MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

e彩 V2.0.7.APK

APP名称:	e彩
包名:	com.alpha.ecai335
域名线索:	9条
URL线索:	33条
邮箱线索:	3条
分析日期:	2022年1月19日 11:12

文件信息

文件名: 18155287.apk
文件大小: 30.16MB
MD5值: 649eb789b4002823ee422e605fab4aea
SHA1值: 67d67b0cd20e123e9778ca3a5245cecf49db0487
SHA256值: b3571eb9c3f435226fb3b9a7469365fc60c665caba75d2241aead7d63a7af77b

APP 信息

App名称: e彩
包名: com.alpha.ecai335
主活动**Activity:** com.cp99.tz01.lottery.ui.activity.SplashActivity
安卓版本名称: V2.0.7
安卓版本: 107

域名线索

域名	是否危险域名	服务器信息
yun-hl.3g.qq.com	good	**IP:** 175.27.0.142 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
support.rongcloud.cn	good	**IP:** 101.254.240.151 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
analytics.map.qq.com	good	**IP:** 182.254.63.54 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
schemas.android.com	good	没有服务器地理信息.
ue.indoorloc.map.qq.com	good	**IP:** 182.254.50.54 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
0335ec-api3kdk.apixdll7.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
cc.map.qq.com	good	**IP:** 182.254.57.47 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
up-hl.3g.qq.com	good	**IP:** 109.244.209.98 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
upload.ffmpeg.org	good	**IP:** 213.36.253.119 所属国家: France 地区: Ile-de-France 城市: Paris 纬度: 48.853409 经度: 2.348800 查看地图: Google Map

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
https://0335ec-api3kdk.apixdll7.com:5869	com/cp99/tz01/lottery/ui/activity/personalCenter/setting/c.java
https://0335ec-api3kdk.apixdll7.com:5869	com/cp99/tz01/lottery/ui/fragment/homePage/j.java
http://support.rongcloud.cn/kb/Mjc2	com/cp99/tz01/lottery/ui/fragment/chat/k0.java
https://0335ec-api3kdk.apixdll7.com:5869	com/cp99/tz01/lottery/e/h.java
http://schemas.android.com/apk/res/android	com/cp99/tz01/lottery/widget/FixedSlidingTabLayout.java
http://schemas.android.com/apk/res/android	com/cp99/tz01/lottery/widget/FixCommonTabLayout.java
https://up-hl.3g.qq.com/upreport	c/t/m/g/at.java
https://analytics.map.qq.com/?wf4	c/t/m/g/cs.java
https://ue.indoorloc.map.qq.com/	c/t/m/g/ek.java
https://cc.map.qq.com/?get_c3	c/t/m/g/cz.java
https://yun-hl.3g.qq.com/halleycloud	c/t/m/g/cd.java
https://ue.indoorloc.map.qq.com/?wl	c/t/m/g/eh.java
https://analytics.map.qq.com/?sf	c/t/m/g/cu.java
ftp://upload.ffmpeg.org/incoming/	lib/armeabi-v7a/libijkplayer.so

URL信息	Url所在文件
ftp://upload.ffmpeg.org/incoming/	lib/x86/libijkplayer.so
ftp://upload.ffmpeg.org/incoming/	lib/armeabi/libijkplayer.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so
ffmpeg-devel@ffmpeg.org	lib/x86/libijkplayer.so
ffmpeg-devel@ffmpeg.org	lib/armeabi/libijkplayer.so

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.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

向手机申请的权限	是否危险	类型	详细情况
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.MOUNT_FORMAT_FILESYSTEMS	危险	格式化外部存储器	允许应用程序格式化可移动存储
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_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_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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
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.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

向手机申请的权限	是否危险	类型	详细情况
android.hardware.sensor.accelerometer	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.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.RECEIVE_USER_PRESENT	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.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

向手机申请的权限	是否危险	类型	详细情况
com.huawei.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.action.UPDATE_BADGE	未知	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
android.permission.READ_APP_BADGE	正常	显示应用程序通知	允许应用程序显示应用程序图标徽章
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。

向手机申请的权限	是否危险	类型	详细情况
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference
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
com.alpha.ecai335.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
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.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.INTERACT_ACROSS_USERS_FULL	未知	Unknown permission	Unknown permission from android reference
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: OU=tg
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-08-16 09:38:04+00:00
Valid To: 2044-08-09 09:38:04+00:00
Issuer: OU=tg
Serial Number: 0x4426a3d1
Hash Algorithm: sha256
md5: f3fa47860c70ab9d2b272a7c0208aaf3
sha1: 5ff8c02b1a993cbf794faa1e56d0c83f5a5b98fb

sha256: 257a40a06d8f6b63234e7b16f3cbfe3a398be4216b267840b4e1602e46fefde5
sha512: 41814d1f63430412f108a009bf02da6e38d16805e9b30cab3fb0b156d272648cbe9914d577d8a876f3e64424c8a21db61949e9641ef21e2b47aa9ebcc4131f61
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c7bc623031808aad3d07c3fe1fe1f14757fbded033acf50f5bae6b3cf57946fa

Exodus威胁情报

名称	分类	URL链接
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
WeChat Location		https://reports.exodus-privacy.eu.org/trackers/76

硬编码敏感信息

可能的敏感信息
"agent_add_user" : "新增会员"
"charge_bank_username" : "存款人姓名"
"chat_more_room_please_input_password" : "请输入房间密码"
"disable_modify_otheruser" : "不可跨及修改"
"forget_password" : "忘记密码"

可能的敏感信息
"input_pay_password" : "请输入支付密码"
"login_input_password" : "请输入密码"
"my_qrcode_user_name" : "邀请人： "
"odd_password" : "旧密码"
"password" : "密码"
"pref_default_value_account_private_chat" : "0"
"pref_key_account_admin" : "key_account_admin"
"pref_key_account_avatar" : "key_account_avatar"
"pref_key_account_balance" : "key_account_balance"
"pref_key_account_customer_service" : "key_account_customer_service"
"pref_key_account_nick_name" : "key_account_nick_name"
"pref_key_account_private_chat" : "key_account_private_chat"
"pref_key_account_realname" : "key_account_realname"
"pref_key_account_recommended_code" : "key_account_recommended_code"
"pref_key_account_talk" : "key_account_talk"

可能的敏感信息
"pref_key_account_token" : "key_account_token"
"pref_key_account_user_level" : "pref_key_account_user_level"
"pref_key_account_user_level_icon" : "key_account_user_level_icon"
"pref_key_account_user_phone" : "key_account_user_phone"
"pref_key_account_usercode" : "key_account_usercode"
"pref_key_account_userid" : "key_account_userid"
"pref_key_account_userlevel" : "key_account_userlevelname"
"pref_key_account_usertype" : "key_account_usertype"
"pref_key_agent_max_bonus_diff" : "key_agent_max_bonus_diff"
"pref_key_agent_user_manage_lower_authority" : "key_agent_user_manage_lower_authority"
"pref_key_api_lines" : "key_api_lines"
"pref_key_bet_cancel_order" : "key_bet_cancel_order"
"pref_key_bet_slips_preset_money" : "key_bet_slips_preset_money"
"pref_key_bet_total_limit" : "key_bet_total_limit"
"pref_key_betting_help_menu_visible" : "key_betting_help_menu_visible"

可能的敏感信息
"pref_key_betting_info_push" : "key_betting_info_push"
"pref_key_betting_random_show_guide" : "key_betting_random_show_guide"
"pref_key_betting_show_guide" : "key_betting_show_guide"
"pref_key_chat_room_customer_amount" : "key_chat_room_customer_amount"
"pref_key_chat_room_danmu" : "key_chat_room_danmu"
"pref_key_chat_room_global_banned" : "key_chat_room_global_banned"
"pref_key_chat_room_target_id" : "key_chat_room_target_id"
"pref_key_chat_room_top" : "key_chat_room_top"
"pref_key_config_web_site_url" : "key_config_web_site_url"
"pref_key_device_id" : "key_device_id"
"pref_key_enable_background_play" : "pref.enable_background_play"
"pref_key_enable_no_view" : "pref.enable_no_view"
"pref_key_enable_surface_view" : "pref.enable_surface_view"
"pref_key_expand_bonus_group_status" : "key_expand_bonus_group_status"
"pref_key_forbid_chat_red_packet" : "key_forbid_chat_red_packet"

可能的敏感信息
"pref_key_free_trial" : "key_free_trial"
"pref_key_free_trial_amount" : "key_free_trial_amount"
"pref_key_free_trial_set" : "key_free_trial_set"
"pref_key_game_account_auto_transform" : "key_game_account_auto_transform"
"pref_key_has_agree_jiebe" : "key_has_agree_jiebe"
"pref_key_has_agree_yuebao" : "key_has_agree_yuebao"
"pref_key_has_notice_auto_transform" : "key_has_notice_auto_transform"
"pref_key_has_set_betting" : "key_has_set_betting"
"pref_key_homepage_chat_room" : "key_homepage_chat_room"
"pref_key_homepage_show_guide" : "key_homepage_show_guide"
"pref_key_invitation_code" : "key_invitation_code"
"pref_key_is_open_banker" : "key_is_open_banker"
"pref_key_last_directory" : ""
"pref_key_line_name" : "key_line_name"
"pref_key_line_url" : "key_line_url"

可能的敏感信息
"pref_key_max_bonus_group_name" : "key_max_bonus_group_name"
"pref_key_media_codec_handle_resolution_change" : "pref.media_codec_handle_resolution_change"
"pref_key_min_bonus_group_name" : "key_min_bonus_group_name"
"pref_key_notification_close_tip" : "key_notification_close_tip"
"pref_key_pixel_format" : "pref.pixel_format"
"pref_key_platform_flag" : "key_platform_flag"
"pref_key_player" : "pref.player"
"pref_key_private_chat_notify" : "key_private_chat_notify"
"pref_key_red_bag" : "key_red_bag"
"pref_key_register_gift" : "key_register_gift"
"pref_key_register_gift_content" : "key_register_gift_content"
"pref_key_register_invitation_code" : "key_register_invitation_code"
"pref_key_register_lead_background" : "key_register_lead_background"
"pref_key_senior_betting" : "key_senior_betting"
"pref_key_server_red_bag" : "key_server_red_bag2"

可能的敏感信息
"pref_key_set_fund_password" : "key_set_fund_password"
"pref_key_simple_bet_menu_position" : "key_simple_bet_menu_position"
"pref_key_simple_betting_ksan_show_guide" : "key_simple_betting_ksan_show_guide"
"pref_key_third_games" : "key_third_games"
"pref_key_using_media_codec" : "pref.using_media_codec"
"pref_key_using_media_codec_auto_rotate" : "pref.using_media_codec_auto_rotate"
"pref_key_using_mediadatasource" : "pref.using_mediadatasource"
"pref_key_using_opensl_es" : "pref.using_opensl_es"
"pref_key_visitor_rong_yun_id" : "key_visitor_rong_yun_id"
"pref_key_visitor_rong_yun_name" : "key_visitor_rong_yun_name"
"pref_key_winning_notify" : "key_winning_notify"
"pref_key_yi_dun_captcha" : "key_yi_dun_captcha"
"pref_key_yubao_balance_show" : "key_yubao_balance_show"
"private_chat" : "发送消息"
"rc_authorities_fileprovider" : ".FileProvider"

可能的敏感信息
"rc_conversation_list_my_private_conversation" : "我的私人会话"
"rc_emoji_hear_no_monkey" : "不听"
"rc_emoji_see_no_monkey" : "不看"
"register_input_password" : "请输入登录密码(至少6位)"
"register_input_username" : "请输入用户名(须包含字母和数字)"
"setting_fund_password" : "资金密码"
"setting_login_password" : "登录密码"
"setting_private_chat_notify" : "私聊通知"
"token_invalid" : "登录过期，请重新登录"
"token_login_on_others" : "账号在其他设备登录，请重新登录"
"username" : "用户名"
"rc_conversation_list_my_private_conversation" : "My private conversation"
"rc_emoji_hear_no_monkey" : "Hear-No-Monkey"
"rc_emoji_see_no_monkey" : "See-No-Monkey"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.cp99.tz01.lottery.ui.activity.SplashActivity	Schemes: ecai335lottery://, Hosts: ecai335lottery,

加壳分析

文件列表	分析结果
classes.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>Build.MANUFACTURER check Build.BOARD check possible Build.SERIAL check SIM operator check subscriber ID check</td></tr><tr><td>编译器</td><td>r8</td></tr></table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
