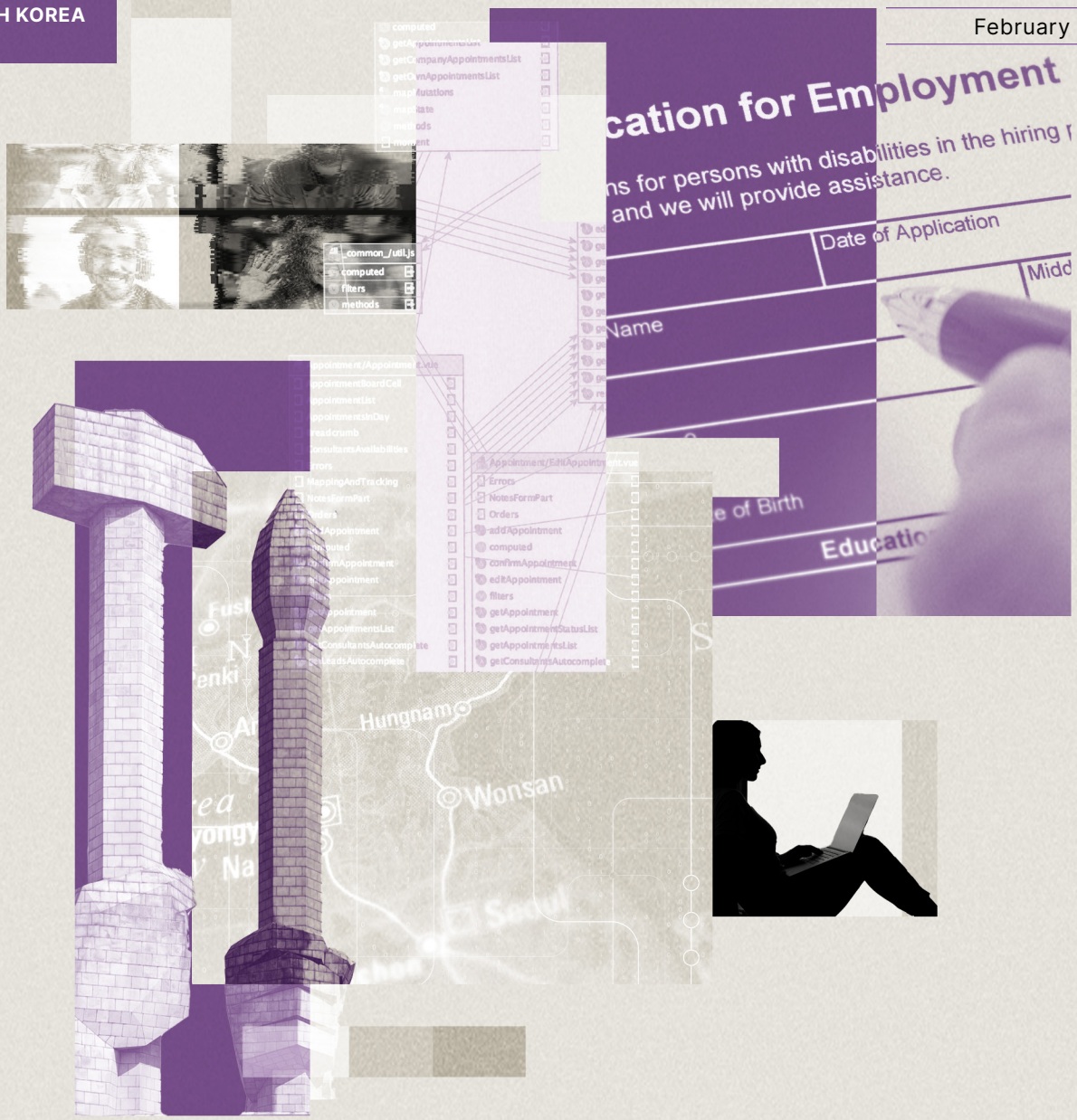
CYBER THREAT ANALYSIS

NORTH KOREA

Recorded Future®

By Insikt Group®

February 13, 2025



Inside the Scam:
North Korea's IT Worker Threat

PurpleBravo has targeted at least seven entities, three of which are in the cryptocurrency sector, including a market-making firm, an online casino, and a blockchain software company.

PurpleBravo was active on at least three hiring websites, Telegram, and GitHub, regularly posting job advertisements and updating repositories.

Insikt Group identified at least seven suspected North Korea-linked front companies operating in China spoofing legitimate IT firms in China, India, Pakistan, Ukraine, and the United States.

Executive Summary

In an era in which remote work has become the norm, North Korea has seized the opportunity to manipulate hiring processes, using fraudulent information technology (IT) employment to generate revenue for the regime. North Korean IT workers infiltrate international companies and secure remote positions under false identities. These operatives not only violate international sanctions but also pose severe cybersecurity threats, engaging in fraud and data theft and potentially disrupting business operations.

Beyond financial fraud, these IT workers have been linked to cyber espionage. Insikt Group tracks PurpleBravo (formerly Threat Activity Group 120 [TAG-120]), a North Korean-linked cluster that overlaps with the "Contagious Interview" campaign, which primarily targets software developers in the cryptocurrency industry. The campaign employs malware such as BeaverTail, an infostealer that gathers sensitive information; InvisibleFerret, a cross-platform Python backdoor; and OtterCookie, a tool used to establish persistent access on compromised systems. At least three organizations in the broader cryptocurrency space were targeted by PurpleBravo between October and November 2024: a market-making company, an online casino, and a software development company.

The findings also highlight North Korea's expansion into other areas of fraud, with the establishment of front companies that mimic legitimate IT firms. TAG-121, a separate cluster of activity, has been identified as operating a network of these companies across China. Each front company spoofs a different legitimate organization by copying large parts of their website. These entities create an added layer of deniability and make detection more challenging, allowing North Korean actors to further embed themselves in global IT supply chains.

The implications of this threat are far-reaching. Organizations that unknowingly hire North Korean IT workers may be in violation of international sanctions, exposing themselves to legal and financial repercussions. More critically, these workers almost certainly act as insider threats, stealing proprietary information, introducing backdoors, or facilitating larger cyber operations. Given North Korea's history of financial theft, the risks extend beyond individual companies to the broader global financial system and national security interests.

To mitigate these threats, organizations must adopt stringent identity verification measures, ensuring that remote hires undergo thorough screening. This includes requiring video interviews, notarized identification documents, and continuous monitoring of remote workers for anomalies. Employers should also implement technical controls to detect unauthorized access, restrict data exposure, and flag suspicious remote connections. Awareness and training for human resources (HR) teams and IT security personnel are essential in preventing these actors from infiltrating critical business operations.

While the threat posed by North Korean IT workers is a fraud issue, it is also a key component of a sophisticated cyber strategy that financially sustains an internationally sanctioned regime. As these operations continue to evolve, businesses, governments, and cybersecurity organizations must work together to close the gaps that enable North Korea to exploit the remote work environment.

Key Findings

- North Korea's use of IT workers to secure fraudulent employment and execute coordinated cyber campaigns highlights its evolving tactics to fund its military programs while undermining global intellectual property security.
- Insikt Group assesses that PurpleBravo has targeted at least seven entities, three of which are in the cryptocurrency sector, including a market-making firm, an online casino, and a software company.
- Insikt Group found evidence that PurpleBravo uses Astrill VPN to manage its command-and-control (C2) servers.
- PurpleBravo was found posting job advertisements on at least three hiring websites, Telegram, and GitHub.
- Insikt Group identified at least seven suspected North Korean-linked front companies operating in China spoofing legitimate IT firms in China, India, Pakistan, Ukraine, and the United States (US).
- Organizations should implement robust technical safeguards, such as, where feasible, disabling remote desktop software, conducting regular checks of open ports across networks, deploying insider threat monitoring, and geolocating devices.
- Insikt Group expects to continue to see groups like PurpleBravo and TAG-121 exploit the remote work environment, threatening global IT supply chains and intellectual property.
- North Korea's shift toward fraudulent remote employment and front companies will likely outpace traditional hiring protocol checks, driving organizations and governments to adopt more rigorous identity verification, enhanced remote work security, and robust international intelligence-sharing to counter this expanding threat.

Background

On January 23, 2025, the US Department of Justice (US DOJ) indicted two North Korean nationals and three facilitators for remote worker fraud that enriched the North Korean regime. In the indictment, the US DOJ described a six-year scheme in which two US citizens and one Mexican national conspired with North Korean IT workers to remotely work for at least 64 US companies. Payments from ten companies generated at least $866,255 in revenue that was laundered through a Chinese bank account. In addition to the indictment, stories of organizations and individuals that have come across North Korean IT workers can be regularly found in open sources (1, 2, 3). Besides sanctions violations, the threat from these workers, whether stealing sensitive data or installing malware on internal systems, presents unique challenges to organizations, especially in remote work environments.

North Korea remains highly isolated from the outside world due to the regime's strict control over goods, people, and information, as well as international sanctions placed upon the country. Despite this, Pyongyang's leadership is well-versed in exploiting emerging technologies to fund its operations. As sanctions have tightened, the regime adapted by escalating illicit activities, including smuggling and cybercrime. In recent years, the regime has achieved significant success in stealing from traditional financial institutions and digital assets like cryptocurrency. Between 2020 and 2024, the rise of remote work created new opportunities for North Korea to deploy skilled IT workers who infiltrate global companies under false identities. Their activities directly support the regime's military programs while posing a significant threat to industries reliant on intellectual property.

Research into North Korean IT workers has focused on the following aspects of the threat: North Korean IT workers gaining fraudulent employment through proxies; North Korean front companies, often in the software development space, imitating legitimate organizations; and fake employment opportunities targeting software developers in cryptocurrency and AI, among other industries. Other research has established links between IT workers and ongoing malicious campaigns by North Korean threat actors.

Threat Analysis

PurpleBravo

The Contagious Interview campaign, first documented in November 2023, targeted software developers primarily in the cryptocurrency space and was attributed to North Korea. The campaign used the JavaScript infostealer BeaverTail, the cross-platform Python backdoor InvisibleFerret, and most recently OtterCookie, a new backdoor identified in December 2024. The group responsible for this activity is known as CL-STA-0240, Famous Chollima, and Tenacious Pungsan in open sources. Insikt Group has given this cluster of activity the designation PurpleBravo (formerly TAG-120).

PurpleBravo's Fraudulent Profiles

On December 3, 2024, a developer posted a blog about their experience with a suspected PurpleBravo operator. An individual claiming to be a recruiter contacted them about a job offer and then followed up with an interview. During the interview, the interviewer asked the developer to download a coding challenge from a repository. The developer realized there was a malicious function in the file and ended the interview. While the developer does not attribute the malware or actor, Insikt Group assesses with high confidence the file is a BeaverTail infostealer.

The interviewer used a LinkedIn account with the name Javier Fiesco, who describes themself as the CTO of AgencyHill99. Further investigation into Javier Fiesco uncovered an individual with the same name available for work on remote3, a Web3 development job board. The website *agencyhill99[.]com* was registered on Hostinger on September 13, 2024. As of early February 2025, this website no longer resolved, but it previously displayed a Hostinger landing page. Research into AgencyHill99 uncovered a job posting seeking a developer with blockchain knowledge on *levels[.]fyi*, with the following contact info:

- Contact us: *alexander@agencyhill99[.]com*
- Recruiter: *vision.founder1004@gmail[.]com*

Pivoting on the text in the job description returned two private job postings on Upwork (1, 2). Additionally, a profile with the name of Lucifer, and what appears to be an AI-generated headshot, who works for AgencyHill99 was observed on the website DoraHacks, which is a hackathon, bounty, and grant organization. The profile on DoraHacks states that AgencyHill99 is looking to hire a developer. Insikt Group also discovered a company with the name Agencyhill99 on the website Intch, a part-time and remote job platform. The company posted a "Part-Time IT Developer Opportunity" by an individual with the name Newton Curtis, who is a recruiter at AgencyHill99.

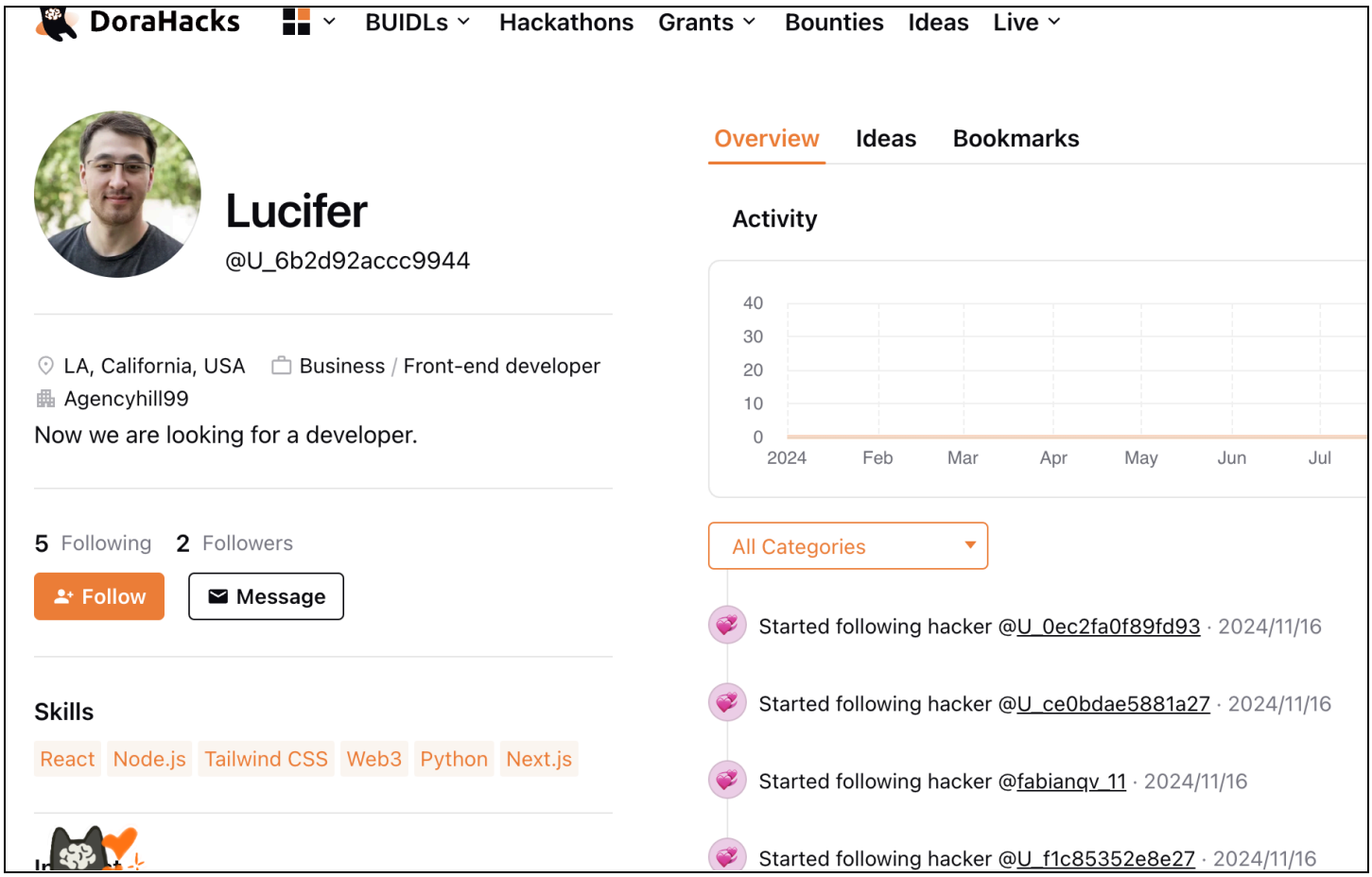


Figure 1: *PurpleBravo operator's account on DoraHacks (Source: DoraHacks)*

Insikt Group found several posts in Telegram channels from individuals with *@agencyhill99[.]com* email addresses advertising jobs. Below is a summary of the posts:

- On September 16, 2024, an account with the username Dale_V and email address *ayat@agencyhill99[.]com* posted in the Telegram channel "freelancerclients" that they were looking to hire a developer.
- On September 26, 2024, an account with the username jaxtonhol and email address *ysai@agencyhill99[.]com* posted in the Telegram channel "indeedemploijobeur" that they were looking to hire a developer. On the same day, the account Dale_V using the email *ysai@agencyhill99[.]com* posted in the Telegram channel "cryptolux_b" that they were looking to hire a blockchain developer. They posted the same message in the "itkita", "andexzuxiaomichat", and "usvacancy" channels. On September 27, 2024, Dale_V posted the same message in the "crypto_brazil" and "cryptolux_br" channels.
- On October 2, 2024, Dale_V posted the same message with a new email address, *sam@agencyhill99[.]com*, in the "fortifiedx_chat", "family_indonesia_uae_ph", "cryptolux_br", and "freelancerclients" channels.

- On October 3, 2024, a user in an Indonesian-language Telegram channel posted a screenshot of an email message they received from PurpleBravo operators.
- On October 9, 2024, Dale_V posted job advertisements in the "andexzuxiaomichat", "family_indonesia_uae_ph", "cryptolux_br", "crypto_brazil", and "freelancerclients" channels.
- On October 22, 2024, Dale_V posted in the Telegram channel "hiringofm" seeking individuals to help maintain a game called Destiny War, and added the X link, *hxxps://twitter[.]com/destinywarnft*. It is unclear if the actor controls this X account or game.
- On November 13, 2024, the Telegram user jaxtonhol posted in the Telegram channel "near_jobs" seeking blockchain engineers. The same user posted again on December 7, 2024, in the same channel with the email address *ysai@agencyhill99[.]com*.
- On November 30, 2024, a Telegram user posted asking if a job offer on LinkedIn from the account mentioned above, Javier Feisco associated with Agencyhill99, was legitimate and shared a screenshot of the message.

GitHub Repository

Insikt Group discovered a GitHub repository named agencyhill99 with the email address *admin@agencyhill99[.]com*. A GitHub user, dev-astro-star, made several commits to the repository between October 9 and 19, 2024. Based on the commits, it appears the website used Firebase, a Google backend service for web applications. The user added a button to download a file at the Google Drive link *https://drive.google[.]com/uc?id=166zcmpqj-C7NPltm4iwRolz8XuxqZIXt*, which is no longer accessible. The email address *admin@agencyhill99[.]com* was also added to the repository, along with the Telegram channel *hxxps://t[.]me/+2AurfGZWxZo0MDgx*, which is also no longer live. The user also added a download link to *hxxp://65.108.20[.]73/BattleTank[.]exe*, which is no longer live and was later updated to *hxxp://65.108.20[.]73[:]3000/BattleTank[.]exe*. Port 3000 was open from October 20, 2024, to November 22, 2024, on *65.108.20[.]73*. The link was then updated to *hxxp://locahost[:]3000/BattleTank[.]rar*.

PurpleBravo Malware and Infrastructure

PurpleBravo uses the malware families BeaverTail, InvisibleFerret, and OtterCookie. BeaverTail is a malware family initially distributed via NPM packages as a JavaScript payload and later as executables and downloaders targeting Windows and macOS environments. BeaverTail also acts as an infostealer, gathering cryptocurrency wallet and browser information. InvisibleFerret is a collection of post-compromise payloads that collectively act as a backdoor in victim environments. InvisibleFerret introduces additional malicious payloads into victim environments, performs information stealing and fingerprinting actions within the victim environment, and leverages legitimate protocols and software for C2 communications. Like InvisibleFerret, OtterCookie is a post-compromise malware family used as a backdoor, which establishes C2 connectivity via Socket[.]IO, receives and executes shell commands from C2 servers, and exfiltrates sensitive victim data.

Insikt Group analyzed BeaverTail, InvisibleFerret, and OtterCookie malware samples (See **Appendix B** for related file hashes). The BeaverTail samples were identified as PE variants targeting Windows

environments. These samples included URLs linked to *freeconference[.]com*, a legitimate conferencing website, which aligns with Unit42's findings of Contagious Interview payloads posing as FreeConference executables. The OtterCookie samples were two separate versions of the malware family; however, static analysis of these samples included strings that demonstrated both samples' ability to gather and send system fingerprinting information to attacker C2 servers, including strings that indicated OtterCookie is capable of identifying cryptocurrency assets and sensitive information found in specific file types by using regex patterns, including executables, photos, and config and env files, among others.

The InvisibleFerret samples analyzed were Python scripts with the following functionalities:

- Determining victim device location via local IP address lookup
- Fingerprinting device details (user and hostname)
- Connecting to a Base64-encoded C2 address via HTTP POST requests
- Performing local directory discovery using hard-coded strings
- Creating a reverse shell for SSH session management and data exfiltration
- Copying clipboard data, keylogging, and tracking mouse movements.

Previous samples of InvisibleFerret were analyzed by Zscaler, which described a two-part infection chain in which the initial reconnaissance took place over HTTP traffic and FTP was used for data exfiltration, as shown in **Figure 2**.

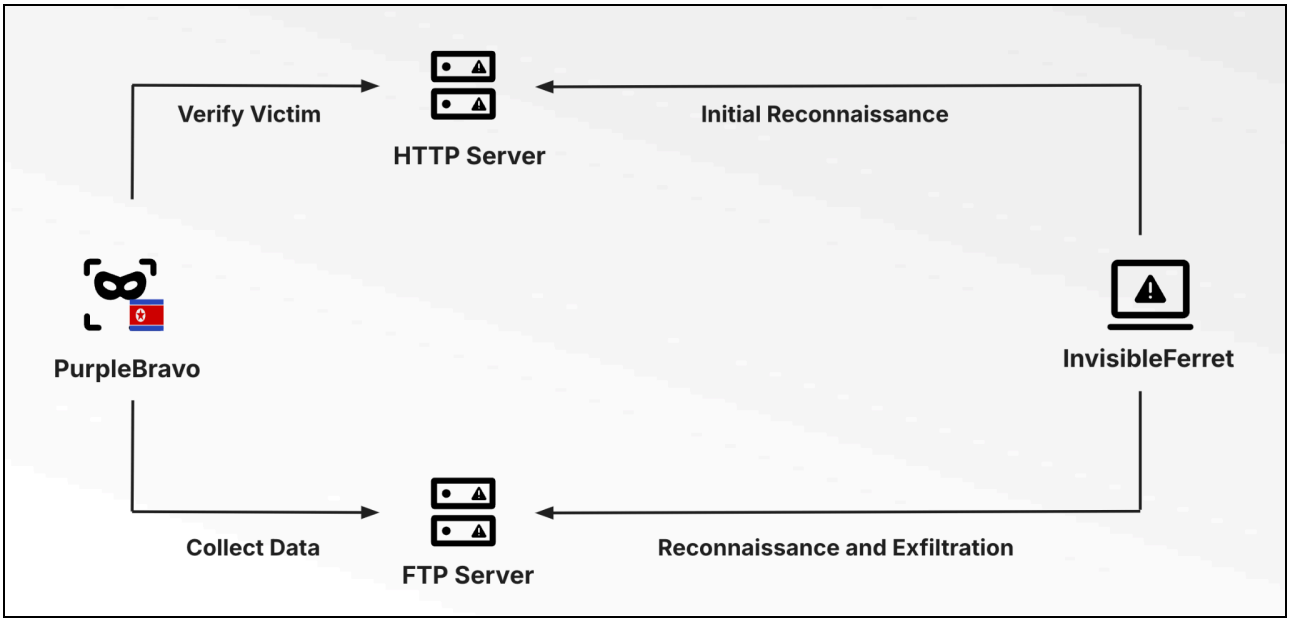


Figure 2: *InvisibleFerret Infection chain (Source: Recorded Future and Zscaler)*

Insikt Group identified 21 PurpleBravo servers between August 2024 and February 2025 (see **Appendix B** for the complete list). The majority of servers use Tier[.]Net hosting, with Majestic Hosting, Stark Industries, Leaseweb Singapore, and Kaopu Cloud HK also being used in this campaign. Insikt Group has previously observed other North Korean threat groups favor many of these hosting providers. In

addition to the C2 servers, using Recorded Future Network Intelligence, Insikt Group observed at least seven suspected victims between September 2024 and February 13, 2025. The victims are located in at least six countries, including the United Arab Emirates, Costa Rica, India, Vietnam, Türkiye, and South Korea. Open-source research identified Astrill VPN as a favored service by North Korean IT workers, with evidence that they use the service with remote administration tools. Insikt Group also observed network traffic between known Astrill VPN endpoints and PurpleBravo servers, corroborating this connection.

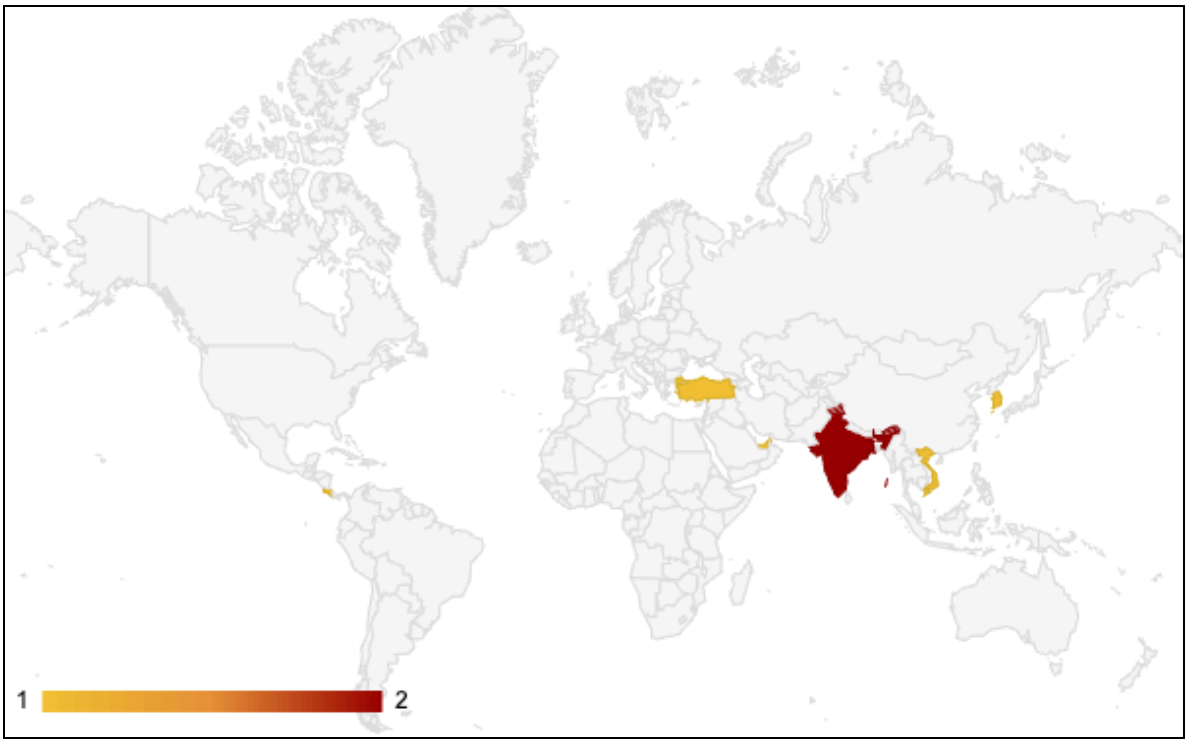


Figure 3: *Location of PurpleBravo victims (Source: Recorded Future)*

At least three victims in the cryptocurrency space were identified in the findings summarized below:

- On October 3, 2024, Insikt Group observed likely reconnaissance traffic between a BeaverTail C2 and a market-making company in the cryptocurrency space based in the United Arab Emirates. Shortly after the reconnaissance traffic, we observed likely exfiltration FTP traffic between the same IP addresses.
- On October 15, 2024, Insikt Group observed likely reconnaissance traffic between a BeaverTail C2 and a gambling company that offers online games and sells slot machines in the cryptocurrency space. The company is registered in Costa Rica. Reconnaissance traffic followed by FTP exfiltration traffic was observed between the C2 and the company's infrastructure on November 25 and 26, 2024.
- On October 2, 2024, Insikt Group observed potential FTP exfiltration traffic between a BeaverTail C2 and a software development company based in India that builds blockchain, AI, and mobile, among other applications.

TAG-121

On November 21, 2024, SentinelLabs published a report on North Korean front companies and their links to China. The report identified the company Shenyang Huguo Technology (*huguotechltd[.]com*) and assessed it to be a North Korean IT front company. Insikt Group investigated the company by pivoting on the hosting infrastructure and identified seven additional front companies imitating legitimate ones in the software engineering space. Insikt Group is unable to determine other links to North Korean operators, such as the listed owners of these organizations having links to North Korea, at this time. However, the overlapping infrastructure and characteristics of the front companies are consistent with North Korean operations. Insikt Group designates this cluster of activity as TAG-121.

The aforementioned front companies spoof software development organizations in China, India, Pakistan, Ukraine, and the US. All of the front companies copy most, if not all, of their websites from the legitimate organizations they are spoofing (See **Appendix D** for the full list of front company information). The front company domains are hosted on the Asia Web Service and Serverfield hosting providers (see **Appendix B** for IP addresses). Four of these front companies list their owners as Wang Peng (王鹏) and/or Zhou Baoyu (周宝玉). The companies are:

- Shenyang Pengzhou Trading (沈阳蓬舟贸易有限公司)
- Shenyang Di Di Technology LTD (沈阳蒂迪科技有限公司)
- Deep Sea Luc Co. Limited (深海露斯有限公司)
- Hi-solution E-commerce LTD (沈阳海萨露深电子商务有限公司)

The remaining three front companies — Shenyang Xiwang Technology (沈阳喜网科技有限公司), Hi-Devs E-commerce LTD (沈阳海萨露深电子商务有限公司), and Shenyang Wuxian Technology Co. (沈阳芜限科技有限公司) — list their owners as Sun Weiye, Huang Jingbin, and Zhou Zhenbang (周震邦), respectively. One of the front company websites can be seen in **Figure 4**. The front companies are all located in China, and the websites were registered between April 2022 and September 2024. Previous North Korean front companies have been located in China. Insikt Group is unable at this time to determine if the listed individuals are real people and assess the extent of business activities these front companies may have engaged in.

Figure 4: *Front company Shenyang Xiwang Technology's website (Source: urlscan)*

Mitigations

The following mitigation measures are compiled from multiple sources, including the US Internet Crime Complaint Center (IC3), the US Department of the Treasury (USDT), the government of the Republic of Korea (South Korea), and other cybersecurity experts. These steps are designed to help organizations and individuals protect themselves against North Korean IT worker scams.

Identity Verification

- Conduct thorough video interviews to verify a potential freelance worker's identity.
- Require notarized proof of identity and real ID cards during interviews.
- Implement identity verification processes during hiring, onboarding, and throughout employment.
- Verify all remote workers' identification information at E-Verify.gov.
- Check simple portfolio websites, social media profiles, or developer profiles for authenticity.

Background Checks and Due Diligence

- Conduct pre-employment background checks, including drug tests and fingerprint/biometric log-ins.
- Verify employment and education history directly with listed institutions.
- Check the consistency of personal details across all platforms and documents.
- Request documentation of background check processes from third-party staffing firms.
- Do not accept background check documentation from untrusted or unknown authorities.

Technical Measures

- Regularly use port-checking capabilities to detect remote access via desktop sharing or VPNs.
- Prevent remote desktop use on company devices.
- Install insider threat monitoring software on company devices.
- Regularly geolocate company laptops to verify they match employee login locations.
- Require freelancers to shut off commercial VPNs when accessing company networks.

Financial Precautions

- Avoid payments in virtual currency.
- Verify that banking information corresponds to other identifying documents.
- Request voided checks or certified documentation from financial institutions.
- Watch for unauthorized, small-scale transactions that may be fraudulent.
- Verify that check numbers and routing numbers match actual banks, not money service businesses.

Communication and Work Practices

- Be cautious of developers requesting communication outside the original freelance platform.
- Note inconsistencies in interviews, especially regarding an applicant's location or key details about their past.
- Be wary of unknown programmers offering small development fees while avoiding video interviews.
- Monitor for changes in addresses, particularly after hiring but before equipment delivery.
- Only send work-related equipment to addresses listed on identification documents.

Organizational Policies

- Implement zero trust and need-to-know policies.
- Avoid granting access to proprietary information when possible.
- Use only reputable online freelance platforms with robust identity verification measures.
- Educate HR staff, hiring managers, and development teams about this threat.
- Conduct security awareness training for employees, emphasizing social engineering tactics.

Additional Precautions for Individuals

- Remain cautious of random outreach on job-seeking sites for remote positions or account sharing.
- Be alert to job offers involving receipt of packages in exchange for proceeds.
- If you receive unexpected tax forms (such as a W-4 or 1099-NEC), contact the issuing business and the FBI.
- Consider placing a Self-Lock through E-Verify.gov to protect against employment-related identity fraud.

Outlook

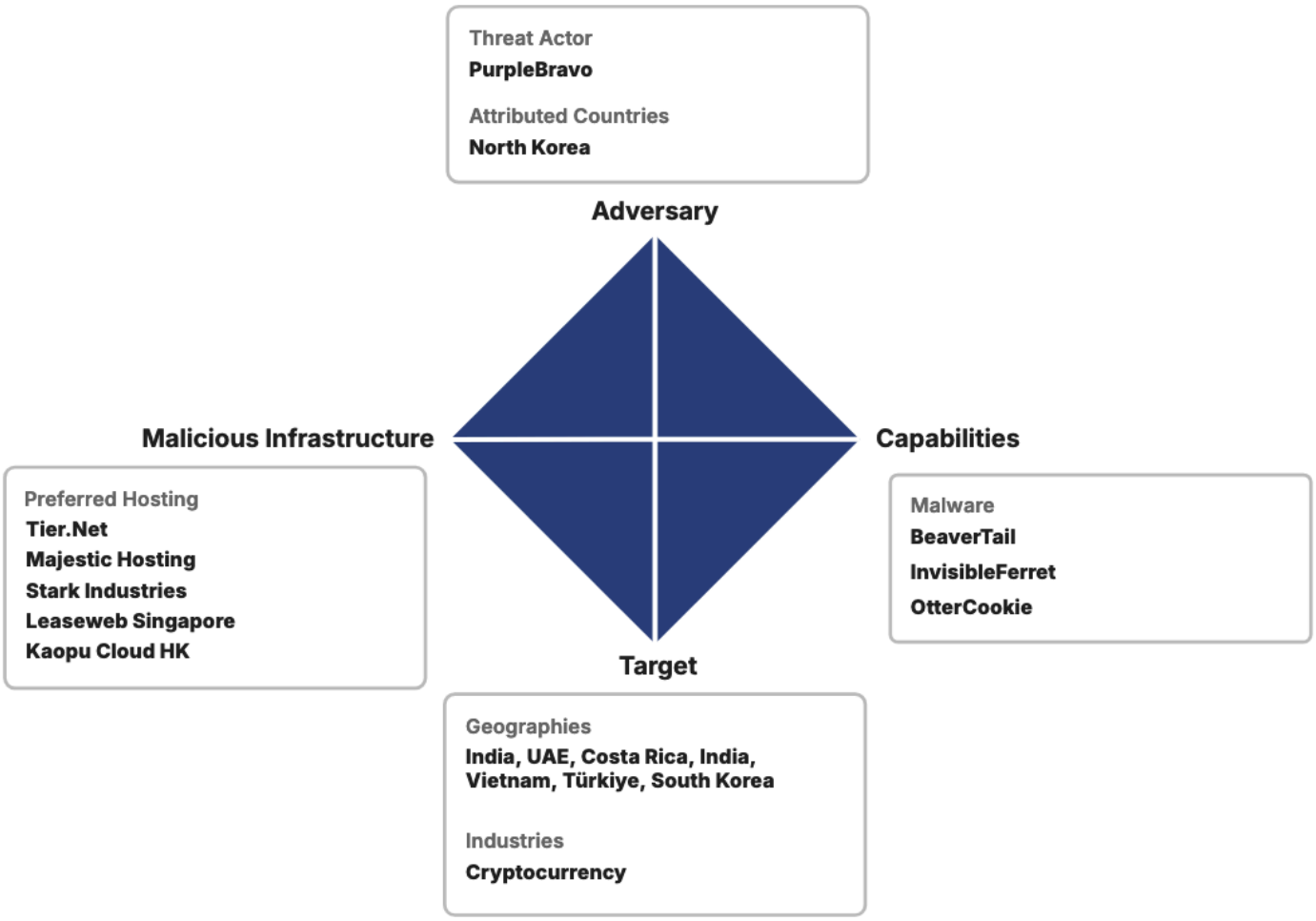
As international sanctions continue to tighten, North Korea has adapted by exploiting the rise of remote work, allowing its operatives to masquerade as legitimate IT professionals. These actors not only generate revenue for the state but, as seen in previous research, can also serve as strategic assets, facilitating cyberattacks and eroding trust, especially during a time of conflict. Companies across various industries — not just cryptocurrency, but also fintech, artificial intelligence, and even defense contracting — may find themselves at risk of infiltration. By embedding its operatives within global IT supply chains, North Korea can gain access to intellectual property, exfiltrate sensitive data, and establish persistent access within corporate networks.

The findings in this report highlight a sophisticated operation that spans multiple threat vectors, from the deployment of malware to the establishment of front companies designed to mimic legitimate IT firms. Looking ahead, North Korea's cyber operations are expected to grow in both scale and complexity. The tactics observed by both PurpleBravo and TAG-121 suggest that the regime will continue a multifaceted approach of seeking fraudulent remote employment, targeting developers in the cryptocurrency and tech industries, and establishing fraudulent companies as a means of generating revenue for the regime.

To counter this growing threat, organizations must adopt a more rigorous approach to identity verification and remote work security. Traditional hiring protocols are no longer sufficient in the face of adversaries leveraging sophisticated schemes. Governments and cybersecurity agencies must also enhance intelligence-sharing efforts and enforce stricter compliance measures on freelance hiring platforms.

As North Korea continues to exploit the vulnerabilities in remote work, businesses and government agencies must remain vigilant. The threat posed by North Korean IT workers extends beyond economic loss — it is a national security concern with far-reaching implications. Without coordinated efforts to close the gaps that enable these operations, North Korea's ability to penetrate global networks will only become more dangerous in the years ahead.

Appendix A: PurpleBravo Diamond Model



Appendix B: Indicators of Compromise

PurpleBravo Servers:
147[.]124[.]214[.]237
67[.]203[.]7[.]163
147[.]124[.]214[.]129
147[.]124[.]214[.]131
23[.]106[.]70[.]154
147[.]124[.]197[.]138
66[.]235[.]168[.]232
45[.]43[.]11[.]201
38[.]92[.]47[.]85
165[.]140[.]86[.]227
38[.]92[.]47[.]151
38[.]92[.]47[.]91
66[.]235[.]168[.]238
86[.]104[.]74[.]51
147[.]124[.]197[.]149
154[.]205[.]155[.]71
67[.]203[.]7[.]205
147[.]124[.]212[.]125
45[.]59[.]163[.]56
66[.]235[.]175[.]109
67[.]203[.]7[.]200

PurpleBravo Files:
4e0034e2bd5a30db795b73991ab659bda6781af2a52297ad61cae8e14bf05f79
7846a0a0aa90871f0503c430cc03488194ea7840196b3f7c9404e0a536dbb15e
0621d37818c35e2557fdd8a729e50ea662ba518df8ca61a44cc3add5c6deb3cd
d5c0b89e1dfbe9f5e5b2c3f745af895a36adf772f0b72a22052ae6dfa045cea6
07183a60ebcb02546c53e82d92da3ddcf447d7a1438496c4437ec06b4d9eb287
10f86be3e564f2e463e45420eb5f9fbdb14f7427eac665cd9cc7901efbc4cc59
cde5afd20b7bb5c9457b68e02c13094125025fb974df425020361303dc6fcdfc
d0a5b9dc988834cc930624661e6e7dd1943d480d75594fff0f4bc39d229c5999
8de446957ce96826628c88da9fd4e7ff9d6327d8004afc4e9e86d59e7d6948dc

TAG-121 Domains:
pengzhoutrading[.]com
xiwangtechltd[.]com
wuxiantechltd[.]com
diditechltd[.]com
deepsealuc[.]com
hisolution[.]io
hi-devs[.]com

TAG-121 Servers:
103.15.29[.]45
202.53.148[.]16
180.235.135[.]180
202.53.148[.]32
180.235.135[.]184
103.51.141[.]153
103.51.141[.]152

Appendix C: MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Initial Access: Spearphishing Attachment	T1566.001
Phishing: Spearphishing via Service	T1566.003
Command and Scripting Interpreter: Python	T1059.006
Command and Scripting Interpreter: JavaScript	T1059.007
System Information Discovery	T1082
Acquire Infrastructure: Domains	T1583.001
Acquire Infrastructure: Server	T1583.004
Credentials from Password Stores: Credentials from Web Browsers	T1555.003
User Execution: Malicious File	T1204.002
Obfuscated Files or Information: Encrypted/Encoded File	T1027.013
File and Directory Discovery	T1083
Archive Collected Data: Archive via Utility	T1560.001
Application Layer Protocol: Web Protocols	T1071.001
Application Layer Protocol: File Transfer Protocols	T1071.002
Data from Local System	T1005
Exfiltration Over C2 Channel	T1041

Appendix D: TAG-121 Front Companies

Shenyang Pengzhou Trading (沈阳蓬舟贸易有限公司)

- Observed at the domain *pengzhoutrading[.]com*
- Hosted at the IP address *103.15.29[.]45*
- Address: Room 133, No. 52, Liaohe Street, Huanggu, Shenyang, Liaoning 110087 China (辽宁省沈阳市皇姑区辽河街52号133)
- Owner listed as Wang Peng (王鹏)

Shenyang Xiwang Technology (沈阳喜网科技有限公司)

- Observed at the domain *xiwangtechltd[.]com*
- Hosted at the IP address *202.53.148[.]16*
- Address: Suqing Tower 4016-A024, Nujiang Street North NO.233-11, Huanggu District, Shenyang, Liaoning 110034
- Owner: Sun Wei Ye

Shenyang Wuxian Technology Co. (沈阳芜限科技有限公司)

- Observed at *wuxiantechltd[.]com*
- Hosted at the IP address *180.235.135[.]180*
- Address: 1-8-1, #40, North 2nd West Road 36, Tiexi, Shenyang, Liaoning 110020 China (辽宁省沈阳市铁西区北二西路36乙40号 [1-8-1])
- Owner: Zhen Bang (周震邦)
- Phone: +86 18842592573

Shenyang Di Di Technology LTD (沈阳蒂迪科技有限公司)

- Observed at *diditechltd[.]com*
- Hosted at the IP address *180.235.135[.]180*
- Address: Room NO.4016-A089, Suqing Tower, Nujiang Street North 233-11
- Huanggu District, Shenyang, Liaoning (辽宁省沈阳市皇姑区怒江北街233-11号苏青大厦4层4016室-A089)
- Owners: Wang Peng (王鹏), Zhou Baoyu (周宝玉)
- Phone: +86 17341011982

Deep Sea Luc Co. Limited (深海露斯有限公司)

- Observed at *deepsealuc[.]com*
- Hosted at the IP address *202.53.148[.]32*
- Address: Unit 1406B 14/F The Belgian Bank Building, Nos. 721 - 725 Nathan Road, Kowloon, Hong Kong
- Hong Kong Company Registry Information:
    - Business registration number: 75013353
    - Company registration number: 3248897
- Owner: Zhou Baoyu (周宝玉)

Hi-solution E-commerce LTD (沈阳海萨露深电子商务有限公司)

- Observed at *hisolution[.]io*
- Hosted at the IP address *180.235.135[.]184*
- Address: Xingshun Street no.92, Tiexi district, Shenyang, Liaoning, China
- Ownser: Zhou Baoyu (周宝玉)
- Email: hisolutions.soft@gmail[.]com

Hi-Devs E-commerce LTD (沈阳海萨露深电子商务有限公司)

- Observed at *hi-devs[.]com*
- Hosted at the IP addresses *103.51.141[.]153* and *103.51.141[.]15*
- Address Changbaisan Street No.169-3, Heping District, Shenyang, Liaoning province (辽宁省沈阳市沈阳市和平区长白三街169-3号 [1-3-3] 110057)
- Contact: Huang Jing Bin
- Phone: +86 17641562274

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering customers to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com