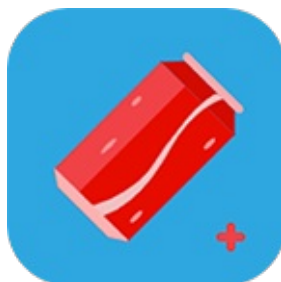




MoGua

可乐云PLUS 400.APK 分析报告



APP名称:

可乐云PLUS

包名: com.rocket.e5fa45aa603f90b

域名线索: 16条

URL线索: 10条

邮箱线索: 0条

分析日期: 2024年5月8日

分析平台: [摸瓜反编译平台](#)

文件名: 400.apk
文件大小: 18.73MB
MD5值: c737ed102c6236f2b7ca6f0a62f03d13
SHA1值: 5b270eaf731d4589920635850dabd9bda8431b4a
SHA256值: 659cf4149919ab19a9943f9a32696a75d5c01ac150532672c9058d66b768f367

i APP 信息

App名称: 可乐云PLUS
包名: com.rocket.e5fa45aa603f90b
主活动Activity: com.github.kr328.clash.SplashActivity
安卓版本名称: 400
安卓版本: 400

🔍 域名线索

域名	服务器信息
developer.umeng.com	IP: 59.82.29.163 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
alogsus.umeng.com	IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania

xmlpull.org	城市: California 纬度: 40.065647 经度: -79.891724
cuojue.org	IP: 172.67.189.129 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
hydra.alibaba.com	IP: 203.119.144.20 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
t.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington 纬度: 52.184460 经度: -0.687590
developer.android.com	IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514

ouplog.umeng.com	IP: 47.246.110.94 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
cmnsguider.yunos.com	IP: 203.119.175.203 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
alogus.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
play.google.com	IP: 59.24.3.174 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam 纬度: 37.420624 经度: 127.126717
ulogs.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
ulogs.umengcloud.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing

	纬度: 32.061668 经度: 118.777992
d.alipay.com	IP: 123.125.216.242 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
plbslog.umeng.com	IP: 36.156.202.78 所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435600

URL线索

URL信息	Url所在文件
https://d.alipay.com	com/github/kr328/clash/BrowserActivity\$initWebView\$2\$shouldOverrideUrlLoading\$1.java
http://hydra.alibaba.com/	com/ta/utdid2/a/b.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/c/a/a.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/c/a/e.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java

https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/s.java
https://developer.android.com/platform/technology/app-bundle	Mogua Engine V1
https://github.com/Kr328/ClashForAndroid	Mogua Engine V1
https://github.com/Dreamacro/clash	Mogua Engine V1
https://github.com/naicfeng/ClashRForAndroid	Mogua Engine V1
https://github.com/sh4d0wfiend/clash	Mogua Engine V1
https://github.com/Kr328/ClashForAndroid/issues	Mogua Engine V1
https://github.com/Kr328/ClashForAndroid/releases	Mogua Engine V1
https://play.google.com/store/apps/details?id=com.github.kr328.clash	Mogua Engine V1
https://cuojue.org	Mogua Engine V1
https://t.me/clash_for_android_channel	Mogua Engine V1

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=rocket, ST=rocket, L=rocket, O=rocket, OU=rocket, CN=rocket.keystore

签名算法: rsassa_pkcs1v15

有效期自: 2019-10-30 09:27:47+00:00

有效期至: 2029-10-27 09:27:47+00:00

发行人: C=rocket, ST=rocket, L=rocket, O=rocket, OU=rocket, CN=rocket.keystore

序列号: 0x39dc27ab

哈希算法: sha256

md5值: ddb2ee1fd665d34d8231334330559d70

sha1值: 9830300488a6b83bf435e9b06310454fb6462a51

sha256值: bd71c74b22c595cfd2d6c93777b387a0fd7fbc8592eac143b787b01829193c9b

sha512值: ff532622b1dd5b2be42d287f20e105352d1a3a27ceb42ca0bc3df47e2dc0137b4615a66f2245d461bf5312e865ff1de453ebf74165d6f1e2f144e5feacf10431

公钥算法: rsa

密钥长度: 1024

指纹: be0dce1fadd398f93d8defcf5edf6386f3b11c96dcc6fb1384501a8867840178

硬编码敏感信息

可能的敏感信息
"bypass_private_network" : "Bypass Private Network"
"bypass_private_network_summary" : "Bypass private network addresses"

bypass_private_network_summary : Bypass private network addresses
"forget_password" : "Forgot your password?"
"register_user" : "User registration"
"username" : "Account"
"bypass_private_network" : "绕过私有网络"
"bypass_private_network_summary" : "绕过私有网络地址"
"forget_password" : "忘记密码？ "
"register_user" : "没有账号,立即注册"
"username" : "账号"
"bypass_private_network" : "繞過私有網絡"
"bypass_private_network_summary" : "繞過私有網絡地址"
"forget_password" : "忘記密碼？ "
"register_user" : "沒有賬號,立即註冊"
"username" : "賬號"
"bypass_private_network" : "繞過私有網絡"
"bypass_private_network_summary" : "繞過私有網絡地址"
"forget_password" : "忘記密碼？ "
"register_user" : "沒有賬號,立即註冊"

"username" : "賬號"

加壳分析

第三方SDK

名称	分类	URL链接
Microsoft Visual Studio App Center Analytics	数据分析	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	异常检测	https://reports.exodus-privacy.eu.org/trackers/238
友盟统计	数据分析	https://reports.exodus-privacy.eu.org/trackers/119

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.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
		查看Wi-Fi状	

android.permission.ACCESS_WIFI_STATE	正常	态	允许应用程序查看有关 Wi-Fi 状态的信息
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.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。
com.rocket.e5fa45aa603f90b.permission.RECEIVE_BROADCASTS	未知	Unknown permission	Unknown permission from android reference

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。