DTEX

Exposing DPRK's Cyber Syndicate and Hidden IT Workforce

Contents

"Every business leader and security professional needs to recognize the risks of accommodating remote workers. Remote work is a shift change that accelerated massively during the COVID pandemic in 2020, and became the new normal overnight. To empower companies to trust their remote resources is paramount—especially with North Korea leveraging the opportunity to fund its weapons program. The threat of unintentionally hiring North Korean IT workers is larger than most people realize. It's covert, it's global, and it's active right now—which is why industry and government need to work together to come up with solutions to counter the threat."

Kevin Mandia
Co-Founder and General Partner of Ballistic Ventures,
and former Founder and CEO of Mandiant

"DPRK's cyber operations challenge the traditional nation-state playbook—merging cryptocurrency theft, espionage, and nuclear ambition within a self-funded system driven by profit, loyalty, and survival. Recognizing it as a family-run mafia syndicate unblurs the lines between cybercrime and statecraft. This report pulls back the curtain on their inner workings and psychology, revealing how deeply embedded they already are within our workforce—providing the context needed to anticipate their next move."

The Honorable Sue Gordon
President of GordonVentures, LLC, and former
Principal Deputy Director of National Intelligence

Executive Summary

Unmasking the DPRK's Nation-State Crime Syndicate: Time to Rethink the Threat

The Democratic People's Republic of Korea (DPRK) has emerged as a far more sophisticated and dangerous cyber actor than widely recognized. Often reduced to familiar labels like Lazarus Group or Hidden Cobra, its cyber operations are, in fact, part of a deeply integrated, state-sponsored enterprise—one that transcends traditional nation-state models of cyber conflict.

What we face is not a series of isolated Advanced Persistent Threats (APTs), but a self-funding offensive apparatus—decentralized and powered by a network of cyber talent and resources that fluidly shifts focus, personnel, and infrastructure across borders. These activities are often synchronized with physical operations, reflecting a seamless integration of digital and kinetic objectives.

At its core, the DPRK's cyber program functions more like a state-sanctioned crime syndicate than a conventional military or intelligence apparatus. The profits—from ransomware, cryptocurrency theft, financial fraud, and insider infiltration—flow upward to fund weapons development and sanctions evasion. Simultaneously, parallel operations engage in state espionage, accelerating nuclear and military programs through stolen intelligence.

But what sets the DPRK apart is the survival-based incentive structure at the heart of its engine. Cyber operatives are not motivated by ideology, but by material necessities: food, shelter, healthcare, and education for their families.

In a country defined by scarcity, participation in cyber operations offers a rare path to a better life. Loyalty is not the core driver. Survival is.

Understanding DPRK's cyber architecture requires seeing it through the lens of criminal-state fusion, where cybercrime, statecraft, espionage, and survival are not separate domains—but one and the same.

> **To truly grasp this threat, we must pivot from asking "Who did it?" to "Why was it done, and how was it enabled?" This is a call for a more strategic framework—one that aligns technical signals with geopolitical context, mission objectives, and the human drivers behind the keyboard. It is not about discarding past attribution models, but evolving beyond them to meet the threat where it is today.**

Why Now?

The urgency of this report stems from a sobering reality: critical infrastructure and global supply chains are already compromised. DPRK operatives are not just knocking on the door—they're inside the house. Masquerading as IT professionals, they have embedded themselves within organizations, leveraging trust to gain access to sensitive systems and data.

What powers it is one of the world's most disciplined and covert cyber talent pipelines. For decades, the DPRK has systematically identified and trained promising students from a young age, funneling them through elite technical institutions and foreign placements to refine their skills. Today, these highly skilled operatives are embedded across global workforces, executing missions with precision—advancing state objectives while securing resources and status for themselves and their families. Now amplified by AI, this talent engine is accelerating the threat beyond anything conventional defenses were designed to handle.

The rise of Research Center 227—North Korea's AI-driven cyber division—marks a decisive evolution. Combining human expertise with machine learning, DPRK is now capable of high-velocity operations that dissolve the line between cyber disruption and physical sabotage. From deepfake propaganda to AI-powered suicide drones, the spectrum of threats has widened dramatically.

With operatives on the ground in Russia, AI-assisted suicide drones, and Intercontinental Ballistic Missiles (ICBM) programs advancing, this is no longer just a cybersecurity issue. It's a physical threat with frightening national security consequences. And it's being bankrolled by the DPRK's financially motivated cybercrime operations.

Leaders across the enterprise and government—not just CISOs—must act now to identify and eliminate embedded operatives from their networks.

This report is an urgent call for action, requiring a shift from attribution to full-spectrum threat awareness. Only by mapping the DPRK's operational ecosystem, mission objectives, and personal motivations can we begin to anticipate and disarm an adversary that is using our own systems against us.

This is not a distant threat—it is unfolding in real time, at alarming speed and scale, accelerated by AI.

About This Report

This report is the result of a collaborative effort involving numerous intelligence experts and analysts, who have contributed their insights and research to paint a comprehensive picture of the DPRK's cyber-physical capabilities. DTEX Systems is proud to be the vehicle for information sharing in this important awareness campaign, and grateful for the opportunity to contribute its own investigative findings to the broader community.

The goal of this report is to foster greater collaboration and knowledge exchange among those tracking and combating the DPRK threat.

By bringing together trusted perspectives, we hope to better equip organizations worldwide to proactively defend against the growing and multifaceted threat posed by DPRK operatives.

The findings and perspectives shared throughout this report reflect the collective judgment of the lead author (Michael Barnhart), other contributing experts, and DTEX. References to "we" should be understood in that collaborative context.

Note to the Reader

This report is meant to be more than a briefing—it's a tool for understanding, anticipating, and staying ahead of one of the most complex and underestimated cyber threats of our time.

It's structured to help connect the dots: from the DPRK's strategic objectives and cyber talent pipeline to the operational tactics and human motivations behind its campaigns. Readers are encouraged to move through it with both a strategic lens and a sense of urgency—this is not just about cyber incidents, but about a system designed to exploit trust, infrastructure, and global norms.

Whether in government, enterprise security, or policy, the insights here are meant to sharpen defenses, reframe the threat, and drive smarter, faster decision making. This is an invitation to reassess assumptions, recalibrate approaches, and engage more deeply—because confronting a threat this adaptive demands a response that is just as agile, informed, and unflinching.

Author's Note

I first began tracking DPRK activity in 2016, alongside a small group of individuals who, though not DPRK specialists by training, were drawn to the challenge posed by the Hermit Kingdom's cyber operations. Over time, that interest grew into a broader network—victims, targets, vested interests, and multidisciplinary intelligence professionals—piecing together the regime's sprawling cybercriminal enterprise. Our collective now has decades of experience focused squarely on this threat, with new personnel joining us consistently to join this fight for the greater good.

Written by

Michael "Barni" Barnhart

Lead Author

Principal i³ Insider

Investigator, DTEX Systems

To make this investigation as comprehensive as possible, I compiled open-source intelligence, vetted defector accounts, analysis of cryptocurrency artifacts, and Web3 infrastructure. I also relied on datasets and organic open-source collections obtained through trusted partners—sources that cannot be fully disclosed due to the sensitivity of access or reluctance to be named. I've done my best to synthesize that data here, and although only some sources are linked to this document due to brevity, I encourage readers to consult the full endnotes for trusted, publicly available sources on DPRK cyber activity.

This investigation was not a solo effort. Prior to publication, I consulted with trusted experts in the DPRK space to ensure accuracy, applicability, and multi-source validation. Special thanks to those who prefer to remain unnamed—and to 38 North and Martyn Williams, who can be. I am forever grateful for your time and candor. Special thanks also to DTEX for its critical role as a key contributor, bringing invaluable expertise and support throughout the process. Our affectionately self-named "misfit alliance" of public and private partners remains strong, and we'll continue supporting the U.S. and its allies in countering the DPRK cyber threat.

Lastly, a word of caution: DPRK operatives are persistent and will try to uncover who is studying them and how. They do not take kindly to scrutiny. I've personally accepted that risk, but for newcomers, I urge caution and strong operational security.

DPRK Org Chart

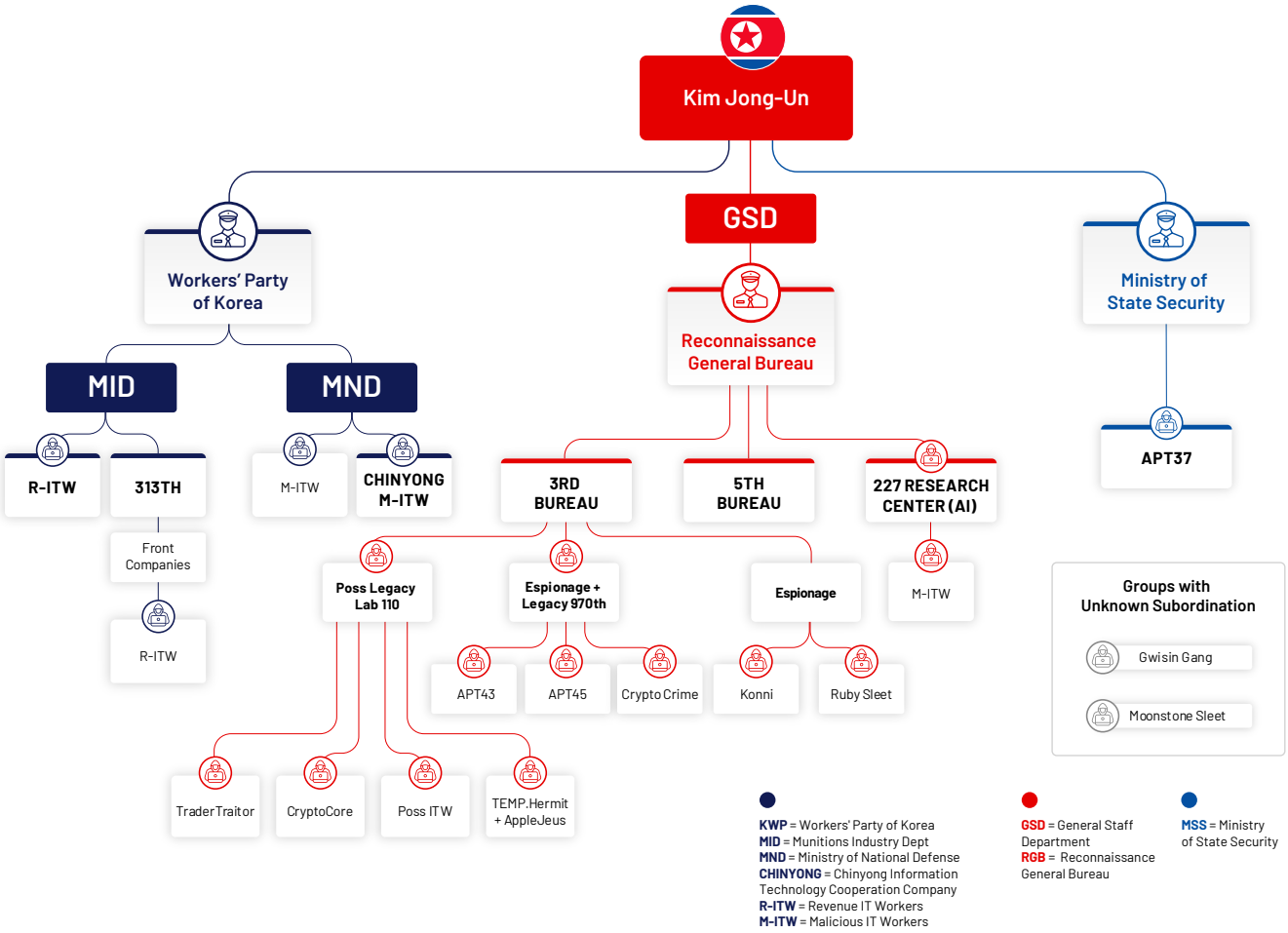


Figure 1. DPRK cyber to physical: Organizational assessment.

Based on 2025 intelligence, this assessed organizational chart provides a comprehensive view of North Korea's cyber structure, highlighting key units like the AI-driven Research Center 227, decentralized offensive cells, and the talent pipeline that supports them. These components will be referred to throughout the report in depth, illustrating how cyber operations are seamlessly integrated with the DPRK's state, military, and financial objectives, and how the system's fluidity allows for rapid shifts in resources and personnel across borders to support a range of missions.

Unconventional Attribution Methods for an Unconventional Program

We have reached a key inflection point for the DPRK cyber program—one that calls for a reassessment of long-held assumptions about its sophistication and capabilities. By embracing less conventional attribution methods, we can open the door to more effective and relevant ways of understanding and thwarting DPRK cyber operations.

When historically tracking the DPRK, we likely never would have predicted that North Korea would be providing men and materials in support of a Russian land war in Europe while having hacked Russian hypersonic missile information just three years prior. Nor could we have foreseen that DPRK operatives would successfully steal over $1.4 billion in cryptocurrency from a single victim. What would have felt impossible for those tracking the DPRK back then is very obviously in the realm of the possible now.

There is no "one size fits all" approach that can be taken when trying to understand the DPRK and its cyber activities. We are a firm advocate of meeting the adversary where they are and learning to adapt as the adversary does. Pyongyang's cyber operations are hardly conventional. The DPRK can chain together multiple supply chain compromises and then seemingly only target cryptocurrency and financial firms, despite having access to thousands of companies worldwide, as noted with the 3CX hack.

DPRK espionage actors not only steal information to further the regime's economic and military goals, but also engage in diverse cybercriminal activities to fund themselves, and more recently, have worked to sway public opinion through propaganda-style efforts. DPRK IT workers (ITW) have gained fraudulent employment at a multitude of Fortune 500 companies and have likely also infiltrated the cryptocurrency space to such a great extent that it would seem that every other Web3 project has a North Korean on the payroll.

At the same time, discussions in both the public and private sectors have focused on defining what truly constitutes DPRK malicious cyber activity, determining the significance of certain subgroups, and deciding when to cluster or uncluster subsets of activity.

Protecting our organizations and critical assets from DPRK operatives requires a deep reset in how we think about the threat in the first place. This starts with unpacking what the DPRK is not.

Rethinking the DPRK: Correcting Misconceptions

Before we dive in to how we understand the DPRK cyber program, let's consider a few standard assumptions that are all too common in the DPRK watcher community.

1. First, the most sophisticated DPRK APT is TraderTraitor, and TraderTraitor only conducts cryptocurrency thefts, right? Not quite. Actors likely associated with TraderTraitor have been mobilized for ad hoc cyber espionage efforts targeting the defense industrial base. Therefore, comparing TraderTraitor to groups such as TEMP.Hermit may not be entirely productive.
2. The second assumption, that roles within the DPRK cyber program are as rigid as the regime that sponsors it, and we would never see people changing jobs the way they do in the West. This is not the case, as observed infrastructure changes reflect operatives shifting between APTs and missions. Former APT operators seemingly shift to managerial roles over IT teams, and APTs brokering animation jobs to help programmers raise illicit funds for Pyongyang.
3. Lastly, the actors that we tracked over a decade ago are surely doing something else now, right? Whatever happened to Park Jin Hyok? While we can't definitively place specific individuals and personas, we assess that the regime is unlikely to cast aside a generation of successful operatives just because they got older—these operatives are likely professors, advisors, and managers now (and they're probably still using the same personas with some mention of Zeus, Panda, Simba, Hades, Helios, etc.).

Figure 2. This image shows two IT workers, personas "Naoki Murano" and "Jenson Collins", who were relocated from Laos to Vladivostok, Russia. Related information has been passed on to the appropriate authorities. Naoki, left, is associated with the DeltaPrime Heist of $6 million USD. Both are suspected to be associated with Chinyong related IT worker efforts.

Clearly, the DPRK's cyber program is a more complex organization than traditional cyber threat intelligence methods can adequately capture. An intelligence professional once advised to "stop looking at North Korea's cyber program as a government program like the other major state programs and liken them to a single-family mafia organization and the lines begin to unblur." This frame has aided in the understanding of this nation state.

Given the unconventional nature of the DPRK cyber ecosystem, we need to be unconventional in our approach to understanding it if we have any hope of stopping their activity.

Mapping the DPRK's Cyber Strategy

Since 2020, tracking DPRK cyber threat activity has become increasingly difficult compared to other top-tier state-sponsored threat activity such as China, Russia, and Iran. Compared to other cyber programs, Pyongyang makes much more frequent changes to structure and unit designations, realigning and creating new units to support North Korean leader Kim Jong-un's stated priorities and respond to global events. North Korea's limited internet access and highly regimented training pipeline for future cyber actors also sets it apart from other programs, with selected personnel training for future roles in cyber units from a very young age.

The DPRK's cyber program is therefore best understood in terms of the program's key mission areas, capabilities, and overarching organizations that sponsor cyber activity.

Mapping DPRK cyber activity against the regime's stated objectives is key to understanding, tracking, and proactively disrupting Pyongyang's operations.

We group the regime's priorities for the DPRK cyber program into the following key areas:

- Cyber espionage to support regime, economic, and military development goals, including the Weapons of Mass Destruction (WMD) program.
- Development of disruptive and destructive cyber attack capabilities for use in a wartime scenario.
- Domestic and international counterintelligence and surveillance.
- Revenue generation.
- Traditional foreign intelligence collection, especially targeting the U.S. and the Republic of Korea (ROK).
- The strategic placement of personnel for "knowledge theft"—focusing on skills-based training to replicate the mindset and capabilities of talented individuals in creating innovative products and services that benefit the regime.

New Day, New Tactics: Keeping up With the Regime

We assess with high confidence that Pyongyang frequently authorizes changes to the structure and mandate of individual cyber units to ensure that the unit's activities are aligned to the most critical regime objectives. Kim Jong-un frequently signals his priorities for economic and military development in his annual addresses to the Korean Workers' Party (KWP) plenary meetings. After his addresses, we have consistently observed the cyber program's units quickly shifting to new mission areas in line with Kim's statements. For example, in 2024, we observed clusters of activity from multiple North Korean cyber groups shift from their normal mission set to steal information that would allow the DPRK to meet the stated goals of Kim's 20x10 policy—a plan to build local industrial "modernized factories" in 20 cities and counties per year over the next 10 years.

The Talent Pipeline: Cultivating DPRK's Cyber Syndicate

In addition to frequent personnel realignments, DPRK also recruits talent differently from other state-sponsored threat actors. Rather than relying on domestic cybersecurity contractors, former military cyber operators, or cybercriminals, the DPRK selects promising elementary school-age children who demonstrate proficiency in science and math for training to become military cyber threat actors or regime-sponsored IT workers. These students then move through a pipeline of prestigious schools and universities and receive benefits for themselves and their families, such as relocation to Pyongyang and additional rations.

The training pipeline almost certainly diverges once these students reach university, when the best students are selected to study computer science and hacking at the country's best universities in Pyongyang. Upon graduation, they are either commissioned as officers in the Korean People's Army (KPA) and assigned to the Reconnaissance General Bureau (RGB) or are selected to join one of many IT-focused organizations subordinate to the Munitions Industry Department (MID) or Ministry of National Defense (MND).

Figure 3. A mural in the courtyard of the Kumsong Academy complex depicts Kim Il Sung and Kim Jong-un smiling alongside students working on computers.

Assessed Talent Pipeline

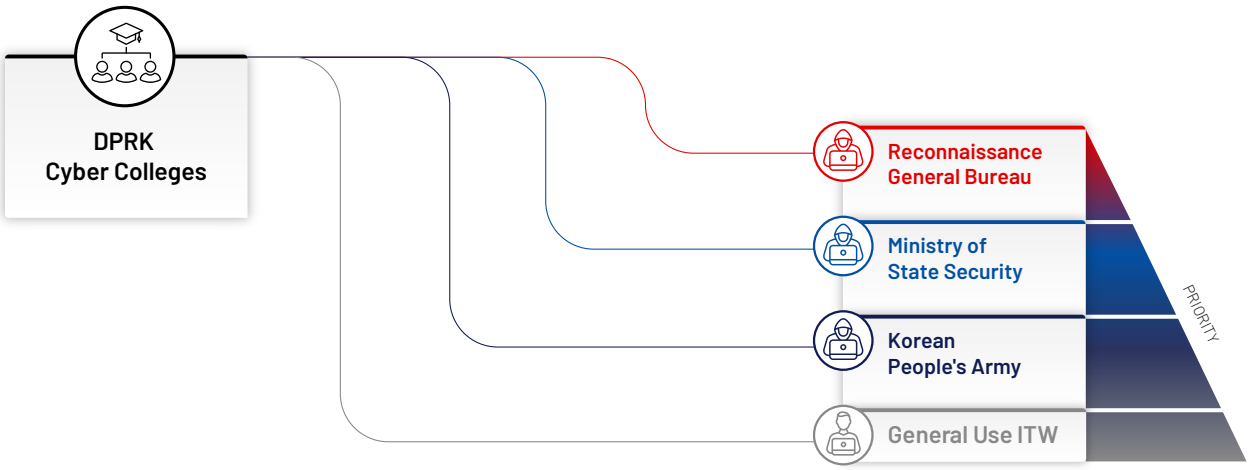


Figure 4. Assessed DPRK cyber talent pipeline based on our collective analysis.

Survival at Stake: The Pressure of DPRK Cyber Quotas

The regime sets annual earnings quotas for both cyber and IT teams, and notably, each cyber organization must fund themselves while also meeting their revenue generation goals. These earnings goals are rigid and force North Korean workers to constantly adapt and seek new means of generating income. These quotas also foster a culture of competition within teams, with workers seeking to gain advantages over their colleagues to receive favors and be allowed to send more money back to their families. In 2025, North Korea doubled the monthly quotas for overseas workers based in China, suggesting that the regime might be imposing similar requirements on cyber and IT units even after TraderTraitor actors stole $1.4 billion from cryptocurrency exchange Bybit.

Figure 5. This image depicts Rim Jin Hyok, an APT45 operative indicted by the U.S. for his role in the Maui ransomware attacks targeting U.S. healthcare entities.

We assess that these quotas are probably one of the primary driving forces behind DPRK cyber actors and ITWs' changes in focus over the last five years, and the continued diversification into new types of cybercrime. All forward-deployed and domestic teams are required to self-fund, meaning that all their operational infrastructure, utilities, and salaries are derived from what they can earn, rather than money received from a central authority in Pyongyang. Historically, this self-funding activity has involved everything from ATM scams to ransomware and even in some cases subcontracting of IT work to non-North Korean individuals. Much of this activity falls below the threshold where it would be formally tracked and reported as attributable to North Korea, complicating our understanding of what activities these groups undertake.

The Rise of Side Gigs

It appears that Pyongyang is also catching on to the potential windfall that would accompany more units' involvement in cybercriminal activities beyond merely permitting these groups to steal enough money to keep the lights on. Reporting indicates that the regime has been authorizing "side gigs" and new missions, suggesting that we may see more North Koreans experimenting with cybercriminal operations to meet their quotas.

According to a blog on Moonstone Sleet actors—whose malware bears some similarities to historic TEMP.Hermit malware—using the Qilin ransomware gang's payload to compromise several targets. This is one of the first reported instances of a North Korean threat group working with another cybercriminal outfit to conduct operations, suggesting that their mandate may have been expanded based on their successes over the last few years.

DTEX Insider Intelligence and Investigations (i^3) has identified that North Korean IT workers frequently hold multiple remote positions, balancing personal financial gain with state-directed objectives.

These workers have been observed using corporate infrastructure as bastion hosts to carry out non-work-related activities linked to their side gigs. Such activities include creating sock puppet accounts on freelance platforms (e.g., Upwork, Fiverr, etc.) to secure additional work, recruiting facilitators, and engaging in money laundering and cryptocurrency operations that would typically be restricted by regional controls.

See the In Focus: IT Workers section for more information.

Navigating DPRK's Cyber Ranks

The DPRK's cyber program has rapidly evolved since the Sony Attack in 2014, suggesting that the original operators tracked as APT38/Lazarus/Hidden Cobra have similarly aged up in the ranks. These individuals are very likely to be middle to senior managers of cyber units and IT teams, judging from defector reports of computer science career progression. If true, these individuals are assessed to have certainly brought the knowledge and tools developed over the course of their careers to their new units. This would partially explain why so many North Korean threat groups have shared infrastructure, malware, and missions today.

These former cyber actors may also remain in communication, sharing knowledge across teams and organizations even if the regime does not formally allow such communication. We specifically noticed this with APT45, where APT managers seemed to have communication or oversight of IT teams.

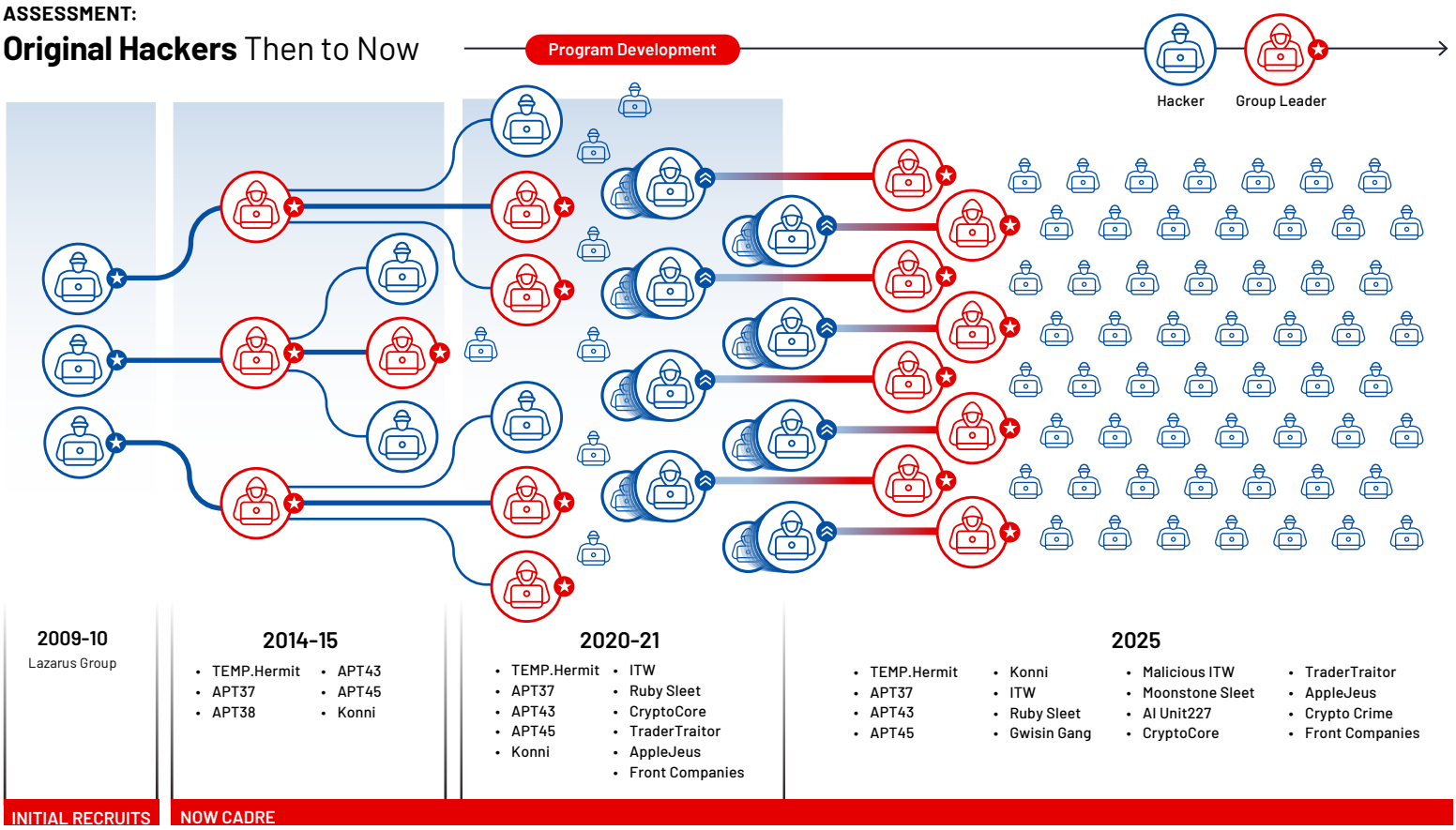


Figure 6. DPRK APT groups over the years.

Advancing the Regime Through Information Sharing

Alongside the likely movement of former Ministry of State Security (MSS) and RGB cyber operatives into managerial roles, North Korea's cyber units may also benefit from insights gleaned from overseas workers; information from their employers and skills acquired through work experience may be gathered on any topic that may benefit the regime and remitted to North Korea on a consistent basis.

While the bulk of this data is likely irrelevant to cyber operations, it is assessed that some of the information sent back to Pyongyang may highlight vulnerabilities and access vectors to targets of interest to the cyber program, even if the overseas workers are unwitting of its ultimate use. DPRK IT teams are required to report their projects and earnings up their managerial chain on a regular basis and keep detailed records of their work, which may provide additional insight for hacking teams if they are able to access these reports.

The Family Lens

It is also important to understand how interrelated many of the North Koreans in cyber units and IT teams are—having attended the same schools from a young age, often coming from privileged families in Pyongyang, or marrying into each other's families as they complete mandatory service, overseas tours, and formally join the KWP.

Upward mobility in the North Korean system requires KWP membership and marrying well, so it is possible that these individuals may share information or operational infrastructure that will give their relatives or families a comparative advantage over others in their units.

Exploiting Insider Access: Lessons in Vetting and Monitoring

Hypothetically, a North Korean cyber unit with access to information collected by an IT team specializing in blockchain freelance work could obtain critical information about code vulnerabilities and project teams to target in a future cybercrime operation. Even if this rarely occurs, the possibility highlights the importance of carefully vetting employees and understanding who has access to an organization's information. The average North Korean overseas worker may not be formally trained to hack or use their insider access, but it is possible that the information they collect from an organization may be received and operationalized by an extremely capable North Korean cyber unit. In the limited cases we've observed where IT workers attempt to extort their former employers, they allude to this exact scenario in their threats.

The Cutthroat Reality of the DPRK

The DPRK cyber ecosystem could be best described as a "dog eat dog world," where the only real winners are Kim Jong-un's family and the North Korean elites who benefit from the luxury goods that are likely purchased using funds generated by the cyber program.

The average North Korean threat actor or IT worker almost certainly keeps less than 20% of their earnings; like other criminal syndicate models, there are supply chain costs that need to be accounted for. In one partnered effort, intelligence showed that of the $5,000 USD earned per month for the IT worker, only $200 could be kept. We have never seen indications that North Korea's best cybercriminal units like TraderTraitor or AppleJeus get to keep any of the billions in stolen cryptocurrency that they've generated over the years. They only ever keep enough to buy a server or register a domain for the next operation.

Judging from the hours TraderTraitor operatives keep when laundering their post-heist hauls on the blockchain, they may work up to six days a week for 16 hours or more, with limited breaks in between tasks. Compared to the four- or five-day average work week in most Western countries, it's not hard to see how the North Koreans are able to evade even the most proactive governments and organizations.

We have never seen indications that North Korea's best cybercriminal units like TraderTraitor or AppleJeus get to keep any of the billions in stolen cryptocurrency that they've generated over the years.

Spotlight: Operational Security Lapses Reveal Hidden Patterns

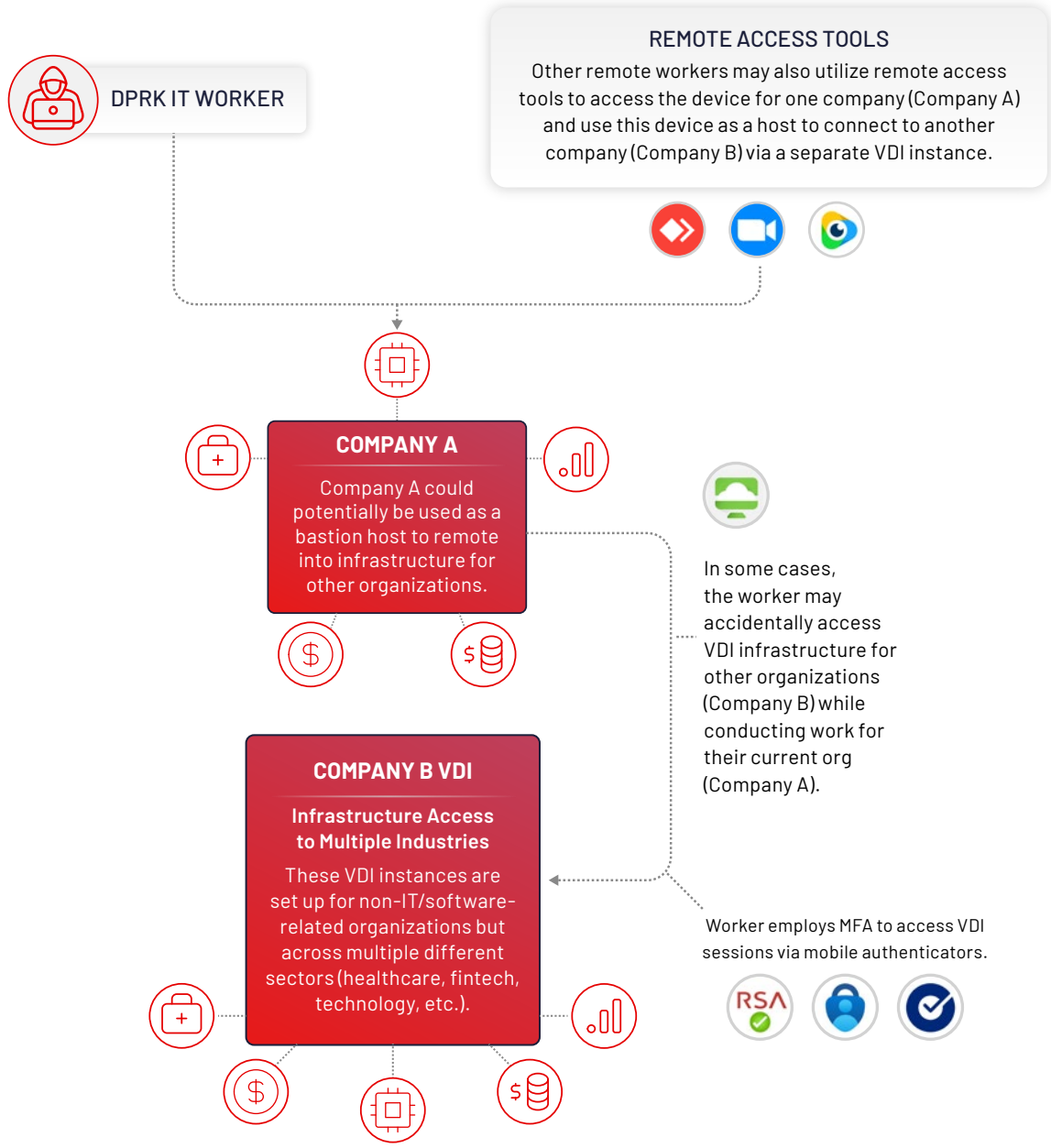


Figure 7. DPRK OPSEC lapses.

Despite their sophistication, DPRK operatives often exhibit critical operational security (OPSEC) lapses. In multiple instances, actors have used the same or similar credentials across entirely separate victim environments—unwittingly linking their false identities across employer networks. These mistakes, observed during active operations, suggest fatigue or inexperience in maintaining cover. Many operatives are overextended, working far beyond standard hours, which may contribute to these errors. Such lapses offer rare windows into true identities, intentions, and the underlying human vulnerabilities within an otherwise disciplined ecosystem.

The Human Cost: When Betrayal is Rewarded

And it's not just "dog eat dog" because the units work terrible hours, in poor conditions, while competing with their colleagues to steal the most money or information. The system also incentivizes reporting colleagues for "unpatriotic" behavior and using every advantage to stay on top, with little regard for the impact that may have on them and their families. We assess that some North Korean teams have probably stolen from other North Koreans, even if they didn't realize they were stealing from a compatriot.

With the amount of North Korean activity targeting software and blockchain developers on sites like Github and LinkedIn from groups like CryptoCore and those conducting the Contagious Interview campaigns, it's very likely that North Korean developers masquerading under a different nationality or pseudonymous usernames have been targeted and ultimately victims of these groups' operations (similar activity also echoed in IT worker activity).

We have moderate confidence that there is little to no formal deconfliction between cyber units, with multiple APT groups and IT workers operating against the same target, especially if that target possesses large amounts of cryptocurrency or sensitive information important to the regime.

For example, as of 2023, APT37, APT43, and two hybrid mission clusters of DPRK activity were all actively targeting North Korean defector Lee Min-Bok, who defected in 1991 and previously worked for the Agricultural Research Institute in Pyongyang. As recently as February 2025, there has also been overlap in high-profile cryptocurrency targets, with both TraderTraitor and Contagious Interview campaigns (hereafter referred to by my proposed name of Gwisin Gang) targeting Bybit in seemingly separate operations.

DPRK: Missions

To advance a collective understanding of the distinct missions of the DPRK's cyber program, we outline below the primary objectives of the program (listed alphabetically, because we cannot confirm the regime's specific prioritization or resourcing of these missions) and the groups we assess are aligned to these missions. These missions are assessed to be relatively stable while the unit designations and personnel supporting each mission may move between missions on a much more regular basis than was previously understood. Between 2021 and 2025, we have observed evolutions consistent with this, including the rise of hybrid groups and numerous instances of multiple groups targeting the same victim.

We also want to highlight that DPRK's cyber program probably houses at most a few hundred skilled operators—far fewer than the 7,000+ personnel figures often cited. These higher estimates likely conflate actual APT operators with a much broader ecosystem that includes IT workers, internal developers, analytic arms, logistical support staff, and front company facilitators. In reality, becoming a trusted APT operator in North Korea requires years of rigorous vetting, including familial and political ties. Operators frequently rotate across missions or go dormant for extended periods, as we've observed in our tracking of personas like Zeus, Simba, and Hades moving between APT groups. These patterns strongly suggest that the core of trained, mission-ready hackers is much smaller than commonly assumed.

The AI Mission

We define the AI mission as activities in support of North Korea's development of their own indigenous artificial intelligence (AI), AI use in support of cyber operations, and AI research generally. On March 27, 2025, after the announcement of the new Research Center 227, North Korean state media announced the launch of a new AI-equipped suicide drone. The report stated that North Korean leader Kim Jong-un supervised tests of new AI-equipped suicide drones, marking a significant advancement in the nation's military capabilities. These drones, designed for precision strikes, utilize artificial intelligence to autonomously identify and engage targets, enhancing their effectiveness on the battlefield. State media reported that Kim emphasized the importance of prioritizing unmanned systems and AI technologies in modernizing the armed forces. To further the point of blended operations and how each part plays into the larger system, trusted partners and investigations noted APT groups such as TEMP.Hermit, Ruby Sleet, and likely APT45 elements had drone-specific targeting and interests. From a timeline perspective, this activity was done concurrently as IT workers associated with Kim Chaek University of Technology conducted detailed research on specific laser, drone, and drone detection technologies.

On March 27, 2025, after the announcement of the new Research Center 227, North Korean state media announced the launch of a new AI-equipped suicide drone.

Research Center 227

Research Center 227 is a newly established North Korean cyber warfare unit focused on the development of advanced hacking technologies, particularly those leveraging AI, to enhance the DPRK's offensive cyber capabilities.

Located in Pyongyang's Mangyongdae District, Research Center 227 operates continuously, enabling real-time responses to intelligence gathered by RGB-affiliated hacking groups deployed overseas.

This organization is based in very close proximity to Kim Sung Il Military University and the Kumsong Academy (more information on these two colleges in the Overarching Units and Colleges section), two of the most elite computer science-focused schools in Pyongyang, which feed the cyber talent pipelines for the APT groups. **Other key institutions fueling the DPRK's cyber talent pipeline include Mirim College and Kimchaek University of Technology, the latter of which has been directly observed supporting the sanctioned Korea Ryonbong General Corporation.**

The center has recruited approximately 90 computer experts, including top graduates from major universities and doctoral programs, specializing in areas such as program development, automation systems, and information security.

The primary objectives of Research Center 227 include creating techniques to neutralize security networks, developing AI-based information theft technologies, hacking financial assets, and establishing automated programs for information collection and analysis.

This initiative underscores DPRK's commitment to strengthening its cyber warfare capabilities, aiming to neutralize foreign cybersecurity systems, steal sensitive information, and disrupt computer networks.

Figure 8. Kim Il Sung Military University.

Research Center 227: Three Hypotheses

We have developed three competing hypotheses to explain why the regime has created Research Center 227 now, with one (number three) leading the charge:

1. The Research Center 227 staff are IT workers specializing in AI-related freelance work. This organization could be the new designator for this clustering of IT workers in AI roles.

2. Research Center 227 is providing 24/7 support to ongoing cyber operations while conducting AI research. The center is supposed to aid in DPRK offensive operations and may also engage in hacking. Research Center 227 staff could be tasked with providing AI-related support to operations, such as using AI to create phishing lure documents, fake IDs, etc.

3. The most likely theory is that Research Center 227 will support all AI-related objectives for the regime, APTs, and IT workers. As we have seen with China's AI model, each country is pioneering into this industry with the efforts to create a model internally, and this would be consistent with North Korean "Juche" self-reliance philosophy.

The presence of skilled IT workers embedded in AI organizations globally—alongside clear concerns about being isolated from external technologies and an inability to rely on foreign AI systems if cut off—strongly indicates the underlying motive behind this group's formation. Developing a domestic AI capability is likely a calculated move to ensure operational continuity and strategic advantage.

The Crypto Mission

It is widely reported that the DPRK has units that specialize in cryptocurrency theft, particularly after the SWIFT network hardened to prevent further bank heists like APT38's $81 million heist from the Bank of Bangladesh. Since cryptocurrency theft and cryptocurrency-related cybercrime are so lucrative, nearly every DPRK group we track has dabbled in cryptocurrency operations at some point in their history, even if these operations were limited to providing funding for other mission areas. For the sake of brevity, we detail the primary crypto-targeting groups here.

TraderTraitor (a.k.a. Jade Sleet, UNC4899)

TraderTraitor is a designation used by U.S. authorities, including the Federal Bureau of Investigation (FBI), and the likely leading element in the restructuring and seeming death of the APT38 mission. This group has been implicated in significant cryptocurrency thefts, notably the $1.4 billion heist from the Dubai-based cryptocurrency exchange Bybit in February 2025 and the $625 million theft from Axie Infinity in March 2022. In the Bybit heist, TraderTraitor actors exploited vulnerabilities during routine wallet transfers, manipulating transaction processes to redirect substantial funds to addresses under their control. Additionally, in May 2024, they were responsible for the theft of approximately $308 million from Japan-based Bitcoin.DMM.com, employing sophisticated social engineering techniques to gain unauthorized access. Post Bangladesh heist, APT38 appeared to fracture into TraderTraitor and CryptoCore, and took on the new face of financial theft for the regime, cryptocurrency, and blockchain efforts. TraderTraitor is arguably the most prolific of any of the DPRK APT groups when it comes to cryptocurrency theft and seems to have housed the most talent from the original APT38 effort. TraderTraitor has also conducted cyber espionage operations against defense industrial base targets, furthering the idea that DPRK watchers need to focus on missions to not be fooled when a cluster seems to have "gone rogue" and targeted an element that appears anomalous to the defender.

"North Korea's cyber operations remain a multifaceted challenge—blending espionage, system intrusions, theft, and fraud in uniquely adaptive ways. Until our response matches their agility and coordination, they will continue to harm people, companies, and organizations around the globe."

Taylor Monahan (a.k.a. Tayvano)
Crypto expert, MetaMask

AppleJeus (a.k.a. Citrine Sleet, Gleaming Pisces, UNC1720, UNC4736)

AppleJeus has been active since at least 2018 and is probably an outgrowth of the TEMP. Hermit intrusion set. AppleJeus primarily targets the cryptocurrency industry with the objective of stealing digital assets to support the regime's financial needs. The group employs tactics such as spear-phishing emails and fake cryptocurrency trading software to infiltrate systems and steal funds. AppleJeus was responsible for the theft of $50 million from Radiant Capital after an extended social engineering campaign targeting multiple Radiant employees. Like TraderTraitor and CryptoCore, AppleJeus emerged following the increased attention brought by the Bangladesh Bank heist and challenges related to stealing and laundering traditional currency. Compared to these groups, however, AppleJeus has a slower operational tempo, preferring to conduct lengthy social engineering operations that enable access versus less discriminating targeting. In March 2025, an established cryptocurrency security researcher's accounts were revealed to belong to AppleJeus, demonstrating the insidious nature of the threat they present. While the group's malware tools overlap with those of the TEMP.Hermit mission, their targeting profiles differ, suggesting likely same operators under the ever-incestuous Lab 110 or 110 Research Center, but with distinct operational goals.

CryptoCore (a.k.a. CageyChameleon, CryptoMimic,DangerousPassword, LeeryTurtle, Sapphire Sleet)

CryptoCore has been active since at least 2018, likely splitting out of APT38 with TraderTraitor. CryptoCore has primarily targeted cryptocurrency exchanges in the U.S., Israel, Europe, and Japan. Although not as advanced as TraderTraitor, this group is extremely effective and stolen hundreds of millions of dollars in digital assets since we began tracking it. The group's modus operandi involves spear-phishing attacks to gain initial access, which often include masquerading as venture capitalists, followed by infiltrating networks to exfiltrate cryptocurrency wallets.

Moonstone Sleet (a.k.a. Storm-1789)

Moonstone Sleet has been active since at least 2023 and has notable overlaps with historic TEMP.Hermit Comebacker malware. Moonstone Sleet conducts financial operations targeting cryptocurrency and has developed its own strain of ransomware called FakePenny. More recently, Moonstone Sleet actors have also been observed collaborating with the Qilin ransomware-as-a-service group, suggesting a broader role in the cybercriminal ecosystem. Notably, Moonstone Sleet also conducts defense-related espionage against the aerospace sector. We do not know Moonstone Sleet's current organizational subordination.

In a sensitive image that has been withheld, but been passed on to appropriate authorities, a likely Chinese national acting as a suspected Crypto P2P broker for the Moonstone Sleet group is standing in front of a U.S.-based tech company's logo displayed inside a remote office building in Beijing, China.

Independent reporting assesses with moderate confidence that a separate individual identified as Sin Chong Min, believed to be operating near the DPRK-China border, is managing a network of DPRK IT workers associated with activity attributed to Moonstone Sleet. Investigations upon the release of the Moonstone Sleet group also highlighted the use of an online game—DeTankWar (also referred to as DeFiTankWar, DeTankZone, and TankWarsZone)—as part of the group's tactics. Although the game appeared legitimate and maintained a credible social media footprint, it is assessed to be a fraudulent imitation of the online game DeFiTankLand, utilizing copied branding elements and game play imagery.

The Destructive Mission

North Korea probably maintains a destructive cyber attack capability for use in times of heightened tension or a wartime scenario. Since the 2010s, we have not observed DPRK cyber operatives conducting destructive attacks, although their capability has probably improved during the last decade.

APT45 (a.k.a. Andariel, Jumpy Pisces, Onyx Sleet, Silent Chollima)

APT45 has been active since at least 2009, primarily targeting government agencies, military organizations, and various domestic companies around the world. Their operations encompass ransomware, espionage, and destructive activities, cyber financial operations against ATMs, banks, and cryptocurrency exchanges. APT45 was responsible for the March 2013 DarkSeoul attack, which was a destructive cyber operation targeting major South Korean banks (Shinhan Bank, Nonghyup Bank, and Jeju Bank) and broadcasting companies (KBS, MBC, and YTN). The attackers deployed wiper malware that erased hard drives and rendered thousands of computers inoperable, while also launching DDoS attacks to overwhelm networks. The incident disrupted online banking, ATM services, and television broadcasts, causing significant operational damage. The attack was part of a broader campaign aimed at destabilizing South Korea through coordinated cyber warfare.

In July 2024, the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and international partners released an advisory highlighting the group's global cyber espionage campaign, which targets defense, aerospace, nuclear, and engineering organizations. Additionally, in July 2024, the U.S. Department of State announced a reward of up to $10 million for information leading to the identification or location of Rim Jong Hyok, a leader of a section of the group involved in cyberattacks against U.S. hospitals and healthcare institutions. These developments underscore APT45's significant role in DPRK's cyber operations, blending espionage with financially motivated attacks to further the regime's objectives. Although this group does overlap heavily with espionage efforts, the usage of destructive activities led us to place the organization in this category.

The Espionage Mission

North Korea's cyber espionage mission looks most like other state-sponsored programs, with the objectives of gathering key foreign intelligence and information that will assist the regime. However, unlike other state-sponsored programs, the groups conducting espionage have to self-fund their operations, which has led to these groups dabbling in various types of cybercrime.

APT43 (a.k.a. Black Banshee, Emerald Sleet, Kimsuky, Velvet Chollima)

APT43 has been active since at least 2012. The group primarily engages in cyber espionage, targeting government organizations, research institutions, think tanks, and entities related to nuclear security and foreign policy, particularly those in the U.S. and South Korea. APT43 employs sophisticated social engineering techniques, including spear-phishing campaigns, to harvest credentials and infiltrate networks. Notably, the group is also involved in cybercrime activities, such as cryptocurrency theft and laundering, to fund its espionage operations, aligning with North Korea's strategy of self-reliance. These financially motivated operations enable APT43 to sustain its activities without state funding.

Konni (Opal Sleet, OSMIUM)

The sometimes-conflated Konni Group is a North Korean cyber espionage entity active since at least 2014 that primarily targets Russia. It is known for deploying the KONNI Remote Access Trojan (RAT)—a malware capable of capturing keystrokes, taking screenshots, and exfiltrating data from compromised systems. Although Konni is the name of the malware used and not the name of the group itself, the name did catch on. The group is extremely like APT43, but with slight shifts in Tactics, Techniques, and Procedures (TTPs). This group has primarily targeted government agencies and organizations in South Korea and Russia. For instance, in January 2022, Konni targeted Russian embassy diplomats with phishing emails disguised as New Year greetings, aiming to deliver malware. Additionally, Konni has been observed exploiting vulnerabilities such as the WinRAR flaw (CVE-2023-38831) to disseminate its malware through weaponized documents.

Ruby Sleet (a.k.a. CERIUM)

Ruby Sleet, which was historically known as Bureau 325 and formerly CERIUM, was probably formed by operators of both APT43's Japan-focused team and TEMP.Hermit. Announced publicly in early 2021, the group initially focused on cyber operations related to COVID-19, directly reporting to North Korea's leadership. Over time, its activities expanded beyond pandemic-related targets, encompassing a broader range of espionage operations, much akin to APT45. We do not know whether this unit still exists or if it was reabsorbed by other units after completing its "special temporary project."

TEMP.Hermit (a.k.a. Diamond Sleet, Labyrinth Chollima, Selective Pisces, TA404)

TEMP.Hermit is closely associated with the AppleJeus cluster of activity, but maintains an espionage focus and has been active since at least 2013. TEMP.Hermit primarily targets defense, energy, financial, government, and technology sectors globally, aligning with North Korean strategic interests. Their tactics include spear-phishing with job-themed lures, leading to malware deployment such as MISTPEN, a previously undocumented backdoor. TEMP.Hermit is probably responsible for the Operation DreamJob campaign that targeted defense and industrial job seekers during the COVID-19 pandemic. This group has also targeted security researchers who specialize in vulnerability research, suggesting that TEMP. Hermit may play a key role in developing North Korean malware. This group is arguably the most critical within DPRK cyber operations—serving as the Swiss Army knife of the regime's cyber capabilities and the primary entity behind the conflated "Lazarus Group" label.
It overlaps across all areas of APT activity and now extends into IT worker operations in various forms.

This group is arguably the most critical within DPRK cyber operations—serving as the Swiss Army knife of the regime's cyber capabilities and the primary entity behind the conflated "Lazarus Group" label.

The Surveillance Mission

APT37 (a.k.a. Group123, Reaper, Scarcruft)

This organization is a surveillance-related effort active since at least 2012 and often conflated with similar organizations such as APT43 and Konni due to their likely operator, mission, and targeting overlaps at times. The group's composition, which has been stated by one subject matter expert as a "conglomerate", primarily targets South Korean entities but has also extended its operations to countries including Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other regions in the Middle East. Although this organization shares the same mission focus as the MSS, it is likely to be comprised of multiple organizations. APT37 employs sophisticated tactics such as exploiting zero-day vulnerabilities and utilizing custom malware to conduct espionage and intelligence-gathering missions. Notably, in 2018, APT37 conducted a spear-phishing campaign targeting North Korean defectors and South Korean journalists, employing malware with wiretapping capabilities to monitor victims' activities. Additionally, in October 2023, APT37, along with other North Korean hacking groups, attempted to hack the communications of Lee Min-bok, a prominent figure in South Korea's defector community known for sending propaganda leaflets into North Korea, and focus for multiple DPRK cyber threat actors. These operations underscore APT37's focus on surveilling and disrupting activities related to North Korean defectors and human rights advocates.

The IT Worker Mission

North Korea probably has several thousand IT workers who operate from both inside and outside of North Korea. The IT worker (ITW) mission originally started as a means of revenue generation and sanctions evasion, especially after the implementation of U.S. and U.N. sanctions, but has now grown into an odd blend of "traditional" IT work and malicious cyber activity. It's important to reiterate that the ITW personnel and the cyber operators likely attend the same schools and come from the same families, so aside from more specialized hacking coursework in the latter part of their education, some ITW almost certainly have the skills required to hack, albeit in a less-sophisticated manner.

ITW (a.k.a. UNC5267, Wagemole)

A global network of IT professionals to clandestinely generate substantial revenue for its regime, circumventing international sanctions. These operatives secure remote freelance positions with companies worldwide by misrepresenting their identities and locations, often utilizing stolen or falsified credentials. Earnings from these activities are predominantly seized by the North Korean government, contributing hundreds of millions of dollars annually to fund its weapons programs, including those involving WMD and ballistic missiles. To facilitate these deceptions, intermediaries have established "laptop farms" within the U.S., hosting employer-provided devices to create the illusion of domestic work locations for overseas North Korean workers.

Chinyong IT Cooperation Company

Chinyong is one of many North Korean IT organizations and has been active since at least 2016. Chinyong's teams primarily operate out of China, Laos, and Russia, and are involved in a mixture of "traditional" freelance IT work and cryptocurrency theft using their insider access to blockchain projects. Chinyong and its Russia-based representative, Kim Sang Man, are subject to OFAC sanctions for their funding of North Korean military entities. According to blockchain analysis, Chinyong ITW have stolen and earned tens of millions in cryptocurrency since 2017.

Gwisin Gang (a.k.a. BeaverTail, Contagious Interview, Famous Chollima, Tenacious Pungsan, UNC5342, Void Dokkaebi)

This group probably emerged from an IT organization but primarily conducts malicious activity targeting developers to gain company access versus the longer employment process. This group is associated with the Contagious Interview campaign, and the BeaverTail, InvisibleFerret, and OtterCookie malware. Gwisin Gang threat actors pose as recruiters to target software developers, particularly in the cryptocurrency sector. They conduct fake job interviews, during which they persuade victims to download malicious software, leading to the deployment of this JavaScript-based infostealer and downloader malware, and is capable of exfiltrating data, including cryptocurrency wallet information, from both Windows and macOS systems. To further the point of deconfliction of targets, open-source information indicates that these actors were also targeting Bybit at the same time as TraderTraitor in early 2025.

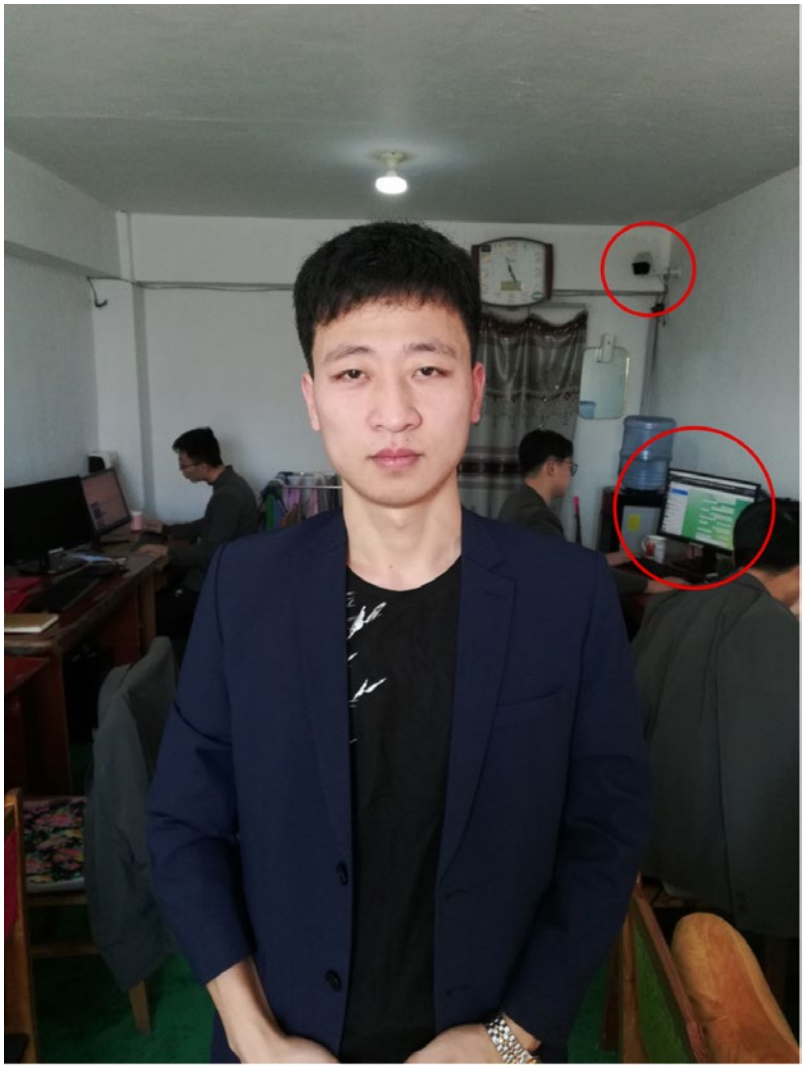


Figure 9. Inside ITW operations.

Figures 9 and 10 detail IT worker operations as one IT worker creates altered IDs and the persona "Benjamin" from the start to finish. Notice the government-monitored camera in the top right, the WhatsApp messaging in use on the IT worker laptop, their working space, and working attire.

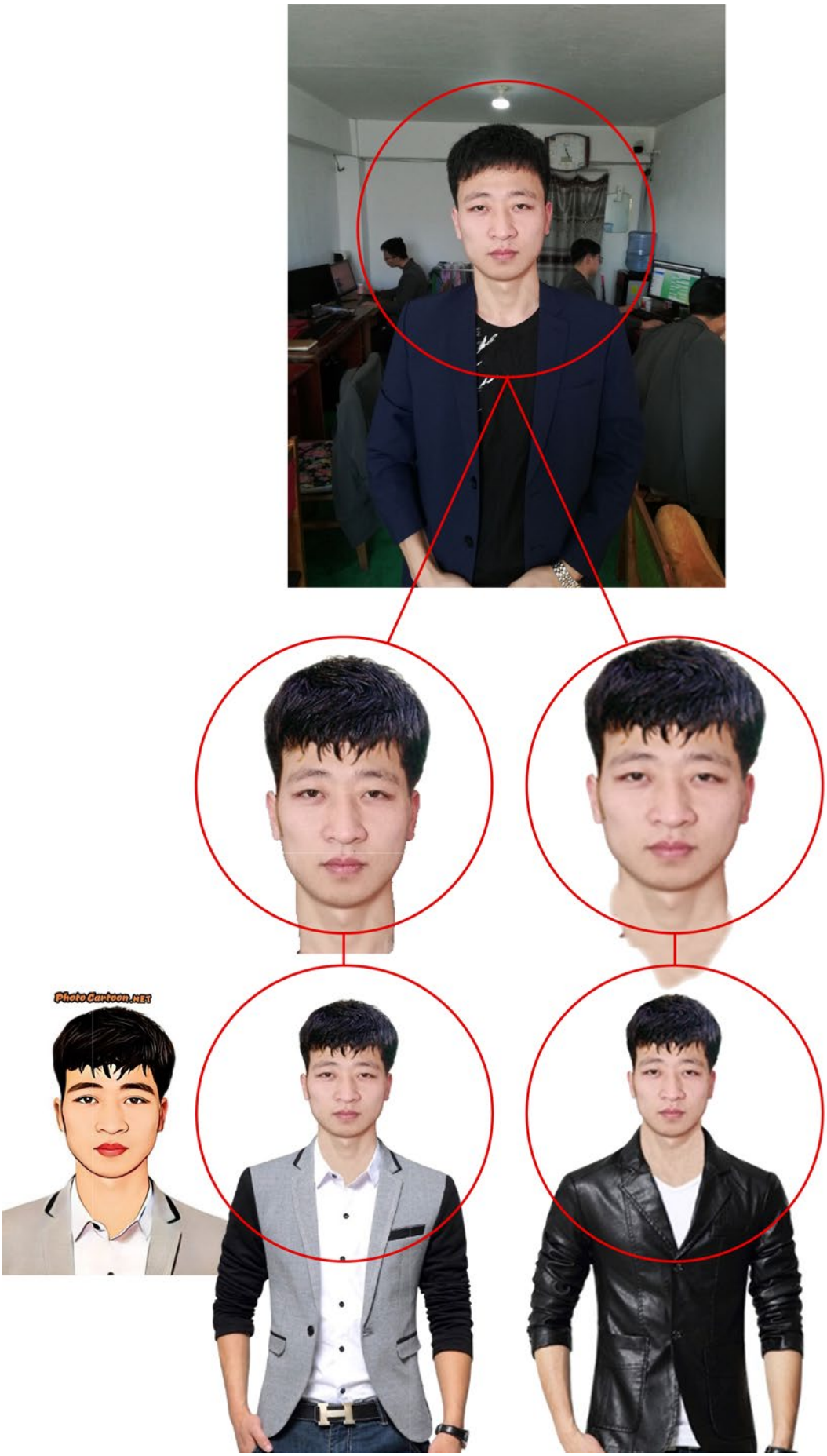


Figure 10.

Administrative notes from a separate team list names and organizational ITW tasking units—including the Department of Education, the 313 General Bureau, and a category labeled "other" which may serve as a placeholder for RGB-affiliated ITW activity. The associated location—Building 10, Gangwan Community, Zhenxing District 118000, Dandong, China—is linked to ITW operations and sits in close proximity to known DPRK APT and ITW infrastructure in both Dandong and across the border in Sinuiju, North Korea.

Name	Netkey_ID	Room no.	Belong to
ChaeJuHyok	stack4world21	409	313
HanGukPeom	hgtiger0620	409	313
RiSongHyok	developer123	409	313
HongKangJin	achilles0314	409	313
WuangUnRyong	wur20011125	409	Educ
SonSuBok	ssb2428	409	Educ
JoHeon	jh1107	409	Educ
PaekUnHyok	puh20020519	409	Educ
KimYongBeom	kyb0614	409	Other
RiKumSong	rks2002	409	Other
OmChungGuk	challenger	409	Educ
LiMyongSong	lms361244	409	Other

Figure 11. Administrative notes link true IT workers to units to a Dandong site near DPRK cyber infrastructure.

In Focus: IT Workers

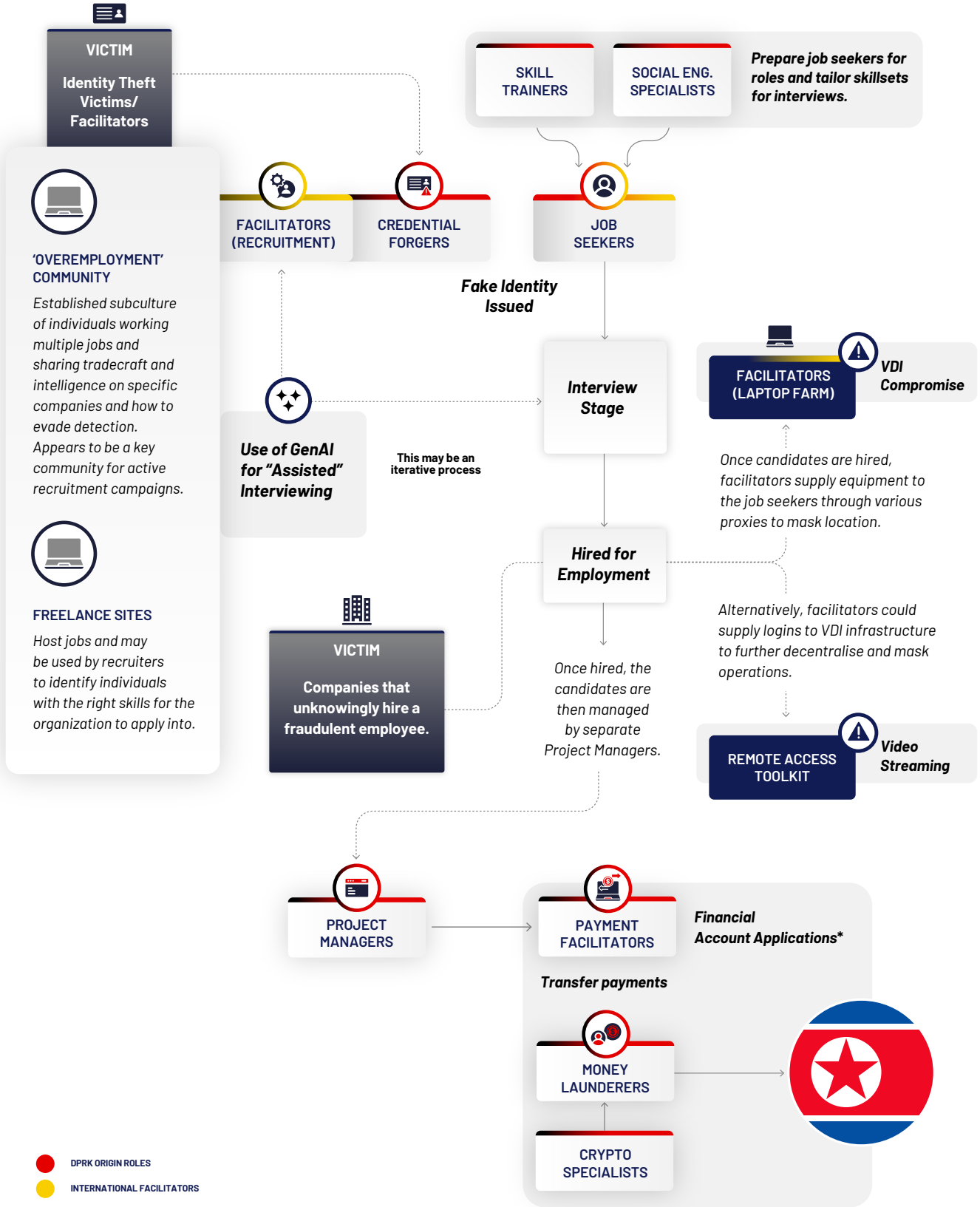


Figure 12. R-ITW: Crime syndicate players.

The methodology flow stems from a revenue-generating IT worker (ITW) team. While this instance was derived from DTEX investigations focused on revenue motives, the framework applies equally to teams driven by intellectual property theft or espionage. It uncovers key intricacies often overlooked by defenders and highlights the criminal nature of these operations.

Identity Theft Victims/Facilitators: Individuals who have had their identity stolen through some compromising campaign (e.g., a hack, physical theft, etc. or individuals who have supplied their identity willingly for monetary gain).

Facilitators (Recruiters): English-speaking freelancers.

> Several DTEX i[3] investigations reveal active recruitment of English-speaking technical freelancers who may knowingly or unknowingly support job seeker and video interview stages.

Facilitators (Laptop Farm): Non-DPRK representatives (e.g., U.S. citizens or front companies). Facilitators may be recruited through a variety of means, including LinkedIn, as in the Chapman indictment.

> DTEX i[3] has observed incidents where a laptop from company A has been used to access the VDI of company B for the purposes of bypassing network restrictions of company B.

Remote Access Toolkit: The facilitators ensure any devices are correctly configured with the necessary software to manipulate companies into believing the legitimacy of the user's identity (e.g., KVM switches, remote access software, virtual webcams, etc.).

> DTEX i[3] has observed incidents where video streaming services are leveraged to facilitate multiple individuals being connected to the same company under a single account.

Use of GenAI for "Assisted" Interviewing: Recruiters or skill trainers may promote the use of GenAI or deepfake tools to assist job seekers in the interview process. This may be to help answer questions to back up the user's fake resume or to help disguise the user's physical appearance to match the fake identity supplied to the organization.

Interview Stage: The interview stage is crucial to embed job seekers into the organization without raising suspicion. This will have to cover a few major requirements to prepare candidates for successful employment:

- **English speaking:** Candidates must have a good English-speaking background to converse comfortably with interviewers in the U.S.
- **Technical knowledge:** Candidates must have the right technical knowledge (as developed by skill trainers or identified through freelance platforms) for the job at hand
- **Soft skills:** Candidates must have strong communication, presentation, and writing skills to appear lucrative for employment

Project Managers: Ensure job seeker completes tasks and avoids suspicion.

Financial Account Applications: Used by payment facilitators/launderers to funnel funds through various accounts, especially through the use of cryptocurrencies to bypass sanctions.

Money Launderers: The money launderers may communicate with other cryptocurrency or avoidance specialists to bypass any sanctions and convert funds, or they themselves could be experts in this.

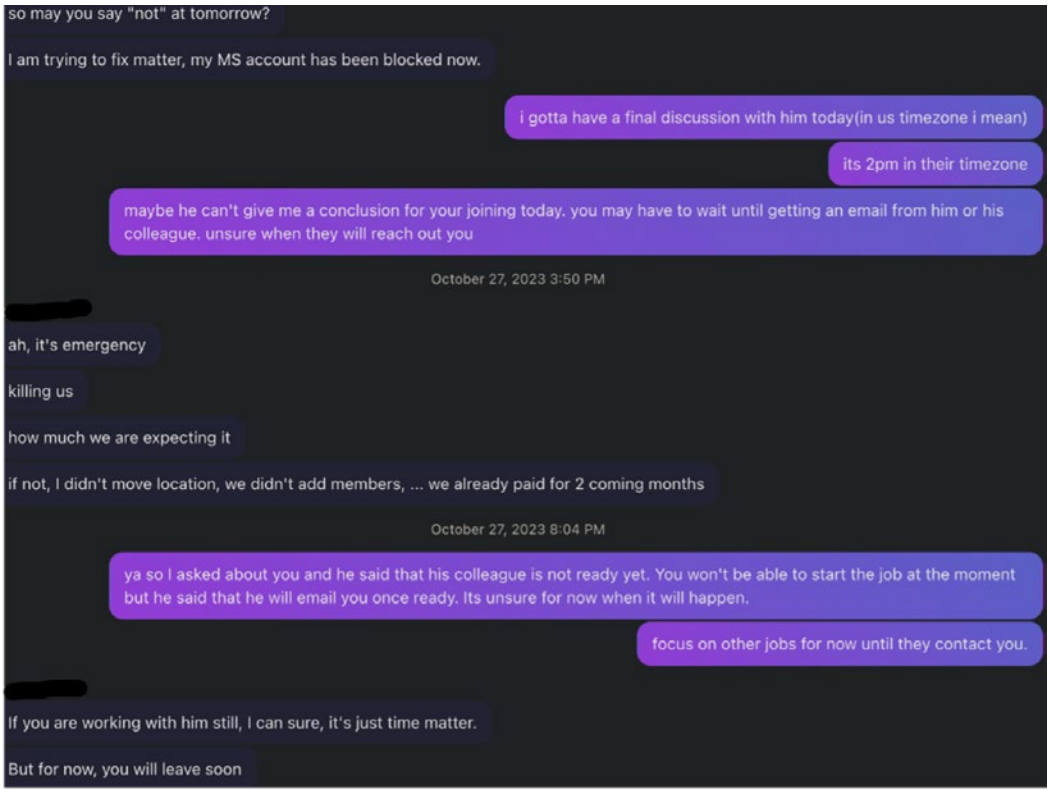
Behavioral Indicators Reveal Non-State Facilitators in DPRK ITW Activity

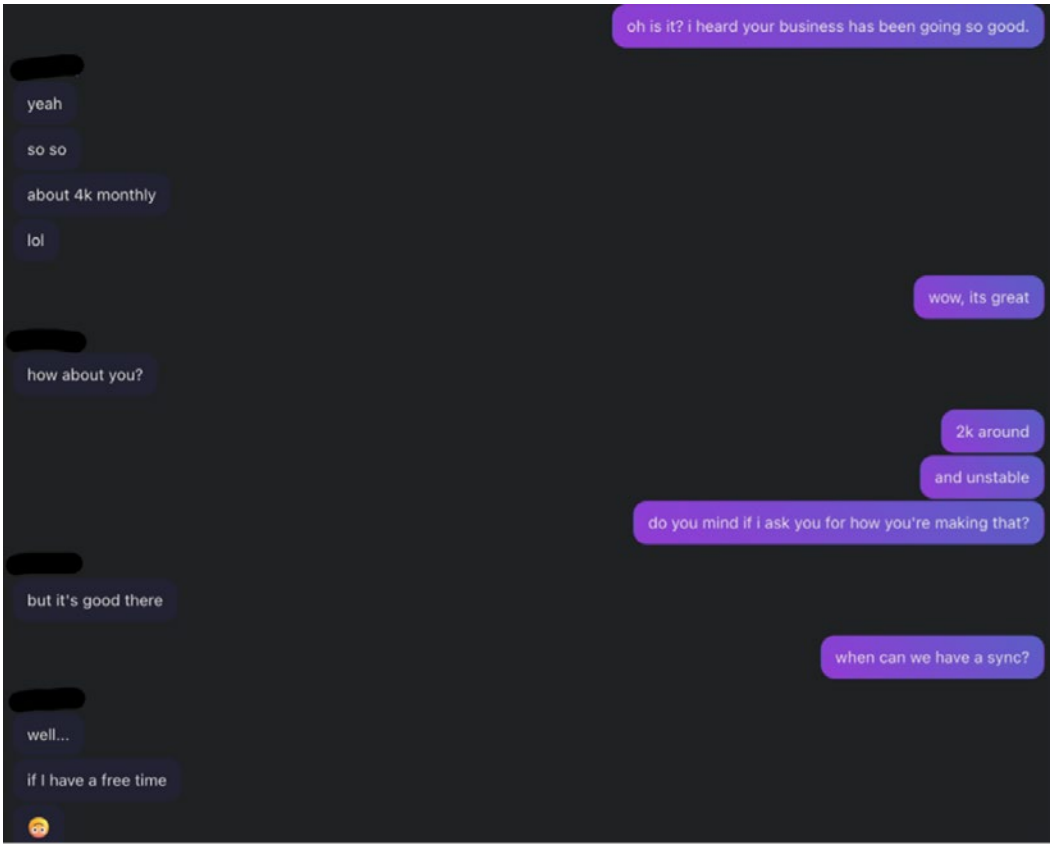
DTEX Insider Intelligence and Investigations (i^3) analysis has determined that a singular focus on APT attribution risks overlooking key elements of DPRK's ITW operational schemes. Notably, many facilitators involved are not DPRK operatives, but third-country individuals motivated by financial gain rather than ideological alignment with the regime.

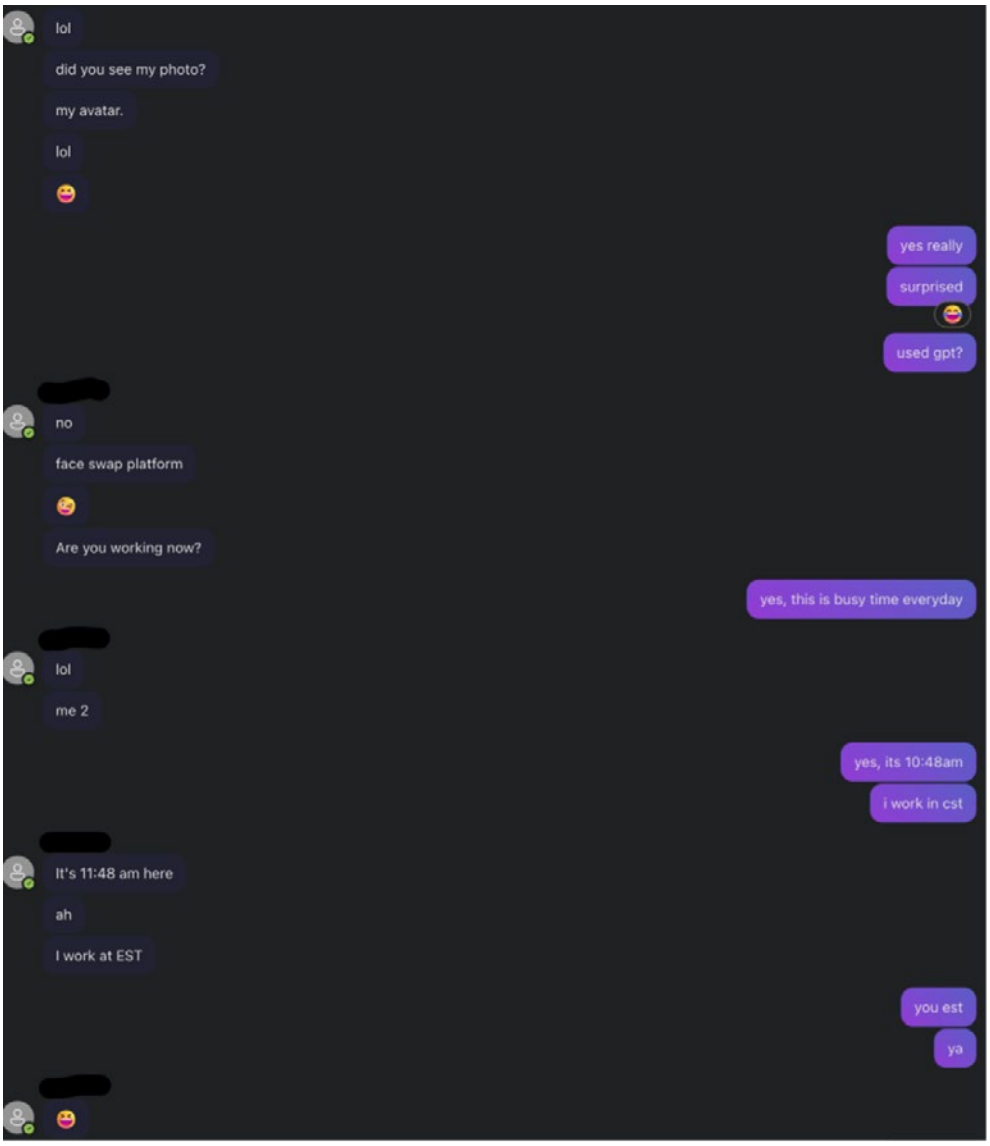
Behavioral signals—particularly those observed post-pandemic within the Overemployed community—enabled early identification of DPRK-linked ITW activity. These indicators surfaced well before traditional attribution processes confirmed state involvement.

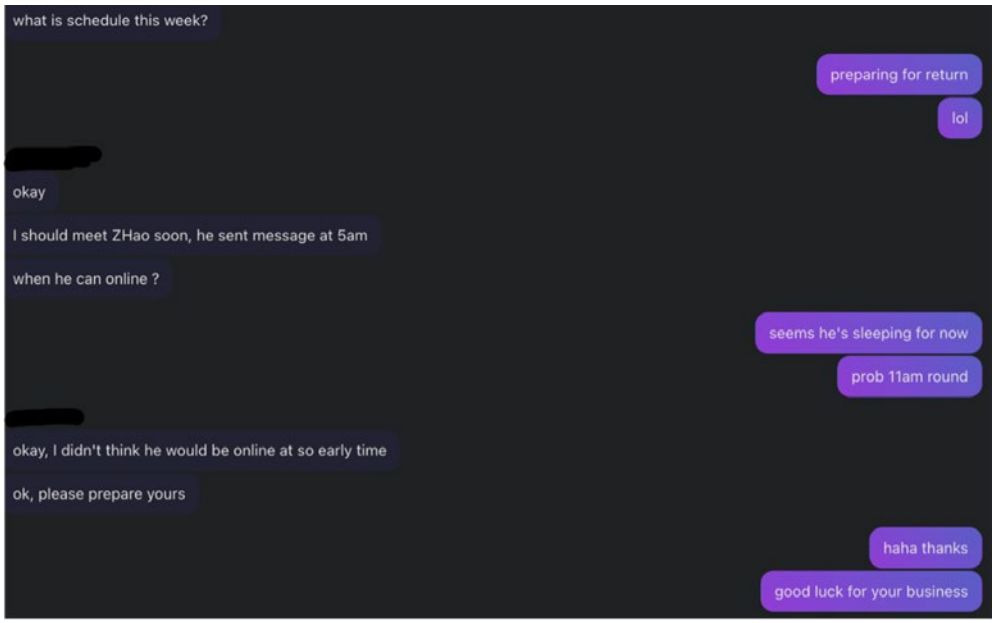
Viewing DPRK cyber operations through a behavioral lens, rather than a conventional APT framework, allowed for earlier detection, a deeper understanding of intent, and exposure of a broader network of enablers beyond known TTPs.

The below graphics detail the day-to-day communication and coordination of operations between members of related ITW teams in 2023. It is assessed that when communicating with external ITW teams, a continuance of their relationships in training and in school persists.

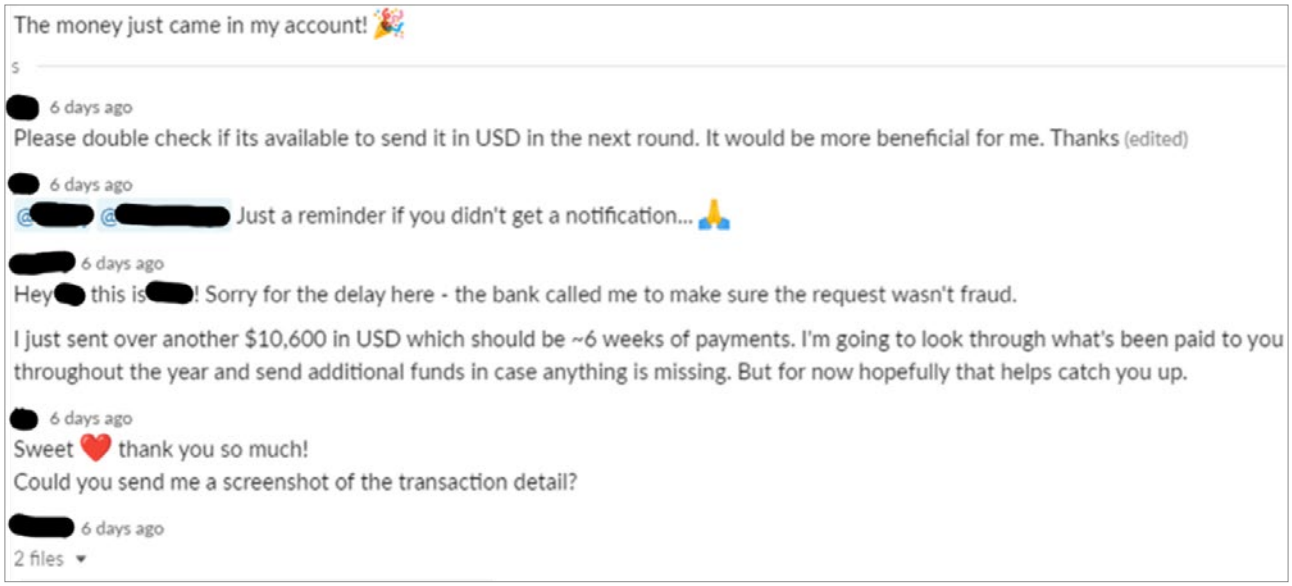


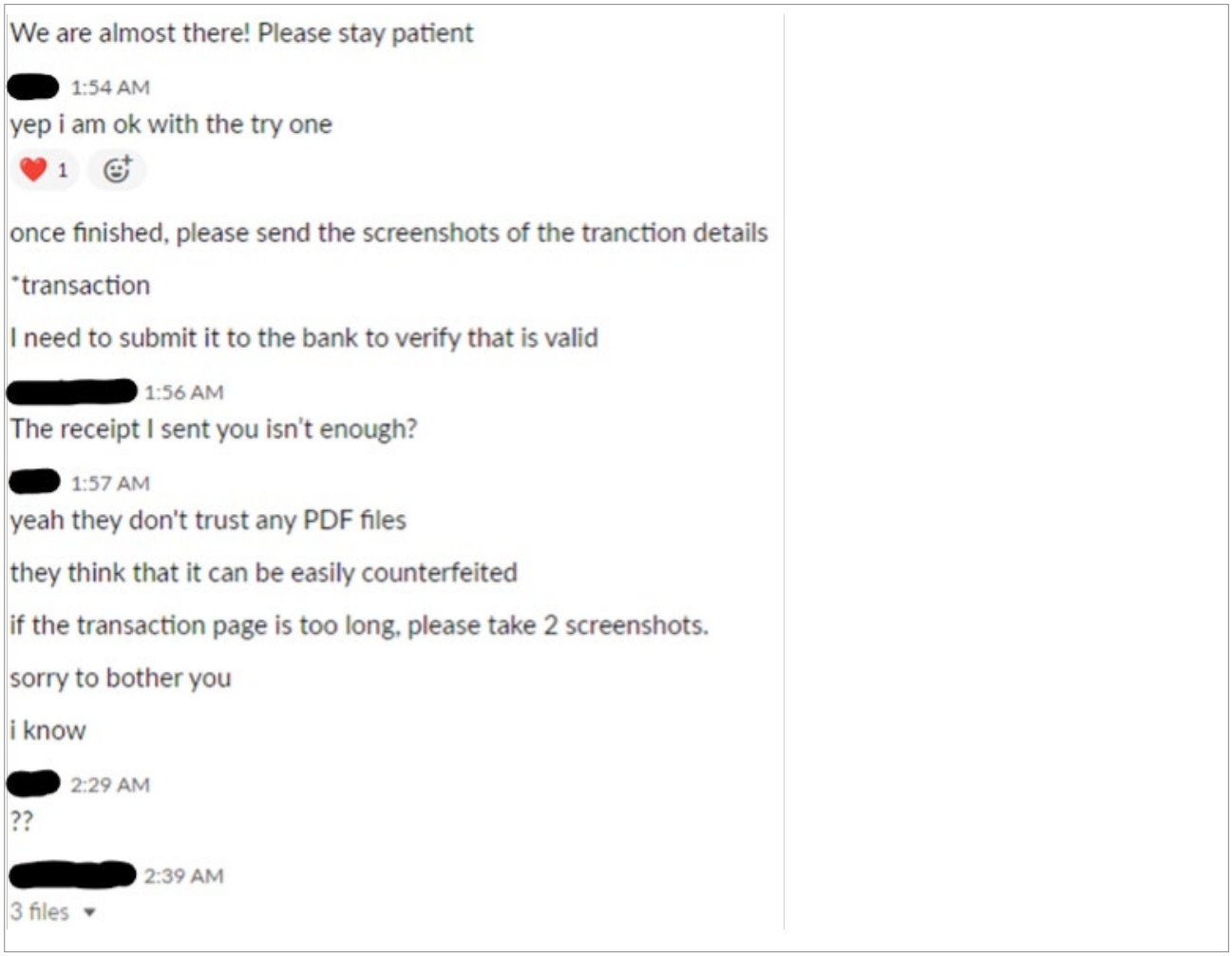



lol
did you see my photo?
my avatar.
lol
yes really
surprised
used gpt?
[redacted]
no
face swap platform
Are you working now?
yes, this is busy time everyday
[redacted]
lol
me 2
yes, its 10:48am
i work in cst
[redacted]
It's 11:48 am here
ah
I work at EST
you est
ya
[redacted]


what is schedule this week?
preparing for return
lol
[redacted]
okay
I should meet ZHao soon, he sent message at 5am
when he can online ?
seems he's sleeping for now
prob 11am round
[redacted]
okay, I didn't think he would be online at so early time
ok, please prepare yours
haha thanks
good luck for your business

The below images show communications between IT workers and their multiple facilitators as they transfer money from U.S. financial institutions to Hong Kong-based front companies to funnel and launder money back to their units. These images are from the same team but in 2025. These images also highlight TTPs in bypassing multifactor authentication for email accounts.





Overarching Units and Colleges

The following section outlines notable locations mentioned in this report. Each entry includes relevant background or contextual details to provide additional geographic and operational clarity.

Korean People's Army (KPA)

KPA is the armed forces of North Korea and the central institution of the country's military establishment, operating under the guidance of the Workers' Party of Korea (WPK). Founded on February 8, 1948, the KPA comprises five branches: the Ground Force, Navy, Air and Anti-Air Force, Strategic Force, and Special Operation Force. It is one of the largest standing militaries in the world, with an estimated 1.2 million active personnel and several million more in reserve. The KPA plays a critical role not only in national defense but also in domestic economic activities and political enforcement. Its doctrine emphasizes asymmetric warfare, including the development of nuclear weapons, cyber capabilities, and special forces operations to counter technologically superior adversaries. The KPA is highly centralized, with leadership structures closely tied to the ruling Kim Jong-un family, particularly Kim Jong-un, who serves as its Supreme Commander. The KPA's influence extends beyond traditional military functions, shaping North Korean society and serving as a key tool for maintaining regime stability.

Reconnaissance General Bureau (정찰총국)
Location: 39° 6′28″N 125°43′54″E

North Korea's primary intelligence agency responsible for clandestine operations, including cyber warfare, espionage, psychological warfare, and special operations. Established in 2009 through the consolidation of various intelligence entities, the RGB reports directly to the KPA and ultimately to the leadership of the DPRK. It is known for overseeing North Korea's most prominent cyber units, which have been involved in high-profile attacks targeting financial institutions, government agencies, and defense contractors worldwide. The RGB is structured into multiple bureaus, each focusing on specific domains like cyber operations, covert military missions, and intelligence gathering. Its activities are aimed at undermining adversaries' security, enhancing North Korea's asymmetric warfare capabilities, and generating revenue through cybercrime. The U.S. and other countries have sanctioned the RGB for its involvement in cyberattacks, espionage, and weapons proliferation.

Research Center 227

A new AI-centric entity within North Korea's cyber operations framework that, according to reports, was established in late February 2025 under the directive of North Korean leadership, aiming to enhance the country's overseas information warfare capabilities. Operating under RGB, Research Center 227 focuses on developing offensive hacking technologies and programs intended to neutralize Western cybersecurity systems and critical infrastructure. The center plans to recruit approximately 90 computer experts, including graduates from prestigious university and doctoral programs, to advance its mission of information theft and network disruption.

Korean Workers' Party (KWP)

The Korean Workers' Party (KWP) is North Korea's dominant political entity, holding a monopoly on power since its founding in 1946. As the central governing force, the KWP shapes all aspects of North Korean society through its strict hierarchical structure, with ultimate authority resting in its leader, Kim Jong-un. Guided by the doctrines of Juche and Songun (military-first policy), the party exerts control over the nation's political, economic, military, and ideological systems. The KWP directly oversees various intelligence and military units, including those responsible for offensive cyber operations. The KWP's extensive control mechanisms are designed to maintain regime stability, enforce loyalty, and pursue strategic objectives domestically and abroad.

Ministry of State Security (MSS) (국가안전보위성)
Location: 39°4′27″N 125°46′6″E

North Korea's MSS is the country's primary intelligence, counterintelligence, and secret police agency, responsible for maintaining internal security and protecting the regime from domestic and foreign threats. It operates under the direct control of the State Affairs Commission, which is led by Kim Jong-un, ensuring loyalty and alignment with the ruling party's objectives. The MSS plays a crucial role in suppressing dissent, monitoring political loyalty, and conducting espionage both domestically and internationally. Its activities include surveillance of North Korean citizens, control over political prison camps, and intelligence operations targeting foreign governments, defectors, and dissident groups. While most known for its internal security role, the MSS is also believed to collaborate with military and cyber units, contributing to broader intelligence efforts aimed at supporting regime stability and strategic objectives.

Munitions Industry Department (MID)

North Korea's MID is a powerful entity responsible for overseeing the development, production, and procurement of the country's conventional and strategic weapons, including ballistic missiles, nuclear technology, and advanced military hardware. Operating under the Central Committee of the KWP, the MID plays a critical role in enhancing North Korea's military capabilities and ensuring the regime's self-reliance in defense production. It manages research institutes, production facilities, and procurement networks, often working closely with the Academy of National Defense Science to advance the regime's nuclear and missile programs. Due to its pivotal role in weapons development, the MID has been subjected to international sanctions, aimed at restricting its access to materials, technology, and financial resources needed to further its military ambitions. The MID and its subordinate 313 General Bureau, located at 38°42′38″N 127°35′45″E, are responsible for remitting large amounts of revenue earned by overseas IT teams to Pyongyang.

Ministry of National Defense (MND) (국방성)
Location: 39° 3′36″N 125°44′13″E

North Korea's MND serves as the central authority responsible for managing and directing the country's armed forces under the KWP and State Affairs Commission. Its primary functions include overseeing military strategy, defense policy, logistics, and administrative operations of the KPA, which encompasses the Ground Force, Navy, Air Force, Strategic Force, and Special Operations Force. Though nominally a significant institution, real power over military affairs is largely concentrated under the Central Military Commission and the Supreme Commander, Kim Jong-un. The MND operates more as an administrative body coordinating military readiness, training, and defense production rather than exercising independent control over strategic decision-making. Its activities are closely integrated with other agencies involved in security and intelligence, reflecting North Korea's highly centralized and tightly controlled military structure.

Kumsong Academy

The campus includes Kumsong No.1 Secondary School (**금성제1중학교**) that offers intensive computer education courses to gifted students. Students reportedly receive 1,660 hours of computer education over six years in areas including Linux, C, C++, Windows, networking and artificial intelligence. The school is one of a handful that feeds the computer science programs at prestigious universities including Kim Il Sung Military University, Kim Chaek University of Technology, and the Institute of Sciences. After graduating, these students go on to work in North Korea's IT industry as programmers, cyber operatives or overseas IT workers. It is visited by foreign delegations to look around as a centerpiece of North Korea's education system. The computer school campus is housed in a large, eight story building alongside the main building.

Figure 13. Kumsong Academy (금성학원) in Pyongyang's Mangyondae District is one of North Korea's centers of computing expertise.

The same site is/was also home to the IT center of the Pyongyang International Information Centre of New Technology and Economy (PIINTEC) (**평양국제새기술경제정보센터**) (a.k.a. Pyongyang International New Technology and Economic Information Company). The organization was established in October 2003 to promote international knowledge exchange in areas including information technology. Among its stated activities is the dissemination of foreign scientific and IT information on the local intranet.

Figure 14. The IT center of the Pyongyang International Information Centre of New Technology and Economy (PIINTEC).

In the mid-2000s when North Korea was attempting to create a software outsourcing industry, PIINTEC exhibited at IT exhibitions in China and, in a 2005 presentation, said it intended to open an "IT training and internship center" in Dalian, China, another hotspot for DPRK cyber activity. It also said it planned to send North Korean IT experts to "foreign universities and companies for training and research on the development of OS programs using Linux tools and network services." It is unclear if the organization is still in operation.

Kim Il Sung Military University (김일성군사종합대학)

Kim Il Sung Military University, also in Mangyondae District, is North Korea's most important military academy. During a visit in April 2024, Kim Jong-un said "the main duty of Kim Il Sung Military University to train a larger number of talented military personnel who are fully prepared for modern warfare."

The university has a college of computer science that includes a computer networking lab, operating systems lab, data security lab, multimedia contents lab and software engineering lab, according to South Korea's Ministry of Unification.

Figure 15. Kim Il Sung Military University.

The Way Forward

Until a RGB cyber operator or high-level IT worker defects and is willing to publicly share their story, we may never know the exact inner workings of DPRK's cyber ecosystem. Everything laid out in this document is the product of years of research, combining numerous cyber, military, and policy experts' perspectives in an effort to capture the complexity of the DPRK's cyber program.

The DPRK is operating with a much more agile cyber force today than a decade ago, which has serious implications for any organization or government that is likely to become a target of DPRK operations. While the DPRK cyber program probably will still experience some challenges due to infighting and organization stove piping, its operatives have clearly proven that they can overcome limited internet access, crushing sanctions, and a lack of resources to achieve their objectives.

To effectively address the evolving threat, it's important to understand the DPRK on its own terms, rather than relying solely on conventional frameworks.

Applying a mission-centric mindset to track, predict, and thwart DPRK cyber operations requires collaboration and communication between defenders and targets, and gives us the best chance of beating the DPRK at their own game.

Conclusion

Beyond Attribution: A Call to Action for Security Leadership

The DPRK cyber threat is no longer just a matter of espionage—it is a multi-layered, state-aligned criminal enterprise that blurs the lines between cybercrime, geopolitical strategy, and economic warfare. What we're facing is not a collection of isolated threats, but a coordinated ecosystem: elite operatives from sanctioned universities, IT workers embedded inside global companies, and facilitators laundering funds and providing identities.

This ecosystem is designed to exploit trust, technology, and complacency.

And it's already inside the walls.

Three key insights must drive the next phase of defense:

- This is a national security challenge. DPRK operators are embedded in global supply chains and systems. Waiting is not an option.
- Attribution is only the beginning. Countering this threat requires behavioral insight, contextual intelligence, and awareness of the motivations driving these operatives.
- The APT vs. IT worker distinction is obsolete. These actors function as one enterprise in support of regime priorities—and they must be understood and countered as such.

Immediate Steps to Counter the DPRK Insider Threat

Security leaders must take immediate and concrete steps:

- Review existing internal and external personnel with access to sensitive systems—including remote or contract workers—swiftly removing suspected DPRK operatives where appropriate.

Protective Measures:

Pre-Employment

- Require cameras on to confirm identity and observe background indicators.
- Watch for signs of cheating (e.g., long pauses, eye-scanning movements).
- Verify geolocation through call logs and Zoom login IP addresses.
- Where possible, arrange in-person identity verification.
- Assist HR in validating technical experience claims and randomizing interview questions.
- Include HR in security briefings and threat awareness sessions.

Post-Employment

- Monitor for unauthorized remote access tools; monitor endpoint activity outside company hours.
- Track browser use for VDI access and multiple email aliases.
- Watch for low engagement across emails, messaging, and meetings.
- Monitor leavers for extortion attempts, ransomware, or severance exploitation encouraged by overwork communities.

For the latest DPRK-linked behavioral indicators and email IOCs, visit dtexsystems.com/resources/i3-threat-advisory-inside-the-dprk/

- Invest in tooling and technology that enables behavioral monitoring, identity validation, and early insider risk detection. The right infrastructure doesn't just help respond to threats—it helps anticipate and mitigate them.
- Share threat observations with vendors, researchers, and law enforcement. Increase internal visibility and cross-functional coordination across legal, HR, and finance.
- Report suspicious activity through trusted channels such as the Defense Cyber Crime Center (DC3) (www.dc3.mil) and the FBI's Internet Crime Complaint Center (www.ic3.gov).
- Drive collaboration across sectors. Establish real-time information-sharing channels between private organizations, government agencies, and trusted partners, such as the U.S. Insider

The future of defense against DPRK cyber operations will not be won with technology alone. What will make the difference is strategic alignment, intelligence-driven operations, and leadership that acts as decisively as the adversary does.

This is the moment for leadership to act.
The threat is evolving. Our response must too.

Sources

Jeong Tae Joo, "Mecca for North Korean Hackers," Daily NK, March 12, 2025, https://www.dailynk.com/english/mecca-for-north-korean-hackers/

"How North Korea Recruits, Trains and Deploys Its Army of Hackers," NBC News, December 20, 2017, https://www.nbcnews.com/news/north-korea/how-north-korea-recruits-trains-its-army-hackers-n825521

Sangwon Yoon, "North Korea Recruits Hackers at School," Al Jazeera, June 20, 2011, https://www.aljazeera.com/features/2011/6/20/north-korea-recruits-hackers-at-school

Insikt Group, "North Korea's Cyber Strategy," Recorded Future, June 23, 2023, https://www.recordedfuture.com/research/north-koreas-cyber-strategy

Cybersecurity and Infrastructure Security Agency, "North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs," Cybersecurity Advisory AA24-207A, July 25, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a

Jeong Tae Joo, "N. Korea Ramps Up Cyber Offensive: New Research Center to Focus on AI-Powered Hacking," Daily NK, March 12, 2025, https://www.dailynk.com/english/n-korea-ramps-up-cyber-offensive-new-research-center-to-focus-on-ai-powered-hacking/

Elisabeth Suh, "North Korea's Cyber Capabilities and Strategy," German Council on Foreign Relations (DGAP), January 7, 2022, https://dgap.org/en/research/publications/north-koreas-cyber-capabilities-and-strategy-0

United Nations Security Council, "Letter Dated 6 March 2023 from the Panel of Experts Established Pursuant to Resolution 1874 (2009) Addressed to the President of the Security Council," S/2023/171, March 6, 2023, https://docs.un.org/en/S/2023/171

Insikt Group, "Despite Sanctions, North Koreans Continue to Use Foreign Technology," Recorded Future, July 18, 2024, https://www.recordedfuture.com/research/north-koreans-continue-to-use-foreign-technology

Jason Bartlett, "Mapping Major Milestones in the Evolution of North Korea's Cyber Program," The Diplomat, July 18, 2022, https://thediplomat.com/2022/07/mapping-major-milestones-in-the-evolution-of-north-koreas-cyber-program/

Hyuk Kim, "North Korea's International Network for Artificial Intelligence Research," 38 North, August 21, 2024, https://www.38north.org/2024/08/north-koreas-international-network-for-artificial-intelligence-research/

Hyuk Kim, "North Korea's Artificial Intelligence Research: Trends and Potential Civilian and Military Applications," 38 North, January 23, 2024, https://www.38north.org/2024/01/north-koreas-artificial-intelligence-research-trends-and-potential-civilian-and-military-applications/

Lee Sang Yong and Hwang Hyun-uk, "Digital Warfare: N. Korea's Evolving Cyber Arsenal and Global Threats," Daily NK, March 28, 2025, https://www.dailynk.com/english/digital-warfare-north-korea-evolving-cyber-arsenal-global-threats/

Office of Foreign Assets Control, "Guidance on the Democratic People's Republic of Korea Information Technology Workers," U.S. Department of the Treasury, November 2022, https://ofac.treasury.gov/media/923126/download?inline=

Hayato Sasaki, "Tempted to Classify APT Actors: Practical Challenges of Attribution in the Case of Lazarus's Subgroup," JPCERT/CC Eyes, March 25, 2025, https://blogs.jpcert.or.jp/en/2025/03/classifying-lazaruss-subgroup.html

Dan Goodin, "Gemini Hackers Can Deliver More Potent Attacks with a Helping Hand from Gemini," Ars Technica, March 2025, https://arstechnica.com/security/2025/03/gemini-hackers-can-deliver-more-potent-attacks-with-a-helping-hand-from-gemini/

Microsoft Threat Intelligence, "Moonstone Sleet Emerges as New North Korean Threat Actor with New Bag of Tricks," Microsoft Security Blog, May 28, 2024, https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/

Jeong Tae Joo, "N. Korea Doubles Foreign Currency Quotas for Overseas Workers," Daily NK, March 25, 2025, https://www.dailynk.com/english/north-korea-doubles-foreign-currency-quotas-overseas-workers/

Jeong Tae Joo, "N. Korea Ramps Up Cyber Offensive: New Research Center to Focus on AI-Powered Hacking," Daily NK, March 12, 2025, https://www.dailynk.com/english/n-korea-ramps-up-cyber-offensive-new-research-center-to-focus-on-ai-powered-hacking/

Lawrence Abrams, "CryptoCore Hackers Made Over $200M Breaching Crypto Exchanges," BleepingComputer, June 24, 2020, https://www.bleepingcomputer.com/news/security/cryptocore-hackers-made-over-200m-breaching-crypto-exchanges/

United States v. Park Jin Hyok. Criminal Complaint, U.S. District Court for the Central District of California, September 6, 2018. https://int.nyt.com/data/documenthelper/274-park-jin-hyo-complaint/7b40e5ed5b185f141e1a/optimized/full.pdf#page=1

Cimpanu, Catalin. "The Many Personalities of Lazarus." Risky Business, March 2024. https://risky.biz/laz/

Kong, Ji Young, Jong In Lim, and Kyoung Gon Kim. "The All-Purpose Sword: North Korea's Cyber Operations and Strategies." NATO Cooperative Cyber Defence Centre of Excellence, 2019. https://www.ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf

U.S. Department of the Treasury. "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups." Press Release, September 13, 2019. https://home.treasury.gov/news/press-releases/sm774

"The Deadly 4." Gwangju News, July 2013. https://gwangjunewsgic.com/arts-culture/korean-myths/the-deadly-4/

Cha, Victor. "North Korea's Cyber Operations: Strategy and Responses." Center for Strategic and International Studies, December 2015. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf

Defense Intelligence Agency. "North Korea Military Power: A Growing Regional and Global Threat." 2021. https://www.dia.mil/Portals/110/Documents/News/North_Korea_Military_Power.pdf

"North Korea Creates Army of Cyber Trolls." Sky News, July 2013. https://news.sky.com/story/north-korea-creates-army-of-cyber-trolls-10437459

Ford, Glyn. "Forks in the Road to Reform: Socio-Economic Changes under Kim Jong Un." Global Asia 9, no. 1 (2014). https://www.globalasia.org/v9no1/cover/forks-in-the-road-to-reform-socio-economic-changes-under-kim-jong-un_glyn-ford

Jang, Seulkee. "Kim Jong Un Is Directly Handling Results of New COVID-19 Hacking Organization's Work." Daily NK, February 5, 2021. https://www.dailynk.com/english/kim-jong-un-directly-handling-results-new-covid-19-hacking-organization-work/

Phylum. "Smuggling Malware in Test Code." Phylum Blog, February 2024. https://blog.phylum.io/smuggling-malware-in-test-code/

Park, Seongsu. "The actor continues with familiar tactics, incorporating a cleverly obfuscated BeaverTail script. The endgame remains the InvisibleFerret script, with the C2 using IP addresses previously employed by the actor: 147.124.212.89:1244." X, December 2023. https://mobile.twitter.com/unpacker/status/1737993034934169855

Reddit user. "Obfuscated code a 'recruiter' sent me." Reddit, December 2023. https://www.reddit.com/r/hacking/comments/18npzcl/obfuscated_code_a_recruiter_sent_me/

Sharma, Ax. "Blockchain dev's wallet emptied in 'job interview' using npm package." BleepingComputer, December 28, 2023. https://www.bleepingcomputer.com/news/security/blockchain-devs-wallet-emptied-in-job-interview-using-npm-package/

Qi An Xin. "针对区块链从业者的招聘陷阱：疑似Lazarus (APT-Q-1) 窃密行动分析 [Recruitment Traps Targeting Blockchain Practitioners: Suspected Lazarus (APT-Q-1) Espionage Operation Analysis]." FreeBuf, May 2024. https://www.freebuf.com/articles/paper/400513.html

Phylum. "North Korea Still Attacking Developers via npm." Phylum Blog, August 2024. https://blog.phylum.io/north-korea-still-attacking-developers-via-npm/

Bestuzhev, Dmitry. "It is safe to say it is a North Korean Op. Threat Actor: North Korean Cluster Context." X, April 2025. https://x.com/dimitribest/status/1782609281897902426

User @asdasd13asbz. "The Lazarus group appears to be currently reaching out to targets via LinkedIn and spreading malware." X, April 2025. https://x.com/asdasd13asbz/status/1782951380568936481

Soni, Abhishek Singh. "Blockchain Security, Crypto Scam Alert, DeFi Jobs." LinkedIn, April 2025. https://linkedin.com/posts/abhisheksinghsoni_blockchainsecurity-cryptoscamalert-defijobs-activity-7127542067001475073-71xU/

0x50D4. "Python Malware." GitHub, April 3, 2024. https://github.com/0x50D4/0x50d4.github.io/blob/main/_posts/2024-04-03-python-malware.md

Karlo Zanki, "Fake Recruiter Coding Tests Target Devs with Malicious Python Packages," ReversingLabs, September 2024, https://www.reversinglabs.com/blog/fake-recruiter-coding-tests-target-devs-with-malicious-python-packages

Microsoft Threat Intelligence, "Moonstone Sleet Emerges as New North Korean Threat Actor with New Bag of Tricks," Microsoft Security Blog, May 28, 2024, https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/

Seulkee Jang, "Kim Jong Un Is Directly Handling Results of New COVID-19 Hacking Organization's Work," Daily NK, February 5, 2021, https://www.dailynk.com/english/kim-jong-un-directly-handling-results-new-covid-19-hacking-organization-work/

ClearSky Cyber Security, "Attributing CryptoCore Attacks Against Crypto Exchanges to Lazarus," May 2021, https://www.clearskysec.com/cryptocore-lazarus-attribution/.:contentReference[oaicite:4]{index=4}

Josh Smith and Jack Stubbs, "Exclusive: North Korea-Linked Hackers Targeted AstraZeneca in COVID-19 Spying Campaign – Sources," Reuters, November 27, 2020, https://www.reuters.com/article/us-healthcare-coronavirus-astrazeneca-no-idUSKBN2871A2/

Tom Burt, "Cyberattacks Targeting Health Care Must Stop," Microsoft On the Issues, November 13, 2020, https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/

U.S. Department of Justice, "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyberattacks and Intrusions," September 6, 2018, https://www.justice.gov/usao-cdca/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyberattacks

U.S. Department of Justice, "Criminal Complaint: United States v. Park Jin Hyok," September 6, 2018, https://www.justice.gov/archives/opa/press-release/file/1367701/dl?inline=

"Third Floor," North Korea Leadership Watch, accessed April 15, 2025, https://nkleadershipwatch.wordpress.com/kji-2/third-floor/

Kim Chong Woo, "The Evolution of North Korean Cyber Threats," The Asan Institute for Policy Studies, February 20, 2019, https://en.asaninst.org/contents/the-evolution-of-north-korean-cyber-threats/

Analyst1, North Korea Intelligence Assessment 2022, October 2022, https://analyst1.com/north-korea-intelligence-assessment-2022/

Kai Weiss, "Fighting for Freedom With Balloons: The Story of Lee Min-Bok," Austrian Economics Center, April 12, 2021, https://austriancenter.com/fighting-freedom-balloons-lee-min-bok/

Cybersecurity and Infrastructure Security Agency, "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector," Alert (AA22-187A), July 6, 2022, https://www.cisa.gov/news-events/alerts/2022/07/06/north-korean-state-sponsored-cyber-actors-use-maui-ransomware-target

Jason Nelson, "FBI: North Korea's Lazarus Group Behind $100M Harmony Bridge Hack," Decrypt, February 14, 2023, https://decrypt.co/119861/fbi-north-korea-lazarus-horizon-harmony-bridge-hack

Ax Sharma, "Hackers Stole $620 Million from Axie Infinity via Fake Job Interviews," BleepingComputer, March 30, 2022, https://www.bleepingcomputer.com/news/security/hackers-stole-620-million-from-axie-infinity-via-fake-job-interviews/

Andy Greenberg, "North Korean Hackers Stole $3 Billion in Crypto—and They're Just Getting Started," Wired, June 3, 2022, https://www.wired.com/story/north-korea-hackers-apt38-cryptocurrency/

U.S. Department of the Treasury, "Treasury Continues to Counter North Korea's Use of Cryptocurrency to Evade Sanctions," April 14, 2022, https://home.treasury.gov/news/press-releases/sm924

Cybersecurity and Infrastructure Security Agency, "North Korean Remote Access Trojan: H0lyGh0st," Advisory (AA21-048A), February 17, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-048a

Ravie Lakshmanan, "North Korean UNC2970 Hackers Expands Attacks to More Sectors with Phishing Campaigns," The Hacker News, March 2023, https://thehackernews.com/2023/03/north-korean-unc2970-hackers-expands.html

AhnLab Security Emergency Response Center (ASEC), Andariel: A Subgroup of Lazarus, November 2022, https://www.ahnlab.com/en/global/upload/download/techreport/%5BAhnLab%5DAndariel_a_Subgroup_of_Lazarus%20(3).pdf

Cybersecurity and Infrastructure Security Agency, "North Korean State-Sponsored APT Targets Blockchain Companies," Advisory (AA22-108A), April 18, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a

Google Cloud Threat Intelligence, "North Korea Targets Security Researchers with Supply Chain Attacks," Google Cloud Blog, January 25, 2024, https://cloud.google.com/blog/topics/threat-intelligence/north-korea-supply-chain

Google Cloud Threat Intelligence, "3CX Software Supply Chain Compromise: What Happened and What You Need to Know," Google Cloud Blog, March 30, 2023, https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise

AhnLab Security Emergency Response Center (ASEC), "APT37 Group's Active Exploitation of Abandoned Korean Web Server," February 20, 2024, https://asec.ahnlab.com/ko/49180/

Zscaler ThreatLabz, "An Unintentional Leak: A Glimpse into the Attack Vectors of APT37," Zscaler Blog, August 23, 2023, https://www.zscaler.com/blogs/security-research/unintentional-leak-glimpse-attack-vectors-apt37

Cybersecurity and Infrastructure Security Agency, National Security Agency, and FBI, "Ransomware Attacks on Critical Infrastructure Fund DPRK Activities," February 9, 2023, https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_DPRK_ACTIVITIES.PDF

Google Cloud Threat Intelligence, "APT43: North Korean Cybercrime and Espionage," Google Cloud Blog, April 4, 2023, https://cloud.google.com/blog/topics/threat-intelligence/apt43-north-korea-cybercrime-espionage

Google Cloud Threat Intelligence, "APT38: Details on New North Korean Regime-Backed Threat Group," Google Cloud Blog, July 25, 2023, https://cloud.google.com/blog/topics/threat-intelligence/apt38-details-on-new-north-korean-regime-backed-threat-group

Google Cloud Threat Intelligence, "APT37: An Overlooked North Korean Actor," Google Cloud Blog, September 28, 2023, https://cloud.google.com/blog/topics/threat-intelligence/apt37-overlooked-north-korean-actor

Google Cloud Threat Intelligence, "Mapping North Korea's Cyber Threat Structure and Alignment," Google Cloud Blog, November 1, 2023, https://cloud.google.com/blog/topics/threat-intelligence/north-korea-cyber-structure-alignment-2023

Jenny Town, "Inside a North Korean Internet Server: How Well Do You Know Your Partners?" Stimson Center, January 17, 2024, https://www.stimson.org/2024/inside-a-north-korean-internet-server-how-well-do-you-know-your-partners/

Katie Bo Lillis, "US Animation Studio Uncovers Sketches on a North Korean Server," CNN, April 22, 2024, https://www.cnn.com/2024/04/22/politics/us-animation-studio-sketches-korean-server/index.html

Federal Bureau of Investigation, "Rim Jong Hyok," FBI Cyber's Most Wanted, accessed April 15, 2025, https://www.fbi.gov/wanted/cyber/rim-jong-hyok

U.S. Department of Justice, "North Korean Government Hacker Charged in Involvement in Ransomware Attacks Targeting U.S. Hospitals," July 19, 2021, https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals

Alexandra Kelley, "FBI, Mandiant Designate Advanced North Korean Hackers Stealing US Defense Secrets," Nextgov, July 3, 2024, https://www.nextgov.com/cybersecurity/2024/07/fbi-mandiant-designate-advanced-north-korean-

hackers-stealing-us-defense-secrets/398308/

Andy Greenberg, "A Max Cartoon Studio Unwittingly Exposed a North Korean Server," Wired, April 22, 2024, https://www.wired.com/story/north-korea-amazon-max-animation-exposed-server/

Internet Crime Complaint Center (IC3), "Public Service Announcement PSA250226: North Korean IT Workers Continue Malicious Activity," February 26, 2025, https://www.ic3.gov/psa/2025/psa250226

Peter W. Singer, "Here's What We Actually Know About North Korea's Cyber Program," Foreign Policy, March 21, 2013, https://foreignpolicy.com/2013/03/21/heres-what-we-actually-know-about-north-koreas-cyber-program/

Michelle Delio, "North Korea's School for Hackers," Wired, June 9, 2003, https://www.wired.com/2003/06/north-koreas-school-for-hackers/

David Martin, "Experts: North Korea Training Teams of Cyber Warriors," CBS News, June 18, 2009, https://www.cbsnews.com/news/experts-north-korea-training-teams-of-cyber-warriors/

University of Washington Jackson School of International Studies, "North Korea Cyber Attacks: A New Asymmetrical Military Strategy?" May 3, 2022, https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/

Pinkston, Daniel A. "Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the 'Sŏn'gun' Era." Georgetown Journal of International Affairs 17, no. 3 (2016): 60–76. http://www.jstor.org/stable/26395976

Agence France-Presse, "North Korea Leader Kim Jong Un Supervises Test of AI Suicide Drones, KCNA Says," NDTV, March 12, 2024, https://www.ndtv.com/world-news/north-korea-leader-kim-jong-un-supervises-test-of-ai-suicide-drones-kcna-says-8019495

Chad O'Carroll, "Kim Jong Un Says Army Obedience Top Priority as Troops Fight in Russia's War," NK News, February 20, 2025, https://www.nknews.org/2025/02/kim-jong-un-says-army-obedience-top-priority-as-troops-fight-in-russias-war/

Ina Fried, "North Korea Hacked Social Media Accounts Including Twitter and Google," Axios, January 27, 2021, https://www.axios.com/2021/01/27/north-korea-hack-social-media-twitter-google

Erin Banco, "U.S. Firms Including Hired North Korean IT Workers Posing as Americans, FBI Claims," The Daily Beast, May 17, 2022, https://www.thedailybeast.com/us-firms-including-hired-north-korean-it-workers-posing-as-americans-fbi-claims/

Secureworks Counter Threat Unit, "Nickel Tapestry: Infrastructure Associated with Crowdfunding Scheme," Secureworks, July 13, 2023, https://www.secureworks.com/blog/nickel-tapestry-infrastructure-associated-with-crowdfunding-scheme

U.S. Department of the Treasury, "Treasury Sanctions North Korean Individuals Supporting the Regime's Malicious Cyber Activities," March 2, 2020, https://home.treasury.gov/news/press-releases/sm481

OpenSanctions, "Entity Profile: North Korea, Reconnaissance General Bureau," accessed April 15, 2025, https://www.opensanctions.org/entities/NK-6NLTZnjnNAFrkjwReoNb5T/

U.S. Department of Justice, "Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent IT Worker Scheme," October 19, 2023, https://www.justice.gov/archives/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information

U.S. Department of the Treasury, Office of Foreign Assets Control, "Entity List: Volasys Silver Star," accessed April 15, 2025, https://sanctionssearch.ofac.treas.gov/Details.aspx?id=24977

U.S. Department of State, Rewards for Justice – Yanbian Silverstar and Volasys Silverstar, accessed April 15, 2025, https://rewardsforjustice.net/rewards/yanbian-silverstar-and-volasys-silverstar/

DPRK Cyber Threat Intelligence Project, "Volasys Silver Star," accessed April 15, 2025, https://dprk-reports.org/entities/6e90657ef72588ed1d79af94be13901da1135b90.aae6d5f504d62e2c8d5a8089caf9de1f03d703a2

United Nations Security Council, "Letter Dated 31 August 2023 from the Panel of Experts Established Pursuant to Resolution 1874 (2009) Addressed to the President of the Security Council," S/2023/668, https://documents.un.org/doc/undoc/gen/n23/238/69/pdf/n2323869.pdf

Jesse Coghlan, "ZachXBT Claims 21 North Korea Crypto Devs Making $500K a Month," Cointelegraph, July 25, 2023, https://cointelegraph.com/news/zachxbt-claims-21-north-korea-crypto-devs-making-500k-month

Staffing Industry Analysts, "US Departments Warn on North Korean IT Workers, Hold Symposium for IT Staffing Firms," August 1, 2023, https://www.staffingindustry.com/news/global-daily-news/us-departments-warn-north-korean-it-workers-hold-symposium-it-staffing-firms

U.S. Department of the Treasury, "U.S. Sanctions Hundreds of Targets in Response to Russia's Illegal Annexation of Ukrainian Regions," September 30, 2022, https://home.treasury.gov/news/press-releases/jy2215

U.S. Department of the Treasury, "Treasury Targets North Korean Weapons Representatives in Russia," March 1, 2023, https://home.treasury.gov/news/press-releases/jy1498

Chainalysis, "OFAC's Sanctions on North Korea and What They Mean for the Crypto Industry," May 26, 2023, https://www.chainalysis.com/blog/ofac-north-korea-sanctions-may-2023/

CNBC, "North Korean Leader's Half-Brother Killed in Malaysia: South Korean Media," February 14, 2017, https://www.cnbc.com/2017/02/14/north-korean-leaders-half-brother-killed-in-malaysia-south-korea-media.html

Adam Entous, "North Korea's Abduction Project," The New Yorker, February 8, 2024, https://www.newyorker.com/news/news-desk/north-koreas-abduction-project

Jesse Coghlan, "Lazarus Group's 2024 Pause Was Repositioning for $1.4B Bybit Hack," Cointelegraph via TradingView, March 4, 2025, https://www.tradingview.com/news/cointelegraph:7211acb81094b:0-lazarus-group-s-2024-pause-was-repositioning-for-1-4b-bybit-hack/

Leo Schwartz, "North Korea's Bybit Hack Shows How Hard It Is to Keep Ethereum Safe," Fortune Crypto, March 4, 2025, https://fortune.com/crypto/2025/03/04/north-korea-bybit-hack-ethereum-safe-dprk-lazarus-group-tradertraitor/

Chainalysis, "Crypto Hacking Trends: How North Korea Stole Billions in 2025," Chainalysis Blog, March 2025, https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/

Commonplace Facts, "Internet in North Korea," September 26, 2024, https://commonplacefacts.com/2024/09/26/internet-in-north-korea/

Security.com Threat Intelligence, "CLASIOPA: Targeting Materials Research Through Cyber Espionage," accessed April 15, 2025, https://www.security.com/threat-intelligence/clasiopa-materials-research

Bruce Klingner, "North Korean Cyberattacks: A Dangerous and Evolving Threat," The Heritage Foundation, April 27, 2021, https://www.heritage.org/asia/report/north-korean-cyberattacks-dangerous-and-evolving-threat

Patrick Brzeski, "Walt Disney Characters Make Unauthorized Appearance in North Korean Concert," The Hollywood Reporter, July 9, 2012, https://www.hollywoodreporter.com/news/general-news/walt-disney-characters-north-korea-dictator-34801-346975/

Nancy Tartaglione, "Disney Characters Shown at North Korea Concert During Kim Jong-Un's Appearance," Deadline, July 9, 2012, https://deadline.com/2012/07/disney-characters-north-korea-concert-unauthorized-kim-jong-un-297618/

Emma Chanlett-Avery, North Korea: U.S. Relations, Nuclear Diplomacy, and Internal Situation, Congressional Research Service, December 18, 2015, https://goodtimesweb.org/diplomacy/2015/R41259.pdf

Dan Robinson and Anish Agnihotri, "Demystifying the North Korean Threat," Paradigm, March 19, 2025, https://www.paradigm.xyz/2025/03/demystifying-the-north-korean-threat

North Korea Leadership Watch, "Mid-Level Managers," September 13, 2024, https://www.nkleadershipwatch.org/2024/09/13/mid-le-managers/

Daily NK, "Former Spy Student Caught Trying to Flee North Korea," March 28, 2025, https://www.dailynk.com/english/former-spy-student-caught-trying-t/

Associated Press, "North Korean Hackers Target South With Online Attacks," NBC News, May 17, 2011, https://www.nbcnews.com/id/wbna42998012

Tayvano, "Atomic Wallet Hack – North Korean-Linked Onchain Analysis," Dune Analytics, accessed April 15, 2025, https://dune.com/tayvano/atomic-wallet-hack

Tayvano, "BTC Avalanche Bridge – Transaction Visuals and Timeline," Dune Analytics, accessed April 15, 2025, https://dune.com/tayvano/btc-avalanche-bridge

Tayvano, "Bybit Thorchain Shitshow – DPRK Tracing," Dune Analytics, accessed April 15, 2025, https://dune.com/tayvano/bybit-thorchain-shitshow

Tayvano, "DPRK TXNs – Transaction Monitoring Dashboard," Dune Analytics, accessed April 15, 2025, https://dune.com/tayvano/dprk-txns

Tayvano, "BingX Flows Associated with DPRK-linked Wallets," Dune Analytics, accessed April 15, 2025, https://dune.com/tayvano/bingx

Tayvano, "Alphapo Exploit – DPRK Attribution Mapping," Dune Analytics, accessed April 15, 2025, https://dune.com/tayvano/alphapo

TRM Labs, Update on DPRK Cyber Activity and Cryptocurrency Theft, January 2025, https://www.trmlabs.com/resources/reports/update-on-dprk-cyber-activity-and-cryptocurrency-theft

Cheyenne Ligon, "Here's How North Korea Launders Billions of Stolen Crypto," CoinDesk, March 7, 2025, https://www.coindesk.com/policy/2025/03/07/here-s-how-north-korea-launders-billions-of-stolen-crypto

Jonathan Greig, "North Koreans Begin Initial Laundering of Funds from Bybit Hack," The Record by Recorded Future, March 8, 2025, https://therecord.media/north-koreans-initial-laundering-bybit-hack

Internet Crime Complaint Center (IC3), "Public Service Announcement PSA250123: DPRK-Linked IT Workers and Cryptocurrency Laundering," January 23, 2025, https://www.ic3.gov/PSA/2025/PSA250123

Ministry of Foreign Affairs of the Republic of Korea, Overview of Sanctions and Measures Against North Korea, accessed April 15, 2025, https://www.mofa.go.kr/eng/wpge/m_25525/contents.do

AJ Vicens, "North Korea's Technical Workers Land Full-Time Jobs Abroad," CyberScoop, March 2024, https://cyberscoop.com/north-korea-technical-workers-full-time-jobs/

Radio Free Asia, "North Korean Authorities Order Tech Workers to Ramp Up Industrial Espionage in China," RFA, July 15, 2016, https://www.rfa.org/english/news/korea/north-korean-authorities-order-tech-workers-to-ramp-up-industrial-espionage-in-china-07152016150820.html

Radio Free Asia, "North Korean Authorities Order Tech Workers to Ramp Up Industrial Espionage in China," RFA, July 15, 2016, https://www.rfa.org/english/news/korea/north-korean-authorities-order-tech-workers-to-ramp-up-industrial-espionage-in-china-07152016150820.html

Kevin Helms, "Radiant Capital Hack: How Hackers Used a PDF to Steal $50 Million," Bitcoin News, March 25, 2025, https://news.bitcoin.com/radiant-capital-hack-how-hackers-used-a-pdf-to-steal-50-million/

Tayvano (@tayvano_), "North Korea Is Already Moving Funds from the Radiant Hack," X (formerly Twitter), March 25, 2025, https://x.com/tayvano_/status/1905761068741459974

Chainalysis, "OFAC's Sanctions on North Korea and What They Mean for the Crypto Industry," Chainalysis Blog, May 26, 2023, https://www.chainalysis.com/blog/ofac-north-korea-sanctions-may-2023/

U.S. Department of the Treasury, "Treasury Targets North Korean Weapons Representatives in Russia," March 1, 2023, https://home.treasury.gov/news/press-releases/jy1498

Baek, Jieun. North Korea's Hidden Revolution: How the Information Underground Is Transforming a Closed Society. New Haven: Yale University Press, 2016. https://archive.org/details/northkoreashidde0000baek

Lee Sang Yong and Hwang Hyun-uk, "Digital Warfare: N. Korea's Evolving Cyber Arsenal and Global Threats," Daily NK, March 28, 2025, https://www.dailynk.com/english/digital-warfare-north-korea-evolving-cyber-arsenal-global-threats/

Andy Greenberg, "The Huge 3CX Breach Was Actually Two Linked Supply Chain Attacks," Wired, April 20, 2023, https://www.wired.com/story/3cx-breach-supply-chain-attacks-north-korea/

Insikt Group, "North Korea's Cyber Strategy: An Initial Analysis," Recorded Future, June 2023, https://www.recordedfuture.com/research/north-koreas-cyber-strategy

Pyongyang Papers, "Moonstone Sleet & Sin Chong Min," accessed April 15, 2025, https://pyongyangpapers.com/moonstone-sleet-sin-chong-min/

Council on Foreign Relations, "Moonstone Sleet," Cyber Operations Tracker, accessed April 15, 2025, https://www.cfr.org/cyber-operations/moonstone-sleet

Aja Romano, "The 2014 Sony Hacks, Explained," Vox, December 19, 2014, https://www.vox.com/2014/12/19/7420113/sony-hack-explained

Ed Caesar, "The Incredible Rise of North Korea's Hacking Army," The New Yorker, April 25, 2022, https://www.newyorker.com/magazine/2022/05/02/the-incredible-rise-of-north-koreas-hacking-army

Chad O'Carroll, "Lifestyles of the Loyalists: How North Korea's Upper Classes Live," NK News, September 1, 2021, https://www.nknews.org/2021/09/lifestyles-of-the-loyalists-how-north-koreas-upper-classes-live/

James Pearson, "Inside the Kim Family Business: Office 39," NK News, July 8, 2014, https://www.nknews.org/2014/07/inside-the-kim-family-business-office-39/

Colin Zwirko, "How North Korea Compels Citizens to Spy on Each Other with New Surveillance Law," NK Pro (NK News), March 8, 2023, https://www.nknews.org/pro/how-north-korea-compels-citizens-to-spy-on-each-other-with-new-surveillance-law/

Nicholas Hamisevicz, "The Jig Is Not Yet Up: Kim Jong Un Turns to Cyber Crime," Korea Economic Institute of America (KEIA), November 15, 2022, https://keia.org/the-peninsula/the-jig-is-not-yet-up-kim-jong-un-turns-to-cyber-crime/

Rekt News, "The Impersonator," February 9, 2024, https://rekt.news/the-impersonator

MSN News, "North Korea Unveils AI Suicide Drones and AWACS Plane," June 27, 2023, https://www.msn.com/en-us/news/world/north-korea-unveils-ai-suicide-drones-and-awacs-plane/ar-AA1C1Te5

To request a threat briefing with DTEX on the DPRK, visit dtexsystems.com/exposing-dprk/#dprk-contact

To access the latest DPRK-linked behavioral indicators and email IOCs, visit dtexsystems.com/resources/i3-threat-advisory-inside-the-dprk/

ABOUT DTEX SYSTEMS

As the trusted leader of insider risk management, DTEX transforms enterprise security by displacing reactive tools with a proactive solution that stops insider risks from becoming data breaches. DTEX InTERCEPT™ consolidates Data Loss Prevention, User Activity Monitoring, and User Behavior Analytics in one lightweight platform to enable organizations to achieve a trusted and protected workforce. Backed by behavioral science, powered by AI, and used by governments and organizations around the world, DTEX is the trusted authority for protecting data and people at scale with privacy by design.