MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Alleviate day 2.9.APK

APP名称:	Alleviate day
包名:	com.yxxinglin.xzid108686
域名线索:	33条
URL线索:	27条
邮箱线索:	1条
分析日期:	2022年1月22日 17:43

文件信息

文件名: Alleviate day.apk
文件大小: 7.9MB
MD5值: c5c9cf627e0482575ab2a660fa7ee154
SHA1值: 85f2980ac19ad0314d7a97341a533de6b4f18329
SHA256值: 49a0cd3fd666cfc40ea1ec8e4dc845c9957ac9621abf2412824c46ac6fee7787

APP 信息

App名称: Alleviate day
包名: com.yxxinglin.xzid108686
主活动**Activity:** com.bufanapprn.MainActivity
安卓版本名称: 2.9
安卓版本: 1048580

域名线索

域名	是否危险域名	服务器信息
sdk.open.lbs.igexin.com	good	**IP:** 183.134.98.68 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
wspeed.qq.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
mta.qq.com	good	**IP:** 111.161.14.94 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map
pingma.qq.com	good	**IP:** 119.45.78.184 **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.android.com	good	没有服务器地理信息.
www.npes.org	good	**IP:** 216.33.126.92 **所属国家:** United States of America **地区:** Virginia **城市:** Vienna **纬度:** 38.926575 **经度:** -77.262360 **查看地图:** Google Map
purl.org	good	**IP:** 207.241.239.242 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.781734 **经度:** -122.459435 **查看地图:** Google Map

域名	是否危险域名	服务器信息
twitter.com	good	**IP:** 69.63.176.15 所属国家: United States of America 地区: California 城市: Menlo Park 纬度: 37.436935 经度: -122.193604 查看地图: Google Map
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
cgi.connect.qq.com	good	**IP:** 183.2.143.207 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map
c-hzgt2.getui.com	good	**IP:** 124.160.127.198 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
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
plus.google.com	good	IP: 47.88.58.234 所属国家: United States of America 地区: California 城市: San Mateo 纬度: 37.547424 经度: -122.330589 查看地图: Google Map
wx.tenpay.com	good	IP: 182.254.88.166 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
xml.org	good	IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246 查看地图: Google Map

域名	是否危险域名	服务器信息
ns.useplus.org	good	IP: 54.83.4.77 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.043720 经度: -77.487488 查看地图: Google Map
pinterest.com	good	IP: 69.63.176.59 所属国家: United States of America 地区: California 城市: Menlo Park 纬度: 37.436935 经度: -122.193604 查看地图: Google Map
iptc.org	good	IP: 3.64.29.21 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.115520 经度: 8.684170 查看地图: Google Map
www.facebook.com	good	IP: 31.13.82.33 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map

域名	是否危险域名	服务器信息
appsupport.qq.com	good	**IP:** 183.2.143.207 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000 **查看地图:** Google Map
c.isdspeed.qq.com	good	没有服务器地理信息.
d.gt.igexin.com	good	**IP:** 183.134.98.71 **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
ns.adobe.com	good	没有服务器地理信息.
www.aiim.org	good	**IP:** 199.60.103.225 **所属国家:** United States of America **地区:** Massachusetts **城市:** Cambridge **纬度:** 42.370129 **经度:** -71.086304 **查看地图:** Google Map
javax.xml.xmlconstants	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
xerces.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
fusion.qq.com	good	IP: 121.51.36.15 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
s-gt.getui.com	good	IP: 183.131.7.106 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
cipa.jp	good	IP: 118.82.81.189 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map

域名	是否危险域名	服务器信息
sdk.open.phone.igexin.com	good	IP: 183.131.7.102 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
qzs.qq.com	good	IP: 121.51.49.51 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
mta.oa.com	good	IP: 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690 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

URL线索

URL信息	Url所在文件
https://wx.tenpay.com	com/reactnativecommunity/webview/RNCWebViewManager.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/connect/common/b.java
http://ns.adobe.com/xmp/note/	c/b/c/v/c.java
http://ns.adobe.com/xap/1.0/	c/b/c/v/c.java
http://ns.adobe.com/xmp/extension/	c/b/c/v/c.java
http://bi.	c/e/d/d/o.java
http://config.	c/e/d/d/o.java
http://stat.	c/e/d/d/o.java
http://log.	c/e/d/d/o.java
http://lbs.	c/e/d/d/o.java
http://sdk.open.phone.igexin.com/api.php	c/e/d/d/a.java
http://c-hzgt2.getui.com/api.php	c/e/d/d/a.java
http://s-gt.getui.com/api.php	c/e/d/d/a.java
http://d.gt.igexin.com/api.htm	c/e/d/d/a.java

URL信息	Url所在文件
http://sdk.open.lbs.igexin.com/api.htm	c/e/d/d/a.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	c/f/b/b/k.java
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	c/f/b/b/f.java
http://openmobile.qq.com/oauth2.0/m_authorize?	c/f/b/b/f.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1	c/f/b/c/c.java
http://pingma.qq.com:80/mstat/report	c/f/e/a.java
http://pingma.qq.com:80/mstat/report	c/f/f/a/t.java
http://mta.qq.com/	c/f/f/a/v.java
http://mta.oa.com/	c/f/f/a/v.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	c/f/d/c/j.java
http://appsupport.qq.com/cgi-bin/appstage/mstats_batch_report	c/f/d/a/k.java
http://wspeed.qq.com/w.cgi	c/f/d/a/j.java
http://c.isdspeed.qq.com/code.cgi	c/f/d/a/d.java
http://ns.adobe.com/xap/1.0/	c/a/a/a/s.java
http://purl.org/dc/elements/1.1/	c/a/a/a/s.java

URL信息	Url所在文件
http://ns.adobe.com/xap/1.0/rights/	c/a/a/a/s.java
http://ns.adobe.com/pdf/1.3/	c/a/a/a/s.java
http://ns.adobe.com/photoshop/1.0/	c/a/a/a/s.java
http://ns.adobe.com/tiff/1.0/	c/a/a/a/s.java
http://ns.adobe.com/png/1.0/	c/a/a/a/s.java
http://www.w3.org/XML/1998/namespace	c/a/a/a/s.java
http://www.w3.org/1999/02/22-rdf-syntax-ns#	c/a/a/a/s.java
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	c/a/a/a/s.java
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	c/a/a/a/s.java
http://ns.adobe.com/DICOM/	c/a/a/a/s.java
http://ns.useplus.org/ldf/xmp/1.0/	c/a/a/a/s.java
http://ns.adobe.com/iX/1.0/	c/a/a/a/s.java
http://ns.adobe.com/xap/1.0/mm/	c/a/a/a/s.java
http://ns.adobe.com/xap/1.0/bj/	c/a/a/a/s.java
http://ns.adobe.com/xmp/note/	c/a/a/a/s.java

URL信息	Url所在文件
http://ns.adobe.com/pdfx/1.3/	c/a/a/a/s.java
http://www.npes.org/pdfx/ns/id/	c/a/a/a/s.java
http://www.aiim.org/pdfa/ns/schema#	c/a/a/a/s.java
http://www.aiim.org/pdfa/ns/property#	c/a/a/a/s.java
http://www.aiim.org/pdfa/ns/type#	c/a/a/a/s.java
http://www.aiim.org/pdfa/ns/field#	c/a/a/a/s.java
http://www.aiim.org/pdfa/ns/id/	c/a/a/a/s.java
http://www.aiim.org/pdfa/ns/extension/	c/a/a/a/s.java
http://ns.adobe.com/album/1.0/	c/a/a/a/s.java
http://ns.adobe.com/exif/1.0/	c/a/a/a/s.java
http://cipa.jp/exif/1.0/	c/a/a/a/s.java
http://ns.adobe.com/exif/1.0/aux/	c/a/a/a/s.java
http://ns.adobe.com/jpeg/1.0/	c/a/a/a/s.java
http://ns.adobe.com/jp2k/1.0/	c/a/a/a/s.java
http://ns.adobe.com/camera-raw-settings/1.0/	c/a/a/a/s.java

URL信息	Url所在文件
http://ns.adobe.com/StockPhoto/1.0/	c/a/a/a/s.java
http://ns.adobe.com/creatorAtom/1.0/	c/a/a/a/s.java
http://ns.adobe.com/asf/1.0/	c/a/a/a/s.java
http://ns.adobe.com/xmp/wav/1.0/	c/a/a/a/s.java
http://ns.adobe.com/bwf/bext/1.0/	c/a/a/a/s.java
http://ns.adobe.com/riff/info/	c/a/a/a/s.java
http://ns.adobe.com/xmp/1.0/Script/	c/a/a/a/s.java
http://ns.adobe.com/TransformXMP/	c/a/a/a/s.java
http://ns.adobe.com/swf/1.0/	c/a/a/a/s.java
http://ns.adobe.com/xmp/1.0/DynamicMedia/	c/a/a/a/s.java
http://ns.adobe.com/xmp/transient/1.0/	c/a/a/a/s.java
http://ns.adobe.com/xap/1.0/t/	c/a/a/a/s.java
http://ns.adobe.com/xap/1.0/t/pg/	c/a/a/a/s.java
http://ns.adobe.com/xap/1.0/g/	c/a/a/a/s.java
http://ns.adobe.com/xap/1.0/g/img/	c/a/a/a/s.java

URL信息	Url所在文件
http://ns.adobe.com/xap/1.0/sType/Font#	c/a/a/a/s.java
http://ns.adobe.com/xap/1.0/sType/Dimensions#	c/a/a/a/s.java
http://ns.adobe.com/xap/1.0/sType/ResourceEvent#	c/a/a/a/s.java
http://ns.adobe.com/xap/1.0/sType/ResourceRef#	c/a/a/a/s.java
http://ns.adobe.com/xap/1.0/sType/Version#	c/a/a/a/s.java
http://ns.adobe.com/xap/1.0/sType/Job#	c/a/a/a/s.java
http://ns.adobe.com/xap/1.0/sType/ManifestItem#	c/a/a/a/s.java
http://ns.adobe.com/xmp/Identifier/qual/1.0/	c/a/a/a/s.java
http://purl.org/dc/1.1/	c/a/a/a/f.java
http://purl.org/dc/elements/1.1/	c/a/a/a/f.java
http://www.w3.org/1999/02/22-rdf-syntax-ns#	c/a/a/a/f.java
http://javax.xml.XMLConstants/feature/secure-processing	c/a/a/a/m.java
http://apache.org/xml/features/disallow-doctype-decl	c/a/a/a/m.java
http://xml.org/sax/features/external-general-entities	c/a/a/a/m.java
http://xerces.apache.org/xerces2-j/features.html#disallow-doctype-decl	c/a/a/a/m.java

URL信息	Url所在文件
http://xml.org/sax/features/external-parameter-entities	c/a/a/a/m.java
http://xerces.apache.org/xerces2-j/features.html#external-parameter-entities	c/a/a/a/m.java
http://apache.org/xml/features/nonvalidating/load-external-dtd	c/a/a/a/m.java
http://www.w3.org/1999/02/22-rdf-syntax-ns#	c/a/a/a/m.java
http://purl.org/dc/elements/1.1/	c/a/a/a/q.java
http://ns.adobe.com/exif/1.0/	c/a/a/a/q.java
http://ns.adobe.com/xmp/1.0/DynamicMedia/	c/a/a/a/q.java
http://ns.adobe.com/xap/1.0/rights/	c/a/a/a/q.java
http://ns.adobe.com/xap/1.0/mm/	c/a/a/a/q.java
http://schemas.android.com/apk/res/android	a/b/d/a/a/i.java
https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/a/b.java
https://twitter.com/intent/tweet?text={message}&url={url}	cl/json/a/n.java
https://pinterest.com/pin/create/button/?url={url}&media=$media&description={message}	cl/json/a/h.java
https://plus.google.com/share?url={url}	cl/json/a/e.java
https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/a/c.java

URL信息	Url所在文件
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libimagepipeline.so

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	c/d/a/b/c/s.java

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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
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.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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕

向手机申请的权限	是否危险	类型	详细情况
getui.permission.GetuiService.com.bcloud.YUQGBHHK	未知	Unknown permission	Unknown permission from android reference
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=US, O=Android, CN=Android Debug
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-01-19 03:05:49+00:00
Valid To: 2045-01-11 03:05:49+00:00
Issuer: C=US, O=Android, CN=Android Debug
Serial Number: 0x54bc748d
Hash Algorithm: sha1
md5: 252e3ded833125ed3e3bb010bc24f4dc
sha1: f16147ecc298f4f2eddeb55ec94b62922f52be2c
sha256: 3adb9e16eee384816391f7cea0fff0bf248ff2c300ea06972b838baa95ff488a
sha512: b66c74d551b913b56c8c0b9c00acefa2e2719003c6ec92e2b122d2c604dfdade3a3a7ec876210090e82131b0aba5591a65493c303f096347356e953db921d432

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent://,

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机: Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check possible Build.SERIAL check subscriber ID check 编译器: dexlib 2.x

---