MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

vivo游戏扩展引擎 1.0.0.0.APK

APP名称:	vivo游戏扩展引擎
包名:	com.vivo.apf
域名线索:	20条
URL线索:	26条
邮箱线索:	0条
分析日期:	2022年1月20日 22:17

文件信息

文件名: vivoyxkzyq550486.apk
文件大小: 8.6MB
MD5值: a3b56b99aff6dddc366d13b312ccef5f
SHA1值: ee8bea265d22d1a2cbc555d5647511d3782cfa39
SHA256值: 7e83ac8558dafb4174c48905519a3e0476f028bc2323dd1fabf697de08c33c74

APP 信息

App名称: vivo游戏扩展引擎
包名: com.vivo.apf
主活动Activity:
安卓版本名称: 1.0.0.0
安卓版本: 1000

域名线索

域名	是否危险域名	服务器信息
www.slf4j.org	good	**IP:** 83.173.251.158 **所属国家:** Switzerland **地区:** Zurich **城市:** Zurich **纬度:** 47.366669 **经度:** 8.550000 **查看地图:** Google Map
hapjs.org	good	**IP:** 140.179.146.114 **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
appdetailh5.vivo.com.cn	good	**IP:** 182.254.59.146 **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
st-offlinegame.vivo.com.cn	good	**IP:** 182.254.61.50 **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
xmlpull.org	good	**IP:** 74.50.62.60 **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
hybrid.vivo.com	good	**IP:** 161.117.186.64 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
ro.usdk.vivo.com.cn	good	**IP:** 182.254.52.82 **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
st-onlinegame.vivo.com.cn	good	**IP:** 182.254.52.56 **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
gamebattlestatic.vivo.com.cn	good	**IP:** 219.154.245.23 **所属国家:** China **地区:** Henan **城市:** Xuchang **纬度:** 34.016670 **经度:** 113.816673 **查看地图:** Google Map
pay.vivo.com.cn	good	**IP:** 117.50.131.151 **所属国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.222219 **经度:** 121.458061 **查看地图:** Google Map
quickgame.vivo.com.cn	good	**IP:** 182.254.52.82 **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
topic.vivo.com.cn	good	**IP:** 219.154.245.23 **所属国家:** China **地区:** Henan **城市:** Xuchang **纬度:** 34.016670 **经度:** 113.816673 **查看地图:** Google Map
schemas.android.com	good	没有服务器地理信息.
usrsysjoint.vivo.com.cn	good	**IP:** 117.50.131.84 **所属国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.222219 **经度:** 121.458061 **查看地图:** Google Map
f.up.vivo.com.cn	good	**IP:** 39.97.6.111 **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
appupgrade.vivo.com.cn	good	**IP:** 116.198.8.99 **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

域名	是否危险域名	服务器信息
joint.vivo.com.cn	good	**IP:** 182.254.61.116 **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
zhan.vivo.com.cn	good	**IP:** 219.147.108.225 **所属国家:** China **地区:** Nei Mongol **城市:** Baotou **纬度:** 40.652222 **经度:** 109.822220 **查看地图:** Google Map
issuetracker.google.com	good	**IP:** 172.217.163.46 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
dfp.vivo.com.cn	good	**IP:** 116.198.7.116 **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

URL线索

URL信息	Url所在文件
https://appupgrade.vivo.com.cn/appSelfUpgrade	com/vivo/upgradelibrary/normal/d.java
http://schemas.android.com/apk/res-auto	com/vivo/game/apf/kp0.java
https://st-offlinegame.vivo.com.cn	com/vivo/game/apf/b42.java
https://st-onlinegame.vivo.com.cn	com/vivo/game/apf/b42.java
http://www.slf4j.org/codes.html	com/vivo/game/apf/ua3.java
http://www.slf4j.org/codes.html#StaticLoggerBinder	com/vivo/game/apf/ua3.java
http://www.slf4j.org/codes.html#null_LF	com/vivo/game/apf/ua3.java
http://www.slf4j.org/codes.html#multiple_bindings	com/vivo/game/apf/ua3.java
http://www.slf4j.org/codes.html#version_mismatch	com/vivo/game/apf/ua3.java
http://www.slf4j.org/codes.html#substituteLogger	com/vivo/game/apf/ua3.java
http://www.slf4j.org/codes.html#unsuccessfulInit	com/vivo/game/apf/ua3.java
https://quickgame.vivo.com.cn/	com/vivo/game/apf/s21.java
http://quickgame.vivo.com.cn/	com/vivo/game/apf/s21.java
http://schemas.android.com/apk/res/android	com/vivo/game/apf/le.java
https://joint.vivo.com.cn/ops/allowChannelInfo	com/vivo/game/apf/rz1.java
http://www.slf4j.org/codes.html#null_MDCA	com/vivo/game/apf/va3.java
http://www.slf4j.org/codes.html#no_static_mdc_binder	com/vivo/game/apf/va3.java

URL信息	Url所在文件
http://xmlpull.org/v1/doc/features.html#indent-output	com/vivo/game/apf/je1.java
https://dfp.vivo.com.cn/public/generate/post	com/vivo/game/apf/j32.java
https://appdetailh5.vivo.com.cn/detail/1873310	com/vivo/game/apf/e12.java
http://ro.usdk.vivo.com.cn	com/vivo/game/apf/a42.java
http://f.up.vivo.com.cn	com/vivo/game/apf/a42.java
https://joint.vivo.com.cn	com/vivo/game/apf/a42.java
https://pay.vivo.com.cn	com/vivo/game/apf/a42.java
https://gamebattlestatic.vivo.com.cn/E624IBNkyQifBO1f/battle/20200117/b62699f20ef12ab2f37bcc59680f9af6.apk	com/vivo/game/apf/d41.java
https://topic.vivo.com.cn/joint/TP32em3gbsibi0/index.html	com/vivo/game/apf/ky1.java
https://pay.vivo.com.cn/vcoin/wap/cashier#	com/vivo/game/apf/g22.java
https://joint.vivo.com.cn/game-subaccount-login	com/vivo/game/apf/zz1.java
https://usrsysjoint.vivo.com.cn/realNameAuth/isAuthed	com/vivo/game/apf/zz1.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/vivo/game/apf/kf1.java
https://issuetracker.google.com/issues/new?component=413107&template=1096568	com/vivo/game/apf/ku.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/vivo/game/apf/to1.java
http://hybrid.vivo.com/app/	com/vivo/hybrid/sdk/a.java
https://hybrid.vivo.com/app/	com/vivo/hybrid/sdk/a.java

URL信息	Url所在文件
http://hapjs.org/app/	com/vivo/hybrid/sdk/a.java
https://hapjs.org/app/	com/vivo/hybrid/sdk/a.java
https://zhan.vivo.com.cn/gameactivity/wk21070828d00470	com/vivo/casualgamecenter/core/base/BaseMVPActivity.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.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.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

向手机申请的权限	是否危险	类型	详细情况
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.GET_PACKAGE_SIZE	正常	测量应用程序存储空间	允许应用程序找出任何包使用的空间
android.permission.FORCE_STOP_PACKAGES	合法	强制停止其他应用程序	允许一个应用程序强行停止其他应用程序
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.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。
com.bbk.account.permission.receivebroadcast.removeaccount	未知	Unknown permission	Unknown permission from android reference
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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.AUTHENTICATE_ACCOUNTS	危险	充当帐户验证器	允许应用程序使用帐户管理器的帐户验证器功能,包括创建帐户以及获取和设置其密码
com.bbk.account.permission.READ_ACCOUNTINFO	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器

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.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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
android.permission.WRITE_SECURE_SETTINGS	系统需要	修改安全系统设置	允许应用程序修改系统固定好设置数据。不供普通应用程序使用
vivo.game.permission.OPEN_JUMP_INTENTS	未知	Unknown permission	Unknown permission from android reference
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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

向手机申请的权限	是否危险	类型	详细情况
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.READ_SHTTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.WRITE_SHTTINGS	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.INTERACT_ACROSS_USERS	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERACT_ACROSS_USERS_FULL	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.BATTERY_STATS	合法	修改电池统计信息	允许修改收集的电池统计信息。不供普通应用程序使用
android.permission.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.PERSISTENT_ACTIVITY	危险	让应用程序始终运行	允许应用程序使部分持续,从而使系统能够' T选用其用于其他应用程序。
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证令牌
com.android.alarm.permission.SET_ALARM	未知	Unknown permission	Unknown permission from android reference
android.permission.GET_INTENT_SENDER_INTENT	未知	Unknown permission	Unknown permission from android reference
android.permission.BIND_DIRECTORY_SEARCH	未知	Unknown permission	Unknown permission from android reference
android.permission.UPDATE_APP_OPS_STATS	未知	Unknown permission	Unknown permission from android reference
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
android.permission.DELETE_PACKAGES	系统需要	删除应用程序	允许应用程序删除 Android 包。恶意应用程序可以使用它来删除重要的应用程序
android.permission.CLEAR_APP_USER_DATA	合法	删除其他应用程序数据	允许应用程序清除用户数据

向手机申请的权限	是否危险	类型	详细情况
android.permission.WRITE_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_CACHE_FILESYSTEM	系统需要	访问缓存文件系统	允许应用程序读取和写入缓存文件系统
android.permission.DEVICE_POWER	合法	打开或关闭手机	允许应用程序打开或关闭手机
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=Guangdong, L=Dongguan View, O=BBK, OU=IQOO, CN=bbkmobile.com.cn, E=bbktel@bbktel.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-09-25 14:19:43+00:00
Valid To: 2040-02-11 14:19:43+00:00
Issuer: C=CN, ST=Guangdong, L=Dongguan View, O=BBK, OU=IQOO, CN=bbkmobile.com.cn, E=bbktel@bbktel.com
Serial Number: 0xb153730d8a352539
Hash Algorithm: sha1

md5: cb3817d94474ee58ab37d0825bd25f69
sha1: 283d60ddcd20c56ea1719ce90527f1235ae80efa
sha256: bcc35d4d3606f154f0402ab7634e8490c0b244c2675c3c6238986987024f0c02
sha512: 2d6aabac1c1f32fd9f09468931a1c2fcd7de62b318be8376afa485818e08c620ea3397dd3ec3eaf466ae194e870efad72980e2b38516bbaedd2a5f2f60a0a9c3
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 3c7404f44f4f68b51d5b5c8f6ccf32af0b72d471d1f6acc0ac637ffd645957ea

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.vivo.casualgamecenter.core.utils.router.RouterActivity	Schemes: apf://, Hosts: vivo.com,
com.vivo.unionsdk.ui.UnionActivity	Schemes: vivounion://, Hosts: union.vivo.com, Paths: /openjump,

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.MANUFACTURER check
network operator name 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>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>模糊器</td><td>unreadable field names
unreadable method names</td></tr>
</table>
</td></tr>
</table>
