Research

How To Proactively Mitigate The DPRK IT Worker Employment Scam

March 2025

Table of Contents

Executive Summary

Nisos is tracking a network of likely North Korean (DPRK)-affiliated IT workers posing as Singaporean, Turkish, Finnish and US nationals with the goal of obtaining employment in remote IT, engineering, and full-stack blockchain positions. Through our research and client work we have detected and identified a number of fake personas since 2023. Successful mitigation of the risk relies on an improved vetting process for external remote candidates, which heavily relies on open-source intelligence (OSINT) checks of portfolio content and contact information, as the network re-uses this information. To assist security teams and business leaders with protecting their organizations and their clients, Nisos provides several steps that we recommend businesses implement in their hiring process to mitigate the DPRK-affiliated IT worker threat. Nisos also provides examples of how we used OSINT to identify four active fake personas. Karl Chong, currently appears to be employed as an engineer at a US-based strategic digital consultancy company. Two additional fake personas, Roman Kryveha and Ram Maharjan, who share contact information with Karl Chong, were likely created to also obtain remote employment as part of the employment scheme. Nisos also identified a fourth fake persona, John Alexander Bird, whose resume was created and updated via GitHub account imcode65 in 2024. This persona does not have an active personal website, suggesting that it is likely not actively seeking employment as part of the employment scheme yet.

Risk Mitigation Steps

The DPRK IT worker scheme is pervasive and targets companies of all sizes and in numerous industries, including cybersecurity. Learning opportunities for enterprise leaders include the following, which we recommend communicating to HR and IT teams within the organization:

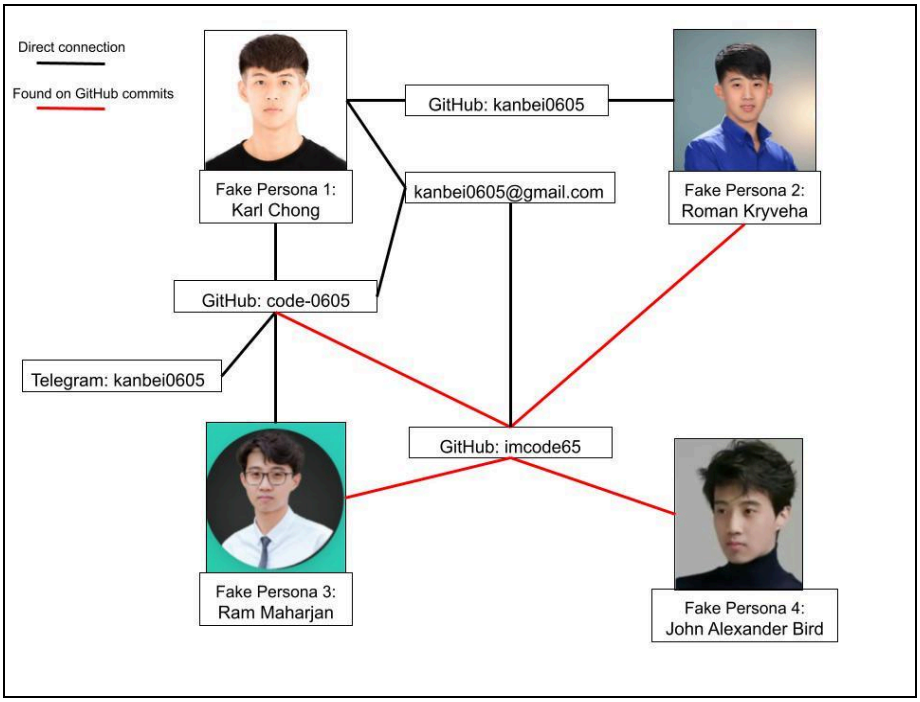
- Conduct reverse image searches to identify digitally manipulated profile pictures.
- Conduct expeditious OSINT checks to verify whether the provided phone numbers, email addresses, and GitHub accounts belong to the applicant and/or have been associated with other individuals.
- Review phone numbers and email addresses to determine whether applicants applied using the same contact information.
- Review stylometric attributes of the resume content to determine whether other resumes include the same language.
- Verify that locations match for all accounts linked to the applicant.
- Conduct a detailed review of the applicant’s online presence for consistency in name, appearance, work history, education, and other biographical details.
- Verify prior employment. Applicants often list major companies in their employment history, likely both to inflate their experience and to deter the hiring organization from contacting their provided references.
- Verify educational claims by contacting the institution's registrar office.

- Collect and retain all contact information for the references reviewed by HR in relation to the job applicant. References are often the same individual or connected to the same network of people as the job applicant.
- Ensure the interview process involves on-camera and/or in-person interviews.

Nisos researchers were able to identify four active personas by researching GitHub account activity and cross referencing contact information and profile photos. Nisos solely used OSINT checks and did not rely on proprietary tools or paid third party subscription tools.

Fake Persona Network

Nisos identified one persona, Karl Chong, who appears to have gained employment and three newly created personas seeking remote positions in Singapore, Turkey, Finland, and the United States. The newly created personas were all created and updated in 2024 in repositories linked to GitHub account imcode65. The account is associated with the email address kanbei0605@gmail[.]com, which is also associated with the persona Karl Chong.



Graphic 1: Network map of likely DPRK-affiliated personas.

Karl Chong

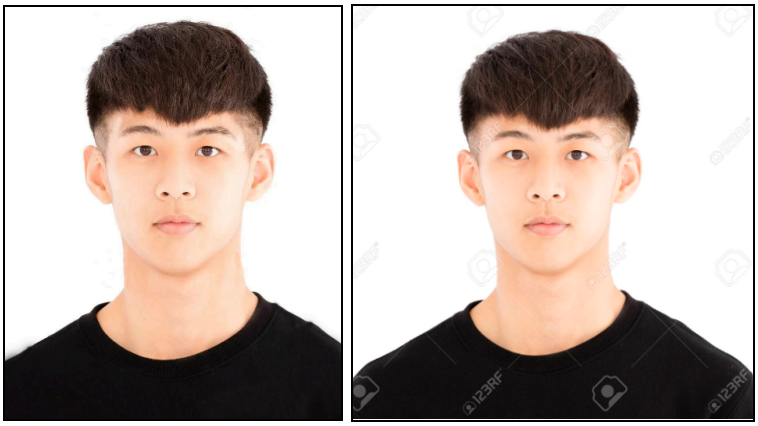
Nisos identified Karl Chong—used by a likely DPRK IT worker to obtain remote work in the United States—by investigating the GitHub account superredstar, which Nisos previously linked to a likely DPRK-affiliated network of remote worker personas.[1] The GitHub account superredstar was used to

[1]https://nisos[.]com/research/dprk-github-employment-fraud/

create a resume website for Karl Chong via GitHub in April 2022.[2] Karl Chong claims to be from Singapore and appears to be employed as a remote MERN Stack Developer at US-based Mongrov Inc since May 2023. Karl Chong has several freelancer accounts, which claim that he is located in the United States and Turkey. A review of the Karl Chong accounts and website revealed several tactics, techniques, and procedures (TTPs) previously associated with the DPRK employment scheme, including fake profile pictures, a lack of consistency of information across all accounts, the persona claiming to have experience developing web and mobile applications, knowledge of multiple programming languages, and reused resume content from other personas.

Fake Profile Photo

Karl Chong's website and freelancer accounts use the photo featured in Graphics 2-4, which is available for purchase on a number of stock photo websites. Nisos assesses that likely DPRK IT workers used this method to hide their true identities before using possible AI-enabled tooling to merge their faces onto pictures of other individuals.



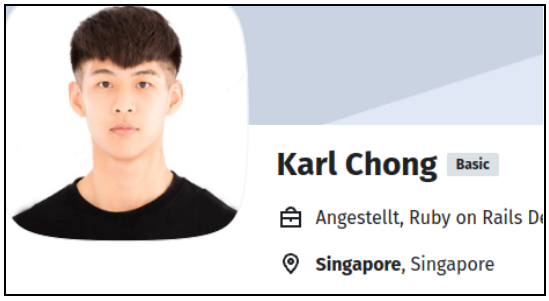
Graphics 2 and 3: Photo from Karl Chong's website (left).[3] Stock Photo used in Graphic 2 (right).[4]

Graphic 4: Mongrov Inc's website.[5]

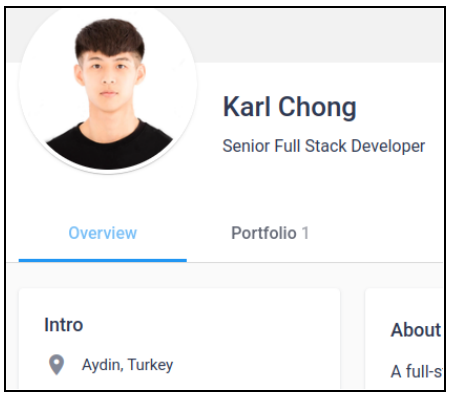
[2]https://github[.]com/kamaalsultan/shaorun-dev116.github.io/commit/584db387dc40149040b2b69cd301e5310d696cde
[3]https://kanbei-profile.vercel[.]app (inactive as of 18 March 2025)
[4]https://de.123rf[.]com/photo_66889836_nahaufnahme-asiatischen-jungen-mann-gesicht-portr%C3%A4t.html
[5]https://mongrov[.]com/about

Misaligned locations

Karl Chong claims to be located in Singapore, the United States, and Turkey on his various online resumes. Nisos assesses that the same persona is used to seek employment in different countries, which is why the persona's stated locations vary.



Graphics 5 and 6: Claimed location in the United States (left).[6] Claimed location in Singapore (right).[7]

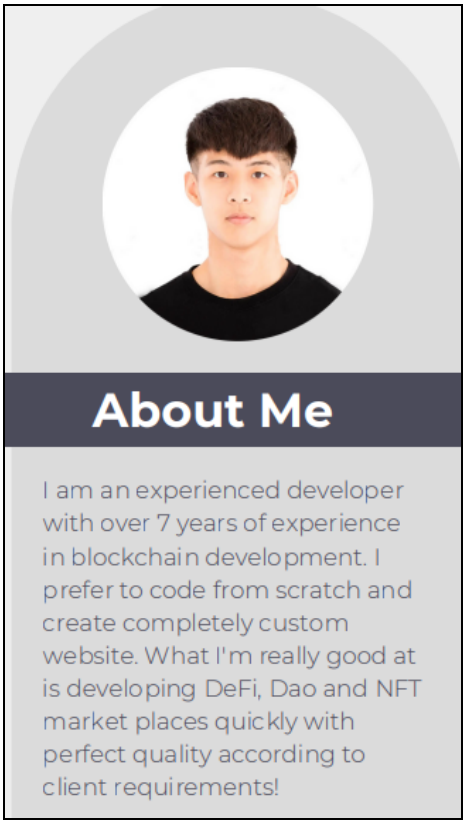


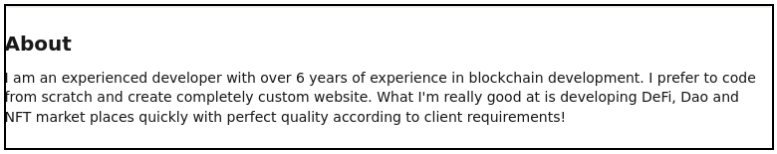
Graphic 7: Claimed location in Turkey.[8]

Reused Resume Content

Nisos found that Karl Chong's resume referenced the same employment history as another likely DPRK-affiliated persona, Naoyuki Tanaka, who appears to have been employed at Enver Studio.[9] Nisos assesses that likely DPRK IT workers reuse GitHub accounts and work portfolios to backstop their newly created personas. Additionally, another fake persona, Roman Kryveha, reused Karl Chong's about me intro paragraph from his resume and his stock photo.

[6]https://uploads.laborx[.]com/cv/JnxsPze0PBWteLNlGC6Fy0Axekuw3t2-.pdf
[7]https://www.xing[.]com/profile/Karl_Chong
[8]https://www.remotehub[.]com/karl.chong
[9]https://portfolio-one-navy-24[.]vercel.app





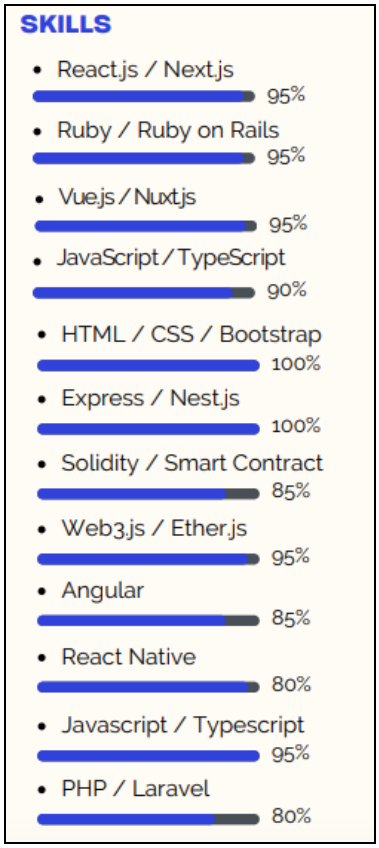
Graphics 8 and 9: Karl Chong's about me section (left).[10] Roman Kryveha's about me section (right).

Graphic 10: Karl Chong's resume lists work at Enver Studio.[11]

Significant Development Experience

Karl Chong lists a number of programming languages and certificates on his website. He also claims to have seven years of experience in front and back-end web development.

[10]https://uploads.laborx[.]com/cv/JnxsPze0PBWteLNlGC6Fy0Axekuw3t2-.pdf
[11]https://kanbei-profile.vercel[.]app/karlchong_resume.pdf



Graphic 11: Karl Chong's claimed skills.[12]

Freelancer Employment Websites Linked To Karl Chong

Nisos identified four freelance employment websites, which listed the persona name, location, GitHub, and work history of the persona. Many of the resumes indicated that Karl Chong worked at Overflow and studied at Singapore University of Technology and Design. The persona's profiles on freelancer websites include:

- https://remoteok[.]com/@karlchong
- https://laborx[.]com/freelancers/users/id100369
- https://www.remotehub[.]com/karl.chong
- https://www.xing[.]com/profile/Karl_Chong

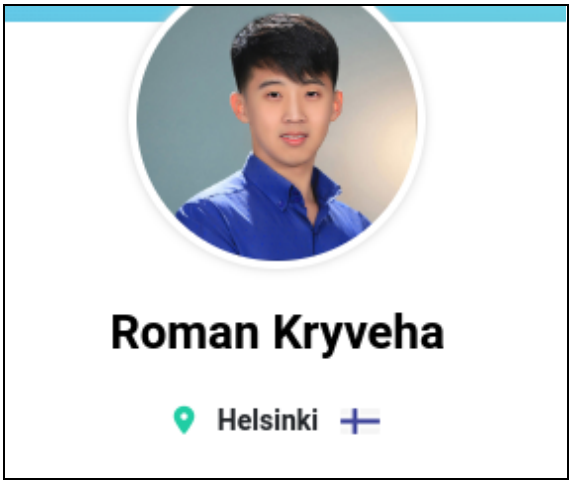
Newly Created Personas

Nisos identified three personas that share usernames and GitHub accounts with Karl Chong. A review of GitHub commits shows that the three accounts were all created and updated between March and May 2024.

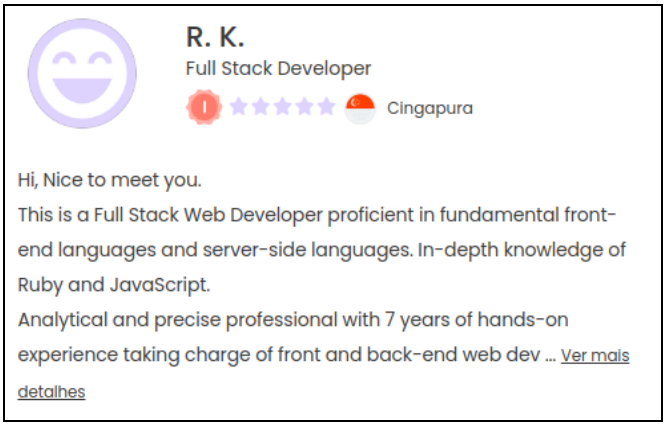
[12]https://kanbei-profile.vercel[.]app/karlchong_resume.pdf

Roman Kryveha

Roman Kryveha claims to be a senior front-end and full-stack developer from Finland. His website lists the same date of birth as Karl Chong's website, and he claims to be the user of GitHub account kanbei0605.[13] Roman Kryveha has two accounts on freelancer websites, which list his locations as Finland and Singapore.



Graphic 12: Roman Kryveha claiming to be located in Finland.[14]



Graphic 13: Roman Kryveha claiming to be located in Singapore.[15]

Reused portfolio content

Many of the portfolio examples on Roman Kryveha's website were designed by a different individual, Haoming, and are based on templates linking to website Bootstrapmade[.]com.

[13]https://roman-profile.vercel[.]app
[14]https://www.freelancermap[.]com/profile/roman-kryveha
[15]https://www.workana[.]com/freelancer/9f5b1c09ff8c3e6e7316632859332e11

Graphic 14: Example of work experience designed by someone else.[16]

Ram Maharjan

Ram Maharjan claims to be a full-stack and senior front-end developer. His website lists the same GitHub account, code-0605, as Karl Chong's website.[17]

Digital Photo Manipulation

Ram Maharjan's website contains a photograph of the likely DPRK IT worker, which was digitally manipulated. Nisos assess that the head of the individual was pasted onto a photo of remote content writer, Tan Dang.

Graphic 15: Photo from Ram Maharjan's website.[18]

Graphic 16: Photo of remote content writer Tan Dang.[19]

Backstopping

Both the Karl Chong and Ram Maharjan personas listed GitHub username code-0605 in their contact information in their resumes.[20] [21] Nisos assesses that likely DPRK IT workers reuse GitHub accounts to backstop their newly created personas with matured work profiles.

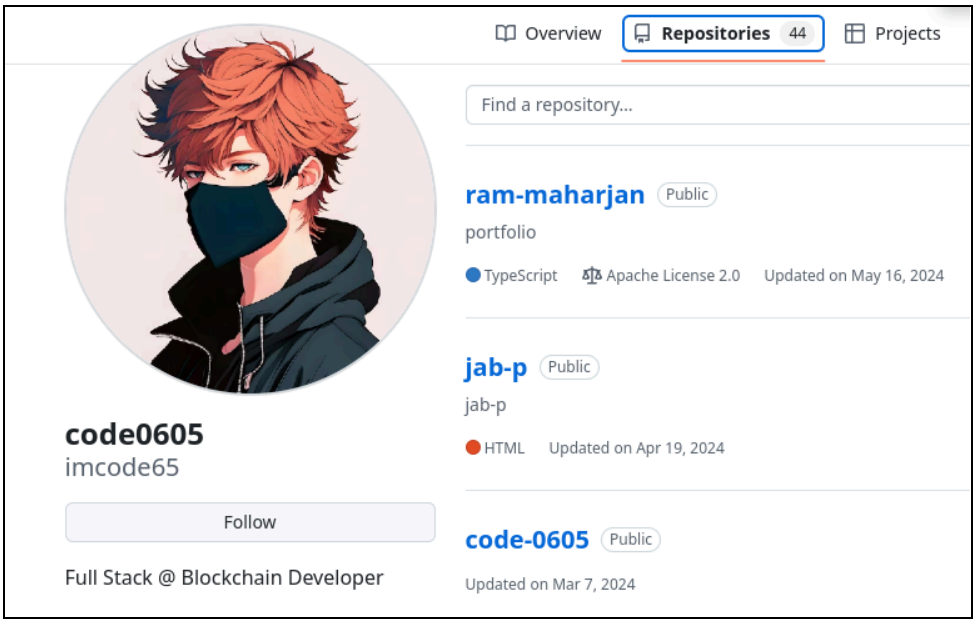
While GitHub account code-0605 is not active, GitHub account imcode65 with user name code0605 is active and is associated with email address kanbei0605@gmail[.]com, suggesting that the possible

[16]https://roman-profile[.]vercel.app/#/
[17]https://ram-maharjan[.]vercel.app
[18]https://ram-maharjan.vercel[.]app
[19]https://jp.orientsoftware[.]com/blog/author/tan-dang
[20]https://kanbei-profile.vercel[.]app/karlchong_resume.pdf
[21]https://ram-maharjan.vercel[.]app

DPRK-affiliated IT workers either included the wrong GitHub account on both personas, or set up a new GitHub account that is similarly named. Nisos did not identify any freelancer accounts for this persona, which suggests that it was likely created recently and has not been used to obtain remote work yet.

John Alexander Bird

John Alexander Bird claims to be a senior front-end engineer and full-stack developer based in Maryland. While this persona does not have an active website on vercel[.]app, his accounts reference multiple created personal websites on that platform, which no longer appear active.[22] [23] GitHub account imcode65 also has a repository labeled jab-p, which includes updates to John Alexander Bird's resume.[24]

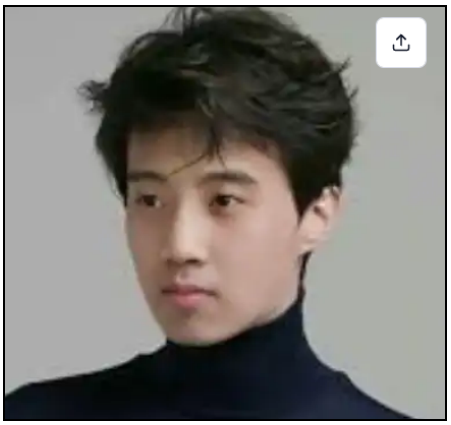


Graphic 17: Imcode65's Github repositories for fake persona resume updates.[25]

Digital Photo Manipulation

John Alexander Bird's freelancer account contains a photograph of the likely DPRK IT worker, which was digitally manipulated. Nisos found that the head of the individual was pasted onto a photo of South Korean actor, Lee Dong-wook.

[22] jab-p.vercel[.]app
[23] jab-p-7dbr.vercel[.]app
[24] https://github[.]com/imcode65/jab-p
[25] https://github[.]com/imcode65?tab=repositories



Graphic 18: Photo from John Alexander Bird's freelancer account.[26]

Graphic 19: Photo of South Korean actor Lee Dong-wook.[27]

Conclusion

The North Korean IT worker scheme is pervasive and targets companies of all sizes and in numerous industries in different countries. Successful mitigation of the risk relies on an improved vetting process for external remote candidates. In this article Nisos provided several risk mitigation steps enterprise leaders and companies can take to identify North Korean IT workers via OSINT research. If however a company is unable to conduct OSINT investigations during hiring on their own, we recommend partnering with an intelligence and investigations firm like Nisos to help enterprise leaders more quickly understand, prevent and in some cases cease unwanted activity within their companies.

[26]https://pangea[.]app/profile/john-bird
[27]https://www.pinterest[.]com/pin/107312403610955808