Global Companies Are Unknowingly Paying North Koreans: Here's How to Catch Them

By Evan Gordenker

Published: 2024-11-13 · Archived: 2026-04-05 12:53:51 UTC

Executive Summary

Workers with allegiances to the Democratic People's Republic of Korea (DPRK) have been infiltrating organizations worldwide through a fraudulent remote work scheme. This operation not only violates international sanctions but also poses cybersecurity risks to unwitting employers.

Drawing on publicly available information, including recent U.S. Department of Justice reports, Unit 42 has developed a guide for network defenders. While no single technique alone will detect these operatives, we propose a multi-faceted strategy that combines enhanced IT asset management, contextual analysis and strengthened security awareness.

Key to our recommendations is the implementation of a risk matrix tailored to each organization's specific environment. This matrix helps identify red flags, including the use of stolen identities, unusual work patterns and suspicious shipping addresses. We also stress the importance of rigorous background checks and the need for organizations to share information about suspicious activities.

With these strategies, organizations can strengthen their ability to detect and mitigate the risks posed by DPRK IT workers. While the threat is evolving, a proactive, informed approach can go a long way in preventing the exfiltration of sensitive data and inadvertent funding of North Korea's ambitions.

Palo Alto Networks customers are better protected from the threats discussed in this article through our Network Security platform, Prisma Access Browser offerings and Cortex line of products.

Organizations can engage the Unit 42 Incident Response team for specific assistance with this threat and others.

Introduction

A scheme orchestrated by the DPRK has been infiltrating companies worldwide, posing significant cybersecurity risks and violating international sanctions. DPRK IT workers, operating under the direction of their government, are securing remote positions with businesses across the globe.

These operatives pose as legitimate freelancers or applicants from various countries, generating substantial revenue that directly funds North Korea's weapons of mass destruction (WMD) programs. According to U.S. Department of Justice reports, individual IT workers can earn up to $300,000 annually. The North Korean government retains up to 90% of these earnings, which collectively totals hundreds of millions of dollars each year.

The tactics, techniques and procedures (TTPs) employed by these operatives include the following:

- Using stolen or synthetic identities
- Using falsified employment and identity documents
- Working with U.S.-based accomplices to create the appearance of domestic work locations
- Using virtual private networks (VPNs) to mask true geographic locations
- Manipulating employment verification processes
- Extorting employers [PDF] by threatening to publish sensitive information

This operation puts global companies at risk of data breaches, intellectual property theft and legal consequences. The scheme takes advantage of the heightened prevalence of remote work and the challenges in verifying digital identities.

Traditional insider threat programs are unlikely to fully address this state-sponsored activity. Organizations need an approach that combines identity verification, remote work security and insider risk management.

In this analysis, Unit 42 will provide:

- An examination of DPRK IT workers' TTPs
- Strategies for enhancing identity verification processes
- Detection methodologies for identifying anomalous behavior in remote work setups
- Guidance on improving organizational resilience against social engineering
- Practical solutions for strengthening defenses against this threat

Our objective is to equip cybersecurity professionals and organizations with detection and defensive strategies.

IT Worker's Toolbox

DPRK IT workers employ an array of tools and techniques to infiltrate organizations and generate revenue. Their toolkit is designed to create a disposable persona, establishing false identities and maintaining the appearance of a typical legitimate employee. If any one persona is burned, the DPRK IT workers can leverage a new one easily.

Identity Manipulation

The DPRK IT worker scheme begins with obtaining or fabricating identity documents.

- Use of genuine identities
  - Operatives build fraudulent identities using documents such as passports, driver's licenses and Social Security cards. Operatives may use legitimately issued documents obtained through identity theft or identity muling [PDF]. In other cases, they rely on forgeries of varying quality. (For observations of these behaviors, see page 5 of this September 2024 report [PDF] from the UK's Office of Financial Sanctions Implementation.)
- Synthetic/blended identities
  - When authentic documents are unavailable, DPRK IT workers create synthetic identities by combining real and fake information. This can include using AI-generated or AI-manipulated photos to create convincing profile pictures that withstand basic scrutiny, as shown in Figure 1.

Figure 1. An example of a stock photograph manipulated by DPRK IT workers. Source: KnowBe4.

Remote Access Tools

To maintain the illusion of being a local employee, operatives use remote desktop access software such as Chrome Remote Desktop, AnyDesk, Splashtop Streamer, TeamViewer and RustDesk.

Hardware devices like TinyPilot or PiKVM serve as physical keyboard, video or mouse (KVM) over internet protocol (IP) solutions, allowing operatives to remotely control computers as if they were physically present. These small devices connect directly to a computer's HDMI and USB ports, capturing video output and relaying user inputs. This hardware-based approach can bypass many software security measures and leave few traces.

Threat actors often abuse, take advantage of or subvert legitimate products for malicious purposes. This does not imply that the legitimate product is flawed or malicious.

Network Obfuscation Tools

To avoid detection, DPRK IT workers must conceal their true geographic location. VPNs, virtual private servers (VPSs) and proxy services mask the user's source IP address and encrypt internet traffic, making it appear as though the worker is connecting from an expected location.

The combination of remote desktop software and network obfuscation tools allows operatives to convincingly mimic the online behavior of an authentic remote worker.

Job Acquisition Tools

DPRK IT workers leverage popular freelancing and job search platforms to find potential targets. Operatives create accounts on popular job search websites, using their false identities to apply for positions. To support their cover stories, DPRK IT workers may create elaborate fake company websites. These sites lend credibility to their professional personas and can pass basic background checks.

To withstand video interviews, DPRK IT workers appear to prepare detailed responses and backstories to maintain consistency during job interviews. The quality of backstory varies, with some organizations reporting that operatives are unable to answer basic questions about their life outside of what they have presented in their resume.

Financial Tools

DPRK IT workers use a variety of financial services to monetize their activities. These include:

- Online payment platforms
  - DPRK IT workers use these platforms, which could have less stringent verification processes than traditional banks, for receiving payments and transferring funds
- Cryptocurrency
  - Bitcoin and other cryptocurrencies provide a level of anonymity and ease of cross-border transfers
- Money service transmitters
  - DPRK IT workers use online money transfer services to move funds between domestic and international accounts while maintaining an appearance of legitimacy

Supporting Infrastructure

To tie all these elements together, DPRK IT workers rely on both physical and virtual infrastructure:

- U.S.-based "laptop farms"
  - DPRK IT workers can gain assistance from accomplices based in the target locality who operate laptop farms. These accomplices receive corporate hardware on behalf of the DPRK IT workers and install the necessary tools to facilitate access.
- Mail forwarding services
  - DPRK IT workers use these services to establish mailing addresses for correspondence and receiving equipment
- Virtual phone numbers
  - DPRK IT workers use virtual phone numbers to get local phone numbers that they can answer from anywhere in the world.

Putting It Together

Based on publicly available information, a typical DPRK IT worker operation targeting a U.S. enterprise might unfold as follows:

An operative begins by establishing a false identity. They obtain the personal information of a U.S. citizen and create fraudulent documents, such as a driver's license, using the stolen information with the operative's photo substituted for the citizen’s.

Using this synthetic identity, the operative applies for remote IT positions at multiple U.S. companies through popular job search platforms. To maintain the illusion of being U.S.-based, they enlist a U.S. facilitator who agrees to receive and set up laptop computers, creating a laptop farm.

The facilitator receives company-issued laptops at their U.S. address and installs remote desktop applications on the device. This allows the operative to control the laptops from their actual location, often in China or Russia, while appearing to work from the U.S..

The operative secures employment with multiple companies, often at substantial salaries. They use VPNs and proxy services to mask their true IP address when connecting to the laptops. For video interviews and meetings, they may use prepared scripts or employ U.S.-based facilitators to participate on their behalf.

Companies pay fraudulently earned wages into U.S. bank accounts, which DPRK IT workers then move through various online payment platforms [PDF] and accounts, laundering the proceeds.

You Should Have a Risk Matrix

To counter the DPRK IT worker threat, organizations should develop a risk matrix tailored to their specific environment. This approach can detect potential operatives and enhance the overall security visibility of both internal and external threats.

DPRK IT workers employ diverse techniques, meaning there is unlikely to be any single mechanism for detection. Public records reveal a sophisticated and adaptable adversary. A risk matrix could chart the risk factor, its likelihood to occur in a DPRK IT worker matter, and the associated risk level to an organization if found in isolation.

One hypothetical risk matrix for an organization combating DPRK IT workers could be as follows:

Risk Factor	Likelihood	Risk Level
Use of stolen or synthetic identities	High	High
Unusual IP addresses or VPN usage	High	Low

Unauthorized remote desktop software usage	High	High
Inconsistencies in background checks	High	Medium
Abnormal work hours or productivity	High	Low
Heavy use of AI or translation software	High	Low
Logon from Russia or China, when a worker is supposedly based elsewhere	Medium	High
Use KVM over IP solutions like TinyPilot	Medium	High
Discrepancies in who appears in video calls	Medium	High
Use of U.S.-based facilitators (laptop farms; devices sent to individuals with no connection to job duties)	Medium	High
Unusual equipment shipping addresses	Medium	Medium
Attempts to access sensitive data outside job scope	Medium	High
Direct deposit to newer internet banking institutions	Medium	Low
Potential use of streaming software (to forward video/audio outputs through a remote machine)	Medium	Low
Use of cryptocurrency for payments	Low	Medium

IT Asset Management

Keeping accessible records of IT asset distribution helps defense staff and incident responders track anomalies, such as unexpected delivery locations or shipping forwarding services.

We recommend establishing protocols that flag the use of forwarding services and identifying when different employees have shipped multiple devices to the same address. By auditing the physical addresses associated with equipment shipments, organizations can add an additional layer of security to their network defense strategies.

We also recommend using endpoint security and endpoint management solutions for:

- Enforcing device compliance policies
- Managing and monitoring devices within the organization's network
- Ensuring that endpoints adhere to security best practices

These tools can provide a variety of useful functionalities:

- Offering insights into device health
- Detecting irregularities in application installations
- Remote isolation and wiping capabilities in case a device is compromised

Additionally, DPRK IT workers may leave crucial evidence in log sources often overlooked in log centralizing solutions, such as a security information and event management (SIEM) product. For example, Unit 42 recommends the ingestion of logs from:

- Video conferencing applications such as Zoom or Microsoft Teams, which insider risks could use from unmanaged devices like a personal laptop or cellphone.
- Customer relationship management SaaS solutions such as Salesforce, which can contain sensitive information prime for exfiltration by insiders.
- High volume clipboard or screenshot activity on a managed endpoint, which could indicate data harvesting activities by insiders.

Contextualizing IP Addresses

Scrutinizing anomalous IP addresses significantly bolsters a company's security stance. DPRK IT workers rely on VPN services that function well in China, such as Astrill VPN.

Companies can also employ Spur Intelligence Corporation's tools, including their free service at spur[.]us/app/context, which offers insights into IP addresses. This tool can identify a VPN exit node used by a DPRK IT worker, providing context for further investigation, as seen in Figure 2.

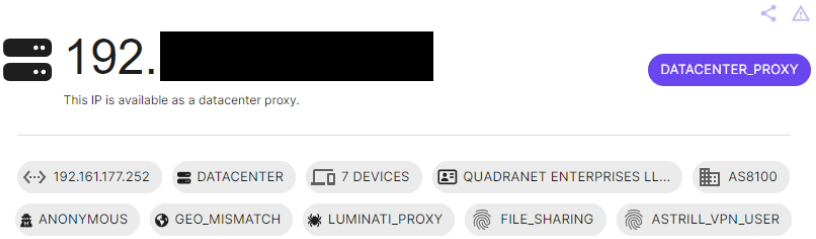

Figure 2. User interface elements of Spur's product Context, which provides context on a given IP address. This example illustrates an Astrill VPN exit node, a popular service in China, where many DPRK IT workers are based.

Spur continually updates its detections, which are available by API or client-side databases.

Strengthening the Human Firewall

The human element is a critical factor in the security breaches orchestrated by DPRK IT workers. These actors often exploit the inherent positivity bias—the tendency to overlook red flags in favor of a more favorable view of a person. Organizations must enhance their human firewall (i.e., the collective vigilance and security awareness of their staff).

Instill a culture of caution and responsibility. Security awareness training should be comprehensive, going beyond annual videos to actively engage employees in security practices. Train your staff to recognize and report anomalies, understanding that they play a critical role in the organization's security.

Organizations that employ remote tech workers, particularly in a contract capacity, should implement manager training focused on this threat and provide incident reporting channels.

Operational Security Measures

Operational security measures are also crucial. Enforce the principle of least privilege, ensuring that individuals have access only to the resources necessary for their job functions and no more. Regular reviews and audits of access privileges can prevent the accumulation of access rights that a DPRK IT worker might exploit.

Network segmentation is another effective strategy. By dividing the network into separate segments, organizations can contain and limit the movement of DPRK IT workers within their systems, reducing the reach of any potential compromise.

Moreover, organizations can employ monitoring strategies such as anomaly detection systems to spot not just DPRK IT workers, but other threats as well. If possible, the integration of advanced threat detection tools along with a defined incident response team can provide speedier containment.

Further, organizations should implement secure coding practices, regular security patches and updates along with endpoint protection, contributing to a robust security posture that can withstand attempts at infiltration. These activities can also help mitigate the damage done by DPRK IT workers.

Background Checks

We recommend organizations engage specialized firms that offer identity document verification services to mitigate the risks associated with manipulated identification documents. These firms are equipped with tools and expertise to detect inconsistencies and signs of tampering in documents that might not be evident to untrained personnel. Unit 42, working with Vcheck Global, has created a workflow specifically designed to combat worker identity fraud. Unit 42 can facilitate an introduction to interested parties. Identity verification is the single best opportunity for network defenders when tackling this threat before network intrusion.

Additionally, we recommend correlating worker IDs with liveness checks by their hiring manager, who can compare the ID provided during the background check with the individual on camera, as well as during the interview process.

Some organizations rely on staffing firms to manage identity verification and background checks, relying on a statement of completion from the providers. Organizations should not assume that a staffing firm's attestation guarantees identity verification. Independent verification or strict oversight of the staffing firm's procedures mitigates the risk of infiltration by malicious actors. This could include:

- Requiring that staffing agencies use a defined background check workflow
- Ensuring access to verification documents for audits
- Working with trusted agencies that prioritize due diligence and background investigations

Information Sharing

Unit 42 encourages organizations to proactively share information on suspicious employees or applicants with others. DPRK IT workers' resumes and social media profiles could provide clues to other potential victims.

We further encourage organizations to prioritize information sharing around known DPRK IT workers with the following types of organizations:

- Peer companies through Information Sharing and Analysis Center (ISAC) groups
- The applicable security teams of social media platforms and contract worker platforms

Finally, we believe organizations that report their incidents to law enforcement (particularly the FBI) could receive helpful guidance on containment.

Go Hunting

NGFW customers with Panorama can use the following dashboard to identify remote access users in their environment:

```
[{"viewID":"RMM and VPN","viewConfig":[[[{"xtypeConfig":"ACC_Application_Usage","localfilters":[{"name":"subcategory-of-app","value":"p
app","originalvalue":"proxy","negate":false,"display":"App Sub Category","logtype":"trsum"},{"name":"subcategory-of-app","value":"remote-acce
access","negate":false,"display":"App Sub Category","logtype":"trsum"},{"name":"subcategory-of-app","value":"encrypted-tunnel","originalname"
tunnel","negate":false,"display":"App Sub Category","logtype":"trsum"},
{"name":"app","value":"ssl","originalname":"app","originalvalue":"ssl","negate":true,"display":"Application","logtype":"trsum","vtype":"objectNar
[{"key":"bytes","val":[]}],"inlinelocalfilters":[]},{"xtypeConfig":"ACC_Sources","localfilters":[{"name":"subcategory-of-app","value":"proxy","ori
app","originalvalue":"proxy","negate":false,"display":"App Sub Category","logtype":"trsum"},{"name":"subcategory-of-app","value":"remote-acce
access","negate":false,"display":"App Sub Category","logtype":"trsum"},{"name":"subcategory-of-app","value":"encrypted-tunnel","originalname"
tunnel","negate":false,"display":"App Sub Category","logtype":"trsum"},
{"name":"app","value":"ssl","originalname":"app","originalvalue":"ssl","negate":true,"display":"Application","logtype":"trsum","vtype":"objectNar
{"xtypeConfig":"ACC_Decryption_Traffic_Activity","localfilters":[]}],[{"xtypeConfig":"ACC_Rule_Usage","localfilters":[{"name":"subcategory-
app","originalvalue":"proxy","negate":false,"display":"App Sub Category","logtype":"trsum"},{"name":"subcategory-of-app","value":"remote-acce
access","negate":false,"display":"App Sub Category","logtype":"trsum"},{"name":"subcategory-of-app","value":"encrypted-tunnel","originalname"
tunnel","negate":false,"display":"App Sub Category","logtype":"trsum"},
{"name":"app","value":"ssl","originalname":"app","originalvalue":"ssl","negate":true,"display":"Application","logtype":"trsum","vtype":"objectNar
{"xtypeConfig":"ACC_Destinations","localfilters":[{"name":"subcategory-of-app","value":"proxy","originalname":"subcategory-of-app","originalv
Category","logtype":"trsum"},{"name":"subcategory-of-app","value":"remote-access","originalname":"subcategory-of-app","originalvalue":"remote
{"name":"subcategory-of-app","value":"encrypted-tunnel","originalname":"subcategory-of-app","originalvalue":"encrypted-tunnel","negate":false,"
{"name":"app","value":"ssl","originalname":"app","originalvalue":"ssl","negate":true,"display":"Application","logtype":"trsum","vtype":"objectNar
{"xtypeConfig":"ACC_Dest_Regions","localfilters":[{"name":"subcategory-of-app","value":"proxy","originalname":"subcategory-of-app","original
Category","logtype":"trsum"},{"name":"subcategory-of-app","value":"remote-access","originalname":"subcategory-of-app","originalvalue":"remote
{"name":"subcategory-of-app","value":"encrypted-tunnel","originalname":"subcategory-of-app","originalvalue":"encrypted-tunnel","negate":false,"
{"name":"app","value":"ssl","originalname":"app","originalvalue":"ssl","negate":true,"display":"Application","logtype":"trsum","vtype":"objectNar
[]}]]]}]
```

Cortex XDR customers can use the following query to hunt for executions of certain remote monitoring and management (RMM) tools in their environment over the past 30 days:

```
// Name: RMM Sweep
// Purpose: Detect and analyze RMM tools in environment
// Configuration: Turn off case sensitivity, set timeframe to last 30 days (adjustable)
config case_sensitive = false timeframe = 30D
// Dataset
| dataset = xdr_data
// Filter for various remote execution clients
| filter event_type = PROCESS and event_sub_type = PROCESS_START and (
// AnyDesk
lowercase(action_process_image_name) ~= "anydesk.*[.]exe|anydesk" or
lowercase(action_file_path) contains "anydesk" or
// Action1
```

```
lowercase(action_process_image_name) ~= "action1|action1.*[.]exe" or
lowercase(action_file_path) contains "action1" or
// Atera
lowercase(action_process_image_name) ~= "ateraagent|ateraagent.exe" or
lowercase(action_file_path) contains "atera agent" or
action_process_signature_vendor = "Atera Networks" or
// ConnectWise
action_process_signature_vendor in ("ConnectWise, LLC", "ConnectWise, Inc.") or
// Google Chrome Remote Desktop
lowercase(action_process_image_name) ~= "remoting.*host[.]exe|remoting_host.*" or
(lowercase(action_process_image_path) contains "appdata\\google\\chrome\\extensions" and
lowercase(action_process_image_command_line) ~=
"inomeogfingihgjfjlpeplalcfajhgai|gbchcmhmhahfdphkhkmpfmihenigjmpp") or
// FleetDeck
action_process_signature_vendor = "FleetDeck Inc" or
lowercase(action_process_image_name) contains "fleetdeck" or
// Level.io
lowercase(action_process_image_name) ~= "level[.]io.*[.]exe|level[.]io" or
// MeshCentral
lowercase(action_process_image_name) contains "meshagent" or
// NetSupport Manager
lowercase(action_process_image_path) contains "netsupport manager" or
lowercase(action_file_path) contains "netsupport manager" or
lowercase(action_process_image_name) in ("pcilic.exe", "pcideply.exe") or
// Quick Assist
lowercase(action_process_image_name) ~= "quick assist|quickassist.exe" or
lowercase(action_file_path) contains "quick assist" or
// RustDesk
lowercase(action_process_image_name) ~= "rustdesk|rustdesk.exe" or
lowercase(action_file_path) contains "rustdesk" or
// SimpleHelp
lowercase(action_process_image_name) contains "simpplehelp.exe" or
lowercase(action_process_signature_vendor) contains "simplehelp ltd" or
lowercase(action_file_path) contains "simplehelp" or
// Splashtop
lowercase(action_process_image_name) contains "srservice.exe" or
lowercase(action_process_signature_vendor) contains "splashtop inc" or
lowercase(action_file_path) contains "splashtop" or
// TeamViewer
lowercase(action_process_image_name) in ("teamviewer", "tv_w32.exe") or
```

```
(lowercase(action_process_image_name) = "mshta.exe" and lowercase(action_process_image_command_line) contains "teamviewer") or
// VS Code Developer Tunnel
lowercase(action_process_image_command_line) ~= "vscode[.]dev\\tunnel|code tunnel.*" or
lowercase(action_file_path) contains "microsoft vs code" or
(lowercase(action_process_image_name) = "code.exe" and lowercase(action_process_image_command_line) contains "code tunnel")
)
// Label detected RMM tools
| alter Note = if(
lowercase(action_process_image_name) = "mshta.exe", "TeamViewer",
lowercase(action_process_image_name) contains "fleetdeck", "Fleetdeck",
lowercase(action_process_image_name) contains "anydesk", "AnyDesk",
lowercase(action_process_image_name) contains "action1", "Action1",
lowercase(action_process_image_name) contains "ateraagent", "Atera Agent",
lowercase(action_process_image_name) contains "level.io", "Level.io",
lowercase(action_process_image_name) contains "quickassist", "Quick Assist",
lowercase(action_process_image_name) contains "meshagent", "MeshCentral Agent",
lowercase(action_process_image_path) contains "netsupport manager", "NetSupport Manager",
lowercase(action_process_image_name) in ("pcideply.exe", "client32.exe"), "NetSupport Manager",
lowercase(action_process_image_name) ~= "remoting.*host[.]exe|remoting_host.*", "Google Chrome Remote Desktop",
lowercase(action_process_signature_vendor) contains "splashtop", "Splashtop",
lowercase(action_process_image_name) contains "rustdesk", "Rust Remote Desktop",
lowercase(action_file_path) contains "microsoft vs code", "VS Code Developer Tunnel",
lowercase(action_process_image_name) contains "tv_w32.exe", "TeamViewer",
action_process_signature_vendor in ("ConnectWise, LLC", "ConnectWise, Inc."), "ConnectWise",
action_process_signature_vendor = "FleetDeck Inc", "FleetDeck",
action_process_signature_vendor = "SimpleHelp Ltd", "Simple Help",
action_process_signature_vendor = "NetSupport Ltd", "NetSupport Manager",
action_process_signature_vendor = "Zhou Huabing", "Rust Remote Desktop",
lowercase(action_process_image_name) contains "teamviewer", "TeamViewer",
"Unknown RMM Tool"
)
// Aggregate results, count occurrences and display most recent execution time
| comp count() as runCount, max(_time) as lastTime by agent_hostname, action_process_image_command_line, action_process_username, action_process_image_name, action_process_image_path, action_process_image_sha256, Note
// Return fields of interest
| fields agent_hostname, action_process_image_command_line, action_process_username, action_process_image_name, action_process_image_path, action_process_image_sha256, runCount, lastTime, Note
```

```
// Sort results by hostname and run count
| sort desc runCount
```

169	
170	
171	
172	
173	
174	
175	

Conclusion

The threat posed by DPRK IT workers represents a challenge for organizations. These state-sponsored actors have demonstrated adaptability and resourcefulness in their efforts to infiltrate companies, generate revenue for North Korea's weapons programs, and potentially exfiltrate sensitive information.

Our analysis reveals a sophisticated operation that exploits the architecture of human resources operations. The operation leverages a combination of identity fraud, technological tools and social engineering to compromise organizations.

While no single measure can guarantee protection against this threat, a layered defense strategy significantly improves an organization's ability to detect and mitigate against DPRK IT workers and a variety of similar threats. Regular audits, continuous monitoring and staying informed about evolving TTPs will help in maintaining an effective security posture.

As DPRK IT workers continue to refine their methods, the global cybersecurity community must remain vigilant and adaptive. By implementing the strategies outlined in this analysis and fostering collaboration between private sector entities and law enforcement agencies, we can work toward disrupting this revenue stream and protecting sensitive assets.

Palo Alto Networks customers can better protect against the threats discussed above through the following products:

- Cortex XDR can be configured to block and hunt for the tool sets discussed in this article.
- Organizations can leverage next-generation firewalls to identify and block access vectors for DPRK IT workers. In environments with outbound SSL decryption enabled, more granular App-ID based policies can be implemented.
- Prisma Access Browser can be configured to block logins from devices with active remote access sessions, preventing access to sensitive browser-based data in managed or unmanaged environments.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Additional Resources

- Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of DPRK Threat Actors – Unit 42, Palo Alto Networks
- Advisory on North Korean IT Workers [PDF] – U.K. Office of Financial Sanctions Implementation
- Final Report of the Panel of Experts Assisting the 1718 DPRK Sanctions Committee [PDF] – Security Council Report, United Nations
- Justice Department Disrupts DPRK Remote IT worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator – Press release, U.S. Department of Justice
- Democratic People's Republic of Korea Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue – Public Service Announcement, Federal Bureau of Investigation
- Justice Department Announces Arrest, Premises Search, and Seizures of Multiple Website Domains to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea – Press release, U.S. Department of Justice
- Justice Department Announces Court-Authorized Action to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea Information Technology Workers – Press release, U.S. Department of Justice
- Justice Department Announces Court-Authorized Action to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea Information Technology Workers – Press release, U.S. Department of Justice, Office of Public Affairs

- Publication of North Korea Information Technology Workers Advisory – U.S. Department of the Treasury, Office of Foreign Assets Control
- Assessed Cyber Structure and Alignments of North Korea in 2023 – Mandiant
- Treasury Targets DPRK Malicious Cyber and Illicit IT worker Activities – Press release, U.S. Department of the Treasury
- Updated Guidance on the Democratic People's Republic of Korea Information Technology Workers – Press release, U.S. Department of State
- Response to DPRK cyber threats – Various government agencies from the Republic of Korea (South Korea)
- Thousands of remote IT workers sent wages to North Korea to help fund weapons program, FBI says – AP News
- For DPRKs in China, Seeking Freedom Is More Perilous Than Ever – New York Times
- The Incredible Rise of North Korea's Hacking Army – The New Yorker
- We found DPRK engineers in our application pile. Here's what our ex-CIA co founders did about it. – Cinder
- How a DPRK Fake IT Worker Tried to Infiltrate Us – KnowBe4

Table of Contents

Related Articles

- Boggy Serpens Threat Assessment
- Suspected China-Based Espionage Operation Against Military Targets in Southeast Asia
- Introducing Unit 42's Attribution Framework