MoGua

Magisk 30.2.APK 分析报告

APP名称: Magisk

包名:	com.topjohnwu.magisk
域名线索:	11条
URL线索:	13条
邮箱线索:	0条
分析日期:	2025年9月1日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.topjohnwu.magisk.apk
文件大小: 11.77MB
MD5值: 2691c30ccf059af2536cb0af803c787c
SHA1值: de0dc14e6429769c064d30a52f099820cbb0f027
SHA256值: 123093f51eeb1aa459ac188a22ac3e775e8243293d48df2ceda9ca9dad22d2d6

APP 信息

App名称: Magisk
包名: com.topjohnwu.magisk
主活动Activity: com.topjohnwu.magisk.ui.MainActivity
安卓版本名称: 30.2
安卓版本: 30200

域名线索

域名	服务器信息
youtrack.jetbrains.com	**IP**: 63.33.88.220 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
example.com	**IP**: 23.192.228.80 **所属国家**: United States of America **地区**: California **城市**: Santa Clara **纬度**: 37.354111 **经度**: -121.955490
www.patreon.com	**IP**: 103.252.114.11 **所属国家**: Singapore **地区**: Singapore

	城市: Singapore **纬度**: 1.289987 **经度**: 103.850281
paypal.me	**IP**: 151.101.129.21 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api.github.com	**IP**: 20.205.243.168 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
commons.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
twitter.com	**IP**: 31.13.88.26 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
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
schemas.android.com	没有服务器地理信息.

issuetracker.google.com	**IP**: 142.250.217.110 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
cloudflare-dns.com	**IP**: 104.16.248.249 **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://cloudflare-dns.com/dns-query	C0/e.java
https://issuetracker.google.com/issues/116541301	b0/u.java
https://twitter.com/	a2/r.java
https://www.patreon.com/topjohnwu	a2/s.java
https://paypal.me/magiskdonate	a2/s.java
https://github.com/sponsors/yujincheng08	a2/s.java
https://github.com/topjohnwu/Magisk	a2/q.java

https://github.com/	a2/C0173c.java
http://schemas.android.com/apk/res/android	I/d.java
http://schemas.android.com/apk/res/android	I/b.java
https://youtrack.jetbrains.com/issue/KT-55980	N2/j.java
https://example.com/	G0/c.java
https://api.github.com/	G0/c.java
http://schemas.android.com/apk/res/android	K0/r.java
http://schemas.android.com/apk/res/android	K0/a.java
https://commons.apache.org/proper/commons-compress/zip.html	C3/K.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: False
找到 1 个唯一证书
主题: C=TW, L=Taipei, CN=John Wu
签名算法: rsassa_pkcs1v15
有效期自: 2016-08-14 17:23:44+00:00

有效期至: 2116-07-21 17:23:44+00:00
发行人: C=TW, L=Taipei, CN=John Wu
序列号: 0x50514879
哈希算法: sha256
md5值: ceda68c1e174710aef58897dae6eab4f
sha1值: dc0f2b61cbd7e9d3dbbe060b2b870d46bb060211
sha256值: b4cb83b4dad99f997dbe872f013aa16c14eec41d167021f371f7e1330f273ee6
sha512值: 5436ae2a381f3a93c451989e10a2eef26abee31e5b9aa1d43779f113ba46beb67aed60c33a715552c95be7679abc1d12715c66ddaa7f2aa58cf6f75d7bafb41d
公钥算法: rsa
密钥长度: 2048
指纹: b86a20d8d92b4137362a0669da6fd9bd96c4b239a0616bb077e74cc666d967ab

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.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.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.HIDE_OVERLAY_WINDOWS	正常	防止非系统覆盖窗口	允许应用程序防止在其上绘制非系统覆盖窗口
android.permission.UPDATE_PACKAGES_WITHOUT_USER_ACTION	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.RUN_USER_INITIATED_JOBS	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.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

应用内通信