MoGua

PHK Key 1.1.7.APK 分析报告

APP名称: PHK Key

包名:	com.phillip.android.apps.authenticator2
域名线索:	16条
URL线索:	15条
邮箱线索:	1条
分析日期:	2025年2月22日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: PHK Key_1.1.7_APKPure.apk
文件大小: 2.62MB
MD5值: 951ddb88164347351d5fdda8ceaa82f2
SHA1值: 7955c102e88045054d761b024333b64bc5e8ed72
SHA256值: 0408ce5fb8c2b0d8a9cbc0c30890c196a4ce505137a83228a112826a8fadcd22

APP 信息

App名称: PHK Key
包名: com.phillip.android.apps.authenticator2
主活动Activity: com.phillip.android.apps.authenticator.AuthenticatorActivity
安卓版本名称: 1.1.7
安卓版本: 31

域名线索

域名	服务器信息
trading.poems.com.hk	**IP**: 45.60.15.245 **所属国家**: United States of America **地区**: California **城市**: Redwood City **纬度**: 37.532440 **经度**: -122.248833
www.cyberquote.com.hk	**IP**: 210.177.196.129 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
182.92.20.189	**IP**: 182.92.20.189 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397102
phk-key-217809.firebaseio.com	**IP**: 34.120.206.254 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
www.openmobilealliance.org	**IP**: 104.26.8.105 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.google.com	**IP**: 31.13.94.41 **所属国家**: Argentina **地区**: Ciudad Autonoma de Buenos Aires **城市**: Buenos Aires **纬度**: -34.603600 **经度**: -58.381554
www.wireless-village.org	**IP**: 104.21.11.240 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
192.168.18.40	**IP**: 192.168.18.40 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
	IP: 210.176.239.58

2fa.cyberquote.com.hk	**所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
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
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
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
pagead2.googlesyndication.com	IP: 114.250.64.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
xmlpull.org	IP: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724

www.poems.com.hk	**IP**: 210.177.196.135 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
schemas.xmlsoap.org	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903

URL线索

URL信息	Url所在文件
http://182.92.20.189:9099/	cn/jiguang/a/a/c/i.java
http://www.cyberquote.com.hk/cyberquote/mobile_apps/barcodeScanner.apk	com/phillip/android/apps/authenticator/Utilities.java
https://play.google.com/store/apps/details?id=com.srowen.bs.android	com/phillip/android/apps/authenticator/Utilities.java
https://www.google.com	com/phillip/android/apps/authenticator/timesync/NetworkTimeProvider.java
http://192.168.18.40:15805/	com/phillip/android/apps/authenticator/connectivity/MyVolleySingleton.java
http://2FA.cyberquote.com.hk/	com/phillip/android/apps/authenticator/connectivity/WebServiceFunction.java
https://2FA.cyberquote.com.hk/webservice/twofa.asmx	com/phillip/android/apps/authenticator/connectivity/WebServiceFunction.java

https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	defpackage/dm.java
http://schemas.xmlsoap.org/soap/encoding/	org/ksoap2/SoapEnvelope.java
http://schemas.xmlsoap.org/soap/envelope/	org/ksoap2/SoapEnvelope.java
http://xml.apache.org/xml-soap	org/ksoap2/serialization/MarshalHashtable.java
http://xmlpull.org/v1/doc/features.html	org/xmlpull/v1/XmlPullParser.java
http://www.wireless-village.org/CSP	org/kxml2/wap/wv/WV.java
http://www.wireless-village.org/PA	org/kxml2/wap/wv/WV.java
http://www.wireless-village.org/TRC	org/kxml2/wap/wv/WV.java
http://www.openmobilealliance.org/DTD/WV-CSP	org/kxml2/wap/wv/WV.java
http://www.openmobilealliance.org/DTD/WV-PA	org/kxml2/wap/wv/WV.java
http://www.openmobilealliance.org/DTD/WV-TRC	org/kxml2/wap/wv/WV.java
http://www.	org/kxml2/wap/wml/Wml.java
https://www.	org/kxml2/wap/wml/Wml.java
http://xmlpull.org/v1/doc/features.html	org/kxml2/io/KXmlSerializer.java
http://xmlpull.org/v1/doc/	org/kxml2/io/KXmlParser.java
http://xmlpull.org/v1/doc/properties.html	org/kxml2/kdom/Document.java
http://trading.poems.com.hk/PHK_Key/FAQ.asp?lang=en&channel=11	摸瓜V1引擎
https://phk-key-217809.firebaseio.com	摸瓜V1引擎

http://www.poems.com.hk/zh-hk/phillip-apps/download/mobile-apps/	摸瓜V1引擎
http://www.poems.com.hk/zh-hk/site-information/privacy/	摸瓜V1引擎
http://trading.poems.com.hk/PHK_Key/Terms_of_Service.asp?lang=en&channel=11	摸瓜V1引擎
http://trading.poems.com.hk/PHK_Key/FAQ.asp?lang=zh&channel=11	摸瓜V1引擎
http://trading.poems.com.hk/PHK_Key/Terms_of_Service.asp?lang=zh&channel=11	摸瓜V1引擎
http://trading.poems.com.hk/PHK_Key/FAQ.asp?lang=gb&channel=11	摸瓜V1引擎
http://trading.poems.com.hk/PHK_Key/Terms_of_Service.asp?lang=gb&channel=11	摸瓜V1引擎

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	defpackage/hq.java

手机线索

手机号	所在文件
15552000000	defpackage/yi.java

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=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2018-02-06 05:58:59+00:00
有效期至: 2048-02-06 05:58:59+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xe132b14824d035d7529cc25deae632a7ba6f22af
哈希算法: sha256
md5值: ad1065c78e6690d13cbce3e4a219a9d4
sha1值: 5b8833860b3457dfb1049079963abd0bc020dfed
sha256值: 9d555b4b39d98bae9ade4e4f9dc1436a46efc0d612b63a3a899e087f58cf741c
sha512值: bcbf80cdb344edd7e4b6be9e21717306f27dca2360828cab9784c75e03ebdd4d14f5c7a3a54afb8d167294e500d0255a98f928351b8d593f746edaadd3e6ea19
公钥算法: rsa
密钥长度: 4096
指纹: 004eefba4750c2f65e42a34300977bb523c4cc6119645a455b5e34537ac93933

硬编码敏感信息

可能的敏感信息
"firebase_database_url" : "https://phk-key-217809.firebaseio.com"
"google_api_key" : "AIzaSyCbO3Kxw5g4z0rw4KQMdEQaceExn9GfINI"
"google_crash_reporting_api_key" : "AIzaSyCbO3Kxw5g4z0rw4KQMdEQaceExn9GfINI"
"secret_saved" : "Secret saved"
"secret_saved" : "秘密金鑰已儲存"

"secret_saved" : "Secret saved"
"secret_saved" : "綁定碼已儲存"
"secret_saved" : "绑定码已保存"
"secret_saved" : "秘密金鑰已儲存"

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	类型	详细情况

	险		
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.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.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.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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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_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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	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
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

com.phillip.android.apps.authenticator2.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
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.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
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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。

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.phillip.android.apps.authenticator.AuthenticatorActivity	Schemes: phillipauth://,

---