南明离火
移动应用检测平台

ANDROID 静态分析报告

Meta_Task • v1.0

分析日期: 2024-05-06 09:28:41

应用概览

文件名称:	Meta_Task.apk
文件大小:	13.45MB
应用名称:	Meta_Task
软件包名:	com.chatwithme.syonife
主活动:	.LoginActivity
版本号:	1.0
最小SDK:	16
目标SDK:	34
加固信息:	未加壳
应用程序安全分数:	42/100 (中风险)
跟踪器检测:	2/432
杀软检测:	9 个杀毒软件报毒
MD5:	65f39a9c18de5c6b73bc45a720922b96
SHA1:	18d6a661627645579eb01330cd7a06639a9abb34
SHA256:	e4abbb2bb1af62a858739022564e9ca0297f7a22cf540e41bf3e6f5c1be5778c

分析结果严重性分布

高危	中危	信息	安全	关注
2	1	2	0	0

四大组件导出状态统计

Activity组件：29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: True
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:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea3039772720179587704d89b7711292a4569

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.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.STORAGE_INTERNAL	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.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。
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。

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 4.1-4.1.2, [minSdk=16]	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 (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个Broadcast Receiver被共享给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。

代码安全漏洞检测

高危: **2** | 警告: **6** | 信息: **2** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息，不应记录敏感信息	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	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
3	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

4	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
5	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
6	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
7	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
8	向Firebase上传文件	警告		升级会员：解锁高级权限
9	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
10	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	2/30	android.permission.VIBRATE android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.CHANGE_NETWORK_STATE android.permission.FOREGROUND_SERVICE 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
www.firebase.com	安全	否	**IP地址:** 151.101.1.195 **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
chat-with-me-syonife-default-rtdb.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
scar.unityads.unity3d.com	安全	否	**IP地址:** 34.49.168.197 **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

URL 链接安全分析

URL信息	源码文件
• https://scar.unityads.unity3d.com/v1/capture-scar-signals	com/unity3d/services/ads/gmascar/utils/ScarConstants.java
• javascript:window.nativebridge.receiveEvent	com/unity3d/services/ads/webplayer/WebPlayerView.java
• https://scar.unityads.unity3d.com/v1/capture-scar-signals • 127.0.0.1 • www.firebase.google.com/storage • https://www.firebase.com/docs/android/guide/offline-capabilities.html#section-handling-transactions-offline • https://console.firebase.google.com/ • javascript:window.nativebridge.receiveEvent • https://chat-with-me-syonife-default-rtdb.firebaseio.com • https://github.com/firebase/firebase-android-sdk • https://plus.google.com/ • 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	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。
Unity Ads	Unity Technologies	Unity Ads SDK 由领先的移动游戏引擎创建，无论您是在 Unity、xCode 还是 Android Studio 中进行开发，都能为您的游戏提供全面的变现服务框架。
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 App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和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。

第三方追踪器检测

名称	类别	网址
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121

敏感凭证泄露检测

可能的密钥
"firebase_database_url" : "https://chat-with-me-syonife-default-rtdb.firebaseio.com"
"google_api_key" : "AIzaSyCW8[illegible]PQJxblVwvq9W8CR[illegible]Dirn88I-Y"
IjUqQV0hezRIX[illegible]CcyQkos
GztmZF[illegible]XSF0BUJWOzEIWVE[illegible]=
NjsiSFY0OSMNdBwfAw0HdRs[illegible]CNBGBkdDWgYag==
IjUqQV0hezVYWgokJ1[illegible]clUwIC5CXCY=
IjUqQV0hezZM[illegible]InODEyRVcxJw==
NDoiX1c8[illegible]GhEViExKFkWMCwyX1I7BxJ/fRQZ
NjsrA1k7MDRCUTF6JUxVMCYnA1k2IC9CVnsXFGJo
DDszDVs0OmZDVyF0I0NMMCZmQk87dDRIXjAmZm5XMTE=

MTUvQUEKMCdZWXogKUlZLAs1Tko0ICVFWzQmIg==
FjsoSko0IDNBWSE9KUNLdF4fQk11MylZGGd0BUJROydma0o6OWZ+SDw6
NDoiX1c8MGhMSCV6B11IEjgpT1k5Jw==
HDoiSEAaITJiXhc7M0NcJhE+Tl0lIC9CVg==
FHQQSEo8Mi9OWSE9KUMYGT0oRhgdNTUNejAxKA1rMDoyDWw6dB9CTSd0A0BZPDhmblAwNy0NYTohNA1xOzYpVRgaJmZ+SDQ5ZmtXOTAjXw==
GjgiDWg0JzVaVycwZmRLdR0oTlcnJiNOTA==
FjsoSko0IDNBWSE9KUNLdXVmJ2E6IWZKVyF0
BTU1Xk86JiINajAnI1kYHTU1DXowMSgNazA6Mg1sOnQfQk0ndBRIXzwnMkhKMDBmaFU0PSoDGAU4I0xLMHQFRV02P2Z0VyAmZmBZPDhmZFY3Oz4Ndyd0FV1ZOHo=
PSAyXUtve2lZXTkxIV9ZOHorSBc4MTJMZyE1NUZnOjIgRFs8NSo=
NjsoWV07IHwCFzE7MUNUOjUiXhclISRBUTYLIkJPOzgpTFwm
BTgjTEswdANDTDAmZn9dMj01WV0nMSINfTg1L0E=
BTU1Xk86JiINcDQnZm5QNDohSFx1BzNOWzAnNUtNOTg/
BTgjTEswdAdJXHUNKVhKdQQnVFUwOjINfDAgJ0RUJnQAQko4dBZfVzM9Kkg=
PSAyXUtve2lAXSE7MkhLITk/X1cgICNEVns2KkJfJiQpWRY2OysCSHo5I1lZITU1RhU0JDYA5Cc9MExbLHk2QlQ8Nz8DUCE5Kg==
BiA0RFYyHShJXS0bM1l3MxYpWFYxJwNVWzAkMkRXOw==
GztmZFYhMTRDXSF0BUJWOzElWVE6OmcM
MTBrYHUYeT9UQSx0LkUCODl8Xkt1NQ==
FjUoCkx1FSJJGBoyIERbPDUqDXE7dAhMVTA=
HDowTFQ8MGZ/XTMxNA17OjAjAxgBJj8NeTl1L0MY
dQIvSV06J2ZsXCZ0YA19NCYoDX0tIDRMG3Y7L0NLdQ==
Mz0qSBglNTJFGDE7NUhWIXQjVVEmIA==
GDskRFQwdAhYVTcxMA1XjnQPQ1s6JjRIWyE=
BTU1Xk86JiINdSAnMg16MHQBX100ICNfGAE8I0MYYHQFRVknNSVZXScn
BTgjTEswdAdJXHUNKVhKdQQnVFUwOjINfDAgJ0RUJnQAX1c4dBZfVzM9Kkg=
GTshSl0ndCdBSjA1IlQYJyEoQ1EXMw==
DDszXxgUNyVCTTsgZmVXJnQESFc7dARMVjsxIg18IDFmeVd1BzNeSDw3L0JNJnQHTkw8Ii9ZQQ==
NjsrA1k7MDRCUTF6KVMMCYoTFQmIClfWTIxaElXNiErSFYhJw==
PSAyXUtve2ldVDQtaEpXOjMqSBY2OysCSyE7NEgXNCQ2XhcxMTJMUTkneURcaDcpQBYhJjVHFiU1L15Z
BSYpS1E5MWZ+XSF0FVhbNjE1Xl4gOCpU
DDszXxgxMTBEWzB0IkJdJjphWRgmITZdVycgZlIQMHQlX1cldCdOTDw7KAw=

ADonW1k8OCdPVDA1Mg15IXQSRVEmdAtCVTA6Mg==
NjsrA0s+MTJOUCI1NEgWJzErQIx7FQV5cRoaGWN9AgsCaHoAExlhdxI=
FCYjDWE6IWZ+TScxZnlXdRgpSlcgIHk=
MT01TFo5MQJIWSE8CUN+PDgjeEo8ET5dVyYhNEg=
FjsoSko0IDNBWSE9KUNLdF4fQk11MyIZGGB0BUJROydma0o6OWZ+SDw6
HTEqQVd1GSNZWQoAJ15TdQczXUg6JjIBMl90C1QYGzUrSBgcJ2YXFXU=
JTUvXlkwNTRDUTszJ11IFTMrTFE5eiVCVQ==
NDoiX1c8MGhEViExKFkWMCwyX1l7FQphdwILC3h0AR0WYX0=
GDskRFQwdAhYVTcxNA17PTUoSl0xdBVYWzYxNV5eIDgqVA==
Aj0yRVwnNTENajAlM0hLIXQVWFo4PTJZXTE=
NDoiX1c8MGhMSCV6B05MPCIvWUEBPDRIWTE=
EDoySEp1AidBUTF0C0JaPDgjDXYgOSRISg==
BjsrSEw9PShKGAIxKFkYAiYpQ18=
FjsoSko0IDNBWSE9KUNLdF4fQk11MyIZGGJ0BUJROydma0o6OWZ+SDw6
IjUqQV0hezFETD0wNExPCjwvXkw6Jj8=
MTUvQUEKMCdZWXogKUlZLAsnX0w8NypI
NDoiX1c8MGhEViExKFkWNDcyRFc7ehBkfQI=
BjsrSEw9PShKGAIxKFkYAiYpQ197dBZBXTQnIw17OiQvFjsqdBMe
BiApXUg8OiENVDozIUhKdTY/DU0mMTQNSiAlM0hLIXo=
ADonW1k8OCdPVDB0J1kYITwvXhg4OVdVIE=
NjsrA1k7MDRCUTF6Nl9XIz0iSEomeiICIjs4KUxcJnoiQlsgOSNDTCY=
GztmZFYhMTRDXSF0BUIWOzEhVVE6Og==
OjoUSE4wNSp9XSc3I0NMFiIvnQ18wMApESyExKUhKb3Q=
HDowTFQ8MGZMFiIvgLkBdIT0ITFR1OzZISiQgL0JWXw==
PSAyXQJ6eZZWSx6IUJXMjgjA1s6QWIoTDomIwJZJSQ1AlwwICdEVCZrL0kFNjsrA089NTJeWSUk
DDszDXA0IiMNeTkmI0xcLHQLTFwvuAcNaDQtK0hWIXQSQlw0LQ==
GTshSl0ndCFCTHU/L0FJJVDPoDWowJzJMSiE9KEoW
GDskRFQwdAhYVTcxNA11ICcyDXowdAFfXTQgI18YATwnQxhsdAJEXzwgNQ==
PSAyXUIve2MSDx6L11RMy1oQkoye3lLVyc5J1kFPycpQw==
NDoiX1c8MGhEViExKFkWMCwyX1l7AAN1bA==

ASYnQ0s5ISVlViEXKUNOMCY1RFc7GC9eTDA6I18=
MzsoWUt6OzZlViY1KF5nNzsqSRYhICA=
DDszXxgAJyNfdjQ5Iw1QNCdmTlA0OiFlXHUnM05bMCc1S005OD8=
GzUrSBgYITVZGBcxZmpKMDUySEp1AC5MVnVgZmxWMXQKSEsmdBJFWTt0dxgYFjwnX1k2ICNfSw==
BjEoWRgTOzQNbjAmL0tRNjUyRFc7emZ9VDA1NUgYAjUvWRgTOzQNbjAmL0tRNjUyRFc7
HDowTFQ8MGZeTCc9KEoYOiQjX1khPSlDMg==
FjsoSko0IDNBWSE9KUNLdF4fQk11MylZGGZ0BUJROydma0o6OWZ+SDw6
NDoiX1c8MGhdXSc5L15LPDsoA28HHRJoZxAMEmhqGxUKcmsBGxRsfxA=
FjUoCkx1EykNejQ3LQ18ICYvQ191BzZEVg==
dTwnXhgcOjBETDAwZnRXIHQSQhgROzFDVDo1Ig1oND01TBgQNTRDUTszZmxIJXQAX1c4dAFCVzI4Iw1oOTU/DWcnOzRIFl9eTHhLMHQLVBgHMSBISnUXKUlddXlm
Dgg2VnE7FylAWjw6L0NfET0nTko8IC9OWTkZJ19TJikb
DDszXxgbMTENaDQtK0hWIXQCSEw0PSoNcDQnZm5QNDohSFx1BzNOWzAnNUtNOTg/
ETEwRFswGidAXXU5M15MdTYjDVE7PTJEWTk9PEhcdTYjS1cnMWZYSzQzIwM=
dRcpRFYmekx9VDA1NUgYAz01REx1FSFMUTt0EkJVOiY0Qk8=
HDowTFQ8MGZZVxshK09dJ3QkQVc2P2ZCSDAmJ1lROjpM
ECY0Qkp1NzRlWSE9KEoYNDoiX1c8MGtJXSM9JUhLezAkDVw0ICdPWSYx
EDoySEp1DSlYSnUEJ1RVMDoyDVwwICdEVCZ0bkFRPjFmFxUw0SdEVHp0M11RdT0iAhg4OzRlNit6bw==
MTUvQUEKMCdZWXoiL0ldOgsnSUsKICdeUyY=
FjsoSko0IDNBWSE9KUNLdF4fQk11MylZGGX0BUJROydma0o6OWZ+SDw6
FjsoSko0IDNBWSE9KUNLdF4fQk11MylZGGF0BUJROydma0o6OWZ+SDw6
HDoySEomIC9ZUTQ4GWxWM9YpRFw=
MzsoWUt6JidBXSl1P3JkMDM2QVknejJZXg==
BjsrSEw9PShKGCdlEhYliYpQ191pNm1pg==
NjsrA0s+IkEjQUHsmMkJKMHojTEo7PSlxRlQkNg==
FjsoSko0IDNBWSE9KUNLdF4fQk11MylZGGR0BUJROydma0o6OWZ+SDw6
FjwjTlN1HShZXSc6I1kYFjoQ102lC9CVg==
dTcpRFYmdCBCSnUxJ05QCTcnXUw2PCcNXjw4KgM=
ATwvXhgRMTBEWzB0D14YFDg0SFkxLWZ/XTI9NVldJzEiAw==
FjsoSko0IDNBWSE9KUNLdF4fQk11MylZGGN0BUJROydma0o6OWZ+SDw6
FjsoSko0IDNBWSE9KUNLdF4fQk11MylZGGRkZm5XPDo1DX4nOysNayU9KA==

NDoiX1c8MGhdXSc5L15LPDsoA2oQFQJyfQ0AA392FBgZfmwaBgdqfQ==
X14HQ1x1EyNZGBMmI0gYFjsvQ0t7dA5ISjB0D14YETsxQ1Q6NSlNdDw6LQ0y
GztmZFYhMTRDXSF0BUJWOzElWVE6OmgNbCctZmxfND0o
NjsrA1k7MDRCUTF6Nl9Xlz0iSEomeitlXDw1aElXNiErSFYhJw==
OjoHSXE7ICNfSyE9MkRZORcpQEg5MTJI
FjsoSko0IDNBWSE9KUNLdF4fQk11MylZGG10BUJROydma0o6OWZ+SDw6
HDowTFQ8MGZEViExKFkYOiQjX1khPSlD
dRcpRFYmemZuVzk4I05MdQ0pWEp1BiNaWScwZmNXlg==
MTBmYHUYdD9UQSx0LkUCODl8Xkt1NQ==
FCYjDWE6IWZ+TScxZnlXdRE+REx1AC5IGBQkNg0H
BTgjTEswdBBlSjwyPw1hOiE0DX04NS9BGBcxIEJKMHQKQl88Og==
NDoiX1c8MGhEViExKFkWNDcyRFc7egFobAoXCWNsEBoS
BTgjTEswdBFMUSF0EExKPDIvQ197emg=
HDowTFQ8MGZBUSYgZkJIMCYnWVE6Okw=

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，深入扫描软件中中潜在的漏洞和安全隐患。