



魔梯加速器 1.0.6.01.APK 分析报告



APP名称:

魔梯加速器

包名:	com.pluto.moti
域名线索:	23条
URL线索:	18条
邮箱线索:	3条
分析日期:	2025年9月29日
分析平台:	摸瓜APK反编译平台

文件名: 魔梯加速器.apk
文件大小: 25.77MB
MD5值: 5b7a9081024836777a62d0499ab3b7f3
SHA1值: ceb9b9e8673b091421c138e37c882a4baee8ad9e
SHA256值: 348414d05e4bb3cb0ca5fc9d4de06e10461187d1c8e78af289cc9a81ac5c9b9f

i APP 信息

App名称: 魔梯加速器
包名: com.pluto.moti
主活动Activity: com.pluto.demo.ui.SplashActivity
安卓版本名称: 1.0.6.01
安卓版本: 106010

🔍 域名线索

域名	服务器信息
www.google.com	IP: 128.242.240.93 所属国家: United States of America 地区: California 城市: Milpitas 纬度: 37.428268 经度: -121.906616
t.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Lowestoft 纬度: 52.475201 经度: 1.751590
ssp-demo-488e7.firebaseio.com	IP: 34.120.160.131 所属国家: United States of America 地区: Missouri

	城市: Kansas City 纬度: 39.099731 经度: -94.578568
play.google.com	IP: 59.24.3.174 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul 纬度: 37.568260 经度: 126.977829
aaxc.cc	IP: 128.242.240.218 所属国家: United States of America 地区: California 城市: Milpitas 纬度: 37.428268 经度: -121.906616
1.2345345.xyz	IP: 172.67.190.50 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
twitter.com	IP: 104.244.42.129 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
azhong.tk	没有服务器地理信息.
image.crisp.chat	IP: 104.18.29.91 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700

	经度: -122.395203
raw.githubusercontent.com	IP: 185.199.111.133 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
xpluto.cyou	IP: 172.67.180.125 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
m.me	IP: 31.13.82.1 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696
wx.tenpay.com	IP: 121.51.73.12 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298
dashif.org	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
ns.adobe.com	没有服务器地理信息.

icon-icons.com	IP: 151.106.39.238 所属国家: France 地区: Hauts-de-France 城市: Roubaix 纬度: 50.694210 经度: 3.174560
telegram.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Lowestoft 纬度: 52.475201 经度: 1.751590
motivpnn.top	IP: 172.67.184.191 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
settings.crisp.chat	IP: 104.18.29.91 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
gitee.com	IP: 182.255.34.126 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.222219 经度: 121.458061
crisp.chat	IP: 104.18.28.91 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700

	经度: -122.395203
malio.aaxc.cc	IP: 128.242.240.221 所属国家: United States of America 地区: California 城市: Milpitas 纬度: 37.428268 经度: -121.906616
github.com	IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903

 URL线索

URL信息	Url所在文件
https://settings.crisp.chat/client/website/	im/crisp/client/internal/l/a.java
https://m.me/	im/crisp/client/internal/c/a.java
https://telegram.me/	im/crisp/client/internal/c/a.java
https://twitter.com/	im/crisp/client/internal/c/a.java
https://image.crisp.chat/	im/crisp/client/internal/k/a.java
https://image.crisp.chat/avatar/operator/	im/crisp/client/internal/k/a.java
https://image.crisp.chat/avatar/website/	im/crisp/client/internal/k/a.java

https://crisp.chat/en/	im/crisp/client/internal/u/b.java
https://www.google.com/	im/crisp/client/internal/u/b.java
https://crisp.chat/	im/crisp/client/internal/j/b.java
https://xpluto.cyou/	com/pluto/presentation/remote/o00000.java
https://motivpnn.top/	com/pluto/presentation/remote/o00000.java
https://gitee.com/pluto_theme/androidpackagenamelist/raw/master/proxy.txt	com/pluto/presentation/remote/o00000.java
https://raw.githubusercontent.com/2dust/androidpackagenamelist/master/proxy.txt	com/pluto/connect/free/AppConfig.java
https://1.2345345.xyz/ads.html	com/pluto/connect/free/AppConfig.java
https://raw.githubusercontent.com/2dust/v2rayCustomRoutingList/master/	com/pluto/connect/free/AppConfig.java
https://github.com/2dust/v2rayNG/issues	com/pluto/connect/free/AppConfig.java
http://azhong.tk:8081/api/	com/pluto/demo/u2.java
https://play.google.com/store/apps/details?id=	com/pluto/demo/eq.java
https://t.me/pluto_theme	com/pluto/demo/cu.java
https://xpluto.cyou/	com/pluto/demo/cu.java
http://dashif.org/guidelines/last-segment-number	com/pluto/demo/le.java
http://dashif.org/guidelines/trickmode	com/pluto/demo/le.java
http://ns.adobe.com/xap/1.0/	com/pluto/demo/xc.java
https://www.google.com/generate_204	com/pluto/demo/utils/Oooo000.java

https://wx.tenpay.com	com/pluto/demo/widget/webview/CustomWebView.java
https://t.me/mars_vpn	com/pluto/demo/ui/FeedbackActivity.java
https://icon-icons.com/downloadimage.php?id=89781&root=1368/PNG/512/&file=-avatar_89781.png	Mogua Engine V1
https://ssp-demo-488e7.firebaseio.com	Mogua Engine V1
https://github.com/castorflex	Mogua Engine V1
https://github.com/castorflex/SmoothProgressBar	Mogua Engine V1
https://github.com/castorflex/SmoothProgressBar.git	Mogua Engine V1
https://t.me/pluto_theme	Mogua Engine V2
https://aaxc.cc/link/041HlcW1nqXDdVWD?sub=1<=2	Mogua Engine V2
https://malio.aaxc.cc/	Mogua Engine V2

 邮箱线索

邮箱地址	所在文件
super.vps.mars@gmail.com	com/pluto/demo/ui/FeedbackActivity.java
name@site.ru	Mogua Engine V1
theme.pluto@gmail.com	Mogua Engine V2

 手机线索

手机号	所在文件
18144000000	com/pluto/common/cache/DiskCache.java
13846158196	com/haibin/calendarview/OooOo.java
17471680261	com/haibin/calendarview/OooOo.java
18826691036	com/haibin/calendarview/OooOo.java
14159265359	com/haibin/calendarview/OooOo.java
13446589358	com/haibin/calendarview/OooOo.java
19870156017	com/haibin/calendarview/OooOo.java
19846674381	com/haibin/calendarview/OooOo.java
17387749012	com/haibin/calendarview/OooOo.java
13516237631	com/haibin/calendarview/OooOo.java
17882652114	com/haibin/calendarview/OooOo.java
18914945834	com/haibin/calendarview/OooOo.java
16832995016	com/haibin/calendarview/OooOo.java

 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=CN, L=Beijing, O=Joy, OU=Joy, CN=Joy Whale
签名算法: rsassa_pkcs1v15
有效期自: 2018-06-07 03:09:51+00:00
有效期至: 3017-10-08 03:09:51+00:00
发行人: C=CN, L=Beijing, O=Joy, OU=Joy, CN=Joy Whale
序列号: 0x3e0e7ea7
哈希算法: sha256
md5值: 29e1c133e0776862f9207f34508d22ad
sha1值: a39bfc840693dd7e8f7f316d64a8fdee8bda81c2
sha256值: d9b88a2342979b7dcd71fb1c126e14473f3922a78199c980707cb23875fbee3e
sha512值: 72fe9227a2215593609959142c90e376a1b0de6161ab2b08974bbb3772d1d23d3f6dddee8e5a952871fc4105156594ced7ffb257365f891aa8cbc3d3177db2ff
公钥算法: rsa
密钥长度: 2048
指纹: d0f68a6831b9b516ed15979706beaf88bdef1615da353b083cc468f58e8c72b4

硬编码敏感信息

可能的敏感信息
"connect_status_request_secret" : "Verifying"
"connect_status_request_secret_failure" : "Verify failure %s"
"crisp_debug_reset_session" : "Reset chat session"
"crisp_debug_reset_token_id" : "Reset Token ID"
"crisp_debug_set_token_id" : "Set Token ID"
"crisp_debug_token_id" : "Token ID"
"crisp_debug_token_id" : "Token ID"

"digits_username" : "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ@_-"
"firebase_database_url" : "https://ssp-demo-488e7.firebaseio.com"
"google_api_key" : "AlzaSyBNzgYXCJZdtS43Em_uA2Ch365b_wlQ58s"
"google_crash_reporting_api_key" : "AlzaSyBNzgYXCJZdtS43Em_uA2Ch365b_wlQ58s"
"library_smoothprogressbar_author" : "Antoine Merle"
"library_smoothprogressbar_authorWebsite" : "https://github.com/castorflex"
"success_reset_pwd" : "Reset password successfully"
"success_upload_password" : "The password has been modified successfully. Please log in again."
"connect_status_request_secret" : "Verifying"
"connect_status_request_secret_failure" : "Verify failure %s"
"success_reset_pwd" : "Reset password successfully"
"success_upload_password" : "The password has been modified successfully. Please log in again."
"connect_status_request_secret" : "正在校验"
"connect_status_request_secret_failure" : "校验失败 %s"
"success_reset_pwd" : "重置密码成功"
"success_upload_password" : "密码修改成功，请重新登录"
"connect_status_request_secret" : "正在校驗"
"connect_status_request_secret_failure" : "校驗失敗 %s"

"success_reset_pwd" : "重置密碼成功"
"success_upload_password" : "密碼修改成功，請重新登錄"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何

android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.ACCESS_WIFI_STATE	正常	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.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
com.pluto.moti.permission.RECEIVE_BROADCASTS	未知	Unknown permission	Unknown permission from android reference

android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
---	----	---------	---

应用内通信

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