MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

多米盒 1.0.APK

APP名称:	多米盒
包名:	com.chszyx.dmh
域名线索:	15条
URL线索:	18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: duomihe.apk
文件大小: 7.32MB
MD5值: 833e303bf05e3a49c1db7a16a4416b6f
SHA1值: 5e2d5a0dbc91a90eb5cc62dcb4f477211056843b
SHA256值: 3b8c4f555d2ccc56533551dac0f081ffe3aaa67c5f817ea01ca1f26ef0a1767c

APP 信息

App名称: 多米盒
包名: com.chszyx.dmh
主活动**Activity:** com.yibeixxkj.makemoney.activity.MoneySplashActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
m.chzeus.com	good	**IP:** 75.2.18.233 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.606209 经度: -122.332069 查看地图: Google Map

域名	是否危险域名	服务器信息
oss.aliyuncs.com	good	IP: 118.178.29.5 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
alogsus.umeng.com	good	IP: 59.82.29.246 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
ulogs.umeng.com	good	IP: 106.11.86.76 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
plbslog.umeng.com	good	IP: 59.82.43.171 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
oss-cn-.aliyuncs.comor	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
127.0.0.1	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
ulogs.umengcloud.com	good	IP: 106.11.43.144 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
api.chuanhuoapp.com	good	IP: 47.91.170.222 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692 查看地图: Google Map
developer.umeng.com	good	IP: 59.82.31.95 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

域名	是否危险域名	服务器信息
alogus.umeng.com	good	IP: 106.11.86.77 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
image.cnamedomain.com	good	没有服务器地理信息.
cmnsguider.yunos.com	good	IP: 203.119.169.44 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
ouplog.umeng.com	good	IP: 47.74.172.218 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map
oss-cn-hangzhou.aliyuncs.com	good	IP: 118.31.219.248 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/s.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java
https://m.chzeus.com/policy/index.html?type=	com/yibeixxkj/makemoney/ConstantKt.java
https://m.chzeus.com/policy/privacy-agreement.html	com/yibeixxkj/makemoney/ConstantKt.java
https://api.chuanhuoapp.com	com/yibeixxkj/makemoney/net/MaoneyServerApiKt.java
https://m.chzeus.com/policy/index.html?type=2	com/yibeixxkj/makemoney/activity/MoneyAboutOurActivity$onSingleClick$1.java
https://m.chzeus.com/policy/index.html?type=4	com/yibeixxkj/makemoney/activity/MoneyTaskDetailActivity$showPopupDialog$1.java

URL信息	Url所在文件
https://m.chzeus.com/policy/index.html?type=2	com/yibeixxkj/makemoney/activity/MoneyTaskDetailActivity$showPopupDialog$1.java
https://m.chzeus.com/policy/index.html?type=4	com/yibeixxkj/makemoney/dialog/MoneyTaskStepDialog.java
https://ip.	com/alibaba/sdk/android/oss/OSSImpl.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/OSSImpl.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/OSSImpl.java
http://oss.aliyuncs.com	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://127.0.0.1	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://oss-cn-hangzhou.aliyuncs.com	com/alibaba/sdk/android/oss/common/OSSConstants.java

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_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_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.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.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
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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-10-29 06:14:58+00:00
Valid To: 2119-10-05 06:14:58+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Serial Number: 0x30f38108
Hash Algorithm: sha256
md5: 21794ec049d310e4dccb7156d623bf6d
sha1: f3c0dd4e8dc9d5e506344a4ef8547680fd44762a
sha256: 92d9b7c80592e1d48eeadd6e125365318033e51d3b6a5f5d047bd88e50c9c9a6
sha512: 7f922517b3bad15dc088fc32c7fa3adf1fe06a8ef28427ca283d4ae4469920d091bdd988b9a2d991c8cc7241e2dfc0f8e1b6ca7f6dfdcc1a49a5bd80a78a04b4
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 04bd2a439b482a079f2e66b99e9106b8b64d6c0722715614277d4e9bbca5a84b

Exodus威胁情报

名称	分类	URL链接
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

加壳分析

文件列表	分析结果

<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.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
