MoGua

КРЕЙЗИ SLOTS 1.0.APK 分析报告

APP名称: КРЕЙЗИ SLOTS

包名:	com.kpen.nsst4
域名线索:	20条
URL线索:	16条
邮箱线索:	8条
分析日期:	2025年7月31日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: КРЕИЗИ_SLOTS_V4.apk
文件大小: 52.8MB
MD5值: 131e7078a5f70cc6d3d05f51cb0ceff7
SHA1值: 44da5cf0e3243fb01d2d433e3ee8d1c5d006d558
SHA256值: 5eb9a594764e33f8cc5f7a32c4def591afee34cce0a72adcce71b56d0498212c

APP 信息

App名称: КРЕЙЗИ SLOTS
包名: com.kpen.nsst4
主活动Activity: org.cocos2dx.javascript.AppActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	服务器信息
www.cocos.com	**IP**: 218.11.0.24 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
ru.game-365.app	**IP**: 47.254.186.78 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996
www.example.com	**IP**: 23.55.51.197 **所属国家**: Australia **地区**: New South Wales

	城市: Sydney **纬度**: -33.867779 **经度**: 151.207047
issuetracker.google.com	**IP**: 142.250.217.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.saxproject.org	**IP**: 204.68.111.100 **所属国家**: United States of America **地区**: California **城市**: San Diego **纬度**: 32.799797 **经度**: -117.137047
www.apple.com	**IP**: 221.194.154.187 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
api.vk.com	**IP**: 87.240.139.193 **所属国家**: Russian Federation **地区**: Sankt-Peterburg **城市**: Saint Petersburg **纬度**: 59.894440 **经度**: 30.264200
purl.eligrey.com	**IP**: 104.236.163.66 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
	IP: 8.7.198.46

cdn.jsdelivr.net	**所属国家**: United States of America **地区**: Louisiana **城市**: Monroe **纬度**: 32.548328 **经度**: -92.045235
www.khronos.org	**IP**: 159.65.181.57 **所属国家**: United States of America **地区**: New Jersey **城市**: Clifton **纬度**: 40.858585 **经度**: -74.163605
eligrey.com	**IP**: 104.236.163.66 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
my.com	没有服务器地理信息.
crbug.com	**IP**: 216.239.32.29 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
heycam.github.io	**IP**: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
	IP: 93.186.237.1 **所属国家**: Russian Federation **地区**: Moskva

id.vk.com	**城市**: Moscow **纬度**: 55.752258 **经度**: 37.615471
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
vk.com	**IP**: 87.240.137.164 **所属国家**: Russian Federation **地区**: Sankt-Peterburg **城市**: Saint Petersburg **纬度**: 59.894440 **经度**: 30.264200
goo.gle	**IP**: 67.199.248.12 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.750134 **经度**: -73.997009
dom.spec.whatwg.org	**IP**: 165.227.248.76 **所属国家**: United States of America **地区**: New Jersey **城市**: Clifton **纬度**: 40.858585 **经度**: -74.163605
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

URL线索

URL信息	Url所在文件
https://my.com/?	com/my/tracker/obfuscated/n.java
https://vk.com/dev/access_token	com/vk/api/sdk/auth/VKAuthParams.java
https://dev.	com/vk/api/sdk/auth/VKAuthResultContract.java
http://www.example.com	com/vk/api/sdk/browser/BrowserSelector.java
https://api.vk.com/oauth/authorize	com/vk/api/sdk/ui/VKWebViewAuthActivity.java
http://www.example.com	com/vk/id/internal/auth/web/BrowserSelector.java
https://api.vk.com	com/vk/id/network/InternalVKIDRealApi.java
https://id.vk.com	com/vk/id/network/InternalVKIDRealApi.java
https://vk.com	com/vk/id/test/VKIDMockCall.java
https://goo.gle/compose-feedback	f0/q.java
https://ru.game-365.app/login/vk-redirect.html	org/cocos2dx/javascript/WebViewActivity.java
https://ru.game-365.app/login/tg-redirect.html	org/cocos2dx/javascript/WebViewActivity.java
https://issuetracker.google.com/issues/297974033	w/d0.java
https://issuetracker.google.com/issues/300280216	w/d0.java
https://github.com/google/gson/blob/main/Troubleshooting.md	t5/n.java

http://eligrey.com	摸瓜V2引擎
https://github.com/dsamarin	摸瓜V2引擎
https://github.com/eligrey/Blob.js/blob/master/LICENSE.md	摸瓜V2引擎
http://purl.eligrey.com/github/Blob.js/blob/master/Blob.js	摸瓜V2引擎
https://dom.spec.whatwg.org/	摸瓜V2引擎
https://heycam.github.io/webidl/	摸瓜V2引擎
https://github.com/taylorhakes	摸瓜V2引擎
https://github.com/taylorhakes/promise-polyfill/blob/master/LICENSE	摸瓜V2引擎
https://cdn.jsdelivr.net/npm/promise-polyfill@8/dist/polyfill.js	摸瓜V2引擎
http://www.cocos.com	摸瓜V2引擎
https://www.khronos.org/registry/OpenGL/extensions/ARB/ARB_texture_float.txt	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/helpers/DefaultHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ContentHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ErrorHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ext/LexicalHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ext/DeclHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ext/EntityResolver2.html	摸瓜V2引擎

http://www.saxproject.org/apidoc/org/xml/sax/DTDHandler.html	摸瓜V2引擎
http://www.cocos.com	摸瓜V2引擎
https://www.cocos.com/	摸瓜V2引擎
https://crbug.com/v8/8520	lib/arm64-v8a/libcocos2djs.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/arm64-v8a/libcocos2djs.so
https://crbug.com/v8/8520	lib/armeabi-v7a/libcocos2djs.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/armeabi-v7a/libcocos2djs.so

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	g4/q.java
z@p.maly	摸瓜V2引擎
c@9-qsbt5.xmml	摸瓜V2引擎
lдz@g.5cq	摸瓜V2引擎
w@h.rз	摸瓜V2引擎
dek-@2.rk10	摸瓜V2引擎
cocos@cocoss-macbook-pro.local	lib/arm64-v8a/libcocos2djs.so

cocos@cocoss-macbook-pro.local	lib/armeabi-v7a/libcocos2djs.so

手机线索

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=HK, ST=Unknown, L=Central, O=FinPlus Technologies Limited, OU=Engineering, CN=Jason Hee
签名算法: rsassa_pkcs1v15
有效期自: 2025-07-16 11:27:54+00:00
有效期至: 2052-12-01 11:27:54+00:00
发行人: C=HK, ST=Unknown, L=Central, O=FinPlus Technologies Limited, OU=Engineering, CN=Jason Hee
序列号: 0x3546493ae5ed5af5
哈希算法: sha256
md5值: fc5d5cc317b2688282489d0644c5b88e
sha1值: 02f735c6d5c5843f0f872ab019ea24ff63b2c50f
sha256值: c4a54b83a90310ab2713e0ff02e75bad8a137d98d391efc340ce4af5025169c1
sha512值: f342b84cb44b4a4555492c8c9c01f6d201b8aef5c2f1cea4cd0e02cfb5a8656808addb28064833e875f5ec481cd59403aeaf8a4c03cc492eefddd1fdc524ba47
公钥算法: rsa
密钥长度: 2048
指纹: 3409071726ac4f2bdce557b2643ae129402f7875d76c65178f7bd64995ce46f3

硬编码敏感信息

可能的敏感信息
"vkid_oauth_list_widget_note" : "or sign in with VK ID using information from a service"
"vkid_oauth_list_widget_note" : "oder melden Sie sich mit Ihrer VK-ID an, indem Sie Informationen aus dem Dienst verwenden"

"vkid_oauth_list_widget_note" : "або увійти через VK ID з використанням даних із сервісу"
"vkid_oauth_list_widget_note" : "lub wejdź poprzez VK ID przy użyciu danych z serwisu"
"vkid_oauth_list_widget_note" : "ou se connecter avec VK ID en utilisant les informations d'un service"
"vkid_oauth_list_widget_note" : "Ya da hizmetteki verileri kullanarak VK ID hizmeti yardımıyla gir"
"vkid_oauth_list_widget_note" : "o iniciar sesión con VK ID utilizando la información de un servicio"
"vkid_oauth_list_widget_note" : "или войти через VK ID с использованием данных из сервиса"

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.kpen.nsst4.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.vk.id.internal.auth.RedirectUriReceiverActivity	Schemes: vk53689217://, Hosts: vk.com,