NISOS

Likely DPRK Network Backstops on GitHub, Targets Companies Globally

March 2025

Table of Contents

Executive Summary

Nisos is tracking a network of likely North Korean (DPRK)-affiliated IT workers posing as Vietnamese, Japanese, and Singaporean nationals with the goal of obtaining employment in remote engineering and full-stack blockchain developer positions in Japan and the United States. While the personas claim to be located in Asia, the network appears to be globally focused, aiming to obtain jobs both in and outside of Asia. The network appears to be using GitHub to create new personas and is reusing matured GitHub accounts and portfolio content from older personas to backstop their new personas. Two of the personas in the network appear to be employed at companies with fewer than 50 employees, and we assess that the network's objective is to earn cash to fund Pyongyang's ballistic missile and nuclear weapons development programs.

Several indicators suggest that the network is likely DPRK-affiliated. These indicators are consistent with tactics, techniques, and procedures (TTPs) attributed to DPRK employment fraud actors.[1]

- Personas claim to have experience in three areas: 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, IT industry-specific freelance contracting platforms, software development tools and platforms, and common messaging applications, but they typically lack social media accounts, suggesting that the personas are created solely for the purpose of acquiring employment.

- Profile photos are digitally manipulated. Often the DPRK-affiliated IT worker's face is pasted on top of a stock photo to show the individual working with colleagues.

- Personas within the network use similar email addresses.

- Email addresses often include the same numbers, such as 116, and the word "dev".

Fake Persona Network

Nisos identified two personas who appear to have gained employment and four personas looking to obtain remote positions in Japan and the United States. The personas were all linked via shared GitHub and contact information, which we identified via open sources.

---

[1] https://nisos[.]com/blog/dprk-workers-scheme
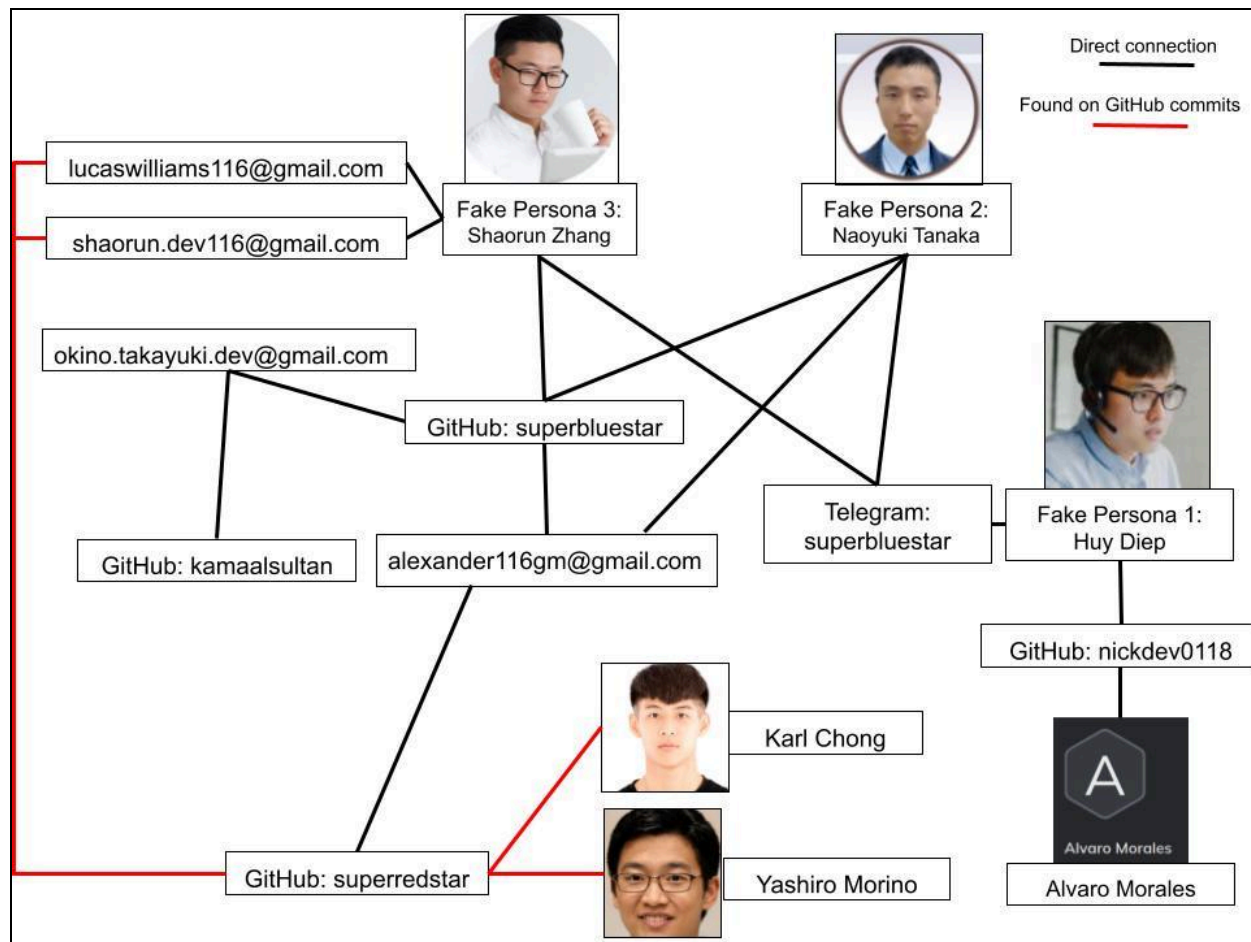
Graphic 1: Network map of likely DPRK-affiliated personas.

Fake Persona 1: Huy Diep/HuiGia Diep

We investigated the GitHub account nickdev0118 and found this account listed on a website belonging to persona Huy Diep/HuiGia Diep.[2] Nisos focused on nickdev0118 because the account co-authored commits with a previously identified, likely DPRK IT worker persona, which used the GitHub account AnacondaDev0120.[3] Huy Diep appears to have been employed as a software engineer specializing in web and mobile app programming at Japanese consulting company Tenpct Inc since September 2023. Huy Diep's personal website linked to Tenpct Inc's website and included several TTPs previously associated with DPRK employment schemes: digitally manipulated photos, the persona claiming to have experience developing web and mobile applications, and knowledge of multiple programming languages.[4]

---

[2] https://huy-diep.web[.]app
[3] https://www.nisos[.]com/research/dprk-it-threat-japan
[4] https://huy-diep.web[.]app

```
From dbfb4c9be96b290136ba23d4fcdd2b2db3b20779 Mon Sep 17 00:00:00 2001
From: O_O <96062458+AnacondaDev0120@users.noreply.github.com>
Date: Tue, 12 Mar 2024 20:34:48 +0800
Subject: [PATCH] This is coautorized

Co-authored-by: AnacondaDev0120 <ancondadev0120@gmail.com>
Co-authored-by: nickdev0118 <nickdev0118@gmail.com>
---
```

Graphic 2: An example of a commit AnacondaDev0120 and nickdev0118 co-authored.[5]

Graphic 3: Diep Huy's employment history lists employment at several Japanese companies.[6]

Graphic 4: Description of Huy Diep's role at Tenpct *Inc. Translation: "A software engineer specializing in web and mobile app programming. A full-stack engineer with experience working remotely for many companies, he is currently involved in system development as a backend engineer."[7]*

---

[5]https://github[.]com/AnacondaDev0120/Web-scrappy-py/commit/c229ba57ae904c5fff6539cef53f7aaaa4c5ba58.patch
[6]https://www.f6s[.]com/member/huydiep#about
[7]https://www.tenpct[.]jp/member
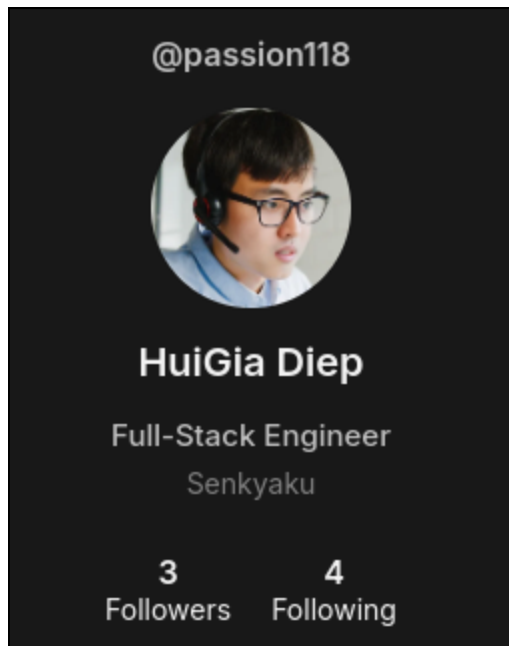
Graphic 5: Alternate Name for the same persona referencing employment for Senkyaku.[8]

Digital Photo Manipulation

Huy Diep's website contains two photographs of the likely DPRK IT worker, which were digitally manipulated. Nisos found that the head of the individual was pasted onto stock photos of other individuals to show the persona working. The individual also pasted his head onto a stock photo on website F6S, which helps startups hire talent.

Graphic 6: Photo from Huy Diep's website.[9]
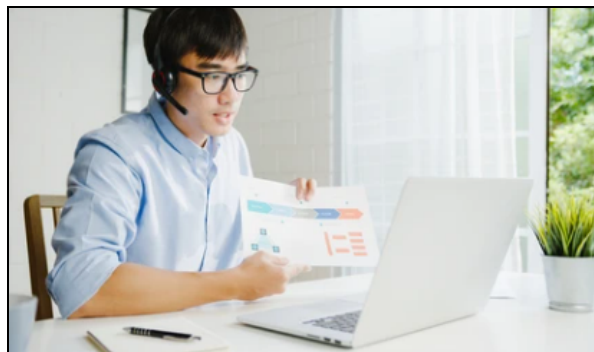
Graphic 7: Stock photo used in Graphic 6.

---

[8]https://joinentre[.]com/profile/passion118
[9]https://huy-diep.web[.]app

Graphic 8: Photo from Huy Diep's website.

Graphic 9: Stock photo used in Graphic 8.

Graphic 10: Photo from Huy Diep's profile on F6S.[10]

Graphic 11: Stock photo used in Graphic 10.

Significant Development Experience

DPRK IT worker personas frequently claim to have experience developing web and mobile applications, knowledge of multiple programming languages, and an understanding of blockchain technology. On the persona's website, Huy Diep lists a number of programming languages and certificates. Huy Diep also claims to have eight years of experience in software engineering working as a freelancer and team member for domestic and international clients, including those in Japan.

Graphic 12: Listed program languages on Huy Diep's website.[11]

---

[10]https://www.f6s[.]com/member/huydiep#about
[11]https://huy-diep.web[.]app

Over my 8-year tenure as a professional Software Engineer, I've honed the skills and expertise necessary to drive the success of numerous company projects. I derive immense satisfaction from every stage of the work process and view my role not merely as a freelancer, but as an integral member of the team.

Graphic 13: Huy Diep's experience description on freelancer website.[12]

Fake Persona 2: Naoyuki Tanaka

Nisos identified the persona Naoyuki Tanaka—used by a likely DPRK IT worker to obtain remote work in the United States—by investigating the Telegram username superbluestar, which was listed on Huy Diep's and Naoyuki Tanaka's resumes. Naoyuki Tanaka appears to have been employed at New York-based video game developer Enver Studio since November 2021 as a full stack and blockchain engineer. Naoyuki Tanaka's personal website lists experience in developing web and blockchain projects as well as multiple programming languages. Nisos also found Naoyuki Tanaka on a number of freelancer websites. In addition to typical TTPs associated with DPRK-affiliated personas, the resume for Naoyuki Tanaka also included email address alexander116gm@gmail[.]com, which is not related to the name Naoyuki Tanaka.
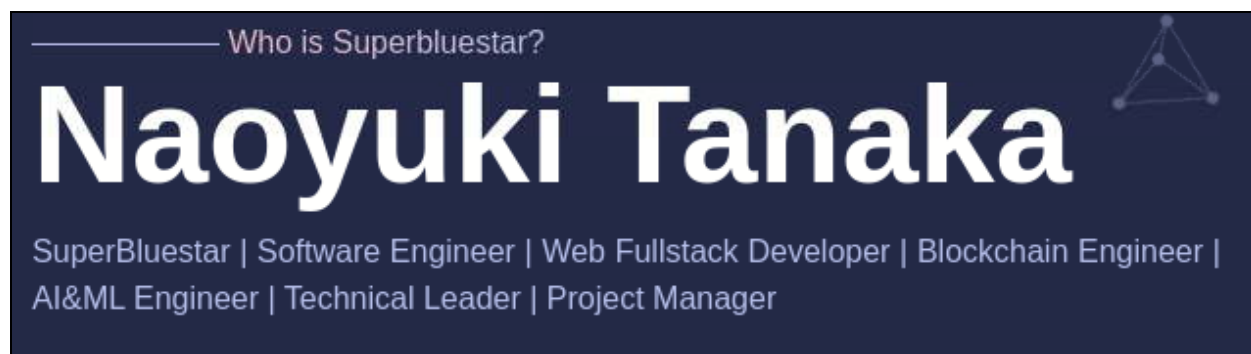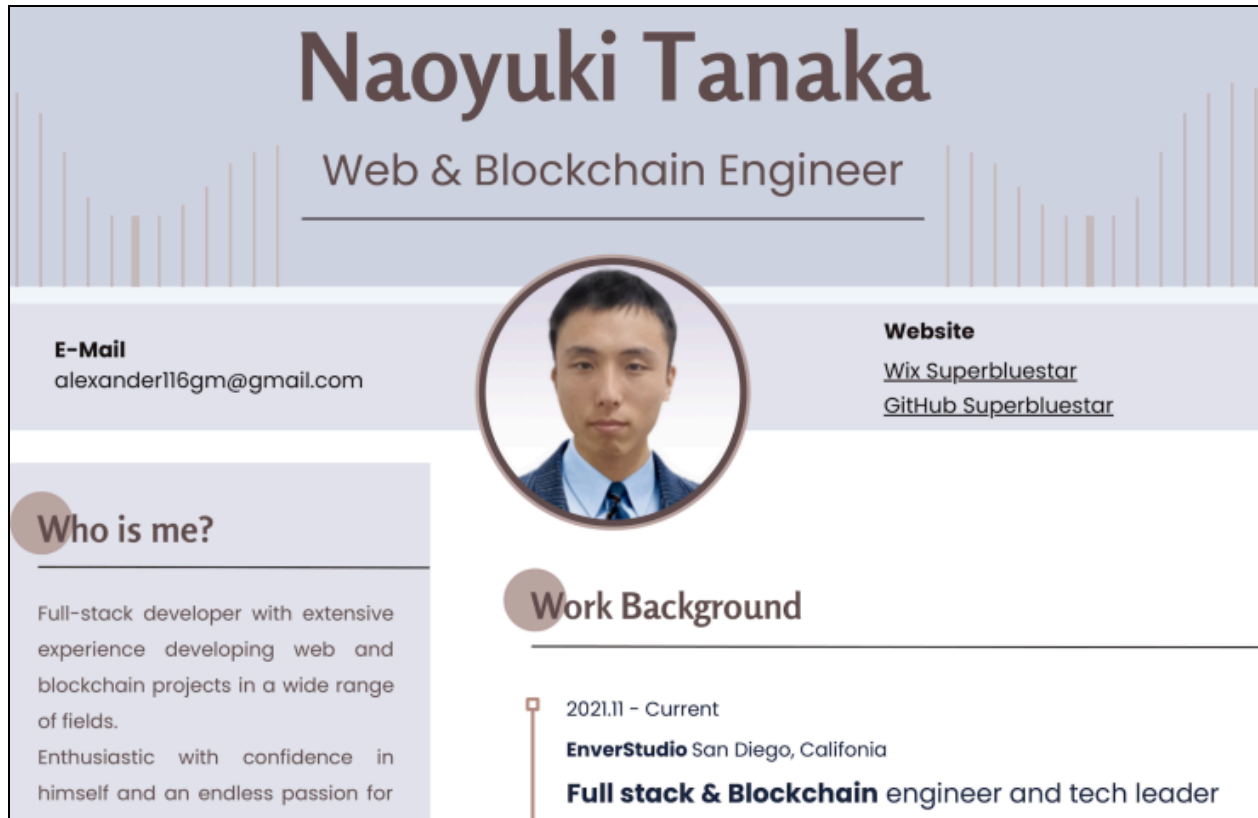

Graphic 14: Naoyuki Tanaka's work experience.[13]

Graphic 15: Enver Studio website showing Naoyuki Tanaka.[14]

---

[12]https://www.f6s[.]com/member/huydiep#about
[13]https://portfolio-one-navy-24[.]vercel.app
[14]https://www.enverstudio[.]com/career

Graphic 16: Naoyuki Tanaka's resume.[15]

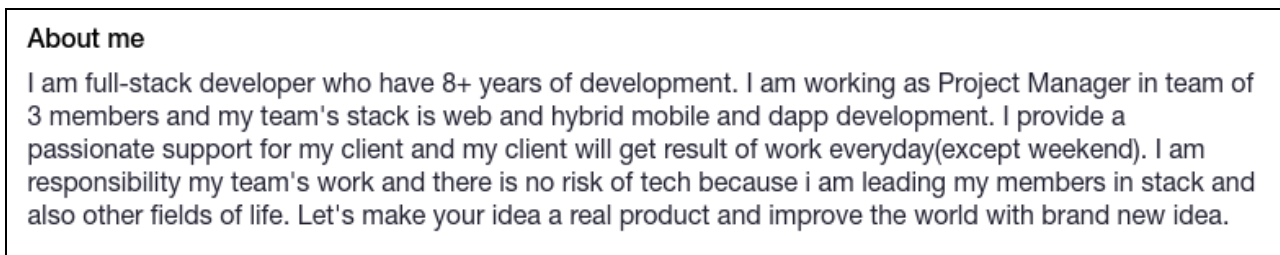*Graphic 17: Additional photo of Naoyuki Tanaka from a freelancer website.[16]*

[15]https://uploads.laborx[.]com/cv/N9JnNVX8Ie63TY6JwuI9k8UAl-JisIUM.pdf
[16]https://www.upwork[.]com/freelancers/naoyukit

Significant Development Experience

Naoyuki Tanaka's website lists a number of programming languages and certificates. Naoyuki Tanaka also claims to have over eight years of experience in software development.

About me

I am full-stack developer who have 8+ years of development. I am working as Project Manager in team of 3 members and my team's stack is web and hybrid mobile and dapp development. I provide a passionate support for my client and my client will get result of work everyday(except weekend). I am responsibility my team's work and there is no risk of tech because i am leading my members in stack and also other fields of life. Let's make your idea a real product and improve the world with brand new idea.

Graphic 18: Naoyuki Tanaka's work experience.[17]

Freelancer Employment Websites Linked To Naoyuki Tanaka

Nisos identified seven freelance employment websites, which listed the persona name, location, GitHub account superbluestar, and work history of the persona. Many of the resumes claimed that Naoyuki Tanaka worked at Enver Studio.

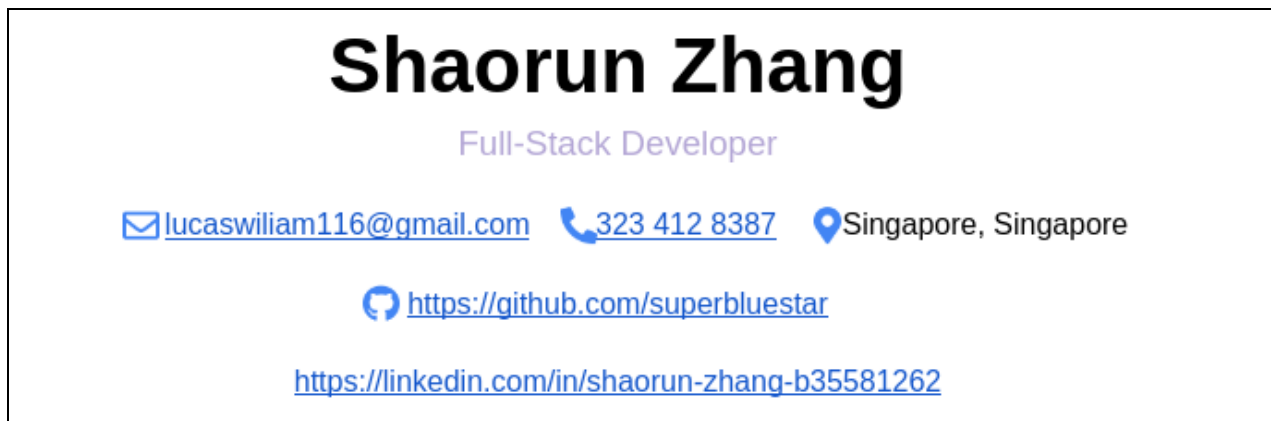| FREELANCER WEBSITE |
| --- |
| https://laborx[.]com/freelancers/users/id32867 |
| https://himalayas[.]app/@superbluestar |
| https://www.xing[.]com/profile/Naoyuki_Tanaka |
| https://superbluestar.wixsite[.]com/superbluestar |
| https://torre[.]ai/alexander116gm?r=CjJZoVok |
| https://www.producthunt[.]com/@superbluestar |
| https://www.upwork[.]com/freelancers/naoyukit |

Fake Persona 3: Shaorun Zhang

Nisos identified the persona Shaorun Zhang—used by a likely DPRK IT worker to obtain remote work in the past—by investigating the GitHub account superbluestar and Telegram account superbluestar, which were listed on the resume for Naoyuki Tanaka. Shaorun Zhang's website and freelancer accounts listed a number of email addresses and had profile photos of the individual.[18]

---

[17]https://laborx[.]com/freelancers/users/id32867
[18]https://shaorun-portfolio.vercel[.]app
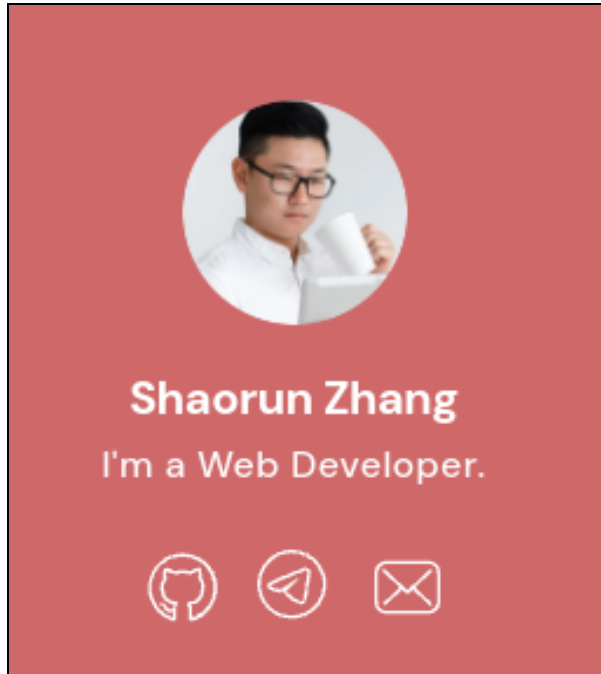
Graphic 19: Shaorun Zhang's linktr.ee profile.[19]

Graphic 20: Shaorun Zhang's resume information.[20]

[19]https://linktr[.]ee/shaorunzhang
[20]https://docs.google[.]com/document/d/1BdUyEgoXs-PzZbFbdlO1pDv4yTCQMmlyJ9C1ZyAc6RU/edit?tab=t.0

Graphic 21: Shaorun Zhang's partial photo from a freelancer website.[21]

Digital Photo Manipulation

Shaorun Zhang's linktr.ee website has a photograph of the likely DPRK IT worker, which was digitally manipulated. Nisos found that the head of the individual was pasted onto an advertisement image of another individual.

Graphic 22: Photo from Shaorun Zhang's linktr.ee page.[22]

Graphic 23: Advertisement photo used in Graphic 22.[23]

---

[21]https://www.xing[.]com/profile/Shaorun_Zhang019833
[22]https://linktr[.]ee/shaorunzhang
[23]https://www.qornerstone[.]com/commercial
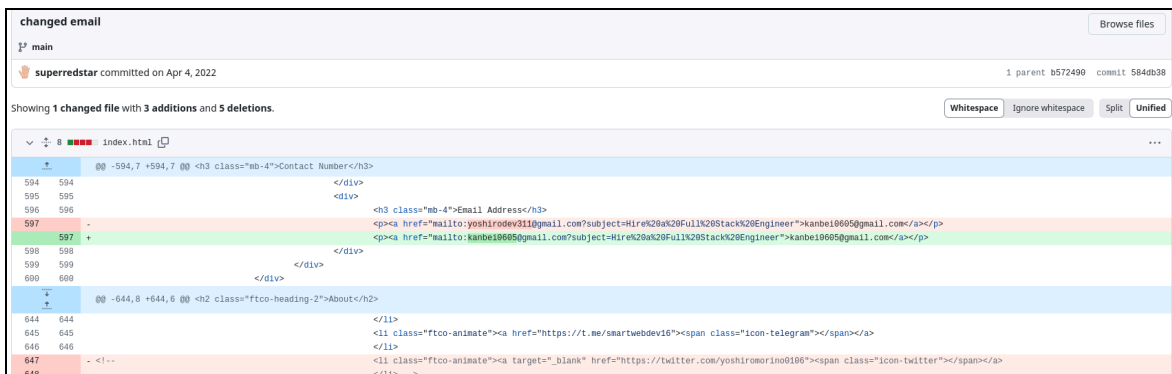
Persona Creation and Backstopping

Nisos assesses that DPRK-affiliated IT workers likely use GitHub to create new personas and to backstop them with matured content. GitHub commits revealed multiple GitHub accounts importing, editing, and creating new persona resumes. Additionally, likely DPRK IT workers almost certainly reuse GitHub accounts and resume content to backstop their newly created personas with matured work profiles.

Persona Creation Process

Likely DPRK-affiliated IT workers are using multiple GitHub accounts to import, edit, and create new persona resumes. Nisos found that personas within the network, Shaorun Zhang and Kamaal Sultan, shared a GitHub repository that was edited by a third GitHub account, superredstar, in April 2022. Nisos assess that Kamaal Sultan is likely a DPRK-affiliated persona: The account listed the email address okino.takayuki.dev@gmail[.]com as a contact email, which was also associated with GitHub account superbluestar. A review of the commits on GitHub account kamaalsultan showed that a number of GitHub users worked on several personas including two named Karl Chong and Yoshiro Morino.

Graphic 24: An example of the persona creation process on GitHub.[24]

Graphic 25: A second example of the persona creation process on GitHub.[25]

---

[24]https://github[.]com/kamaalsultan/shaorun-dev116.github.io/commit/584db387dc40149040b2b69cd301e5310d696cde

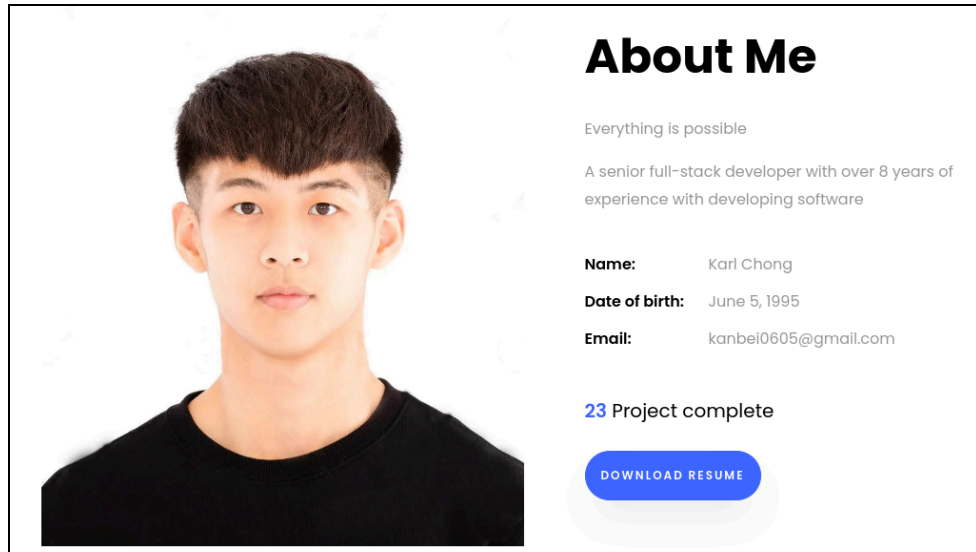[25]https://github[.]com/kamaalsultan/shaorun-dev116.github.io/commit/e35f8c735cf13bc1f6edc305d0ed91fae9c5e494

kamaalsultan on Feb 27, 2024   Owner   · · ·

reply with your answer to this mail
okino.takayuki.dev@gmail.com
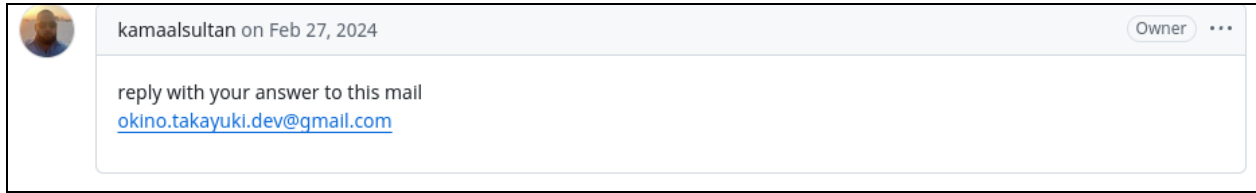
Graphic 26: Kamaalsultan's post on Github.[26]

About Me

Everything is possible

A senior full-stack developer with over 8 years of experience with developing software

Name: Karl Chong
Date of birth: June 5, 1995
Email: kanbei0605@gmail.com

23 Project complete

DOWNLOAD RESUME

Graphic 27: Example of a persona created on Github.[27]

About Me

Nothing is impossible!

A full-stack developer who has accumulated skills through 6+ years of practical experience!

Name: Yoshiro Morino
Email: yoshirodev311@gmail.com
Phone: (+1) 412-528-1796

63 Project complete

DOWNLOAD RESUME
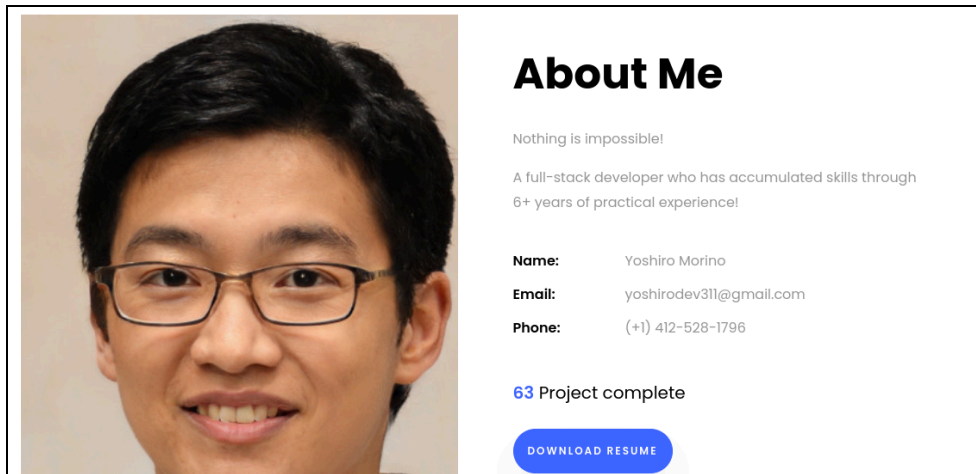
Graphic 28: Example of a second persona created on Github.[28]

---

[26]https://github[.]com/kamaalsultan/kamaalsultan/issues/8
[27]https://kanbei-profile.vercel[.]app
[28]https://ninjadev0329[.]github.io

Backstopping

Likely DPRK IT workers almost certainly reuse GitHub accounts to backstop their newly created personas with matured work profiles. Nisos found that two personas, Shaorun Zhang and Naoyuki Tanaka, claimed to be the users of GitHub account superbluestar. Similarly, both Huy Diep and likely newly created persona Alvaro Morales were associated with username nickdev0118. Nisos was unable to find any additional freelancer websites or resumes for Alvaro Morales, which likely suggests that the persona was recently created and would be backstopped with the GitHub account superbluestar.
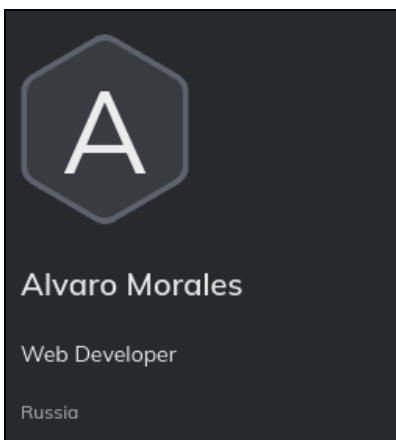
Graphic 29: Resume for Alvaro Morales associated with username nickdev0118.[29]

Nisos also found that newly created persona Karl Chong's resume included Naoyuki Tanaka's claimed Enver Studio work in its portfolio. Nisos assesses that Karl Chong's portfolio is being backstopped using Naoyuki Tanaka's work.
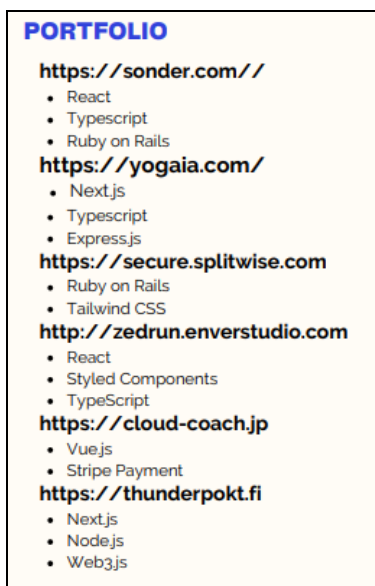
Graphic 30: Karl Chong's resume lists work at Enver Studio.[30]

---

[29]https://torre[.]ai/nickdev0118?r=lX1jAn71
[30]https://kanbei-profile.vercel[.]app/karlchong_resume.pdf

Contact Information and Usernames

Nisos found the following contact information and usernames associated with the likely DPRK IT workers.

PLATFROM	USERNAME	PERSONA
Email	nickdev0118@gmail[.]com	Huy Diep
Telegram	superbluestar	Huy Diep, Naoyuki Tanaka, Shaorun Zhang
GitHub	https://github[.]com/nickdev0118	Huy Diep
Username	Passion118	Huy Diep
GitHub	https://github[.]com/superbluestar	Naoyuki Tanaka, Shaorun Zhang
Email	alexander116gm@gmail[.]com	Naoyuki Tanaka
Email	alexander116@gmail[.]com	Naoyuki Tanaka
Email	alexander116@hotmail[.]com	Naoyuki Tanaka
Phone	81 50 5532 6308	Naoyuki Tanaka
Wix	superbluestar	Naoyuki Tanaka
calendly	alexander116gm	Naoyuki Tanaka
Trello	superbluestar	N/A
Email	okino.takayuki.dev@gmail[.]com	GitHub accounts superbluestar and kamaalsultan
Username	superbluestar	Naoyuki Tanaka, Shaorun Zhang
Email	shaorun.dev116@gmail[.]com	Shaorun Zhang
Phone	323 412 8387	Shaorun Zhang
Email	lucaswiliam116@gmail[.]com	Shaorun Zhang
Email	shaorun@sweply[.]com	Shaorun Zhang

Conclusion

The employment fraud scheme perpetrated by the Democratic People's Republic of Korea (DPRK) has presented US and Japan-based companies with significant cybersecurity and employment risks since at least 2022. Nisos is investigating a network that appears to be responsible for obtaining remote jobs in both countries. The network is likely setting up personas via GitHub often reusing existing GitHub accounts to backstop new personas. Nisos recommends that companies ensure applicants provide identification documentation in-person to enable human resource teams to better identify falsified documentation. Nisos also recommends that companies conduct a detailed review of the applicant's online presence for consistency in name, appearance, work history, and education prior to offering employment.