MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

e家平安 3.4.APK

APP名称:	e家平安
包名:	com.akson.business.epingantl.activity
域名线索:	22条
URL线索:	37条
邮箱线索:	0条
分析日期:	2022年2月2日 22:09

文件信息

文件名: pinganxinejia.apk
文件大小: 6.37MB
MD5值: d653b6ed4912025846f72916fbed3b8c
SHA1值: 9e2bf0ad3bf1e3dbae1aa2da27ecb2c8dad54d53
SHA256值: 99230be0f1067dcbf8c0d543b8a9fdcc9fd8f4c40d78c2afe17566e3bdab095b

APP 信息

App名称: e家平安
包名: com.akson.business.epingantl.activity
主活动**Activity:** com.akson.business.epingantl.activity.SplashActivity
安卓版本名称: 3.4
安卓版本: 3

域名线索

域名	是否危险域名	服务器信息
api.exc.mob.com	good	**IP:** 203.107.55.19 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map

域名	是否危险域名	服务器信息
api.share.mob.com	good	IP: 203.107.55.19 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
graph.qq.com	good	IP: 113.96.208.232 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
www.baidu.com	good	IP: 110.242.68.4 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 查看地图: Google Map
xmlpull.org	good	IP: 74.50.61.58 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204 查看地图: Google Map

域名	是否危险域名	服务器信息
www.openmobilealliance.org	good	IP: 104.26.9.105 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map
www.ejpingan.com	good	没有服务器地理信息.
xml.apache.org	good	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map
www.wireless-village.org	good	IP: 172.67.131.214 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map
www.w3.org	good	IP: 128.30.52.100 所属国家: United States of America 地区: Massachusetts 城市: Cambridge 纬度: 42.365078 经度: -71.104523 查看地图: Google Map

域名	是否危险域名	服务器信息
one.pingan.com	good	IP: 43.230.223.2 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
cca.mob.com	good	IP: 115.227.43.65 所属国家: China 地区: Zhejiang 城市: Taizhou 纬度: 28.666668 经度: 121.349998 查看地图: Google Map
l.mob.com	good	IP: 203.107.55.19 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
up.sharesdk.cn	good	IP: 115.227.43.65 所属国家: China 地区: Zhejiang 城市: Taizhou 纬度: 28.666668 经度: 121.349998 查看地图: Google Map

域名	是否危险域名	服务器信息
devs.data.mob.com	good	**IP:** 203.107.55.19 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map
openmobile.qq.com	good	**IP:** 113.96.208.233 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
www.myapp.com	good	**IP:** 182.254.51.124 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
home.pingan.com.cn	good	**IP:** 124.196.49.17 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.pingan.com	good	IP: 202.69.26.11 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
api.weixin.qq.com	good	IP: 81.69.216.43 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
www.mob.com	good	IP: 116.62.130.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
schemas.xmlsoap.org	good	IP: 184.30.11.185 所属国家: United States of America 地区: Massachusetts 城市: Cambridge 纬度: 42.363598 经度: -71.085205 查看地图: Google Map

URL线索

URL信息	Url所在文件
http://cca.mob.com:80/ca	com/mob/commons/appcollector/PackageCollector.java
http://cca.mob.com:80/ca	com/mob/commons/appcollector/RuntimeCollector.java
http://cca.mob.com:80/caconf	com/mob/commons/appcollector/a.java
http://api.exc.mob.com:80	com/mob/commons/logcollector/c.java
http://devs.data.mob.com:80/dinfo	com/mob/commons/authorize/a.java
http://devs.data.mob.com:80/dsign	com/mob/commons/authorize/a.java
http://devs.data.mob.com/macinfo	com/mob/commons/iosbridge/UDPServer.java
http://devs.data.mob.com/udpsconf	com/mob/commons/iosbridge/UDPServer.java
https://.*:	com/unionpay/uppay/net/HttpConnection.java
http://www.baidu.com	com/unionpay/uppay/net/a.java
http://www.ejpingan.com:8080/pingane	com/akson/business/epingantl/http/Https.java
http://www.ejpingan.com:8080/pingane/DaoServlet.do	com/akson/business/epingantl/http/Https.java
http://www.ejpingan.com:8080/	com/akson/business/epingantl/http/Https.java
http://www.ejpingan.com:8080/pingane/notice/notice.jsp	com/akson/business/epingantl/http/Https.java

URL信息	Url所在文件
http://www.ejpingan.com:8080/pingane/	com/akson/business/epingantl/http/Https.java
http://www.ejpingan.com:8080/pinganeserviceSys/AndroidManifest.xml	com/akson/business/epingantl/help/Help.java
http://www.ejpingan.com:8080/WS_WAP_PAYWAP-JAVA-UTF-8/index.jsp?zzjgbh=	com/akson/business/epingantl/help/Help.java
http://one.pingan.com/@#$	com/akson/business/epingantl/help/Value.java
http://home.pingan.com.cn/@#$	com/akson/business/epingantl/help/Value.java
www.pingan.com/YZ查询	com/akson/business/epingantl/help/Value.java
http://www.ejpingan.com:8080/WS_WAP_PAYWAP-JAVA-UTF-8/	com/akson/business/epingantl/help/Config.java
http://www.ejpingan.com:8080/WS_WAP_PAYWAP-JAVA-UTF-8/policyInfo.jsp?xzbh=	com/akson/business/epingantl/help/HelpTwo.java
http://www.ejpingan.com:8080/pingane/H/hnews.jsp?id=	com/akson/business/epingantl/help/HelpTwo.java
http://www.ejpingan.com:8080/pinganeserviceSys/AndroidManifest.xml	com/akson/business/epingantl/help/HelpTwo.java
http://www.ejpingan.com:8080/pingane/H/hnews.jsp?id=	com/akson/business/epingantl/activity/TextMessageActivity.java
http://www.ejpingan.com:8080/pingane/clause/P0141A16.htm	com/akson/business/epingantl/activity/WebActivity.java
http://www.ejpingan.com:8080/pingane/clause/	com/akson/business/epingantl/activity/WebActivity.java
http://www.ejpingan.com:8080/pinganeserviceSys/AndroidManifest.xml	com/akson/business/epingantl/activity/LoginActivity.java
http://www.ejpingan.com:8080/pingane/papay/pay.jsp?access_token=	com/akson/business/epingantl/activity/InputMoneyMessageActivity.java

URL信息	Url所在文件
http://www.ejpingan.com:8080/pinganeserviceSys/E-PingAntl.apk	com/akson/business/epingantl/utils/UpdateAPK.java
http://xmlpull.org/v1/doc/properties.html#xmldecl-standalone	org/kxml2/kdom/Document.java
http://www.w3.org/XML/1998/namespace	org/kxml2/wap/WbxmlParser.java
http://www.w3.org/2000/xmlns/	org/kxml2/wap/WbxmlParser.java
http://www.	org/kxml2/wap/wml/Wml.java
https://www.	org/kxml2/wap/wml/Wml.java
http://www.wireless-village.org/CSP	org/kxml2/wap/wv/WV.java
http://www.wireless-village.org/PA	org/kxml2/wap/wv/WV.java
http://www.wireless-village.org/TRC	org/kxml2/wap/wv/WV.java
http://www.openmobilealliance.org/DTD/WV-CSP	org/kxml2/wap/wv/WV.java
http://www.openmobilealliance.org/DTD/WV-PA	org/kxml2/wap/wv/WV.java
http://www.openmobilealliance.org/DTD/WV-TRC	org/kxml2/wap/wv/WV.java
www.wireless-village.org	org/kxml2/wap/wv/WV.java
http://xmlpull.org/v1/doc/features.html#indent-output	org/kxml2/io/KXmlSerializer.java
http://www.w3.org/XML/1998/namespace	org/kxml2/io/KXmlSerializer.java

URL信息	Url所在文件
http://xmlpull.org/v1/doc/	org/kxml2/io/KXmlParser.java
http://www.w3.org/XML/1998/namespace	org/kxml2/io/KXmlParser.java
http://www.w3.org/2000/xmlns/	org/kxml2/io/KXmlParser.java
http://schemas.xmlsoap.org/soap/encoding/	org/ksoap2/SoapEnvelope.java
http://www.w3.org/2001/12/soap-encoding	org/ksoap2/SoapEnvelope.java
http://schemas.xmlsoap.org/soap/envelope/	org/ksoap2/SoapEnvelope.java
http://www.w3.org/2001/12/soap-envelope	org/ksoap2/SoapEnvelope.java
http://www.w3.org/2001/XMLSchema	org/ksoap2/SoapEnvelope.java
http://www.w3.org/1999/XMLSchema	org/ksoap2/SoapEnvelope.java
http://www.w3.org/2001/XMLSchema-instance	org/ksoap2/SoapEnvelope.java
http://www.w3.org/1999/XMLSchema-instance	org/ksoap2/SoapEnvelope.java
http://xml.apache.org/xml-soap	org/ksoap2/serialization/MarshalHashtable.java
http://xmlpull.org/v1/doc/features.html#process-docdecl	org/xmlpull/v1/XmlPullParser.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	org/xmlpull/v1/XmlPullParser.java
http://xmlpull.org/v1/doc/features.html#report-namespace-prefixes	org/xmlpull/v1/XmlPullParser.java

URL信息	Url所在文件
http://xmlpull.org/v1/doc/features.html#validation	org/xmlpull/v1/XmlPullParser.java
http://api.share.mob.com:80	cn/sharesdk/framework/b/c.java
http://up.sharesdk.cn/upload/image	cn/sharesdk/framework/b/c.java
http://l.mob.com/url/ShareSdkMapping.do	cn/sharesdk/framework/b/c.java
https://){1}	cn/sharesdk/framework/b/a.java
http://www.myapp.com/down/	cn/sharesdk/tencent/qq/n.java
http://openmobile.qq.com/api/check?	cn/sharesdk/tencent/qq/e.java
https://graph.qq.com	cn/sharesdk/tencent/qq/e.java
https://graph.qq.com/oauth2.0/me	cn/sharesdk/tencent/qq/e.java
https://graph.qq.com/user/get_simple_userinfo	cn/sharesdk/tencent/qq/e.java
https://graph.qq.com/oauth2.0/m_authorize?response_type=token&client_id=	cn/sharesdk/tencent/qq/e.java
https://graph.qq.com/photo/upload_pic	cn/sharesdk/tencent/qzone/f.java
https://graph.qq.com	cn/sharesdk/tencent/qzone/f.java
https://graph.qq.com/user/get_simple_userinfo	cn/sharesdk/tencent/qzone/f.java
https://graph.qq.com/oauth2.0/me	cn/sharesdk/tencent/qzone/f.java

URL信息	Url所在文件
https://graph.qq.com/oauth2.0/m_authorize?response_type=token&client_id=	cn/sharesdk/tencent/qzone/f.java
https://api.weixin.qq.com/sns/oauth2/access_token	cn/sharesdk/wechat/utils/h.java
https://api.weixin.qq.com/sns/userinfo	cn/sharesdk/wechat/utils/i.java
http://www.mob.com	Android String Resource

☷ 此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取

向手机申请的权限	是否危险	类型	详细情况
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。

向手机申请的权限	是否危险	类型	详细情况
android.permission.CHANGE_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率

签名证书

```
APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=AnHui, L=HeFei, O=Akson MobileGroup, OU=Akson Inc, CN=e-Pingan
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-05-20 07:15:44+00:00
Valid To: 2038-05-14 07:15:44+00:00
Issuer: C=CN, ST=AnHui, L=HeFei, O=Akson MobileGroup, OU=Akson Inc, CN=e-Pingan
Serial Number: 0x5199cda0
Hash Algorithm: sha1
md5: 53a1ee7a2a3fa3527f5ebe7a6cb952c9
sha1: f26f4ebf0bed2c122b5953bccf7afb0d5791356d
sha256: 518cd1080506f2f004e86d27948d34e303e985594636c9654f75b9257eae19b2
sha512: e66314f2835ecbfed19680258feb3a517c5f05a5a5e78246328c370e432c3595626df3c768eb2be45be60ae800ff306d78bc057af6660bd3736887ccfe393a7d
```

硬编码敏感信息

可能的敏感信息
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.mob.tools.MobUIShell	Schemes: tencent100371282://,

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>APK包</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.MANUFACTURER check
possible Build.SERIAL check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td><table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
possible Build.SERIAL check
SIM operator check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table></td></tr>
</table>

报告由 摸瓜平台 自动生成，并非包含所有检测结果，有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析