

Appendix 2

1) TV Peppa Pig (pname: kr.co.smartstudy.peppapig1.en_googlemarket)

This app was identified as Android.Adware.SKplanet, Android.Trojan.Generic, Android.Adware.InMobiAd that has some malicious activities, such as obtain SIM serial number, obtain SIM status, read phone number, enable camera automatically, connect to the Internet, image capture, make phone call, and send out phone information, etc.

a) Obtain SIM serial number

```
String s3 = (new  
StringBuilder()).append(telephonymanager.getSimSerialNumber()).toString();
```

b) Obtain SIM status

```
com.feelingk.lguiab.b.i.c((new StringBuilder("USIM \uC0C1\uD0DC :  
")).append(telephonymanager.getSimState()).toString());
```

c) Read phone number

```
String s1 = ((TelephonyManager) getSystemService("phone")).getLine1Number();
```

d) Enable camera automatically

```
D = Camera.open();
```

e) Connect to the Internet

```
URL url = new URL(s);  
URLConnection httpURLConnection = (URLConnection)url.openConnection();  
httpURLConnection.setConnectTimeout(3000);  
httpURLConnection.setRequestMethod("GET");  
httpURLConnection.connect();
```

f) Image capture

```
intent2 = new Intent("android.media.action.IMAGE_CAPTURE");
```

g) Make phone call

```
Intent intent = new Intent("android.intent.action.DIAL", Uri.parse(s1));
```

h) Send out phone information

```
Intent intent = new Intent("android.intent.action.SEND");
```

2) 周星馳電影 (pname: e8888.ccss)

This app was identified as Android.Adware.Adwo, Android.Adware.Domob that has some malicious activities, such as enable voice record automatically, connect to the Internet, and make phone call, etc.

a) Enable voice record automatically

```
___ = new MediaRecorder();
```

b) Connect to the Internet

```
AdUtil.a(httpURLConnection, activity(getApplicationContext()));  
httpURLConnection.setInstanceFollowRedirects(false);  
httpURLConnection.connect();  
i = httpURLConnection.getResponseCode();
```

c) Make phone call

```
Intent intent5 = new Intent("android.intent.action.DIAL", uri);
```

3) 週末影院 (pname: e8888.sat_mov)

This app was identified as Android.Adware.Adwo, Android.Adware.Domob, Android.Trojan.Generic that has some malicious activities, such as enable voice record automatically, connect to the Internet, and make phone call, etc.

a) Enable voice record automatically

```
___ = new MediaRecorder();
```

b) Connect to the Internet

```
AdUtil.a(httpURLConnection, activity(getApplicationContext()));  
httpURLConnection.setInstanceFollowRedirects(false);  
httpURLConnection.connect();  
i = httpURLConnection.getResponseCode();
```

c) Make phone call

```
Intent intent5 = new Intent("android.intent.action.DIAL", uri);
```

4) 2014 年開運寶典完整版-獨家開運轉運秘笈，讓你馬年行好運！ (pname: oms.mmc.fortunetelling.shengxiao.master_chen)

This app was identified as Android.Adware.AdMogo, Android.Adware.Adwo that has malicious activities, such as obtain SIM serial number, obtain SIM status, read phone number, connect to the

Internet, send out phone information, and make phone call, etc.

a) Obtain SIM serial number

```
b.g = telephonymanager.getSimSerialNumber();
```

b) Obtain SIM status

```
b.h = String.valueOf(telephonymanager.getSimState());
```

c) Read phone number

```
telephonymanager.getLine1Number();
```

d) Connect to the Internet

```
URL url = new URL(s);  
HttpURLConnection httpURLConnection = (HttpURLConnection)url.openConnection();  
httpURLConnection.setConnectTimeout(2000);  
httpURLConnection.setRequestMethod("GET");  
httpURLConnection.connect();
```

e) Send out phone information

```
Intent intent = new Intent("android.intent.action.SEND");
```

f) Make phone call

```
Intent intent5 = new Intent("android.intent.action.DIAL", Uri.parse(s1));
```

5) 猛男让女人满足到巅峰的 69 式 (pname: com.ffff.xxxpronvideos)

This app was identified as Android.Adware.AirPush, Android.Adware.MobWIN that has malicious activities, such as obtain SIM serial number, obtain SIM status, enable voice record automatically, connect to the Internet, image capture, make phone call, and send out phone information, etc.

a) Obtain SIM serial number

```
s1 = (new  
StringBuilder(String.valueOf(s))).append("&deviceId=").append(com.fxxkj.fml.e.  
e.a(telephonymanager.getSimSerialNumber())).toString();
```

b) Obtain SIM status

```
telephonymanager.getSimState();
```

c) Enable voice record automatically

```
b = new MediaRecorder();
```

d) Connect to the Internet

```
StringBuilder stringBuilder = new StringBuilder();
HttpURLConnection httpURLConnection = a(context, s, i, j);
httpURLConnection.connect();
BufferedReader bufferedReader = new BufferedReader(new
InputStreamReader(httpURLConnection.getInputStream()));
```

e) Image capture

```
Intent intent = new Intent("android.media.action.IMAGE_CAPTURE");
```

f) Make phone call

```
intent1 = new Intent("android.intent.action.DIAL", Uri.parse((new
StringBuilder()).append("tel:").append(number).toString()));
```

g) Send out phone information

```
Intent intent = new Intent("android.intent.action.SEND");
```

6) Race Illegal: High Speed 3D (pname: com.herocraft.game.raceillegal)

This app was identified as Android.Adware.Domob, Android.Trojan.Generic that has malicious activities, such as read phone number, enable Bluetooth automatically, enable voice record automatically, connect to the Internet, make phone call, image capture, send out phone information, and read phone content, etc.

a) Read phone number

```
s3 = ((TelephonyManager)c.getSystemService("phone")).getLineNumber();
```

b) Enable Bluetooth automatically

```
bluetoothadapter = BluetoothAdapter.getDefaultAdapter();
```

c) Enable voice record automatically

```
mRecorder = new MediaRecorder();
```

d) Connect to the Internet

```
com.google.ads.util.b.a((new StringBuilder()).append("Pinging URL:
").append(b).toString());
httpURLConnection = a(new URL(b));
AdUtil.a(httpURLConnection, a);
httpURLConnection.setInstanceFollowRedirects(true);
httpURLConnection.connect();
```

e) Make phone call

```
Intent intent = new Intent("android.intent.action.DIAL",  
Uri.parse(sl.toString()));
```

f) Image capture

```
intent = new Intent("android.media.action.IMAGE_CAPTURE");
```

g) Send out phone information

```
intent = new Intent("android.intent.action.SEND");
```

h) Read phone content

```
Intent intent = new Intent("android.intent.action.GET_CONTENT");
```

7) Bubble Mania (pname: com.appgame7.bubblemania)

This app was identified as Android.AdWare.Leadbolt, Adware.Android.AirPush, Android.Trojan.Generic that has malicious activities, such as obtain SIM status, read phone number, connect to the Internet, send out phone information, modify user data, image capture, and make phone call, etc.

a) Obtain SIM status

```
telephonymanager.getSimState();
```

b) Read phone number

```
f = telephonymanager.getLine1Number();
```

c) Connect to the Internet

```
URLConnection httpurlconnection = (URLConnection)(new  
URL(val$imageURL)).openConnection();  
httpurlconnection.setDoInput(true);  
httpurlconnection.connect();  
Bitmap bitmap = BitmapFactory.decodeStream(httpurlconnection.getInputStream());
```

d) Send out phone information

```
intent = new Intent("android.intent.action.SEND");
```

e) Modify user data

```
intent = new Intent("android.intent.action.EDIT");
```

f) Image capture

```
intent2 = new Intent("android.media.action.IMAGE_CAPTURE");
```

g) Make phone call

```
Intent intent = new Intent("android.intent.action.DIAL", Uri.parse((new  
StringBuilder()).append("tel:").append(s).toString()));
```

8) 捕鱼达人 2 FREE (pname: com.play.buyudarxl2)

This app was identified as Android.Trojan.Generic, Android.Riskware.SmsReg, Android.Adware.TapjoyAds that has malicious activities, such as obtain SIM status, read phone number, enable wifi automatically, connect to the Internet, send out phone information, make phone call, and image capture, etc.

a) Obtain SIM status

```
mTelephonyManager.getSimState()
```

b) Read phone number

```
d = telephonymanager.getLine1Number();
```

c) Enable wifi automatically

```
wifimanager.setWifiEnabled(false);
```

d) Connect to the Internet

```
com.google.ads.util.b.a((new StringBuilder()).append("Pinging URL:  
").append(b).toString());  
httpurlconnection = a(new URL(b));  
AdUtil.a(httpurlconnection, a);  
httpurlconnection.setInstanceFollowRedirects(true);  
httpurlconnection.connect();
```

e) Send out phone information

```
intent2 = new Intent("android.intent.action.SENDTO", Uri.parse((new  
StringBuilder("sms:")).append((String)i.h().get(0)).toString()));
```

f) Make phone call

```
intent = new Intent("android.intent.action.DIAL", Uri.parse((new  
StringBuilder("tel:")).append((String)i.h().get(0)).toString()));
```

g) Image capture

```
Intent intent = new Intent("android.media.action.IMAGE_CAPTURE");
```