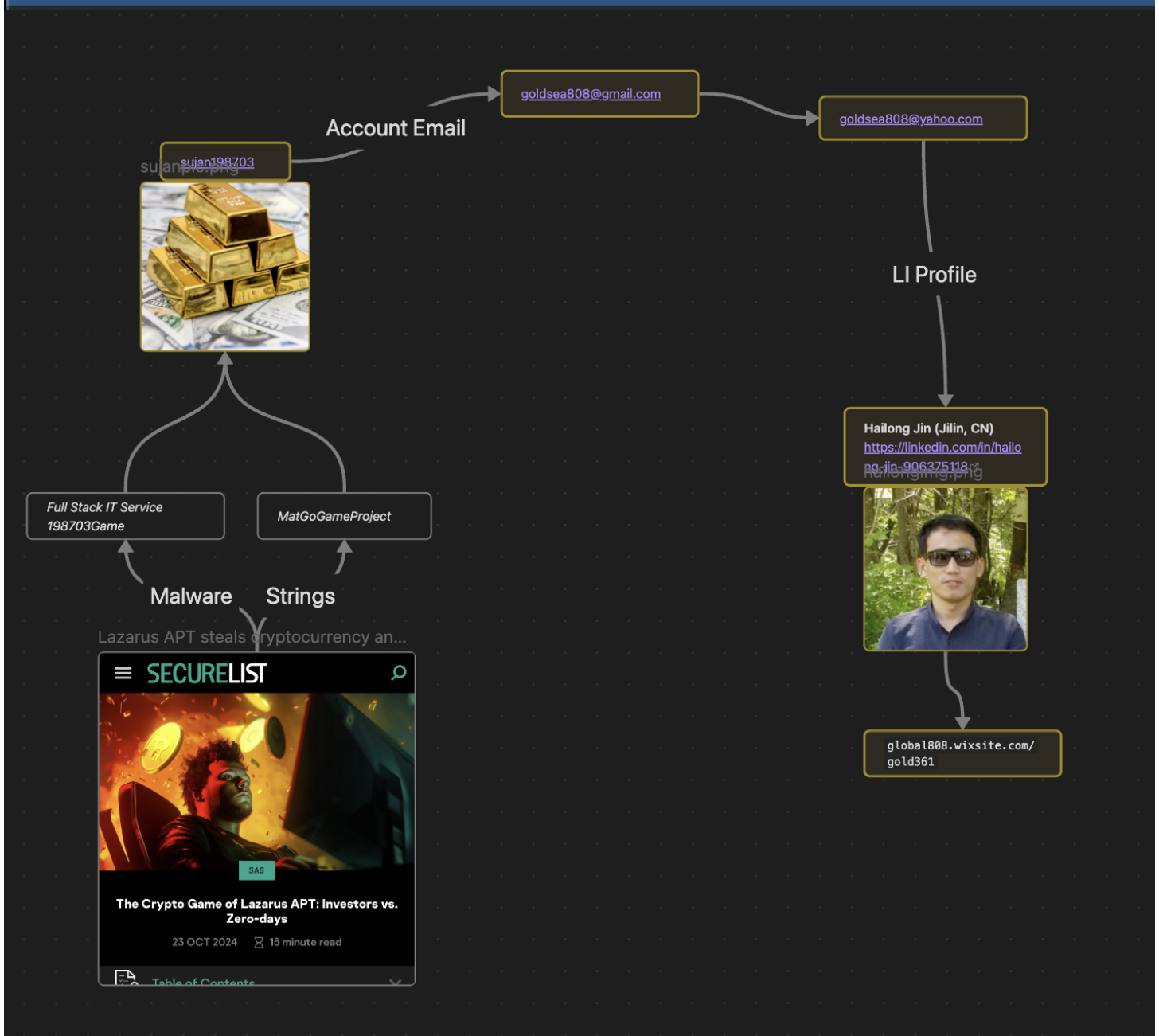
The bio of this LinkedIn account takes us to `global808.wixsite[.]com/gold361`, where we can confirm then that Hailong Jin is indeed the owner of the DeTankZone repo, based off his contact info:



Skype
sujan198703




Contact
goldsea808@gmail.com



This discovery obviously led to us wanting to learn more about Hailong Jin and how he got mixed into all of this. From here, we made two further pivots that yielded some additional key information.

We first decided to pivot off of the website ([global808.wixsite\[.\]com/gold361](https://global808.wixsite.com/gold361)) and see if we could identify any additional references to it. Sure enough, this website was also listed on a Github profile we had not previously seen before: `intellichain555`:



TopNorch

intellichain555

Follow

Cross-Platform IT Service Mobile, Web & Desktop

6 followers · 15 following

<https://global808.wixsite.com/gold361>

Block or Report

Pinned

AI-Inpainting-PhotoshopPublic

C# ☆ 1

DragonDev-frontendPublic

TypeScript

Universal-voting--ElectChainPublic

Dart

flutter_buyerPublic

Dart

cryptofolioPublic

Python

24 contributions in the last year

2025

2024

2023

2022

	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
Mon												
Wed												
Fri												

Learn how we count contributions

LessMore

The `intellichain555` profile, which we believe to belong to Hailong Jin or another related individual, was primarily focused on blockchain, with several additional repositories related to video game reverse engineering, and pentesting. Although this profile appeared very similar to many IT Worker profiles we have seen before, it did not share any connections with other DPRK profiles we were aware of, which is quite unusual.

By analyzing leak data for `intellichain555@gmail.com`, we can see that it has previously originated from the DPRK IP `45.126.3.252`, an IP associated with NetKey/OConnect. We believe this means that Hailong Jin, the owner of the repository containing strings from DeTankZone, or a closely related individual is also a North Korean IT Worker.

Although this was interesting for us to discover, there was one additional thing on Hailong Jin's website that we decided to look into: a company called Our Dream Technologies Pvt. LTD.

Tanzania Calling.

A quick google search for Our Dream Technologies Pvt. LTD, wielded a hit on a Vercel hosted website: `our-dream-technologies.vercel.app`. Upon visiting this site, we immediately had alarm bells going off in our head (no pun intended) due to company logo on the top left-hand side:



WE ARE A TEAM OF INNOVATORS

Innovating Your Digital Future

At Bells International Trading, our motto reflects our commitment to pushing the boundaries of technology. We strive to deliver cutting-edge solutions that propel your business forward in the digital landscape.

About Us

Contact Us



Searching back through our archives we got a hit on the name and quickly remembered why it sounded so familiar: months before we identified a North Korean IT Worker based out of Tanzania who we refer to as Lian Hung.

Although we originally did not spend much time looking into Lian, we did remember that he claimed to be based out of Dar Es Salaam, Tanzania, worked as a Project Manager at a company called StarMobile Ltd, and said that he went to Yanbian University of Science.

His now deleted LinkedIn showed that his listed skill set was almost the same as Hailong Jin -- heavily focused on game development, Unity, AR/VR, and mobile apps.



Liu Wilson/Lian Hung



Hailong Jin

While investigating these personas we believe with low-medium confidence that Hailong Jin and Lian Hung may be the same person. In any case, we are confident that Lian is a North Korean IT Worker. This is based on that fact that he frequently visited DPRK-owned websites in the Korean language (primarily Rodong, the Workers Party newspaper), used multiple different personas and names (Liu Wilson, Evans John Mboye, Brian DWingo), and also visited a Russian social media page hosting Korean-translated Soviet films that we have observed many North Koreans visit, amongst several other factors.

Bells Inter Trading Ltd.

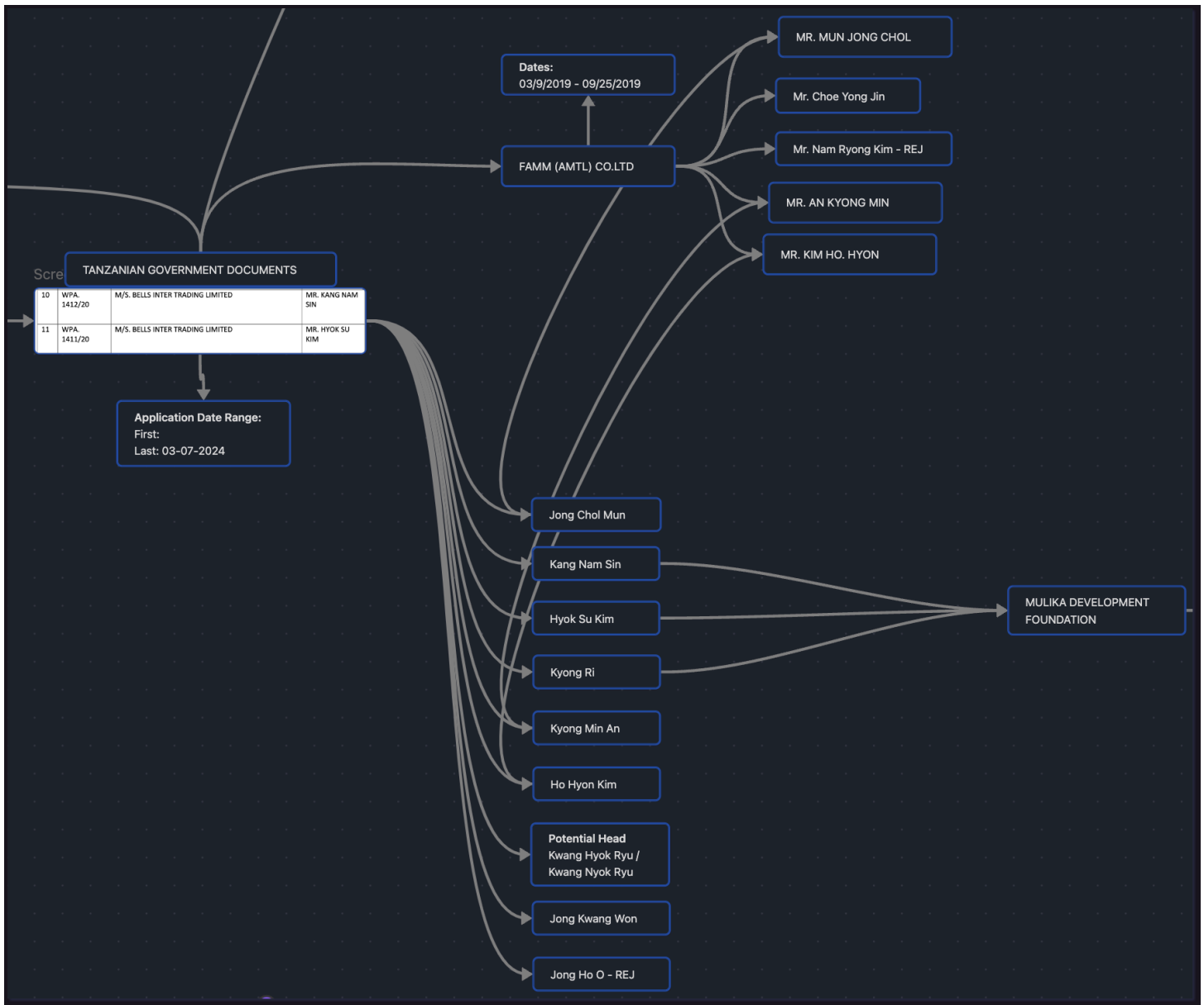
We now have two personas that we believe are North Korean IT Workers, but what is the company that bonds them together, Bells Inter Trading Ltd? A quick google search for "Bells Inter Trading" turns up several interesting results showing that it appears to be a company name of an Apple App Store publisher, with two apps: Tiles Matching and Swift VPN, and secondly that it appears to be a business based in Dar Es Salaam, Tanzania associated with some work permits.

Based on what we know about Lian Hung, this information adds up, but what are these work permits?

In Tanzania, granted and rejected work permits for foreigners are published publicly to `kazi.go.tz`. Our google search for Bells Inter Trading pulled up one of these listing the following individuals as having applied for work permits using the following companies as their employer:

Work Permit	Employer	Applicant's Name	GRANTED
WPA 1412/20	M/S. BELLS INTER TRADING LIMITED	MR. KANG NAM SIN	12.06.2020
WPA 1411/20	M/S. BELLS INTER TRADING LIMITED	MR. HYOK SU KIM	12.06.2020
WPC/2090/20	M/S. BELLS INTER TRADING LIMITED	MR. JONG CHOL MUN	04.12.2020

Since we didn't get any additional hits on BELLS INTER TRADING LIMITED, we decided collect all of the publicly available work permit documents and pivot off of applicant names and run them through OCR. At the end, we identified 9 individuals, all with Korean names (sometimes variations of the same names, or with single letter changes), working at BELLS INTER TRADING LIMITED. Additionally, we identified that some of these individuals had also worked at two other companies, which we have even less information about: FAMM (AMTL) CO Ltd. and MULIKA DEVELOPMENT FOUNDATION:



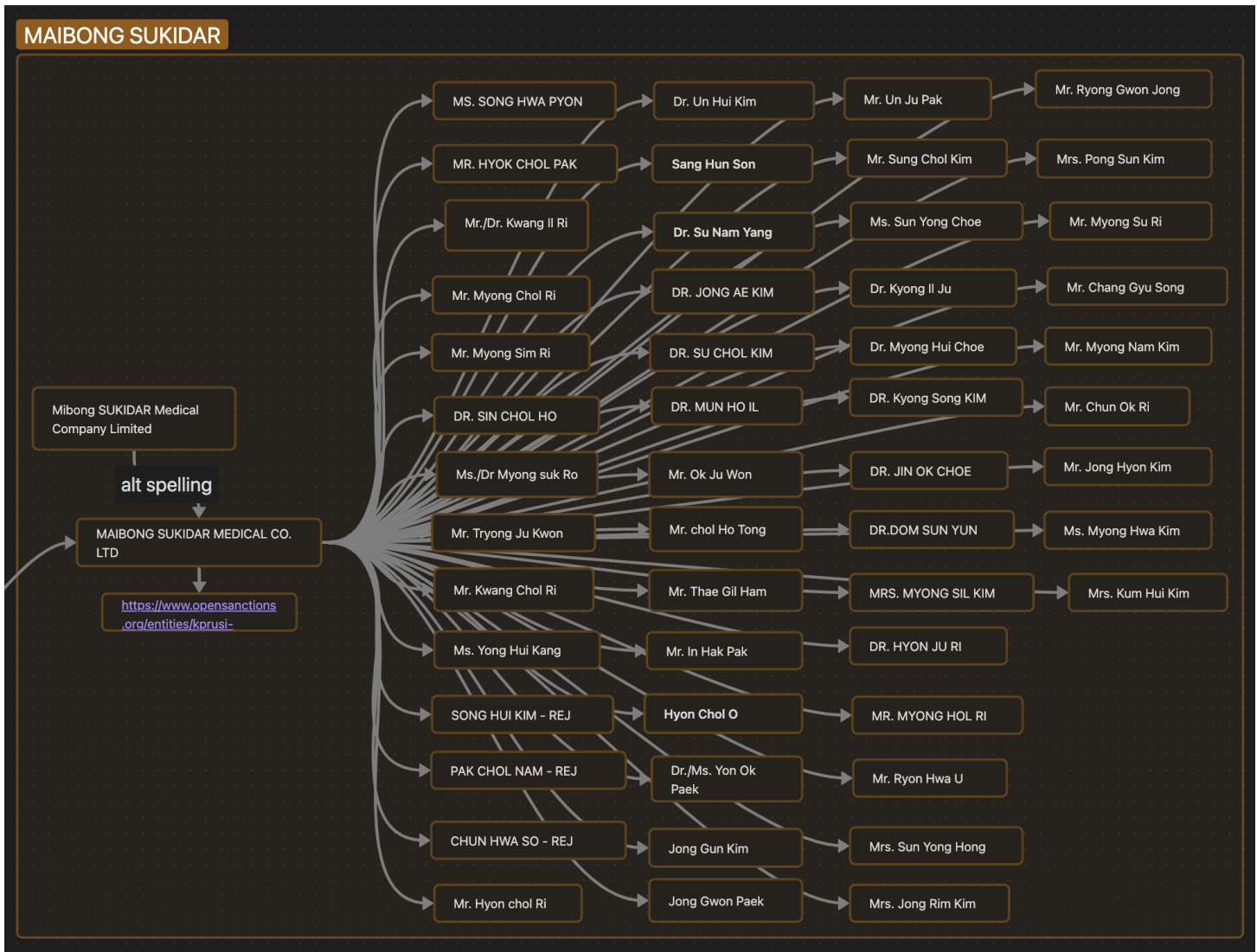
Associated Individuals:

Work Permit	Employer	Applicant's Name	Date Action
WPA 1412/20	M/S. BELLS INTER TRADING LIMITED	MR. KANG NAM SIN	12.06.2020
WPA 1411/20	M/S. BELLS INTER TRADING LIMITED	MR. HYOK SU KIM	12.06.2020
WPC/2090/20	M/S. MULIKA DEVELOPMENT FOUNDATION	MR. JONG CHOL MUN / MR. MUN JONG CHOL	04.12.2020
WPC/2091/20	M/S. FAMM (AMTL) CO LTD	MR. KWANG HYOK RYU / MR. KWANG NYOK RYU /	16.10.2020

Work Permit	Employer	Applicant's Name	Date Action
		MR. KYONG HYOK RYU (?)	
WPC/2088/20	M/S. BELLS INTERNATIONAL TRADING LIMITED	MR. HO HYON KIM / MR. KIM HO HYON	16.10.2020
WPC/2089/20	M/S. FAMM (AMTL) CO LTD M/S. BELLS INTERNATIONAL TRADING LIMITED	MR. KYONG MIN AN / MR AN KYONG MIN	16.10.2020
WPC/2087/20	M/S. FAMM (AMTL) CO LTD. M/S. BELLS INTERNATIONAL TRADING LIMITED	MR. KYONG RI	16.10.2020
N/A	M/S. MULIKA DEVELOPMENT FOUNDATION		
	M/S. BELLS INTER TRADING LIMITED	MR. JONG KWANG WON	03.07.2024
WPC 0286/22	M/S. BELLS INTER TRADING LIMITED	MR. JONG HO O	06.02.2023

We believe it is highly likely that BELLS INTER TRADING LIMITED is a North Korean run front company employing IT Workers in Tanzania. Although Tanzania, and Africa in general, is not commonly known to be associated with the DPRK -- countries across the African continent, including Tanzania, have had good or great relations with North Korea throughout the nations history. In fact, during the Cold War some African countries instead opted for North Korean advisors or Soviets.

In one such example, seen in the same dataset that we found the workers associated with Bells Inter Trading, is a another suspected North Korean company: MAIBONG SUKIDAR MEDICAL CO. LTD, which was documented in a 2020 UN Council of Experts report. This company, associated with 51 different individuals, ran several medical clinics in Tanzania before being kicked out of the country after UN investigation.

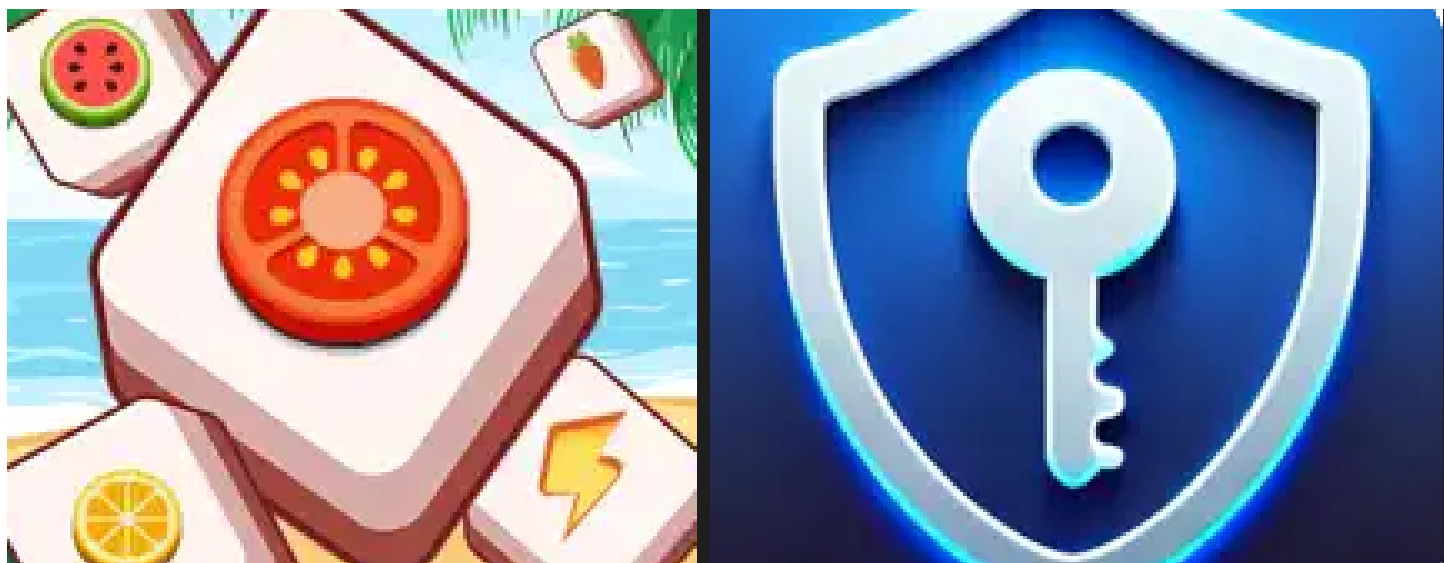


The other two companies besides Bells (FAMM (AMTL) and Mulikda Development Foundation) had very little information online, however we found that FAMM (AMTL) is involved in gold mining and has appeared on several websites being accused of running 501 scams. Mulika Development Foundation was listed in several freelancers online portfolios claiming to be based out of India and Bangladesh.

Millions on Millions.

So what is Bells Inter Trading doing in Tanzania? At least part of their operations, or at least Lian Hung, are focused on app development -- primarily mobile VPNs, which he has had a good amount of success with.

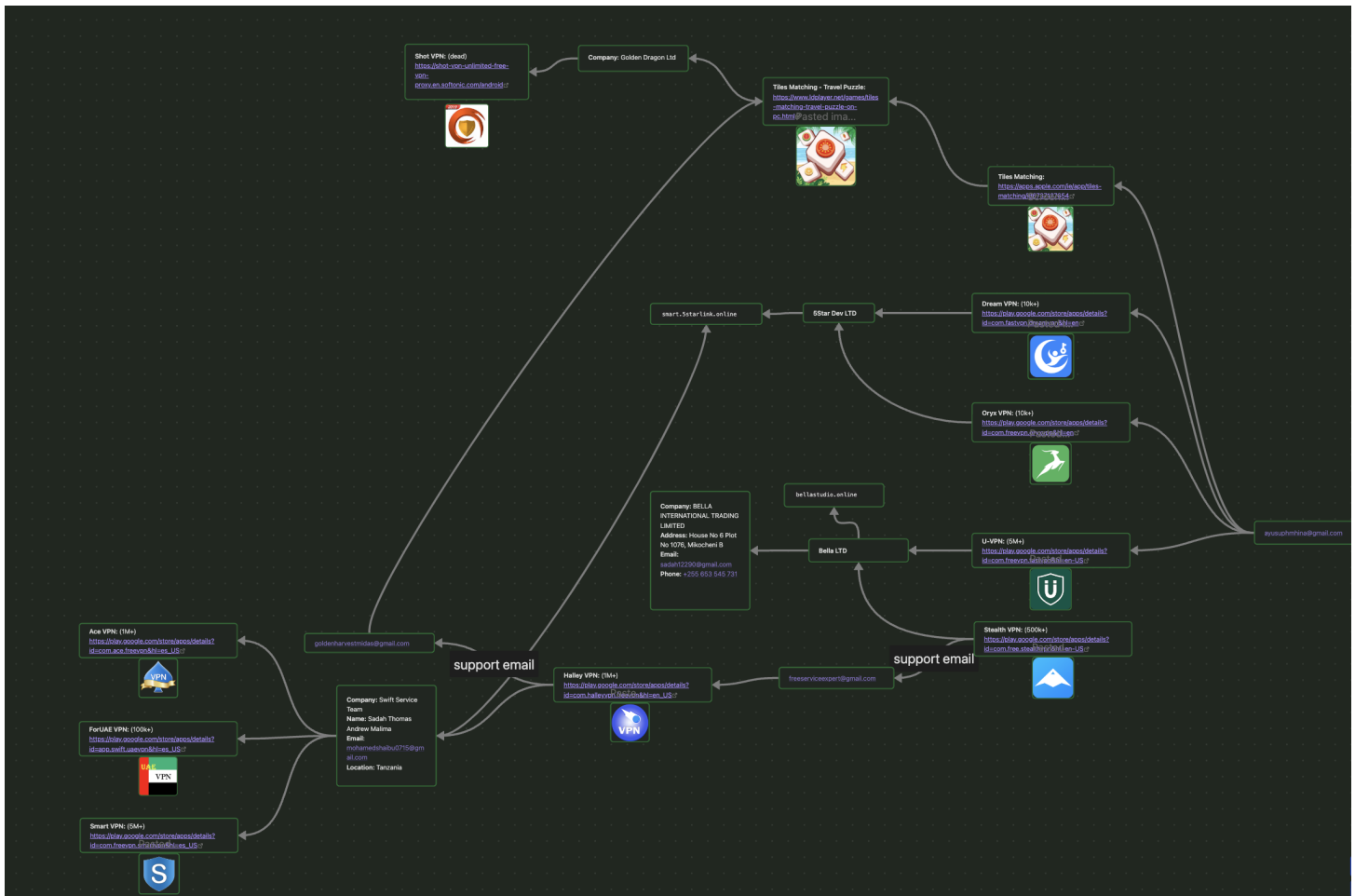
The first two apps directly tied to Bells Inter Trading are on Apple's App Store, SwiftVPN and Tiles Matching:



```
https://apps.apple.com/ie/app/tiles-matching/id6737127654  
https://apps.apple.com/us/app/swift-vpn/id1612950256
```

Although the Apple App Store does not list the number of installs for an app, it does list the support email for these two as `ayusuphmhina@gmail.com`, which we have also observed Lian Hung logging into, in addition to a SwiftVPN admin panel.

Pivoting off this email opened a floodgate of different apps, primarily VPNs, that total around 12M+ total installs once we had finished pivoting:



App Store	App Name	Publisher	Total Installs
Apple	SwiftVPN	Bells Inter Trading Ltd	N/A
Apple	Tiles Matching	Bells Inter Trading Ltd	N/A
Google	Stealth VPN	Bella LTD	500k+
Google	U-VPN	Bella LTD	5M+
Google	Oryx VPN	5Star Dev LTD	10k+
Google	Dream VPN	5Star Dev LTD	10k+
Google	Halley VPN	Swift Service Team	1M+
Google	ForUAE VPN	Swift Service Team	100k+
Google	Ace VPN	Swift Service Team	1M+
Google	Smart VPN	Swift Service Team	5M+
N/A	Shot VPN	Golden Dragon Ltd	N/A

Total: ~12,620,000 installs

Additionally, Lian Hung is associated with the following VPNs with much lower install rates or which were taken down from the app store (in the case of GulfGuard VPN, Google Play removed the app stating that the reasoning was due to malicious code/trojans):

App Name	App Identifier	Publisher
GulfGuard VPN	com.mobilesecure.gulfguardvpn	LeoX Tech

App Name	App Identifier	Publisher
UltraConnect VPN	com.ultraconnect.ultraconnectvpn	N/A
GuardianVPN	app.star.guardianvpn	StarMobDev
EmirateSecure VPN	com.bells.emiratefreevpn	N/A
StreakVPN	N/A	N/A
SmartVPN	com.bells.smartvpn	N/A

Last, but not least, we identified 3 US-based IPv4-IP ranges registered to Bells Inter Trading Co. Ltd:

```
69.30.210.152 - 69.30.210.159 (WholeSale Internet - Kansas)
107.150.47.16 - 107.150.47.23 (Nocix LLC - Kansas)
173.208.245.144 - 173.208.245.151 (WholeSale Internet - Kansas)
```

Although we did not identify any interesting traffic originating from these ranges, if others do please contact us at chollima_group@proton.me.

Closing Thoughts.

This is our second and final part documenting connections to DPRK actors related to Moonstone Sleet's DeTankZone operation. While Tanzania, and Africa more broadly, has not been widely recognized as the hotbed of North Korean activity that it is, we hope that this analysis contributes to better understanding DPRK operations there.

North Korean entities operate illicitly around the world, often thriving in the underbelly of the global economy where many are not paying attention. Bells Inter Trading is only one such example.

North Korean corporations and organizations, such as Haegumgang Trading Corporation (which has historically operated in this area), often establish front companies very similar to Bells Inter Trading in the lesser-scrutinized areas of the world. These companies, operating in structures most comparable to organized crime families, a concept best outlined in [DTEX's "Exposing the DPRK's Cyber Syndicate" report](#), then bring on IT Workers such as Lian Hung to generate additional revenue for the company to sustain itself.

We believe that this is an important consideration to make regarding IT Workers, who are commonly misunderstood as a single-unified threat group. Rather than viewing them as a monolithic entity, North Korean IT Workers are more akin to individual entrepreneurs operating under the blessing of a higher-status boss. These bosses are often themselves working under the banner of a larger company or organization subservient to a DPRK government bureau, agency, or the KPA. As an IT Worker gains more status and respect, they are able to climb the organization's ranks and eventually become bosses themselves. From there they may form their own front companies and gain the status necessary to take on more malicious

activity (if they so choose). We believe Lian Hung and Hailong Jin, both appearing to be in their 30s-40s, may be operating as middle managers or hold higher statuses in this structure, which may explain their titles of choice being "Project Manager".

This structure is precisely why we believe that understanding the IT Workers as a single threat is a significant mistake and why we believe that there should be more effort placed on investigating unique activity clusters. The IT Workers are an ecosystem, and in order to better understand them, comprehend their associated risk levels, and ultimately counter them, it is important to identify how they fit into the larger North Korean economy and how the broader IT ecosystem that they are a part of functions. The North Korean in Rason trying to get hired at your enterprise is part of the same ecosystem as the North Korean in Tanzania picking up jobs on UpWork, the Andariel operator ransoming a hospital, and the Solidity developer in Laos who just stole millions from another blockchain project.

Recognizing the interconnected nature of North Korean cyber operations, and framing it as an ecosystem that varies from low-level IT workers to sophisticated APT groups, is crucial for developing more effective countermeasures and attribution frameworks. Only by understanding the full scope of this ecosystem can we hope to learn from it and meaningfully disrupt it.

IOCs.

Lian Hung:

Emails:

ayusuphnhina@gmail.com
lianhung21@hotmail.com
lianhung21@gmail.com
mano12@gmail.com
liuqimi21@gmail.com
alex@bellsstudio.site
libfredrick@gmail.com
michaeldein243@gmail.com
josephdgray211@hotmail.com
marogus211@outlook.com
briandwingo55@yahoo.com
silverbeach613@gmail.com
wilsonliuq2111@outlook.com
munjin22@gmail.com
guangheli211@gmail.com
wilsondovi21@gmail.com
asemenovboyarka@gmail.com
alex@bellsstudio.site

freeserviceexpert@gmail.com
sadah12290@gmail.com
leoxtechdev@gmail.com
goldenharvestmidas@gmail.com

Sites:

marogus211.wixsite.com
youtube.com/@liberathachannel
linkedin.com/in/lian-hung-129b47158
smart.5starlink.online
facebook.com/LeoXTech

IPs:

102.215.28.11

Hailong Jin:

Personas:

Hailong Jin
Gabriel Rodrigues de Souza
Volodymyr Yakubovskiy

Emails:

goldsea808@gmail.com
goldsea808@yahoo.com
ddksniper@gmail.com

Sites:

linkedin.com/in/hailong-jin-906375118
facebook.com/profile.php?id=100083340646764
youtube.com/@jackddk7187
global808.wixsite.com
our-dream-technologies.vercel.app

intellichain555:

Emails:

intellichain555@gmail.com
chainerspace@gmail.com
fullasher@gmail.com

cyberos999@gmail.com
odincui@gmail.com
sunnykan314@gmail.com
salbu15154@gmail.com
salbuvabybit@hotmail.com
mykytadunaiev@outlook.com
moktamd3@gmail.com

Sites:

github.com/intellichain555

Bells Inter Trading:

Sites:

bellastudio.online
bellsstudio.site

IPs:

69.30.210.152 - 69.30.210.159
107.150.47.16 - 107.150.47.23
173.208.245.144 - 173.208.245.151

VPNs:

<https://apps.apple.com/us/app/swift-vpn/id1612950256>
<https://apps.apple.com/ie/app/tiles-matching/id6737127654>
<https://play.google.com/store/apps/details?id=com.free.stealthvpn&hl=en-US>
<https://play.google.com/store/apps/details?id=com.freevpn.fastvpn&hl=en-US>
<https://play.google.com/store/apps/details?id=com.freevpn.oryxvpn&hl=en>
<https://play.google.com/store/apps/details?id=com.fastvpn.dreamvpn&hl=en>
<https://www.ldplayer.net/games/tiles-matching-travel-puzzle-on-pc.html>
https://play.google.com/store/apps/details?id=com.halleyvpn.freevpn&hl=en_US
https://play.google.com/store/apps/details?id=com.ace.freevpn&hl=es_US
https://play.google.com/store/apps/details?id=app.swift.uaevpn&hl=es_US
https://play.google.com/store/apps/details?id=com.freevpn.smartvpn&hl=es_US
<https://shot-vpn-unlimited-free-vpn-proxy.en.softonic.com/android>
<https://play.google.com/store/apps/details?id=com.fastvpn.dreamvpn&hl=en>
<https://apkcombo.com/ultraconnect-vpn/com.ultraconnect.ultraconnectvpn/>

<https://apkpure.com/guardian-vpn/app.star.guardianvpn/download>