A Strange Tour of North Korea: Red Star OS

By LambdaCalculus
for DC212 & NYCLUG
Fat Cat Fab Lab
15 April 2024

What is Red Star OS?

Red Star OS is a Linux distro developed by Korean Computer Center (KCC), the North Korean IT research center. The initial release was v1.0 in 2008, followed by Version 2.0 in 2009 and then Version 3.0 in 2012. Version 3.0 is based on Fedora 15 and can (potentially) use its .rpm packages.

A version 4.0 was released sometime in 2019, but no copy of this version was leaked to the internet, although a South Korean newspaper did write an article about it.

Some notes before I begin:

* This talk is based on information gleamed from researching several sources, the biggest of which is Chaos Computer Club's talk at 32C3 (https://media.ccc.de/v/32c3-7174-lifting_the_fog_on_red_star_os)
* If I'm repeating things from 32C3's talk, I do it only because it's one of the better sources of info
* Live interaction has been through both bare metal and an isolated VM
* I've never been to DPRK
* Most of the knowledge gleaned has been through additional research and collecting info from blogs and old sites (most of which I had to find via the Wayback Machine)
* No, Kim Jong Un isn't watching this!

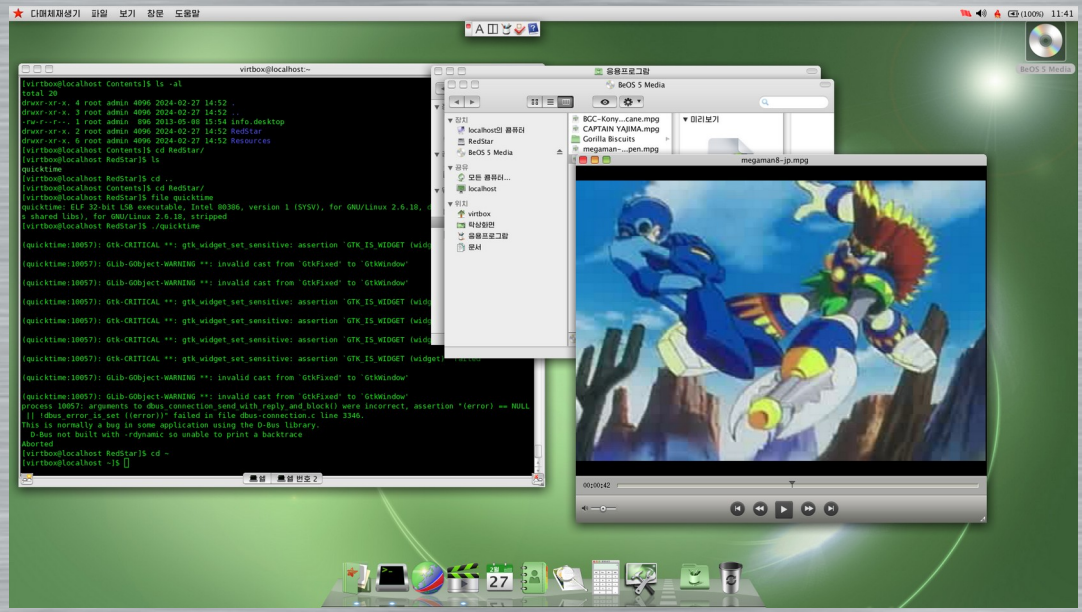
Some Features of Red Star OS

* Uses KDE as DE/WM with macOS skin applied
* “Naenara” browser is a rebranded Mozilla Firefox 3.6 with Korean language pack
* “Sogwang Office” is rebranded OpenOffice 3.x
* Gnash included for Flash applications
* “Crosswin” Windows compatibility layer (it’s just Wine 1.2.2)
* Root not available by default but a “Rootsetting” tool lets users set a root password to use the root account

Additional features

* Bokem (“sword”) - a cryptography tool
* swmng - A software manager
* MusicScore - A music composer
* Companero IDE - A reskinned/renamed Eclipse IDE
* “QuickTime Movie Player” - A media player (might be something else? Mplayer?)

There are also some other interesting packages as well in the local DVD repository that we’ll look at soon.



If you wonder why the macOS-like UI is prominent in Red Star OS, this is why.

Kim Jong-Un was photographed with an iMac on his desk around 2013. This might have been the influence in the decision to make the macOS-like skin for Red Star OS 3.0, as he may have wanted everyone to use the same style GUI, behavior and all, as he did.

Those more dubious features (and normally not dubious features!) which can be used for not nice purposes:

* Snort (not installed by default)
* System file modification detector that can warn about modified files (located at /usr/share/autostart/initcheck_kde.desktop)
* Firewall settings to keep network access limited to only the North Korean Intranet's IP address block (175.45.176.0-175.45.179.255) (simple to defeat by flushing iptables rules)
* SELinux enforcement preventing modification of the system; has custom modules
* securityd (puts system into a reboot loop if system files are modified)
* scnprc (claims to be a virus scanner but is much nastier)
* opprc (responsible for watermarking of certain filetypes)

Wait, watermarking!?

* Every file that passes through a Red Star OS is watermarked by the opprc daemon
* Files are checked by filetypes and metadata (document files, video files, audio files, picture files are all marked)
* Watermarking is done by an AES encrypted segment of data added somewhere in the file
* All vulnerable filetypes are marked as soon as they pass into the OS; read-only volumes won't be affected
* Checking the md5sum or using a hex editor will reveal the file has been touched

```
preview bottle_original.jpg
00000 6EB0:  5A 51 D9 A0 07 A5 D1 0C  06 9B 17 11 EC 1D 8B 50  ZQ..... .......P
00000 6EC0:  EC 10 EC 57 F4 79 7D 73  E5 3F B7 14 68 C7 EA D8  ...W.y}s .?..h...
00000 6ED0:  B2 00 55 81 A0 FA 03 22  4B 35 CC 41 3D F1 2B 3F  ..U...." K5.A=.+?
00000 6EE0:  FC 76 C3 C9 27 50 A4 57  06 C4 F1 1A B3 0E 89 1D  .v..'P.W ........
00000 6EF0:  60 13 2C F0 C6 53 35 23  0A 4E 13 C2 FC 4F 20 B4  `.,..S5# .N...O .
00000 6F00:  76 FA D7 0D 26 37 6F 03  35 AE 2A 12 A3 07 5D 50  v...&7o. 5.*...]P
00000 6F10:  2A 5A 5C 90 A0 D8 D1 00  81 39 60 0A 48 55 A6 74  *Z\..... .9`.HU.t
00000 6F20:  AC 37 3F 4C 93 00 1B 55  D4 CD 6F CB D0 CA 8E 1A  .7?L...U ..o.....
00000 6F30:  04 1A 40 8F 34 AA F6 69  DD 43 15 DA 0B BF A2 AB  ..@.4..i .C......
00000 6F40:  B6 FD AD 03 22 A1 F9 87  27 87 E8 F0 40 42 23 DC  ....".. '...@B#.
00000 6F50:  71 EE 0F 24 C8 0C A2 90  9B 4C 91 55 2D 64 D3 BC  q..$.... .L.U-d..
00000 6F60:  C0 D5 85 E2 09 5F 48 C2  0F 80 80 DC 61 13 1A AB  ....._H. ....a...
00000 6F70:  43 DE AB FA 7C BE B9 F2  9F E0 AB C8 02 F3 C3 5D  C...|... .......]
00000 6F80:  48 42 09 A0 DD BF A9 7E  D1 E0 B1 56 F5 BA 97 94  HB.....~ ...V....
00000 6F90:  30 75 10 3A 24 CA CA 22  93 A5 45 81 A0 E0 34 7E  0u.:$.." ..E...4~
00000 6FA0:  A5 AD 11 02 77 6A 2E 8F  D5 E5 F5 CF 94 FF 00 3D  ....wj.. .......=
00000 6FB0:  CB EB 9F 29 FE 7B 97 D7  3E 53 FC F7 2F AE 7F A1  ...).{.. >S../...
00000 6FC0:  DD FE 7B FD 5E 0C FF D9                          ..{.^...
00000 6FD0:
00000 6FE0:
00000 6FF0:
00000 7000:
00000 7010:

preview bottle_firstuser.jpg
00000 6EB0:  5A 51 D9 A0 07 A5 D1 0C  06 9B 17 11 EC 1D 8B 50  ZQ..... .......P
00000 6EC0:  EC 10 EC 57 F4 79 7D 73  E5 3F B7 14 68 C7 EA D8  ...W.y}s .?..h...
00000 6ED0:  B2 00 55 81 A0 FA 03 22  4B 35 CC 41 3D F1 2B 3F  ..U...." K5.A=.+?
00000 6EE0:  FC 76 C3 C9 27 50 A4 57  06 C4 F1 1A B3 0E 89 1D  .v..'P.W ........
00000 6EF0:  60 13 2C F0 C6 53 35 23  0A 4E 13 C2 FC 4F 20 B4  `.,..S5# .N...O .
00000 6F00:  76 FA D7 0D 26 37 6F 03  35 AE 2A 12 A3 07 5D 50  v...&7o. 5.*...]P
00000 6F10:  2A 5A 5C 90 A0 D8 D1 00  81 39 60 0A 48 55 A6 74  *Z\..... .9`.HU.t
00000 6F20:  AC 37 3F 4C 93 00 1B 55  D4 CD 6F CB D0 CA 8E 1A  .7?L...U ..o.....
00000 6F30:  04 1A 40 8F 34 AA F6 69  DD 43 15 DA 0B BF A2 AB  ..@.4..i .C......
00000 6F40:  B6 FD AD 03 22 A1 F9 87  27 87 E8 F0 40 42 23 DC  ....".. '...@B#.
00000 6F50:  71 EE 0F 24 C8 0C A2 90  9B 4C 91 55 2D 64 D3 BC  q..$.... .L.U-d..
00000 6F60:  C0 D5 85 E2 09 5F 48 C2  0F 80 80 DC 61 13 1A AB  ....._H. ....a...
00000 6F70:  43 DE AB FA 7C BE B9 F2  9F E0 AB C8 02 F3 C3 5D  C...|... .......]
00000 6F80:  48 42 09 A0 DD BF A9 7E  D1 E0 B1 56 F5 BA 97 94  HB.....~ ...V....
00000 6F90:  30 75 10 3A 24 CA CA 22  93 A5 45 81 A0 E0 34 7E  0u.:$.." ..E...4~
00000 6FA0:  A5 AD 11 02 77 6A 2E 8F  D5 E5 F5 CF 94 FF 00 3D  ....wj.. .......=
00000 6FB0:  CB EB 9F 29 FE 7B 97 D7  3E 53 FC F7 2F AE 7F A1  ...).{.. >S../...
00000 6FC0:  DD FE 7B FD 5E 0C FF D9  E3 E0 D9 04 55 9D 35 F9  ..{.^... ....U.5.
00000 6FD0:  9B 3B FD DA 6B D6 B6 A9  5A 13 A0 E6 29 4B 75 B1  .;..k... Z...)Ku.
00000 6FE0:  18 00 00 00 45 4F 46                             ....EOF
00000 6FF0:
00000 7000:
00000 7010:

 Arrow keys move  F find  N next  RET next difference  ESC quit  T move top
 C  ASCII/EBCDIC  E edit  P prev  G   goto position    Q   quit  B move bottom
```

The opprc daemon

* Runs in the background and is not transparent to the user
* Normally can't kill the process (the PID is protected by rtscan)
* Shares code with scnprc (we'll come to that next)
* Remember how I said "files that pass through the OS"? You don't even have to open the file!
* The watermarks in files contain information on the computer; this is how they suppress free speech!

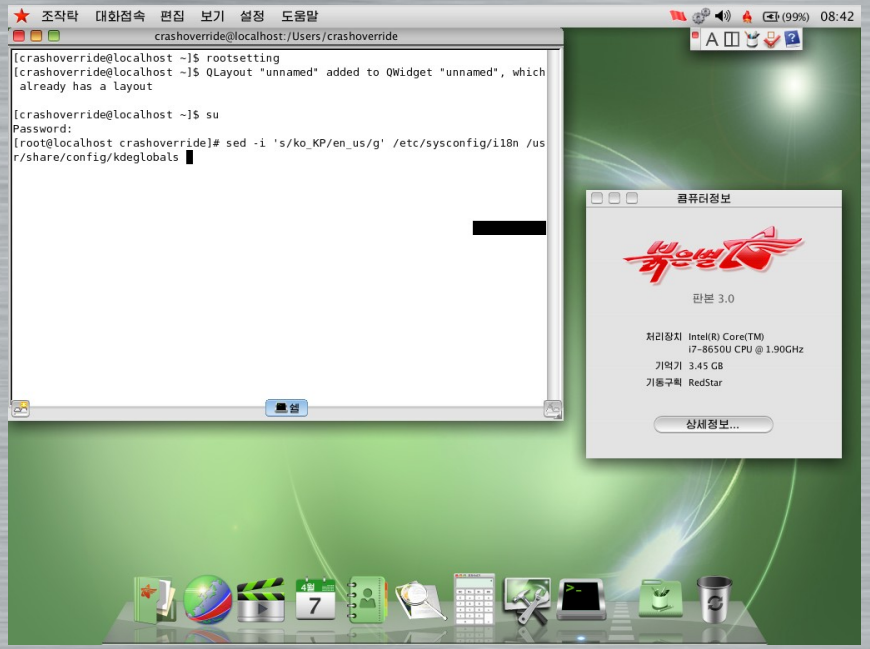
```
preview bottle_original.jpg
00000 6EB0:  5A 51 D9 A0 07 A5 D1 0C  06 9B 17 11 EC 1D 8B 50  ZQ..... .......P
00000 6EC0:  EC 10 EC 57 F4 79 7D 73  E5 3F B7 14 68 C7 EA D8  ...W.y}s .?..h...
00000 6ED0:  B2 00 55 81 A0 FA 03 22  4B 35 CC 41 3D F1 2B 3F  ..U...." K5.A=.+?
00000 6EE0:  FC 76 C3 C9 27 50 A4 57  06 C4 F1 1A B3 0E 89 1D  .v..'P.W ........
00000 6EF0:  60 13 2C F0 C6 53 35 23  0A 4E 13 C2 FC 4F 20 B4  `.,..S5# .N...O .
00000 6F00:  76 FA D7 0D 26 37 6F 03  35 AE 2A 12 A3 07 5D 50  v...&7o. 5.*...]P
00000 6F10:  2A 5A 5C 90 A0 D8 D1 00  81 39 60 0A 48 55 A6 74  *Z\..... .9`.HU.t
00000 6F20:  AC 37 3F 4C 93 00 1B 55  D4 CD 6F CB D0 CA 8E 1A  .7?L...U ..o.....
00000 6F30:  04 1A 40 8F 34 AA F6 69  DD 43 15 DA 0B BF A2 AB  ..@.4..i .C......
00000 6F40:  B6 FD AD 03 22 A1 F9 87  27 87 E8 F0 40 42 23 DC  ....".. '...@B#.
00000 6F50:  71 EE 0F 24 C8 0C A2 90  9B 4C 91 55 2D 64 D3 BC  q..$.... .L.U-d..
00000 6F60:  C0 D5 85 E2 09 5F 48 C2  0F 80 80 DC 61 13 1A AB  ....._H. ....a...
00000 6F70:  43 DE AB FA 7C BE B9 F2  9F E0 AB C8 02 F3 C3 5D  C...|... .......]
00000 6F80:  48 42 09 A0 DD BF A9 7E  D1 E0 B1 56 F5 BA 97 94  HB.....~ ...V....
00000 6F90:  30 75 10 3A 24 CA CA 22  93 A5 45 81 A0 E0 34 7E  0u.:$.." ..E...4~
00000 6FA0:  A5 AD 11 02 77 6A 2E 8F  D5 E5 F5 CF 94 FF 00 3D  ....wj.. .......=
00000 6FB0:  CB EB 9F 29 FE 7B 97 D7  3E 53 FC F7 2F AE 7F A1  ...).{.. >S../...
00000 6FC0:  DD FE 7B FD 5E 0C FF D9                          ..{.^...
00000 6FD0:
00000 6FE0:
00000 6FF0:
00000 7000:
00000 7010:

preview bottle_firstuser.jpg
00000 6EB0:  5A 51 D9 A0 07 A5 D1 0C  06 9B 17 11 EC 1D 8B 50  ZQ..... .......P
00000 6EC0:  EC 10 EC 57 F4 79 7D 73  E5 3F B7 14 68 C7 EA D8  ...W.y}s .?..h...
00000 6ED0:  B2 00 55 81 A0 FA 03 22  4B 35 CC 41 3D F1 2B 3F  ..U...." K5.A=.+?
00000 6EE0:  FC 76 C3 C9 27 50 A4 57  06 C4 F1 1A B3 0E 89 1D  .v..'P.W ........
00000 6EF0:  60 13 2C F0 C6 53 35 23  0A 4E 13 C2 FC 4F 20 B4  `.,..S5# .N...O .
00000 6F00:  76 FA D7 0D 26 37 6F 03  35 AE 2A 12 A3 07 5D 50  v...&7o. 5.*...]P
00000 6F10:  2A 5A 5C 90 A0 D8 D1 00  81 39 60 0A 48 55 A6 74  *Z\..... .9`.HU.t
00000 6F20:  AC 37 3F 4C 93 00 1B 55  D4 CD 6F CB D0 CA 8E 1A  .7?L...U ..o.....
00000 6F30:  04 1A 40 8F 34 AA F6 69  DD 43 15 DA 0B BF A2 AB  ..@.4..i .C......
00000 6F40:  B6 FD AD 03 22 A1 F9 87  27 87 E8 F0 40 42 23 DC  ....".. '...@B#.
00000 6F50:  71 EE 0F 24 C8 0C A2 90  9B 4C 91 55 2D 64 D3 BC  q..$.... .L.U-d..
00000 6F60:  C0 D5 85 E2 09 5F 48 C2  0F 80 80 DC 61 13 1A AB  ....._H. ....a...
00000 6F70:  43 DE AB FA 7C BE B9 F2  9F E0 AB C8 02 F3 C3 5D  C...|... .......]
00000 6F80:  48 42 09 A0 DD BF A9 7E  D1 E0 B1 56 F5 BA 97 94  HB.....~ ...V....
00000 6F90:  30 75 10 3A 24 CA CA 22  93 A5 45 81 A0 E0 34 7E  0u.:$.." ..E...4~
00000 6FA0:  A5 AD 11 02 77 6A 2E 8F  D5 E5 F5 CF 94 FF 00 3D  ....wj.. .......=
00000 6FB0:  CB EB 9F 29 FE 7B 97 D7  3E 53 FC F7 2F AE 7F A1  ...).{.. >S../...
00000 6FC0:  DD FE 7B FD 5E 0C FF D9  E3 E0 D9 04 55 9D 35 F9  ..{.^... ....U.5.
00000 6FD0:  9B 3B FD DA 6B D6 B6 A9  5A 13 A0 E6 29 4B 75 B1  .;..k... Z...)Ku.
00000 6FE0:  18 00 00 00 45 4F 46                             ....EOF
00000 6FF0:
00000 7000:
00000 7010:

Arrow keys move  F find  N next  RET next difference  ESC quit  T move top
C  ASCII/EBCDIC  E edit  P prev  G   goto position    Q   quit  B move bottom
```

The scnprc daemon

* Looks and acts like a virus scanner but is far nastier
* Started by kdeinit via /usr/share/autostart/scnprc.desktop
* Can be triggered automatically, even without touching a file
* Loads the rtscan.ko kernel module
* Starts opprc as well
* Files it targets are removed from the computer, but what happens afterwards?
  * Are they actually deleted, or are they copied to a police server and then deleted from the source?



And now the fun part...

LIVE DEMO TIME!!
LIVE DEMO TIME!!
LIVE DEMO TIME!!

Here's a bonus!

This is the map of the North Korean Intranet posted on the DPRK 360 Facebook page.

홈페지명	홈페지주소	기 관 명
광 명	http://10.41.1.2	중앙과학기술통보사
진 달 래	http://10.76.12.2	만경대정보쎈터
선 구 자	http://10.208.0.34	함경남도과학기술통보소
내 나 라	http://10.76.1.11	내나라정보쎈터
남 산	http://192.168.1.101	인민대학습당
리 상	http://10.15.15.8	김책공업종합대학
아 침	http://172.16.34.100	조선과학기술총련맹 중앙위원회
정 보 21	http://10.21.1.22	명양정보쎈터
과학기술전시관	http://192.168.10.10	3대혁명전시관
기 둥	http://10.205.1.5	청진광산금속대학
만 방	http://10.61.61.3	조선중앙방송위원회
새 세 기	http://10.41.1.10	중앙과학기술통보사
방 역	http://10.41.50.3	발명국 비루스감독부
래 일	http://10.66.1.3	국가규격제정위원회
발 명	http://10.41.50.9	과학원 발명국
클 락 새	http://10.240.100.11	김일성종합대학 정보쎈터
한 마 음	http://10.76.1.20	오산덕정보쎈터
북 극 성	http://10.76.1.2	국가망정보쎈터
고려의술	http://10.76.1.18	고려의학과학원 조선침구쎈터
지 황	http://10.208.1.2	함흥화학공업대학
룡 라	http://172.16.4.200	룡라프로그람쎈터
비 약	http://10.15.15.5	김책공업종합대학
로동신문	http://10.10.3.100	로동신문사
생 명	http://10.65.3.2	의학과학정보쎈터
해 양	http://10.17.1.5	특해운성
천 리 마	http://172.16.11.23	중앙정보통신국

Some Additional Resources!

* Lifting the Fog on Red Star OS (Chaos Computer Club's original talk): https://media.ccc.de/v/32c3-7174-lifting_the_fog_on_red_star_os
* redstar-tools: https://github.com/takeshixx/redstar-tools
* RichardG's Ramblings - Notes on Red Star OS 3.0: https://richardg867.wordpress.com/2015/01/01/notes-on-red-star-os-3-0/
* InfoWorld - Is It Safe to Install North Korean Linux? https://www.infoworld.com/article/3190558/is-it-safe-to-install-north-korea-linux.html
* Insinuator - RedstarOS Watermarkings: https://insinuator.net/2015/07/redstar-os-watermarking/

Where to go from here?

* Keep digging into Red Star OS further and see how much it can be modified
* Search for Red Star OS 4.0
* Look at more esoteric Linux distros from other countries with oppresive or authoritarian governments
* Share this shit online, of course! Vids, blogs, papers, talks, everything!

Information wants to be free, and we gotta be the datarunners and Netrunners to bring that information out!

SHOUT OUTS!!

* DC212, NYC2600, NYCLUG, Fat Cat, Hack Manhattan, and NYC Resistor!
* All my friends who supported me!
* Hackers.town and corteximplant.com!
* Chaos Computer Club for their original talk and exploration of Red Star OS!
* All those hackers and cyberpunks who fight against injustice and corruption every day of their lives
* And YOU!!

Find me online!

* Mastodon (https://hackers.town/@LambdaCalculus)
* Bluesky (https://bsky.app/profile/lambdacalculus.bsky.social)
* GitHub (https://github.com/LambdaCalculus37)
* YouTube (https://www.youtube.com/@LambdaCalculus379)

Support me online!

https://ko-fi.com/lambdacalculus