MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Tameshk 1.5.0.APK

APP名称:	Tameshk
包名:	com.rosha.tameshk
域名线索:	7条
URL线索:	14条
邮箱线索:	1条
分析日期:	2022年1月28日 23:19

文件信息

文件名: tameshk550731.apk
文件大小: 7.11MB
MD5值: c2d4a6addaaf4f572841dd7b072202e7
SHA1值: 849ea28863dc42a32e3be1ee3d69d82312426f25
SHA256值: bdec069a0cedbed7861dcdac8b4483ce436d8d5b82c81da6f1866a482ab7524a

APP 信息

App名称: Tameshk
包名: com.rosha.tameshk
主活动**Activity:** com.rosha.tameshk.activities.splash.SplashActivity
安卓版本名称: 1.5.0
安卓版本: 5

域名线索

域名	是否危险域名	服务器信息
minigame-b9eff.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

域名	是否危险域名	服务器信息
google.github.io	good	**IP:** 185.199.111.153 **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
beshnavim.com	good	没有服务器地理信息.
google.com	good	**IP:** 172.217.160.110 **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
tameshk.info	good	没有服务器地理信息.
tameshksocial.ir	good	没有服务器地理信息.
cdn.bamdad.net	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://google.com	com/worldsnas/forceupdate/ForceUpdateService.java

URL信息	Url所在文件
http://google.com	com/worldsnas/forceupdate/activity/c.java
http://google.com	com/worldsnas/forceupdate/activity/a.java
http://tameshk.info/	com/rosha/tameshk/app/b/e.java
http://tameshk.info:8080/	com/rosha/tameshk/app/b/e.java
http://tameshk.info/static/pages/privacy_policy	com/rosha/tameshk/activities/setting/SettingActivity.java
http://tameshk.info/static/pages/rules	com/rosha/tameshk/activities/setting/SettingActivity.java
http://tameshk.info/errors/banned/	com/rosha/tameshk/activities/splash/SplashActivity.java
http://tameshk.info/api/v1/utils/version_check	com/rosha/tameshk/activities/splash/SplashActivity.java
http://cdn.bamdad.net/tameshk/avatar/null	com/rosha/tameshk/activities/chat/otherchat/OtherChatVH.java
http://cdn.bamdad.net/tameshk/avatar/null	com/rosha/tameshk/activities/chat/selfchat/SelfChatVH.java
https://google.github.io/dagger/testing	b/a/b.java
https://minigame-b9eff.firebaseio.com	Android String Resource
http://beshnavim.com/apk.apk?test	Android String Resource
http://tameshksocial.ir/download	Android String Resource

邮箱线索

邮箱地址	所在文件
sdk@jwplayer.com	Android String Resource

数据库线索

FIREBASE链接地址	详细信息
https://minigame-b9eff.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.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.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

向手机申请的权限	是否危险	类型	详细情况
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_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	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
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.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.rosha.tameshk.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=98, ST=itparsa, L=itparsa, O=itparsa, OU=itparsa, CN=itparsa
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-01-18 11:37:22+00:00
Valid To: 2043-01-12 11:37:22+00:00
Issuer: C=98, ST=itparsa, L=itparsa, O=itparsa, OU=itparsa, CN=itparsa
Serial Number: 0x2e30c33a
Hash Algorithm: sha256
md5: 10547ccefe670f759015c702c3f26f9e
sha1: 1b4ea6fb3af18e544ee5a524ae439df511a571a6
sha256: 2a195960e1e22799b13e5afe7b39074adba32b0d22f0bc38e12a7ae5def8caab
sha512: 7dd14befb2180897d6ae3b7a1408eedcf94f00aff0cab3363b9eeb9210f879950e9006ed275919bfaa67b3503452f3127d33feb03607dd890a4c86c47f2a981d
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b1a72a08645be87b5c05720b653cb23e405c4b679df84a8cccf6294beacf1f14

Exodus威胁情报

名称	分类	URL链接
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
"block_by_user" : "شما توسط این کاربر مسدود شده اید"
"block_user" : "شما مسدود شده اید"
"exist_user" : "کاربر موجود است لطفااز قسمت ورود وارد شوید"
"firebase_database_url" : "https://minigame-b9eff.firebaseio.com"
"forget_password" : "رمز خود را فراموش کرده ام"
"google_api_key" : "AIzaSyCfIMXQmxNQ7jVdkQGp38WM1SEDbVdAtEI"
"google_crash_reporting_api_key" : "AIzaSyCfIMXQmxNQ7jVdkQGp38WM1SEDbVdAtEI"
"insert_correct_user_name" : "نام کاربری نباید با عدد شروع شود"
"insert_user_name" : "نام کاربری خود را وارد نمایید"
"login_with_username" : "ورود با حساب کاربری"
"not_valid_retry_user_password" : "تکرار کلمه عبور نادرست است"
"not_valid_user_name" : "نام کاربری نادرست است"
"not_valid_user_password" : "کلمه عبور نادرست است"
"private_information" : "اطلاعات خصوصی"
"private_privacy" : "سیاست حفظ حریم خصوصی"

可能的敏感信息
"register_with_username" : "ثبت نام با حساب کاربری"
"setting_password" : "تغییر کلمه عبور"
"submit_user_name" : "ثبت نام کاربری"
"success_submitting_user_name" : "نام کاربری با موفقیت ثبت شد"
"user_name" : "نام کاربری"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.rosha.tameshk.activities.splash.SplashActivity	Schemes: tmk://, http://, https://, Hosts: dl, www.tameshk.info, tameshk.info, Path Prefixes: /dl/, Path Patterns: /{id},

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.MANUFACTURER check</td></tr>
<tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
