Evaluation Warning: The document was created with Spire.Doc for Python.

**汤头条（ 9.3.1版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 汤头条 |
| 版本 | 9.3.1 |
| 包名 | com.xkagb.alpxnl |
| 域名线索 | 31条 |
| URL线索 | 40条 |
| APP图标 |  |
| 分析日期 | 2025年6月15日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | ttt\_9.3.1\_250610\_6.apk |
| 文件大小 | 36.97MB |
| MD5值 | 6422c7e269adde108788bb83d7c344ee |
| SHA1值 | 9492aece37fd3732da7d60fb586b6e622ac633ee |
| SHA256值 | cc1799a06c8f7f85e415fb58b35abb100c70f0f7fc2f4e5882a1d84ed8902f66 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 汤头条 |
| 包名 | com.xkagb.alpxnl |
| 主活动Activity |  |
| 安卓版本名称 | 9.3.1 |
| 安卓版本 | 931 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| mov.bn.netease.com | IP: 125.38.11.59 所属国家: China 地区: Tianjin 城市: Tianjin  |
| api2.vzabrvru.xyz | IP: 154.207.77.38 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| jiajunhui.cn | IP: 192.30.252.154 所属国家: United States of America 地区: California 城市: San Francisco  |
| yuyin.baidu.com | IP: 153.3.237.166 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.baidu.com | IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding  |
| www.slf4j.org | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| dpi4.dr4gv5cd.com | IP: 104.21.88.9 所属国家: United States of America 地区: California 城市: San Francisco  |
| p.mlss8.com | 没有服务器地理信息.  |
| new.ycomesc.live | IP: 104.21.54.163 所属国家: United States of America 地区: California 城市: San Francisco  |
| imgpublic.ycomesc.com | 没有服务器地理信息.  |
| upl.baidu.com | IP: 110.242.68.242 所属国家: China 地区: Hebei 城市: Baoding  |
| examine.xmyy8.co | IP: 172.67.192.139 所属国家: United States of America 地区: California 城市: San Francisco  |
| rank.hyys.info | IP: 172.67.223.212 所属国家: United States of America 地区: California 城市: San Francisco  |
| othstr.beacon.qq.com | IP: 112.65.194.211 所属国家: China 地区: Shanghai 城市: Shanghai  |
| vop.baidu.com | IP: 111.206.209.68 所属国家: China 地区: Beijing 城市: Beijing  |
| xx.125.com | 没有服务器地理信息.  |
| otheve.beacon.qq.com | IP: 113.56.189.125 所属国家: China 地区: Hubei 城市: Huangshi  |
| h.trace.qq.com | IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi  |
| jsoup.org | IP: 104.21.16.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| xmlpull.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| api1.vzabrvru.xyz | IP: 156.255.123.38 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.smpte-ra.org | IP: 52.20.185.129 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| raw.githubusercontent.com | IP: 185.199.109.133 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| api.t.sina.com.cn | IP: 123.125.107.13 所属国家: China 地区: Beijing 城市: Beijing  |
| open-image.nosdn.127.net | IP: 125.39.155.22 所属国家: China 地区: Tianjin 城市: Tianjin  |
| vse.baidu.com | IP: 110.242.68.241 所属国家: China 地区: Hebei 城市: Baoding  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| oss.ycomesc.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://h.trace.qq.com/kv  | c/c/a/b/b/b.java  |
| http://xmlpull.org/v1/doc/features.html  | c/c/b/b/a/c.java  |
| http://xml.apache.org/xslt  | c/b/a/k.java  |
| http://yuyin.baidu.com/voice?osname=voiceopen&action=usereventflow&  | com/baidu/speech/g/o/a.java  |
| http://vop.baidu.com/v2  | com/baidu/speech/core/a.java  |
| https://vse.baidu.com/v2  | com/baidu/speech/e/k.java  |
| https://vse.baidu.com/echo.fcgi  | com/baidu/speech/e/k.java  |
| https://upl.baidu.com//words/add  | com/baidu/speech/e/j.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/videocache/k.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/videocache/k.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/videocache/k.java  |
| http://%s:%d/%s  | com/danikula/videocache/m.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/videocache/m.java  |
| http://%s:%d/%s  | com/danikula/videocache/i.java  |
| http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt  | com/googlecode/mp4parser/authoring/tracks/SMPTETTTrackImpl.java  |
| http://127.0.0.1:%d%s  | com/m3u8/download/i/b.java  |
| https://otheve.beacon.qq.com/analytics/upload  | com/tencent/beacon/base/net/c/b.java  |
| https://othstr.beacon.qq.com/analytics/upload  | com/tencent/beacon/base/net/c/b.java  |
| http://xmlpull.org/v1/doc/features.html  | com/tencent/cos/xml/transfer/s.java  |
| http://xmlpull.org/v1/doc/features.html  | com/tencent/cos/xml/transfer/q.java  |
| http://api.t.sina.com.cn/short\_url/shorten.json?source=3271760578&url\_long=  | com/tencent/mm/base/q.java  |
| http://imgpublic.ycomesc.com/img.xiao/04c9fb02a8c30ae84aa2f943e873af2d.jpg  | com/tencent/mm/bean/HomeBean.java  |
| https://api1.vzabrvru.xyz/api.php  | com/tencent/mm/network/a.java  |
| https://api2.vzabrvru.xyz/api.php  | com/tencent/mm/network/a.java  |
| https://raw.githubusercontent.com/little-5/backup/master/50dh.txt  | com/tencent/mm/network/a.java  |
| https://dpi4.dr4gv5cd.com/pwa.php  | com/tencent/mm/network/f.java  |
| http://rank.hyys.info/api.php  | com/tencent/mm/network/f.java  |
| https://p.mlss8.com/useruploadfiles/e392fd6aa2abf5633a4f06bc82b85535/e392fd6aa2abf5633a4f06bc82b85535\_001.ts  | com/tencent/mm/uitls/m2.java  |
| https://mov.bn.netease.com/open-movie/nos/mp4/2017/12/04/SD3SUEFFQ\_hd.mp4  | com/tencent/mm/uitls/b0.java  |
| https://mov.bn.netease.com/open-movie/nos/mp4/2017/05/31/SCKR8V6E9\_hd.mp4  | com/tencent/mm/uitls/b0.java  |
| http://jiajunhui.cn/video/kaipao.mp4  | com/tencent/mm/uitls/b0.java  |
| http://jiajunhui.cn/video/kongchengji.mp4  | com/tencent/mm/uitls/b0.java  |
| http://jiajunhui.cn/video/allsharestar.mp4  | com/tencent/mm/uitls/b0.java  |
| http://jiajunhui.cn/video/edwin\_rolling\_in\_the\_deep.flv  | com/tencent/mm/uitls/b0.java  |
| http://jiajunhui.cn/video/crystalliz.flv  | com/tencent/mm/uitls/b0.java  |
| http://jiajunhui.cn/video/big\_buck\_bunny.mp4  | com/tencent/mm/uitls/b0.java  |
| http://jiajunhui.cn/video/trailer.mp4  | com/tencent/mm/uitls/b0.java  |
| http://open-image.nosdn.127.net/image/snapshot\_movie/2016/11/b/a/c36e048e284c459686133e66a79e2eba.jpg  | com/tencent/mm/uitls/b0.java  |
| https://mov.bn.netease.com/open-movie/nos/mp4/2016/06/22/SBP8G92E3\_hd.mp4  | com/tencent/mm/uitls/b0.java  |
| http://open-image.nosdn.127.net/image/snapshot\_movie/2016/11/0/4/e4c8836bfe154d76a808da38d0733304.jpg  | com/tencent/mm/uitls/b0.java  |
| https://mov.bn.netease.com/open-movie/nos/mp4/2015/08/27/SB13F5AGJ\_sd.mp4  | com/tencent/mm/uitls/b0.java  |
| http://open-image.nosdn.127.net/57baaaeaad4e4fda8bdaceafdb9d45c2.jpg  | com/tencent/mm/uitls/b0.java  |
| https://mov.bn.netease.com/open-movie/nos/mp4/2018/01/12/SD70VQJ74\_sd.mp4  | com/tencent/mm/uitls/b0.java  |
| http://open-image.nosdn.127.net/image/snapshot\_movie/2016/11/e/9/ac655948c705413b8a63a7aaefd4cde9.jpg  | com/tencent/mm/uitls/b0.java  |
| http://open-image.nosdn.127.net/image/snapshot\_movie/2016/11/e/4/75bc6c5227314e63bbfd5d9f0c5c28e4.jpg  | com/tencent/mm/uitls/b0.java  |
| https://mov.bn.netease.com/open-movie/nos/mp4/2016/01/11/SBC46Q9DV\_hd.mp4  | com/tencent/mm/uitls/b0.java  |
| http://open-image.nosdn.127.net/image/snapshot\_movie/2018/3/b/c/9d451a2da3cf42b0a049ba3e249222bc.jpg  | com/tencent/mm/uitls/b0.java  |
| https://mov.bn.netease.com/open-movie/nos/mp4/2018/04/19/SDEQS1GO6\_hd.mp4  | com/tencent/mm/uitls/b0.java  |
| http://open-image.nosdn.127.net/image/snapshot\_movie/2018/1/c/8/1aec3637270f465faae52713a7c191c8.jpg  | com/tencent/mm/uitls/b0.java  |
| https://mov.bn.netease.com/open-movie/nos/mp4/2018/01/25/SD82Q0AQE\_hd.mp4  | com/tencent/mm/uitls/b0.java  |
| http://open-image.nosdn.127.net/image/snapshot\_movie/2017/12/2/8/f30dd5f2f09c405c98e7eb6c06c89928.jpg  | com/tencent/mm/uitls/b0.java  |
| http://www.baidu.com,  | com/tencent/mm/view/HttpTextView.java  |
| https://xx.125.com  | com/tencent/mm/view/HttpTextView.java  |
| http://examine.xmyy8.co/uploadMp4.php  | com/tencent/mm/p/b.java  |
| http://oss.ycomesc.com/  | com/tencent/mm/p/h.java  |
| https://new.ycomesc.live/uploadMp4.php  | com/tencent/mm/p/h.java  |
| http://api.t.sina.com.cn/short\_url/shorten.json?source=3271760578&url\_long=  | com/tencent/mm/p/j.java  |
| http://127  | com/tencent/mm/app/VideoApplication.java  |
| http://xmlpull.org/v1/doc/features.html  | com/youngfeng/snake/config/b.java  |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection  | f/b/a.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/rxjava3/exceptions/UndeliverableException.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/h.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/p0.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/x.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/q.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/g0.java  |
| http://127.0.0.1:%d%s  | jaygoo/library/m3u8downloader/o/b.java  |
| http://'  | org/jsoup/helper/d.java  |
| https://'.  | org/jsoup/helper/d.java  |
| https://jsoup.org/cookbook/extracting-data/working-with-urls  | org/jsoup/helper/d.java  |
| http://undefined/  | org/jsoup/helper/d.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/e.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/d.java  |
| https://github.com/vinc3m1  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView.git  | 摸瓜V1引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | com/danikula/videocache/k.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15778476000  | org/joda/time/chrono/GregorianChronology.java  |
| 15778800000  | org/joda/time/chrono/d.java  |
| 15778800000  | org/joda/time/chrono/JulianChronology.java  |
| 15308640144  | org/joda/time/chrono/IslamicChronology.java  |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=. 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-10 23:09:03+00:00 有效期至: 2026-06-10 23:09:03+00:00 发行人: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=. 序列号: 0x4ab5059 哈希算法: sha256 md5值: fb88fba8275cdafe49e8fb9f7d521a1e sha1值: 870185ce4d1ed70c0c2871c13a13b9975f742879 sha256值: 208697f91625d785ce595a135aed8cc50732316dcac50fa9ddd000812abfbac3 sha512值: c8ce2b5f86b546f04b4fc5422f420d1f4b9d86df862f97955b1136ee9ece1b3157eb7e36da1bc0086f17ea24e87d6e4e0bd3403955e2ade065ad3696a15cad7c 公钥算法: rsa 密钥长度: 2048 指纹: 459b745c981606c5585d12dcc93f48514657036533cf145a1c00bb3bbdf5bd6d**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_roundedimageview\_author" : "Vince Mi"  |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1"  |
| "login\_auth\_ing" : "正在授權登錄"  |
| "str\_up\_auth" : "博主"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 此APP的危险动作**

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**