NISOS

THREAT ANALYSIS

Investigation: Probable DPRK Online Personas Used To Fraudulently Obtain Remote Employment At U.S. Companies

December 2023

RESEARCH

Table of Contents

EXECUTIVE SUMMARY

Nisos investigators identified a number of online personas probably used by the Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) information technology (IT) workers to fraudulently obtain remote employment from unwitting companies in the United States. IT workers, like the ones identified, provide a critical stream of revenue that helps fund the DPRK regime's highest economic and security priorities, such as its weapons development program, and may also leak intellectual property (IP) and other sensitive information to the DPRK. Hiring DPRK employees is a violation of U.S. and United Nations (UN) sanctions.

The identified personas claim to have highly sought after technical skills and experience and often represent themselves as U.S.-based teleworkers, but Nisos investigators found indications that they are based abroad. Boasting expert level skills in mobile and web-based applications as well as a number of programming languages, the personas also list significant remote work experience which can be difficult to verify. The personas further obfuscate their identities by impersonating U.S. based individuals' identities and/or copying resume content from publicly visible profiles of unassociated individuals, further increasing the difficulty of identifying the personas.

Investigators found the following commonalities in the personas' profiles and resumes:

- Personas claim to have experience developing web and mobile applications, knowledge of multiple programming languages, and an understanding of blockchain technology.
- Personas have accounts on employment and people information websites as well as IT industry-specific freelance contracting platforms, software development tools and platforms, and common messaging applications, but typically lack social media accounts, suggesting that the personas are created solely for the purpose of acquiring employment.
- Photos of the same individual are used to create multiple personas.
- Personas have several accounts with the same name and photo that are sometimes associated with different locations, some of which are abroad.
- Personas' accounts contain only minimal information, and some of the resume content on the accounts is likely copied from real individuals in the IT industry.

DISCLAIMER:

The reporting contained herein from the Nisos research organization consists of analysis reflecting assessments of probability and levels of confidence and should not necessarily be construed as fact. All content is provided on an as-is basis and does not constitute professional advice, and its accuracy reflects the reliability, timeliness, authority, and relevancy of the sourcing underlying those analytic assessments.

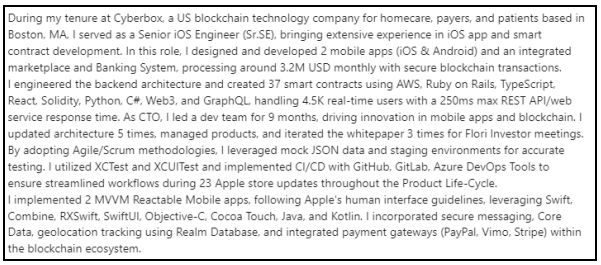
BACKGROUND

On 16 May 2022, the U.S. Department of State, the U.S. Department of the Treasury, and the Federal Bureau of Investigation (FBI) issued an advisory for the international community, the private sector, and the public, which warned of attempts by DPRK IT workers to obtain employment while posing as non-North Korean nationals.

According to the advisory, all DPRK IT workers earn money to support North Korean leader Kim Jong Un's regime. The vast majority of them are subordinate to and working on behalf of entities directly involved in the DPRK's UN-prohibited Weapons of Mass Destruction (WMD) and ballistic missile programs, as well as its advanced conventional weapons development and trade sectors. This results in revenue generated by these DPRK IT workers being used by the DPRK to develop its WMD and ballistic programs, in violation of U.S. and UN sanctions. Many of these entities have been designated for sanctions by the UN and United States.[1]

SKILLS AND INTERESTS

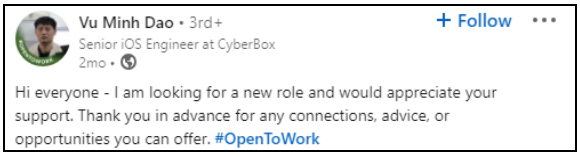
Investigators found that the personas often claimed to be proficient in developing several different types of applications and have experience working with crypto and blockchain transactions. Further, all of the personas sought remote-only positions in the technology sector and were singularly focused on obtaining new employment.


During my tenure at Cyberbox, a US blockchain technology company for homecare, payers, and patients based in Boston, MA, I served as a Senior iOS Engineer (Sr.SE), bringing extensive experience in iOS app and smart contract development. In this role, I designed and developed 2 mobile apps (iOS & Android) and an integrated marketplace and Banking System, processing around 3.2M USD monthly with secure blockchain transactions.
I engineered the backend architecture and created 37 smart contracts using AWS, Ruby on Rails, TypeScript, React, Solidity, Python, C#, Web3, and GraphQL, handling 4.5K real-time users with a 250ms max REST API/web service response time. As CTO, I led a dev team for 9 months, driving innovation in mobile apps and blockchain. I updated architecture 5 times, managed products, and iterated the whitepaper 3 times for Flori Investor meetings. By adopting Agile/Scrum methodologies, I leveraged mock JSON data and staging environments for accurate testing. I utilized XCTest and XCUITest and implemented CI/CD with GitHub, GitLab, Azure DevOps Tools to ensure streamlined workflows during 23 Apple store updates throughout the Product Life-Cycle.
I implemented 2 MVVM Reactable Mobile apps, following Apple's human interface guidelines, leveraging Swift, Combine, RXSwift, SwiftUI, Objective-C, Cocoa Touch, Java, and Kotlin. I incorporated secure messaging, Core Data, geolocation tracking using Realm Database, and integrated payment gateways (PayPal, Vimo, Stripe) within the blockchain ecosystem.

Graphic 1: Vu Minh Dao's experience in blockchain transactions.[2]

Graphic 2: Alex Lu's experience in blockchain development.[3]

[1] https://ofac.treasury[.]gov/media/923126/download?inline
[2] https://www.linkedin[.]com/in/brunodao1
[3] https://www.linkedin[.]com/in/alex-lu-59592b270



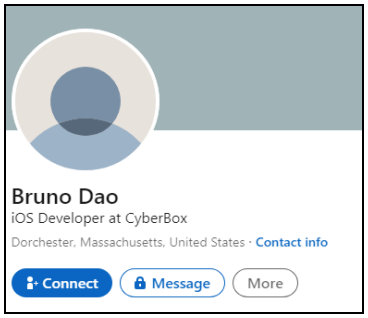
Graphic 3: Example of an online persona seeking a remote job.

Graphic 4: Bruno Dao refers to himself as an iOS and Blockchain Developer on his GitHub profile.[4]

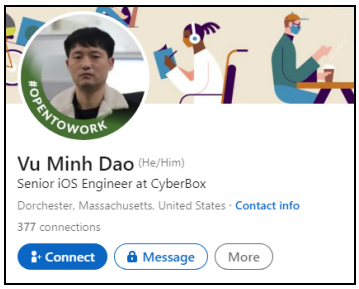
ONLINE PRESENCE

Nisos investigators found that although the personas are often active on professional networking sites, IT industry-specific freelance contracting platforms, software development platforms, and common messaging applications, they are usually not active on social media platforms. **Nisos assesses that the accounts were created solely for the purpose of acquiring employment.** Investigators found instances of several accounts, associated with a persona, using the same picture but different names; other accounts lacked profile photos. Investigators also found that many of the accounts are only active for a short period of time before they are disabled. **Nisos assesses the accounts remained active only for a short period of time because they were created in support of an application for a specific position or were flagged for fraudulent behavior and removed by the platform provider.**

Graphic 5: Bruno Dao LinkedIn profile that has since been disabled.[5]

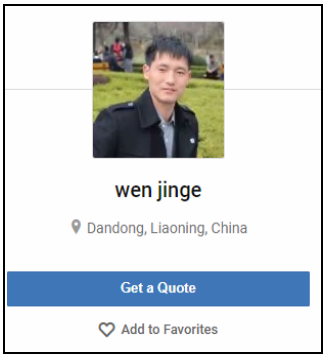


Graphic 6: Bruno Dao Linkedin profile.[6]

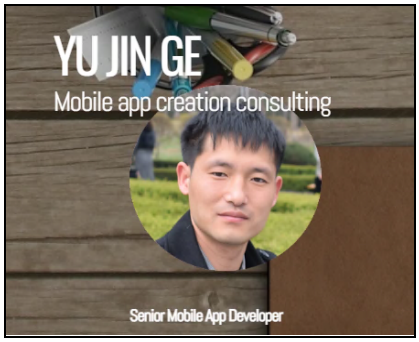


Graphic 7: Vu Minh Dao Linkedin profile features a different photo of the same individual.[7]

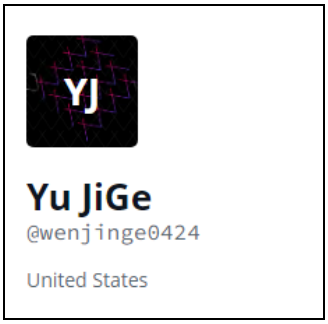
[4] https://www.github[.]com/wenjinge0424
[5] https://www.linkedin[.]com/in/brunodao
[6] https://www.linkedin[.]com/in/bruno-dao-270068274
[7] https://www.linkedin[.]com/in/brunodao1



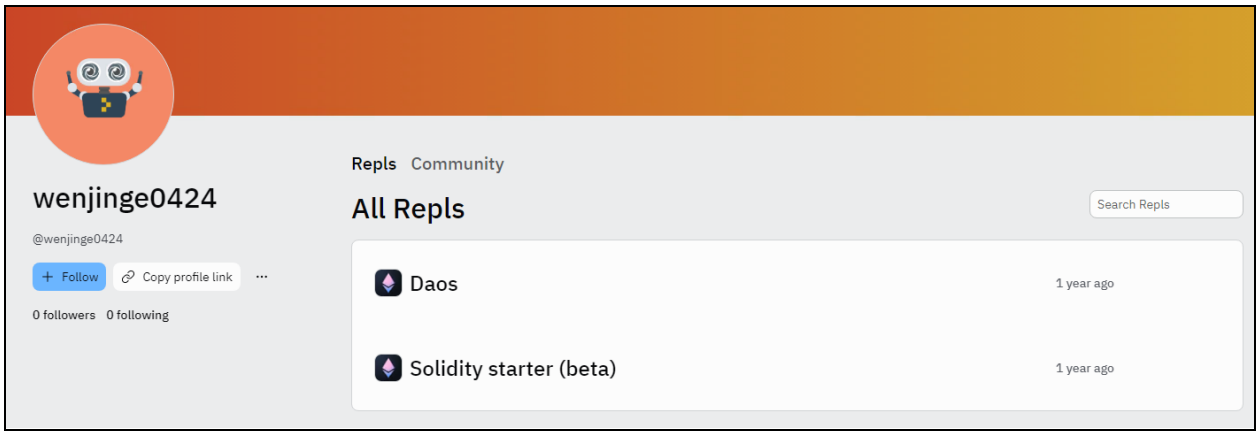
Graphic 8: Same photo used for "wen jinge" in Dandong, China on freelancer site Guru.[8]



Graphic 9: Same photo found on a personal website for mobile app developer "Yu Jin Ge."[9]



Graphics 10-11: Investigators identified two HackerRank profiles for the actor under different names.[10] [11] *HackerRank is a technology hiring platform that helps companies hire skilled developers in a remote-first environment and to evaluate tech talent during the recruiting process.*[12]



Graphic 12: Profile for @wenjinge0424 on Replit, an online integrated development environment, that contains a repl on Solidity, an object-oriented language designed to target the Ethereum Virtual Machine.[13]

[8] https://www.guru[.]com/freelancers/wen-jinge
[9] https://wenjinge.yahoosites[.]com/index.html
[10] https://www.hackerrank[.]com/profile/wenjinge0424
[11] https://www.hackerrank[.]com/profile/vuminhdao1984
[12] https://support.hackerrank[.]com/hc/en-us/articles/360045658233-Getting-Started-for-Recruiters
[13] https://replit[.]com/@wenjinge0424

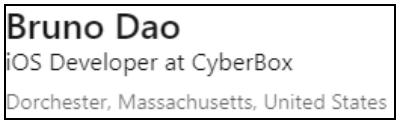
PERSONA INCONSISTENCIES

Investigators found that the profiles had inconsistencies in their location, with some accounts listing a location outside the U.S. The personas had little or no presence on common social networking sites, suggesting the aforementioned accounts had been created solely to support employment applications. Furthermore, investigators found that many of the personas' accounts were set up using enough information to showcase experience in the technology industry and to be publicly visible, but often used non-personalized content or templated language in posts. **Nisos assesses the persona accounts were created specifically to attract U.S. employers without providing a consistent online presence across multiple social media platforms.**

Location Inconsistencies

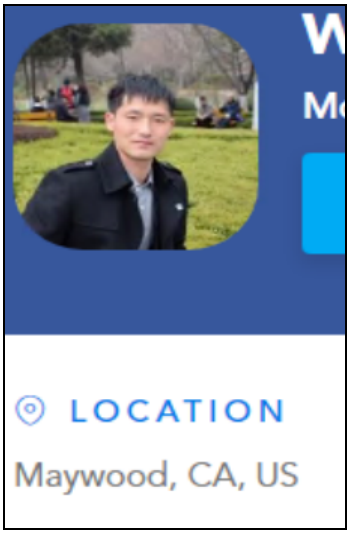
Investigators found that a large number of the identified individuals claim to be U.S. and Canada based, often based in the same location as the individual whose identity the account stole. Specifically, accounts claimed to be located in Alabama, California, Massachusetts, and Alberta (Canada). During the investigation into the accounts, investigators identified several U.S. based and likely U.S. citizens whose information was stolen by DPRK workers for location and employment verification purposes. The information stolen included name, address, driver's license, and social security number/card. A few of the accounts however, which included the same names and profile photographs, were located abroad, revealing inconsistency with the accounts and likely suggesting that the user is trying to appeal to a different client set with those accounts.

Graphic 13: Vu Min Dao's LinkedIn profile lists his location as Dorchester, Massachusetts.



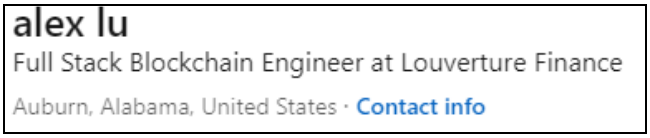
Graphic 14: Bruno Dao's LinkedIn profile lists his location as Dorchester, Massachusetts.

Graphic 15: Yu Jinge's ContactOut profile lists his location as Calgary, Alberta, Canada.



Graphic 16: Wen Jinge's RocketReach profile lists his location as Maywood, California.[14]

Graphic 17: Wen Jinge's Guru profile lists his location as Dandong, China.[15]



Graphic 18: Alex Lu's LinkedIn profile lists his location as Auburn, Alabama.

Graphic 19: Alex Lu's Language Exchange profile lists his location as Hong Kong.[16]

APPROPRIATED RESUME CONTENT

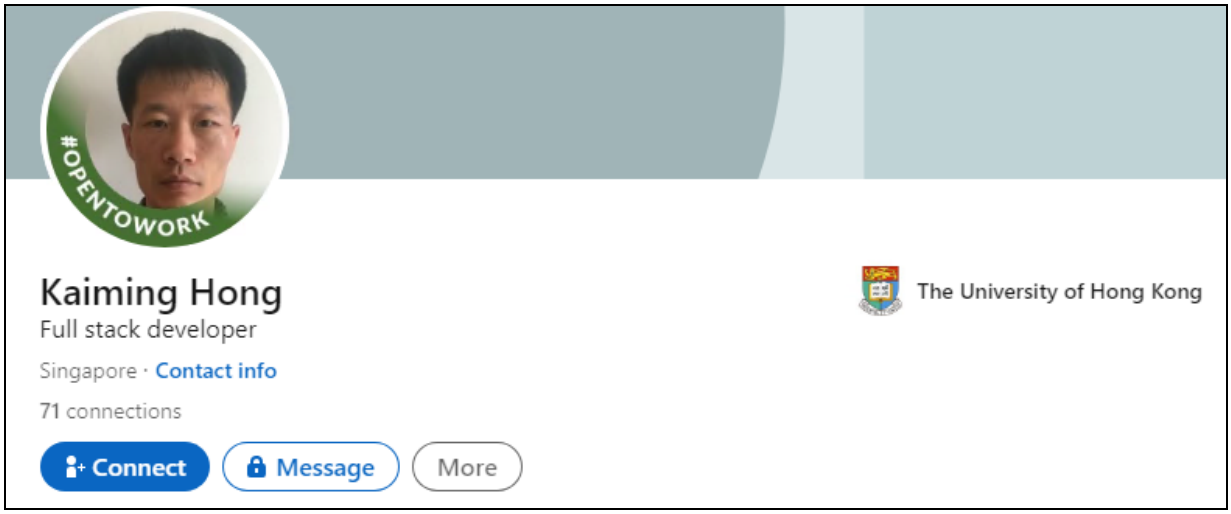
Investigators found that some of the resume content on the personas' accounts is identical to publicly visible resume content from other individuals in the technology industry. Investigators found no associations between the personas and the individuals, and **we assess that the personas' accounts were populated with appropriated content.**

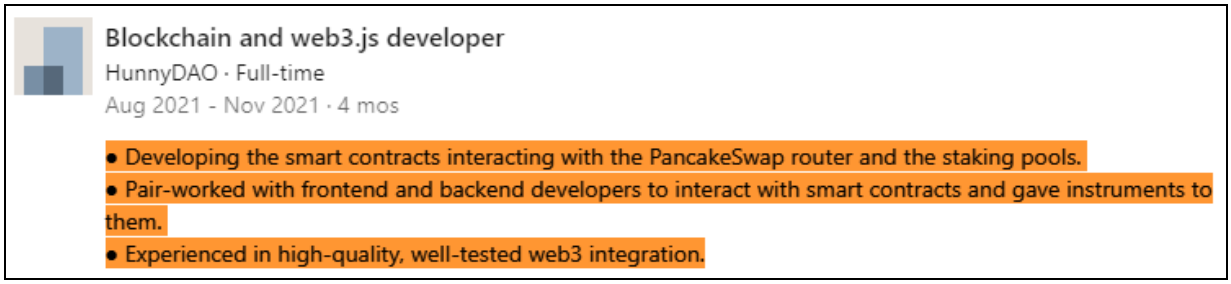
[14] https://rocketreach[.]co/wen-jinge-email_112745346
[15] https://www.guru[.]com/freelancers/wen-jinge
[16] https://en.language[.]exchange/friend/alexlu0917

Blockchain developer and web3.js developer 5/2021 - 11/2021
HunnyDAO

- Developing the smart contracts interacting with the PancakeSwap and the staking pools.
- Pair-worked with frontend and backend developers to interact with smart contracts and gave instruments to them.
- Experienced in high-quality, well-tested web3 integration.

Graphic 20: Section of Alex Lu's resume that matches other LinkedIn profiles.





Graphics 21-22: Kaiming Hong's LinkedIn profile with appropriated content highlighted.[17]

[17] https://www.linkedin[.]com/in/kaiming-hong-594679233