MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

掌活 v1.3.0-release.APK

APP名称:	掌活
包名:	com.wisder.linkinglive.prod
域名线索:	4条
URL线索:	15条
邮箱线索:	0条
分析日期:	2022年2月3日 13:32

文件信息

文件名: zhrlzy.apk
文件大小: 6.16MB
MD5值: 9c190364ee1c9c85a4d3b55bc65dd6ee
SHA1值: 8472defae6f69ce962320d0a3a9e1dfc8b9b2907
SHA256值: 2f25ec38352dc1492fb80ccc4a3638bf150eb160ba50e7bbf5996d400ecc98eb

APP 信息

App名称: 掌活
包名: com.wisder.linkinglive.prod
主活动**Activity:** com.wisder.linkinglive.module.login.SplashActivity
安卓版本名称: v1.3.0-release
安卓版本: 130

域名线索

域名	是否危险域名	服务器信息
ce3e75d5.jpush.cn	good	**IP:** 183.232.58.243 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

域名	是否危险域名	服务器信息
configapi-api.glqa.jpushoa.com	good	**IP:** 172.17.5.42 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
github.com	good	**IP:** 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903 查看地图: Google Map
www.baidu.com	good	**IP:** 110.242.68.3 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

URL线索

URL信息	Url所在文件
https://www.baidu.com	com/wisder/linkinglive/base/webview/Html5Activity.java

URL信息	Url所在文件
http://***	com/wisder/linkinglive/request/base/NetworkConstant.java
https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties	com/liulishuo/filedownloader/services/BaseFileServiceUIGuard.java
http://configapi-api.glqa.jpushoa.com/v1/status	cn/jiguang/ay/e.java
https://ce3e75d5.jpush.cn/wi/op8jdu	cn/jiguang/p/c.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/au/c.java
https://ce3e75d5.jpush.cn/wi/d8n3hj	cn/jiguang/au/c.java
https://github.com/vinc3m1	Android String Resource
https://github.com/vinc3m1/RoundedImageView	Android String Resource
https://github.com/vinc3m1/RoundedImageView.git	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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_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.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.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.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
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
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.wisder.linkinglive.prod.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
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.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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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
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.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

向手机申请的权限	是否危险	类型	详细情况
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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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。
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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=linkinglive
Signature Algorithm: rsassa_pkcs1v15

Valid From: 2021-01-05 07:01:33+00:00
Valid To: 2045-12-30 07:01:33+00:00
Issuer: CN=linkinglive
Serial Number: 0x504e2b34
Hash Algorithm: sha256
md5: d6516cc2cbb195e7f2b90ea8967af48d
sha1: e4ed50dfe18ca9daa8950e37becca59cd7ee46dc
sha256: 7b0caa1735ae9b3faed01f1ce9ecd86cab92d96bc3edf5495983008c7a935027
sha512: ef0767c1ce8186e20ea0be3fc6c3429810ea27f83774fa7ea123c14f8a0fa6f89636e23fd450323b2e2e6d3f826217504668991ed406d32eda9ef3bcff8a5ba5
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 8cde861cf7692280cef5678216e5fc7d59af64c821c9eb4fe57c75292a036ab0

Exodus威胁情报

名称	分类	URL链接
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343

硬编码敏感信息

可能的敏感信息
"forget_password" : "忘记密码"
"input_6_16_password" : "请输入6-16位密码"
"input_password" : "请输入密码"
"library_roundedimageview_author" : "Vince Mi"

可能的敏感信息
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"pwd_is_different" : "前后密码输入不一致，请重新输入"
"upload_certificate" : "上传凭证"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.wisder.linkinglive.module.login.SplashActivity	Schemes: wisder://, Hosts: linkinglive.com,
com.wisder.linkinglive.module.product.SignUpActivity	Schemes: esign://, Hosts: demo, Paths: /signBack,

加壳分析

文件列表	分析结果

<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
Build.PRODUCT check
Build.BOARD check
possible Build.SERIAL check
network operator name check
device ID check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
