



Marketing Research

Saja DPRK Employment Scam Network

May 2025

Table of Contents

Executive Summary	3
Lion-Themed GitHub Avatars	3
Similar “Century” Email Address	6
Identical Portfolio Websites	6
“About” Section	7
“Portfolio” Section	7
“Testimonial” Section	9
Same Threat Actor, Different Personas	9
Taylor Fuller	9
Inspiration With Digital Living	10
Damian Kowalczyk	11
Wojciech Mazur	12
Thomas Richard	13
Same Persona, Different Threat Actor	13
Jan Kowalski #1	13
Portfolio website	13
GitHub	14
Jan Kowalski #2	14
Summary	15

Executive Summary

Nisos is tracking an IT worker employment scam network posing as Polish and US nationals with the goal of obtaining employment in remote engineering and full-stack blockchain developer roles. Threat actors in this network are using GitHub accounts, portfolio websites, freelancer accounts, and a global freelance software development company, Inspiration With Digital Living (IWDL), to trick companies into hiring them for full-time remote positions and project-based freelance jobs. This network is the first indication that possibly DPRK-affiliated IT workers are setting up fake freelance software development companies with legitimate looking websites to gain freelancer work.

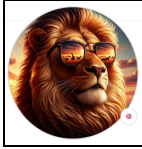

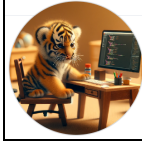
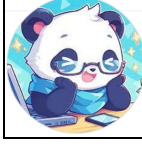




Several indicators suggest that the network is likely affiliated with the Democratic People's Republic of Korea (DPRK). Nisos identified the following tactics, techniques, and procedures (TTPs) commonly attributed to DPRK employment fraud actors on the network's GitHub accounts, portfolio websites, and IWDL's website:

- GitHub accounts exhibited an unusual consistency in avatars, in this case many displayed similar lion-themed pictures.
- Personas within the network used similar email addresses, which frequently included the word "century" in their contact information.
- Portfolio websites exhibited an unusual consistency, suggesting that they were created from the same template with identical information.
- The same threat actor had accounts in different names attempting to gain employment.
- Profile photos were digitally manipulated. Threat actors' faces were often pasted on top of stock photos.
- The same persona was reused by different threat actors.




Lion-Themed GitHub Avatars

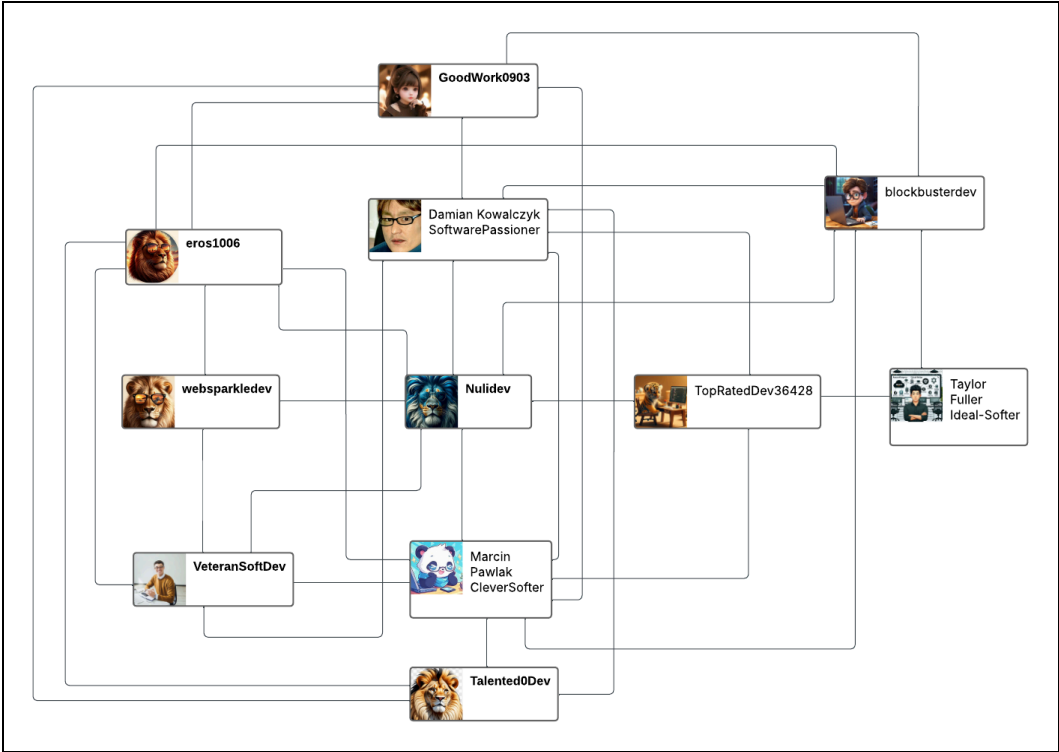
Nisos identified a network of GitHub accounts, which contained repositories for fake portfolio websites likely used to gain employment with unwitting companies. The portfolio websites linked to freelancer and professional networking platform accounts. On these accounts, threat actors claimed to be full-stack developers and engineers located in Poland and the United States looking for employment. Four of the eight most interconnected GitHub accounts in the network have animals as their avatars, three of which were lions. Nisos identified several other GitHub accounts sharing followers with the accounts within this network that also exhibited lion-themed avatars.

GitHub accounts of interest within the network include the following:

URL	Avatar
https://github.com/eros1006	
https://github.com/websparkledev	
https://github.com/TopRatedDev36428	
https://github.com/CleverSofter	
https://github.com/GoodWork0903	
https://github.com/VeteranSoftDev	
https://github.com/SoftwarePassioner	
https://github.com/Ideal-Softer	

Additional GitHub accounts linked to the network by following multiple of the accounts above include the following:

URL	Avatar
https://github.com/nulidev	
https://github.com/Talented0Dev	
https://github.com/blockbusterdev	



Graphic 1: Saja GitHub network connections.

Similar “Century” Email Address

Nisos found that three GitHub accounts and two portfolio websites within the network used email addresses that included the word “century.” We assess that the threat actors used the word to possibly distinguish the network and accounts from other networks.

Email	GitHub URL	Portfolio Website URL
apollo21century@gmail[.]com	https://github[.]com/Ideal-Soft-er	https://portfolio-ideal-softer.vercel[.]app/contact
solomon21century@outlook[.]com	https://github[.]com/GoodWork0903	
erosnewcentury@gmail[.]com	https://github[.]com/websparkldev	
apollo21century@gmail[.]com		https://cleversofter.github[.]io
apollo21century@gmail[.]com		https://softwarepassionner.github[.]io

Identical Portfolio Websites

Nisos found five active portfolio websites on GitHub[.]io and vercel[.]app and two inactive websites. The portfolio websites are mostly designed with identical elements, which include “about” sections, portfolios, and testimonials.

The portfolio websites associated within this network include the following:

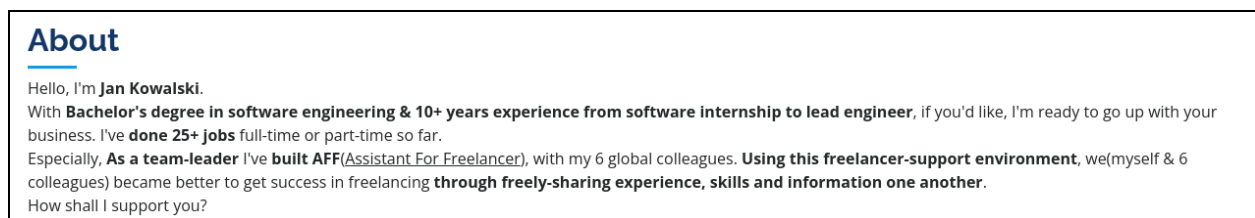
- [https://veteransoftdev.github\[.\]io](https://veteransoftdev.github[.]io) (active)
- [https://softwarepassionner.github\[.\]io](https://softwarepassionner.github[.]io) (active)
- [https://cleversofter.github\[.\]io](https://cleversofter.github[.]io) (active)
- [https://goodwork0903.github\[.\]io](https://goodwork0903.github[.]io) (active)
- [https://portfolio-ideal-softer.vercel\[.\]app](https://portfolio-ideal-softer.vercel[.]app) (active)
- [https://dedicatedsoftwaredev.github\[.\]io](https://dedicatedsoftwaredev.github[.]io) (inactive)
- [https://seasonedsoftdev.github\[.\]io](https://seasonedsoftdev.github[.]io) (inactive)



Graphic 2: Example of a portfolio website.¹

“About” Section

The “about” sections frequently included references to working 10+ years, having built an “Assistant for Freelancer,” and having completed more than 25 jobs.



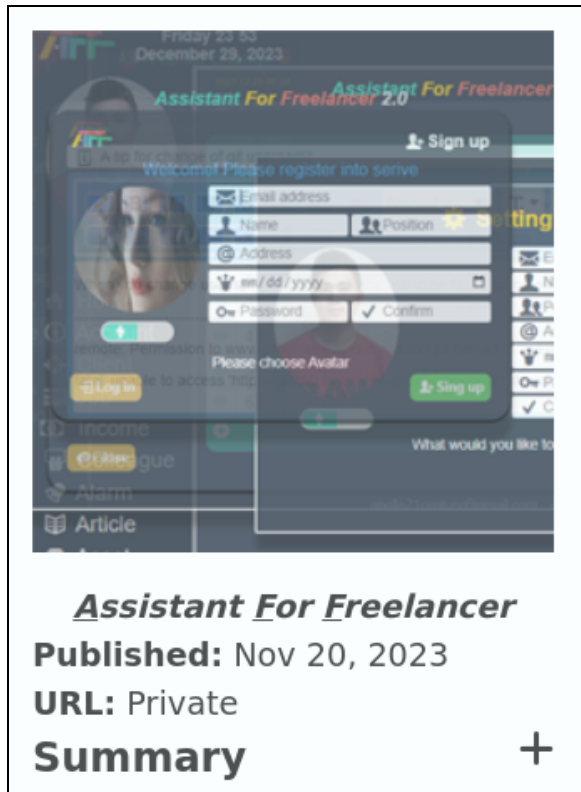
Graphic 3: Jan Kowalski's about section in his portfolio website.²

“Portfolio” Section

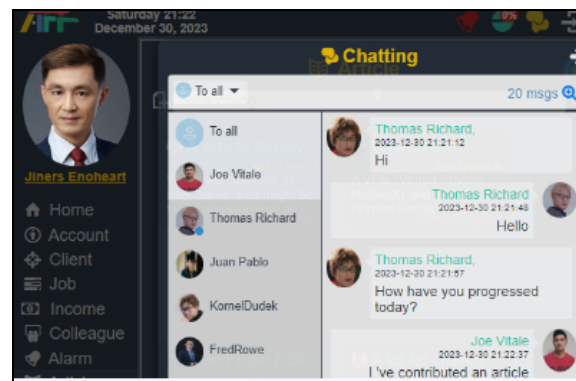
The “portfolio” sections frequently referenced having worked on a service called “Assistant For Freelancer (AFF),” which was described as a private service supporting freelancers. Many portfolios also included work on the development of an “Anti-Game-Cheat engine focusing on AI components to detect cheating.”

¹<https://veteransoftdev.github.io>

²<https://veteransoftdev.github.io>



Graphic 4: AFF portfolio example.³



Graphic 5: AFF portfolio example 2.⁴



Graphic 6: “Anti-Game-Cheat” engine portfolio example.⁵

³[https://portfolio-ideal-softer.vercel\[.\]app/portfolio](https://portfolio-ideal-softer.vercel[.]app/portfolio)

⁴[https://softwarepassioner.github\[.\]io](https://softwarepassioner.github[.]io)

⁵[https://cleversofter.github\[.\]io](https://cleversofter.github[.]io)

“Testimonial” Section

The “testimonial” sections frequently contained fake testimonials from other personas included within the network and personas listed as examples in the AFF service screenshots on the portfolio websites. The personas included: Kornel Dudek, Fred Rowe, Juan Pablo Torres, and Thomas Richard.



Graphic 7: Testimonials section example.⁶

Same Threat Actor, Different Personas

Nisos identified one threat actor, who is likely the operator of four different personas aiming to obtain remote work. Nisos identified four digitally enhanced photographs of likely the same individual, who claimed to be four different people located in Poland and the United States.

Taylor Fuller

Nisos identified a portfolio website, an active professional networking platform account, a GitHub account, and a software solutions company, which use digitally manipulated photos of the threat actor using the name Taylor Fuller and claiming to be located in the United States.

- The portfolio website claimed that Taylor Fuller led the development of the AFF service, as well as the website of software company, Inspiration With Digital Living (IWDL).⁷

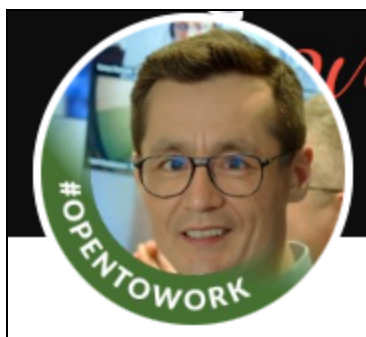
⁶<https://softwarepassioner.github.io>

⁷[https://portfolio-ideal-softer.vercel\[.\]app/portfolio](https://portfolio-ideal-softer.vercel[.]app/portfolio)



Graphic 8: Photo of the threat actor on Taylor Fuller's portfolio website.⁸

- A professional networking platform account linked to the portfolio website and the software solutions company. The account is named ideal-softer, similar to the GitHub account associated with Taylor Fuller.



Graphic 9: Photo of the threat actor on Taylor Fuller's professional networking platform account.

- The GitHub account Ideal-Softer claimed over nine years of experience in web service and mobile applications. The account linked to the portfolio website, as well as the professional networking platform account for IWDL.⁹ Ideal-Softer updated the website address for IWDL in the GitHub repository for IWDL in mid-April 2025, suggesting that the website is possibly less than one year old.¹⁰

Inspiration With Digital Living

Nisos identified a website for software solutions company IWDL, which is linked to Taylor Fuller. The website contains digitally manipulated images, lists employees that are not affiliated with the company, and a fake address in the United States. Whois information shows that the website was registered on 22 November 2024, confirming that it is less than a year old. We assess that the website

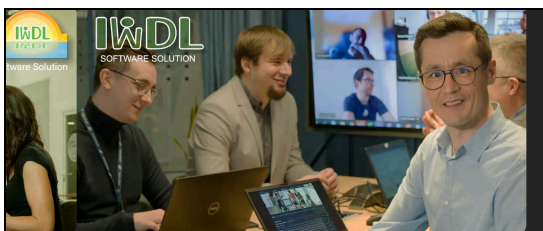
⁸[https://portfolio-ideal-softer.vercel\[.\]app/home](https://portfolio-ideal-softer.vercel[.]app/home)

⁹[https://github\[.\]com/Ideal-Softer](https://github[.]com/Ideal-Softer)

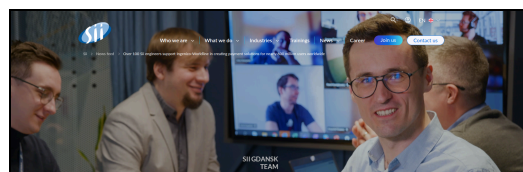
¹⁰[https://github\[.\]com/orgs/IWLD/repositories](https://github[.]com/orgs/IWLD/repositories)

was set up to gain new clients for the threat actors and enhance the perception of legitimacy. Nisos identified a number of red flags on the website, which suggest that the company is not legitimate:

- The landing page for the website contained a photo of the threat actor, which was identical to the photo on the professional networking platform account. The photo, however, was digitally manipulated.



Graphic 10: Photo from IWDL website.¹¹



Graphic 11: Original photo from SII website.¹²

- The website listed a number of key executives, including Taylor Fuller, Maurice Antoine Jr, and Adedayo Onasanya. Nisos investigators reviewed Maurice Antoine Jr's and Adedayo Onasanya's work history and social media accounts and did not identify any references to IWDL, suggesting that they are likely not part of the executive team.
- The website lists 1301 Ruby Ave, Houghton, MI 49931 as a business address. A review of the address however shows that the location is rental housing near Michigan Technological University.¹³

Damian Kowalczyk

Nisos identified a GitHub account, softwarepassioner, which included a photo of the threat actor with the name Damian Kowalczyk. The GitHub account stated that Damian Kowalczyk has 10+ years of experience and listed a number of completed projects. This information is similar to the information included on the portfolio websites listed in the section above, suggesting that this account is linked to the network. The GitHub account stated that Damian Kowalczyk is located in Poland and links to an inactive professional networking platform account. The GitHub account created a repository for a portfolio website in late June 2024, however, the website is not active.

¹¹[https://www.iwdl\[.\]org/home](https://www.iwdl[.]org/home)

¹²[https://sii\[.\]pl/en/news-feed/over-100-sii-engineers-support-ingenico-worldline-in-creating-payment-solutions-for-nearly-600-million-users-worldwide/?category=career-development&tag=newsletter-en,career](https://sii[.]pl/en/news-feed/over-100-sii-engineers-support-ingenico-worldline-in-creating-payment-solutions-for-nearly-600-million-users-worldwide/?category=career-development&tag=newsletter-en,career)

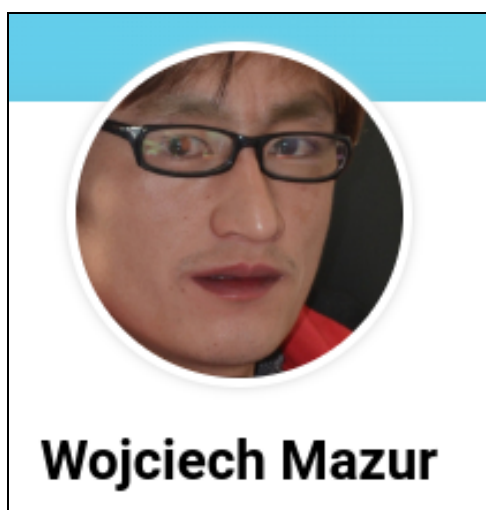
¹³[https://www.houghtonforrent\[.\]com/university-suites-1/1301-ruby-university-suites](https://www.houghtonforrent[.]com/university-suites-1/1301-ruby-university-suites)



Graphic 12: Photo of the threat actor alongside the name Damian Kowalczyk.¹⁴

Wojciech Mazur

Nisos investigators identified a freelancer website, which included a photo of the threat actor listed with the name Wojciech Mazur, who claimed to be an AI/Web/Mobile/Desktop app developer from Poland. Of note, the persona claimed to have worked on developing the IWDL company website, which is also associated with Taylor Fuller, further suggesting that the same threat actor is the user of multiple personas.



Graphic 13: Photo of the threat actor alongside the name Wojciech Mazur.¹⁵

¹⁴<https://github.com/SoftwarePassioner>

¹⁵<https://www.freelancermap.com/profile/wojciech-mazur>

Thomas Richard

A photo of the threat actor was included alongside the name Thomas Richard in a screenshot of the AFF service on the portfolio section of several portfolio websites linked to the network.



Graphic 14: Photo of the threat actor alongside the name Thomas Richard.¹⁶

Same Persona, Different Threat Actor

Nisos identified a fake persona associated with the network, Jan Kowalski, who has accounts containing photos of different individuals. We assess that the two Jan Kowalski accounts are used to obtain employment in different locations.

Jan Kowalski #1

Nisos identified a portfolio website and a GitHub account for Jan Kowalski, which are linked to several other accounts in the network.

Portfolio website

The portfolio website claimed that Jan Kowalski has 10+ years of experience in software engineering. The website also lists 25+ successful projects, including work on “AFF” and the “Anti-Game-Cheat engine focusing on AI components to detect cheating.” The website included a testimonial section, which listed many of the other network personas, including Kornel Dudek, Juan Pablo Torres and Thomas Richard.

The website contained an image of the threat actor that was digitally manipulated.



Graphic 15: Photo of Jan Kowalski from his portfolio website.¹⁷



Graphic 16: Stock photo of graphic 15.¹⁸

¹⁶[https://softwarepassioner.github\[.\]io](https://softwarepassioner.github[.]io)

¹⁷[https://veteransoftdev.github\[.\]io](https://veteransoftdev.github[.]io)

¹⁸[https://www.freepik\[.\]com/premium-photo/young-successful-brunette-man-sitting-his-office-working-with-papers_12622443.htm](https://www.freepik[.]com/premium-photo/young-successful-brunette-man-sitting-his-office-working-with-papers_12622443.htm)

GitHub

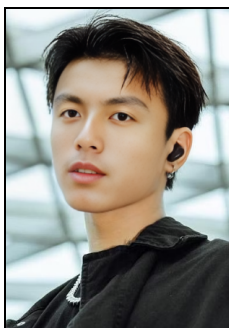
The same threat actor is also associated with GitHub account VeteranSoftDev, which uses the same profile picture and links to the portfolio website. The account contains a repository labeled “Web”, which mentions AFF and highlights work from another network persona, Jiner Enoheart, who was also listed in the AFF screenshots above.¹⁹

Nisos investigators found that according to a talent acquisition platform, Jiners Enoheart claimed to have been located in the United States and appears to have worked for IWDL and Upwork.²⁰

Jan Kowalski #2

Nisos identified a second portfolio website for Jan Kowalski, which claimed that the persona is located in Poland.²¹ The website contained a profile photo of Singaporean actor Glenn Yong and resume content that was used on another freelancer persona account (Mark Lisowski). We assess that this is an indication that the portfolio website is set up as part of an employment scam.

- Nisos found that both Jan Kowalski and Mark Lisowski claimed to be located in Poland and to have worked for the same employers on the same projects. Both individuals listed the same work experience, which included the following complaint about their employer: “During my time at my previous company, I realized that there were limited opportunities to gain extensive knowledge and stay updated with cutting-edge trends. This prompted me to start my freelance career. Through working with various clients, I acquired valuable experience and built a strong foundation in the programming world. Additionally, I developed team management skills while collaborating with freelancers from multiple countries.”^{22 23}



Graphic 17: Photo of Jan Kowalski and Glenn Yong.^{24 25}

¹⁹<https://github.com/VeteranSoftDev/Web/commit/a56b8e07e23afef352cefe9dceffa855c4cfeb2#diff-e0520fec6061d8d891d243d5af05d5a21c5427204587712c5cd376ea60c5f61a>

²⁰<https://www.signalhire.com/profiles/jiners-enoheart/223245812>

²¹<https://portfolio-seven-umber-18.vercel.app/>

²²<https://portfolio-seven-umber-18.vercel.app>

²³<https://www.freelancermapping.com/profile/marek-lisowski>

²⁴<https://portfolio-seven-umber-18.vercel.app>

²⁵<https://www.straitstimes.com/life/entertainment/singapore-actor-glenn-yong-among-tc-candler-s-100-most-handsome-faces>

Summary

Nisos has been tracking DPRK-affiliated employment scam networks since early 2023. Our analysis of the Saja network identified many of the same TTPs commonly associated with DPRK-affiliated IT workers, specifically:

- GitHub accounts exhibited an unusual consistency in avatars
- Personas used similar email addresses
- Portfolio websites exhibited an unusual consistency
- The same threat actor used accounts with different names attempting to gain employment
- Threat actors used digitally manipulated profile photos
- The same persona was reused by different threat actors.

This network is the first indication that possibly DPRK-affiliated IT workers are setting up fake freelance software development companies with legitimate looking websites to gain freelancer work. Nisos recommends that companies looking to partner with freelance software development companies conduct robust reviews of the website and company information to ensure that companies are legitimate businesses and not fronts for freelance work scams.