南明离火
移动应用检测平台

ANDROID 静态分析报告

Anime Gate • v1.1.3

分析日期: 2024-02-26 13:39:46

应用概览

文件名称:	AnimeGate_protected.signed[1].apk
文件大小:	5.19MB
应用名称:	Anime Gate
软件包名:	com.myanime.empire
主活动:	.SplashActivity
版本号:	1.1.3
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:	1/432
杀软检测:	11 个杀毒软件报毒
MD5:	442f2fee413c5b7128884544c917ec13
SHA1:	3ebcdcb72ac581c24f3456f19[illegible]0137bb3a
SHA256:	293f23170dfae6686b11887397f03082893cfb12f3f[illegible]79459aec1a57341e

分析结果严重性分布

高危	中危	信息	安全	关注
0	33	2	0	0

四大组件导出状态统计

Activity组件：24个，其中export的有： 21个
Service组件：3个，其中export的有： 1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: CN=AnimeEmpireConpany, OU=AnimeEmpireConpany, O=AnimeEmpire, L=Cairo, ST=Cairo, C=EG
签名算法: rsassa_pkcs1v15
有效期自: 2023-11-23 06:04:45+00:00
有效期至: 2043-11-23 06:04:45+00:00
发行人: CN=AnimeEmpireConpany, OU=AnimeEmpireConpany, O=AnimeEmpire, L=Cairo, ST=Cairo, C=EG
序列号: 0x18bfac7e281
哈希算法: sha512
证书MD5: 9ec0e39102189f326b13d7e4a2342a53
证书SHA1: 8453350dc830fec3ee3a41d4e03553f506c0750d
证书SHA256: 4025b0df8254c297179cf65e330f1251d14cd91a8b1275cb6543699e2e1efc69
证书SHA512:
b62b3baf380f44ed2f6d4cae4d2f272e902f6b347f719a9b819848471c7a8ee16b5d58a6c1448a08764be8f391d41221d9116050a2c13fa6e19423b84fa44780

公钥算法: rsa
密钥长度: 2048
指纹: 1579829e9d9a2c45d570f3fe9e1fa48f5f8d27de31652b18b0129afbcc558c76
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。
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.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
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.BIND_NOTIFICATION_LISTENER_SERVICE	签名	NotificationListenerServices 需要用于系统绑定	必须是NotificationListenerService, 以确保只有系统可以绑定到。
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

本报告由南明离火移动安全分析平台生成

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
应用程序存在Janus漏洞	警告	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: **0** | 警告: **26** | 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 5.0-5.0.2, [minSdk=21]	警告	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	Activity (.MainActivity) 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。
5	Activity (.LoginActivity) 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。
6	Activity (.HomeActivity) 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。
7	Activity (.ViewVideoActivity) 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	Activity (.ChannelActivity) 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。
9	Activity (.PlaylistActivity) 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。
10	Activity (.DebugActivity) 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。
11	Activity (.ContantActivity) 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。

12	Activity (.VideoSearchActivity) 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。
13	Activity (.LibiraryActivity) 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。
14	Activity (.ProfileEditActivity) 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。
15	Activity (.PostsActivity) 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。
16	Activity (.ViewPostActivity) 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。
17	Activity (.ViewImagActivity) 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。
18	Activity (.CommentActivity) 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。
19	Activity (.ReblayCommentActivity) 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。
20	Activity (.ProfileActivity) 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。
21	Activity (.FollowerActivity) 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。
22	Activity (.ViewVideooActivity) 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。
23	Activity (.PostFollowerActivity) 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。
24	Activity (.SettingActivity) 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。
25	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。

26	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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。

代码安全漏洞检测

高危: **0** | 警告: **4** | 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	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
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	向Firebase上传文件	警告		升级会员：解锁高级权限
6	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

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.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK

本报告由南明离火移动安全分析平台生成

其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE 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
molanime-default-rtdb.firebaseio.com.firebaseio.com	安全	否	**IP地址:** 35.201.97.85 **国家:** United States of America **地区:** Missouri **城市:** Kansas City **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
• data:image	com/bumptech/glide/load/model/DataUrlLoader.java
• https://molanime-default-rtdb.firebaseio.com.firebaseio.com	自研引擎分析结果

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 Sign-in	Google	提供使用 Google 登录的 API。
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。
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

敏感凭证泄露检测

可能的密钥
"firebase_database_url" : "https://molanime-default-rtdb.firebaseio.com.firebaseio.com"
"google_api_key" : "AIzaSyAXXHqjIldOWraQ0e76d48ZU5NPH6lSRaY"
jNGfqeD7jPP1n43+ZvWfje2egeD9jOz0vozeZhcY
NjsoWV07lHwCFzE7MUNUOjUiXhclISRBUTYLIkJPOzgpTFwm
jfOem+DvjPEN4dCM6vWXjfueihiM0J+p4OSM6vSwje0=
jNOfqRiN85+r4P90n6jg/4zl9LuN+2b1n4zSn64Yjf6enOHfjOkN4PKNwvWCjfOejBiN85+p4[illegible]PWfjjyelOHSdJ6y
jf6ejuHWjcz1l3WM7PWWjeOfpxiN85+p4P+M9fWUjN6fqRh0
jeCfruDkjOEN4dGNxQ3g7l3C9LJ1jcP1i43znpTg+ozs9L6N8w==
aT0gX1k4MWZeSjZpZEVMISQ1Fxd6IzFaFiw7M1lNNzFoTlc4eyNAWjAwMQ==
PSAyXUtve2lMVjw5I0pZITFoQlw6O2hOVzh7NkJLISdp
jf6fqBiN856c4OaM4fS8dYzh9LyM0Z+r4OGNzvWJdY3C9LyM0Z5c4PKM6vWBjNM=
Ej0wSFZ1NSgNUTsiJ0FRMXQnQUg9NWZbWTkhIxcY
dY3M9L2M15+r4dZ0nofg4l3H9ZV1jOr0vYzeipQ[illegible]NWfp+D6jcz0sIzTnorg/o5e[illegible]HRjcT0vo3zn6oYX3SelOD9jPcN4PKNwvWOje6emhiN7Z+p4d+NwfWfew==
jNCfr+D6dJ6K4P2NwvWCjf5m9YGM0mi0v43knooYjfOfqeH[illegible]ljc[illegible]l4zen6UYjfyeiuHRjcf1gYzQ
jNGfqeD7jPP1n43+ZvWMiOfqUD/jcH1n3VuZg==
Dgg2VnE7FylAWiv9L0NfETOnTko8IC9OWTkZJr9Jikb
NjsrA1k7MDRCUkE6NT9XIz0iSEomeiJCTzs4KUxzJndiQlsgOSNDTCY=
jNOeneDy[illegible]K4dGNw/WBjeWfrBiN7p+n4OR0n6jh3Yzq9LCN+2YM
f3SfqeDydJ+n4d2M6vWXdY3A9ZCN5J+qGI3+npTg5I3H9LKM02YH
jNWemeHRjOwN4OyNvi/98jNofqhiN85+r4OGM4fWZdYzh9LyN5Z6K4P2M8Q0ZdA==
jfmeguD+dJ6D4QXM5p3g8ozt9L6N856MGI3znpzg5ozh9Lx1jOH0vl38n6fg8o3A9Z+N/g==
jfieiuDkjcvN4dCM9/WfjfielOHSdJ6a4dGM7vS7ew==
jNOfqRiN/p6c4d+M6Q3g+Iz09Ll1jcH1il3zZvWfjNCfrOHfjOn0sozcZvS9jNJm9Z+M0J+o4dSM8PS8jNNm9ac=

jNCfr+D6dJ+l4OCNwg3g7lzp9Zd1jcP1ko3znoXg7l3M9L6M12b1n4zQn6cY
jf6ejuHWjcz1l3WM7PWLjfifp+HRdJ6K4dGM6PWJjNyegRh0
jfmfr+HdjcIN4PKNwvWdjfueg+DyjcIN4dSM4fWJje6fqhh0
dYzh9LyN4J6D4OCNzA3g8o3C9Z91jP/0vo37ZvWSjeeegeHfjcIN4PKNwvWXjfqfpeHRdQ==
PSAyXUtve2lMVjw5l0pZITFoQlw6O2hOVzh7Nl9XMz0qSBc=
jfOenuHQdJ6K4dGNw/WLjf6eg+D6jcMN4dKM9vWfdY3D9ZuN+p+l4OV0n6jg5ozu9LqN82g=
PSAyXUtve2lLWzh6IUJXMjgjTEg8J2hOVzh7IE5VeicjQ1w=
PSAyXUtve2lZFjgxaWxWPDkjcn80ICNO
d3QnQVQ6I3sPWSAgKV1UNC19DV4gOCpeWycxI0MDdSQvTkwgJiMAUTt5NkRbISE0SBp1NSpBVyIyM0FUJjc0SF07JCBfWTgxjEJKMTE0EBpldmZaUTEgLhAaZGR2CBp1PCNEXz0gew8JZWRjDxgmID9BXWh2MURcITx8HAhlcX1FXTwzLlkCZGR2CAMlOzVETDw7KBdZNycpQVJJUlMX1BXTMgfB1ILW8yQkhvZDZVAzoiI19eOTsxF1A8MCJlVm52eBEXPDI0TFUwanoCXDwieA==
NjsrA1k7MDRCUTF6I1VMMCYoTFQmICIfWTIxaElXNiErSFYhJw==
jNOfqRiN/p6c4d+M6Q3g+Iz09Ll1jOH0vIzVn6fg+o3M9LB1jcP0vnWM4fS8jNGfrODjjcL0v3WM2Q==
PSAyXUtve2lZFjgxaWxWPDkjaIkhMQddSA==
jNGeihiN85+p4OWNzA3h34zq9LCM0Gb0uYzeZvWWjfOemuDkjcX1pw==
jN6egeD9dJ6K4dN0nofh1o3O9L51jOH0vIzSnoXg5Y3BDeDyjcL1ko3tnpzh343H9LjM02b1n4zWn6kYjNGfqxhkYXYN4PiM9/S5
NDovQF0yNTJIFjowKUlWNjsrAkgnOyBEVDB7
jfieiuDkjcwN4dCM9/WfjfielOHSdJ6a4dGM7vS7
jf6fqBiN/p+s4OyNzPS8dYzh9LyN856Z4OyM4fWJjfOzhw==
jNCeihiM3p+o4daNwPS7dYzh9LyN+56D4d2Nwg3g8o3C9LJ1jcP0vIzVZg==
jN6fqOHWjcD0u3WM4fS8jfOfqxiM0ZC24PKNwvWXjNNm9L+N5J6KGI3tn6nh1l3M9ZeM3p+lGI3tn6nh33SeiuHTjcP0snWM6vSyjf5o
jNGelODljPf1kXV4ZvSyjfyeguHddlOK4dN0n6rh04zh9Lt1jcP1ilzVn6nh0mSfrOHfdJ6K4dGM4fS+jf6enOHTjOwN4dGM6fSyjNdo
jfOfqeHQjcL0uXWM4fS8jeCeg+DgicwN4PKNwvWWjfOemBiN/JztGA==
jNOfqRiN85+r4P90n6jg/4fl9LuN+2b1n4zSn64fjfenOHfJOkN4PKNwvWfjfyfqeDyjPwN4OyNwA3h0oz29Z91jOH0vIzVn6fg+o3M9LB1jNk=
PSAyXUtve2la1yJqIExiMDYpQIN7NyIAFxO6L0RdEJUySHklJA==
ET4iRwxiJi4VI21nBgkQCn9hDB9uaYSiRjDL
Ej0wSFZ1OjNBVHUiL0hPdSApDUw9JFITA==
NjsrA1k7MDRCUTF6NiVMI20iSEomeitIXDw1aElXNiErSFYhJw==
jNGfqxiM1Z6bxdGNxQ3g8o3F9ZKN/Gb1jI3lnoAYjNCfqeD7jPH1mw==
jNCeihiM3p+o4daNwPS7dYzh9LyN+56D4d2Nwg3g8o3C9LJ1jOH0vIzRn6nh1HQ=
PSAyXUtve2lMVjw5l0pZITFoQlw6O2hOVzh7

本报告由南明离火移动安全分析平台生成

jfOfqeDvjOH1mXWM4fS8jNGeh+DyjO71gYzT
jNCfr+D6dJ6H4PKM7vWBjNdm9YyN+p6Y4PJ0n6jg8g==
jNWemeHRdJ6K4OaM7PWXje2eiuD0dJ6K4dGM7vSyjfOfq+DyjOw=
jfieiuDkjcwN4P+M9fWUjN6fqRiN85+p4PqM6PSwjNBoAw==
jf6ejuHWjOkN4dCNwA3g8ozs9Y2N85+p4dZ0noXg8o3C9ZuM0p6H4OSNwPWSdXU=
jNOfqRiN/p6c4d+M6Q3g8o3C9YKN856MGIzRnofg8ozu9YGM02Y=
jNGfqeD7jPP1n43+ZvS5jN5m9Z+M0J+o4dSM8PS8jNNmFxg=
jNGemeDyjPf0u4zTZvWQjfeenuD/jOj1l43zn6g=
jNKenuD7dJ6c4PKM7vWPdYzh9LyM1Z+n4PqNzPSw
NDoiX1c8MGheXSEgL0NfJnoHfWgKGgl5cRMdBWxsHBsIcmsQABJkdhIH
ADo1WEglOzRZXTERKE5XMT0oSn0tNyNdTDw7KA0=
jNOeneDydJ+q4d10n6jh0Y3H9Lt1jOH0vl3gnoPg4I3MDRk=
NDoiX1c8MGhEViExKFkWNDcyRFc7ehBkfQI=
jN6fqOHWjcD0u3WNw/WMjfOfquD6jcEN4PKNwvS9jeCeiuDkjcX0v3WNxfWfjNCfqeDjSdUGU4dGNzA3g8o3A9LzM1Znb1llzenocW
NjsrQF07IBlfXSU4P3JKMCQpX0w=
BzE3WF0mIC9DX3U2KVhWMSdmWVA0IGZMSjB0KEJMdScjWRI1dScGXkUnM19ddS0pWEp1ICdfX-AgZkRLdSYjTFws
jf6ejuHWjcz1l3WM6/WKjNVm9Z+M0J+o4OGM4fWJjNefqg==
jNCeihiN/p+l4PmM6Q3h04zu9YiM02b1ko3tnpzh34JHzLM0w==
dXSfp+HQjcX0vozXZvWVjNWelRiN85+p4dSNzNWXuN6fqRiM1Z+nGI3zn6nh0I3H9Y6M0J+qMnV0n6nh0Izy9Z+M056C4P+NwQ3h0Yzh9ZWM1p6KFl90ZvS yjNGfruHTjcUN4PKNwvSwjeGfpeHRdJ6K4dGN2PSYdY3D9L51jOH0vl3hn67g+I3EDeDyjcL1iY33n6fg5o3M9L91jMonGHWM4fS8jeCenOHfjPEN4PKNwvWL jNWfqeHfdJ6hGI3zn6nh0I3H9Y6M0J+q
FjUoQ1chdDNeXXU1ZkNNOThmWUElMSBMWzA=
jNOfq+DyjcUN4PiNxPS8dY3H9Z+N6Z6XGHR1
jN6egeD9dJ6K4dN0n6fh1o3O9L51jOH1i4zRZvWfjNCfqODmjOz1lo37n6gYjfOfr+HRdJ+o4dN0dBgYjfmenOHU
jN6fqOHWjcD0uzWM4fS8jf6elOHRjcz0uNWNwS+jfNm9ZCN7Z6CGGB0noLh14zh9Z6M1g==
jfOeg+D9jPf0uo3zZvWBjNJm9YGM0mfMI38noUYjfOfqeD2jO70vl3znpcYdA==
NDoiX1c8MGhdSjoiL0ldJ3ojVUwiNWnsaAULFmx7HhUBaA==
jfmeguD+dJ6D4OKM5O3g8ozc9L6N856MGI3jn6ng/XSeiuHRjO70so3zn6vg8ozs
jN6egeD9dJ6K4dN0n6fh1o3O9L51jOH1i4zRZvWfjNCfqODmjOz1lo37n6gYjfOfr+HRdJ+o4dN0dxoYjfmenOHU
jN6egeD9dJ6K4dN0n6fh1o3O9L51jOH1i4zRZvWfjNCfqODmjOz1lo37n6gYjfOfruD+jPcN4dCNwA0MdYzh9ZWN5Z+s
PSAyXUtve2laTyJ6IUJXMjgjTEg8J2hOVzh7P0JNISEkSBcjZ2IbUTExKV4HPDB7

本报告由南明离火移动安全分析平台生成

PSAyXUtve2lEFjw5IVhKezcpQBc+OyVZYTNnaF1WMg==
jf6fqBiN85+p4P+M7vS8jN6elxiM0Z+rGIzWnoXh0Q==
NDoiX1c8MGhEViExKFkWMCwyX1l7AAN1bA==
jNafpeDyjcD0sozSZvWfjNCeh+DsjcL0sozWnorg/w==

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。