MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Oordrz 3.3.8.APK

APP名称:	Oordrz
包名:	com.oordrz.buyer
域名线索:	12条
URL线索:	22条
邮箱线索:	1条
分析日期:	2022年1月22日 23:27

文件信息

文件名: oordrz553596.apk
文件大小: 5.84MB
MD5值: 45e7dde990dc8d45ea817581a97c9e6d
SHA1值: 92bc0f19a6dfe0e97d5482f503ca6f43a50d9a6d
SHA256值: 7ac27e7d1fcbed3d1107f6c174199c37fe9d3f130535732ed43e1c7b3b263be4

APP 信息

App名称: Oordrz
包名: com.oordrz.buyer
主活动**Activity:** com.oordrz.buyer.activities.SplashActivity
安卓版本名称: 3.3.8
安卓版本: 86

域名线索

域名	是否危险域名	服务器信息
logs.juspay.in	good	**IP:** 35.244.140.219 **所属国家:** United States of America **地区:** Missouri **城市:** Kansas City **纬度:** 39.099731 **经度:** -94.578568 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.oordrz.com	good	**IP:** 103.53.40.64 **所属国家:** India **地区:** Delhi **城市:** Delhi **纬度:** 28.666670 **经度:** 77.216667 **查看地图:** Google Map
api.instamojo.com	good	**IP:** 104.20.94.103 **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
play.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
redir1.juspay.in	good	没有服务器地理信息.
s3-ap-southeast-1.amazonaws.com	good	**IP:** 108.160.166.253 **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

域名	是否危险域名	服务器信息
d3e0hckk6jr53z.cloudfront.net	good	**IP:** 99.84.55.34 **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
maps.googleapis.com	good	**IP:** 142.251.42.234 **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
oordrz.com	good	**IP:** 103.53.40.64 **所属国家:** India **地区:** Delhi **城市:** Delhi **纬度:** 28.666670 **经度:** 77.216667 **查看地图:** Google Map
www.oordrz.in	good	**IP:** 13.59.109.159 **所属国家:** United States of America **地区:** Ohio **城市:** Columbus **纬度:** 39.961182 **经度:** -82.998787 **查看地图:** Google Map

域名	是否危险域名	服务器信息
goo.gl	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
oordrz-android-app.firebaseio.com	good	**IP:** 35.201.97.85 **所属国家:** United States of America **地区:** Missouri **城市:** Kansas City **纬度:** 39.099731 **经度:** -94.578568 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
https://api.instamojo.com/	com/instamojo/android/network/Urls.java
https://api.instamojo.com/	com/instamojo/android/helpers/Constants.java
https://goo.gl/ow56KR	com/oordrz/buyer/activities/CommunityGuestsLogActivity.java
https://goo.gl/9MBwsK	com/oordrz/buyer/activities/CommunityGuestsLogActivity.java
www.oordrz.in	com/oordrz/buyer/activities/CommunityGuestsLogActivity.java

URL信息	Url所在文件
https://goo.gl/ow56KR	com/oordrz/buyer/activities/HomePage.java
http://play.google.com/store/apps/details?id=	com/oordrz/buyer/activities/HomePage.java
https://goo.gl/ow56KR	com/oordrz/buyer/activities/ItemsDetailsActivity.java
https://goo.gl/ow56KR	com/oordrz/buyer/activities/AddGuestDetailsActivity.java
https://goo.gl/9MBwsK	com/oordrz/buyer/activities/AddGuestDetailsActivity.java
https://api.instamojo.com/oauth2/token/	com/oordrz/buyer/activities/PaymentRequestActivity.java
http://www.oordrz.com/instamojo/webhook/	com/oordrz/buyer/activities/PaymentRequestActivity.java
http://oordrz.com/base-url.json	com/oordrz/buyer/activities/SplashActivity.java
http://maps.googleapis.com/maps/api/geocode/json?latlng=%1$f,%2$f&sensor=true&language=	com/oordrz/buyer/utils/NextWorkUtils.java
http://play.google.com/store/apps/details?id=	com/oordrz/buyer/utils/RateUsUtil.java
https://oordrz.com/oordrzadmin/oordrzapi/android/	com/oordrz/buyer/utils/Constants.java
https://oordrz.com/oordrzadmin/	com/oordrz/buyer/utils/Constants.java
https://oordrz.com/oordrzadmin/images/	com/oordrz/buyer/utils/Constants.java
https://oordrz.com/oordrzadmin/oordrzapi/test/	com/oordrz/buyer/utils/Constants.java
https://s3-ap-southeast-1.amazonaws.com/godel-remote-assets/imageResources/info/juspay_info_dialog.png	in/juspay/godel/ui/dialog/JuspaySafeDialogManager.java

URL信息	Url所在文件
https://oordrz-android-app.firebaseio.com	Android String Resource
https://logs.juspay.in/godel/analytics	Android String Resource
https://d3e0hckk6jr53z.cloudfront.net/godel/config.zip	Android String Resource
https://redir1.juspay.in/config/dynamic	Android String Resource
https://redir1.juspay.in/gateway/sc	Android String Resource

邮箱线索

邮箱地址	所在文件
feedback@oordrz.com	com/oordrz/buyer/activities/HomePage.java

数据库线索

FIREBASE链接地址	详细信息
https://oordrz-android-app.firebaseio.com	info App talks to a Firebase Database.

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
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.android.launcher.permission.INSTALL_SHORTCUT	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

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_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_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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=91, ST=Telangana, L=Hyderabad, O=Oordrz, OU=Oordrz, CN=Buyer
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-01-22 14:20:04+00:00
Valid To: 2041-01-15 14:20:04+00:00
Issuer: C=91, ST=Telangana, L=Hyderabad, O=Oordrz, OU=Oordrz, CN=Buyer
Serial Number: 0x5ea33202
Hash Algorithm: sha256
md5: 7bd6a786c8310f97139085a53c3a6d59
sha1: 52f61a511cc8c87ede42c99ed36dec57528cdca9
sha256: c6993b6c53df65381e622dee3195ff15d278c61e7e8db445be15e88db3dc3fd5
sha512: 607ef39b8871fbb813b6a2a181f047069cdb2157f2ffd388113270b34390749a86a9c8b0f9778a45109597256aa0d7c45af8aaa826c48b6f69088d6b438c6ec7
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b4be14f20a359e9e4b6c5657afc89ae2d43a9545b4f0655f0ae11535a4de00e1

Exodus威胁情报

名称	分类	URL链接
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

硬编码敏感信息

可能的敏感信息
"API_KEY" : "AIzaSyCtBWbpiqiUvEn7aGcNC5BF_ZB5unH3NxI"
"firebase_database_url" : "https://oordrz-android-app.firebaseio.com"
"google_api_key" : "AIzaSyAhqobf_Itsp1S_jDcERL9p_co7pF5fZk0"
"google_crash_reporting_api_key" : "AIzaSyAhqobf_Itsp1S_jDcERL9p_co7pF5fZk0"

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
Build.TAGS check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
