Lifting the Fog on RedStar OS

Agenda

- Motivation
- Architecture of RedStar OS
  - Operating System
  - Additional components
- Lifting the Fog
  - Deep dive into the most interesting features
- Conclusions
- Questions

Disclaimer

http://kimjongunlookingatthings.tumblr.com/image/128274906179

- We never visited DPRK
  - What we say about DPRK are mostly speculations.
- We have analyzed ISOs found on the Internet
  - No guarantee that they are not fake…
  - …but seems legit.
- It’s not about making fun of them
  - Not of the developers …
  - … and certainly not of the people of DPRK.
- No focus on security in this talk

Motivation

http://media.salon.com/2013/04/north_korea1.jpg

- RedStar ISOs leaked some time ago
  - Most recent: end of 2014
- No in-depth analysis yet
  - Most blogs/news articles to date are superficial
- The world should know what it's really about
  - What RedStar users are subjected to
  - State of development in DPRK

Some Previous Work

http://kimjongunlookingatthings.tumblr.com/image/122442252299

- "Closely resembles Mac OS X"
  - http://motherboard.vice.com/read/you-can-now-install-the-north-korean-operating-system-redstar-30
- "Computer Science in the DPRK"
  - Will Scott at 31C3
- "North Korea's Naenara Web Browser: It's Weirder Than We Thought"
  - Mostly covering the browser and email client
  - Interception of traffic
  - https://blog.whitehatsec.com/north-koreas-naenara-web-browser-its-weirder-than-we-thought/

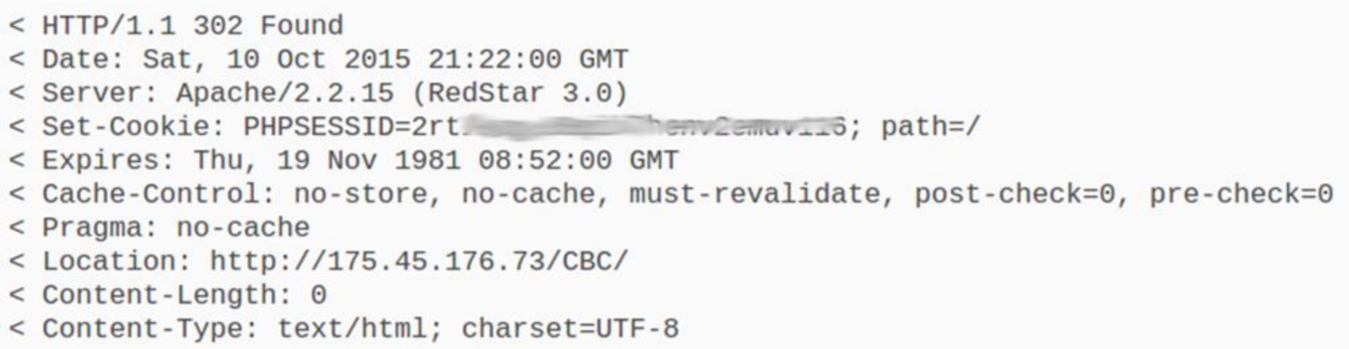
RedStar OS 3.0

http://www.iskrae.eu/wp-content/uploads/2014/12/Kim-Jong-un-al-computer-coi-suoi-generali-se-la-ride-1024x683.jpg

The basis and custom components

Operating System

- Different leaked versions
  - Server (3.0) and Desktop (2.0 (and 2.5?) and 3.0)
  - We focused on Desktop 3.0
  - Version 3.0 **might** even be the latest version:



```
< 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
```

RedStar OS 3.0 Desktop Timeline (Our Guess)

2009

Based on
Fedora 11

2011

Kernel 2.6.38
(Fedora 15)

June 2013

Latest package
build dates

December 2014

Public leak

Operating System

- Fully featured, general purpose desktop system based on KDE
  - Look and Feel of Mac OS X
  - Email client, calendar, word processor, media player, disc/file encryption utility…
- Kernel version 2.6.38.8
  - Additional kernel modules (rtscan, pilsung, kdm, kimm, …)
- Developed by Korean Computer Center (KCC)
  - DPRK's leading government research center for information technology
  - Had a branch office in Germany (KCCE)
- System hardening
  - SELinux (with custom modules)
  - iptables
  - Snort (not running per default)
  - Custom services

http://www.businessinsider.com/brand-new-photo-confirms-that-kim-jong-un-is-a-mac-user-2013-3?IR=T

A quote from Kim Jong-Il says:

“In the process of programming, it is important to develop one in our own style […]”

Custom applications

- Naenara ("my country") -> Browser, based on FF
- Bokem ("sword") -> Crypto tool
- Sogwang Office -> Open Office
- swmng -> Software Manager
- MusicScore -> Compose music!
- "rootsetting" -> get root!
- They even touched KDM

RedStar OS

Demo

http://i.telegraph.co.uk/multimedia/archive/02492/north-korea-jong-i_2492687b.jpg

Lifting the Fog

RedStar's custom components

http://kimjongunlookingatthings.tumblr.com/image/127509112289

Interesting Red Star Packages

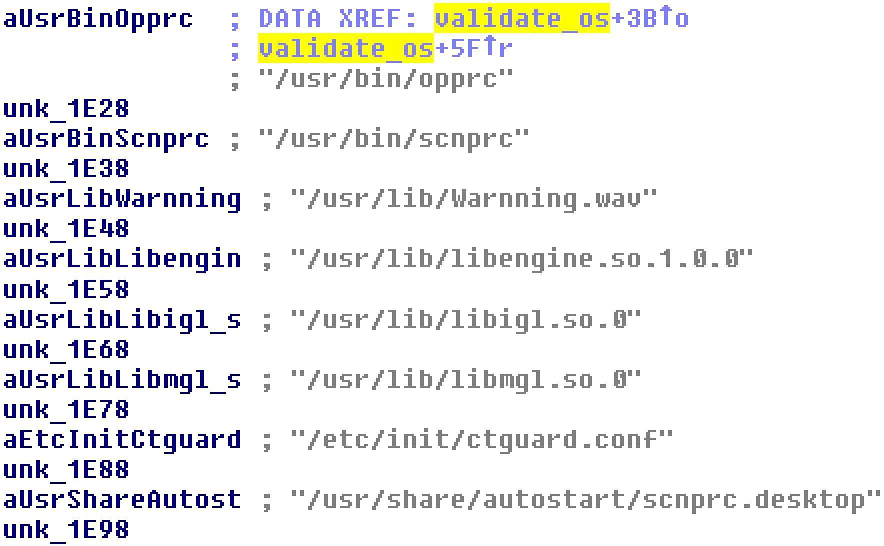
- esig-cb-2.0-a.rs3.0
- esig-cb-db-1.1-1.rs3.0
- intcheck-1.0-23.rs3.0
- selinux-policy-3.9.7-3.rs3.0
- selinux-policy-targeted-3.9.7-3.rs3.0
- kdebase-3.5.1-5.rs3.0
- securityd-1.0-1.rs3.0

intcheck – Integrity Checking

- A daemon that checks integrity of various files
  - Comes with a SQLite database with signatures
  - Checks mostly system related files
  - Includes signatures for some custom RedStar files
- Configurable via system preferences
  - Check integrity at boot-up/run-time
  - Log output available in system preferences
- Prints error messages when integrity checks fail
  - No other relevant actions

securityd – More Integrity Checking…

- Kind of mimics OS X's securityd
  - Includes various plugins
- Includes /usr/lib/libos.so.0.0.0
  - Provides a validate_os() function
  - Integrity checking
  - Hardcoded MD5 checksums
- kdm also calls validate_os()
  - During startup
  - Reboot loop if integrity check fails!



```
aUsrBinOpprc    ; DATA XREF: validate_os+3B↑o
                ; validate_os+5F↑r
                ; "/usr/bin/opprc"
unk_1E28
aUsrBinScnprc   ; "/usr/bin/scnprc"
unk_1E38
aUsrLibWarnning ; "/usr/lib/Warnning.wav"
unk_1E48
aUsrLibLibengin ; "/usr/lib/libengine.so.1.0.0"
unk_1E58
aUsrLibLibigl_s ; "/usr/lib/libigl.so.0"
unk_1E68
aUsrLibLibmgl_s ; "/usr/lib/libmgl.so.0"
unk_1E78
aEtcInitCtguard ; "/etc/init/ctguard.conf"
unk_1E88
aUsrShareAutost ; "/usr/share/autostart/scnprc.desktop"
unk_1E98
```

청봉
전자서명
프로그람
조선콤퓨터쎈터
이 제품은 조선민주주의인민공화국 쏘프트웨어보호법에 의하여 보호됩니다.

esig-cb-2.0-a.rs3.0

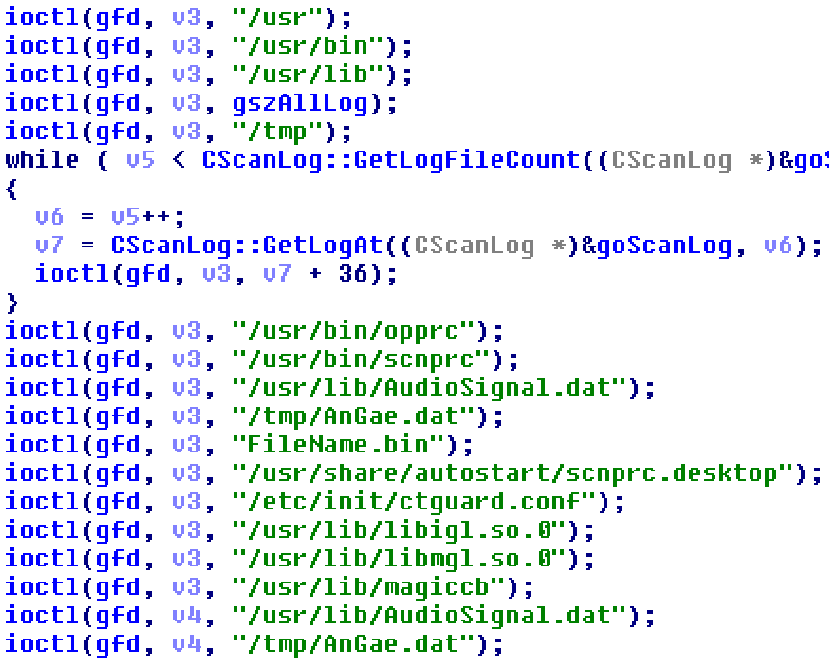
“Electronic Signature Systems”

esig-cb-2.0-a.rs3.0 - Interesting Files

- /etc/init/ctguard.conf
- /lib/modules/2.6.38.8-24.rs3.0.i686.PAE/kernel/fs/rtscan.ko
- /lib/modules/2.6.38.8-24.rs3.0.i686/kernel/fs/rtscan.ko
- /usr/bin/opprc
- /usr/bin/redflag.bmp
- /usr/bin/scnprc
- /usr/lib/AudioSignal.dat
- /usr/lib/Warnning.wav
- /usr/lib/libengine.so
- /usr/lib/libigl.so.0
- /usr/lib/libmgl.so.0
- /usr/lib/magiccb

rtscan.ko – The Interface to the Kernel

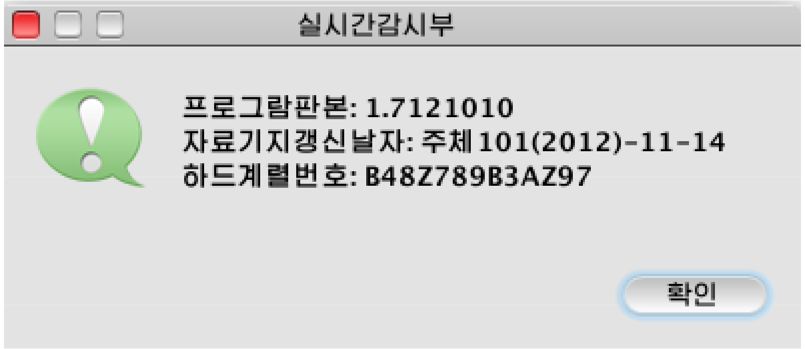
- Hooks several system calls
  - kill, open, close, unlink, rename
- Creates /dev/res
  - Interaction via ioctl calls
- Protects PIDs
  - Processes not killable
- Protects files
  - Files not editable
- Hides files
  - Files not readable



```
ioctl(gfd, v3, "/usr");
ioctl(gfd, v3, "/usr/bin");
ioctl(gfd, v3, "/usr/lib");
ioctl(gfd, v3, gszAllLog);
ioctl(gfd, v3, "/tmp");
while ( v5 < CScanLog::GetLogFileCount((CScanLog *)&go
{
  v6 = v5++;
  v7 = CScanLog::GetLogAt((CScanLog *)&goScanLog, v6);
  ioctl(gfd, v3, v7 + 36);
}
ioctl(gfd, v3, "/usr/bin/opprc");
ioctl(gfd, v3, "/usr/bin/scnprc");
ioctl(gfd, v3, "/usr/lib/AudioSignal.dat");
ioctl(gfd, v3, "/tmp/AnGae.dat");
ioctl(gfd, v3, "FileName.bin");
ioctl(gfd, v3, "/usr/share/autostart/scnprc.desktop");
ioctl(gfd, v3, "/etc/init/ctguard.conf");
ioctl(gfd, v3, "/usr/lib/libigl.so.0");
ioctl(gfd, v3, "/usr/lib/libmgl.so.0");
ioctl(gfd, v3, "/usr/lib/magiccb");
ioctl(gfd, v4, "/usr/lib/AudioSignal.dat");
ioctl(gfd, v4, "/tmp/AnGae.dat");
```

scnprc – “The Virus Scanner”

- Provides a GUI that looks like an actual virus scanner
  - Transparent for the user
- Started by kdeinit
  - Via /usr/share/autostart/scnprc.desktop
- Different ways to trigger scanning
  - Automatically w/o opening files
  - By selecting folders in the GUI
- Loads rtscan.ko kernel module
- Starts opprc



실시간감시부

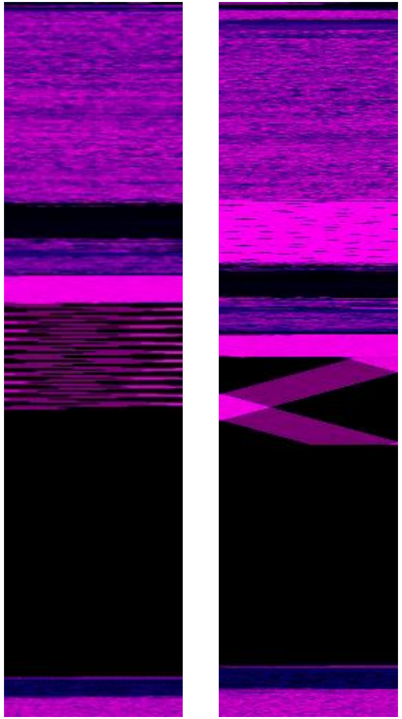
프로그람판본: 1.7121010
자료기지갱신날자: 주체101(2012)-11-14
하드계렬번호: B48Z789B3AZ97

scnprc – Pattern Matching

- /tmp/AnGae.dat file includes signatures
  - "Angae" means "fog" in Korean
  - Not readable, even by root (hidden by rtscan)
- Includes UTF-16 strings with Korean/Chinese/$whatever
  - Google translate says terms like "strike with fists", "punishment", "hungry"
  - We cannot confirm this
- Pattern updating
  - Built-in update functionality (hardcoded intranet IPs)
  - New AnGae.dat versions by updating esig-cb-db package
- Can be used to delete malicious files
  - Developers decide what is "malicious"

opprc - The Evil Twin

- Running in background
  - Not transparent for the user
- Cannot be killed
  - Protected PID (by rtscan)
- Shares a lot of code with scnprc
- Applies watermarks to files



Watermarking

- Watermarks are applied by opening files
  - Sometimes even without opening
- Supported file types
  - We can confirm: DOCX (from M$ Office), JPG, PNG, AVI
  - Code indicates additional media file formats

→ This is not a security feature, they watermark free speech!

Watermarks

- Encrypted hard disk serial
  - DES encryption
  - Hardcoded key: 0x13 0x52 0x07 0x0d 0x13 0x3A 0x08 0x10
    - 1982 7 13 1958 8 16
- ASCII “EOF” at the end
  - For .jpg and .avi it just appends it to the end
  - For .docx it puts it near the beginning, lots of null bytes

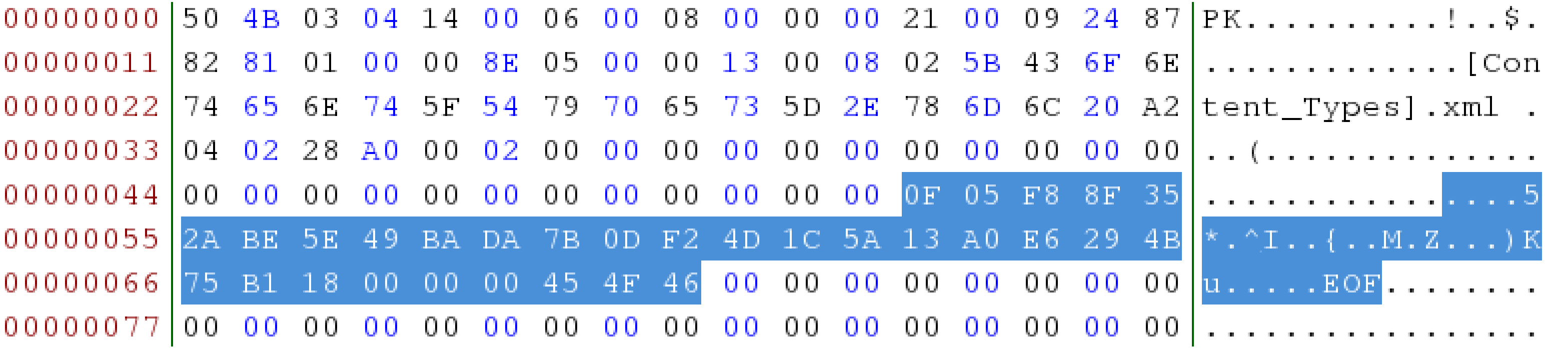
Watermarking

Demo

http://cdnph.upi.com/sv/b/i/UPI-4041448563737/2015/1/14485638341700/Kim-Jong-Uns-unannounced-trips-a-headache-for-North-Korea-security.jpg

Watermark – Example in DOCX

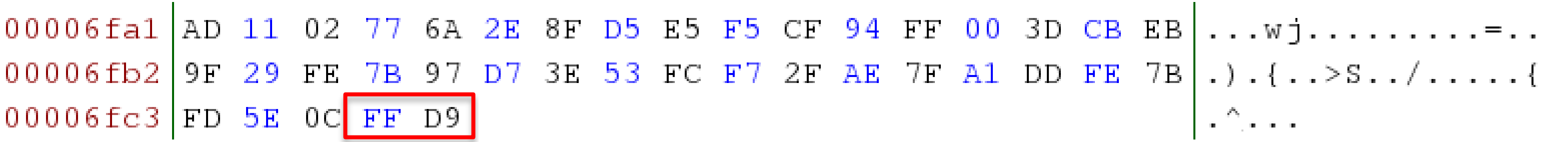
Plaintext: **WMB48Z789B3AZ97**



```
00000000 50 4B 03 04 14 00 06 00 08 00 00 00 21 00 09 24 87 PK..........!..$.
00000011 82 81 01 00 00 8E 05 00 00 13 00 08 02 5B 43 6F 6E .............[Con
00000022 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D 6C 20 A2 tent_Types].xml .
00000033 04 02 28 A0 00 02 00 00 00 00 00 00 00 00 00 00 00 ..(..............
00000044 00 00 00 00 00 00 00 00 00 00 00 00 0F 05 F8 8F 35 ................5
00000055 2A BE 5E 49 BA DA 7B 0D F2 4D 1C 5A 13 A0 E6 29 4B *.^I..{..M.Z...)K
00000066 75 B1 18 00 00 00 45 4F 46 00 00 00 00 00 00 00 00 u.....EOF........
00000077 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
```

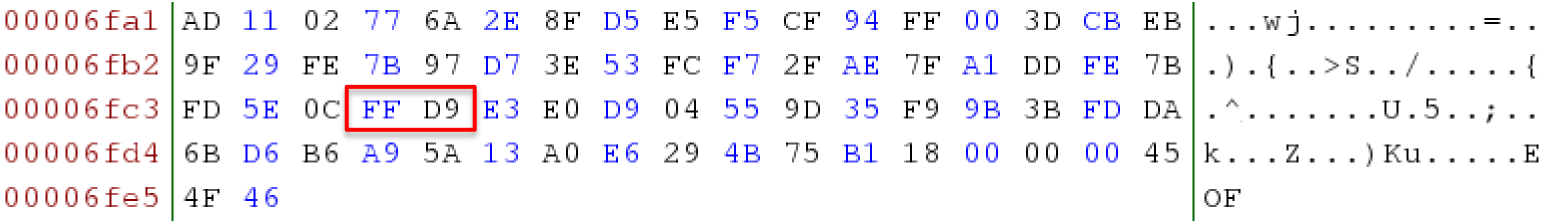
bottle.jpg

Original



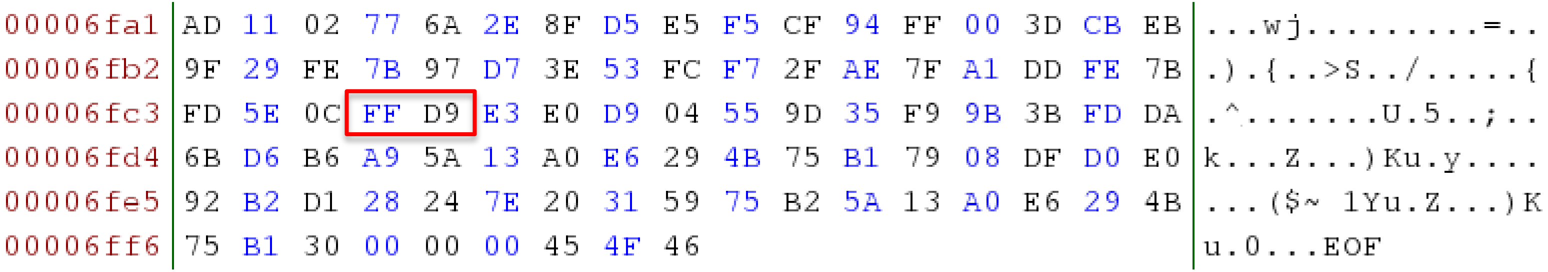
```
00006fa1 | AD 11 02 77 6A 2E 8F D5 E5 F5 CF 94 FF 00 3D CB EB | ...wj.........=..
00006fb2 | 9F 29 FE 7B 97 D7 3E 53 FC F7 2F AE 7F A1 DD FE 7B | .).{..>S../.....{
00006fc3 | FD 5E 0C FF D9                                     | .^...
```

First user

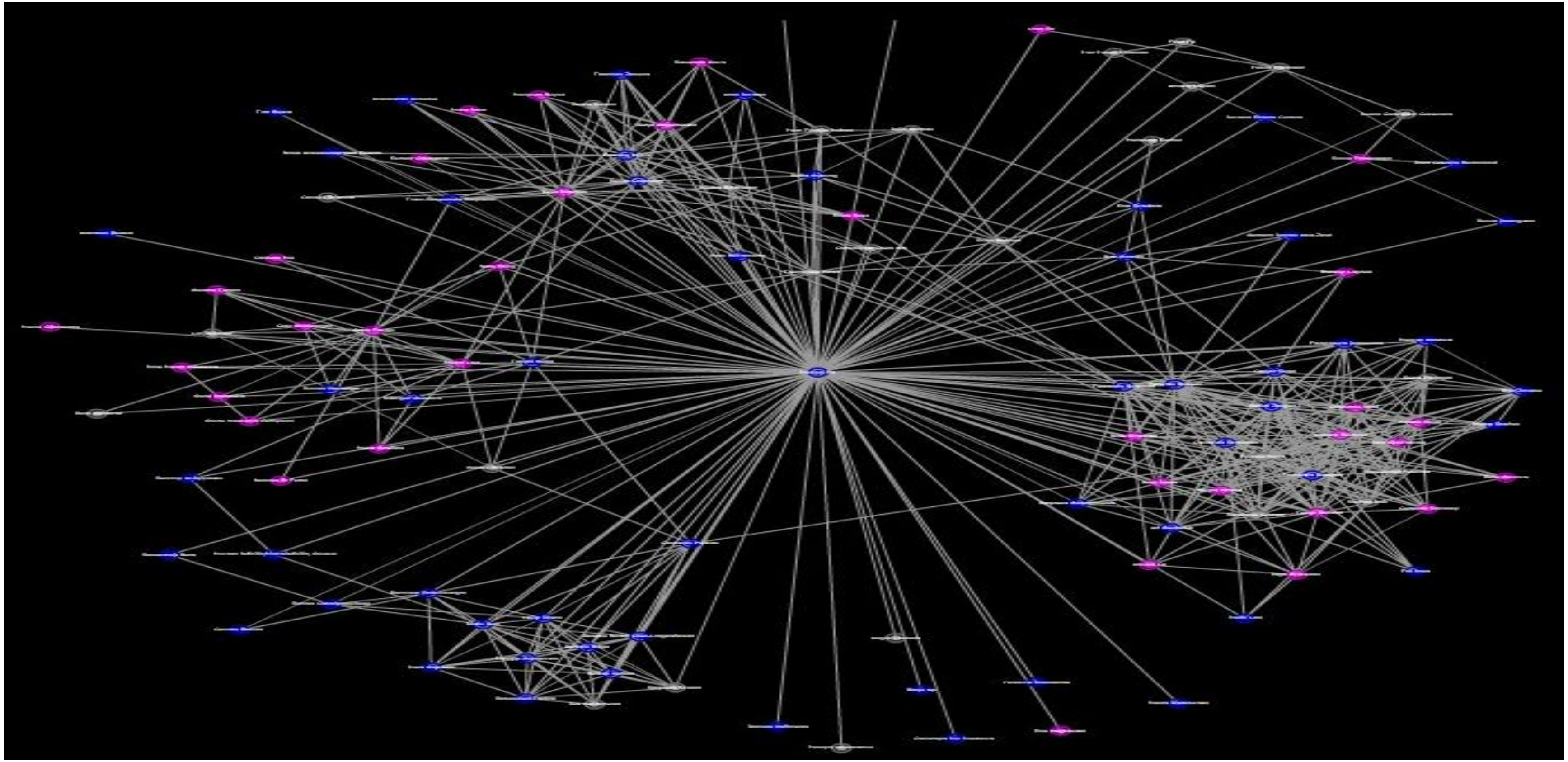


```
00006fa1 | AD 11 02 77 6A 2E 8F D5 E5 F5 CF 94 FF 00 3D CB EB | ...wj.........=..
00006fb2 | 9F 29 FE 7B 97 D7 3E 53 FC F7 2F AE 7F A1 DD FE 7B | .).{..>S../.....{
00006fc3 | FD 5E 0C FF D9 E3 E0 D9 04 55 9D 35 F9 9B 3B FD DA | .^.......U.5..;..
00006fd4 | 6B D6 B6 A9 5A 13 A0 E6 29 4B 75 B1 18 00 00 00 45 | k...Z...)Ku.....E
00006fe5 | 4F 46                                              | OF
```

Second user



```
00006fa1 | AD 11 02 77 6A 2E 8F D5 E5 F5 CF 94 FF 00 3D CB EB | ...wj.........=..
00006fb2 | 9F 29 FE 7B 97 D7 3E 53 FC F7 2F AE 7F A1 DD FE 7B | .).{..>S../.....{
00006fc3 | FD 5E 0C FF D9 E3 E0 D9 04 55 9D 35 F9 9B 3B FD DA | .^.......U.5..;..
00006fd4 | 6B D6 B6 A9 5A 13 A0 E6 29 4B 75 B1 79 08 DF D0 E0 | k...Z...)Ku.y....
00006fe5 | 92 B2 D1 28 24 7E 20 31 59 75 B2 5A 13 A0 E6 29 4B | ...($~ 1Yu.Z...)K
00006ff6 | 75 B1 30 00 00 00 45 4F 46                         | u.0...EOF
```



Completely Disable Custom Components

- Get root (via rootsetting application)
- Kill securityd
- Kill intcheck
- Disable rtscan via ioctl
- Kill scnprc and opprc
- Replace /usr/lib/libos.so.0
- Delete /usr/share/autostart/scnprc.desktop

Evolution – Differences between 2.0 and 3.0

http://dailygarlic.com/userImages/300_you-think-your-job-is-stressful-.jpg

- A lot of code statically linked in opprc/scnprc
  - Older version used many shared libraries
- opprc not started by scnprc
  - /sbin/init (highly customized)
  - /usr/bin/signature
- Integrity checking by
  - /sbin/init
  - /usr/bin/signature
- File permissions on /dev/res
  - Various binaries do “chmod 777 /dev/res”
- Custom code build into hald
- They moved from “init 0” to “reboot”

The Organ Mystery (thx @_fel1x)

- File missing on system, but referenced:
  - */usr/lib/organ*
- Is read by opprc
  - Decrypts -> Gets crypto information from file
- opprc uses this for extended watermarking information

Conclusions

- No backdoors?
  - Probably because:
    - They use it on the Internet
    - Backdoors via updates
    - Not included because ISO could be leaked
    - Vast parts of code tainted by DPRK → Maybe we didn't find it?
- Self protecting system
  - Integrity checking
  - System hardening

Conclusions

- “Virus scanning” and watermarking
  - Track origin and distribution of files
  - Prevent distribution of files
  - Wet dream for an oppressive regime
- Security
  - Problems with file permissions
  - Custom code uses basic protections (Stack cookies, NX, ASLR, …)

Conclusions

- → Guess: They preliminary tried to protect the system.
- → Guess: The system was built for home computers.
- → Guess: They know backdoors are bullshit! ;-)
- → Please contribute to lifting the fog even more:

https://github.com/takeshixx/redstar-tools

http://kimjongunlookingatthings.tumblr.com/image/110131458869

Questions?

Niklaus:	@_takeshix
Florian:	@0x79

Thank you!

Go make the world a safer place!