

Hangro: Investigating North Korean VPN Infrastructure

Part 1

 nkinternet.wordpress.com/2025/01/06/hangro-north-korean-vpn-infrastructure/

nick

January 6, 2025

In a post from a now-deleted user on the webdev subreddit, someone asked about how to acquire a .kp TLD. While there were a few decent responses, the original poster shared an update: they successfully obtained a domain but noted that a VPN is required to access the website. This raised intriguing questions about VPN usage in North Korea.

While several VPN providers claim to operate from North Korea, most merely offer false IP geolocation. However, the poster provided the domain they acquired: hani.star-co.net.kp. This sparked an investigation into what might be legitimate North Korean VPN infrastructure.

↑ [-] [deleted] • 2 points 1 year ago
↓ well its running good and somany people use it
also im implement a exchange service for foriegn currencies
if you want kp domain you must go to nk embassy in your country and send request to country. it takes a few weeks but its worth it
heres my domain (you need north korean ip to enter it so use vpn)
hani.star-co.net.kp
[permalink](#) [embed](#) [save](#) [parent](#) [report](#) [reply](#)

Is Hangro a VPN?

North Korea's tightly controlled internet environment relies on specific tools for access. One such tool is the software NetKey, which authenticates users inside the country for internet access. However, it appears there is another program, Hangro, which may potentially function as a VPN for users outside the country. Let's dig into the infrastructure a little more

Hangro's IP Infrastructure

Historically, four IP addresses supported Hangro's operations. These included two IPs located in North Korea and two in Russia. These IPs shared certificates on port 3225 and also had port 8888 open:

- 175.45.176.21
- 175.45.176.22
- 188.43.136.115
- 188.43.136.116

Until November 1, 2024, these IPs displayed the following certificate information on port 3225:

- **Subject:** CN=hangro.net.kp
- **Issuer:** CN=hrira2024
- **Names:** hangro.net.kp

Additionally, the IP **175.45.176.32** matched this certificate data.

Despite these technical similarities, the exact purpose of these IPs remains unclear. Further investigation of the domain **hangro.net** on archive.org reveals a 2012 snapshot of a remote access page written in Korean:



Screenshot of hangro.net from 2012.

<https://web.archive.org/web/20121231174908/http://www.hangro.net:80/user/login.php>

This domain was apparently used for some kind of remote access and is similar to a current North Korean TLD but there's still more that can be investigated to tie this to North Korea as well as how it is used for remote access.

Whois Records and DPRK Connections

Luckily whois data from that time reveals who had registered hangro.net:

- **Registrar:** XIN NET TECHNOLOGY CORPORATION
- **Registrant:** Jo Myong Chol
- **Address:** "District Heping, Road Wenhua, No 17 4-24-1," Shenyangshi, Liaoningsheng, China
- **Email:** support@silibank.com

Jo Myong Chol is listed as a North Korean national in [OpenSanctions](#). The email address support@silibank.com was also used to register other DPRK-affiliated websites, including:

- ournation-school.com
- uriminzogkiri.com

This strongly ties Hangro's infrastructure to North Korea. The use of silibank.com—a domain associated with other DPRK-related websites—suggests a coordinated effort to manage internet resources and infrastructure tied to state activities. Furthermore, the Shenyang address and registrant details align with known patterns of North Korean operations abroad, further solidifying its connection to the regime's broader internet strategy.

Silibank and Hangro Software

At this point we can conclude that all of this is related to North Korea but it still doesn't answer the question about what hangro.net.kp is used for. However, back in 2014 archive.org also captured the following page for silibank.com

Index of /

[ICO]	Name	Last modified	Size	Description
[DIR]	fog/	2014-09-23 03:05	-	
[DIR]	moranbong/	2014-09-23 03:05	-	

Apache/2.4.10 (Win32) OpenSSL/1.0.1i PHP/5.5.15 Server at silibank.com Port 80

<https://web.archive.org/web/20141218100818/http://silibank.com/>

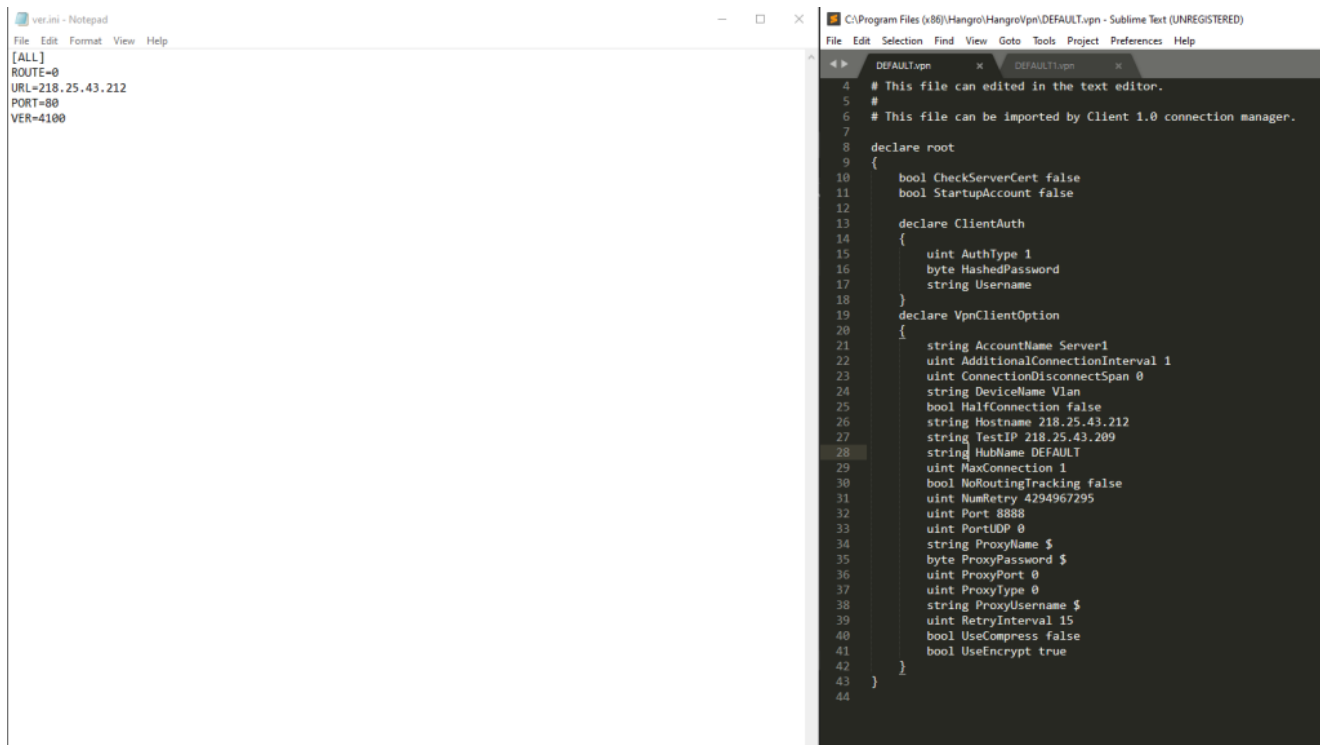
While archive.org doesn't have a copy of the files, VirusTotal provides us a list of files in the fog directory

```
http://silibank.com/fog/update_files/  
http://silibank.com/fog/update_files/HangroMessenger.exe  
http://silibank.com/fog/update_files/HangroDi_x64.exe  
http://silibank.com/fog/update_files/HangroVPN.exe
```

Side note if anyone knows what moranbong is or has a copy of the files feel free to reach out.

What is Hangro Used For?

Judging by the name it's probably a VPN client that was downloaded from silibank.com. While the file on VirusTotal may be an older file I was able to find what I think is a newer version of Hangro. The interesting thing is that it came with a default config in place that is designed to connect back to 218.25.43.212 on port 8888



```
[ALL]
ROUTE=0
URL=218.25.43.212
PORT=80
VER=4100
```

```
{
  # This file can edited in the text editor.
  #
  # This file can be imported by Client 1.0 connection manager.

  declare root
  {
    bool CheckServerCert false
    bool StartupAccount false

    declare ClientAuth
    {
      uint AuthType 1
      byte HashedPassword
      string Username
    }

    declare VpnClientOption
    {
      string AccountName Server1
      uint AdditionalConnectionInterval 1
      uint ConnectionDisconnectSpan 0
      string DeviceName Vlan
      bool HalfConnection false
      string Hostname 218.25.43.212
      string TestIP 218.25.43.209
      string HubName DEFAULT
      uint MaxConnection 1
      bool NoRoutingTracking false
      uint NumRetry 4294967295
      uint Port 8888
      uint PortUDP 0
      string ProxyName $
      byte ProxyPassword $
      uint ProxyPort 0
      uint ProxyType 0
      string ProxyUsername $
      uint RetryInterval 15
      bool UseCompress false
      bool UseEncrypt true
    }
  }
}
```

Pulling some additional details for that IP reveals an abuse contact email of postmaster@silibank.com

Summary

ASN	AS4837 - CHINA UNICOM China169 Backbone
Hostname	No Hostname
Range	218.25.0.0/16
Company	Liaoning Clear channel data Communication, Inc
Hosted domains	0
Privacy	⊗ False
Anycast	⊗ False
ASN type	ISP
Abuse contact	postmaster@silibank.com

What does this all mean? It seems to be some infrastructure used for possibly connecting back to the Kwangmyong potentially. There's not a lot of information available online about the Hangro software. So far the only thing that I've been able to find is this article from rfa.org that claims the following:

"The newly developed computer startup program detects the internet connection status in real time and opens a channel to use only North Korean e-mail. You can download instructions from Pyongyang, and access lecture materials and study materials only through North Korean e-mail," the second source said.

"The software, called 'Hangro,' disables external emails from China and the rest of the world. It has become the only email channel where messages can be exchanged between the North Korean authorities and the company," said the second source.

"North Korean trading companies must pay \$350 to the Shenyang consulate to use Hangro," the second source said.

https://www.rfa.org/english/news/korea/smartphone_surveillance-09202022164642.html

Looking Ahead: Part 2 Preview

While the article mentions it is used for just email, some brief investigation of the software reveals that there may be more to it. Part 2 of this series will have additional details about the software. Further, it appears that North Korea is using infrastructure outside of it's typical ASN. Doing some quick digging into the 188 addresses shows the following ranges in the RIPE database as being related to the 188 IP addresses.

Resources

by Resources, Sponsored Resources

RIPE Database

Query Database

Full Text Search

Syncupdates

Create an Object

Documentation

Feedback/Support

RIPE Database Text Search

This service allows searches over the full text of the RIPE Database. The search is done on object text without regard for object type.

KPOST-NET

☐ Advanced Search

By submitting this form you explicitly express your agreement to the [Terms and Conditions](#) of the RIPE Database.

Search results

This is the RIPE Database full text search service. The RIPE Database is subject to [Terms and Conditions](#).

Number of results - all object types

inetnum

inetnum: 188.43.88.0 -188.43.88.255

netname=KPOST-NET

inetnum: 80.237.84.0 -80.237.84.255

netname=KPOST-NET

inetnum: 188.43.136.0 -188.43.136.255

netname=KPOST-NET2

Indicators mentioned in this post are below. If you have any additional details about Hangro please reach out contact@dprkinternetwatch.com

Indicators:

- 175.45.176.21
- 175.45.176.22
- 175.45.176.32
- 188.43.136.115
- 188.43.136.116
- 218.25.43.212
- hangro.net.kp
- hangro.net
- silibank.com
- ournation-school.com
- uriminzogkiri.com
- support@silibank.com
- postmaster@silibank.com

Discover more from North Korean Internet

Subscribe to get the latest posts sent to your email.