Jasper Sleet: North Korean remote IT workers' evolving tactics to infiltrate organizations

microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/

By Microsoft Threat Intelligence June 30, 2025

Since 2024, Microsoft Threat Intelligence has observed remote information technology (IT) workers deployed by North Korea leveraging AI to improve the scale and sophistication of their operations, steal data, and generate revenue for the Democratic People's Republic of Korea (DPRK). Among the changes noted in the North Korean remote IT worker tactics, techniques, and procedures (TTPs) include the use of AI tools to replace images in stolen employment and identity documents and enhance North Korean IT worker photos to make them appear more professional. We've also observed that they've been utilizing voice-changing software.

North Korea has deployed thousands of remote IT workers to assume jobs in software and web development as part of a revenue generation scheme for the North Korean government. These highly skilled workers are most often located in North Korea, China, and Russia, and use tools such as virtual private networks (VPNs) and remote monitoring and management (RMM) tools together with witting accomplices to conceal their locations and identities.

Historically, North Korea's fraudulent remote worker scheme has focused on targeting United States (US) companies in the technology, critical manufacturing, and transportation sectors. However, we've observed North Korean remote workers evolving to broaden their scope to target various industries globally that offer technology-related roles. Since 2020, the US government and cybersecurity community have identified thousands of North Korean workers infiltrating companies across various industries.

Organizations can protect themselves from this threat by implementing stricter pre-employment vetting measures and creating policies to block unapproved IT management tools. For example, when evaluating potential employees, employers and recruiters should ensure that the candidates' social media and professional accounts are unique and verify their contact information and digital footprint. Organizations should also be particularly cautious with staffing company employees, check for consistency in resumes, and use video calls to confirm a worker's identity.

Microsoft Threat Intelligence tracks North Korean IT remote worker activity as Jasper Sleet (formerly known as Storm-0287). We also track several other North Korean activity clusters that pursue fraudulent employment using similar techniques and tools, including Storm-1877 and Moonstone Sleet. To disrupt this activity and protect our customers, we've suspended 3,000 known Microsoft consumer accounts (Outlook/Hotmail) created by North Korean IT workers. We have also implemented several detections to alert our customers of this activity through Microsoft Entra ID Protection and Microsoft Defender XDR as noted at the end of this blog. As with any observed nation-state threat actor activity, Microsoft has directly notified targeted or compromised customers, providing them with important information needed to secure their environments. As we continue to observe more attempts by threat actors to leverage AI, not only do we report on them, but we also have principles in place to take action against them.

This blog provides additional information on the North Korean remote IT worker operations we published previously, including Jasper Sleet's usual TTPs to secure employment, such as using fraudulent identities and facilitators. We also provide recent observations regarding their use of AI tools. Finally, we share detailed guidance on how to investigate, monitor, and remediate possible North Korean remote IT worker activity, as well as detections and hunting capabilities to surface this threat.

From North Korea to the world: The remote IT workforce

Since at least early 2020, Microsoft has tracked a global operation conducted by North Korea in which skilled IT workers apply for remote job opportunities to generate revenue and support state interests. These workers present themselves as foreign (non-North Korean) or domestic-based teleworkers and use a variety of fraudulent means to bypass employment verification controls.

North Korea's fraudulent remote worker scheme has since evolved, establishing itself as a well-developed operation that has allowed North Korean remote workers to infiltrate technology-related roles across various industries. In some cases, victim organizations have even reported that remote IT workers were some of their most talented employees. Historically, this operation has focused on applying for IT, software development, and

administrator positions in the technology sector. Such positions provide North Korean threat actors access to highly sensitive information to conduct information theft and extortion, among other operations.

North Korean IT workers are a multifaceted threat because not only do they generate revenue for the North Korean regime, which violates international sanctions, they also use their access to steal sensitive intellectual property, source code, or trade secrets. In some cases, these North Korean workers even extort their employer into paying them in exchange for not publicly disclosing the company's data.

Between 2020 and 2022, the US government found that over 300 US companies in multiple industries, including several Fortune 500 companies, had unknowingly employed these workers, indicating the magnitude of this threat. The workers also attempted to gain access to information at two government agencies. Since then, the cybersecurity community has continued to detect thousands of North Korean workers. On January 3, 2025, the Justice Department released an indictment identifying two North Korean nationals and three facilitators responsible for conducting fraudulent work between 2018 and 2024. The indicted individuals generated a revenue of at least US$866,255 from only ten of the at least 64 infiltrated US companies.

North Korean threat actors are evolving across the threat landscape to incorporate more sophisticated tactics and tools to conduct malicious employment-related activity, including the use of custom and AI-enabled software.

Tactics and techniques

The tactics and techniques employed by North Korean remote IT workers involve a sophisticated ecosystem of crafting fake personas, performing remote work, and securing payments. North Korean IT workers apply for remote roles, in various sectors, at organizations across the globe.

They create, rent, or procure stolen identities that match the geo-location of their target organizations (for example, they would establish a US-based identity to apply for roles at US-based companies), create email accounts and social media profiles, and establish legitimacy through fake portfolios and profiles on developer platforms like GitHub and LinkedIn. Additionally, they leverage AI tools to enhance their operations, including image creation and voice-changing software. Facilitators play a crucial role in validating fraudulent identities and managing logistics, such as forwarding company hardware and creating accounts on freelance job websites. To evade detection, these workers use VPNs, virtual private servers (VPSs), and proxy services as well as RMM tools to connect to a device housed at a facilitator's laptop farm located in the country of the job.

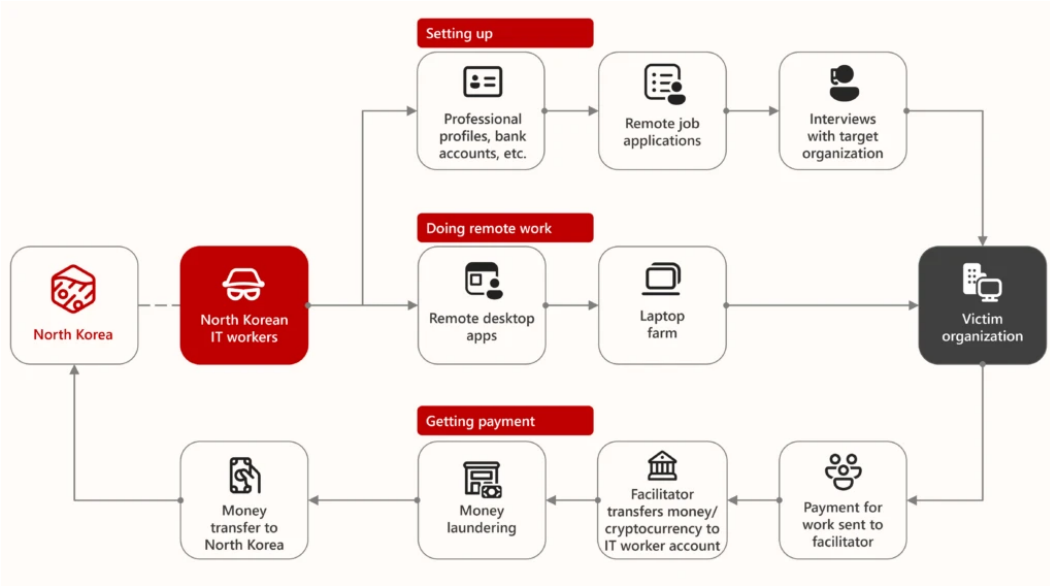

Figure 1. The North Korean IT worker ecosystem

Crafting fake personas and profiles

The North Korean remote IT worker fraud scheme begins with the procurement of identities for the workers. These identities, which can be stolen or “rented” from witting individuals, include names, national identification numbers, and dates of birth. The workers might also leverage services that generate fraudulent identities, complete with seemingly legitimate documentation, to fabricate their personas. They then create email accounts and social media pages they use to apply for jobs, often indirectly through staffing or contracting companies. They also apply for freelance opportunities through freelancer sites as an additional avenue for revenue generation. Notably, they often use the same names/profiles repeatedly rather than creating unique personas for each successful infiltration.

Additionally, the North Korean IT workers have used fake profiles on LinkedIn to communicate with recruiters and apply for jobs.

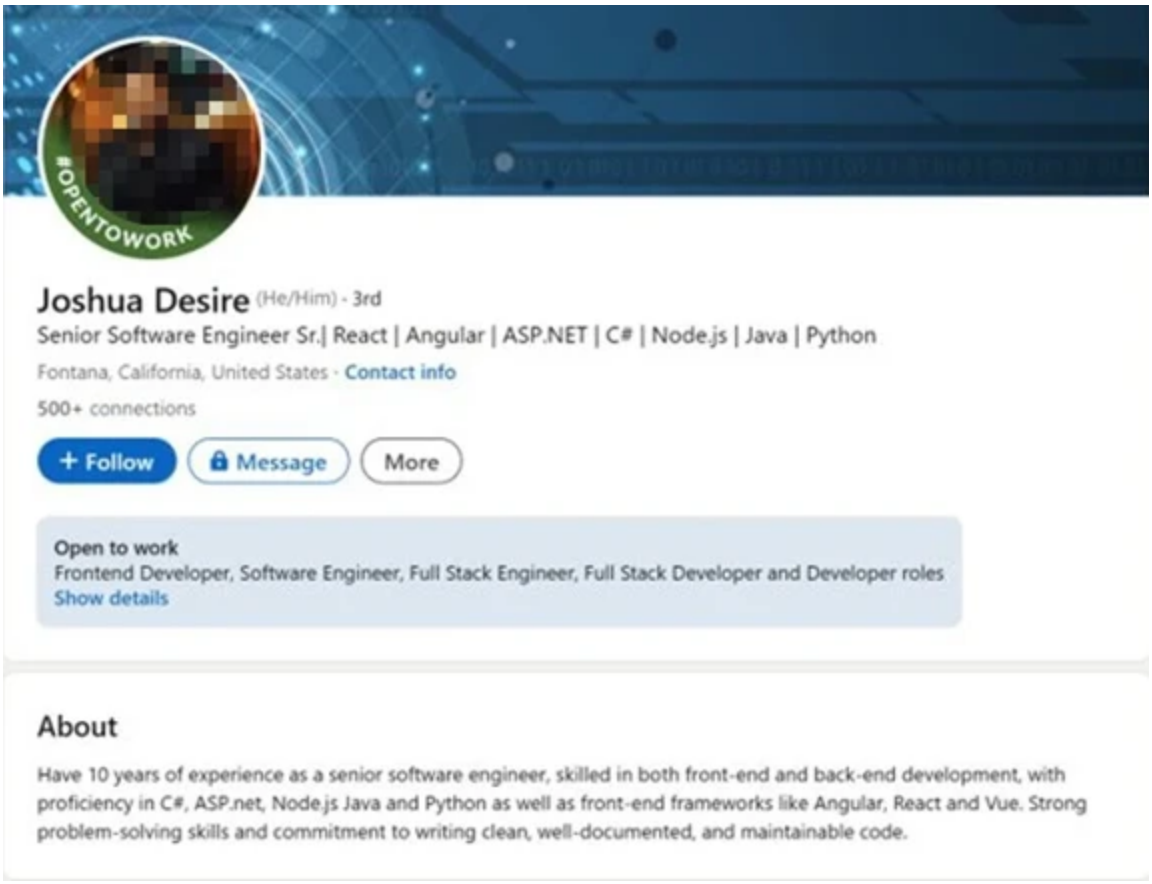

Figure 2. An example of a North Korean IT worker LinkedIn profile that has since been taken down.

The workers tailor their fake resumes and profiles to match the requirements for specific remote IT positions, thus increasing their chances of getting selected. Over time, we've observed these fake resumes and employee documents noticeably improving in quality, now appearing more polished and lacking grammatical errors facilitated by AI.

Establishing digital footprint

After creating their fake personas, the North Korean IT workers then attempt to establish legitimacy by creating digital footprints for these fake personas. They typically leverage communication, networking, and developer platforms, (for example, GitHub) to showcase their supposed portfolio of previous work samples:

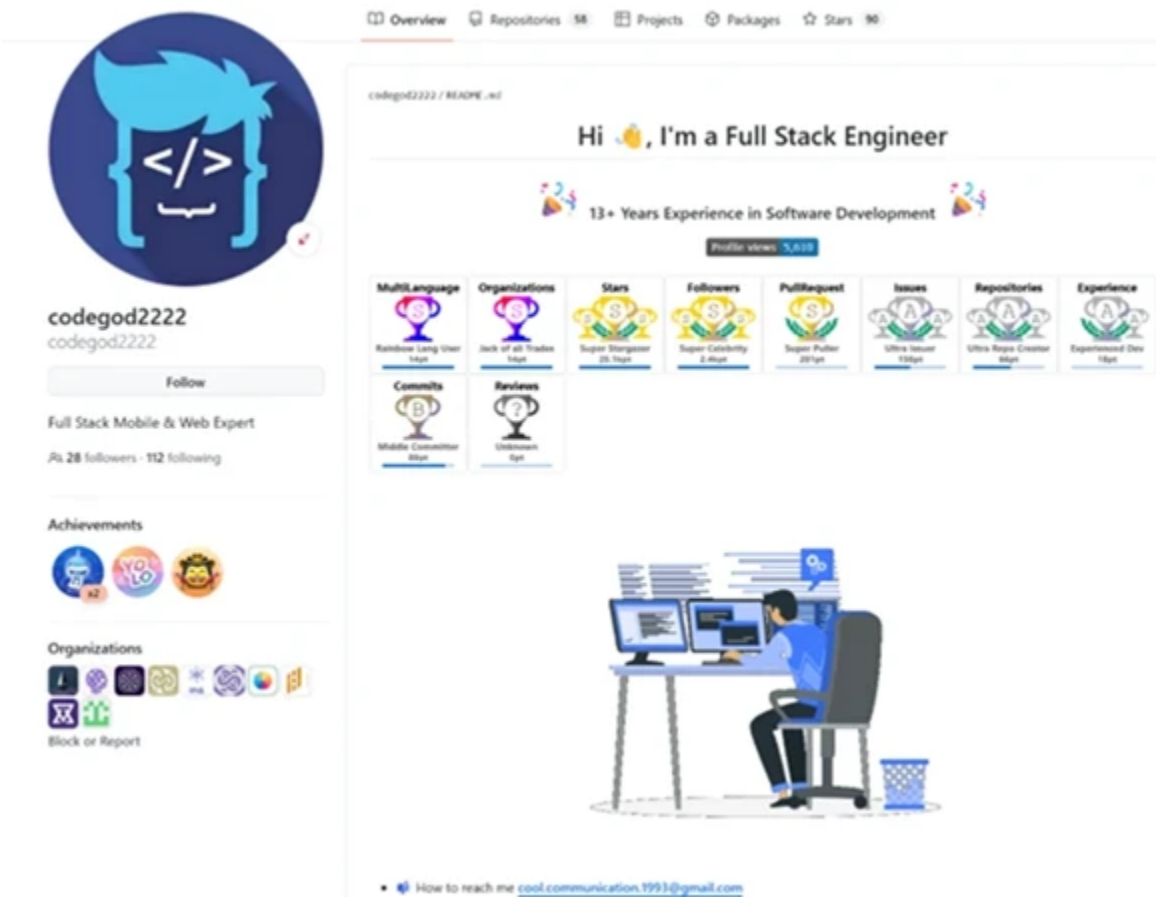

Figure 3. Example profile used by a North Korean IT worker that has since been taken down.

Using AI to improve operations

Microsoft Threat intelligence has observed North Korean remote IT workers leveraging AI to improve the quantity and quality of their operations. For example, in October 2024, we found a public repository containing actual and AI-enhanced images of suspected North Korean IT workers:

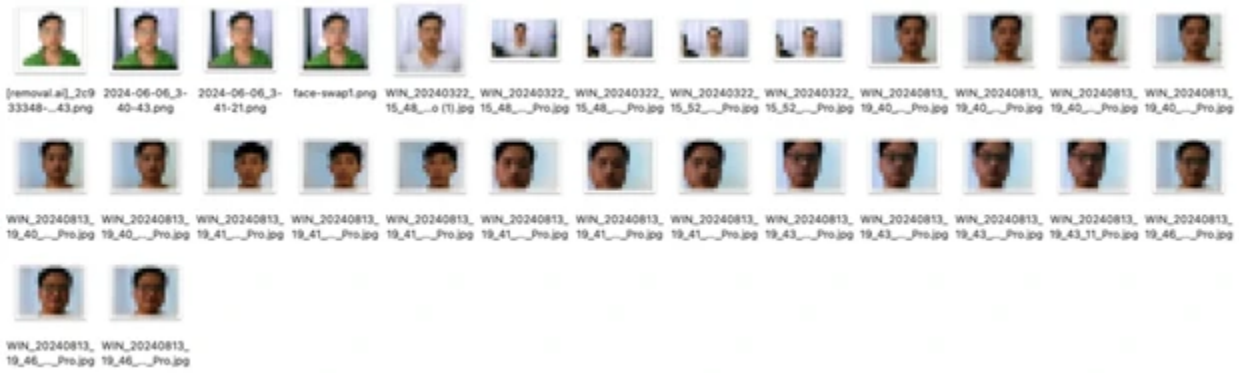

Figure 4. Photos of potential North Korean IT workers

The repository also contained the resumes and email accounts used by the said workers, along with the following tools and resources they can use to secure employment and to do their work:

- VPS and VPN accounts, along with specific VPS IP addresses
- Playbooks on conducting identity theft and creating and bidding jobs on freelancer websites
- Wallet information and suspected payments made to facilitators
- LinkedIn, GitHub, Upwork, TeamViewer, Telegram, and Skype accounts
- Tracking sheet of work performed, and payments received by the IT workers

Image creation

Based on our review of the repository mentioned previously, North Korean IT workers appear to conduct identity theft and then use AI tools like Faceswap to move their pictures over to the stolen employment and identity documents. The attackers also use these AI tools to take pictures of the workers and move them to more professional looking settings. The workers then use these AI-generated pictures on one or more resumes or profiles when applying for jobs.

Figure 5. Use of AI apps to modify photos used for North Korean IT workers' resumes and profiles

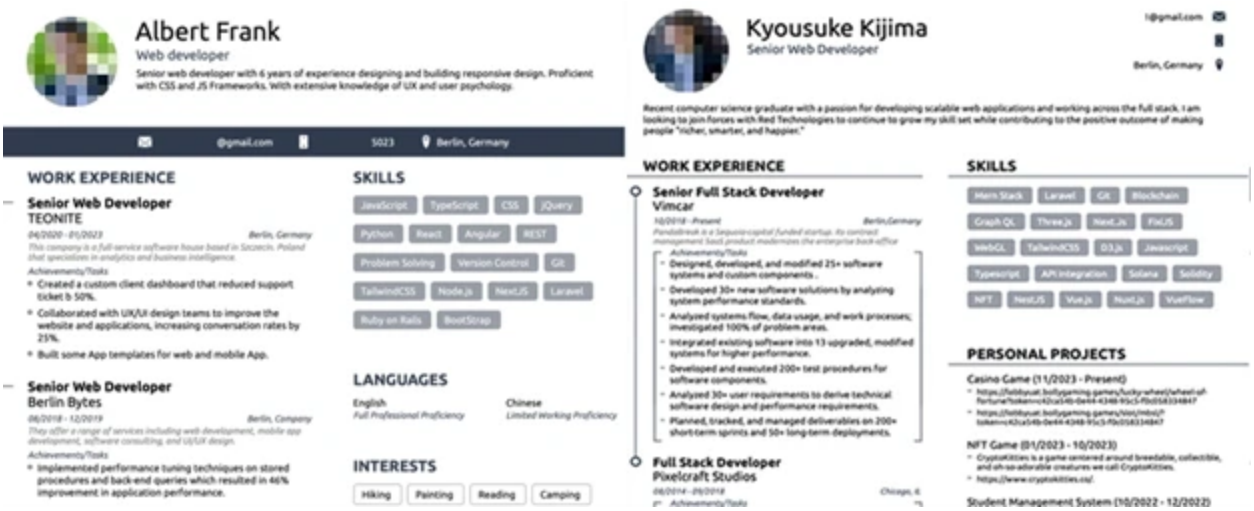

Figure 6. Examples of resumes for North Korean IT workers. These two resumes use different versions of the same photo.

Communications

Microsoft Threat Intelligence has observed that North Korean IT workers are also experimenting with other AI technologies such as voice-changing software. While we haven't observed threat actors using combined AI voice and video products as a tactic first hand, we do recognize that combining these technologies could allow future threat actor campaigns to trick interviewers into thinking they aren't communicating with a North Korean IT worker. If successful, this tactic could allow the North Korean IT workers to do interviews directly and no longer rely on facilitators standing in for them on interviews or selling them account access.

Facilitators for initial access

North Korean remote IT workers require assistance from a witting facilitator to help find jobs, pass the employment verification process, and once hired, successfully work remotely. We've observed Jasper Sleet advertising job opportunities for facilitator roles under the guise of partnering with a remote job candidate to help secure an IT role in a competitive market:

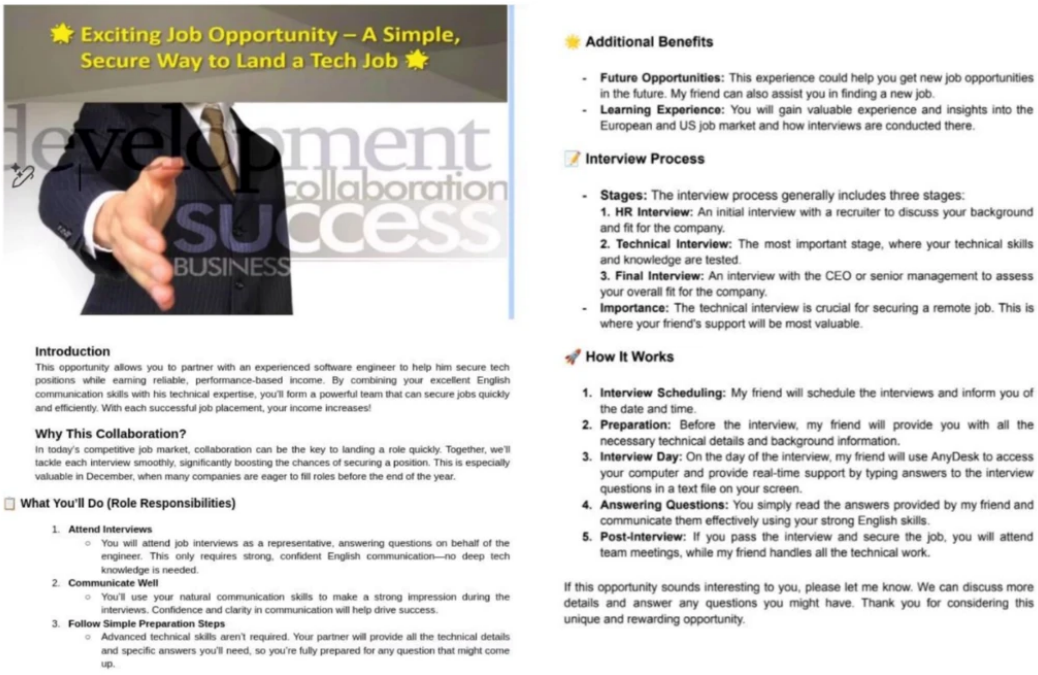

Figure 7. Example of a job opportunity for a facilitator role

The IT workers may have the facilitators assist in creating accounts on remote and freelance job websites. They might also ask the facilitator to perform the following tasks as their relationship builds:

- Create a bank account for the North Korean IT worker, or lend their (the facilitator's) own account to the worker
- Purchase mobile phone numbers or SIM cards

During the employment verification process, the witting accomplice helps the North Korean IT workers validate the latter's fraudulent identities using online background check service providers. The documents submitted by the workers include fake or stolen drivers' licenses, social security cards, passports, and permanent resident identification cards. Workers train using interview scripts, which include a justification for why the employee must work remotely.

Once hired, the remote workers direct company laptops and hardware to be sent to the address of the accomplice. The accomplice then either runs a laptop farm that provides the laptops with an internet connection at the geo-location of the role or forwards the items internationally. For hardware that remain in the country of the role, the accomplice signs into the computers and installs software that enables the workers to connect remotely. Remote IT workers might also access devices remotely using IP-based KVM devices, like PiKVM or TinyPilot.

Defense evasion and persistence

To conceal their physical location as well as maintain persistence and blend into the target organization's environment, the workers typically use VPNs (particularly Astrill VPN), VPSs, proxy services, and RMM tools. Microsoft Threat Intelligence has observed the persistent use of JumpConnect, TinyPilot, Rust Desk, TeamViewer, AnyViewer, and Anydesk. When an in-person presence or face-to-face meeting is required, for example to confirm banking information or attend a meeting, the workers have been known to pay accomplices to stand in for them. When possible, however, the workers eliminate all face-to-face contact, offering fraudulent excuses for why they are not on camera during video teleconferencing calls or speaking.

Attribution

Microsoft Threat Intelligence uses the name Jasper Sleet (formerly known as Storm-0287) to represent activity associated with North Korean's remote IT worker program. These workers are primarily focused on revenue generation, use remote access tools, and likely fall under a particular leadership structure in North Korea. We also track several other North Korean activity clusters that pursue fraudulent employment using similar techniques and tools, including Storm-1877 and Moonstone Sleet.

How Microsoft disrupts North Korean remote IT worker operations with machine learning

Microsoft has successfully scaled analyst tradecraft to accelerate the identification and disruption of North Korean IT workers in customer environments by developing a custom machine learning solution. This has been achieved by leveraging Microsoft's existing threat intelligence and weak signals generated by monitoring for many of the red flags listed in this blog, among others. For example, this solution uses impossible time travel risk detections, most commonly between a Western nation and China or Russia. The machine learning workflow uses these features to surface suspect accounts most likely to be North Korean IT workers for assessment by Microsoft Threat Intelligence analysts.

Once Microsoft Threat Intelligence reviews and confirms that an account is indeed associated with a North Korean IT worker, customers are then notified with a Microsoft Entra ID Protection risk detection warning of a risky sign-in based on Microsoft's threat intelligence. Microsoft Defender XDR customers also receive the alert *Sign-in activity by a suspected North Korean entity* in the Microsoft Defender portal.

Defending against North Korean remote IT worker infiltration

Defending against the threats from North Korean remote IT workers involves a threefold strategy:

- Ensuring a proper vetting approach is in place for freelance workers and vendors

- Monitoring for anomalous user activity
- Responding to suspected Jasper Sleet signals in close coordination with your insider risk team

Investigate

How can you identify a North Korean remote IT worker in the hiring process?

To protect your organization against a potential North Korean insider threat, it is important for your organization to prioritize a process for verifying employees to identify potential risks. The following can be used to assess potential employees:

- Confirm the potential employee has a digital footprint and look for signs of authenticity. This includes a real phone number (not VoIP), a residential address, and social media accounts. Ensure the potential employee's social media/professional accounts are not highly similar to the accounts of other individuals. In addition, check that the contact phone number listed on the potential employee's account is unique and not also used by other accounts.
- Scrutinize resumes and background checks for consistency of names, addresses, and dates. Consider contacting references by phone or video-teleconference rather than email only.
- Exercise greater scrutiny for employees of staffing companies, since this is the easiest avenue for North Korean workers to infiltrate target companies.
- Search whether a potential employee is employed at multiple companies using the same persona.
- Ensure the potential employee is seen on camera during multiple video telecommunication sessions. If the potential employee reports video and/or microphone issues that prohibit participation, this should be considered a red flag.
- During video verification, request individuals to physically hold driver's licenses, passports, or identity documents up to camera.
- Keep records, including recordings of video interviews, of all interactions with potential employees.
- Require notarized proof of identity.

Monitor

How can your organization prevent falling victim to the North Korean remote IT worker technique?

To prevent the risks associated with North Korean insider threats, it's vital to monitor for activity typically associated with this fraudulent scheme.

Monitor for identifiable characteristics of North Korean remote workers

Microsoft has identified the following characteristics of a North Korean remote worker. Note that not all the criteria are necessarily required, and further, a positive identification of a remote worker doesn't guarantee that the worker is North Korean.

- The employee lists a Chinese phone number on social media accounts that is used by other accounts.
- The worker's work-issued laptop authenticates from an IP address of a known North Korean IT worker laptop farm, or from foreign—most commonly Chinese or Russian—IP addresses even though the worker is supposed to have a different work location.
- The worker is employed at multiple companies using the same persona. Employees of staffing companies require heightened scrutiny, given this is the easiest way for North Korean workers to infiltrate target companies.
- Once a laptop is issued to the worker, RMM software is immediately downloaded onto it and used in combination with a VPN.
- The worker has never been seen on camera during a video telecommunication session or is only seen a few times. The worker may also report video and/or microphone issues that prohibit participation from the start.
- The worker's online activity doesn't align with routine co-worker hours, with limited engagement across approved communication platforms.

Monitor for activity associated with Jasper Sleet access

- If RMM tools are used in your environment, enforce security settings where possible, to implement MFA:
  - Use Windows Defender Application Control or AppLocker to create policies to block unapproved IT management tools. Consider hunting for unapproved RMM software installations and creating custom detections (**Investigation & response** > **Hunting** > **Advanced hunting** > **Manage rules** > **Create custom detection**) for any advanced hunting queries that are useful indicators of anomalous or unapproved activity in your environment.
  - If an unapproved installation is discovered, reset passwords for accounts used to install the RMM services. If a system-level account was used to install the software, further investigation may be warranted.
- Monitor for impossible travel—for example, a supposedly US-based employee signing in from China or Russia.
- Monitor for use of public VPNs such as Astrill. For example, IP addresses associated with VPNs known to be used by Jasper Sleet can be added to Sentinel watchlists. Or, Microsoft Defender for Identity can integrate with your VPN solution to provide more information about user activity, such as extra detection for abnormal VPN connections.
- Monitor for signals of insider threats in your environment. Microsoft Purview Insider Risk Management can help identify potentially malicious or inadvertent insider risks.
- Monitor for consistent user activity outside of typical working hours.

Remediate

What are the next steps if you positively identify a North Korean remote IT worker employed at your company?

Because Jasper Sleet activity follows legitimate job offers and authorized access, Microsoft recommends approaching confirmed or suspected Jasper Sleet intrusions with an insider risk approach using your organization's insider risk response plan or incident response provider like Microsoft Incident Response. Some steps might include:

- Restrict response efforts to a small, trusted insider risk working group, trained in operational security (OPSEC) to avoid tipping off subjects and potential collaborators.
- Rapidly evaluate the subject's proximity to critical assets, such as:
    - Leadership or sensitive teams
    - Direct reports or vendor staff the subject has influence over
    - Suppliers or vendors
    - People/non-people accounts, production/pre-production environments, shared accounts, security groups, third-party accounts, security groups, distribution groups, data clusters, and more
- Conduct preliminary link analysis to:
    - Detect relationships with potential collaborators, supporters, or other potential aliases operated by the same actor
    - Identify shared indicators (for example, shared IP addresses, behavioral overlap)
    - Avoid premature action that might alert other Jasper Sleet operators
- Conduct a risk-based prioritization of efforts, informed by:
    - Placement and access to critical assets (not necessarily where you identified them)Stakeholder insight from potentially impacted business units
    - Business impact considerations of containment (which might support additional collection/analysis) or mitigation (for example, eviction)

- Conduct open-source intelligence (OSINT) collection and analysis to:
    Determine if the identity associated with the threat actor is associated with a real person. For example, North Korean IT workers have leveraged stolen identities of real US persons to facilitate their fraud. Conduct OSINT on all available personally identifiable information (PII) provided by the actor (name, date of birth, SSN, home of record, phone number, emergency contact, and others) and determine if these items are linked to additional North Korean actors, and/or real persons' identities.
    Gather all known external accounts operated by the alias/persona (for example, LinkedIn, GitHub, freelance working sites, bug bounty programs).
    Perform analysis on account images using open-source tools such as FaceForensics++ to determine prevalence of AI-generated content. Detection opportunities within video and imagery include:
        - **Temporal consistency issues:** Rapid movements cause noticeable artifacts in video deepfakes as the tracking system struggles to maintain accurate landmark positioning.
        - **Occlusion handling:** When objects pass over the AI-generated content such as the face, deepfake systems tend to fail at properly reconstructing the partially obscured face.
        - **Lighting adaptation:** Changes in lighting conditions might reveal inconsistencies in the rendering of the face
        - **Audio-visual synchronization:** Slight delays between lip movements and speech are detectable under careful observation
            - Exaggerated facial expressions.
            - Duplicative or improperly placed appendages.
            - Pixelation or tearing at edges of face, eyes, ears, and glasses.
- Engage counterintelligence or insider risk/threat teams to:
    Understand tradecraft and likely next steps
    Gain national-level threat context, if applicable
- Make incremental, risk-based investigative and response decisions with the support of your insider threat working group and your insider threat stakeholder group; one providing tactical feedback and the other providing risk tolerance feedback.
- Preserve evidence and document findings.
- Share lessons learned and increase awareness.
- Educate employees on the risks associated with insider threats and provide regular security training for employees to recognize and respond to threats, including a section on the unique threat posed by North Korean IT workers.

After an insider risk response to Jasper Sleet, it might be necessary to also conduct a thorough forensic investigation of all systems that the employee had access to for indicators of persistence, such as RMM tools or system/resource modifications.

For additional resources, refer to CISA's Insider Threat Mitigation Guide. If you suspect your organization is being targeted by nation-state cyber activity, report it to the appropriate national authority. For US-based organizations, the Federal Bureau of Investigation (FBI) recommends reporting North Korean remote IT worker activity to the Internet Crime Complaint Center (IC3).

Microsoft Defender XDR detections

Microsoft Defender XDR customers can refer to the list of applicable detections below. Microsoft Defender XDR coordinates detection, prevention, investigation, and response across endpoints, identities, email, apps to provide integrated protection against attacks like the threat discussed in this blog.

Customers with provisioned access can also use Microsoft Security Copilot in Microsoft Defender to investigate and respond to incidents, hunt for threats, and protect their organization with relevant threat intelligence.

Microsoft Defender XDR

Alerts with the following title in the security center can indicate threat activity on your network:

> Sign-in activity by a suspected North Korean entity

Microsoft Defender for Endpoint

Alerts with the following titles in the security center can indicate Jasper Sleet RMM activity on your network. These alerts, however, can be triggered by unrelated threat activity.

- Suspicious usage of remote management software
- Suspicious connection to remote access software

Microsoft Defender for Identity

Alerts with the following titles in the security center can indicate atypical identity access on your network. These alerts, however, can be triggered by unrelated threat activity.

- Atypical travel
- Suspicious behavior: Impossible travel activity

Microsoft Entra ID Protection

Microsoft Entra ID Protection risk detections inform Entra ID user risk events and can indicate associated threat activity, including unusual user activity consistent with known patterns identified by Microsoft Threat Intelligence research. Note, however, that these alerts

can be also triggered by unrelated threat activity.

> Microsoft Entra threat intelligence (sign-in): (RiskEventType: investigationsThreatIntelligence)

Microsoft Defender for Cloud Apps

Alerts with the following titles in the security center can indicate atypical identity access on your network. These alerts, however, can be triggered by unrelated threat activity.

> Impossible travel activity

Microsoft Security Copilot

Security Copilot customers can use the standalone experience to create their own prompts or run the following prebuilt promptbooks to automate incident response or investigation tasks related to this threat:

- Incident investigation
- Microsoft User analysis
- Threat actor profile

Note that some promptbooks require access to plugins for Microsoft products such as Microsoft Defender XDR or Microsoft Sentinel.

Hunting queries

Microsoft Defender XDR

Because organizations might have legitimate and frequent uses for RMM software, we recommend using the Microsoft Defender XDR advanced hunting queries available on GitHub to locate RMM software that hasn't been endorsed by your organization for further investigation. In some cases, these results might include benign activity from legitimate users. Regardless of use case, all newly installed RMM instances should be scrutinized and investigated.

If any queries have high fidelity for discovering unsanctioned RMM instances in your environment, and don't detect benign activity, you can create a custom detection rule from the advanced hunting query in the Microsoft Defender portal.

Microsoft Sentinel

The alert *Insider Risk Sensitive Data Access Outside Organizational Geo-location*joins Azure Information Protection logs (*InformationProtectionLogs_CL*) with Microsoft Entra ID sign-in logs (*SigninLogs*) to provide a correlation of sensitive data access by geo-location. Results include:

- User principal name
- Label name
- Activity
- City
- State
- Country/Region
- Time generated

The recommended configuration is to include (or exclude) sign-in geo-locations (city, state, country and/or region) for trusted organizational locations. There is an option for configuration of correlations against Microsoft Sentinel watchlists. Accessing sensitive data from a new or unauthorized geo-location warrants further review.

References

Acknowledgments

For more information on North Korean remote IT worker operations, we recommend reviewing DTEX's in-depth analysis in the report Exposing DPRK's Cyber Syndicate and IT Workforce.

Learn more

Meet the experts behind Microsoft Threat Intelligence, Incident Response, and the Microsoft Security Response Center at our VIP Mixer at Black Hat 2025. Discover how our end-to-end platform can help you strengthen resilience and elevate your security posture.

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn, X (formerly Twitter), and Bluesky.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast.