南明离火
移动应用检测平台

ANDROID 静态分析报告

Space War Ship • v1.0

分析日期: 2024-03-28 10:35:56

应用概览

文件名称:	8fc9cc71999c07db3ae09878db4cb762816df766a1d9e25f80675fc2ed412ffb.apk
文件大小:	7.03MB
应用名称:	Space War Ship
软件包名:	batch.arcade.space.war.ship.combat
主活动:	com.qbiki.seattleclouds.AppStarterActivity
版本号:	1.0
最小SDK:	10
目标SDK:	17
加固信息:	未加壳
应用程序安全分数:	36/100 (高风险)
跟踪器检测:	5/432
杀软检测:	9 个杀毒软件报毒
MD5:	196ffced350d273ffd6133645b2b5940
SHA1:	2556a664acd8e94ed22af5181e4[illegible]8ea274fd43
SHA256:	8fc9cc71999c07db3ae09878db4cb762816df766a1d9e25f80675fc2ed412ffb

分析结果严重性分布

高危	中危	信息	安全	关注
8	15	1	1	4

四大组件导出状态统计

Activity组件：29个，其中export的有：3个
Service组件：3个，其中export的有：0个
Receiver组件：3个，其中export的有：1个
Provider组件：2个，其中export的有：1个

应用签名证书信息

二进制文件已签名
v1 签名: True

本报告由南明离火移动安全分析平台生成

v2 签名: False
v3 签名: False
v4 签名: False
主题: CN=Keah HB
签名算法: rsassa_pkcs1v15
有效期自: 2014-08-20 17:22:16+00:00
有效期至: 2042-01-05 17:22:16+00:00
发行人: CN=Keah HB
序列号: 0x76a2166a
哈希算法: sha256
证书MD5: 49a8230617b268522c5fd117cf5126d9
证书SHA1: defad55ea8c4741947d16fb59a3f9939c9f0c6be
证书SHA256: 52924e53260486419cbab9b8c36dbfb94a248ae4ed3b197513d19e73f4057eea
证书SHA512:
c1581378cd26f6cebe715de72a630599131e28d43009b72e93e50097dd7276aa23b13fe34ee953015d15ff87de72d9b494c146b5[illegible]6463190eb7dab813bf2fe1c

找到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
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.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
batch.arcade.space.war.ship.combat.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.qbiki.paypal.PayPalMessage	Schemes: mobile-appbuilder.hbkeah14.gamesapp039://,

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: 1 | 警告: 0 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名

应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: **3** | 警告: **6** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 2.3.3-2.3.7, [minSdk=10]	警告	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 <= 10、API 29 以接收合理的安全更新。
2	Activity (com.qbiki.modules.search.SearchActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (17) 更新到 29 或更高版本以在平台级别修复此问题。
3	Activity (com.qbiki.modules.search.SearchActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
4	Activity (com.qbiki.paypal.PayPalMessage) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (17) 更新到 29 或更高版本以在平台级别修复此问题。
5	Activity (com.qbiki.paypal.PayPalMessage) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
6	Activity (net.sourceforge.zbar.android.ZBarScanner) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (17) 更新到 29 或更高版本以在平台级别修复此问题。
7	Activity (net.sourceforge.zbar.android.ZBarScanner) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
8	Content Provider (com.qbiki.util.InternalFileContentProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
9	Broadcast Receiver (com.qbiki.gcm.GCMBroadcastReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

代码安全漏洞检测

高危: **3** | 警告: **8** | 信息: **1** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
3	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
4	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	升级会员：解锁高级权限
5	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
6	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
7	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
8	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

9	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
10	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
11	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
12	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
13	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.GET_ACCOUNTS
其它常用权限	4/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

恶意域名威胁检测

域名	状态	中国境内	位置信息
www.google-analytics.com	安全	是	**IP地址:** 180.163.151.33 **国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.224333 **经度:** 121.469139 **查看:** 高德地图

example.com	安全	否	**IP地址:** 93.184.216.34 **国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
lbdb.pollfish.com	安全	否	**IP地址:** 173.255.115.49 **国家:** United States of America **地区:** Iowa **城市:** Council Bluffs **纬度:** 41.261940 **经度:** -95.860839 **查看:** Google 地图
www.wireless-village.org	安全	否	**IP地址:** 104.21.11.240 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
media.admob.com	安全	否	**IP地址:** 142.250.141.100 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
s.ytimg.com	安全	否	**IP地址:** 142.250.68.78 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
purl.org	安全	否	**IP地址:** 207.241.239.241 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.781734 **经度:** -122.459435 **查看:** Google 地图
schemas.xmlsoap.org	安全	否	**IP地址:** 13.107.213.71 **国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看:** Google 地图
www.amazon.com	安全	否	**IP地址:** 13.225.150.180 **国家:** United States of America **地区:** California **城市:** Los Angeles **纬度:** 34.052860 **经度:** -118.243568 **查看:** Google 地图

wss.pollfish.com	安全	否	**IP地址:** 34.69.135.100 **国家:** United States of America **地区:** Iowa **城市:** Council Bluffs **纬度:** 41.261940 **经度:** -95.860832 **查看:** Google 地图
market.android.com	安全	否	**IP地址:** 142.250.68.78 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
www.onbarcode.com	安全	否	**IP地址:** 47.90.243.155 **国家:** United States of America **地区:** California **城市:** San Mateo **纬度:** 37.547424 **经度:** -122.330589 **查看:** Google 地图
www.googletagmanager.com	安全	是	**IP地址:** 180.163.150.41 **国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.224333 **经度:** 121.469139 **查看:** 高德地图
ssl.google-analytics.com	安全	是	**IP地址:** 180.163.150.169 **国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.224333 **经度:** 121.469139 **查看:** 高德地图
www.starbucks.com	安全	否	**IP地址:** 23.222.168.30 **国家:** United States of America **地区:** California **城市:** El Segundo **纬度:** 33.919182 **经度:** -118.416473 **查看:** Google 地图
www.daisy.org	安全	否	**IP地址:** 65.52.139.180 **国家:** Netherlands **地区:** Noord-Holland **城市:** Amsterdam **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
schemas.microsoft.com	安全	否	**IP地址:** 13.105.221.22 **国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看:** Google 地图

www.upcdatabase.org	安全	否	**IP地址:** 104.21.64.53 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
android.revmob.com	安全	否	No Geolocation information available.
i.ytimg.com	安全	否	**IP地址:** 142.250.217.150 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.40599 **经度:** -122.078514 **查看:** Google 地图
googleads.g.doubleclick.net	安全	是	**IP地址:** 180.163.150.38 **国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.224333 **经度:** 121.469139 **查看:** 高德地图
www.openmobilealliance.org	安全	否	**IP地址:** 104.26.8.105 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
revmob.com	安全	否	No Geolocation information available.
www.idpf.org	安全	否	**IP地址:** 217.70.184.56 **国家:** France **地区:** Ile-de-France **城市:** Paris **纬度:** 48.858364 **经度:** 2.294532 **查看:** Google 地图
goo.gl	安全	否	**IP地址:** 142.250.176.14 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
s3.amazonaws.com	安全	否	**IP地址:** 52.217.224.112 **国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图

www.wapforum.org	安全	否	**IP地址:** 172.67.190.29 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• http://www.opensource.org/licenses/mit-license.php • http://bassistance.de/jquery-plugins/jquery-plugin-validation/ • http://www.wapforum.org/DTD/xhtml-mobile10.dtd • http://www.apple.com/DTDs/PropertyList-1.0.dtd • http://projects.scottsplayground.com/iri/ • http://sizzlejs.com/ • http://jquery.org/license • http://projects.scottsplayground.com/email_address_validation/ • http://www.gnu.org/licenses/gpl.html	自研引擎分析结果
• https://www.amazon.com/appstore-error-help	com/amazon/android/framework/prompt/e.java
• http://www.onbarcode.com • http://www.onbarcode.com/products/android_barcode/	com/onbarcode/barcode/android/LicenseInformation.java
• https://developer.android.com/google/play-services/setup.html#ensure	com/pollfish/c/a.java
• http://lbdb.pollfish.com:3000/notifier_api/v2/notices • http://lbdb.pollfish.com:3000	com/pollfish/f/b/a.java
• javascript:pollfish.nativeaccess.losefocus(true	com/pollfish/g/a.java
• https://wss.pollfish.com	com/pollfish/main/PollFish.java
• data:image/jpg;base64	com/qbiki/feedback/FieldProcessing.java
• http://www.upcdatabase.org/api/xml/30a634c9cad463a5e5c7afb2496ff2/	com/qbiki/modules/barcodescanner/BarcodeScannerFragment.java
• https://graph.facebook.com/%1$s?fields=name,picture&accesstoken=%2$s • https://graph.facebook.com/%1$s/likes?limit=0&summary=1&accesstoken=%2$s • https://graph.facebook.com/%1$s/comments?limit=0&summary=1&accesstoken=%2$s	com/qbiki/modules/facebookfeeds/FeedsListFragment.java
• data:image/png;base64 • javascript:document.getelementbyid('stable').contentwindow.document.getelementbyid(' • javascript:document.getelementbyid(	com/qbiki/modules/favorites/Favorites.java
• http://graph.facebook.com/	com/qbiki/modules/fbfanpage/FacebookFunPageFragment.java
• javascript:karaokejsinterface.linetimesparsed(getlinetimes	com/qbiki/modules/karaoke/KaraokeFragment.java
• http://www.wapforum.org/dtd/xhtml-mobile10.dtd	com/qbiki/modules/sharepoint/SPListViewAdapter.java

• http://schemas.microsoft.com/sharepoint/soap/getlistcollection • http://schemas.microsoft.com/sharepoint/soap/getlistitems • http://schemas.microsoft.com/sharepoint/soap/getlistandview • http://schemas.microsoft.com/sharepoint/soap/getwebcollection • http://schemas.microsoft.com/sharepoint/soap/updatelistitems • http://schemas.microsoft.com/sharepoint/soap/getitem • http://schemas.microsoft.com/sharepoint/soap/copyintoitems • http://schemas.microsoft.com/sharepoint/soap/	com/qbiki/modules/sharepoint/SPServer.java
• javascript:window.htmlout.showhtml(document.getelementbyid('fetch_balance').getelementsbytagname('span' • https://www.starbucks.com/card	com/qbiki/modules/starbucks/ViewCardActivity.java
• http://market.android.com/details?id=	com/qbiki/seattleclouds/AppStarterActivity.java
• http://s.ytimg.com/yt/m/cssbin/mobile-blazer-sprite • http://s.ytimg.com/yt/m/cssbin/mobile-swatch-sprite • http://s.ytimg.com/yt/cssbin/mobile-swatch-sprite • http://s.ytimg.com/yts/imgbin/mobile-nightshade • http://i.ytimg.com/vi/ • javascript:document.getelementbyid('rsstable').contentwindow.document.getelementbyid(' • javascript:document.getelementbyid('	com/qbiki/seattleclouds/WebViewFragment.java
• javascript:document.getelementbyid	com/qbiki/shoppingcart/ShoppingCart.java
• http://revmob.com	com/revmob/client/InstallClientListener.java
• https://android.revmob.com • http://revmob.com	com/revmob/client/RevMobClient.java
• https://s3.amazonaws.com/www.revmob.com/revmob_i_agree_terms.txt	com/revmob/internal/HTTPHelper.java
• http://www.daisy.org/z3986/2005/ncx/	nl/siegmann/epublib/epub/NCXDocument.java
• http://purl.org/dc/elements/1.1/ • http://www.idpf.org/2007/opf	nl/siegmann/epublib/epub/PackageDocumentBase.java
• http://schemas.xmlsoap.org/soap/encoding/ • http://schemas.xmlsoap.org/soap/envelope/	org/ksoap2/SoapEnvelope.java
• http://www.wireless-village.org/csp • http://www.wireless-village.org/pa • http://www.wireless-village.org/trc • http://www.openmobilealliance.org/dtd/wv-csp • http://www.openmobilealliance.org/dtd/wv-pa • http://www.openmobilealliance.org/dtd/wv-trc • www.wireless-village.org	org/kxml2/wap/wv/WV.java
• https://graph.facebook.com/%1$s/comments?limit=0&summary=1&accesstoken=%2$s • javascript:cordova.fireDocumentEvent('backbutton' • http://lbdb.pollfish.com:3000/notifier_api/v2/notices • https://www.googletagmanager.com • 127.0.0.1 • http://www.wireless-village.org/csp • https://s3.amazonaws.com/www.revmob.com/revmob_i_agree_terms.txt • javascript:document.getelementbyid(' • javascript:cordova.firedocumentevent('searchbutton' • http://www.idpf.org/2007/opf • http://schemas.microsoft.com/sharepoint/soap/ • http://market.android.com/details?id=	

本报告由南明离火移动安全分析平台生成

- http://goo.gl/nafqqk
- http://schemas.microsoft.com/sharepoint/soap/getitem
- javascript:karaokejsinterface.linetimesparsed(getlinetimes
- javascript:cordova.firedocumentevent('volumeupbutton'
- http://schemas.microsoft.com/sharepoint/soap/updatelistitems
- http://www.daisy.org/z3986/2005/ncx/
- http://www.onbarcode.com
- http://www.wireless-village.org/pa
- https://graph.facebook.com/%1$s?fields=name,picture&accesstoken=%2$s
- www.wireless-village.org
- http://www.onbarcode.com/products/android_barcode/
- http://schemas.xmlsoap.org/soap/encoding/
- javascript:cordova.firedocumentevent('volumedownbutton'
- https://www.amazon.com/appstore-error-help
- http://revmob.com
- http://hostname/?
- https://graph.facebook.com/
- http://schemas.microsoft.com/sharepoint/soap/copyintoitems
- http://schemas.xmlsoap.org/soap/envelope/
- http://www.wapforum.org/dtd/xhtml-mobile10.dtd
- http://schemas.microsoft.com/sharepoint/soap/getwebcollection
- data:image/jpg;base64
- javascript:try{cordova.firedocumentevent('pause');}catch(e){console.log('exception
- http://schemas.microsoft.com/sharepoint/soap/getlistandview
- http://i.ytimg.com/vi/
- javascript:cordova.firedocumentevent('menubutton'
- javascript:window.htmlout.showhtml(document.getelementbyid('fetch_balance').getelementsbytagname('span'
- javascript:document.getelementbyid('rsstable').contentwindow.document.getelementbyid('
- javascript:try{cordova.firedocumentevent('resume');}catch(e){console.log('exception
- http://s.ytimg.com/yts/imgbin/mobile-nightshade
- http://lbdb.pollfish.com:3000
- javascript:pollfish.nativeaccess.losefocus(true
- http://s.ytimg.com/yt/m/cssbin/mobile-swatch-sprite
- http://schemas.microsoft.com/sharepoint/soap/getlistcollection
- http://purl.org/dc/elements/1.1/
- javascript:afma_receivemessage('
- https://developer.android.com/google/play-services/setup.html#ensure
- http://plus.google.com/
- http://schemas.microsoft.com/sharepoint/soap/getlistitems
- javascript:document.getelementbyid
- https://www.starbucks.com/card
- http://www.openmobilealliance.org/dtd/wv-trc
- http://cdv_exec/
- javascript:try{cordova.require('cordova/channel').ondestroy.fire();}catch(e){console.log('exception
- http://www.openmobilealliance.org/dtd/wv-csp
- http://www.openmobilealliance.org/dtd/wv-pa
- http://graph.facebook.com/
- http://s.ytimg.com/yt/m/cssbin/mobile-blazer-sprite
- data:image/png;base64
- http://s.ytimg.com/yt/cssbin/mobile-swatch-sprite
- https://api.facebook.com/restserver.php
- https://graph.facebook.com/%1$s/likes?limit=0&summary=1&accesstoken=%2$s
- http://www.wireless-village.org/trc
- http://developers.facebook.com/docs/reference/rest/
- https://m.facebook.com/dialog/
- https://wss.pollfish.com
- https://android.revmob.com
- http://www.ivsoftabase.org/api/xml/30a634c9cad463a5e5d5c7afb2496ff2/

自研引擎分析结果

第三方 SDK 组件分析

SDK名称	开发者	描述信息
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。

邮箱地址敏感信息提取

EMAIL	源码文件
dimame032@gmail.com	com/qbiki/modules/order/OrderFragment.java
example@mail.com	com/qbiki/modules/product/order/POGeneralInfo.java
dimame032@gmail.com example@mail.com myemail@mail.com	自研引擎分析结果

第三方追踪器检测

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
Pollfish	Profiling	https://reports.exodus-privacy.eu.org/trackers/305
Revmob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/263

敏感凭证泄露检测

可能的密钥
谷歌地图的 "com.google.android.maps.v2.API_KEY" : "@string/google_maps_v2_api_key"
"username" : "hbkeah1"
"fb_api_key" : "2687[redacted]4893"
"google_maps_api_key" : "0jbe4NyXN[redacted]_lPyfn_mg"
"google_maps_v2_api_key" : "AIza[redacted]"
"app_licensing_public_key" : ""
"sc_api_key" : "s1[redacted]"
"auth_client_requested_by_msg" : "%1$sによるリクエスト"
"auth_client_using_bad_version_title" : "[redacted]"
"auth_client_needs_enabling_title" : "[redacted]"

"auth_client_needs_installation_title" : "[redacted]"
"auth_client_requested_by_msg" : "「%1$s」提出要求"
"auth_client_requested_by_msg" : "由“%1$s”发出"
"auth_client_requested_by_msg" : "提出要求的應用程式：%1$s"
Y29tLmFuZHJvaWQudmVuZGluZy5saWNlbnNpbmcuSUxpY2Vuc2luZ1NlcnZpY2U=
30a634c9cad463a5e5d5c7afb2496ff2
3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b13084661636536 5626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e3020170d3039303833313231353231365a180f32303530303933235231353231365a307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b13084661636536 5626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c207d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66b99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de2018ebbb0d5a77c261bd97581ccfef76afc7135ba6d5 3855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864886f70d0101040500038181009ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be5559e21416164839989 4d4673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe a7750 5916c07940656b5811745 b42bd928a2
boundary=3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
AIzaSyDcbnDqRozxjlddKHhKwfQEflvej1qd8A
E213051E4666E9872FA6F50E57A3102C
8288f9f5ef393b70d5121604a25da736

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。