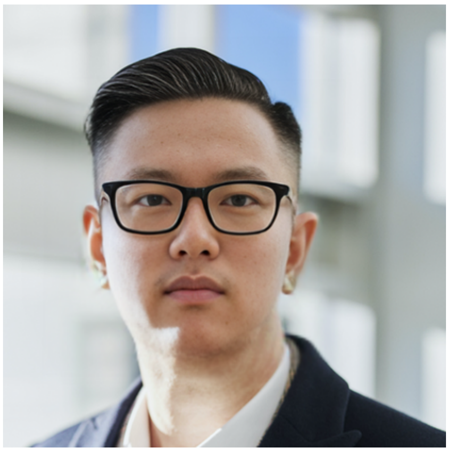
How a North Korean Fake IT Worker Tried to Infiltrate Us

Stu Sjouwerman ∷ 7/23/2024

Stu Sjouwerman



Incident Report Summary: Insider Threat

First of all: No illegal access was gained, and no data was lost, compromised, or exfiltrated on any KnowBe4 systems. This is not a data breach notification, there was none. See it as an organizational learning moment I am sharing with you. If it can happen to us, it can happen to almost anyone. Don't let it happen to you. We wrote an FAQ, answering questions from customers. Story updated 7/27/2024.

TLDR: KnowBe4 needed a software engineer for our internal IT AI team. We posted the job, received resumes, conducted interviews, performed background checks, verified references, and hired the person. We sent them their Mac workstation, and the moment it was received, it immediately started to load malware.

Our HR team conducted four video conference based interviews on separate occasions, confirming the individual matched the photo provided on their application. Additionally, a background check and all other standard pre-hiring checks were performed and came back clear due to the stolen identity being used. This was a real person using a valid but stolen US-based identity. The picture was AI "enhanced".

The EDR software detected it and alerted our InfoSec Security Operations Center. The SOC called the new hire and asked if they could help. That's when it got dodgy fast. We shared the collected data with our friends at Mandiant, a leading global cybersecurity expert, and the FBI, to corroborate our initial findings. It turns out this was a fake IT worker from North Korea. The picture you see is an AI fake that started out with stock photography (below). The detail in the following summary is limited because this is an active FBI investigation.

SUMMARY: This report covers the investigation of Employee ID: XXXX hired as a Principal Software Engineer. On July 15, 2024, a series of suspicious activities were detected on that user account. Based on the SOC teams evaluation of the activities it was found this may have been intentional by the user and suspected he may be an Insider Threat/Nation State Actor. Upon initial investigation and containment of host, a more detailed inquiry into the new hire took place.

On July 15, 2024, a series of suspicious activities were detected on the user beginning at 9:55pm EST. When these alerts came in KnowBe4's SOC team reached out to the user to inquire about the anomalous activity and possible cause. XXXX responded to SOC that he was following steps on his router guide to troubleshoot a speed issue and that it may have caused a compromise.

The attacker performed various actions to manipulate session history files, transfer potentially harmful files, and execute unauthorized software. He used a raspberry pi to download the malware. SOC attempted to get more details from XXXX including getting him on a call. XXXX stated he was unavailable for a call and later became unresponsive. At around 10:20pm EST SOC contained XXXX's device.

How this works is that the fake worker asks to get their workstation sent to an address that is basically an "IT mule laptop farm". They then VPN in from where they really physically are (North Korea or over the border in China) and work the night shift so that they seem to be working in US daytime. The scam is that they are actually doing the work, getting paid well, and give a large amount to North Korea to fund their illegal programs. I don't have to tell you about the severe risk of this. It's good we have new employees in a highly restricted area when they start, and have no access to production systems. Our controls caught it, but that was sure a learning moment that I am happy to share with everyone.

TIPS TO PREVENT THIS

- Scan your remote devices, to make sure no one *remotes into those.*
- Better vetting, making sure that they are physically where they are supposed to be.
- Better resume scanning for career inconsistencies.
- Get these people on video camera and ask them about the work they are doing.
- The laptop's shipping address different from where they are supposed to live/work is a red flag.

RECOMMENDED PROCESS IMPROVEMENT

- Background check appears inadequate. Names used were not consistent.
- References potentially not properly vetted. Do not rely on email references only.
- Implement enhanced monitoring for any continued attempts to access systems.
- Review and strengthen access controls and authentication processes.
- Conduct security awareness training for employees, emphasizing social engineering tactics

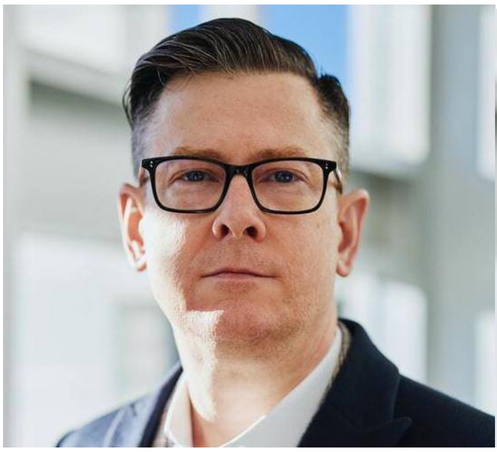
WHAT TO LOOK OUT FOR:

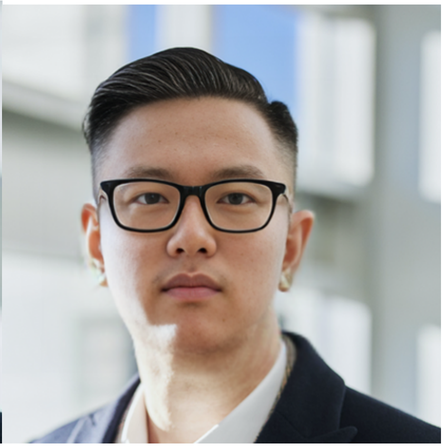
- Use of VOIP numbers and lack of digital footprint for provided contact information
- Discrepancies in address and date of birth across different sources
- Conflicting personal information (marital status, "family emergencies" explaining unavailability)
- Sophisticated use of VPNs or VMs for accessing company systems
- Attempt to execute malware and subsequent cover-up efforts

ALERT HR ABOUT:

The subject has demonstrated a high level of sophistication in creating a believable cover identity, exploiting weaknesses in the hiring and background check processes, and attempting to establish a foothold within the organization's systems.

This is a well-organized, state-sponsored, large criminal ring with extensive resources. The case highlights the critical need for more robust vetting processes, continuous security monitoring, and improved coordination between HR, IT, and security teams in protecting against advanced persistent threats. Left is the original stock picture. Right is the AI fake submitted to HR.





Recommended Resources:

- The U.S. Government is aware of this threat and has been warning against it since 2022. Here is the link.
- Google: Assessed Cyber Structure and Alignments of North Korea in 2023
- Mandiant Podcast on Spotify: The North Korean IT Workers
- Mandiant Blog
- Brian Krebs shared the post on LinkedIn and the comments are heartwarming.