



ANDROID 静态分析报告



HEX BOT 6 PRO v1.0

分析日期: 2024-05-15 06:13:35

i应用概览

文件名称:	6e1b16da2d900dadbbfd863f656995ee44ed7a55b20dc925e8f90070dfa63ef4.apk
文件大小:	28.39MB
应用名称:	HEX BOT 6 PRO
软件包名:	nikola.tesla
主活动:	.MainActivity
版本号:	1.0
最小SDK:	19
目标SDK:	22
加固信息:	未加壳
应用程序安全分数:	58/100 (中风险)
杀软检测:	18 个杀毒软件报毒
MD5:	c7846a8ac1277792e642a900eae7b74c
SHA1:	ecd3628d1e5e046a4f47b191bb1c5eb21a0a7c7d
SHA256:	6e1b16da2d900dadbbfd863f656995ee44ed7a55b20dc925e8f90070dfa63ef4

分析结果严重性分布

高危	中危	信息	安全	关注
0	7	1	1	0

四大组件导出状态统计

Activity组件: 3个, 其中export的有: 0个
Service组件: 2个, 其中export的有: 0个
Receiver组件: 1个, 其中export的有: 1个
Provider组件: 1个, 其中export的有: 0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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccb6b34ec4233f5f640703581053abfea303977272d17958704d89b1711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
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.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.BIND_DEVICE_ADMIN	签名	绑定设备管理	允许持有对象将意向发送到设备管理器。普通的应用程序一律无需此权限。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
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.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。
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.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。

android.permission.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
-----------------------------	----	------	---

🔒 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: 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: 0 | 警告: 3 | 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 4.4-4.4.4, [minSdk=19]	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	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
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	Broadcast Receiver (Alarm Receiver) 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。

🔧 代码安全漏洞检测

高危: 0 | 警告: 3 | 信息: 1 | 安全: 0 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	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

2	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
3	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
4	向Firebase上传文件	警告		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	10/30	android.permission.CALL_PHONE android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.READ_SMS android.permission.READ_CONTACTS android.permission.READ_CALL_LOG android.permission.ACCESS_FINE_LOCATION android.permission.GET_ACCOUNTS android.permission.SET_WALLPAPER android.permission.SEND_SMS
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.BIND_DEVICE_ADMIN android.permission.FOREGROUND_SERVICE

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
apkfromhelltoyouforthisweb.app	安全	否	IP地址: 172.67.75.166 国家: 美利坚合众国 地区: 加利福尼亚 城市: 山景城 纬度: 37.405991 经度: -122.078514 查看: Google 地图

www.arbada.com	安全	否	IP地址: 104.27.206.92 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
jokar-rat-dragon-default-rtddb.firebaseio.com	安全	否	IP地址: 35.190.39.113 国家: 美利坚合众国 地区: 密苏里州 城市: 堪萨斯城 纬度: 39.099731 经度: -94.578568 查看: Google 地图
api.db-ip.com	安全	否	IP地址: 172.67.15.166 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
www.firebase.com	安全	否	IP地址: 51.101.69.195 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

🌐 URL 链接安全分析

URL信息	源码文件
- https://script.google.com/macros/s/akfyshysvxg/qophouburfbag-vninqyve-momk2_ly_udz1_pg7yqqyhnk7yiutvaztsoe86w/exec - https://drive.google.com/uc?id= - https://www.arbada.com/ - https://api.db-ip.com/v2/free/self	nikola/tesla/MainActivity.java
https://apkfromhelltoyouforthis.web.app/	nikola/tesla/UpdateActivity.java

- https://api.db-ip.com/v2/free/self - https://drive.google.com/uc?id= - https://www.arbada.com/ - https://plus.google.com/ - https://console.firebase.google.com/ - www.firebase.google.com/storage - https://apkfromhelltoyouforthis.web.app/ - https://www.firebase.com/docs/android/guide/offline-capabilities.html#section-handling-transaction-s-offline - https://firebase.google.com/docs/database/ios/structure-data#best_practices_for_data_structure - https://firebase.google.com/docs/database/android/retrieve-data#filtering_data - https://jokar-rat-dragon-default-rtadb.firebaseio.com - https://script.google.com/macros/s/akfycbyqswxgyqophouburfbag-vninqqyemomk2_ly_udz1_pg7yqqyhnk7yiutvaztsoe86w/exec 127.0.0.1	自研引擎-S
---	--------

 Firebase 配置安全检测

标题	严重程度	描述信息

 第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Play Service	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。
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 App Startup	Google	App Startup 库提供了一种直接，高效的方法在应用程序启动时初始化组件。库开发人员 and 应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。

 邮箱地址敏感信息提取

EMAIL	源码文件

firebase-database-client@google.com	自研引擎-S
-------------------------------------	--------

 敏感凭证泄露检测

可能的密钥
"firebase_database_url" : "https://jokar-rat-dragon-default-rtdb.firebaseio.com"
"google_api_key" : "AlzaSyB26Shm0qI5_nbSVlJXSImWz3z4gleNe3k"
pG7yQQyHNK7YiUTVaZtsoe86w/exec

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端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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成