MoGua

None 180.74.0.2-family.APK 分析报告

APP名称:	None

包名:	com.qustodio.qustodioapp
域名线索:	19条
URL线索:	19条
邮箱线索:	0条
分析日期:	2025年6月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: base.apk
文件大小: 23.41MB
MD5值: efb415b8000bd4240553d7da6fa9ff5d
SHA1值: 7212db6bc8cd70ec08fdbba778dc7481075ffce2
SHA256值: 962be84eb4b73d8825d47b00b3a3f2c67e794e357c81ad46615883c11111a60e

APP 信息

App名称: None
包名: com.qustodio.qustodioapp
主活动Activity: com.qustodio.qustodioapp.ui.splash.SplashScreenActivity
安卓版本名称: 180.74.0.2-family
安卓版本: 1807400

域名线索

域名	服务器信息
plus.google.com	**IP**: 66.220.147.11 **所属国家**: United States of America **地区**: California **城市**: Menlo Park **纬度**: 37.436935 **经度**: -122.193604
issuetracker.google.com	**IP**: 74.125.142.139 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
qustodio.com	**IP**: 52.21.98.137 **所属国家**: United States of America **地区**: Virginia

	城市: Ashburn **纬度**: 39.039474 **经度**: -77.491806
www.google.com	**IP**: 199.16.158.12 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
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
conf.rollout.io	**IP**: 108.156.144.93 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.604309 **经度**: -122.329842
push.rollout.io	**IP**: 34.239.4.249 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.039474 **经度**: -77.491806
firebase-settings.crashlytics.com	**IP**: 114.250.65.34 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 199.59.148.96

www.youtube.com	**所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
statestore.rollout.io	IP: 3.175.227.9 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
schemas.android.com	没有服务器地理信息.
x-api.rollout.io	IP: 3.234.60.87 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.039474 **经度**: -77.491806
console.firebase.google.com	IP: 142.250.99.139 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.w3.org	IP: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
cdn-settings.segment.com	IP: 13.33.45.217 **所属国家**: Singapore **地区**: Singapore

	城市: Singapore **纬度**: 1.289987 **经度**: 103.850281
jsoup.org	**IP**: 104.21.64.1 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.bing.com	**IP**: 202.89.233.101 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
analytic.rollout.io	**IP**: 52.70.95.64 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.039474 **经度**: -77.491806
notify.bugsnag.com	**IP**: 35.186.205.6 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568

URL线索

URL**信息**	Url**所在文件**

https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	F2/g.java
http://undefined/	M8/d.java
http://'	M8/d.java
https://'.	M8/d.java
https://jsoup.org/cookbook/extracting-data/working-with-urls	M8/d.java
https://null	com/qustodio/accessibility/parser/browser/BrowserParser.java
http://null	com/qustodio/accessibility/parser/browser/BrowserParser.java
https://qustodio.com	com/qustodio/qustodioapp/model/UpdateInfoModel.java
https://www.youtube.com/watch?v=	com/qustodio/qustodioapp/youtube/YoutubeConstantsKt.java
https://cdn-settings.segment.com/v1/projects/	com/segment/analytics/h.java
http://schemas.android.com/apk/res/android	i2/C1746f.java
https://console.firebase.google.com	d3/C1526b.java
https://x-api.rollout.io/device/get_configuration	io/rollout/client/Environment.java
https://conf.rollout.io	io/rollout/client/Environment.java
https://x-api.rollout.io/device/update_state_store	io/rollout/client/Environment.java
https://statestore.rollout.io	io/rollout/client/Environment.java
https://analytic.rollout.io	io/rollout/client/Environment.java
https://push.rollout.io/sse	io/rollout/client/Environment.java

https://notify.bugsnag.com	io/rollout/reporting/ErrorReporter.java
https://plus.google.com/	n1/K.java
https://github.com/google/gson/blob/main/Troubleshooting.md	u3/n.java
http://www.google.com	w7/d.java
https://issuetracker.google.com/issues/new?component=413107&template=1096568	o0/C2005c.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	P/m.java
http://www.	Z4/a.java
https://www.	Z4/a.java
https://www.google.com/search?safe=active	l5/C1873a.java
https://www.bing.com/search?q=	T4/a.java
https://www.google.com/search?q=	T4/a.java

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: True
找到 1 个唯一证书
主题: C=ES, ST=Barcelona, L=Barcelona, O=Qustodio Technologies, OU=Qustodio Technologies, CN=Qustodio
签名算法: rsassa_pkcs1v15
有效期自: 2013-02-18 13:10:08+00:00
有效期至: 2040-07-06 13:10:08+00:00
发行人: C=ES, ST=Barcelona, L=Barcelona, O=Qustodio Technologies, OU=Qustodio Technologies, CN=Qustodio
序列号: 0x51222830
哈希算法: sha1
md5值: 1daa93b2a686d2b44401d495380f72cb
sha1值: e76c16365a7cc5afdee2e42b42e0c1a3ff570e3a
sha256值: 73c071f6e370086c92e8cac50b4e6593af12404b38924a5bdca46c66e24b23d3
sha512值: ccd1c382a4908bc4c2997b49d3790d959fae2537908ea82dbd3958996db449a7c2951b226416b0cb5c3891d896847ecd45346c140dd31dd3be4f847d3515a30c
公钥算法: rsa
密钥长度: 2048
指纹: 6249dd1cd2474d8f68a178ebf2dcee0c19db6d99a55572ebe8736c5c813aa781

硬编码敏感信息

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.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.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.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.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.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.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
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.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.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.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
com.android.browser.permission.READ_HISTORY_BOOKMARKS	未知	Unknown permission	Unknown permission from android reference
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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.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.FOREGROUND_SERVICE_SYSTEM_EXEMPTED	未知	Unknown permission	Unknown permission from android reference

android.permission.USE_EXACT_ALARM	未知	Unknown permission	Unknown permission from android reference
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.qustodio.qustodioapp.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.qustodio.qustodioapp.ui.splash.SplashScreenActivity	Schemes: qustodiofamily://,
com.qustodio.qustodioapp.ui.onboarding.chromeextension.setup.ChromeExtensionSetupActivity	Schemes: qustodio://, Hosts: chrome-extension,
com.qustodio.qustodioapp.ui.passwordrequest.login.LoginPasswordRequestActivity	Schemes: qustodio://, Hosts: parent-login,