

APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



♣ 环球智答 00.00.0001.APK

APP名称: 环球智答

包名: org.zywx.wbpalmstar.widgetone.uex11815790

域名线索: 5条

URL线索: 14条

邮箱线索: 0条

分析日期: 2022年2月2日 11:50

文件名: huanqiuzhida.apk

文件大小: 3.45MB

MD5值: 0a11ccb4ce0039d94c50f7798c83e133

SHA1值: 2da30f792f249a628f1bba0fc7ab8859ab048741

\$HA256值: b2f9ef75dcf23f2f15fd5e8cd6474a26627775d60670af0c398fef0de1ab7c6e

i APP 信息

App名称: 环球智答

包名: org.zywx.wbpalmstar.widgetone.uex11815790 主活动**Activity:** org.zywx.wbpalmstar.engine.LoadingActivity

安卓版本名称: 00.00.0001

安卓版本: 101

Q 域名线索

域名	是否危险域名	服务器信息
www.baidu.com	good	IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 查看地图: Google Map

域名	是否危险域名	服务器信息
newdc.appcan.cn	good	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
newpush.appcan.cn	good	P: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
storeb.appcan.cn	good	P: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
wgb.tx100.com	good	IP: 199.180.112.148 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.043240 经度: -118.250916 查看地图: Google Map



URL信息	Url所在文件
http://www.baidu.com	org/zywx/wbpalmstar/plugin/uexdataanalysis/analytics/AnalyticsHttpClient.java
http://wgb.tx100.com/mobile/adver.wg	org/zywx/wbpalmstar/engine/universalex/w.java
http://newdc.appcan.cn/	Android String Resource
http://newpush.appcan.cn/	Android String Resource
http://storeb.appcan.cn/	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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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

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 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.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_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_LOGS	危险	读取敏感日志数 据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.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.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。



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

Found 1 unique certificates

Subject: C=CN, ST=BJ, L=BJ, O=DEV, OU=ZYWX, CN=YSN

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2011-05-09 02:40:36+00:00 Valid To: 2066-02-09 02:40:36+00:00

Issuer: C=CN, ST=BJ, L=BJ, O=DEV, OU=ZYWX, CN=YSN

Serial Number: 0x4dc75424 Hash Algorithm: sha1

md5: d382d671c6672cba4b87980992cd9d77

sha1: 493e528709e1b4d2b8ff126e2cc8406d3b5e4dbb

sha256: 81dcb74499b79b2d3b4f4c5c6fdabd68c2ba7cfd1d04083bec8e560a809e67e1

sha512: 24e36e00d4d3d8c1100df2ad2269c17ca4518b94fd939604664ebc01c5679d5934696a67a46d4819c5e81865c494e1104b5f617713a2cbca3c46d85535322a49



₽ 硬编码敏感信息

可能的敏感信息

"appkey": "174c48e7-d72b-4467-fb01-2cf91bb921a5"



活动(ACTIVITY)	通信(INTENT)
org.zywx.wbpalmstar.engine.EBrowserActivity	Schemes: appcanscheme://,



文件列表	分析结果		
	売列表	详细情况	
classes.dex	反虚拟机	Build.MODEL check Build.MANUFACTURER check	
	编译器	dx	

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