南明离火

移动应用检测平台

ANDROID 静态分析报告

汤不热视频 • v1.1.9

分析日期: 2025-10-14 22:26:00

ℹ应用概览

文件名称:	汤不热视频.APK
文件大小:	22.35MB
应用名称:	汤不热视频
软件包名:	com.video.wx.t1
主活动:	com.video.tx.activity.LauncherActivity
版本号:	11.9
最小SDK:	21
目标SDK:	28
加固信息:	自定义加固
开发框架:	Java/Kotlin
应用程序安全分数:	45/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：可能有安全隐患
MD5:	4bd8d9c8e435d7e3fc3d3a5cc01e9cc7
SHA1:	b4eee6e4b3bbbf38d8e8ae83c071b0cc91f2f6bd
SHA256:	f5c3465a50d2d11b7f2475ae093dcc2dbde65df02b03c30a8b53ad9a05ccc23e

分析结果严重性分布

高危	中危	ℹ 信息	✓ 安全	关注
5	15	3	2	0

四大组件导出状态统计

Activity组件：119个，其中export的有： 1个
Service组件：8个，其中export的有： 2个
Receiver组件：7个，其中export的有： 0个
Provider组件：5个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=1, ST=1, L=1, O=1, OU=1, CN=1
签名算法: rsassa_pkcs1v15
有效期自: 2021-07-27 06:42:30+00:00
有效期至: 2046-07-21 06:42:30+00:00
发行人: C=1, ST=1, L=1, O=1, OU=1, CN=1
序列号: 0x2d1eaa05
哈希算法: sha256
证书MD5: 68812afc1821d2514767c1f8c4e113cf
证书SHA1: 427eaf53dfd476c400525cb3f3ba9a4ee599cf60
证书SHA256: efa5f895461c32d1e50d822dc68eaf8e93f624f3264f470d20d3f6b14c1f52c7
证书SHA512:
b9a6f696a70058f74c07c42ac2bec4e40e56c3d9295062908aa66cae3c0f6ceaa5d43d2f9e0410da1c276811569a674bd[illegible]9d7626085685103af60b09ccb32e16

公钥算法: rsa
密钥长度: 2048
指纹: abdd478d19d4bfc0877bf03f71f64ba3b1dc26bcc1a3e73e6d9db9b6123c73e2
共检测到 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.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.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。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
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.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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.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.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.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。

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: **4** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用已配置网络安全策略 [android:networkSecurityConfig=@7F130003]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	Activity-Alias (com.video.tx.activity_alias) 未受保护。 存在 intent-filter。	警告	检测到 Activity-Alias 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity-Alias 被显式导出，存在安全风险。
4	Service (com.video.tx.service.PlayMusicService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
5	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: **5** | 警告: **9** | 信息: **3** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置

1	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
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	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
4	MD5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
5	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
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	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
8	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
9	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	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-2	升级会员：解锁高级权限

10	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
11	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
12	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
13	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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
14	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
15	该文件是World Writable。任何应用程序都可以写入文件	高危	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
16	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
17	使用弱加密算法	高危	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
18	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限

19	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

应用行为分析

编号	行为	标签	文件
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
00112	获取日历事件的日期	信息收集 日历	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
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
00130	获取当前WIFI信息	WiFi 信息收集	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
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
00013	读取文件并将其放入流中	文件	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
00094	连接到 URL 并从中读取数据	命令 网络	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
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	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
00183	获取当前相机参数并更改设置	相机	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
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
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限

00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	升级会员：解锁高级权限
00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00056	修改语音音量	控制	升级会员：解锁高级权限
00029	动态初始化类对象	反射	升级会员：解锁高级权限
00157	使用反射实例化新对象，可能用于 dexClassLoader	反射 dexClassLoader	升级会员：解锁高级权限
00026	方法反射	反射	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00002	打开相机并拍照	相机	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	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	7/30	android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.VIBRATE
其它常用权限	7/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.FLASHLIGHT android.permission.READ_EXTERNAL_STORAGE

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
ncp.maimaitom.com	安全	否	**IP地址:** 23.224.249.171 **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
www.color.org	安全	否	**IP地址:** 104.26.5.16 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
ns.useplus.org	安全	否	**IP地址:** 54.83.4.77 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
p7.itc.cn	安全	是	**IP地址:** 221.230.244.113 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图
mmt.maimaitom.com	安全	否	**IP地址:** 23.224.249.171 **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
p4.itc.cn	安全	是	**IP地址:** 221.230.244.108 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图
iptc.org	安全	否	**IP地址:** 172.67.183.61 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 **查看:** Google 地图

link.maimaitom.com	安全	否	**IP地址:** 45.13.92.138 **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
api1.111api.com	安全	否	No Geolocation information available.
google.com	安全	否	**IP地址:** 142.250.179.174 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
vip.123pan.cn	安全	是	**IP地址:** 59.47.225.55 **国家:** 中国 **地区:** 辽宁省 **城市:** 沈阳 **纬度:** 41.805699 **经度:** 123.431472 **查看:** 高德地图
cipa.jp	安全	否	**IP地址:** 118.32.81.189 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
www.npes.org	安全	否	**IP地址:** 172.67.183.61 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
vpic-cover.puui.qpic.cn	安全	是	**IP地址:** 114.237.67.68 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图
www.xfa.org	安全	否	No Geolocation information available.
uri.etsi.org	安全	否	**IP地址:** 195.238.226.27 **国家:** 法国 **地区:** 普罗旺斯-阿尔卑斯-蔚蓝海岸 **城市:** 索菲亚·安蒂波利斯 **纬度:** 43.622223 **经度:** 7.050000 **查看:** Google 地图

www.aiim.org	安全	否	**IP地址:** 199.60.103.225 **国家:** 美国 **地区:** 马萨诸塞州 **城市:** 剑桥 **纬度:** 42.375111 **经度:** -71.105743 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
https://img1.dongqiudi.com/fastdfs6/M00/0A/8C/rBUESWCJB4iAZETJAAA1gvjGzrY630.png https://img1.dongqiudi.com/fastdfs3/M00/B5/74/ChOxM1xC2DyASaamAAAEq1PV5Sc240.png https://img1.dongqiudi.com/fastdfs6/M00/0A/D9/rBUCgGCKDu6AEhOIAAAiU2PY4Ak211.png http://www.baidu.com20210612126094142.html https://img1.dongqiudi.com/fastdfs3/M00/B5/7A/ChOxM1xC2MSAQaWAAAAL1VFSq5U098.png http://www.baidu.com20210612111395435.html https://img1.dongqiudi.com/fastdfs3/M00/B5/7C/ChOxM1xC2PyAX4i0AAAJXV6GRFw977.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7F/ChOxM1xC2T2AQEEOAAADhe1936s504.png https://img1.dongqiudi.com/fastdfs3/M00/B5/80/ChOxM1xC2VGAZ2dFAAAAvGpFhCs628.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7D/ChOxM1xC2RGARlXJAAADZRt3Z5E811.png https://img1.dongqiudi.com/fastdfs3/M00/B5/78/ChOxM1xC2JeAO7rgAAAGzyj6na8302.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7A/ChOxM1xC2NaAWgOvAAAGlRJHN_4198.png https://img1.dongqiudi.com/fastdfs3/M00/B5/76/ChOxM1xC2HaAbuY8AAABFkE-5tU690.png http://www.baidu.com20210612121117208.html http://www.baidu.com20210612115542406.html https://img1.dongqiudi.com/fastdfs3/M00/B5/72/ChOxM1xC2A-AI_uOAAAHB-5pMAU501.png https://img1.dongqiudi.com/fastdfs3/M00/B9/F9/ChOxM1xIEDOAbu7VAAAWn39BUY0523.png https://img1.dongqiudi.com/fastdfs3/M00/B5/73/ChOxM1xC2CWASHOYAAAAyoY-ylg117.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7A/ChOxM1xC2MaAKUtjAAAIlv2Zm1Y471.png https://img1.dongqiudi.com/fastdfs3/M00/B5/72/ChOxM1xC2BWAbY9WAAACSOFuQyc213.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7E/ChOxM1xC2TCAWMemAAAJsy8Pgbg246.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7D/ChOxM1xC2RmAK60TAAAIMnb4c1Y203.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7A/ChOxM1xC2MWAG6p0AAAImngwC6g016.png https://img1.dongqiudi.com/fastdfs3/M00/B5/73/ChOxM1xC2DiAczBuAAADSRncl0Y205.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7A/ChOxM1xC2MSAAk5xAAAGSzGQEW4468.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7A/ChOxM1xC2MqAROxuAAAIpUh3B3s509.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7F/ChOxM1xC2UeADe-pAAABM6khVfc558.png https://img1.dongqiudi.com/fastdfs3/M00/B5/77/ChOxM1xC2IKANG6tAAABFW9OqCQ523.png https://img1.dongqiudi.com/fastdfs3/M00/B5/73/ChOxM1xC2DOAJT7PAAAKPkvn3ik047.png https://img1.dongqiudi.com/fastdfs3/M00/B5/74/ChOxM1xC2EuAYSDaAAACk9Rvueg747.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7A/ChOxM1xC2NSAFMKRAAAGgGY97bU036.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7B/ChOxM1xC2OyAMboLAAAE67UTWH4126.png https://img1.dongqiudi.com/fastdfs3/M00/B5/72/ChOxM1xC2BSAd33sAAAAwSmUl1c875.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7D/ChOxM1xC2QmAWthoAAAKQAUuoQY168.png https://img1.dongqiudi.com/fastdfs3/M00/B5/78/ChOxM1xC2KKAUYxJAAAETkn3xgs261.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7F/ChOxM1xC2UeAQ_ZRAAAAsB-WszA660.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7B/ChOxM1xC2OeABcv-AAAShQE7bQc288.png https://img1.dongqiudi.com/fastdfs3/M00/B5/74/ChOxM1xC2DyAdvQWAAAVO7FIRv8232.png https://img1.dongqiudi.com/fastdfs3/M00/B5/77/ChOxM1xC2JGAd79VAAAAyGVvoVQ975.png http://www.baidu.com20210612117398692.html https://img1.dongqiudi.com/fastdfs3/M00/B5/7F/ChOxM1xC2T2AEHoVAAAA5MoIiDo797.png https://img1.dongqiudi.com/fastdfs3/M00/B5/78/ChOxM1xC2JqALrn0AAAAwxNi5qI444.png https://img1.dongqiudi.com/fastdfs3/M00/B5/76/ChOxM1xC2G2Acp31AAABNMvdP0U855.png https://img1.dongqiudi.com/fastdfs3/M00/B5/75/ChOxM1xC2FSADy_DAAALaURezqo279.png https://img1.dongqiudi.com/fastdfs3/M00/B5/80/ChOxM1xC2U-AeyGIAAAEcEYRRbw864.png http://www.baidu.com20210612120131997.html https://img1.dongqiudi.com/fastdfs3/M00/B5/79/ChOxM1xC2MCAdQv0AAAPDjbzE80360.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7B/ChOxM1xC2OeAQNGHAAAC7NfdKHY533.png https://img1.dongqiudi.com/fastdfs3/M00/B5/74/ChOxM1xC2EOAbUHIAAAOg6JpgzM729.png https://img1.dongqiudi.com/fastdfs3/M00/B5/7B/ChOxM1xC2OqAfwdHAAAH6SdwgRY392.png	自研引擎-A

• https://img1.dongqiudi.com/fastdfs3/M00/B5/7F/ChOxM1xC2TeAejqdAAABczmP1jg125.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/7A/ChOxM1xC2MqAPFfHAAAUDL2kByg454.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/80/ChOxM1xC2UyAFIQpAAAJFbiniWQ532.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/80/ChOxM1xC2VGAYhOTAAAbZ1CFkQg735.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/7B/ChOxM1xC2N6AEWYMAAABPByVIVM465.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/75/ChOxM1xC2FGAU4XgAAABUo4hnUQ558.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/78/ChOxM1xC2J2APzLYAAAFNtkA6fs883.png • http://www.baidu.com20210611211415 6736.html • https://img1.dongqiudi.com/fastdfs3/M00/B5/7A/ChOxM1xC2MuAclOjAAADLLXexC4159.png • http://www.baidu.com202106112107554447.html • https://img1.dongqiudi.com/fastdfs3/M00/B5/79/ChOxM1xC2LeASiR_AAABM1z3kEY093.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/73/ChOxM1xC2DCAM4slAAAMODYb5Wo093.png • http://www.baidu.com202106112127198983.html • https://img1.dongqiudi.com/fastdfs3/M00/B5/74/ChOxM1xC2EGAaUoxAAABWBGyGJo937.png • http://www.baidu.com202106112103113641.html • https://img1.dongqiudi.com/fastdfs3/M00/B5/79/ChOxM1xC2L6AHvC4AAAEdawnP9Q689.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/7C/ChOxM1xC2PGALY-zAAAAqYWqc08697.png • https://img1.dongqiudi.com/fastdfs3/M00/BF/B7/ChOxM1xRP8qAEPF2AAAXzzSv8Hw670.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/79/ChOxM1xC2L6AGgTIAAANmHUMfBQ160.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/7C/ChOxM1xC2PuALvwRAAAK3F_koeE108.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/72/ChOxM1xC2BaALNi5AAAD52lYRiY037.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/7D/ChOxM1xC2QeAOXCOAAABR2T9Umw550.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/6D/ChOxM1xC0DiAaO-VAAAC0MLMB0M179.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/72/ChOxM1xC2BGALh9vAAAQzrycW40209.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/78/ChOxM1xC2KGAIsqKAAAVUXXXPL0755.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/7F/ChOxM1xC2USABwJuAAAP6Wb9bq[illegible]97[illegible].png • https://img1.dongqiudi.com/fastdfs3/M00/B5/7F/ChOxM1xC2TyANIAKAAABeUfO5gM520.png • http://www.baidu.com202106112124047753.html • https://img1.dongqiudi.com/fastdfs3/M00/B5/7F/ChOxM1xC2UOAAUUEAAAE_rl2nXk849.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/80/ChOxM1xC2U-ACKo5AAADlnvYmoE306.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/80/ChOxM1xC2U2ALNGOAAAHRFugRNE631.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/7E/ChOxM1xC2TCADlR9AAAvdE0h-W0179.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/78/ChOxM1xC2KAOb[illegible]9AAAA7100FM4797.png • http://www.baidu.com202106112129132683.html • https://img1.dongqiudi.com/fastdfs3/M00/B5/7D/ChOxM1xC2ReAbcneAAAEdjusY1A976.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/72/ChOxM1xC2CKAJTG3AAAAypTh1A8948.png • https://img1.dongqiudi.com/fastdfs3/M00/B5/7B/ChOxM1xC2OyABnv3AAAXNhIZ8ng953.png	
• file:anonymous-string	com/c/a/a/t.java
• https://api1.111api.com/	com/video/tx/a.java

• http://iptc.org/std/iptc4xmpcore/1.0/xmlns/ • http://ns.useplus.org/ldf/xmp/1.0/ • http://iptc.org/std/iptc4xmpext/2008-02-29/ • http://www.npes.org/pdfx/ns/id/ • http://www.aiim.org/pdfa/ns/schema# • http://cipa.jp/exif/1.0/ • http://www.aiim.org/pdfua/ns/id/ • http://www.aiim.org/pdfa/ns/type# • http://www.aiim.org/pdfa/ns/field# • http://www.aiim.org/pdfa/ns/property# • http://www.aiim.org/pdfa/ns/extension/ • http://www.aiim.org/pdfa/ns/id/	com/d/d/a.java
• 2.5.29.37 • 2.5.29.15	com/d/c/h/m/e.java
• 2.5.4.7 • 2.5.4.44 • 2.5.4.42 • 2.5.4.11 • 2.5.4.4 • 2.5.4.10 • 2.5.4.3 • 2.5.4.43 • 2.5.4.8 • 2.5.4.45 • 2.5.4.6 • 2.5.4.5 • 2.5.4.12	com/d/c/h/m/c.java
• http://uri.etsi.org/01903#signedproperties • http://uri.etsi.org/01903/v1.3.2#	com/d/c/h/m/af.java
• http://www.xfa.org/schema/xfa-data/1.0/	com/d/c/h/gi.java
• http://javax.xml.xmlconstants/feature/secure-processing	com/d/d/a/o.java
• https://p4.itc.cn/images01/20230619/67cb12812f8e400cb4bfdd615236d562.png • https://p7.itc.cn/q_70/images03/20230414/29dbf38b1ff94c57a8555ce32bbb8c48.jpeg • https://pic.rmb.bdstatic.com/bjh/video/c0feac9bd15005f78f769c41acfd5042.jpeg?for=bg • https://vpic-cover.puui.qpic.cn/n3552vshb0l/n3552vshb0l_1718133181_vt.jpg/720?max_age=7776000 • https://img2.baidu.com/it/u=4033782870,3388369610&fm=253&fmt=auto&app=138&f=jpeg?w=800&h=1412	com/app/shortPlay/c/a.java
• https://google.com	com/tonyodev/fetch2core/g.java
• http://23.224.200.102/ • www.com • http://23.224.200.66/ • http://172.247.59.43/	com/jetpack/lib/common/c/f.java

• http://23.224.200.58/ • http://172.247.59.34/ • http://23.224.200.34/ • http://23.225.232.2/	com/jetpack/lib/common/c/e.java
• 2.5.29.15	cn/a/g/a/h.java
• 192.168.255.255 • 10.255.255.255 • 172.31.255.255 • 127.0.0.1	cn/a/e/q/b.java
• http://www.color.org	com/d/c/h/fl.java
• https://link.maimaitom.com?key=nptjrj • https://link.maimaitom.com?key=smbx • https://link.maimaitom.com?key=xsyfk • https://link.maimaitom.com?key=cmapp • https://link.maimaitom.com?key=jixie • https://link.maimaitom.com?key=wdsj • https://link.maimaitom.com?key=ltxx • https://link.maimaitom.com?key=hnh • https://link.maimaitom.com?key=nzxt • https://link.maimaitom.com?key=mxw • https://link.maimaitom.com?key=wdxgbj • https://link.maimaitom.com?key=xmds • https://link.maimaitom.com?key=emnh • https://link.maimaitom.com?key=zwrj • https://link.maimaitom.com?key=12god • https://link.maimaitom.com?key=bxya • https://link.maimaitom.com?key=hg • https://link.maimaitom.com?key=bln • https://link.maimaitom.com?key=syxl • https://link.maimaitom.com?key=dldx • https://link.maimaitom.com?key=gbshdxz • https://link.maimaitom.com?key=lost_moon • https://link.maimaitom.com?key=fuyou • https://link.maimaitom.com?key=llkz • https://link.maimaitom.com?key=tg17 • https://link.maimaitom.com?key=wdxfs	com/app/gameBus/b.java
• https://p4.itc.cn/images01/20230619/67cb12812f8e400cb40fdd015236d562.png • https://p7.itc.cn/q_70/images03/20230414/29dbf38b1ff94c57a8555ce32bbb8c48.jpeg • https://pic.rmb.bdstatic.com/bjh/video/e0feac9bd15005f78f769c41acfd5042.jpeg?for=bg • https://vpic-cover.puui.qpic.cn/n3552vshb0l/n3552vshb0l_1718133181_vt.jpg/720?max_age=7776000 • https://img2.baidu.com/it/u=4033782870,3388369610&fm=253&fmt=auto&app=138&f=jpeg?w=800&h=1412	com/app/gameBus/e/a.java
• https://mint.maimaitom.com/assets/66dashun.zip • https://ncp.maimaitom.com/assets/66dashun.zip • https://vip.123pan.cn/1841533097/source/77dashun.zip	com/video/tx/ipNet/LoadDomianZipWorker.java
• 23.224.31.70 • 23.225.155.106	com/video/tx/ipNet/a.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
FreeReflection	tiann	在 Android P 及以上版本中不受任何限制地使用反射。
OpenCV	OpenCV	OpenCV 是一个跨平台的计算机视觉库，可用于开发实时的图像处理、计算机视觉以及模式识别程序。
RenderScript	Android	RenderScript 是用于在 Android 上以高性能运行计算密集型任务的框架。RenderScript 主要用于数据并行计算，不过串行工作负载也可以从中受益。RenderScript 运行时可在设备上提供的多个处理器（如多核 CPU 和 GPU）间并行调度工作。这样您就能够专注于表达算法而不是调度工作。RenderScript 对于执行图像处理、计算摄影或计算机视觉的应用来说尤其有用。
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。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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 WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

✉ 邮箱地址敏感信息提取

EMAIL	源码文件
cthxx@xxmail.com	com/video/tx/widget/e.java
cthxx@xxmail.com	com/app/gameBus/activity/game/LoadListActivity.java

第三方追踪器检测

名称	类别	网址
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
凭证信息=> "APP_ID" : "com.video.wx.t1"
d005d14d7ce6372ae54527a659be2c55
29dbf38b1ff94c57a8555ce32bbb8c48
e392a8ddf08a08dcae5514168b8dfb53

本报告仅用于学习与研究目的，禁止用于任何商业或非法用途。

664dbacccac2a664de39def2
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
123456789012345678901234
664db61ccac2a664de39d984
946eca6b182e63ebe50cf82e483715bf
542c34779b2fb2295313ded1fdd2e84d
88ce35562a6f085b53a00145444c445f
eU9ZnV46iYnLaFjXqM0peerbhB6gTrq2UvsrYkqwxFksmLxupK2qU8GOfC5VTxKS
67cb12812f8e400cb4bfdd615236d562
0123456789ABCDEFGHJKLMNPQRTUWXY
5bc1786994ce276210fa38e1fe46b1b3
e0feac9bd15005f78f769c41acfd5042
460643a974555d792b8f5a6e1a5d323c
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
jhjlpKWdCoFcQnvCIkBbRWkWpVHNvZUGFZ2kJQLNdLk1tYCKAYC6oosAfEPFJzmE
1oaCdygBKwvea3xtj3kVCELqyBfMjZ6T
746811187b2f8039a352265c7995a8d6

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隐患。