The Prestige

Detecting DPRK IT Workers during before and after hiring

uid=1000(kirushan)

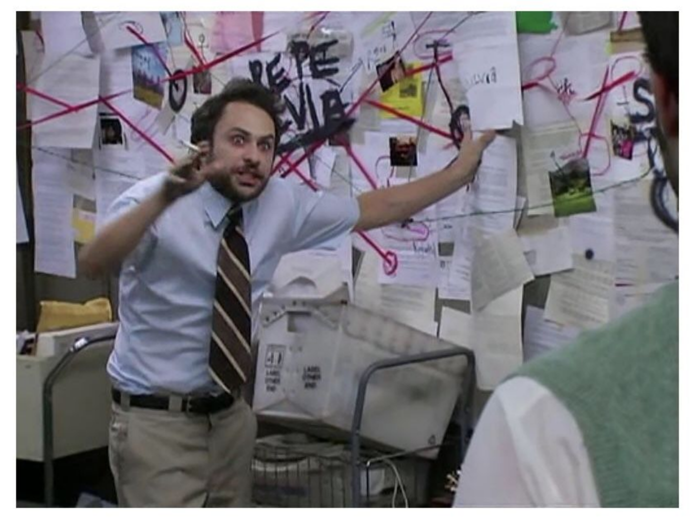
- Kirushan Rasendran
- kirushan.com

Agenda

- Introduction to DPRK
- Motivation of DPRK IT workers
- Detecting the techniques used in pre-hiring
- Detecting the techniques used in post-hiring

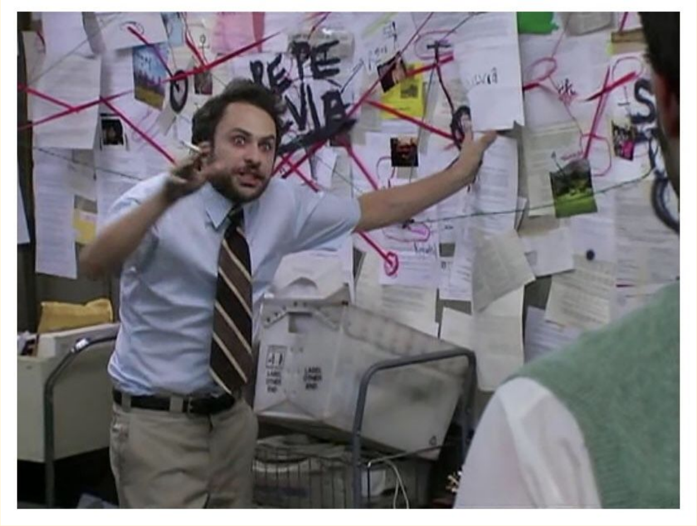
DISCLAIMER

- The opinions are my own
- The information presented herein are collected from publicly available sources
- Techniques presented here are for educational purposes only

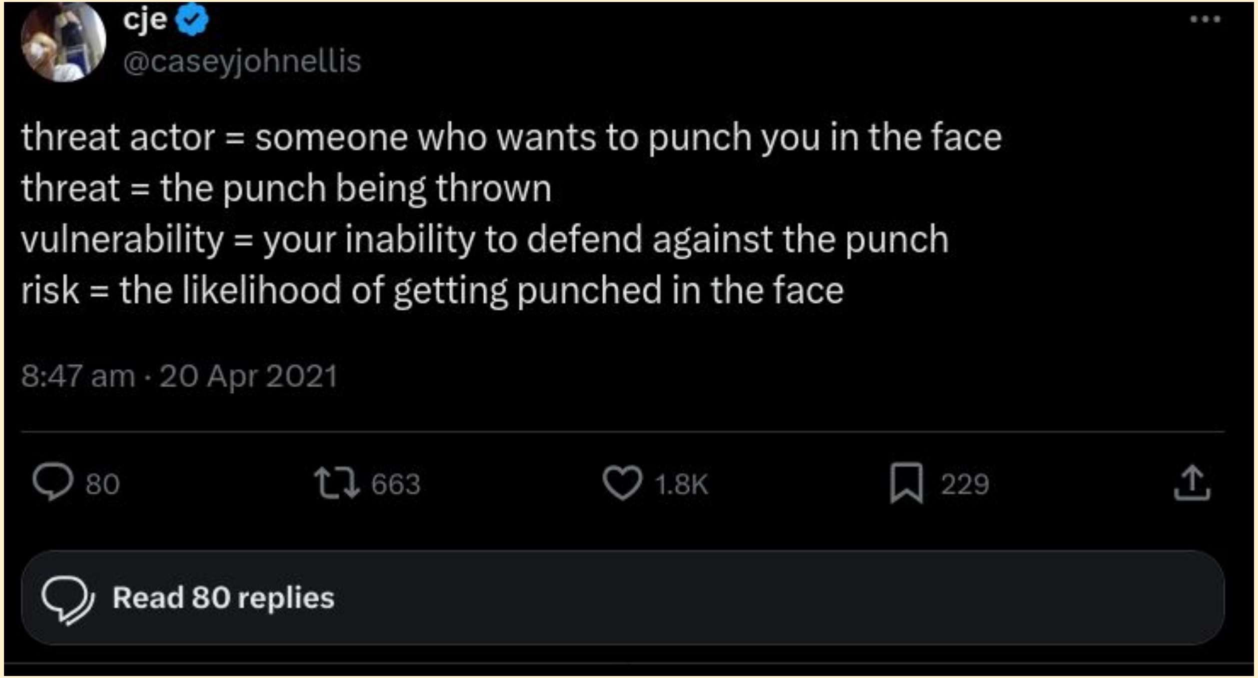


DISCLAIMER

- This is not a legal advice
- I have no affiliations with
    - Vendors/Persons/Agencies/Organisations mentioned in the talk



Terminology



cje
@caseyjohnellis

threat actor = someone who wants to punch you in the face
threat = the punch being thrown
vulnerability = your inability to defend against the punch
risk = the likelihood of getting punched in the face

8:47 am · 20 Apr 2021

[1] The Bar Fight Risk Taxonomy : https://cje.io/2021/06/27/the-bar-fight-risk-taxonomy/

Who is DPRK ?

- Democratic People's Republic of Korea

- DPRK is currently sanctioned [2] by the USA, and their allies for **Nuclear proliferation**

[2] Sanctions source : https://ofac.treasury.gov/media/9221/download?inline
[3] GDP Per Capita Facts https://www.cia.gov/the-world-factbook/countries/korea-north/
[4] DPRK Spending source: https://cove.army.gov.au/kyr/north-korea

Who is DPRK ?

- GDP Per Capita 600 USD (Rank 217) [2]

- On average, DPRK spends **$USD 1.60 billions** on military spending [3]

[2] Sanctions source : https://ofac.treasury.gov/media/9221/download?inline
[3] GDP Per Capita Facts https://www.cia.gov/the-world-factbook/countries/korea-north/
[4] DPRK Spending source: https://cove.army.gov.au/kyr/north-korea

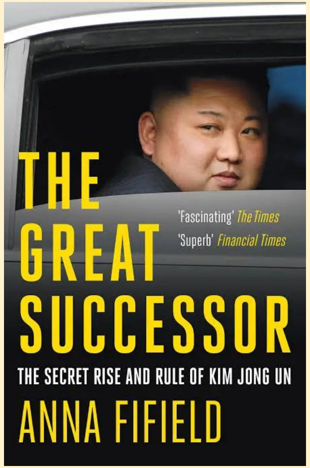
DPRK Activities (Notable)

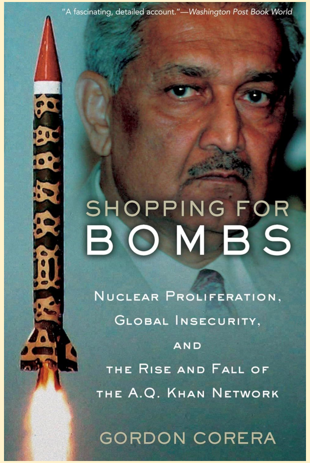
- Sony Hack (2014) [5]
- Bangladesh Bank Heist (2016) [6]
- WannaCry Ransomware (2017) [7]
- Crypto Heists (2017 - Present) [5]
- DPRK IT Workers (2018 - Present) [8]

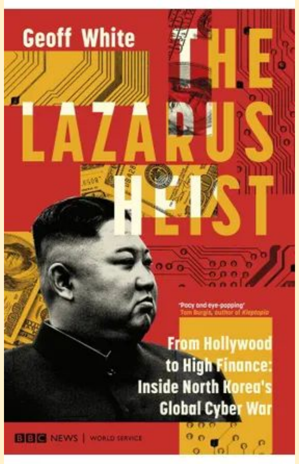
[5] https://www.justice.gov/usao-cdca/pr/3-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyber-attacks-and
[6] Bangladesh Bank Heist https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/
[7] WannaCry Ransomware https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
[8] DPRK IT Workers source : https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote

DPRK + Nuclear Proliferation

Lazarus Heist Podcast on BBC




"A fascinating, detailed account."—Washington Post Book World
SHOPPING FOR BOMBS
Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the A.Q. Khan Network
GORDON CORERA


Geoff White
THE LAZARUS HEIST
'Pacy and eye-popping' Tom Burgis, author of Kleptopia
From Hollywood to High Finance: Inside North Korea's Global Cyber War
BBC NEWS | WORLD SERVICE

Books

DPRK IT Workers

- Targeting Remote positions
- Claiming to be from the USA, UK, Italy, Japan, Singapore, Europe, Colombia, Vietnam[9]
- In 2024, the DPRK likely earned around $350-800 million from its IT workers worldwide[9]

[9] The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities https://msmt.info/Publications/detail/MSMT%20Report/4221 [Pages 52-90]

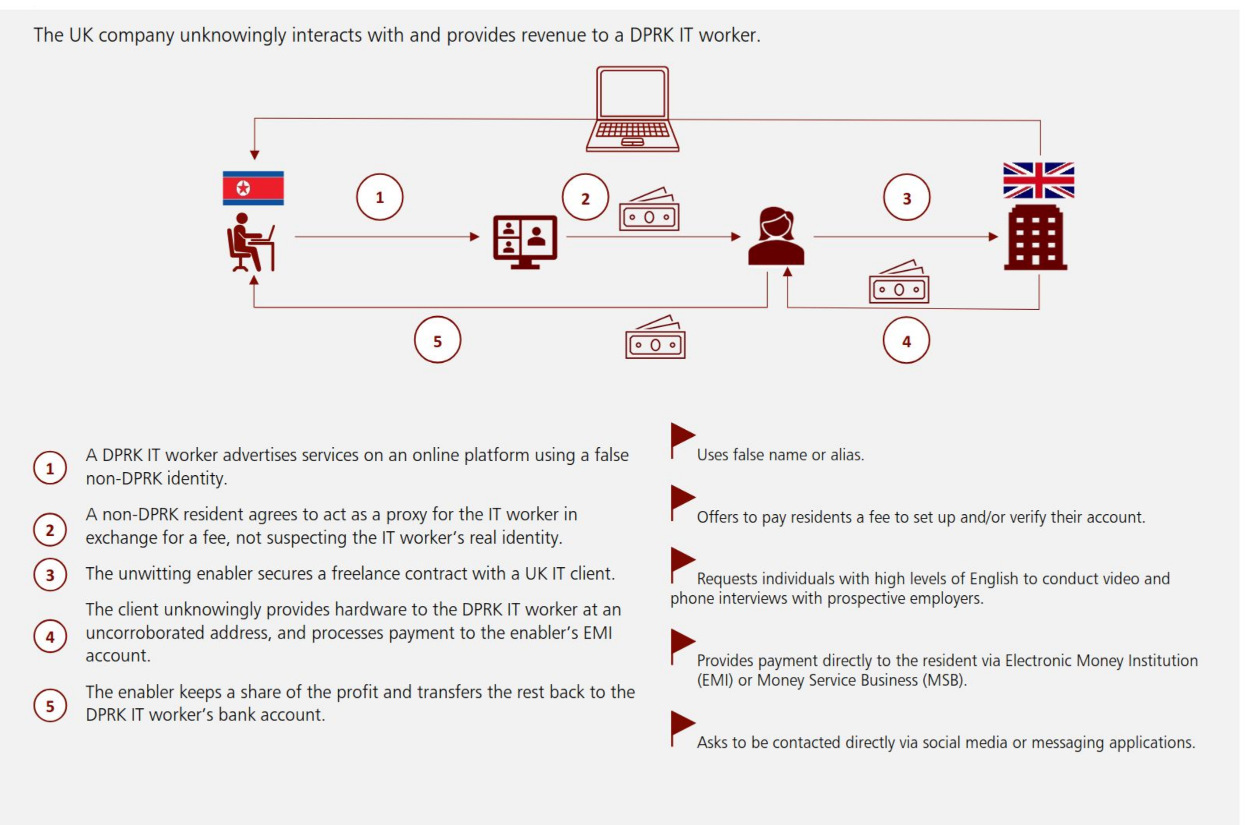
DPRK IT Workers

- Targeting industries in Insurance, Technology, Retail, Legal, and Finance [9]

- Workers work in teams, each team has a manager [9]
  - Target minimum of 3,500 - 10 000 USD Per month per worker

[9] The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities https://msmt.info/Publications/detail/MSMT%20Report/4221 [Pages 52-90]

DPRK IT Workers



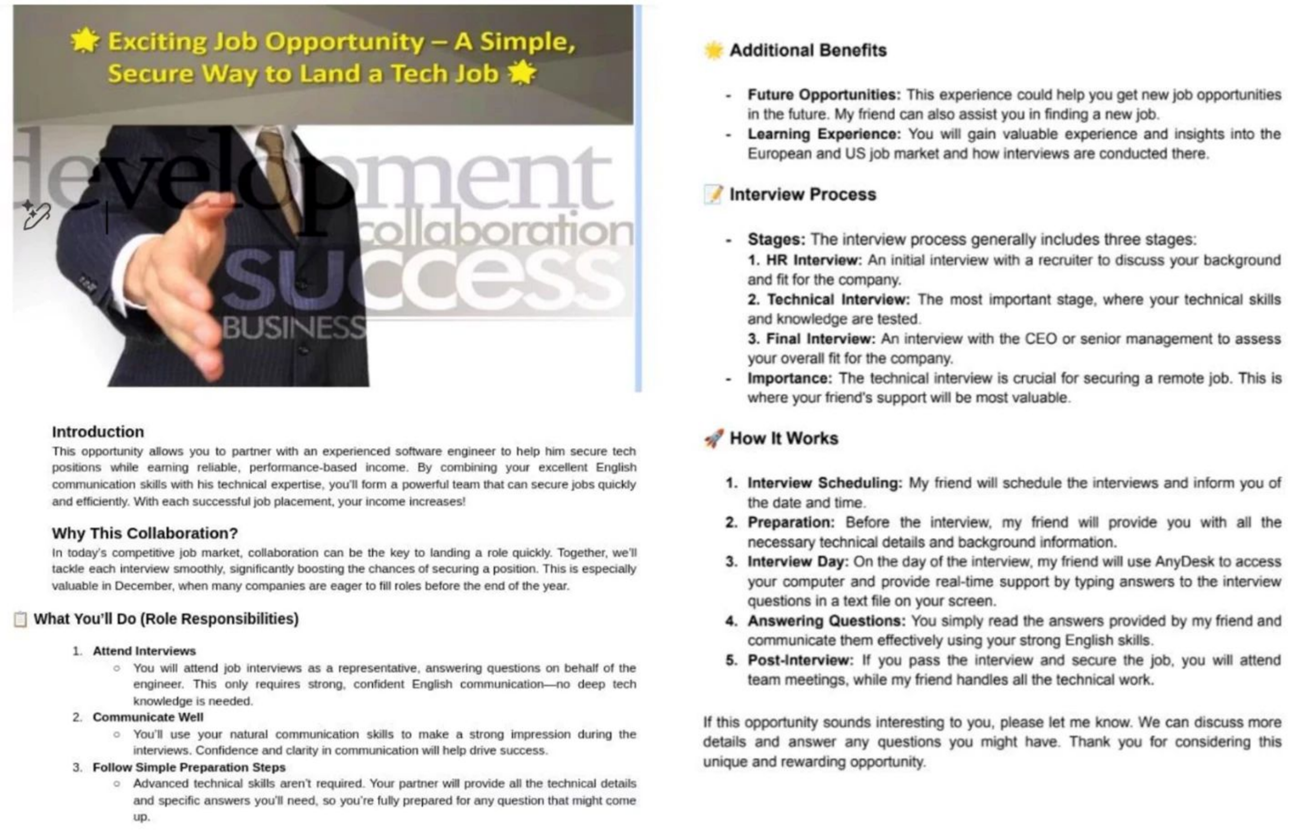
The UK company unknowingly interacts with and provides revenue to a DPRK IT worker.

1. A DPRK IT worker advertises services on an online platform using a false non-DPRK identity.
2. A non-DPRK resident agrees to act as a proxy for the IT worker in exchange for a fee, not suspecting the IT worker's real identity.
3. The unwitting enabler secures a freelance contract with a UK IT client.
4. The client unknowingly provides hardware to the DPRK IT worker at an uncorroborated address, and processes payment to the enabler's EMI account.
5. The enabler keeps a share of the profit and transfers the rest back to the DPRK IT worker's bank account.

- Uses false name or alias.
- Offers to pay residents a fee to set up and/or verify their account.
- Requests individuals with high levels of English to conduct video and phone interviews with prospective employers.
- Provides payment directly to the resident via Electronic Money Institution (EMI) or Money Service Business (MSB).
- Asks to be contacted directly via social media or messaging applications.

[10] Advisory on North Korean IT Workers https://assets.publishing.service.gov.uk/media/66e2ec410d913026165c3d91/OFSI_Advisory_on_North_Korean_IT_Workers.pdf

DPRK IT Workers



🌟 Exciting Job Opportunity – A Simple, Secure Way to Land a Tech Job 🌟

Introduction

This opportunity allows you to partner with an experienced software engineer to help him secure tech positions while earning reliable, performance-based income. By combining your excellent English communication skills with his technical expertise, you'll form a powerful team that can secure jobs quickly and efficiently. With each successful job placement, your income increases!

Why This Collaboration?

In today's competitive job market, collaboration can be the key to landing a role quickly. Together, we'll tackle each interview smoothly, significantly boosting the chances of securing a position. This is especially valuable in December, when many companies are eager to fill roles before the end of the year.

📋 What You'll Do (Role Responsibilities)

1. **Attend Interviews**
   - You will attend job interviews as a representative, answering questions on behalf of the engineer. This only requires strong, confident English communication—no deep tech knowledge is needed.
2. **Communicate Well**
   - You'll use your natural communication skills to make a strong impression during the interviews. Confidence and clarity in communication will help drive success.
3. **Follow Simple Preparation Steps**
   - Advanced technical skills aren't required. Your partner will provide all the technical details and specific answers you'll need, so you're fully prepared for any question that might come up.

🌟 Additional Benefits

- **Future Opportunities:** This experience could help you get new job opportunities in the future. My friend can also assist you in finding a new job.
- **Learning Experience:** You will gain valuable experience and insights into the European and US job market and how interviews are conducted there.

📝 Interview Process

- **Stages:** The interview process generally includes three stages:
  1. HR Interview: An initial interview with a recruiter to discuss your background and fit for the company.
  2. Technical Interview: The most important stage, where your technical skills and knowledge are tested.
  3. Final Interview: An interview with the CEO or senior management to assess your overall fit for the company.
- **Importance:** The technical interview is crucial for securing a remote job. This is where your friend's support will be most valuable.

🚀 How It Works

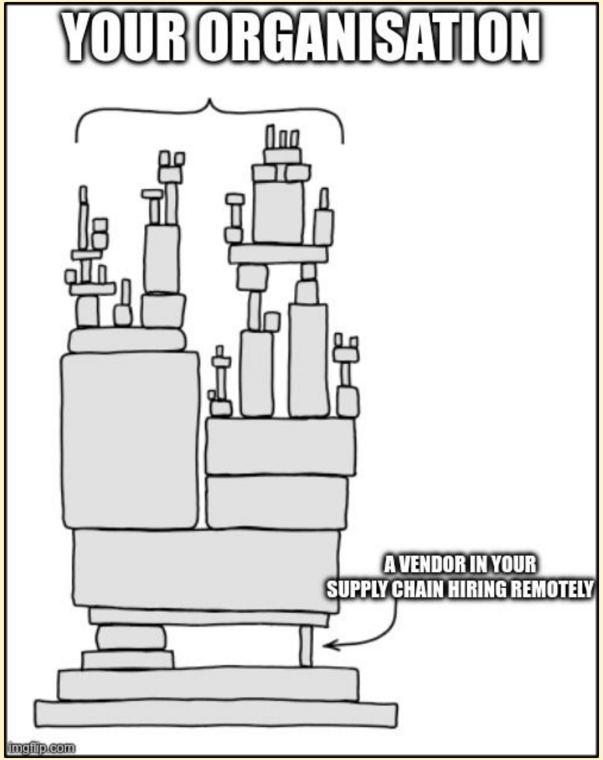
1. **Interview Scheduling:** My friend will schedule the interviews and inform you of the date and time.
2. **Preparation:** Before the interview, my friend will provide you with all the necessary technical details and background information.
3. **Interview Day:** On the day of the interview, my friend will use AnyDesk to access your computer and provide real-time support by typing answers to the interview questions in a text file on your screen.
4. **Answering Questions:** You simply read the answers provided by my friend and communicate them effectively using your strong English skills.
5. **Post-Interview:** If you pass the interview and secure the job, you will attend team meetings, while my friend handles all the technical work.

If this opportunity sounds interesting to you, please let me know. We can discuss more details and answer any questions you might have. Thank you for considering this unique and rewarding opportunity.

[11] Jasper Sleet: North Korean remote IT workers' evolving tactics to infiltrate organisations https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/

Threat

- Intellectual property theft
- Extortion
- Supply chain poisoning



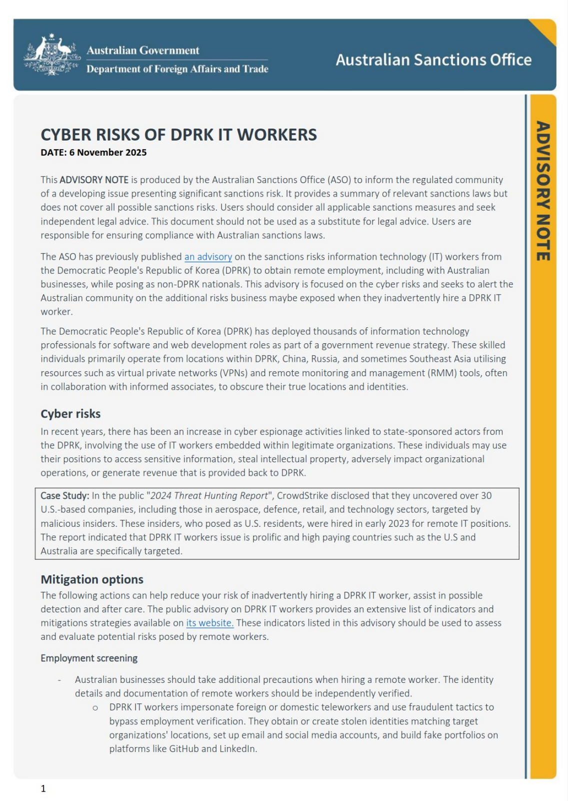
Impact

- Financial Loss

- **Bonus:** Fines for organisations violating sanctions [12]
    - For Individuals : 825,000
    - For Body corporate : 3 Million
        - Or 3X time value of the transaction (Which ever is greater !)

[12] Department of Foreign Affairs and Trade (DFAT) Advisory note on DPRK https://www.dfat.gov.au/international-relations/security/sanctions/guidance/advisory-democratic-peoples-republic-korea-dprk-information-technology-it-workers

ASO ADVISORY



Australian Government
Department of Foreign Affairs and Trade

Australian Sanctions Office

ADVISORY NOTE

CYBER RISKS OF DPRK IT WORKERS

DATE: 6 November 2025

This **ADVISORY NOTE** is produced by the Australian Sanctions Office (ASO) to inform the regulated community of a developing issue presenting significant sanctions risk. It provides a summary of relevant sanctions laws but does not cover all possible sanctions risks. Users should consider all applicable sanctions measures and seek independent legal advice. This document should not be used as a substitute for legal advice. Users are responsible for ensuring compliance with Australian sanctions laws.

The ASO has previously published an advisory on the sanctions risks information technology (IT) workers from the Democratic People's Republic of Korea (DPRK) to obtain remote employment, including with Australian businesses, while posing as non-DPRK nationals. This advisory is focused on the cyber risks and seeks to alert the Australian community on the additional risks business maybe exposed when they inadvertently hire a DPRK IT worker.

The Democratic People's Republic of Korea (DPRK) has deployed thousands of information technology professionals for software and web development roles as part of a government revenue strategy. These skilled individuals primarily operate from locations within DPRK, China, Russia, and sometimes Southeast Asia utilising resources such as virtual private networks (VPNs) and remote monitoring and management (RMM) tools, often in collaboration with informed associates, to obscure their true locations and identities.

Cyber risks

In recent years, there has been an increase in cyber espionage activities linked to state-sponsored actors from the DPRK, involving the use of IT workers embedded within legitimate organizations. These individuals may use their positions to access sensitive information, steal intellectual property, adversely impact organizational operations, or generate revenue that is provided back to DPRK.

Case Study: In the public "*2024 Threat Hunting Report*", CrowdStrike disclosed that they uncovered over 30 U.S.-based companies, including those in aerospace, defence, retail, and technology sectors, targeted by malicious insiders. These insiders, who posed as U.S. residents, were hired in early 2023 for remote IT positions. The report indicated that DPRK IT workers issue is prolific and high paying countries such as the U.S and Australia are specifically targeted.

Mitigation options

The following actions can help reduce your risk of inadvertently hiring a DPRK IT worker, assist in possible detection and after care. The public advisory on DPRK IT workers provides an extensive list of indicators and mitigations strategies available on its website. These indicators listed in this advisory should be used to assess and evaluate potential risks posed by remote workers.

Employment screening

- Australian businesses should take additional precautions when hiring a remote worker. The identity details and documentation of remote workers should be independently verified.
    - DPRK IT workers impersonate foreign or domestic teleworkers and use fraudulent tactics to bypass employment verification. They obtain or create stolen identities matching target organizations' locations, set up email and social media accounts, and build fake portfolios on platforms like GitHub and LinkedIn.

1

[13] Australian Sanctions Office https://www.dfat.gov.au/sites/default/files/advisory-note-cyber-risks-dprk-it-workers.pdf

Stages of the Hiring Process

Act 1

Application

Interview

Act 2

Verification

Offer

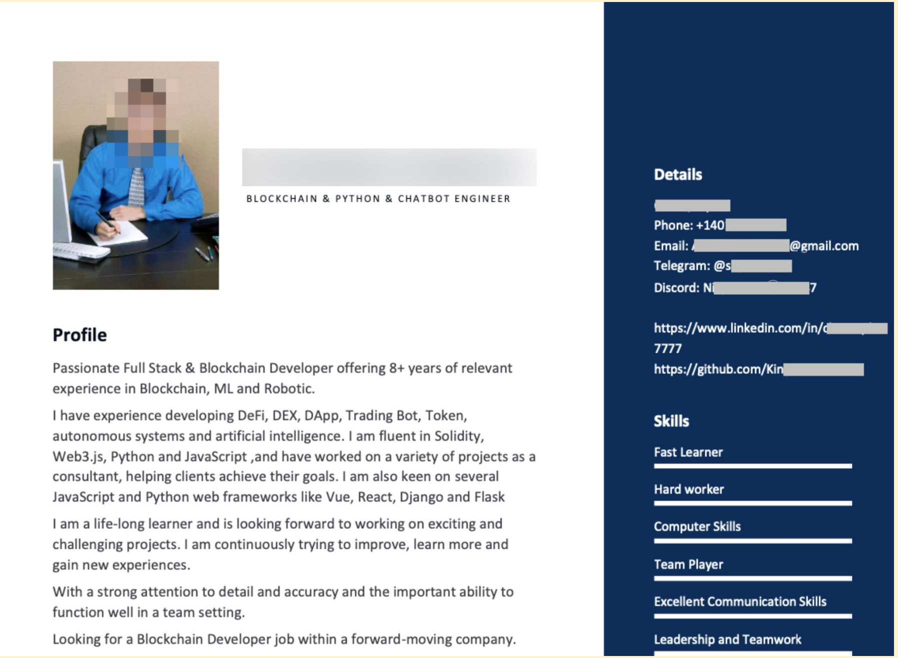
Act 3

Onboarding

Act 1 : The Pledge

“ The magician shows you something ordinary : a deck of cards, a bird, or a man.”

Quote is from the movie “The Prestige”



[redacted]

BLOCKCHAIN & PYTHON & CHATBOT ENGINEER

Profile

Passionate Full Stack & Blockchain Developer offering 8+ years of relevant experience in Blockchain, ML and Robotic.

I have experience developing DeFi, DEX, DApp, Trading Bot, Token, autonomous systems and artificial intelligence. I am fluent in Solidity, Web3.js, Python and JavaScript ,and have worked on a variety of projects as a consultant, helping clients achieve their goals. I am also keen on several JavaScript and Python web frameworks like Vue, React, Django and Flask

I am a life-long learner and is looking forward to working on exciting and challenging projects. I am continuously trying to improve, learn more and gain new experiences.

With a strong attention to detail and accuracy and the important ability to function well in a team setting.

Looking for a Blockchain Developer job within a forward-moving company.

Details

[redacted]
Phone: +140[redacted]
Email: [redacted]@gmail.com
Telegram: @s[redacted]
Discord: Ni[redacted]7

https://www.linkedin.com/in/d[redacted]
7777
https://github.com/Kin[redacted]

Skills

Fast Learner

Hard worker

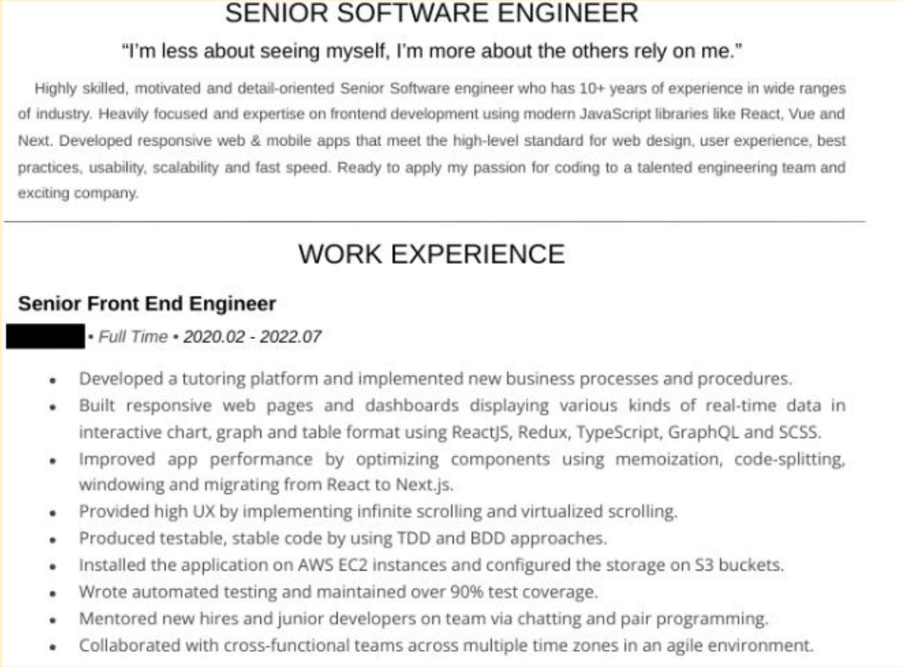
Computer Skills

Team Player

Excellent Communication Skills

Leadership and Teamwork

Example 1



SENIOR SOFTWARE ENGINEER

"I'm less about seeing myself, I'm more about the others rely on me."

Highly skilled, motivated and detail-oriented Senior Software engineer who has 10+ years of experience in wide ranges of industry. Heavily focused and expertise on frontend development using modern JavaScript libraries like React, Vue and Next. Developed responsive web & mobile apps that meet the high-level standard for web design, user experience, best practices, usability, scalability and fast speed. Ready to apply my passion for coding to a talented engineering team and exciting company.

WORK EXPERIENCE

Senior Front End Engineer

[redacted] • *Full Time • 2020.02 - 2022.07*

- Developed a tutoring platform and implemented new business processes and procedures.
- Built responsive web pages and dashboards displaying various kinds of real-time data in interactive chart, graph and table format using ReactJS, Redux, TypeScript, GraphQL and SCSS.
- Improved app performance by optimizing components using memoization, code-splitting, windowing and migrating from React to Next.js.
- Provided high UX by implementing infinite scrolling and virtualized scrolling.
- Produced testable, stable code by using TDD and BDD approaches.
- Installed the application on AWS EC2 instances and configured the storage on S3 buckets.
- Wrote automated testing and maintained over 90% test coverage.
- Mentored new hires and junior developers on team via chatting and pair programming.
- Collaborated with cross-functional teams across multiple time zones in an agile environment.

Example 2

[14]Source of Example 1 Resume : https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/
[15] Source of Example 2 Resume : https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat

DPRK IT Worker Resume

- Resume may reflect the work experiences of stolen identities [9]

- Extensive experience on Web and blockchain technologies

- Use of disposable email[9]

Resume -Detection

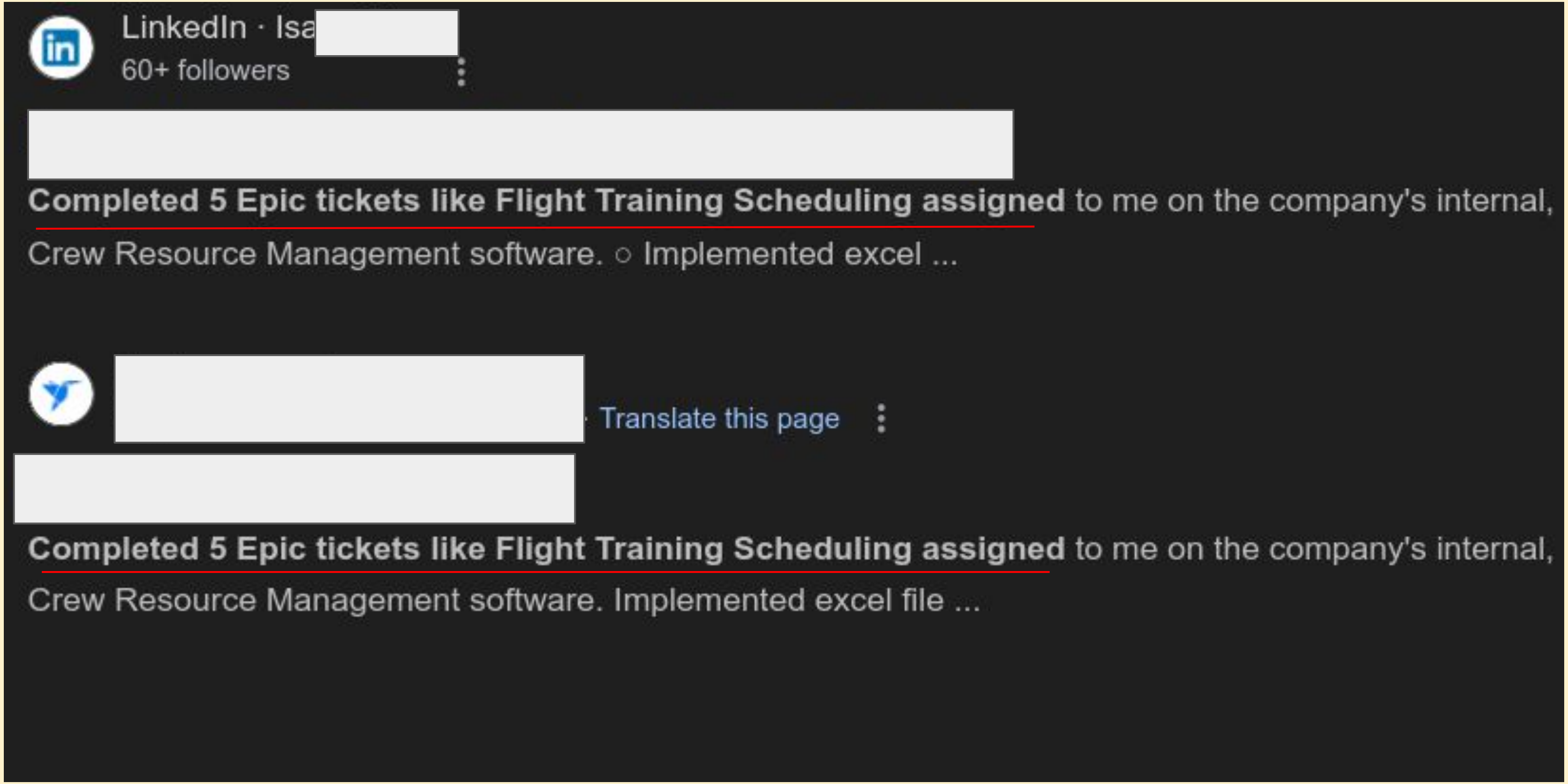
- Check for online presence of the candidate
  - LinkedIn (Account creation date)
    - All experiences will be remote !
    - Do not trust LinkedIn verification !

- Check education experience offered by the university

Resume -Detection

- Identify a unique accomplishment and perform a search on Google
  E.g. “Completed 5 Epic tickets like Flight Training Scheduling assigned to me”

Resume - Detection Example



LinkedIn · Isa[redacted]

60+ followers

[redacted]

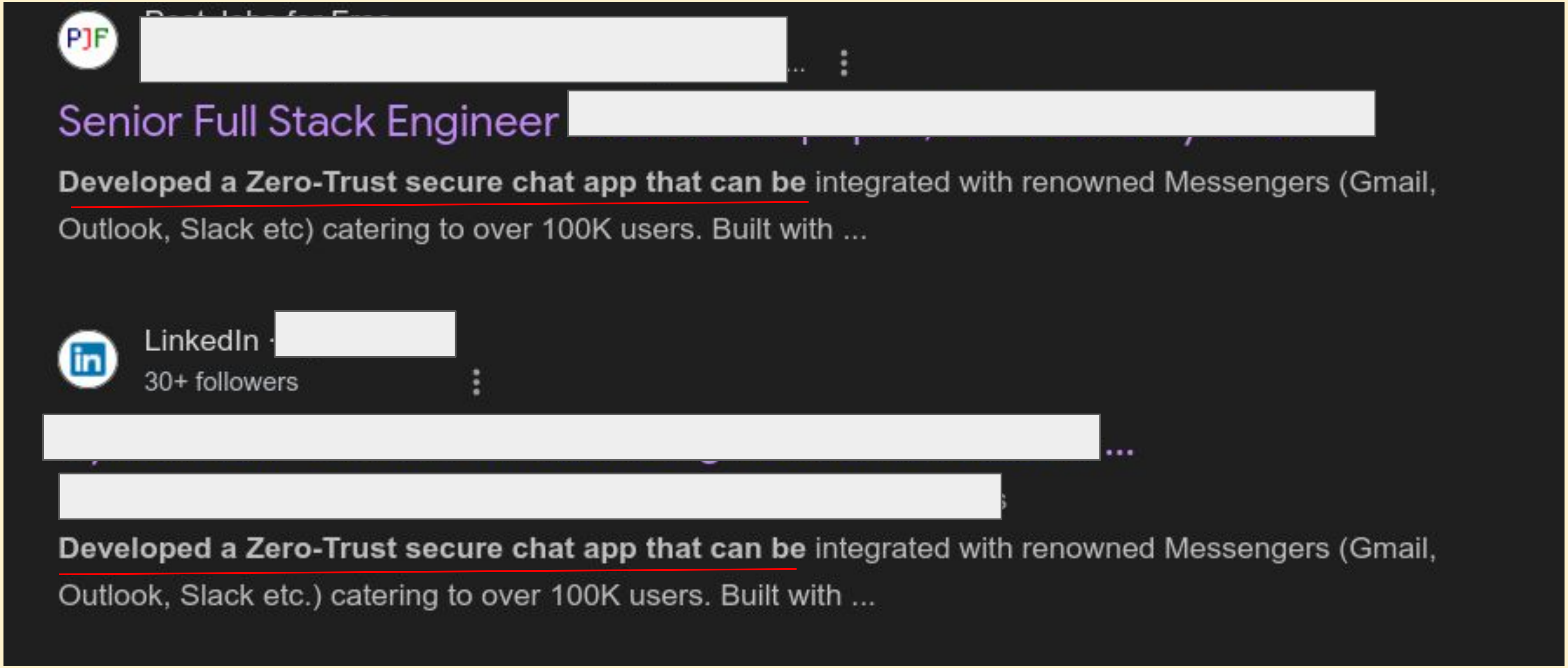
Completed 5 Epic tickets like Flight Training Scheduling assigned to me on the company's internal, Crew Resource Management software. ○ Implemented excel ...

[redacted] · Translate this page

[redacted]

Completed 5 Epic tickets like Flight Training Scheduling assigned to me on the company's internal, Crew Resource Management software. Implemented excel file ...

Resume - Detection Example



[redacted] ...

Senior Full Stack Engineer [redacted]

Developed a Zero-Trust secure chat app that can be integrated with renowned Messengers (Gmail, Outlook, Slack etc) catering to over 100K users. Built with ...

LinkedIn · [redacted]

30+ followers

[redacted] ...

Developed a Zero-Trust secure chat app that can be integrated with renowned Messengers (Gmail, Outlook, Slack etc.) catering to over 100K users. Built with ...

Interviews with IT Worker

- Two categories
  - Interview with a proxy worker
  - Interview with an IT worker

- Interviewee may use AI to mimic purchased/stolen/synthetic identity

Interviews with IT Worker

- Record the interview
  - Consult with your legal department

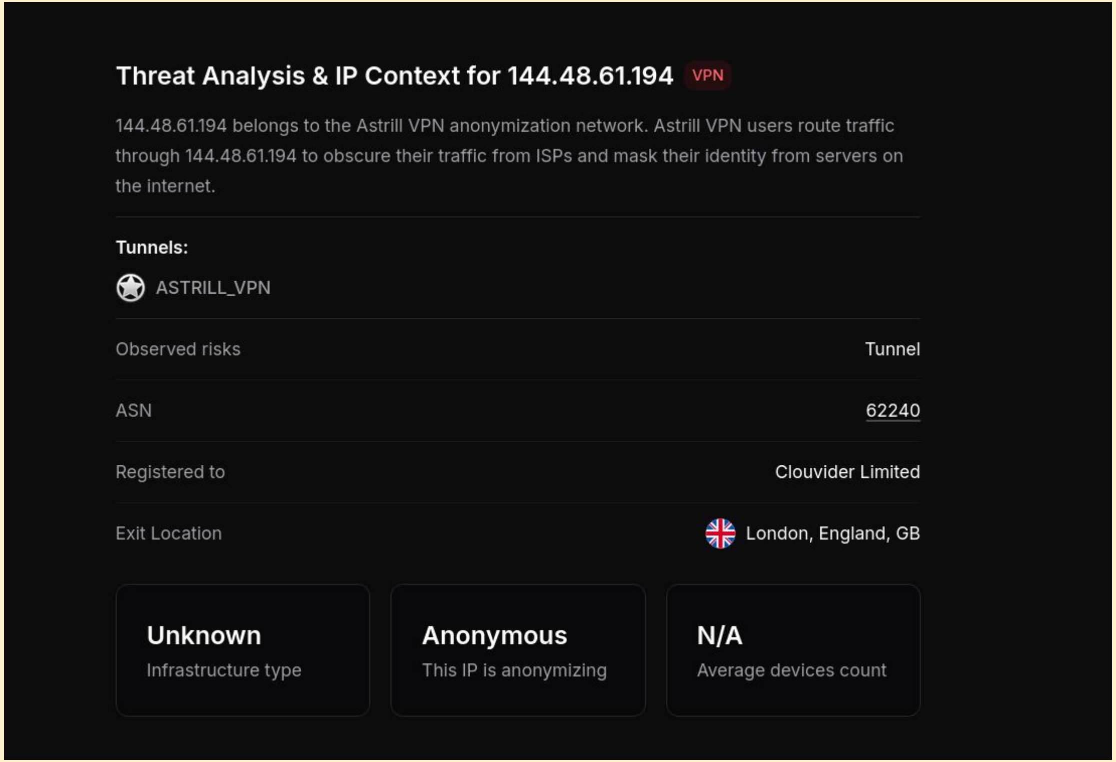
- Gather IP logs of video calls and check for VPN usage
  - Microsoft Teams
  - Google

Interview - VPN Detection

- IT Workers use VPN to hide their location or mimic their country
  - You can use spur[.]us [16] to determine VPN usage
  - https://spur[.]us/context/REPLACE_IP_ADDR

[16] Astrill VPN and DPRK Remote Worker Fraud https://spur.us/astrill-vpn-and-remote-worker-fraud/

Interview - VPN Detection



Threat Analysis & IP Context for 144.48.61.194 VPN

144.48.61.194 belongs to the Astrill VPN anonymization network. Astrill VPN users route traffic through 144.48.61.194 to obscure their traffic from ISPs and mask their identity from servers on the internet.

Tunnels:

ASTRILL_VPN

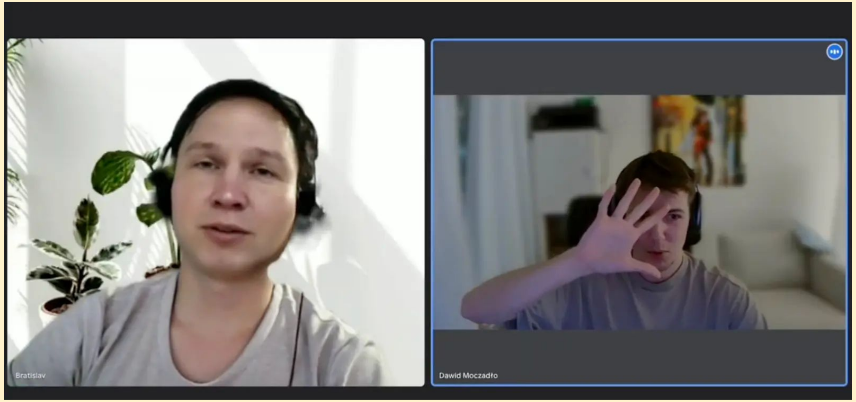
Observed risks	Tunnel
ASN	62240
Registered to	Clouvider Limited
Exit Location	London, England, GB

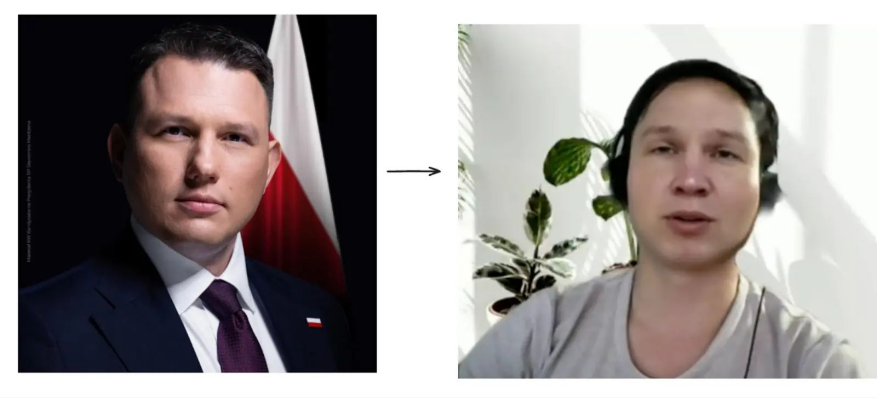
Unknown
Infrastructure type

Anonymous
This IP is anonymizing

N/A
Average devices count

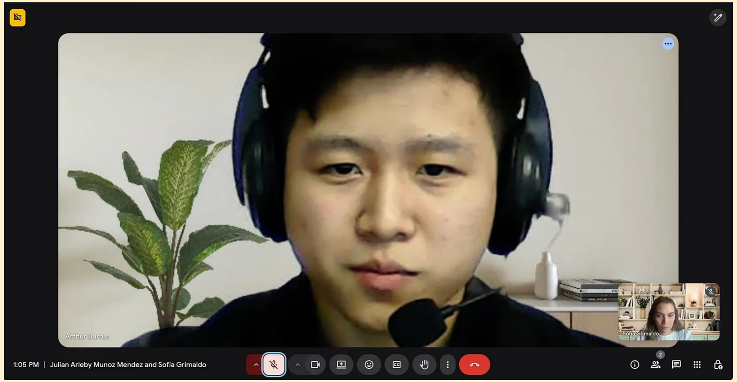
Interviews AI Usage - Examples



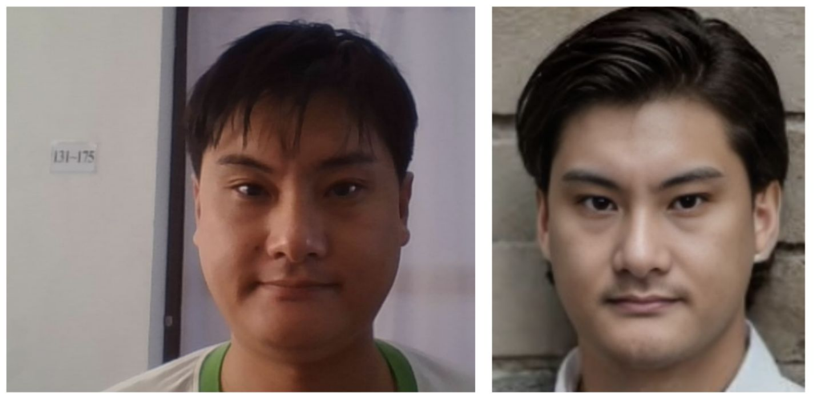


[17]Fake Engineer - Advanced Deepfake Fraud and How to Detect It https://blog.vidocsecurity.com/blog/deepfake-fraud-2

Interviews AI Usage - Examples

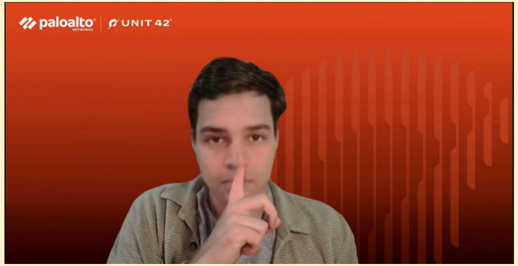


[18]Interview with the Chollima III
https://quetzal.bitso.com/p/interview-with-the-chollima-iii

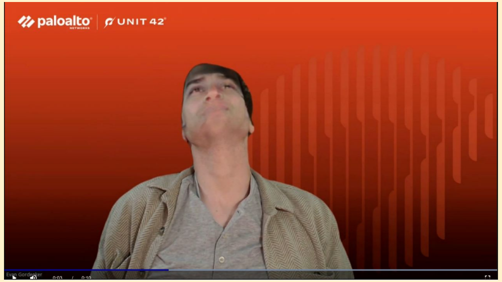


[19]False Face: Unit 42 Demonstrates the Alarming Ease of Synthetic Identity Creation
https://unit42.paloaltonetworks.com/north-korean-synthetic-identity-creation/

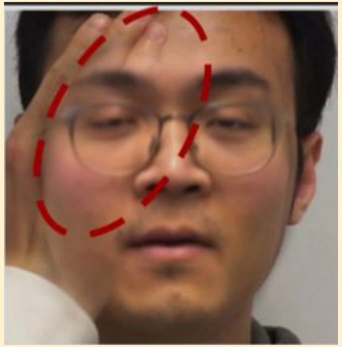
Interviews AI Detection



Nose Show [19]



Sky or Ground [19]



Vanishing Object [20]

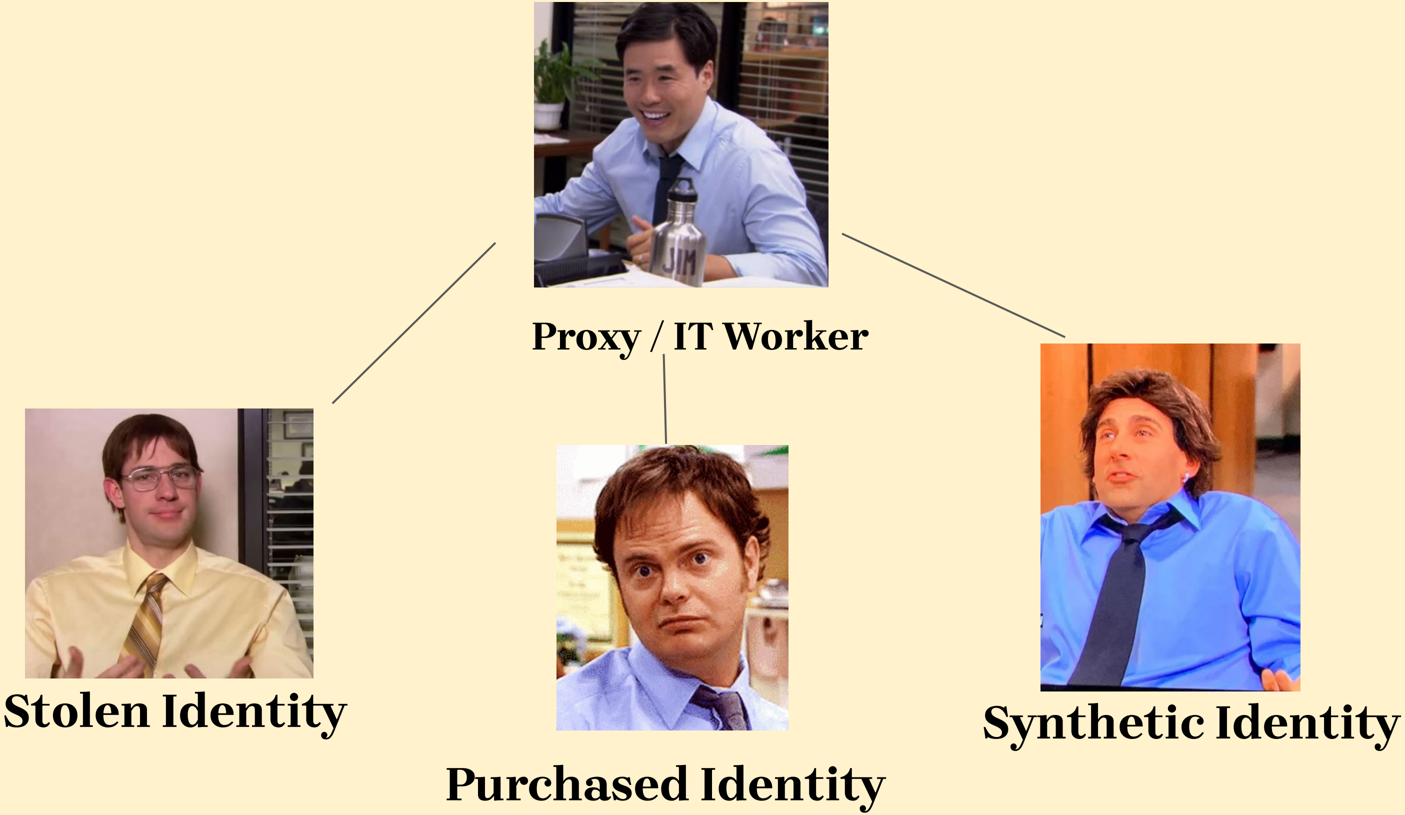
[20] Gotcha: Real-Time Video Deepfake Detection via Challenge-Responsehttps://arxiv.org/html/2210.06186v4

Act 2 : The Turn

“ The magician takes the ordinary something and makes it do something extraordinary. Now you're looking for the secret... but you won't find it ”.

Quote is from the movie “The Prestige”

Identity theft is not a joke, Jim!



Proxy / IT Worker

Stolen Identity

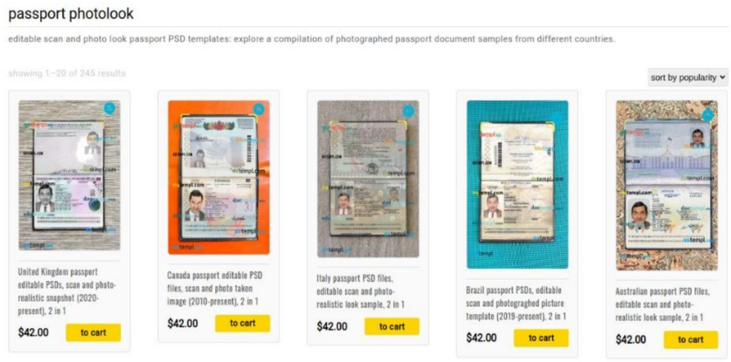
Purchased Identity

Synthetic Identity

[9] The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities https://msmt.info/Publications/detail/MSMT%20Report/4221 [Pages 52-90]

Identity theft is not a joke, Jim!

Figure 21: Example of Synthetic Document Services



passport photolook

editable scan and photo look passport PSD templates: explore a compilation of photographed passport document samples from different countries.

showing 1–20 of 245 results

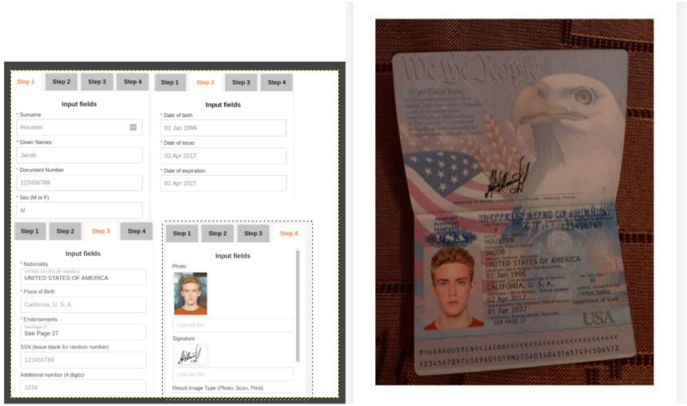
United Kingdom passport editable PSDs, scan and photo-realistic snapshot (2020-present), 2 in 1 — $42.00

Canada passport editable PSD files, scan and photo taken image (2010-present), 2 in 1 — $42.00

Italy passport PSD files, editable scan and photo-realistic look sample, 2 in 1 — $42.00

Brazil passport PSDs, editable scan and photograghed picture template (2019-present), 2 in 1 — $42.00

Australian passport PSD files, editable scan and photo-realistic look sample, 2 in 1 — $42.00



Step 1 — Input fields

- * Surname: Housten
- * Given Names: Jacob
- * Document Number: 123456789
- * Sex (M or F): M

Step 2 — Input fields

- * Date of birth: 01 Jan 1996
- * Date of issue: 02 Apr 2017
- * Date of expiration: 01 Apr 2027

Step 3 — Input fields

- * Nationality: UNITED STATES OF AMERICA
- * Place of Birth: California, U. S. A.
- * Endorsements: See Page 27
- SSN (leave blank for random number): 123456789
- Additional number (4 digits): 1234

Step 4 — Input fields

- Photo: Upload file
- Signature: Upload file
- Result image Type (Photo, Scan, Print)

Source: Information provided for the MSMT report by a private sector partner

[9] The DPRK’s Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities https://msmt.info/Publications/detail/MSMT%20Report/4221 [Pages 52-90]

ID Verification - Detection

- Request passports as ID Proof
  - Consult with Legal about data collection
  - Do not rely on local identifications
  - Use KYE platforms (e.g. Persona) to verify

ID Verification - Detection

- Ask for address proof from an institution
  - That you can independently verify
  - No utility bills, please !
- Correlate person's age and compare with Resume
  - Look for discrepancies (e.g. Graduation date)

IT Worker References

- Known to use other IT Workers as references [9]
- Chances of using shell companies that do no exist
- Usage of paid proxies for references

[9] The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities https://msmt.info/Publications/detail/MSMT%20Report/4221 [Pages 52-90]

References - Detection

- Find the online presence of references and the organisation
  - Independently verify the reference and the interviewee, if possible

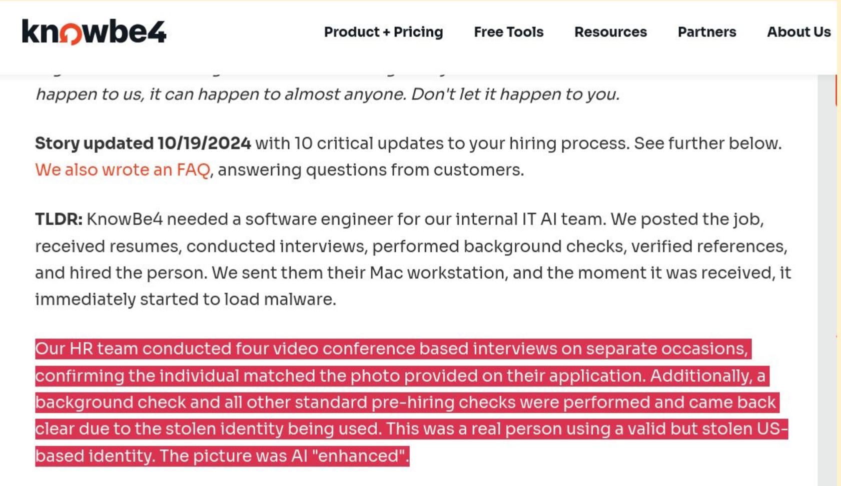
- Check the usage of VoIP Phone numbers
  - Use Twilio API check the type [22]
  - https://www.ipqualityscore[.]com/phone-number-validator

[21] How to filter out VoIP numbers https://www.twilio.com/en-us/blog/filter-voip-before-otp-verification

References - Detection

- Ask the reference about their tenure at the organisation - contact them via phone

- Do not rely on email based reference checks
  - ○ Anyone can buy a domain and set up a company !



happen to us, it can happen to almost anyone. Don't let it happen to you.

Story updated 10/19/2024 with 10 critical updates to your hiring process. See further below. We also wrote an FAQ, answering questions from customers.

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".

[22] How a North Korean Fake IT Worker Tried to Infiltrate Us https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

Act 3 : The Prestige

“Because making something disappear isn't enough”

Quote is from the movie “The Prestige”

Onboarding - Detection

- IT Worker may request to ship Laptop or hardware to an address not related to them
  - Verify the address proof document

- IT Workers may request payment information sent to a bank account controlled by a facilitator

Onboarding - Detection

- IT Workers may share their calendar with a handler
- IT Workers may sign up to services with your corporate email

Onboarding - Detection

- IT Workers may attempt to install VPN on your corporate device
  - E.g. Astrill VPN (Most Common)
  - <u>Do not allow BYOD</u> (Bring Your Own Disaster !)

- IT Workers may attempt to install RMM tools(remote monitoring and management)

Onboarding - Detection RMM

- Use LORMM project
  - Lolrmm[.]io
    - Audit/Block unapproved RMM usage
    - Monitor the Egress traffic

- Most Commonly used RMMs
  - AnyDesk
  - Chrome Remote Desktop
  - Parsec

Onboarding - Behaviour Detection

- Working unusual hours
  - Hours that do not align with location
  - Use git log (Time analysis)

- Not turning on Webcam during meetings
  - Signs that may indicate that the device reached a Laptop Farm

Onboarding - Activity Detection

- IT Workers may have high/unprivileged access
  - Use Canary tokens [23]
    - Check out canarytokens[.]org

[23] CanaryTokens https://help.canary.tools/hc/en-gb/articles/4701687447325-What-are-Canarytokens

What to do if you detect DPRK IT Worker ?

- Ensure that the alleged employee is not aware of this !
  - Chances that this can end badly

- Start IR
  - Consult with Legal
  - Revoke all privileged access
  - Do not Pay - Contact ASO

YOU ARE DPRK, YOU ARE FIRED
I WILL LEAK YOUR INFO, IF YOU DONT PAY
imgflip.com

Bibliography

1. The Bar Fight Risk Taxonomy : https://cje.io/2021/06/27/the-bar-fight-risk-taxonomy/
2. North Korea Sanctions Program : https://ofac.treasury.gov/media/9221/download?inline
3. GDP Per Capita Facts https://www.cia.gov/the-world-factbook/countries/korea-north/
4. DPRK Spending source: https://cove.army.gov.au/kyr/north-korea
5. 3 North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyber-attacks and Financial Crimes Across the Glob https://www.justice.gov/usao-cdca/pr/3-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyber-attacks-and
6. Bangladesh Bank Heist https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/
7. North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyberattacks and Intrusions https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
8. Two North Korean Nationals and Three Facilitators Indicted for Multi-Year Fraudulent Remote Information Technology Worker Scheme that Generated Revenue for the Democratic People's Republic of Korea https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote
9. The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities https://msmt.info/Publications/detail/MSMT%20Report/4221 [Pages 52-90]
10. Advisory on North Korean IT Workers https://assets.publishing.service.gov.uk/media/66e2ec410d913026165c3d91/OFSI_Advisory_on_North_Korean_IT_Workers.pdf
11. Jasper Sleet: North Korean remote IT workers' evolving tactics to infiltrate organisations https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/
12. Department of Foreign Affairs and Trade (DFAT) Advisory note on DPRK https://www.dfat.gov.au/international-relations/security/sanctions/guidance/advisory-democratic-peoples-republic-korea-dprk-information-technology-it-workers
13. Australian Sanctions Office Advisory note https://www.dfat.gov.au/sites/default/files/advisory-note-cyber-risks-dprk-it-workers.pdf
14. Source of Example 1 Resume : https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/
15. Source of Example 2 Resume : https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat
16. Astrill VPN and DPRK Remote Worker Fraud https://spur.us/astrill-vpn-and-remote-worker-fraud/
17. Fake Engineer - Advanced Deepfake Fraud and How to Detect It https://blog.vidocsecurity.com/blog/deepfake-fraud-2
18. Interview with the Chollima III https://quetzal.bitso.com/p/interview-with-the-chollima-iii
19. False Face: Unit 42 Demonstrates the Alarming Ease of Synthetic Identity Creation https://unit42.paloaltonetworks.com/north-korean-synthetic-identity-creation/
20. Investigation: Probable DPRK Online Personas Used To Fraudulently Obtain Remote Employment at U.S. Companies https://6068438.fs1.hubspotusercontent-na1.net/hubfs/6068438/dprk-it-worker-scam.pdf
21. How to filter out VoIP numbers https://www.twilio.com/en-us/blog/filter-voip-before-otp-verification
22. How a North Korean Fake IT Worker Tried to Infiltrate Us https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us
23. CanaryTokens https://help.canary.tools/hc/en-gb/articles/4701687447325-What-are-Canarytokens
24. From Laptops to Laundromats https://dti.domaintools.com/from-laptops-to-laundromats-how-dprk-it-workers-infiltrated-the-global-remote-economy/
25. Unmasking DPRK IT Workers: Email Address Patterns as Hiring Red Flags https://theravenfile.com/2025/08/19/unmasking-dprk-it-workers-email-address-patterns-as-hiring-red-flags/
26. The Lazarus Heist: From Hollywood to High Finance: Inside North Korea's Global Cyberwar- Geoff White
27. The Great Successor: The Divinely Perfect Destiny of Brilliant Comrade Kim Jong-un
28. Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the A.Q. Khan Network

That's all Folks!