

COUNTERINTELLIGENCE IN THE AGE OF DUCHENET SIGNALS, SPOOFS, AND SUBVERSION

BY

DACK SESSIONS

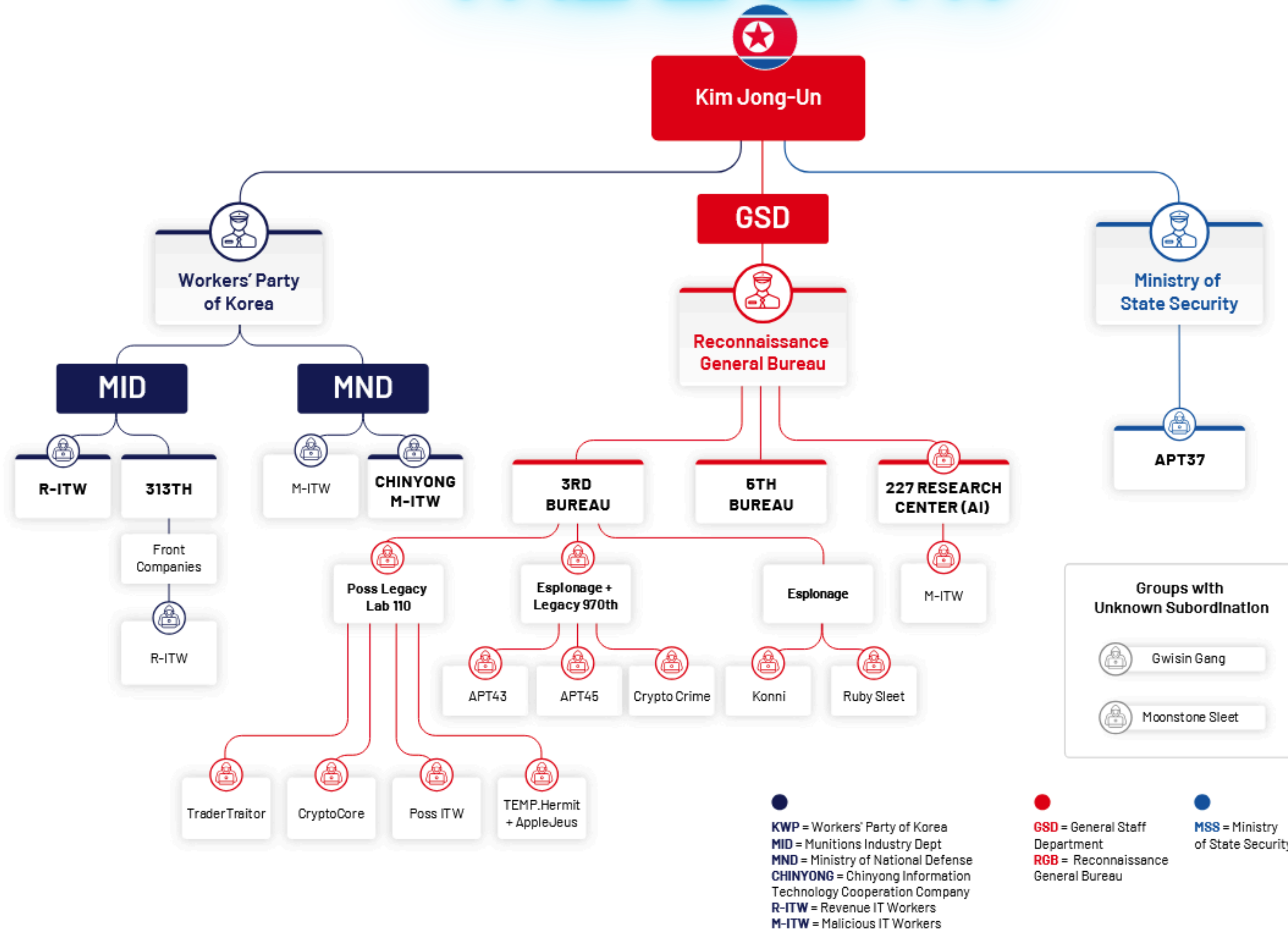
ROOT://_WHO I AM

- Mobile Security & Counterintel Researcher (also a memelord)
- Bartender IRL, Hacker in VR, and working in AR/AXI
- Fix ITS security for the memez
- CyberSec Rapper
- Pre Seed Money Comp Sci Student
- CyberSec YouTuber @JackSessions
- 2x CVE-2025-50861, CVE-2025-50862
- Wanted for Treason... (Kim did not like my rap)



DPRK Org Chart

THE ENEMY



WPK = Workers' Party of Korea
MID = Munitions Industry Dept
MND = Ministry of National Defense
CHINYONG = Chinyong Information Technology Cooperation Company
R-ITW = Revenue IT Workers
M-ITW = Malicious IT Workers

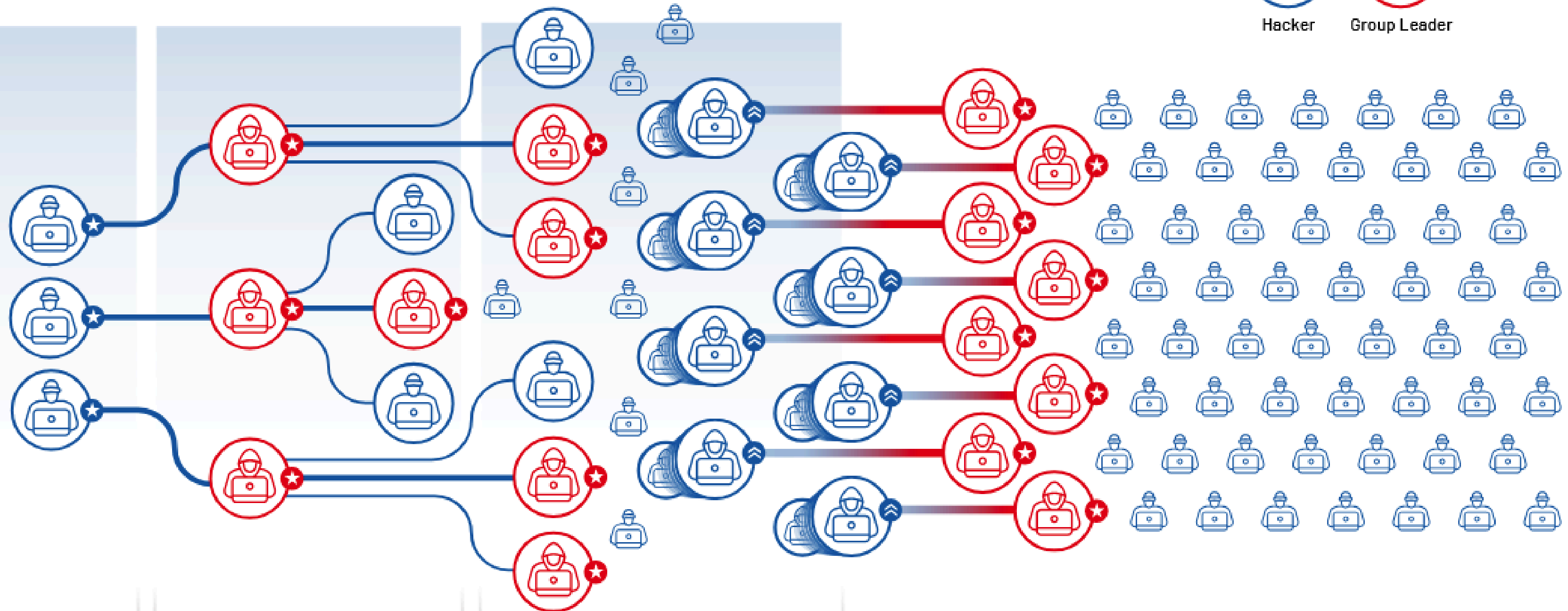
GSD = General Staff Department
RGB = Reconnaissance General Bureau

MSS = Ministry of State Security

CI = BATTLEFIELD OF SHADOWS

Original Hackers Then to Now

Program Development



2009-10

Lazarus Group

2014-15

- TEMP.Hermit
- APT37
- APT38
- APT43
- APT45
- Konni

2020-21

- TEMP.Hermit
- APT37
- APT43
- APT45
- Konni
- ITW
- Ruby Sleet
- CryptoCore
- TraderTraitor
- AppleJeus
- Front Companies

2025

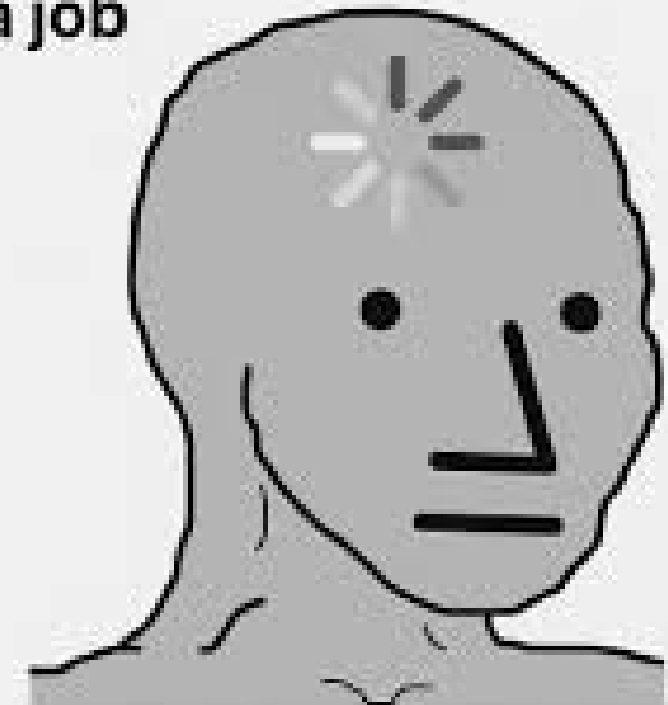
- TEMP.Hermit
- APT37
- APT43
- APT45
- Konni
- ITW
- Ruby Sleet
- Gwisin Gang
- Malicious ITW
- Moonstone Sleet
- AI Unit227
- CryptoCore
- TraderTraitor
- AppleJeus
- Crypto Crime
- Front Companies

GOALS OF MODERN CI

- Gain access while avoiding sanctions or detection.
- Bypass org background checks using fake LinkedIn, resumes.
- Blend into remote workforces via false personas = it's strategic infiltration.



Me when the LinkedIn recruiter asks me to write a national security white paper to apply to a job



Brain.exe has stopped working.

HUMINT + SIGINT MERGE

- DPRK uses real time behavioral cues (keyboard layout, time zones, syntax) to align false personas.
- HUMINT elements: personal websites, resumes, GitHub, job interviews.
- SIGINT: infra use, malware deployment, traffic evasion.

LEARN MORE ABOUT ME



Senior Software Engineer

(For App and my job), I'm ready to collect only on me.

Website: www.example.com

Phone: (555) 123-4567

City: Sancho-Cusamanga, CA

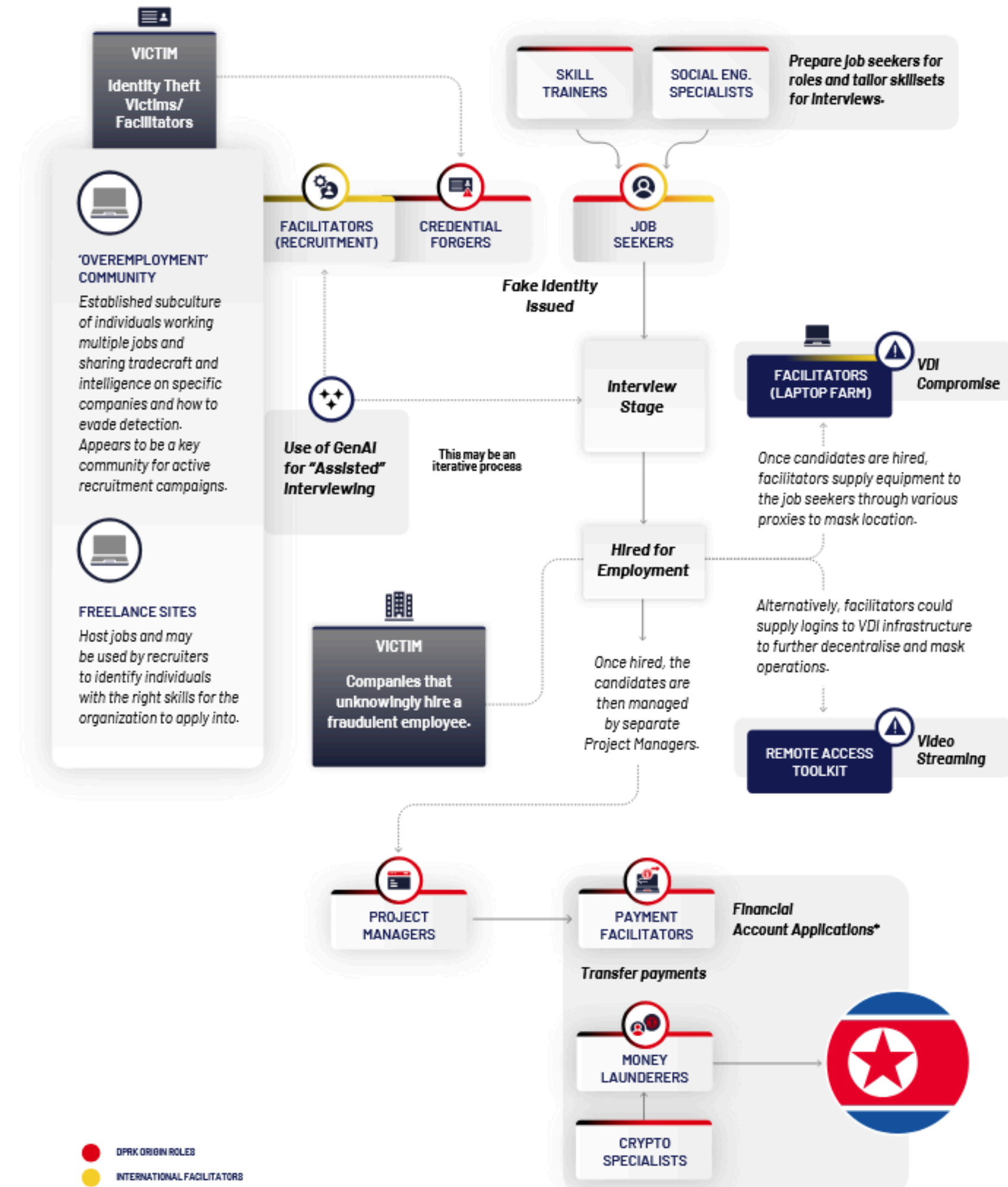
Degree: Bachelor

Email: example@example.com

Interview: Active

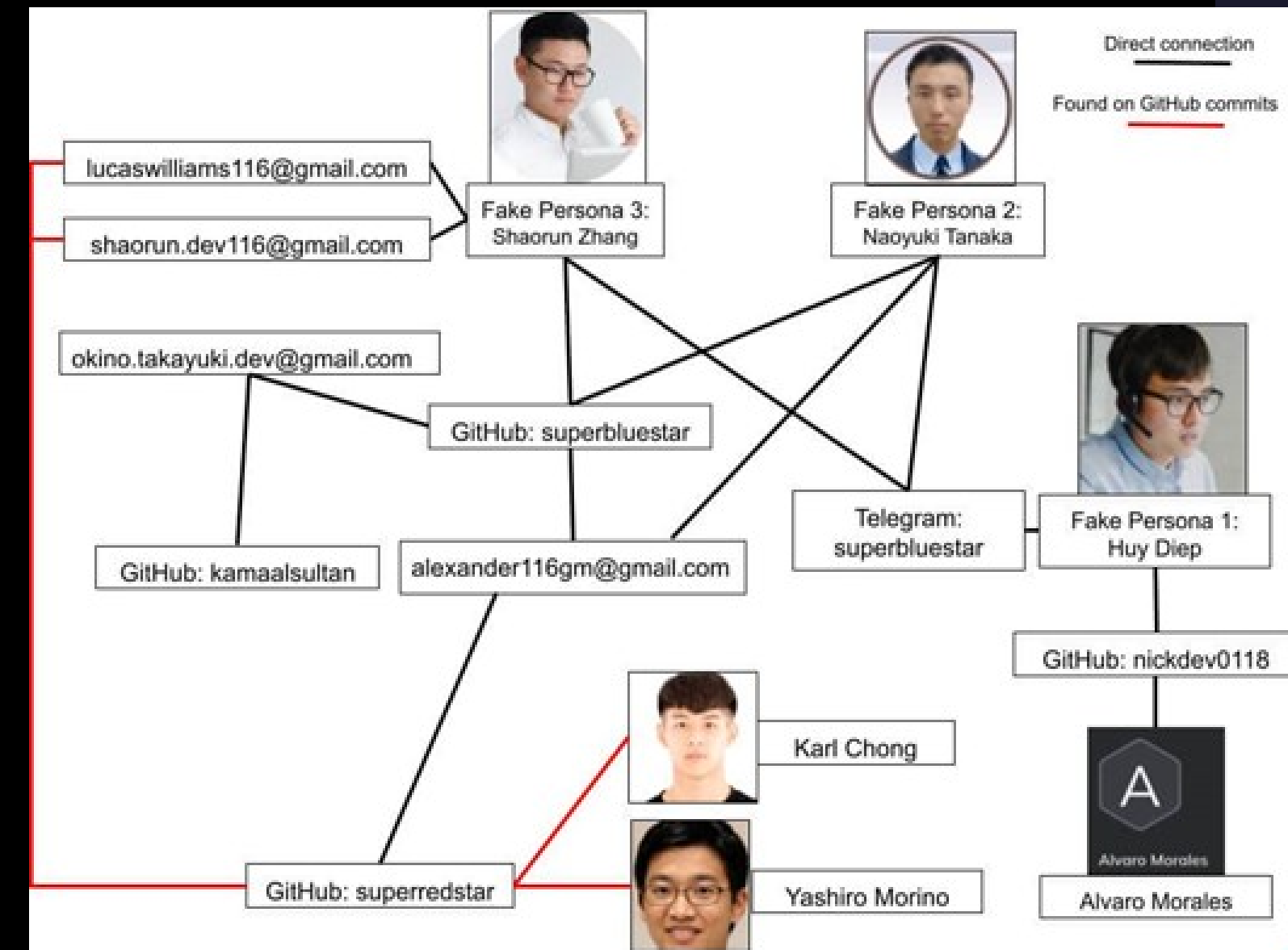
Highly skilled, detail-oriented, organized and meticulous software engineer with 10+ years of experience in web development. Works as fast pace to meet tight deadlines. Specialized in working with React, Node, MySQL, and Redux Frameworks to create interactive, secure experiences for users.

In Focus: IT Workers



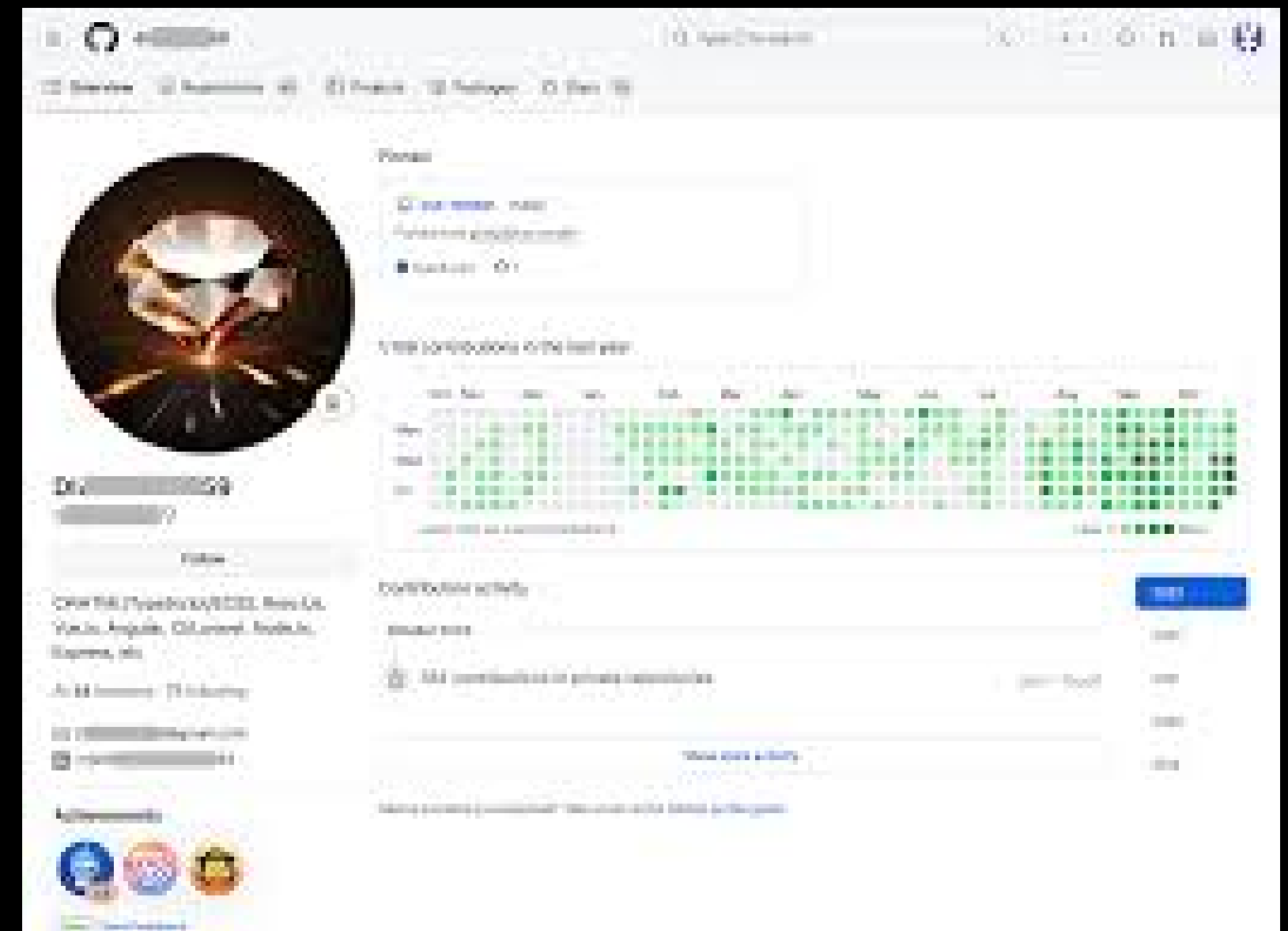
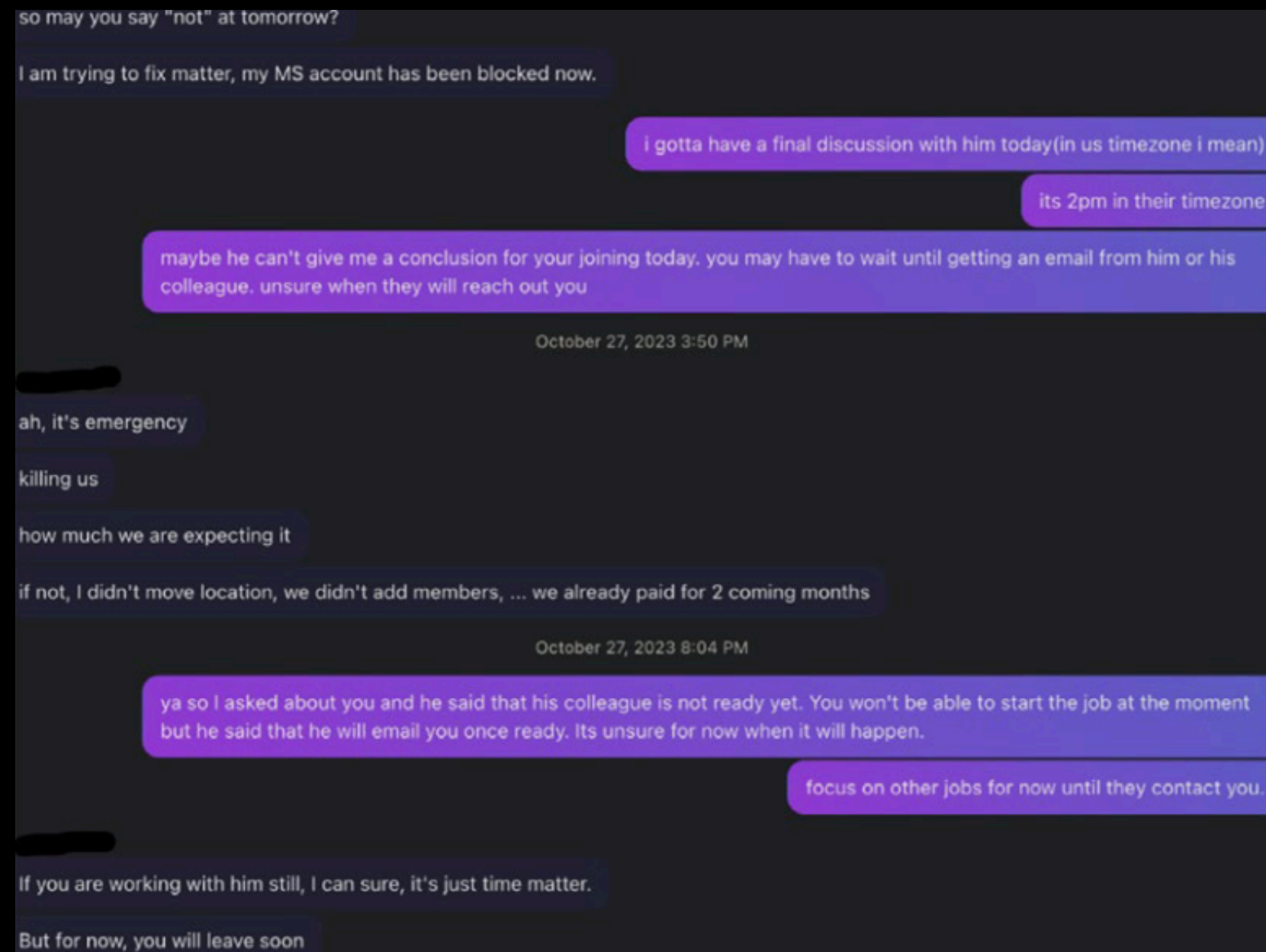
LOGS, CODE, TELEMETRY = ALL SPOOFABLE

- LOGS CAN BE CLEAN BUT IDENTITIES BEHIND THEM ARE NOT.
- DPRK ACTORS USE WESTERN INFRASTRUCTURE + FAKE LOGINS TO OBSCURE TRUE AFFILIATIONS.
- CREDENTIAL REUSE ACROSS FALSE IDENTITIES SHOWS WEAK POINTS IN LOG-ONLY ATTRIBUTION.



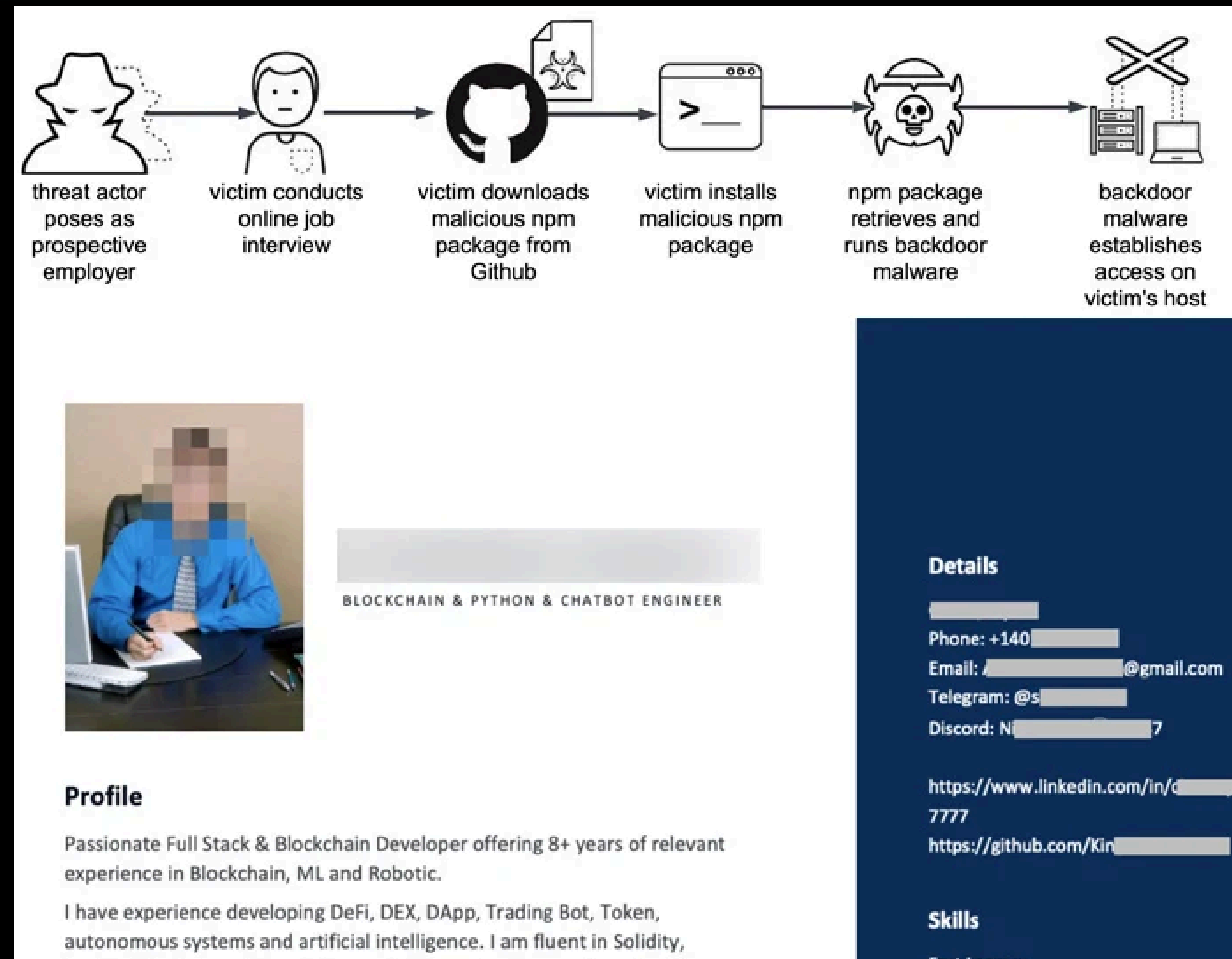
SPOOFED SIGNALS

- Employees spoof US time zones, write in English fluently, mask MAC and location.
- DPRK “hidden” IT workers used GitHub and LinkedIn accounts to simulate location legitimacy.



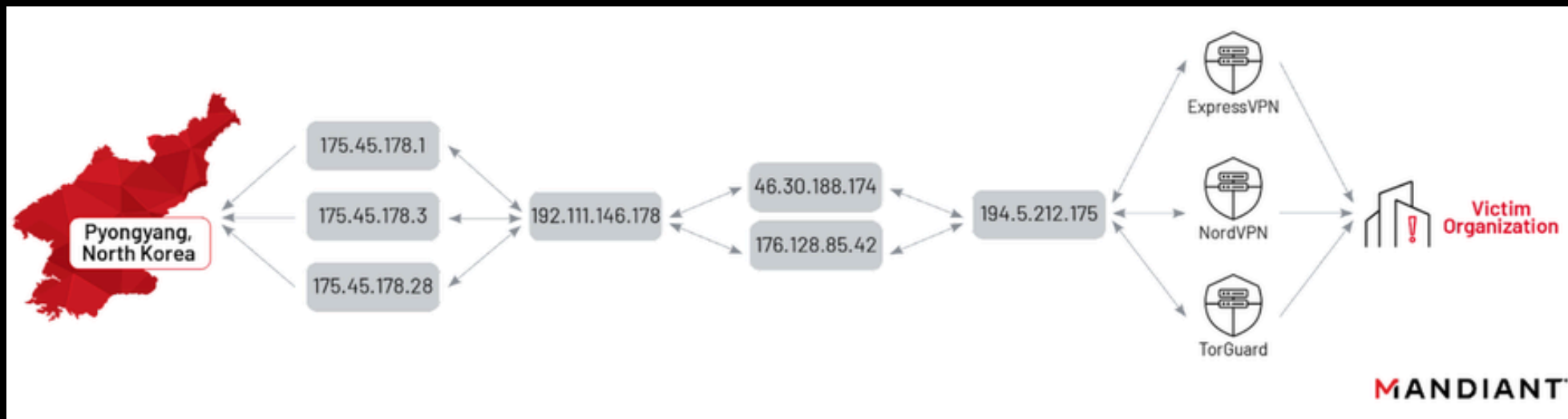
FALSE FLAGS IN CODE

- Use of English language commits, Western naming conventions in repos.
- Targeting US/EU orgs while appearing as freelancers from NA/EU.
- Use of compromised or falsely registered devices and VM profiles.



FAKE LOGS & METADATA

- Users spoof IPs with VPNs and change machine fingerprinting data.
- Login locations misaligned with actual behavioral times (e.g., active at 3AM PST daily).
- Resume metadata and cloud based activity logs conflict with claimed persona.



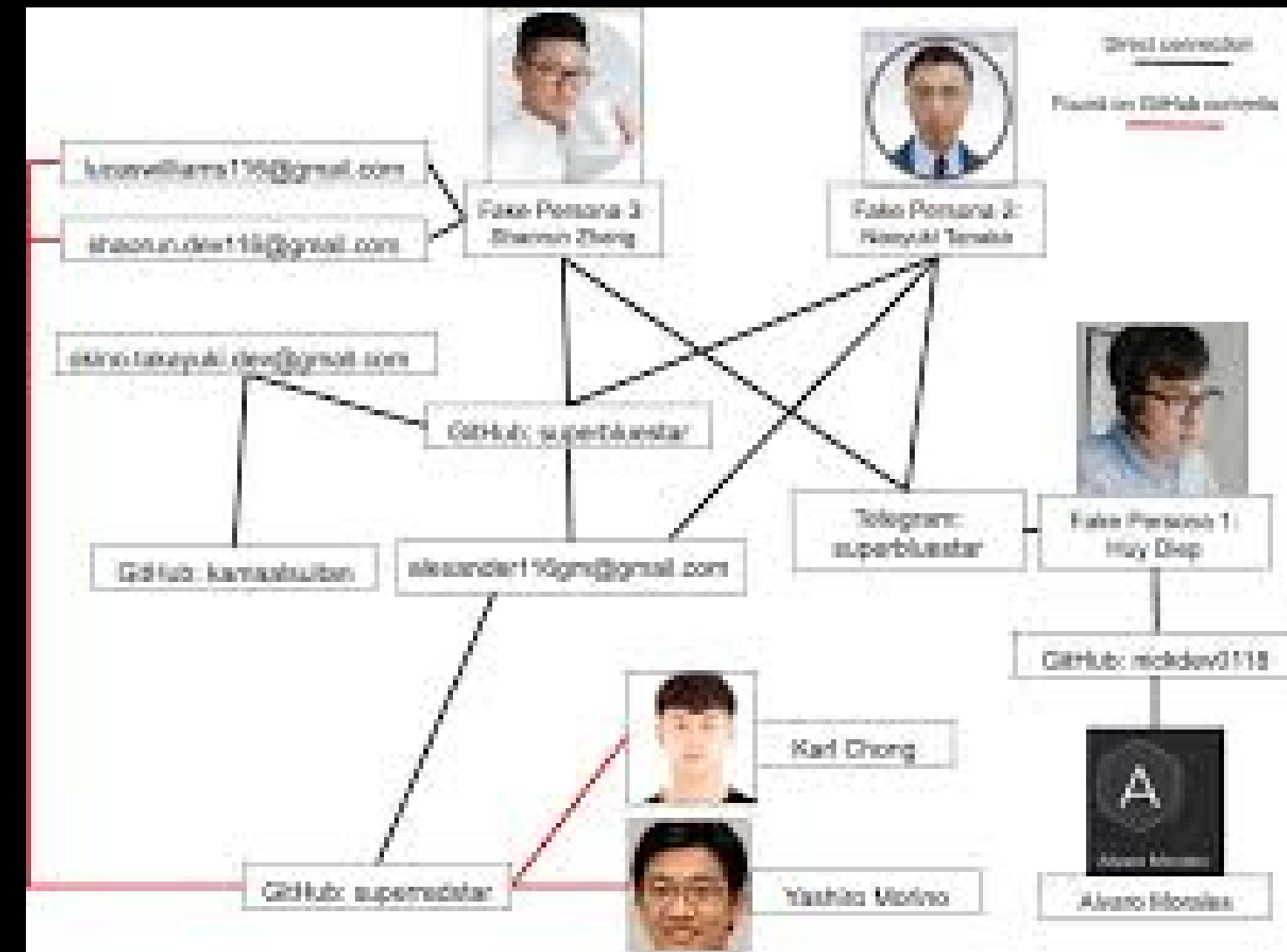
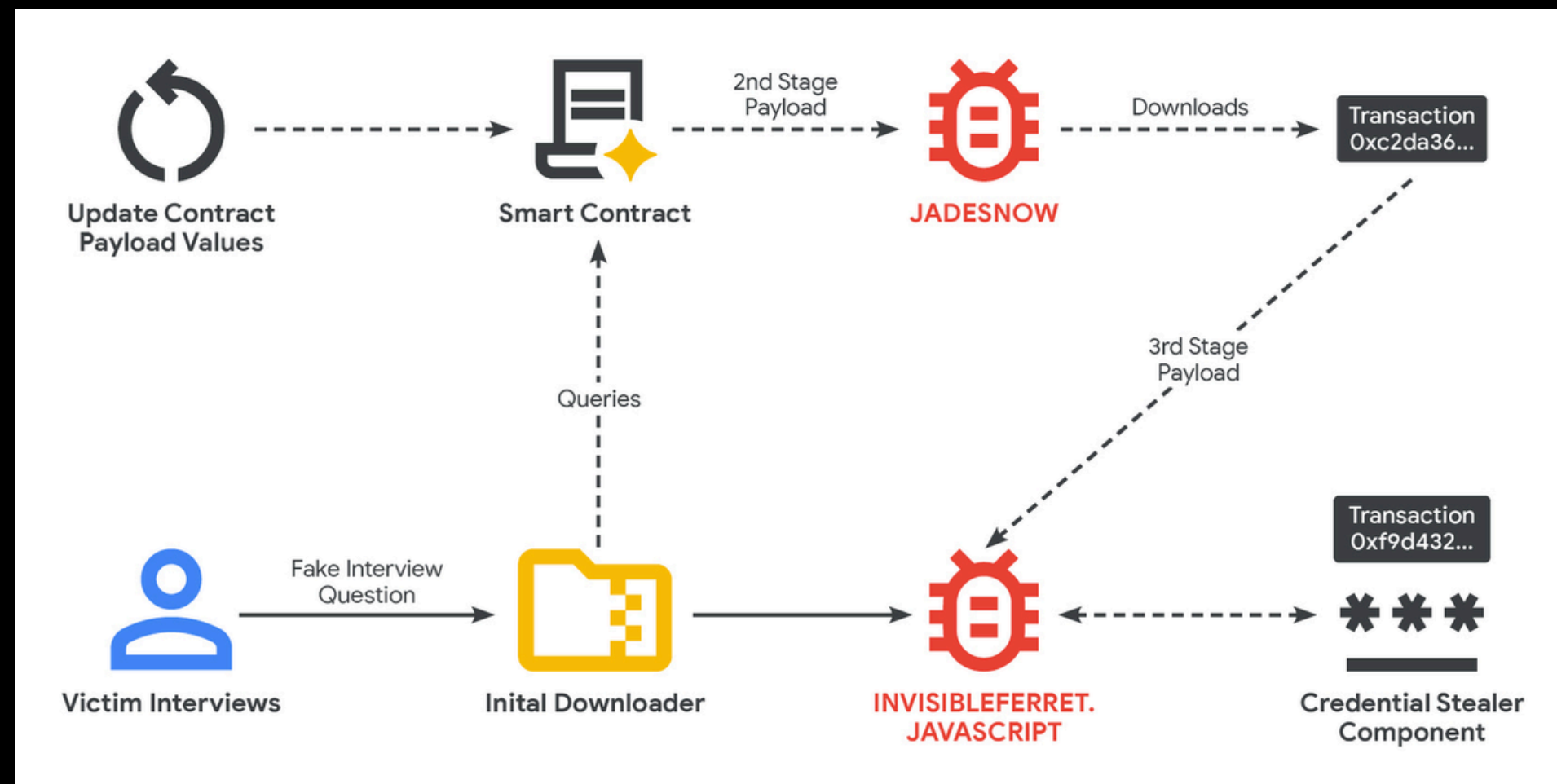
MEME WARFARE / NARRATIVE CI

- DPRK workers posed as job candidates during peak remote work period.
- Their narrative: just a freelance dev, skilled, lives in US thus never questioned.
- Resume artifacts were fabricated using real English speaking templates.



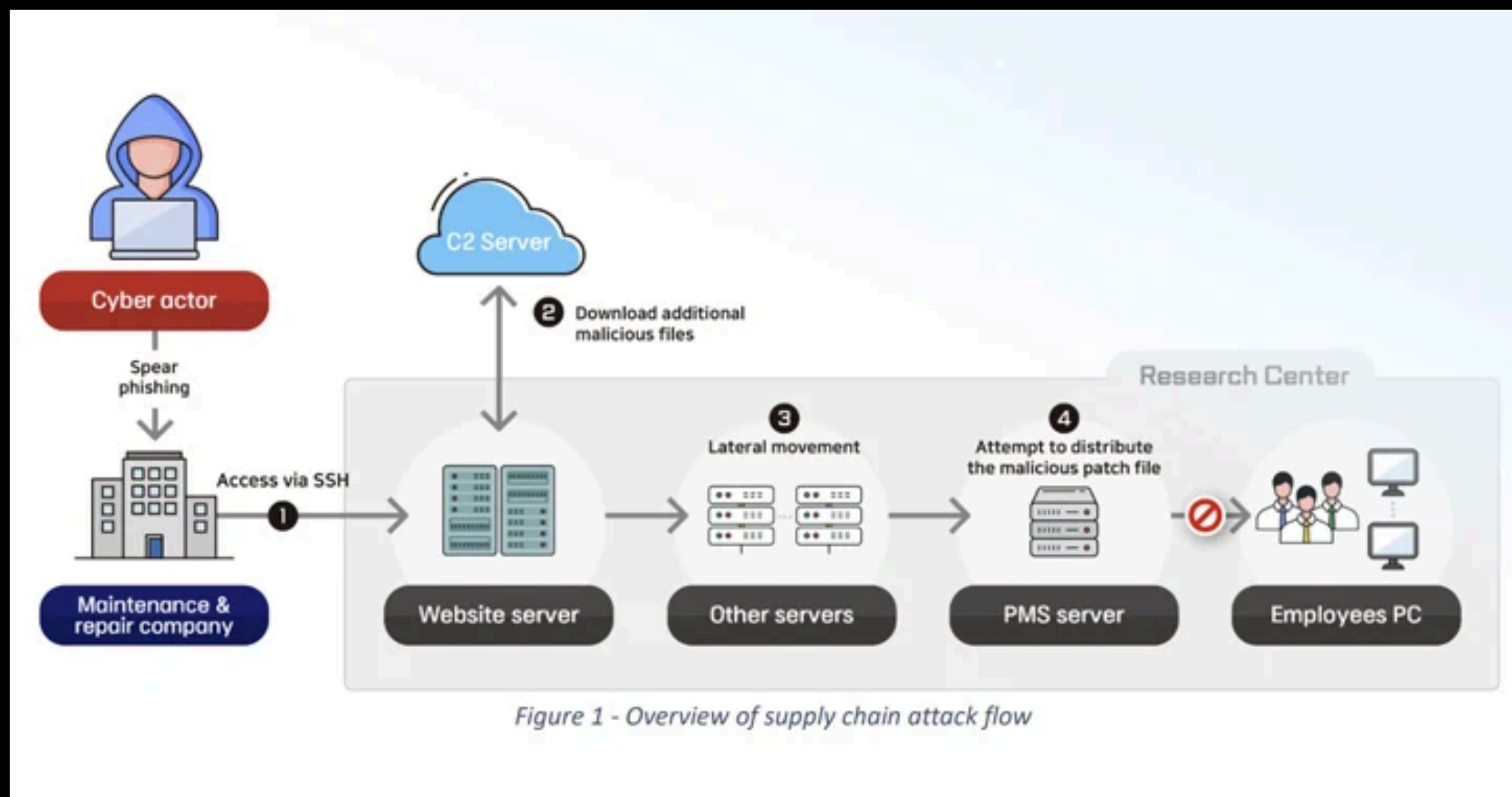
CASE STUDY: MALWARE FLAG PLANTING

- **Hidden IT workers uploaded malicious code via GitHub repos linked to fake names.**
- **Malware misattributed to legitimate companies due to reused environments.**



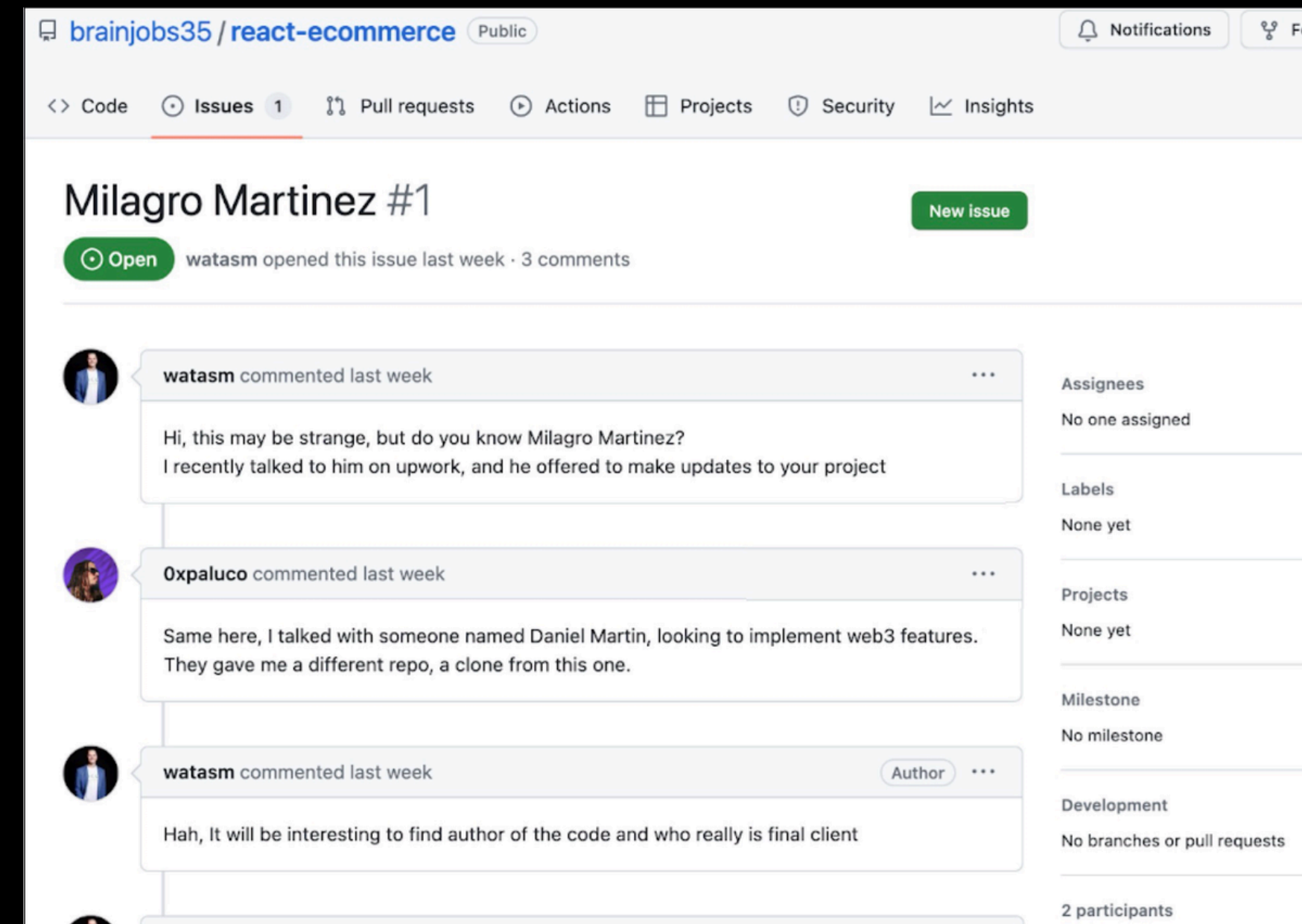
CASE STUDY: CLEAN LOGS, DIRTY INTENT

- Clean activity logs on cloud services (GCP, GitHub), yet behavioral data exposed anomalies.
- Cross reference login data with working hours & biometric signals/Pysch data.
- Keyboard layout + persistent C2 callbacks showed real origin vs logs.



BEHAVIORAL INVARIANTS

- DPRK devs reused keyboard layouts (non-QWERTY), file naming schemes.
- Behavioral slips: time of work, mistake in payment info, reused email aliases.



CI MINDSET FOR BLUE TEAMS

Logs lie. Patterns don't.

Run behavior based profiling of dev environments

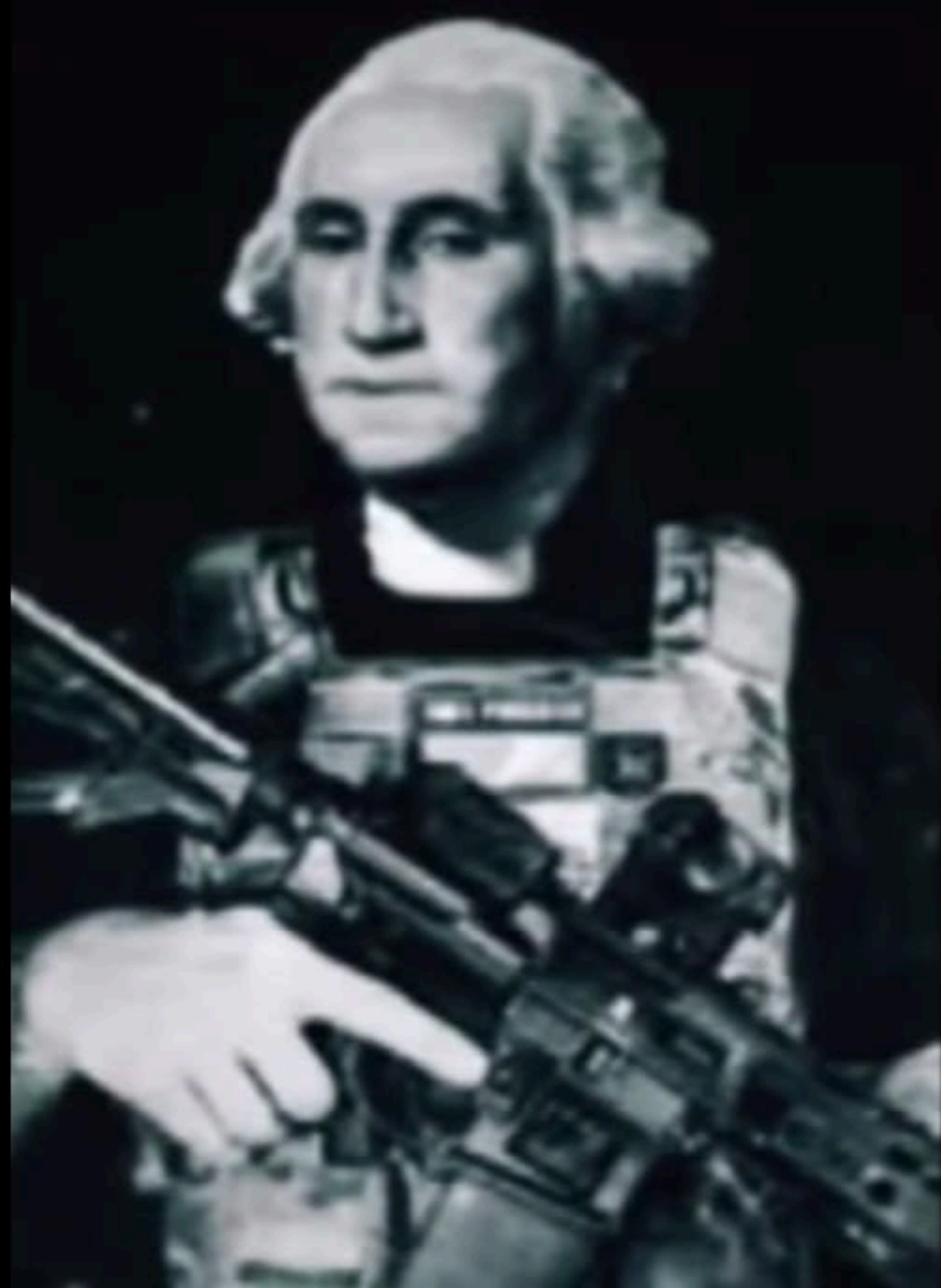
Validate human layer + machine layer. THAT IS HOW YOU WIN AT CI!

Assume persona masking in all remote interactions.

Use OSINT on email aliases, blockchain txns for payout matching/Chain tracing.

THREE KEY INSIGHTS THAT MUST DRIVE THE NEXT PHASE OF DEFENSE

- **This is a national security challenge. DPRK operators are embedded in global supply chains and systems. Waiting is not an option.**
- **Attribution is only the beginning. Countering this threat requires behavioral insight, contextual intelligence, and awareness of the motivations driving these operatives.**
- **The APT vs. IT worker distinction is obsolete. These actors function as one enterprise in support of regime priorities.**



“Stay strapped or get
clapped”

– *George Washingmachine*

THANK YOU



—
GET IN TOUCH ↘



+7 (499) 244-16-06



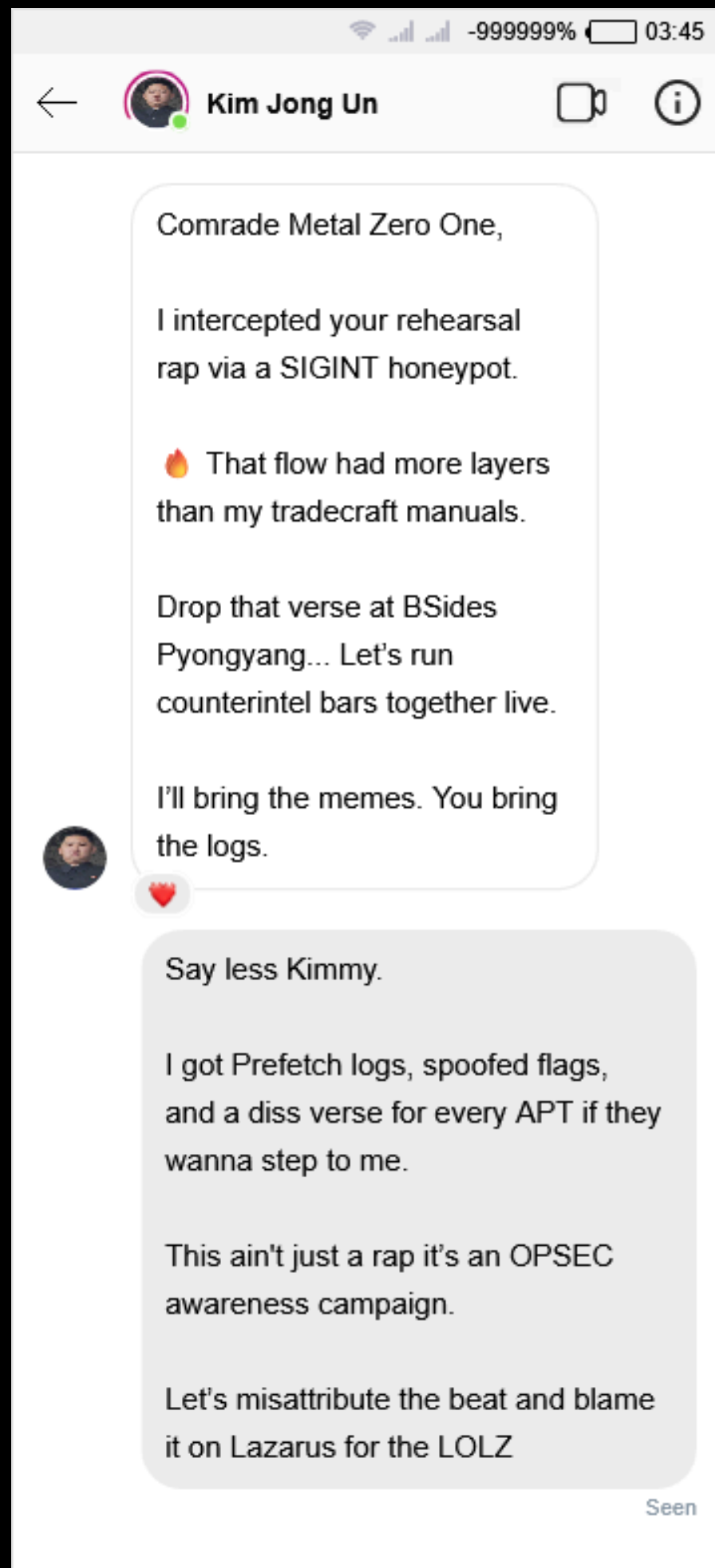
[WWW.LINKEDIN.COM/IN/DACKSESSIONS](https://www.linkedin.com/in/dacksessions)



DACKSESSIONS@PROTONMAIL.COM



_Jack.34



BSIDES PYONGYANG RAP

