



A look at North Korea's 'paranoid' Red Star OS computer operating system

January 1, 2016 By Pierluigi Paganini



Experts at the last Chaos Communication Congress in Hamburg analyzed the North Korean 'paranoid' Red Star OS computer operating system.

North Korea has its new operating system, the Red Star OS, which is used by the population of a country NOT connected to the World Wide Web to access state media and some officially approved sites.

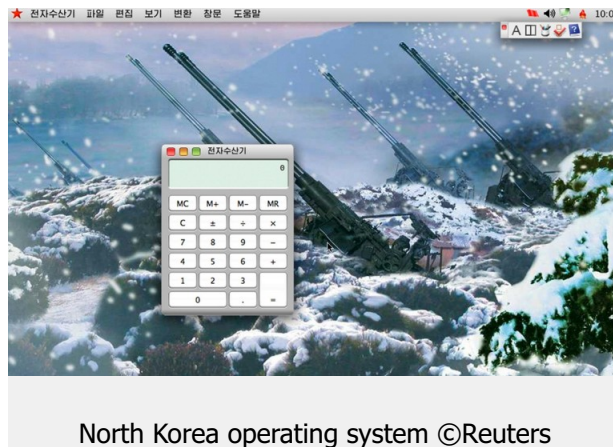
The operating system mirrors its political posture, characterized by a high degree of paranoia and invasive surveilling on users, according to two German researchers from the IT security company ERNW.

Florian Grunow and Niklaus Schiess downloaded the software from a website outside North Korea

This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish.

Accept

Read More



North Korea operating system ©Reuters

These are their findings:□

- Latest version is from around 2013.
- Red Star OS is based on the Fedora Linux distro.
- It has an Apple OSX look, the country's leader Kim Jong-un, like his father, has been photographed near Macs.
- Own version of encryption files, the North Korea□ wants to avoid the spread of any code that might compromise OS files.□

“This is a full blown operation system where they control most of the code,” “Maybe this is a bit fear-driven,” Grunow said. “They may want to be independent of other operating systems because they fear back doors,” which might allow others to spy on them.

- Tampering with the OS difficult: If a user makes□ any changes to core functions, like trying to disable its antivirus checker or firewall, the□ computer will display an error message or reboot itself
- Cracking underground exchange of foreign movies, music and writing: tagging, or watermarking, every document or media file on□ a computer / USB stick connected to it. That means that all files can be traced.□

“It’s definitely privacy invading. It’s not transparent□ to the user,” Grunow said. “It’s done stealthily and touches files you haven’t even opened.”□

- Research did not show any sign of cyber-attack capability North-Korea has been accused of.

“It really looks like they’ve just tried to build an operating system for them, and give the user a basic set of applications,” Grunow said. Including a Korean word processor, a calendar and an app for composing and transcribing music.

An authority on the spread of foreign media in North Korea, Nat Kretchun, said such efforts reflected North Korea’s realization that it needs “new ways to update their surveillance and security procedures to respond to new types of technology and new sources of information”.

Other countries have designed their own OS, including China, Russia and Cuba, the latter for example has the National Nova OS.

Let’s see if further research into Red Star OS reveals more things North Korea is planning to do, meantime give a look to their presentation:

Written by: Cordny Nederkoorn

Author Bio:

Software test engineer, Founder TestingSaaS, a social network about researching cloud applications with a focus on forensics, software testing and security.

Pierluigi Paganini

(Security Affairs – Red Start OS, North Korea)

Share it please ...





SHARE ON



Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of

the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".






PREVIOUS
ARTICLE

**US Eavesdropping on
Netanyahu
Communications**

NEXT ARTICLE

**All BBC Websites
went down after a
major DDoS attack**



- [1. 10 Best Operating Systems](#) 
- [2. Ubuntu Operating Systems](#) 
- [3. New Mobile Operating System](#) 
- [4. Android Operating System](#) 
- [5. Google Android OS List](#) 





◦ +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".



1. 10 Best Operating Systems



2. Ubuntu Operating Systems



3. New Mobile Operating System



4. Android Operating System



5. Google Android OS List



6. Cheap Mac Os



7. Buy Os X Mavericks



8. RISC OS



Copyright 2015 Security Affairs by Pierluigi Paganini
All Right Reserved.

Back to top ^