MoGua

综合办公 3.6.0.0.16.APK 分析报告

APP名称: 综合办公

包名:	om.smartdot.mobile.platform.no
域名线索:	19条
URL线索:	6条
邮箱线索:	0条
分析日期:	2025年7月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: android.apk
文件大小: 75.98MB
MD5值: c7cbc3bc44173ff70b8429ebe425c236
SHA1值: 6e2e92ad2917af1e0cec4fc73d205005c623837f
SHA256值: e0440b55c8c991553a6fa877c4d31abae015f746c1d57a56e1ad45899b3b3e6e

APP 信息

App名称: 综合办公
包名: om.smartdot.mobile.platform.no
主活动Activity: om.smartdot.mobile.platform.no.login.SplashActivity
安卓版本名称: 3.6.0.0.16
安卓版本: 31

域名线索

域名	服务器信息
grs.dbankcloud.asia	**IP**: 121.36.116.8 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
metrics2.data.hicloud.com	**IP**: 80.158.38.48 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
	IP: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast'

metrics5.data.hicloud.com	**城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
grs.dbankcloud.com	IP: 60.28.200.159 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
grs.dbankcloud.eu	没有服务器地理信息.
metrics1-drcn.dt.dbankcloud.cn	IP: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.w3.org	IP: 104.18.22.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
data-dra.push.dbankcloud.com	IP: 119.8.163.189 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987

	经度: 103.850281
data-drru.push.dbankcloud.com	IP: 159.138.202.31 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
jsperf.com	IP: 104.16.227.18 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
data-drcn.push.dbankcloud.com	IP: 121.36.117.8 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
grs.platform.dbankcloud.ru	没有服务器地理信息.
issues.apache.org	IP: 168.119.33.54 **所属国家**: Germany **地区**: Bayern **城市**: Gunzenhausen **纬度**: 48.323860 **经度**: 11.601019
cordova.apache.org	IP: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

metrics5.dt.dbankcloud.ru	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
www.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
data-dre.push.dbankcloud.com	**IP**: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
grs.dbankcloud.cn	**IP**: 121.36.117.149 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL**信息**	Url**所在文件**
http://'	摸瓜V2引擎
https://data-drcn.push.dbankcloud.com	摸瓜V2引擎

https://data-dra.push.dbankcloud.com	摸瓜V2引擎
https://data-dre.push.dbankcloud.com	摸瓜V2引擎
https://data-drru.push.dbankcloud.com	摸瓜V2引擎
https://metrics1-drcn.dt.dbankcloud.cn:443	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.dt.dbankcloud.ru:6447	摸瓜V2引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://grs.platform.dbankcloud.ru	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://jsperf.com/b64tests	摸瓜V2引擎
http://server/myapp/index.html	摸瓜V2引擎
https://issues.apache.org/jira/browse/CB-11522)	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎

http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://cordova.apache.org/docs/en/latest/cordova/events/events.html	摸瓜V2引擎

邮箱线索

手机线索

手机号	所在文件
15896934676	摸瓜V1引擎

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=smartdot, ST=beijing, L=beijing, O=smartdot, OU=smartdot, CN=smartdot
签名算法: rsassa_pkcs1v15
有效期自: 2019-05-29 02:15:03+00:00
有效期至: 2044-05-22 02:15:03+00:00
发行人: C=smartdot, ST=beijing, L=beijing, O=smartdot, OU=smartdot, CN=smartdot
序列号: 0x36adb235
哈希算法: sha256
md5值: b9fe93e0c1fd9157dc3ac2059825e2ca
sha1值: 47ba543c43ae1cd42ea9f3d1d1c855346dd4bcc3
sha256值: 293fe6900d9204dfd6ef7e2ffd6d4fa7c84f720bd280225161c7e6e64af4738e
sha512值: 7067b7bc1a2dc7859f8bf9d2601d46255ce98b9c2b84277c43009200ba525d278f28792a701baa695260154a95c746e9229c73cdc5de43cc47776d67426d3cae
公钥算法: rsa
密钥长度: 2048
指纹: 209ec23ca701e7adf0b16f782f8f6e7c3da67f4c819d98106e3176afe18398c4

硬编码敏感信息

可能的敏感信息
"fat_auth_desc_pre" : "为了"
"fin_applet_admin_auth_err_title" : "没有审核权限"
"fin_applet_authorization_setting" : "小程序授权管理"
"fin_applet_default_userinfo_auth_notice" : "您授权后，小程序开发者（包括小程序代开发服务商的开发者及小程序中使用插件的开发者）将%1$s，为您提供相关服务。开发者收集、存储、处理或使用用户隐私及数据，应当遵守网络安全法与个人信息保护规范等相关法律法规。若您认为开发者未遵守上述规定或存在其他侵害用户隐私或数据的情况，可进行%2$s。"
"fin_applet_third_userinfo_auth" : "第三方用户信息授权说明"
"fin_applet_third_userinfo_auth_notice" : "您授权后，小程序开发者（包括小程序代开发服务商的开发者及小程序中使用插件的开发者）将%1$s，为您提供相关服务。开发者严格按照%2$s处理您的个人信息，如您发现开发者不当处理您的个人信息，可进行%3$s。"
"rc_authorities_fileprovider" : ".FileProvider"
"rc_emoji_hear_no_monkey" : "不听"
"rc_emoji_see_no_monkey" : "不看"
"rc_gathered_conversation_private_title" : "单聊消息"
"fat_auth_desc_pre" : "in order to"
"fin_applet_admin_auth_err_title" : "No examine access"
"fin_applet_authorization_setting" : "Authorization setting"
"fin_applet_default_userinfo_auth_notice" : "Upon your authorization, the mini-app developers (including mini-app developers on behalf of development services and develo

pers of embedded plugins in mini-app) will %1$s to provide services for you. The developer shall process your personal information in strict accordance with network securit y law and personal information protection norms and other relevant laws and regulations when collecting, storing, processing or using user privacy and data. In the event of the developer's improper use of your personal information, please %2$s to us."
"fin_applet_third_userinfo_auth" : "Third-party user information authorization description"
"fin_applet_third_userinfo_auth_notice" : "Upon your authorization, the mini-app developers (including mini-app developers on behalf of development services and develop ers of embedded plugins in mini-app) will %1$s to provide services for you. The developer shall process your personal information in strict accordance with %2$s. In the eve nt of the developer's improper use of your personal information, please %3$s to us."
"rc_emoji_hear_no_monkey" : "Hear-No-Monkey"
"rc_emoji_see_no_monkey" : "See-No-Monkey"
"rc_gathered_conversation_private_title" : "Private"
"rc_emoji_hear_no_monkey" : "قرد2"
"rc_emoji_see_no_monkey" : "قرد1"
"rc_gathered_conversation_private_title" : " خاص "

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.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.PROCESS_OUTGOING_CALLS	危险	拦截拨出电话	允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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定数据。恶意应用可能会损坏你的系统的配置。
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.REPLACE_EXISTING_PACKAGE	未知	Unknown permission	Unknown permission from android reference
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.huawei.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
om.smartdot.mobile.platform.no.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference

android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_SCAN	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_ADVERTISE	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERACT_ACROSS_USERS_FULL	未知	Unknown permission	Unknown permission from android reference
android.permission.USE_FULL_SCREEN_INTENT	正常		针对想要使用通知全屏意图的 Build.VERSION_CODES.Q 的应用程序是必需的
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
om.smartdot.mobile.platform.no.permission.RONG_ACCESS_RECEIVER	未知	Unknown permission	Unknown permission from android reference
om.smartdot.mobile.platform.no.permission.RONG_BRIDGE_ACTIVITY	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.REORDER_TASKS	正	重新排序正在运行的	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受

	常	应用程序	您控制的情况下将自己强加于前
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
android.permission.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
om.smartdot.mobile.platform.no.permission.FIN_APPLET_RECEIVER	未知	Unknown permission	Unknown permission from android reference
om.smartdot.mobile.platform.no.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
om.smartdot.mobile.platform.no.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.hihonor.push.permission.READ_PUSH_NOTIFICATION_INFO	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
om.smartdot.mobile.platform.no.login.SplashActivity	Schemes: huijiayuan://, Hosts: startup,
om.smartdot.mobile.platform.no.main.MainActivity	Schemes: huijiayuan://,

	Hosts: operation,
om.smartdot.mobile.platform.no.main.NoMainActivity	Schemes: huijiayuan://, Hosts: operation,
om.smartdot.mobile.platform.no.chat.ChatActivity	Schemes: huijiayuan://, Hosts: openchat,
om.smartdot.mobile.platform.no.work.WorkWebViewActivity	Schemes: huijiayuan://, Hosts: openwebview,
com.finogeeks.lib.applet.modules.urlrouter.UrlRouterActivity	Schemes: @string/fin_applet_router_url_scheme://,

---