Bundesamt für Verfassungsschutz

Private Sector Security Advisory | 02/2024 | 1 October 2024

Subject | North Korean IT Workers

Situation

North Korean intelligence services carry out offensive cyber operations worldwide to obtain foreign currency. In this context, undercover IT specialists (IT workers) are offering their services to companies around the globe via remote work. The proceeds benefit the North Korean regime. There have already been contractual relationships between North Korean IT workers and German companies, too.

Facts

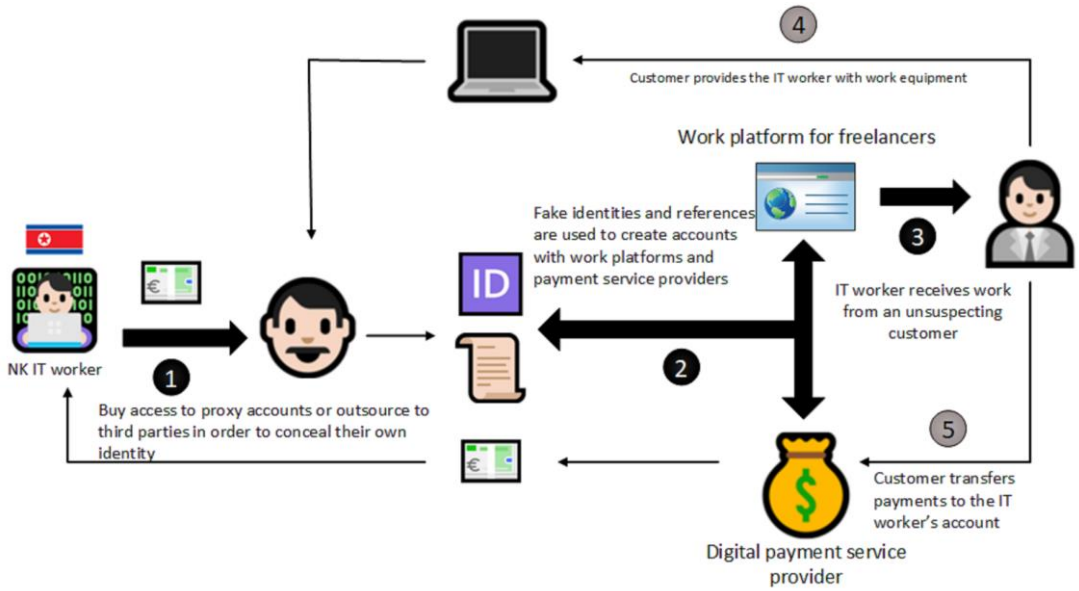
Search for freelance jobs and manifold fields of operation

IT workers sometimes work directly from North Korea but sometimes also from abroad. They mainly look for freelance jobs on platforms for freelancers such as “Fiverr”, “Upwork” and “freelancer.com”. From general IT support to programming apps and games or smart contract development, they cover a broad range of fields. Furthermore, they are active in various sectors, including healthcare, entertainment and finance.

Concealing the origin

North Korean IT workers professionally conceal their true origins and use purely fictitious as well as stolen identities. To this end, they use forged or stolen documents such as identity cards, passports and educational qualifications. Application photographs are sometimes generated using AI programmes. Alternatively, stolen photographs are altered using image editing software. The countries of origin that are indicated the most are South Korea and Japan. However, Eastern European countries are also repeatedly indicated. The false names that are used are sometimes adapted to the alleged origin. The geographical location is also adapted and the possibly North Korean location is concealed from the client by using Virtual Private Networks (VPN) or proxy accounts. The locations that are indicated the most are America, Japan and China. In order to further increase their credibility, North Korean IT workers, in addition to their accounts on freelancer platforms, often also have profiles on popular social media platforms and messenger services. In the profiles, the different accounts are sometimes linked

with each other. Most particularly, the platforms and services used include “LinkedIn”, “X” (formerly “Twitter”), “GitHub”, “Facebook”, “Telegram” and “Skype”. Often, the individuals pretend to have several years of professional experience in the field of IT and especially in the field of software development. The individuals often provide a broad spectrum of references in order to underline their expertise.



Digital payment

The payment is preferentially effected through cryptocurrency such as “Bitcoin” and “Ethereum” or digital payment solutions such as “PayPal” or “Wise”. That makes transfers easy to manage and difficult to trace. Occasionally, the IT workers use accounts that are provided by intermediaries in order to further conceal their identities. Declining advance or bonus payments frequently leads to aggressiveness and aggravation. Often, threats are made to publish parts of the company’s internal source code if demands are not met.

Impersonal communication

Preferably, communication takes place in written form via text messages. To this end, the chat feature of the freelancer platforms as well as independent applications such as “Telegram” are used. In most cases, video and telephone calls are avoided and meetings on site, for example to carry out face-to-face job interviews, are declined. The preferred language is English. However, communication in Korean is frequently offered too, even if another origin is indicated.

Inconsistent CVs

Personal details as well as information on the IT worker's professional career, such as spellings of names, work experience, educational qualifications and languages spoken, are often inconsistent. For example, if the alleged university studies took place in China, Japan, Malaysia, Singapore or other Asian countries, but the individual has so far only been employed in the US, in Korea or in Canada, this might point to an application from North Korea.

Conspicuous features of social media profiles and addresses

In many cases, social network profiles indicated do not match the CV provided. Sometimes, there are also several profiles under the same name but with different pictures. Residential and delivery addresses (for work equipment such as laptops and other hardware) often change in rapid succession. Accounts are characterised by long time spans of online activity. Furthermore, the customer ratings on the accounts on the freelancer platforms are usually extremely positive. The remuneration demanded, however, tends to be in the lower price segment.

Placement of malware

In confirmed cases, North Korean IT workers have been proven to have installed malware immediately upon receiving their work equipment.

Assessment

Potentially severe consequences

Companies that work with North Korean IT workers help the regime to procure foreign currency and thus indirectly support it in financing its nuclear weapons and missile programme. This can not only lead to risks regarding the reputation of the company due to compliance infringements but also to a breach of sanctions and ensuing legal consequences. Furthermore, there is a risk that intellectual property and internal data of a company are leaked.

Recommended actions

Measures for HR recruiters:

- Carry out job interviews in a face-to-face setting or as video calls so that you can verify the identity of freelancers.
- During video calls, please check for eye movements or long speaking breaks that might suggest that the answers are being read off somewhere.
- Avoid paying salaries exclusively with cryptocurrencies.
- Make sure that personal details such as the spelling of the name, the nationality, the place where the person is staying, the contact details, the course of education, former employers etc. are consistent throughout all profiles, portfolios and payroll accounts.
- Become suspicious when you are being asked whether communication could take place via separate platforms outside of the freelancer or work platform.
- Verify the qualifications indicated directly with the institutions that have issued them. Only use contact details that you have verified independently of information provided by applicants.

Measures for IT (safety) officers:

- Only send work equipment to the addresses indicated on the identification documents and become suspicious when allegedly no deliveries can be accepted at the address indicated.

- Make sure that remote staff cannot download programmes of their own choice (such as remote maintenance software) to their work equipment without consent.
- Check the access rights of new staff and make sure that staff members only have access to files they need for their work.
- Use end device protection and install new updates in a timely manner.

How to reach us

For information about threats to your sector in terms of espionage and sabotage, terrorism or violence-prone extremism and in case of concrete security-related questions or cases of suspicion, please contact our Prevention/Economic Protection Unit:

wirtschaftsschutz@bfv.bund.de
+49 30 18792-3322

Of course, you can also contact the domestic intelligence service of your respective German federal state. If you do not know the contact details, we will be happy to communicate them to you.

In any case, your information will be treated confidentially.

PREVENTION
ECONOMIC PROTECTION