North Korean "WaterPlum," commonly referred to as “Contagious Interview,” Cyber Actor Group Targeting IT Professionals; Activities of North Korean IT Workers in Japan, the United States and Europe

September 18, 2026

The National Police Agency of Japan (NPA), the National Cybersecurity Office of Japan (NCO), the US Federal Bureau of Investigation (FBI) and the US Department of Defense Cyber Crime Center (DC3), Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), Germany Federal Intelligence Service (BND) and Germany Federal Office for the Protection of the Constitution (BfV) have determined the following:

North Korean “WaterPlum,” commonly referred to as “Contagious Interview,” Cyber Actor Group – Executive Summary

The North Korean "WaterPlum" cyber actor group (commonly referred to as “Contagious Interview”) conducts cyberattacks by infiltrating unsuspecting job seekers’ computer networks, harvesting sensitive information, and stealing cryptocurrency. WaterPlum is victimizing individual IT professionals in Japan, the United States, Europe, and other countries.

The NPA and the FBI assess both WaterPlum cyber actors and some North Korean IT workers operate under the 313 General Bureau of the Munitions Industry Department subordinate to the Central Committee of the Workers Party of Korea.

WaterPlum actors pose as prospective employers to target software developers and IT professionals worldwide under the pretext of attractive job opportunities. They often impersonate legitimate Artificial Intelligence (AI), cryptocurrency, or Non-Fungible Token (NFT) companies and have also used recruiting services.

WaterPlum actors have infected at least 30,000 devices in more than 100 countries and exfiltrated funds or account credentials from over 7,000 cryptocurrency wallets. WaterPlum actors have transferred 1.7 billion Japanese yen (JPY) (equivalent to 10.71 million USD) of cryptocurrency assets to the Democratic People’s Republic of Korea (DPRK).

Some WaterPlum actors also operate as North Korean IT workers performing web system design and development tasks on corporate web systems for clients.
For the first time in Japan, authorities successfully identified, investigated, and dismantled a “laptop farm” operated by an enabler in Japan. Japanese authorities obtained evidence this cyber actor group transferred several hundred million Japanese yen in cryptocurrency to foreign locations outside of Japan.

The FBI continues to identify and prosecute US-based actors providing illicit facilitation services to North Korean IT workers. These prosecutions have occurred across the US, in a wide variety of jurisdictions, for multiple facilitation related crimes. The FBI is working with US-based victim companies, and appreciates victim cooperation in disrupting North Korean efforts to infiltrate private businesses and funnel salaries to the Kim regime and its military.

The NPA and the FBI will continue to cooperate with other partners to expose and combat cyberattacks that benefit North Korea and North Korean IT worker revenue-generation activities.

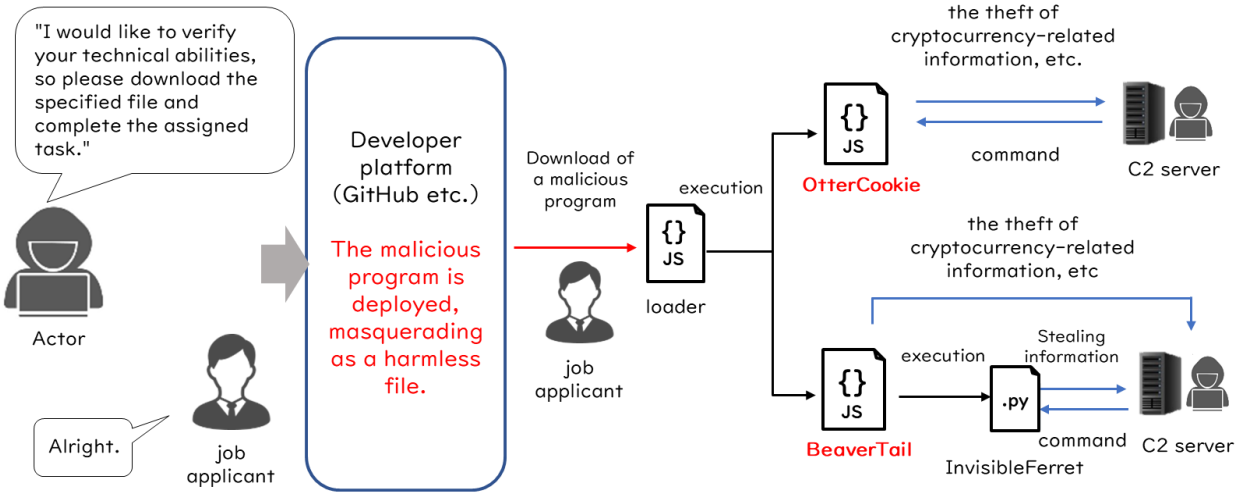
The WaterPlum tactics, techniques, and procedures (TTPs) disclosed in this announcement were discovered by the National Cyber Department of Japan’s Kanto Regional Police Bureau, relevant prefectural police, the FBI, and via cooperation and information sharing with private sector partners.

IT professionals in Japan and the United States -- and businesses that outsource or commission work via crowdsourcing or other means -- are encouraged to refer to the TTPs and mitigation measures below and implement appropriate security controls.

1. Targeting IT Professionals to Steal Cryptocurrency

The North Korean WaterPlum cyber actor group is targeting IT professionals, including web freelancers, to steal cryptocurrency assets from individual victims. The actors steal cryptocurrency wallet credentials and personal data from compromised victim networks or from companies that hire North Korean IT workers, enabling potential abuse or extortion involving sensitive information.

WaterPlum actors recruit job seekers internationally through social media platforms, online job platforms, gig work platforms, or freelance marketplaces. During the recruitment cycle, WaterPlum actors require job seekers participate in technical online virtual interviews or complete technical coding assignments. During interviews, WaterPlum actors instruct job seekers to download and execute malicious files, hosted on multiple online collaboration software developer platforms and code repositories, to complete a coding assignment or troubleshoot an error in the online video conferencing platform. WaterPlum actors upload malicious Node Package Manager (NPM[1]) packages embedded with either BeaverTail[2], InvisibleFerret[3], OtterCookie[4], OtterCandy[5], or StoatWaffle[6] malware and related variants.



Once WaterPlum actors obtain backdoor access to victim computer networks through malicious loader downloads, they use Remote-Access Trojans (RATs) to preserve connectivity, persistence, and pathways to pivot across victim systems. The actors use infostealers to exfiltrate the victim's sensitive data and cryptocurrency to a Command-and-Control (C2) IP address for remote management of infected devices or networks.

In some instances, WaterPlum actors use online chat platforms to communicate with US and Japanese developers. They also employ international enablers within Japan, the

---

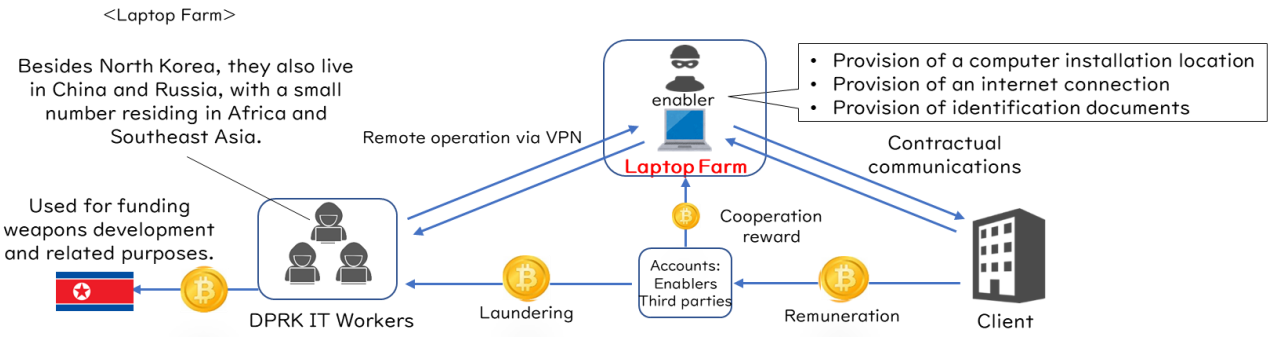
[1] NPM is the default package manager for the JavaScript runtime environment, Node.js, and is used by software developers to install, share, and manage third-party code libraries.
[2] BeaverTail is JavaScript-based malware hidden inside Node Package Manager (NPM) packages, and can be downloaded from GitHub or Bitbucket.
[3] InvisibleFerret malware is a Python-based backdoor to the victims' computer networks.
[4] OtterCookie is a JavaScript-based Remote Access Trojan (RAT) and information-stealing malware.
[5] OtterCandy malware combines the features of OtterCookie and RATatouille.
[6] StoatWaffle is a modular Node.js malware family combining a malware loader, credential harvesting components, and a RAT for persistence and pivoting across victim systems via malicious Microsoft Visual Studio Code (VS Code) projects. This malware uses blockchain-themed project repositories as decoys, embedding a malicious VS Code configuration file that triggers auto-run code execution when the folder is opened and trusted by the victim.

United States, and other countries to set up and manage “laptop farms” for remote device management. Enablers also create and manage virtual private servers (VPS) on the WaterPlum actors’ behalf, obfuscating the actors’ physical work locations while they perform contracted IT work and generate revenue.

Beyond immediate credential theft, successful infections provide WaterPlum actors opportunities to infiltrate organizations employing targeted developers, enabling espionage, intellectual property theft, and additional lateral movement in corporate environments. Stolen ID images can also be used by North Korean IT workers to impersonate victims and generate foreign currency. Other sensitive data targeted for exfiltration includes:

- Authentication data stored in web browsers (ID, password, etc.);
- Clipboard information, key-logs (recorded keystrokes), screenshots;
- Cryptocurrency-wallet data (private key, seed phrase, etc.); and
- Any files or data of interest to the actors on a PC or in shared folders (ID pictures of driver's licenses, passports, etc.)

2. North Korean IT Workers’ Use of “Laptop Farms” to Generate Foreign Currency



(1) Overview of Activities

A “laptop farm” is a location, often an enabler’s residence, where employment-related computers are set up and remotely controlled by North Korean IT workers. By leveraging laptop farms and VPS services, the IT workers obtain and perform employment contracts on crowdsourcing platforms or for domestic and international companies. The North Korean actors conducting this work are usually located in North Korea, China, or Russia, with a small number residing in Africa and Southeast Asia.

North Korean IT workers use ID images supplied by domestic enablers for impersonation, to obtain contracts, and receive payment. The actors also use enabler bank accounts to receive payments, with the enablers then transferring funds to the

actors. Evidence from our investigations suggests North Korean IT workers transferred several hundred million Japanese yen abroad, including cryptocurrency assets.

Paying remuneration to North Korean IT workers for commissioning work or facilitating their activities of generating foreign currency may constitute violations of domestic laws and sanctions against DPRK.

(2) Destructive Actions Taken by IT Workers

While North Korean IT workers primarily focus on revenue generation, there have been cases of additional malicious cyber activity. In one case, a North Korean IT worker extorted a company over payment and published its proprietary source code online. In another case, an IT Worker hired for website maintenance defaced the hiring company's website and rendered the site inaccessible.

(3) Mitigating North Korean IT Workers

- Do not provide remote-operatable PCs in your home to third parties indiscriminately. Brokers may offer work without explaining their true associations or the circumstances.
- If you suspect that a business partner or contractor may be a North Korean IT worker, contact the police immediately. Depending on individual circumstances, knowingly providing payment or personal ID images to North Korean actors could constitute a crime.
- When commissioning work, consider the possibility that subcontractors or further downstream partners may associate with North Korean IT workers. Clarify requirements and contractual clauses to reduce the risk of facilitating North Korea's scheme.
- During recruitment, follow the mitigation measures outlined in section 3. (2) to prevent hiring individuals who appear to be North Korean IT workers.
- Enforce security controls such as limiting information (source code, credentials, etc.) and access rights to the minimum necessary. If you discover a subcontractor is possibly a North Korean IT worker or otherwise malicious, promptly revoke accounts and sessions.

3. Recruitment Activities of North Korean IT Workers at Domestic Cryptocurrency Exchanges

(1) Details of Applicants and Interviews

In May 2025, a Japanese cryptocurrency exchange received an application for an engineering position. The applicant appeared to be a North Korean IT worker who submitted a forged resume through the company's recruitment form. The applicant accessed the recruitment form via a virtual private network (VPN) service. The applicant's resume contained the following characteristics:

- An unusually wide range of skills covering many programming languages, blockchain/cryptocurrency technologies, and cloud services (over 10 items of knowledge and experience for each).
- Education at a European university, followed in quick succession by work experience in various cities across Europe and Asia.
- During the video interview, the applicant had an Asian appearance, claimed he was born in Malaysia, and resided in Finland. The applicant claimed his native languages were Malay and Chinese.
- The interview was conducted in English; however, the applicant's English language abilities did not match his claimed academic and professional background. The applicant could answer simple questions but could not speak to most of the claimed skills in his resume.

The company recognized these behaviors as suspicious, did not hire the applicant, and no damage occurred.

- Observations from interviews with other suspected North Korean IT workers have included:

  - Refusals or excuses regarding in-person meetings.
  - Requests to receive payment in cryptocurrency.
  - Frequent glances at another monitor, as if reading from the screen.
  - Occasional background voices.
  - Repeated video or audio freezes.

(2) Countermeasures and Mitigations

- Be cautious when numerous applications arrive in short periods for positions that typically receive few applicants. If possible, verify that IP addresses generally match the applicant's claimed residence.
- Carefully check all contact information. Calling an applicant's phone number may reveal the number is out of service.

- During interviews, request detailed explanations of the skills listed on the resume. Even if a single individual appears to be applying, multiple people may be collaborating behind the scenes, inflating the perceived skill set. Verify certifications by checking registration numbers and, when inconsistencies arise, ask for detailed explanations.
- Ask questions about personal details such as the applicant's hometown, weather, or hobbies.
- North Korean IT workers tend to favor payment in cryptocurrency, and they may request that remuneration be sent to an account in another person's name.

4. CyberAttacks by WaterPlum Targeting Individual IT Professionals

(1) NPA Information on Scale of Malicious Activity

From around December 2025 through July 2026, WaterPlum exploited at least 30,000 PCs in over 100 countries (including Japan and the United States). The primary targets were individual web designers, engineers, and specialists in cryptocurrency, blockchain, and Web3 technologies. The actors transferred funds or account credentials from over 7,000 cryptocurrency wallets, exfiltrating at least 1.7 billion JPY (10.71 million USD) of cryptocurrency from victims on behalf of DPRK.

(2) Possible Follow-on Damage

Stolen IDs can be used by North Korean IT workers to impersonate victims and generate foreign currency. Stolen credentials may be leveraged to exfiltrate crypto assets, personal data, trade secrets, etc., from victims' employers, clients, or contracting parties. The actors can also use stolen sensitive information for extortion.

(3) Countermeasures and Mitigations

- Avoid executing code from untrusted third parties on your PC or machines handling cryptocurrency assets or personal data. Only run unknown code inside a sandbox or virtual machine, and verify no obfuscated or unreadable sections are present before execution.
- Be especially cautious of commands or scripts containing strings such as "curl," "base64," "-enc," "mshta," "lnvoke -WebRequest-uri," "iwr-uri," or "hidden." Avoid running these scripts unless you fully understand their behavior.
- If antivirus software detects an infection or you suspect compromise, immediately disconnect the impacted device from the internet to disable external

communications.
- Even after detection and removal, assume that data (including cryptocurrency wallet information) may already have been exfiltrated. Create a new wallet on a separate device, transfer all assets to it, and store the new seed phrase offline.
- Because undetected malware may remain on an impacted machine, back up essential data and perform a full reset of the operating system.
- For companies, deploy Endpoint Detection and Response (EDR) tools to monitor for malicious behavior and prevent exploitation.
- Avoid opening unknown VSCode projects, or only open in "Restricted Mode," which prevents execution of ".vscode/tasks.json" on launch. To open in “Restricted Mode,” answer “No” to the "Do you trust the author of the files in this folder?" prompt.
- Verify the contents of any ".vscode/tasks.json" file (in Restricted Mode or with another editor) for code that attempts to download or execute additional files.
- Avoid opening unknown projects in VSCode from a folder or file path you have previously marked as “trusted.”

(4) Observed Activities of WaterPlum Members

- Conducted online interviews using Al face-swapping software. After a few minutes the actors disabled their video and advised the target to disable their video due to network issues.
- On holidays celebrated in North Korea, the actors played games and watched soccer videos instead of conducting their usual malicious activities.
- Practiced Japanese pronunciation with text-to-speech software.
- Consistently used free machine-translation and AI service plans.

5. Relationship Between WaterPlum and North Korean IT Workers

WaterPlum actors and North Korean IT Workers used the same IP addresses when accessing laptop farms, using cloud-sourcing services, and applying for positions at the Japanese cryptocurrency exchange.

6. Final Remarks

The techniques described in this advisory are only examples; actors continuously evolve and refine their methods. Stay informed by monitoring alerts from domestic and international security agencies and by reviewing reports published by security vendors.

7. Acknowledgements

We would like to express our deepest gratitude to the following organizations for their cooperation in the preparation of this advisory:

- NTT Security (Japan) KK
- bitFlyer, Inc.

8. Reference Information (Links)

Alert to Countries, Companies, and Other Entities Regarding North Korean IT Workers (National Police Agency and other agencies)
https ://www.npa.go.jp/bureau/security/northkorea_IT/NK_IT_202607.html

Fact Sheet: Guidance on the Democratic People's Republic of Korea Information Technology Workers (May 16, 2022) –
https://ofac.treasury.gov/media/923131/download?inline

Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers (October 18, 2023) –
https://www.ic3.gov/PSA/2023/PSA231018

North Korean IT Workers Conducting Data Extortion (January 23, 2025) –
https://www.ic3.gov/PSA/2025/PSA250123

Private Sector Security Advisory 02/24: North Korean IT Workers (October 1, 2024) –
https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/economic-and-scientific-protection/2024-10-01-security-advisory.html