南明离火
移动应用检测平台

ANDROID 静态分析报告

HiGo

HiGo Play服务框架安装器 • v1.3.0.1

分析日期: 2024-06-06 07:39:34

应用概览

文件名称:	com.higoplayservice.higoplay_1.3.0.1.apk
文件大小:	17.44MB
应用名称:	HiGo Play服务框架安装器
软件包名:	com.higoplayservice.higoplay
主活动:	com.higoplayservice.higoplay.SplashActivity
版本号:	1.3.0.1
最小SDK:	24
目标SDK:	30
加固信息:	360加固 加固
应用程序安全分数:	47/100 (中风险)
跟踪器检测:	4/432
杀软检测:	3 个杀毒软件报毒
MD5:	a97507340a0561eb9088cfe63deda37c
SHA1:	135788d065cb10fbb75a5eaa5246e51255a88c5
SHA256:	e8ab4cb3fff92905cbbb1739130c75213dcd55fa342a671aaa20cb799cbee93e

分析结果严重性分布

高危	中危	信息	安全	关注
1	16	3	0	1

四大组件导出状态统计

Activity组件：43个，其中export的有：7个
Service组件：8个，其中export的有：3个
Receiver组件：3个，其中export的有：0个
Provider组件：5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: O=Play, OU=Go, CN=Hi
签名算法: rsassa_pkcs1v15
有效期自: 2020-11-06 08:37:50+00:00
有效期至: 2145-10-07 08:37:50+00:00
发行人: O=Play, OU=Go, CN=Hi
序列号: 0x195f5395
哈希算法: sha256
证书MD5: 830bc7c5a2293be32f1b4fcadb422d15
证书SHA1: 2271fd6b0768ea273e6043a38e6bf3fb7571d3ad
证书SHA256: c984e4129f69cf13af27bb19add8eba8b04bd50199f42c1c0388817f8cebde03
证书SHA512:
91776e4ce70d0b52e6b94f744922d38b43127b1502c70addf1bc27b1b05778958e411db1c4725c1ee0adc0d4ab425a797bcfa71c7b1077bc99f4cb3c4ce285a

公钥算法: rsa
密钥长度: 2048
指纹: ed0b3a418cd372017c953dbbb2c3309d311c0f29dc53d1bc88be17e07f5c1ecd
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_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.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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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.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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。
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.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.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
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.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.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。
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	未知权限	来自 android 引用的未知权限。
com.higoplayservice.higoplay.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.higoplayservice.higoplay.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
android.permission.BROADCAST_STICKY	普通	发送置顶广播	允许应用程序发送顽固广播，这些广播在结束后仍会保留。恶意应用程序可能会借此使手机使用太多内存，从而降低其速度或稳定性。
com.hihonor.permission.MANAGE_FOLD_SCREEN	未知	未知权限	来自 android 引用的未知权限。
com.hihonor.permission.MANAGE_FOLD_SCREEN_PRIVILEGED	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.higoplayservice.higoplay.SplashActivity	Schemes: um.5[illegible]b11c520d30739f89d8://,
com.huawei.openalliance.ad.activity.PPSLauncherActivity	Schemes: hwpps://, Hosts: com.higoplayservice.higoplay,

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: **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 7.0, [minSdk=24]	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	Activity (com.higoplayservice.higoplay.HuaweiEmptyActivity) 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。
5	Service (com.higoplayservice.higoplay.MyAccessibilityService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_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。
6	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护。 Permission: com.higoplayservice.higoplay.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	发现 Broadcast Receiver被导出，但受权限保护。
7	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护。 Permission: com.higoplayservice.higoplay.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	发现 Broadcast Receiver被导出，但受权限保护。
8	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 未被保护。 [android:exported=true]	警告	发现 Service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。
9	Content Provider (com.huawei.hms.support.api.push.PushProvider) 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。
10	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。

11	Activity (com.huawei.openalliance.ad.activity.PPSLauncherActivity) 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。

代码安全漏洞检测

高危: **1** | 警告: **6** | 信息: **3** | 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	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
4	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
5	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
6	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
7	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

8	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
9	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
10	此应用程序使用SQL Cipher。SQLCipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-1	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/liberrno-lib.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	5/30	android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.SYSTEM_ALERT_WINDOW android.permission.ACCESS_COARSE_LOCATION android.permission.VIBRATE
其它常用权限	9/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.CHANGE_NETWORK_STATE android.permission.REORDER_TASKS android.permission.BROADCAST_STICKY

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

dd.higoazq.cn	安全	是	**IP地址:** 58.220.53.74 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435600 **查看:** 高德地图
greenrobot.org	安全	否	**IP地址:** 85.13.163.69 **国家:** 德国 **地区:** 图林根 **城市:** 弗里德斯多夫 **纬度:** 50.604919 **经度:** 11.035770 **查看:** Google 地图
chat.openai.com	安全	否	**IP地址:** 172.64.150.28 **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://developer.huawei.com/consumer/cn/doc/development/HMSCore-Guides/privacy-statement-0000001050042021 • https://developer.huawei.com/consumer/cn/doc/app/20213 • https://www.pangle.cn/privacy • https://qzs.gdtimg.com/union/res/union_cdn/page/dev_rules/ylh_sdk_privacy_statement.html	自研引擎-A
• 1.3.0.1	自研引擎-M
• https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/database/DatabaseOpenHelper.java
• http://chat.openai.com/invite/accepted	com/higoplayservice/higoplay/HuaweiInstallActivity.java
• http://www.google.com • http://chat.openai.com	com/higoplayservice/higoplay/DcActivity.java
• 1.3.0.1	com/higoplayservice/higoplay/BuildConfig.java
• 4.0.0.132	com/higoplayservice/higoplay/utils/DevicesUtils.java
• http://attavi.oss-cn-hangzhou.aliyuncs.com/higo_host.txt • http://dd.higoazq.cn/higo/higo_host.txt • http://47.114.181.15/higoplay/user/	com/higoplayservice/higoplay/utils/HttpUtils.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息

岳鹰全景监控	Alibaba	岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。
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。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
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。
HMS Core	Huawei	HMS Core 是华为终端云服务提供的端、云开放能力的合集，助您高效构建精品应用。
Huawei Push	Huawei	华为推送服务（HUAWEI Push Kit）是华为为开发者提供的消息推送平台，建立了从云端到终端的消息推送通道。开发者通过集成 HUAWEI Push Kit 可以实时推送消息到用户终端应用，构筑良好的用户关系，提升用户的感知度和活跃度。
腾讯广告 SDK	Tencent	腾讯广告汇聚腾讯公司全量的应用场景，拥有核心行业数据、营销技术与专业服务能力。
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。
AppGallery Connect	Huawei	为开发者提供移动应用全生命周期服务，覆盖全终端全场景，降低开发成本，提升运营效率，助力商业成功。
HMS Core AAID	Huawei	华为推送服务开放能力合集提供的匿名设备标识(AAID)实体类与令牌实体类包。异步方式获取的 AAID 与令牌通过此包中对应的类承载返回。
HMS Analytics Kit	Huawei	华为分析服务（Analytics Kit）是针对移动应用、Web、快应用等产品的一站式用户行为分析平台，贴合业务全景，提供数据采集、数据管理、数据分析、数据应用的一体化解决方案，驱动企业实现精准拉新、产品优化、精益运营、业务增长。
Jetpack Media	Google	与其他应用共享媒体内容和操作。已被 media2 取代。

第三方追踪器检测

名称	类别	网址
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333
IAB Open Measurement	Identification, Advertisement	https://reports.exodus-privacy.eu.org/trackers/328
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Crash reporting, Analytics	https://reports.exodus-privacy.eu.org/trackers/448

敏感凭证泄露检测

可能的密钥
友盟统计的=> "UMENG_CHANNEL" : "Tencent"
友盟统计的=> "UMENG_APPKEY" : "5fa12ba11c520d30739f89d8"

华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "appid=103224961"
69318414a070e59c977c67c27d4dd024
52c60fbbc3c4e03edeb5d72dd7fbd718
9ee0c028649cc203e0af209c17ad8bd8
830bc7c5a2293be32f1b4fcadb422d15
cf2ec5a6cce32f51285dc8e269968bcf
47c2cd9871a9b289a720420e531a0e0469365a08126bd9ffccfd4b7efc6ec3e9ebcb5acc24b4d812dc81c7359d855d0d9ea3325f42330 1fd7a410df0f0308 aa6872cfd6e34cf652bc7f1abc71841af2c854dab37d8b67b10c1ef7e171235bcfe03065e2652cb872bde44f687b53ae922397a3 d18b79ee73de01b039d 208aaea214aa79bce72ec6f5e611a12edd94ab63cafd71ff9f623a1c8fa4a1677bad5d4be2a33371cfde29a3864d4b3ee5a051 6784221568a96b8326af1c ed0b5565e4416c8b708bebcf18dc1af520d082cea0ba8117c9a508fbff524ae55d970eb285f5b232e01c1e8262acde62 65dfdb286d13c09df02c5f2cb8e5 27c1c74c50459068cb3aa1f027dac7ed6b5c280127861aaf13570c43c26b30a634648a767e0e4340d9d13a935dc9fe24 3c6d0664134d9fabfaccdc52b7ef dcb1b791dca6181fb72cb7127c491d3f1b36e2217a318d7affb7b16f6318adab7945147832ff0f3817ed25bfd37f 06bdcabc04138baa9d8c9dae2225de0a 3feefaa064aa19a47eabee6c2c4ed03396fdf9d6e9a9017fe0b77ac5399e29b3924d69033db9b3e136137e83b9 e 9f716fac22b2ef0963b54fec4aa2e91 a7f04ae0bbf9911dde74bfae93e665207a68107d525875799dd80cdd0da8d530ce39b2aeb5079db00caa90a 3dd875bb9d187cfa756 8147d9df805f 7f02b58e8e41b633960f2e0353f7040cee023c47cc9f7eef3677b6174833f820f65f6082b496ae5c7df405 76 7dcd627b13ed2f874fc6 f82 a50ab9fa4 e3c8736b8d3bc30f977651dc19340f0d14484bc901bc32d42477b94b1c5d7b635fa4b377b270989a3140 1088e7ecff43cc3f2582d911 2 93390b292b7 76e8960737f5eac056abb0d641d3b80f144fe79a8b0e6df9e09ff70f0861751da8ed484f205fc842 f4 87ec7a4197e151ea d 6d7f8c69d7c60097b5f6 985fec57d507fc6ac4a8e383714f98599d36f45967da73dfd2be5e37d3df6a4667c896e309726b3 b8 e 5b38a95326340b3239d63 e47d9fe054d7b1be9 b10b825dc122fcd312b53cb91f46aeb22870caa83b6d999bde1345cfcc371c3d9cbb65f77 7d7 d49e2ecbe646c129d9 5 4b798d7f7c218052343c6baf33 14e1216903d48b4e7fd74e031f6d5e9f56a8f19819419a31dd039f4993fdc37b44911cb5c a1 4a5e2db131231dc49f39 23bf6d5cf787a087f0837e39eba 66c8d2c5f73ca97f0038e81ade0ed626f2c175ce6e492670235e365b87d931287c7 b4159d6b 3724d711b1d48 013e7336d9e3e97e8b8a1729fad6b249 0c09bc84dd11d4bf79530a794c625e79ea7114dd57b7401b582e439ffecd21c628 a1 4f ac9a4dc8f27b1b777238 ddfeccca94ab58f5e0b7918efbc5bae 7a9a060b50ba2f88e2aa211df72bedc56d9063371e7ad4c9ba5532b781383 9 b e fd 4956b2206d92a7 2f 3952859b01d3c106dd25f9bb97bb4bdd5 2377d48231d466ee0a404821dfe73d22b946dc79a197bce5fd28cead2c1 caf1745326346a641de557 69e9 c18dd296d4fe9646492d7d53d4a5fefda 8264bf1c2952ae4db0e39631907ec45cc97d7ce6c65599708d21777 484e1 a 156c1f7a9bc3a97f5e188 201d47b712d96c3716bb92789a09ddfb2c71 6b167e9e8a6e5291b82feff9b35ecce0de9cc5f90e1e59cab7e647b 4c 3954df46fe1acd31d 5 4328219e003f5ffcbc32eaac40466e979c3f66880ba 5ed510faeb25e38e6bdf36ec69277aadae8fd1d7d1637ecc3fe36b 9 c49dd5c2cd28a7abc3a53 5 ee 54214a90be31574eea29121559119529bc14a88 a84657c8228c750c26ed13e59294b8c797140eee24bc0b5d 0a b2b6326675f19c2521a1 1368c6177873d16e54b07894fa9c58152c9c7c24db9d1f2cdc 885686c296330554362ce765b80ce6dd322fedd3ffdedf1fe7 c eabffbfb1bf04b5fa4a78e bf 82b67773175d57f2a826af23b5bb9565ca4ab15dc750e9 01223927da3f45e4f5d87c9a71a87d6b7e2a782e98f9 1 26bc456e08b94fcb886 b 6 441b2165b57640edd50fcd328fb4a1b9c231d42f58103ced93ef2 cdf57b881dee71f7b29aab2fe33d716f749dfb7ab2 3 d 15df5375aba692a0c 1 c2 ad1088a243c0e0ef8503a64a7371b079ad54d7c1ca25bd7caf91 2e18bf75560c38abd34bd7a6116bfd18e5f32f 6 cf0c d e3a521eb47c1011 c 2cc8276c05013653f55613cabe7852b5eebbe70556f5bca6a7e59980dae 2e5f268f70278f692f8b1e699dd5f396a147f 2 e 2d 3ab73a96e7c0c6a 9 a 178b4c164ae5deb997ff4e981bddcebd742b7917abf900b26fa40b16fa2 69d78d626ff5a0c22c22c1229667147f6fbe4b e 3 eab7aba946f8c44 ed8a0 8 81d88e2bbbd8e7c383fb553f79f641d09f2d3e4d4e9f3e9eede6f2adcdc 9f54a8b028facdedccf6152c7def3b67f 6 dc e6d3f9dd15c854c3 f 5 e0d2762686b2cf8a67f8023ebddd86aca81017450586c5e4111cf8460297918f2 80d890eeeb8de4f976ffb7f4828d627 6 3 30f1d7db64c7044d6a4 9 b e6540c73d95fefaf44dc84bba9a83af5fd3bc79792ee17b041a94b74788a4b5 ce6e0b9fda952107f4ed8c9290 0 8012e7b7a5d2b68ea 2 d853 1 c135b917abfb52578c58918d9a0fb2360d1d9e2a15dbb320c4bd7c0b046a3353d ed452dad368b8be48366a19 fbf d5 6396aac5b46ceadf1 a 4039aed07b27b8f8eda06acd4e966f05f9761a0fcab0e4a9f5d0b30dad65eb03762f73da 6960ae28b94766bc8b3fd cb2e 5 5606aa11c0529e 4 1af 7 c961a7a44e24eff7ce8a1add708ef80f1734c26a419c3a
986a55bfe6a2d8 a 1375 d d6fcd3681
0eae4029fb96e 4 d d696d706a4c16
08699a06f 4602f5b01c666f1c4739
4887bded799406f6c121be4634 0 e7
fc54d4eb2f71aac3b1c 0 5 4c17ca8
f3b75ad67adba 5 c 1 a74c48d7585
a9d77d d 5 45643084316bfb1b3ca97c
c07be3abe7074db36460fd377a8160b5

31293308b3af2dea130418d4c325ac90
b7bbd9ad92049d34c54168d29c6e860d
72367d23f7832700f03a43f46f1472b1
a82c3ccae31fd1c3eab94f62d3d06895
fdc80791375d2c4453ee751aa1c1d706
b762ae53f58cd32a6fcfec71da97cf7a
5fa12ba11c520d30739f89d8
5a2a2166b0bdfd935a9710f6c0145951
10f2423d70c54b4ade3a0e101dc53154
009d56873d14698f6d1b525f18e2ae99
93e19ea2e19f8ae19eb7e19e93e19e82e19f92e19e9ae19eb8e19e94e19e93e19f85e19e80e19f92e19e9ae19ebbe19e84e19e80e19e9ae19e94e19e98e19f92e19e9ae19ebbe19e84e19e91e19ebbe19e80e19ea1e19ebee19e84e19e9ce19eb7e19e89e19e91e19eb6e19f80e19e84e19e9fe19f92e19e9ae19ebbe19e84e19e9fe19eb7e19e9320e19e91e19ebee19e94e19ea2e19eb6e19e85e19e85e19ebce19e9be19e94e19f92e19e9ae19ebee19e9ce19eb6e19e94e19eb6e19e93e19f94001b41e19e85e19ebbe19e85e19e94e19e98e19f92e19e9ae19ebbe19e84e19e91e19eb6e19e80e19e93e19f85e19e80e19f92e19e93e19ebbe19e8420486953756974650001c54e19e85e19ebbe19f87e19e88e19f92e19e98e19f84e19f87e19e85e19ebce19e9be2808be19e8ae19f84e19e99e19e9fe19f92e19e9ce19f90e19e99e19e94e19f92e19e9ae19e9ce19e8fe19f92e19e8fe19eb700b21e19e85e19ebbe19f87e19e88e19f92e19e98e19f84e19f87e19e85e19f81e19e89004580c5e19e85e19ebce19e9ae19e94e19f92e19e9ae19eb6e19e80e19e8ae19e90e19eb620e2808be19ea7e19e94e19e80e19e9ae19e8ee19f8de19e93e19f81e19f87e19e8fe19f92e19e9ae19ebce19e9ce19e94e19eb6e19e93e19e97e19f92e19e87e19eb6e19e94e19f8be19e91e19f85e2808be19e94e19e8ee19f92e19e8ae19eb6e19e80e19e8ee19f92e19e9ae19ebce19e85e19e82e19f92e19e93e19eb6e2808be19e93e19eb9e19e84e2808be19ea7e19e94e19e80e19e9ae19e8ee19f8d204e4153e19f94001030e19e85e19ebce19e9be19e80e19f92e19e93e19ebbe19e84e19e94e19f92e19e9ae19e96e19f90e19e93e19f92e19e92003180e19e85e19ebce19e9be19e80e19f92e19e93e19ebbe19e84e19e94e19f92e19e9ae19e96e19f90e19e93e19f92e19e92e19e8ae19ebee19e98e19f92e19e9ae19eb8e19e9ae19eb8e19e80e19e9ae19eb6e19e99e19e87e19eb6e19e98e19ebde19e99e19e9fe19f81e19e9ce19eb6e19e80e19e98e19f92e19e93e19e85e19f92e19e9ae19ebe19e93e19e91e19f80e19e8f00152be19e85e19ebce19e9be19e94e19f92e19e9ae19e96e19f90e19e93e19f92e19e9220485541574549204940f2de19e85e19f82e19e80e19e9ae19f86e19e9be19f82e19e80e2808be19e87e19eb6e2808be19e98e19ebde19e9900133e19e85e19f82e19e80e2808be19e9ae19f86e19e9be19f82e19e80e2808be19e87e19eb6e2808be19e98e19ebde19e9920257300091be19e85e19f92e19e9ae19ebee19e93e2808be19e91e19f80e19e8f000e2ae19e87e19e98e19f92e19e9ae19ebee19e9fe19e85e19f92e19e9ae19ebee19e93e19e9ae19f80e19e8f00050fe19e87e19f86e1
20133f6fbb00d5c13cff462942d5b50b
55d27a08a0116646e257872dab9f7296
26bcd6f35f7d99c873a72d7cc89a22f7
0e67ed77e70093c8b5e91e1f16ccde6
db90c96ed7f7be75cd9fa0500399efdb
677d0a8[illegible]26871705bec18ab8831073

本报告由南明离火移动安全分析平台生成

免责声明及风险提示: