



MoGua

Titanium Backup 8.4.0.2.APK 分析报告



APP名称:

Titanium Backup

包名: `com.keramidas.TitaniumBackup`

域名线索: 19条

URL线索: 22条

邮箱线索: 5条

分析日期: 2025年7月6日

分析平台: [摸瓜APK反编译平台](#)

文件名: taibeifen_14395.apk

文件大小: 7.77MB

MD5值: ac89af74cf5178d5eaed927af076dfb0

SHA1值: ab953fb96bc263644a72e408249fbcc2254445b4

SHA256值: e2cb198893dd9b3f62699f1e706a1f22e919a16a04c026d6cb7679217f18a5f0

i APP 信息

App名称: Titanium Backup

包名: com.keramidas.TitaniumBackup

主活动Activity: .MainActivity

安卓版本名称: 8.4.0.2

安卓版本: 417

🔍 域名线索

域名	服务器信息
www.googleapis.com	IP: 172.217.163.42 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
app.box.com	IP: 78.16.49.15 所属国家: Ireland 地区: Galway 城市: Galway 纬度: 53.272072 经度: -9.049173
upload.box.com	IP: 74.112.186.128 所属国家: United States of America 地区: California

	<p>城市: Redwood City 纬度: 37.485001 经度: -122.236839</p>
crowdin.net	<p>IP: 52.20.176.128 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806</p>
www.youtube.com	<p>IP: 108.160.169.171 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203</p>
www.python.org	<p>IP: 151.101.88.223 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203</p>
lab75.jp	<p>IP: 76.76.21.142 所属国家: United States of America 地区: California 城市: Walnut 纬度: 34.015400 经度: -117.858223</p>
schemas.android.com	<p>没有服务器地理信息.</p>
accounts.google.com	<p>IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig 纬度: 52.266121</p>

	经度: 10.526730
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
android.clients.google.com	IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
code.google.com	IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
api.box.com	IP: 74.112.186.144 所属国家: United States of America 地区: California 城市: Redwood City 纬度: 37.485001 经度: -122.236839
www.titaniumtrack.com	IP: 46.127.137.226 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790
	IP: 74.112.186.144 所属国家: United States of America

www.box.com	地区: California 城市: Redwood City 纬度: 37.485001 经度: -122.236839
android.modaco.com	没有服务器地理信息.
lookout.go2cloud.org	IP: 18.202.12.61 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
www.dropbox.com	IP: 202.160.128.203 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
matrixrewriter.com	IP: 46.127.137.226 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790

URL线索

URL信息	Url所在文件
https://matrixrewriter.com/android/	com/keramidas/TitaniumBackup/MainActivity.java
https://matrixrewriter.com/wiki/	com/keramidas/TitaniumBackup/MainActivity.java

http://android.modaco.com/	com/keramidas/TitaniumBackup/MainActivity.java
http://android.modaco.com/category/363/device-specific/	com/keramidas/TitaniumBackup/MainActivity.java
http://www.youtube.com/user/wwjoshdew	com/keramidas/TitaniumBackup/MainActivity.java
http://www.youtube.com/results?search_query=titanium+backup	com/keramidas/TitaniumBackup/MainActivity.java
http://lab75.jp/	com/keramidas/TitaniumBackup/MainActivity.java
https://code.google.com/p/android-market-api/	com/keramidas/TitaniumBackup/MainActivity.java
http://www.apache.org/licenses/LICENSE-2.0	com/keramidas/TitaniumBackup/MainActivity.java
https://www.titaniumtrack.com/privacy-policy.html	com/keramidas/TitaniumBackup/MainActivity.java
https://www.box.com/signup/	o/aA.java
http://www.dropbox.com/referrals/NTY3NzU5OTM5	o/aO.java
https://www.googleapis.com/auth/drive	o/aT.java
http://www.titaniumtrack.com/ns/titanium-backup/wifi-networks	o/C1246b.java
http://www.titaniumtrack.com/	o/C1249ba.java
http://lookout.go2cloud.org/aff_c?offer_id=4&aff_id=158&aff_sub=TitaniumTrack&aff_sub2=TitaniumBackup&aff_sub3=Featured_App&source=Partner	o/eY.java
https://api.box.com/2.0	o/C0227.java
https://upload.box.com/api/2.0	o/C0227.java
http://android.clients.google.com/market/api/ApiRequest	o/C0080.java

https://matrixrewriter.com/android/titanium_backup_changelog.txt	o/C0330.java
https://app.box.com/static/sync_redirect.html	o/C0380.java
https://matrixrewriter.com/wiki/	o/DialogInterface\$OnClickListenerC0459.java
https://accounts.google.com/o/oauth2/auth	o/C0647.java
https://accounts.google.com/o/oauth2/token	o/C0650.java
https://accounts.google.com/o/oauth2/token	o/C0691.java
https://api.box.com	o/C0831.java
https://api.box.com/oauth2/token	o/C0831.java
https://api.box.com/oauth2/revoke	o/C0831.java
http://www.python.org/topics/xml/dtds/xbel-1.0.dtd	o/C1060.java
http://www.titaniumtrack.com/ns/titanium-backup/bookmarks	o/C1060.java
http://www.titaniumtrack.com	o/C1060.java
http://www.titaniumtrack.com/ns/titanium-backup/calls	o/C1094.java
https://www.googleapis.com/	o/C1152.java
http://crowdin.net/project/titanium-backup	o/C1151.java
http://schemas.android.com/apk/res/android	o/C1151.java
http://www.titaniumtrack.com/ns/titanium-backup/messages	o/C1192.java
http://crowdin.net/translate/titanium-backup/644/en-el	Mogua Engine V1

✉ 邮箱线索

邮箱地址	所在文件
support@dropbox.com	com/dropbox/core/android/AuthActivity.java
titanium.android@gmail.com getsupport@titaniumtrack.com	com/keramidas/TitaniumBackup/MainActivity.java
getsupport@titaniumtrack.com	o/C0248.java
joel.bourquard@gmail.com	o/DialogInterface\$OnClickListenerC0588.java
framework@boot.art framework@boot.oat	o/C0658.java

📱 手机线索

🌟 签名证书

APK已签名

v1 签名: True

v2 签名: False

v3 签名: False

找到 1 个唯一证书

主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Joël Bourquard

签名算法: rsassa_pkcs1v15

有效期自: 2009-12-11 14:03:41+00:00

有效期至: 2146-11-03 14:03:41+00:00

发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Joël Bourquard

序列号: 0x4b22513d

哈希算法: sha1

md5值: cdcbc5529bfe4ba3c4bba450ea1113e5

sha1值: 8f07144e14eb24e9b39679b4db770869f7ba74ae

sha256值: d25e2072260182485b7182e527134f52daed598a0df1253987e0a2ea0cddc8a0

sha512值: 04cf9f0e79f3f39a81bd86a23f7fb3c183f11b04df5f67f719364ed86d5e6c4656da7f0c01d3604581282fd63b003d2b356121b8107d604aa061c3950c17e8cb

硬编码敏感信息

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_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.READ_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.WRITE_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证令牌
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
com.android.browser.permission.READ_HISTORY_BOOKMARKS	未知	Unknown permission	Unknown permission from android reference
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	未知	Unknown	Unknown permission from android reference

		permission	
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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.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_SUPERUSER	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。
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.keramidas.TitaniumBackupAddon.USE_CP	未知	Unknown permission	Unknown permission from android reference
com.android.voicemail.permission.ADD_VOICEMAIL	未知	Unknown permission	Unknown permission from android reference
com.android.voicemail.permission.READ_WRITE_ALL_VOICEMAIL	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)

.ImportBackupActivity	Schemes: file://, http://, https://, Hosts: *, Mime Types: application/vnd.titaniumbackup.archive, */*, Path Patterns: .*\\TiBkp, .*\\.*\\TiBkp, .*\\.*\\.*\\TiBkp, .*\\.*\\.*\\.*\\TiBkp, .*\\.*\\.*\\.*\\.*\\TiBkp, .*\\.*\\.*\\.*\\.*\\.*\\TiBkp, .*\\.*\\.*\\.*\\.*\\.*\\.*\\TiBkp, .*\\.*\\.*\\.*\\.*\\.*\\.*\\.*\\TiBkp, .*\\.*\\.*\\.*\\.*\\.*\\.*\\.*\\.*\\TiBkp, .*\\.*\\.*\\.*\\.*\\.*\\.*\\.*\\.*\\.*\\TiBkp,
.cloud.OAuth2ResponseHandler	Schemes: com.keramidas.titaniumbackup://,
com.dropbox.core.android.AuthActivity	Schemes: db-pflv2wm5i1gixnb://,

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。