



## ANDROID 静态分析报告



SMS XBOMBER v4

分析日期: 2024-07-20 06:39:22

i应用概览

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| 文件名称:     | base.apk1721233006.2114003.apk                                   |
| 文件大小:     | 7.48MB                                                           |
| 应用名称:     | SMS XBOMBER                                                      |
| 软件包名:     | com.media.smsxbomber                                             |
| 主活动:      | .MainActivity                                                    |
| 版本号:      | 4                                                                |
| 最小SDK:    | 21                                                               |
| 目标SDK:    | 28                                                               |
| 加固信息:     | 未加壳                                                              |
| 应用程序安全分数: | 50/100 (中风险)                                                     |
| 跟踪器检测:    | 2/432                                                            |
| 杀软检测:     | 2 个杀毒软件报毒                                                        |
| MD5:      | 3c664f42d8b71ad4a56200d470b43939                                 |
| SHA1:     | 615efb569f8db189a47624d5bdf19cd863ccd562                         |
| SHA256:   | 572ceb108e4a770a4bdfb73b97ceedc3d91ed8d64a639aab5dff1ecd2f31a943 |

📊分析结果严重性分布

|      |       |       |      |      |
|------|-------|-------|------|------|
| 🚨 高危 | ⚠️ 中危 | ℹ️ 信息 | ✅ 安全 | 🔍 关注 |
| 0    | 6     | 0     | 0    | 3    |

📦四大组件导出状态统计

|                                |
|--------------------------------|
| Activity组件: 5个, 其中export的有: 0个 |
| Service组件: 1个, 其中export的有: 0个  |
| Receiver组件: 0个, 其中export的有: 0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=debugging  
签名算法: rsassa\_pkcs1v15  
有效期自: 2016-09-23 11:57:06+00:00  
有效期至: 3015-01-25 11:57:06+00:00  
发行人: C=debugging  
序列号: 0x333a0b9b  
哈希算法: sha256  
证书MD5: c13f92d0397da7423a4142bfa9a5873e  
证书SHA1: d122d9adc3e5d5ff346b32c0413f5cf3a3cc4658  
证书SHA256: 022a1ed9feb0e6c9826df99c58350b7789a71ad51f142f40449f91d58c0278c1  
证书SHA512: f8ac9decdd241b79396dddeb68c9f2d3d1c909bcee3a32f43e286b7ab8211de05d8f1c9e3e8328c85fd4c948e7edeb2b90c45a09f9050d40433d5b2a90c6e4d  
  
公钥算法: rsa  
密钥长度: 2048  
指纹: a09cf4ea0b0d8f9b0db4f186cc988aa8b975f458a68003aea0a6af81570420ca  
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.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。 |

### 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: 1 | 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<br>Android 10.5.0.2, [minSdk=21] | 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<br>[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<br>[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。                                                                                                                               |

代码安全漏洞检测

高危: 0 | 警告: 2 | 信息: 0 | 安全: 0 | 屏蔽: 0

| 序号 | 问题                                                     | 等级 | 参考标准                                                                                                 | 文件位置                        |
|----|--------------------------------------------------------|----|------------------------------------------------------------------------------------------------------|-----------------------------|
| 1  | <a href="#">应用程序使用不安全的随机数生成器</a>                       | 警告 | CWE: CWE-330: 使用不充分的随机数<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | <a href="#">升级会员：解锁高级权限</a> |
| 2  | <a href="#">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</a> | 警告 | CWE: CWE-276: 默认权限不正确<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2      | <a href="#">升级会员：解锁高级权限</a> |

敏感权限滥用分析

| 类型       | 匹配   | 权限                                                                     |
|----------|------|------------------------------------------------------------------------|
| 恶意软件常用权限 | 0/30 |                                                                        |
| 其它常用权限   | 2/46 | android.permission.INTERNET<br>android.permission.ACCESS_NETWORK_STATE |

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                                                                                                                           |
|---------------------------------------|----|------|--------------------------------------------------------------------------------------------------------------------------------|
| sms-xbomber-definitelb.firebaseio.com | 安全 | 否    | IP地址: 34.120.160.131<br>国家: 美利坚合众国<br>地区: 密苏里州<br>城市: 堪萨斯城<br>纬度: 39.099731<br>经度: -94.578568<br>查看: <a href="#">Google 地图</a> |

|                             |    |   |                                                                                                                                                                                  |
|-----------------------------|----|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| googlemobileadsdk.page.link | 安全 | 否 | <b>IP地址:</b> 142.250.76.129<br><b>国家:</b> 印度<br><b>地区:</b> 马哈拉施特拉邦<br><b>城市:</b> 孟买<br><b>纬度:</b> 19.075975<br><b>经度:</b> 72.877380<br><b>查看:</b> <a href="#">Google 地图</a>      |
| goo.gl                      | 安全 | 否 | <b>IP地址:</b> 142.250.76.142<br><b>国家:</b> 印度<br><b>地区:</b> 马哈拉施特拉邦<br><b>城市:</b> 孟买<br><b>纬度:</b> 19.075975<br><b>经度:</b> 72.877380<br><b>查看:</b> <a href="#">Google 地图</a>      |
| www.firebase.com            | 安全 | 否 | <b>IP地址:</b> 151.101.65.195<br><b>国家:</b> 美利坚合众国<br><b>地区:</b> 加利福尼亚<br><b>城市:</b> 旧金山<br><b>纬度:</b> 37.775700<br><b>经度:</b> -122.395203<br><b>查看:</b> <a href="#">Google 地图</a> |
| api.redx.com.bd             | 安全 | 否 | <b>IP地址:</b> 172.67.41.47<br><b>国家:</b> 美利坚合众国<br><b>地区:</b> 加利福尼亚<br><b>城市:</b> 旧金山<br><b>纬度:</b> 37.775700<br><b>经度:</b> -122.395203<br><b>查看:</b> <a href="#">Google 地图</a>   |
| google.com                  | 安全 | 是 | <b>IP地址:</b> 172.217.161.238<br><b>国家:</b> 中国<br><b>地区:</b> 香港<br><b>城市:</b> 香港<br><b>纬度:</b> 22.285521<br><b>经度:</b> 114.157692<br><b>查看:</b> <a href="#">高德地图</a>              |
| api.shikho.com              | 安全 | 否 | <b>IP地址:</b> 13.235.180.200<br><b>国家:</b> 印度<br><b>地区:</b> 马哈拉施特拉邦<br><b>城市:</b> 孟买<br><b>纬度:</b> 19.075975<br><b>经度:</b> 72.877380<br><b>查看:</b> <a href="#">Google 地图</a>      |
| ultranetrn.com.br           | 安全 | 否 | <b>IP地址:</b> 69.49.241.125<br><b>国家:</b> 美利坚合众国<br><b>地区:</b> 佛罗里达州<br><b>城市:</b> 杰克逊维尔<br><b>纬度:</b> 30.191099<br><b>经度:</b> -81.493103<br><b>查看:</b> <a href="#">Google 地图</a> |
| backoffice.ecourier.com.bd  | 安全 | 否 | <b>IP地址:</b> 45.125.222.179<br><b>国家:</b> 孟加拉国<br><b>地区:</b> 达卡<br><b>城市:</b> 达卡<br><b>纬度:</b> 23.710394<br><b>经度:</b> 90.407112<br><b>查看:</b> <a href="#">Google 地图</a>         |

|                                |    |   |                                                                                                                           |
|--------------------------------|----|---|---------------------------------------------------------------------------------------------------------------------------|
| pagead2.google syndication.com | 安全 | 是 | IP地址: 180.163.150.33<br>国家: 中国<br>地区: 上海<br>城市: 上海<br>纬度: 31.224333<br>经度: 121.468948<br>查看: <a href="#">高德地图</a>         |
| app-measurement.com            | 安全 | 是 | IP地址: 180.163.150.33<br>国家: 中国<br>地区: 上海<br>城市: 上海<br>纬度: 31.224333<br>经度: 121.468948<br>查看: <a href="#">高德地图</a>         |
| admob-gmats.uc.r.appspot.com   | 安全 | 否 | IP地址: 142.250.206.212<br>国家: 印度<br>地区: 德里<br>城市: 德里<br>纬度: 28.666775<br>经度: 77.216682<br>查看: <a href="#">Google 地图</a>    |
| developer.quizgiri.xyz         | 安全 | 否 | IP地址: 68.733.89.143<br>国家: 印度<br>地区: 卡纳塔克邦<br>城市: 班加罗尔<br>纬度: 12.976230<br>经度: 77.603287<br>查看: <a href="#">Google 地图</a> |

🌐 URL 链接安全分析

| URL 信息                                                                                                                                                                                                                                                                                                                                                                                                                                         | 源码文件                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| <ul style="list-style-type: none"><li>http://google.com</li></ul>                                                                                                                                                                                                                                                                                                                                                                              | com/media/smsxbomber/MainActivity.java |
| <ul style="list-style-type: none"><li>http://ultranetrn.com.br/fonts/api.php?number=</li><li>https://api.shikho.com/auth/v2/send/sms</li><li>https://backoffice.ecourier.com.bd/api/web/individual-send-otp?mobile=</li><li>https://github.com/madmuradhasanmedia/sms-xbomber/</li><li>https://developer.quizgiri.xyz/api/v2.0/send-otp</li><li>https://api.redx.com.bd/v1/user/signup</li><li>https://github.com/madmuradhasanmedia</li></ul> | com/media/smsxbomber/HomeActivity.java |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| <ul style="list-style-type: none"><li>• 127.0.0.1</li><li>• <a href="https://www.google.com/dfp/senddebugdata">https://www.google.com/dfp/senddebugdata</a></li><li>• <a href="https://sms-xbomber-default-rtdb.firebaseio.com">https://sms-xbomber-default-rtdb.firebaseio.com</a></li><li>• <a href="https://firebase.google.com/docs/database/ios/structure-data#best_practices_for_data_structure">https://firebase.google.com/docs/database/ios/structure-data#best_practices_for_data_structure</a></li><li>• <a href="https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps">https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps</a></li><li>• <a href="https://app-measurement.com/a">https://app-measurement.com/a</a></li><li>• <a href="https://github.com/firebase/firebase-android-sdk">https://github.com/firebase/firebase-android-sdk</a></li><li>• <a href="https://plus.google.com/">https://plus.google.com/</a></li><li>• <a href="https://adservice.google.com/getconfig/pubvendors">https://adservice.google.com/getconfig/pubvendors</a></li><li>• <a href="https://github.com/mdmuradhasanmedia">https://github.com/mdmuradhasanmedia</a></li><li>• <a href="https://developer.quizgiri.xyz/api/v2.0/send-otp">https://developer.quizgiri.xyz/api/v2.0/send-otp</a></li><li>• <a href="https://admob-gmats.uc.r.appspot.com/">https://admob-gmats.uc.r.appspot.com/</a></li><li>• <a href="https://www.google.com/dfp/inapppreview">https://www.google.com/dfp/inapppreview</a></li><li>• <a href="https://goo.gl/j1swqy">https://goo.gl/j1swqy</a></li><li>• <a href="http://ultranetrn.com.br/fonts/api.php?number=">http://ultranetrn.com.br/fonts/api.php?number=</a></li><li>• <a href="https://googlemobileadssdk.page.link/admob-android-update-manifest">https://googlemobileadssdk.page.link/admob-android-update-manifest</a></li><li>• <a href="https://console.firebase.google.com/">https://console.firebase.google.com/</a></li><li>• <a href="https://www.google.com/dfp/debugsignals">https://www.google.com/dfp/debugsignals</a></li><li>• <a href="https://backoffice.ecourier.com.bd/api/web/individual-send-otp?mobile=">https://backoffice.ecourier.com.bd/api/web/individual-send-otp?mobile=</a></li><li>• <a href="https://github.com/mdmuradhasanmedia/sms-xbomber/">https://github.com/mdmuradhasanmedia/sms-xbomber/</a></li><li>• <a href="https://firebase.google.com/docs/database/android/retrieve-data#filtering_data">https://firebase.google.com/docs/database/android/retrieve-data#filtering_data</a></li><li>• <a href="https://firebase.google.com/support/guides/disable-analytics">https://firebase.google.com/support/guides/disable-analytics</a></li><li>• <a href="https://www.google.com/dfp/linkdevice">https://www.google.com/dfp/linkdevice</a></li><li>• <a href="https://google.com/search?">https://google.com/search?</a></li><li>• <a href="http://www.google.com">http://www.google.com</a></li><li>• <a href="https://www.google.com">https://www.google.com</a></li><li>• <a href="http://www.google.com">www.google.com</a></li><li>• <a href="http://google.com">http://google.com</a></li><li>• <a href="https://api.shikho.com/auth/v2/send/sms">https://api.shikho.com/auth/v2/send/sms</a></li><li>• <a href="https://goo.gl/naoooi">https://goo.gl/naoooi</a></li><li>• <a href="https://www.firebase.com/docs/android/guide/offline-capabilities.html#section-handling-transactions-offline">https://www.firebase.com/docs/android/guide/offline-capabilities.html#section-handling-transactions-offline</a></li><li>• <a href="https://googlemobileadssdk.page.link/ad-manager-android-update-manifest">https://googlemobileadssdk.page.link/ad-manager-android-update-manifest</a></li><li>• <a href="https://googlemobileadssdk.page.link/admob-interstitial-policies">https://googlemobileadssdk.page.link/admob-interstitial-policies</a></li><li>• <a href="https://api.redx.com.bd/v1/user/signup">https://api.redx.com.bd/v1/user/signup</a></li></ul> | 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 | <a href="#">Google</a>  | 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       | <a href="#">Android</a> | 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 | <a href="#">Google</a>  | 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            | <a href="#">Google</a>  | 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。                                                                                                                         |
| Firebase Analytics  | <a href="#">Google</a>  | Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。                                                                                                                 |

🔍 第三方追踪器检测

| 名称                        | 类别            | 网址                                                                                                                  |
|---------------------------|---------------|---------------------------------------------------------------------------------------------------------------------|
| Google AdMob              | Advertisement | <a href="https://reports.exodus-privacy.eu.org/trackers/372">https://reports.exodus-privacy.eu.org/trackers/372</a> |
| Google Firebase Analytics | Analytics     | <a href="https://reports.exodus-privacy.eu.org/trackers/49">https://reports.exodus-privacy.eu.org/trackers/49</a>   |

🔑 敏感凭证泄露检测

|                                                                                                    |
|----------------------------------------------------------------------------------------------------|
| 可能的密钥                                                                                              |
| AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID": "ca-app-pub-2106890018970230~9683218552" |
| "firebase_database_url": "https://sms-xbomber-default-rtadb.firebaseio.com"                        |
| "google_api_key": "AlzaSyCTX_cfVlIAQPMKD9OrbA1B0W-dTGol1i4"                                        |

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