

APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



♠海棠赚转发赚钱福利 3.14.01.APK

APP名称: 海棠赚转发赚钱福利

包名: com.shoujizhuan.jiayou

域名线索: 1条

URL线索: 1条

邮箱线索: 0条

分析日期: 2022年2月2日 11:50

文件名: haitangzhuan.apk

文件大小: 13.09MB

MD5值: a838f24dcd6de2c5fcbb009c0a8b1a86

SHA1值: f88dcc3ab4251689316960e55e3a83ad727a1048

SHA256值: 8b2c921101a8c87ff6faf839398d61366d4baf2872114fee1dcbbfe4bfd8968d

i APP 信息

App名称: 海棠赚转发赚钱福利 包名: com.shoujizhuan.jiayou

主活动**Activity:** com.lushi.duoduo.start.ui.SplashActivity

安卓版本名称: 3.14.01 安卓版本: 31401

0 域名线索

域名	是否危险域名	服务器信息
a.tn990.com	good	IP: 42.81.213.227 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map



URL信息	Url所在文件
http://a.tn990.com/app.apk	Android String Resource

畫此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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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。

向手机申请的权限	是 否 危 险		详细情况	
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.ACCESS_DOWNLOAD_MANAGER	未知	Unknown permission	Unknown permission from android reference	
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.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.GET_TASKS	危险	检索正在运行 的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序 发现有关其他应用程序的私人信息	
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.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.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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference	
android.permission.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低	
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低	

向手机申请的权限		类型	详细情况	
android.permission.GET_PACKAGE_SIZE	正常	测量应用程序 存储空间	允许应用程序找出任何包使用的空间	
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。	
android.permission.INSTANT_APP_FOREGROUND_SERVICE	系统 需要		允许免安装应用创建前台服务	
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.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	
com.shoujizhuan.jiayou.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference	
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference	
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上 显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。	
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference	

向手机申请的权限	是否危险	类型	详细情况
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



APK is signed v1 signature: True v2 signature: False v3 signature: False

Found 1 unique certificates

Subject: C=CN, ST=HuBei, L=WH, O=Ls, OU=VideoB, CN=Xuxiong

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2020-06-29 02:01:38+00:00 Valid To: 2075-04-02 02:01:38+00:00

Issuer: C=CN, ST=HuBei, L=WH, O=Ls, OU=VideoB, CN=Xuxiong

Serial Number: 0x31194e59 Hash Algorithm: sha256

md5: 032d876edc11eb0414b8ba65544fb3d3

sha1: 2ff23cae01c08d9527d7cb1df4663ba837b0f955

sha256: 20bdc8b851ef992684c7704bfcd8387b84f1b237712a22cfdabd766d9f0852a6

sha512: db4a507f38fcb2092b0288c093e07724295e971bedf5aaab21c575ae399af86a63fd5258c3161c388c54a73be6b9d34eb6c9094422c51c4371ced340a1344f35



活动(ACTIVITY)	通信(INTENT)]
		ı

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent1109118142://,

命 加壳分析

文件列表	分析结果
APK包	売列表 详细情况
	打包 Tencent's Legu
	売列表 详细情况
assets/gdt_plugin/gdtadv2.jar!assets/yaq3_0.sec	反虚拟机 Build.MODEL check
	编译器 dexlib 2.x
	7,74.1, 7,7

文件列表	分析结果
	売列表 详细情况
	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check subscriber ID check
assets/gdt_plugin/gdtadv2.jar!classes.dex	编译器 dexlib 2.x
assets/gdt_plugin/gdtadv2.jar!lib/armeabi/libturingau.so	売列表 详细情况
22212.021_p.30044412.jul.mb/d1110421/mb/d111054	模糊器 Obfuscator-LLVM version unknown
assets/gdt_plugin/gdtadv2.jar!lib/arm64-v8a/libturingau.so	売列表 详细情况
	模糊器 Obfuscator-LLVM version unknown

文件列表	分析结果
lib/armeabi-v7a/libnms.so	売列表 详细情况 模糊器 ByteGuard 0.9.3
lib/armeabi/libnms.so	売列表 详细情况 模糊器 ByteGuard 0.9.3
lib/x86/libnms.so	売列表 详细情况 模糊器 ByteGuard 0.9.3
assets/libshellx-super.2019.so	壳列表 详细情况 反虚拟机 emulator file check
classes2.dex	壳列表 详细情况 编译器 unknown (please file detection issue!)

文件列表	分	分析结果		
classes.dex		壳列表	详细情况	
		防止反汇编	non-zero link size non-zero link offset	
		打包	Mobile Tencent Protect	
		编译器	dexlib 2.x	

报告由 摸瓜平台 自动生成,并非包含所有检测结果,有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析