南明离火
移动应用检测平台

ANDROID 静态分析报告

MOD • v1.0

分析日期: 2025-04-07 13:46:30

应用概览

文件名称:	MOD v1.0.apk
文件大小:	1.73MB
应用名称:	MOD
软件包名:	com.exclude.regret
主活动:	com.example.mmm.replace_1
版本号:	1.0
最小SDK:	26
目标SDK:	29
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	44/100 (中风险)
跟踪器检测:	1/432
杀软检测:	22 个杀毒软件报毒
MD5:	149d6768caf7f42e480fdc577806efad
SHA1:	584050aa0ca1ea52bda7af97c6905535c860e2e6
SHA256:	c9062e1abe13a47[illegible]1d2f7d348c679da17c1251f7eb05867d79af63665df6

分析结果严重性分布

高危	中危	信息	安全	关注
2	18	1	0	0

四大组件导出状态统计

Activity组件：10个，其中export的有： 2个
Service组件：10个，其中export的有： 2个
Receiver组件：3个，其中export的有： 3个
Provider组件：0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: False
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Android, CN=Android Debug
签名算法: rsassa_pkcs1v15
有效期自: 2013-12-31 22:35:04+00:00
有效期至: 2052-04-30 22:35:04+00:00
发行人: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Android, CN=Android Debug
序列号: 0x232eae62
哈希算法: sha1
证书MD5: 20f46148b72d8e5e5ca23d37a4f41490
证书SHA1: 5e8f16062ea3cd2c4a0d547876baa6f38cabf625
证书SHA256: fac61745dc0903786fb9ede62a962b399f7348f0bb6f899b8332667591033b9c
证书SHA512:
926c0550edaee7aed1211b91fde06be4cc4748e61d8f1afbe0bd12f3949a0d09a1cf4306c72e6662ae4c7b8ae7a573a81d7252e5b6124444eaf8f413e6b1fa69

公钥算法: rsa
密钥长度: 2048
指纹: b759a55bdc298b16f7a102f3107f3db38110f3dc7da00b1e981e9b257a9cf1af
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.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.READ_CONTACTS	危险	读取联系人信息	允许此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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
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.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.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.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.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.ACTION_MANAGE_OVERLAY_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。

android.permission.GET_PACKAGE_SIZE	普通	测量应用程序空间大小	允许一个程序获取任何package占用空间容量。
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。
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.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.BLUETOOTH_SCAN	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够发现和配对附近的蓝牙设备。
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.RECEIVE_LAUNCH_BROADCASTS	未知	未知权限	来自 android 引用的未知权限。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android 8.0 以上系统允许安装未知来源应用程序权限。
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.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.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。
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.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.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.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.PACKAGE_USAGE_STATS	签名	更新组件使用统计	允许修改组件使用情况统计
com.google.android.gms.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
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.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。

本报告由南明离火移动安全分析平台生成

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.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粗略的经纬度信息，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.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
android.permission.QUICKBOOT_POWERON	普通	接收设备重启或快速启动的广播的权限	一个用于接收设备重启或快速启动的广播的权限。它允许应用程序在设备重新启动后执行一些操作，例如启动一个服务，更新一些数据，或者显示一些通知。
android.permission.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.example.mmm.replace_1	Schemes: sms://, mms://, mmsto://, smsto://,

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: **1** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名
应用程序使用了调试证书进行签名	高危	应用程序使用了调试证书进行签名。生产环境的应用程序不能使用调试证书发布。

Manifest 配置安全分析

高危: **0** | 警告: **11** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	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。
2	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。

3	Activity-Alias (com.example.mmm.two) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
4	Activity-Alias (com.example.mmm.one) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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	Broadcast Receiver (com.example.mmm.Admin.ReceiverDeviceAdmin) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_DEVICE_ADMIN [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。
6	Broadcast Receiver (com.example.mmm.replace_2) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_WAP_PUSH [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。
7	Service (com.example.mmm.replace_3) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.SEND_RESPOND_VIA_MESSAGE [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。
8	Broadcast Receiver (com.example.mmm.Receiver.bootReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_SMS [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。
9	Service (com.example.mmm.Service.srvSccessibility) 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。
10	高优先级的Intent（12） -{1} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。
11	高优先级的Intent（979） -{1} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

代码安全漏洞检测

高危: **1** | 警告: **5** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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
3	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	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	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	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
7	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

本报告由南明离火移动安全分析平台生成

应用行为分析

编号	行为	标签	文件

00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00079	隐藏当前应用程序的图标	规避	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	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	17/30	android.permission.READ_CONTACTS android.permission.GET_TASKS android.permission.READ_PHONE_STATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.ACCESS_FINE_LOCATION android.permission.CAMERA android.permission.RECEIVE_SMS android.permission.SEND_SMS android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_SMS android.permission.WAKE_LOCK android.permission.SYSTEM_ALERT_WINDOW android.permission.CALL_PHONE android.permission.PACKAGE_USAGE_STATS android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.ACCESS_COARSE_LOCATION
其它常用权限	12/46	android.permission.FOREGROUND_SERVICE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.CHANGE_WIFI_STATE android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE com.google.android.gms.permission.ACTIVITY_RECOGNITION android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.ACCESS_BACKGROUND_LOCATION

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
s3-us-west-2.amazonaws.com	安全	否	**IP地址:** 52.92.241.208 **国家:** 美国 **地区:** 俄勒冈 **城市:** 波特兰 **纬度:** 45.523460 **经度:** -122.676468 **查看:** Google 地图
mtg-native.rayjump.com	安全	否	**IP地址:** 18.154.206.94 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图

oneclient.sfx.ms	安全	否	**IP地址:** 23.35.26.233 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 埃尔塞贡多 **纬度:** 33.919201 **经度:** -118.416580 **查看:** Google 地图
cdn-adn-https.rayjump.com	安全	否	**IP地址:** 18.164.154.128 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
whatwg.org	安全	否	**IP地址:** 185.22[illegible]248.76 **国家:** 美国 **地区:** 新泽西州 **城市:** 竞利夫顿 **纬度:** 40.858585 **经度:** -74.163605 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件

• https://recs.richrelevance.com/rrserver/ • https://bugzilla.mozilla.org/show_bug.cgi?id=1776869 • https://id.cxense.com/public/user/id • https://scomcluster.cxense.com/Repo/rep.html • https://scomcluster.cxense.com/Repo/rep.gif • http://cdn.cxpublic.com/ • https://smartblock.firefox.etp/play.svg • https://bugzilla.mozilla.org/show_bug.cgi?id=1638383 • https://cdn-templates.cxpublic.com/ • https://bugzilla.mozilla.org/show_bug.cgi?id=1746439 • https://sp.auth.adobe.com • https://kinja.com • https://bugzilla.mozilla.org/show_bug.cgi?id=1656171 • https://officecdn.microsoft.com/pr/uiraas/android/ • https://tsrid.cxense.com/lookup?callback= • https://hcaptcha.com/1/api.js • https://www.history.com/mvpd-auth • https://www.crave.ca • https://bugzilla.mozilla.org/show_bug.cgi?id=1792395 • https://smartblock.firefox.etp/facebook.svg • https://cdn.cxpublic.com/ • https://bugzilla.mozilla.org/show_bug.cgi?id=1804445 • https://api.cxense.com/profile/user/segment?callback= • https://accounts.google.com/SignOutOptions • https://ogs.google.com • https://comcluster.cxense.com/dmp/push?callback= • https://scdn.cxense.com/empty.html • https://scdn.cxense.com/sclear.html • https://api.cxense.com/public/widget/data • https://s-adserver.cxad.cxense.com/adserver/search • https://scdn.cxense.com/sp1.html • https://blogger.com • https://www.facebook.com • https://www.tsn.ca • https://login.microsoftonline.com • https://clientstorage.cxense.com • https://bugzilla.mozilla.org/show_bug.cgi?id=1803340 • https://bugzilla.mozilla.org/show_bug.cgi?id=1777650 • https://bugzilla.mozilla.org/show_bug.cgi?id=1624855 • https://p1cluster.cxense.com/p1.js • http://adserver.cxad.cxense.com/adserver/search • https://searchfox.org/mozilla-central/source/dom/media/gtest/negative_duration.mp4 • https://comcluster.cxense.com/cce/pdm?callback= • https://scdn.cxense.com/sglobal.html • https://ogs.google.com/ • http://mozilla.org/MPL/2.0/. • https://s-adserver.sandbox.cxad.cxense.com/adserver/search • https://accounts.google.com/ServiceLogin • http://cdn-templates.cxpublic.com/ • https://scomcluster.cxense.com/public/cleared • https://github.com/gorhill/uBlock/blob/f49e079db0262e669b70f4169924f796ac8db7c/src/web_accessible_resources/google-analytics_ga.js • http://adserver.sandbox.cxad.cxense.com/adserver/search	自研引擎-A
• https://oneclient.sfx.ms/mobile/ts_configuration.jwt	com/microsoft/tokenshare/j.java
• javascript:window.mraidbridge.firereadyevent	com/mbridge/msdk/mbsignalcommon/mraid/a.java
• https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js • https://mtg-native.rayjump.com/omsdk/omsdkjs_common_js.txt	com/mbridge/msdk/c/b.java
• https://s3-us-west-2.amazonaws.com/omsdk-files/compliance-js/omid-validation-verification-script-v1.js	com/mbridge/msdk/a/b.java

• javascript:window.navigator.vibrate	com/mbridge/msdk/click/f.java
• https://play.google.com	com/mbridge/msdk/mbsignalcommon/windvane/WindVaneWebView.java
• http://whatwg.org/html/webappapis.html#dom-windowbase64-atob • http://whatwg.org/c#alphanumeric-ascii-characters • http://whatwg.org/html/common-microsyntaxes.html#space-character • https://gist.github.com/atk/1020396 • http://whatwg.org/html/webappapis.html#dom-windowbase64-btoa	com/mbridge/msdk/c/b/b.java
• https://play.google.com/	com/mbridge/msdk/click/a.java

第三方追踪器检测

名称	类别	网址
Mintegral	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/200

敏感凭证泄露检测

可能的密钥
a5be7b1c-2d9e-f330-e824-8fc73a4eb4a4
f3b77c67-df61-ae1a-9986-41cb05b47170
1271869c-f7f7-4420-869f-5f2ac9fdc16b
061c05b1-c64d-f8f7-07ed-4c4656851526
cd00d55b-e342-4bde-b494-5dc5abb14e01
4fd5f506-2c99-bec7-2e0e-438b581e42e8
9c7058d3-c20e-d214-1498-2d7d8ed[illegible]e60
ddda02ba-d8c7-609c-f23e-562e[illegible]a1615

免责声明及风险提示: