Attendance Form:

Red Star OS
A Deep Dive into North Korea's Operating System

Version History

- First started development in 1998
- Previously used Red Hat and modified Windows
- Red Star has had 4 releases
  - 1.0 (2008?)
  - 2.0 (2009)
  - 3.0 (2012)
  - 4.0 (2019)

PROGRAM

Local Linux system upgraded

Red Star 4.0 server operating system has recently been developed.

The developers established Red Star in accordance with the liking and emotion of Koreans and has improved the OS by making the most of the fertile features, performances and security elements of Linux.

According to server managers, Red Star 4.0 offers several service setting tools to make it convenient to manage and maintain the server.

The OS is compatible with computers equipped with UEFI function and mass-storage devices and its bonding for increasing network throughput has been improved remarkably.

The developers have applied migration which keeps the network and service configurations of the previous version, thereby reducing the time for configuring the server during installation. And they have added more than thirty system and service daemon management tools such as tools for boot configuration, disk management and integrity monitoring, in order to make the server management much easier than other Linux-based server OSs.

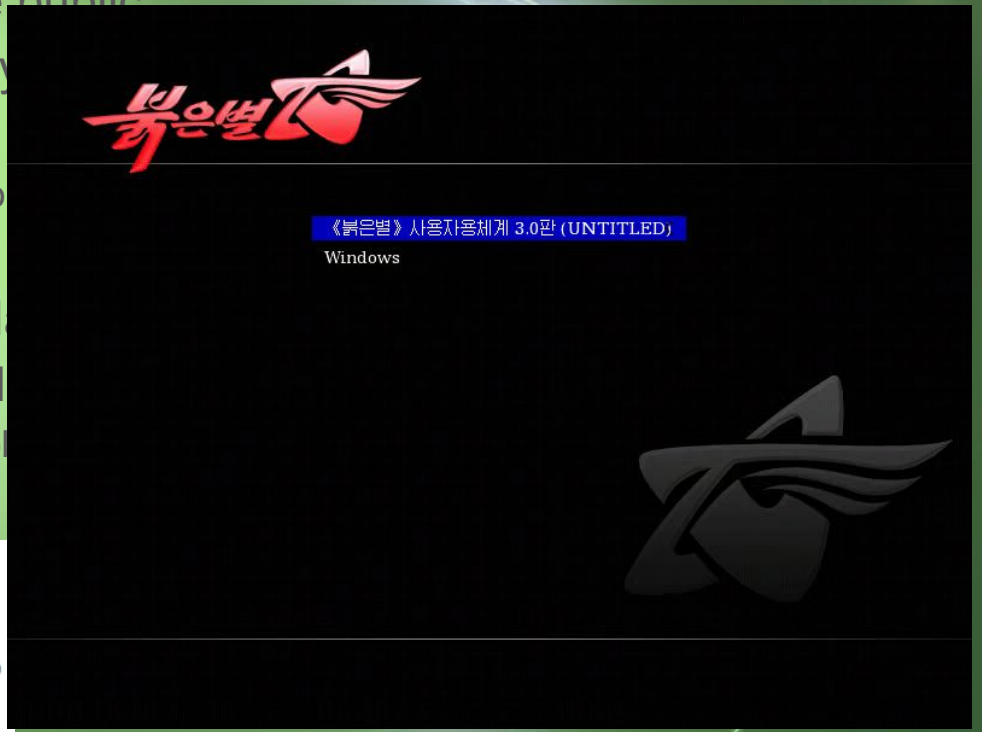
Red Star 4.0 was highly appreciated at the 29th national exhibition of IT achievements.

By **Kim Kum Myong** *PT*

Why’d they make this?

What's the deal with this OS anyways

- Not quite as commonly used by the public
- Thought to be used more commonly
  settings
  - A server version of the OS does exist fo
- Built off of Fedora 11/15 and KDE
- Version 3.0 is heavily inspired by M
- 3.0 first thought to be leaked by red
  - Comes with a variety of preinstalled tool
- It also includes lots of spyware




```
< HTTP/1.1 302 Found
< Date: Sat, 10 Oct 2015 21:22:00 GMT
< Server: Apache/2.2.15 (RedStar 3.0)
< Set-Cookie: PHPSESSID=2rt[redacted]; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Location: http://175.45.176.73/CBC/
< Content-Length: 0
< Content-Type: text/html; charset=UTF-8
```

Demo Time!

What about the “internet”?

What about the “Internet”

- Select North Koreans have filtered public internet access
  - Often government officials or people involved in higher education
- More freely available is North Korea’s Intranet (Kwangmyong)
  - 10.0.0.0/8 Private network
  - Estimated to be several thousand sites in total
  - There are places that citizens can request foreign articles to be made accessible within the intranet
  - Four public IPv4 /24 Subnets 175.45.176-179.0/24
  - They have their own local DNS service, however it hasn’t always been around
  - Within their custom DNS system they have their own TLD’s not registered with ICANN
  - Most citizens still use the IP addresses because it’s easier to understand than the english text
  - DHCP doesn’t really exist they had to enter their own gateway to proxy traffic through

Spyware? Custom Firmware?

- Custom kernel modules like rtscan, pilsung, kdm, and kimm
- System Hardening?
  - Iptables config, Selinux, intcheck, securityd
- Rtscan.ko
  - Protects files & processes
  - Hides files - makes them unreadable
- Antivirus (SCNPRC)
- Watermarking System (opprc)
  - USB devices that are plugged into the system will have a watermark appended to all the media files with a hash of the Hard Drive's serial number. Theoretically allowing for illegal media to be traced by authorities

Some Honerable Mentions

- Astra Linux - Russia
- Gendbuntu - France
- Canaima - Venezuelan
- LiMux - Munich
- Nova - Cuba
- Red Flag - China

ASTRA LINUX®

CANAIMA
DISTRIBUCIÓN GNU/LINUX

LiMux
Die IT-Evolution

红旗®
Linux

NOVA

Any Questions?