

SILENT PUSH THREAT RESEARCH

PROACTIVELY DEFENDING FINANCIAL INSTITUTIONS AGAINST NORTH KOREAN REMOTE IT WORKERS

How North Korean IT workers use Western proxies, stolen identities, and domestic IP addresses to get hired and paid, and how HR, fraud, and cybersecurity teams at financial institutions can detect them before onboarding.

IN THIS REPORT

	KEY FINDINGS	03
01	UNDERSTANDING THE NORTH KOREAN IT WORKER PROBLEM	04
	The scale of the problem	05
	Investigating a suspicious job advertisement	06
	Primary tactic: identity fraud and proxy hiring	07
	Interview fraud and the video capture	08
02	HOW THE SCHEME GETS PAST IDENTITY CHECKS	09
	Why a stolen or rented identity passes KYC and AML checks	10
	Laptop farms and the last hop	11
	What this means for financial institutions	12
	Tracing where a connection really starts	13
03	DETECTING NORTH KOREAN IT WORKERS BEFORE ONBOARDING	14
	Indicators of a North Korean IT worker	15
	Application data as a detection source	16
	How HR, fraud, and cybersecurity work together	17
	Defining the handoffs and next steps	18
	SOURCES	19

LEGAL DISCLAIMER: This report is for information only and reflects Silent Push research at the time of publication, with no warranty as to its completeness. It is not legal, compliance, or regulatory advice. Applicant IP addresses are personal data under U.K. and E.U. data protection law and several U.S. state privacy laws, so organizations collecting them should review lawful basis, privacy notices, and retention with their own counsel. Third-party trademarks belong to their respective owners.

KEY FINDINGS

- 01 Silent Push assesses with high confidence that "Tec Guru," a recruiter who advertised remote work on a Discord server, is a North Korean IT worker recruiting U.S., E.U., and Latin American citizens to act as proxies in job applications.
- 02 The proxy is offered 35% of the salary. The remaining 65% is sent back to the North Korean worker through cryptocurrency, wire transfers, or third-party payment processors.
- 03 The scheme passes document-based KYC and AML checks because the identity is legitimate and the connection appears to come from a domestic residential IP address, routed through residential proxies or laptop farms that use keyboard-video-mouse (KVM)-over-IP hardware.
- 04 Financial institutions are exposed as employers of remote technical staff and as the banks, payment providers, and electronic money institutions (EMIs) that receive and move the salary. In June 2025, the U.S. Department of Justice seized 29 financial accounts used to launder funds from these schemes.
- 05 Silent Push Traffic Origin data shows where traffic behind a domestic IP address starts. In one example in this report, a proxy IP in a U.S.-registered Starlink range (AS14593) carried traffic originating in Pyongyang.

Financial institutions can reduce this exposure by checking where applicant and employee connections originate, and by routing hiring, payroll, and connection data between HR, fraud, and cybersecurity teams before a new hire is onboarded.

— SECTION 01

UNDERSTANDING THE NORTH KOREAN IT WORKER PROBLEM

THE SCALE OF THE PROBLEM

North Korean operatives and professional money launderers have been drawing six-figure salaries from [Fortune Global 500](#) companies by exploiting a flaw in identity verification.

In June 2025, the U.S. Department of Justice [announced coordinated actions](#) across 16 states against North Korean remote IT worker schemes. According to court documents, the workers used stolen and fake identities and obtained employment with more than 100 U.S. companies. Silent Push has also found domestic U.S. IP addresses used by North Koreans and assesses that they were likely used to appear as suitable candidates for jobs at major U.S. corporations.

Once a North Korean IT worker is on the payroll, the salary flows through banks and payment providers that cannot see where the worker is really connecting from. On 31 July 2026, the U.S. Department of State and the FBI, with agencies from 10 other countries, issued a [joint alert](#) outlining North Korean IT workers' methods and warning the international community and private sector of the threat they pose.

This report draws on Silent Push research published between January and September 2026. It follows a North Korean recruiting scheme found on a Discord server, explains how it gets past the KYC (know your customer) and AML (anti-money laundering) checks run by employers and financial institutions, shows how connection origin data exposes it, and sets out how HR, fraud, and cybersecurity teams can spot a North Korean IT worker before onboarding.

KEY RISKS FOR EMPLOYERS

- 01 Remote identity fraud:** Candidates hired for remote roles may be sitting on camera while a completely different entity writes code, answers technical queries via chat, or controls the interviewee's machine via remote desktop.
 - 02 Insider threat and data exfiltration:** Once hired, these workers often use their corporate access to exfiltrate source code, steal intellectual property, and extort victim organizations.
 - 03 Sanctions compliance:** Companies that unknowingly hire or pay North Korean IT workers, even through a proxy, risk sanctions from the U.S. Treasury's Office of Foreign Assets Control (OFAC).
-

INVESTIGATING A SUSPICIOUS JOB ADVERTISEMENT

The September 2026 investigation began with a job advertisement on Discord. A cybersecurity colleague spotted it being promoted on a server channel named "Mouse Review," created to find and write computer mouse reviews.

The Discord account tecguru113 was responsible for spreading the fake job advertisement. A Silent Push principal threat research analyst created a fake persona and contacted the Telegram account Tecguru0618 mentioned in the ad. Based on technical indicators and the representative's speech patterns, among other flags, Silent Push assesses with high confidence that the representative, "Tec Guru," is a North Korean IT worker.

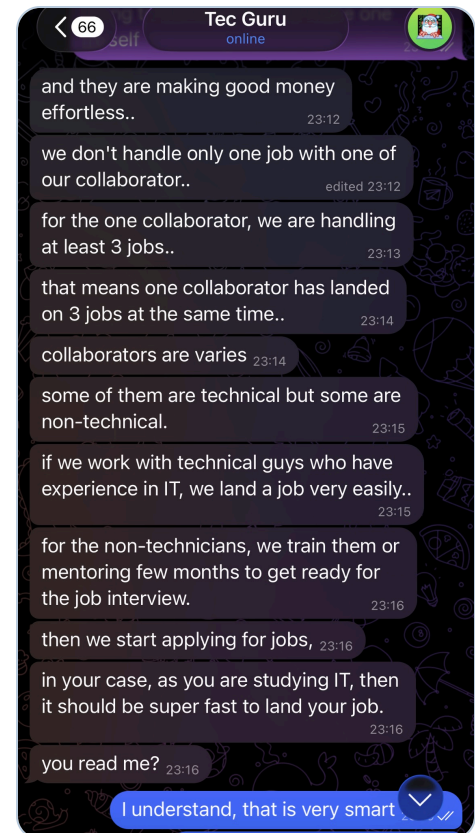
SCREENSHOT OF THE JOB RECRUITMENT SCAM WEB PAGE

IDENTIFIER	DETAIL
Discord account	tecguru113 · ID 1453753519436861505
Telegram	Tecguru0618 · @tecguru0618
Target regions	U.S., E.U. and LATAM: Brazil, Mexico, Argentina, Colombia, Chile
Contact channels	Telegram, VoIP numbers with a +1 (North America) country code

PRIMARY TACTIC: IDENTITY FRAUD AND PROXY HIRING

The North Korean IT worker's primary goal is proxy hiring: using Western or Latin American citizens as the "face" and legal identity to bypass sanctions, KYC controls, and regional hiring restrictions. The advertisement explicitly requests a proxy to "turn on your camera during interviews," "communicate with clients," and "represent the necessary skills confidently."

The proxy accepts salary payments into a local U.S. or E.U. bank account and transfers the balance back through cryptocurrency, wire transfers, or third-party payment processors. The scheme is framed as a standard "subcontracting arrangement," with reassuring language such as "100% Legitimate" and "100% Privacy Guaranteed" to reduce the proxy's perception of legal risk.



THE THREAT ACTOR EXPLAINED THE SCAM IN THE CHAT LOG

65%

Salary share transferred back to the North Korean IT worker

35%

Salary share kept by the recruited proxy

INTERVIEW FRAUD AND THE VIDEO CAPTURE

To bypass live technical assessments, the threat actor relies on real-time assistance and remote access tools: live coaching over Google Meet while the proxy sits on camera, remote desktop control through AnyDesk, TeamViewer, or Chrome Remote Desktop, and AI tools such as ChatGPT to generate responses on the fly.

"I can remotely access your screen and complete coding tasks while you continue the conversation smoothly."

TEC GURU, TO A SILENT PUSH ANALYST PERSONA

DURING THE VIDEO CALL

- 01 The analyst prompted Tec Guru to enable his video feed while keeping the persona's camera off.
- 02 Pretending not to understand remote software, the analyst tried to get a screen share. Tec Guru declined.
- 03 As soon as Tec Guru heard "North Korea," he turned off his camera.
- 04 Asked to disparage North Korea, he avoided saying anything negative.

ATTRIBUTION

Silent Push bases the attribution on the technical analysis that followed the call, covering the financial, operational, and infrastructure data the operator provided. When asked for VPN recommendations, Tec Guru named Astrill VPN, a service commonly used by North Korean threat actors. Additional technical detail is published in Silent Push TLP Amber reports for enterprise customers.

— SECTION 02

HOW THE SCHEME GETS PAST IDENTITY CHECKS

WHY A STOLEN OR RENTED IDENTITY PASSES KYC AND AML CHECKS

The recruiting scheme depends on two things passing the employer's and the bank's checks: the proxy's identity documents and the operator's internet connection.

KNOW YOUR CUSTOMER (KYC)

Checks that confirm a person or company is who they claim to be before they are hired, onboarded, or paid.

ANTI-MONEY LAUNDERING (AML)

Checks that money is not moving to criminals or sanctioned entities. Employers, banks, and payment providers all rely on them.

Traditional KYC and AML protocols rely on static document validation. These processes fail when an adversary presents a legitimate, stolen identity that is backed by a clean residential IP address. When organizations cannot distinguish between a local user and a keyboard-video-mouse (KVM)-over-IP relay, their payroll can end up paying a sanctioned entity.

HOW OPERATORS MAKE A CONNECTION LOOK LOCAL

Security tools that rely on historical databases flag actors that are already known. An adversary that rotates infrastructure regularly stays out of those databases.

Residential Proxy-as-a-Service (RPaaS). The first method uses rented residential IP addresses.

Fraudsters and sanctioned actors use residential proxies to appear as legitimate domestic customers. This allows them to bypass geo-fencing and pass initial KYC checks undetected.



Attackers use residential proxy networks



Automated credential stuffing & IP rotation



"Suspicious logins" become noise. High-Risk sessions are hidden.

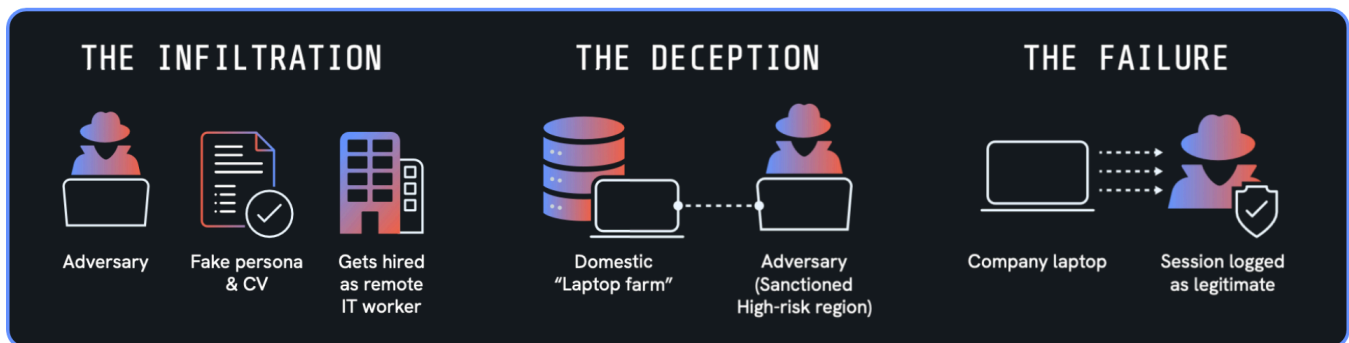


The failure: Risk engines bypassed, impossible to tell attacker from customer

RESIDENTIAL PROXY-AS-A-SERVICE · SOURCE: SILENT PUSH, JAN 2026

LAPTOP FARMS AND THE LAST HOP

Laptop farms and KVM switches. The second method uses physical hardware inside the target country. A facilitator keeps employer-issued laptops in a domestic residence, and the North Korean worker controls them remotely through KVM-over-IP devices. In June 2025, the U.S. Department of Justice [reported searches](#) of 29 known or suspected laptop farms across 16 states. Because the software runs on a legitimate local machine, security tools see a domestic ISP and a local MAC address.



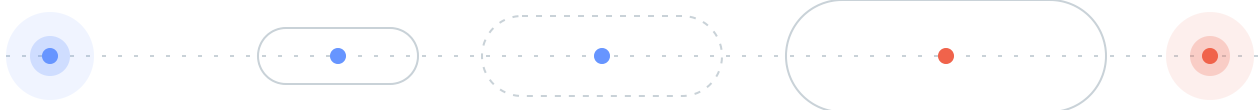
LAPTOP FARMS AND KVM SWITCHES · SOURCE: SILENT PUSH, JAN 2026

BEYOND LAST-MILE GEOLOCATION

Identity systems that rely on IP geolocation only see the exit node, or the "last hop." If the IP address says "London," the alert is dismissed. Banks that only see the last hop cannot see a transaction's true geographic origin, which lets illicit funds pass through them.

WHAT THE TWO METHODS HAVE IN COMMON

In both methods, the employer and the bank see a legitimate identity connecting from a domestic IP address, so document checks and IP geolocation both pass. The salary is then paid into a domestic account that the proxy controls. For financial institutions, this creates exposure in two places, set out on the next page.



WHAT THIS MEANS FOR FINANCIAL INSTITUTIONS

Financial institutions are exposed to this scheme in two ways: as employers that hire remote technical staff, and as the banks, payment providers, and electronic money institutions (EMIs) that hold the proxy's account and process the salary.

AS AN EMPLOYER

A North Korean IT worker hired through a proxy receives the same access as any other new hire. The exposure matches the risks on page 05: remote identity fraud, data exfiltration, and OFAC sanctions risk for paying the worker, even through a proxy.

AS AN ACCOUNT PROVIDER

The proxy receives the salary into a local U.S. or E.U. bank account and sends the balance on through cryptocurrency, wire transfers, or third-party payment processors. The account holder presents a legitimate identity, so document-based KYC on that account passes.

"Trust is a liability in an era where an adversary can rent a domestic identity and a clean residential IP for a few dollars."

SILENT PUSH, THE INVISIBLE INSIDER, JAN 2026

WHERE THE MONEY GOES

The operators and the money launderers working with them move illicit revenue through shell companies and EMIs to evade international sanctions, or cash out through high-risk crypto mixers. The U.K. Office of Financial Sanctions Implementation (OFSI) has highlighted several indicators of this activity, including upstream connection mismatches where domestic IPs show active links to high-risk jurisdictions. In June 2025, the U.S. Department of Justice [seized 29 financial accounts](#) used to launder illicit funds from North Korean remote IT worker schemes.

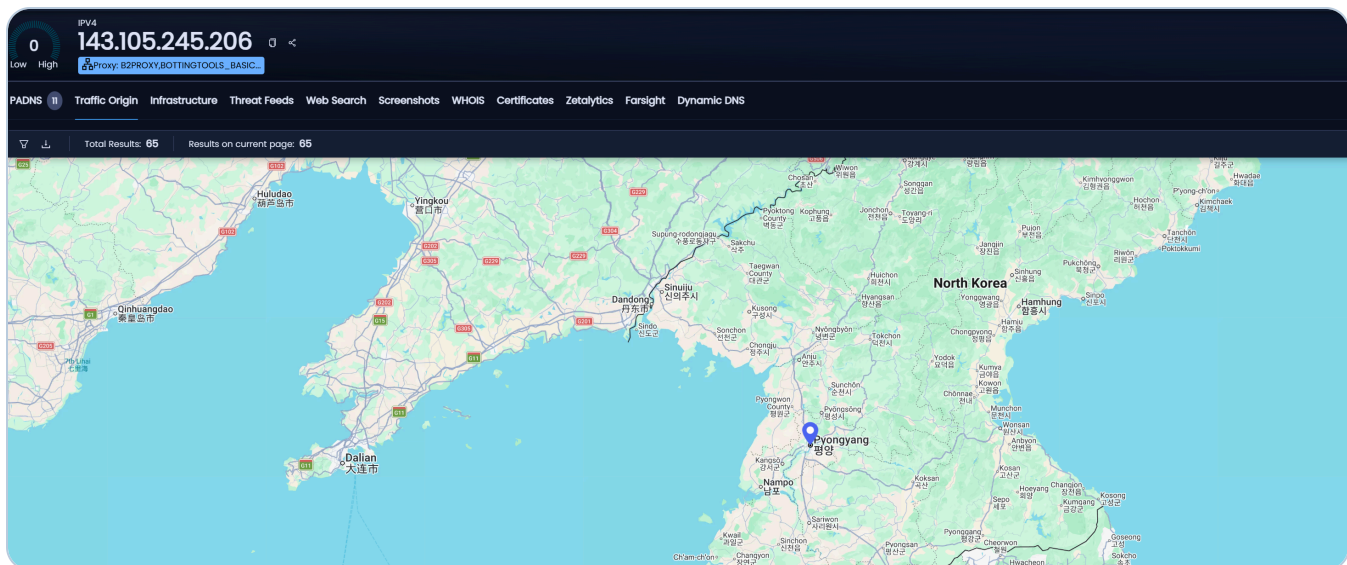
Checking for an upstream mismatch needs data on where a connection starts, in addition to the IP address the institution sees.

TRACING WHERE A CONNECTION REALLY STARTS

Silent Push [Traffic Origin](#) data identifies the countries associated with an IP address, showing where traffic physically starts. Identity and security tools typically see the local address used to hide a connection. Origin data exposes the upstream infrastructure used to spoof a location and shows whether the connection starts in a high-risk or sanctioned country.

NO.	HOW ORIGIN DATA HELPS TRACE THIS ACTIVITY
01	Automatically assess applicant and employee logins and identify when an IP address is masking traffic from an unexpected location or country of concern.
02	Combine with Silent Push residential proxy data, which identifies tens of millions of residential proxy IPs and their service providers, to separate innocuous residential IPs from those rented for criminal use.
03	Evaluate host diversity, subnet reputation, and behavioral density to reveal a true upstream source, even when it is masked by VPNs or residential proxies.

A background check confirms the identity a candidate presents. Origin data adds a second check: whether the person using that identity is physically located where they claim to be.



U.S. STARLINK PROXY IP 143.105.245[.]206 WITH TRAFFIC FROM PYONGYANG

— SECTION 03

DETECTING NORTH KOREAN IT WORKERS BEFORE ONBOARDING

INDICATORS OF A NORTH KOREAN IT WORKER

The indicators below come from Silent Push research into North Korean IT worker activity. Each one pairs a technical signal with the risk it points to.

RED FLAG	TECHNICAL INDICATOR	RISK PROFILE	SEEN BY
Geographic mismatch	Domestic IP with an active upstream connection to a sanctioned or high-risk zone	High: sanctions evasion	Cybersecurity
Infrastructure density	Numerous unrelated devices (high host diversity) appear to originate from a single residential IP	Medium to high: proxy usage	Cybersecurity
Interview and meeting friction	Persistent refusal to appear on camera, unusual audio lags, or background environments inconsistent with claimed locations	High: identity spoofing	HR
Employment anomaly	A "highly skilled" employee who fails to complete basic tasks, refuses 1:1 video syncs, or delegates work to "partners"	High: work outsourcing, potentially North Korean	HR and hiring managers
Financial redirection	Urgent requests to pivot salary payments to an EMI or third-party account shortly after onboarding	High: money laundering	Fraud and payroll

Each indicator is recorded by a different team, as the last column shows, so detection depends on HR, fraud, and cybersecurity sharing what they find. The next three pages cover the applicant data these teams already hold and how to route it between them.

APPLICATION DATA AS A DETECTION SOURCE

North Korean IT workers almost always enter through a standard hiring process. That process records technical data about each applicant, which an analyst can check before the worker is onboarded.

WHAT HIRING SYSTEMS ALREADY COLLECT

Applicant data usually stays in the applicant tracking system (ATS) and does not reach the cybersecurity team, even though most of it exists before equipment ships and before payroll is set up. The timeline below shows when each data point is created and what an analyst can establish from it.

01 · APPLICATION	Whether the connection originates in a high-risk or sanctioned country, and whether a residential proxy, VPN exit, or KVM relay sits between the applicant and the employer
Job application portal IP and later HR portal logins	
02 · SCREENING	Use of VoIP numbers carrying a +1 (North America) country code and contact routed through Telegram, both documented in this recruiting scheme
Contact numbers and messaging handles	
03 · REFERENCES	Infrastructure behind a referenced employer or staffing agency, and any link to adversary infrastructure already tracked
Email domains on the CV and from references	
04 · TECHNICAL REVIEW	Shared accounts, reused commits, and contribution timing inconsistent with the claimed location
Repository and portfolio links	
05 · EQUIPMENT SHIPPING	Laptop farm indicators, including an address that moves shortly after onboarding
Shipping addresses and later changes	
PAYROLL SET UP	Most of this data exists before the first salary payment, which gives an analyst time to check it.

Applicant IP addresses are personal data under U.K. and E.U. data protection law and several U.S. state privacy laws. See the legal disclaimer on page 02.

HOW HR, FRAUD, AND CYBERSECURITY WORK TOGETHER

Applicant data only works as a detection source once it leaves the ATS and reaches the teams that can act on it.

Security tooling alone cannot resolve this activity. HR, fraud, and cybersecurity teams often work separately and use different terms for the same risk. A recruitment team may not recognize a “geographic mismatch” as a risk, and a SOC analyst cannot act on a declined 1:1 video sync if nobody reports it. In a financial institution, the fraud and financial crime team already runs KYC and AML checks on customers, and the same checks can be applied to a new hire's identity and to the account that receives their salary.

In organizations that have successfully stopped these workers before onboarding, hiring teams were trained on the indicators and applicant data reached the cybersecurity team early enough for an analyst to act on it.

FUNCTION	RESPONSIBILITY	CONTRIBUTION TO DETECTION
HR and Talent	Workplace integrity	• Background checks and know your employee verification • Unscheduled live video calls • In-person verification, where geography allows • Continued video engagement after hire • Recruiter training on deep fake technology and interview friction • Application data
Fraud and Risk	Anti-fraud and financial crime controls	• KYC on the individual • Know your business (KYB) checks on any contractor entity • AML screening on the payment destination • Duplicate bank detail checks across payroll records • Escalation of early salary redirection to an EMI or third-party account
Cybersecurity	Investigation and attribution	• Verification of where a connection originates • Residential proxy and laptop farm identification • Infrastructure analysis of the domains behind fake hires, agencies, and references • Indicators of Future Attack® (IOFAs) that identify additional infrastructure linked to known clusters

DEFINING THE HANDOFFS AND NEXT STEPS

These controls work as one process only where the handoffs are defined in advance.

Agree who receives each type of finding before a case comes up. For example, failed video verifications go to the cybersecurity team, a named owner in HR can pause an offer while a flagged connection origin is checked, and early requests to move salary to an EMI or third-party account go to the fraud team.

RECOMMENDED ACTIONS

- 01 Verify that applicants are physically located where they claim to be during job interviews.
- 02 Verify the upstream origin of a connection, not only the final residential hop, so a residential proxy or KVM relay does not pass as a local user.
- 03 Treat early requests to move salary to an EMI or third-party account as a sanctions and money laundering signal.
- 04 Train recruiters and hiring managers on the interview and employment anomalies in this report, and repeat the session whenever the hiring team changes.
- 05 Agree which applicant fields HR shares with the cybersecurity team, and define the point in the process at which they are shared.
- 06 Open one escalation channel for live cases, with a named owner in HR, fraud, and cybersecurity, and return a result to the team that raised each case.
- 07 Review flagged and cleared hires across all three functions each quarter.

FREE RESOURCE

RISK-BASED HIRING PIPELINE

A scoring guide that combines Silent Push enrichment with phone, identity, and reporting signals to rate each applicant as high, medium, or low risk.

[GET THE GUIDE →](#)

SOURCES

This report draws on three posts published on the Silent Push blog and two U.S. government publications. The full versions carry additional screenshots, chat logs, queries and indicators.

21 JAN 2026 [The invisible insider: why AML and KYC compliance fail against digital deception](https://silentpush.com/blog/the-invisible-insider)
silentpush.com/blog/the-invisible-insider

09 FEB 2026 [Silent Push Traffic Origin data combined with residential proxy data uncovers suspicious Chinese VPN](https://silentpush.com/blog/traffic-origin-chinese-vpn)
silentpush.com/blog/traffic-origin-chinese-vpn

14 SEP 2026 [Silent Push exposes North Korean IT worker recruiting facilitators through Discord servers](https://silentpush.com/blog/nk-it-worker)
silentpush.com/blog/nk-it-worker

EXTERNAL SOURCES

30 JUN 2025 [U.S. Department of Justice: Justice Department announces coordinated, nationwide actions to combat North Korean remote information technology workers' illicit revenue generation schemes](https://justice.gov/opa/pr)
justice.gov/opa/pr

31 JUL 2026 [U.S. Department of State, FBI, and international partners: Alert to countries, companies, and other entities regarding North Korean IT workers](https://ic3.gov/CSA/2026/260731.pdf)
ic3.gov/CSA/2026/260731.pdf



NEUTRALIZE BEFORE COMPROMISE

Silent Push flags residential proxies and masked connection origins so hiring, KYC, and fraud teams at financial institutions can act before an operative is onboarded.

[BOOK A DEMO →](#)[RESEARCH HUB →](#)