Research

Exposing a Fraudulent DPRK Candidate: How Nisos Identified a Suspected North Korean Operative

March 2026

Table of Contents

Executive Summary

Since early 2023, Nisos has provided our clients with critical insights and conducted OSINT (Open-Source Intelligence) pre-employment and insider risk investigations to mitigate the threat of North Korean (DPRK) IT worker employment schemes. In June 2025, we used a combination of pre-employment OSINT due diligence and targeted interview questions to expose a suspected DPRK operative, who applied for a remote Artificial Intelligence (AI) architect role at Nisos. The operative unsuccessfully used stolen personally identifiable information (PII), a newly created email, and an AI-created resume to pose as a Florida-based lead AI architect and senior full stack developer. Nisos subsequently identified an employment fraud network involving the IT worker, which included a laptop farm located in Florida. Our investigation of the laptop farm identified that DPRK IT workers leverage Raspberry Pi-based KVM (Keyboard-Video-Mouse) devices to remotely access desktops and mesh VPN services like Tailscale to connect multiple devices to a network they control despite being located across US residences. Nisos also identified the following well-known suspected operative tactics, techniques, and procedures (TTPs) during the investigation and interview, which are linked to DPRK IT workers:

DPRK remote IT worker TTPs	Observed?
Use of Astrill VPN	✓
Establish a US-based identity to apply for roles at US-based companies	✓
Created a new email address	✓
Lack of compromised data for email address	✓
Use of VoIP phone number	✓
Re-use of resume content across multiple accounts	✓
Leverage AI tools to assist with resume content creation and interview answers	✓
Provide a different mailing address for the laptop	✓
Establish legitimacy through fake profiles on LinkedIn and other resume platforms	✓
Leverage of IP-KVM devices like PiKVM for remote access of highly secured corporate laptops without detection	✓
Leverage of mesh VPN service like Tailscale to connect devices	✓

Establish legitimacy through fake portfolios on GitHub or portfolio websites	N/A

Operative Details

The suspected DPRK operative applied to the Lead AI Architect role using the following PII.

- Phone: 850-308-4867
- Email address: Jo***@gmail[.]com
- Address: Palm Beach Gardens, FL 33410
- IPs: 167.88.61.250 and 167.88.61.117

Graphic 1: Image of the suspected DPRK operative during the interview.

Astrill VPN

The operative is likely connected to the DPRK remote hiring scheme as his IP address appears to follow common TTPs associated with DPRK IT workers. The operative used IP addresses 167.88.61.250 and 167.88.61.117 when interacting with Nisos, which likely belong to the Astrill VPN anonymization network.[1] [2] Cybersecurity firms like Mandiant have published lists of IP addresses that DPRK remote workers used. Many of these IP addresses are associated with the Astrill VPN service, a popular VPN in China.[3]

[1]https://spur[.]us/context/167.88.61.250
[2]https://spur[.]us/context/167.88.61.117
[3]https://spycloud[.]com/blog/how-we-identified-fake-north-korean-it-workers/

VoIP Phone Number

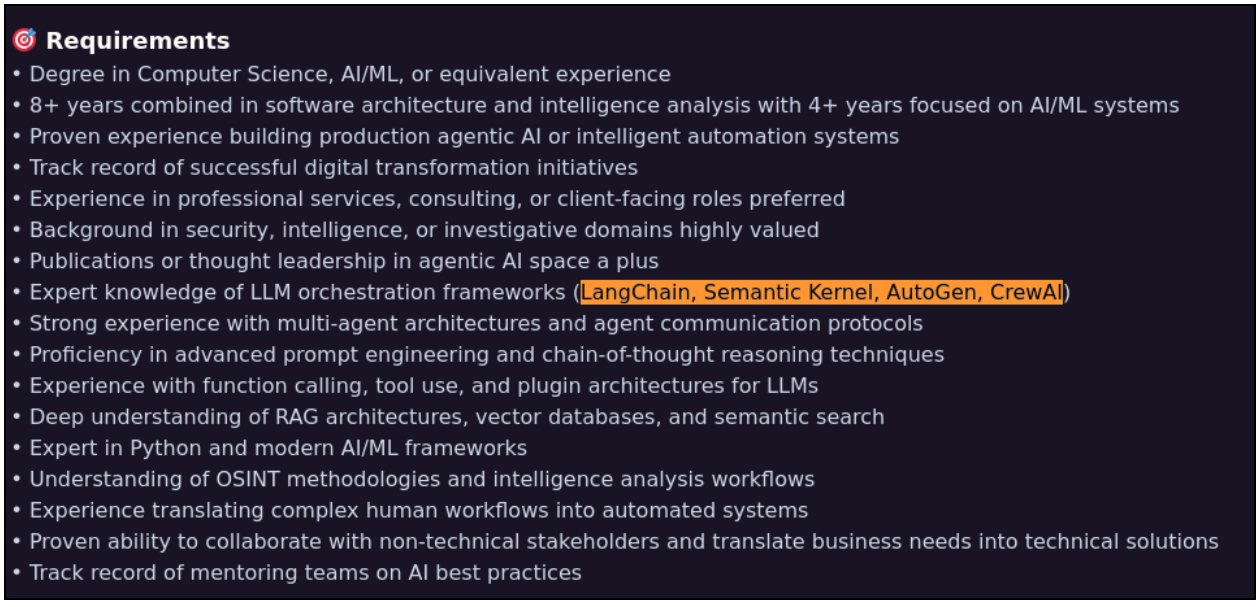
Nisos found that phone number 850-308-4867 is likely a Voice over Internet Protocol (VoIP) number, which allowed the suspected DPRK operative to make phone calls over the internet instead of traditional phone lines. While some people use VoIP numbers as a legitimate method for contact, scammers regularly use VoIP numbers to choose phone numbers matching their applicant's alleged location.

Use of AI for Resume Creation

The operative likely used an AI chatbot to create his resume as the resume repeated many of the skills mentioned in the Lead AI Architect job description.

List of Skills

The suspected DPRK operative's resume contained a list of skills, which included a number of programming languages, agentic AI tools, databases, cloud platforms and OSINT tools that he almost certainly copied from the job description. DPRK IT workers have been known to include large amounts of skills and program languages in their resumes in order to make their resumes more attractive to potential employers.



Graphic 2: List of skills in the Lead AI Architect role.

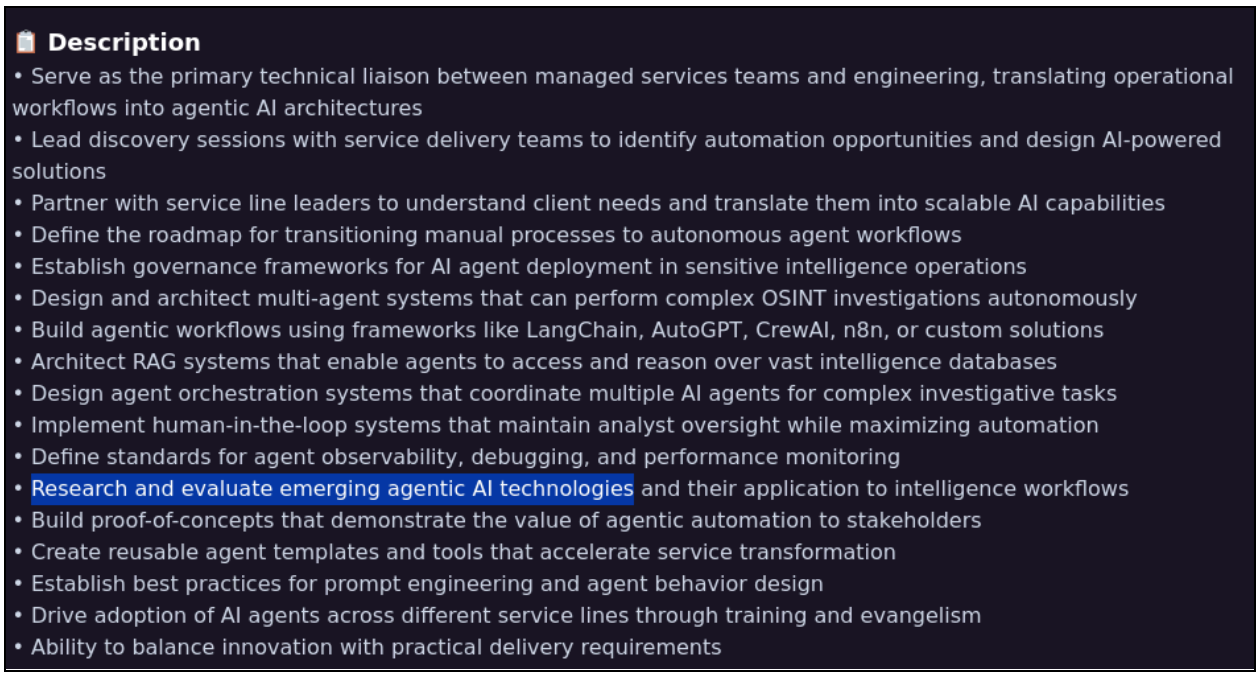
SKILLS

- **Programming Languages:** Python, Java, JavaScript, C++, R, Scala, Go, Ruby
- **AI/ML Frameworks:** TensorFlow, PyTorch, Keras, Scikit-learn, Hugging Face, OpenAI, AutoML, LangChain
- **Agentic AI Tools:** LangChain, AutoGPT, CrewAI, n8n, Semantic Kernel, AutoGen, RAG systems, Agent Orchestration
- **Databases:** Vector Databases, SQL, NoSQL, MongoDB, PostgreSQL, Neo4j, Redis, Elasticsearch
- **Cloud Platforms:** AWS, Azure, Google Cloud, IBM Cloud, Oracle Cloud, Alibaba Cloud, Heroku, DigitalOcean
- **DevOps Tools:** Docker, Kubernetes, Jenkins, GitLab CI/CD, Terraform, Ansible, Puppet, Chef
- **OSINT Tools:** Maltego, Shodan, Recon-ng, SpiderFoot, theHarvester, Metasploit, Censys, FOCA

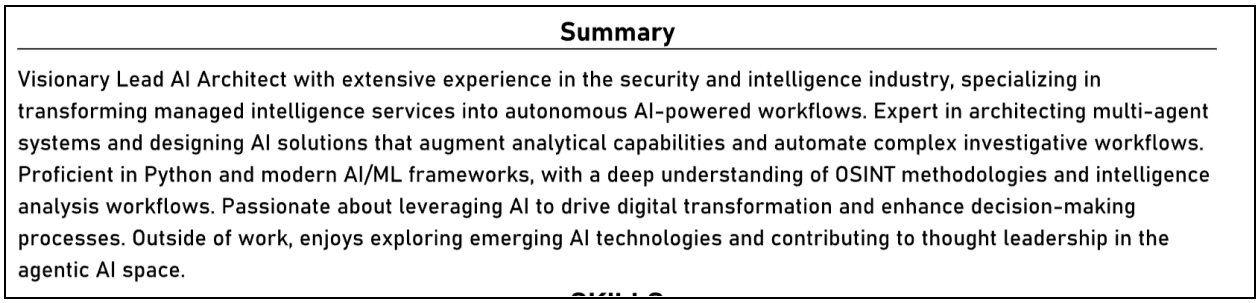
Graphic 3: List of skills in the suspected DPRK operative's resume.

Mirrored Job Description Language

The suspected DPRK operative's resume included a summary section, which reused content from the Lead AI Architect job description. The job description included language about researching and evaluating emerging agentic AI technologies, which the resume mirrored.



Graphic 4: Description of the Lead AI Architect role.



Graphic 5: Summary section of the DPRK operative's resume.

Use of Conversational AI Chatbot/Scripts for Video Interview

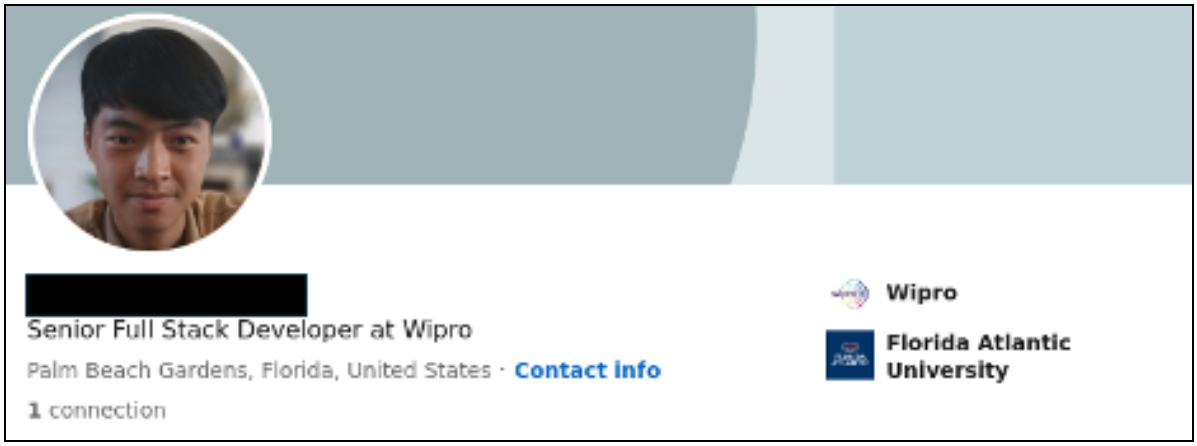
On 24 June 2025, Nisos conducted a virtual interview with the suspected DPRK operative. During the interview, which was conducted in English, the operative frequently looked away from the camera while answering the questions. While some of the answers could have been scripted, Nisos asked the operative a fake question about hurricane George, which supposedly impacted Florida within the last week. The operative started his reply with "How can I say?" while looking at another screen. The operative used the same phrase to start his answers to other questions that also required him to not read a script, suggesting he was waiting for the AI chatbot to provide him an answer before replying to the question.

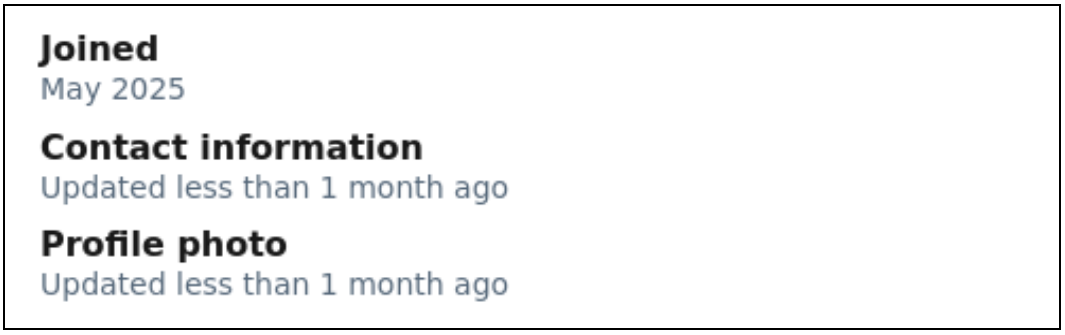
Multiple Resume Accounts with the Same Name but Different Details

The pre-employment OSINT investigation into the suspected DPRK operative revealed three different resumes, which suggested that the operative likely set up accounts on resume platforms to gain employment as a senior full stack developer. The operative created one of the accounts in May 2025, suggesting that the persona that applied for the role at Nisos was likely a new persona. Nisos found that the resumes listed two different universities and many different employers, suggesting that the accounts and resumes were set up at different times. Of note, all resumes appear to be linked based on the true addresses of a real individual who likely had his identity stolen.

Resume Site #1

Nisos identified an account for the operative, which listed the same name, same location (Palm Beach Gardens), same university (Florida Atlantic University) and one possible previous employer (Wipro). The account however stated that the person was a full stack developer. Further research into the account showed that it was created in May 2025 and had less than five connections.

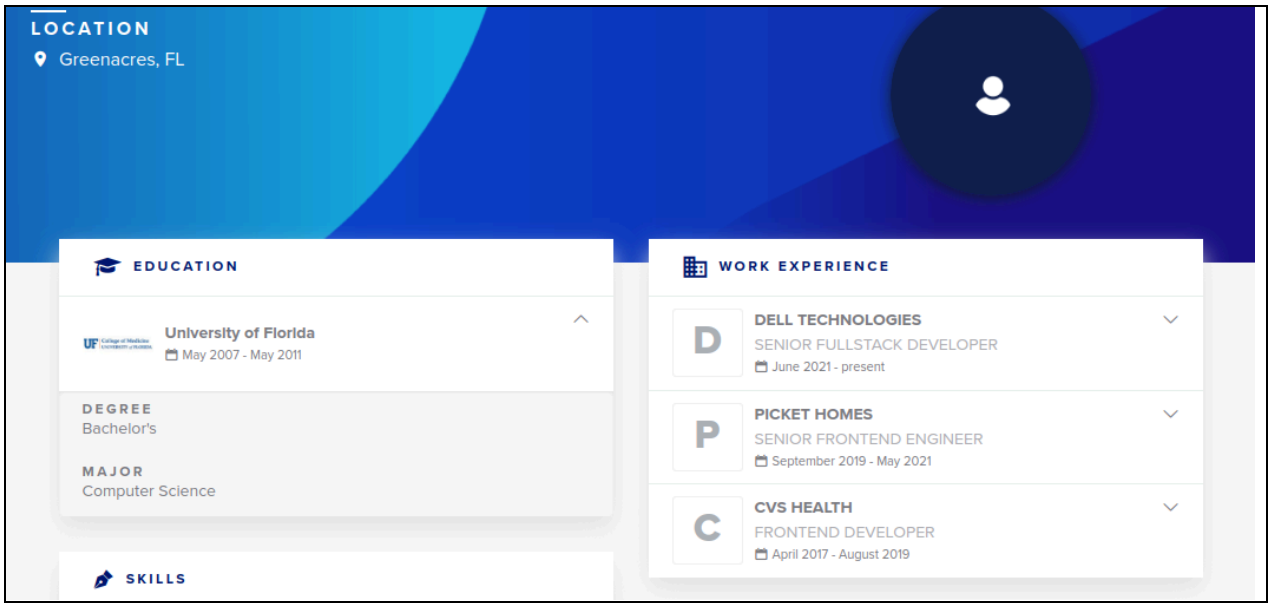




Graphics 6 and 7: Profile details from the DPRK operative's resume account.[4]

Resume Site #2

Nisos identified a second resume for the operative, which listed the same name but a different location (Greenacres), a different university (University of Florida) and different possible previous employers (Dell, Picket Homes and CVS). The resume stated that the person was also a full stack developer.

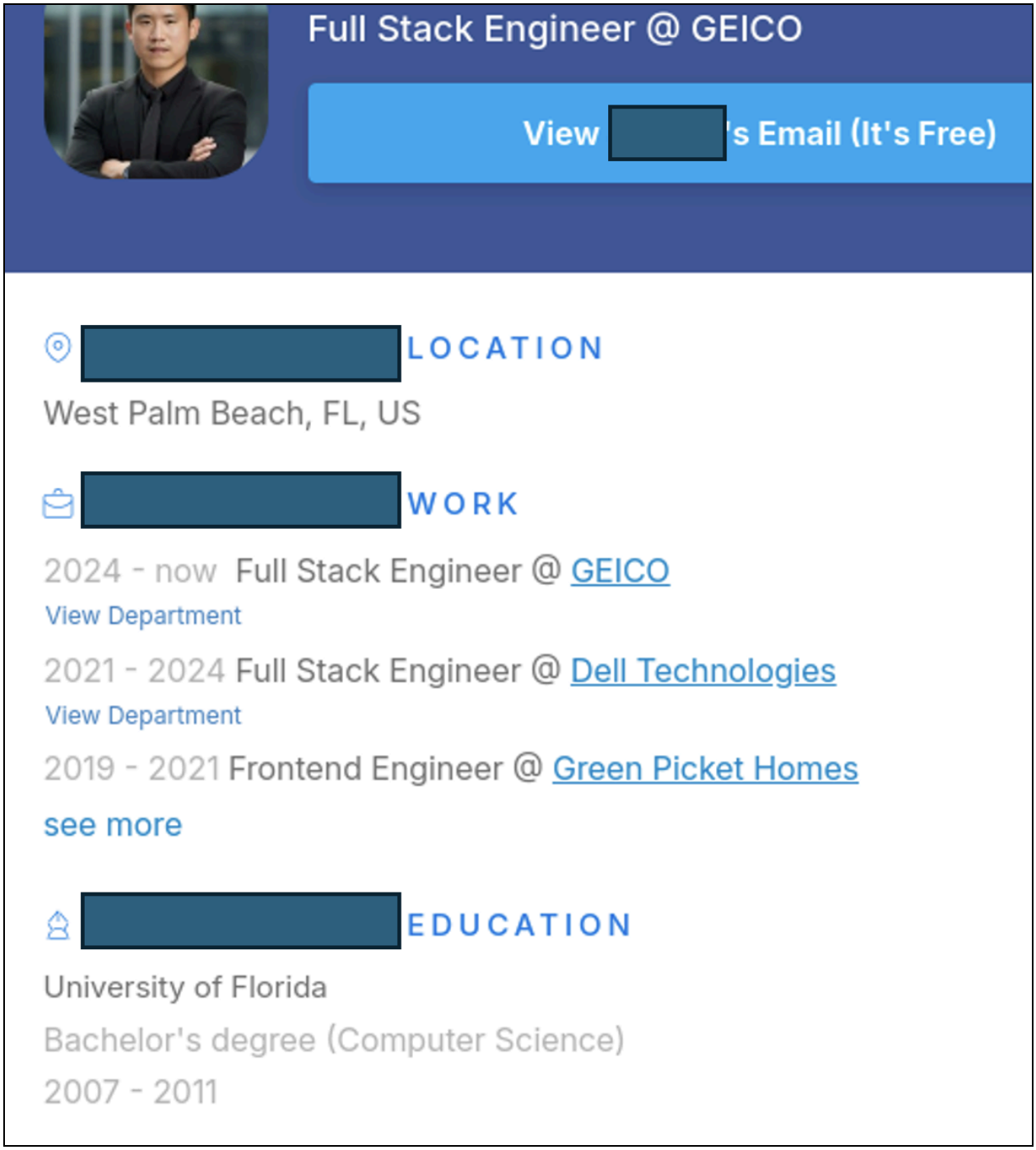


Graphic 8: Possible profile details of a DPRK operative's resume account.[5]

Resume Site #3

Nisos identified a third resume for the operative, which was more closely aligned with resume two above. The resume listed the same name but a different location (West Palm Beach), the same university (University of Florida) and similar possible previous employers (Geico, Dell, Green Picket Homes, and CVS). The resume stated that the person was also a full stack developer.

[4]https://www.linkedin[.]com/in/xxxxxx-xxxxx-36ab17368 (full URL redacted to protect real Florida resident)
[5]https://www.wayup[.]com/profile/xxxxxx-xxxxx-706a59d4b7 (full URL redacted to protect real Florida resident)

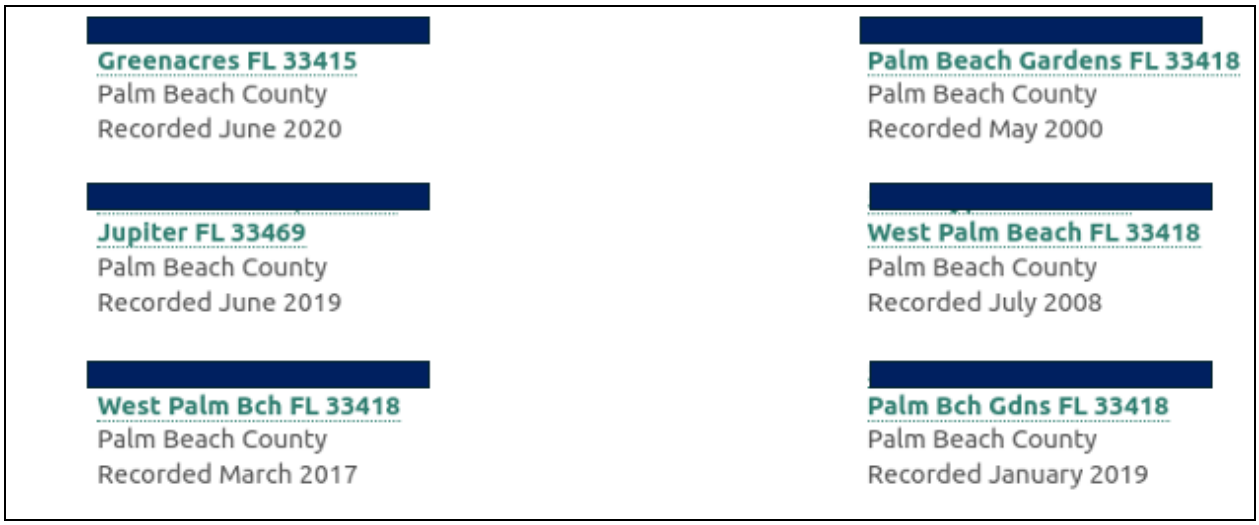


Graphic 9: Possible profile details of a DPRK operative's resume account.[6]

Fake Identity

[6] https://rocketreach[.]co/xxxxxx-xxxxx-email_788004320 (full URL redacted to protect real Florida resident)

The suspected DPRK operative provided a name and address, which Nisos used to conduct an OSINT investigation. Nisos identified an individual with the same name, who lived in Palm Beach Gardens, West Palm Beach and Greenacres, Florida and who attended Florida Atlantic University. Nisos was unable to determine how the operator obtained the person's name and location or whether the individual is connected to the suspected DPRK operator. Our access to the laptop farm however showed that the suspected DPRK operative looked up information about the individual via Google searches. Nisos coordinated victim notification in connection with law enforcement.



Graphic 10: Previous addresses associated with the real Florida resident.

Graphic 11: Previous college experience associated with the real Florida resident.

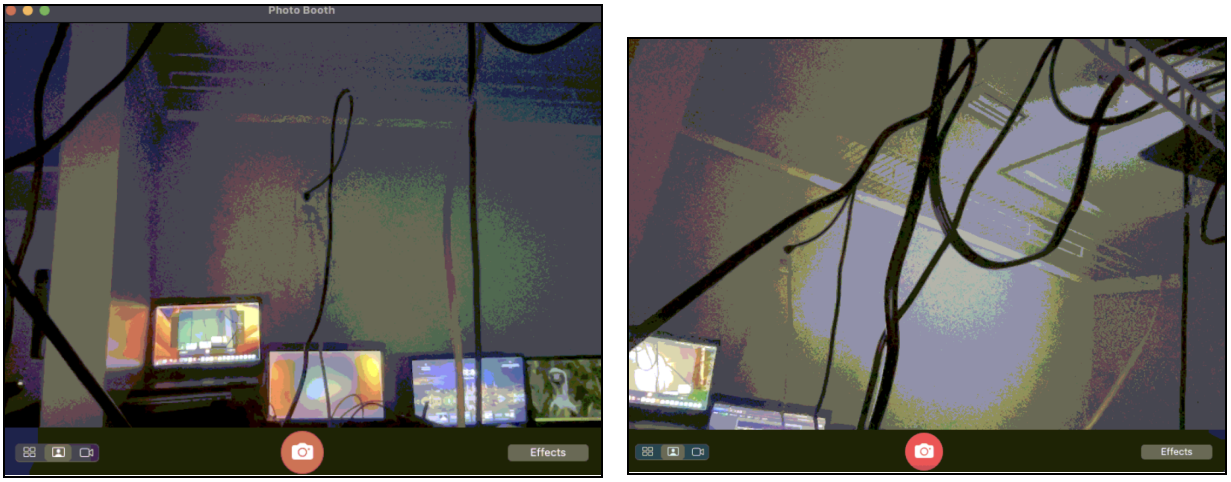
Lack of Portfolio and GitHub Content

During the virtual interview, the suspected DPRK operative claimed to have a little over 10 years experience in AI architecture, mostly in the security and intelligence space. When asked if he had a GitHub account, the operative stated that all of his work had been in private repositories that he could not share. When asked if he had a portfolio of his work or research, the operative stated that he could

send samples later. When Nisos asked him to screenshare and walk the interviewers through some of the work, the operative appeared to frantically close tabs on his screen and left the interview. Since the persona was set up recently, the operative did not create a portfolio page or link an existing GitHub account to the persona.

Laptop Farm

Following the virtual interview, Nisos elected to send a laptop to the suspected DPRK operative's provided mailing address, to identify additional indications that the individual was connected to the DPRK IT worker employment scheme. The address was different from the one provided on the resume and not associated with the individual who lived in Palm Beach Gardens, typical of these types of workforce fraud. Multiple location tracking devices showed that the laptop remained at the mailing address after it was accessed by the IT worker. Nisos used the laptop to take photos of the room via a built-in camera, which revealed that it was likely located in a closet along with several other laptops.



Graphics 12-13: Photos of the laptop farm from the built in camera on the Nisos provided laptop.

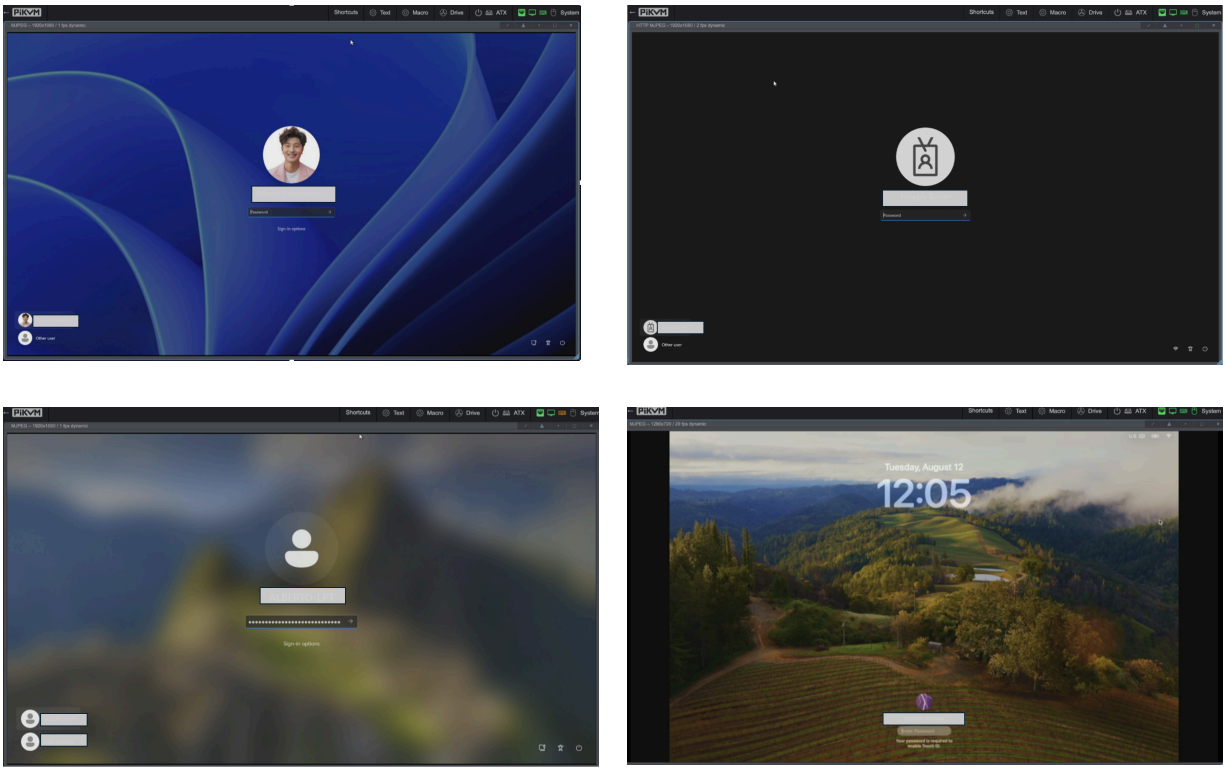
PiKVM

Our access to the network revealed that the laptop was controlled remotely via PiKVM. PiKVM allows users to remotely access and control a computer as if they were physically present, even before the operating system boots. PiKVM devices maintain stealthy, persistent access to laptops, which are harder to detect for company cyber security teams often requiring enforcement of Corporate-Owned, Business-Only policies and USB device controls.[7] Prior tactics employed the use of remote access

[7]https://reliaquest[.]com/blog/threat-spotlight-identifying-north-korean-insider-threats/

software, collaboration tools, or other applications that needed to be installed on the corporate laptop and ran the risk of triggering the owner's endpoint detection.

Once we gained access to the PiKVM admin account, we identified other personas used by the network, which are logged in on other devices on the network. Each of the PiKVM machines are running different laptops for different employee names in different companies. In all, we identified circa 40 devices on the network, 20 of which are likely part of the laptop farm.



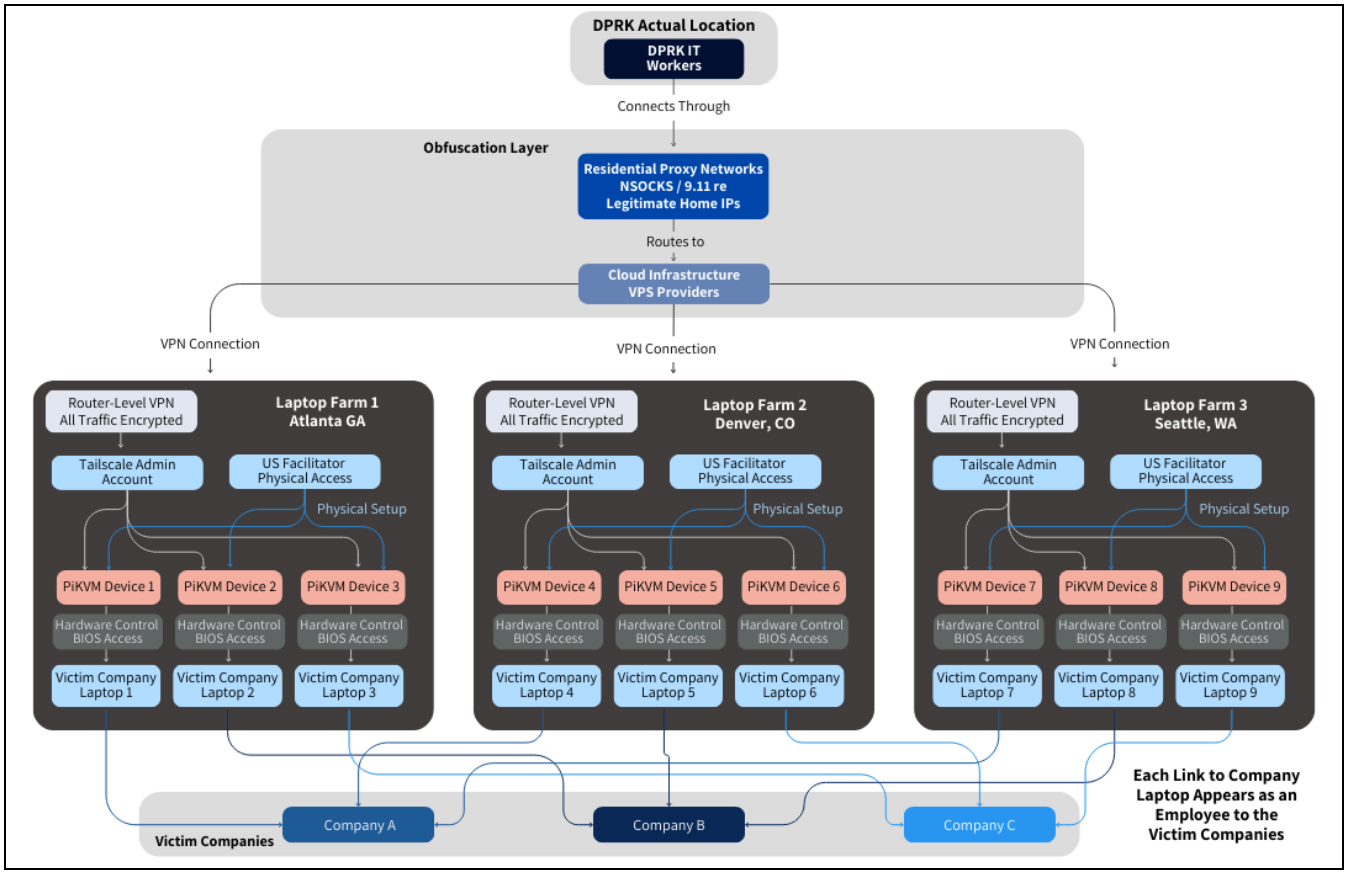
Graphics 14-17: Screenshots of four employee profiles on different laptops administered by PiKVM machines at the laptop farm.

Mesh VPN Service

Our access to the network revealed that the suspected DPRK IT workers used Tailscale to establish a private network allowing the devices on the network to communicate with encrypted point-to-point connections. Tailscale is used by attackers to establish a secure, private network connection, facilitating remote command execution and data exfiltration.[8] Using Tailscale allows the suspected DPRK IT workers to simplify their secure and remote access to the laptops, improving performance and

[8]https://www.cyware[.]com/resources/threat-briefings/daily-threat-briefing/cyware-daily-threat-intelligence-july-18-2024-b702

scalability. As a Toronto, Ontario based company, Tailscale is not required to comply with US law, increasing the difficulty for US law enforcement organizations to mitigate this TTP.



Graphic 18: Conceptual network diagram of DPRK scam.

Lessons Learned

The North Korean IT worker scheme is pervasive and targets companies of all sizes across numerous industries and countries - including companies such as Nisos who have been publishing research relating to DPRK employment fraud for a number of years. Cyber threat hunters have identified hundreds of potential laptop farms in the US (seemingly run by willing Americans) as well as US bank accounts set up with fake identities to allow paychecks to be moved to North Korea. Successful mitigation of the risk relies on an improved vetting process for external remote candidates. Given our experience and expertise with the DPRK scheme and its indicators, Nisos was able to successfully identify a suspected DPRK operative who applied for a remote role at the company. We did this through a combination of pre-employment OSINT research and targeted interview questions to expose employment fraud. Hiring individuals linked to the DPRK employment fraud scheme can expose an organization to IP and data breaches, loss of trust, and regulatory sanctions and fines. If companies are

unable to conduct pre-employment 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 and prevent employment fraud and insider threat activity within their organizations.