MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Fuhu 1.5.0.APK

APP名称:	Fuhu
包名:	net.funhub
域名线索:	13条
URL线索:	17条
邮箱线索:	0条
分析日期:	2022年1月28日 22:03

文件信息

文件名: fuhu585249.apk
文件大小: 5.89MB
MD5值: cbd2ed51455f61bc67ae74a28dae6686
SHA1值: 63ad3f29e3e5ee60f15bcf55036076cc0a2fa435
SHA256值: 84806c2ced83a8e6c1681602a03af804bdacb6b981de076c5fa9d89bcc09685b

APP 信息

App名称: Fuhu
包名: net.funhub
主活动**Activity:** net.funhub.MainActivity
安卓版本名称: 1.5.0
安卓版本: 13

域名线索

域名	是否危险域名	服务器信息
appleid.apple.com	good	**IP:** 17.141.5.102 **所属国家:** United States of America **地区:** California **城市:** Cupertino **纬度:** 37.316605 **经度:** -122.046486 **查看地图:** Google Map

域名	是否危险域名	服务器信息
pagead2.googlesyndication.com	good	**IP:** 220.181.174.102 **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
schemas.android.com	good	没有服务器地理信息.
pinterest.com	good	**IP:** 31.13.85.53 **所属国家:** Brazil **地区:** Sao Paulo **城市:** Sao Paulo **纬度:** -23.547501 **经度:** -46.636108 **查看地图:** Google Map
app-measurement.com	good	**IP:** 220.181.174.161 **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
ns.adobe.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
goo.gl	good	**IP:** 142.251.43.14 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
cliphub-98093-default-rtdb.firebaseio.com	good	**IP:** 35.201.97.85 **所属国家:** United States of America **地区:** Missouri **城市:** Kansas City **纬度:** 39.099731 **经度:** -94.578568 **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
www.facebook.com	good	**IP:** 108.160.165.139 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map

域名	是否危险域名	服务器信息
twitter.com	good	**IP:** 157.240.6.35 **所属国家:** Colombia **地区:** Distrito Capital de Bogota **城市:** Bogota **纬度:** 4.609710 **经度:** -74.081749 **查看地图:** Google Map
plus.google.com	good	**IP:** 162.125.32.6 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map
play.google.com	good	**IP:** 142.251.42.238 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
https://appleid.apple.com/auth/authorize	com/RNAppleAuthentication/h.java

URL信息	Url所在文件
https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/h.java
https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/j.java
http://ns.adobe.com/xap/1.0/	b/k/a/a.java
http://schemas.android.com/apk/res/android	b/g/e/e/g.java
https://goo.gl/J1sWQy	d/b/a/d/f/h/c3.java
https://app-measurement.com/a	d/b/a/d/f/h/wc.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	d/b/a/d/a/a/b.java
https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/f/b.java
https://pinterest.com/pin/create/button/?url={url}&media=$media&description={message}	cl/json/f/k.java
https://plus.google.com/share?url={url}	cl/json/f/f.java
https://play.google.com/store/apps/details?id=com.instagram.android	cl/json/f/h.java
https://play.google.com/store/apps/details?id=com.instagram.android	cl/json/f/g.java
https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/f/c.java
https://twitter.com/intent/tweet?text={message}&url={url}	cl/json/f/q.java
https://cliphub-98093-default-rtdb.firebaseio.com	Android String Resource

数据库线索

FIREBASE链接地址	详细信息
https://cliphub-98093-default-rtdb.firebaseio.com	info App talks to a Firebase Database.

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.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.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.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
com.android.vending.CHECK_LICENSE	未知	Unknown permission	Unknown permission from android reference
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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限

向手机申请的权限	是否危险	类型	详细情况
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-04-06 10:25:00+00:00
Valid To: 2051-04-06 10:25:00+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x31d55753a71da78cb167c4d6858eab6f72ea5c8f
Hash Algorithm: sha256
md5: d2e17ae774391c62e49fd1ed063ca41a
sha1: 6f0c749447f72e9fb0ddd0a8d8525a236a6c633c
sha256: 0fb5e7b41e431649b734906206b9489e2b5efbd4b88f5e4a9aa7e0e92547b2ca
sha512: 3f32286369814b4e7884006d29bd5a62d672bececf2f6bcd37e1bcbcb4aeb1c2360ac0d0c6b2eba62ec2cc6e3e211b3c9a30a21e752a31a6c07206bc0b83d27c
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 4bf31352f2981b2cf128460b80bcf4478cf0e2935663f33ae7e77567229b0673

Exodus威胁情报

名称	分类	URL链接
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

硬编码敏感信息

可能的敏感信息
"com_facebook_device_auth_instructions" : "Visit facebook.com/device and enter the code shown above."
"facebook_client_token" : "08d7217f3e04ca046b65b24b7a03f8fb"
"firebase_database_url" : "https://cliphub-98093-default-rtdb.firebaseio.com"
"google_api_key" : "AIzaSyCSrFERM3Xwukdw4yguhdxpmfQ9TksDpo4"
"google_crash_reporting_api_key" : "AIzaSyCSrFERM3Xwukdw4yguhdxpmfQ9TksDpo4"

应用内通信

活动(ACTIVITY)	通信(INTENT)
net.funhub.MainActivity	Schemes: https://, Hosts: funhub.net, m.funhub.net, fuhuz.com, m.fuhuz.com, Path Prefixes: /channel, /kenh, /video, /movie, /phim, /comic, /truyen, /post, /bai-viet, /comic-chapter, /movie-eps,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.net.funhub,

加壳分析

文件列表	分析结果
classes.dex	<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.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check possible VM check</td></tr><tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>编译器</td><td>unknown (please file detection issue!)</td></tr></table>

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