HAYDEN MCKENZIE
INDEPENDENT SECURITY RESEARCHER

RESEARCH

DISSECTING THE IDENTITY LIFECYCLE

An operation's own archive — a manual on stealing an identity and surviving a background check, an interview answer bank, an expense ledger, and a signed revenue-sharing contract with an American. Eleven stages, from choosing a victim to cashing out.

DATE	TOPIC	SERIES	REPORT
13 Aug 2026	DPRK Operations	Inside a DPRK IT Worker Operation	02

CONTENTS

DISSECTING THE IDENTITY LIFECYCLE

EDITOR'S NOTE

This investigation was conducted using open-source intelligence methods — no unauthorized access occurred at any point. The material mentioned throughout the article came from a publicly reachable file-transfer link with no access control whatsoever. Screenshots are likely redacted: SSNs, driver's license numbers, DOBs, passport numbers, home addresses, and credentials are removed. All materials of investigative value are in the process of being referred to federal law enforcement and key details have been heavily redacted. This investigation continues *Inside a DPRK IT Worker Operation: How North Korea Outsources Job Fraud at Scale*, published May 19, 2026. Employers who believe they were impacted: intel@haydenmckenzie.com.

Investigative Methodology

I hold and utilize a paid account with a legitimate, GDPR-compliant breach-intelligence platform. I queried it against an identity confirmed to be identified as DPRK-affiliated in a prior investigation. That query surfaced a sendgb.com transfer link — a mainstream file-sharing service in the same category as WeTransfer — sitting in the device's browser history. I never accessed, connected to, or interacted with that device itself; I queried a commercial index of already-public data.

Before touching the link, I confirmed it was live via urlscan.io, a standard passive check that also produced an independent, timestamped record of the link's state. The transfer had no password, no login, and no access control of any kind — anyone holding the URL could retrieve the same files. I downloaded the contents (zip archives) into an isolated sandbox and examined them statically; nothing was executed. No credential was presented, none was requested, and no authentication or technical barrier was bypassed.

Material of clear investigative value — identity documents, victim data, financial records, evidence of a physical U.S. facilitation site — is being referred to law enforcement. Everything tied to existing and future referrals was either stripped or redacted.

How to Read This Article

This article builds on work other researchers have already done well. Group-IB, Flare and IBM X-Force, Nisos, and DTEX Systems have each documented pieces of this system — personas, back-office infrastructure, organizational structure, self-funding quotas — and what follows corroborates a lot of it independently, from a different source. To supplement existing intelligence, this article details and archive involving a NK operators own training materials — a written manual on stealing an identity and surviving a background check, an interview answer bank, an expense ledger, a signed revenue-sharing contract with an American.

The article is in two parts. First, a short update on what's changed since the bidding piece I published in May — different pricing, additional services, and a few other things. Then the new intelligence: a multi-stage lifecycle walkthrough, in order, from choosing a victim to cashing out, each stage anchored to a specific document in the archive.

Together, old and new techniques give a picture of how this operation runs **now** — not just a snapshot from whenever it was last written about.

Section 1 | Continued

What the Last Article Established

In my previous article, *Inside a DPRK IT Worker Operation: How North Korea Outsources Job Fraud at Scale*, I investigated a group of DPRK IT workers who were participating in a growing trend of **outsourcing their job application process to third-party gig workers**.

Incase you didn't read my previous article, the basics of their operation included:

- **Buyers** — DPRK-operated personas needing applications submitted at volume.
- **Bidders** — third-party gig workers paid **$0.05–$0.10 per application submitted**, plus **$1–$3 per interview secured**, with rates set by interview yield, spreadsheet accuracy, and resume tailoring quality.
- A workflow in which the bidder (typically) creates a persona's Gmail account, configures email forwarding to the buyer's central inbox, **tailors the resume** with ChatGPT and ResumeKit, **submits through Workday and similar systems**, and **logs everything in a shared spreadsheet** with color-coded status columns.
- Payments are in **USDT over BEP20**.

The main takeaways from that article were the separation of labor and their ability to avoid VPN-based detections through Workday and other applicant platforms:

- The bidder **never needs to be able to impersonate a senior engineer**. They only need to submit applications at volume and configure a forwarding rule.
- The buyer (or DPRK operative) can further **eliminate the risk of being flagged through talent acquisition services** (such as Workday) for using VPS or VPN infrastructure (such as Astrill).

Notable Observations Since May

Bidding-as-a-Service: "Bid Pro"

The bidding arrangements documented in my previous article are still accurate, however, activity shows that **individuals are starting to advertise dedicated services**, marketed on the open web, **with a portfolio**, price lists, and payment terms.

The greatest example of this involves **BidPro** (bidpro-ochre[.]vercel[.]app), a website hosted on a free Vercel subdomain that advertises strategic, ATS-optimized applications for clients. The operator behind BidPro labels themselves as a "Job Bidding Specialist" focused on "Reverse Recruiting" while claiming that they've completed 15,000+ applications and served 30+ clients.

The previous article documented a market at **$0.05–$0.10 per application** with **$1–$3 bonuses per interview secured.** BidPro publishes a two-tier menu instead, priced per batch:

Normal Applications ("standard high-quality bids") — $10 for 100, $20 for 200/250, $24 for 300, $34 for 400, $40 for 500. Effective rate: **$0.08–$0.10/app.**

Tailored Applications ("ATS-optimized + custom work") — $17 for 100, $30 for 200/250, $42 for 300, $54 for 400, $65 for 500. Effective rate: **$0.13–$0.17/app.**

The prices for these specialized services, especially those that recruit groups of bidders, typically seem to fall above the average rate of pay per application.

The site's "**Past Clients**" grid names fifteen clients, each with a one-line campaign blurb and a live link to a Google Sheets application log. Within these Google Sheet documents are hundreds of rows displaying companies and their associated job listing URLs, all mapped out per role and application date.

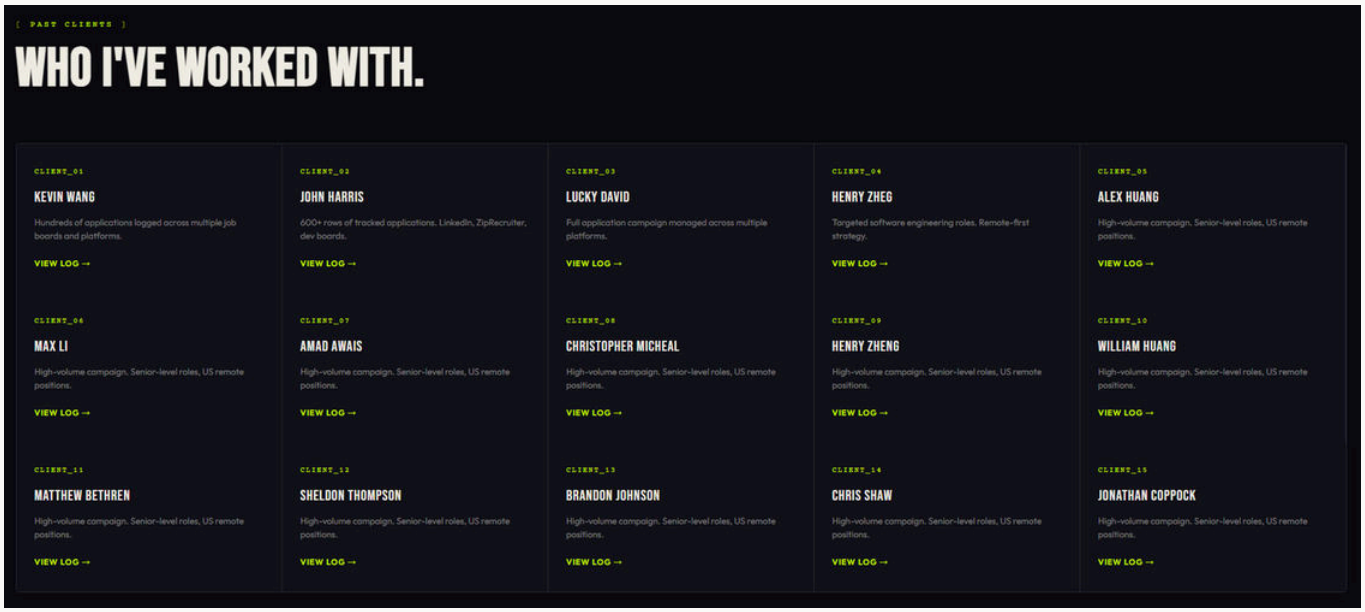


FIG. 01 | List of 15 different identities with publicly available Google Spreadsheets

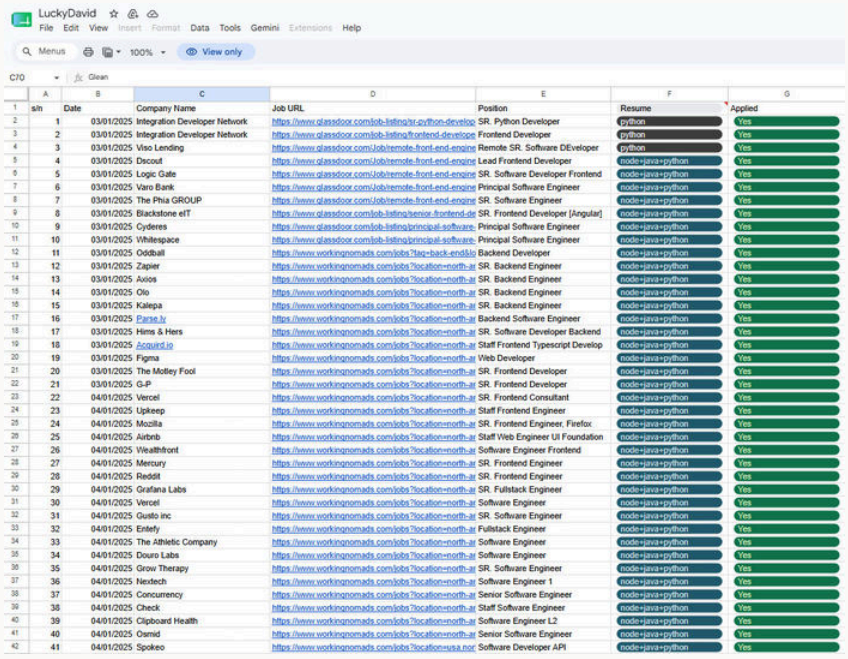


FIG. 02 | Closer look at one of the Google Spreadsheets associated with an identity

A "**Proof of Work**" section adds a screenshot of a supposedly real inbox with recruiter replies and a sample application log.

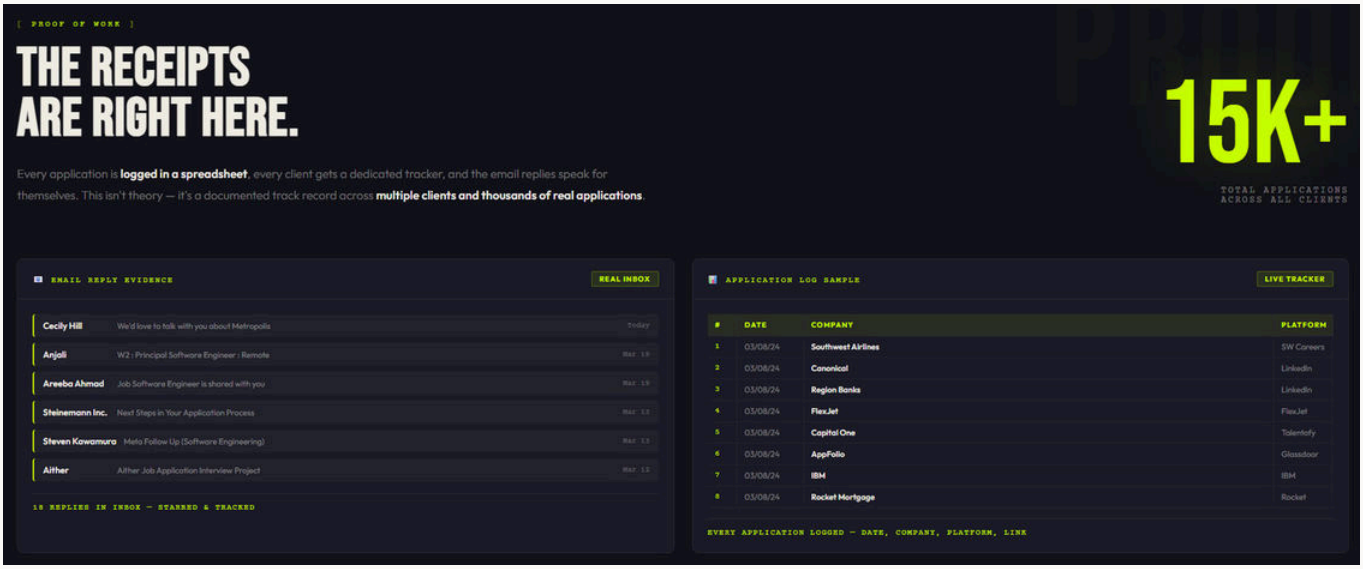


FIG. 03 | Additional records showing how efficient they are

The contact page features a WhatsApp number in the **+234** country code — Nigeria — plus a Telegram handle that's a common Yoruba surname (I will cover the significance of this shortly).

> Note: As of 8/13/2026, only eleven of the fifteen spreadsheets are still live or public. These spreadsheets include applications submitted between September 2024 and September 2025.

Where the Applications Come From: Kenya and Nigeria

Kenya and Nigeria seem to be the most common countries these bidders operate out of. For a DPRK applicant, utilizing a Kenyan or Nigerian IP address is usually better than settling for a known VPS or VPN service such as Astrill.

In the event a bidder mentions that they are based in the United States, most NK operatives tends to ignore the need for a bidder and requests (or sometimes begs) the would-be bidder to let them remote into their laptop or computer via Anydesk.

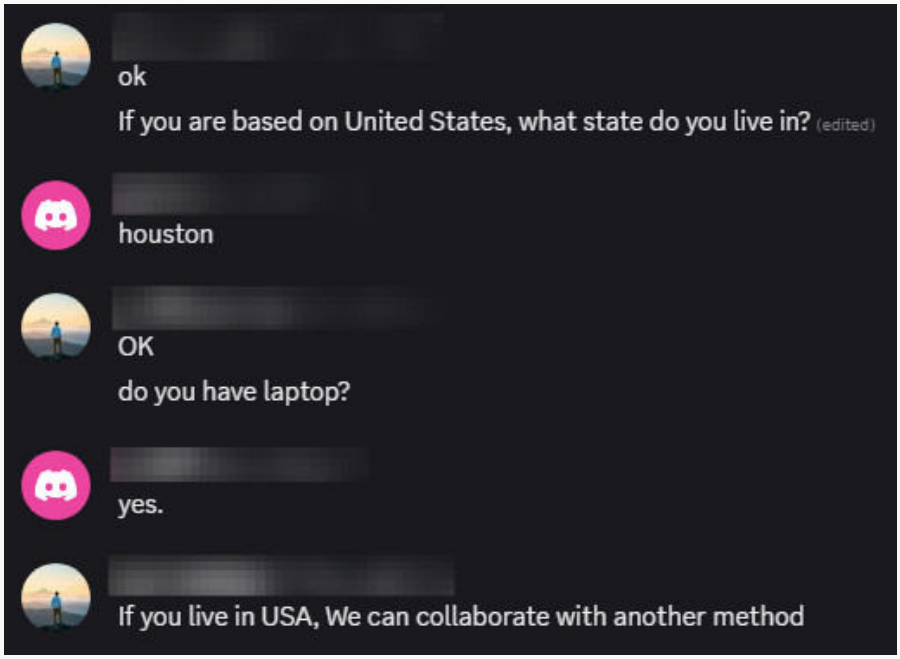


FIG. 04 | US-based bidder getting asked to collaborate differently

Note: As an analyst, if you are viewing your companies applicant logs and notice suspicious naming conventions (e.g..dev@domain.com, suspicious resume names) it may be worth it to check what country the IP address resolves back to (especially if you are a US-based company).

The Resume Says Outlook. The ATS Says Gmail.

In analyzing the personas, resumes, and submission information from these Discord groups, I observed that often times, **the email on the resume PDF does not match the email used to register the applicants account in talent acquisition platforms such as Workday and Greenhouse.**

The cause can partially be attributed to the account architecture documented in my last article. The Gmail account is operational: created by the bidder, forwarding to the buyer's central inbox, used to register and submit. The Outlook address on the resume belongs to an older persona layer and is carried forward in a static document nobody re-checks. Legitimate candidates do this occasionally, however, it can be used as one of many indicators when hunting for possible DPRK applicants.

Section Two | Identification

An introduction as to how the data was obtained and what it contains.

The Handoff

How The Archive Was Found

The process for how this data was acquired is documented in the Methodology section above; in brief, a paid query against a commercial stealer-log index, run against a device already identified as DPRK-affiliated in the previous investigation, returned a **SendGB transfer link** sitting in the devices browser history. A passive urlscan check confirmed it was live. Behind it were **zip archives** containing everything described in this article.

```
33 Url: https://sendgb.com/
34 Title: SendGB | Send Large Files | Free file transfer
```

FIG. 05 | Infostealer logs displaying an active SendGB URL

SendGB is a mainstream free file-transfer service in the same category as WeTransfer. Upload requires no account; download requires no account. Crucially, **transfers expire.** The free retention window is measured in days, not months.

What makes SendGB attractive to threat actors is that file uploads can be set to **expire in a single day** (with the default expiration time set to three days). An abandoned cloud folder left open for years isn't likely to contain important or up-to-date information, however, a file-transfer link with a retention window measured in days is essentially a handoff in progress. Somebody packaged the operation's manuals, reports, identity documents, contracts, and financial records into zip archives and sent them elsewhere, and the only reason any of it is visible is that one machine in that exchange was infected with an infostealer.

These documents aren't just one person's working files, they are a collection of identities, infrastructure credentials, and paperwork bundled together as a unit. This goes hand-in-hand with what Group-IB described in a similar assessment about the persona archive they recovered, describing it as showing how packages were assembled, maintained, and *potentially handed over between operators or working groups.*

A link that dies in three days leaves no persistent or indexable artifacts. If you compare it to the archive's other choices, such as protectedtext.com, it thrives in the fact that information doesn't linger.

What's In The Archive?

The zip archive contained years of accumulated material, organized by identity, by function, and by year, and bundled for delivery. **The material goes as far back as 2023 and is dated as recent as 2026.**

Category	Contents
Training manuals	A complete written curriculum: victim selection, identity acquisition, infrastructure, resumes, application volume, LinkedIn laundering, interview performance, U.S. business formation
Per-identity dossiers	One file per persona — credentials, documents, KVM logins, VPS access, mail, stubs, shipping addresses
Identity documents	Driver's licenses, Social Security cards, passports belonging to real people
Background reports	Full commercial background checks on victims, including relatives and vehicle records
Financial records	Operational expense ledgers, pay stubs, direct deposit confirmations, payment platform KYC material
Contracts	Signed revenue-sharing agreements between operators, facilitators, and an intermediary LLC
Recruitment material	Written pitches used to solicit American collaborators
Employment artifacts	Company-specific resumes, offer letters, onboarding paperwork
Imagery	Screenshots of company systems, and photographs of the operators themselves

FIG. 06

What makes this new collection stand out is the first and the last two rows. Prior reporting has documented persona packages — Group-IB's Dominic Williams and Dejan Teofilovic archive — and in Flare and IBM X-Force's article they

discuss timesheet and “RB Site” material. In this article, however, I aim to combine that existing intelligence with new and up-to-date methods such as a thoroughly crafted job hunting document and LLC creation instructions.

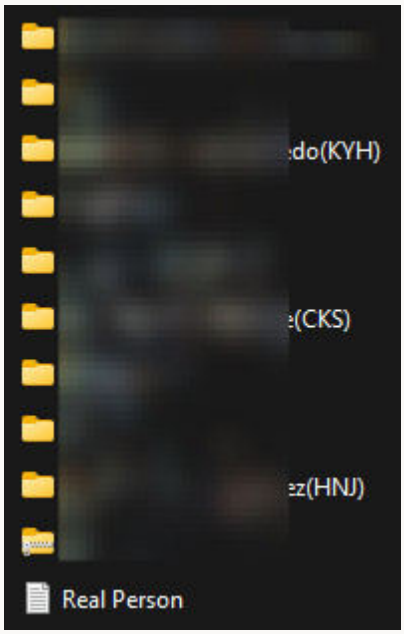


FIG. 07 | Identities directory with a “Real Person” document

Section Three | The Identity Lifecycle

Eleven stages. Each is documented somewhere in this archive.

The next few parts are centered around a step-by-step document, Job Hunting.pdf, that details a DPRK ITW’s entire starting process and helps establish personas.

Stage 1 Choose a Victim

The first and most consequential page of the operation’s training manual defines what makes a stolen identity usable. The criteria are explicit:

Must be a U.S. citizen. Green Card and H-1B holders are rejected by name. The stated reasoning is that visa status creates additional documentation, background check, and verification failure points. The manual is direct about it: most companies require citizens, and non-citizen statuses are a risk.

Must be roughly 28 to 35 years old. The reasoning is purely commercial. A younger identity can only credibly support junior roles, and junior roles are — in the document’s own phrase — a small budget. The 28–35 band is described as optimal for the U.S. IT market.

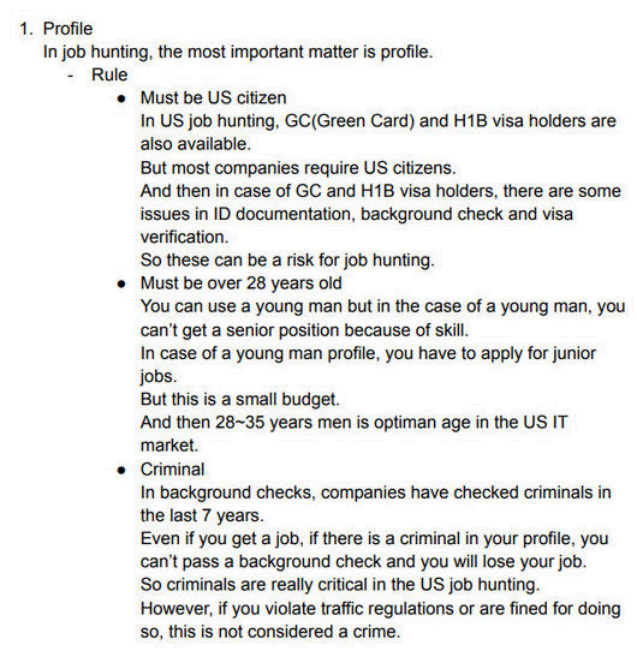
Must have no criminal record in the last seven years. Seven years matches standard U.S. background check lookback windows. Traffic violations and fines are explicitly noted as acceptable.

In addition to these requirements, a list of preferable attributes are also listed to help find and secure reputable and profitable identities.

- Search for **common American names** — *Daniel Smith* is the worked example.

- Search by role: Java Developer,.NET Developer, and so on.
- **Prefer profiles with no photograph.** The manual states this outright as a desirable property.
- From the profile, harvest name, approximate location, work history, university, and certifications.
- Then run the name through a commercial background-check service to obtain the full legal name, exact address, and criminal history — and retain the social links and location history to infer a birthplace.

The entry criteria for having your identity stolen by a North Korean employment fraud operation is as simple as having **a LinkedIn profile, a common name, a developer job title, and no profile picture.**



1. Profile
   In job hunting, the most important matter is profile.
   - Rule
     - Must be US citizen
       In US job hunting, GC(Green Card) and H1B visa holders are also available.
       But most companies require US citizens.
       And then in case of GC and H1B visa holders, there are some issues in ID documentation, background check and visa verification.
       So these can be a risk for job hunting.
     - Must be over 28 years old
       You can use a young man but in the case of a young man, you can't get a senior position because of skill.
       In case of a young man profile, you have to apply for junior jobs.
       But this is a small budget.
       And then 28~35 years men is optiman age in the US IT market.
     - Criminal
       In background checks, companies have checked criminals in the last 7 years.
       Even if you get a job, if there is a criminal in your profile, you can't pass a background check and you will lose your job.
       So criminals are really critical in the US job hunting.
       However, if you violate traffic regulations or are fined for doing so, this is not considered a crime.

FIG. 08 | Screenshot from the document itself detailing requirements

Stage 2 Acquire the Identity

The manual describes three acquisition paths and is candid about the trade-offs between them including quality complaints about criminal suppliers.

Path A — the credential broker. A Ukraine-based broker operating as "Sergey" provides free name-and-address lookups. Additionally, driver's license and SSN data can also be purchased from him. The manual warns that his profiles are frequently criminal-record-tainted and therefore often unusable — describes this as making him "not a good way" to source American profiles.

Path B — the "hacker." Two Telegram handles and one Telegram channel are given for an individual claimed to have access to U.S. government databases. Given only a full name and address, he returns DL number, SSN, DOB, and a background check PDF. **The stated price is $44.** Payment is up front. The manual describes him as trustworthy and notes he is much cheaper than the broker.

Path C — stolen license images. A third broker supplies driver's license photographs of real people. The manual instructs that these be checked against a background-check service, and if clean, the name, address, DL number and DOB retained — leaving only the SSN to be purchased separately from Path B. The manual's own assessment of this route: *"This is not gentle but a good way for us."*

The market price for background information and broker payments correlate with financial records obtain from the archive. The color team expense ledger contains a single crypto line item, paid to a broker:

> **SSN number — $22.50**

That is what an American's Social Security number costs in this supply chain.

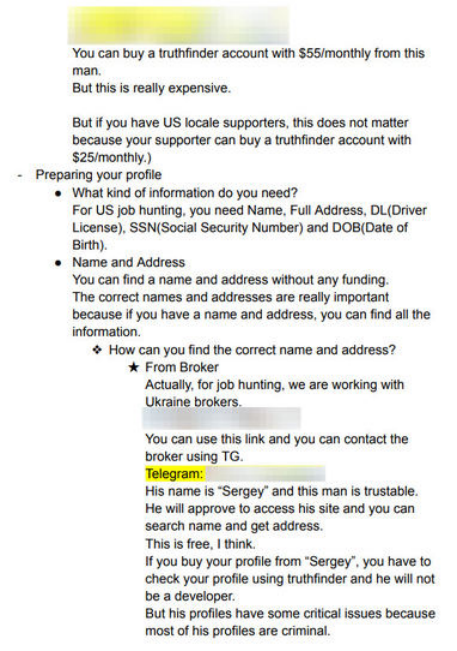


FIG. 09 | Screenshot from the document itself for obtaining identities

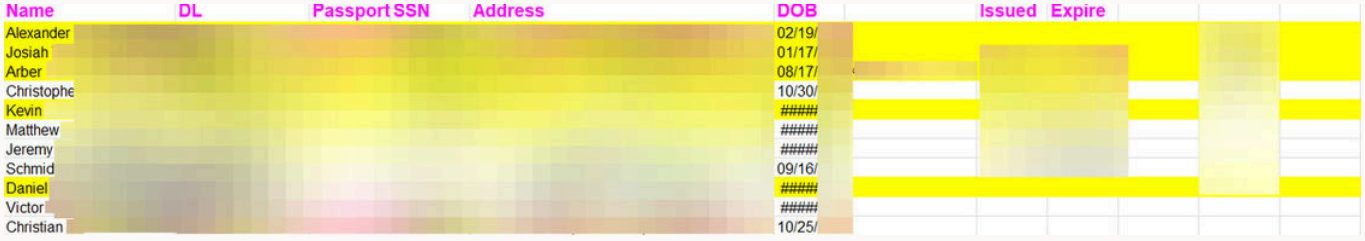


FIG. 10 | Exported document containing eleven different identities

---

Stage 3 Validate the Identity

The manual instructs that all purchased identities be verified before use, and provides the verification methods.

Criminal and identity verification runs through three named commercial background-check services: **TruthFinder**, **Intelius**, and **FastPeopleSearch**. TruthFinder requires a premium account, which the manual says to purchase from a broker at **$55/month** — with a note that this is expensive, and that a **U.S.-based supporter can obtain the same access for $25/month**.

SSN validation runs through a public verification service such as **ssn-check[.]org**.

Driver's license validation runs through **state DMV self-service portals**. The manual lists ten, by state, with direct links: **Texas, Michigan, South Carolina, Alabama, New York, Kansas, Maryland, Arizona, Pennsylvania, New Jersey**

FIG. 11 | List of DMV self-service portals and SSN validation checker

As expected, many of these states are the some of the most targeted due to the ease of information access.

Stage 4 Manufacture the Documents

The manual compares two options. A broker service (**trustidcard.com**) produces documents to order but is described as expensive. The recommended alternative is Russian-hosted generator website **veriftools** (oldie.veriftools.ru) which the manual describes as far cheaper and usable at any time with any photo and any information. It is important to note that since August 2025, veriftools is no longer available due to it's domain being seized by law enforcement.

The embedded screenshot of the generator's interface shows the product catalog in a sidebar: **Passports, Driver's License, ID Cards, Bills & Statements, USA, CIS, Facebook**. The right pane shows a rendered fake bank card, mid-generation, for a fabricated Bank of America account.

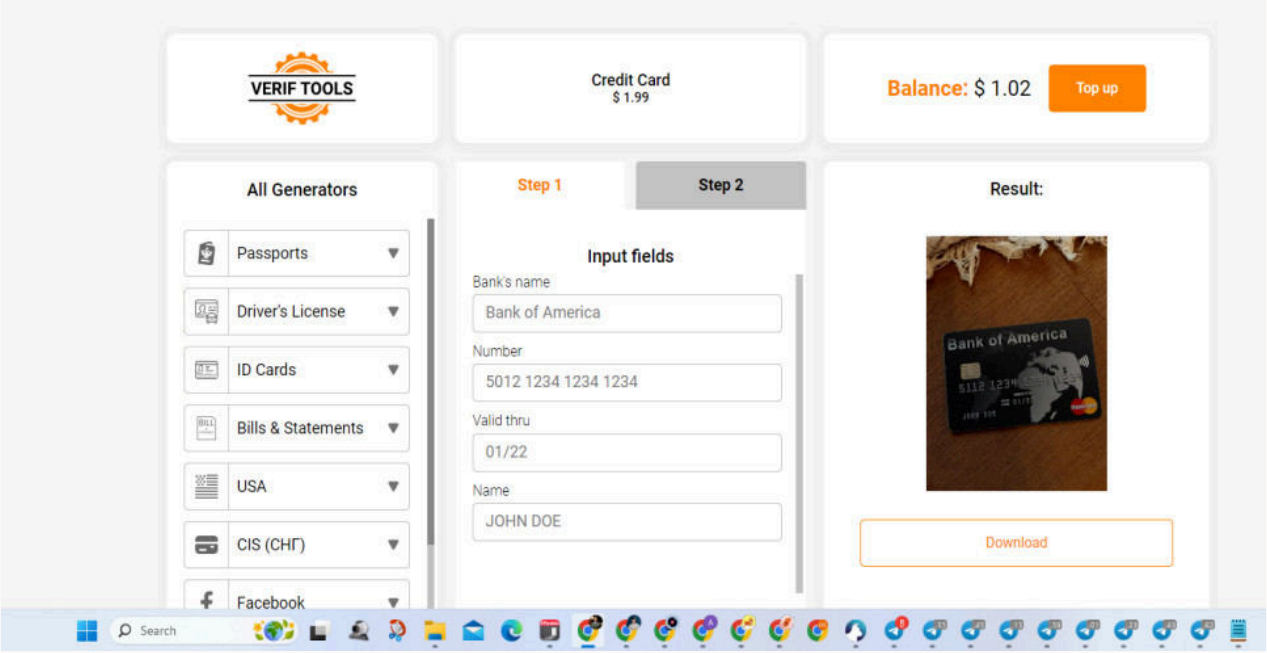


FIG. 12 | Veriftools being used but it went extinct

Under a supplemental document, the “Photo Editor” category lists two AI face-manipulation tools: **faceswapper.ai** and **instant-portrait.com**. These are how a document photo gets matched to whoever will appear on camera — corroborating Nisos’s finding that operations obtain genuine state-issued licenses and then digitally alter the photograph, and Flare’s finding that images are run through AI editors specifically to defeat reverse image search.

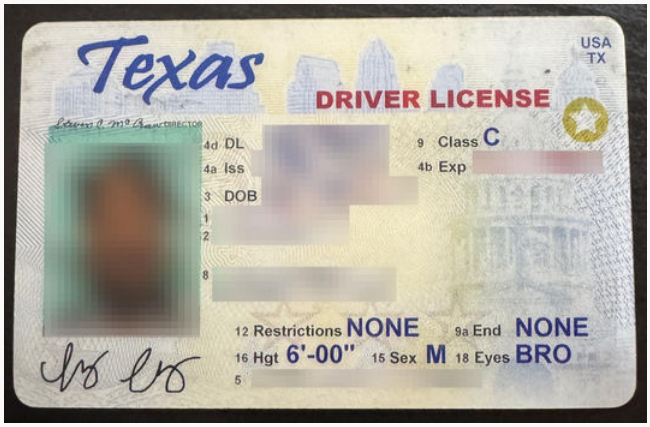


FIG. 13 | Photo of drivers license (heavily redacted) before being modified

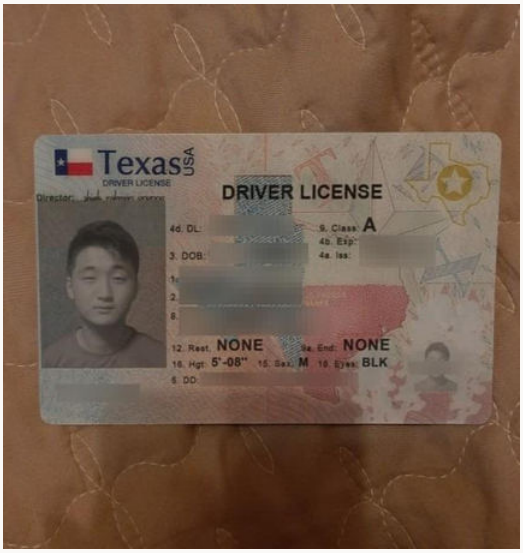


FIG. 14 | Photo of modified drivers license (note the different height and eyes listed)

FIG. 15 | Photo of another drivers license (there are dozens of them)

Stage 5 Build the Environment

As mentioned previously, operatives want to avoid being flagged for using VPNs during the application process — a mention of the following reinforces that point:

> **Commercial VPNs are explicitly rejected** — because job portals block them.

In addition to these dated methods, the previously mentioned method of outsourcing of their job applications is another route they choose to take. In this document, the instruction is to use a **U.S.-based VPS** instead. Two providers are named and compared:

- **ishosting.com** — described as having more stable IPs.
- **cloudzy.com** — described as preferable for job hunting *because it bills hourly*, allowing instances to be created, reinstalled, resized, and destroyed at will. The manual states that a New York region VPS is specifically recommended.

Both appear as recurring line items in the expense ledger, and both appear as credentialed accounts through multiple identity documents.

Date of Payme	Method of Payme	Paid to	Description	Amount Pa	Total Spe			Deposite	Date	Sum	Remainin
24 June	Card payment	Ishosting site	VPS server	20				200	7 Aug		
24 June	Card payment	Ishosting site	VPS Dedicated Server	100				100	14 Aug		
4 July	Card payment	Ishosting site	VPS Server	20				30	16 Aug		
14 Aug	Card payment	Ishosting site	Dedicated Server(for MFA and zoom session and emulator)	100							

FIG. 16 | Financial sheet displaying ishosting.com

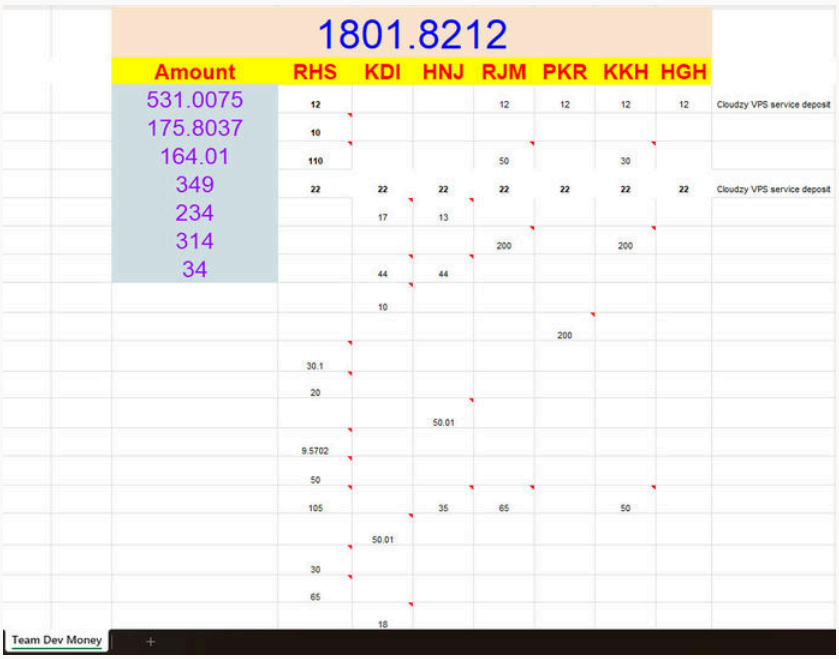


FIG. 17 | Financial sheet displaying Cloudzy.com

The Cloudzy console shows **11 services, 11 active VPS, 7 open tickets, 10 invoices**, an account balance of $37.79, and $200.16 spent that month. Four instances are visible with names, specifications, and IP addresses:

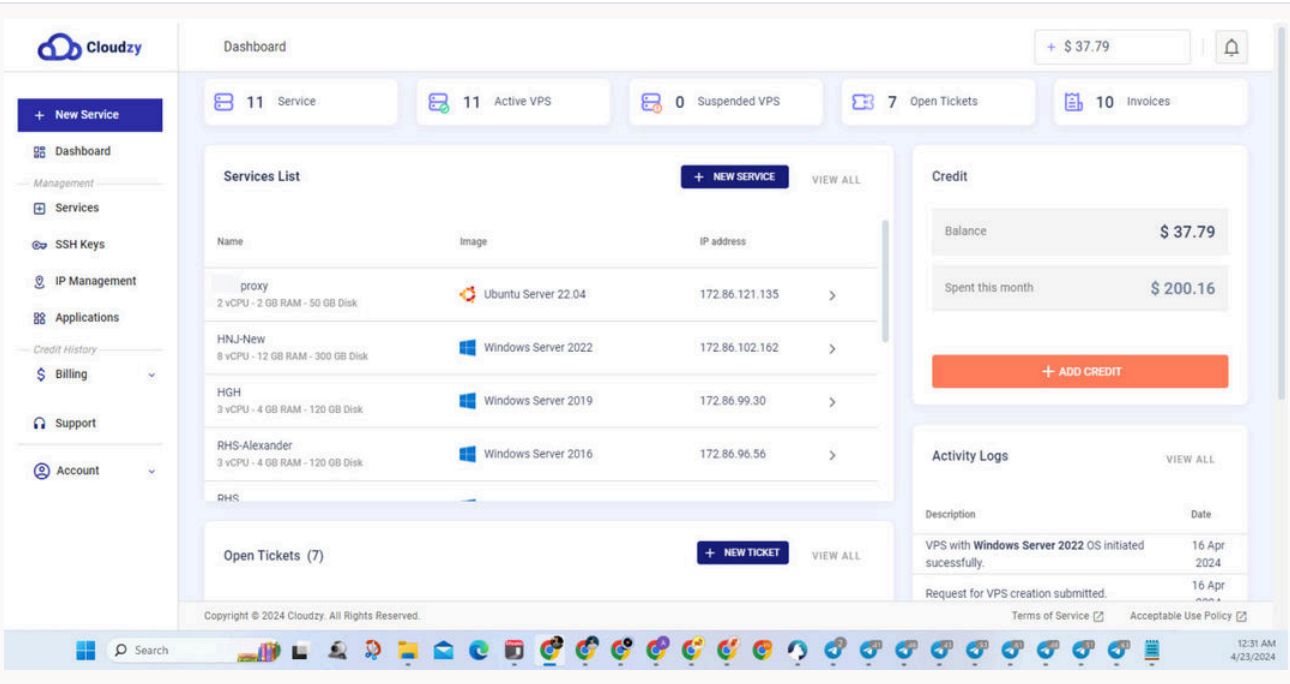


FIG. 18 | Cloudzy.com dashboard taken straight from manual

The naming convention by itself is informative. One instance is named for its function (###-proxy). One is named for a persona (RHS Alexander). The others carry three-letter prefixes consistent with initials.

The ishosting.com console shows five additional servers:

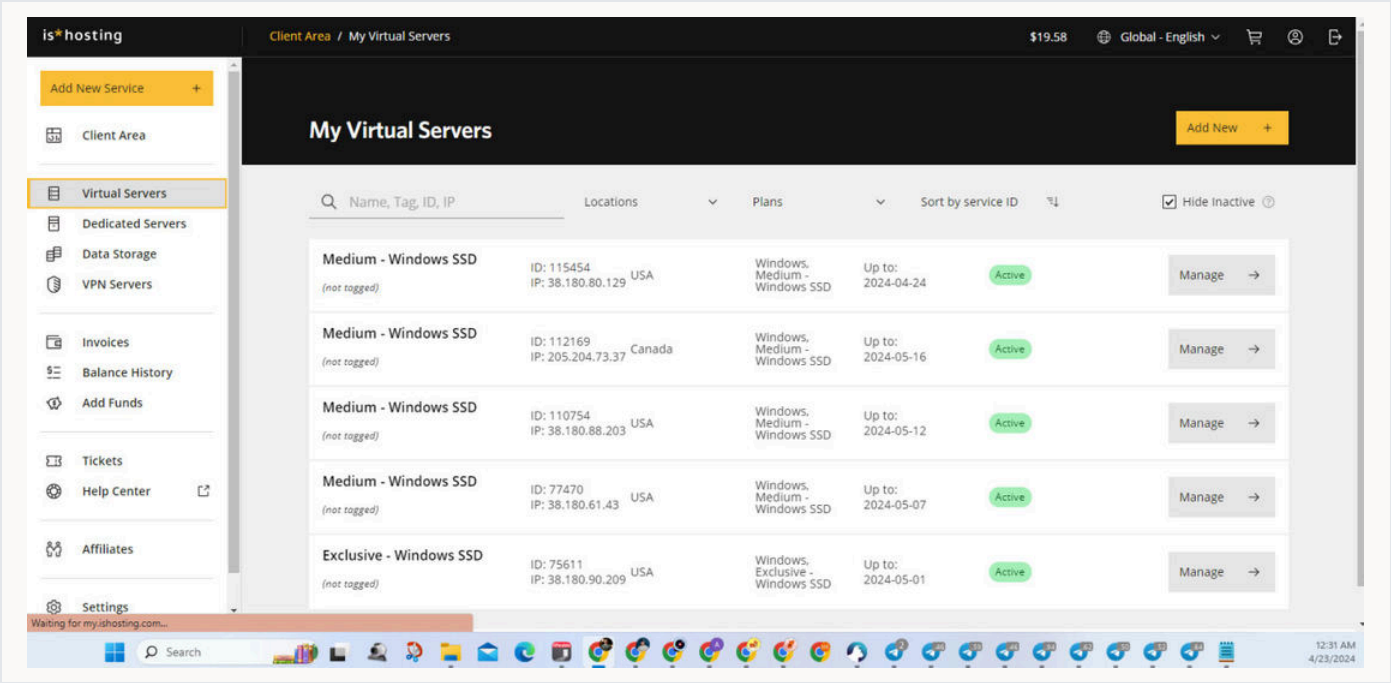


FIG. 19 | Ishosting.com dashboard taken straight from manual

A residential proxy service, **IPRoyal**, also appears repeatedly in the ledger — including a $47 entry described as a broker fee **for passing identity verification**, and a $20 entry for restoring a suspended account.

The manual recommends **Gmail** over other mail alternatives for ease of maintenance, with the requirement that account creation be performed **from the VPS or a U.S.-located machine**.

> Note: As of mid-2026, there seems to be an increasing trend of NK operatives choosing Outlook over Gmail.

The manual explicitly rejects **Google Voice** for **phone numbers** on the stated grounds that *recruiters recognize it as a virtual number immediately*. **Skype** was recommended instead; the manual concedes Skype is also virtual but assesses that it draws less suspicion. Similar to the previous instruction, Skype is no longer active and therefore no longer attractive for NK operatives — newer documentation and browsing history suggest a strong preference to **slynumber.com** and **hushed.com**.

In the past, NK operatives had their Skype numbers funded through crypto gift-card gateway **CoinGate**, paid in **USDT on Binance Smart Chain**, and redeemed for Skype credits. It appears that CoinGate is still used by operatives for other crypto-related purchases, however, Skype is no longer included in that. In addition, when using the site, the billing address entered must match the city of the VPS IP — the manual's example: if the VPS is New York, enter a New York billing address.

> Note: If you apply these tactics to newer phone services, much of the process stays the same.

Additional service providers mentioned in the manual include:

- **SMS verification services** — *sms-man.com*, *sms-activate.org* — for phone-verifying accounts at scale.
- **Temporary email** — *mailforspam.com* — used as the secondary verification address when creating Gmail accounts.
- **TOTP generation** — *2fa.live* — browser-based 2FA code generation, meaning MFA secrets are shared across a team rather than bound to a device.

- **AirDroid** — remote control of a physical Android device from a computer.
- **A dedicated server**, per the ledger, at $100, annotated as being **"for MFA and zoom session and emulator."** One machine consolidating multi-factor authentication, interview calls, and the Android emulator.

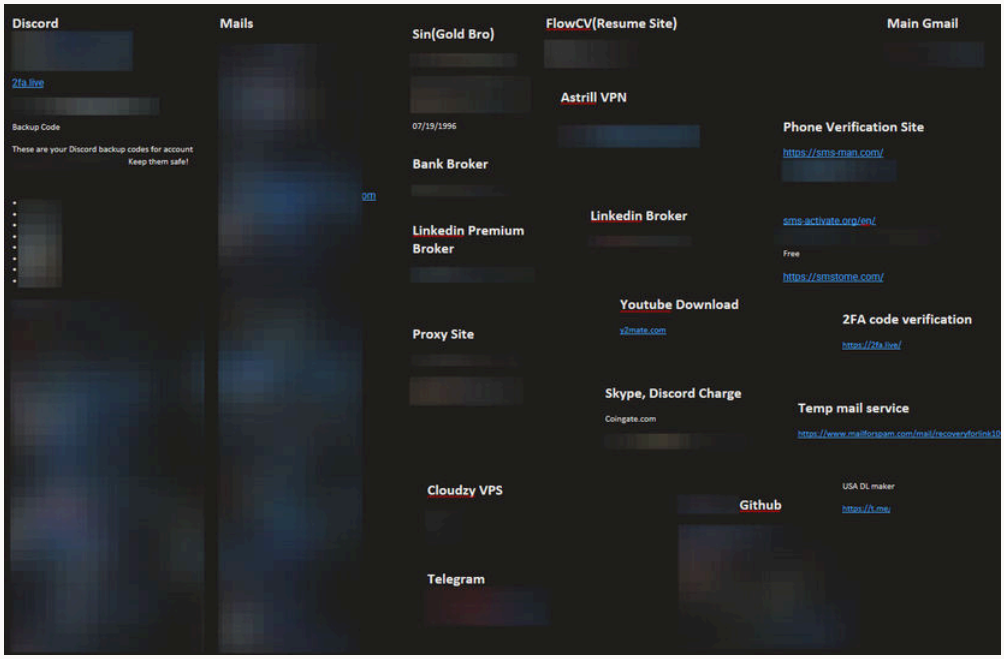


FIG. 20 | A list of services and their credentials

Stage 6 Build the Persona

The manual advises focusing each persona on a **single tech stack**, with two named archetypes:

- **Java** — Spring Boot + AWS + Angular, padded with some Go and Python.
- **C#** —.NET + React + Azure DevOps.

For backend roles, emphasize DevOps and microservice architecture. ChatGPT and Claude are recommended for drafting, with a warning that the technical content must actually be correct. Resumes are built on **FlowCV** — a $70 annual line item in the ledger.

Aged LinkedIn accounts are purchased from either a broker on Telegram or through bidding-focused Discord channels. The problem is that editing name, location, summary, and experience triggers LinkedIn's identity verification challenge and can restrict or block the account. The manual's solution to that is centered around capturing the verification QR code from the screen using **ShareX**, redirecting the challenge into **LDPlayer** (an Android emulator), and supplying a passport image to the verification vendor **through screen capture rather than a physical camera**.

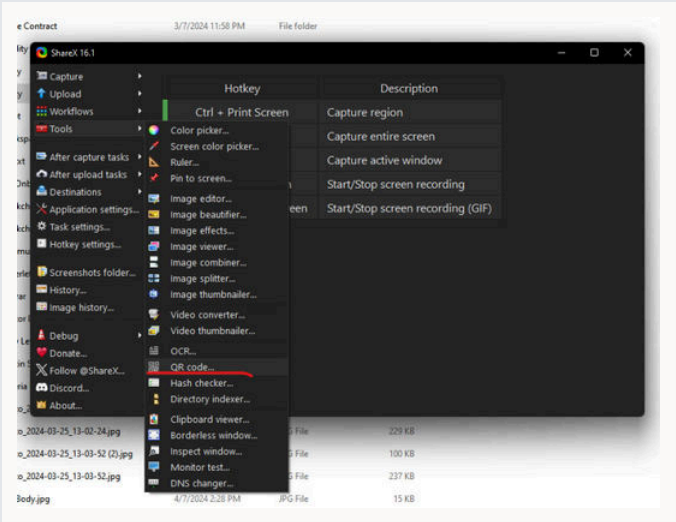


FIG. 21 | ShareX dashboard

FIG. 22 | QR code scanning through ShareX

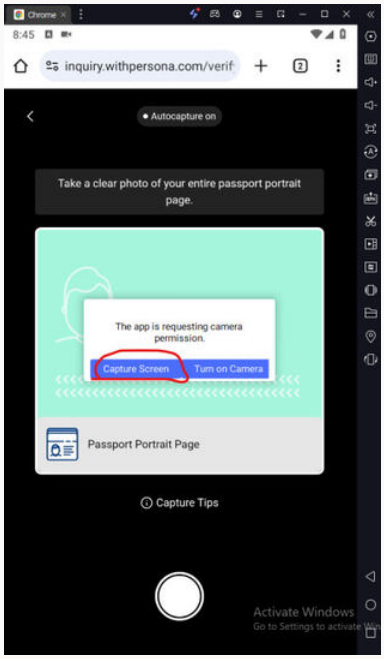


FIG. 23 | Additional instructions for identification verification

1. Any verification flow that offers a “capture from screen” fallback is exposed to the same technique. The manual lists **VCAM** and **OBS** under a heading explicitly noting they should be used *instead of* a camera, with QR scanning as the example.
2. The manual admits the bypass is unreliable and states that using a real person’s genuine ID achieves a 100% pass rate.
3. After one real job, the persona verifies LinkedIn with the corporate email address. Every successful placement permanently legitimizes the persona for all future applications.

The manual adds one more piece: the **Cookie-Editor** Chrome extension, listed specifically for importing LinkedIn session cookies. That means an authenticated LinkedIn session can be moved between machines and operators without ever re-authenticating which makes a persona’s LinkedIn presence portable across a team.

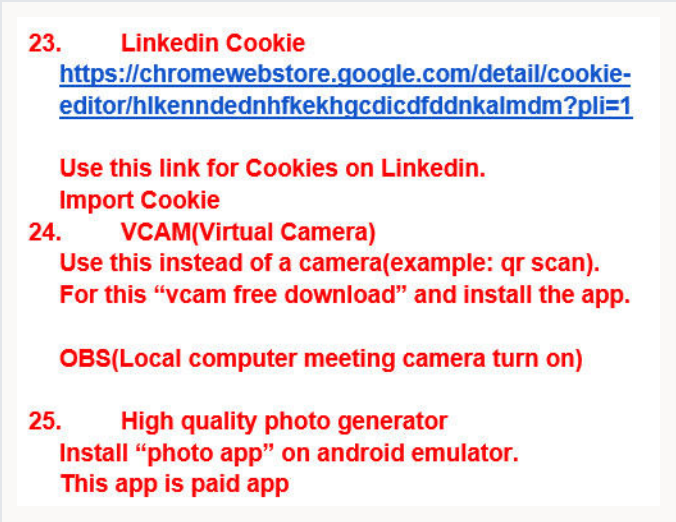


FIG. 24 | Highlighted tools associated with LinkedIn and camera verification

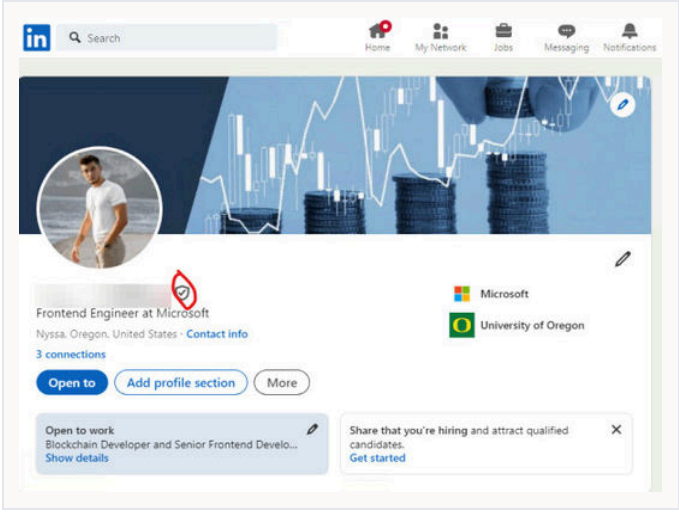


FIG. 25 | LinkedIn profile used in the instruction manual

Stage 7 Recruit an American (Optional)

Everything to this point can be done from abroad. Sure, there are tons of operatives who avoid U.S. based operations due to the strict requirements, however, that's where a majority of the money is made — and they know it too. The hesitation to focus on U.S. operations is due to the fact that their identities often require someone to physically receive a laptop, appear on camera, sign an I-9, or hold a U.S. bank account. For that the operation needs an American and the manual contains one of many pitches used to recruit them.

This stage has also become dramatically more important to the operation than it once was after an identity broker this network relied on was seized and arrested in May 2024. The strategy shifted away from buying stolen identities and toward recruiting real, willing Americans — whose own term for such a person, in their communications, is a *"real guy."*

In a document, written in the first person, there are two options when pitching collaboration ideas to a potential American prospect:

Collaboration 1 (Identity)

The recruit is asked to:

1. Keep a PC powered on and allow the operator to **connect remotely 24/7**.
2. Create an **Upwork account in their own real identity**.
3. Create a **Payoneer or PayPal account**.

The stated reason is explicit and revealing: *Upwork tracks IP addresses, and an account created from another country will be blocked.* The author states his own location plainly — **Singapore**.

The operator then bids on projects using the recruit's Upwork account, performs the work, withdraws earnings to the recruit's Payoneer or PayPal, and pays the recruit **20% of total income**.

There is a tiered upsell: **30% if the recruit is willing to appear in video meetings** — with a parenthetical noting that in that case, the recruit should know something about IT.

The pitch closes this section with a line that is almost a slogan: *in this way, you can earn the money without the sweat.*

1. **Collaboration 1**

You can either buy a new PC or use your current one.

Here are the steps you need to follow:

1) Please turn on PC and let me connect to your PC remotely 24/7.
2) Please create Upwork(https://www.upwork.com) account with your identity.
3) Please create the Payoneer or Paypal account.

It is because Upwork Inc track the IP address.

If I create other country Upwork account here in Singapore, the account will be blocked.

As you know, the time is important for everybody. We should save the time to earn the money and enjoy the life.

After this, what I could do as the following:

1) I bid on the project with your Upwork account and earn the job or project on your Upwork account.
2) I earn money and withdraw to your Payoneer or Paypal account.
3) I will give you 20% of total income.

(Some clients prefer to conduct video meeting for discussions. If you can do video meeting, you will earn 30% of the earnings. By the way, I think you should know about Information technologies in that case.)

4) In this way, you can earn the money without the sweat.

FIG. 26 | First listed collaboration method

Collaboration 2 (Hardware)

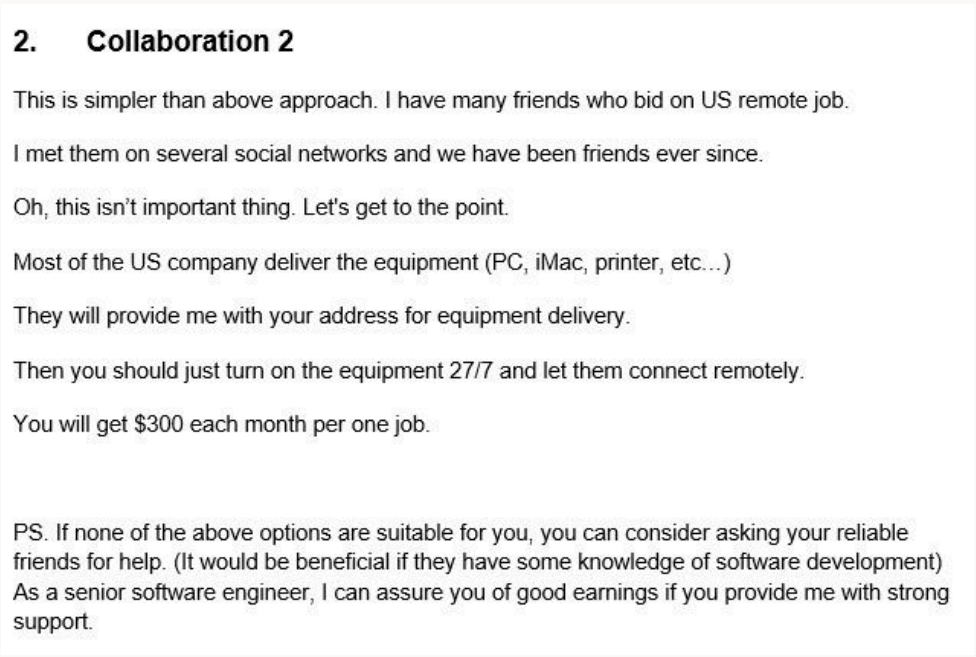
Described as simpler. The author says he has **many friends who bid on US remote jobs**, met on social networks. U.S. companies ship equipment — PC, iMac, printer. The recruit provides their address, receives the equipment, keeps it powered on, and allows remote connection.

$300 per month, per job.

That figure matches Nisos's finding precisely: facilitators recruited through Reddit, Discord, and adult cam sites, offered 50/50 salary splits or $300 payments.

Referrals (Tell a friend!)

The document closes by asking the recruit to refer **reliable friends**, noting it would be beneficial if they had software development knowledge, and signing off as *a senior software engineer* who can assure good earnings in exchange for strong support.



2. **Collaboration 2**

This is simpler than above approach. I have many friends who bid on US remote job.

I met them on several social networks and we have been friends ever since.

Oh, this isn't important thing. Let's get to the point.

Most of the US company deliver the equipment (PC, iMac, printer, etc...)

They will provide me with your address for equipment delivery.

Then you should just turn on the equipment 27/7 and let them connect remotely.

You will get $300 each month per one job.

PS. If none of the above options are suitable for you, you can consider asking your reliable friends for help. (It would be beneficial if they have some knowledge of software development) As a senior software engineer, I can assure you of good earnings if you provide me with strong support.

FIG. 27 | Second collaboration method

Stage 8 **Apply at Volume**

Several job boards are named including **LinkedIn, Indeed, Dice, Glassdoor, SimplyHired, ZipRecruiter, and CareerBuilder.**

The **LazyApply** Chrome extension is purchased at roughly **$170**, which the manual claims supports **750 applications per day across five profiles**.

The manual also instructs that LinkedIn should not be used for bidding — only as a profile — because its policy enforcement is strict.

And then there is the exclusion, which is interesting in it's own way:

> *Do not bid on public trust or security clearance jobs. You cannot pass the background check. These are government jobs — do not bid on them.*

Federal roles appear to be off the target list — which would be somewhat surprising given the recent report that a North Korean IT worker spent months at at US federal agency. Additional artifacts prove that guidance regarding federal roles serve as more of a suggestion given one of the persona's included in the archive includes a.gov email address.

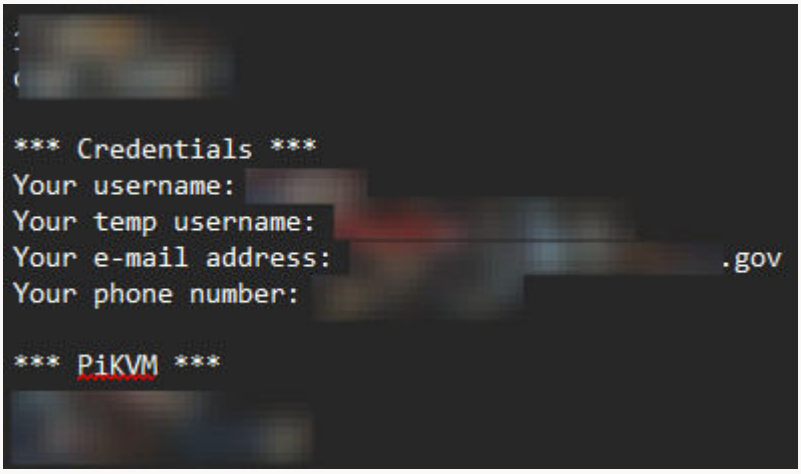


FIG. 28 | Exposed.gov credentials and PiKVM login

Between the manual's 100/day manual floor, the bot's claimed 750/day ceiling, and the outsourced bidder network mentioned earlier in the article, application volume is an important aspect of the operation. Nisos measured a comparable cell at **170,000 applications across 22 operatives in ten months, yielding 76 offers** — a 0.35% conversion rate.

Date	Job Tittle	Company	Job Post URL	Status
09/27/2024	Senior Software Engineer	Kalderos	https://app.otta.com/jobs/E0HsYE8a/apply	Applied
09/27/2024	Senior Software Engineer	Seismic	https://app.otta.com/jobs/GX3Mo7-W/apply	Applied
09/27/2024	Senior Software Engineer	Pulumi	https://boards.greenhouse.io/pulumicorporation/jobs/6056746003?utm_sour	Applied
09/27/2024	Senior Full Stack Developer	Ascend Analytics	https://boards.greenhouse.io/ascendanalytics/jobs/4468905005?utm_source	Applied
09/27/2024	Senior Full Stack Engineer	Maze	https://jobs.ashbyhq.com/mazedesign/2b09b847-92ff-4f77-af54-ea3904f48b3	Applied
09/27/2024	Senior Software Engineer	Restaurant365	https://jobs.lever.co/restaurant365/842b8c91-573c-4a00-abd7-2aabe9b7e84	Applied
09/27/2024	Senior Software Engineer	Steno	https://ats.rippling.com/steno-careers-page/jobs/83639fe8-1f9b-4464-987d-e	Applied
09/27/2024	Senior Software Engineer	Reveleer	https://reveleer.breezy.hr/p/cc35c7107f18-sr-software-engineer?source=Otta	Applied
09/27/2024	Software Engineer	First Financial Capital	https://www.indeed.com/viewjob?jk=74840f792da17c2e&q=.Net+software+E	Applied
09/27/2024	Software Engineer	SESO	https://job-boards.greenhouse.io/sesolabor/jobs/4013067005?utm_source=C	Applied
09/27/2024	Senior Software Engineer	Loyal	https://job-boards.greenhouse.io/loyal/jobs/5321416004?utm_source=Otta	Applied
09/27/2024	Senior Software Engineer	Vimeo	https://job-boards.greenhouse.io/vimeo/jobs/6117027?utm_source=Otta	Applied
09/27/2024	Software Engineer	Earnest	https://www.earnest.com/careers?gh_jid=6197371&utm_source=Otta	Applied
09/27/2024	Senior Software Engineer	ProsperOps	https://careers.prosperops.com/senior-software-engineer-185442/?utm_sour	Applied
09/27/2024	Senior Software Engineer	Confidential	https://www.indeed.com/viewjob?jk=3ede2032d0aba1af&q=.Net+software+E	Applied
09/27/2024	Senior Software Engineer	RE/MAX, LLC	https://www.indeed.com/viewjob?jk=756c9707b8e82f86&q=Full+Stack+Engi	Applied
09/27/2024	.NET Software Engineer	NeuroFlow	https://boards.greenhouse.io/neuroflow/jobs/6212816003?utm_source=zipre	Applied
09/27/2024	.NET Software Developer	NinthBrain	https://www.ziprecruiter.com/jobs/ninthbrain-99e59771/net-software-develope	Applied
09/27/2024	Senior Software Engineer	Pavlus Travel & Cruise	https://www.indeed.com/viewjob?jk=20fa748cd8b9b319&q=.Net+software+E	Applied
09/27/2024	Sr .NET Developer	Client Company	https://www.ziprecruiter.com/jobs/client-company-9fa650bf/sr-net-developer-	Applied
09/27/2024	Software Engineer, .NET / C#	Scribe	https://scribehow.com/jobs?gh_jid=4518324007&utm_source=ziprecruiter	Applied
09/27/2024	.Net Full Stack Developer - Remot	cyberThink, Inc	https://www.ziprecruiter.com/jobs/cyberthink-inc-954dd4a4/net-full-stack-de	Applied
09/27/2024	Senior Software Engineer	HonorVet Technologies	https://www.ziprecruiter.com/jobs/honorvet-technologies-f5f95f52/senior-soft	Applied
09/27/2024	Senior Software Developer	Chroma Consulting	https://www.indeed.com/viewjob?jk=73e3d01f6cf1d129&q=.Net+software&l=	Applied
09/27/2024	Senior Software Engineer	50158 Specialty Program Group	https://hubinternational.wd1.myworkdayjobs.com/HUBInternational/job/Seni	Applied
09/27/2024	Senior Full Stack Engineer	SiteZeus	https://www.ziprecruiter.com/jobs/sitezeus-5977a284/senior-full-stack-engin	Applied
09/27/2024	Full Stack .NET Developer	Codeworks L.L.C	https://www.ziprecruiter.com/jobs/codeworks-l-l-c-6025b351/full-stack-net-de	Applied
09/27/2024	Senior Software Engineer	NeuAnalytics	https://www.ziprecruiter.com/jobs/neuanalytics-dfedf1a2/senior-software-eng	Applied
09/27/2024	Full Stack Engineer	Package Retriever	https://www.ziprecruiter.com/jobs/package-retriever-e8a96563/full-stack-eng	Applied
09/27/2024	Full Stack Developer	Aurora Mental Health & Recovery	https://www.paycomonline.net/v4/ats/web.php/jobs/ViewJobDetails?job=217	Applied
09/27/2024	Software Engineer	Venafi	https://boards.greenhouse.io/venafi/jobs/6264043?utm_source=ziprecruiter	Applied
09/27/2024	Full Stack Developer	IPeople	https://www.ziprecruiter.com/jobs/ipeople-acb4151a/full-stack-developer-a59	Applied
09/27/2024	Senior .Net Full Stack Developer	Horizon Resource Services	https://www.ziprecruiter.com/jobs/horizon-resource-services-6bb12a1f/senio	Applied
09/27/2024	Senior Full-Stack Engineer	Transfr	https://jobs.lever.co/transfyr/7a2114ac-5f70-4b2c-b974-76e1e553b825?lever	Applied
09/27/2024	Senior Full Stack Software Engine	MagicSchool AI	https://jobs.ashbyhq.com/magicschool/70ad0264-1e89-4675-94f5-2fa9d005	Applied
09/27/2024	Senior Software Engineer	Pilot	https://boards.greenhouse.io/pilothq/jobs/6981966002?utm_source=Otta	Applied
09/27/2024	Senior Fullstack Software Engine	Coinbase	https://www.coinbase.com/careers/positions/5961013?gh_jid=5961013&utm	Applied
09/27/2024	Software Engineer	Limble CMMS	https://jobs.ashbyhq.com/limble/480f5f5c-5aa4-4e95-a06a-a242286c6c02?ut	Applied
09/27/2024	Full Stack Engineer	Red Ventures	https://www.redventures.com/careers/positions/open?gh_jid=6044156&utm_	Applied
09/27/2024	Software Developer	Aquila Technology	https://www.indeed.com/viewjob?jk=fe1ba54bb2dcc382&tk=1i8rmll8cgct28b	Applied
09/27/2024	Full-Stack Engineer	Splitero	https://app.otta.com/jobs/fAV0UIsl/apply	Applied
09/27/2024	Senior Software Engineer	Garner Health	https://job-boards.greenhouse.io/garnerhealth/jobs/5059690004?utm_source	Applied
09/27/2024	Senior Fullstack Software Engine	Wild Alaskan	https://boards.greenhouse.io/wildalaskancompany/jobs/5271744004?utm_so	Applied
09/27/2024	Senior Software Engineer	OneSignal	https://job-boards.greenhouse.io/onesignal/jobs/4370512006?utm_source=C	Applied
09/27/2024	Senior Software Engineer	CircleCI	https://circleci.com/careers/jobs/7593440002?gh_jid=7593440002&utm_so	Applied
09/27/2024	Senior Software Engineer	Evolve	https://boards.greenhouse.io/evolvevacationrental/jobs/6021391003?utm_so	Applied

FIG. 29 | Bidding spreadsheet

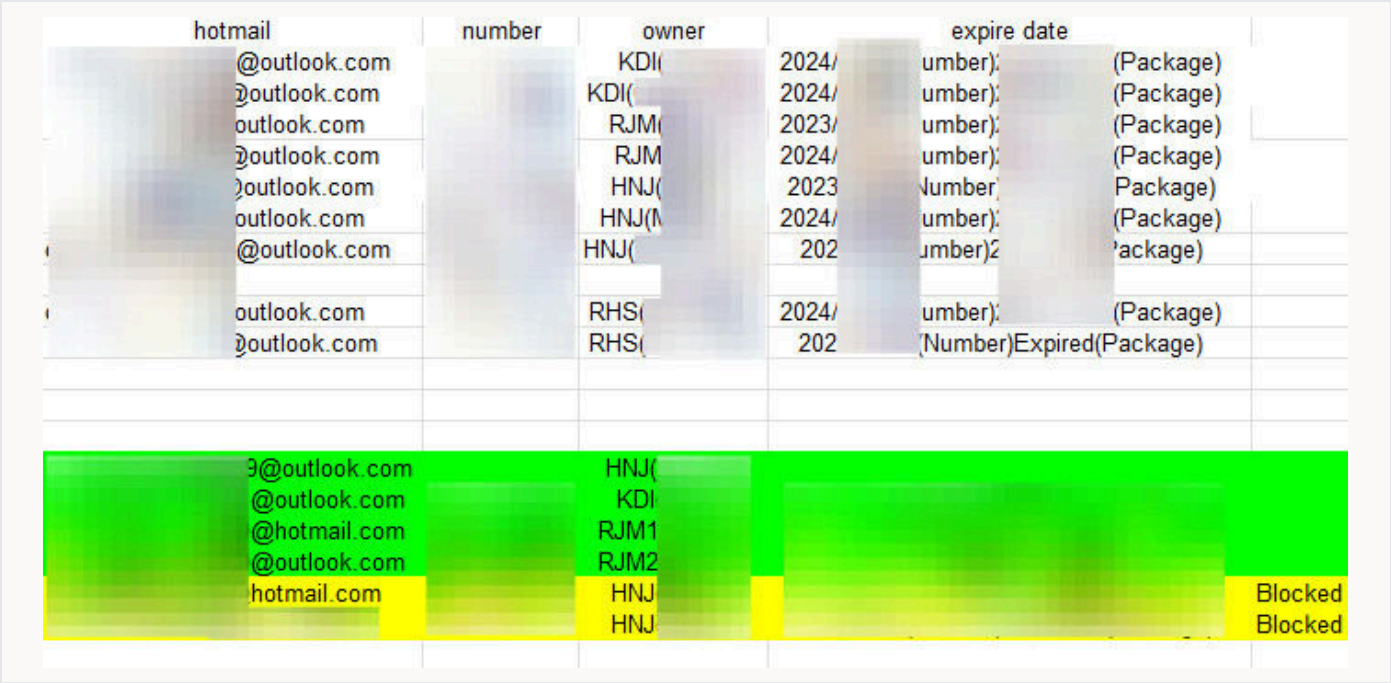


FIG. 30 | Packaged identities for spam applications for

Stage 9 Pass the Interview

An all inclusive **40-item index** — a self-introduction, a named flagship project, then behavioral and technical questions followed by fully written answers to each. Three details make this far more valuable than its contents suggest.

It is written to be read aloud

Embedded at intervals in the prose are **phonetic pronunciation guides in dictionary notation**, attached to exactly the words a non-native English speaker would stumble on. They appear inline, mid-sentence, in otherwise ordinary answers:

> *"I also have a knack /nak/ for optimizing performance..." "...allowing frontend and backend teams to work more autonomously /əˈtänəməslē/." "...strengthened my technical acumen /əˈkyo͞omən/..." "...exceed expectations and achieve /əˈCHēv/ excellence..."*

It explains one of the most commonly cited DPRK interview red flags as Group-IB lists *"inconsistent English fluency that fluctuates during the call"* as a warning sign.

The interview is not necessarily the person

The manual contains an entry that changes how any video interview should be read. Under a heading about calls on a remote laptop, it describes using **Voicemeeter Banana** — a virtual audio mixer — to route voice between a remote laptop and a local one, by joining the same meeting from both machines and setting both the meeting client and the conferencing application to use the virtual audio device.

This is how a person in one country can speak through a video call that a person in another country appears to be attending.

Nisos documented this pattern behaviorally — a U.S.-based "native" on camera while the operative supplies technical answers remotely via KVM. This is the configuration guide for it. Combined with the virtual camera tooling from Stage 6, a single video call can have **one person's face, another person's voice, and a third person's hands on the keyboard.**

FIG. 31 | Methods used to bypass interview restrictions

Stage 10 Onboard and Receive the Hardware

Once an offer lands, the physical issues arise as a laptop must be shipped to a U.S. address, and someone must sign an I-9.

The *Job Hunting* manual's final page addresses this directly as it lists a handful of known **U.S. supporters** based in a few different states.

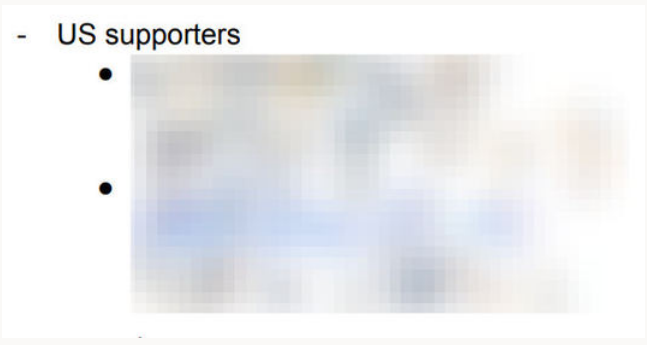


FIG. 32 | Heavily redacted list of U.S. facilitators

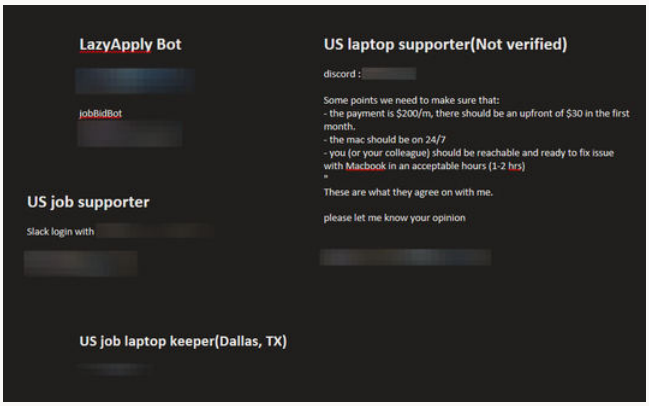


FIG. 33 | Another heavily redacted list of U.S. supporters

Once the hardware arrives, remote access is established. The next few sections will detail many of the logistical issues and bypass methods used to make this process easier.

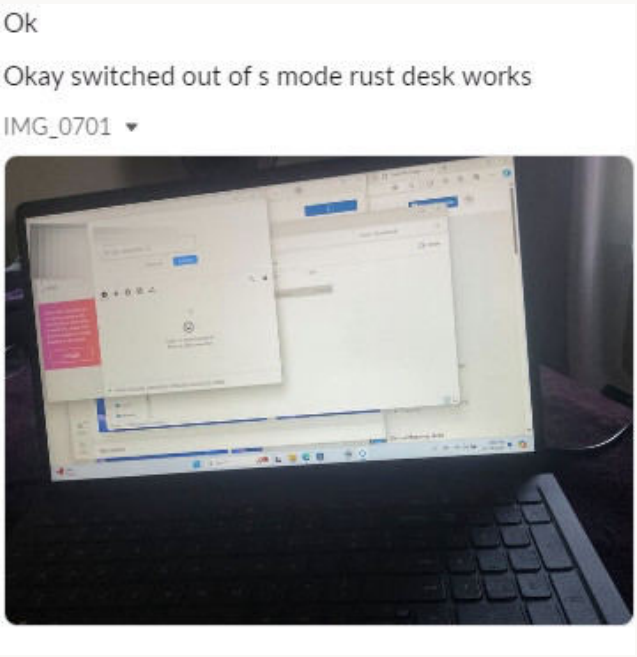


FIG. 34 | Photo for a specific identity documenting RustDesk compatibility

Stage 11 Get Paid, Split It, and Cash Out

The money is covered in depth in Part Three. In summary, the chain runs:

1. The employer's payroll deposits the salary into an account created in the persona's or facilitator's name.
2. The split is executed per a revenue-sharing contract — 50/50, 70/30, with the facilitator's 15–25% coming from the intermediary's share.
3. The funds are then moved out of the traditional banking system. The ledger shows conversion into payment platforms with broker and bank withdrawal fees due to their movement across **BEP20, TRC20, ERC20, Polygon, and Arbitrum**.
4. The ledger repeatedly references an Ethereum address for the "Color team," identified in descriptions only by its final characters.

In the next section, newer mechanisms and services are mentioned which allow for easier and more reliable payouts.

17 July	Crypto	**ETH for Color team**	ETH shared on Color team wallet ends with f2	55
17 July	Crypto	**ETH for Color team**	ETH shared on Color team wallet ends with f2	57
18 July	Crypto	**TRC20 for Color team**	Website payment for TRC20	36
18 July	Crypto	**Exchange fee**	Converting 200 from USDC to USDT	1

FIG. 35 | Payments associated with crypto expenses and conversions

Section Three | Diving Deeper

Identity Architecture

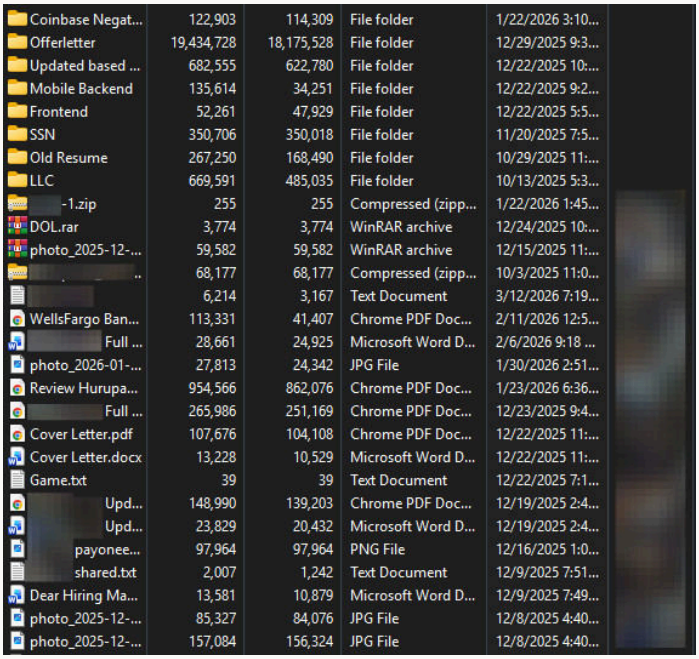
Centralized identity documentation

The bulk of their documentation contains per-identity files or directories which could be anywhere from a group of.txt files and pictures to massive OneNote pages. In a notable number of cases, a link **protectedtext.com** — a free, password-protected plaintext note service requiring no additional verification, is used to distribute identities to anyone.

The person who runs the interview, the person who receives the laptop, and the person who does the work may be three different people in three countries who need the same reference sheet and cannot be trusted with a shared account. A password-protected URL is the ideal solution for this type of operation.

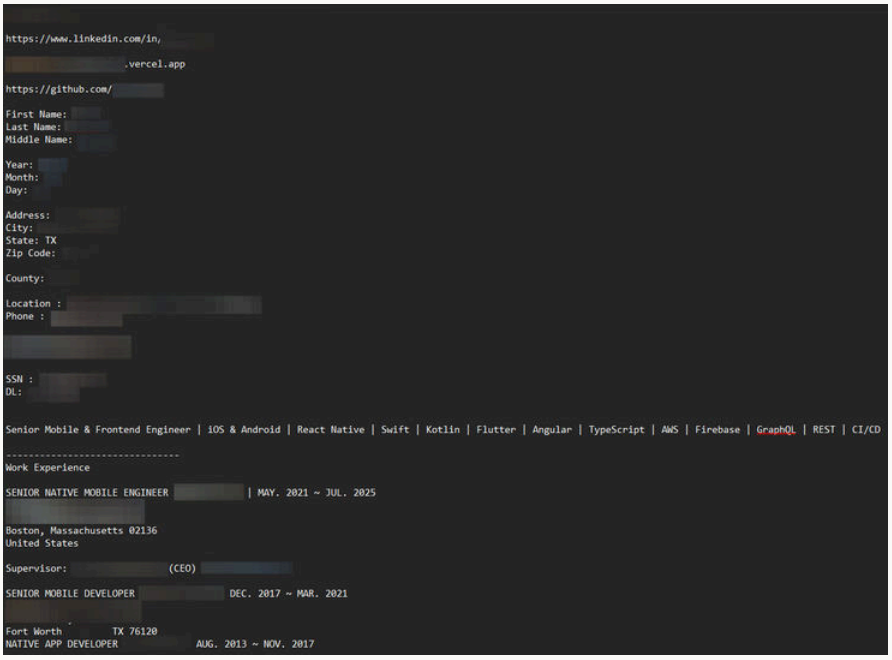
Each identity used is then sorted and documented in great detail containing personal and professional artifacts for reuse such as:

- Full legal name, date of birth, and SSN
- Altered driver's license and/or passport with scans
- Address of record — plus, separately, the shipping address actually used
- Current and historical phone numbers, typically VoIP
- Email credentials, its recovery address, and the forwarding target
- KVM login credentials — device address, username, password
- VPS access — provider, IP, credentials
- Specific proxy configurations
- Employer-specific credentials for jobs already landed
- Pay stub records and direct deposit details
- Which personas serve as this persona's references



Coinbase Negat...	122,903	114,309	File folder	1/22/2026 3:10...
Offerletter	19,434,728	18,175,528	File folder	12/29/2025 9:3...
Updated based ...	682,555	622,780	File folder	12/22/2025 10:...
Mobile Backend	135,614	34,251	File folder	12/22/2025 9:2...
Frontend	52,261	47,929	File folder	12/22/2025 5:5...
SSN	350,706	350,018	File folder	11/20/2025 7:5...
Old Resume	267,250	168,490	File folder	10/29/2025 11:...
LLC	669,591	485,035	File folder	10/13/2025 5:3...
-1.zip	255	255	Compressed (zipp...	1/22/2026 1:45...
DOL.rar	3,774	3,774	WinRAR archive	12/24/2025 10:...
photo_2025-12-...	59,582	59,582	WinRAR archive	12/15/2025 11:...
..	68,177	68,177	Compressed (zipp...	10/3/2025 11:0...
	6,214	3,167	Text Document	3/12/2026 7:19...
WellsFargo Ban...	113,331	41,407	Chrome PDF Doc...	2/11/2026 12:5...
Full ...	28,661	24,925	Microsoft Word D...	2/6/2026 9:18 ...
photo_2026-01-...	27,813	24,342	JPG File	1/30/2026 2:51...
Review Hurupa...	954,566	862,076	Chrome PDF Doc...	1/23/2026 6:36...
Full ...	265,986	251,169	Chrome PDF Doc...	12/23/2025 9:4...
Cover Letter.pdf	107,676	104,108	Chrome PDF Doc...	12/22/2025 11:...
Cover Letter.docx	13,228	10,529	Microsoft Word D...	12/22/2025 11:...
Game.txt	39	39	Text Document	12/22/2025 7:1...
Upd...	148,990	139,203	Chrome PDF Doc...	12/19/2025 2:4...
Upd...	23,829	20,432	Microsoft Word D...	12/19/2025 2:4...
payonee...	97,964	97,964	PNG File	12/16/2025 1:0...
shared.txt	2,007	1,242	Text Document	12/9/2025 7:51...
Dear Hiring Ma...	13,581	10,879	Microsoft Word D...	12/9/2025 7:49...
photo_2025-12-...	85,327	84,076	JPG File	12/8/2025 4:40...
photo_2025-12-...	157,084	156,324	JPG File	12/8/2025 4:40...

FIG. 36 | Extensive identity documentation



https://www.linkedin.com/in/

.vercel.app

https://github.com/

First Name:
Last Name:
Middle Name:

Year:
Month:
Day:

Address:
City:
State: TX
Zip Code:

County:

Location :
Phone :

SSN :
DL:

Senior Mobile & Frontend Engineer | iOS & Android | React Native | Swift | Kotlin | Flutter | Angular | TypeScript | AWS | Firebase | GraphQL | REST | CI/CD

Work Experience

SENIOR NATIVE MOBILE ENGINEER | MAY. 2021 ~ JUL. 2025

Boston, Massachusetts 02136
United States

Supervisor: (CEO)

SENIOR MOBILE DEVELOPER DEC. 2017 ~ MAR. 2021

Fort Worth TX 76120
NATIVE APP DEVELOPER AUG. 2013 ~ NOV. 2017

FIG. 37 | Supplemental information for an identity

They use each other as references

A persona's listed professional references are, in multiple observed cases, **other personas in the same collection.** When a hiring team calls to verify prior employment, the call is answered by the operator running another persona.

Nisos documented the same structure. What this section adds is the bookkeeping aspect of the references as each one is predetermined and assigned in advance.

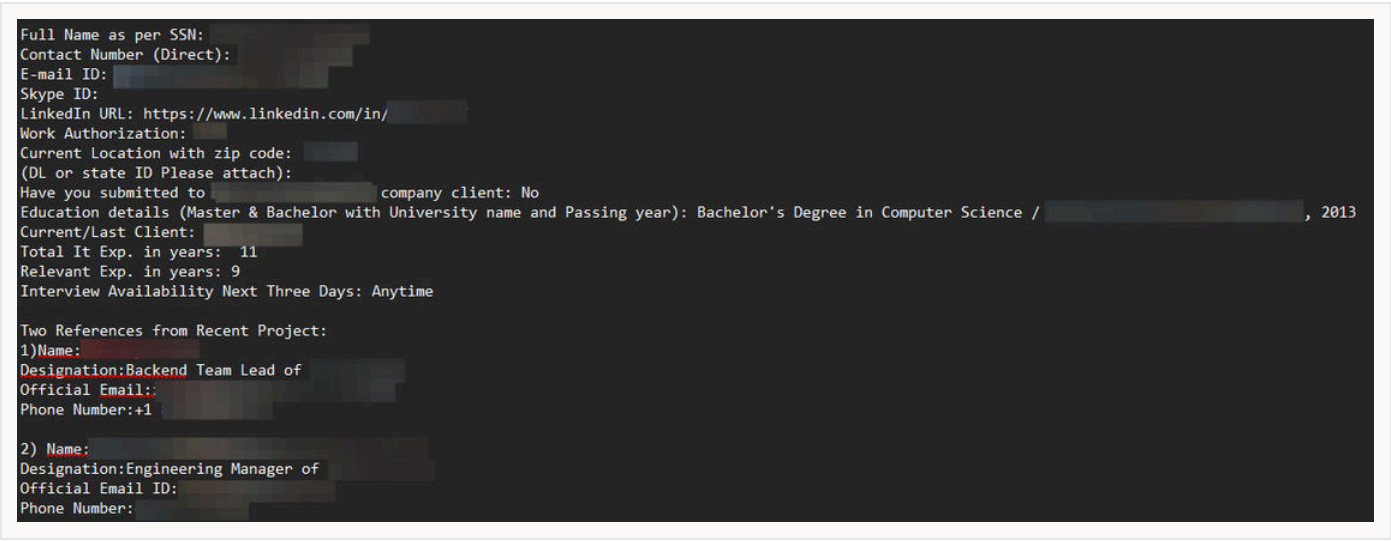


FIG. 38 | Designated references listed under identity profile

> Note: A company that quietly terminates a suspected DPRK worker without reporting it has handed the operation a legitimate reference.

Background checks on real people

As previously mentioned, background checks are typically ran on real people to verify their identities and to make sure their background is clear.

The standard output of the three consumer services named in the manual typically contain:

- Address history going back years
- Relatives and known associates, with ages and locations
- Vehicle registrations
- Employment and education history
- Current and historical phone numbers
- Court and civil records where present

The manual describes this part of the process as "*important*" an emphasizes being able to answer questions about where they grew up or went to school — this is precisely the rapport-building question Group-IB recommended interviewers use to catch inconsistencies.

The exposure for victims also extends well past their own identity. **Their family members are in these files.**

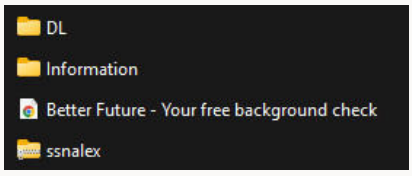


FIG. 39 | Identity folder

FIG. 40 | Identity folder separated into family members

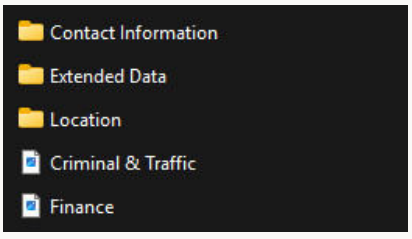


FIG. 41 | PII associated with a victims family member

> Note: Even though many of these identities are stolen, a surprising amount of them are willingly given to the NK operator — documentation shows dozens of individuals were willing to recording videos of themselves, file LLCs, and assist throughout the hiring and banking processes of the operation.

Infrastructure and Remote Access

CCProxy

CCProxy is a Windows proxy server marketed to small offices for sharing a single internet connection. The archive's configuration guide walks through installing it on a U.S.-region VPS (or, in some documentation, on a supporter's home machine) and enabling HTTP and SOCKS5 with per-user authentication (used for proxy chaining). Operators abroad then point their browsers and applications at that host, and every request they make egresses from one U.S. IP.

The effect is that a team spread across multiple countries presents to an employer, a job board, or an identity verification vendor as a single user sitting at a single American address. It also gives them a cheap second hop in front of the residential proxy layer: traffic can be chained from the operative, through CCProxy on the VPS, out through IPRoyal, and arrive looking like a consumer broadband connection near the victim's address of record.

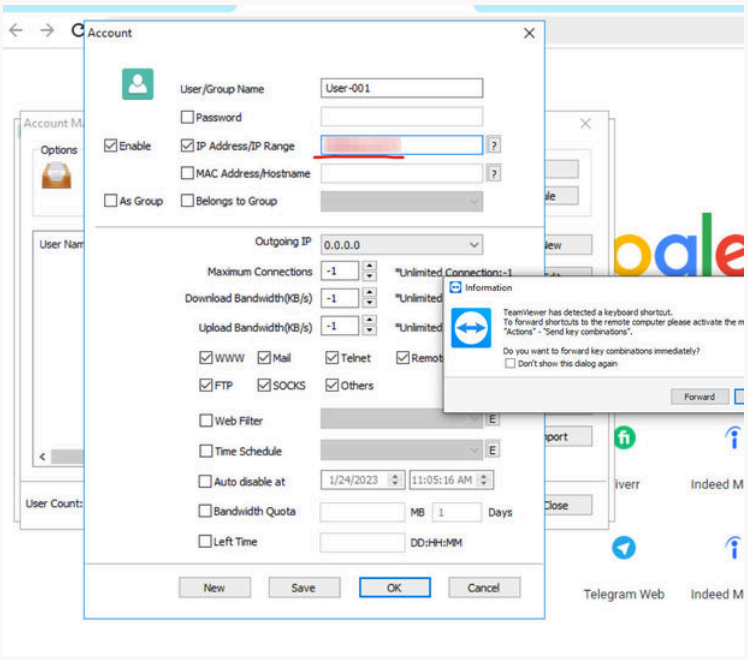


FIG. 42 | Image of CCProxy settings

Remote Access Patterns

The artifacts contained dozens of photographs detailing **PiKVM** device usage — a well-known indicator of potential DPRK activity. Photographic and documentary evidence indicates PiKVM devices are still being heavily used in 2026.

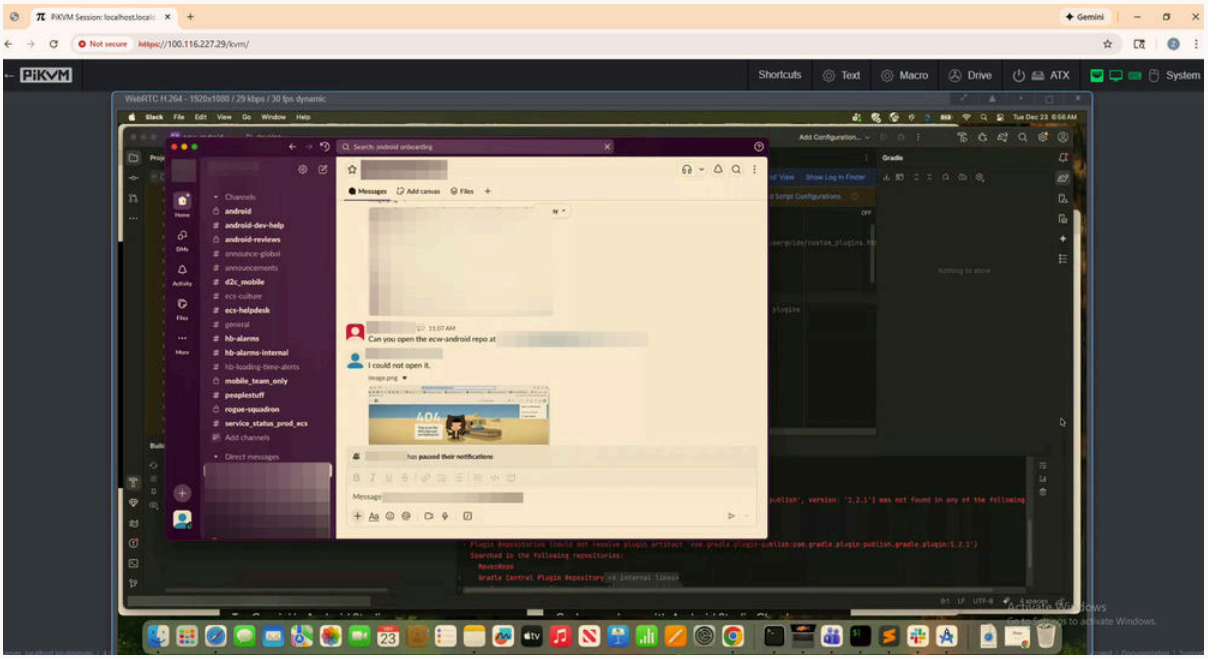


FIG. 43 | Documented PiKVM usage

Alongside the hardware approach, the operation can use a software approach such as **RustDesk, AnyDesk, and TeamViewer** — all notable remote desktop tools.

When these methods are blocked, or when the operator fears detection by using these methods, evidence shows common attempts to bypass detection by using **Webex** and **Zoom** — common and typically approved services across large enterprises.

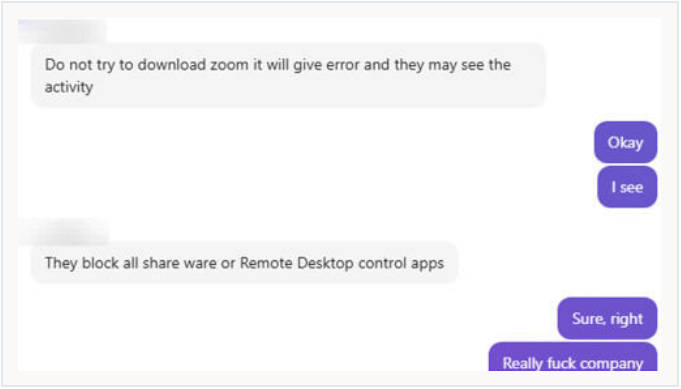


FIG. 44 | I'm not sure why they screenshotted their conversations, and I clipped some of the conversation out, but this discusses bypass methods via software

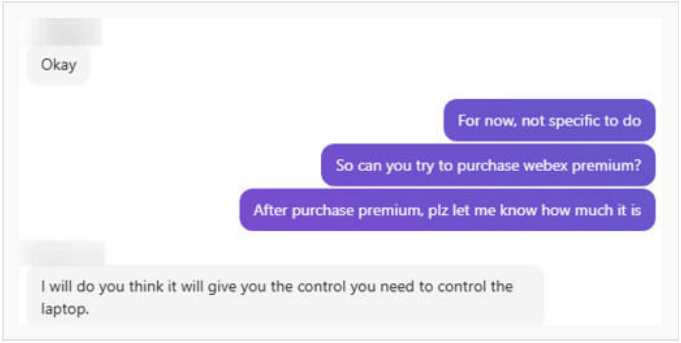


FIG. 45 | Discussion on using Webex as a work-around

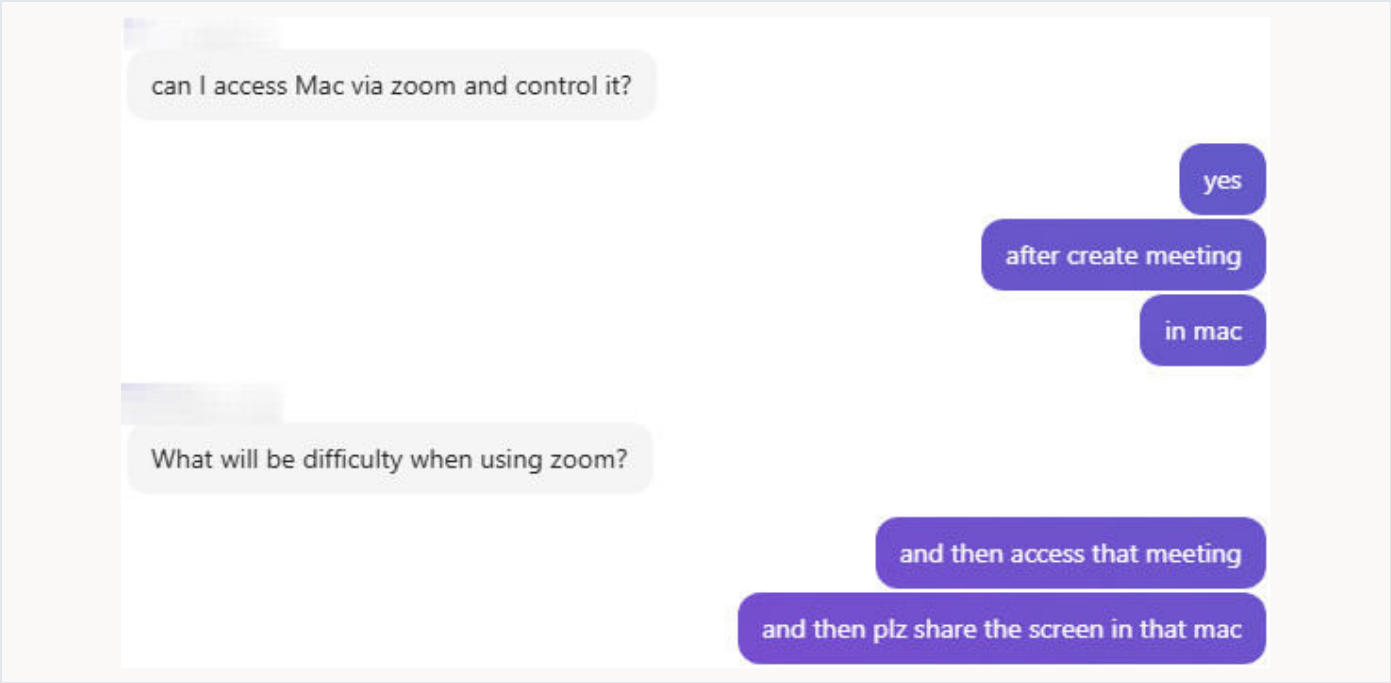


FIG. 46 | Discussion on using Zoom via Mac as a work-around

If your company does not block Zoom or it's remote-control feature, a network indicator that occasionally presents itself is the file *saveUserDisclaimer* — typically observed when a feature being utilized within the meeting requires user acceptance.

If you want to dive deeper into Webex logs for this activity, I advise you to check out Grumpy Goose Labs article detailing their successful identification of remote-control logs from the application. They also provide a helpful guide which discusses methods to identity KVM usage across an enterprise.

> Note: In the event NK operators refuse to use remote-control access and opt for screen-sharing methods, look for excessive Zoom or Webex usage across multiple days, on weekends, or outside of typical work hours.

Payment Records and Documentation

Documented financial processes

For each successfully used identity, there is a complete and organized financial history documented for payment tracking and future verification.

The payments associated with one identity may need to be split amongst teams, facilitators, and other groups that assisted in onboarding and maintaining access for an identity. Additionally, a pay stub is proof of employment. It supports the next application, the next background check, the next account opened in that identity's name.

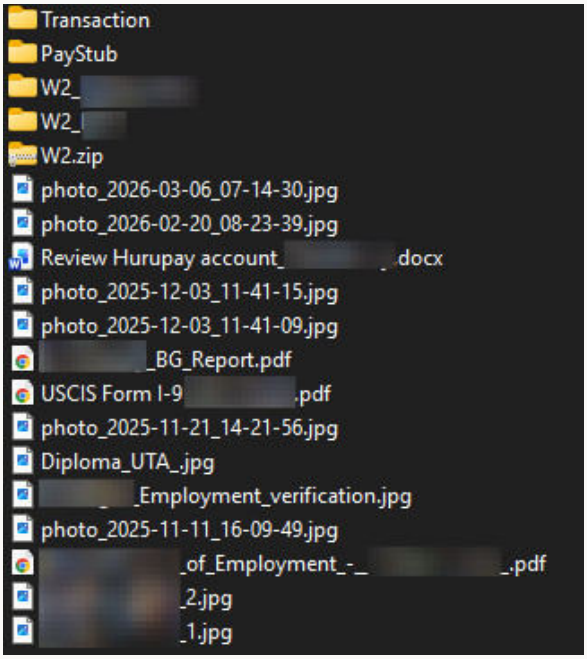


FIG. 47 | A list of financial and payment documents

As a complimentary aspect, many operators document every thing resume they've created and organize it by company and role — combining these files makes future operations run smooth.

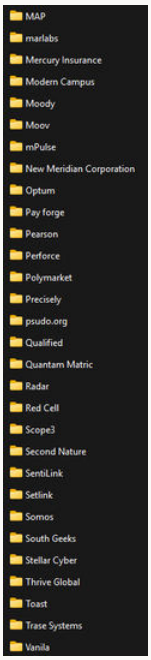


FIG. 48 | These companies were only applied to and not verifiably infiltrated, these files only document resumes for future use

Among the new methods of separating and facilitating payments, a prepared script for the platform **HuruPay** was observed within the archive.

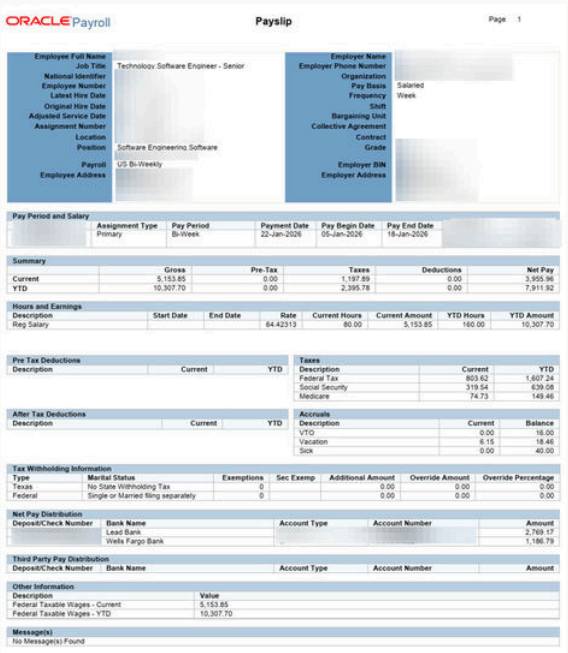


FIG. 49 | Though HuruPay is not explicitly used here, pay stubs like these are documented regardless of payment type for every identity

HuruPay is used to receive bi-weekly salaries from an employer as part of regular payroll payments. HuruPay provides **stablecoin-backed virtual USD, EUR, and GBP accounts** aimed at freelancers, remote workers, and businesses in Africa and other emerging markets — explicitly marketed, in the company's own app store listing, as letting you *receive USD payments with a US account, even if you're not a US resident.* It supports 50+ countries including Nigeria, Ghana, South Africa, the Philippines, and the United States, and allows near-instant off-ramping to stablecoin wallets, local banks, and mobile money.

Group-IB's guidance to employers is to pay salaries only into licensed, deposit-accepting institutions, and to prohibit pooled accounts, e-wallets, and remitters.

LLC Formation and the Corp-to-Corp

In great detail, and with tons of supplementary paperwork and instructions, lays the instructions for creating a LLC and what purpose it serves.

Alongside the interview scripts and the identity manual, the archive contains a short plaintext file — a step-by-step guide to filing a Texas LLC through SOSDirect, the Secretary of State's online filing portal. Those documents also contain a completed filing package for a Texas LLC, formed in October 2025.

- Create a SOSDirect client account; credentials arrive by email.
- Pre-fund the account so filings can be paid for.
- Submit the Certificate of Formation (Form 205) — entity name, address, registered agent, organizer, purpose, management structure.
- Pay $300.
- Wait for the stamped certificate.
- Then: obtain an EIN from the IRS, draft an operating agreement, open a business bank account, and handle Texas franchise tax.

In documented exchanges with other NK operatives, discussions rose asking whether forming an LLC in the U.S. requires a "real guy" — the term Section 7 established for a willing American collaborator. One of the operatives

then explain why an LLC would be needed: he wants to try a **CTC role**.

CTC is corp-to-corp — in a corp-to-corp engagement, the client does not hire a person; the client contracts with a company, and that company supplies the worker. What the client collects is not an I-9 and a driver's license but a certificate of formation, a W-9, a certificate of insurance, and bank details. Employment-track identity controls do not fire, because there is no employment.

- The peer notes that his **team manager's real guy has his own company**, and that a teammate secured a CTC role through it — meaning an existing American-owned entity can be reused rather than formed fresh.
- He describes a volume of available project opportunities through that channel.
- Asked whether the work is in the U.S., the reply is that the American then **needs to be added into the LLC**.

That last point deserves emphasis. The LLC is not built around the operative and then handed to an American. It is built around the American — his name, his address, his signature, his tax status — and the operative is added afterward.

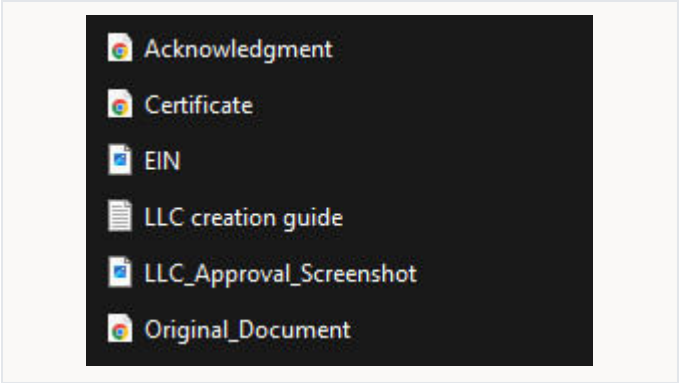


FIG. 50 | Documentation for the creation of, and to maintain, existing LLCs

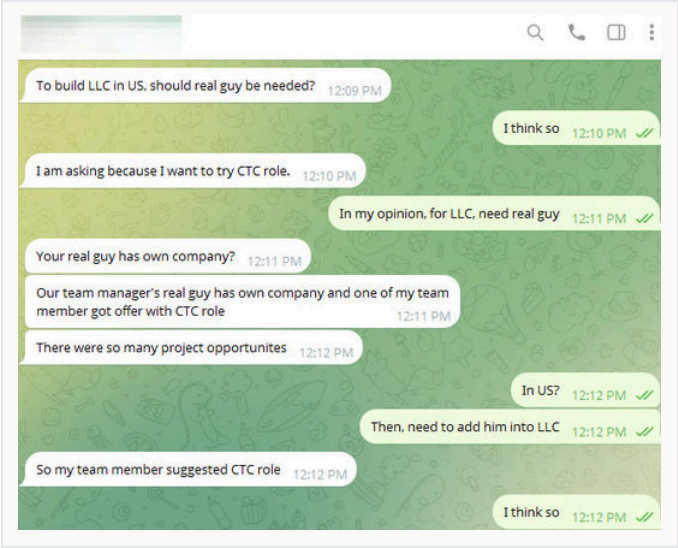
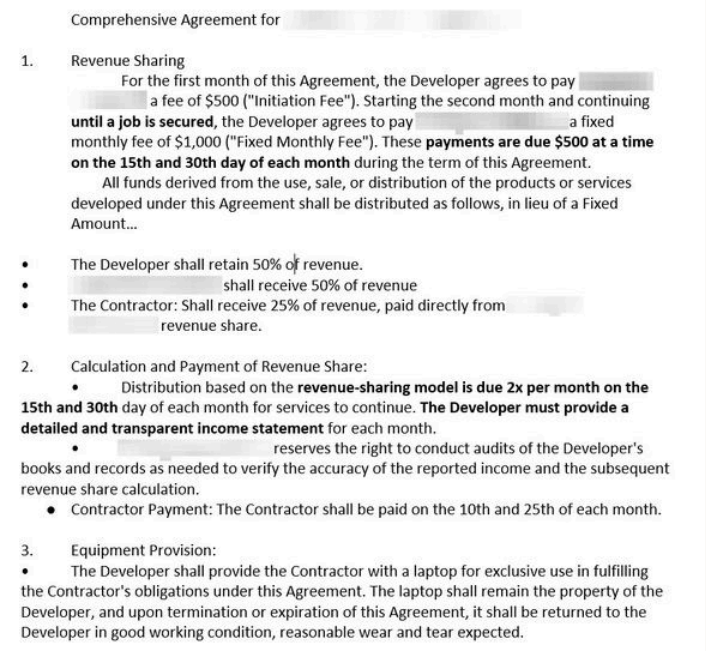


FIG. 51 | A documented discussion (I guess a reminder?) on why LLCs are useful and what is needed to obtain one

In addition to filing documentation and instructions, written contracts for multiple shell companies were observed within the archive.



Comprehensive Agreement for [redacted]

1. Revenue Sharing

For the first month of this Agreement, the Developer agrees to pay [redacted] a fee of $500 ("Initiation Fee"). Starting the second month and continuing **until a job is secured**, the Developer agrees to pay [redacted] a fixed monthly fee of $1,000 ("Fixed Monthly Fee"). These **payments are due $500 at a time on the 15th and 30th day of each month** during the term of this Agreement.

All funds derived from the use, sale, or distribution of the products or services developed under this Agreement shall be distributed as follows, in lieu of a Fixed Amount...

- The Developer shall retain 50% of revenue.
- [redacted] shall receive 50% of revenue
- The Contractor: Shall receive 25% of revenue, paid directly from [redacted] revenue share.

2. Calculation and Payment of Revenue Share:

- Distribution based on the **revenue-sharing model is due 2x per month on the 15th and 30th** day of each month for services to continue. **The Developer must provide a detailed and transparent income statement** for each month.
- [redacted] reserves the right to conduct audits of the Developer's books and records as needed to verify the accuracy of the reported income and the subsequent revenue share calculation.
- Contractor Payment: The Contractor shall be paid on the 10th and 25th of each month.

3. Equipment Provision:

- The Developer shall provide the Contractor with a laptop for exclusive use in fulfilling the Contractor's obligations under this Agreement. The laptop shall remain the property of the Developer, and upon termination or expiration of this Agreement, it shall be returned to the Developer in good working condition, reasonable wear and tear expected.

FIG. 52 | Contract associated with a NK shell company detailing specific conditions

The details provided in the contract are consistent with historical shell companies and the payment models used correlate with existing fraudulent remote work prices.

Historical Corroboration

- In a **June 2025 coordinated action**, DOJ described U.S. facilitators Kejia Wang and Zhenxing Wang standing up shell companies — **Hopana Tech LLC, Tony WKJ LLC, and Independent Lab LLC** — with matching websites and financial accounts, specifically to make overseas IT workers appear affiliated with legitimate U.S. businesses. Kejia Wang was sentenced to 108 months; Zhenxing Wang to 92 months. Nine co-defendants charged in the same action remain at large, with a State Department reward of up to $5 million outstanding.

Section Four | What Else?

Who is our new friend?

According to documentation and chat logs, our NK operator goes by the name of “spring day” and goes by the initials RJM. There weren’t enough details to map out their full name, however, I was able to note that he manages a team of three and was born on 03/06/2000. There were a few teams our friend may have been associated with, these had names such as *Color Team* and *Team Dev Money*. In his free time, he loves to play Counter Strike.

You shouldn’t be surprised to find out that there are dozens, maybe hundreds, of photos of our friend within the archive.

FIG. 53 | NK Photo #1

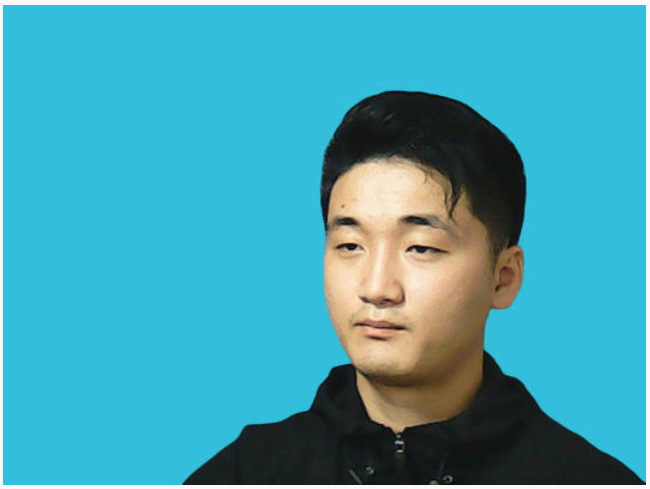


FIG. 54 | NK Photo #2

FIG. 55 | NK Photo #3

The Didenko Indictment (Relevance)

On May 16, 2024, the Justice Department seized upworksell.com and diverted its traffic to the FBI. The site was operated by Oleksandr Didenko, a Kyiv resident who also used the name "Alexander Didenko," and it functioned as a storefront for exactly what Stage 2 describes: stolen U.S. identities and pre-built freelance platform accounts, sold or rented to overseas IT workers. Polish authorities arrested him; he was extradited to the United States on December 31, 2024. He pleaded guilty on November 10, 2025 to wire fraud conspiracy and aggravated identity theft, and in February 2026 was sentenced to 60 months in prison, 12 months of supervised release, forfeiture of more than $1.4 million, and roughly $46,500 in restitution.

Didenko managed as many as 871 proxy identities and created more than 2,500 fraudulent accounts across freelance job platforms, money service transmitters, email providers, and social media. His clients obtained work at

more than 40 U.S. companies. He also paid U.S. residents to receive and host company hardware, operating at least three laptop farms across California, Tennessee, and Virginia — and in late 2023, at a customer's request, shipped a computer to the Arizona laptop farm run by Christina Chapman, who was arrested the same month his domain was seized and later sentenced to 102 months.

In the archive, Didenko is mentioned as a reliable broker associated with the fraudulent identity gathering and verification. After Didenko was arrested, discussions arose between operatives detailing changes in their preferences.

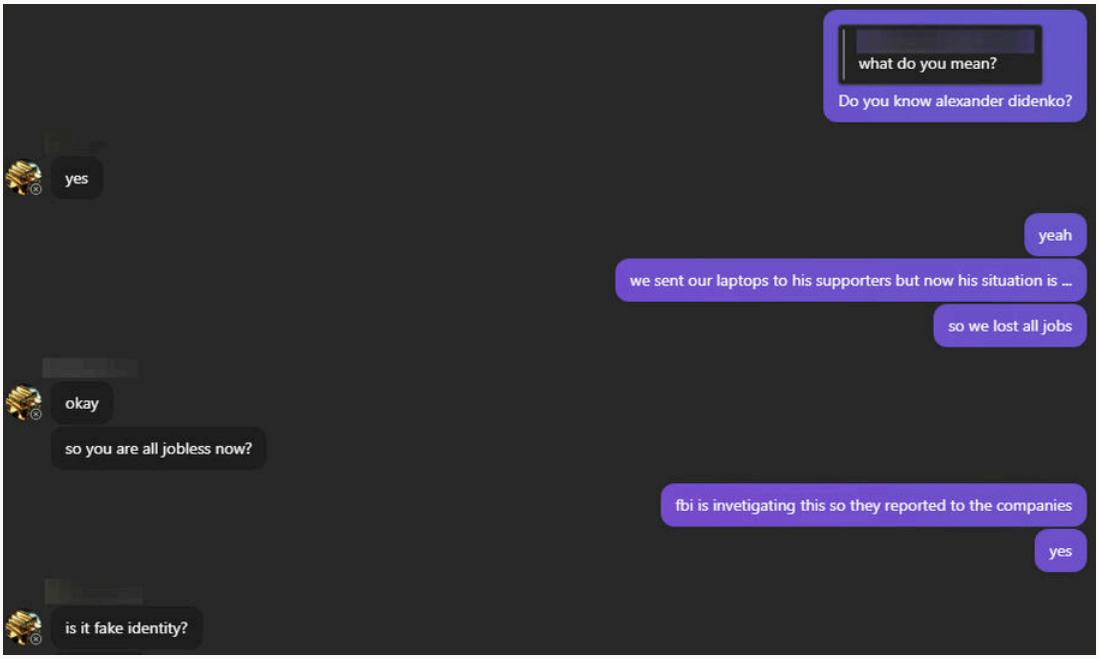


FIG. 56 | Documented discussion (presumably for instructions) on what not to do

> Note: Upworksell sold freelance-platform accounts. The current model now prefers direct employment or corp-to-corp vendor contracts using reliable American facilitators.

Identity Verification Methods (Tips)

A weak but occasionally useful check: pull a suspicious applications address into **Google Street View**.

A recurring pattern across addresses tied to these applications — shipping addresses, registered office addresses on entity filings, addresses of record on resumes — is that the property is blurred out in Street View, or the address resolves to a strip-mall suite, a mail center, or a virtual office shared with a long list of thinly documented LLCs. Neither is evidence of anything on its own. Blur requests are free, take minutes, and are made by ordinary homeowners for ordinary privacy reasons.

Appendix | Notable IOCs and TTPs

Every service, site, platform, and application named anywhere in this article.

Victim selection and identity acquisition

LinkedIn — Primary victim-sourcing pool. Search by common American name and developer job title; profiles without photographs are explicitly preferred.

TruthFinder — Background report on the selected victim.

Intelius — Same function: address history, relatives, employment, court records.

FastPeopleSearch — Same function; free tier used for initial confirmation.

Telegram — One of their main communication channels; used for contacting brokers, facilitators, etc.

upworksell.com — Historical. Didenko's marketplace for stolen identities and pre-built freelance accounts; seized May 16, 2024.

Identity validation

State DMV self-service portals (TX, MI, SC, AL, NY, KS, MD, AZ, PA, NJ) — Confirm a purchased driver's license number is live and matches the name before spending money on documents.

Public SSN validation services (e.g. ssn-check[.]org) — Confirm a purchased SSN is structurally valid and issued.

Document fabrication and photo manipulation

oldie.veriftools.ru — Russian-hosted generator for passports, driver's licenses, ID cards, and bills/statements. Domain seized in August 2025.

trustidcard.com — Broker producing documents to order; described in the manual as the expensive option.

faceswapper.ai — Match a document photograph to whoever will appear on camera.

instant-portrait.com — Same; also used to defeat reverse image search on persona photos.

Network infrastructure

cloudzy.com — U.S.-region VPS, billed hourly so instances can be created and destroyed at will.

ishosting.com — U.S. and Canada VPS, preferred where a stable long-lived IP is needed.

IPRoyal — Residential proxy.

CCProxy — HTTP/SOCKS proxy on a VPS or supporter machine.

Astrill VPN — VPN provider.

Windscribe VPN — Same role, secondary.

Hostinger — Domain registration and hosting (also used for mailbox infrastructure).

Vercel — Free subdomain hosting.

bidpro-ochre[.]vercel[.]app — Bidding-as-a-service storefront: batch pricing, client list, live Google Sheets application logs (is not directly associated with the DPRK)

Accounts, phone numbers, and verification

mailforspam.com — Disposable secondary address during Gmail account creation.

sms-man.com — SMS verification numbers at scale.

sms-activate.org — Same.

2fa.live — Browser-based TOTP generation. MFA secrets shared across a team rather than bound to a device.

Skype — Historical persona phone numbers and broker contact; assessed as drawing less suspicion than Google Voice. Now defunct.

slynumber.com — Current phone number replacement for Skype numbers.

hushed.com — Same.

Google Voice — Explicitly rejected form of VoIP phone numbers.

AirDroid — Remote control of a physical Android handset from a computer.

LDPlayer — Android emulator used to redirect ID verification challenges away from a real camera.

ShareX — Screen capture of verification QR codes for redirection into emulator.

VCAM — Virtual camera.

OBS — Recording software with same role as VCAM.

Persona (inquiry.withpersona.com) — Identity verification vendor.

Cookie-Editor (Chrome extension) — Import LinkedIn session cookies so an authenticated session moves between machines and operators without re-authenticating.

protectedtext.com — Free password-protected plaintext notes.

OneNote — Per-identity dossiers in the archive.

SendGB — Free file transfer with a retention window measured in days.

Persona construction and application

FlowCV — Resume builder.

ChatGPT — Resume drafting, tailoring, and interview answer generation.

Claude — Same, named alongside ChatGPT in the manual.

ResumeKit — Per-application resume tailoring in outsourced bidder workflow.

LazyApply (Chrome extension) — Bulk application bot.

Workday — ATS submission target. IP-aware, which is why VPNs are rejected.

Greenhouse — ATS submission target.

Indeed, Dice, Glassdoor, SimplyHired, ZipRecruiter, CareerBuilder — Named job boards for volume application.

LinkedIn — Shares an individuals current and historical employment history.

Google Sheets — Shared application logs with color-coded status columns, between buyer and bidder.

Discord — Bidder recruitment and coordination; also a source of aged LinkedIn accounts.

WhatsApp — Documented channel of communication.

Reddit and adult cam sites — Facilitator recruitment channels documented by Nisos.

Interview and presence

Voicemeeter Banana — Virtual audio mixer routing one person's voice into a call another person appears to be attending.

Zoom — Interviews; also abused for remote control where enterprise policy permits it.

Webex — Video conferencing tool used for remote control and screen sharing.

Google Meet — Another viable option for abusing remote control and screen sharing.

Excalidraw — Whiteboarding during technical interviews.

Remote access to employer hardware

PiKVM — Hardware KVM on the employer-issued endpoint.

AnyDesk — Remote access software.

RustDesk — Same, open-source alternative.

TeamViewer — Same.

Google Remote Desktop — Same.

Entity formation and contracting

Texas SOSDirect — Online filing portal for the Certificate of Formation (Form 205).

IRS online EIN application — Federal tax ID assigned immediately after formation, enabling a business bank account.

Upwork — Freelance platform. Accounts created in a real American's identity because the platform tracks IP.

Payments and cash-out

HuruPay — Stablecoin-backed virtual USD/EUR/GBP accounts marketed to non-U.S. residents. Receives bi-weekly payroll and off-ramps near-instantly.

Payoneer — Withdrawal target for Upwork earnings held in the recruit's real name.

PayPal — Same.

CoinGate — Crypto-to-gift-card gateway.

Binance — Exchange and BSC on-ramp.

USDT (BEP20, TRC20) — Primary settlement asset for bidder payments and broker fees.

USDC, ERC20, Polygon, Arbitrum — Additional rails visible in the ledger for splitting and moving proceeds.

MITRE ATT&CK Mapping

T1589.001 — Gather Victim Identity Information
Written victim selection criteria; LinkedIn name-and-role sourcing; background report acquisition.

T1585.001 — Establish Accounts: Social Media
Purchased and laundered LinkedIn accounts; purchased Facebook accounts.

T1586 — Compromise Accounts
Aged LinkedIn account takeover; session cookie portability.

T1588.007 — Obtain Capabilities: Artificial Intelligence
ChatGPT for resumes and answers; AI face-swap tooling.

T1583.003 — Acquire Infrastructure: Virtual Private Server
Cloudzy and ishosting U.S.-region instances.

T1583.008 — Acquire Infrastructure: Malvertising/Proxy
IPRoyal residential proxies; CCProxy chaining.

T1199 — Trusted Relationship
Employment as the access vector; intermediary LLC contracting.

T1078 — Valid Accounts
Employer-issued credentials retained in dossiers.

T1219 — Remote Access Software
RustDesk, AnyDesk, Google Remote Desktop.

T1200 — Hardware Additions
PiKVM on employer-issued endpoints.

Prior Reporting

This investigation builds on and corroborates published work by other researchers. Anyone working this problem should read all of it:

Hayden McKenzie, *Inside a DPRK IT Worker Operation: How North Korea Outsources Job Fraud at Scale* — the outsourced bidder network, per-application and per-interview pricing, the Gmail forwarding architecture, and the AI-assisted submission workflow.

Group-IB, *Uncovering the DPRK's fake remote developer ecosystem* — persona archives, identity reuse across GitHub and portfolio infrastructure, the service stack behind a synthetic developer identity, and the most usable set of HR, finance, and security mitigations published to date.

Flare Research and IBM X-Force, *Inside the North Korean Infiltrator Threat* — internal DPRK back-office platforms (RB Site, NetkeyRegister), NetKey/OConnect, IP Messenger, timesheet and ranking systems, Astrill VPN use, and the Google Translate tradecraft underpinning daily work.

Nisos, *Inside a DPRK Employment Fraud Operation* — organizational hierarchy, 170,000 applications to 76 offers, facilitator recruitment channels and pricing, AI-assisted interviewing, and the three revenue models.

DTEX Systems, *Exposing DPRK's Cyber Syndicate and Hidden IT Workforce* — organizational structure, self-funding quotas and the sub-20% earnings retention figure, the IT worker ecosystem role map, cross-employer bastion access, and rare operational imagery.

If you believe your organization may have employed one of these individuals, or if you have information relevant to this investigation, reach out at intel@haydenmckenzie.com.

Hayden McKenzie · Independent Security Researcher
haydenmckenzie.com · intel@haydenmckenzie.com · Substack ↗ · LinkedIn ↗ · CV ↗