MoGua

Greenify 4.7.5.APK 分析报告

APP名称:	Greenify

包名:	com.oasisfeng.greenify
域名线索:	21条
URL线索:	27条
邮箱线索:	3条
分析日期:	2024年4月19日
分析平台:	摸瓜反编译平台

文件信息

文件名: 绿色守护Greenify_v4.7.5_解锁捐赠版_Alphaeva.apk
文件大小: 3.99MB
MD5值: d824ed9e60fafdd9e89d8707f99342a3
SHA1值: 892d72f17bbe0e8018ad2897bc78037e6b197a93
SHA256值: 1db77d1ffc87946685aa364da5eb2e563d34224d6542beb817273d6b085ff9cc

APP 信息

App名称: Greenify
包名: com.oasisfeng.greenify
主活动Activity: com.oasisfeng.greenify.GreenifyActivity
安卓版本名称: 4.7.5
安卓版本: 47500

域名线索

域名	服务器信息
www.google-analytics.com	**IP**: 220.181.174.97 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
play.google.com	**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
pagead2.googlesyndication.com	**IP**: 220.181.174.230 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397232
ssl.google-analytics.com	IP: 220.181.174.169 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
oasisfeng.github.io	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
fabric.io	IP: 216.239.32.29 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
github.com	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
xmlpull.org	IP: 74.50.61.58 **所属国家**: United States of America **地区**: Texas **城市**: Dallas **纬度**: 32.814899 **经度**: -96.879204
	IP: 157.240.11.40

www.google.com	**所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052231 **经度**: -118.243683
repo.xposed.info	**IP**: 45.55.233.97 **所属国家**: United States of America **地区**: New Jersey **城市**: Clifton **纬度**: 40.858429 **经度**: -74.163757
plus.google.com	**IP**: 199.16.156.11 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
www.googletagmanager.com	**IP**: 220.181.174.233 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
goo.gl	**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
greenify.github.io	**IP**: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065632

	经度: -79.891708
e.crashlytics.com	没有服务器地理信息.
greenify.firebaseio.com	**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
app-measurement.com	**IP**: 220.181.174.97 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
settings.crashlytics.com	没有服务器地理信息.
greenify.uservoice.com	**IP**: 104.17.27.92 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
schemas.android.com	没有服务器地理信息.
api.github.com	**IP**: 20.205.243.168 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903

URL线索

URL信息	Url所在文件
http://repo.xposed.info/module/de.robv.android.xposed.installer	com/oasisfeng/greenify/pro/SetupGuideActivity.java
http://greenify.uservoice.com/knowledgebase/articles/633133	defpackage/xa1.java
http://greenify.uservoice.com/knowledgebase/articles/749142	defpackage/xa1.java
https://oasisfeng.github.io/island/	defpackage/xa1.java
www.google.com	defpackage/xa1.java
https://api.github.com/repos/	defpackage/ej1.java
https://www.google.com/	defpackage/br1.java
http://schemas.android.com/apk/res/android	defpackage/ym1.java
http://www.google-analytics.com	defpackage/fu.java
https://ssl.google-analytics.com	defpackage/fu.java
https://play.google.com/store/apps/details?id=	defpackage/yf.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	defpackage/yf.java
http://greenify.github.io/schemas/prescription/v	defpackage/yf.java
https://goo.gl/NAOOOI.	defpackage/ii0.java
https://goo.gl/NAOOOI	defpackage/ii0.java

https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	defpackage/fl.java
www.google.com	defpackage/lg0.java
https://www.google.com	defpackage/lg0.java
https://fabric.io/sign_up,	defpackage/sj.java
https://settings.crashlytics.com/spi/v2/platforms/android/apps/%s/settings	defpackage/fv1.java
http://xmlpull.org/v1/doc/features.html#indent-output	defpackage/wd1.java
http://goo.gl/naFqQk	defpackage/rs.java
https://github.com/	defpackage/zk1.java
http://goo.gl/8Rd3yj	defpackage/pt.java
http://hostname/?	defpackage/fx.java
www.googletagmanager.com	defpackage/ya1.java
http://goo.gl/8Rd3yj	defpackage/mt.java
http://schemas.android.com/apk/res/android	defpackage/e.java
https://www.googletagmanager.com	defpackage/ek0.java
https://e.crashlytics.com/spi/v2/events	defpackage/zu1.java
https://www.google-analytics.com	defpackage/s50.java
https://app-measurement.com/a	defpackage/ld0.java

https://plus.google.com/	defpackage/rp.java
http://hostname/?	defpackage/km0.java
https://greenify.firebaseio.com	Android String Resource
http://greenify.uservoice.com/knowledgebase/articles/828357	Android String Resource
http://greenify.uservoice.com/knowledgebase/articles/745179	Android String Resource
http://greenify.uservoice.com/knowledgebase/articles/828360	Android String Resource

邮箱线索

邮箱地址	所在文件
oasisfeng@github.com	defpackage/ej1.java
u0013android@android.com0 u0013android@android.com	defpackage/wq.java
arifguler@yandex.com	Android String Resource

手机线索

手机号	所在文件
15552000000	defpackage/zf0.java

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=Shanghai, L=Shanghai, O=moenet, OU=moenet, CN=moenet
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-07-29 18:08:52+00:00
Valid To: 2071-05-02 18:08:52+00:00
Issuer: C=CN, ST=Shanghai, L=Shanghai, O=moenet, OU=moenet, CN=moenet
Serial Number: 0x58ab6886
Hash Algorithm: sha256
md5: 385900a609a65c5f02ec81eddba1f2d4
sha1: 98774d0c5c27b70ca3d3684a4647270f70ee53de
sha256: 405a71acecaf9b3c03ae6f2018f797992ab825533281a619eaca4944d7975ff4
sha512: 34cc73a5f4ee016e10441adbd5864e18f4747db0d8121d531f38e87a8712fe04cc73d9304633404c6f66e9485042895d7cdfd00d68b3d14f2785f971cb7adf07

硬编码敏感信息

可能的敏感信息
"app_state_woken_by_authenticator" : "%1$s ago authenticated"
"firebase_database_url" : "https://greenify.firebaseio.com"
"google_api_key" : "AIzaSyCsnMDdPdz0SDKoTwVzfv23S4c7xPOQuLQ"
"google_crash_reporting_api_key" : "AIzaSyCsnMDdPdz0SDKoTwVzfv23S4c7xPOQuLQ"
"service_superuser" : "Root Validator"
"app_state_woken_by_authenticator" : "fa %1$s hem autenticat"

"app_state_woken_by_authenticator" : "%1$s پیش تصدیق شد"

"service_superuser" : "تأیید روت"

"app_state_woken_by_authenticator" : "%1$s 前に自動同期"

"service_superuser" : "Root 検証ツール"

"app_state_woken_by_authenticator" : "%1$s yang lalu terkonfirmasi"

"app_state_woken_by_authenticator" : "Vor %1$s authentifiziert"

"service_superuser" : "Root Überprüfung"

"app_state_woken_by_authenticator" : "%1$ לפניs בוצע אימות"

"app_state_woken_by_authenticator" : "Удостоверено е преди %1$s"

"service_superuser" : "Root проверка"

"app_state_woken_by_authenticator" : "%1$s 前账号授权"

"service_superuser" : "ROOT权限检查"

"app_state_woken_by_authenticator" : "Đã xác nhận %1$s phút trước"

"service_superuser" : "Xác thực Root"

"app_state_woken_by_authenticator" : "Overené pred %1$s"

"service_superuser" : "ROOT schvalovač"

"app_state_woken_by_authenticator" : "системний вхід здійснено %1$s тому"

"service_superuser" : "Перевірка root"

"app_state_woken_by_authenticator" : "%1$s temu uwierzytelniono"

"service_superuser" : "Weryfikacja Roota"

"app_state_woken_by_authenticator" : "overil pred %1$s"

"service_superuser" : "Preverjanje skrbniškega dostopa"

"app_state_woken_by_authenticator" : "%1$s yang lalu terkonfirmasi"

"app_state_woken_by_authenticator" : "%1$s 전, 인증됨 (authenticated)"

"service_superuser" : "루트 검사기"

"app_state_woken_by_authenticator" : "Acum %1$s s-a autentificat"

"service_superuser" : "Validator Root"

"app_state_woken_by_authenticator" : "%1$s منذ اخر مصادقة"

"service_superuser" : "متحري الروت"

"app_state_woken_by_authenticator" : "Authentifié il y a %1$s"

"service_superuser" : "Root Validateur"

"app_state_woken_by_authenticator" : "Potvrđeno pred %1$s"

"service_superuser" : "Provjera Root-a"

"app_state_woken_by_authenticator" : "Проверено пре %1$s"

"service_superuser" : "Провера рута"

"app_state_woken_by_authenticator" : "%1$s süre önce yetkilendirildi"

"service_superuser" : "Root Doğrulayıcı"

"app_state_woken_by_authenticator" : "Ověřeno před %1$s"

"service_superuser" : "Root ověření"

"app_state_woken_by_authenticator" : "Autentificada hace %1$s"

"service_superuser" : "Validador root"

"app_state_woken_by_authenticator" : "%1$s fa autenticato"

"service_superuser" : "Convalidatore di Root"

"app_state_woken_by_authenticator" : "%1$s atrás foi autenticado"

"service_superuser" : "Validação de Root"

"app_state_woken_by_authenticator" : "%1$s-el ezelőtt hitelesítve"

"service_superuser" : "Root érvényesítő"

"app_state_woken_by_authenticator" : "%1$s назад авторизовалось"

"service_superuser" : "Подтверждение рута"

"app_state_woken_by_authenticator" : "%1$ לפני s בוצע אימות"

"app_state_woken_by_authenticator" : "%1$s 前通過認證"

"app_state_woken_by_authenticator" : "%1$s yang lalu terkonfirmasi"

"app_state_woken_by_authenticator" : "%1$s atrás autenticado"
"service_superuser" : "Validador de Root"
"app_state_woken_by_authenticator" : "Prieš %1$s autentifikuota"
"service_superuser" : ""Root" patikrinimas"
"app_state_woken_by_authenticator" : "%1$s 前通過認證"
"service_superuser" : "Root 檢查"
"app_state_woken_by_authenticator" : "%1$s siden godkendt"
"app_state_woken_by_authenticator" : "%1$s sitten todennettu"
"app_state_woken_by_authenticator" : "Επικυρώθηκε πριν από %1$s"
"service_superuser" : "Έλεγχος ύπαρξης root"
"app_state_woken_by_authenticator" : "%1$s geleden ingelogd"
"app_state_woken_by_authenticator" : "%1$s আগে অনুমোদিত হয়েছে"
"app_state_woken_by_authenticator" : "%1$s siden autentisert"
"service_superuser" : "Rootsjekker"
"app_state_woken_by_authenticator" : "%1$s əvvəl təsdiqləndi"

加壳分析

加壳类型	所属文件
{'anti_debug': ['Debug.isDebuggerConnected() check'], 'anti_vm': ['Build.MODEL check', 'Build.MANUFACTURER check', 'Build.PRODUCT check', 'Build.TAGS check', 'network operator name check'], 'compiler': ['dexlib 2.x']}	classes.dex

第三方SDK

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
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

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
com.oasisfeng.greenify.INTERNAL	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

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
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.REAL_GET_TASKS	未知	Unknown permission	Unknown permission from android reference
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
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
android.permission.READ_SYNC_STATS	正常	读取同步统计信息	允许应用程序读取同步统计信息；例如已经发生的同步历史
android.permission.READ_SYNC_SETTINGS	正常	读取同步设置	允许应用程序读取同步设置,例如是否为联系人启用同步
android.permission.WRITE_SYNC_SETTINGS	正常	写入同步设置	允许应用程序修改同步设置,例如是否为联系人启用同步
android.permission.DUMP	系统需要	检索系统内部状态	允许应用程序检索系统的内部状态。恶意应用程序可能会检索到它们通常永远不需要的各种隐私和安全信息
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.SYSTEM_ALERT_WINDOW	危	显示系统级	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个

	险	警报	屏幕
android.permission.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
android.permission.FORCE_STOP_PACKAGES	合法	强制停止其他应用程序	允许一个应用程序强行停止其他应用程序
android.permission.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.WRITE_SECURE_SETTINGS	系统需要	修改安全系统设置	允许应用程序修改系统固定好设置数据。不供普通应用程序使用
android.permission.UPDATE_CONFIG	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERACT_ACROSS_USERS	未知	Unknown permission	Unknown permission from android reference
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.GET_APP_OPS_STATS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.oasisfeng.island.permission.FREEZE_PACKAGE	未知	Unknown permission	Unknown permission from android reference

com.oasisfeng.island.permission.LAUNCH_PACKAGE	未知	Unknown permission	Unknown permission from android reference
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.oasisfeng.greenify.prescription.ui.PrescriptionImportActivity	Schemes: https://, http://, greenify://, Hosts: greenify.github.io, Path Patterns: /.*/rx-.*, /.*/rxs-.*,
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.oasisfeng.greenify://,

---