DPRK IT Fraud Network Uses GitHub to Target Global Companies

By Nisos

Published: 2025-03-04 · Archived: 2026-04-05 14:15:00 UTC

Threat Analysis

Likely DPRK Network Backstops on GitHub, Targets Companies Globally

Executive Summary

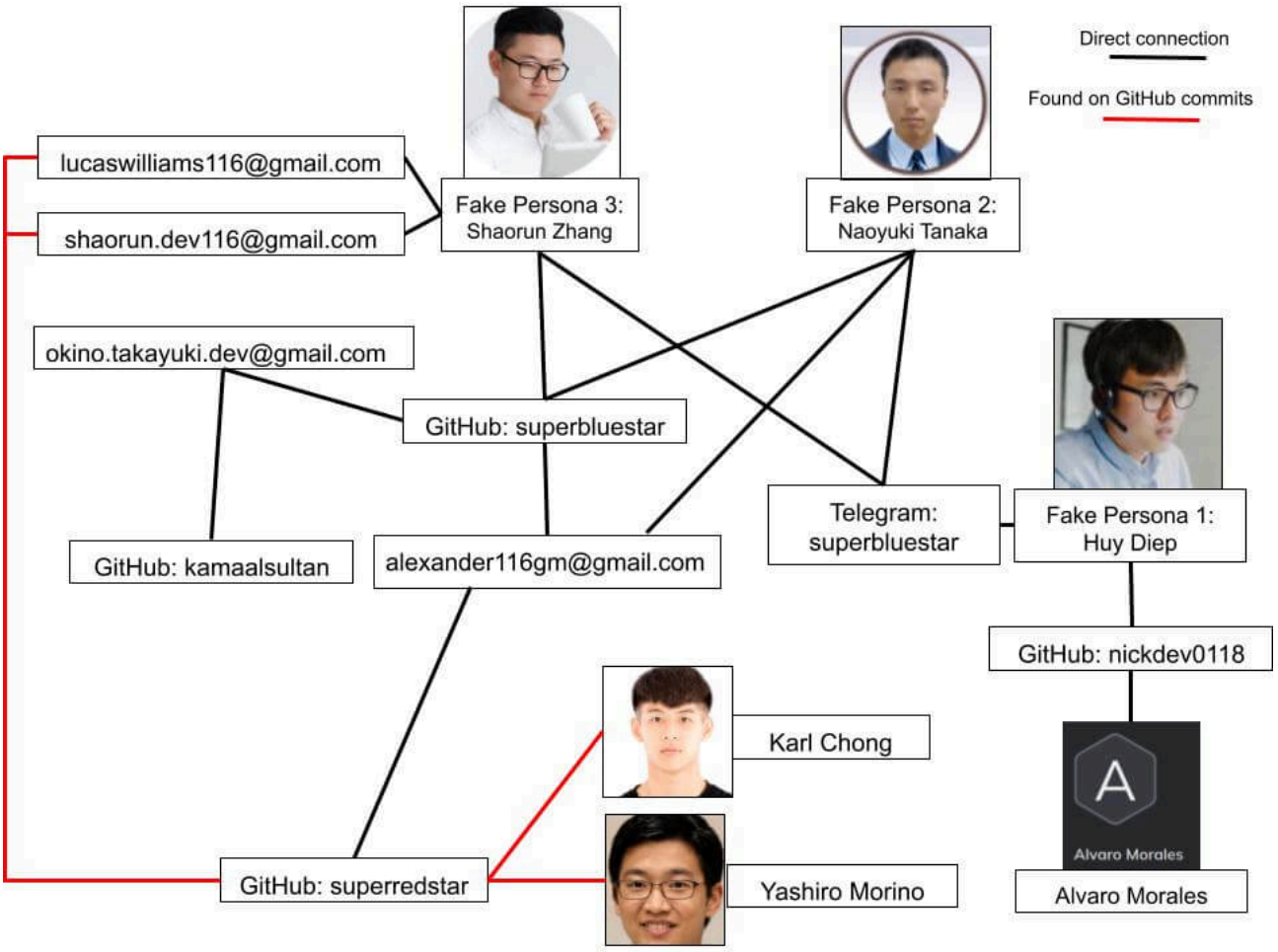
Nisos is tracking a network of likely North Korean (DPRK)-affiliated IT workers posing as Vietnamese, Japanese, and Singaporean nationals with the goal of obtaining employment in remote engineering and full-stack blockchain developer positions in Japan and the United States. While the personas claim 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.



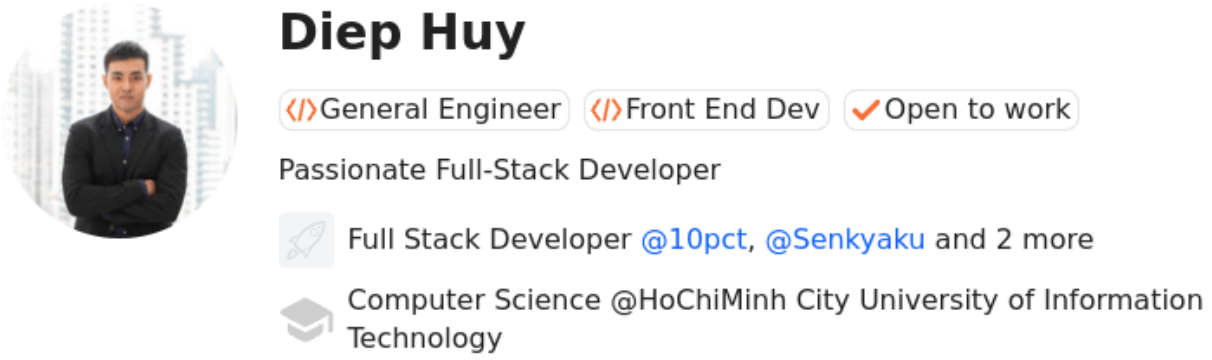
Graphic 1: Network map of likely DPRK-affiliated personas.

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]

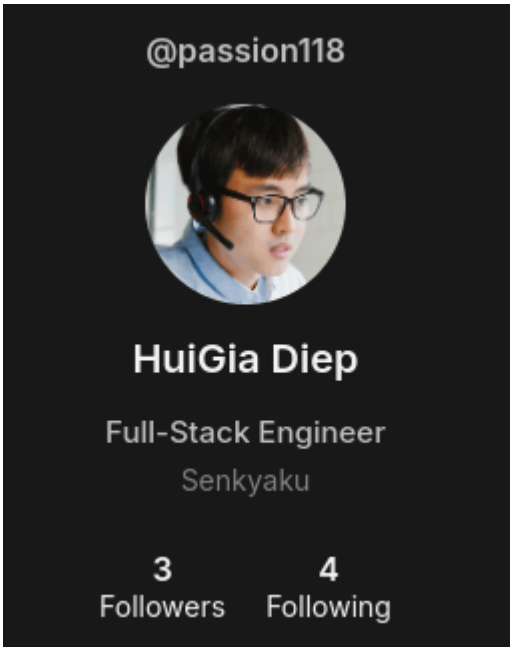
```
From dbfb4c9be96b290136ba23d4fcdd2b2db3b20779 Mon Sep 17 00:00:00 2001
From: O_O <96062458+AnacondaDev0120@users.noreply.github.com>
Date: Tue, 12 Mar 2024 20:34:48 +0800
Subject: [PATCH] This is coautorized

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]



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.

Graphic 8: Photo from Huy Diep’s website.

Graphic 9: Stock photo used in Graphic 8.

Graphic 8: Photo from Huy Diep's website.

Graphic 9: Stock photo used in Graphic 8.

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]

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]

To obtain the complete research report, including endnotes, please click the button below.

About Nisos®

Nisos is the Managed Intelligence Company. We are a trusted digital investigations partner, specializing in unmasking threats to protect people, organizations, and their digital ecosystems in the commercial and public sectors. Our open source intelligence services help security, intelligence, legal, and trust and safety teams make critical decisions, impose real world consequences, and increase adversary costs. For more information, visit: https://nisos.com.
