DPRK IT Workers Expanding in Scope and Scale

By Google Threat Intelligence Group

Published: 2025-04-01 · Archived: 2026-04-05 19:43:21 UTC

Written by: Jamie Collier

Since our September 2024 report outlining the Democratic People's Republic of Korea (DPRK) IT worker threat, the scope and scale of their operations has continued to expand. These individuals pose as legitimate remote workers to infiltrate companies and generate revenue for the regime. This places organizations that hire DPRK IT workers at risk of espionage, data theft, and disruption.

In collaboration with partners, Google Threat Intelligence Group (GTIG) has identified an increase of active operations in Europe, confirming the threat's expansion beyond the United States. This growth is coupled with evolving tactics, such as intensified extortion campaigns and the move to conduct operations within corporate virtualized infrastructure.

On The March: IT Workers Expand Globally with a Focus on Europe

DPRK IT workers' activity across multiple countries now establishes them as a global threat. While the United States remains a key target, over the past months, DPRK IT workers have encountered challenges in seeking and maintaining employment in the country. This is likely due to increased awareness of the threat through public reporting, United States Department of Justice indictments, and right-to-work verification challenges. These factors have instigated a global expansion of IT worker operations, with a notable focus on Europe.

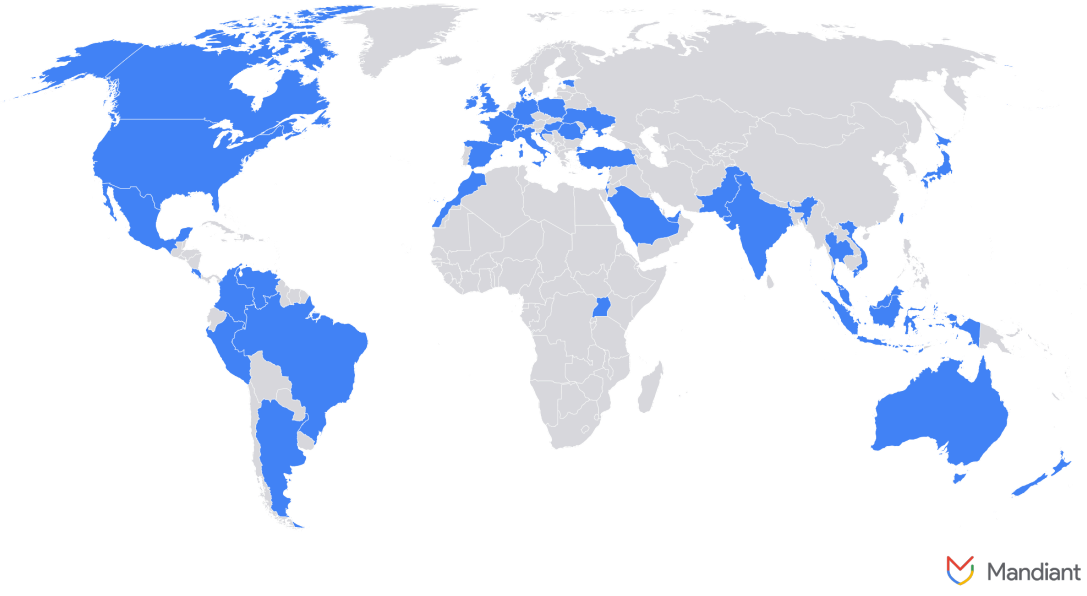

Figure 1: List of countries impacted by DPRK IT workers

IT Worker Activity in Europe

In late 2024, one DPRK IT worker operated at least 12 personas across Europe and the United States. The IT Worker actively sought employment with multiple organizations within Europe, particularly those within the defense industrial base and government sectors. This individual demonstrated a pattern of providing fabricated references, building a rapport with job recruiters, and using additional personas they controlled to vouch for their credibility.

Separately, additional investigations uncovered other IT worker personas seeking employment in Germany and Portugal, alongside login credentials for user accounts of European job websites and human capital management platforms.

GTIG has also observed a diverse portfolio of projects in the United Kingdom undertaken by DPRK IT workers. These projects included web development, bot development, content management system (CMS) development, and blockchain technology, indicating a broad range of technical expertise, spanning traditional web development to advanced blockchain and AI applications.

Specific projects identified include:

- Development of a Nodexa token hosting plan platform using Next.js, React, CosmosSDK, and Golang, as well as the creation of a job marketplace using Next.js, Tailwind CSS, MongoDB, and Node.js.
- Further blockchain-related projects involved Solana and Anchor/Rust smart contract development, and a blockchain job marketplace built using the MERN stack and Solana.
- Contributions to existing websites by adding pages using Next.js and Tailwind CSS,
- Development of an artificial intelligence (AI) web application leveraging Electron, Next.js, AI, and blockchain technologies.

In their efforts to secure these positions, DPRK IT workers employed deceptive tactics, falsely claiming nationalities from a diverse set of countries, including Italy, Japan, Malaysia, Singapore, Ukraine, the United States, and Vietnam. The identities used were a combination of real and fabricated personas.

IT workers in Europe were recruited through various online platforms, including Upwork, Telegram, and Freelancer. Payment for their services was facilitated through cryptocurrency, the TransferWise service, and Payoneer, highlighting the use of methods that obfuscate the origin and destination of funds.

Facilitators Support European Operations

The facilitators used by IT workers to help them get jobs, defeat identity verification, and receive funds fraudulently have also been found in Europe. One incident involved a DPRK IT worker using facilitators located in both the United States and the United Kingdom. Notably, a corporate laptop, ostensibly intended for use in New York, was found to be operational in London, indicating a complex logistical chain.

An investigation into infrastructure used by a suspected facilitator also highlighted heightened interest in Europe. Resources discovered contained fabricated personas, including resumes listing degrees from Belgrade University in Serbia and residences in Slovakia, as well as instructions for navigating European job sites. Additionally, contact information for a broker specializing in false passports was discovered, indicating a coordinated effort to acquire fraudulent identification documents. One document provided specific guidance on seeking employment in Serbia, including the use of a Serbian time zone during communications.

Extortion Heating Up

Alongside global expansion, DPRK IT workers are also evolving their tactics. Based on data from multiple sources, GTIG assesses that since late October 2024, IT workers have increased the volume of extortion attempts and gone after larger organizations.

In these incidents, recently fired IT workers threatened to release their former employers' sensitive data or to provide it to a competitor. This data included proprietary data and source code for internal projects.

The increase in extortion campaigns coincided with heightened United States law enforcement actions against DPRK IT workers, including disruptions and indictments. This suggests a potential link, where pressure on these workers may be driving them to adopt more aggressive measures to maintain their revenue stream.

Previously, workers terminated from their places of employment might attempt to provide references for their other personas so that they could be rehired by the company. It is possible that the workers suspected they were terminated due to discovery of their true identities, which would preclude attempts to be rehired.

The Virtual Workspace: BYOD Brings IT Worker Risks

To avoid distributing corporate laptops, some companies operate a bring your own device (BYOD) policy, allowing employees to access company systems through virtual machines. Unlike corporate laptops that can be monitored, personal devices operating under a BYOD policy may lack traditional security and logging tools, making it difficult to track activities and identify potential threats. This absence of conventional security measures means that typical evidence trails linked to IT workers, such as those derived from corporate laptop shipping addresses and endpoint software inventories, are unavailable. All of this increases the risk of undetected malicious activity.

GTIG believes that IT workers have identified BYOD environments as potentially ripe for their schemes, and in January 2025, IT workers are now conducting operations against their employers in these scenarios.

Conclusion

Global expansion, extortion tactics, and the use of virtualized infrastructure all highlight the adaptable strategies employed by DPRK IT workers. In response to heightened awareness of the threat within the United States, they've established a global ecosystem of fraudulent personas to enhance operational agility. Coupled with the discovery of facilitators in the UK, this suggests the rapid formation of a global infrastructure and support network that empowers their continued operations.

For detailed mitigation and detection strategies, please read our previous report on DPRK IT workers. For even more details, read our IT worker Transform post.

Posted in

- Threat Intelligence
