MoGua

XAPK Installer 2.2.2.APK 分析报告

APP名称:	XAPK Installer

包名:	com.apkpure.installer
域名线索:	4条
URL线索:	8条
邮箱线索:	1条
分析日期:	2025年7月13日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: xapkanzhuangqi2020.apk
文件大小: 3.5MB
MD5值: d0963fb89781f0314cacc66454bbd34d
SHA1值: 5bc576c558e6894fa323317a3987fc2ea98c45a2
SHA256值: 7434811b4d628f64bf88b0bfb4d534514c4ced58ed2a71e3f396462903be68ee

APP 信息

App名称: XAPK Installer
包名: com.apkpure.installer
主活动Activity: com.apkpure.installer.MainActivity
安卓版本名称: 2.2.2
安卓版本: 82

域名线索

域名	服务器信息
goo.gl	**IP**: 172.217.160.110 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
apkpure.com	**IP**: 208.77.47.172 **所属国家**: United States of America **地区**: California **城市**: San Jose **纬度**: 37.323776 **经度**: -121.914719
pagead2.googlesyndication.com	**IP**: 220.181.174.102 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397102
schemas.android.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res-auto	c/d/a/e/a.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	c/e/a/a/a/a/a.java
http://goo.gl/8Rd3yj	c/e/a/a/g/b/m.java
http://schemas.android.com/apk/res/android	a/b/h/b/e/g.java
http://schemas.android.com/apk/res/android	com/gc/materialdesign/views/Slider.java
http://schemas.android.com/apk/res-auto	com/gc/materialdesign/views/Slider.java
http://schemas.android.com/apk/res/android	com/gc/materialdesign/views/ButtonFlat.java
http://schemas.android.com/apk/res/android	com/gc/materialdesign/views/ProgressBarCircularIndeterminate.java
https://apkpure.com/p/%s	Mogua Engine V1
https://apkpure.com/p/com.apkpure.installer	Mogua Engine V1
https://apkpure.com	Mogua Engine V1
https://apkpure.com/api/v1/device	Mogua Engine V1

https://apkpure.com/api/v1/check_update?p=com.apkpure.installer	Mogua Engine V1
https://apkpure.com/app	Mogua Engine V1
https://apkpure.com/game	Mogua Engine V1

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	c/e/a/a/d/o.java

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=CA, ST=California, L=Silicon Valley, O=APKFab, OU=Development, CN=Installer
签名算法: rsassa_pkcs1v15
有效期自: 2019-08-09 17:16:30+00:00
有效期至: 2044-08-02 17:16:30+00:00
发行人: C=CA, ST=California, L=Silicon Valley, O=APKFab, OU=Development, CN=Installer
序列号: 0x3d878cb9
哈希算法: sha256
md5值: a095b97e8d209cbb46ba73e4a8a62ef8

sha1值: 2731562784d85ac33c27f61dc36e993eac13e580
sha256值: aeb60b6d6f6864d6c348c17ae11ebdfc35586433d18b44b946353a6ea1491e1c
sha512值: dba355c6cd11fa06f8cc1b25a9886e101dca27300278fa787639b3939018791cd6470506beb07b814f7c156167798f657fb4b8505fd237310f5799b653c886c2
公钥算法: rsa
密钥长度: 2048
指纹: d7cdbf08b2791ced0c4931fe3e2e005a8ddb6f8f1c20c59ce9ddc89864bc6ee9

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.READ_PHONE_STATE	危险	读取电话状态和	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

		身份	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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.apkpure.installer.XAPKActivity	Schemes: file://, content://, Hosts: *, Mime Types: */*, Path Patterns: .*\\.xapk, .*\\..*\\.xapk, .*\\..*\\..*\\.xapk, .*\\..*\\..*\\..*\\.xapk, .*\\..*\\..*\\..*\\..*\\.xapk, .*\\..*\\..*\\..*\\..*\\..*\\.xapk, .*\\..*\\..*\\..*\\..*\\..*\\..*\\.xapk, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.xapk,