MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

MyDress 2.65.0.APK

APP名称:	MyDress
包名:	hk.com.nineyi.shop.s000020
域名线索:	46条
URL线索:	66条
邮箱线索:	3条
分析日期:	2022年1月25日 22:22

文件信息

文件名: mydress592069.apk
文件大小: 15.41MB
MD5值: ba85e12b58fb62a6a5b88d080a137974
SHA1值: e3183e0acd8d12c8d98caa7fbd2b499a566fd078
SHA256值: 826adabbe6f19366c0ebb5a4efbfa73ce1d5edb27108ec99ea98b91e8b8d87ed

APP 信息

App名称: MyDress
包名: hk.com.nineyi.shop.s000020
主活动**Activity:** com.nineyi.WelcomePageActivity
安卓版本名称: 2.65.0
安卓版本: 18

域名线索

域名	是否危险域名	服务器信息
prod-redirect.tappaysdk.com	good	**IP:** 143.204.86.49 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map

域名	是否危险域名	服务器信息
www.facebook.com	good	IP: 202.160.128.203 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map
tw.91app.com	good	IP: 143.204.86.129 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map
aiqua-recommendation.c.appier.net	good	IP: 54.151.179.205 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map
jdom.org	good	IP: 208.95.104.182 所属国家: United States of America 地区: Oregon 城市: Corvallis 纬度: 44.517742 经度: -123.298096 查看地图: Google Map

域名	是否危险域名	服务器信息
mobilegw.alipay.com	good	IP: 203.209.250.2 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
graph.facebook.com	good	IP: 199.96.59.61 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446 查看地图: Google Map
www.w3.org	good	IP: 128.30.52.100 所属国家: United States of America 地区: Massachusetts 城市: Cambridge 纬度: 42.365078 经度: -71.104523 查看地图: Google Map
api.rollbar.com	good	IP: 35.201.81.77 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
m.alipay.com	good	IP: 203.209.245.74 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
cdn.qgraph.io	good	IP: 18.65.200.81 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199 查看地图: Google Map
f1.zenclerk.com	good	IP: 99.86.218.29 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map
mcgw.alipay.com	good	IP: 203.209.250.50 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map

域名	是否危险域名	服务器信息
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
mean.nothing.domain	good	没有服务器地理信息.
mclient.alipay.com	good	IP: 203.209.250.6 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
sandbox.tappaysdk.com	good	IP: 13.225.174.126 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map
xml.org	good	IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246 查看地图: Google Map

域名	是否危险域名	服务器信息
prod.tappaysdk.com	good	IP: 99.84.128.15 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map
www.youtube.com	good	IP: 108.160.166.148 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
sandbox-redirect.tappaysdk.com	good	IP: 13.225.174.48 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map
loggw-exsdk.alipay.com	good	IP: 110.76.3.1 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map

域名	是否危险域名	服务器信息
aftee.tw	good	IP: 143.204.86.84 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
mobilegw.alipaydev.com	good	IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
w3.org	good	IP: 128.30.52.100 所属国家: United States of America 地区: Massachusetts 城市: Cambridge 纬度: 42.365078 经度: -71.104523 查看地图: Google Map
m.me	good	IP: 157.240.22.19 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958 查看地图: Google Map

域名	是否危险域名	服务器信息
sandbox-crt.tappaysdk.com	good	**IP:** 18.65.214.69 **所属国家:** United States of America **地区:** Washington **城市:** Seattle **纬度:** 47.627499 **经度:** -122.346199 **查看地图:** Google Map
wappaygw.alipay.com	good	**IP:** 203.209.250.50 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map
prod-crt.tappaysdk.com	good	**IP:** 13.226.78.17 **所属国家:** Japan **地区:** Tokyo **城市:** Tokyo **纬度:** 35.689507 **经度:** 139.691696 **查看地图:** Google Map
publish.zenclerk.com	good	**IP:** 35.73.78.27 **所属国家:** Japan **地区:** Tokyo **城市:** Tokyo **纬度:** 35.689507 **经度:** 139.691696 **查看地图:** Google Map

域名	是否危险域名	服务器信息
access.line.me	good	IP: 198.27.124.186 所属国家: Canada 地区: Quebec 城市: Beauharnois 纬度: 45.316780 经度: -73.865898 查看地图: Google Map
h5.m.taobao.com	good	IP: 36.99.228.231 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
img.youtube.com	good	IP: 31.13.95.35 所属国家: United States of America 地区: Texas 城市: Fort Worth 纬度: 32.725410 经度: -97.320847 查看地图: Google Map
line.me	good	IP: 103.56.16.112 所属国家: China 地区: Jiangsu 城市: Changzhou 纬度: 31.783331 经度: 119.966667 查看地图: Google Map

域名	是否危险域名	服务器信息
tw.91mai.com	good	**IP:** 54.199.136.122 **所属国家:** Japan **地区:** Tokyo **城市:** Tokyo **纬度:** 35.689507 **经度:** 139.691696 **查看地图:** Google Map
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
config.quantumgraph.com	good	**IP:** 54.254.28.119 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
mobilegw.stable.alipay.net	good	没有服务器地理信息.
users.quantumgraph.com	good	**IP:** 18.141.112.151 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map

域名	是否危险域名	服务器信息
goo.gl	good	IP: 172.217.163.46 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
visitor-fleet.zenclerk.com	good	IP: 35.76.84.67 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map
www.apache.org	good	IP: 151.101.2.132 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
api.quantumgraph.com	good	IP: 13.228.245.10 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map

域名	是否危险域名	服务器信息
hk-nine-yi-firebase-19.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
line.naver.jp	good	IP: 162.125.32.10 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

🌐 URL线索

URL信息	Url所在文件
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java

URL信息	Url所在文件
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://users.quantumgraph.com/qg-data	com/quantumgraph/sdk/NotificationJobIntentService.java
https://f1.zenclerk.com/api/v1/	com/appier/AiDeal.java
http://wasap	com/nineyi/ui/ShopBrandView.java
https://wasap	com/nineyi/ui/ShopBrandView.java
http://m.me	com/nineyi/ui/ShopBrandView.java
https://m.me	com/nineyi/ui/ShopBrandView.java

URL信息	Url所在文件
http://www.facebook.com/	com/nineyi/web/FanPageWebFragment.java
http://tw.91app.com/act/openshop/intro.html#form	com/nineyi/web/OpenShopWebPageFragment.java
https://tw.91mai.com/login/ForgetPwd?	com/nineyi/web/WebViewWithControlsFragment.java
http://line	com/nineyi/web/WebViewWithControlsFragment.java
https://www.youtube.com/embed/%s	com/nineyi/product/secondscreen/ProductSecondScreenFragment.java
https://tw.91mai.com/login/ForgetPwd?	com/nineyi/activity/ActivityDetailActivity.java
http://line.naver.jp/ti/p/	com/nineyi/sidebar/newsidebar/SidebarView.java
http://www.facebook.com/	com/nineyi/fanpage/FanPageFragment.java
http://www.facebook.com/	com/nineyi/shopapp/ShopMainFragmentV2.java
http://www.w3.org/TR/REC-html40/strict.dtd	org/htmlcleaner/DoctypeToken.java
http://www.w3.org/TR/html4/strict.dtd	org/htmlcleaner/DoctypeToken.java
http://www.w3.org/TR/html4/loose.dtd	org/htmlcleaner/DoctypeToken.java
http://www.w3.org/TR/html4/frameset.dtd	org/htmlcleaner/DoctypeToken.java
http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd	org/htmlcleaner/DoctypeToken.java
http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd	org/htmlcleaner/DoctypeToken.java

URL信息	Url所在文件
http://www.w3.org/TR/xhtml1/DTD/xhtml1-frameset.dtd	org/htmlcleaner/DoctypeToken.java
http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd	org/htmlcleaner/DoctypeToken.java
http://www.w3.org/TR/xhtml11/DTD/xhtml-basic11.dtd	org/htmlcleaner/DoctypeToken.java
http://www.w3.org/1999/xhtml	org/htmlcleaner/HtmlCleaner.java
https://www.w3.org/1999/xhtml	org/htmlcleaner/HtmlCleaner.java
http://w3.org/1999/xhtml	org/htmlcleaner/HtmlCleaner.java
http://www.w3.org/TR/REC-html40	org/htmlcleaner/HtmlCleaner.java
http://jdom.org/jdom2/transform/JDOMResult/feature	org/jdom2/JDOMConstants.java
http://jdom.org/jdom2/transform/JDOMSource/feature	org/jdom2/JDOMConstants.java
http://www.w3.org/XML/1998/namespace	org/jdom2/JDOMConstants.java
http://www.w3.org/2000/xmlns/	org/jdom2/JDOMConstants.java
http://xml.org/sax/features/external-general-entities	org/jdom2/JDOMConstants.java
http://xml.org/sax/features/namespaces	org/jdom2/JDOMConstants.java
http://xml.org/sax/features/namespace-prefixes	org/jdom2/JDOMConstants.java
http://xml.org/sax/features/validation	org/jdom2/JDOMConstants.java

URL信息	Url所在文件
http://xml.org/sax/properties/declaration-handler	org/jdom2/JDOMConstants.java
http://xml.org/sax/handlers/DeclHandler	org/jdom2/JDOMConstants.java
http://xml.org/sax/properties/lexical-handler	org/jdom2/JDOMConstants.java
http://xml.org/sax/handlers/LexicalHandler	org/jdom2/JDOMConstants.java
http://www.w3.org/XML/1998/namespace	org/jdom2/Namespace.java
http://temporary	org/jdom2/adapters/AbstractDOMAdapter.java
http://jdom.org/jaxp/xpath/jdom	org/jdom2/xpath/XPath.java
http://jdom.org/jdom2/transform/JDOMSource/feature	org/jdom2/transform/JDOMSource.java
http://jdom.org/jdom2/transform/JDOMResult/feature	org/jdom2/transform/JDOMResult.java
http://www.w3.org/2001/XMLSchema	org/jdom2/input/sax/XMLReaders.java
http://www.w3.org/2001/XMLSchema	org/jdom2/input/sax/XMLReaderXSDFactory.java
https://mobilegw.alipaydev.com/mgw.htm	k1/a/b/a/a.java
https://mobilegw.alipay.com/mgw.htm	k1/a/b/a/a.java
https://h5.m.taobao.com/mlapp/olist.html	i/c/b/c/a.java
https://mcgw.alipay.com/sdklog.do	i/c/b/f/d/c.java

URL信息	Url所在文件
https://loggw-exsdk.alipay.com/loggw/logUpload.do	i/c/b/f/d/d.java
http://m.alipay.com/?action=h5quit	i/c/b/j/h.java
https://visitor-fleet.zenclerk.com/	i/f/a/s.java
https://api.rollbar.com/api/1/item/	i/f/a/r.java
https://publish.zenclerk.com/assets/campaigns/coupon/icons/bell.png	i/f/a/x/b.java
https://mean.nothing.domain	i/a/m2.java
https://graph.facebook.com/v11.0/	i/a/m2.java
https://line.me/R/ti	i/a/f5/j/n.java
http://line.naver.jp/ti/p/	i/a/f5/j/l.java
http://tw.91mai.com/	i/a/f5/j/l.java
https://goo.gl/	i/a/x4/a.java
http://(	i/a/x4/a.java
https://access.line.me/	i/a/a/a/a/b0/f.java
https://aftee.tw/privacypolicy/	i/a/f4/p1/j/b.java
https://aftee.tw/privacypolicy/	i/a/f4/p1/j/c.java

URL信息	Url所在文件
http://line.naver.jp/ti/p/	i/a/p4/d/c/a.java
https://graph.facebook.com/v11.0/	i/a/r3/a.java
https://)(	i/a/g/q/x.java
http://img.youtube.com/vi/%s/0.jpg	i/a/g/i/q.java
www.youtube.com/watch	i/a/g/i/q.java
www.youtube.com/embed/(.*	i/a/g/i/q.java
http://www.facebook.com/	i/a/r4/d/s.java
https://api.quantumgraph.com/qga/	i/i/b/g0.java
https://api.rollbar.com/api/1/item/	i/i/b/k.java
https://cdn.qgraph.io/config/android/%s.json	i/i/b/f.java
https://aiqua-recommendation.c.appier.net	i/i/b/f.java
https://config.quantumgraph.com/api/v1.0/user_config?os=android&verNo=%s&appId=%s&userId=%s&appVerName=%s	i/i/b/a.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://prod-crt.tappaysdk.com/certificate-server/certificate/get	t1/a/a/g/c.java
https://sandbox-crt.tappaysdk.com/certificate-server/certificate/get	t1/a/a/g/c.java
http://www.apache.org/licenses/LICENSE-2.0	n0/a/a/a/v0/c/e1/j.java
https://prod-redirect.tappaysdk.com	n0/a/a/a/v0/m/k1/c.java
https://sandbox-redirect.tappaysdk.com	n0/a/a/a/v0/m/k1/c.java
https://prod.tappaysdk.com/tpc	n0/a/a/a/v0/m/k1/c.java
https://sandbox.tappaysdk.com/tpc	n0/a/a/a/v0/m/k1/c.java
https://hk-nine-yi-firebase-19.firebaseio.com	Android String Resource
http://line.naver.jp/R/msg/text/?	Android String Resource

邮箱线索

邮箱地址	所在文件
cs_tw@netprotections.co	i/a/f4/p1/j/c.java
cs_tw@netprotections.co	i/a/f4/p1/j/a.java
this@productskuview.salepageda	i/a/f4/u1/i.java

数据库线索

FIREBASE链接地址	详细信息
https://hk-nine-yi-firebase-19.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
hk.com.nineyi.shop.s000020.permission.C2D_MESSAGE	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

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.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
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.providers.gsf.permission.READ_GSERVICES	未知	Unknown permission	Unknown permission from android reference
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度

向手机申请的权限	是否危险	类型	详细情况
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
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

签名证书

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=TW, ST=Taiwan, L=Taipei, O=NineYi Shopping Ltd. Co., OU=Product Department, CN=CH Lin
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-04-26 04:50:47+00:00
Valid To: 2040-09-11 04:50:47+00:00
Issuer: C=TW, ST=Taiwan, L=Taipei, O=NineYi Shopping Ltd. Co., OU=Product Department, CN=CH Lin
Serial Number: 0x517a07a7
```

Hash Algorithm: sha1
md5: f49f3884ba53fe15cb172029a26e1dbd
sha1: 1ab978edc2baeb0045487866d36d3c393340b938
sha256: 4e69e086b60c2baa6203fadb6e8893472fb83382240cf82af3635bc3ea2c45fc
sha512: 2bf5a21903a6ee528c5a8bed26c03c235f1dccc34a4f001ea9acc6cc935d77fd60982981c72ba4b36e809cae75126a7b1eb663ab63f4bbba553327e2ba91ec3e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 4add4cea0c90d617cabbfa1876bc87817d1190a5fb1ec6b6e5a7f21ea0ebef04

Exodus威胁情报

名称	分类	URL链接
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
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 <b>facebook.com/device</b> and enter the code shown above."
"content_des_login_password" : "pw_textField"

可能的敏感信息

"content_des_member_zone_item_password" : "memberChangePwBtn"
"firebase_database_url" : "https://hk-nine-yi-firebase-19.firebaseio.com"
"google_api_key" : "AIzaSyCXDoxly2DdcVV0aZvREKrIv5-CpfxRY1M"
"google_crash_reporting_api_key" : "AIzaSyCXDoxly2DdcVV0aZvREKrIv5-CpfxRY1M"
"login_force_reset_pwd_title" : "為確保資料安全，請先修改密碼以完成登入"
"login_thirdparty_forget_password" : "請洽詢客服＋886-2-8226-5777 星期1~5 09:00~12:30 / 13:30~18:00 / 19:00~21:00 星期6 09:00~12:30 / 13:30~16:00"
"login_thirdparty_forgetpassword" : "忘記密碼?"
"login_thirdparty_password" : "密碼"
"map_api_key" : "AIzaSyDrLz5GKyRtyUdRZytCwe-3e8RFW8j-wlU"
"member_setting_outer_password" : "密碼"
"shoppingcart_key_in_gift_coupon" : "輸入贈品券號"
"user_login_id_pwd_isnull" : "請輸入手機號碼與密碼"
"user_login_pwd_incorrect_alert" : "密碼請輸入6~8碼英數字"
"user_login_register_pwd_cfm_wrong_alert" : "您的密碼與確認密碼不一致，請檢查後重新輸入"

可能的敏感信息
"com_facebook_device_auth_instructions" : "Gå til <b>facebook.com/device</b> og indtast koden, som er vist ovenfor."
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>にアクセスして、上のコードを入力してください。"
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b> '■■ ■■■■■ ■■■ ■■■ ■■■■ ■■■■■ ■■■ ■■■ ■■■■■ ■■■▯"
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b> ■■■ ■■■■■■■■■■■■, ■■■■ ■■■■■■■■■■■ ■■■■■■■■■■ ■■■■■■■■■■■"
"com_facebook_device_auth_instructions" : "Gå til <b>facebook.com/device</b> og skriv inn koden som vises over."
"com_facebook_device_auth_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di atas."
"com_facebook_device_auth_instructions" : "Gehe zu <b>facebook.com/device</b> und gib den oben angezeigten Code ein."
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>■■ ■■■■■■■■■■ ■■■■■ ■■■■■ ■■■■■■ ■■■■■ ■■■■■■■"
"com_facebook_device_auth_instructions" : "Besoek <b>facebook.com/device</b> en voer die kode wat hierbo gewys word, in."
"com_facebook_device_auth_instructions" : "■■■■■ <b>facebook.com/device</b> ■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"com_facebook_device_auth_instructions" : "Siirry osoitteeseen <b>facebook.com/device</b> ja anna oheinen koodi."
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b> ■■ ■■■■■■ ■■■■ ■■ ■■■ ■■■■■■ ■■■ ■■■ ■■■■■■"
"com_facebook_device_auth_instructions" : "Truy cập <b>facebook.com/device</b> và nhập mã được hiển thị bên trên."
"com_facebook_device_auth_instructions" : "Navštívte stránku <b>facebook.com/device</b> a zadajte kód zobrazený vyššie."
"com_facebook_device_auth_instructions" : "Πηγαίνετε στη διεύθυνση <b>facebook.com/device</b> και εισαγάγετε τον παραπάνω κωδικό."

可能的敏感信息
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b> ■■■■ ▯■■■■■■ ■■■■■ ▯ ■■■■■■■■■■■■■■■■■ ■■■■■ ■ ▯■ ■■■■"
"com_facebook_device_auth_instructions" : "Ga naar <b>facebook.com/device</b> en voer de bovenstaande code in."
"com_facebook_device_auth_instructions" : "Odwiedź stronę <b>facebook.com/device</b> i wprowadź powyższy kod."
"com_facebook_device_auth_instructions" : "Puntahan ang <b>facebook.com/device</b> at ilagay ang code na ipinapakita sa itaas."
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b> ■■■■■ ■■■ ■■■■ ■■■■■■■ ■■■■■■■■ ■■■■■■ ■■■■■"
"com_facebook_device_auth_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di bawah ini."
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b> ■■ ■■■■■ ■■■■■ ■■■■■ ■■■■■ ■■■■■■■■■ ■■■■■■ ■■■ ■■ ■■■■■■■■"
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>▯ ▯▯▯▯ ▯ ▯▯▯ ▯▯▯▯▯."
"com_facebook_device_auth_instructions" : "Vizitează <b>facebook.com/device</b> şi introdu codul de mai sus."
"com_facebook_device_auth_instructions" : "تفضل بزيارة <b>facebook.com/device</b> وإدخال الرمز الموضح أعلاه."
"com_facebook_device_auth_instructions" : "Consultez <b>facebook.com/device</b> et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "Posjetitw <b>facebook.com/device</b> i unesite gore prikazani kôd."
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b> ■■■ ■■■■ ■■■ ■■■■ ■■■ ■■■■■■■■ ■■■■"
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b> adresine git ve yukarıda gösterilen kodu gir."
"com_facebook_device_auth_instructions" : "Přejděte na <b>facebook.com/device</b> a zadejte nahoře uvedený kód."

可能的敏感信息

"com_facebook_device_auth_instructions" : "Ve a <b>facebook.com/device</b> e ingresa el código que se muestra arriba."
"com_facebook_device_auth_instructions" : "Lawati <b>facebook.com/device</b> dan masukkan kod yang ditunjukkan di atas."
"com_facebook_device_auth_instructions" : "Visita <b>facebook.com/device</b> e inserisci il codice mostrato qui sotto."
"com_facebook_device_auth_instructions" : "Acesse <b>facebook.com/device</b> e insira o código mostrado acima."
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b&gt ■■ ■■■ ■■■ ■■■ ■■■■■■■ ■■■ ■■■■ ■■■■"
"com_facebook_device_auth_instructions" : "Keresd fel a <b>facebook.com/device</b> címet, és írd be a fent megjelenített kódot."
"com_facebook_device_auth_instructions" : "Откройте <b>facebook.com/device</b> и введите код, показанный выше."
"com_facebook_device_auth_instructions" : "Gå till <b>facebook.com/device</b> och skriv in koden som visas ovan."
"com_facebook_device_auth_instructions" : "יש לבקר בכתובת facebook.com/device</b&gt ולהזין את הקוד המוצג למעלה."
"com_facebook_device_auth_instructions" : "Accédez à <b>facebook.com/device</b> et entrez le code affiché ci-dessus."
"login_force_reset_pwd_title" : "[WWWWWWWWWWWWWWWWWWWW]"
"login_thirdparty_forget_password" : "[WWWWWWWWWWWWWWWWWWWWWW WWWWWWWWWWWWWWWWWWWWWW W WWWWWWWWWWW W WWWWWWWWWWW WWWWWWWWWWWWWWWWWWWW W WWWWWWWWWWW]"
"login_thirdparty_forgetpassword" : "[WWWWW]"
"login_thirdparty_password" : "[WW]"

可能的敏感信息
"map_api_key" : "[WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW]"
"member_setting_outer_password" : "[WW]"
"shoppingcart_key_in_gift_coupon" : "[WWWWWW]"
"user_login_id_pwd_isnull" : "[WWWWWWWWWW]"
"user_login_pwd_incorrect_alert" : "[WWWWWWWWWWWW]"
"user_login_register_pwd_cfm_wrong_alert" : "[WWWWWWWWWWWWWWWWWWWWWWW]"
"login_force_reset_pwd_title" : "[WWWWWWWWWWWWW WWWWW WWWWWWWWW WWWWW WWWWWWWWWWW WWWWWWW WWWWWWWWWWWWWWWWW WWWWW WWWWWWWWWWWWWWWWWW WWWWWWW WWWWWWWWWWWWWW]"
"login_thirdparty_forget_password" : "[WWWWWWWWWWWWW WWWWWWWWWWWWWWWW WWWWWWWWWWWWWWWWWW WWWWWWWWWWWWWWWW WWWWW WW WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW WWWWW WWWWWWWWW WWWWWWWWW WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW WWW WW WWWWWWWWWWWWWWWWWWWWWWWW WW WWWWWWWWWWWWWWWWWWWWWWWW WWWWW WWWWWWWWWWWWWWWWWWWWWWWWWWWWW WWWWWWWWW WW WWWWWWWWWWWWWWWWWWWWWWWWWW]"
"login_thirdparty_forgetpassword" : "[WWWWWWWWWWWWW WWWWWWWWWWWWWWWWWWWW]"
"login_thirdparty_password" : "[WWWWWWWWWWWWWWWWW]"
"map_api_key" : "[WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW]"
"member_setting_outer_password" : "[WWWWWWWWWWWWWWWWWW]"
"shoppingcart_key_in_gift_coupon" : "[WWWWWWWWWWW WWWWWWWWW WWWWWWWWWWWWWWWW WWWWWWWWW]"

可能的敏感信息
"user_login_id_pwd_isnull" : "[WWWWWWWWWWWW WWWWWWWWWW WWWWWWWW WWWWWWWWWWWW WWWWWWWWWWWW WWWWWW WWWWWW WWWWWWWWWW]"
"user_login_pwd_incorrect_alert" : "[WWWWWWWWWWWW WWWWWWWWWW WW WWWWWWWWWWWWWWWW WWWWWWWWWW WWWWWWWWWWWWW WWWWWW WWWWWWWWWWWWWWWW]"
"user_login_register_pwd_cfm_wrong_alert" : "[WWWWWWWWWWWWWWWWWWWWWWWW WWWWWWWWWWWWWWWWWW WWWWWWWWWWWW WWWW WWWWWWWWWWWWWW]"
"com_facebook_device_auth_instructions" : "前往<b>facebook.com/device</b&gt，並輸入上方顯示的代碼。"
"login_force_reset_pwd_title" : "為確保帳戶安全，請更新密碼以完成會員登入"
"login_thirdparty_forget_password" : "請洽詢客服＋886-2-8226-5777 星期1~5 09:00~12:30 / 13:30~18:00 / 19:00~21:00 星期6 09:00~12:30 / 13:30~16:00"
"login_thirdparty_forgetpassword" : "忘記密碼？"
"login_thirdparty_password" : "密碼"
"map_api_key" : "AIzaSyDrLz5GKyRtyUdRZytCwe-3e8RFW8j-wlU"
"member_setting_outer_password" : "密碼"
"shoppingcart_key_in_gift_coupon" : "輸入贈品券號"
"user_login_id_pwd_isnull" : "請輸入手機號碼與密碼"
"user_login_pwd_incorrect_alert" : "密碼請輸入6-8位字母或數字"
"user_login_register_pwd_cfm_wrong_alert" : "您的密碼與確認密碼不一致，請檢查後重新輸入"

可能的敏感信息
"com_facebook_device_auth_instructions" : "请访问<b>facebook.com/device</b>并输入以上验证码。"
"login_force_reset_pwd_title" : "为确保资料安全，请先修改密码以完成登入"
"login_thirdparty_forget_password" : "请洽询客服＋886-2-8226-5777 星期1~5 09:00~12:30 / 13:30~18:00 / 19:00~21:00 星期6 09:00~ 12:30 / 13:30~16:00"
"login_thirdparty_forgetpassword" : "忘记密码?"
"login_thirdparty_password" : "密码"
"map_api_key" : "AIzaSyDrLz5GKyRtyUdRZytCwe-3e8RFW8j-wlU"
"member_setting_outer_password" : "密码"
"shoppingcart_key_in_gift_coupon" : "输入赠品券号"
"user_login_id_pwd_isnull" : "请输入手机号码与密码"
"user_login_pwd_incorrect_alert" : "密码请输入6~8码英数字"
"user_login_register_pwd_cfm_wrong_alert" : "您的密码与确认密码不一致，请检查后重新输入"
"login_force_reset_pwd_title" : "[5bc410ecb530640001221a2d.login_force_reset_pwd_title]"
"login_thirdparty_forget_password" : "[5bc410ecb530640001221a2d.login_thirdparty_forget_password]"
"login_thirdparty_forgetpassword" : "[5bc410ecb530640001221a2d.login_thirdparty_forgetpassword]"
"login_thirdparty_password" : "[5bc410ecb530640001221a2d.login_thirdparty_password]"

可能的敏感信息
"map_api_key" : "[5bc410edb530640001221ac4.map_api_key]"
"member_setting_outer_password" : "[5bc410edb530640001221ac4.member_setting_outer_password]"
"shoppingcart_key_in_gift_coupon" : "[5bc410ecb530640001221a52.shoppingcart_key_in_gift_coupon]"
"user_login_id_pwd_isnull" : "[5bc410edb530640001221ac4.user_login_id_pwd_isnull]"
"user_login_pwd_incorrect_alert" : "[5bc410edb530640001221ac4.user_login_pwd_incorrect_alert]"
"user_login_register_pwd_cfm_wrong_alert" : "[5bc410edb530640001221ac4.user_login_register_pwd_cfm_wrong_alert]"
"com_facebook_device_auth_instructions" : "Visita <b>facebook.com/device</b> e introduce el código que se muestra más arriba."
"login_force_reset_pwd_title" : "Please be sure to reset the password to complete the login."
"login_thirdparty_forget_password" : "Please contact customer service at ＋886-2-8226-5777 Mon. thru Fri. 09:00~12:30 / 13:30~18:00 / 19:00~21:00 Sat. 09:00~12:30 / 13:30~16:00"
"login_thirdparty_forgetpassword" : "Forgot Password?"
"login_thirdparty_password" : "Password"
"map_api_key" : "AIzaSyDrLz5GKyRtyUdRZytCwe-3e8RFW8j-wlU"
"member_setting_outer_password" : "Password"
"shoppingcart_key_in_gift_coupon" : "Enter Gift Voucher Code"
"user_login_id_pwd_isnull" : "Please enter your Mobile Number and Password"

可能的敏感信息
"user_login_pwd_incorrect_alert" : "Please enter a password (6-20 letters and numbers)"
"user_login_register_pwd_cfm_wrong_alert" : "Inconsistent Password. Please re-enter."
"com_facebook_device_auth_instructions" : "Visita <b>facebook.com/device</b> e insere o código apresentado abaixo."
"com_facebook_device_auth_instructions" : "前往<b>facebook.com/device</b&gt，並輸入上方顯示的代碼。"
"login_force_reset_pwd_title" : "為確保資料安全，請先修改密碼以完成登入"
"login_thirdparty_forget_password" : "請洽詢客服＋886-2-8226-5777 星期1~5 09:00~12:30 / 13:30~18:00 / 19:00~21:00 星期6 09:00~12:30 / 13:30~16:00"
"login_thirdparty_forgetpassword" : "忘記密碼?"
"login_thirdparty_password" : "密碼"
"map_api_key" : "AIzaSyDrLz5GKyRtyUdRZytCwe-3e8RFW8j-wlU"
"member_setting_outer_password" : "密碼"
"shoppingcart_key_in_gift_coupon" : "輸入贈品券號"
"user_login_id_pwd_isnull" : "請輸入手機號碼與密碼"
"user_login_pwd_incorrect_alert" : "密碼請輸入6~8碼英數字"
"user_login_register_pwd_cfm_wrong_alert" : "您的密碼與確認密碼不一致，請檢查後重新輸入"
"login_force_reset_pwd_title" : "Untuk memastikan keselamatan data, sila ubah kata laluan anda untuk melengkapkan log masuk"

可能的敏感信息
"login_thirdparty_forget_password" : "Sila hubungi khidmat pelanggan pada＋886-2-8226-5777 Isnin ke Jumaat. 09:00~12:30 / 13:30~18:00 / 19:00~21:00 Sabtu. 09:00 ~12:30 / 13:30~16:00"
"login_thirdparty_forgetpassword" : "Lupa Kata Laluan?"
"login_thirdparty_password" : "Kata Laluan"
"map_api_key" : "AIzaSyDrLz5GKyRtyUdRZytCwe-3e8RFW8j-wlU"
"member_setting_outer_password" : "Kata Laluan"
"shoppingcart_key_in_gift_coupon" : "Masukkan kod baucar hadiah"
"user_login_id_pwd_isnull" : "Isikan Nombor Telefon"
"user_login_pwd_incorrect_alert" : "Isikan 6~8 alfanumerik untuk kata laluan"
"user_login_register_pwd_cfm_wrong_alert" : "Kata Laluan Tidak Konsisten. Sila masukkan semula."

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.nineyi.DeepLinkActivity	Schemes: @string/ref_scheme://, @string/face_book_ref_scheme://,
com.nineyi.WelcomePageActivity	Schemes: http://, https://, Hosts: @string/dynamic_link_domain,

活动(ACTIVITY)	通信(INTENT)
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.hk.com.nineyi.shop.s000020,

加壳分析

<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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
device ID check
subscriber ID check
ro.product.device check
ro.kernel.qemu check
emulator file check
possible VM check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</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.TAGS 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>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.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.MANUFACTURER check
Build.TAGS check
subscriber ID check
possible ro.secure check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</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