Staying a Step Ahead: Mitigating the DPRK IT Worker Threat

By Mandiant

Published: 2024-09-23 · Archived: 2026-04-05 13:33:41 UTC

Written by: Codi Starks, Michael Barnhart, Taylor Long, Mike Lombardi, Joseph Pisano, Alice Revelli

---

Strategic Overview of IT Workers

Since 2022, Mandiant has tracked and reported on IT workers operating on behalf of the Democratic People's Republic of Korea (DPRK). These workers pose as non-North Korean nationals to gain employment with organizations across a wide range of industries in order to generate revenue for the North Korean regime, particularly to evade sanctions and fund its weapons of mass destruction (WMD) and ballistic missile programs. A U.S. government advisory in 2022 noted that these workers have also leveraged privileged access obtained through their employment in order to enable malicious cyber intrusions, an observation corroborated by Mandiant and other organizations.

IT workers employ various methods for evading detection. We have observed the operators leverage front companies to disguise their true identities; additionally, U.S. government indictments show that non-North Korean individuals, known as “facilitators,” play a crucial role in enabling these IT workers in their efforts to seek and maintain employment. These individuals provide essential services that include, but are not limited to, laundering money and/or cryptocurrency, receiving and hosting company laptops at their residences, using stolen identities for employment verification, and accessing international financial systems.

This report aims to increase awareness of the DPRK's efforts to obtain employment as IT workers and shed light on their operational tactics for obtaining employment and maintaining access to corporate systems. Understanding these methods can help organizations better detect these sorts of suspicious behaviors earlier in the hiring process. In this blog post we’ve included a sampling of the types of behaviors identified during our incident response engagements, and strategies for the detection and disruption of DPRK IT worker activity.

UNC5267

Mandiant tracks IT worker operations we have identified in various environments as UNC5267. UNC5267 remains highly active in the present day, posing an ongoing threat. Some sources suggest that the origins of these operations can be traced back to 2018. Importantly, UNC5267 is not a traditional, centralized threat group. IT workers consist of individuals sent by the North Korean government to live primarily in China and Russia, with smaller numbers in Africa and Southeast Asia. Their mission is to secure lucrative jobs within Western companies, especially those in the U.S. tech sector.

UNC5267 gains initial access through the use of stolen identities to apply for various positions or are brought in as a contractor. UNC5267 operators have primarily applied for positions that offer 100% remote work. Mandiant

observed the operators engaging in work of varying complexity and difficulty spanning disparate fields and sectors. It is not uncommon for a DPRK IT worker to be working multiple jobs at once, pulling in multiple salaries on a monthly basis. One American facilitator working with the IT workers compromised more than 60 identities of U.S. persons, impacted more than 300 U.S. companies, and resulted in at least $6.8 million of revenue to be generated for the overseas IT workers from in or around October 2020 until October 2023.

UNC5267's objectives include:

- Financial gain through illicit salary withdrawals from compromised companies
- Maintaining long-term access to victim networks for potential future financial exploitation
- Potential use of access for espionage or disruptive activity (though this hasn't been definitively observed)

Incident Response Observations

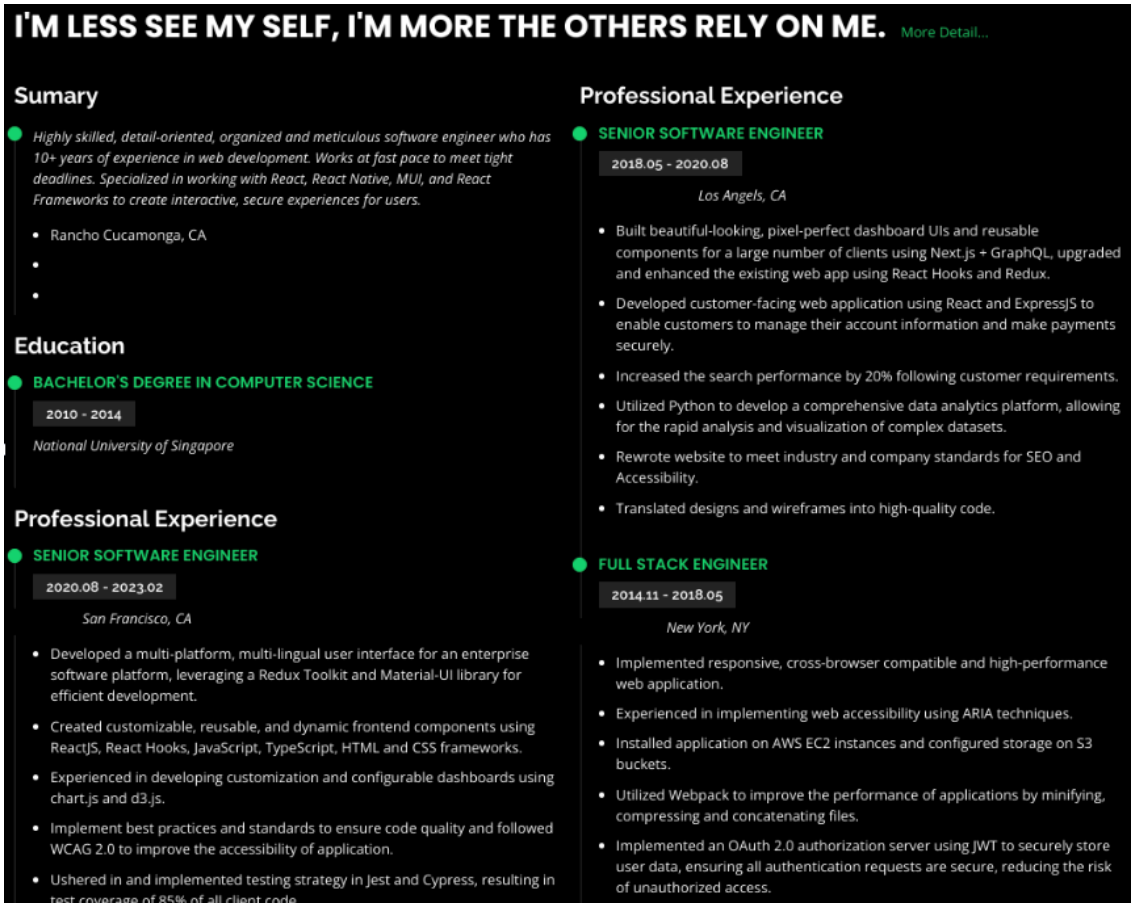
Mandiant's incident response engagements to date have primarily observed DPRK IT workers functioning within the scope of their job responsibilities. However, the remote workers often gain elevated access to modify code and administer network systems. This heightened level of access granted to fraudulent employees presents a significant security risk.

Mandiant has identified a substantial number of DPRK IT worker resumes used to apply for remote positions. In one resume from a suspected IT worker, the email address—previously observed in IT worker-related activities—was also linked to a fabricated software engineer profile hosted on Netlify, a platform often used for quickly creating and deploying websites. The profile claimed proficiency in multiple programming languages and included fake testimonials with stolen images from high-ranking professionals, likely stolen from CEOs, directors, and other software engineers' LinkedIn profiles.

Figure 1: Observed image of threat actor resume (likely altered)

Within the suspected DPRK IT worker's Netlify page, we discovered a resume accompanied by a link to another resume hosted on Google Docs, presenting a different identity. The linked resume featured a different name, phone number, and email address compared to the information on the Netlify page. Further discrepancies between the Netlify page and the linked resume included differing universities and years of attendance, as well as

variations in past job titles and company work history. However, both of the resumes included a slight variation of the phrase “I'm less about seeing myself, I'm more about the others rely on me.”



I'M LESS SEE MY SELF, I'M MORE THE OTHERS RELY ON ME. More Detail...

Sumary

Highly skilled, detail-oriented, organized and meticulous software engineer who has 10+ years of experience in web development. Works at fast pace to meet tight deadlines. Specialized in working with React, React Native, MUI, and React Frameworks to create interactive, secure experiences for users.

- Rancho Cucamonga, CA

Education

BACHELOR'S DEGREE IN COMPUTER SCIENCE

2010 - 2014

National University of Singapore

Professional Experience

SENIOR SOFTWARE ENGINEER

2020.08 - 2023.02

San Francisco, CA

- Developed a multi-platform, multi-lingual user interface for an enterprise software platform, leveraging a Redux Toolkit and Material-UI library for efficient development.
- Created customizable, reusable, and dynamic frontend components using ReactJS, React Hooks, JavaScript, TypeScript, HTML and CSS frameworks.
- Experienced in developing customization and configurable dashboards using chart.js and d3.js.
- Implement best practices and standards to ensure code quality and followed WCAG 2.0 to improve the accessibility of application.
- Ushered in and implemented testing strategy in Jest and Cypress, resulting in test coverage of 85% of all client code

Professional Experience

SENIOR SOFTWARE ENGINEER

2018.05 - 2020.08

Los Angels, CA

- Built beautiful-looking, pixel-perfect dashboard UIs and reusable components for a large number of clients using Next.js + GraphQL, upgraded and enhanced the existing web app using React Hooks and Redux.
- Developed customer-facing web application using React and ExpressJS to enable customers to manage their account information and make payments securely.
- Increased the search performance by 20% following customer requirements.
- Utilized Python to develop a comprehensive data analytics platform, allowing for the rapid analysis and visualization of complex datasets.
- Rewrote website to meet industry and company standards for SEO and Accessibility.
- Translated designs and wireframes into high-quality code.

FULL STACK ENGINEER

2014.11 - 2018.05

New York, NY

- Implemented responsive, cross-browser compatible and high-performance web application.
- Experienced in implementing web accessibility using ARIA techniques.
- Installed application on AWS EC2 instances and configured storage on S3 buckets.
- Utilized Webpack to improve the performance of applications by minifying, compressing and concatenating files.
- Implemented an OAuth 2.0 authorization server using JWT to securely store user data, ensuring all authentication requests are secure, reducing the risk of unauthorized access.

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.

These two resumes are a small sampling of the total amount of fraudulent resumes identified by Mandiant. However, the resumes provide evidence of the DPRK IT workers utilizing multiple personas in attempts to gain employment across multiple organizations.

A recurring characteristic of resumes utilized by UNC5267 is the use of addresses based in the United States coupled with education credentials from universities outside of North America, frequently in countries such as Singapore, Japan, or Hong Kong. While possible, Mandiant noted that the acceptance rate for foreign students at many of the universities is low. This discrepancy may serve to hinder potential North American employers from verifying or contacting these overseas institutions regarding the applicant. Mandiant has also observed that the universities listed on the background check may not align with the candidate's education background stated in their resume, including time of enrollment and completed degree programs. Furthermore, UNC5267's resumes often exhibit significant overlap with publicly available resumes or are heavily reused across multiple UNC5267 personas.

To accomplish their duties, UNC5267 often remotely accesses victim company laptops situated within a laptop farm. These laptop farms are typically staffed with a single facilitator who is paid monthly to host numerous devices in one location. Mandiant has identified evidence that these laptops are often connected to an IP-based Keyboard Video Mouse (KVM) device, although a recurring theme across these incidents is the installation of multiple remote management tools on victim corporate laptops immediately following shipment to the farm. These indicate that the individual is connecting to their corporate system remotely via the internet, and may not be geographically located in the city, state, or even country in which they report to reside. The following is a list of remote administration tools identified during Mandiant engagements:

- GoToRemote / LogMeIn
- GoToMeeting
- Chrome Remote Desktop
- AnyDesk
- TeamViewer
- RustDesk

Connections to these remote management solutions primarily originated from IP addresses associated with Astrill VPN, likely originating from China or North Korea. Lastly, feedback from team members and managers who spoke with Mandiant during investigations consistently highlighted behavior patterns, such as reluctance to engage in video communication and below-average work quality exhibited by the DPRK IT worker remotely operating the laptops.

Another common characteristic identified across Mandiant's engagements was that DPRK IT workers typically claimed to live in one location, but requested laptop shipment to another location (laptop farm or outside enablement entity). We have observed the DPRK IT workers using the location associated with the stolen identity used for employment, including the stolen driver's license, which often doesn't match the location where the laptop is ultimately shipped and stored.

Detection Methods

Mandiant highlights a number of strategies that organizations can use to identify and hinder DPRK IT worker operations based on information from trusted sources and government advisories. Countering the threat posed by North Korean cyber actors requires a multifaceted approach that combines technical defenses, user awareness training, and proactive threat hunting. Key recommendations include:

Vetting of Job Candidates

- Requiring stringent background checks, including the collection of biometric information for comparison against known identities via specialized background checking services, may deter the use of forgeries.
- Implementing careful interview processes, such as requiring cameras to be used during interviews to ensure visual appearance matches online profiles, checking that the interviewee matches the provided identification, and asking questions to establish the consistency of a candidate's responses in line with their purported background.
    - U.S. government advisories and trusted third parties have additionally noted IT workers' reluctance to turn on cameras and their use of fake backgrounds during interviews.
- Training human resources departments to spot inconsistencies broadly and learn IT worker tactics, techniques, and procedures (TTPs).
- Monitoring for the use of artificial intelligence (AI) to modify employment profile pictures.
    - Mandiant has observed multiple instances in which DPRK IT workers utilized AI to modify profile pictures.
    - Impacted organizations have leveraged open-source tooling to determine if the image was created using AI.
- Require notarized proof of identity prior to employment.

Observations of Potential Technical Indicators

- Verify phone numbers to identify Voice over Internet Protocol (VoIP) phone numbers. The use of VoIP phone numbers is a common tactic used by UNC5267.
- Verify that the corporate laptop is shipped to and subsequently geolocated where the individual reports to reside during onboarding.
    - Mandiant has observed instances where the deployed corporate laptop was never geolocated in the location that the individual reported to reside.
- Monitor and restrict the use and installation of remote administration tools:

    - Prevent any remote connections to company-issued computers that could subsequently access the corporate network.
    - Monitor for uncommon remote admin tools.
    - Monitor for multiple remote admin tools installed on one system.
- Monitor for the use of VPN services to connect to corporate infrastructure. IP addresses associated with VPN services, such as Astrill VPN, should be further reviewed.
- Monitor for the use of “mouse jiggling” software.
    - Mandiant has observed instances of DPRK IT workers using the Caffeine mouse jiggling software to remain active across several laptops and profiles. This allows for ease of use at facilitator locations, where keeping laptops on and running are key and for the DPRK IT workers who often hold many jobs at once and need to appear online.
- Request verification of the laptop serial number at the time of IT onboarding. This information should be readily available for anyone with physical possession of their corporate device.
- Utilize a hardware based multi-factor for multi-factor authentication to enforce physical access to corporate devices.
- Monitor and restrict the use of IP-based KVM devices. IP-based KVMs are frequently utilized by DPRK IT workers to maintain persistent remote access to corporate devices.

Ongoing Mitigation Strategies

- Consider utilizing periodic mandatory spot checks where remote employees are required to go on camera.
- Offer continuous education for users and employees on current threats and trends, which is critical for identifying potentially malicious activity. Provide additional training on reporting suspicious activity.
- Collaborate with information-sharing communities and security vendors to stay abreast of the latest threats and mitigation strategies.
- Require the use of U.S. banks for financial transactions to hinder IT worker efforts, as the acquisition of U.S. bank accounts is more difficult and entails stricter identity verification than those in many other countries.

For Google SecOps Enterprise+ customers, the IOCs listed in this blog post are available for prioritization with Applied Threat Intelligence.

Mandiant also offers intelligence-led human-driven Custom Threat Hunt services to reveal ongoing or past threat actor activity in both cloud and on-premise environments. The service includes analysis tailored to the particulars of your tech stack and the threats targeting you. Learn more about Mandiant Custom Threat Hunt services.

Outlook and Implications

North Korea's IT workforce, despite operating under significant constraints, presents a persistent and escalating cyber threat. The dual motivations behind their activities—fulfilling state objectives and pursuing personal financial gains—make them particularly dangerous. Their technical proficiency, coupled with sophisticated evasion tactics, poses a formidable challenge, especially for HR and recruiting teams tasked with identifying potential threats during the hiring process.

Given their past successes and the DPRK regime's reliance on cyber operations for revenue and strategic goals, we anticipate a continued surge in sophisticated attacks and intrusions targeting businesses globally. The IT workers continue to be particularly impactful to Western organizations, with a growing number of European organizations targeted. These attacks can lead to data breaches, financial losses, intellectual property theft, and disruption of critical services.

The activities of North Korea's IT workforce underscore the need for sustained vigilance and a proactive cybersecurity posture. While the threat is complex, a combination of robust security measures, employee awareness, and collaborative efforts can significantly enhance an organization's resilience against these malicious actors. Additionally, leveraging advanced threat detection tools and maintaining robust incident response plans are crucial for minimizing the impact of potential breaches. Collaboration with industry peers and cybersecurity agencies to share threat intelligence can further strengthen defenses against this evolving threat.

Mandiant successfully operates in this effort by leveraging partnerships either publicly or privately with key organizations and victims alike. If your organization has been affected or you have information regarding DPRK cyber operations, we can help get the information to the people that need to be protected or informed. We are all in this together.

Network IOCs

Indicator	ASN	NetBlock	Service	Location
103.244.174.154	9541	Cybernet		(PK)
104.129.55.3	8100	QuadraNet		(US)
104.206.40.138	62904	Eonix Corporation	AstrillVPN	(US)
104.223.97.2	8100	QuadraNet		(US)
104.223.98.2	8100	QuadraNet		(US)

104.243.33.74	23470	ReliableSite.Net LLC		(US)
104.250.148.58	53850	GorillaServers	AstrillVPN	(US)
109.82.113.75	35819	Mobily		(SA)
113.227.237.46	4837	China Unicom		(CN)
119.155.190.202	56167	Ufone		(PK)
123.190.56.214	4837	China Unicom		(CN)
155.94.255.2	8100	QuadraNet		(US)
174.128.251.99	46844	Sharktech	AstrillVPN	(US)
18.144.99.240	16509	Amazon.com		(US)
184.12.141.109	5650	Frontier Communications		(US)
192.119.10.67	55081	24 Shells	AstrillVPN	(US)
192.119.11.250	55081	24 Shells	AstrillVPN	(US)
192.74.247.161	54600	Peg Tech	AstrillVPN	(US)
198.135.49.154	396073	Majestic Hosting Solutions, LLC	AstrillVPN	(US)
198.2.228.20	54600	Peg Tech	AstrillVPN	(US)

198.23.148.18	36352	ColoCrossing		(US)
199.115.99.34	46844	Sharktech	AstrillVPN	(US)
204.188.232.195	46844	Sharktech	AstrillVPN	(US)
207.126.89.11	6939	Hurricane Electric		(US)
208.68.173.244	29838	Atlantic Metro Communications		(US)
23.105.155.2	396362	Leaseweb New York		(US)
23.237.32.34	174	Fdcservers		(US)
3.15.4.158	16509	Amazon.com		(US)
37.19.199.133	212238	Datacamp Limited		(US)
37.19.221.228	212238	Datacamp Limited		(US)
37.43.225.43	35819	Mobily		(SA)
38.140.49.92	174	Cogent Communications	AstrillVPN	(US)
38.42.94.148	27611	Starry		(US)
42.84.228.232	4837	China Unicom		(CN)
5.244.93.199	35819	Mobily		(SA)

50.39.182.185	27017	Ziply Fiber		(US)
51.39.228.134	43766	Zain Saudi Arabia		(SA)
54.200.217.128	16509	Amazon.com		(US)
60.20.1.234	4837	China Unicom		(CN)
66.115.157.242	46562	Performive		(US)
67.129.13.170	209	CenturyLink		(US)
67.82.9.140	6128	Optimum Online		(US)
68.197.75.194	6128	Optimum Online		(US)
70.39.103.3	46844	Sharktech	AstrillVPN	(US)
71.112.196.114	701	Verizon Fios Business		(US)
71.112.196.115	701	Verizon Fios Business		(US)
72.193.13.228	22773	Cox Communications		(US)
74.222.20.18	74.222.20.18	Perfect International	AstrillVPN	(US)
74.63.233.50	46475	Limestone Networks	AstrillVPN	(US)
98.179.96.75	22773	Cox Communications		(US)

URLs

URL
hxxps://daniel-ayala[.]netlify[.]app

Posted in

- Threat Intelligence
