

Research

DPRK IT Worker Tradecraft Between 2022 and 2025

May 2025

Table of Contents

Executive Summary	3
Use of AI in Profile Images	3
Cartoon Images	3
Digitally Manipulated Images	4
AI-assisted Images	5
Templates For Websites	6
Bootstrapmade	6
Reused Resume Content	7
Introduction Section	7
GitHub accounts	8
Fake Locations	9
Tennessee	9
West Virginia	10
Repurpose Accounts	10
Regulations	12
Conclusion	13

Executive Summary

Since early 2023 Nisos has been investigating and monitoring North Korean (DPRK) IT workers, who use fake personas and stolen identities to fraudulently obtain remote employment from unwitting companies in the United States and abroad. DPRK IT workers pose as Japanese, Singaporean, Turkish, Finnish and US nationals with engineering and full-stack developer backgrounds to fund Pyongyang's ballistic missile and nuclear weapons development programs. Nisos observed that DPRK IT workers have used the following tactics, techniques, and procedures (TTPs) to mask their true identities over the past three years:

- Advanced technology, such as Artificial Intelligence (AI) for image manipulation
- Templates for persona website creation via Github repositories
- Reused resume content
- Fake addresses

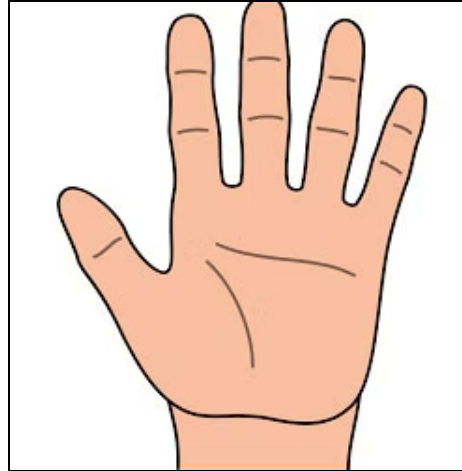
Nisos also observed DPRK IT workers quickly pivoting to other personas if a persona was fired by an employer or flagged and removed from GitHub or freelancer websites. DPRK IT workers quickly create new personal websites and freelancer accounts to continue the work the previous persona was doing.

Use of AI in Profile Images

Nisos observed increased sophistication related to how DPRK IT workers use AI to generate profile pictures for their personas. In 2022, DPRK IT workers did not include photos of themselves on their portfolio website or freelancer accounts and instead relied on cartoons to hide their true identities. Starting in 2023, DPRK IT workers began putting their faces on stock photo bodies, to make their accounts seem more legitimate. Since 2024, DPRK IT workers have used AI to combine their faces with stock images to make their profile photos appear more legitimate.

Cartoon Images

Nisos observed a number of instances of DPRK-affiliated personas using cartoons or other images to mask the true identity of the IT worker. Most of these personas were created in 2022.



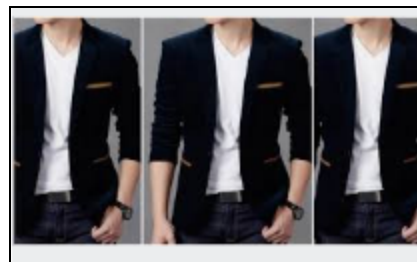
Graphic 1: Profile Photo of likely DPRK persona Naoyuki Tanaka.¹

Digitally Manipulated Images

Nisos observed a number of instances of digitally manipulated profile images, which combine the faces of IT workers onto stock photos. These personas were created before 2024.



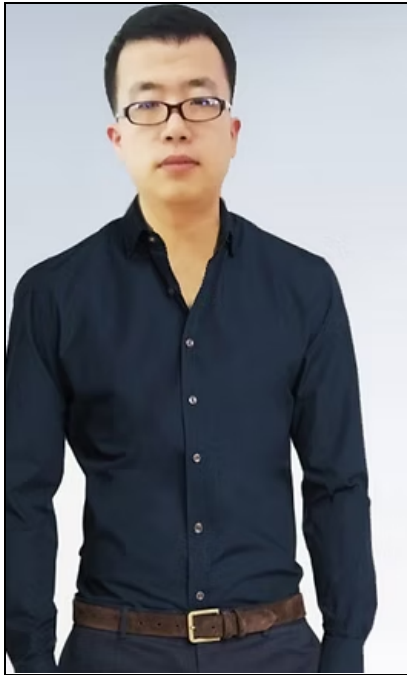
Graphic 2: Profile Photo of likely DPRK persona WeiTao Wang.²



Graphic 3: Stock Photo of the outfit in Graphic 2.

¹[https://superbluestar.wixsite\[.\]com/superbluestar](https://superbluestar.wixsite[.]com/superbluestar)

²[https://wwt-nu.vercel\[.\]app](https://wwt-nu.vercel[.]app)



Graphic 4: Profile Photo of likely DPRK persona Osamu Odaka.³



Graphic 5: Stock Photo of the outfit used in Graphic 4.

AI-Manipulated Images

Nisos observed a number of instances of AI-manipulated profile images, which combine the faces of IT workers with stock photos. These personas were all created in 2024.



Graphic 6: Profile photo of likely DPRK persona Shaorun Zhang.⁴



Graphic 7: Advertisement photo used in Graphic 6.⁵

³[https://cvdesignr\[.\]com/p/61f00eb8eca12](https://cvdesignr[.]com/p/61f00eb8eca12)

⁴[https://linktr\[.\]ee/shaorunzhang](https://linktr[.]ee/shaorunzhang)

⁵[https://www.qornerstone\[.\]com/commercial](https://www.qornerstone[.]com/commercial)



Graphic 8: Photo of likely DPRK persona John Alexander Bird.⁶



Graphic 9: Photo of South Korean actor Lee Dong-wook.⁷

Templates For Websites

According to the US Office of Foreign Assets Control (OFAC), DPRK IT workers build “portfolio” websites, generally simple in design, in an effort to boost the credibility of their fabricated, freelance developer personas. These virtual portfolios represent the work of DPRK IT workers’ personas and are often linked to their online freelance developer accounts.⁸ Nisos observed that DPRK IT workers began using templates to build portfolio websites for their personas in 2023. These included templates from websites such as bootstrapmade[.]com.

Bootstrapmade

Nisos observed that likely DPRK-affiliated GitHub account imcode65 created a portfolio website for a persona named John Alexander Bird importing a template from website bootstrapmade[.]com on 30 November 2023. Several other likely affiliated DPRK personas also used website templates that appear similar to the Bootstrapmade template, to post the portfolio websites on vercel[.]app. Vercel is a platform that provides developer tools and cloud infrastructure to individuals to personalize the website for them.⁹

⁶[https://pangea\[.\]app/profile/john-bird](https://pangea[.]app/profile/john-bird)

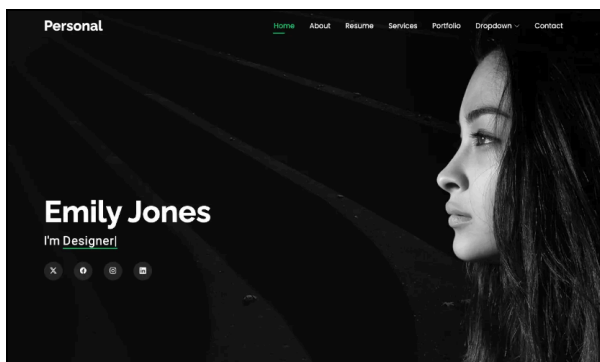
⁷[https://www.pinterest\[.\]com/pin/107312403610955808](https://www.pinterest[.]com/pin/107312403610955808)

⁸[https://ofac.treasury\[.\]gov/media/923126/download?inline](https://ofac.treasury[.]gov/media/923126/download?inline)

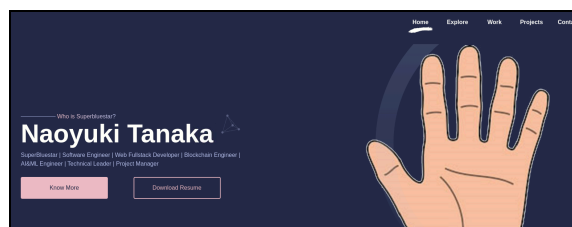
⁹[https://vercel\[.\]com/home](https://vercel[.]com/home)

```
assets/js/main.js
... 00 -0,0 +1,247 00
1 + /**
2 + * Template Name: Personal - v4.7.0
3 + * Template URL: https://bootstrapmade.com/personal-free-resume-bootstrap-template/
4 + * Author: BootstrapMade.com
5 + * License: https://bootstrapmade.com/license/
6 + */
```

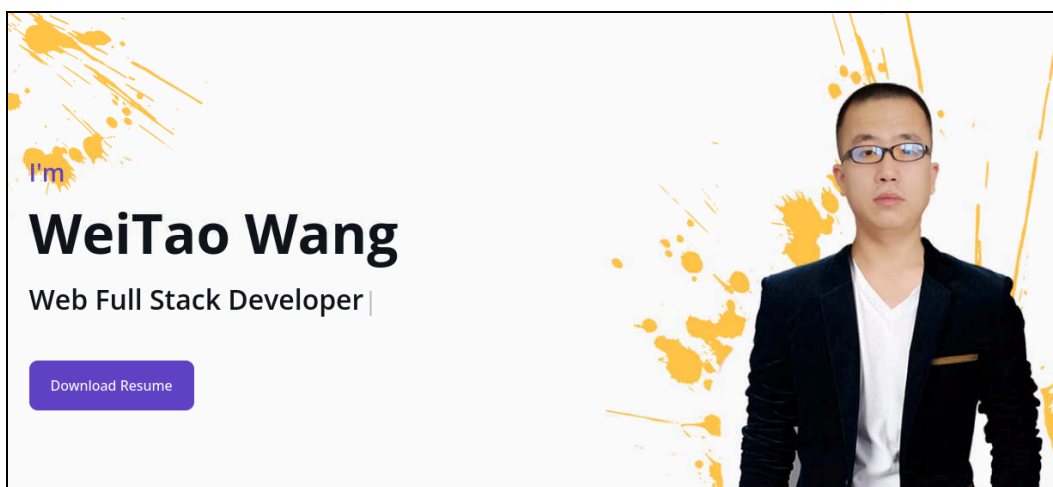
Graphic 10: GitHub commit showing the use of templates for portfolio websites.¹⁰



Graphic 11: Bootstrapmade website template.¹¹



Graphic 12: Naoyuki Tanaka website.¹²



Graphic 13: WeiTao Wang website.¹³

Reused Resume Content

Introduction Section

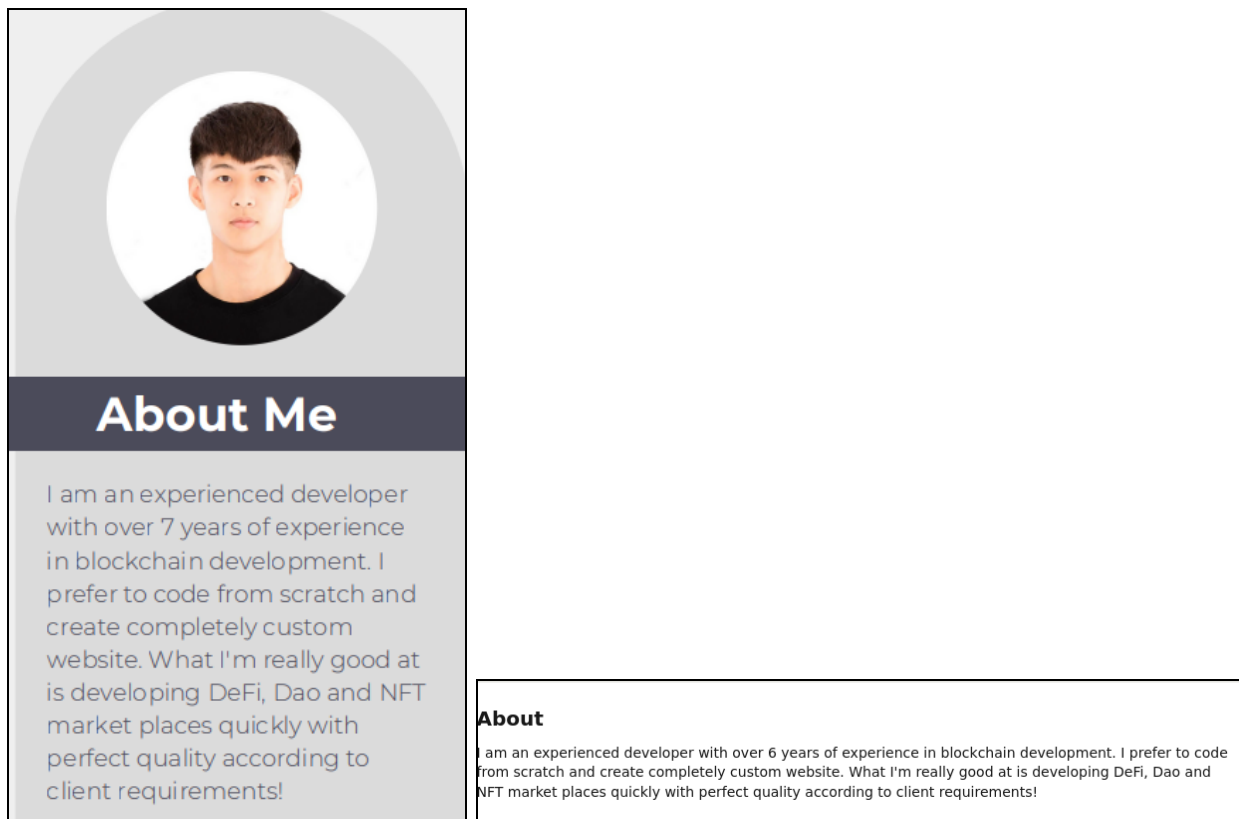
Nisos observed a number of DRPK-affiliated personas use the same or similar introduction section on their resumes. DRPK-affiliated personas Karl Chong and Roman Kryveha for example stated that they both are experienced developers with over seven years of experience in blockchain development.

¹⁰<https://github.com/imcode65/jab-p/commit/99ef14829b03685f67862a53164393eaaef23f3>

¹¹<https://bootstrapmade.com/personal-free-resume-bootstrap-template>

¹²<https://portfolio-one-navy-24.vercel.com>

¹³<https://wwt-nu.vercel.com>



Graphics 14 and 15: Karl Chong’s about me section (left).¹⁴ Roman Kryveha’s about me section (right).

GitHub accounts

Nisos observed that GitHub accounts are re-used to backstop different personas. Nisos assesses that DPRK affiliated IT workers reuse the accounts in order to provide fake work history to their personas. GitHub account redsky500, which is no longer active, for example was associated with the personas Code Solution, CodeJourney, and Ryosuke Yamamoto.^{15 16 17} Code Solution claims to be the user of redsky500 and claims to have 10 years of work experience.¹⁸ Redsky500 is also associated with likely DPRK persona Ryosuke Yamamoto, who has six years of work experience and appears to be employed at WowDAO as a Web3 Full Stack Developer.¹⁹ In addition to their association with the same GitHub account, Code Solution and Ryosuke Yamamoto share association with the number 0302. Code Solution lists their contact information as Telegram ID doom0302 while Ryosuke Yamamoto lists Telegram ID Ryosuke0302 and email address phantomdev0302@gmail[.]com.^{20 21}

¹⁴[https://uploads.laborx\[.\]com/cv/JnxsPze0PBWteLNIGC6Fy0Axe kuw3t2-.pdf](https://uploads.laborx[.]com/cv/JnxsPze0PBWteLNIGC6Fy0Axe kuw3t2-.pdf)

¹⁵[https://laborx\[.\]com/freelancers/users/id53436](https://laborx[.]com/freelancers/users/id53436)

¹⁶[https://yhype\[.\]me/github/@redsky500?tab=followings](https://yhype[.]me/github/@redsky500?tab=followings)

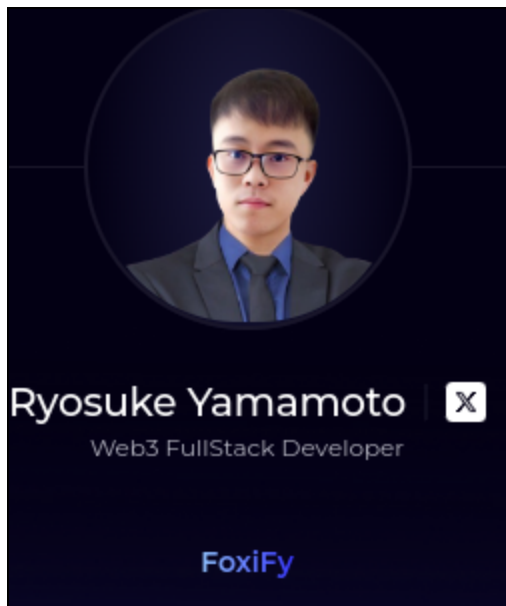
¹⁷[https://people.bayt\[.\]com/ryosuke-yamamoto-77053255/#activities](https://people.bayt[.]com/ryosuke-yamamoto-77053255/#activities)

¹⁸[https://laborx\[.\]com/freelancers/users/id53436](https://laborx[.]com/freelancers/users/id53436)

¹⁹[https://people.bayt\[.\]com/ryosuke-yamamoto-77053255](https://people.bayt[.]com/ryosuke-yamamoto-77053255)

²⁰[https://laborx\[.\]com/freelancers/users/id53436](https://laborx[.]com/freelancers/users/id53436)

²¹[https://uploads.laborx\[.\]com/cv/Ma2FCDjmlNI8brXdEYa7L97axuCQRXRP.pdf](https://uploads.laborx[.]com/cv/Ma2FCDjmlNI8brXdEYa7L97axuCQRXRP.pdf)



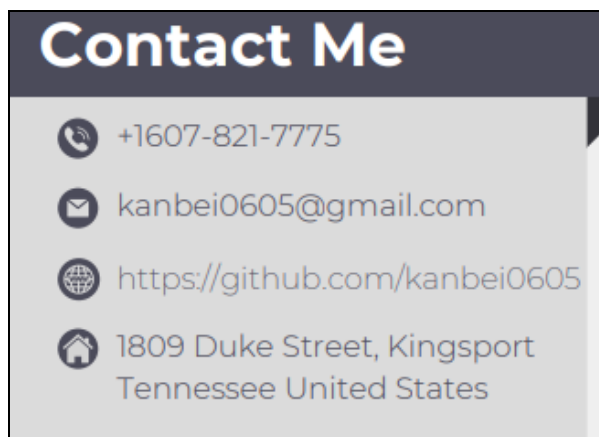
Graphic 16: Ryosuke Yamamoto's profile on WowDAO's website.²²

Fake Locations

Nisos observed that some of the DPRK-affiliated personas listed US-based addresses on their resumes. A review of the addresses, however, shows that they do not match the name of the person residing at the address and in some cases are not residential addresses.

Tennessee

Karl Chong's resume lists his address as 1809 Duke Street, Kingsport, Tennessee, US. A review of the resident of the address does not list him as a current or previous resident.



Graphic 17: Karl Chong's address.²³

²²[https://wowdao\[.\]ai/Community](https://wowdao[.]ai/Community)

²³[https://uploads.laborx\[.\]com/cv/JnxsPze0PBWteLNIGC6Fy0Axe kuw3t2-.pdf](https://uploads.laborx[.]com/cv/JnxsPze0PBWteLNIGC6Fy0Axe kuw3t2-.pdf)

West Virginia

Ryosuke Yamamoto's resume lists his address as 949 3rd Ave, Huntington, WV. A review of the address, however, shows that it is a retail property and not a residential address, listing a number of companies at the same address.

Contact

Address

949 3rd Ave Huntington, WV

Phone

+1 (864) 485-9594

Email

phantomdev0302@gmail.com

Github

<https://github.com/redsky500>

Portfolio

<https://redsky500.github.io>

Linkedin

<https://linkedin.com/in/ryosuke-yamamoto>

Graphic 18: Ryosuke Yamamoto's address.²⁴



Graphic 19: Commercial real estate listing for 949 3rd Ave, Huntington, WV.²⁵

Repurposed Accounts

Nisos observed that DPRK IT workers are able to quickly repurpose personas to ensure continuity with their work if GitHub accounts are closed. Nisos identified a likely DPRK-affiliated persona, Justine Carlo, who appears to be employed at Japanese company 10pct Inc as a full stack Engineer and appears to have been previously employed at a US educational company.²⁶ The persona is associated with two GitHub accounts, justine-carlo²⁷ and justine-carlo-0116.²⁸ GitHub account justine-carlo was created in 2022, but was only used sparingly. GitHub account justine-carlo-0116, however, was created in March 2025, following the removal of DPRK-affiliated GitHub account superredstar from the platform, and has been used to continue the work of that account.

²⁴[https://www.cryptotask\[.\]org/en/freelancers/ryosuke-yamamoto/14380#](https://www.cryptotask[.]org/en/freelancers/ryosuke-yamamoto/14380#)

²⁵[https://www.loopnet\[.\]com/Listing/949-3rd-Ave-Huntington-WV/24677889](https://www.loopnet[.]com/Listing/949-3rd-Ave-Huntington-WV/24677889)

²⁶[https://sg.wantedly\[.\]com/id/justine_carlo_0116](https://sg.wantedly[.]com/id/justine_carlo_0116)

²⁷[https://github\[.\]com/justine-carlo](https://github[.]com/justine-carlo)

²⁸[https://github\[.\]com/justine-carlo-0116](https://github[.]com/justine-carlo-0116)

Nisos assesses that Justine Carlo is a DPRK-affiliated persona as the account exhibits a number of DPRK-related TTPs, including reused resume content, multiple listed locations, and the use of the number 116. Nisos assesses that the persona was created quickly, since its personal website is not fully finished even though the persona claims to have been working professionally since 2016.

- Nisos observed that Justine Carlo claims to be employed at 10Pct Inc since October 2024. Nisos has identified two other DPRK-affiliated personas, Weitao Wang and Huy Diep, who appeared to have worked at 10Pct Inc in the past.²⁹
- Nisos observed a number of profiles on freelancer websites for Justine Carlo, which claim that he is located in the Philippines, the United States, and Japan. Each of these websites contains the same work history, suggesting that they are the same person but target different audiences.^{30 31 32}
- Nisos observed that likely DPRK-affiliated IT workers continued to use numbers, such as 116 in their persona usernames and email addresses.
- Nisos identified a personal website for Justine Carlo, which listed the same work and educational history as his freelancer accounts. The website, however, does not appear to be set up correctly, as all the buttons that are supposed to link to social media or contact information are not working.³³

```
From 1947aa22d968de93d3ee9ef3d14860e4304aaef2 Mon Sep 17 00:00:00 2001
From: justine-carlo-0116 <justinecarlo0116@gmail.com>
Date: Fri, 28 Mar 2025 03:54:02 -0400
Subject: [PATCH] init repo
```

Graphic 20: GitHub commit showing that justine-carlo-0116 is associated with justinecarlo0116@gmail[.]com.³⁴

²⁹[https://6068438.fs1.hubspotusercontent-na1\[.\]net/hubfs/6068438/dprk-it-threat-japan.pdf](https://6068438.fs1.hubspotusercontent-na1[.]net/hubfs/6068438/dprk-it-threat-japan.pdf)













³⁰[https://sg.wantedly\[.\]com/id/justine_carlo_0116](https://sg.wantedly[.]com/id/justine_carlo_0116)

³¹[https://www.wantedly\[.\]com/id/justine_dev](https://www.wantedly[.]com/id/justine_dev)

³²[https://www.wantedly\[.\]com/id/justinecarlo0116](https://www.wantedly[.]com/id/justinecarlo0116)

³³[https://my-portfolio-3bca0.web\[.\]app/index.html](https://my-portfolio-3bca0.web[.]app/index.html)

³⁴[https://github\[.\]com/justine-carlo-0116/fe-assessment-next-static-generation/commit/1947aa22d968de93d3ee9ef3d14860e4304aaef2.patch](https://github[.]com/justine-carlo-0116/fe-assessment-next-static-generation/commit/1947aa22d968de93d3ee9ef3d14860e4304aaef2.patch)

Commits on Apr 2, 2025	<div> <div>update</div> <div>justine-carlo-0116 committed 2 weeks ago</div> <div>503cc95</div> <div> </div> </div>
Commits on Feb 24, 2025	<div> <div>feat: complete many components</div> <div>superredstar committed on Feb 23</div> <div>06a70f0</div> <div> </div> </div>
Commits on Feb 18, 2025	<div> <div>Doing basic components</div> <div>superredstar committed on Feb 17</div> <div>97f5984</div> <div> </div> </div>
Commits on Feb 10, 2025	<div> <div>Update index.js from ui-library</div> <div>superredstar committed on Feb 10</div> <div>bfeff67</div> <div> </div> </div> <div> <div>Update</div> <div>superredstar committed on Feb 10</div> <div>05970e1</div> <div> </div> </div> <div> <div>remove mui/base, and installed mui/material</div> <div>superredstar committed on Feb 10</div> <div>bdb88df</div> <div> </div> </div>

Graphic 21: List of GitHub commits linking superredstar to justine-carlo-0116.³⁵

Regulations

The US Department of State, the US Department of the Treasury, and the Federal Bureau of Investigation (FBI) issued a joint advisory on 16 May 2022, for the international community, the private sector, and the public to warn of attempts by DPRK IT workers to obtain employment while posing as non-North Korean nationals.³⁶ Involvement in prohibited or sanctionable conduct can have legal, financial, and reputational repercussions for companies. To help potential employers protect themselves, the advisory listed indicators and behaviors of DPRK IT workers.

Per OFAC, individuals and entities engaged in or supporting DPRK IT worker-related activity, including processing related financial transactions, should be aware of the potential legal consequences for involvement in prohibited or sanctionable conduct.

- UN Security Council resolution 2375 prohibits UN Member States from providing new work authorizations, or renewing expired authorizations, for DPRK nationals in their jurisdictions in connection with admission to their territories unless approved in advance by the UN Security Council's 1718 Committee.
- OFAC has the authority to impose financial sanctions on any person determined to have, materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the DPRK government or the Workers' Party of Korea.³⁷

³⁵<https://github.com/justine-carlo-0116/ui-react/commits/master>

³⁶<https://ofac.treasury.gov/media/923126/download?inline>

³⁷<https://ofac.treasury.gov/media/923126/download?inline>

Conclusion

The employment fraud scheme perpetrated by DPRK IT workers has presented US-based and foreign companies with significant cybersecurity and employment risks since at least 2022. Nisos observed DPRK IT workers have used AI for image manipulation, templates for persona website creation, reused resume content, and listed fake addresses to mask their true identities over the past three years. Since engaging in prohibited and sanctionable conduct can have legal and financial repercussions for companies, Nisos recommends that companies conduct a detailed review of an applicant's online presence for consistency in name, appearance, work history, and education prior to offering employment.