

“ ”



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>
```

```

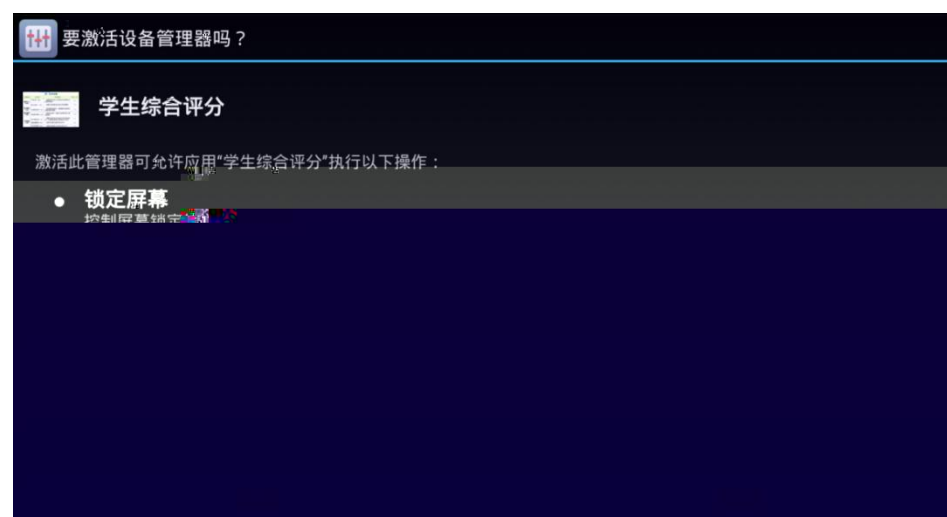
public class MyAdmin
    extends DeviceAdminReceiver {

    @Override
    public void onDisabled() {
        super.onDisabled();
        new a().a("已被取消激活");
    }

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

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

```



```

localg = new BeckhamOwenUtil();
localg.<init>();
if (((BeckhamOwenUtil.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));
    localObject1 = str;
    if (str.length() > 100) {
        str = str.substring(0, 100);
    }
}

```


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

★★★★★

尝试查询用户信息

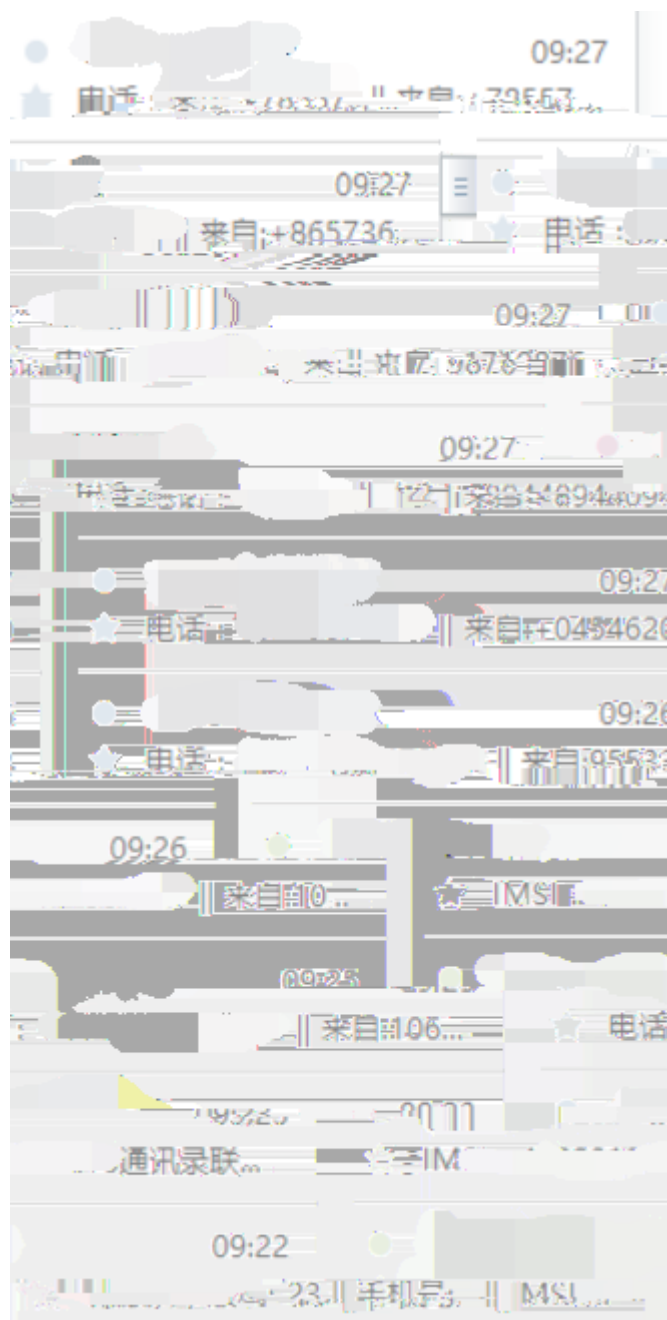
危险等级

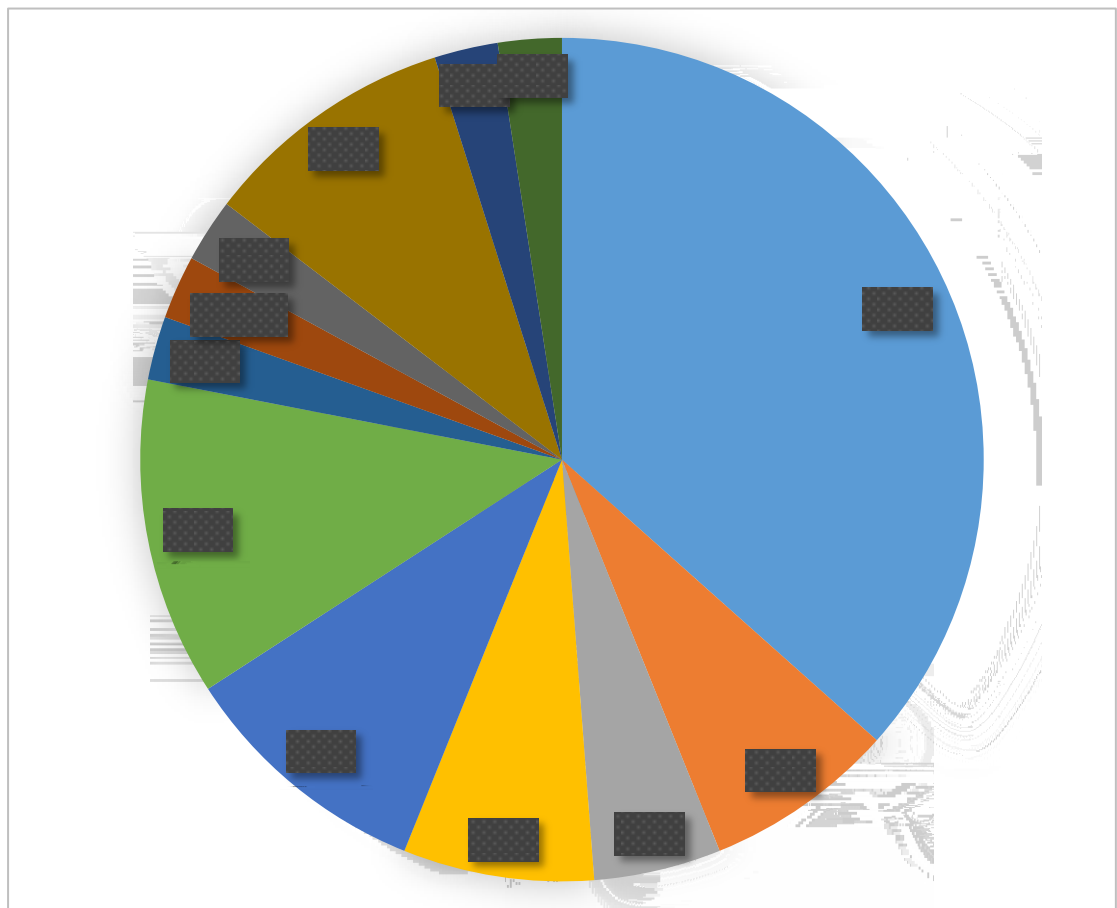
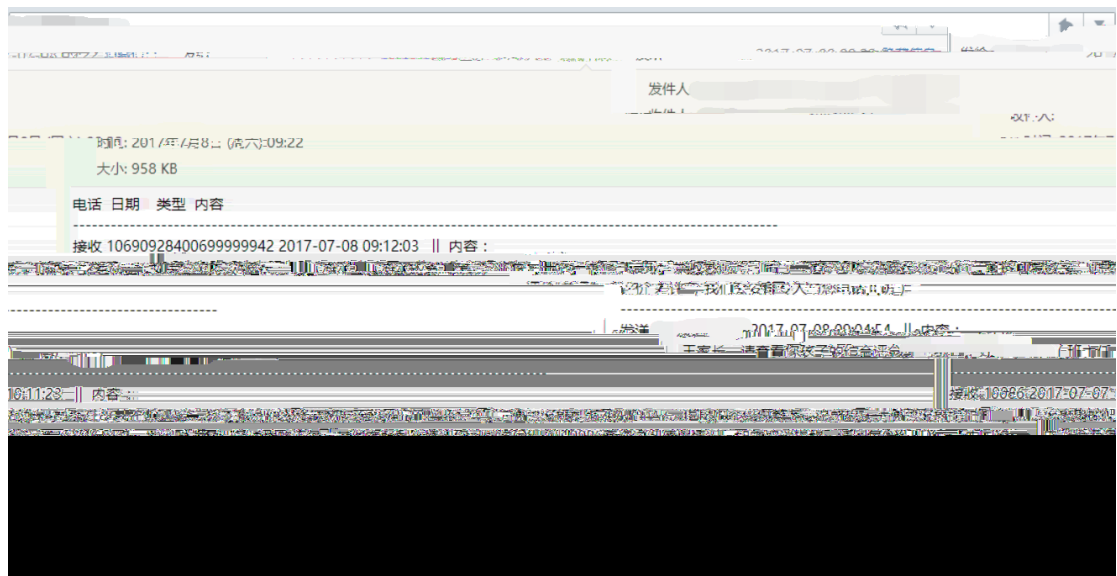
★★★★★

尝试读取设备信息

危险等级

★★★★★





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.*.*		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.*.*		