南明离火
移动应用检测平台

ANDROID 静态分析报告

风驰 • v2.9.3

分析日期: 2024-05-13 15:20:44

应用概览

文件名称:	fengchi11035.apk
文件大小:	32.23MB
应用名称:	风驰
软件包名:	com.suijin.fengchi
主活动:	com.suijin.booster.ui.welcome.SplashActivity
版本号:	2.9.3
最小SDK:	22
目标SDK:	28
加固信息:	360加固 加固
应用程序安全分数:	49/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：可能有安全隐患
MD5:	732b82cb4fa320e05bdaad5222199ded
SHA1:	611e1007930e7d5014ff11053bc9f2044b2458ba
SHA256:	e7b5918239f420a4ed34f1be9e63d749f9744e69edd04f5cfa9cdf149398b4ed

分析结果严重性分布

高危	中危	信息	安全	关注
3	7	2	2	4

四大组件导出状态统计

Activity组件：43个，其中export的有：2个
Service组件：11个，其中export的有：2个
Receiver组件：9个，其中export的有：2个
Provider组件：4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

v2 签名: True
v3 签名: False
v4 签名: False
主题: C=boosterbooster, ST=boosterbooster, L=boosterbooster, O=boosterbooster, OU=boosterbooster, CN=boosterbooster
签名算法: rsassa_pkcs1v15
有效期自: 2020-07-06 08:26:28+00:00
有效期至: 2045-06-30 08:26:28+00:00
发行人: C=boosterbooster, ST=boosterbooster, L=boosterbooster, O=boosterbooster, OU=boosterbooster, CN=boosterbooster
序列号: 0x19ca44c0
哈希算法: sha256
证书MD5: 71e7257bd2d4481315a111c0dead81bb
证书SHA1: 71780cc0b1eda7764a4ea81ee9845e690de1c5e7
证书SHA256: f5607dafd093446368952995aa99f0569f4732c052a02355ef5214a489dac10d
证书SHA512:
2186ef5c1724f12074b974c8388b097a79b193d9775acf671793d1d696e0cf5df973e0ec9a7a72778073451de2382a007aead8a4ba6a06140a12164c896137402

公钥算法: rsa
密钥长度: 2048
指纹: 7d1e048544d959eb9548db8623c276433279e663d2e035a4578880cfe1062f36
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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
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.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
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.ACCESS_WIFI_STATE	普通	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.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
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置方面的数据。恶意应用程序可借此破坏您的系统配置。

android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
com.suijin.fengchi.SERVICE	未知	未知权限	来自 android 引用的未知权限。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
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.suijin.booster.ui.welcome.SplashActivity	Schemes: mtjd619ceecc6://,
com.github.booster.UrlImportActivity	Schemes: ss://,

网络通信安全风险分析

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

证书安全合规分析

高危: **0** | 警告: **1** | 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

Manifest 配置安全分析

高危: **1** | 警告: **8** | 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 5.1-5.1.1, [minSdk=22]	信息	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	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
3	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
4	Activity (com.suijin.booster.ui.MainActivity) 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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
5	Activity (com.suijin.booster.ui.MainActivity) 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，因此可被设备上的任何其他应用程序访问。
6	Broadcast Receiver (com.suijin.booster.receiver.ActionListener) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
7	Activity (com.github.booster.UrlImportActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
8	Broadcast Receiver (com.github.booster.BootReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
9	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service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。
10	Service (androidx.work.impl.background.gcm.WorkManagerGcmService) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_SERVICE [android:exported=true]	警告	发现一个 Service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。
11	Content Provider (com.github.booster.plugin.v2ray.BinaryProvider) 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，因此可被设备上的任何其他应用程序访问。

代码安全漏洞检测

高危: **1** | 警告: **7** | 信息: **2** | 安全: **2** | 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	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
3	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
4	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
5	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
6	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
7	该应用程序使用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
8	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
9	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

10	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
11	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
12	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)

1	arm64-v8a/libjni-helper.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk', '__memmove_chk', '__fwrite_chk', '__memcpy_chk', '__memset_chk', '__memchr_chk', '__strchr_chk', '__vsnprintf_chk']	False warning 符号可用
2	arm64-v8a/libredsocks.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__strlen_chk', '__vsprintf_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__memcpy_chk']	False warning 符号可用

3	arm64-v8a/libss-local.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strrchr_chk', '__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__read_chk', '__strchr_chk', '__vsprintf_chk', '__umask_chk', '__strcpy_chk']	False warning 符号可用
4	arm64-v8a/libssr-client.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__memset_chk', '__strlen_chk', '__strncpy_chk', '__memcpy_chk', '__memmove_chk', '__umask_chk', '__vsprintf_chk', '__strcpy_chk', '__strrchr_chk', '__strchr_chk', '__recvfrom_chk', '__strcat_chk', '__vsnprintf_chk', '__readlink_chk', '__fgets_chk', '__read_chk', '__write_chk', '__getcwd_chk', '__pread_chk', '__poll_chk', '__pwrite_chk', '__fwrite_chk', '__fread_chk']	False warning 符号可用

5	arm64-v8a/libv2ray.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	9/30	android.permission.CAMERA android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE android.permission.ACCESS_FINE_LOCATION android.permission.SYSTEM_ALERT_WINDOW android.permission.WRITE_SETTINGS android.permission.GET_TASKS android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
其它常用权限	13/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.REORDER_TASKS android.permission.BLUETOOTH android.permission.CHANGE_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_VIDEO 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
and.fengchiapp.com	安全	是	**IP地址:** 34.96.224.30 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
and.dianchictl.com	安全	是	**IP地址:** 45.132.238.5 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
feiniaojs.info	安全	否	**IP地址:** 104.21.29.161 **国家:** 美利坚合众国 **地区:** 华盛顿 **城市:** 西雅图 **纬度:** 47.627499 **经度:** -122.346199 **查看:** Google 地图
feiniaojiasu.com	安全	否	**IP地址:** 104.21.29.161 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
and.dianchiapp.com	安全	是	**IP地址:** 45.132.238.3 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
dm.feiniaovm.com	安全	否	**IP地址:** 103.224.212.213 **国家:** 澳大利亚 **地区:** 维多利亚 **城市:** 博马里斯 **纬度:** -37.982201 **经度:** 145.038940 **查看:** Google 地图
feiniaojs.net	安全	否	No Geolocation information available.
feiniaojs.org	安全	否	No Geolocation information available.
fengchijs.vip	安全	否	No Geolocation information available.

and.fengchictl.com	安全	是	**IP地址:** 34.150.106.10 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
feiniaovpn.com	安全	否	**IP地址:** 103.224.212.213 **国家:** 澳大利亚 **地区:** 维多利亚 **城市:** 博马里斯 **纬度:** -37.982201 **经度:** 145.038940 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://tongji.baidu.com/web/help/article?id=330&amp • https://github.com/gfwlist/gfwlist/blob/master/gfwlist.txt	自研引擎-A
• https://api.github.com/	com/allen/library/download/DownloadHelper.java
• https://api.github.com/	com/allen/library/upload/UploadHelper.java
• 8.8.8.8	com/github/booster/bg/DnsResolverCompat.java
• 127.0.0.1	com/github/booster/bg/TransproxyService.java
• 172.19.0.1 • 172.19.0.2 • 127.0.0.1	com/github/booster/bg/VpnService.java
• 127.0.0.1	com/github/booster/preference/DataStore.java
• http://and.fengchiapp.com:10000 • http://and.dianchiapp.com:10000 • http://and.fengchictl.com:10000 • http://34.150.106.10:10000 • http://45.132.238.154:10000 • http://and.dianchictl.com:10000 • http://34.96.224.30:10000 • http://45.132.238.170:10000	com/suijin/booster/app/App.java
• https://www.google.com.hk	com/suijin/booster/ui/booster/BoosterFragment.java
• https://fengchijs.vip/fwxy.html • https://fengchijs.vip/yszc.html	com/suijin/booster/ui/mine/ProtocolActivity.java

• http://feiniaojiasu.com • http://feiniaojs.info • http://feiniaojs.net • http://feiniaojs.org • http://dm.feiniaovpn.com • http://feiniaovpn.com	com/suijin/booster/utils/PingUtil.java
• https://fengchijs.vip/fwxy.html • https://fengchijs.vip/yszc.html	com/suijin/booster/widget/NoticeDialogView.java
• 1.9.0.4	com/thefinestartist/finestwebview/FinestWebView.java
• http://docs.google.com/gview?embedded=true&url=	com/thefinestartist/finestwebview/FinestWebViewActivity.java
• http://play.google.com/store/apps/details?id=	com/thefinestartist/utils/pkg/PackageUtil.java
• https://github.com/shadowsocks/shadowsocks-android/blob/master/.github/faq.ru.md • https://github.com/shadowsocks/shadowsocks-android/blob/master/.github/faq.md	自研引擎-S
• 1.2.3.4 • 18.244.0.188	lib/arm64-v8a/libredsocks.so
• 127.0.0.1	lib/arm64-v8a/libss-local.so
• 127.0.0.1	lib/arm64-v8a/libssr-client.so
• http://hybull;hyphen;iacute;igrave;iiiint;iinfin;incare;inodot;intcal;integerinvalidiques;isinsv;itilde;jsercy;kappav;kcedil;keytypekgreen;latail;lacute;lagran;lambda;langle;larrfs;larrhk;larrlp;larrpl;larrtl;latail;lbrace;lbrack;lcaron;lcedil;ld	lib/arm64-v8a/libv2ray.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
Tun2Socks	Jason Lyu（Jason Lyu）	Tun2Socks 是一个网络通信库，它可以处理来自当前设备的任意应用的所有网络流量，并通过 HTTP/Socks4/Socks5/Shadowsocks 远程连接，支持 Windows、macOS 等多平台，并且支持 IPv6，可以提供最佳的性能。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。
Google Play Services	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
PictureSelector	LuckSiege	一款针对 Android 平台下的图片选择器，支持从相册获取图片、视频、音频 & 拍照，支持裁剪(单图 or 多图裁剪)、压缩、主题自定义配置等功能，支持动态获取权限&适配 Android 5.0+ 系统的开源图片选择框架。

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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

第三方追踪器检测

名称	类别	网址
Baidu Mobile Stat	Analytics	https://reports.exodus-privacy.eu.org/trackers/101

敏感凭证泄露检测

可能的密钥
百度统计的=> "BaiduMobAd_CHANNEL" : "\ 11035"
凭证信息=> "io.fabric.ApiKey" : "123"
百度统计的=> "BaiduMobAd_STAT_ID" : "d619ceecc6"
凭证信息=> "com.google.android.backup.api_key" : "AEdPqrEAAAAI_zVxZ[illegible]"
"sitekey" : "Password"
f1aab1fb633378621635c344dbc8ac7b
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA71[illegible]
4FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE[illegible]
a79ada0ab5ab3b894f420add507b1e8[illegible]
328f96313ad78d1bad1480a46b1[illegible]
3617DE4A96262C6F5D9E98BF[illegible]
AA87CA22BE8B05[illegible]
5AC635D8AA3A9[illegible]
5f237ef7b4[illegible]
HqY6yU8f4nO8AeBkq1fcrSOl[illegible]
8D91E471E0989CDA27[illegible]
6B17D1F2E12C[illegible]
6bd62d[illegible]
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF

免责声明及风险提示: