DPRK IT Workers | A Network of Active Front Companies and Their Links to China

Tom Hegel

Executive Summary

- SentinelLabs has identified unique characteristics of multiple websites, now seized by the US Government, associated with the DPRK IT Worker front companies.
- We assess with high confidence that DPRK actors seek to impersonate US based software and technology consulting businesses by copying the online brands of legitimate organizations, seeking to use these for financial objectives.
- SentinelLabs has linked the activity to several active front companies and links these with high confidence to a larger set of organizations being created in China.
- Our findings link additional companies, which remain active today, to the DPRK IT Workers scheme.

Background

North Korea operates a global network of IT workers, both as individuals and under front companies, to evade sanctions and generate revenue for the regime. These workers are highly skilled in areas like software development, mobile applications, blockchain, and cryptocurrency technologies. By posing as professionals from other countries using fake identities and forged credentials, they secure remote jobs and freelance contracts with businesses worldwide.

Our PinnacleOne team has compiled an executive summary of this threat, available here.

Front companies, often based in China, Russia, Southeast Asia, and Africa, play a key role in masking the workers' true origins and managing payments. Notable examples include China-based Yanbian Silverstar Network Technology Co. Ltd., disrupted in October 2023, and Russia-based Volasys Silver Star, sanctioned by the U.S. Department of the Treasury in 2018, for their roles in facilitating fraudulent IT operations. These entities helped DPRK workers launder earnings through online payment services and Chinese bank accounts. The payments, often routed through cryptocurrencies or shadow banking systems, ultimately support state programs, including weapons development, circumventing international sanctions.

These schemes present significant risks to employers, including potential legal violations, reputational damage, and insider threats such as intellectual property theft or malware implantation. Addressing these risks requires heightened awareness and stringent vetting processes to limit North Korea's ability to exploit global tech markets.

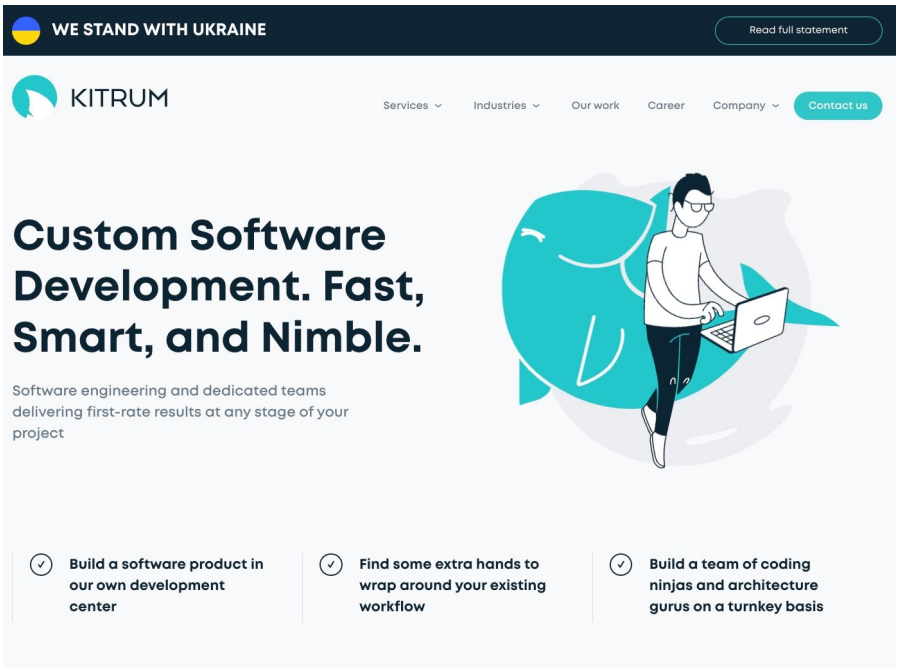
This blog explores four newly identified examples of DPRK IT Worker front companies, analyzing their online presence and the methods they use to appear legitimate to unsuspecting targets in recent months. These four companies' websites were recently subject to law enforcement action and taken offline.

Independent Lab LLC

The Independent Lab LLC website, `inditechlab[.]com` was active since at least February 2024, with indication it was acquired and operated using InterServer hosting since May 2022 (`174.138.181[.]198`). The domain itself was registered through NameCheap.

The content of the website is in line with what you would expect of a legitimate software development outsourcing business, with no obvious major indicators associated with the DPRK, or even illegitimate in any way. In the case of Independent Lab LLC, the website format and content was copied from Kitrum, a legitimate custom software firm headquartered in the United States. The DPRK actors did not retain the "We Stand with Ukraine" link or menu header.

DPRK IT Worker Front Company Website – Independent Lab LLChot



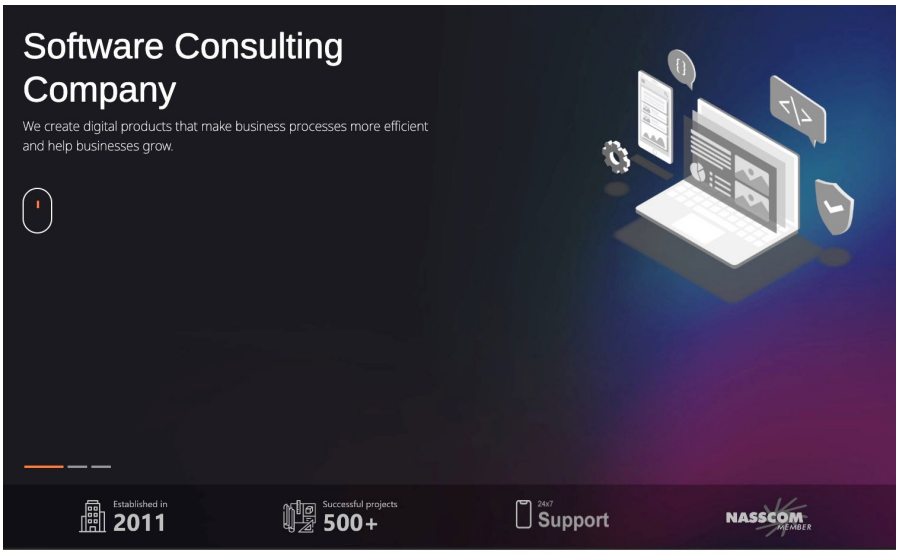
Legitimate business, source of copied website design used by DPRK

The content of the website centered around the Contact Us form, enticing visitors to engage in communications, providing no contact details on the website itself.

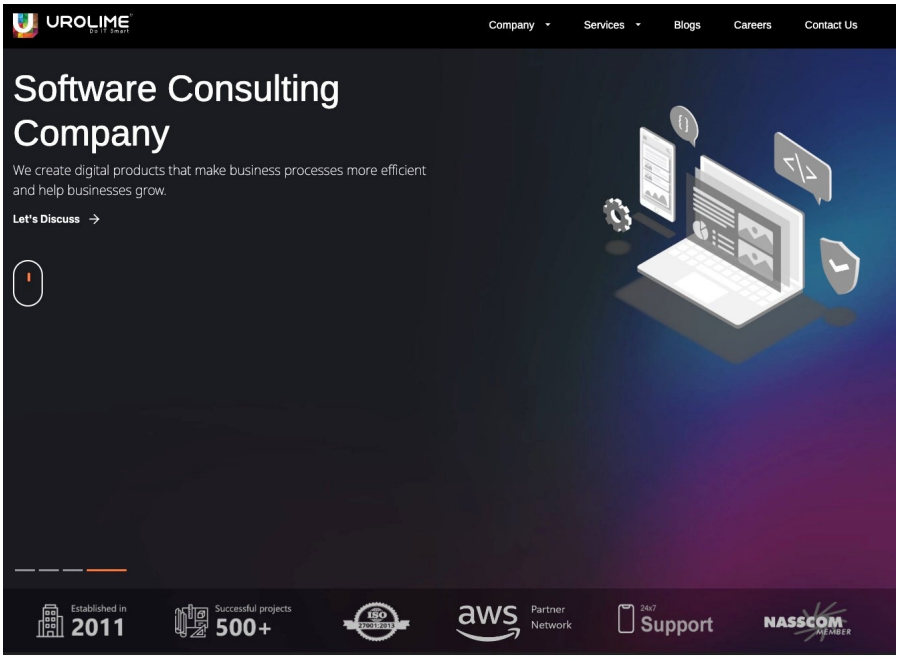
Shenyang Tonywang Technology LTD

The name “Shenyang Tonywang Technology” was used in the formal content of the website; however, the domain itself is `tonywangtech[.]com`. The website first became active in November 2023, overlapping with previously used InterServer hosting infrastructure (`174.138.181[.]198`), and was also registered via NameCheap.

Similar to the previous example, Shenyang Tonywang Technology advertises itself as a top software consulting company with bespoke solutions, including DevOps & cloud consulting. In this case, the website format and content was copied from Urolime, a legitimate DevOps consulting company headquartered in the United States.



DPRK IT Worker Front Company Website – Shenyang Tonywang Technology LTD



Legitimate Urolime business, source of copied website design used by DPRK

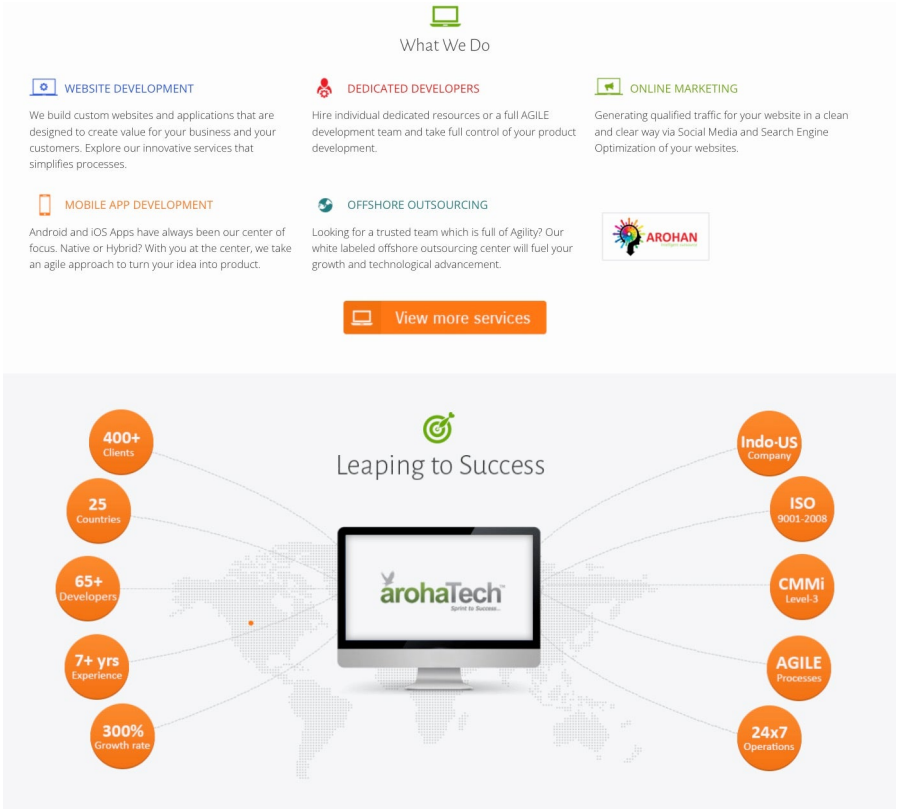
Tony WKJ LLC

Tony WKJ LLC IT Services website, `wkjllc[.]com`, was active since at least May 2024, with indication it was acquired and operated using InterServer hosting (`174.138.181[.]198`) since May 2022. The domain itself was registered through NameCheap.

Tony WKJ LLC advertises itself as a leading software development company that specializes in Agile IT development. Once again, In this case the website format and content was copied from a legitimate business. Specifically, this website is a copy from ArohaTech IT Services, a software and web development company headquartered in Noida, India.

However, a comparison to the legitimate website reveals that the DPRK actors have not only placed their own name, and removed original ArohaTech logos, they have also modified the content to clearly attempt to brand Tony WKJ LLC as a US based company.

DPRK IT Worker Front Company Website – Tony WKJ LLC

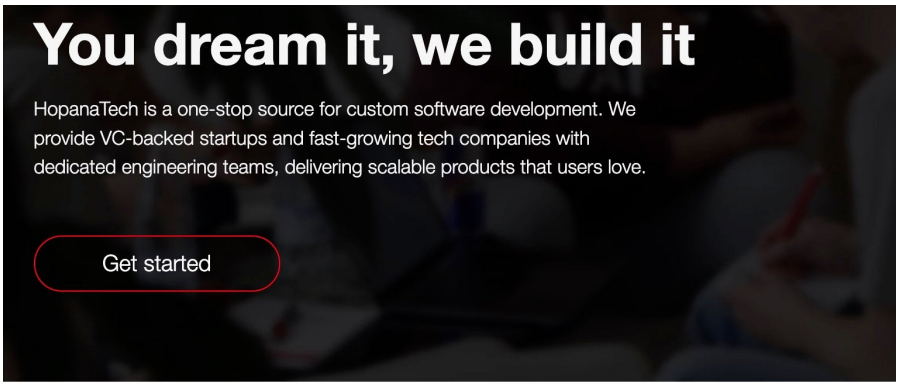


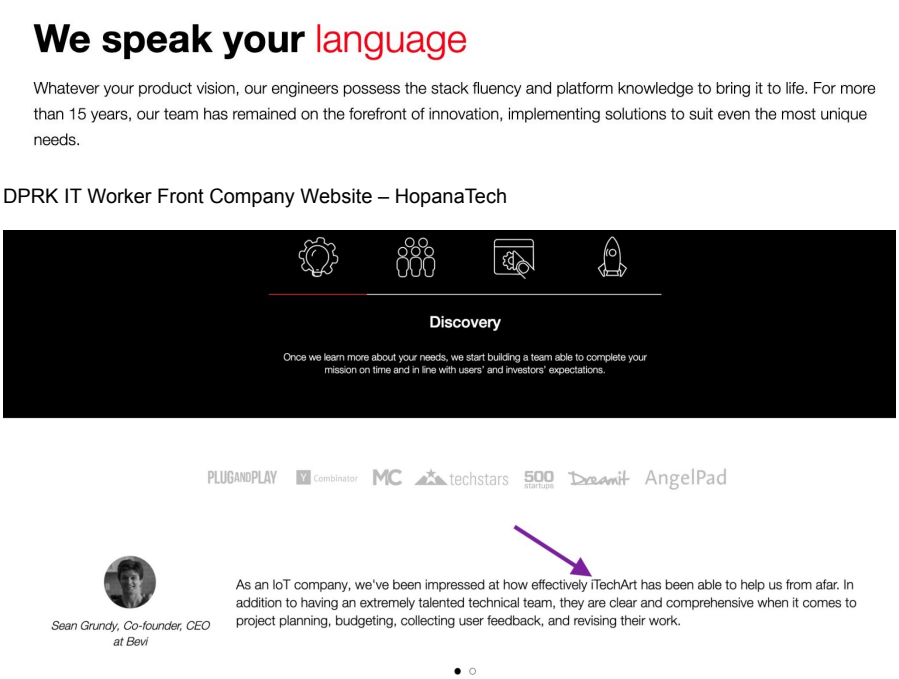
Legitimate business, source of copied website design used by DPRK

HopanaTech

HopanaTech website, `hopanatech[.]com` is a bit more unique from the others above. The domain itself was first registered in November 2020, and began hosting publicly via Asia Web Services Ltd (`180.235.135[.]177`) in December 2020. The website has been presented as shown below since at least the end of 2021. The domain was registered through NameCheap.

The website content aligns with the previous examples, including the description of being a custom software development company. The HopanaTech version of the content has been modified significantly; however, it continued to make use of customer reviews and marketing content from legitimate public websites. However, in some cases, content that would have required more than a simple text edit remains unchanged, showing the original sources name, such as the legitimate ITechArt firm's website.





DPRK IT Worker Front Company Website – HopanaTech

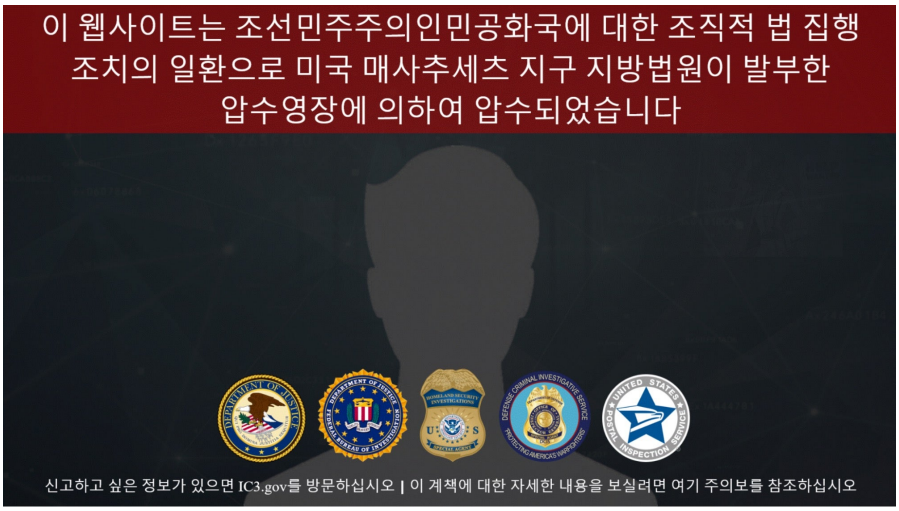
DPRK IT Worker Front Company Website – HopanaTech – Showing content source

United States Government Response

Each of the above four companies has been disrupted by US Government agencies, specifically the Department of Justice, Federal Bureau of Investigation, Homeland Security Investigations, Defense Criminal Investigative Service, and the United States Postal Inspection Service.

On October 10th, the US Government seized the four domains belonging to the front companies, each of which now shows the standard takedown alert and links to the 2022 US Treasury fact sheet on DPRKs IT Worker scheme. The websites rotate between English and Korean language versions.

Domain Seized Alert – English



Domain Seized Alert – Korean

Expanded Analysis

Drawing on details from the four companies disrupted by US Government agencies, SentinelLabs was able to find multiple leads to an active network of DPRK IT front companies originating in China.

The Mysterious A1 Building

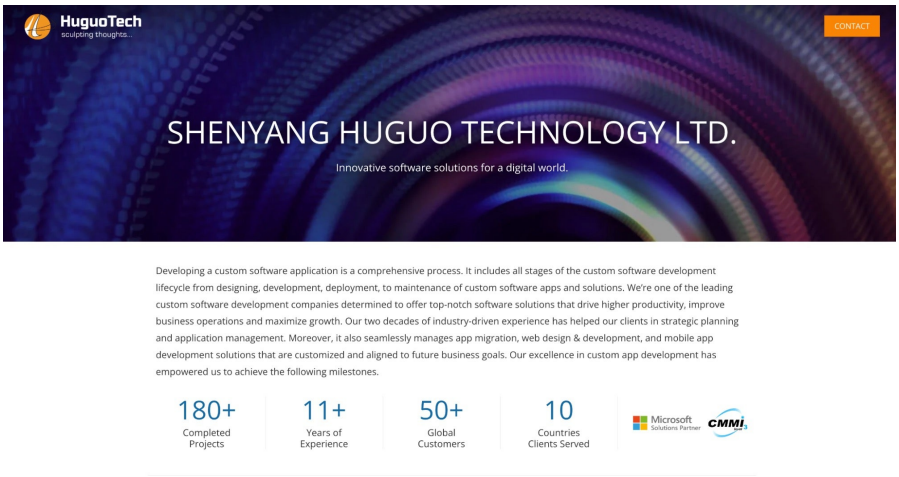
In an early 2024 archived snapshot of Shenyang Tonywang Technology's website, `tonywangtech[.]com`, we can see the actor added the following address:

No. 1006-25, Building A1, No. 11, Tawan Street, Huanggu District, Shenyang City Liaoning 110036

tonywangtech[.]com listed address and contact details

We identified an additional company with similar traits. First, the address happens to be highly close in proximity – listed next to each other on the same floor of the same building. *No. 1006-23, Building A1, No. 11, Tawan Street, Huanggu, Shenyang, Liaoning, China*

The additional company is Shenyang Huguo Technology Ltd, which uses the domain `huguotechltd[.]com` in a similar way to the previous four. The website uses copied content and logos from the legitimate Indian software firm TatvaSoft.



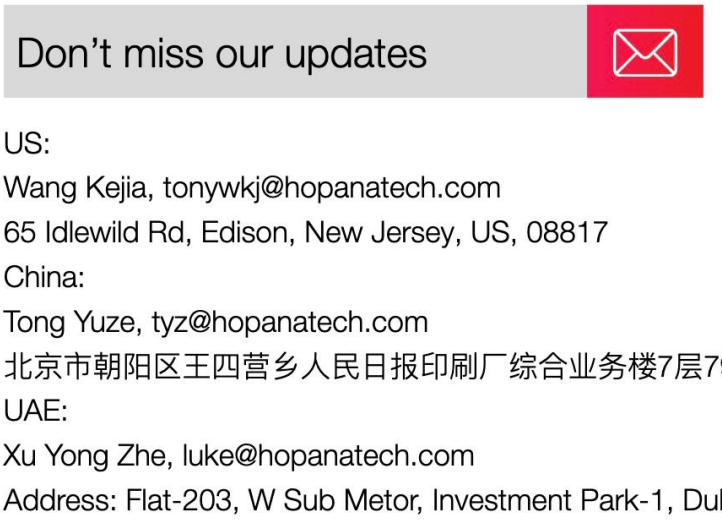
Active DPRK linked company website -Shenyang Huguo Technology Ltd

The `huguotechltd[.]com` domain was registered in October 2023 via NameCheap. The domain has since been and continues to be hosted at `103.15.29[.]44`, of Asia Web Services Ltd.

We assess Shenyang Huguo Technology Ltd. is closely associated with the previously four reviewed DPRK IT Worker front companies, and had remained online long enough to have been used to achieve the DPRKs objectives.

The Tony Wang Link

HopanaTech's website, `hopanatech[.]com`, listed three contacts before it was taken down by law enforcement. The first person, Wang Kejia, is listed with the email address "Tonywkj".



Contacts from the now-seized HopanaTech website

The "wkj" is almost certainly the acronym for the preceding Chinese name, Wang Kejia. The `Tonywkj@Hopana` email address establishes a link between Wang Kejia, a real person who is a resident of the address in New Jersey and the "Tony Wang" identity. The Shenyang Tonywang Technology Company website discussed above was also subject to law enforcement action, and its name bears resemblance to the same Tongwkj listed by Hopana. Furthermore, the Tonywkj email also directly matches the domain of another taken-down DPRK IT Worker site discussed above, Tony WKJ LLC.

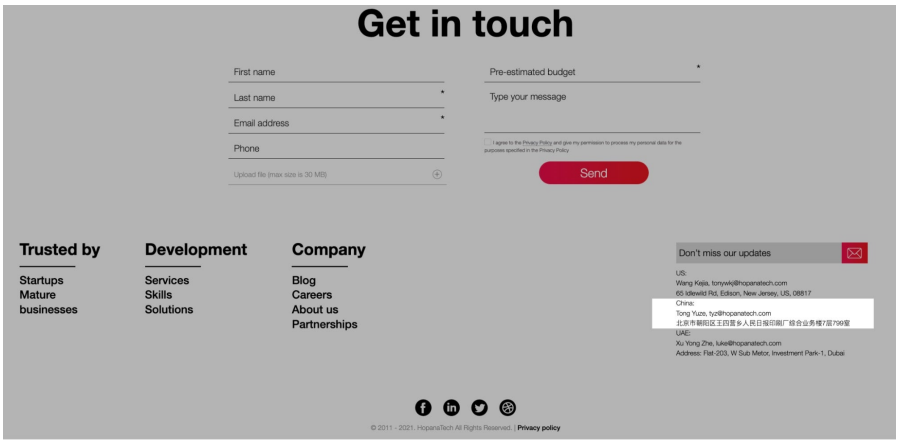
The Tong Yuze Identity

Law enforcement action established that Hopana Tech and `Hopanatech[.]com` are DRPK IT Worker Front companies. This analysis expands on the Hopana Tech company corporate registration data inside China.

A corporate records website from the PRC indicates the Beijing Xiwang Technology Company (北京市戏网科技有限公司), previously used the name Beijing Hou Pa Na Technology Company (北京后帕纳科技有限公司), a clear cognate for the English-translated "HopanaTech."

Corporate record showing Xiwang's previous use of the Hopana Technology name

Furthermore, the above screenshot of HopanaTech's website, which lists the Tonywkj email address, also lists Tong Yuze (佟雨泽). The same name is used for the corporate registrant of Beijing Xiwang Technology Company.Highlighted text shows that Beijing Xiwang Technology was previously known as Hopana Tech.



Contacts from the now-seized HopanaTech website

As if to allay concerns that Beijing Xiwang Technology Company was not a front company, corporate records show the firm only pays unemployment insurance, health insurance, and employee injury liability insurance for one person.

Corporate records for Bejing Xiwang Technology Company

Tong Yuze is currently listed as the corporate registrant of 25 companies in China, including many restaurants and catering companies. Owing to increased data protection measures by the PRC, a complete accounting of Tong Yuze's companies is not possible.

Some companies identified as Tong Yuze's include:

- 海口宜路畅佟科技贸易有限公司
- 北京上日清新食品有限公司
- 京山味诚（北京）餐饮管理有限公司
- 泽日启程（北京）餐饮管理有限公司
- 北京哈巴萨科贸有限公司

This foray into restaurants does not appear to be a case of mistaken identity. The email provided for Tong Yuze on the registration of Beijing Xiwang Technology Company is `tongyuze@jswc[.]com[.]cn`. The email domain "JSWC" aligns with the name of some of Tong Yuze's restaurant companies. In this case, Jing Shan Wei Cheng (京山味诚), matches the acronym of the email domain. This provides reasonable evidence of a legitimate connection between Tong Yuze and the mentioned food service companies.

Given the very real businesses being run by Tong Yuze's other corporate registrations– seemingly many franchises of Yiwei Yicheng (一味一诚) –it's possible this individual is serving as a cut-out for the DPRK. We hypothesize that his collection of businesses may serve to provide cover for illegal ones.

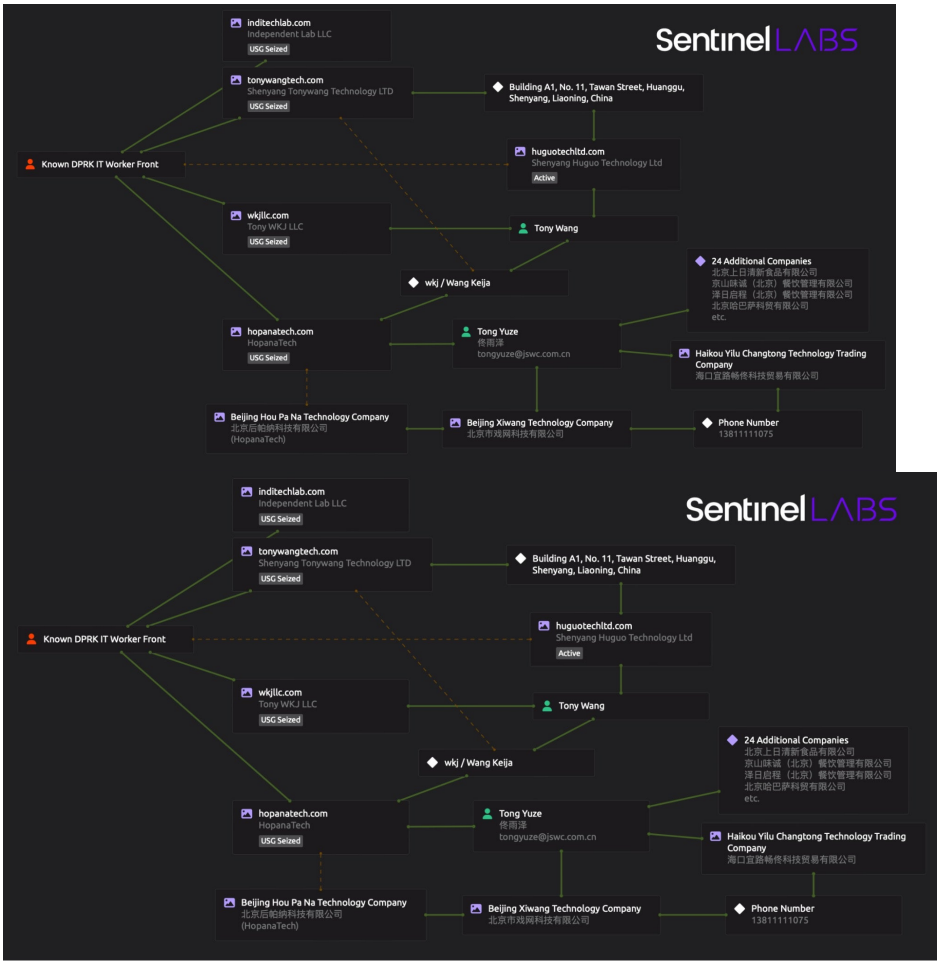
The Haikou Yilu Changtong Technology Trading Company

One of the companies connected to the Tong Yuze identity and accessible on corporate registration sites is Haikou Yilu Changtong Technology Trading Company (海口宜路畅佟科技贸易有限公司).

Haikou Yilu Changtong Technology Trading Company corporate registration

Haikou Yilu is distinct from the other Tong Yuze-registered companies for two reasons. First, it is another technology company–not a restaurant. Second, its corporate registration makes use of a telephone number that differs from Tong Yuze's restaurant businesses but is shared with the Beijing Xiwang Technology Company corporate registration.

To help visualize the connections we described, the graphic below provides a simplified representation of the key relationships and pivots.



Visual representation of front company connections

Conclusion

The DPRK's use of the IT Worker scheme underscores the regime's adaptability in exploiting global markets to further its financial objectives. By impersonating legitimate U.S.-based software and technology consulting firms, North Korean actors aim to gain trust and access to sensitive contracts, circumventing sanctions and evading detection. These tactics highlight a deliberate and evolving strategy that leverages the global digital economy to fund state activities, including weapons development.

Our research not only exposes the deceptive tactics employed by DPRK IT workers but also connects these efforts to a broader, active network of front companies originating in China. This linkage emphasizes the scale and complexity of North Korea's financial schemes and the importance of vigilance across industries. Organizations are urged to implement robust vetting processes, including careful scrutiny of potential contractors and suppliers, to mitigate risks and prevent inadvertent support of such illicit operations. By shedding light on these activities, SentinelLabs aims to equip businesses, governments, and the public with the insights needed to stay ahead of these threats and safeguard the integrity of global markets.