

**LIBERTY
IN
NORTH
KOREA**

×

DEFCON





×

DEFCON



Cracking North Korea's Information Control

I. INTRODUCTION

Who I am and why this matters



Jon Thompson

Chief Technology Officer
Liberty in North Korea



Sysadmin > Threat Hunter > I ROOT NORTH KOREAN PHONES

OSCP + SANS + MSc Cyber Security → NK Human Rights

WHY NORTH KOREA?



North Korea has architected the world's most extreme info control system.



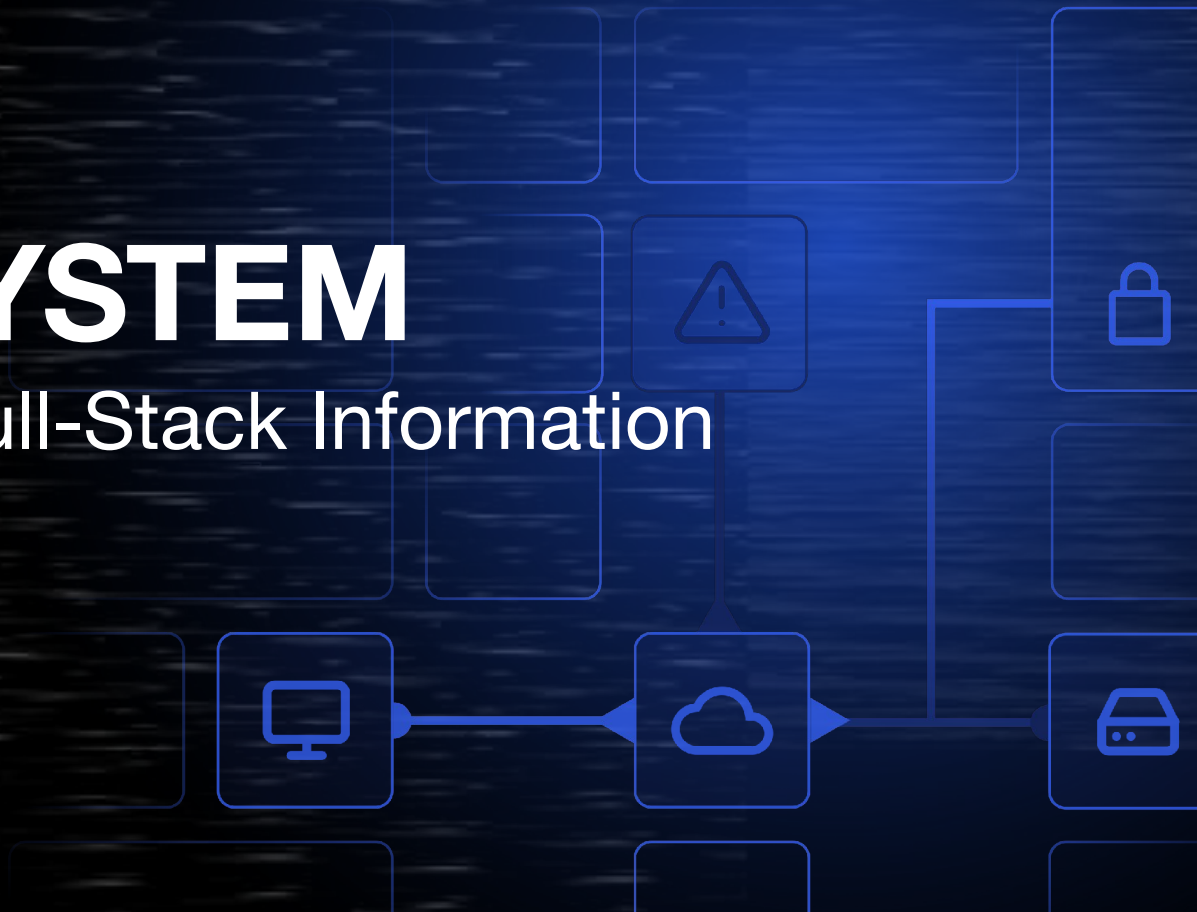
Citizens limited to a national network that is cut off from the global internet.



Sharing unauthorized information or media can result in torture or death.

II. THE SYSTEM

North Korea's Full-Stack Information
Control System



2

providers connect North Korea to the
outside internet.

China Unicom + Russia's TranTeleCom -
Dual-homed since 2017





1,024

Publicly routable IP addresses for the entire nation.

175.45.176.0/22 - less than a single mid-size company.

Scanning North Korean servers

The screenshot displays the Shodan search engine interface. At the top, there's a navigation bar with tabs for Hosts, Archive, Monitors, and Scans. A search bar on the right contains the text "Search banners...". Below the navigation bar, a summary row shows statistics: 14 Discovered Hosts, 61 Open Ports, 1 Active Monitors, 1 Total Scans, and 0 Running. Below this, a "SERVICE CATEGORIES" section lists various service types with their respective counts: New (11 hosts, 21 services), Websites (10 hosts, 19 services), Storage (1 hosts, 1 services), Databases (0 hosts, 0 services), Remote Access (1 hosts, 1 services), Mail (0 hosts, 0 services), Infrastructure (0 hosts, 0 services), and Interesting (0 hosts, 0 services). The "Current Results" section, titled "Showing hosts from the most recent scan per monitor", lists several IP addresses with their scan details and open ports. Each result includes a host icon, the IP address, a status label, a description of the scan, the number of open ports, and action buttons for "Scanned: Just now", a flag, and a trash icon.

IP Address	Status	Description	Open Ports	Scanned: Just now	Flag	Trash
175.45.178.161	Unknown	175.45.178.0/24 subnet - no DNS records found	32 open ports	Scanned: Just now	Flag	Trash
175.45.177.65			11 open ports	Scanned: Just now	Flag	Trash
175.45.177.11			11 open ports	Scanned: Just now	Flag	Trash
175.45.177.10			38 open ports	Scanned: Just now	Flag	Trash
175.45.177.1 Gateway/Router		175.45.177.0/24 subnet - likely network infrastructure	4 open ports	Scanned: Just now	Flag	Trash
175.45.176.91			6 open ports	Scanned: Just now	Flag	Trash
175.45.176.82			3 open ports	Scanned: Just now	Flag	Trash
175.45.176.81 Multi-host server		Shared hosting: cook.org.kp, friend.com.kp, kanz.org.kp, kyctz.com.kp, knic.com.kp, korfilm.com.kp, mtgaw.kp, sdprk.org.kp	6 open ports	Scanned: Just now	Flag	Trash
175.45.176.80			6 open ports	Scanned: Just now	Flag	Trash

24+ phone brands

No app store

Apps install only at state-run “IT Exchange Centers”



The hardware



Photos of a Pyongyang 2423 with its base model,
the Blu Vivo XL3

The hardware



Photos of a Pyongyang 2421

The hardware

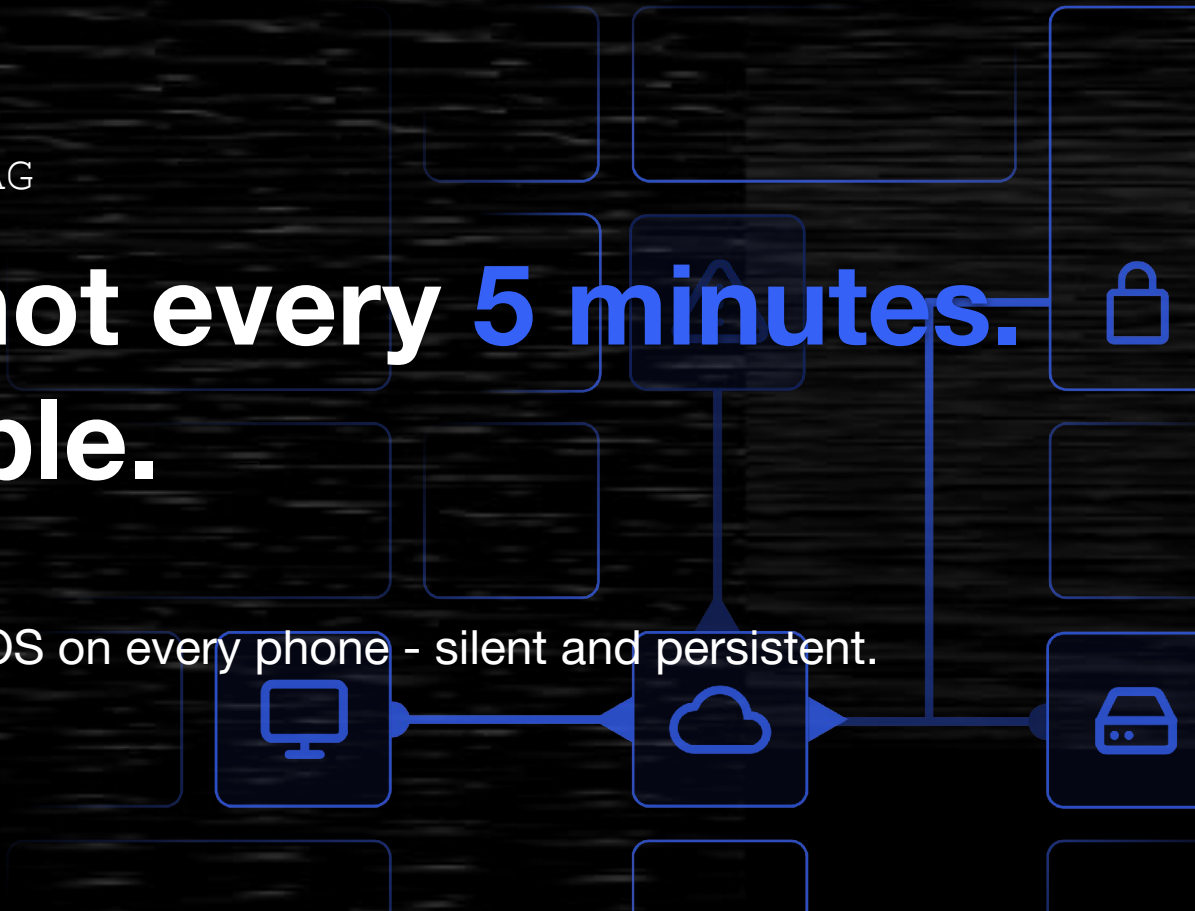


Photos of a Han 701

TRACEVIEWER / REDFLAG

A screenshot every 5 minutes.
Not deletable.

Bundled into the Android OS on every phone - silent and persistent.



The keyboard “autocorrects”

“oppa”



“comrade”

South Korean style affection rewritten into ideology.



RedFlag: only state-signed files can spread

SELSIGN

device signature

NATISIGN

state signature

Unsigned files are auto-deleted on transfer - enforced at the OS level

If the state didn't sign it, it cannot move from phone to phone.

RedFlag: analyzing the signature

```
0050ec40: 6470 692f 646b 5f62 746e 5f62 616e 6b5f dpi/dk_btn_bank_
0050ec50: 6e6f 726d 616c 2e39 2e70 6e67 504b 0102 normal.9.pngPK..
0050ec60: 0a00 0a00 0000 0000 ed70 4147 5f98 f41c .....pAG_...
0050ec70: af58 0000 af58 0000 2000 0000 0000 0000 .X...X.....
0050ec80: 0000 0000 0000 b8fc 4f00 6173 7365 7473 .....O.assets
0050ec90: 2f6d 6d69 6170 2f73 706c 6173 682f 7370 /mmiap/splash/sp
0050eca0: 6c61 7368 5f68 2e6a 7067 504b 0506 0000 lash_h.jpgPK....
0050ecb0: 0000 cb01 cb01 0597 0000 a555 5000 0000 .....UP...
0050ecc0: 80ee a1a6 eba4 ed20 1bed 70ee 684b 3ac5 .....p.hK:...
0050ecd0: 57d6 3a19 3bf4 78d5 8f38 0783 f808 1e92 W.:.;x.w.8.....
0050ece0: 9521 3ea0 73a8 fbba 89f7 a192 ebc1 adf3 .!>.s.....
0050ecf0: 80ee a1a6 724c 57d5 9618 65f5 073f 21cd ....rLW...e.?!..
0050ed00: e4d4 4df7 b332 800b 8c68 77be 52b4 9760 ..M..2...hw.R..`
0050ed10: 7fcc 946d ccef 5485 deb2 15e6 2e2a 3a4a ..m..T.....*:J
0050ed20: 7037 cae4 2df1 5173 70d5 da5f 2e4f ef05 p7.-.Qsp..._O..
0050ed30: ed81 8af7 f050 bd89 73bf de22 3031 8105 .....P.s...01..
0050ed40: e359 5400 cc0f bf53 9440 c997 b442 bb52 .YT.....S.@...B.R
0050ed50: 7155 feea 2935 8358 876d d2fc fa8b a533 qU..)5.X.m.....3
0050ed60: b8e1 5f6e bdfc 5377 051a dbd7 e91c 6788 .._n..Sw.....g.
0050ed70: de92 195b c5ab 59b0 8273 acb6 6ad4 62a6 u{[.Y..s...j.b.
0050ed80: 755c df16 11f9 0960 9aa1 25aa f0cf 6999 ..L.....%...i.
0050ed90: a02e 180a 03d0 f89a 694f 5b83 2164 9e25 .....iO[.!d.%
0050eda0: 9764 9631 27ee 3ed5 5db8 6aba e27d e4bf .d.1'>.]j...}..
0050edb0: 115b f9a4 0474 84b4 6084 95bc f3ef 7190 .[...t...q.....
0050edc0: 3e6c 1f97 9fe7 726c 368f 1c78 63df a10c >1....rl6..xc...
0050edd0: 1e3f b46c 052c bdb2 bd18 7063 cea1 5835 .?..l...pc..X5
0050ede0: 4b7c 6564 1bbe 9644 9458 86e8 d6b0 9724 K|ed...n.X...S
0050edf0: 1c2c df10 4001 0000 4e41 5449 5349 474e ...@...NATISIGN
```

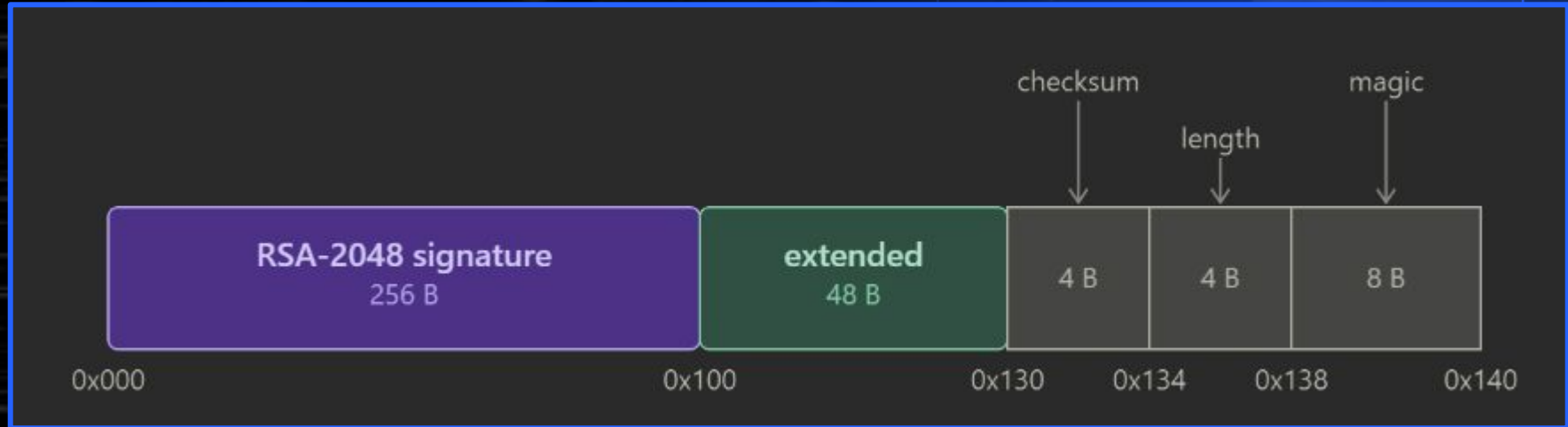
```
002c9ad0: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9ae0: 7b6f 41ff 56fc b0d2 a09a 8946 525c 4ed7 {oA.V.....FR\N.
002c9af0: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9b00: 7b6f 41ff 56fc b0d2 a09a 8946 525c 4ed7 {oA.V.....FR\N.
002c9b10: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9b20: 7b6f 41ff 56fc b0d2 a09a 8946 525c 4ed7 {oA.V.....FR\N.
002c9b30: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9b40: 7b6f 41ff 56fc b0d2 a09a 8946 525c 4ed7 {oA.V.....FR\N.
002c9b50: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9b60: 7b6f 41ff 56fc b0d2 a09a 8946 525c 4ed7 {oA.V.....FR\N.
002c9b70: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9b80: 7b6f 41ff 56fc b0d2 a09a 8946 525c 4ed7 {oA.V.....FR\N.
002c9b90: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9ba0: 7b6f 41ff 56fc b0d2 a09a 8946 525c 4ed7 {oA.V.....FR\N.
002c9bb0: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9bc0: 7b6f 41ff 56fc b0d2 a09a 8946 525c 4ed7 {oA.V.....FR\N.
002c9bd0: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9be0: 7b6f 41ff 56fc b0d2 a09a 8946 525c 4ed7 {oA.V.....FR\N.
002c9bf0: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9c00: 7b6f 41ff 56fc b0d2 a09a 8946 525c 4ed7 {oA.V.....FR\N.
002c9c10: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9c20: 7b6f 41ff 56fc b0d2 a09a 8946 525c 4ed7 {oA.V.....FR\N.
002c9c30: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9c40: 7b6f 41ff 56fc b0d2 a09a 8946 525c 4ed7 {oA.V.....FR\N.
002c9c50: c55d 63ca c92a d4e5 785b f537 a18c 9bf4 .]c...*.x[.7....
002c9c60: 7b6f 3309 a37e 5374 038c cd2c 8d9a 9b81 {o3...~St.....
002c9c70: 9503 6ddf 5572 9a53 5ff0 126f e5f4 4fa2 ..m.Ur.S_...o..O.
002c9c80: d4fd 1803 0000 0000 0000 5345 4c46 5349 .....SELEFSI
002c9c90: 474e GN
```



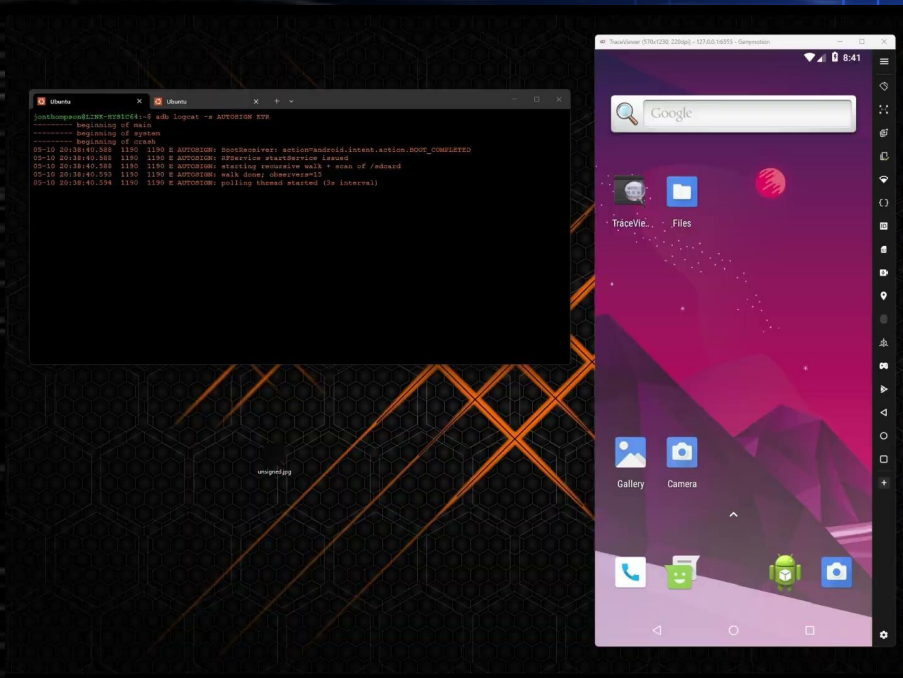
SELSIGN: 792-byte cryptographic media signature



NATISIGN: 320-byte cryptographic APK signature



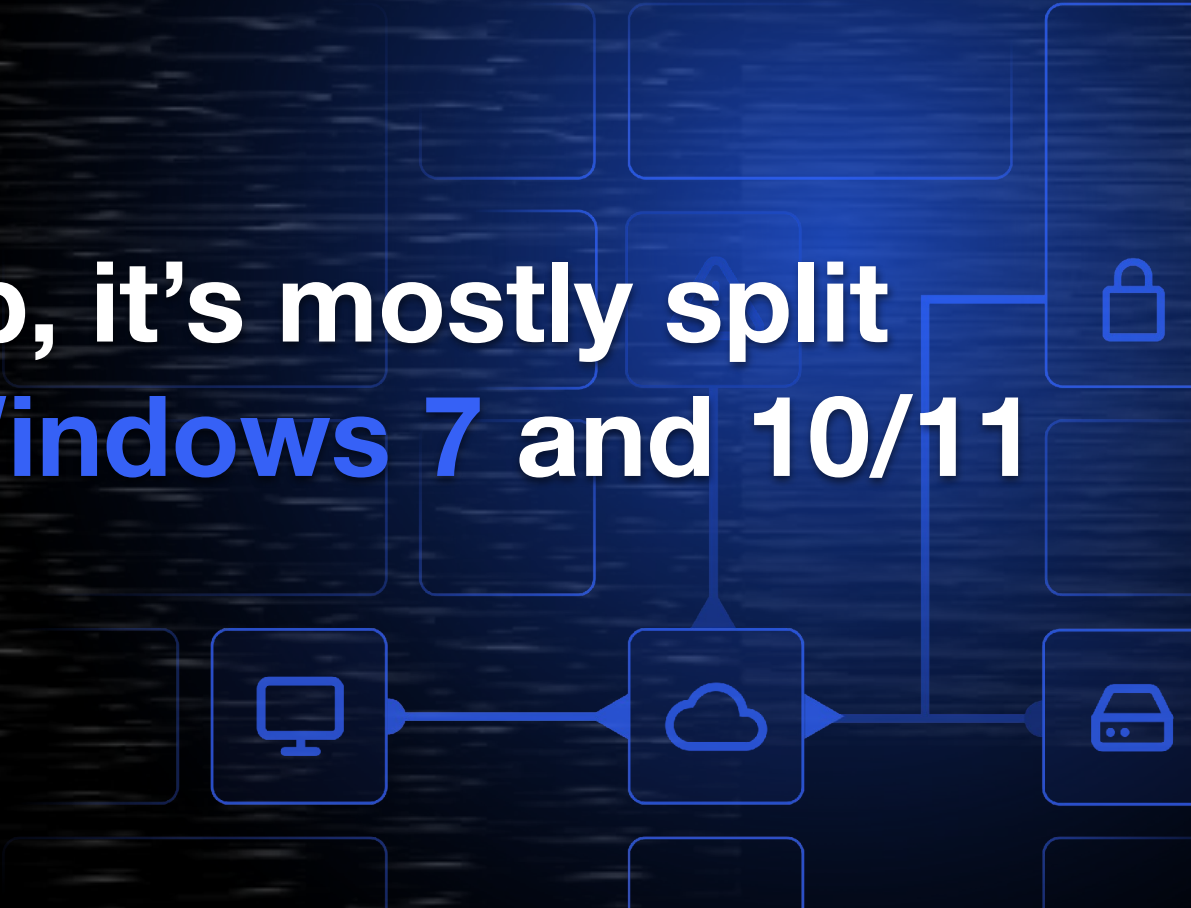
Traceviewer + RedFlag Demo



traceviewer_demo.mp4

DESKTOP

On desktop, it's mostly split
between **Windows 7** and 10/11



Exfil'd Data.

Operating System

Architecture: 32-bit
BuildNumber: 7600
Caption: Microsoft Windows 7 Professional

Input Details (InputSnapshot)

Code Pages

ACP: 950
OEMCP: 950

Locale IDs (LCIDs)

System: 1028 (0x0404)
User: 1033 (0x0409)
Thread: 1028 (0x0404)

Keyboard / IME

Layout Handle (HKL): 0x00000000E0200404
IME Description: 하 나 9.10
IME File: UniKorHn.ime

Process

Integrity Level: High (0x3000)
Collected at: 2026-04-28T07:40:04.1059435Z

Open DB Load Crypto Keys Refresh Export JSON

Sessions

Overview Timeline Host Details Command Outputs Raw Header

ProcessArchitecture: X86

Operating System

- Architecture: 32-bit
- BuildNumber: 7600
- Caption: Microsoft Windows 7 Professional

Hardware

- CPU
 - Cores: 2
 - LogicalProcessors: 4
 - Manufacturer: GenuineIntel
 - Name: Intel(R) Core(TM) i5-4300U CPU @ 1.90GHz
- Memory
 - FreePhysicalMemoryKb: 2697016
 - PagefileTotalKb: 6751860
 - TotalPhysicalBytes: 3457955488
 - TotalUsableMemoryKb: 3376812
- BIOS
 - Manufacturer: LENOVO

Input Details (InputSnapshot)

Code Pages

- ACP: 950
- OEMCP: 950

Locale IDs (LCIDs)

- System: 1028 (0x0404)
- User: 1033 (0x0409)
- Thread: 1028 (0x0404)

Keyboard / IME

- Layout Handle (HKL): 0x00000000E0200404
- IME Description: 하 나 9.10
- IME File: UniKorHn.ime

Process

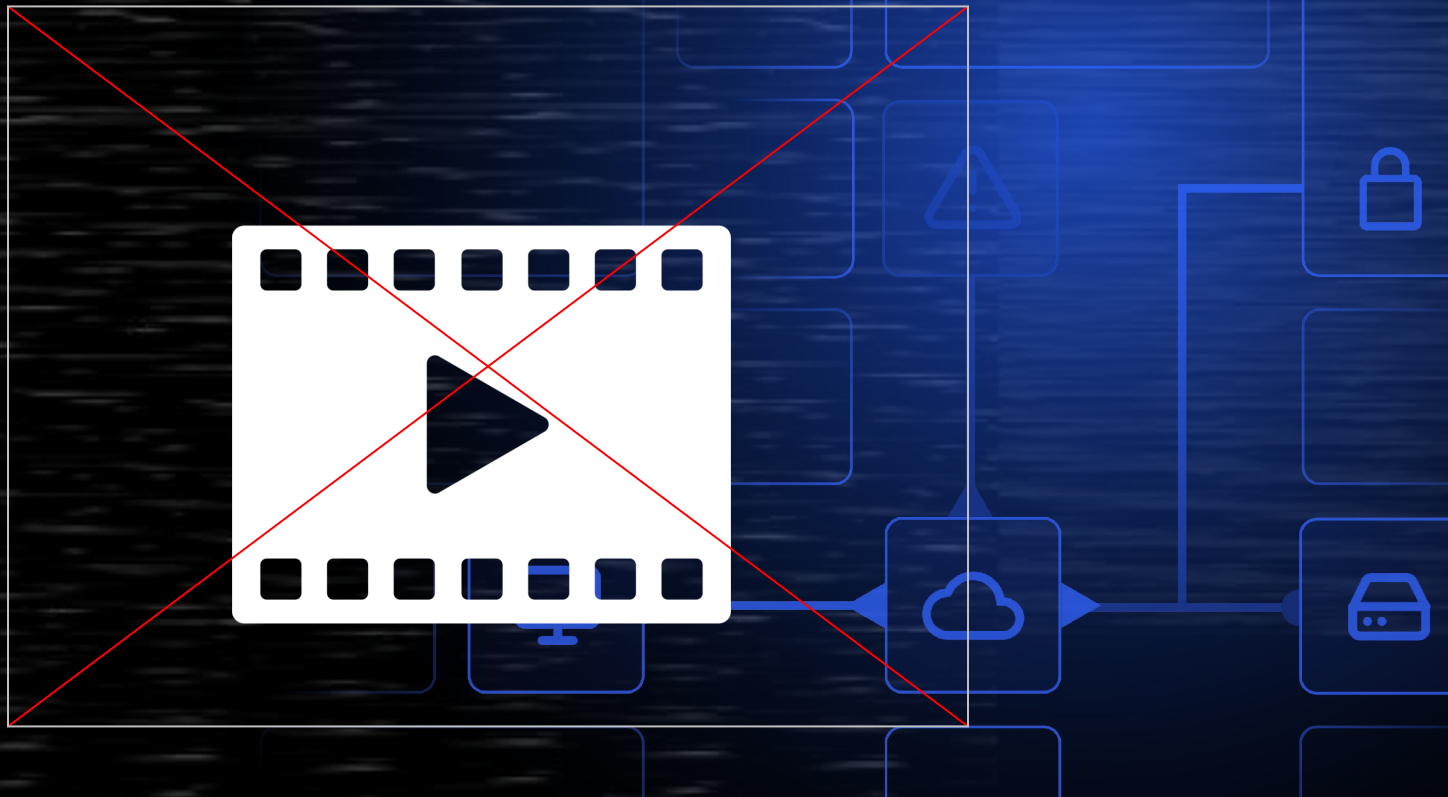
- Integrity Level: High (0x3000)
- Collected at: 2026-04-28T07:40:04.1059435Z

Keyboard / IME

- Layout Handle (HKL): 0x00000000E0200404
- IME Description: 하 나 9.10
- IME File: UniKorHn.ime

Internal Use Only

Hana IME



Hana IME:

Get OS version and modify the registry

```
110 if ((param_1 != 0) && (DAT_1014afc8 != 0)) {  
111     plVar7 = &DAT_1014afc8;  
112     uVar8 = uVar10;  
113     uVar9 = uVar10;  
114     do {  
115         if ((* (uint *) ((longlong) &DAT_1014afc0 + uVar9) & osMask) == osMask) {  
116             DAT_10086e28 = (HKEY) *plVar7;  
117             lVar6 = (longlong) (int) uVar8 * 0x3a8;  
118             WriteRecord(s_SYSTEM\CurrentControlSet\Control_1014afd0 + lVar6, &DAT_1014b0d0 + lVar6,  
119                 (LPCWSTR) (&DAT_1014b158 + lVar6), * (uint *) ((longlong) &DAT_1014b154 + uVar9),  
120                 * (DWORD *) ((longlong) &DAT_1014b150 + uVar9));  
121         }  
122         uVar10 = uVar10 + 1;  
123         uVar8 = (ulonglong) ((int) uVar8 + 1);  
124         uVar9 = uVar10 * 0x3a8;  
125         plVar7 = &DAT_1014afc8 + uVar10 * 0x75;  
126     } while ((&DAT_1014afc8)[uVar10 * 0x75] != 0);  
127 }  
128 FUN_10008010(param_1);  
129 FUN_10008290(param_1);  
130 return 0;  
131 }
```

OS bitmask from
jGetOSVersion

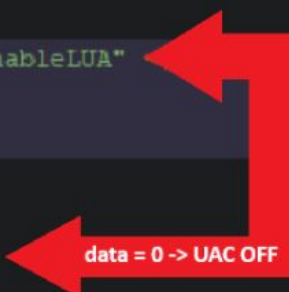
RegSetValueExA writes
EnableLUA = 0



Hana IME:

The hidden feature that no one asked for...

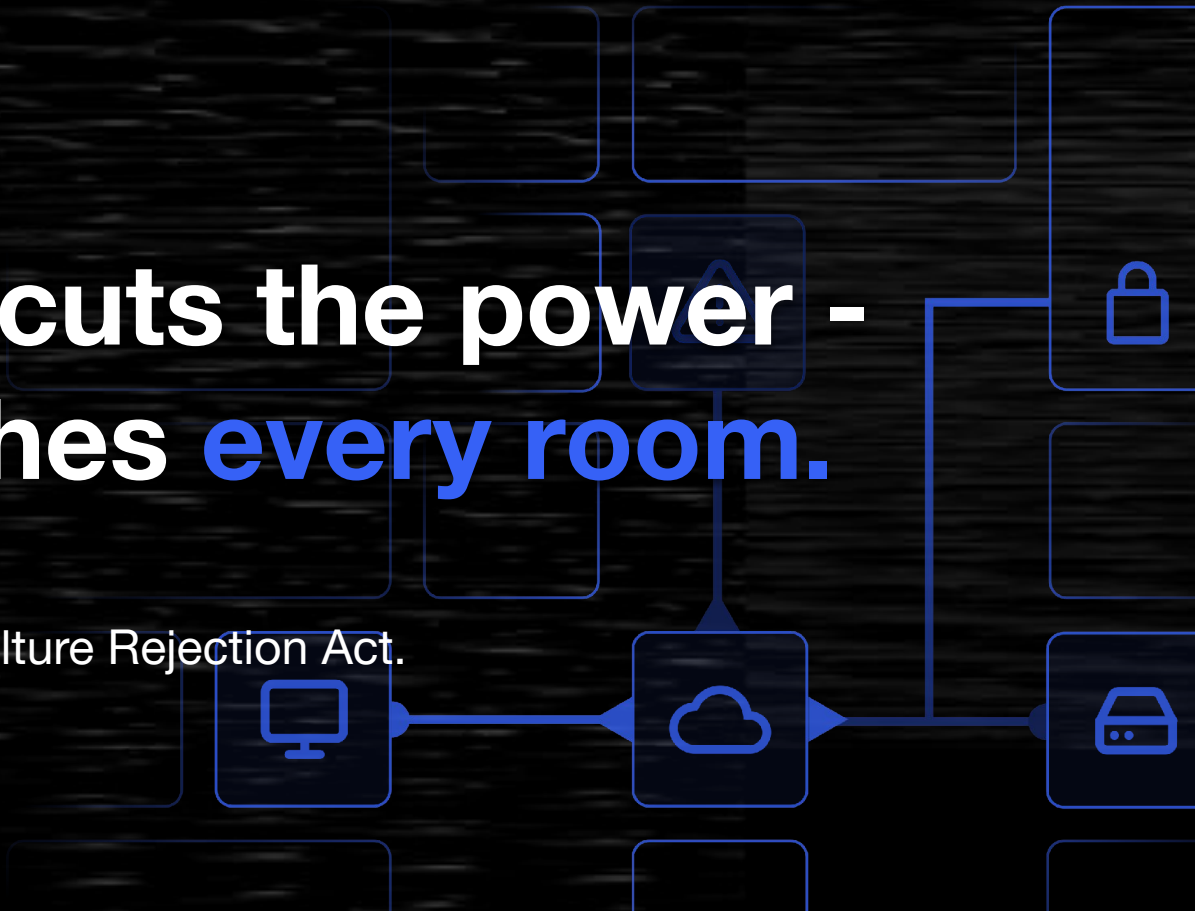
```
10155f40 0f ff 00 00 RegRecord
00 00 00
ff ff 02 ...
10155f40 0f ff 00 00 hana_dwordFF0Fh marker_lo
10155f44 00 00 ff ff hana_dwordFFFF0000h marker_hi
10155f48 02 00 00 80 ff hana_qwordFFFFFFFF80000002h hKey
ff ff ff
10155f50 53 4f 46 54 57 char[256] "SOFTWARE\\Microsoft\\... keyPath
41 52 45 5c 4d
69 63 72 6f 73...
10156050 45 6e 61 62 6c char[128] "EnableLUA" valueName
65 4c 55 41 00
00 00 00 00 00...
101560d0 04 00 00 00 hana_dword4h dataSize
101560d4 04 00 00 00 hana_dword4h dataType
101560d8 00 00 00 00 00 hana_byt... " data
00 00 00 00 00
00 00 00 00 00
```



2020

Group 109 cuts the power - then searches **every room.**

Reactionary Ideology & Culture Rejection Act.



MONITORING

Bureau 27 hunts smuggled phones by their radio signals

New detection methods can catch sub-minute calls



Distribution can mean the death penalty.

Roving inspection units · warrantless raids · device seizures



III. THE CRACKS

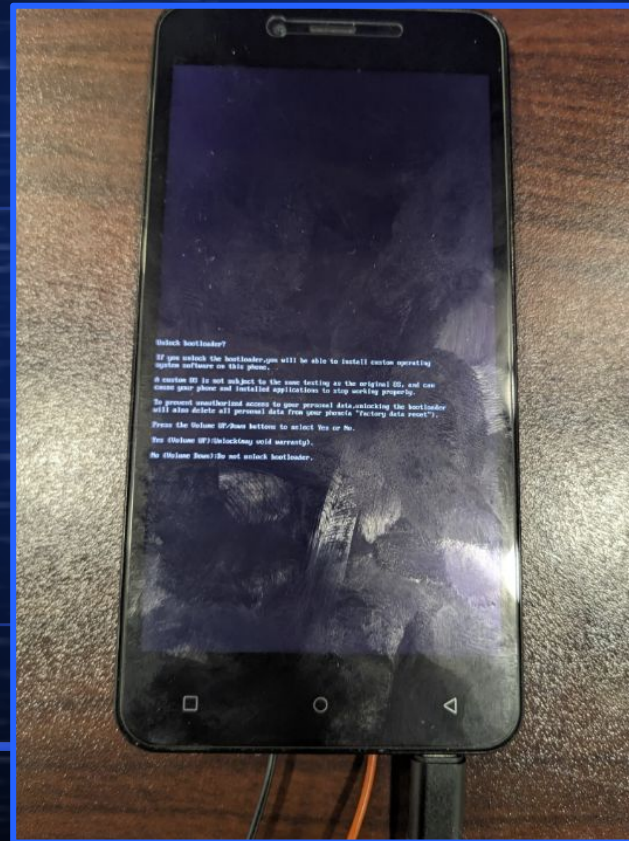
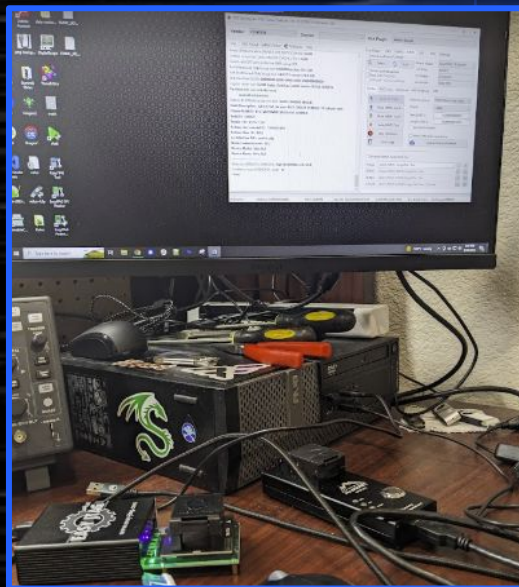
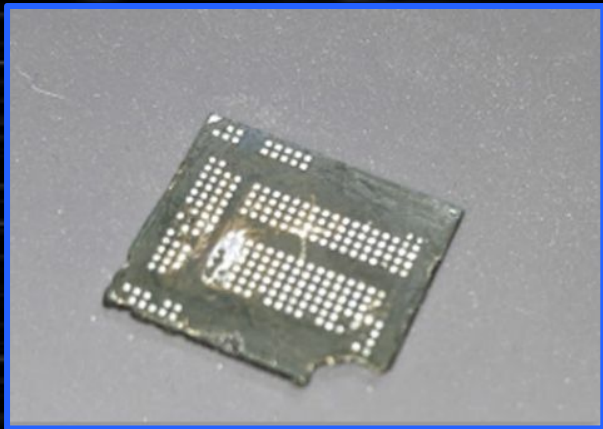
How people beat the system anyway



Smuggled media



Trial and error

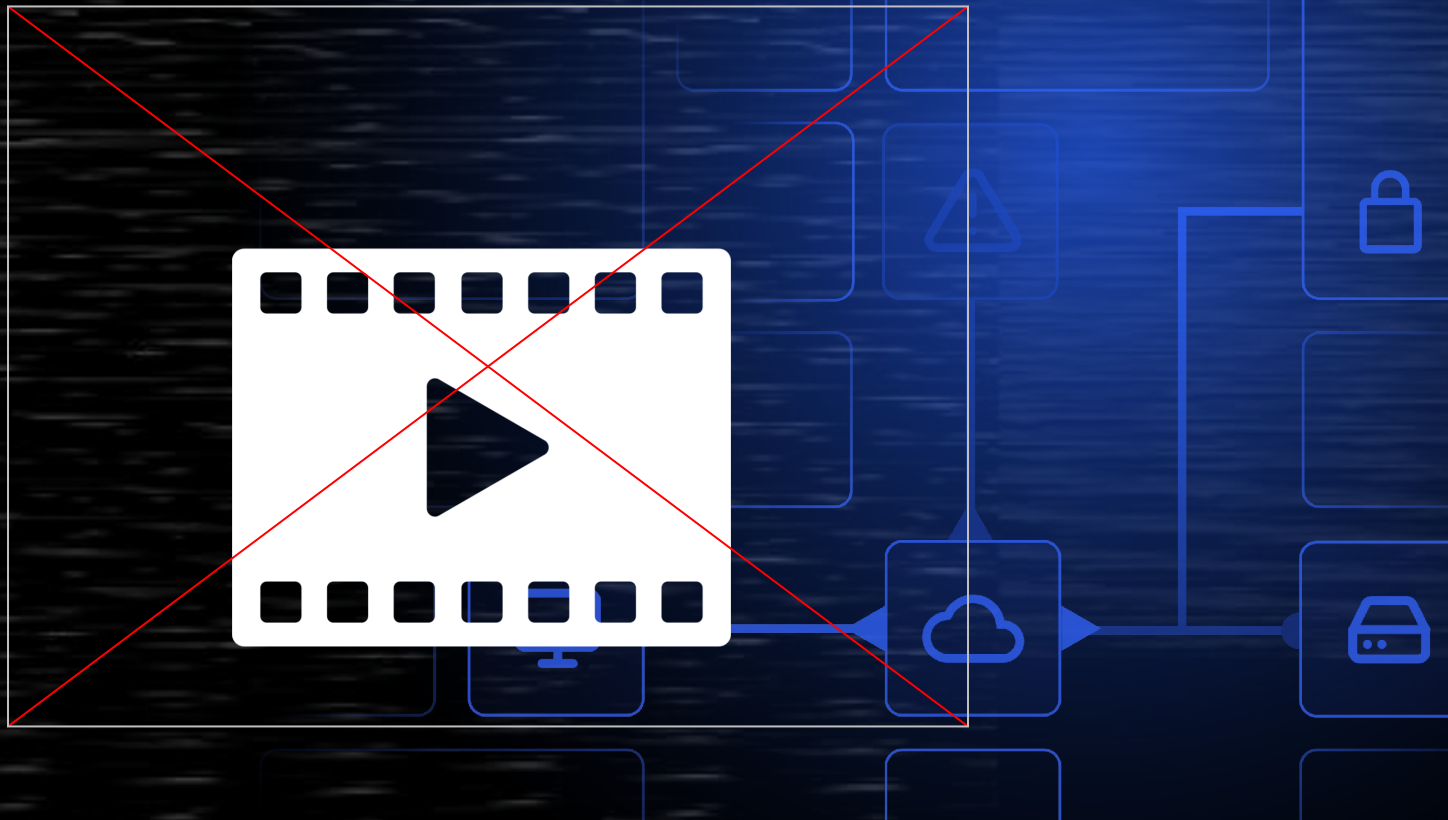


“Pigeon” Self-sign to beat the check.

Self-signing media to defeat RedFlag’s signature enforcement.



Pigeon



Contextual anti-forensic tools



Product Activation Required
This CD may be used as an emergency boot disk.
Retrieve files, scan for viruses, check for errors, and restore
backup images with Symantec Recovery Disk. 256 MB RAM required.
Please see manual for instructions.

Copyright © 2005 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, Ghost, and Norton Ghost are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Windows is a registered trademark of Microsoft Corporation. Other names may be trademarks of their respective owners. Printed in Ireland.

9/05 10440176-IN

IV. THE GAPS

The support system is collapsing



The biggest crisis for the movement **since the 1990s.**

But a small community of defectors, activists, and technologists persists.



V. OUR WORK

What we're doing about it



What we've built so far...

4

Software projects in active development

68

Defector user tests in 2025

SECURITY

The primary design requirement in all of our products

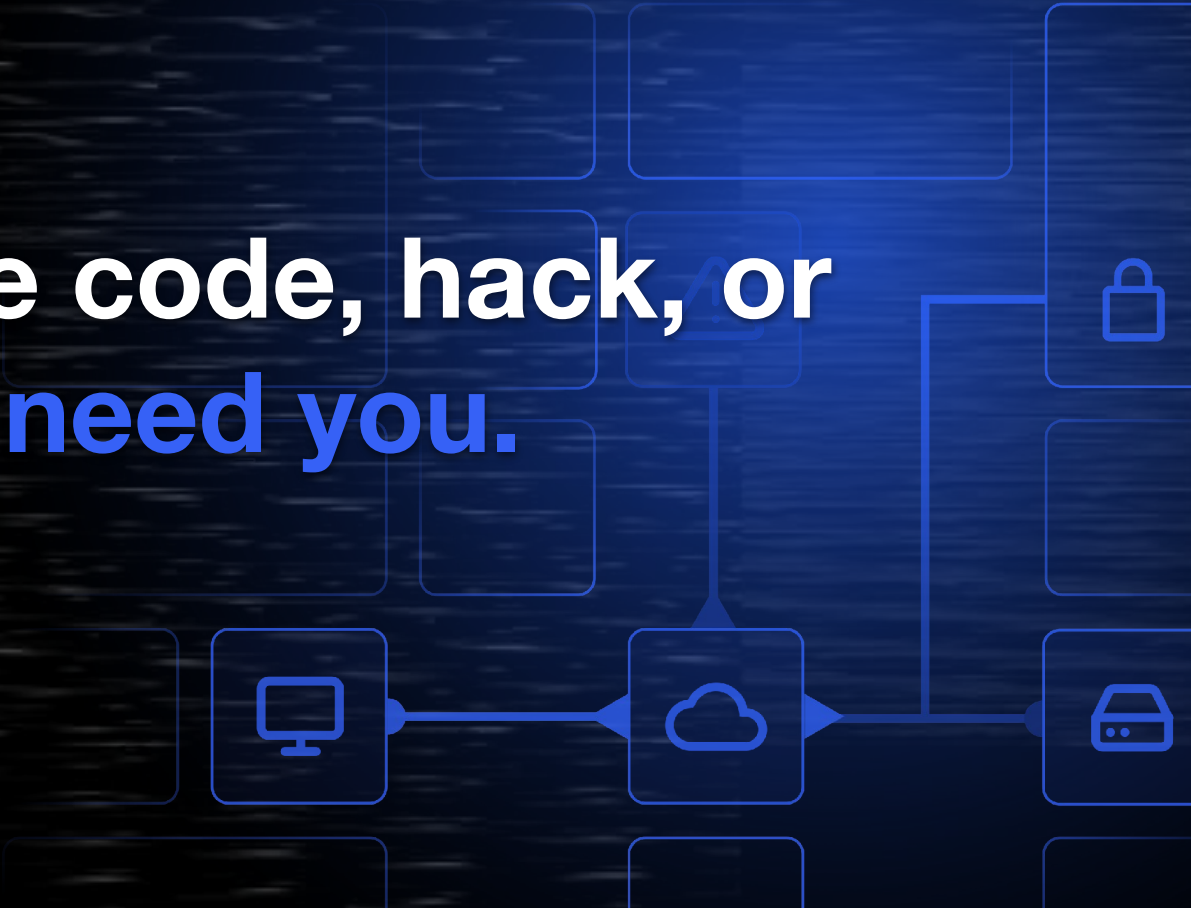


VI. THE ASK

This is where you come in



If you write code, hack, or
build - **we need you.**

A network diagram is visible in the background, consisting of blue lines connecting various nodes. Some nodes contain icons: a monitor, a cloud, a server, and a padlock. The diagram is set against a dark blue background with a subtle grid pattern.

What you'd work on.

PHONE EXPLOITS

Root, unlock, and exploit NK handsets

EMBEDDED SYSTEMS

Hardware analysis, application development, censorship bypass

AI

Scale analysis, future state, application development

DIRECT-TO-CELL

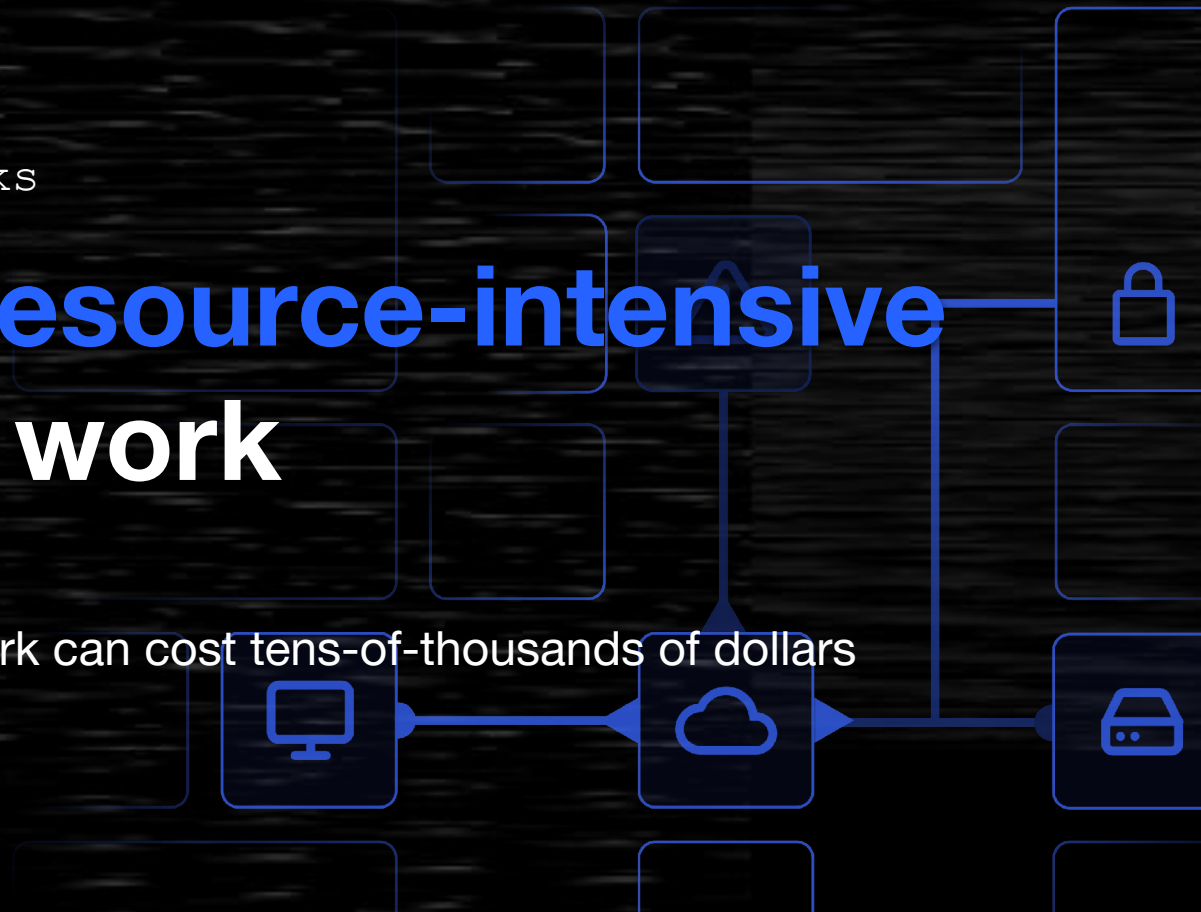
Reach devices independent of the state network



Di\$tribution Networks

The most **resource-intensive** part of our work

Developing a single network can cost tens-of-thousands of dollars





“LiNK is developing technology to break barriers which I have no doubt will create a free world for North Koreans. I promise to contribute in whatever small way I can until the day when our dreams of a beautiful society and freedom in North Korea come true.”

- Jang Hyeok, escaped NK in 2019

 volunteer.libertyinnorthkorea.org

 volunteers@libertyinnorthkorea.org



Scan to volunteer!



THANK YOU