MoGua

MainActivity 1.0.APK 分析报告

APP名称: MainActivity

包名:	com.metasploit.stage
域名线索:	0条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年8月9日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: shell.apk
文件大小: 0.01MB
MD5值: cf1d3e82c77fec1f7fd103f62fc17669
SHA1值: 8f7e7d561cb078b3b6a2d4fb3dbf21193f87ba5b
SHA256值: 00ae982ef5a94714b343ec2931dcb6ecc9410789ae49e3d57a7c0df2c928d00a

APP 信息

App名称: MainActivity
包名: com.metasploit.stage
主活动Activity: .MainActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

URL线索

URL**信息**	Url**所在文件**
http://schemas.android.com/apk/res/android	摸瓜V3引擎
play.googleapis.com	摸瓜V3引擎

邮箱线索

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=US/O=Android/CN=Android Debug
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-24 18:48:32+00:00
有效期至: 2036-08-31 02:36:47+00:00
发行人: C=US/O=Android/CN=Android Debug
序列号: 0x1
哈希算法: sha1
md5值: f882c2a51ec9ed54e6ea7a24dd2a39b6
sha1值: 117847a43f25664e219b08b1a854ca1d48cbe82d
sha256值: 59fdaf81d3fff981bd7b568b643e1a5d6e0873a73c69864411a0c2d7dcc75161
sha512值: 9e537ea02bdbe844421847231b34d1f2b0e0c116abfde5969e2dff24caecdc7da2228fd7530d97cde5c1a3646b5056f1abc213df3cf4373cac3d36782ee9cf56

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_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_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.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.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.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示

android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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.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.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.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
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.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.SET_WALLPAPER	正常	设置壁纸	允许应用程序设置系统壁纸
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.WRITE_CALL_LOG	危险		允许应用程序写入（但不读取）用户号召日志数据。
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
.MainActivity	Schemes: metasploit://, Hosts: my_host,
