MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Scan Light 2.7.2.APK

APP名称:	Scan Light
包名:	com.finarx.android.scanlight
域名线索:	29条
URL线索:	25条
邮箱线索:	4条
分析日期:	2022年2月2日 19:58

文件信息

文件名: finarxscanlight556271.apk
文件大小: 8.88MB
MD5值: e0bf69a4e9c23c61ea564f3ef214707e
SHA1值: 972bb44f394798859a591b93b2ef5adaf5ec657b
SHA256值: d83cb0d1153eaeeb51c9e1c068917cab6561f7083768ea24012c94a6b4199b73

APP 信息

App名称: Scan Light
包名: com.finarx.android.scanlight
主活动**Activity:** com.finarx.android.scanlight.activity.ScanLightSplashScreenActivity
安卓版本名称: 2.7.2
安卓版本: 1301

域名线索

域名	是否危险域名	服务器信息
secure.sipgate.de	good	**IP:** 217.10.72.43 所属国家: Germany 地区: Nordrhein-Westfalen 城市: Dusseldorf 纬度: 51.221722 经度: 6.776160 查看地图: Google Map

域名	是否危险域名	服务器信息
portal.fastbill.com	good	**IP:** 52.219.168.44 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.115520 经度: 8.684170 查看地图: Google Map
192.168.2.157	good	**IP:** 192.168.2.157 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
data.flurry.com	good	**IP:** 69.147.88.7 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.731323 经度: -73.990089 查看地图: Google Map
faxgw02.finarx.net	good	**IP:** 54.217.201.218 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.343990 经度: -6.267190 查看地图: Google Map

域名	是否危险域名	服务器信息
scan.finarx.net	good	**IP:** 3.125.71.93 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.115520 经度: 8.684170 查看地图: Google Map
api.pamfax.biz	good	**IP:** 185.3.40.226 所属国家: Germany 地区: Thuringen 城市: Friedersdorf 纬度: 50.604919 经度: 11.035770 查看地图: Google Map
faxgw01.finarx.net	good	**IP:** 54.217.201.218 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.343990 经度: -6.267190 查看地图: Google Map
ws.interfax.net	good	**IP:** 54.217.7.159 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.343990 经度: -6.267190 查看地图: Google Map

域名	是否危险域名	服务器信息
play.google.com	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
clientsmartfax.web.de	good	**IP:** 212.227.23.87 所属国家: Germany 地区: Nordrhein-Westfalen 城市: Strang 纬度: 51.968700 经度: 8.753360 查看地图: Google Map
192.168.7.73	good	**IP:** 192.168.7.73 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
finarx.eu	good	**IP:** 89.31.143.1 所属国家: Germany 地区: Bayern 城市: Starnberg 纬度: 48.001930 经度: 11.344160 查看地图: Google Map
proton.flurry.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
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
portal.pamfax.biz	good	**IP:** 185.3.40.226 **所属国家:** Germany **地区:** Thuringen **城市:** Friedersdorf **纬度:** 50.604919 **经度:** 11.035770 **查看地图:** Google Map
market.android.com	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
www.finarx.eu	good	**IP:** 54.77.65.231 **所属国家:** Ireland **地区:** Dublin **城市:** Dublin **纬度:** 53.343990 **经度:** -6.267190 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.interfax.cc	good	**IP:** 15.197.142.173 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
timesheet.finarx.net	good	**IP:** 143.204.170.111 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London 纬度: 51.508530 经度: -0.125740 查看地图: Google Map
secure.interfax.net	good	**IP:** 52.212.178.118 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.343990 经度: -6.267190 查看地图: Google Map
interfax.net	good	**IP:** 23.185.0.4 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.792030 经度: -122.406853 查看地图: Google Map

域名	是否危险域名	服务器信息
sandbox-api.pamfax.biz	good	**IP:** 185.3.40.226 所属国家: Germany 地区: Thuringen 城市: Friedersdorf 纬度: 50.604919 经度: 11.035770 查看地图: Google Map
www.amazon.com	good	**IP:** 13.32.60.92 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.fastbill.com	good	**IP:** 52.212.115.228 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.343990 经度: -6.267190 查看地图: Google Map
secure.footprint.net	good	**IP:** 203.98.7.65 所属国家: New Zealand 地区: Auckland 城市: Auckland 纬度: -36.866669 经度: 174.766663 查看地图: Google Map

域名	是否危险域名	服务器信息
schemas.xmlsoap.org	good	**IP:** 104.69.120.16 **所属国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.783058 **经度:** -96.806671 **查看地图:** Google Map
www.finarx.net	good	没有服务器地理信息.
registrierung.web.de	good	**IP:** 217.72.199.94 **所属国家:** Germany **地区:** Nordrhein-Westfalen **城市:** Strang **纬度:** 51.968700 **经度:** 8.753360 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
http://www.amazon.com/gp/mas/dl/android?p=	com/finarx/android/b/b.java
http://play.google.com/store/apps/details?id=	com/finarx/android/b/b.java
http://www.finarx.eu/android/updates/	com/finarx/android/widget/UpdateChecker.java
https://timesheet.finarx.net/support/acra	com/finarx/android/scanlight/FinarxScanLightApplication.java

URL信息	Url所在文件
https://sandbox-api.pamfax.biz/	com/finarx/android/fax/client/f.java
https://api.pamfax.biz/	com/finarx/android/fax/client/f.java
https://portal.pamfax.biz/PortalLogin/Register?idev_id=170	com/finarx/android/fax/client/f.java
https://registrierung.web.de/?mc=hp@fm@modullink.produkte@freemail	com/finarx/android/fax/client/h.java
https://clientsmartfax.web.de/fax-submission-service/webde/fax/2.0/Authentication?clientType=WEBDE_iFAX	com/finarx/android/fax/client/h.java
https://clientsmartfax.web.de/fax-submission-service/webde/fax/2.0/FaxCapabilities?attr=MAX_WEBCENT	com/finarx/android/fax/client/h.java
https://clientsmartfax.web.de/fax-submission-service/webde/fax/2.0/FaxSubmission?clientType=WEBDE_iFAX	com/finarx/android/fax/client/h.java
https://clientsmartfax.web.de/fax-submission-service/webde/fax/2.0/FaxTarif?clientType=WEBDE_iFAX	com/finarx/android/fax/client/h.java
https://secure.sipgate.de/user/products.php	com/finarx/android/fax/client/g.java
https://secure.interfax.net/Default.aspx?Target=regservice&method=displayform&Agent=45&lang=	com/finarx/android/fax/client/e.java
http://interfax.net/Admin	com/finarx/android/fax/client/e.java
https://ws.interfax.net/admin.asmx?WSDL	com/finarx/android/fax/client/e.java
http://interfax.net/Admin/AuthenticateUser	com/finarx/android/fax/client/e.java

URL信息	Url所在文件
http://interfax.net/Admin/CalculateOfficeCost	com/finarx/android/fax/client/e.java
http://interfax.net/Admin/GetAccountPPCardsBalance2	com/finarx/android/fax/client/e.java
http://www.interfax.cc	com/finarx/android/fax/client/e.java
https://ws.interfax.net/dfs.asmx?WSDL	com/finarx/android/fax/client/e.java
http://www.interfax.cc/SendfaxEx_2	com/finarx/android/fax/client/e.java
http://interfax.net/Admin/GetAccountProperties	com/finarx/android/fax/client/e.java
http://www.w3.org/2001/XMLSchema-instance	com/finarx/android/fax/client/e.java
http://www.w3.org/2001/XMLSchema	com/finarx/android/fax/client/e.java
http://schemas.xmlsoap.org/soap/envelope/	com/finarx/android/fax/client/e.java
http://www.interfax.cc/StartFileUpload	com/finarx/android/fax/client/e.java
http://www.interfax.cc/UploadFileChunk	com/finarx/android/fax/client/e.java
http://www.interfax.cc/CancelFileUpload	com/finarx/android/fax/client/e.java
www.finarx.net	com/finarx/android/fax/client/c.java
http://faxgw01.finarx.net:444/FaxProxy/register_de.jsp	com/finarx/android/fax/client/c.java
http://faxgw01.finarx.net:444/FaxProxy/register.jsp?lang=	com/finarx/android/fax/client/c.java

URL信息	Url所在文件
http://finarx.eu/	com/finarx/android/scan/activity/AbstractMainScanEnterpriseActivity.java
https://www.fastbill.com/mobil/?kampagne=FNX12	com/finarx/android/scan/activity/AbstractMainScanEnterpriseActivity.java
http://192.168.7.73:8080/scanserver	com/finarx/android/scan/a/f.java
https://scan.finarx.net/scanserver	com/finarx/android/scan/a/f.java
https://faxgw01.finarx.net/scanserver	com/finarx/android/scan/a/f.java
https://faxgw02.finarx.net/scanserver	com/finarx/android/scan/a/f.java
https://timesheet.finarx.net/FaxProxy/register_de.jsp	com/finarx/android/scan/a/f.java
https://timesheet.finarx.net/FaxProxy/register.jsp?lang=	com/finarx/android/scan/a/f.java
http://192.168.7.73:8080/scanserver	com/finarx/android/scan/a/g.java
https://scan.finarx.net/scanserver	com/finarx/android/scan/a/g.java
https://faxgw01.finarx.net/scanserver	com/finarx/android/scan/a/g.java
https://faxgw02.finarx.net/scanserver	com/finarx/android/scan/a/g.java
https://timesheet.finarx.net/register_de.jsp	com/finarx/android/scan/a/g.java
https://timesheet.finarx.net/register.jsp?lang=	com/finarx/android/scan/a/g.java
https://portal.fastbill.com/services/finarx/	com/finarx/android/scan/a/e.java

URL信息	Url所在文件
https://www.fastbill.com/mobil/anmelden.html?kampagne=FNX12	com/finarx/android/scan/a/e.java
http://192.168.2.157:8080/scanserver	com/finarx/android/scan/a/c.java
www.finarx.net	com/finarx/android/scan/a/c.java
http://faxgw01.finarx.net:444/FaxProxy/register_de.jsp	com/finarx/android/scan/a/c.java
http://faxgw01.finarx.net:444/FaxProxy/register.jsp?lang=	com/finarx/android/scan/a/c.java
http://192.168.2.157:8080/scanserver	com/finarx/android/scan/a/i.java
www.finarx.net	com/finarx/android/scan/a/i.java
http://faxgw01.finarx.net:444/FaxProxy/register_de.jsp	com/finarx/android/scan/a/i.java
http://faxgw01.finarx.net:444/FaxProxy/register.jsp?lang=	com/finarx/android/scan/a/i.java
http://192.168.2.157:8080/scanserver	com/finarx/android/scan/a/o.java
www.finarx.net	com/finarx/android/scan/a/o.java
http://faxgw01.finarx.net:444/FaxProxy/register_de.jsp	com/finarx/android/scan/a/o.java
http://faxgw01.finarx.net:444/FaxProxy/register.jsp?lang=	com/finarx/android/scan/a/o.java
https://secure.footprint.net/web01afb/docs/fastbill_agb.pdf?ver=1.01	com/finarx/android/scan/data/registration/FastBillRegistrationFormData.java
http://www.fastbill.com/datenschutz.html	com/finarx/android/scan/data/registration/FastBillRegistrationFormData.java

URL信息	Url所在文件
https://timesheet.finarx.net/timesheet/rest/	com/finarx/d/a/a/b.java
https://proton.flurry.com/sdk/v1/config	com/flurry/sdk/v.java
https://data.flurry.com/pcr.do	com/flurry/sdk/ad.java
http://data.flurry.com/aap.do	com/flurry/sdk/an.java
https://data.flurry.com/aap.do	com/flurry/sdk/an.java
http://www.finarx.eu/agbs.pdf.	Android String Resource
http://www.finarx.eu/privacy.	Android String Resource
http://market.android.com/support/bin/answer.py?answer=1050566&hl=%lang%&dl=%region%	Android String Resource

邮箱线索

邮箱地址	所在文件
finarx@gmail.com	com/finarx/android/vending/billing/BillingService.java
fm@modullink.produkte	com/finarx/android/fax/client/h.java
your.account@domain.com	org/acra/sender/DefaultReportSenderFactory.java
android@finarx.de	Android String Resource

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.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.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.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
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.INTERNET	正常	互联网接入	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
com.android.vending.CHECK_LICENSE	未知	Unknown permission	Unknown permission from android reference
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.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
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
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
com.finarx.android.scanlight.SCAN_CROP_SERVICE	未知	Unknown permission	Unknown permission from android reference
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: False
Found 1 unique certificates
Subject: C=DE, ST=Hessen, L=Frankfurt am Main, O=FINARX GmbH, OU=Development, CN=FINARX GmbH
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-02-04 13:30:16+00:00
Valid To: 2110-01-11 13:30:16+00:00
Issuer: C=DE, ST=Hessen, L=Frankfurt am Main, O=FINARX GmbH, OU=Development, CN=FINARX GmbH
Serial Number: 0x4d4bff68
Hash Algorithm: sha1
md5: ba9a5c4e477c8e170e15481da4b283af
sha1: f8efc6ff8216e7fd494a863d5acd841831a08e83
sha256: e2363d567780caa2813e2f137114ed999aa64e1375c0630ed02a07f65188b30d
sha512: 2fece62cf572b9ee1b2aa7173d23013bc57a7da31ea7358d68ab46a8c3cd0981dd9b6070b2fe5d7a2880640f35dece15f5e7836aeeede7241bc666da43f5b834
PublicKey Algorithm: rsa
Bit Size: 1024

Fingerprint: 7e4b7b37c8ac7e50f5380d725c6af557895d3439847542ffaae524f6f577c6d1

Exodus威胁情报

名称	分类	URL链接
Flurry	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/25

硬编码敏感信息

可能的敏感信息
"login_dialog_password" : "Password"
"password" : "Password"
"prefs_scan_use_camera2_api" : "Lollipop Camera"
"prefs_scan_use_camera2_api_summary" : "Use new Android Lollipop camera API."
"username" : "User Name"
"alert_dialog_password" : "Password"
"alert_dialog_username" : "Login"
"login_dialog_password" : "Password"

可能的敏感信息
"password" : "Kennwort"
"prefs_scan_use_camera2_api" : "Lollipop Camera"
"prefs_scan_use_camera2_api_summary" : "Use new Android Lollipop camera API."
"username" : "Benutzername"
"login_dialog_password" : "Password"
"password" : "Password"
"username" : "User Name"
"login_dialog_password" : "Mot de passe"
"login_dialog_password" : "Şifre"
"password" : "Şifre"
"username" : "Kullanıcı adı"
"login_dialog_password" : "Пароль"

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.MANUFACTURER check
Build.BOARD check
network operator name check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
