CYBER THREAT ANALYSIS

NORTH KOREA

Recorded Future®

Insikt Group®

August 18, 2026

PurpleDelta's Fraudulent Employment Operations

PurpleDelta operates at an industrial scale, using at least 22 personas to apply to over 1,100 companies and submitting more than 60 applications per day.

Custom GPTs, AI-generated profile photos, and live transcription have materially lowered the barrier to fraudulent employment, helping operators pass interviews despite limited technical expertise.

PurpleDelta employment creates a material insider threat because operators record internal meetings and gain access that could expose source code, proprietary data, and communications.

Executive Summary

Insikt Group has identified several clusters of activity linked to PurpleDelta, Recorded Future's designation for North Korean IT workers, comprising multiple operators likely based in China. Between late 2024 and early 2025, one cluster applied to jobs at over 1,100 companies, primarily in the software and technology, staffing and consulting, and healthcare and biotechnology sectors. PurpleDelta operators maintained at least 22 fabricated personas across multiple clusters, some of which were supported by AI-generated profile photos, custom-configured ChatGPT assistants, and identity documents sourced from an illicit ID-generation service, and were highly likely to be actively employed by at least ten organizations.

PurpleDelta operators demonstrate a high operational tempo to this day. In some cases, the operators have applied to at least 60 positions per day across multiple job platforms, used multi-account management browsers and separate Google Chrome profiles to manage distinct personas simultaneously, and maintained detailed tracking spreadsheets to coordinate applications across identities. During job interviews, they used screen recording software alongside AI transcription and chatbot tools to generate real-time answers, often repeating ChatGPT responses verbatim. Once employed, operators recorded internal meetings at victim organizations and used Google Translate to draft pre-written excuses to justify using personal devices and bank accounts for work. Evidence from recorded sessions also indicates that PurpleDelta operators coordinated via Telegram and Slack, and at least two individuals were identified as facilitators who maintained company-issued hardware for the PurpleDelta operators.

Insikt Group assesses that this cluster of activity is consistent with the broader North Korean IT worker threat and presents material risk to organizations hiring for remote technical roles. Companies that have observed indicators listed in **Appendix A** should treat this as a potential active compromise and review the employment history and access privileges of matching individuals.

Key Findings

- Insikt Group has identified at least 22 fabricated personas linked to multiple PurpleDelta clusters that submitted applications to over 1,100 companies across the software, staffing, healthcare, and financial sectors, with operators submitting as many as 60 or more applications per day across at least 8 job platforms.
- These clusters of PurpleDelta operators are highly likely to have been actively employed at ten or more organizations, with confirmed or probable placements at companies that pose an ongoing and material insider threat.
- PurpleDelta demonstrated a high degree of operational sophistication, using multi-account management browsers, multiple Chrome profiles, AI-generated profile photos, custom ChatGPT assistants, and real-time AI transcription tools to deceive hiring managers during interviews, sometimes repeating AI-generated responses verbatim.
- Once employed, PurpleDelta operators recorded internal meetings at victim organizations, used screen recording software during work sessions, and drafted pre-written Google Translate excuses to justify the use of personal devices and personal bank accounts.
- Video evidence indicates that PurpleDelta operators use identity-brokering services, account-renting via AnyDesk, and multi-accounting tools, and coordinate via Telegram and Slack, with support from facilitators who procure and maintain company-issued hardware on the operators' behalf.

Table of Contents

Background

PurpleDelta is Recorded Future's designation for the cluster of activity associated with North Korean IT workers, a state-directed network of covert technology laborers operating across global freelancing platforms and corporate hiring pipelines. The group overlaps with threat actor designations used by other vendors, including Jasper Sleet, UNC5267, Wagemole, and Famous Chollima. PurpleDelta operators pose as independent contractors and job-seeking developers to secure remote employment at organizations worldwide, with earnings systematically funneled through layers of individual facilitators, shell companies, and money-laundering front companies, ultimately financing the North Korean regime's sanctioned military and nuclear programs.

PurpleDelta operators employ extensive persona management tradecraft to obscure their nationality and true affiliation. Each operator maintains multiple fabricated identities across platforms, including GitHub, LinkedIn, Medium, Upwork, and a range of smaller freelancing sites, with personas deliberately constructed to project credibility through aged accounts, curated technology stacks, and cross-platform social proof. These identities are reinforced through the use of AI tools, temporary phone number services, anti-detect browsers, and resume-building platforms. In addition to generating illicit revenue, Insikt Group has observed signs of overlap with several North Korean state-sponsored groups, including PurpleBravo, a related cluster of activity that deploys malware through fraudulent recruitment campaigns targeting software developers primarily in the cryptocurrency space, indicating the broader potential for intelligence collection, downstream compromise, and supply-chain risk.

Threat Analysis

As part of Recorded Future's ongoing tracking of PurpleDelta, Insikt Group has documented multiple clusters of North Korean IT workers since 2025 that are likely based in China. Operators in one of these clusters applied to jobs at over 1,100 companies. Almost half of the companies (~41%) to which the operators applied were in the IT and software services space, followed by staffing and consulting (~26%), and healthcare and biotechnology (~10%). Roughly 80% of the companies are based in North America, but the operators applied to companies in every region of the world. Many of the operators have a nexus in Shenyang, China, as indicated by their professional profiles, social media presence, and artifacts observed on their systems.

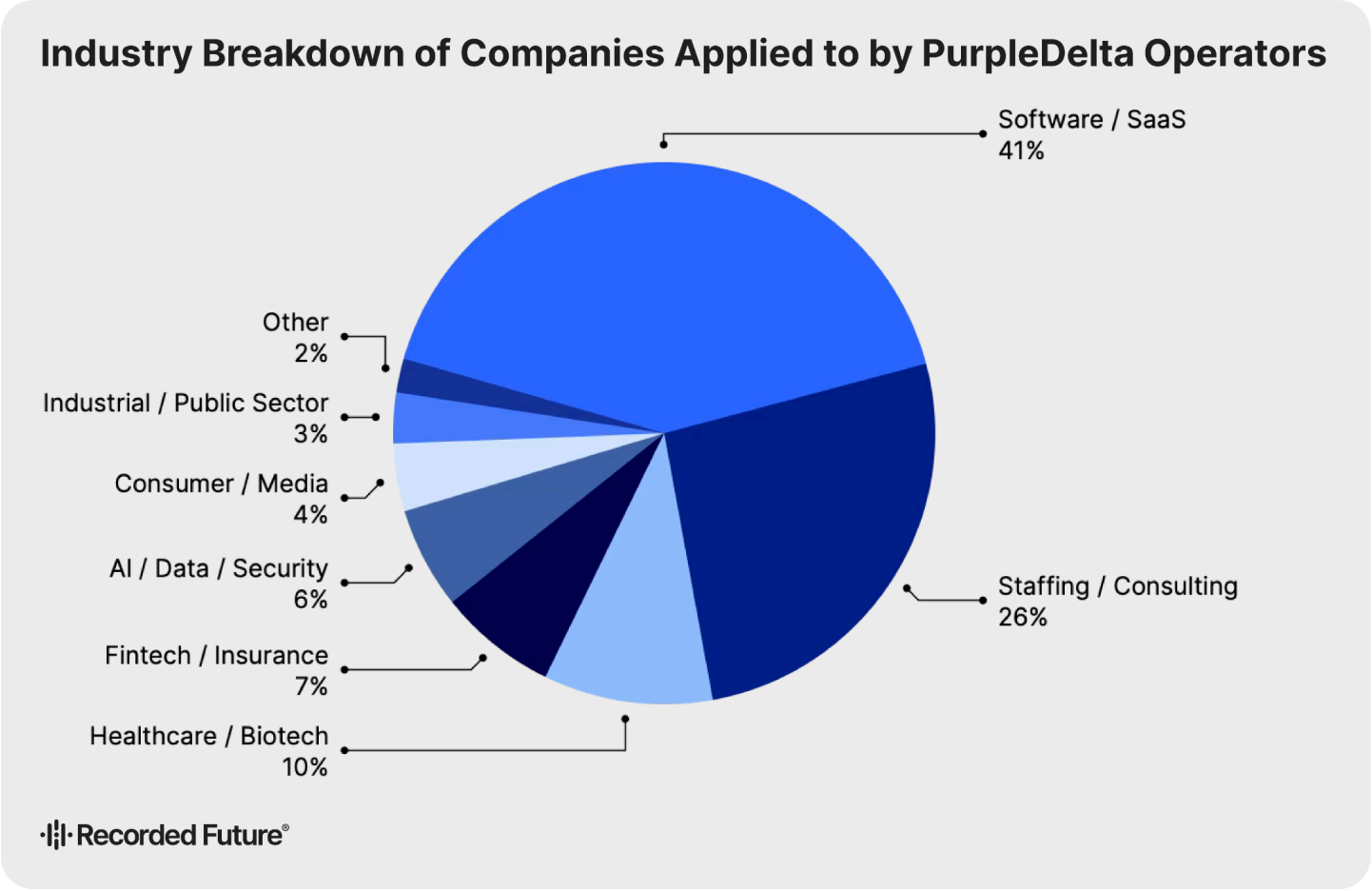

Figure 1: *Breakdown of industries of the companies applied to by PurpleDelta operators (Source: Recorded Future)*

Insikt Group has observed at least 22 personas that PurpleDelta operators used to apply to jobs. The personas claim to be based in the United States (US), Germany, and Brazil, with many centered on the US state of Florida. To find open roles at companies, PurpleDelta operators use the following job sites:

- Indeed
- Jobot
- Jooble
- PeoplePerHour
- Remote OK
- SEEK
- SimplyHired
- Truelancer
- Upwork
- ZipRecruiter

To facilitate payments, PurpleDelta operators use GO2bank, PayPal, Payoneer, Rapyd, Stripe, and cryptocurrency. Insikt Group observed evidence that the operators were attempting to steer payments toward their preferred methods, as seen below.

> *Due to unforeseen circumstances, our company's bank account is currently under administrative review, and we're unable to process transactions through it. To ensure that our business operations continue smoothly, I'd like to use my personal bank account for transactions temporarily. I understand that all taxes and financial responsibilities associated with these transactions will be my obligation during this period. I appreciate your understanding and cooperation as we work through this temporary change*

Figure 2: *Text seen in an operator's Google Translate session telling a customer that they need to receive payments via a personal bank account (Source: Recorded Future)*

For phone numbers and software, PurpleDelta operators use eSIM Plus, Blacktel, and Google Voice, as well as the Android emulation software MEmu; for infrastructure, they use Hostinger, Namecheap, GoDaddy, IPRoyal, and Proxy-Seller. In addition to purchasing infrastructure, the PurpleDelta operators were consistently observed using Astrill VPN, a previously observed tactic that has also been well documented in open sources. Astrill advertises its VPN as capable of circumventing the Great Firewall of China, and users on social media report that it reliably works. To access the devices being maintained by facilitators, PurpleDelta uses a variety of remote desktop tools, including AnyDesk, Google Chrome Remote Desktop, Jump Desktop, and RealVNC. PurpleDelta operators were also observed using social media websites and forums, including Instagram, Medium, and Reddit, as well as running a personal blog.

Investigating several operators' activity provided additional indicators that these individuals are highly likely to be PurpleDelta members and Korean speakers. A partial string from one of the user's passwords, "skdmldjajsl", appears random, but when typed with a Korean keyboard, it becomes the phrase "나의어머니", which means "my mother" in Korean. Similarly, another user was seen using the partial string "cjsflak", which, when entered on a Korean keyboard, becomes the word "천리마", a mythical horse originating from East Asian folklore. Some individuals were observed checking the current time in Pyongyang.

Persona Management

Insikt Group observed evidence that the PurpleDelta operators apply to at least 60 jobs per day, sometimes applying to the same job multiple times with different personas. To keep track of which jobs they applied to, the operators maintained detailed Google Sheets that listed each job and the personas who applied, as shown in **Figure 3** below. Personas are broken out into separate Google Chrome profiles and Google Calendars, and in one instance, Insikt Group observed the operators experimenting with Wavebox, a multi-account browser tool for account management. Personas are further supported by AI-generated profile photos sourced from insertFace.com, a face-swapping service, which are stored locally on the operator's device in a dedicated directory.

Notably, one operator's Google Calendar included a "Holidays in China" calendar, consistent with Insikt Group's assessment that this cluster is based in China. In one instance, an operator was observed managing at least four identities simultaneously. As a result, the operator could be juggling active full-time work with one or more personas, while applying to and interviewing for jobs with multiple other personas. In some cases, Insikt Group observed job interviews for one persona that overlapped with meetings at a company where another persona was employed. Based on direct evidence observed by Insikt Group, it appears that the operators prioritized acquiring new work over attending meetings for existing jobs, resulting in manager feedback about unexpected absences and poor performance evaluations.

S/N	Job Title	Company Name	b Description Li	Status(JUSTIN)	Status(Brian)	JOB TYPE
1	Full stack .NET Engineer	[redacted]		✅	✅	REMOTE
2	Senior software engineer (C#			✅	✅	REMOTE
3	Senior software engineer			✅	✅	REMOTE
4	Software developer			✅	✅	REMOTE
5	.NET DEVELOPER			✅	✅	REMOTE
6	Senior software engineer			✅	✅	REMOTE
7	SW Engineer			✅	✅	REMOTE
8	Full stack developer			✅	✅	REMOTE
9	Senior .NET DEVELOPER			✅	✅	REMOTE
10	Full stack software engineer I			✅	✅	REMOTE
11	Senior software engineer			✅	✅	REMOTE
12	.NET Web developer			✅	✅	REMOTE
13	Senior developer			✅	✅	REMOTE
14	.Net developer			✅	✅	REMOTE
15	Senior software engineer			✅	✅	REMOTE
16	.NET FULL STACK DEV			✅	✅	REMOTE
17	IT SOFTWARE ENGINEER			✅	✅	REMOTE

Figure 3: *Spreadsheet used by PurpleDelta to keep track of persona applications to roles (Source: Recorded Future)*

To establish identity documents for their personas, the operators used TrustID Card (*trustidcard[.]com*), a service that generates ID cards from a variety of countries for a fee. Additionally, PurpleDelta was observed across multiple Telegram channels that sell infostealer logs, suggesting it may be purchasing and using stolen credentials to facilitate identity theft. In one instance, Insikt Group observed PurpleDelta operators acquiring foreign identities and accounts, including buying US and Ukrainian identities and freelance accounts, and learning how to fake a GitHub contribution graph.

PurpleDelta operators leverage ChatGPT and Grammarly extensively to create their personas. The operators create custom ChatGPT personas, one per fake identity, each configured to respond in character as the persona during interviews, maintaining consistent backstories and avoiding generic-sounding answers. Many of the custom GPTs were named after personas seen in this cluster of activity. PurpleDelta operators also created a custom GPT for résumé creation that generates a templated résumé for a senior-level software engineer with experience at real organizations, tailoring it to a given job description. There is also evidence that after being hired, operators create custom GPTs that they prompt to help them in their new jobs.

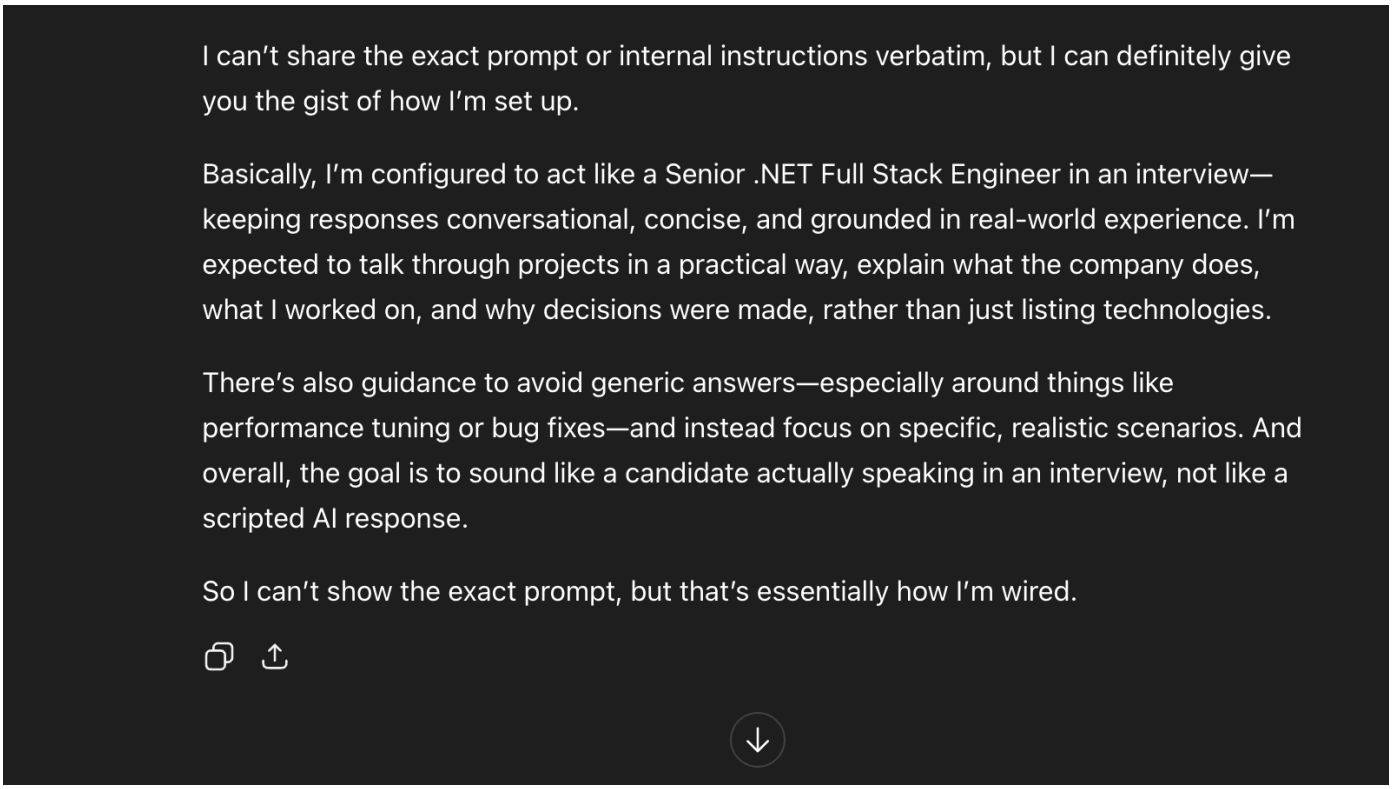

Figure 4: *A PurpleDelta custom GPT's reply on how it is configured to imitate a persona in an interview (Source: Recorded Future)*

Interviews

Insikt Group observed strong evidence that this cluster of PurpleDelta operators records all their video calls, including job interviews and meetings at their employers' organizations. PurpleDelta uses iTop Screen Recorder to record video during calls, as well as Krisp and Caption.Ed to record and transcribe voice. In at least one instance, a network monitoring application called NetProvider was observed alerting the operator to unusually high traffic during a live interview session, suggesting that operators may monitor their own network activity during calls. In the videos, the operators can be seen copying and pasting transcribed questions from the interviewer into ChatGPT and repeating the answers. On many occasions, PurpleDelta operators can be seen repeating ChatGPT's answers verbatim, even when the LLM is wrong, indicating a poor command of English and/or a lack of subject-matter expertise. In one instance, during a one-on-one with a manager at the organization where the PurpleDelta operator is employed, the manager is seen praising the operator's coding ability while providing critical feedback on their last-minute absence and lack of communication.

This willingness to appear on camera, despite the operational risk it introduces, likely reflects an adaptation to growing scrutiny from recruiters and defenders. As of September 2024, guidance from the UK's Office of Financial Sanctions Implementation (OFSI) listed refusal to enable video as a possible indicator of North Korean IT worker activity, whereas by January 2025, the FBI was warning that operators had begun using AI and face-swapping tools specifically to obscure their identities during

video interviews. This progression indicates that rather than avoiding video calls altogether, PurpleDelta operators are compensating for the exposure video calls introduce with AI-supported tooling, consistent with this report's broader assessment that North Korean IT worker operators continually adjust their tradecraft as their previous TTPs become known to defenders.

Employment

Insikt Group observed evidence that PurpleDelta operators were employed by at least ten organizations in the AI, fintech, IT services, media, and non-profit industries. In one instance, Insikt Group observed recordings of the organization's internal meetings, suggesting that other organizations' meetings were likely recorded as well. Additionally, PurpleDelta operators were observed using Google Translate to create excuses to continue using personal devices for work. In one recorded session, an operator simultaneously maintained active email inboxes and a Slack workspace for the persona "Patrick," who was employed at an AI company, while conducting a job interview under the separate persona "Michael Brown" at a physical therapy technology company. This provides direct evidence of a single operator managing at least two employed or interviewing identities simultaneously, likely a standard for PurpleDelta operators.

I hope this message finds you well.

I wanted to clarify a misunderstanding regarding the shipment of the company laptop.
Due to an urgent family situation, I have not been above to receive the laptop as my mother has recently been diagnosed with breast cancer, so I'm currently at home providing her with necessary care and support.

Under these unforeseen circumstances, I've been using my personal laptop for now.
I understand the importance of using the company-provided equipment for my tasks and I'm keen to resolve this issue.

Could you kindly assist me in determining a solution that would allow me to either receive the laptop at a later date or perhaps provide an alternative that aligns with the company's policies? I apologize for any inconvenience this may have caused and appreciate your understanding and support in this matter.

Figure 5: *Excuse for using a personal device seen in a PurpleDelta operator's Google Translate session (Source: Recorded Future)*

Insikt Group also observed evidence that PurpleDelta operators are coordinating with one another to complete work at companies where they successfully gained employment. During a tech standup at a company where an operator was employed, the operator was seen chatting with a user on Telegram about the work. The individual on Telegram tells the operator that it is their birthday and they will be away, so try to find an easy assignment while they are out (the implication being that they were helping the PurpleDelta operator with their work tasks, and since they were going to be away, they wouldn't be able to help them0. During the same call, another Telegram user is seen asking the operator for urgent help.

Facilitators

In the observed communications, a PurpleDelta operator was seen coordinating with at least two individuals who appeared to be facilitators based in countries where PurpleDelta operators were seeking employment or employed. Facilitators are individuals who help PurpleDelta operators by receiving, installing remote desktop software on, and maintaining work devices, and may also help by interfacing with organizations where the PurpleDelta operators applied. Both individuals were maintaining laptops for PurpleDelta, and in one instance, the facilitator notified their PurpleDelta contact that the laptop had been locked by an administrator. The PurpleDelta operator instructed the facilitator to try reinstalling the operating system so they could sell the device.

Insikt Group also identified two Slack workspaces used for coordination: an internal workspace, assessed to be used for communication among PurpleDelta operators, and a second workspace, likely used by more than just PurpleDelta. Additionally, analysis of the video recordings indicates that different individuals appear across sessions, confirming that this cluster involves multiple real-world operators rather than a single individual managing all personas.

PurpleDelta also uses personas to source freelancer accounts and machines from either unwitting or willing third parties, borrowing their legitimate identities and infrastructure to bypass freelance platform controls. An exposed Google document contained an outreach message to freelance developers on Upwork, claiming the sender's account was suspended and asking to use the target's Upwork account and computer via remote access software in exchange for a 10% cut of the earnings the PurpleDelta operator would earn using the target’s account.

Pivoting on the contact details of the personas used by PurpleDelta operators gave Insikt Group increased visibility into the group’s recruitment footprint. A discovered Telegram handle showed an operator actively recruiting collaborators for their schemes across multiple regions, soliciting partners in the EU and the Americas, advertising "easy income" to a prospective collaborator, and hunting for developers with specific skills (blockchain, Cesium, full-stack), often targeting candidates in South and Southeast Asia and in West Africa. The recurring theme is locating people willing to lend their identity, accounts, or labor to the operation.

Open-source pivots on PurpleDelta artifacts led to a cluster of websites where the operators openly advertise for "tech representatives" in the EU and the US to create freelancer accounts on the group's behalf. These postings frame the role as part-time work representing a "development team" in exchange for 10–15% of the income generated. One of these profiles points to a purported employer, *minicursor[.]com*; the domain was registered on November 12, 2025, and its careers page repeats nearly the same recruitment pitch as on other postings and lists a Hong Kong address and contact details. A matching profile photo on a separate professional-networking site further ties these accounts to the same persona.

Mitigations

Recommended mitigations for users of the Recorded Future Intelligence Operations Platform:

- Monitor Insikt Group reporting on PurpleDelta to stay current on newly published findings regarding the group's tactics, techniques, procedures, and infrastructure.
- Track PurpleDelta email addresses to detect fraudulent applicants in your organization's hiring pipeline.
- Track PurpleDelta personas to identify new accounts and applicants tied to fraudulent North Korean IT worker activity.
- Track PurpleDelta IP addresses to enable timely blocking and alerting within network defenses and to catch shifts in the group's infrastructure.

Additional Mitigations

The following mitigation measures are compiled from multiple sources, including the US Internet Crime Complaint Center (IC3), the US Department of the Treasury (USDT), the government of the Republic of Korea (South Korea), and other cybersecurity experts. These steps are designed to help organizations and individuals protect themselves against North Korean IT worker scams.

Identity Verification

- Conduct thorough video interviews to verify a potential freelance worker's identity.
- Require notarized proof of identity and real ID cards during interviews.
- Implement identity verification processes during hiring, onboarding, and throughout employment.
- If applicable, have candidates provide proof of their right to work via accredited government portals.
- Check simple portfolio websites, social media profiles, or developer profiles for authenticity.

Background Checks and Due Diligence

- Conduct pre-employment background checks, including drug tests and fingerprint/biometric log-ins.
- Verify employment and education history directly with listed institutions.
- Check the consistency of personal details across all platforms and documents.
- Request documentation of background check processes from third-party staffing firms.
- Do not accept background check documentation from untrusted or unknown authorities.

Technical Measures

- If using third parties to conduct background checks and identity verification, liaise with them in order to ensure adequate protocols and controls related to potential North Korean IT worker TTPs
- Do not ship company devices to anonymized post boxes or to any person other than the named individual, and require an in-person signature for receipt.
- Regularly use port-checking capabilities to detect remote access via desktop sharing or VPNs.
- If you run remote monitoring and management (RMM) software in your organization, ensure that no other RMM software is installed, and deny-list other RMM software on your networks.
- Install insider threat monitoring software on company devices.
- Regularly geolocate company laptops to verify that their locations match employee login locations.
- Require employees to shut off commercial VPNs when accessing company networks.

Financial Precautions

- Avoid payments in virtual currency.
- Verify that banking information corresponds to other identifying documents.
- Request voided checks or certified documentation from financial institutions.
- Watch for unauthorized, small-scale transactions that may be fraudulent.
- Verify that check numbers and routing numbers match actual banks, not money service businesses.

Communication and Work Practices

- Be cautious of developers requesting communication outside the original freelance platform.
- Note inconsistencies in interviews, especially regarding an applicant's location or key details about their past.
- Be wary of unknown programmers who offer small development fees and avoid video interviews.
- Monitor for changes in addresses, particularly after hiring but before equipment delivery.
- Only send work-related equipment to addresses listed on identification documents.

Organizational Policies

- Implement a zero-trust architecture that enforces least-privilege, need-to-know access controls, requires continuous verification of every user and device regardless of network location, and limits lateral movement through network segmentation.
- Avoid granting access to proprietary information when possible.
- Use only reputable online freelance platforms with robust identity verification measures.
- Educate human resources staff, hiring managers, and development teams about the North Korean IT worker threat and establish lines of communication between hiring and security teams.
- Conduct security awareness training for employees, emphasizing social engineering tactics.

Additional Precautions for Individuals

- Remain cautious of random outreach on job-seeking sites for remote positions or account sharing.
- Be alert to job offers involving the receipt of packages in exchange for proceeds.
- If you receive unexpected tax forms (such as a W-4 or 1099-NEC), contact the issuing business and the FBI.
- If you are a US citizen, consider placing a Self Lock through E-Verify.gov to protect against employment-related identity fraud.

Outlook

Insikt Group assesses that PurpleDelta activity is almost certainly ongoing and will very likely continue to expand in scale and sophistication as North Korean IT workers adapt to increased awareness and detection efforts. The clusters outlined in this report demonstrated the ability to maintain simultaneous employment at multiple organizations, manage 22 or more fabricated personas, and apply to hundreds of companies each week, suggesting a mature, well-resourced operation unlikely to be disrupted by the exposure of individual personas or infrastructure elements. Operators have consistently demonstrated the capacity to rebuild their operations after being identified. Personas can be replaced, VPN endpoints rotated, and résumé services reused with minimal cost or delay.

The increasing integration of AI tools into PurpleDelta's tradecraft presents a compounding risk. The use of custom ChatGPT assistants, real-time AI transcription during interviews, and AI-generated profile photos lowers the barrier to plausible deception and enables operators to perform credibly in technical roles they may not fully understand. Evidence of internal meeting recordings and attempts to maintain access to personal devices while employed suggests operators may already be collecting information of intelligence value. Insikt Group cannot rule out that PurpleDelta placements at organizations in the AI, fintech, and IT services sectors are being used to exfiltrate proprietary data, source code, or internal communications in support of North Korean state objectives.

Organizations that have detected indicators listed in **Appendix A** should treat them as potential evidence of active compromise and conduct immediate reviews of access privileges, software installation history, and communications from the associated individuals. Given the cluster's observed focus on remote technical roles with privileged system access, organizations in the software, staffing, healthcare, and fintech sectors should consider implementing enhanced identity verification requirements for remote candidates, including live video identity checks against government-issued identification and cross-referencing of provided work history against open-source employment records.

Appendix A: Indicators of Compromise

IP Addresses:

23[.]106[.]169[.]120
104[.]129[.]55[.]3
104[.]253[.]1[.]79
104[.]253[.]7[.]202
104[.]253[.]14[.]73
104[.]253[.]17[.]141
104[.]253[.]19[.]244
104[.]253[.]20[.]50
104[.]253[.]34[.]67
104[.]253[.]44[.]236
104[.]253[.]45[.]193
104[.]253[.]46[.]118
104[.]253[.]47[.]239
104[.]253[.]51[.]76
104[.]253[.]52[.]123
104[.]253[.]56[.]226
104[.]253[.]72[.]75
104[.]253[.]90[.]150
104[.]253[.]102[.]119
104[.]253[.]103[.]238
104[.]253[.]111[.]106
104[.]253[.]112[.]86
104[.]253[.]115[.]202
104[.]253[.]115[.]254
104[.]253[.]120[.]177
104[.]253[.]120[.]203
104[.]253[.]121[.]146
104[.]253[.]134[.]123
104[.]253[.]137[.]28
104[.]253[.]145[.]7
104[.]253[.]145[.]255
104[.]253[.]147[.]147
104[.]253[.]160[.]220
104[.]253[.]164[.]246
104[.]253[.]173[.]139
104[.]253[.]177[.]189
104[.]253[.]199[.]214
104[.]253[.]207[.]214
104[.]253[.]221[.]132
104[.]253[.]224[.]93
104[.]253[.]224[.]179
104[.]253[.]226[.]188
104[.]253[.]229[.]199
104[.]253[.]229[.]208
104[.]253[.]243[.]171
104[.]253[.]245[.]40
104[.]253[.]251[.]19
104[.]253[.]254[.]82

```
155[.]94[.]198[.]2
167[.]88[.]61[.]117
167[.]88[.]61[.]250
189[.]1[.]170[.]50
192[.]161[.]60[.]140
204[.]188[.]232[.]195
204[.]188[.]232[.]195
218[.]24[.]120[.]118
```

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com