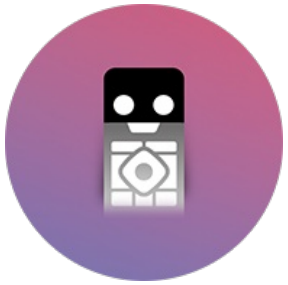
MoGua

FORMULER Remote 1.2.8-r215.APK 分析报告



APP名称: FORMULER Remote

包名:	tv.formuler.remoteupgrade.z
域名线索:	8条
URL线索:	5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: tv.formuler.remoteupgrade.z.10208_2.apk
文件大小: 14.69MB
MD5值: 96371063616ee2d094fdabd137f3cabd
SHA1值: 5d536cae725c6e468d6c767d175faaf6ce82b976
SHA256值: 93618d70a0fffff8e7a5b9964f1739df72f4a1da8d4c07f143073f5ffc4ed2c1

APP 信息

App名称: FORMULER Remote
包名: tv.formuler.remoteupgrade.z
主活动Activity: tv.formuler.remoteupgrade.intro.RemoteIntroActivity
安卓版本名称: 1.2.8-r215
安卓版本: 10208

域名线索

域名	服务器信息
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
formuler-common.firebaseio.com	**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
[illegible]	**IP**: 3.70.2.63 **所属国家**: Germany

gotaupdate.aloys.co.kr	**地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996
testgota.aloys.co.kr	**IP**: 54.180.24.189 **所属国家**: Korea (Republic of) **地区**: Gyeonggi-do **城市**: Icheon **纬度**: 37.279179 **经度**: 127.442421
teststore.png12.com	**IP**: 54.180.24.189 **所属国家**: Korea (Republic of) **地区**: Gyeonggi-do **城市**: Icheon **纬度**: 37.279179 **经度**: 127.442421
info.aloys.co.kr	**IP**: 52.57.56.153 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996
www.youtube.com	**IP**: 31.13.94.37 **所属国家**: Argentina **地区**: Ciudad Autonoma de Buenos Aires **城市**: Buenos Aires **纬度**: -34.603600 **经度**: -58.381554
appstore.png12.com	**IP**: 3.70.2.63 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996

URL线索

URL信息	Url所在文件
http://xml.apache.org/xslt	com/nanosic/www/wnf1x0/remoteupgrade/L.java
https://gotaupdate.aloys.co.kr/	tv/formuler/remoteupgrade/util/RestApiRequestManager.java
https://appstore.png12.com	tv/formuler/remoteupgrade/util/RestApiRequestManager.java
https://testgota.aloys.co.kr/	tv/formuler/remoteupgrade/util/RestApiRequestManager.java
https://teststore.png12.com	tv/formuler/remoteupgrade/util/RestApiRequestManager.java
http://info.aloys.co.kr/api/	tv/formuler/remoteupgrade/t/TUtil.java
https://www.youtube.com/watch?v=WN9-EcjObrA	tv/formuler/remoteupgrade/info/RemoteInfoActivity.java
https://formuler-common.firebaseio.com	摸瓜V1引擎

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=KR, ST=KG, L=BungDang, O=syola, OU=lab, CN=supremo, E=jacob@fortis.co.kr
签名算法: rsassa_pkcs1v15
有效期自: 2016-02-19 03:31:24+00:00
有效期至: 2043-07-07 03:31:24+00:00
发行人: C=KR, ST=KG, L=BungDang, O=syola, OU=lab, CN=supremo, E=jacob@fortis.co.kr
序列号: 0xf4856112389f48b1
哈希算法: sha1
md5值: 858a28eb42bb3c3093e31c5ea0c15b2e
sha1值: 291d494e4cfec82c41c68d48bb9725c3af7de65e
sha256值: 3bfd00c922b081dfb8eb5117fe1a4198ab05270e75b7d250c3536bfbd784a7cc
sha512值: 96bf7abc79a6b6f6f58834a01209b6c97dbb3f2d4f858f5782db8aa5984a1cfef3a5917df820800187e08824095220452834aec6924b3ec8ddfd26854c4b58f4
公钥算法: rsa
密钥长度: 2048
指纹: 9aae4ef50178ee1e444ab6a118a6f836f88da40f80a93d880830cbc914a9f4e4

硬编码敏感信息

可能的敏感信息
"firebase_database_url" : "https://formuler-common.firebaseio.com"
"google_api_key" : "AIzaSyC6Gmdrp3QppVQD9IENX77d--q32WEMOkI"
"google_crash_reporting_api_key" : "AIzaSyC6Gmdrp3QppVQD9IENX77d--q32WEMOkI"

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.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.BLUETOOTH_PRIVILEGED	系统需要		允许应用程序在没有用户交互的情况下配对蓝牙设备,并允许或禁止电话簿访问或消息访问。这不适用于第三方应用程序
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.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.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.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.INJECT_EVENTS	合法	按键和控制按钮	允许应用程序将其自己的输入事件（按键等）传递给其他应用程序。恶意应用程序可以利用它来接管电话
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
android.permission.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
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.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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	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。