关于通过一类 APP 实施刷单诈骗的预警及情况分析

摘要：本报告中对“刷单”诈骗的分析，来源于 2021 年 5 月 CNCERT/CC 对某一类“刷单”诈骗 APP 影响范围的监测分析。“刷单”诈骗是最近几年流行程度很高和受害者人数众多的一种网络诈骗模式。本报告首先给出“刷单”诈骗的典型套路，以及一类较为流行的“刷单”APP 的特征，然后给出互联网上此类 APP 影响面的统计分析。

一、通过“刷单”APP 实施诈骗的模式分析

该诈骗模式是 CNCERT/CC 在对一类“刷单”APP 进行跟踪监测的过程中总结出来的。此类“刷单”诈骗的典型模式如图 1 所示：

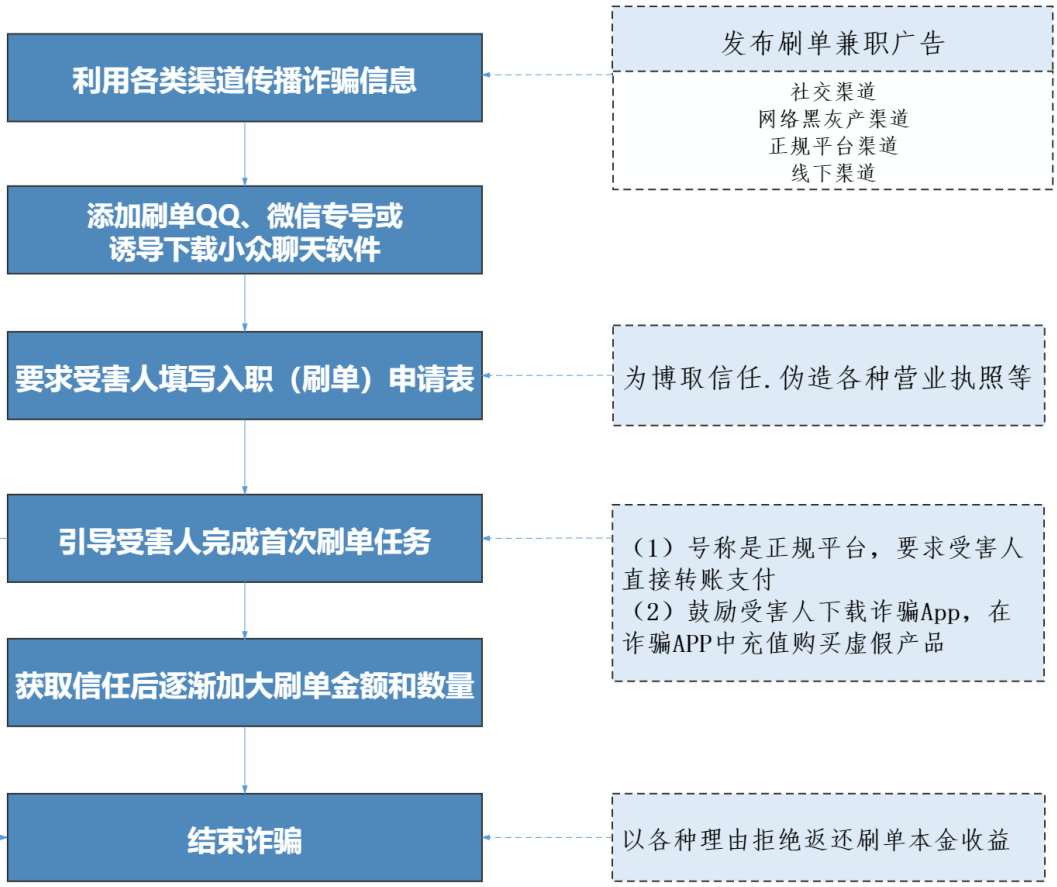

图 1 典型的通过“刷单”APP 实施诈骗的模式

1、传播诈骗信息

诈骗分子利用短信、求职网站、QQ 群、微信等社交渠道以及网页弹窗、邮箱推广等其他多种渠道发布“刷单兼职”广告。广告中往往强调“安全无风险”，“不索要任何密码、验证信息”，并打着“高薪”、“轻松赚钱”等旗号来吸引受害人。

2、与受害人建立联系

受害人依据广告信息联系诈骗分子后，诈骗分子会要求其添加刷单 QQ、微信号，或诱导受害人下载某些相对小众聊天软件，并通过聊天软件指导受害人进行“刷单”。而诈骗分子为骗取受害人信任，还会伪造各种营业执照、企业注册文件、后台交易记录等内容。受害人同意“兼职”后，诈骗分子会首先要求受害人提交入职（刷单）申请表，填写姓名、年龄等信息。

3、诱导受害人首次刷单

诈骗分子会诱导受害人访问“刷单”APP，要求受害人在此类 APP 中充值，购买虚假产品，引导受害者完成首次刷单并支付一定的佣金。之后诈骗分子会根据受害人具体情况决定是否实施进一步诈骗。

4、控制受害人，完成诈骗

完成首次“刷单”后，诈骗分子将低价商品改为高价商品，由“一单一返”改成“多单返利”，必须全部完成才能返还本金和收益。然后鼓励受害人加大刷单的金额和数量，当受害人完成订单要求返利时，骗子会以“任务未完成”、“操作不规范”、“未收到付款”、“提现额度调整”等各种借口，拒绝按照约定返还本金和收益，并不断要求受害人继续刷单，或直接关闭“刷单”APP 的使用。

二、一类流行的“刷单”诈骗 APP 介绍

针对以上描述的刷单诈骗模式，CNCERT/CC 监测发现有一类相似功能的 APP 在众多刷单诈骗事件中出现。

1、在传播诈骗信息阶段，诈骗分子会在各种平台投放“刷单”广告（典型的诈骗传播途径如图 2 所示）。

图 2：典型诈骗传播途径

2、受害人初步受骗后，诈骗分子会向受害人发送“刷单”APP 的登录链接（典型的登录页面如图 3 所示），并要求受害人通过其提供的邀请码注册此类刷单 APP（典型的注册页面如图 4 所示）。

图 3 典型的刷单 APP 的登录页面

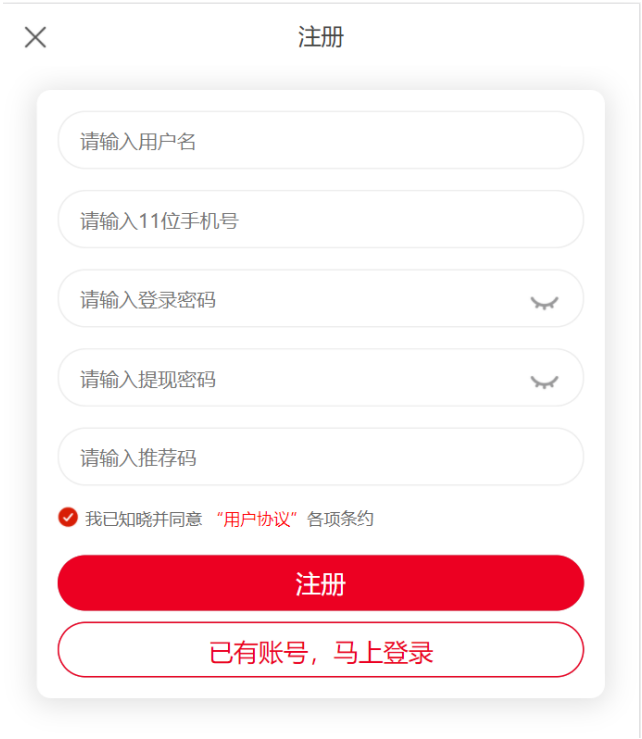

图 4 此类 APP 的注册页面

3、受害人完成注册后，即可登录此类 APP。在 APP 中会提供大量虚假商品信息和引导性较强的话语，引导受害人不断进行“刷单”。此类 APP 登录后的信息如图 5 和图 6 所示：

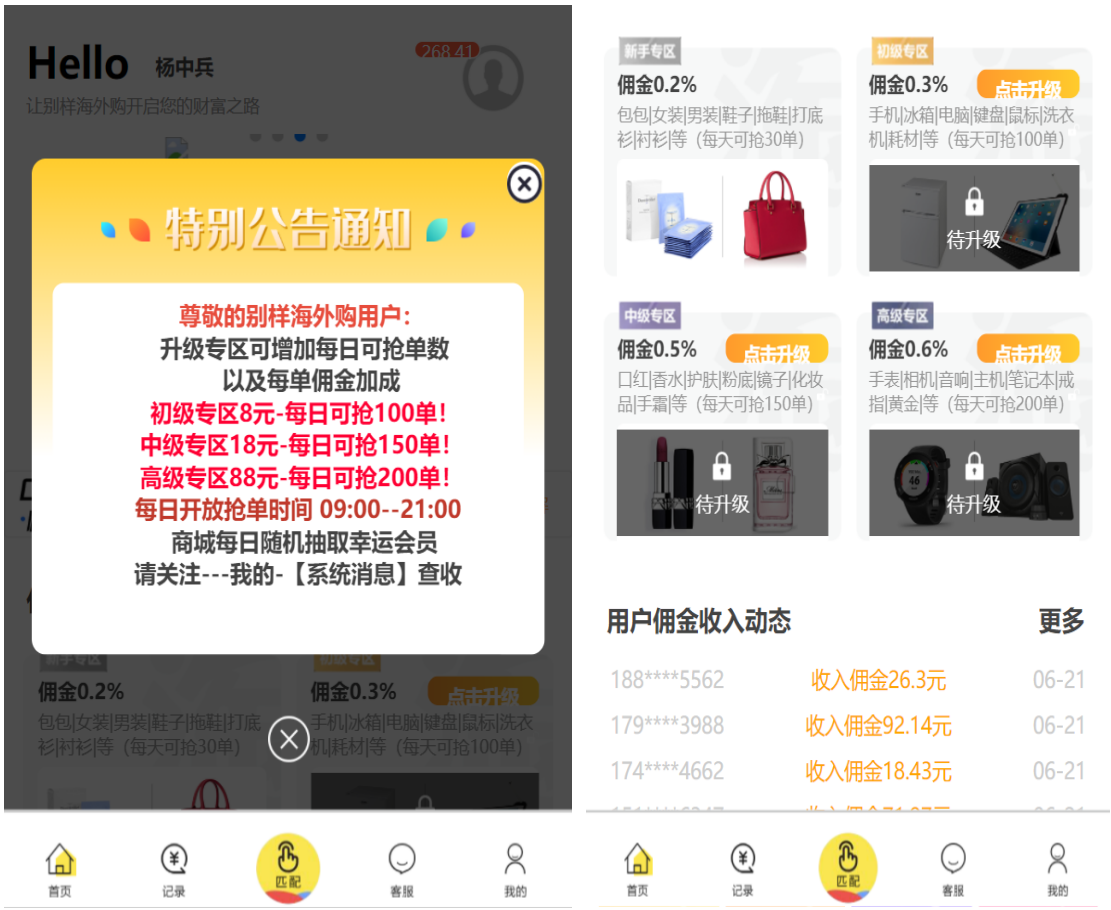

图 5 刷单 APP 首页提示语和虚假信息

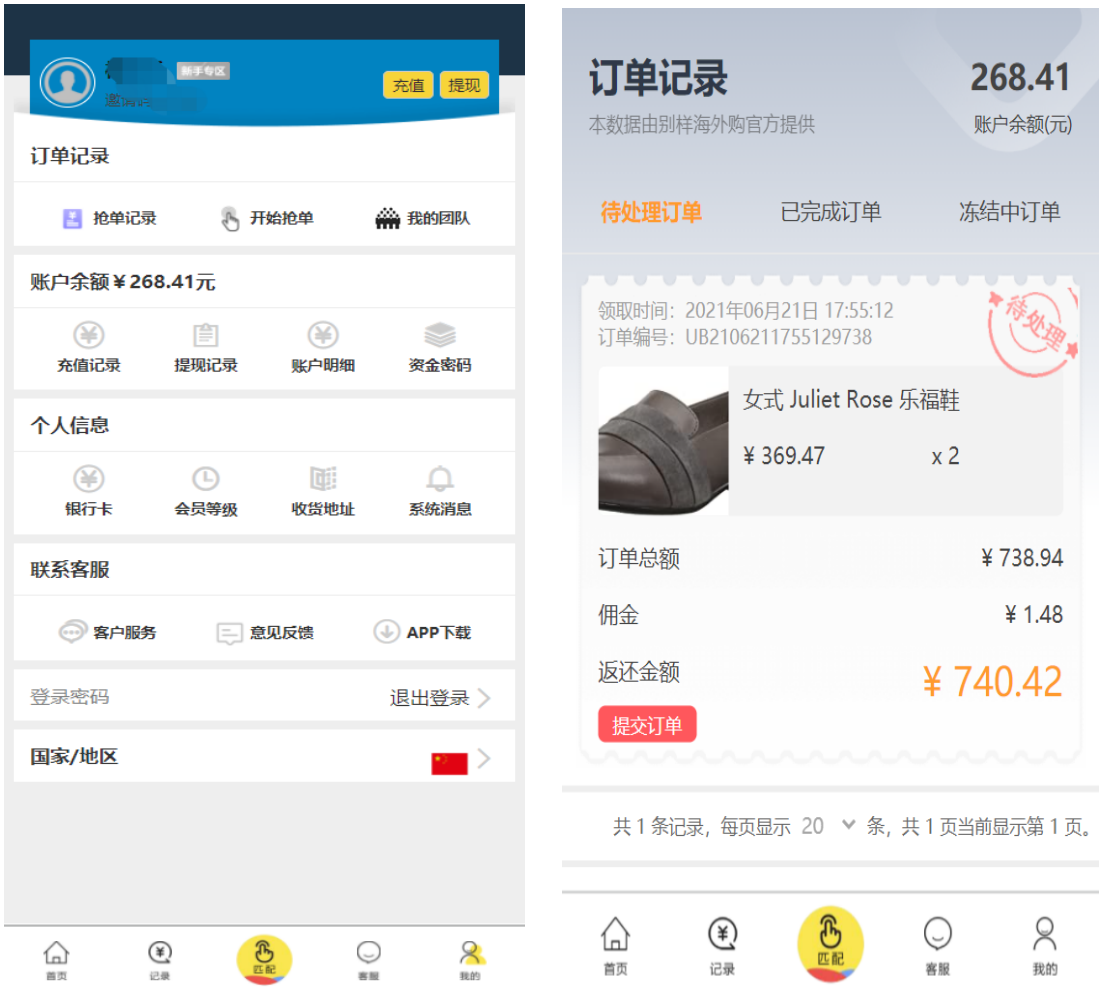

图 6 用户个人账户、订单详情页面

三、2021 年 5 月“刷单”诈骗 APP 相关数据分析情况

1、对诈骗 APP 涉及到的 IP 域名分析情况

2021 年 5 月，CNCERT/CC 监测到的此类 APP 共涉及 2134 个诈骗主机地址。其中影响用户最多的三个刷单诈骗 APP 的主机地址为：154.**.**.18:8855、23.**.**.251、23.**.**.205，其影响的用户数分别为 2546、812、783 个。表 1 列出的是 2021 年 5 月影响用户数量最多的前 10 个诈骗 APP 的主机地址。

表 1：影响用户数量最多的前 10 个诈骗 APP 的主机地址

主机地址	影响用户数量
154. **. **. 18:8855	2546
23. **. **. 251	812
23. **. **. 205	783
qss. ****. com	584
156. **. **. 221	526

qbjz3. ****:8896	485
23. **. **. 14	465
137. **. **. 48	464
45. **. **. 238	411
kkl. ****. xyz	359

对诈骗 APP 的主机地址进行进一步分析，发现在某些二级域名上，存在多个子域名均用于承载不同诈骗 APP 情况。***life. com、***ses. com、***band. com，这三个域名上拥有最多的实施刷单诈骗的子域名，分别为 85、34、27 个。表 2 统计的是在 2021 年 5 月拥有实施刷单诈骗子域名数量最多的前 10 个二级域名。

表 2：拥有实施刷单诈骗子域名数量最多的前 10 个二级域名

二级域名	子域名数量
***life. com	85
***ses. com	34
***band. com	27
***zv0. cn	26
***zz0g. cn	19
***5k5a. cn	18
***yuan. me	16
***06. cn	16
***fga. cn	15
***90. cn	15

2021 年 5 月，CNCERT/CC 发现的 2134 个“刷单”诈骗主机地址中，有 415 个的主机地址为 IP 或 IP 加端口，其余 1719 个诈骗主机地址有相关联的诈骗域名。在这 1719 个相关联诈骗域名中，顶级域分布如表 3 所示。其中.com，.cn 顶级域名出现最多，分别占 44.9%以及 20.5%，此外，.xyz，.top 等顶级域名也不在少数。

表 3：顶级域出现次数

顶级域	出现次数
com	771
cn	353
xyz	251
top	166
vip	27
cc	24
shop	18
me	17

pw	16
work	15

2021 年 5 月，监测发现的 2134 个刷单诈骗 APP 共涉及到 877 个刷单诈骗服务器 IP。中国香港的诈骗服务器 IP 最多，有 430 个，占比为 49%；其次为美国，有 145 个，占比为 16.5%。在所发现的刷单诈骗服务器 IP 中，有 660 个 IP 属于 IDC 机房类型 IP，占所发现诈骗服务器 IP 的 75.3%。图 7 为诈骗服务器 IP 的地理位置分布情况。

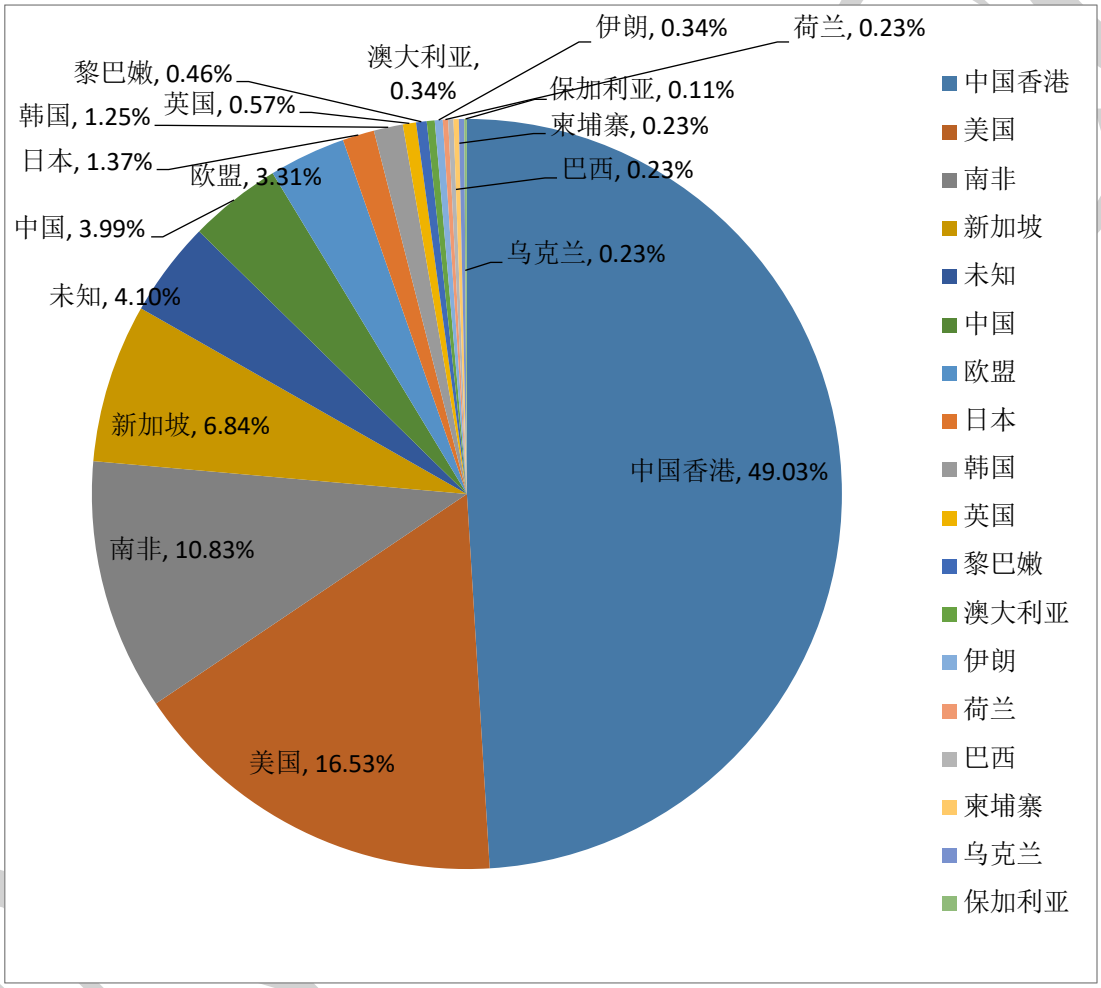

图 7：诈骗服务器的地理位置分布

部分诈骗服务器 IP 上承载着多个诈骗域名，下表为承载诈骗域名数量最多的前 10 个诈骗服务器 IP 地址。

表 4：诈骗服务器 IP 上承载的诈骗域名数量

诈骗服务器 IP	承载域名数量
155. **. **. 51	121
155. **. **. 165	107
185. **. **. 198	85

156. **. **. 205	37
118. **. **. 63	34
47. **. **. 248	33
45. **. **. 122	24
23. **. **. 114	22
45. **. **. 21	21
156. **. **. 138	21

2、对疑似诈骗 APP 的管理员行为分析情况

CNCERT/CC 持续对影响用户数量多的刷单诈骗 APP 进行监测，尝试跟踪发现其管理员行为。下表展示的是某几个可监测到管理员行为的刷单诈骗 APP 情况。

表 5：监测到管理员行为的诈骗 APP

诈骗域名	诈骗服务器 IP	诈骗服务器国家归属	影响用户数量
ab.****.net	47.**.**.248	美国	316
137.**.**.48	137.**.**.48	美国	246
qss.****.com	27.**.**.69	中国香港	224
116.**.**.106	116.**.**.106	中国香港	213
wx.****.top	173.**.**.204	美国	197
***zhuan.xyz	137.**.**.48	美国	195

CNCERT/CC 监测发现有 132 个疑似管理员 IP 访问过这 6 个诈骗 APP，下图为 132 个疑似管理员 IP 的地理位置分布情况。

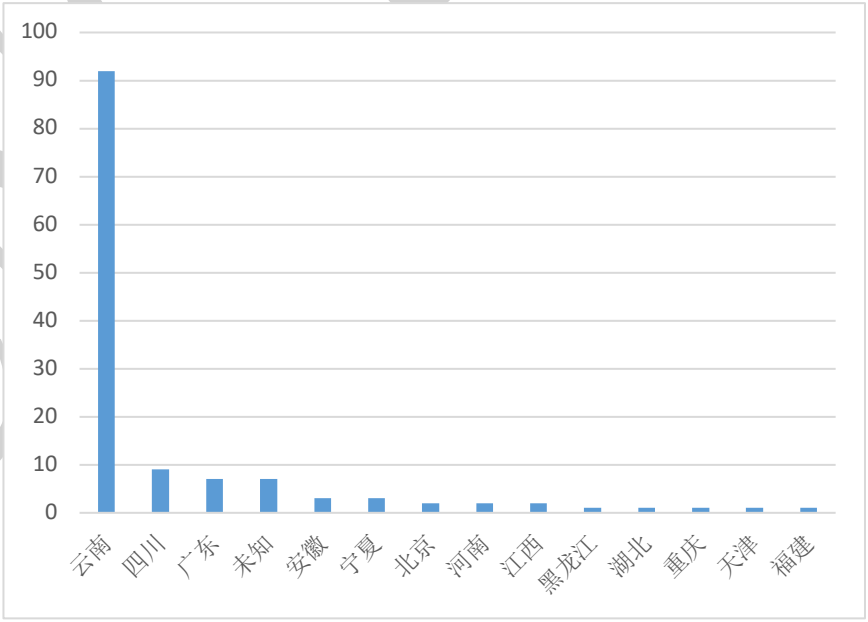

图 8：疑似管理员 IP 分布情况

3、对诈骗 APP 的受害人分析情况

2021 年 5 月，CNCERT/CC 共监测发现同有 26257 个受害人 IP 注册和登录了此类 APP。从受害人的地理位置归属来看，广东、河南、山东受害用户数量最多,考虑和经济发展情况及人口数量。下图 9 为受影响用户的 IP 地理位置归属分布情况。

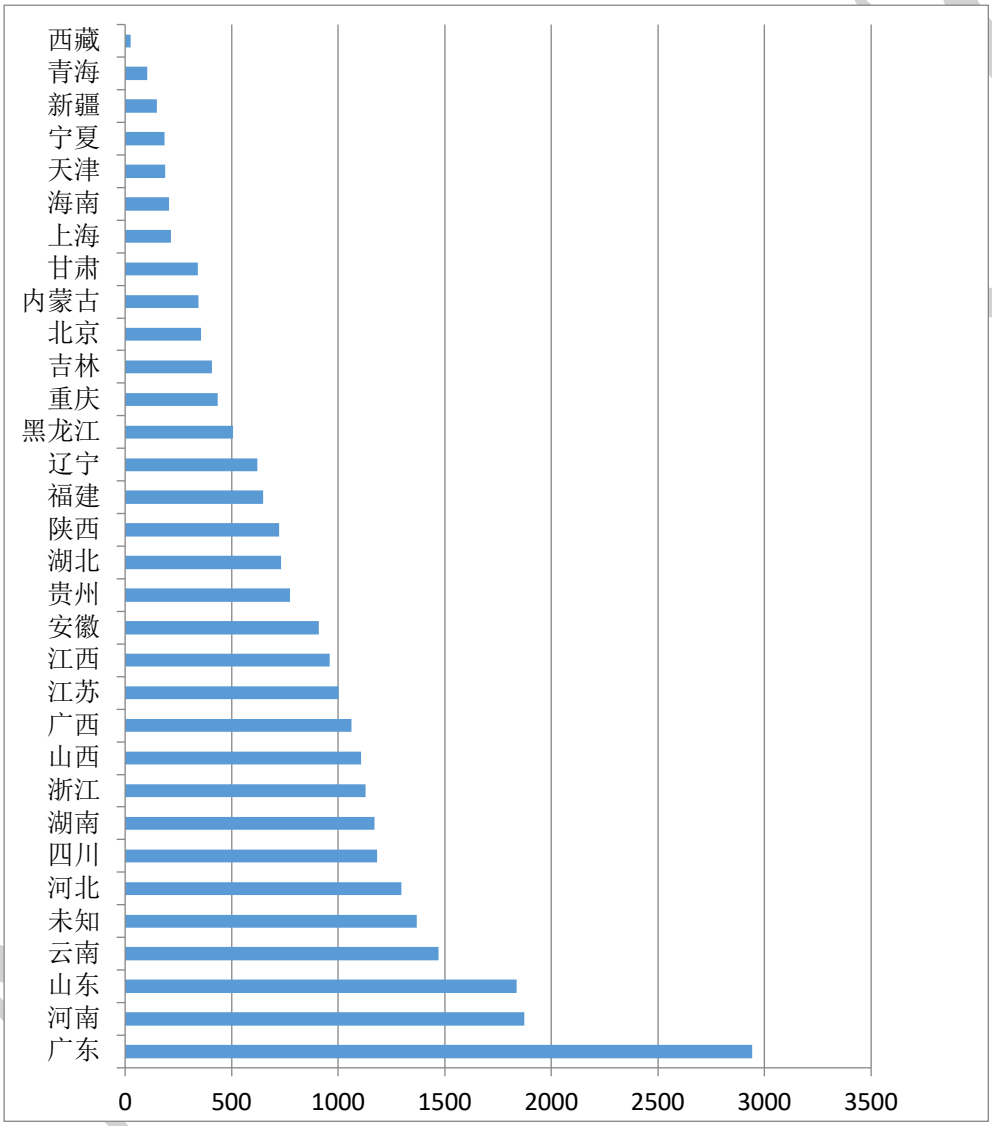

图 9 受害人分布情况