MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

熊猫-XP 1.121.41.APK

APP名称:	熊猫-XP
包名:	com.tencent.mm
域名线索:	7条
URL线索:	11条
邮箱线索:	1条
分析日期:	2022年1月25日 02:38

文件信息

文件名: xiongmao-xp-2021.11.10-141.apk
文件大小: 10.31MB
MD5值: ccbea6f563b70888a4af16f25b845f77
SHA1值: c3d0260e1730c380bb32e8517edde20752e1d481
SHA256值: 3830c410b45586ca2179f5468647ad510dd90983b5e0516043b3f6e65f016352

APP 信息

App名称: 熊猫-XP
包名: com.tencent.mm
主活动**Activity:** com.wantime.wbangapp.ui.activity.WelComeActivity
安卓版本名称: 1.121.41
安卓版本: 141

域名线索

域名	是否危险域名	服务器信息
www.slf4j.org	good	**IP:** 83.173.251.158 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366669 经度: 8.550000 查看地图: Google Map

域名	是否危险域名	服务器信息
image.ywxskj.com	good	IP: 220.194.65.35 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
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
rebus007.altervista.org	good	没有服务器地理信息.
rebus007.github.io	good	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708 查看地图: Google Map
1000myth.com	good	IP: 119.167.183.37 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941 查看地图: Google Map

域名	是否危险域名	服务器信息
open.weixin.qq.com	good	**IP:** 175.24.209.30 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
https://open.weixin.qq.com/connect/confirm?uuid={0}	com/tencent/mm/plugin/view/a.java
http://1000myth.com:8082/authPage?agencyId=	com/wantime/wbangapp/ui/fragment/AuthorityFragment.java
https://image.ywxskj.com/wxHelper/apply.mp4?x-oss-process=video/snapshot,t_0,m_fast,w_414,f_png	com/wantime/wbangapp/ui/fragment/AuthorityFragment.java
http://1000myth.com:85/tutorial/index.html	com/wantime/wbangapp/ui/fragment/PersonFragment.java
http://1000myth.com:8082/	com/wantime/wbangapp/j/a.java
http://1000myth.com:85/	com/wantime/wbangapp/j/a.java
https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection	org/java_websocket/AbstractWebSocket.java
http://www.slf4j.org/codes.html#null_MDCA	g/d/e.java

URL信息	Url所在文件
http://www.slf4j.org/codes.html#no_static_mdc_binder	g/d/e.java
http://www.slf4j.org/codes.html	g/d/d.java
http://www.slf4j.org/codes.html#StaticLoggerBinder	g/d/d.java
http://www.slf4j.org/codes.html#multiple_bindings	g/d/d.java
http://www.slf4j.org/codes.html#null_LF	g/d/d.java
http://www.slf4j.org/codes.html#version_mismatch	g/d/d.java
http://www.slf4j.org/codes.html#substituteLogger	g/d/d.java
http://www.slf4j.org/codes.html#loggerNameMismatch	g/d/d.java
http://www.slf4j.org/codes.html#replay	g/d/d.java
http://www.slf4j.org/codes.html#unsuccessfulInit	g/d/d.java
http://rebus007.altervista.org	Android String Resource
https://rebus007.github.io/PermissionUtils	Android String Resource
https://github.com/rebus007/PermissionUtils	Android String Resource

邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libconscrypt_jni.so

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_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.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.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.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.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

向手机申请的权限	是否危险	类型	详细情况
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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_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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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

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
android.permission.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
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.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_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.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.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

签名证书

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

Found 1 unique certificates
Subject: C=4566588, ST=sichuan, L=meishan, O=wbang, OU=wbang, CN=wbang.oem
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-06-08 05:25:38+00:00
Valid To: 2045-06-02 05:25:38+00:00
Issuer: C=4566588, ST=sichuan, L=meishan, O=wbang, OU=wbang, CN=wbang.oem
Serial Number: 0x3899f1b3
Hash Algorithm: sha256
md5: 1981ebba3107486680457b73216e9aaf
sha1: 4c706e186621ba6469b6c695108c34dd68d37983
sha256: f45261f1c44e55538930ca68d2439f57989e81c094e100e634aa8ac7e5b7de2a
sha512: 094a6c95ff69ce842a818f4a3c5ad044620e38ce1b64d3b1fd87909815bdb77dbc7e5ba2a3a745e04bbbf16fb4cf278fc635e21494ccead0017a83c21f6c1785
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: de3bb785db226d184da941c1df2952390fa3bb15cdbd5e81b569eb7bddd322a2

🔑 硬编码敏感信息

可能的敏感信息
"find_password" : "找回密码"
"library_permissionutils_author" : "Raphaël Bussa"
"library_permissionutils_authorWebsite" : "http://rebus007.altervista.org"
"please_input_password" : "请输入密码！"
"ui_authority_app" : "APP端授权"
"ui_authority_content" : "您将切换授权平台为 PC端 授权"
"ui_authority_failed" : "授权失败，请重新再试！"

可能的敏感信息
"ui_authority_pc" : "PC、网页端授权"
"ui_authority_title" : "授权平台切换"

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
