MoGua

凤凰彩票 2.6.1.APK 分析报告

APP名称: 凤凰彩票

包名:	com.lutra.phoenix
域名线索:	13条
URL线索:	20条
邮箱线索:	0条
分析日期:	2024年10月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 2.apk
文件大小: 96.62MB
MD5值: f70110644280e505eba54e307a656ff5
SHA1值: fbe577ed2c6cfd26298cf593fda63044976eacd6
SHA256值: a3be316a8ab7bdc26909abd5ae97cec4f0ecf2464a4fa3d23adf1750ee62cb23

APP 信息

App名称: 凤凰彩票
包名: com.lutra.phoenix
主活动Activity: com.lutra.MainActivity
安卓版本名称: 2.6.1
安卓版本: 1

域名线索

域名	服务器信息
javax.xml.xmlconstants	没有服务器地理信息.
tagmanager.google.com	**IP**: 142.251.211.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
reactnative.dev	**IP**: 13.57.148.141 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418

storage.googleapis.com	**IP**: 142.250.217.91 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
api.lang948tinghangkonghud1u123anming32bg.com	**IP**: 34.92.161.34 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
ns.adobe.com	没有服务器地理信息.
docs.swmansion.com	**IP**: 172.67.142.188 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api.pushy.me	**IP**: 54.208.164.161 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.039474 **经度**: -77.491806
codepush.appcenter.ms	**IP**: 52.232.227.249 **所属国家**: United States of America **地区**: Virginia **城市**: Boydton **纬度**: 36.667641 **经度**: -78.387497
	IP: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore

github.com	**城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
bit.ly	**IP**: 67.199.248.11 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.750134 **经度**: -73.997009
10.0.2.2	**IP**: 10.0.2.2 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
fh14.com	**IP**: 104.21.59.91 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

URL线索

URL信息	Url所在文件
https://codepush.appcenter.ms/	com/microsoft/codepush/react/CodePush.java
https://api.lang948tinghangkonghud1u123anming32bg.com	com/lutra/BuildConfig.java
https://storage.googleapis.com/lutra/2/2.apk	com/lutra/BuildConfig.java

https://fh14.com	com/lutra/BuildConfig.java
https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting	com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java
https://github.com/software-mansion/react-native-screens/issues/17	com/swmansion/rnscreens/ScreenFragment.java
https://github.com/software-mansion/react-native-screens/issues/17	com/swmansion/rnscreens/ScreenStackFragment.java
https://github.com/software-mansion/react-native-screens/issues	com/swmansion/rnscreens/utils/ScreenDummyLayoutHelper.java
https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot	com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java
http://10.0.2.2:8969/stream	io/sentry/SpotlightIntegration.java
https://api.pushy.me	me/pushy/sdk/config/PushyAPIConfig.java
http://javax.xml.XMLConstants/feature/secure-processing	me/pushy/sdk/lib/jackson/databind/ext/DOMDeserializer.java
https://bit.ly/3GfZoys.	me/pushy/sdk/util/PushyPermissionVerification.java
https://bit.ly/2O3fHEX	me/pushy/sdk/util/PushyServiceManager.java
https://bit.ly/2O3fHEX	me/pushy/sdk/services/PushyJobService.java
https://api.lang948tinghangkonghud1u123anming32bg.com	摸瓜V1引擎
https://storage.googleapis.com/lutra/2/2.apk	摸瓜V1引擎
https://fh14.com	摸瓜V1引擎
https://tagmanager.google.com/	摸瓜V2引擎
https://reactnative.dev/docs/debugging	lib/arm64-v8a/libjsinspector.so

https://reactnative.dev/docs/debugging	lib/armeabi-v7a/libjsinspector.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libstatic-webp.so
https://reactnative.dev/docs/debugging	lib/x86/libjsinspector.so
https://reactnative.dev/docs/debugging	lib/x86_64/libjsinspector.so

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Android, CN=Android Debug
签名算法: rsassa_pkcs1v15
有效期自: 2013-12-31 22:35:04+00:00
有效期至: 2052-04-30 22:35:04+00:00
发行人: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Android, CN=Android Debug
序列号: 0x232eae62
哈希算法: sha1
md5值: 20f46148b72d8e5e5ca23d37a4f41490
sha1值: 5e8f16062ea3cd2c4a0d547876baa6f38cabf625
sha256值: fac61745dc0903786fb9ede62a962b399f7348f0bb6f899b8332667591033b9c
sha512值: 926c0550edaee7aed1211b91fde06be4cc4748e61d8f1afbe0bd12f3949a0d09a1cf4306c72e6662ae4c7b8ae7a573a81d7e52e5b6124444eaf8f413e6b1fa69
公钥算法: rsa
密钥长度: 2048
指纹: b759a55bdc298b16f7a102f3107f3db38110f3dc7da00b1e981e9b257a9cf1af

硬编码敏感信息

可能的敏感信息
"CODEPUSH_ANDROID_KEY" : "nx4mToG6yJYRXda7Loo42HV8y62sAvPgyivQm"
"CODEPUSH_IOS_KEY" : "ahoSe0UHt95L_sw6IOgEoGWM7Q0r8jd0b-xD6"
"CodePushDeploymentKey" : ""
"HCAPTCHA_SITE_KEY" : "b6dcdf93-150e-466b-bc2c-c22f8d6a593a"
"google_api_key" : "AIzaSyCG2Q9Q2WnsKtFPHGHr2o7UCj1m-ThVTcw"
"google_crash_reporting_api_key" : "AIzaSyCG2Q9Q2WnsKtFPHGHr2o7UCj1m-ThVTcw"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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.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.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.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_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.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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储	允许应用程序写入外部存储

		内容	
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.POST_NOTIFICATIONS	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
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.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ADSERVICES_AD_ID	未知	Unknown permission	Unknown permission from android reference
com.lutra.phoenix.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.lutra.phoenix://,

---