MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

HYFYFM 1.0.1.APK

APP名称:	HYFYFM
包名:	com.hyfyfm.hyfyfmlive
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2022年1月28日 22:21

文件信息

文件名: hyfyfm539566.apk
文件大小: 11.04MB
MD5值: 9c7d0aba151b38ad2483615cb670e40c
SHA1值: b5132c55346311f83a2a64c71e7c7492e0daede3
SHA256值: 20e86aac02042ece91ea97cbeacc6e8dc562dc4356d17ceb6cb2b3cb19d66dd5

APP 信息

App名称: HYFYFM
包名: com.hyfyfm.hyfyfmlive
主活动**Activity:** com.hyfyfm.hyfyfmlive.activities.SplashScreen
安卓版本名称: 1.0.1
安卓版本: 2

域名线索

域名	是否危险域名	服务器信息
hyfytv-8a200.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

URL线索

URL信息	Url所在文件
https://hyfytv-8a200.firebaseio.com	Android String Resource

数据库线索

FIREBASE链接地址	详细信息
https://hyfytv-8a200.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.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.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

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.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.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.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.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.hyfyfm.hyfyfmlive.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.android.alarm.permission.SET_ALARM	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=IN, ST=Chandigarh, L=Chandigarh, CN=Manpreet Singh
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-06-29 14:43:04+00:00
Valid To: 2043-06-23 14:43:04+00:00
Issuer: C=IN, ST=Chandigarh, L=Chandigarh, CN=Manpreet Singh
Serial Number: 0x4d2a2eb1
Hash Algorithm: sha256
md5: 95ceeba1e3aa6670390b011dd36028fe
sha1: c95e499c32a2e571951786f7e4326b14b53138e1
sha256: 78509e89ea935d09f95ed97b999df7099da6646815e7e587e9fe1126d7721358
sha512: 95a696e15871474be677cfa313f11e4ccd1526c86756a1d127ce2468c8e947317f3ddcad717719566c1886dce41d197fe0a9bb2625c20014f6193718265051ba
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 3a53dedeb2fa0ea26e0a648fdcb2df31b4465271a33cbc00c5f1a0e397d921eb

Exodus威胁情报

名称	分类	URL链接
AdColony	Advertisement	https://reports.exodus-privacy.eu.org/trackers/90
Adincube		https://reports.exodus-privacy.eu.org/trackers/165
AerServ	Advertisement	https://reports.exodus-privacy.eu.org/trackers/196
Amazon Advertisement		https://reports.exodus-privacy.eu.org/trackers/92
AppLovin (MAX and SparkLabs)	Analytics, Profiling, Identification, Advertisement	https://reports.exodus-privacy.eu.org/trackers/72

名称	分类	URL链接
Appnext		https://reports.exodus-privacy.eu.org/trackers/184
ChartBoost		https://reports.exodus-privacy.eu.org/trackers/53
Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Integral Ad Science		https://reports.exodus-privacy.eu.org/trackers/218
Moat	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/61
Ogury Presage		https://reports.exodus-privacy.eu.org/trackers/34
Tapjoy		https://reports.exodus-privacy.eu.org/trackers/199
Twitter MoPub	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/35
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121
Vungle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/169

🔑 硬编码敏感信息

可能的敏感信息
"add_api_key" : "f7c3ddabfeb04c16833f"
"appnxt_s3t1_install" : "Install"
"appnxt_s3t1_thanks_for_watching" : "Thanks for watching!"
"appnxt_s3t2_install" : "Install"
"appnxt_s3t2_thanks_for_watching" : "Thanks for watching!"
"firebase_database_url" : "https://hyfytv-8a200.firebaseio.com"
"google_api_key" : "AIzaSyCLEIN8zWMtxHJwhCWzf9pRkdS9G7m8wwE"
"google_crash_reporting_api_key" : "AIzaSyCLEIN8zWMtxHJwhCWzf9pRkdS9G7m8wwE"

加壳分析

文件列表	分析结果

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 possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check</td></tr><tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr></table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes2.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.PRODUCT check
Build.BOARD check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>模糊器</td><td>unreadable field names
unreadable method names</td></tr>
</table>
</td></tr>
</table>
