MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

告别手机控 1.0.2.APK

APP名称:	告别手机控
包名:	com.yunlian.awayphone
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2022年1月26日 18:57

文件信息

文件名: gbsjk.apk
文件大小: 5.6MB
MD5值: 89d1c099d523f2f703c7ec04a6a2e8af
SHA1值: 6c5e9824d4503b3847caae586c807e5a7c3b1e6e
SHA256值: a7c398c00efef4b25996aa2054654285021b32e2fb98fb260153fd02d1e09f9d

APP 信息

App名称: 告别手机控
包名: com.yunlian.awayphone
主活动**Activity:** com.yunlian.awayphone.activity.SplashKk
安卓版本名称: 1.0.2
安卓版本: 20191119

域名线索

域名	是否危险域名	服务器信息
github.com	good	**IP:** 20.205.243.166 **所属国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
https://github.com/vinc3m1	Android String Resource
https://github.com/vinc3m1/RoundedImageView	Android String Resource
https://github.com/vinc3m1/RoundedImageView.git	Android String Resource

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.SET_WALLPAPER	正常	设置壁纸	允许应用程序设置系统壁纸
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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器

向手机申请的权限	是否危险	类型	详细情况
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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏
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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=fujian, L=fuzhou, CN=xingkong
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-11-01 10:24:47+00:00
Valid To: 2119-10-08 10:24:47+00:00
Issuer: C=CN, ST=fujian, L=fuzhou, CN=xingkong
Serial Number: 0x4e4b53ac
Hash Algorithm: sha256
md5: 4c782f9cb269c3e0410413964931641b
sha1: fc85ed83bc3f3a8168ad2802d67985d7e2c494f4
sha256: 6cf0d2879e22d574b49d594ad281d49e2cc6128c799def8c19944fb0f8a7790f
sha512: 01b85e981448fe7471af8f7de432c94435394928fbbe2ebb67cf2d446d676bb0bbaa1c4a246e16f4b9c5d37f060952181d3c3c6ff23e30bd72c28a40f38552c4

硬编码敏感信息

可能的敏感信息
"deleted_key" : "已删除 %1$s"
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent101797092://,

加壳分析

文件列表	分析结果
APK包	壳列表 / 详细情况 打包 / Jiagu
assets/gdt_plugin/gdtadv2.jar!classes.dex	壳列表 / 详细情况 反虚拟机 / Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check subscriber ID check 编译器 / dexlib 2.x
assets/gdt_plugin/gdtadv2.jar!lib/arm64-v8a/libturingau.so	壳列表 / 详细情况 模糊器 / Obfuscator-LLVM version unknown

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!lib/armeabi/libturingau.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version unknown</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
<tr><td>模糊器</td><td>unreadable field names
unreadable method names</td></tr>
</table>
</td></tr>
</table>
