南明离火
移动应用检测平台

ANDROID 静态分析报告

Youcine V0D • v1.0

分析日期: 2024-05-24 15:18:44

应用概览

文件名称:	Youcine_VOD_SEM_LOGIN__modapksgratis.apk
文件大小:	18.16MB
应用名称:	Youcine V0D
软件包名:	com.studio.YoucineV0E
主活动:	com.shtvreb.hometv.activities.SplashScreen
版本号:	1.0
最小SDK:	21
目标SDK:	27
加固信息:	未加壳
应用程序安全分数:	45/100 (中风险)
杀软检测:	13 个杀毒软件报毒
MD5:	286e446ab0425b6c3f8eaa657bbfb966
SHA1:	2d42d2e3026aa3f62e3f179638a3b9c90ba6da9
SHA256:	a5b47d10e38206e39a874d20[illegible]b792685e10c2d81a45c1ee87ef949bfd4

分析结果严重性分布

高危	中危	信息	安全	关注
5	17	13	2	0

四大组件导出状态统计

Activity组件：13个，其中export的有：1个
Service组件：4个，其中export的有：2个
Receiver组件：4个，其中export的有：3个
Provider组件：4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: True

本报告由南明离火移动安全分析平台生成

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:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704dc9b5711292a4569

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.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_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_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
net.dinglisch.android.tasker.PERMISSION_RUN_TASKS	未知	未知权限	来自 android 引用的未知权限。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
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.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.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.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.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_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
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.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.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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。

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: **1** | 警告: **9** | 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]	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.shtvreb.hometv.utils.BootUpReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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.google.android.exoplayer2.scheduler.PlatformScheduler$PlatformSchedulerService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
6	Content Provider (com.applisto.appcloner.classes.DefaultProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
7	Service (com.applisto.appcloner.service.RemoteService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
8	Broadcast Receiver (com.applisto.appcloner.classes.DefaultProvider$DefaultReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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	Activity (com.applisto.appcloner.classes.DefaultProvider$MyActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (27) 更新到 29 或更高版本以在平台级别修复此问题。
10	Activity (com.applisto.appcloner.classes.DefaultProvider$MyActivity) 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。
11	Broadcast Receiver (com.applisto.appcloner.classes.FakeCamera$FakeCameraReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。

代码安全漏洞检测

高危: **4** | 警告: **7** | 信息: **3** | 安全: **1** | 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
4	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
5	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
6	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
7	默认情况下，调用Cipher.getInstance("AES")将返回AES ECB模式。众所周知，ECB模式很弱，因为它导致相同明文块的密文相同	高危	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-2	升级会员：解锁高级权限
8	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-4	升级会员：解锁高级权限
9	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
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
11	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限

12	该文件是World Readable。任何应用程序都可以读取文件	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
13	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
14	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
15	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

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/libavutil.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
2	arm64-v8a/libnative-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。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	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.RECEIVE_BOOT_COMPLETED android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.CAMERA android.permission.WRITE_SETTINGS

本报告由南明离火移动安全分析平台生成

其它常用权限	10/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.FLASHLIGHT android.permission.BLUETOOTH_ADMIN android.permission.WRITE_EXTERNAL_STORAGE android.permission.CHANGE_WIFI_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.BLUETOOTH

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
t.me	安全	否	**IP地址:** 149.154.167.99 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 沃灵顿 **纬度:** 52.[illegible] **经度:** -0.687590 **查看:** Google 地图
7go.xyz	安全	否	**IP地址:** 104.21.234.226 **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
whois.domaintools.com	安全	否	**IP地址:** 199.30.228.13 **国家:** 美利坚合众国 **地区:** 华盛顿 **城市:** 西雅图 **纬度:** 47.615700 **经度:** -122.344498 **查看:** Google 地图
aomedia.org	安全	否	**IP地址:** 185.199.109.153 **国家:** 美利坚合众国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图
dashif.org	安全	否	**IP地址:** 185.199.109.153 **国家:** 美利坚合众国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图

exoplayer.dev	安全	否	**IP地址:** 185.199.110.153 **国家:** 美利坚合众国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• 127.0.0.1	com/applisto/appcloner/classes/DefaultProvider.java
• https://t.me/imperioo_iptv	hotXlOoOo.java
• ftp://appcloner:appcloner@	com/applisto/appcloner/classes/DataDirectoryFtpServer.java
• https://aomedia.org/emsg/id3 • https://developer.apple.com/streaming/emsg-id3	t2/a.java
• https://exoplayer.dev/issues/player-accessed-on-wrong-thread	b2/a1.java
• 127.0.0.1 • http://whois.domaintools.com/	com/applisto/appcloner/classes/HostsBlocker.java
• http://dashif.org/guidelines/last-segment-number • data:cs:audiopurposecs:2007 • http://dashif.org/guidelines/trickmode	e3/c.java
• http://7go.xyz:8080/	com/shtvreb/hometv/remote/RetroConfection.java
• http://7go.xyz:8080/	z5/e.java
• http://7go.xyz:8080/ • https://aomedia.org/emsg/id3 • https://t.me/imperioo_iptv • https://developer.apple.com/streaming/emsg-id3 • 127.0.0.1 • http://whois.domaintools.com/ • http://dashif.org/guidelines/last-segment-number • https://exoplayer.dev/issues/player-accessed-on-wrong-thread • data:cs:audiopurposecs:2007 • ftp://appcloner:appcloner@ • http://dashif.org/guidelines/trickmode	自研引擎-S
• http://shadeed--rebrand/	lib/arm64-v8a/libnative-lib.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
FFmpeg	FFmpeg	FFmpeg 是领先的多媒体框架，能够解码，编码，转码，MUX，DEMUX，流式，过滤和播放人类和机器创建的几乎所有内容。

C++ 共享库	Android	在 Android 应用中运行原生代码。
LibVLC	VideoLAN	VLC 是一款免费、自由、开源的跨平台多媒体播放器及框架，可播放大多数多媒体文件，以及各类流媒体协议。
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。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案
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。

敏感凭证泄露检测

可能的密钥
"username" : "UserName"
"password" : "Senha"
"password" : "Password"
9a04f079-9840-4286-ab92-e65be0885f95
nZWtL6D4gxleEjTgRsiZreZ8nNC9qRwx6BC0WIWuyNpCzY/YjalfJgLEw4LPgFs0T+snumNuJ4OD
DhMMFWW6FA22jYzIDlJ0wz0ImjPyBHon78I2i05aWapGoo9cFqJ3R40a8DvJK70+C7R7UZna/qgqRPdH0WkCCMVxbOj9VnyXKVYmBB08A5c=
nlwr5ETjezBRsKULS6ZJWAU8xvoIPcBxwGQRa[illegible]5kiNvjcX7oSARkPgQQQNKjvHJgQugBGYiVLwY
n6ILXhSq+P2Ae7qsIh4HV0REDDQ314F[illegible]QmvQhaYmuwAAAABJRU5ErkJggg==
nsw0NDQ0NDQ0FUesnYpIOBE4BTsKi2ewLTEyYDCfK0MfeUYzYO8RCjmQsca3o2lrYFJm2AXuAL81s
nd7qkHRn2vssMU5VdE3xYVka8ojlTBsDMNuBGM2mi[illegible]a9lhqhj7ifnqmsbvLfG5CH0PGDUkNXMvqV4
nAP7xsB0qOvNGAL+5kirQvBGghKD60AgQmEYAQNDDYoSiM98ndOlrwNdAPL4fjn7G/UKyedoX+C60
n4EPbNtXMNgN[illegible]O0djfLc54Q9QnnUoOaUYA2h3VtjxGkQhzM+wXdSDCxzgR/iipbLklXQNuy2sY
nYfAXeebVn[illegible]CJC3JuHeGh1/vFx2nMyvF[illegible]m8iTvax9jMPgHOBv5OMXlE0tICyhR86SYXchted46h
tXLJ9BeQwwen2aVdH+n0sriS[illegible]WFZ1E3aAoWrvdw=
nzHYAd4WORoWsA24[illegible]xkNgv8jJi6SHgPuC+lQifwMvAu8ZGavhnYmptVM+CLc4RUzgEm42eiehP2E
edef8ba9-79d6-4ace-[illegible]3e8-27dcd51d21ed
n5cgy1k[illegible]3a5cAFuJXKKaF9KpBPgDvM7KP4g1oIIGkCMADcBJwb2p8KOMvMPoUaCCBpALgfmBba
nJ2k5MBi65DXhQ6iwE5b0BHBP6FLXhB3AUWa2u5ImSNKdNMFPcp2Z7YYKaoCkmcDa0CWuCVuBu8zs
Y29tLmFwcGxpc3RvLmFwcGNsb25lci5jbGFzc2VzLnNlY29uZGFyeQ==

n78C8qoIPewXwOcK9V1kHzIi2qIRGLEB3LDSVx3KgP3rEWSIxHzAZt8OgIjPjEvkcWGJmr4dyoA/A
nnEP6ewBXAAflTa7oYJUhwJEetmtGlXCvCL+m3LNYblk7NznmCXnpivcDfARoGWQz+wH3PlZaTRjs
nJBUhcameExFCkEhow4NEJCIST32oW4TEg3ogbg+NklAaSl1KFG2lNGlJimqU0/P3sGZ0nLNn9qx9
nbz2PpFXK5obQPvYskh5WPqaG9rXnkDRR0q6cAjxZdP59oQNQA84ADshpO6vozBsB4DAP2/2KzrwR
nbmhoaGhoaMig8M5S0hTgENxxYMk8kg9v+nAPg34ys79CB6GnkDt8Q5KGon97Er8nPxu1LWU8UsbB
n2olwU2SXZdN1AtzmEfwtI+49oSQRspqj1yT9EUqAMoahx3rYvpW8MLONwFzglxT7WyQ97eOMmX0M
njY7OJr0mLOpwiHpt4BgUi6Q3PCZi8h1SSjpR0vaM9LxEkHSMh69dMRHz7agGfUSIhqhzKG50dHiJ
n+ZGkpzrId6ak3RlpLm1xz5kePn0QOrZ5A3H9GIMf80wHeZ+l7OZo6Qh7HwFWh45t3iCsKEiATkXo
n+AxcP7sT90e4wsx2lRLoVkh6KOeOs1Z8IekeSce3yWOWpL9T0tgIaWGb+w/x8OmdyoJXQPCPkDTc
nEWYD347Bz/VmtmYM96cSWoCWRCLMJVsE38naNXQ+k30gdExyI+kVj3Z1fpu0Jssdnp1GWxEkHSTp
noCasBeYxdhEKpQwBfJ50pb7yY2abgNmki7C4F0QoQ4DC2sIIhFm4VchWLJb0nGeaa3F9QicidEUf
dc932331180af43c77a07b805a1fb2bd
nxtAB6Dkkzc+55W9DaF97Fkkv5BBgPHxbUjgkvZgS+F2SbgztX10o9cGJpAXA1cB03BOr94D[illegible]
nCXBIWXMAAC4jAAAuIwF4pT92AAAHk0lEQVR42u2dW6wdUxjHf98pirqUREIc6t[illegible]qLiEl

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。