

## APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



₩ 蜂巢美云 Failed.APK

APP名称: 蜂巢美云

包名: Failed

域名线索: 2条

URL线索: 4条

邮箱线索: 0条

分析日期: 2022年2月2日 19:45

文件名: fengchaomeiyun584407.apk

文件大小: 7.46MB

MD5值: 7d0cc192647072bd44337969e42fae3b

SHA1值: 065783037683a31203cd99c4881d30f61c2b85e6

**SHA256**值: fdb73886b4fd5ffa9b68914d3f037b0fa3d72a2707dc9eef9bc679f42db83476

#### i APP 信息

App名称: 蜂巢美云

包名: Failed 主活动**Activity:** 

安卓版本名称: Failed 安卓版本: Failed

#### 0 域名线索

域名	是否危险域名	服务器信息
errlogos.umeng.com	good	IP: 47.246.110.18  所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 结度: 22.285521 经度: 114.157692 查看地图: Google Map

域名	是否危险域名	服务器信息
errlog.umeng.com	good	IP: 106.8.130.60 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810001 经度: 114.879440 查看地图: Google Map

## **URL**线索

URL信息	Url所在文件
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/x86/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/x86/libcrashsdk.so
https://errlog.umeng.com	lib/x86/libcrashsdk.so
https://errlogos.umeng.com	lib/x86/libcrashsdk.so

URL信息	Url所在文件
https://errlog.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlog.umeng.com	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com	lib/arm64-v8a/libcrashsdk.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi/libcrashsdk.so



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

Found 1 unique certificates

Subject: C=21000, ST=js, L=nj, O=gs, OU=js, CN=zhou

Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2021-09-09 07:49:35+00:00 Valid To: 2046-09-03 07:49:35+00:00

Issuer: C=21000, ST=js, L=nj, O=gs, OU=js, CN=zhou

Serial Number: 0x1495cda7 Hash Algorithm: sha256

md5: 5325f8cdff1d83837a3ed619576c15fc

sha1: 087411b049ed313e3b2acba003ba64032cbd2652

sha256: d97245971a1f5d8b51907df929d43bd4d4129faae4d4bb44ac2f9723bb18847d

sha512: d436c83eeedc3b842b785e03169ccf15ab64ceb61bb534264476d334b40bd64eb1a822302f5d48dc002c91aa7a4391c62a65e733ddb48ceb2e4e0c24ce1143f2

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 8ceae2f1e46c64fa104db49a14ee404b12702827b3f9090cfdf3f510686c1bbc

# **益** Exodus威胁情报

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

### **命**加壳分析

文件列表	分析结果
------	------

文件列表	分析结果		
	売列表 详细情	青况	
classes.dex	Build.M Build.M Build.P Build.B 反虚拟机 Build.B possibl Build.T SIM op networ	INGERPRINT check MODEL check MANUFACTURER check RODUCT check MARDWARE check OARD check e Build.SERIAL check AGS check erator check k operator name check ber ID check	
	编译器 r8		
classes2.dex	売列表 详细情	青况	
	编译器 r8 with	out marker (suspicious)	

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